



وزارة التعليم العالي والبحث العلمي
جامعة محمد بوضياف بالمسيلة
كلية الحقوق والعلوم السياسية



المنشورات العلمية لكلية الحقوق والعلوم السياسية

مؤلف جماعي حول

مواجهة الجريمة المعلوماتية

إشراف الدكتور: الطيب بلواضح

أكتوبر 2019

مواجهة الجريمة المعلوماتية

أكتوبر 2019

ISBN:978-9961-9566-1-7

المنشورات العلمية لكلية الحقوق والعلوم السياسية

مؤلف جماعي بعنوان:

"مواجهة الجريمة المعلوماتية"

المنسق العام للمؤلف الجماعي:

الدكتور: الطيب بلواضح

أستاذ محاضر قسم (أ)

مسؤول فريق الاختصاص ماستر القانون الجنائي

رئيس فرقة بحث بمخبر الدراسات والبحوث في القانون والأسرة

والتنمية الإدارية

أكتوبر 2019

الناشر: كلية الحقوق والعلوم السياسية - جامعة محمد بوضياف بالمسيلة -
الجزائر

المقر الرئيس: مجمع كلية الحقوق والعلوم السياسية، طريق اشبيليا، المسيلة -
الجزائر

العنوان: كلية الحقوق والعلوم السياسية جامعة محمد بوضياف
ص ب: 166 اشبيليا - المسيلة - الجزائر

ملاحظة:

ما ورد في هذا المؤلف الجماعي من دراسات وأبحاث ومقالات وآراء وتقييمات يعبر عن آراء الكتاب أنفسهم ولا يعكس بالضرورة آراء ومواقف وتقييمات الكلية وجامعة المسيلة ووزارة التعليم العالي والبحث العلمي.

تنبيه:

جميع الحقوق محفوظة لكلية الحقوق والعلوم السياسية بجامعة المسيلة فلا يسمح بإعادة طباعة المؤلف الجماعي، و لا يجوز نسخ أي مادة منه، أو إعادة إنتاجها أو إعادة نشرها أو تخزينها في أنظمة استرجاع المعلومات أو استخدامها أو نقلها في أي صيغة أو بأي وسيلة، سواء كانت إلكترونية أو ميكانيكية، أو بوسائل التصوير الضوئي أو غيره، بدون تصريح مسبق صريح من عميد الكلية. هذا المؤلف ليس له أي غرض ربحي.

رقم الإيداع:

ISBN : 978-9961-9566-1-7

الرئيس الشرفي للمؤلف الجماعي:

الأستاذ الدكتور: كمال بداري

مدير جامعة محمد بوضياف بالمسيلة

مدير المؤلف مسئول النشر:

الدكتور: حمزة خضري

عميد كلية الحقوق والعلوم السياسية

المنسق العام للمؤلف الجماعي:

الدكتور: الطيب بلواضح

أستاذ محاضر قسم (أ)

مسؤول فريق الاختصاص ماستر القانون الجنائي

رئيس فرقة بحث بمخبر الدراسات والبحوث في القانون والأسرة والتنمية

الإدارية

tayeb.belouadah@univ-msila.dz

أعضاء الأمانة العامة: (التحرير القراءة و التحكيم)

د. حمزة خضري (عميد الكلية) - د. بن عمير جمال الدين (نائب العميد
مكلف بالبحث العلمي وما بعد التدرج والعلاقات الخارجية) - د. حمزة
بوخروبة (نائب العميد مكلف بشؤون الطلبة والبيداغوجيا) - د. لجلط فواز
(رئيس المجلس العلمي للكلية) - د. والي عبد اللطيف (مسؤول ميدان
الحقوق والعلوم السياسية) - د. فاضلي سيد علي (رئيس اللجنة العلمية لقسم
الحقوق) - د. مهدي رضا (رئيس قسم الحقوق) - د. بن حميدوش نور الدين
(نائب رئيس القسم مكلف بالبحث العلمي).

كلمة عميد كلية الحقوق والعلوم السياسية

الدكتور / حمزة خضري

الزملاء الأساتذة الأعزاء؛

طلبي الأفاضل؛

الحمد لله وحده والصلاة والسلام على من لا نبي بعده؛

وبعد ها نحن على بركة الله وعونه نتمكن، وبفضل جهود الأسرة الجامعية من أساتذة و طلبة دكتوراه و مختصين في القانون من مختلف المراكز و الجامعات الجزائرية، وبمبادرة من الدكتور الطيب بلواضح، (أستاذ محاضر "أ"، ومسؤول فريق التخصص - ماستر قانون جنائي، و رئيس الملتقى الوطني الموسوم بـ "مواجهة الجريمة المعلوماتية في ضوء التشريعات الجزائرية" المنعقد بتاريخ 06 مارس 2019) قلت نتمكن من إدراج مداخلات و مساهمات المشاركين في هذا الملتقى ضمن هذا المؤلف الجماعي برقم ايداع قانوني (ISBN) ضمن سلسلة المنشورات العلمية لكلية الحقوق والعلوم السياسية التي باشرنا بها منذ مئة، وليكون إضافة علمية جديدة للمكتبة القانونية على مستوى كليات الحقوق على امتداد تراب الجمهورية، وليكون تحت تصرف الطالب الباحث في القانون.

لقد اعتمدت كليتنا سياسة التشجيع والأخذ بيد كل هيئة علمية (لجنة علمية، مجلس علمي، ميدان، شعبة، تخصص)، وكل ما قد يأتي في شكل مبادرة نشر أو نشاط علمي يكون الهدف منه تنظيم نشاطات علمية -

تكوينية (ملتقيات وطنية و/أو دولية ،ندوات وأيام دراسية، ورشات متخصصة)، أو النشر العلمي المنتظم (عن طريق الانترنت وبوابة التعليم الجامعي و كذلك تسهيل نشر الدروس والمحاضرات بواسطة MOODLE -MOOC ، و التشجيع المتواصل للنشر الورقي المحكّم (مجلات الكلية – مجلة الأستاذ الباحث، ومجلة الدراسات والبحوث القانونية)، أو المبادرة بإنجاز مؤلفات جماعية تخص القانون والعلوم السياسية.

الزملاء الأعزاء؛ لن نلّخر جهداً إلا وبذلناه في سبيل الإرتقاء بجامعتنا إلى أعلى المراتب العالمية وسندنا في ذلك الدعم المعنوي والأدبي الموفّر لنا من السيّد مدير الجامعة الأستاذ الدكتور كمال بداري.

آمل أن تتضاعف الجهود، من أجل المزيد من النشر العلمي المتخصص و المتنوع في العلوم القانونية و السياسية، عبر وسائط النشر الالكتروني التي تسمح بإزدياد مقروئية أنشطتنا العلمية، وتتقدم جامعتنا إلى أرقى المراتب على المستويين الوطني والدولي.

تقديم المشرف على المؤلف الجماعي:

أعزاءنا ممن هم مهتمون بمستجدات البحث العلمي في مجال القانون، ها نحن نقدم بين أيديكم هذا المؤلف الذي يندرج ضمن سلسلة منشورات كلية الحقوق والعلوم السياسية بجامعة محمد بوضياف بالمسيلة، المعنون بـ"مواجهة الجريمة المعلوماتية" والذي يهدف أساسا إلى الإحاطة بالجرائم المستحدثة وسبل مواجهتها، وذلك لما يعرفه عالمنا من تطور تكنولوجي رهيب وما ينتج عنه من مخاطر ومضار.

إن هذا المؤلف هو نتاج اختيار مجموعة من مداخلات ومساهمات السادة الأساتذة والباحثين الأفاضل من مختلف الجامعات الجزائرية ضمن فعاليات الملتقى الوطني الموسوم بـ"مواجهة الجريمة المعلوماتية في ضوء التشريعات الجزائرية" المنعقد بتاريخ 06 مارس 2019.

وحري بنا أن نتقدم بالشكر الجزيل إلى مدير الجامعة الأستاذ الدكتور بداري كمال على تشجيعه لنا وسعيه الدائم على تطوير جامعتنا في مجال النشر العلمي و الذي يعد معيارا من معايير تقدم الجامعات و رقيها، كما نخص عميد كلية الحقوق الدكتور حمزة خضري بالشكر والامتنان على الجهود الذي بذلها لتسخير كل الإمكانيات التي من شأنها أن تدفع كليتنا إلى المضي قدما في مجال البحث العلمي.

الدكتور/ الطيب بلواضح

الفهرس

- 11 نشأة وخصائص الجريمة المعلوماتية.
د.مبروك عبد النور — جامعة المسيلة
ط.د.نورالدين أعلي سالم محمد فاضل — جامعة المسيلة
- 23 الجريمة المعلوماتية: في إطار ماهيتها وأنواعها.
د.ضريفي نادية — جامعة المسيلة
ط.د.بن طاية زوليخة — جامعة بسكرة
- 34 تعريف وأركان الجريمة المعلوماتية في ظل الفقه والتشريع المقارن والجزائري
ط.د.بن لقريشي مصطفى — جامعة المسيلة
د.ميهوبي حورية — جامعة المسيلة
- 47 خصوصية الجريمة المعلوماتية - المفهوم والأركان.....
ط.د.فايدة صابر — جامعة برج بوعريرج
ط.د.لعشاش حمزة — جامعة المسيلة
- 58 الجريمة المعلوماتية ودوافع ارتكابها في التشريع الجزائري
د.بن حليلة ليلي — جامعة المسيلة
د.عشور سليم — جامعة المسيلة
- 74 واقع الجريمة المعلوماتية ومكافحتها بموجب التشريع الجزائري
أ.بوعكة الكاملة — جامعة المسيلة
- 86 الجريمة المعلوماتية بين ضيق النص التجريبي و إتساع السلوك الإجرامي
د.بوقرة العمريّة — جامعة المسيلة
أ.عثماني مريم — جامعة خنشلة
- 108 التنظيم القانوني للجريمة المعلوماتية
د.غضبان سمية — جامعة المسيلة
د.محمد حميد — جامعة الجلفة
- 124 خصوصية المجرم المعلوماتي
أ.يرمش مراد — جامعة المسيلة

- 132 تطور الجريمة المعلوماتية
 ط.د. سبع جميلة - جامعة تيزي وزو
 ط.د. مشان عبد الكريم - جامعة المسيلة
- 140 وسائل التحقيق الجنائي في الجرائم الرقمية
 أ.د. شرون حسينة - جامعة بسكرة
 أ. زينب خذير - جامعة غرداية
- 158 القواعد الإجرائية الحديثة لمواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال
 د. إلهام بن خليفة - جامعة الوادي
- 178 الجوانب الإجرائية لمواجهة الجريمة المعلوماتية في التشريع الجزائري
 د. مهدي رضا - جامعة المسيلة
 د. رفاف لخضر - جامعة برج بوعريش
- 187 التدابير الإجرائية الخاصة لمواجهة جريمة المساس بأنظمة المعالجة الآلية للمعطيات
 د. والي عبد اللطيف - جامعة المسيلة
 أ. عمارة عمارة - جامعة المسيلة
- 198 مراقبة الاتصالات الإلكترونية ودورها في مواجهة الجريمة المعلوماتية
 د. مجاوي لعل - جامعة باتنة¹
 ط.د. سويح دنيا زاد - جامعة باتنة¹
- 210 مراقبة المراسلات والاتصالات الإلكترونية كأسلوب للتحقيق في الجرائم
 المعلوماتية
 د. روابح فريد - جامعة سطيف
- 241 إجراء التفتيش وضبط الأدلة في الجريمة المعلوماتية
 د. جلول فواز - جامعة المسيلة
 ط.د. بوعايدة كمال - جامعة الجزائر
- 253 إجراءات التحقيق الجنائي في الجريمة الإلكترونية
 د. بلعيد جميلة - جامعة المسيلة
- 271 إجراءات التحقيق الخاصة بالجرائم الإلكترونية
 ط.د. تباري السعيد - جامعة المسيلة

- 282 التفتيش و ضبط الأدلة كآليتين فعاليتين للتحقيق في الجرائم المعلوماتية
ط.د. كرازدي سارة - جامعة المسيلة
- 299 الجرائم الماسة بنظام المعالجة الآلية للمعطيات وأطر مكافحتها في قانون العقوبات
الجزائري
د. قسمية محمد - جامعة المسيلة
- 315 جريمة الإرهاب الإلكتروني
د. بوقرين حليم - جامعة الأغواط
ط.د. بدارني أحمد - جامعة غرداية
- 335 مواجهة جريمة الإرهاب الإلكتروني في ظل القانون رقم 16 - 02 المتمم للأمر رقم
66 - 156 والمتضمن قانون العقوبات
د. مسعودان فتيحة - جامعة بجاية
- 348 صعوبات الإثبات الجنائي في الجريمة المعلوماتية
د. بلواضح الطيب - جامعة المسيلة
ط.د. الذهبي خليفة - جامعة المسيلة
- 363 المبادئ التي تحكم مقبولية الأدلة الجنائية الرقمية أمام القضاء الجزائري
ط.د. طاهري عبد المطلب - جامعة الأغواط
- 374 القيمة الإثباتية للدليل الجنائي الإلكتروني
د. طيب عمور محمد - جامعة الشلف
- 394 إشكالية الحصول على الدليل الجنائي في الجرائم المعلوماتية
ط.د. فلاك مراد - جامعة أم البواقي
- 413 إجراءات الإثبات في الجريمة المعلوماتية
ط.د. أكرم فراحتية - جامعة المدية
ط.د. سامي كباهم - جامعة خميس مليانة
- 430 مكانة الدليل الإلكتروني في الإثبات الجزائي
د. بن حميدوش نور الدين - جامعة المسيلة
ط.د. رحومني عبد الرزاق - جامعة المسيلة

- 441 مدى خضوع الدليل الرقمي للقواعد المقررة للإثبات الجنائي
د. راجحي لخضر - جامعة الأغواط
ط. د. بومسلة عبد القادر - جامعة سوسة - تونس
- 452 مدى اقتناع الشخصي القاضي الجزائري بالأدلة الجنائية الحديثة
ط. د. حمادي محمد رضا - جامعة أدرار
ط. د. قنقارة سليمان - جامعة بشار
- 469 مكافحة الجرائم المعلوماتية الماسة بالأخلاق والآداب العامة وأولويات السياسة الجنائية
للدولة
د. بوشكيوة عبد الحليم - جامعة جيجل
- 491 الجريمة الالكترونية و أولوية حماية الحلقة الضعيفة (الطفل) في القانون الجزائري ..
عبد المجيد صغير بيرم - جامعة المسيلة
- 508 الجريمة الالكترونية في الجزائر: الواقع، المأمول وآليات المجابهة
د. إبرادشة فريد - جامعة المسيلة
أ. عامر هني - جامعة المسيلة
- 524 مظاهر القصور عن مواجهة الجريمة المعلوماتية - الحالة الجزائرية نموذجاً
د. ذبيح مولود - جامعة المسيلة
- 532 آليات مكافحة الجريمة المعلوماتية في النظام المصرفي الجزائري
ط. د. دبش رياض - جامعة سطيف
- 544 معوقات التحقيق في الجرائم المعلوماتية الدولية وسبل مواجهتها
د/ حيزوم بدر الدين مرغني - جامعة الوادي
د. مقروف محمد - جامعة المسيلة
- 558 مكافحة الجريمة المعلوماتية في إطار منظمة مجلس أوروبا
د. براهيم السعيد - جامعة برج بوعريج
- 566 فعالية التعاون الدولي في مواجهة الجريمة المعلوماتية
د. وهي المختار - جامعة المسيلة

نشأة وخصائص الجريمة المعلوماتية

ط.د/ نورالدين أعلي سالم محمد فاضل

كلية الحقوق والعلوم السياسية

جامعة المسيلة

د/ مبروك عبد النور

أستاذ محاضر (أ) - كلية الحقوق والعلوم

السياسية - جامعة المسيلة

مقدمة:

تعتبر الجريمة المعلوماتية من أهم القضايا التي تقلق رجال الفكر القانوني في الوقت الحاضر، فقد انتشر الكمبيوتر في حياتنا اليومية فمعظم المجالات الحيوية أصبحت تعتمد عليه وادي هذا التطور إلى ظهور مفاهيم جديدة من بينها شبكة الانترنت التي أصبحت العصب الرئيسي للثورة المعلوماتية، وأصبح كل بعيد قريب فأضحى العالم قرية صغيرة.

فالانترنت هي نتاج دمج ما بين الكمبيوتر والاتصالات ظهرت الانترنت سنة ألف وتسعمائة وثلاثة وستون عندما قامت وكالة مشروع الأبحاث المتقدمة التابعة لوزارة الدفاع الأمريكي، بإنشاء شبكة حواسيب لوصول الإدارة والجامعات، ثم تطورت إلى أن تم ظهور شبكة الانترنت حكرًا على أناس معينين. رفع هذا الاحتكار فوصلت إلى كل مكان في العالم خصوصًا عندما استخدمت الخط الهاتفي والأقمار الصناعية في البث.

ومنه: ما هي مفهوم الجريمة المعلوماتية ؟ وما أسباب أوقوعها؟

المبحث الأول: التطور التاريخي ومفهوم جرائم الكمبيوتر والانترنت

سوف نتطرق في هذا المبحث إلى مطلبين هما:

المطلب الأول: التطور التاريخي لجرائم الكمبيوتر والانترنت

مرت جرائم الإنترنت بتطور تاريخي تبعًا لتطور التقنية واستخداماتها، ولهذا مرت بثلاث مراحل:

المرحلة الأولى:

مع شيوع استخدام الحواسيب في الستينات و السبعينات اقتضت المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر، وترافقت هذه النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم مجرد شئ عابر أم ظاهرة إجرامية مستحدثة، وأن الجدل حول ما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في بيئة أو مهنة الحوسبة،

ومع تزايد استخدام الحواسيب الشخصية في السبعينات ظهرت عدد من الدراسات المسحية والقانونية التي اهتمت بجرائم الكمبيوتر وعالجت عددا من قضايا الجرائم الفعلية، وبدأ الحديث عنها بوصفها ظاهرة إجرامية لا مجرد سلوكيات مرفوضة.¹

المرحلة الثانية:

في الثمانينات طفا على السطح مفهوم جديد لجرائم الكمبيوتر والانترنت ارتبطت بعمليات اقتحام نظام الكمبيوتر عن بعد وأنشطة نشر وزرع الفيروسات الالكترونية التي تقوم بعملية تدميرية للملفات أو البرامج شاع اصطلاح «الهاكرز» المعبر عن مقتحمي النظم، لكن الحديث عن الدوافع لارتكاب هذه الأفعال ظل محصورا في رغبة المحترفين تجاوز امن المعلومات وإظهار تفوقهم التقني، لكن هؤلاء المغامرون أصبحوا أداة إجرام، وظهر المجرم المعلوماتي المتفوق المدفوع بأغراض إجرامية خطيرة القادر على ارتكاب أفعال تستهدف الاستيلاء على المال أو التجسس أو الاستيلاء على البيانات السرية والاقتصادية الاجتماعية والسياسية والعسكرية.

المرحلة الثالثة:

شهدت التسعينات تناميا هائلا في حقل الجرائم الالكترونية، وتغيرا في نطاقها ومفهومها وكان ذلك بفعل ما أحدثته شبكة الإنترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكة المعلومات ظهرت أنماط جديدة إنكار الخدمة التي تقوم على فكرة تعطيل نظام تقني ومنعه من القيام بعمله المعتاد وأكثر ما مورست ضد مواقع الانترنت التسويقية الهامة التي يتسبب انقطاعها عن الخدمة لساعات في خسائر مالية بالملايين.

ونشطت جرائم نشر الفيروسات عبر المواقع الالكترونية لما تسهله من انتقالها إلى ملايين المستخدمين في ذات الوقت، وظهرت الرسائل المنشورة على الانترنت أو المراسلة بالبريد الالكتروني المنطوية على إثارة الأحقاد أو المساس بكرامة واعتبار الأشخاص أو المروجة لمواد غير القانونية أو غير المشروعة. رغم تزايد الأبحاث ومحاولات ابتكار أنظمة تكفل لأي كمبيوتر الحماية اللازمة، إلا أنه في المقابل يتم تطوير الإجراءات المضادة لهذه الحصون الأمنية، ومعنى ذلك أن خطر انتهاك أمن وسلامة الكمبيوتر مستمرة مدى استمرارية هذه التحصينات.

¹ بن داعس فيصل، إشكالات الجريمة المعلوماتية في التشريع الجزائري، محاضرة في إطار التكوين المحلي المستمر

للقضاة، 2011، ص 02.

وقد يكون الكمبيوتر في مجال ارتكاب الجرائم هدفا للجرائم للجريمة أو أداة لارتكابها أو مسرحا لها. وقد يكون الكمبيوتر دورا رئيسيا في حقل اكتشاف الجريمة.

ونعرض فيما يلي لأدوار الكمبيوتر والانترنت في مجال ارتكاب الجريمة واكتشافها:

أ- قد يكون الكمبيوتر هدفا للجريمة: ويتحقق ذلك في حالة الدخول غير المصرح به إلى النظام أو زراعة الفيروسات لتدمير المعطيات و الملفات المخزنة أو تعديلها، وكما في حالة الاستيلاء على البيانات المخزنة أو المنقولة عبر النظم.¹

وتوجه هجمات إلى معلومات كمبيوتر أو خدماته قصد المساس بالسرية أو سلامة المحتوى وتكاملته أو تعطيل القدرة والكفاءة للأنظمة للقيام بعملها، وهدفه هو المعلومات المخزنة بهدف السيطرة على النظام دون التصريح و دون دفع وتتضمن بعض طوائف هذا النمط أي كمبيوتر كهدف أنشطة للسرقة والاعتداء على الملكية الفكرية.

ب- قد يكون الكمبيوتر مكان للجريمة: كما في حالة استغلال الكمبيوتر للإستيلاء على الأموال بإجراء تحويلات غير شرعية استخدام التقنية في عمليات التزوير والتزييف، والاستيلاء على أرقام بطاقات الائتمان وإعادة استخدامها للاستيلاء على الأموال بواسطة ذلك.

ج- قد يكون الكمبيوتر أداة للجريمة: وذلك كما في حالة تخزين البرامج المنسوخة أو في حالة استخدامه لنشر المواد الغير قانونية أو استخدامه أداة لتخزين أو اتصال بصفقات ترويج المخدرات وأنشطة الشبكات الإباحية ونحوها.²

المطلب الثاني: ماهية الجريمة المعلوماتية

إن الجريمة المعلوماتية باعتبارها جريمة مستحدثة أثارت ضجة في الأوساط الفقهية من حيث مفهومها والأفعال الإجرامية التي تدخل نطاقها، وهو ماستتناوله:

¹ علاء رضوان، الجريمة المعلوماتية من النشأة في الستينيات إلى «القرصنة» في القرن الـ21، مقال منشور في الانترنت يوم 16 نوفمبر 2018 على الساعة 12:00، ص 02.

² علاء رضوان، الجريمة المعلوماتية من النشأة في الستينيات إلى «القرصنة» في القرن الـ21، مقال منشور في الانترنت يوم 16 نوفمبر 2018 على الساعة 12:00، ص 03.

أولاً: مفهوم الجريمة المعلوماتية

عصر الانترنت أو عصر السموات المفتوحة أو التكنولوجيا الرقمية أو عصر المعلوماتية، كل هذه الأوصاف إنما تعبر عن مدى ضخامة القفزات العلمية الهائلة التي تحققت ومدى تنوع الانجازات التي طرحت ثمارها بشكل ملحوظ في حياتنا في الآونة الأخيرة.¹

ويبدو بالفعل أن تكنولوجيا المعلومات هي وقود الثورة الصناعية الثالثة، وأن المعلومات في حد ذاتها هي المادة الخام الأساسية للإنتاج التي يعتمد المجتمع على إنتاجها وإيجادها والاستفادة منها. وفي الواقع إن هذا الوجه المشرق لتقنية المعلومات يخل من الجانب المظلم الذي تمثل في الإجرام المعلوماتي والذي كان موجودا ليستغل هذه التقنيات المتطورة لتحقيق مصالح ومآرب متنوعة وتعدد.

ثانياً: تعريف الجريمة المعلوماتية

بداية لابد أن نشير إلى أنه لا يوجد مصطلح قانوني موحد للدلال على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها فالبعض يطلق عليها جريمة الغش المعلوماتي، والبعض الآخر يطلق عليها جريمة الاختلاس المعلوماتي أو الاحتيال المعلوماتي، وآخرون يفضلون تسميتها بالجريمة المعلوماتية.

وهناك جانب يرى أن هذه الجريمة ناشئة أساساً من التقدم التكنولوجي، ومدى التطور الذي يطرأ عليه وهو متجدد بصفة دائمة ومستمرة وخاصة في مجال تكنولوجيا المعلومات، ويفضل أن يطلق عليها اصطلاحاً جرائم التكنولوجيا الحديثة فهي جرائم تكنولوجيا باعتبارها مرتبطة ارتباطاً وثيقاً بالتكنولوجيا التي تعتمد أساساً على الحواسيب وغيرها من الأجهزة التقنية التي قد تظهر في المستقبل، وهي كذلك جرائم حديثة نظراً لحداثتها النسبية من ناحية ارتباطها الوثيق بما قد يظهر من أجهزة حديثة تكون ذات طاقة تخزينية وسرعة فائقة ومرونة في التشغيل.²

في إطار تعريف الفقه للجريمة المعلوماتية نجد أن الاتجاهات تباينت في هذا السياق بين موسع لمفهوم الجريمة المعلوماتية وبين مضيق لمفهومها.

¹ أحمد هلالى عبد اللاء، الجوانب الموضوعية والاجرائية لجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة، 2002، ص 12.

² عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، ط1، بدون ناشر، 2000، ص 4

فمن التعريفات المضيقه لمفهوم الجريمة المعلوماتية تعريفها على أنها: كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازماً لارتكابه من ناحية لملاحقته وتحقيقه من ناحية أخرى.¹ وفي المقابل هناك تعريفات حاولت التوسع في مفهوم الجريمة المعلوماتية فعرّفها البعض أنها: كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الاعتداء على الأموال المادية أو المعنوية.

المبحث الثاني: أسباب وخصائص الجريمة الإلكترونية وخصائصها

قسمنا مبحثنا هذا الى:

المطلب الأول: أسباب الجريمة الإلكترونية وخصائصها

لاشك أن فئات مرتكبي الجريمة المعلوماتية تختلف عن مرتكبي الأفعال الإجرامية التقليدية، لذا من الطبيعي أن نجد نفس الاختلاف في الأسباب والعوامل التي تدفع في ارتكاب الفعل غير المشروع، فضلاً عن ذلك، تتمتع جرائم الكمبيوتر والمعلوماتية بعدد من الخصائص التي تختلف تماماً عن الخصائص التي تتمتع بها الجرائم التقليدية، كما أن الجاني الإلكتروني (أو المجرم الإلكتروني) يختلف أيضاً عن المجرم العادي.

ويأتي في مقدمة أسباب الجريمة المعلوماتية، غاية التعلم والتي تتمثل في استخدام الكمبيوتر والإمكانات المستحدثة لنظم المعلومات وهناك أمل الربح وروح الكسب التي كثيراً ما تدفع إلى التعدي على نظم المعلومات بالإضافة إلى الدوافع الشخصية والمؤثرات الخارجية التي قد تكون سبباً في ارتكاب الجريمة المعلوماتية.

- غاية التعلم:

يشير الأستاذ ليفي مؤلف كتاب قراصنة الأنظمة HACKERS إلى أخلاقيات هؤلاء القراصنة والتي تتركز على مبدئين أساسيين:

- 1- أن الدخول إلى أنظمة الكمبيوتر يمكن أن يعلمك كيف يسير العالم.
 - 2- أن جمع المعلومات يجب أن تكون غير خاضعة للقيود.
- وبناء على هذين المبدئين فإن أجهزة الكمبيوتر المعنية ما هي إلا آلات للبحث، والمعلومات بدورها ما هي إلا برامج وأنظمة معلومات.

¹ قورة نائلة، جرائم الحاسب الاقتصادية، دار النهضة العربية، القاهرة، 2003-2004، ص 21.

ومن وجهة نظر هؤلاء القراصنة فإن جميع المعلومات المفيدة بوجه عام يجب أن تكون غير خاضعة للقيود وبعبارة أخرى أن تتاح حرية نسخها وجعلها متناسب مع استخدامات الأشخاص. ويرى هؤلاء القراصنة إغلاق بعض نظم المعلومات وعدم السماح بالوصول إلى بعض المعلومات وخاصة بعض المعلومات السرية التي تخص الأفراد. ويعلق قراصنة الأنظمة أنهم يرغبون في الوصول إلى مصادر المعلومات والحاسبات الإلكترونية والشبكات بغرض التعلم.

وقد لاحظ كل من "ليفي" و "لاندريس" أن قراصنة الأنظمة لديهم الاهتمام الشديد بأجهزة الكمبيوتر والتعلم ويدخل العديد منهم في أجهزة الكمبيوتر على أنهم محترفين ويختار بعض القراصنة الأنظمة لتعلم المزيد عن كيفية عمل الأنظمة.

ويقول "لاندريس" أن هؤلاء القراصنة يرغبون في البقاء مجهولين حتى يتمكنوا من الاستمرار في التواجد داخل الأنظمة لأطول وق ممكن. ويكرس البعض منهم كل وقته في تعلم كيفية اختراق المواقع الممنوعة والتقنيات الأمنية للأنظمة حيث تتفاوت معرفتهم عن الأنظمة والبرمجة إلى حد بعيد. وكتب أحد قراصنة الأنظمة يقول: يكتشف قراصنة الأنظمة نقطة ضعف أمنية فيحاولون استغلالها لأنها موجودة بهدف عدم تخريب المعلومات أو سرقتها، أعتقد أن نقوم به يشبه قيام شخص باستكشاف أساليب جديدة للحصول على المعلومات من المكتبة فيصبح في غاية الإثارة والانهماك.¹

وينبغي ألا نستنهين بكفاءة الشبكات التي يتعلم من خلالها القراصنة حرفتهم. وهم يقومون بالفعل بالبحث واكتشاف الأنظمة والعمل من خلال الجماعة وتعليم بعضهم البعض. حيث ذكر أن قراصنة الأنظمة أنه ينتمي إلى مجموعة بحث مهمتها استخراج كميات كبيرة من المعلومات وتعلم أكبر قدر منها.

ويسعى أعضاء القراصنة إلى التخصص والتعاون في المشاريع البحثية وتقاسم البرامج والأخبار وكتابة المقالات وتعريف الآخرين بمجالات اختصاصهم ويدع قراصنة الأنظمة نظاماً خاصاً لمجال المعرفة

¹ قراصنة أنظمة الكمبيوتر إعداد: دورثي إي. دينغ ورقة مقدمة للمؤتمر القومي الثالث عشر لأمن الكمبيوتر، واشنطن، ترجمة: آمنة علي يوسف، ديسمبر 1998، ص 8.

الذي يجذبهم ويعلمهم التفكير ويسمح لهم بتطبيق ما تعلموه في أنشطة هادفة وإن لم تكن قانونية
دائمة:¹

- السعي إلى الربح:

أشارت إحدى المجالات المتخصصة في الأمن المعلوماتي securite informatique إلى الرغبة في تحقيق الثراء من بين العوامل الأساسية لارتكاب الجريمة المعلوماتية حيث أشارت:

- أن 43% من حالات الغش المعلن عنها قد بوشرت من أجل اختلاس الأموال.
- 23% من أجل سرقة المعلومات.
- 19% أفعال إتلاف.
- 15% سرقة وقت الآلة؛ أي الاستعمال غير المشروع للحاسب الآلي لأجل تحقيق أغراض شخصية.

لذا نجد أن الدافع لارتكاب الجريمة المعلوماتية يمكن أن تكون سببه مجرد سداد الديون المستحقة أو مشاكل عائلية راجعة للنقود أو إدمان ألعاب القمار أو المخدرات لذا فإن بيع المعلومات المختلسة هو نشاط متسع للغاية ويمكن أن نبين في هذا المجال واقعة استيلاء مبرمج يعمل لدى إحدى الشركات الألمانية على 22 شريطاً ممغنطاً تحوي معلومات هامة بخصوص عملاء وإنتاج هذه الشركة حيث هدد السارق ببيعها للشركات المنافسة ما لم تدفع له فدية مقدارها 200.000 دولار. وبعد أن قامت الشركة بتحليل الموقف وقدرت أن الخسائر التي يمكن أن تنشأ عن إفشاء محتواها تفوق بكثير المطلب المطلوب فقد فضلت دفع المبلغ من أجل استرداد الشرائط المسروقة. كذلك أيضاً دفعت الرغبة بمستخدم يعمل بشركة التأمين كي يحتفظ بوظيفته التي سبق وأن فصل منها إلى احتجاز الذاكرة المركزية الخاصة بالشركة كرهينة لديه، حيث هدد المختلس رئيسه في العمل بأنه إذا حاول أن يلغي بطاقة أجرته من ذاكرة الحاسب الآلي فإن هذه الأخيرة سوف تدمر تلقائياً عن طريق ما يعرف بالقنابل المنطقية.

¹ قرصنة أنظمة الكمبيوتر إعداد: دورثي إي. ديننغ ورقة مقدمة للمؤتمر القومي الثالث عشر لأمن الكمبيوتر، واشنطن، ترجمة: آمنة علي يوسف، ديسمبر 1998، ص 8.

- الإثارة والمتعة والتحدي:

يدرك القراصنة: شيئاً عن أساسيات الكمبيوتر وأن هذا الأمر يمكن أن يكون ممتعاً، حيث جاء على لسان أحد القراصنة ما يأتي كانت القرصنة هي النداء الأخير الذي يبعثه دماغه فقد كنت أعود إلى البيت بعد يوم ممل آخر في المدرسة، وأدير تشغيل جهاز الكمبيوتر، وأصبح عضواً في نخبة قراصنة الأنظمة، كان الأمر مختلفاً برمته حيث لا وجود لعطف الكبار وحيث الحكم هو موهبتك فقط. في البدء كنت أسجل أسمى في لوحة النشرات Bulletin Board الخاصة حيث يقوم الأشخاص الآخرون الذين يفعلون مثلي بالتردد على هذا الموقع، ثم أتصفح أخبار المجتمع وأتبادل المعلومات مع الآخرين في جميع أنحاء البلاد.

وبعد ذلك أبدأ عملية القرصنة الفعلية، وخلال ساعة واحدة يبدأ عقلي بقطع مليون ميل في الساعة وأنسي جسدي تماماً بينما أتنقل من جهاز كمبيوتر إلى آخر محاولاً العثور على سبيل للوصول إلى هدي. لقد كان الأمر يشبه سرعة العمل في متاهة إلى جانب الاكتشاف الكبير لإعداد ضخمة من المعلومات.

وكان يرافق تزايد سرعة الأدرينالين الإثارة المحظورة بفعل شيء غير قانوني. وكل خطوة أخطوها كان يمكن أن تسقطني بيد السلطات. كنت على حافة التكنولوجيا واكتشاف ما وراءها، واكتشاف الكهوف الإلكترونية التي لم يكن من المفترض وجودي بها.¹

وذكرت Jutian Dibbell بأنها تعتقد بأن المتعة تكمن في المخاطر التي ترتبط بعملية القرصنة وذكرت قائلة "أن التكنولوجيا تستسلم من الدراما المليئة بالمغامرات وأن قراصنة الأنظمة يعيشون في عالم لا يعتبرون فيه العمل السري سوي لعبة يلو بها الأطفال.

- الدوافع الشخصية

إن الدافع لارتكاب جرائم الكمبيوتر يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح، ويميل مرتكبو جرائم نظم المعلومات إلى إظهار تفوقهم ومستوى ارتقاء براعتهم

¹ حول قراصنة أنظمة الكمبيوتر، راجع: دروئي إي. ديننغ، ورقة مقدمة للمؤتمر القومي الثالث عشر لأمن الكمبيوتر، مرجع سابق، ص 11.

لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبو هذه الجرائم لديهم شغف الآلة يحاولون إيجاد - وغالباً ما يجدون - الوسيلة إلى تحطيمها بل والتفوق عليها.

ويتزايد شيوع هذا الدافع لدى فئات صغار السن من مرتكبي الكمبيوتر الذين يمضون وقتاً طويلاً أما حواسيبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الكمبيوتر وشبكات المعلومات وإظهار تفوقهم على وسائل التكنولوجيا، الأمر الذي دفع بالعديد من الفقهاء إلى المناداة بعدم مساءلة مرتكبي جرائم الحاسب الآلي الذي يتمثل باعتهام في إظهار تفوقهم، واعتبار أعمالهم غير منظوية على نوايا آثمة.

وقد أمكن الكشف في بعض الأحوال عن أن مجرد إظهار شعور جنون العظمة وهو الدافع لارتكاب فعل الجريمة المعلوماتية وفي هذا الشأن نجد المحلل أو المبرمج المعلوماتي وهو مفتاح سر كل نظام قد ينتابه إحساس بالإهمال أو بالنقص داخل المنشأة التي يعمل بها. وقد يندفع تحت تأثير الرغبة القوية من أجل تأكيد قدراته الفنية لإدارة المنشأة إلى ارتكاب الجريمة المعلوماتية، ومن ثم يجد ترضية من خلال الإفصاح عن شخصيه أمام العامة. - ضحايا جريمة سرقة المعلومات

تتميز جرائم الحاسب بالصعوبات البالغة في اكتشافها وبالعجز في حالات كثيرة عن إمكان إثباتها في حالة اكتشافها.

ومرد ذلك الأسباب التالية:

أولاً: لا تخلف جرائم الحاسب أثراً ظاهراً خارجية فهي تنصب على البيانات والمعلومات المخزنة في نظم المعلومات والبرامج مما ينفي وجود أي أثر مادي يمكن الاستعانة به في إثباتها، فالجرائم المعلوماتية ينتفي فيها العنف وسفك الدماء ولا توجد فيها آثار لاقتحام سرقة الأموال، وإنما هي أرقام ودلالات تتغير أو تمحي من السجلات ومما يزيد من هذه الصعوبة ارتكابها في الخفاء، وعدم وجود أثر كتابي مما يجري من خلال تنفيذها من عمليات حيث يتم نقل المعلومات بواسطة النبضات الإلكترونية.

ثانياً: يتم ارتكاب جريمة الحاسب عادة عن بعد فلا يتواجد الفاعل في مسرح الجريمة حيث تتباعد المسافات بين الفاعل والنتيجة، وهذه المسافات لا تقف عند حدود الدولة بل تمتد إلى النطاق الإقليمي لدول أخرى مما يضاعف صعوبة كشفها أو ملاحقتها.

ثالثاً: تبدو أكثر المشاكل جساماً لا في مجال صعوبة اكتشاف وإثبات جرائم الحاسب بل وفي دراسة هذه الظاهرة في مجملها هي مشكلة امتناع المجني عليهم عن التبليغ عن الجرائم المرتكبة ضد نظام

الحاسب وهو ما يعرف بالرقم الأسود chifrenoir حيث لا يعلم ضحايا هذه الجرائم شيئاً عنها إلا عندما تكون أنظمتهم المعلوماتية هدفاً لفعل الغش أو حتى عندما يعلمون فهم يفضلون عدم إفشاء الفعل.¹

المطلب الثاني: خصائص الجريمة الالكترونية.

نتيجة للتداول الداخلي للبيانات المبرمجة عبر الدول وتداول المعلومات البسيطة (غير المبرمجة) وسرعة انتشار شبكة المعلومات كل هذا أدى إلى التغيير التقني المطرد والمتعاضم غي هذا المجال وإلى سهولة تداول المعلومات ومن ثم تساعد على ارتكاب الجريمة المعلوماتية عن طريق الحاسب الشخصي أو الحواسيب الأخرى المستخدمة في دولة معينة على الرغم من أن النتيجة الإجرامية قد تتحقق في دولة أخرى إذ أن الجريمة المعلوماتية أصبحت شكلاً جديداً من الجرائم العابرة للحدود الإقليمية وهذه الصورة تتخذ تلك الجرائم طابعاً يميزها عن غيرها من الجرائم.²

لذا يمكن إيراد بعض الخصائص والسمات التي تجعل الجريمة المعلوماتية عموماً والمرتبكة على شبكة المعلومات بشكل أكثر تحديداً مختلفة عن الجرائم الأخرى والتقليدية.

وتتمثل في:

- 1- الجرائم المعلوماتية جرائم عابرة للدول أي تلك الجرائم التي تقع بين أكثر من دولة بمعنى أنها لا تعترف بالحدود الجغرافية للدول إذ غالباً ما يكون الجاني في بلد والمجني عليه في بلد آخر، وقد يكون الضرر المحتمل في بلد ثالث وعليه تعد الجرائم المعلوماتية شكلاً جديداً من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القارية.
- 2- أنها جرائم صعبة الإثبات حيث يصعب في كثير من الأحيان العثور على أثر مادي للجريمة المعلوماتية ولعل السبب في ذلك يعود إلى استخدام الجان لوسائل فنية وتقنية معقدة في كثير من الأحيان كما يتمثل السلوك المكون للركن المادي فيها بعمل سريع قد لا يستغرق أكثر من

¹ يونس خالد عرب مصطفى، جرائم الحاسوب، دراسة مقارنة، رسالة ماجستير مقدمة إلى الجامعة الأردنية 1994، ص 72.

² محمد محي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 1993، ص 6.

بضع ثوان علاوة على سهولة محو الدليل والتلاعب به في الوقت الذي تفتقر فيه هذه الجرائم إلى الدليل المادي التقليدي.¹

3- تعد الجرائم المعلوماتية أقل عنفا من الجرائم التقليدية أي أنها لا تحتاج إلى أدنى مجهود عضلي بل تعتمد على الدراية الذهنية والتفكير العلمي المدروس القائم على معرفة تقنيات الحاسب الآلي فلا يوجد في واقع الأمر شعور بعدم الأمان تجاه المجرمين في مجال المعالجة الآلية للمعلومات باعتبار أن مرتكبيها ليسوا من محتري الإحرام بصبغته المتعارف عليها.

4- إن الباعث على ارتكاب الجرائم المعلوماتية يختلف عنه بالنسبة إلى الجرائم التقليدية ففي الحالة الأولى يتمثل لباعث في بالرغبة في مخالفة النظام العام والخروج عن القوانين أكثر من استهداف الحصول على الربح في حين نجد أن الباعث لدى مرتكبي الطائفة التالية هو عموما الحصول على النفع المادي السريع أما إذا اقترن الباعث في ارتكاب الجرائم المعلوماتية بهدف تحقيق النفع المادي فإن المبالغ التي يمكن تحقيقها من وراء ذلك تكون طائلة.²

خاتمة:

في ختام مداخلتنا هذه تجدر الإشارة إلى أن أهم إشكالات الجريمة المعلوماتية في التشريع الجزائري وكذا في كل التشريعات المقارنة هو مدى تحقيق التوافق والتوازن بين استعمالات التقنيات والتكنولوجيات الحديثة للإعلام والاتصال واحترام الحريات الفردية والجماعية لجميع الأشخاص المتعاملين في ميدان المعلوماتي وبالنسبة وبالخصوص على شبكة الانترنت والانترانت، وهذا بعد تطور أنظمة المراقبة الالكترونية وكذا تسهيل هذه التقنيات والتكنولوجيات لأعمال الجوسسة والمساحات بالحريات الشخصية.

قائمة المراجع:

¹ هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، ط1، مكتبة الآلات الحديثة، أسبوط، 1994، ص72.

² جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 1992، ص 62.

أولاً: الكتب

- جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 1992.

- هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، ط1، مكتبة الآلات الحديثة، أسبوط، 1994.

- عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، ط1، بدون ناشر، 2000.

- أحمد هلاي عبد اللاء، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة، 2002.

- قورة نائلة، جرائم الحاسب الاقتصادية، دار النهضة العربية، القاهرة، 2003-2004.

ثانياً: مذكرات.

- يونس خالد عرب مصطفى، جرائم الحاسوب، دراسة مقارنة، رسالة ماجستير مقدمة إلى الجامعة الأردنية 1994.

مؤتمرات علمية.

- محمد محي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 1993.

- قراصنة أنظمة الكمبيوتر إعداد: دورثي إي. دينغ ورقة مقدمة للمؤتمر القومي الثالث عشر لأمن الكمبيوتر، واشنطن، ترجمة: آمنة علي يوسف، ديسمبر 1998.

ثالثاً: مقالات.

- علاء رضوان، الجريمة المعلوماتية من النشأة في الستينيات إلى «القرصنة» في القرن الـ21، مقال منشور في الانترنت يوم 16 نوفمبر 2018 على الساعة 12:00.

رابعاً: محاضرات.

بن داعس فيصل، إشكالات الجريمة المعلوماتية في التشريع الجزائري، محاضرة في إطار التكوين المحلي المستمر للقضاة، 2011.

الجريمة المعلوماتية: في إطار ماهيتها وأنواعها

د/ نادية ضريفي

ط.د/ بن طاية زوليخة

أستاذة محاضرة (أ) – كلية الحقوق والعلوم

كلية الحقوق والعلوم السياسية

السياسية – جامعة المسيلة

جامعة بسكرة

مقدمة:

تغطي تكنولوجيا المعلومات و الاتصالات أهمية خاصة في حياتنا اليومية، إذ تساهم بشكل كبير في تخطي الحدود و الحاجز بين مختلف شعوب العالم فضلا عن خدمات أخرى لاسيما في المجالات الاجتماعية و الاقتصادية و التعليمية و ذلك نظرا لما تنسم به من سرعة و حركة دائبة، و أمام تعاظم مزايا تقنية المعلوماتية تعاظم معها مخاطر بسبب استعمالها على نحو غير مشروع مما أدى إلى ظهور طائفة جديدة من الجرائم لتتقود إلى ما يمكن تسميته بجرائم المعلوماتية، و التي باتت اليوم تهدد العديد من المصالح و المراكز القانونية.

إن جرائم المعلوماتية من أعقد الجرائم و أخطرها باعتبارها جرائم لا تحددها حدود، و ما ينجم عنها من خسائر فادحة نتيجة الاستخدام السلبي لهذه التقنية، بما توفره من تسهيلات فضلا على أن مرتكبيها من بين فئات متعددة تجعل التنبؤ بهم أمرا عسيراً، ليس هذا فحسب بل تستهدف معنويات لا ماديات محسوسة.

و قد امتدت الجريمة المعلوماتية لتشمل صور الجريمة المنظمة حيث ظهرت الجماعات الإرهابية على الشبكة و أخذت تمارس أعمالها من خلالها و ذلك من خلال التلاعب بأنظمة و بيانات خاصة وتشمل كذلك أغلب صور الاعتداء على الأشخاص و الأموال من جنح بسيطة إلى جنایات كبرى سواء كان المجرم المعلوماتي كفاعل أصلي أو كفاعل معنوي، و هذا ما أثار تحديا كبيرا و مشاكل عدة بالنسبة لقانون العقوبات من حيث صعوبة إقامة الدليل على هذا النوع من الجرائم و إثباتها و كذا تحديد القانون الواجب التطبيق على الجرائم المرتكبة بواسطة تقنية المعلومات، و في إطار ما سبق ذكره، تظهر ملامح إشكالية هذا البحث في التساؤلات التالية: ما المقصود بالجريمة المعلوماتية؟ و ما هي السمات المميزة لهذه الجريمة؟ و ما هي أنواعها؟

و تهدف الدراسة إلى محاولة تأصيل المفاهيم و إبراز الخصائص المميزة لجرائم المعلوماتية عن الجرائم التقليدية و ذلك من أجل تجنبها و التوعية بمخاطرها.

و قد تطلب منا هذا البحث، اعتماد المنهج الوصفي و ذلك من خلال تحديد وصف هذه الظاهرة و بعض المفاهيم التي تقوم عليها، كما تم الاعتماد على المنهج التحليلي و ذلك من خلال تحليل مفاهيمها.

و في سبيل مناقشة هذا الموضوع، سيتم التطرق إلى ماهية الجريمة المعلوماتية في مطلبين: المطلب الأول يتناول تعريف الجريمة المعلوماتية أما المطلب الثاني فيخصص لخصائصها، أما المبحث الثاني فيوضح تصنيفات الجريمة الإلكترونية في ثلاثة مطالب، بدء بتحديد جرائم الاعتداء على الأشخاص في مطلب أول: ثم جرائم تقع على الأموال في المطلب الثاني، أما المطلب الثالث فيخصص للجرائم الواقعة على أمن الدولة.

المبحث الأول: ماهية الجريمة المعلوماتية

تعد الجرائم الناشئة في البيئة الرقمية من جرائم العصر لارتباطها بالتقنيات الحديثة و كذا تكنولوجيا وسائل الاتصال، فهي جريمة ترتكب خفية و دون عنف، بحيث يتم ارتكابها من طرف أشخاص يتمتعون بقدرة عالية من الذكاء و يكتسبون معارف عملية و علمية كاملة بمحيط الجريمة و ظروفها، و عليه فإن الجريمة المعلوماتية كظاهرة إجرامية لها طبيعة خاصة تميزها عن صور الإجرام البشري التقليدي.

و سوف نتعرض في هذا المبحث إلى تحديد تعريف الجريمة المعلوماتية (المطلب الأول)، ثم نتطرق إلى خصائص الجرائم الإلكترونية المتصلة بشبكة الانترنت (المطلب الثاني).

المطلب الأول: تعريف الجريمة المعلوماتية

بداية لابد أن نشير إلى أنه لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال واستخدام تقنية المعلومات، كون هذه الظاهرة المستحدثة تتطور من حين إلى آخر، و هناك عدة تسميات أطلقت على هذه الجريمة منها الجريمة الإلكترونية أو الجريمة المعلوماتية أو الجرائم التقنية العالية، أو جرائم الشبكة العنكبوتية أو الجرائم المرتبطة بالكمبيوتر أو جرائم الكمبيوتر و الإنترنت.

و تجدر الإشارة إلى أن التعريفات الفقهية لمصطلح الجريمة الإلكترونية تعددت و تباينت فيما بينها تبعاً لحل اهتمام كل فئة، بين موسع لمفهومها و بين مضيق لها.

الفرع الأول: التعريفات المضيقية للجرائم الإلكترونية

من التعريفات المضيقية للجرائم الإلكترونية ما جاء به الفقيه MERWE، حيث يرى بأنها: " الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي"¹، و يرى الأستاذ TREDMAN أن الجريمة المعلوماتية تشمل " أي جريمة ضد المال مرتبطة باستخدام المعالجة الآلية للمعلومات"²، وفي هذا الاتجاه أيضا عرفها جانب من الفقه على أنها تلك الجرائم التي يتطلب لارتكابها توافر معرفة بتقنية الحاسب لدى مرتكبيها³، و يعرف جانب آخر من الفقه هذا النوع من الجرائم بالنظر إلى نتيجة الاعتداء، إذ يرى الأستاذ MASS أن المقصود بالجريمة الناشئة في بيئة إلكترونية هي: " كل اعتداء قانوني يرتكب بواسطة المعلوماتية و يكون الغرض من ارتكابه تحقيق الربح"⁴، و يرى الأستاذ PARKER أن الجريمة المعلوماتية هي: " كل فعل إجرامي يرتكب عمدا و أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالجني عليه أو كسب يحققه الفاعل"⁵.

و ذهب الفقيه ROSBLAT إلى تعريفها بقوله: " هي كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي و التي تحول طريقه"⁶. و يتضح من خلال التعريفات السابقة للجريمة المعلوماتية طبقا للاتجاه المضيق أنها قاصرة عن الإلمام بأوجه هذه الظاهرة، إذ ركز البعض من الفقهاء على معيار موضوع الجريمة و البعض الآخر ركز على وسيلة ارتكابها و البعض الآخر يركز على معيار النتيجة، و إزاء هذه الانتقادات حاول بعض الفقه تعريف الإجرام المعلوماتي على نحو واسع في محاولة لتفادي أوجه القصور التي شابت تعريفات الاتجاه الضيق في التصدي لظاهرة الجريمة المعلوماتية.

¹ محمد أمين الشوابكة، جرائم الحاسوب و الانترنت (الجريمة المعلوماتية)، دار الثقافة للنشر و التوزيع، عمان، طبعة أولى، 2006، ص 8.

محمد أمين الشوابكة، مرجع نفسه، ص 8.

³ سعيداني نعيم، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، كلية الحقوق و العلوم السياسية باتنة. 2012/2013، ص 27.

محمد أمين الشوابكة، مرجع سابق، ص 8.

سعيداني نعيم، مرجع سابق، ص 27.

محمد أمين الشوابكة، مرجع سابق، ص 8.

الفرع الثاني: التعريفات الموسعة للجرائم المنظمة

فعلى عكس من الاتجاه الضيق، فإن أصحاب هذا الاتجاه يذهبون إلى التوسيع من مفهوم هذه الظاهرة، فهناك من يعرفها على أنها: "كل عمل أو امتناع يأتيه الإنسان إضراراً بمكونات الحاسب المادية و المعنوية و شبكات الاتصال الخاصة به، باعتبارها من المصالح و القيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها"¹، و يعرفها البعض الآخر على أنها: "كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية، و يهدف إلى الاعتداء على الأموال المادية أو المعنوية"²، كما عرفها آخر بأنها: "كل تلاعب بالحاسب الآلي و نظامه من أجل الحصول بطريقة غير مشروعة على مكسب أو إلحاق خسارة بالمجني عليه"³.

و لم يسلم هذا الاتجاه من سهام النقد أيضاً، كونه ينطوي على توسيع كبير لمفهوم الجريمة المعلوماتية، إذ يؤخذ عليه هذا التوسع الذي من شأنه أن يصبغ وصف جريمة قد لا تكون كذلك لمجرد مشاركة الحاسب الآلي في النشاط الإجرامي⁴.

و عليه يمكن وصف الجريمة على أنها جرم معلوماتي و ذلك متى توفر عنصرين أساسيين و هما العنصر الشخصي و العنصر الموضوعي، بحيث يتمثل العنصر الشخصي في المهارة الفنية و خبرة الفاعل الضرورية لاستعمالها لارتكاب الفعل المجرم بفعل أو امتناع، أما العنصر الموضوعي فيتمثل في محل ارتكاب الجريمة و يقتضي أن يكون الكمبيوتر هو الأداة الضرورية لارتكابه أو داخل نظامه⁵، سواء على الأشخاص كانتهاك حرمة الحياة الخاصة أو القتل أو على الأموال كالسرقة و الاحتيال و التزوير و غيرها و يسمى هذا النوع من الجرائم الأعمال الجرمية التي ترتكب بمساعدة الكمبيوتر⁶.

¹ سعيداني نعيم، مرجع سابق، ص 29.

² محمد أمين الشوابكة، مرجع سابق، ص 9.

³ سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير، كلية الحقوق و العلوم السياسية تلمسان،

2010/2011، ص 14.

⁴ سعيداني نعيم، مرجع سابق، ص 29.

⁵ فريد منعم جبور، حماية المستهلك عبر الانترنت و مكافحة الجرائم الإلكترونية (دراسة مقارنة)، منشورات الحلبي الحقوقية بيروت، الطبعة الأولى، 2010، ص 187.

⁶ نسرين عبد الحميد نبيه، الجريمة المعلوماتية و المجرم المعلوماتي، منشأة ناشر المعارف، الإسكندرية، دون طبعة،

2008.ص.156.

أما المشرع الجزائري رغم أنه استحدث القانون 04/09¹ الذي يهدف إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، إلا أنه لم يعرف الجريمة المعلوماتية و إنما تبنى للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية و هذا ما نستشفه من خلال أحكام المادة 02 فقرة أ من القانون السالف الذكر و التي تنص على ما يلي: " يقصد بالجرائم المتصلة بتكنولوجيات الإعلام و الاتصال في مفهوم هذا القانون: " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية".

إن عدم تبني المشرع الجزائري لتعريف حول الجريمة المعلوماتية، كان تحسبا للتطور العلمي و التقني المستمر و لعدم إمكانية حصر قاعدة التجريم في نطاق أفعال معينة قد تتغير أو تتبدل في المستقبل².

المطلب الثاني: خصائص الجريمة المعلوماتية

تشكل الجرائم الالكترونية أخطارا جسيمة في ظل العولمة على اعتبار أنها من أبرز الجرائم المستحدثة التي تمس بالأشخاص و الأموال و أمن الدولة نتيجة ارتباطها بالحاسب الآلي و تقنية المعلومات، حيث تتميز الجريمة المعلوماتية بجملة من الخصائص و السمات، لا تتوافر في أي من أفعال الجرائم التقليدية، لا في أسلوبها ولا في أداة ارتكابها، و التي انعكست بدورها على مرتكب هذه الجريمة الذي أصبح يعرف بالمجرم المعلوماتي لتمييزه أيضا عن المجرم التقليدي، و على هذا الأساس سنحاول التطرق إلى أهم خصائص الجريمة المعلوماتية (الفرع الأول)، ثم سنتناول بالدراسة أهم سمات المجرم المعلوماتي (الفرع الثاني).

الفرع الأول: خصائص جرائم المعلوماتية

تميز الجريمة المعلوماتية عن الجريمة التقليدية بجملة من الخصائص، لعل من أبرزها ما يلي:

¹ قانون رقم 04/09، المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام و الاتصال و مكافحتها، مؤرخ في 5 أوت 2009، جريدة رسمية عدد 47، مؤرخة في 16 أوت 2009.
² فريد منعم جبور، مرجع سابق، ص 184.

أولاً: هي جرائم هادئة

أي عدم اتسام الجريمة المعلوماتية بالعنف الذي تتميز به غيرها من الجرائم التقليدية، و رغم ذلك فإن البعض يشبه هذا النوع من الجرائم بجرائم العنف مثل ما ذهب إليه مكتب التحقيقات الفيدرالي بالولايات المتحدة الأمريكية FBS نظرا لتماثل دوافع المعتدين على نظم الحاسب الآلي مع مرتكبي العنف¹.

ثانياً: الجرائم المعلوماتية هي جرائم عابرة للحدود

حيث تعرف بالجريمة التي لا تعرف الحدود الجغرافية بمعنى هي جرائم عابرة للقارات، بحيث لم يعد هناك حدود مربية أو ملموسة تقف أمام نقل المعلومات عبر مختلف الدول، و هذا ما يؤدي إلى تأثير أمكن عديدة في دول مختلفة بالجريمة المعلوماتية في آن واحد²، و أسفر عن هذا الأمر أن شبكة الإنترنت التي ألغت الحدود بين الدول ذات فاعلية تفوق قدرة الأجهزة الدولية المختصة بمكافحة الجريمة³، إذ غالبا ما تتركب في إقليم دولة معينة و يكون ضحاياها في دولة واحدة أو أكثر بحسب نوع الجريمة كأن يتم اختراق كمبيوتر يوجد في أي نقطة من العالم أو إتلاف معطياته دون أن تكون الحدود الجغرافية حائلا أمام ذلك طالما أن هذا الفعل يتم في فضاء معلوماتي لا يعترف بالحدود الجغرافية الأمر الذي يشكل تحديا كبيرا لكل الدول دون استثناء⁴.

هذه الطبيعة التي تتميز بها الجريمة المعلوماتية كونها عابرة للحدود، تثير إشكالات عديدة في مجال جرائم الحاسوب و بشكل خاص الإجراءات الجنائية و الاختصاص و القانون الواجب التطبيق مما يحول دون نجاعة أساليب مكافحتها⁵.

¹ أمينة حشاني، ماهية الجريمة المعلوماتية، مجلة دراسات و أبحاث، المجلد 1، العدد 1، ص 1.453

² سعيداني نعيم، مرجع سابق، ص 31.

³ ميلودية أحمد، نعموش محمد، الجريمة المعلوماتية: المفهوم - حتمية تطوير آليات التعاون الدولي في مجال مكافحتها،

مجلة الدراسات القانونية و السياسية، المجلد الرابع، العدد 2، جوان 2018، ص 269.

⁴ شوقي يعيش تمام، شيري عزيزة، تفعيل مبدأ عالمية النص الجنائي في التصدي للجريمة المعلوماتية، مجلة الاجتهاد

القضائي العدد 15، سبتمبر 2017، ص 95/94.

⁵ نسرين عبد الحميد نبيه، مرجع سابق، ص 133.

ثالثا: الحاسوب هو أداة ارتكاب الجرائم المعلوماتية

فحوى هذه الخاصة، أن كافة الجرائم الإلكترونية ترتكب عن طريق الحاسب الآلي، فلا يمكن تسميتها أو وصفها بجريمة معلوماتية دون استخدام الحاسوب لأنه أداة تنفيذ الجريمة و بالتالي وسيلة الإجرام في هذا الصنف¹.

رابعا: موضوع الاعتداء هو معطيات الجهاز الإلكتروني

إذ تعد البيانات و المعلومات المخزنة على الحاسب الآلي هي موضوع الجرائم الإلكترونية².

خامسا: الجرائم ترتكب عبر شبكة الإنترنت:

تعد شبكة الإنترنت في غالبية الجرائم الإلكترونية حلقة وصل بين كافة الأهداف المحتملة و التي غالبا ما تكون الضحية لتلك الجرائم و هو ما دعا معظم تلك الأهداف على غرار البنوك و الشركات الصناعية و غيرها من الأهداف اللجوء إلى نظم الأمن المعلوماتية في محاولة منها لحماية نفسها من تلك الجرائم أو على الأقل لتحد من خسائرها الفادحة عند وقوعها ضحية لها³.

سادسا: الجريمة المعلوماتية صعبة الاكتشاف والإثبات

فهي من الجرائم التي لا تترك آثار خارجية مادية ملموسة⁴.

الفرع الثاني: سمات المجرم المعلوماتي

إن ارتباط الجرائم المعلوماتية بتكنولوجيا المعلومات كان وراء تمييزها عن الجرائم التقليدية، و هذا الارتباط هو نفسه من أسباب تمييز المجرم المعلوماتي عن غيره من المجرمين العاديين، مما يستدعي بيان سماتهم الأساسية توسلا لأفضل السبل للحد من نشاطهم الإجرامي وردعهم⁵، و عليه يتميز هؤلاء المجرمين بعدة خصائص نذكر أهمها فيما يلي:

¹ حكيم سياب، السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية، مجلة دراسات و أبحاث، المجلد 1، العدد 1، ص 219.

² يوسف خليل يوسف العفيفي، الجرائم الإلكترونية في التشريع الفلسطيني (دراسة تحليلية مقارنة)، مذكرة لنيل شهادة الماجستير كلية الشريعة والقانون، 2013، ص 15.

حكيم سيلب، مرجع سابق، ص 219.

⁴ يوسف خليل يوسف العفيفي، مرجع سابق، ص 16.

فريد منعم جبور، مرجع سابق، ص 189.

— مرتكب الجريمة هو شخص ذو خبرة في مجال الحاسب الآلي و التي تمكنه على تنفيذ عمله المجرم و العمل على عدم اكتشافها¹.

— تعد المهارة المطلوبة لتنفيذ النشاط الإجرامي من أبرز خصائص المجرم المعلوماتي و التي قد يكتسبها عن طريق الدراسة المتخصصة في ها المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات أو بمجرد التفاعل الاجتماعي مع الآخرين².

— ارتفاع مستوى الذكاء لمرتكب الجرائم المعلوماتية، بحيث يتمتع المجرم الإلكتروني بذكاء حاد لا نجده في مرتكب الجريمة التقليدية الذي في الغالب ما يترك آثار تدل عليه، بخلاف مرتكب الجريمة الإلكترونية فقد يكون ملما بجميع الجوانب الفنية و التقنية لجريمته مما يساعده في التخلص من أدلة إدانته في وقت سريع وبدون جهد³.

— التنظيم و التخطيط: ترتكب هذه الجرائم من مجموعة مكونة من عدة أشخاص، بحيث يحدد لكل شخص منهم دورا معينا، و يتم العمل بينهم وفق تخطيط و تنظيم سابق على ارتكاب الفعل المجرم⁴.
— المجرم المعلوماتي إنسان اجتماعي: أي أن المجرم المعلوماتي يتكيف في أوساط اجتماعية من دون قلق أو حيرة، فهو يرتكب جريمته بكل هدوء و تروي ثم يححو آثارها بسلاسة فيكون في لحظة إنسان طبيعي و في لحظة أخرى مجرم محترف⁵.

المبحث الثاني: تصنيف جرائم المعلوماتية

من الصعوبة تماما حصر أنواع الجريمة المعلوماتية، و السبب في ذلك يعود لحدثة ظهور هذه الجريمة و هي تزداد تنوعا و تعدادا كلما أوغل العالم في استخدام الحاسب الآلي و شبكة الإنترنت⁶، و نظرا لذلك تعددت محاولات الفقه في تحديد أنواعها، فمنهم من اعتمد معيارا وظيفيا و غائيا للجرائم المعلوماتية، و هناك من قسمها إلى ثلاثة طوائف تتمثل في جرائم الحاسب الآلي الاقتصادية و جرائم الحاسب الآلي التي تنطوي على الاعتداء على حرمة الحياة الخاصة و أخيرا جرائم الحاسب الآلي التي

حكيم سياب، مرجع سابق، ص 1.224

سعيداني نعيم، مرجع سابق، ص 2.51

يوسف خليل يوسف العفيفي، مرجع سابق، ص 3.19

سعيداني نعيم، مرجع سابق، ص 4.52

يوسف خليل يوسف العفيفي، مرجع سابق، ص 5.18

⁶ حكيم سياب، مرجع سابق، ص 221.

تحدد المصالح القومية أو السلامة الشخصية للأفراد، و نحن بدورنا نقسمها إلى جرائم الاعتداء على الأشخاص (المطلب الأول)، و جرائم تقع على الأموال (المطلب الثاني)، و أخرى ضد أمن الدولة (المطلب الثالث).

المطلب الأول: جرائم الاعتداء على الأشخاص

من أكثر الجرائم انتشارا، جرائم الاعتداء على الأشخاص و حياتهم الخاصة، حيث تعد الانترنت أفضل بيئة تشمل هذه الجرائم نظرا لسرعة تنفيذها و يفضل الكثير من المجرمين ارتكاب هذه الجريمة عبر الانترنت لصعوبة الكشف على هويتهم و إيقاعهم تحت طائلة المسؤولية، و تتنوع الجرائم التي تمس بالأشخاص، فلها عدة صور و أشكال من بينها:

— جرائم الذم و التهديد و التشهير بواسطة شبكات الاتصال.

— جرائم الأخلاق العامة عبر الانترنت.

— جرائم القتل بالحاسب و التسبب في الوفاة.

— جريمة الاعتداء على حرمة الحياة الخاصة.

— جرائم الاستغلال الجنسي للأطفال.

المطلب الثاني: جرائم الاعتداء على الأموال

يقصد بالجرائم ضد الأموال، تلك الجرائم التي تستهدف عناصر الذمة المالية، ويكون الطمع وراء ارتكابها و الاستيلاء و الحصول على تلك الأموال و فكرة المكسب السريع التي تحرك مرتكبيها¹، و من أهم تطبيقات هذه الجرائم في نطاق الجرائم المعلوماتية ما يلي:

— جريمة التحويل الإلكتروني غير المشروع للأموال عبر شبكة الانترنت.

— إدخال معلومات خاطئة أو مزورة إلى نظام الحاسب.

— جرائم الاحتيال و سرقة المال المعلوماتي المعنوي.

— الاختلاس عبر الحاسب.

— استخدام الحاسب للحصول على البطاقات المالية أو استخدامها للغير دون ترخيص أو تدميرها.

حكيم سياب، مرجع سابق، ص 221.

المطلب الثالث: الجرائم المعلوماتية الواقعة على أمن الدولة

يقصد بالجرائم الواقعة على أمن الدولة، تلك الجرائم التي تنال بالاعتداء أو تهدد حقوق ذات طابع عام، و لقد أسفرت الحياة العملية وقوع جرائم معلوماتية تدخل ضمن زمرة هذه الجرائم أهمها¹:

— التجسس الالكتروني.

— الجريمة المنظمة عبر الانترنت.

— الإرهاب الالكتروني.

— جرائم الإخفاق في الإبلاغ عن جرائم الحاسب.

— جرائم تعطيل تنفيذ القانون.

— جرائم تعطيل الأعمال الحكومية.

— تهديد السلامة العامة.

خاتمة:

و في الأخير نتوصل إلى الاستنتاجات و التوصيات التالية:

أولا: النتائج

— إن ظاهرة الجرائم المعلوماتية ظاهرة إجرامية خطيرة لازدياد حجم خسائرها و الأضرار الناجمة عنها، باعتبار أنها جرائم تستهدف الأمن القومي بارتكاب جرائم تمس جهات حكومية و أمنية، ليس هذا فحسب بل حتى الاعتداء على المعطيات بدلالاتها التقنية الواسعة، فضلا عن مساسها بالحياة الخاصة للأفراد، لذا فإن معرفة كل ما يحيط بهذا النوع من الجرائم من تعريف واستظهار لخصائصها و أنواعها يتخذ أهمية بالغة في معرفة كيفية التعامل مع هذه الظاهرة و حجم خطورتها و لتجنبها مستقبلا.

— لحد الساعة لا يوجد تعريف جامع مانع للجريمة المعلوماتية، فكل المحاولات الفقهية في مجالها الواسع و الضيق باءت بالفشل أما عن المشرع الجزائري فأطلق عليها تسمية جرائم المساس بالأنظمة المعلوماتية.

¹ أمينة حمشاشي، مرجع سابق، ص 455.

— تتميز الجريمة المعلوماتية بعدة خصائص تميزها عن الإجرام التقليدي كونها عابرة للحدود وتتم في عالم افتراضي كما أن المجرم المعلوماتي يختلف عن المجرم التقليدي لخبرته ودرايته العالية بالتقنيات المعلوماتية.

ثانيا: التوصيات

- ضرورة إيجاد تعريف جامع للجريمة الإلكترونية في شقيها الواسع و الضيق.
- ضرورة تحديد كافة صور هذا النوع من الجرائم و السعي على توحيدها على المستوى الدولي حتى لا يستغل مرتكب الفعل المجرم هذه الثغرات و أن لا تكون لصالحه.
- ضرورة عقد الدورات المتخصصة لأفراد الضبطية القضائية و أعضاء النيابة العامة و القضاة لتعريفهم بالجرائم المرتكبة في بيئة رقمية و توضيح مدى خطورتها.

تعريف وأركان الجريمة المعلوماتية في ظل الفقه والتشريع المقارن والجزائري

ط.د/ بن لقرشي مصطفى

كلية الحقوق والعلوم السياسية

جامعة المسيلة

د/ ميهوبي حورية

أستاذة محاضرة (أ) جامعة محمد بوضياف

بالمسيلة

مقدمة:

لقد تميز القرن العشرين بثورة المعلومات والتكنولوجيا الحديثة التي ساهمت باختراعات هائلة على المستوى التقني في مجال استخدام الكمبيوتر والشبكات المعلوماتية التي شكلت قفزة نوعية في حياة الأفراد والدول، من خلال عولمة المعلومات التي سهلت الكثير من الخدمات، ومكنت البشرية من السيطرة على المعلومة من خلال استخدام الحاسوب لتخزين ومعالجة واسترجاع المعلومات وربطه بشبكة الاتصال الدولي الانترنت التي شكلت وحدة واحدة تتربط فيها الحسابات وشبكة المعلومات. على الرغم من أهمية هذه التقنية الحديثة وإيجابيات استعمالها، إلا أن الاستخدام غير مشروع لها، قد أدى إلى ظهور نوع جديد من الجرائم المرتبطة بالأنظمة الالكترونية والشبكة المعلوماتية وخصوصا على شبكة الانترنت سميت بالجرائم المعلوماتية أو جرائم الانترنت¹ التي أدت إلى الإضرار بمصالح الأفراد والجماعات وكذا الدول، خاصة أنها جرائم ذكية تنشأ وتحدث في بيئة رقمية، يقترفها أشخاص مرتفعي الذكاء ويمتلكون أدوات المعرفة التقنية مما يسبب خسائر للدولة والمجتمع على جميع الأصعدة الاقتصادية والاجتماعية والثقافية والأمنية. مما يدعو إلى ضرورة تكاتف جهود الدول لمكافحةها باعتبارها جرائم العصر المستحدثة وحتمية الاتفاق الدولي على وضع نظام قانوني متميز لهذه الجريمة الذي يحدد تعريفا موحد لها و ينص على تجريم الفعل وما يميزها عن غيرها من الجرائم الحديثة والتقليدية.

¹ يونس عرب، جرائم الكمبيوتر والانترنت المعنى والخصائص والصور واستراتيجية المواجهة القانونية، أكتوبر، 2006، منشورات على الموقع الالكتروني 6-1p.doc/dios.doc/img/doc/abhatoo.net.ma/www.

أهمية الموضوع: تبدو أهمية الموضوع في تسليط الضوء على الجريمة المعلوماتية، من حيث ما تكتسبه من خطورة وانتشار على مستوى الصعيد الداخلي والدولي، وقصور قواعد القوانين في تحديد مفهوم موحد وشامل لها وتحريم الفعل.

أهداف البحث: تهدف هذه الدراسة إلى ما يلي:

- التعريف بهذه الجريمة من أجل تجنبها.
 - التوعية من مخاطر الوقوع ضحية للجريمة المعلوماتية.
 - التعريف بالوسائل الكفيلة التي تضمن وتحفظ المعلومة المنشورة إلكترونياً.
 - محاولة الوصول إلى معرفة طرق التعامل مع البيئة الإلكترونية للتصدي للجريمة المعلوماتية.
- منهج الدراسة:** واتباعنا في الدراسة منهج يمزج بين المنهج الوصفي باعتباره ضرورة لتوصيف تعريف الجريمة المعلوماتية والتعرف على أركانها، إلى جانب المنهج التحليلي من خلال تحليل بعض النصوص القانونية التي لها علاقة بمجال الدراسة.

إشكالية الموضوع: وللبحث في هذا الموضوع، يتبادر إلى أذهاننا التساؤل التالي:

إلى أي مدى استطاع الفقه والتشريع تجسيد فكرة الشمولية والتميز لتحديد مفهوم الجريمة المعلوماتية؟ لغرض الرد على الإشكال المطروح، سنتناول من خلال دراستنا تعريف الجريمة المعلوماتية في المبحث الأول، أما المبحث الثاني سنتطرق فيه إلى أركان الجريمة المعلوماتية في التشريع المقارن والجزائري .

المبحث الأول: تعريف الجريمة المعلوماتية

لقد اختلفت التسميات التي أطلقت على الجريمة المعلوماتية، فبداية بالاحتتيال المعلوماتي، ثم الجرائم التي يساعد على ارتكابها الحاسب الآلي، ثم التعسف في استعمال الحاسب الآلي. وتقيما للمصطلحات السابقة ترى الدكتورة نائلة عادل محمد فريد قورة أن تعبير الاحتتيال المعلوماتي لا يمثل الجريمة المعلوماتية وإنما هو صورة من صورها، كما أنها لا تتفق وتعبير الجرائم التي يساعد على ارتكابها الحاسب الآلي ذلك أن الحاسب الآلي ونظمه قد يكون محلاً للنشاط الإجرامي وهو ما يؤيده البعض على اعتبار أن مصطلح التعسف في استعمال الحاسب الآلي ينصرف إلى الحالات التي تنطوي إلى إساءة استخدام الحاسب الآلي دون أن تصل إلى درجة السلوك الإجرامي¹.

¹ نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، دراسة تطبيقية ونظرية، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2005، ص 27.

المطلب الأول: التعريف اللغوي للجريمة المعلوماتية

المعلوماتية وهي كلمة مكونة من مقطعين، المقطع الأول information والمقطع الثاني Automatique ويرجع الفضل في اقتراح مصطلح المعلوماتية إلى الأستاذ Drefus حيث استخدمه عام 1962 لتمييز المعالجة الآلية للمعلومات وتبنته بعد ذلك الأكاديمية الفرنسية في أبريل 1966 ومنحته التعريف الآتي: علم المعالجة المنطقية للمعلومات التي تعتبر بمثابة دعامة للمعارف الإنسانية والاتصالات في المجالات الفنية والاقتصادية والاجتماعية وذلك باستخدام معدات آلية¹، التي تعني تكنولوجيا تجميع ومعالجة وإرسال المعلومات بواسطة الكمبيوتر، وبالتالي تعني كلمة الجرائم المعلوماتية كل الأفعال غير المشروعة الماسة بالمعالجة الآلية للمعلومات.

المطلب الثاني: التعريف الاصطلاحي للجريمة المعلوماتية

لقد ثار جدال واختلاف كبير حول تعريف الجريمة المعلوماتية باعتبارها ظاهرة إجرامية حديثة، إلا أن الجهود الفقهية والقانونية المختلفة أعطت عدة تعريفات مختلفة تبعاً لمحل اهتمام كل فئة. فعرفها رجال الفقه من الجانب التقني الفني، وعرفها رجال القانون من الجانب القانوني.

الفرع الأول: التعريف الفقهي للجريمة المعلوماتية: يمكن تصنيف تعريفات الفقه في أربع أصناف:

أولاً: تعريفات تركز حول وسيلة ارتكاب الجريمة: من أنصار هذا الاتجاه الفقيه الألماني LAUS TIEDEMAUN عرف الجريمة المعلوماتية هي كل أشكال السلوك غير المشروع - أو الضار بالمجتمع - الذي يرتكب باستخدام الحاسوب². أما الأستاذ LESLIE DE BALL عرفها على أنها فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية.

ثانياً: تعريفات تركز حول موضوع الجريمة: ويمثل هذا الاتجاه الفقيه ROSANBLATT الذي عرف الجريمة المعلوماتية أنها نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه. كما عرفتها الدكتورة هدى قشقوش بأنها

¹ محمد سامي الشواء، ثورة المعلومات وانعكاساتها على قانون العقوبات، ط1، دار النهضة العربية، القاهرة، 1994، ص 4.

² هشام محمد فريد رسم، قانون العقوبات و مخاطر تقنية المعلومات، مكتبة الآلات الكاتبة، مصر، 1995، ص 35.

جرائم الاعتداء على الأموال المعلوماتية وهي عبارة عن الأدوات المكونة للحاسب الإلكتروني وبرامجه ومعداته¹.

ثالثا: التعريف المستند إلي وجوب الفاعل بتقنية المعلومات: ومن أنصار هذا الاتجاه الفقيه A.SOLARZ الذي عرفها على أنها أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبط بتقنية المعلومات. وعرفها أيضا الفقيه STEIN SCKJOBORG بأنها أي فعل غير مشروع تكون المعرفة بتقنية معلومات أساسية لمرتكبه والتحقيق فيه وملاحقته قضائيا².

رابعا: التعريف المستند إلي معايير مختلفة ومتنوعة: لقد اختلف هذا الاتجاه في المعايير المتبناة لتعريف الجريمة المعلوماتية. فعرفها الخبراء البلجيكيون بأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون بطريق مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية. في حين عرفها الفقيه الفرنسي Massa بـ "الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح"³. أيضا تعريف الخبير الأمريكي PARKER.D الذي قال "أنها فعل إجرامي، أي كانت صلتها بتقنية المعلومات، فيه يتكبد الجاني عليه ونتيجة له خسارة ويحقق الفاعل ربحا عمديا"⁴.

لكن الفقه الجزائري تبني تعريف المؤتمر العاشر للأمم المتحدة لمنع الجريمة حول جرائم الحاسب الآلي وشبكاته إذ عرف الجريمة المعلوماتية بأنها جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب وتتمثل من ناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية⁵.

الفرع الثاني: التعريف القانوني للجريمة المعلوماتية

إن غالبية المشرعين تجنّبوا الخوض في مسألة وضع تعريف تشريعي للجريمة المعلوماتية وأوكلوا مهمة ذلك إلى الفقه، إلا أن البعض منهم اتجه لتعريف أنماط الجريمة المعلوماتية، أو الجريمة المعلوماتية بداية نذكر بعض التعاريف منها:

¹ هدى حامد قشقوش، جرائم التشريع الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992، ص 6.

² أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي الإسكندرية، 2006، ص 84.

³ محمد علي العريان: الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الأزاريطة، 2004، ص 44.

⁴ محمد سامي الشواء، ثورة المعلومات و انعكاساتها على قانون العقوبات، الهيئة المصرية العامة للكتاب، 2003، ص 19.

⁵ زبيخة زيدان، الجريمة المعلوماتية في التشريع الجزائري و الدولي، دار الهدى، عين مليلة، الجزائر، 2011، ص 44.

- عرف المشرع الفرنسي أنماط الجريمة المعلوماتية من خلال القانون رقم 19 لسنة 1988 وميز بين الاعتداء على برامج ومعلومات الحاسب الآلي وبين الاعتداء على أدواته وآلاته ولم ينص هذا القانون على تجريم سرقة البرامج والمعلومات واعتبارها مالا معلوماتيا فحدد جرائم الاعتداء على برامج ومعلومات الحاسب الرقمي الآلي بجريمتين¹.

1- جريمة التوصل بطريق التحايل لنظام المعالجة الآلية للبيانات

2- جريمة إتلاف برامج ومعلومات الحاسب الآلي الرقمي

أما جرائم الاعتداء على أدوات وآلات الحاسوب الآلي الرقمي فهي:

1- جريمة إتلاف آلات وأدوات الحاسوب الآلي الرقمي

2- جريمة الاستخدام غير المستحق لأدوات وآلات الحاسوب الآلي الرقمي

أما موقف التشريع العربي إزاء الجريمة المعلوماتية، فقد صدر القانون العربي النموذجي لمكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات أو بواسطتها خاصة المواد 1، 2، 3، 4².

وجاء في المادة الأولى منه تعريف الجريمة الإلكترونية - ومنها الجرائم التي تقع على نظم الاتصالات الحديثة، وعلى الوسيط الإلكتروني بأن المقصود به هو شبكة الحاسب الآلي أو الانترنت أو أي شبكة إلكترونية أخرى.

أما المادة الثانية فقد نصت على تجريم الاختراق غير المشروع أو البقاء غير المشروع في النظم المعلوماتية سواء كان في صورة بسيطة أو صورته المشددة. ونصت المادة الثالثة على تجريم حالات الإتلاف المعلوماتي التي تقع على شبكات المعلومات وتؤدي إلى إتلاف البيانات أو برامج الحاسب الآلي التي تشغل هذه الشبكات وفي المادة الرابعة نصت على النصب المعلوماتي والتي يترتب عليها الحصول على المعلومات المخزنة أو البيانات عن طريق التحايل أو الالتقاط غير المشروع. هذا عن الموقف الجماعي للمنظومة التشريعية العربية أما على مستوى التشريعات الفردية العربية فنورد موقف المشرع الجزائري.

¹ هدى حامد قشقوش، المرجع السابق، ص 49 إلى 73 .

² عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، دار النهضة العربية، مصر، 2009، ص 52 .

نلاحظ أن المشرع الجزائري في تعديل قانون العقوبات رقم 04 / 15 المؤرخ 10 / 11 / 2004 لم ينص على تعريف الجريمة المعلوماتية، بل اكتفى بذكر العقاب على بعض الأفعال تحت عنوان: " الجرائم الماسة بنظام المعالجة الآلية للمعطيات "، غير أن المشرع الجزائري تدارك الفراغ القانوني في هذا المجال من خلال القانون رقم 09 / 04 المؤرخ في 26 أوت 2009 المتضمن القواعد الخاصة للوقاية من هذه الجرائم، حيث ورد في الثانية منه " الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية " ¹. وهي المادة التي وضحت رغبة المشرع الجزائري في تبني مبدأ المرونة في الصياغة التشريعية حتى تستوعب الأنشطة الإجرامية الإلكترونية التي يتعذر حصرها وتحديدتها لسرعة تطورها.

المبحث الثاني: أركان الجريمة المعلوماتية في التشريع المقارن والجزائري

تتمثل أركان الجريمة المعلوماتية مثل الجريمة العادية في الركن الشرعي و المادي و المعنوي

المطلب الأول: الركن الشرعي والمادي للجريمة المعلوماتية في التشريع المقارن والجزائري

الفرع الأول: الركن الشرعي للجريمة المعلوماتية في التشريع المقارن والجزائري

معناه اعتراف المشرع والنص على تجريم الفعل المرتكب " لا جريمة ولا عقوبة إلا بنص "... بالنسبة للتشريع الجزائري فقد احدث قسم في قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات و الجنح ضد الاموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات ².

الفرع الثاني: الركن المادي للجريمة المعلوماتية في التشريع المقارن والجزائري

يتكون الركن المادي للجريمة الالكترونية من السلوك الاجرامي و النتيجة و العلاقة السببية، علما أنه يمكن تحقق الركن المادي دون تحقق النتيجة، كالتبليغ عن الجريمة قبل تحقيق نتيجتها، (مثلا: انشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة الا أنه لا مناص من معاقبة الفاعل). ويتخذ صور في الاعتداء على نظم المعالجة الآلية للمعطيات متمثلة في:

¹ انظر المادة الثانية من قانون رقم 09 - 04 مؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها، جريدة رسمية الصادرة بتاريخ 1 غشت 2009، عدد 47، ص 5 .

² القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المتمم والمعدل لأمر رقم (66-155)، المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، جريدة رسمية عدد 71.

- الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات.
- الاعتداءات العمدية على نظام المعالجة الآلية للمعطيات.
- الاعتداءات العمدية على سلامة المعطيات الموجودة داخل النظام.

أولاً: الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات:

نصت عليه المادة 02 من الاتفاقية الدولية للإجرام المعلوماتي. الصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء غير المشروع، فيما الصورة المشددة تتحقق بتوافر الظروف المشددة لها و يكون في الحالة التي ينتج فيها عن الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو تخريب لنظام اشتغال المنظومة. أما التشريع الجزائري نص عليها في المادة 394 مكرر قانون العقوبات: "يعاقب بالحبس من ثلاثة أشهر إلى سنة و بغرامة من 50000 إلى 100000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك" تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة "تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 50000 إلى 150000 دج"¹.

ثانياً: الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات:

نصت عليه المادتين 05 و 08 من الاتفاقية الدولية للإجرام المعلوماتي². لم يورد المشرع الجزائري نصاً خاصاً بالاعتداء العمدي على سير النظام و اكتفى بالنص على الاعتداء العمدي على المعطيات الموجودة بداخل النظام و ربما يجد ذلك تفسيره في أن الاعتداء على المعطيات قد يؤثر على صلاحية النظام للقيام بوظائفه، و قد وضع الفقه معياراً للتفرقة بين الاعتداء على المعطيات و الاعتداء على النظام على أساس ما إذا كان الاعتداء وسيلة أم غاية. فإذا كان الاعتداء الذي وقع على المعطيات مجرد وسيلة فإن الفعل يشكل جريمة الاعتداء العمدي على النظام، أما إذا كان الاعتداء الذي وقع على المعطيات غاية فإن الفعل يشكل جريمة الاعتداء العمدي على المعطيات.

¹ المرجع نفسه، المادة 394 مكرر.

² - آمال قارة، الحماية الجزائرية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة و النشر، الجزائر 2006 ص

ثالثا: الاعتداءات العمدية على سلامة المعطيات الموجودة داخل النظام
نصت عليها المادة 08,04,03 من الاتفاقية الدولية للإجرام المعلوماتي، كما نص المشرع الجزائري
عليها في المادة 394 مكرر² في قانون العقوبات، ويتخذ الاعتداء العمدي صورتان:
- الصورة الأولى: الاعتداءات العمدية على سلامة المعطيات الموجودة داخل النظام
النشاط الإجرامي في جريمة الاعتداء العمدي على المعطيات يتجسد في إحدى الصور الثلاث
التالية¹:

* الإدخال L'intrusion.

* المحو L'effacement.

* التعديل Modification.

لا يشترط اجتماع هذه الصور، بل يكفي أن يصدر عن الجاني إحداها فقط لكي يتوافر الركن
المادي

- الإدخال L'intrusion:

يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية، أم كان
يوجد عليها معطيات من قبل.

- المحو L'effacement:

يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة و الموجودة داخل النظام أو تحطيم
تلك الدعامة، أو نقل و تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة.

- التعديل Modification:

يقصد بفعل التعديل تغيير المعطيات الموجودة داخل نظام و استبدالها بمعطيات أخرى، و يتحقق
فعل المحو و التعديل عن طريق برامج غريبة بتلاعب في المعطيات سواء بمحوها كلياً أو جزئياً أو
بتعديلها و ذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات و برنامج المحاة Gomme
d'effacement أو برنامج الفيروسات بصفة عامة².

¹ - آمال قارة، المرجع السابق، ص 120.

² - آمال قارة، المرجع السابق، ص 122.

- الصورة الثانية: المساس العمدي على سلامة المعطيات الموجودة خارج النظام

نص المادة 394 مكرر² يستهدف حماية المعطيات في حد ذاتها لأنه لم يشترط أن تكون داخل نظام المعالجة الآلية للمعطيات أو أن يكون قد تم معالجتها آلياً، فمحل الجريمة هو المعطيات سواء كانت مخزنة كأن تكون مخزنة على أشرطة أو أقراص أو تلك المعالجة آلياً أو تلك المرسلة عن طريق منظومة معلوماتية، ما دامت قد تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

المطلب الثاني: الركن المعنوي للجريمة المعلوماتية في التشريع المقارن والجزائري

إن الركن المعنوي في مختلف الاعتداءات الماسة بالأنظمة المعلوماتية تتخذ صورة القصد الجنائي إضافة إلى نية الغش ويختلف باختلاف أشكالها وعليه ارتأينا التعرض للركن المعنوي لكل جريمة على حده.

الفرع الأول: الدخول و البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات:

الولوج و التحول و البقاء داخل نظام المعالجة الآلية للمعطيات لا يجزمان إلا تما عمداً. المادة 02 من الاتفاقية الدولية للإجرام المعلوماتي تسمح للدولة العضو أن تشترط بأن ترتكب الجريمة عن طريق خرق الحماية الفنية للنظام بهدف الحصول على المعطيات الموجودة بداخله. جريمة الدخول أو البقاء داخل النظام جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصره العلم و الإرادة.

فيلزم لتوافر الركن المعنوي أن تتجه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء و أن يعلم الجاني بأنه ليس له الحق في الدخول إلى النظام و البقاء فيه، و عليه لا يتوافر الركن المعنوي إذا كان دخول الجاني أو بقاءه داخل النظام مسموح به أي مشروع، كما لا يتوافر هذا الركن إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء أو في نطاق هذا الحق، كأن يجهل بوجود حظر للدخول أو البقاء، أو كان يعتقد خطأ أنه مسموح له بالدخول، فإذا توافر القصد الجنائي بعنصره العلم و الإرادة فإنه لا يتأثر بالباعث على الدخول أو البقاء فيظل القصد قائماً حتى و لو كان الباعث هو الفضول أو إثبات القدرة على المهارة و الانتصار على النظام¹. بالنسبة لنية الغش تبدو من خلال الغش الذي يتم به الدخول من خرق الجهاز الرقابي الذي يحمي النظام،

¹ - علي عبد الله القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت،

1999، ص 136-137.

بالنسبة للبقاء فيستنتج من العمليات التي تمت داخل النظام. في الحقيقة أن الدخول و البقاء بالغش لا يتضمن معنى خرق الجهاز الرقابي للنظام، إنما يظهر من خلال الولوج دون وجه حق إلى النظام إلا أن الجهاز الرقابي ما هو إلا وسيلة لإثبات أن الدخول للنظام غير مرمخص به.

الفرع الثاني: الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات:

إن هذه الجريمة جريمة عمدية، إذ أن من المفترض أن أفعال العرقلة والتعطيل لا تكون إلا عمدية وهذا ما يميزه عن الاعتداء غير العمدي لسير النظام الذي يشكل ظرفا مشددا لجريمة الدخول والبقاء الغير مشروع داخل النظام وعليه فالقصد الجنائي مفترض يستنتج من طبيعة الأفعال المجرمة¹.

الفرع الثالث: الاعتداءات العمدية على سلامة المعطيات واستخدامها كوسيلة في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية:

أولا: الاعتداءات العمدية على سلامة المعطيات: جريمة الاعتداء العمدي على المعطيات جريمة عمدية يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصره العلم والإرادة، فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل كما يجب أن يعلم الجاني بان نشاطه الإجرامي يترتب عليه التلاعب في المعطيات، ويعلم أيضا أن ليس له الحق في القيام بذلك وأنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته². كما يشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجنائي العام نية الغش، لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير بل تتوافر الجريمة ويتحقق ركنها بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذلك واتجاه الإرادة إليه، وإن كان الضرر قد يتحقق في الواقع نتيجة النشاط الإجرامي إلا أنه ليس عنصرا في الجريمة.

ثانيا: استخدام المعطيات كوسيلة في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية:

وذلك إما بالتصميم أو البحث أو التجميع أو التوفير أو النشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية. حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان للمعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية. فإن هذا الاستخدام يجب أن يكون عمدا وبطريق الغش أي بتوافر القصد الجنائي العام إضافة إلى القصد الجنائي الخاص المتمثل في نية الغش.

¹ - علي عبد القادر القهوجي، المرجع نفسه، ص142.

² - علي عبد القادر القهوجي، المرجع السابق، ص145.

خاتمة: في ختام هذه الدراسة المتعلقة بالجريمة المعلوماتية دراسة مقارنة يمكن أن نقول أن هذه الجريمة تتميز باختلاف تعاريفها المتنوعة التي بنيت على معيار وسيلة ارتكاب الجريمة أو محل الجريمة أو بواعث ودوافع ارتكاب الجريمة أو المستند على معايير مختلفة ومتنوعة ، أو من خلال تصدى الأنظمة التشريعية لبيان تعريفها وأركانها الثلاثة المعروفة للجرائم التقليدية لكن هذه الأركان تتميز بخصوصيات تجعلها متميزة نوعاً ما عن الأولى.

من خلال الدراسة توصلنا إلي جملة من النتائج:

- بالنظر لحداثة هذا السلوك الإجرامي والذي يتجسد في الجريمة المعلوماتية، فإنه لا يوجد لحد الآن إجماع فقهي أو قانوني موحد على تعريف لها مما أدى بالقول أن الجريمة المعلوماتية تقاوم التعريف.
- قصور القوانين التقليدية أمام هذه الجرائم المستحدثة (الجريمة المعلوماتية).
- إن التطور التكنولوجي والتقني يحتم على المشرع تعديل القواعد القانونية، خاصة في مجال القوانين المتعلقة بمكافحة الجريمة المعلوماتية لم تعد قابلة للتطبيق في بيئة الرقمية.
- في ضوء النتائج السابقة التي أظهرتها الدراسة نستخلص إلى بعض الاقتراحات المتمثلة في:
 - ضرورة إعطاء تعريف موحد للجريمة المعلوماتية يشمل فيه كل السلوكات المجرمة.
 - توعية المجتمع وخلق له ثقافة اجتماعية جديدة عن هذه الجرائم بأنها أعمال غير مشروعة ويتعرض صاحبها لعقوبات جزائية.
 - تدريس مواد الأنظمة المعلوماتية والجرائم في المدارس و كليات الحقوق والمعاهد القضائية.
 - عند وضع النصوص يجب أن يدقق في حماية المواطن، على أساس أن حماية الأمن الرقمي يمكن أن تحيل على مفاهيم متعددة تتراوح ما بين حماية الأشخاص، وحماية المجموعات وغيرها.
- ضرورة التعاون الدولي لمكافحة هذه جرائم من خلال مجموعة تشريعات وطنية واتفاقيات دولية وإقليمية.

قائمة المراجع:

الكتب:

- 01- آمال قارة، الحماية الجزائرية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة و النشر، الجزائر 2006.
- 02- أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2006 .
- 03- زبيخة زيدان، الجريمة المعلوماتية في التشريع الجزائري و الدولي، دار الهدى، عين مليلة، الجزائر، 2011 .
- 04- عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، دار النهضة العربية، مصر، 2009 .
- 05- علي عبد الله القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت، 1999.
- 06- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، ط1، دار النهضة العربية، القاهرة، 1994.
- 07- محمد سامي الشوا: ثورة المعلومات و انعكاساتها على قانون العقوبات، الهيئة المصرية العامة للكتاب، 2003 .
- 08- محمد علي العريان: الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الازارطة، 2004 .
- 09- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، دراسة تطبيقية ونظرية، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2005.
- 10- هدى حامد قشقوش، جرائم التشريع الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992 .
- 11- هشام محمد فريد رسم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الكاتبة، مصر، 1995 .

القوانين:

- 01 القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتتم والمعدل لأمر رقم (66-155) المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، جريدة رسمية عدد 71.

02- القانون رقم 09 – 04 مؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها، جريدة رسمية الصادرة بتاريخ 1 غشت 2009، عدد 47 .

المواقع الإلكترونية:

يونس عرب، جرائم الكمبيوتر والانترنت المعنى والخصائص والصور واستراتيجية المواجهة القانونية، أكتوبر، 2006، منشورات على الموقع الالكتروني:
www.doc.abhatoo.net.ma/img/doc/dios.doc.p1-6

خصوصية الجريمة المعلوماتية

ط.د/ صابر فايدة

كلية الحقوق والعلوم السياسية

جامعة برج بوعرييج

ط.د/ حمزة عشاش

كلية الحقوق والعلوم السياسية

جامعة المسيلة

مقدمة:

تشهد الحياة اليومية تطورات كبيرة في مجال تكنولوجيا الإعلام والاتصال، فالعالم اليوم يعيش أزهى عصوره العلمية والتكنولوجية بسبب هذه الثورة المعلوماتية، هذه الأخيرة إرتقت بمستوى الإنسان إلى العصر المعلوماتي، غير أنها في نفس الوقت مثلت أداة يستعملها مجرموا المعلوماتية، مما أدى إلى ما يسمى بمصطلح الجرائم الإلكترونية أو بمفهوم آخر الجرائم المعلوماتية.

فالنشاط الإجرامي اليوم لم يعد مقتصرًا على فقط على الوسائل التقليدية المعروفة بل أضحى بالإضافة إلى ذلك يعتمد على أكثر حداثة، وذلك بالاستعانة بنظم المعلومات والاتصالات، وهذا ما يجسد الجانب المظلم الذي يواجه المشرع الجنائي في إثبات هذا النوع من الجرائم، ورغم كل هذا فإن المشرع الجزائري تدخل للتصدي لهذه الظاهرة، إنطلاقًا من تجريم ومعاقبة مرتكبي الجريمة المعلوماتية، حيث حدد مجموعة من الأحكام لقيام هاته الجريمة وتحديد العقاب المقرر لها.

ومن هذا المنطلق والمعطيات المذكورة فإن الإشكالية التي تطرح بخصوص هذا الموضوع تتمثل في:

ما المقصود بالجريمة الإلكترونية كمصطلح متميز عن الجريمة التقليدية من حيث المفهوم والأركان؟
ولالإجابة على هذه الإشكالية والإلمام بمختلف جوانب الموضوع تم تقسيم الدراسة إلى مبحثين أساسيين، تناولنا مفهوم الجريمة المعلوماتية في المبحث الأول، في حين تطرقنا في المبحث الثاني إلى أركان هذه الجريمة.

المبحث الأول: مفهوم الجريمة الإلكترونية

إن دراسة مفهوم الجريمة المعلوماتية يقتضي إبراز وتحديد مدلول هذه الجريمة باعتبار أنها تختلف عن الجرائم التقليدية وهو الأمر الذي أثار إختلافا في تعريفها (المطلب الأول)، زيادة على ذلك فإننا سنبين الخصائص التي تتميز بها الجريمة المعلوماتية عن الجريمة التقليدية (المطلب الثاني)، في حين سندرس طبيعة هذا النوع من الجرائم في ظل التشريع الجنائي الجزائري (المطلب الثالث).

المطلب الأول: تعريف الجريمة المعلوماتية

ما يلاحظ في مجال الجريمة المعلوماتية أنه لا يوجد مصطلح موحد للدلالة على هذه الظاهرة، فهناك من يطلق عليها ظاهرة الغش المعلوماتي أو الإختلاس المعلوماتي أو الجريمة السيبرانية أو الإلكترونية، وعلة هاته الإختلافات هو خشية حصر هذه الجريمة في مجال ضيق⁽¹⁾، وعليه سنتطرق إلى مختلف التعريفات الفقهية التي قيلت بشأن الجريمة المعلوماتية بحسب ضيقها أو إتساعها، بالإضافة إلى التعريف الذي قدمه المشرع الجزائري لهذه الجريمة.

أولا: التعريف الضيق للجريمة المعلوماتية

من التعريفات التي وضعها أنصار الإتجاه الضيق للجريمة المعلوماتية بأنها " تلك التي يكون الغرض منها موجه ضد الأموال المعلوماتية متى كانت مرتبطة بإستخدام نظام المعالجة الآلية للمعطيات، مع إقصاء تلك الأفعال المتمثلة في إستخدام الإعلام الألي كوسيلة للإعتداء على الغير، سواء الأشخاص أو الثقة العامة، كما تبني الفقهاء الفرنسيين تعريفا أضيق من ذلك حيث عرفوها كل الأفعال غير المشروعة الموجهة ضد نظام المعالجة الآلية للمعطيات.⁽²⁾

فالجريمة المعلوماتية حسب هذا المذهب هي تلك التي تقع على جهاز الكمبيوتر أو في محيطه داخل نظامه فقط⁽³⁾، والأخذ بالتعريف الضيق يجعل الإجرام المعلوماتي محصورا في

(1) محمد علي العريان، الجرائم المعلوماتية، الطبعة الأولى، دار الجامعة الجديدة للنشر والتوزيع، مصر، 2004، ص 43.

(2) أمين طعباش، الحماية الجنائية للمعاملات الإلكترونية، الطبعة الأولى، مكتبة الوفاء القانونية للنشر والتوزيع، مصر، 2015، ص 15.

(3) مختارية بوزيدي، ماهية الجريمة الإلكترونية، مداخلة مقدمة ضمن فعاليات الملتقى الوطني الذي نظمه مركز جيل البحث العلمي، الموسوم بعنوان: آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر، 29 مارس، 2017، ص 10.

الإعتداءات الواقعة على النال المتداولة في هذا المجال أو على الإعتداءات الموجهة ضد النظام المعلوماتي، دون أن تدخل في إطارها - حسب هذا التعريف - الجرائم الماسة بالحياة الخاصة للأفراد كالسب أو القذف مثلاً.⁽¹⁾

ثانياً: التعريف الواسع للجريمة المعلوماتية

نظراً للإنتقادات التي وجهت للتعريف الضيق للجريمة المعلوماتية، حاول الفقهاء تعريفها على نحو واسع لتفادي القصور الذي لحق بتعريفات الإتجاه الضيق.

وعليه، فقد ذهب هذا الإتجاه إلى التوسيع من مفهوم الجريمة الإلكترونية، فأرأوا بأنها تشمل استخدام الحاسب كأداة لإرتكاب الجريمة، بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسوب المجني عليه أو بياناته، كما تمتد هذه الجريمة لتشمل الإعتداءات المادية⁽²⁾، سواء كان هذا الإعتداء على جهاز الحاسوب ذاته أو المعدات المتصلة به، وكذلك الإستخدام غير المشروع لبطاقات الإئتمان، وإنتهاك ماكينات الحسابات الآلية، بما يتضمنه من شبكات تمويل الحسابات المالية بطريقة إلكترونية، وتزيف المكونات المادية والمعنوية للحاسوب، وحتى سرقة الحاسوب في حد ذاته أو مكون من مكوناته⁽³⁾.

كما نجد من التعريفات الواسعة لهذه الظاهرة الإجرامية أنها "كل عمل أو إمتناع يأتيه الإنسان إضراراً بمكونات الحاسب المادية والمعنوية وشبكات الإتصال الخاصة به بإعتبارها من المصالح والقيم المتطورة التي تمتد نصوص قانون العقوبات لحمايتها، فهي كل فعل إجرامي أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالضحية أو كل كسب يحققه الجاني"⁽⁴⁾.

والأخذ بالتعريفات الواسعة للجريمة المعلوماتية يدخل في نطاقها كل السلوكات غير المشروعة التي لها علاقة بالحاسوب مهما كان دوره فيها، سواء كان وسيلة أو مناسبة لإرتكاب التصرفات غير المشروعة أو كان موضوعاً لها.

(1) أمين طعباش، المرجع السابق، ص 17.

(2) يوسف جفال، التحقيق في الجريمة الإلكترونية، مذكرة ماستر، جامعة محمد بوضياف المسيلة، كلية الحقوق

والعلوم السياسية، قسم الحقوق، 2016-2017، ص 11.

(3) محمد علي العريان، المرجع السابق، ص 45.

(4) أمين طعباش، المرجع السابق، ص 16.

ثالثا: تعريف المشرع الجزائري للجريمة المعلوماتية

جرم المشرع الجزائري الجريمة المعلوماتية نتيجة تأثر الجزائر بالثورة المعلوماتية التي نتج عنها أشكال جديدة من الجرائم، وذلك من خلال التعديل الذي أدخله على قانون العقوبات بموجب القانون 04-15⁽¹⁾ المتمم لقانون العقوبات⁽²⁾ الذي أفرد لها قسما خاصا بها في المواد من 394 مكرر إلى 394 مكرر 07.

وإستعمل القانون رقم 04-09⁽³⁾ تسمية " المساس بأنظمة المعالجة الآلية للمعطيات " للدلالة على الجريمة المعلوماتية معتبرا في ذلك أن النظام المعلوماتي في حد ذاته وما يشمله من مكونات غير مادية محلا للجريمة، ليلتحق بذلك المشرع الجزائري بركب التشريعات الجنائية التي قدمت تعريفا للجريمة والنظم المعلوماتية⁽⁴⁾، حيث جاء ذلك في المادة 02 من نفس القانون، فنصت الفقرة "أ" على أن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية، وعرفت الفقرة " ب " من نفس المادة المنظومة المعلوماتية بأنها " مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين. ".

(1) القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتمم لقانون العقوبات، الجريدة الرسمية العدد 71، الصادرة بتاريخ 10 نوفمبر 2004.

(2) الأمر رقم 66-156 المؤرخ في 10 جوان 1966 يتضمن قانون العقوبات المعدل والمتمم، الجريدة الرسمية العدد 49، بتاريخ 11 جوان 1966.

(3) القانون رقم 04-09 المؤرخ في 05 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47، الصادرة بتاريخ 16 أوت 2009.

(4) سعيدة بعرة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر، جامعة محمد خيضر بسكرة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2015-2016، ص 30.

المطلب الثاني: خصائص الجريمة الإلكترونية

لجريمة الإلكترونية عدة خصائص تميزها عن الجريمة الكلاسيكية يمكن إجمالها فيما يلي:

أولاً: الجريمة المعلوماتية جريمة عابرة للحدود

ساهمت شبكة المعلومات في توسيع عملية الإتصال وتبادل المعلومات بين الدول والأنظمة التي يفصل بينها آلاف الأميال، ومع القدرة التي يتمتع بها الحاسب أدى ذلك إلى إمكانية ارتكاب الجريمة المعلوماتية في أماكن متعددة من العالم وفي وقت واحد، كما يمكن أن يكون المجني عليه في غير الدولة التي يقيم فيها الجاني⁽¹⁾.

ثانياً: صعوبة إثبات الجريمة الإلكترونية

وذلك نظراً لإرتكابها في الخفاء، وعدم وجود أي أثر إيجابي لما يجري خلال تنفيذها من أفعال إجرامية، حيث يتم نقل المعلومات إلكترونياً، فضلاً عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الواحدة، زيادة على ذلك أن الجريمة المعلوماتية لا عنف فيها وإنما هي أرقام وبيانات تمحى من السجلات المخزنة في ذاكرة الحاسوب، حيث تصبح غير مرئية وبمعنى آخر فالجرائم الإلكترونية جرائم فنية هادئة⁽²⁾.

ثالثاً: ارتكاب الجرائم المعلوماتية بالحاسب الآلي

تعتبر هذه الخاصية من أهم الخصائص التي تميز الجرائم المعلوماتية عن الجرائم الكلاسيكية، ذلك لأن شبكة الأنترنت هي إحدى التقنيات الحديثة التي أفرزها تطور الحاسوب، ولذلك فإن إرتباطها بالحاسب الآلي هو أمر لا مفر منه باعتباره النافذة التي تطل بها تلك الشبكة على العالم الخارجي⁽³⁾.

رابعاً: خصوصية مرتكبي الجرائم المعلوماتية

فالجريمة الإلكترونية تتأثر بالمستوى العلمي للمجرم كقاعدة عامة عكس الجريمة التقليدية التي لا تتطلب عادة الإختصاص والمعرفة في مجال تقنية المعلومات، وقد يتعدد تصنيف مجرمي

(1) خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية للطباعة والنشر والتوزيع، مصر، 2008، ص 82.

(2) يوسف جفال، المرجع السابق، ص 13.

(3) أمين طعباش، المرجع السابق، ص 21.

الجرائم المعلوماتية إلى المخترقين والمحترفين والحاquدين، وذلك نظرا للصفات التي تتمتع بها مثل هذه الجرائم⁽¹⁾.

المطلب الثالث: الطبيعة القانونية للجريمة المعلوماتية

على اعتبار ان التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة الى بروز اشكال جديدة من الاجراء، دفع ذلك بالتشريعات الجنائية الى النص على معاقبة هذا النوع من الجرائم، بهدف توفير الحماية الجزائية للأنظمة المعلوماتية واساليب المعالجة الآلية للمعطيات، فقام المشرع الجزائري بتعديل قانون العقوبات بموجب القانون 04-15 مستعملا في ذلك التسمية التي سبق ذكرها أي " المساس بأنظمة المعالجة الآلية للمعطيات "

وقدر المشرع من خلال هذا التعديل ان جوهر المعلوماتية هي المعطيات التي تدخل الى الحاسوب فتحولها الى معلومات بعد معالجتها و تخزينها، فقام بحماية هذه المعطيات من عدة زوايا⁽²⁾، وبصدور القانون 04-09 السابق الذكر عبر فيه المشرع الجزائري عن الجريمة المعلوماتية بتسمية "الجرائم المتصلة بتكنولوجيات الإعلام والإتصال".

وما يلاحظ في هذا الشأن ان المشرع الجزائري لم يستقر على تسمية واحدة، حيث اعتمد على تسميات مختلفة بين قانون العقوبات و القوانين المكملة في المجال الجنائي، فسمها بجريمة المساس بأنظمة المعالجة الآلية للمعطيات في قانون العقوبات المتمم بالقانون 04-15، في حين أعطاها تسمية الجرائم المتصلة بتكنولوجيات الإعلام والإتصال في القانون 04-09، ورغم هذا الاختلاف فإن هاتين التسميتين وغيرها من التسميات الأخرى تصب في هدف واحد وهو مجابهة ومكافحة الجريمة الإلكترونية.

فمن حيث التكييف القانوني فتتخذ هذه الجرائم طبيعة خاصة إذا لم تكن القواعد التقليدية مخصصة لهذه الظواهر الإجرامية المستحدثة، وتطبيق النصوص التقليدية على الجرائم المعلوماتية يثير العديد من المشاكل، والتي في مقدمتها صعوبة إيجاد دليل مادي يدين مرتكب الجريمة⁽³⁾.

(1) عبد الله دغش الجمعي، المشكلات العملية والقانونية للجرائم الإلكترونية، رسالة ماجستير، جامعة الشرق الأوسط، قطر، 2014، ص 21.

(2) سعيدة بكرة، المرجع السابق، ص 32.

(3) نفس المرجع، ص 35.

أما عن محل الجريمة المعلوماتية فيتميز عن محل الجريمة التقليدية، فمحل الجريمة الأولى هو المال المعلوماتي تمييزا لماليتها المغايرة للمال التقليدي في الجريمة الثانية بكل مكوناته، فالجريمة المعلوماتية تشمل كل من أفعال السرقة أو التغيير أو حذف المعلومات مثل النشاط الجرمي الذي يستهدف إختراق بريد إلكتروني والعبث بمحتوياته، والذي يحمل في طياته إنتهاك الخصوصية وحقوق الملكية الفكرية وأنماط جرمية أخرى⁽¹⁾.

المبحث الثاني: أركان الجريمة المعلوماتية

تشكل الجريمة المعلوماتية من الأركان الثلاثة المعروفة للجريمة الكلاسيكية، غير أن الأولى تتميز بخصوصيات تجعلها تختلف نوعا ما عن الجريمة الثانية، وهذا ما سنبينه من خلال هذا المبحث بتفصيل الأركان الثلاثة لهذه الجريمة، والمتمثلة في الركن الشرعي للجريمة المعلوماتية (المطلب الأول)، والركن المادي لها (المطلب الثاني)، وأخيرا الكن المعنوي لقيامها (المطلب الثالث).

المطلب الأول: الركن الشرعي للجريمة المعلوماتية

إنطلاقا من مبدأ الشرعية وفقا لأحكام المادة الأولى من قانون العقوبات الجزائري التي تنص على " لا جريمة ولا عقوبة أو تدابير أمن بغير قانون "، جرم القانون رقم 04-15 بعض صور الجريمة المعلوماتية ونص على العقوبات المقررة لمرتكبيها في القسم السابع مكرر تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات " من الفصل الثالث المعنون بـ " الجنايات والجنح ضد الأموال من الباب الثاني المتعلق بالجنايات والجنح ضد الأفراد، وذلك في المواد من 394 مكرر إلى 394 مكرر 08 من قانون العقوبات المعدل والمتمم.

في حين جاء القانون 09-04 السابق الذكر متضمنا للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها كجانب وقائي يحد من وقوع الجرائم المعلوماتية من خلال وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها، والقيام بإجراءات التفتيش داخل المنظومة المعلوماتية⁽²⁾.

ولجوء المشرع إلى تقنين أو النص على مثل هذه الجرائم وجعلها في نطاق مبدأ الشرعية يمنع القاضي من اللجوء إلى القياس، بمعنى عدم جواز لجوء القاضي الجنائي إلى قياس فعل لم يرد نص

(1) أمين طبعا، المرجع السابق، ص 19، 20.

(2) المادة 03 من القانون 09-04 السابق الذكر.

تجريمه على فعل ورد نص بتجريمه، فيقرر القاضي الجنائي للأول عقوبة الثاني بسبب التشابه بين الفعلين (1).

المطلب الثاني: الركن المادي للجريمة المعلوماتية

يعتبر الركن المادي لأي جريمة هو المظهر الخارجي لها وكيانها المادي، وهو الماديات المحسوسة في العالم الخارجي كما حددها نصوص التجريم، فالقاعدة أنه " لا جريمة دون ركن مادي " أو " لا جريمة دون فعل " (2)، إلا أن الركن المادي للجريمة المعلوماتية يختلف نوعا ما عن الجرائم التقليدية كون أنه يقوم على صور في فعل الإعتداء والمتمثلة في:

أولاً: الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو الشروع في ذلك

نصت المادة 394 مكرر من قانون العقوبات على أن الدخول أو الدخول والبقاء غير المشروع في نظام المعالجة الآلية أو الشروع في ذلك يشكل فعلا إجراميا، ولهذا الفعل حسب المادة المذكورة صورتين كالتالي:

1- الصورة البسيطة

يتمثل النشاط الإجرامي في هذه الصورة في الأفعال الآتية:

أ- **فعل الدخول:** يتحقق فعل الدخول بمجرد الوصول إلى المعلومات المخزنة داخل النظام ودون علم ورضا صاحبه، لأن هذا النظام لا يسمح للدخول فيه إلا لأشخاص معينين أو يسمح بالدخول لكن مقابل نفقات.

ب- **البقاء:** معنى البقاء هو التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، أو بتجاوز المدة المسموح له بالبقاء فيها، أو عدم الإنسحاب فورا وقطع وجوده في نظام البيانات أو بطبع معلومات حين يسمح له بالرؤية فقط (3).

2- الصورة المشددة

(1) أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي للنشر والتوزيع، مصر، 2006، ص 10.
(2) عبد الرحمان خلفي، محاضرات في القانون الجنائي العام، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2013، ص 101.
(3) سعيدة بكرة، المرجع السابق، ص 53.

نصت المادة 394 مكرر في الفقرتين الثانية والثالثة من قانون العقوبات على ظروف تشديد عقوبة فعل الدخول والبقاء غير المشروع عندما ينتج عن هذين الفعلين إما محو أو تحويل المعطيات التي يحتويها النظام وإما عدم صلاحية النظام لأداء وظائفه من خلال تخريب نظام إشغال المنظومة.

ثانيا: إدخال المعطيات بطريق الغش

يقصد بفعل الإدخال حسب المادة 394 مكرر 01 من قانون العقوبات إضافة معطيات جديدة إلى نظام المعالجة الآلية أو التعديل من معلومات داخله كان يتضمنه مسبقا فغير فيها، ومثال ذلك حالة الإستخدام التعسفي لبطاقات السحب والإئتمان سواء من صاحبها الشرعي أو عن غيره كحالة السرقة والتزوير⁽¹⁾.

المطلب الثالث: الركن المعنوي للجريمة المعلوماتية

يتخذ الركن المعنوي في أغلب الجرائم بصفة عامة صورة القصد الجنائي، والذي يتحقق بتوافر إرادة القيام بعمل غير شرعي لدى الجاني مع علمه بأن القانون يجرمه⁽²⁾، ونفس الأمر ينطبق على الجريمة المعلوماتية التي يقوم ركنها المعنوي على توافر الإرادة الجرمية لدى الفاعل، وهذا ما يظهر من خلال إستعمال المشرع الجزائري لعبارة " الغش " و " العمد " و " الإعداد لجريمة " في المواد 394 مكرر و 394 مكرر 1 و 394 مكرر 2 و 394 مكرر 5 من قانون العقوبات، وهذا إن دل فإنما يدل على أن الجريمة المعلوماتية جريمة عمدية بإمتياز ولا يفترض فيها عنصر الخطأ.

هذا ويختلف الركن المعنوي في الجرائم المعلوماتية من جريمة إلى أخرى، فجريمة الدخول غير المصرح به إلى نظام الحاسب الآلي تتطلب قصدا جنائيا يتمثل في علم الجاني بعناصر الركن المادي للجريمة، أي العلم بأن الولوج إلى داخل النظام بشكل غير مصرح يعد جريمة باعتبار حماية المشرع لحل الحق وهو الحاسب الآلي لما يتضمنه من برامج ومعلومات⁽³⁾.

(1) أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية، دار هومو للطباعة والنشر والتوزيع، الجزائر، 2007، ص 121.

(2) احسن بوسقيعة، الوجيز في القانون الجنائي العام، الطبعة الرابعة عشر، دار هومو للطباعة والنشر والتوزيع، الجزائر، 2014، ص 145.

(3) يوسف جفال، المرجع السابق، ص 17.

وفي جريمة الاحتيال الإلكتروني التي بدورها تعد جريمة عمدية يتطلب لقيامها توافر القصد الجنائي لقيام مسؤولية الجاني، والقصد الجنائي المشترط هو القصد الجنائي بنوعيه العام والخاص، فالجرم يعلم بأنه يخالف القانون بسلوكه مع إتجاه نيته إلى تحقيق ربح غير مشروع له أو للغير أو تجريد شخص آخر من ممتلكاته على نحو غير مشروع⁽¹⁾.

خاتمة:

مما سبق، يمكن القول أن الجريمة المعلوماتية هي آفة أنتجت الثورة التكنولوجية والمعلوماتية، حيث لم تسلم منها كل دول العالم سواء كانت متطورة أو ضعيفة، مما جعل الجريمة المعلوماتية أو الإلكترونية كما يسميها البعض تمايز عن الجريمة الكلاسيكية بدءا بتسميتها وتعريفها وصولا إلى الأركان التي تقوم عليها.

وقد أدت الدراسة إلى إستخلاص مجموعة من النتائج يمكن إجمالها فيما يلي:

- عدم وجود مصطلح موحد للدلالة على الجريمة المعلوماتية، فهناك من يطلق عليها ظاهرة الغش المعلوماتي أو الاختلاس المعلوماتي أو الجريمة السيبرانية أو الإلكترونية، وعلة هاته الاختلافات هو خشية حصر هذه الجريمة في مجال ضيق وكلها تصب في معنى واحد.
 - عدم وجود إجماع فقهي بخصوص تعريف الجريمة المعلوماتية، حيث تباينت التعريفات بين المفهوم الواسع والمفهوم الضيق.
 - يلاحظ أن المشرع الجزائري لم يستقر على تسمية واحدة، حيث اعتمد على تسميات مختلفة بين قانون العقوبات و القوانين المكملة في المجال الجنائي، فسمّاها بجريمة المساس بأنظمة المعالجة الآلية للمعطيات في قانون العقوبات المتمم بالقانون 04-15، في حين أعطّاها تسمية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في القانون 09-04، ورغم هذا الاختلاف فإن هاتين التسميتين وغيرها من التسميات الأخرى تصب في هدف واحد وهو مجابهة ومكافحة الجريمة الإلكترونية.
 - تميز الجريمة المعلوماتية بعدة خصائص عن الجريمة التقليدية مع خصوصية أركان الجريمة المعلوماتية مقارنة مع الأركان التقليدية للجرائم العادية.
- هذا ونختتم هذه الدراسة ببعض التوصيات، وهي كما يلي:

(1) أحمد خليفة الملط، المرجع السابق، ص 121.

- ضرورة توحيد النظام التشريعي للجريمة المعلوماتية في قانون خاص كما هو الشأن بالنسبة للقانون رقم 06-01 المتعلق بالوقاية من الفساد ومكافحته، وكذا القانون رقم 04-18 المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الإستعمال والإتجار غير المشروعين بها.
- إدراج مقياس الجريمة المعلوماتية مع المقاييس المدرسة على مستوى كليات الحقوق وبالخصوص ضمن تخصص القانون الجنائي، وكذا تنظيم الأيام الدراسية والملتقيات التي تعالج تطور الإجرام المعلوماتي وكيفية التصدي له.
- ضرورة توعية المجتمع وخاصة مستخدمي شبكات الأنترنت بالمخاطر التي تنجر عن هكذا نوع من الجرائم.

الجريمة المعلوماتية ودوافع ارتكابها في التشريع الجزائري

د/ بن حليمة ليلى

كلية الحقوق والعلوم السياسية

جامعة المسيلة

د/ عشور سليم

كلية الحقوق والعلوم السياسية

جامعة المسيلة

مقدمة:

إن الجريمة ظاهرة اجتماعية ارتبطت في طبيعتها وحجمها بالتحولات المختلفة سواء كانت اقتصادية، اجتماعية وثقافية، الوطنية منها أو الدولية. ومن التحولات الجذرية التي شهدناها عصرنا الحالي والتي ساهمت وبطريقة قياسية في ارتقاء البشرية إلى مستويات عليا، ما يسمى بالثورة المعلوماتية وهي الثورة التي تزاوجت فيها شبكات الاتصال بما وصلت إليه من تطور مع الحاسوب، ذلك الجهاز الذي يملك قدرات هائلة للقيام بالعديد من الوظائف وفي ظرف قياسي.

هذا التمازج مكن الملايين من البشر الاتصال ببعضهم البعض وأتاح لهم الفرص للاطلاع على المعلومات وتبادلها، والقدرة على التفاوض وإبرام العقود والصفقات في ظل بيئة تحاكي واقع البشرية وهي البيئة الافتراضية أو الرقمية.

غير أنه وفي المقابل أنتجت هذه الثورة نمط جديد من الإجرام صنف في سياق الجرائم المستحدثة وهي جرائم المعلوماتية أو الالكترونية، وهي جرائم تمس في صميمها قيما جوهرية تمس الأفراد والمؤسسات وحتى الدول، وفي جميع مناحي الحياة، الأمر الذي خلف شعورا بعدم الثقة بخصوص التعامل والاستفادة من ثمار الثورة المعلوماتية، وبناء عليه فقد تم طرح الإشكالية الرئيسية التالية:

إلى أي مدى تم تحديد مفهوم الجريمة المعلوماتية من خلال تحديد الدوافع التي تؤدي إلى ارتكابها؟ وتندرج تحت هذه الإشكالية مجموعة من التساؤلات الفرعية:

- ما هو مفهوم الجريمة المعلوماتية؟، ما هي أركان الجريمة المعلوماتية؟، بماذا يتميز هذا النوع من الجرائم؟، و هل تختلف هذه الجريمة من حيث أشخاصها عن الجريمة التقليدية؟، و ما هي دوافع ارتكابها؟

أولاً: مفهوم الجريمة المعلوماتية.

أمام تعاظم دور الحاسب الآلي وانتشاره المذهل بسبب استخداماته المتعددة، تعاظمت معه مخاطره بسبب الجرائم التي ترتكب بواسطته، حيث ظهرت الجريمة المعلوماتية أول مرة في الدول المتقدمة ذات التكنولوجيا العالية، وعليه سنتطرق في هذا العنصر إلى دراسة تعريف الجريمة المعلوماتية أولاً ثم بيان طبيعتها القانونية، وبعدها دراسة أهم خصائصها.

1- تعريف الجريمة المعلوماتية:

إذا كانت الجريمة عموماً هي كل فعل غير مشروع صادر عن إرادة جنائية يقر له القانون عقوبة أو تدبيراً احترازياً¹ فإن الجريمة المعلوماتية حسب الفقه هي: « نشاط غير مشروع موجه للنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه»². أو هي: « كل سلوك إجرامي يتم بمساعدة الكمبيوتر أو هي كل جريمة تتم في محيط أجهزة الكمبيوتر»³.

وقد عرفها الأستاذ (فوريستر) في مؤلفه ثورة تقنية المعلومات بأنها: «فعل إجرامي تم باستخدام الحاسوب كأداة رئيسية»⁴.

كما عرفها الخبير الأمريكي (PARKER) بأنها «فعل إجرامي أيا كانت صلته بتقنية المعلومات، فيه يتكبد المجني عليه ونتيجة له خسارة ويحقق الفاعل ربها عمدياً»⁵.

أما المشرع الجزائري فقد عرف هذا النوع من الجرائم في الفقرة الأولى من المادة الثانية من القانون رقم 04-09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، حيث أطلق عليها مصطلح الجرائم المتصلة بتكنولوجيا

¹ - محمود نجيب حسني، شرح قانون العقوبات - القسم العام -، ط6، القاهرة: دار النهضة العربية، 1989، ص 40.

² - هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، ط1، القاهرة: دار النهضة العربية، 1992، ص 20.

³ - خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، دون طبعة، مصر: الدار الجامعية الجديدة، 2008، ص 42.

⁴ - أحمد خليفة الملط، جرائم المعلوماتية، ط2، الإسكندرية: دار الفكر الجامعي، 2006، ص 86.

⁵ - محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دون طبعة، مصر: الهيئة المصرية العامة للكتاب، 2003، ص 19.

الاعلام والاتصال وعرفها بأنها: «جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية»¹.

وبالتمعن في تعريف المشرع الجزائري يتضح لنا أنه أعطى مفهومًا موسعًا لهذا النوع من الجرائم، فبالرغم من تحديد مجالها من كونها متصلة بتكنولوجيات الاعلام والاتصال، إلا أنه ترك المجال مفتوحًا لتضم إليها أي نوع من أنواع الجرائم التي قد يسفر عنها التطور التكنولوجي وذلك من خلال عبارة «أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية».

2- الطبيعة القانونية للجريمة المعلوماتية.

إن دراسة الجريمة المعلوماتية بشكل خاص تدخل ضمن قسم من أقسام قانون العقوبات وهو القسم الخاص، ذلك الفرع الذي يدرس كل جريمة على حدى متناولًا كل عناصرها الأساسية والعقوبة المقررة لها، فالجريمة تتعلق بالقانون المعلوماتي لأنها ظاهرة إجرامية ذات طبيعة خاصة².

إن هذا النوع من الجرائم يرتكب ضمن نطاق المعالجة الإلكترونية للبيانات سواء أكان في تجميعها أو تجهيزها أم في إدخالها إلى الحاسب المرتبط بشبكة المعلومات ولغرض الحصول على معلومات معينة، كما قد ترتكب هذه الجرائم في مجال الكلمات أو معالجة النصوص وهذا النوع الأخير من الجرائم لا يعدُّ أن يكون مجرد طريقة أوتوماتيكية تمكن المستخدم من تحرير الوثائق والنصوص على الحاسب مع توفير إمكانات التصحيح والمسح والتخزين والاسترجاع والطباعة³.

¹ - القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، عدد رقم 47، الصادر بتاريخ 16 أوت 2009.

² - محمد زكي أبو عامر، علي عبد القادر القهوجي، قانون العقوبات - القسم الخاص، دون طبعة، القاهرة: دار النهضة العربية، 1993، ص 09.

³ - سعيد نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير (غير منشورة)، جامعة الحاج لخضر باتنة، 2013/2012، ص 41.

فهذه العمليات كلها هي وثيقة الصلة بالجرائم محل البحث وعليه لابد للجاني من فهمها، فضلا عن أن الجاني قد يتعامل مع مفردات جديدة كالبرامج والمعطيات التي تشكل محل الاعتداء أو تستخدم وسيلة له¹.

تكمن الطبيعة الخاصة لهذه الجرائم في قدرة شبكة المعلومات على نقل وتبادل معلومات ذات طابع شخصي وعام في آن واحد، مما يؤدي إلى الاعتداء على الخصوصية. والسبب في ذلك توسع بنوك المعلومات بأنواعها، علاوة على رغبة الأفراد وسعيهم إلى ربط حواسيبهم بالشبكة. وبالتالي هذه الطبيعة الخاصة للأفعال المجرمة هل تدخل ضمن أحكام خدمات البريد أم التخابر الخاص، أم يكون الهدف الأساسي للتحري عن النظام القانوني المناسب لطبيعة الجرائم المعلوماتية هو معرفة النصوص القانونية الوضعية التي يجب تطبيقها على خدمات نشر المواقع والمعلومات فيها؟ ومن هذا النظام تتحدد المسؤولية التي يفترض تطبيقها على الأشخاص المسؤولين عن هذا النشر، ومن خلال المجال الذي ترتكب فيه الجريمة المعلوماتية والمحل والاعتداء عليها، تظهر لنا الطبيعة القانونية الخاصة للجريمة².

3- خصائص الجريمة المعلوماتية: إن للجريمة الالكترونية خصائص عديدة سنحاول

حصرها وأبرزها فيما يلي:

أ- الجريمة المعلوماتية جريمة عابرة للحدود الوطنية: لأن المجتمع المعلوماتي لا يعترف بالحدود الجغرافية، فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود، وهو ما يعني أن مسرح الجريمة المعلوماتية لم تعد محلية، بل أصبح عالميا الأمر الذي خلق العديد من المشاكل حول تحديد الدولة صاحبة القانون الواجب تطبيقه، بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام³.

¹ - جميل عبد الباقي، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دون طبعة، القاهرة: دار النهضة العربية، 2001، ص 92.

² - طوبى ميشال عيسى، التنظيم القانوني لشبكة الانترنت، ط1، بيروت: دار صادر للمنشورات، 2000، ص 383.

³ - رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الانترنت، رسالة ماجستير، (غير منشورة)، جامعة أبي بكر بلقايد، تلمسان، 2012/2011، ص 43.

وبمعنى آخر أن هذه الجريمة لا تقع في دولة واحدة، ولا تعترف هذه الجريمة بالحدود الجغرافية للدول، إذ غالبا ما يكون الجاني في بلد والمجني عليه في بلد آخر، وقد يكون الضرر المحتمل في بلد ثالث¹.

ب- صعوبة اكتشاف الجريمة المعلوماتية وإثباتها: تمتاز الجرائم المعلوماتية بصعوبة الاكتشاف والاثبات وذلك نظرا لعدم ترك الجاني آثارا تدل على اجرامه، فالجرائم التي تتم بواسطة ادخال الرموز والأرقام، تعد رموزا دقيقة ويصعب اكتشافها وإثباتها، لهذا عادة ما يتم اكتشافها بالصدفة وغالبا ما لا يتم معاقبة المجرمين لعدم وجود أدلة قائمة في حقهم².

حيث يتم نقل المعلومات الكترونيا أضف إلى ذلك إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات³.

إذن يمكن رد أسباب صعوبة اكتشاف الجريمة المعلوماتية إلى عدم تركها أثرا خارجيا مرئيا، فهي مجرد أرقام ودلالات وبيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحواسيب، ولأنها لا تترك أثرا خارجيا مرئيا تكون صعوبة الاكتشاف، ومما يزيد من هذه العسوبة، ارتكابها عادة في الخفاء، وعدم وجود أثر كتابي مما يجري خلال تنفيذها من عمليات حيث تتم بالنبضات الالكترونية لنقل المعلومات وكذلك قدرة الجاني على تدمير دليل الإدانة في أقل من ثانية واحدة⁴.

ج- الجريمة المعلوماتية أقل عنفا من الجرائم التقليدية: تعد الجريمة المعلوماتية أقل عنفا من الجرائم التقليدية، إذ تمتاز الجريمة المعلوماتية بأنها من الجرائم الناعمة وبعدها عن العنف، فلا تتطلب لارتكابها العنف ولا استعمال الأدوات الخطيرة كالأسلحة وغيرها، لأن نقل بيانات ممنوعة أو التلاعب بأرصدة البنوك مثلا لا تحتاج إلا إلى لمسات أزرار، بل وتعتمد على الدراسة الذهنية والتفكير العلمي المدروس القائم على المعرفة بتقنيات الحاسب الآلي⁵.

¹ - محمد علي سالم، حسون عبيد هجيج، "الجريمة المعلوماتية"، مجلة جامعة بابل للعلوم الإنسانية، المجلد 14، العدد 6، (2007)، ص 92.

² - معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، رسالة ماجستير، (غير منشورة)، جامعة الحاج لخضر باتنة، 2011/2012، ص 14.

³ - محمد علي العريان، الجرائم المعلوماتية، دون طبعة، مصر: دار الجامعة الجديدة، 2004، ص 53.

⁴ - المرجع نفسه، ص 54.

⁵ - محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دون طبعة، مصر: دار الجامعة الجديدة، 2007، ص 36.

فلا يوجد في واقع الأمر شعور بعدم الأمان تجاه المجرمين في مجال المعلوماتية باعتبار أن مرتكبيها ليسوا من محترفين الاجرام بصفته المتعارف عليها.

كما أنه عادة ما يكون مرتكبو هذه الجرائم من ذوي المراكز المرموقة والتخصصات العالية في أعمالهم، وغالبا ما ينظر إلى مرتكبي هذه الجرائم بوصفهم مستخدمين مثاليين، والغالبية العظمى منهم لهم مراكز قيادية، ويتمتعون علاوة على ذلك بثقة عالية كبيرة في مجال عملهم¹.

د- وقوع الجريمة المعلوماتية أثناء المعالجة الآلية للمعطيات: إن نظام المعالجة الآلية المعطيات هو تعبير في تقني يصعب على المشتغل بالقانون إدراك حقيقته بسهولة، فضلا عن أنه تعبير متطور يخضع للتطورات السريعة والمتلاحقة في مجال فن الحاسبات الآلية ولذلك فالمشروع الجزائري لم يعرف نظام المعالجة الآلية للمعطيات، فأوكل بذلك مهمة تعريفه لكل من القضاء والفقه².

إذن الجريمة المعلوماتية تقع أثناء عملية المعالجة الآلية للبيانات والمعطيات الخاصة بالكمبيوتر، ويمثل هذا النظام الشرط الأساسي الذي يتعين توافره حتى يمكن البحث عن قيام أو عدم قيام أركان الجريمة المعلوماتية الخاصة بالتعدي على نظام معالجة البيانات وذلك أنه في حالة تخلف هذا الشرط تنتقي في الجريمة المعلوماتية³.

هـ- قلة الإبلاغ عن الجريمة المعلوماتية: لا يتم -في الغالب الأعم- الإبلاغ عن جرائم الانترنت إما لعدم اكتشاف الضحية لها وإما خشية من التشهير، لذا نجد أن معظم جرائم الانترنت تم اكتشافها بالصدفة، بل وبعد وقت طويل من ارتكابها زد على ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي تم كشفها، أي أن الفجوة بين عدد هذه الجرائم الحقيقي وبين ما تم اكتشافه فجوة كبيرة⁴.

¹ - علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة (دراسة مقارنة)، دون طبعة، لبنان: منشورات زين الحقوقية، 2013، ص150.

² - آمال قارة، الحماية الجزائرية للمعلوماتية في التشريع الجزائري، دون طبعة، الجزائر: دار هومو للطباعة والنشر والتوزيع، 2006، ص 101.

³ - خالد محمد كدفور المهيري، جرائم الكمبيوتر والانترنت والتجارة الالكترونية، دون طبعة دبي: دار الغدير للطباعة والنشر، 2005، ص 135.

⁴ - نخلا عبد القادر المومني، الجرائم المعلوماتية، ط1، عمان، الأردن: دار الثقافة للنشر والتوزيع، 2008-2010، ص 54-55.

و- تتطلب وسائل خاصة كالحاسب الآلي وشبكة الانترنت: إن الجريمة المعلوماتية تستلزم لقيامها توفر الحاسب الآلي وكذلك شبكة الانترنت وسيلة لارتكاب الجريمة وأدواتها الرئيسية أماكن المعرفة التقنية فتكون ضرورية بحسب درجة خطورة الجريمة المعلوماتية¹.

ثانيا: أركان الجريمة المعلوماتية: تقوم الجريمة المعلوماتية على ثلاثة أركان أساسية وهي:

1- الركن الشرعي للجريمة المعلوماتية: إن الجريمة هي نتيجة الأفعال المادية الصادرة عن الانسان، هذه الأفعال تختلف حسب نشاطات الانسان، وهذا ما جعل المشرع يتدخل لتجريم هذه الأفعال الضارة بموجب نص قانوني يحدد فيه الفعل الضار أو المجرم والعقوبة المقررة لارتكابه². والقاعدة الأساسية الناتجة عن مبدأ الشرعية وهي عدم رجعية القانون الجنائي بمعنى لا يمكن معاقبة شخص ارتكب فعلا لم يجرمه القانون³ تستمد الجرائم المعلوماتية شرعيتها من مختلف التشريعات الوطنية الصادرة بشأن الجريمة المعلوماتية فقد بذلت هيئة الأمم المتحدة جهودا كبيرة إضافة إلى جهود المجلس الأوروبي لاقتناع الدول بوضع تشريعات لتصدي ومواجهة ومكافحة الجرائم الالكترونية وتعزيز التعاون الدولي في هذا المجال.

وبالنسبة للمشرع الجزائري أورد قسما خاصا للمساس بأنظمة المعالجة الآلية للمعطيات وهو القسم السابع مكرر بمحتوى المادة 394 مكرر إلى 394 مكرر 7 بمقتضى القانون 04-15 المؤرخ في 2004/11/10، ولم يكتف المشرع الجزائري بذلك بل فرض حماية جنائية على الحياة الخاصة للأفراد من خلال القانون 23/06 المؤرخ في 2006/12/20 والذي مس المادة 303 وإقراره بالمادة 303 مكرر إلى 303 مكرر 03، وهذا تصديا للاستخدام السيء لوسائل التكنولوجيا الحديثة⁴.

بالإضافة إلى القانون رقم 09-04 المؤرخ في 05 غشت سنة 2009 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

1 - معتوق عبد اللطيف، المرجع السابق، ص 15.

2 - أحسن بوسقيعة، الوجيز في القانون الجزائري العام، ط10، الجزائر: دار هومه، 2011، ص 20.

3 - أحمد خليفة الملط، المرجع السابق، ص 78.

4 - علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دون طبعة، بيروت: الدار الجامعية للطباعة والنشر، 1999، ص 25.

وكذلك المادتين 87 مكرر 11 و 87 مكرر 12 من القانون رقم 02-16 المؤرخ في 19 يونيو سنة 2016 الذي يتمم قانون العقوبات.

02- الركن المادي للجريمة المعلوماتية: إن الركن المادي للجريمة المعلوماتية يقوم على صورتين أساسيتين، الأولى متمثلة في الاعتداء على نظام المعالجة الآلية، وهذه الأخيرة تحتوي على نوعين من الاعتداء يتمثل النوع الأول في الدخول والبقاء غير المشروع في نظام المعالجة الآلية حيث تنطوي تحت هذا النوع ثلاث أفعال هي: فعل الدخول والبقاء وعرقلة أو التعطيل.

أما النوع الثاني فيتمثل في الاعتداء العمدي على نظام المعالجة الآلية للمعطيات وتندرج تحت هذا النوع كذلك ثلاث أفعال وهي: فعل الادخال والمحور والتعديل، وتتمثل الصورة الثانية في الاعتداء على منتجات الاعلام الآلي، حيث تحتوي هذه الصورة على فعل التزوير المعلوماتي¹.

03- الركن المعنوي في الجريمة المعلوماتية: الجريمة ليست كيانا ماديا خالصا قوامه الفعل وما يترتب عليه، بل هي فوق ذلك كيان نفسي ذلك أن ماديات الجريمة لا تنشئ بمفردها مسؤولية وهذا المنطق يسري كذلك على الجرائم المعلوماتية، فلا بد أن ترتكب من شخص قادر على تحمل تبعه أفعاله (مسؤولية جزائية).

أي أن الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط ماديات الجريمة بشخصية الجاني، ولا شك أن العلاقة بين الركن المعنوي والأركان الأخرى هي علاقة قوة، إذ لا وجود للركن المعنوي ما لم تتوفر بقية أركان الجريمة، ويتخذ الركن المعنوي إحدى هاتين الصورتين (قصد جنائي، خطأ غير عمدي) والقصد الجنائي هو علم بعناصر الجريمة وإرادة متجهة إلى تحقيق هذه العناصر أو قبولها. إذن فالركن المعنوي للجريمة المعلوماتية يختلف باختلاف أشكالها، فجريمة الدخول والبقاء غير المشروع هي جرائم عمدية تتطلب قصدا جنائيا وتعني هذه العبارة أن الفاعل له كامل العلم بأن الدخول أو البقاء غير مشروع.

وبالنسبة لجريمة الاعتداء على سير نظام المعالجة الآلية للمعطيات هي جريمة عمدية، لأن أفعال العرقلة والتعطيل هي من الأفعال العمدية وعليه فالقصد الجنائي المقترح ينتج من طبيعة الأفعال المجرمة².

¹ - مولود ديدان، قانون العقوبات، دون طبعة، الجزائر: دار بلقين للنشر، 2008، ص 120.

² - أمال قارة، المرجع السابق، ص 125.

وكذلك الأمر بالنسبة للاعتداءات العمدية على المعطيات فهي جريمة عمدية يتخذ فيها القصد الجنائي بعنصرية العلم والإرادة، فيجب أن تتجه إرادة الجاني إلى فعل الادخال أو المحو أو التعديل كما يجب أن يعلم الجاني بأن نشاطه الاجرامي يترتب عليه التلاعب في المعطيات ويعلم أيضا أنه ليس له الحق في القيام بذلك ويشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجنائي العام نية الغش.

بالإضافة إلى أن استخدام المعطيات كوسيلة في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية يكون عمديا، وذلك الاستخدام متمثل في التصميم أو البحث أو التجميع أو التوفير أو النشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلّة عن طريق منظومة معلوماتية، ويكون هذا الاستخدام عن طريق الغش فلذلك يتطلب القصد الجنائي العام إضافة إلى القصد الجنائي الخاص المتمثل في نية الغش¹.

ثالثا: أشخاص الجريمة المعلوماتية: إن الجرائم المعلوماتية كغيرها من الجرائم تحتاج إلى طرفين جاني ومجني عليه، إلا أن أطراف الجريمة المعلوماتية يختلفون نوعا ما عن أطراف باقي الجرائم وعليه يمكن تحديد أشكال الجريمة المعلوماتية بالآتي.

1- المجرم المعلوماتي: في الجريمة المعلوماتية لا نكون بصدد مجرم عادي بل أمام مجرم ذي مهارات تقنية وذو علم بالتقنيات المستخدمة في نظام الحاسبات الآلية، فشخصية المجرم المعلوماتي سواء أكان شخصا طبيعيا أو معنويا، وآلية ارتكاب الجريمة تجعل منه شخصا يتسم بصفات خاصة تضاف إلى الصفات الأخرى التي يجب أن تتوفر في المجرم العادي².

ولعل أهم ما يتميز به الشخص المذكور أنه يتوافر لديه خبرة بالمسائل المعلوماتية ومعرفة كافية بآلية عمل الحاسب الآلي وتشغيله باعتبار أن الاجرام المعلوماتي ينشأ من تقنيات التدمير الهادئة التي تتمثل بالتلاعب بالمعلومات والكيانات المنطقية أو البيانات، غير أن ذلك لا يعني أن إمكانية تصور العنف الموجه ضد النظام المعلوماتي فقد يكون محل الجريمة اتلاف الحاسب الآلي ذاته أو وحدة المعالجة

¹ - المرجع نفسه، ص 126.

² - هدى حامد قشقوش، المرجع السابق، ص 32.

المركزية¹. أي أن ما يمكن الاعتماد عليه فقد يكون بهيكلية الحاسب الآلي ذاته لا بالمعلومات المتنقلة عبر شبكات المعلومات وعليه فالإجرام المعلوماتي يُعد إجراماً للأدكفاء مقارنة بالإجرام التقليدي الذي يميل إلى العنف على الرغم من تطور الإجرام العنيف الموجه ضد النظام المعلوماتي الذي يتجسد كما بينا بإتلاف الحاسب الآلي.

كما يتصف مرتكبوا الجرائم المعلوماتية بعدة صفات تميزهم عن غيرهم من المتورطين في أشكال الإجرام الأخرى والمتمثلة في المهارة والمعرفة والوسيلة والسلطة، وهي مجمل الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته كاملاً الشيفرة الخاصة بالدخول إلى النظام². وعليه فإن مرتكبي الجرائم المعلوماتية ليسوا على درجة واحدة من الخطورة أو الكفاءة، وعلى هذا الأساس يمكن تصنيفهم إلى صنفين:

الأول مجرمين مستخدمين وهم من يمارسون مواهبهم لغرض الولوج في نظم المعلومات لأجل ممارسة هواية اللهو، وهم لا يدركون ولا يقدرّون النتائج المحتملة التي يمكن أن تحدثها أفعالهم غير المشروعة بالنسبة إلى نشاط معين³ لذا فإن هذه الفئة من المجرمين تعد أقل خطورة مقارنة بغيرها.

الثاني مجرمين مبرمجين نظراً إلى المستوى المهاري الذي يتمتع به المجرمون من دخول واقتحام للأنظمة الحاسوبية بكل سهولة واقتدار رغم احتياطات الأمن المتعددة ورغم قلة العناصر الخبيرة على اكتشافها مما تبدو معه خطورة هذه الفئة من المجرمين واضحة بصورة كبيرة، إذ غالباً ما تكون جرائم التحويل والنسخ والاضافة للمعلومات على البرامج وتفسير محتواها من هذه الفئة ضخمة⁴. علاوة على ذلك فإنه باستطاعة هذه الفئة استخدام الإمكانيات والأساليب المعلوماتية، ليس في ارتكاب الجريمة فقط بل حتى في التهرب من محاولة كشف أمرهم أو بالعمل على إعاقه ملاحقتهم من خلال تضييع الأدلة الموجودة المؤدية إلى ادانتهم ومن هذا يتضح أن مرتكب الفعل الجرمي المعلوماتي قد يكون فاعلاً أصلياً أو شريكاً في ارتكابه للجريمة، على اعتبار أن هذه الجرائم ترتكب من طرف عدة

1 - أسامة أحمد الناعسة وآخرون، جرائم الحاسب الآلي والانترنت، ط1، الأردن: دار وائل للنشر، 2001، ص 65.

2 - مزبود سليم، "الجرائم المعلوماتية في الجزائر واقعها وآليات مكافحتها"، المجلة الجزائرية للاقتصاد والمالية، عدد1، (أفريل 2014)، ص 98.

3 - أسامة أحمد الناعسة، المرجع السابق، ص 82.

4 - محمد علي سالم، حسون عبيد هجيج، المرجع السابق، ص 15.

أشخاص لكل شخص دور معين، ويتم العمل بينهم وفقا لتخطيط وتنظيم سابق على ارتكاب الجريمة¹.

وينقسم المجرمون في مجال المعلوماتية إلى عدة أنماط أهمها: (البرونكاستر، الهاكرز، الكراكرز).

2- المجني عليه في الجريمة المعلوماتية: قد يكون ضحايا الاجرام المعلوماتي إما مؤسسات حكومية أو شركات تجارية أو أفراد عاديين، فاختراق النظام المعلوماتي قد يرتكب على أي من هؤلاء ويرجع السبب في ذلك إلى انتشار استعمال الحاسب الآلي وشبكة الانترنت مما يوسع من فئات ضحايا الاجرام المعلوماتي، كما أنه في هذا النوع من الجرائم يكون دور المجني عليه ضئيلا وسلبيا إلى حد كبير إذ يفضل الكثير من المجني عليه الإبقاء على ما لحقهم من اعتداء سرا، أي يميلون إلى عدم التكلم عما لحقهم من أضرار ناتجة عن الجريمة المعلوماتية، ولعل مرد ذلك يكمن في رغبتهم في الحفاظ على مركزهم الاجتماعي أو سمعتهم التجارية حماية لمركزهم المالي وثقة العملاء بهم، حتى لا ينظر إلى تدابير الحماية لديهم أنها ضعيفة وغير فعالة فتسبب ضعف الثقة بالمؤسسة ومن ثم عزوف العملاء عنها². فضلا عن عجز المجني عليهم في الاثبات المادي للجريمة وخشيتهم لاحتمالية المساءلة القانونية في الوقت الذي يقع عليهم واجب الاشراف على المعلومات المستهدفة وامتلاكهم السلطة اللازمة لا مكان التقدير ووضع الإجراءات الضرورية في حالة حدوث أضرار ناشئة من افشاء معلومات على قدر من الحساسية والخطورة³.

رابعا: دوافع ارتكاب الجريمة المعلوماتية: إن القاعدة القضائية تقرر أن الباعث ليس من عناصر القصد الجرمي، وأن الباعث لا أثر له في وجود القصد الجنائي.

¹ - أمين عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، ط1، مصر: دار النهضة العربية للنشر والتوزيع، 2005، ص 14.

² - محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، ط1، القاهرة: دار النهضة العربية، 1994، ص 61.

³ - محمد حسام لطفي، عقود وخدمات المعلومات، دراسة في القانون المصري والفرنسي، ط1، القاهرة: دار النهضة العربية، 1998، ص 109.

فالدافع (الباعث) هو العامل المحرك للإرادة الذي يوجه السلوك الاجرامي، كالحبة والشفقة والبغضاء والانتقام¹ وهو إذا قوة نفسية تدفع الإرادة إلى الاتجاه نحو ارتكاب الجريمة ابتغاء تحقيق غاية معينة وهو يختلف من جريمة إلى أخرى تبعاً لاختلاف الناس من حيث السن والجنس ودرجة التعليم وغير ذلك من المؤثرات، كما يختلف بالنسبة للجريمة الواحدة من شخص لآخر². وبالنسبة لجرائم الكمبيوتر والانترنت، فثمة دوافع عديدة تحرك الجناة لارتكاب أفعال الاعتداء المختلفة المنضوية تحت هذا المفهوم وعليه يمكن إيراد الدوافع التالية:

1- الدوافع الشخصية: يمكن رد الدوافع الشخصية لدى المجرم المعلوماتي إلى:

أ- الدوافع المادية (تحقيق الربح وكسب المال): يعد الدافع المادي من أكثر الدوافع التي تحرك الجاني لاقتراض الجريمة المعلوماتية، وذلك أن الربح الكبير والممكن تحقيقه من خلالها يدفع بالمجرم المعلوماتي إلى تطوير نفسه حتى يواكب كل حديث يطرأ على التقنية المعلوماتية ويقتنص الفرص ويسعى إلى الاحتراف حتى يحقق أعلى المكاسب وبأقل المكاسب جهد دون أن يترك أثراً وراءه. فالرغبة في الشراء والربح المادي عادة ما تواجهها صعوبات بالغة لتحقيقها بالطرق القانونية والمقبولة اجتماعياً لذا يلجأ بعض الأفراد إلى الجرائم الالكترونية حيث المستهدف مجتمع أكبر، وسهولة التنفيذ ووفرة المردود وقلة الخطورة، إضافة إلى إمكانية محو الدليل وتوفير الوسائل التقنية التي تعرقل الوصول إليه مع ضمان التستر وعدم التشهير، لذا نجد أن الدافع لارتكاب الجريمة المعلوماتية يمكن أن يكون سببه مجرد سداد الديون المستحقة أو مشاكل عائلية راجعة للنقود أو إدمان ألعاب القمار أو المخدرات لذا فإن بيع المعلومات المختلصة هو نشاط متسع للغاية ويمكن أن في هذا المجال واقعة استيلاء مبرمج يعمل لدى إحدى الشركات الألمانية على 22 شريطاً مغنطاً تحوي معلومات هامة بخصوص عملاء وإنتاج هذه الشركة حيث هدد السارق ببيعها للشركات المنافسة ما لم تدفع له فدية مقدارها 200.000 دولار وقد فضلت الشركة دفع المبلغ من أجل استيراد الشرائط المسروقة.

ب- دوافع ذهنية أو غشبية: غالباً ما يكون الدافع لدى مرتكبي الجرائم عبر الانترنت الرغبة في إثبات الذات، وتحقيق الانتصار على تقنية الأنظمة المعلوماتية، دون أن تكون لهم نوايا آثمة

¹ - كامل السعيد، شرح الاحكام العامة في قانون العقوبات الأردني والقانوني المقارن، ط2، عمان: دار الفكر للنشر والتوزيع، 183، ص 226.

² - فوزية عبد الستار، شرح قانون العقوبات - القسم العام -، القاهرة: دار النهضة العربية، 1991، ص 427.

فيتسابقون لخرق هذه الأنظمة وإظهار تفوقهم عليها ويعتبر دافع المزاح والتسلية من الدوافع التي تجعل الشخص يقوم بتصرفات لا يقصد من ورائها أحداث جرائم، وإنما بغرض المزاح فقط ولكن قد تنتج عنها نتائج ترقى إلى درجة الجريمة¹.

ج- الرغبة في التعلم: والتي تتمثل في استخدام الكمبيوتر والامكانيات المستحدثة لنظم المعلومات في ارتكاب الجريمة المعلوماتية، حيث يشير الأستاذ "ليفى" مؤلف كتاب قراصنة الأنظمة "HACKERS" إلى أن فكر هؤلاء المجرمين يركز على مبدئين أساسيين وهما: أن الدخول إلى أنظمة الكمبيوتر يمكن أن يعلمك كيف يسير العالم، وأن جمع المعلومات يجب أن يكون غير خاضع للقيود.

وبناء على هذين المبدئين فإن أجهزة الكمبيوتر المعنية ما هي إلا آلات للبحث، والمعلومات بدورها ما هي إلا برامج وأنظمة معلومات ويعترف قراصنة الأنظمة أنهم يرغبون في الوصول إلى مصادر المعلومات والحاسبات الالكترونية والشبكات بغرض التعلم.

وقد لاحظ ليفى أن قراصنة الأنظمة لديهم الاهتمام الشديد بأجهزة الكمبيوتر والتعلم، ويدخل العديد منهم في أجهزة الكمبيوتر على أنهم محترفين كما يختار بعض القراصنة الأنظمة لتعلم المزيد عن كيفية عمل الأنظمة².

2- الدوافع الخارجية: يمكن أن يتأثر المجرم المعلوماتي ببعض المواقف قد تكون دافعة له على اقتراف الاجرام المعلوماتي ولا يسعى في ذلك حينها لا للمتعة ولا للتسلية ولا كسب المال، ويمكن إبراز أهم هذه الدوافع فيما يلي:

أ- دافع الانتقام: الانتقام موجود داخل النفس البشرية، فكثير من الافراد يفصلون تعسفيا أو بغير وجه حق من شركة أو منظمة حكومية، أو حتى من مصرف، وهم يملكون المعلومات والتدريبات اللازمة والمعرفة الكافية بخفايا هذه الجهة لذلك يرتكب الجاني الجريمة رغبة منه في الانتقام ليجعل

¹ - يوسف صغيري، الجريمة المرتكبة عبر الانترنت، رسالة ماجستير (غير منشورة)، جامعة مولود معمري -تيزي وزو-، 2013، ص 40-41.

² - دورتي إي ديننغ، ترجمة آمنة علي يوسف، "قراصنة أنظمة الكمبيوتر"، المؤتمر القومي الثالث عشر لأمن الكمبيوتر، واشنطن، ديسمبر، 1998، ص 08.

الشركة أو المؤسسة تتكبد الخسائر المالية الكبيرة من جراء ما يسببه لها من ضرر يحتاج إصلاحه إلى وقت طويل¹.

ويعد دافع من الانتقام من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة، لأنه غالبا ما يصدر من شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها، لأنه غالبا ما يكون أحد موظفيها².

ب- دافع التعاون والتواطؤ على الإضرار: هذا النوع كثير التكرار في الجرائم المعلوماتية، وغالبا ما يحدث من شخص متخصص في أنظمة المعالجة الآلية للمعطيات يقوم بالجانب الفني من الشروع الاجرامي، وشخص آخر من المحيط أو خارج المؤسسة المجني عليها لتغطية عمليات التلاعب، وتحويل المكاسب المادية وعادة ما يمارسون التلصص على الأنظمة وتبادل المعلومات بصفة منتظمة³.

ج- دافع التهديد: ينتشر هذا الدافع نتيجة الوقوع تحت تهديد وضغط من الغير في مجالات الأعمال التجارية والخاصة بالتجسس والمنافسة⁴.

أي أن الضغوط العامة التي يتعرض لها الفرد من ظروف اقتصادية صعبة تولد مشاعر سلبية عنده مما يدفع به إلى أساليب تأقلم سلبية مع هذه الظروف ومنها ارتكاب الجريمة الالكترونية.

د- الدافع السياسي: ويتم غالبا في المواقع السياسية المعادية للحكومة، ويتمثل نقل الأخبار والمعلومات ولو زورا أو حتى الاستناد الى جزء بسيط جدا من الحقيقة ومن ثم نسخ الأخبار المزورة وتداولها.

وتعد الدوافع السياسية من أبرز المحاولات الدولية لاختراق الشبكات الحكومية في مختلف دول العالم.

¹ - نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، دون طبعة، الإسكندرية: منشأة المعارف، 2008، ص 44.

² - أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، ط 1، مصر: دار النهضة العربية للنشر والتوزيع، 2005، ص 20.

³ - أحمد خليفة الملط، المرجع السابق، ص 90.

⁴ - محمد سامي الشوا، المرجع السابق، ص 53.

الخلاصة:

إن عصر المعلوماتية خلف وراءه أثرا سلبية نتجت عن استغلال بعض الأفراد والجهات للتقنيات المعلوماتية في غير الغرض الذي وجدت من أجله، الأمر الذي أثر على حقوق الافراد وحرياتهم حيث وفرت الأنظمة المعلوماتية وسيلة جديدة في أيدي مجرمي المعلوماتية لتسهيل ارتكاب العديد من الجرائم وعلى رأسها الجريمة المعلوماتية. كما أضحت النظام المعلوماتي ذاته محلا للاعتداء عليه وإساءة استخدامه.

هذا التطور التكنولوجي المعلوماتي ألقي على عاتق المشرع الجنائي مسؤولية كبيرة لمواجهة الجرائم المعلوماتية، لذلك فقد تم التوصل من خلال هذه المداخلة إلى النتائج والتوصيات التالية.

النتائج:

- عدم وجود تعريف موحد للجريمة المعلوماتية نظرا لحداتها وطبيعتها التقنية.
- أن خصائص الجريمة المعلوماتية تضيف عليها صبغة مختلفة تمام عن الجريمة التقليدية.
- أن الاجرام المعلوماتي الذي يقع عن طريق الشبكة العالمية (الانترنت) له طبيعة من نوع خاص على خلاف الجرائم الأخرى التقليدية وقد تستمد هذه الطبيعة الخاصة من المجال الذي يمكن أن ترتكب فيه من المحل الذي يقع عليه الاعتداء.
- تبين أن المجرم المعلوماتي يتسم بمهارات عملية وتقنية متطورة.
- تختلف الدوافع التي تجعل المجرم المعلوماتي يتميز عن المجرم التقليدي عند ارتكاب مثل هذا النوع من الجرائم.
- أن المشرع الجزائري حاول مجابهة هذه الظاهرة المستحدثة من خلال سن مجموعة من القوانين أهمها تعديل سنة 2009.

التوصيات:

- ضرورة تقنين قواعد جديدة لمكافحة الجرائم المعلوماتية تأخذ بعين الاعتبار الطبيعة الخاصة لهذه الجرائم.
- على المشرع الجزائري التدخل لتعديل النصوص المتعلقة بالأموال لكي تشمل المال المعلوماتي المعنوي.
- ضرورة تكوين وتخصص القضاة في هذه الجرائم.

- ضرورة التكافل الدولي لردع مثل هذه السلوكيات المنحرفة في مجال المعلوماتية.
- ضرورة تدخل الفقه الجنائي لوضع نظرية عامة للجريمة فالجرم المعلوماتي وذلك لتفادي المعالجة السطحية الخالية من أي دقة.
- ضرورة عقد الدورات التدريبية التي تعنى بمكافحة الجرائم المعلوماتية.

واقع الجريمة المعلوماتية ومكافحتها بموجب التشريع الجزائري

أ/ بوعكة الكاملة

كلية الحقوق والعلوم السياسية - جامعة المسيلة

مقدمة:

عرفت الجريمة منذ فجر البشرية، وقد ناهضها الإنسان منذ اللحظة الأولى حيث استشعر فيها بخطر يهدد كيانه وتقدمه. فقد تطورت الظاهرة الإجرامية في الآونة الأخيرة تطورا مذهلا سواء في أشخاص مرتكبيها أو في أسلوب ارتكابها، والذي يتمثل في استخدام آخر ما توصل إليه العلم وتطويعه في خدمة الجريمة¹. فشهد العالم اتساعا مطردا لنطاق استخدام تقنية المعلومات ولاختراعات هائلة على المستوى التقني وازديادا بالغالدورها في تيسير أمور الحياة، ونتج عن التطور العلمي والتقدم التكنولوجي ظهور النظام المعلوماتي وأصبح يكون نظاما متكاملًا دخل في مجالات الحياة لما يتمتع به من قدرة فائقة على تخزين أكبر قدر ممكن من البيانات والمعلومات يقوم بتصنيفها في أسرع وقت ممكن².

فأصبح في نهاية القرن الماضي من لوازم الحياة الضرورية والمتطورة على المستوى العام والخاص. ولا يخفى أن كل تطور على المستوى التقني له انعكاساته بالرغم من تحقيقه مزايا عديدة لا يمكن إنكارها وأصبح مجالا لمخاطر جسيمة وخسائر فادحة لا يستهان بها تمس الحياة الخاصة للأفراد وتهدد الأعمال التجارية والأمن القومي والسيادة الوطنية وتفقد الثقة في المعاملات الالكترونية. فأفرزت ثورة المعلومات والاتصالات نوع جديد من الجرائم ولعل تطور الشبكة العالمية للانترنت جعلت منها وصفاً مثالية لتنفيذ العديد منها وساحة إجرام نموذجية على رأسها الجريمة المعلوماتية. فظاهرة الجريمة المعلوماتية من المستجدات الإجرامية نسبيا تشكل أنماطا جديدة من السلوك الإجرامي من صورها المادية التقليدية إلى أخرى معنوية³ ترتبط بالتقنيات الالكترونية الحديثة وتستهدف

¹ أحمد خليفة الملط، الجرائم المعلوماتية دراسة مقارنة، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2006، ص 08

² نفس المرجع، ص 19.

³ خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، الدار الجامعية، الإسكندرية، 2008، ص 07.

الاعتداء على البيانات والمعلومات والبرامج بكافة أنواعها، فهي جريمة تقنية يرتكبها مجرمون أذكاء يمتلكون أدوات المعرفة التقنية أو الفنية وتوجه للنيل من أجهزة الحاسوب وشبكات الاتصال وقواعد البيانات والبرمجيات ونظم التشغيل¹.

وللجريمة المعلوماتية مسميات كثيرة فهناك من يسميها جريمة الكمبيوتر والانترنت والبعض الآخر يطلق عليها الجريمة الالكترونية وهي جريمة إساءة استخدام تقنية المعلومات وهناك من يطلق عليها الجرائم المستحدثة والمستترة التي تتسم بالسرعة وهي أقل عنفا في التنفيذ. وهي نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود. وهناك من يرى بأنها الاستخدام غير المشروع للحاسبات والتي تتخذ صورة فيروس يهدف إلى تدمير الثروة المعلوماتية². ونظرا لوقوع هذه الجريمة في بيئة المعالجة الآلية للبيانات حيث تكون المعلومات محل اعتداء عبارة عن نبضات الكترونية فإننا نكون أمام ظاهرة إجرامية ذات طبيعة خاصة تستلزم التعامل مع بيانات مجمعة ومجهزة لدخول الحاسب بغرض معالجتها الكترونيا فأصبح التعامل مع هذه الصورة الإجرامية موضوع اهتمام لدراسات علمية هامة تتعلق بأمن الصرح الالكتروني³.

والغاية من التجريم هي حماية النظام المعلوماتي في حد ذاته ومنتجاته لأن هذا الأخير يتضمن إضافة إلى العتاد البرامج و المعلومات المخزنة في الذاكرة وبالتالي المحتوى⁴. ومن أجل تحقيق التوازن بين مصالح المجتمع في الاستفادة من المستجدات العلمية والأضرار المتولدة عنها وخطورتها وتأثيرها على اقتصاديات الدول فكان لزاما على كافة دول العالم أن تكثف جهودها من خلال المواجهة القانونية لهذه الظاهرة الإجرامية.

وظهرت الحاجة لمواكبة تشريع خاص واستحداث النصوص الملائمة لطبيعتها وكان من الضروري أن تواكب القوانين هذا التطور الملحوظ⁵ قصد الحماية للبرامج المعلوماتية وحماية الحاسبات الالكترونية

¹ نفس المرجع، ص 06.

² عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي دراسة قانونية معمقة في القانون النموذجي، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006، ص 20.

³ نفس المرجع ص 20.

⁴ قارة أمال، الجريمة المعلوماتية، مذكرة ماجستير، بن عكنون، جامعة الجزائر، 2001/2002، ص 16.

⁵ عمرو عيسى الفقي، مرجع سابق، ص 15.

من كل تلاعب وضرر بمضامينها ومحتواها¹، وتحركت العديد من المنظمات الدولية والإقليمية تهدف إلى مكافحة الجريمة المعلوماتية ولعل أهمها اتفاقية بودابست المنعقدة في 23 نوفمبر 2001 تحت إشراف المجلس الأوروبي².

فقد أدرجها المشرع الجزائري بموجب الأمر 15/04 المؤرخ 10 نوفمبر 2004 المعدل والمتمم والذي أدمج في الفصل الثالث من الباب الثاني من الكتاب الثالث قسما سابعا مكرر بموجب المواد من 394 إلى 394 مكرر7 تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات مع إصداره للقانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها³.

وان البحث في المواجهة القانونية للجريمة المعلوماتية مسألة تتسم بالدقة والغموض ولا بد من الإلمام بالإطار المفاهيمي أولا وعليه نطرح الإشكالية التالية:

ما هو واقع الجريمة المعلوماتية؟ وكيف تصدى التشريع العقابي الجزائري لمواجهتها؟ وعليه ستقسم هذه الدراسة إلى محورين نتعرض في المحور الأول إلى تعريف الجريمة المعلوماتية وكذا إلى تبيان سمات الجريمة المعلوماتية، أما المحور الثاني فنخصصه لمكافحة الجريمة المعلوماتية على مستوى التشريع العقابي الجزائري.

المحور الأول: تعريف الجريمة المعلوماتية وسماتها

إن التعرض إلى تعريف الجريمة المعلوماتية يقتضي تقسيم هذا المصطلح إلى مقطعين الأول الجريمة والثاني المعلوماتية. فالجريمة كل فعل أو امتناع يحظره القانون ويقرر عقوبة لمرتكبه وعرفها البعض الآخر بأنها فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبير أمن. أما المعلوماتية فهي المعالجة الآلية للمعلومات وهي ترجمة للمصطلح الفرنسي *informatique* وتعني تكنولوجيا تجميع ومعالجة وإرسال المعلومات بواسطة الكمبيوتر وتعني المعالجة الآلية للبيانات ومصطلح *télématique* يعني من الناحية اللغوية تقنيات المعلومات عبر شبكة اتصالات بعيدة

¹ أحمد خليفة الملط، مرجع سابق، ص 68.

² خلف فاروق، الآليات القانونية لمكافحة الجريمة المعلوماتية، ملتقى وطني الجريمة المعلوماتية بين الوقاية والمكافحة جامعة محمد خيضر بسكرة، يومي 17/16 نوفمبر 2015، ص 01.

³ القانون 04/09 المؤرخ في 05 أوت 2010 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ج ر عدد 47 الصادرة بتاريخ 2009.

وهي تعبير اختصار ناتج عن اندماج كلا من اللفظين informatique أي المعلوماتية ولفظ télécommunication أي اتصالات¹.

بداية تشير أغلبية الدراسات لعدم وجود مصطلح موحد للجريمة المعلوماتية وذلك خشية حصرها في مجال ضيق يمكن أن يضر بها وفيه تعدد للمصطلحات المستخدمة وهناك من يطلق عليها جرائم الحاسبات أو إساءة استخدام الحاسبات أو الجرائم المرتبطة أو المتعلقة بالحاسبات أو جرائم المعالجة الآلية للبيانات أو جرائم التكنولوجيا الحديثة الأمر الذي أفرز تعريفات موسعة وأخرى ضيقة للجريمة المعلوماتية².

فبذل الفقه جهودا في محاولة وضع تعريف موحد للجريمة المعلوماتية فانقسم الفقه إلى اتجاهين الأول يضيق من مفهومها والآخر يوسع من مفهومها³. وعرفها الفقيه الألماني tiederman تيدرمان بأنها "كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب" وعرفت كذلك بأنها "الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا⁴ وهي كل فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية.

وعرفت لدى مكتب تقييم التقنية في و م أ بأنها "الجرائم التي تلعب فيها البيانات الكمبيوترية للجريمة والبرامج المعلوماتية دورا رئيسيا " وهي كذلك "كل جريمة ضد المال مرتبطة بالمعالجة الآلية للمعلومات"، وهناك من عرفها بأنها "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب". فهي جريمة لا تعرف الحدود الجغرافية⁵ والتي يتم ارتكابها بأداة هي الحاسب الآلي عن طريق شبكة الانترنت وبواسطة شخص على دراية بها.

وعرفت كذلك بأنها "غش معلوماتي ينصرف إلى كل سلوك غير مشروع يتعلق بالمعلومات لمعالجتها ونقلها"⁶. ويؤخذ على هذه التعريفات بأنها اعتمدت على الوسيلة في تعريف الجريمة وبهذا فهناك

¹ خالد ممدوح ابراهيم مرجع سابق ص 43

² أحمد خليفة الملط، مرجع سابق، ص 84-85.

³ خالد ممدوح ابراهيم، مرجع سابق، ص 42.

⁴ نفس المرجع، ص 84.

⁵ منير محمد الجنبهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية،

2006، ص 13.

⁶ عبد الفتاح بيومي حجازي، مرجع سابق، ص 25.

تعريفات أخرى تناولت الجانب الموضوعي للجريمة المعلوماتية فهذه الجريمة ليست الجريمة التي يستخدم الحاسب الآلي فيها كأداة في ارتكابها بل تقع على الحاسب أو في داخل نظامه¹. فلا يهتم بالوسيلة أو موضوع الجريمة المعلوماتية ويعرفها بوصفها مرتبطة بالمعرفة الفنية أو التقنية باستخدام الحاسب الآلي وهي أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب وكل فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه².

وعرفت منظمة التعاون الاقتصادي والتنمية و الخاص باستبيان الغش المعلوماتي عام 1982 والذي أوردته في بلجيكا في تقريرها حول الجريمة المعلوماتية بأنها "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل تقنية المعلومات"³. فالجريمة المعلوماتية هي التي يكون المال المعلوماتي موضوعا لها أما الجرائم التقليدية المرتكبة بواسطة المعلوماتية فتقصى من طائفة الجرائم المعلوماتية إذ أن تعريف أية جريمة لا يتم بالاعتماد على الوسيلة المستخدمة في ارتكابها وإنما بالرجوع إلى العمل الأساسي المكون لها⁴.

سمات الجريمة المعلوماتية:

تعد الجريمة المعلوماتية من الجرائم المستحدثة الواقعة على المعلومات بمفهومها الواسع وهي تشمل المعلومات والبيانات والكيانات المنطقية كالبرامج التطبيقية وبرامج التشغيل ومحملها النظام المعلوماتي ومكوناته وتتسبب في تدمير النظام كليا أو جزئيا وتعطيله.

تعتبر الجريمة المعلوماتية ذات خصائص متميزة تختلف عن الجريمة العادية في أسلوب ارتكابها وصعوبة اكتشافها وتتمثل الخصائص في:

- وقوع الجريمة المعلوماتية أثناء المعالجة الآلية للبيانات:

فمن أهم سمات الجريمة المعلوماتية هو وقوعها على المعطيات والبرامج الخاصة بالكمبيوتر وهو شرط أساسي يتعين توافره حتى يمكن البحث في قيام أو عدم قيام الجريمة المعلوماتية الخاصة بالتعدي على نظام معالجة البيانات. وتنتفي الجريمة لعدم وجود هذا الشرط سواء وقعت أثناء عملية المعالجة الآلية

¹ نفس المرجع، ص 24.

² عبد الفتاح بيومي حجازي، مرجع سابق، ص 25.

³ نفس المرجع، ص 66.

⁴ قارة أمال، مرجع سابق، ص 14.

أو في أي مرحلة من المراحل الأساسية، سواء عند إدخال المعلومات أو أثناء مرحلة المعالجة أو أثناء مرحلة إخراج البيانات¹.

فيستلزم التعامل مع بيانات مجمعة ومجهزة للدخول لنظام معلوماتي بغرض معالجتها إلكترونياً وتعديلها ومحوها أو تخزينها وهذه العمليات وثيقة الصلة بارتكاب الجرائم ولا تترك أثراً خارجياً². ونظام المعالجة الآلية للبيانات هو "كل مجموعة مركبة من وحدة أو عدة وحدات للمعالجة سواء كانت متمثلة في ذاكرة الحاسوب وبرامجه أو وحدات الإدخال والإخراج والاتصال التي تساهم في الحصول على نتائج". وهو شرط أساسي لمعرفة إذا كان هناك اعتداء على نظام المعالجة الآلية للبيانات من عدمه³.

وعرفته الاتفاقية الدولية للإجرام المعلوماتي في المادة الأولى بودابست⁴ "يقصد بمنظومة الكمبيوتر أي جهاز أو مجموعة من الأجهزة المتصلة ببعضها البعض أو التي ذات الصلة بذلك ويقوم أحدها أو أكثر واحد منها تبعاً للبرنامج بعمل معالجة آلية للبيانات" وهي مجموع العمليات المنجزة بواسطة وسائل الإعلام الآلي المرتبطة بتجميع أو تسجيل أو إعداد أو حفظ أو تخريب معلومات اسمية وكل العمليات من طبيعة واحدة مرتبطة باستغلال الملفات أو قاعدة المعطيات وخاصة ربط أو تقريب أو فحص أو نشر معلومات اسمية فالعناصر المادية والمعنوية التي يتكون منها المركب جاءت على سبيل المثال لا الحصر لفتح المجال أمام إضافة عناصر جديدة أو حذف بعضها حسب ما يقرره التطور التقني والتكنولوجي⁵.

– الجريمة المعلوماتية عابرة للحدود ولا حدود جغرافية لها:

فتتسم بالطابع الدولي والاعتماد على شبكة الانترنت وارتكابها عن بعد، ولا وجود للفاعل على مسرح الجريمة مما يزيد من صعوبة اكتشافها. فهي تعتبر صورة صادقة من صور العولمة وتتخطى

¹ خالد ممدوح إبراهيم، مرجع سابق، ص 49.

² أحمد خليفة الملط، مرجع سابق، ص 93.

³ عبد الفتاح بيومي حجازي، مرجع سابق، ص 66.

⁴ بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة دكتوراه في العلوم، كلية الحقوق

جامعة بن يوسف بن خدة، الجزائر 1، 2017-2018، ص 155.

⁵ نفس المرجع، ص 156.

حدود الدولة التي ارتكبت فيها لتتعدى آثارها على مستوى العالم¹. وقدرة تقنية المعلومات على اختصار المسافات بين الدول وارتكابها عن بعد من خلال جهاز الكمبيوتر.

-الجريمة المعلوماتية ذات طابع تقني:

فهي ذات طبيعة خاصة كونها تقع في بيئة الكترونية وتستخدم فيها أدوات التقنية المعلوماتية يتم فيها نقل المعلومات وتداولها بالنبضات الالكترونية غير المرئية ولا وجود للمستندات الورقية وتحتاج إلى خبرة فنية والإلمام بتقنيات الكمبيوتر ونظم المعلومات قصد التحقيق فيها، لارتكابها على مستوى شبكة الإنترنت ولتعلقها بأساليب المعالجة الالكترونية للبيانات من تجميع وتجهيز البيانات بغية الحصول على المعلومات وبأساليب معالجة النصوص والوثائق المخزنة في الحاسوب أو توماتيكيا والحاسب الآلي هو أداة ارتكاب الجريمة وهو حلقة الوصل الرئيسية² بين كافة الأهداف المحتملة لتلك الجرائم. ومما يترتب عليه صعوبة اكتشافها وتحديد مكان وقوعها بسبب اتساع نطاقها المكاني وكونها لا تترك أثارا مادية³ وصعوبة الاحتفاظ بدليل الجريمة⁴.

- المجرم المعلوماتي ذو قدرات فنية عالية:

فله دراية وقدرة وخبرة في استعمال الحاسب الآلي، وبالتالي يصعب إثباتها ويتراءى أن المجرم المعلوماتي ليس مجرما عاديا بل له مهارات تقنية عالية وخبرات في تغيير المعلومات أو تقليد البرامج أو تحويل الحسابات⁵ ومن السهل إخفاء معالم الجريمة وصعوبة تتبع مرتكبيها. فهي جرائم تتسم بالغموض خاصة من حيث الكشف عن الجريمة والتحقيق والمتابعة⁶ مع سهولة ارتكابها. فالإجرام المعلوماتي هو إجرام الأذكاء لكون المجرم المعلوماتي ذو مهارات تقنية وإلمام بتكنولوجيات النظم المعلوماتية⁷.

¹ ممدوح محمد الجنبهي، مرجع سابق، ص 15.

² عمرو عيسى الفقي، مرجع سابق، ص 86.

³ خالد ممدوح إبراهيم، مرجع سابق، ص 45.

⁴ نفس المرجع، ص 47.

⁵ عمرو عيسى الفقي، الجرائم المعلوماتية جرائم الحاسوب الآلي والانترنت في مصر والدول العربية، المكتب الجامعي الحديث، الإسكندرية، 2006، ص 15.

⁶ خالد ممدوح إبراهيم، مرجع سابق ص 11

⁷ نفس المرجع، ص 47.

المحور الثاني: مكافحة الجريمة المعلوماتية بموجب قانون العقوبات

يتضمن قانون العقوبات مجموعة القواعد القانونية التي تحدد ما يعتبر من صور السلوك الإجرامي وما يترتب على اقترافها من جزاءات، ويسبغ المشرع العقابي حمايته على الحقوق والمصالح العامة والخاصة من خلال نصوص تجرم الأفعال التي تشكل اعتداء عليها بصورة معينة والقسم الخاص من هذا القانون يشكل التجسيد الواقعي لمبدأ شرعية الجرائم والعقوبات وهو ضرورة لا غنى عنها لوضع هذا المبدأ موضع التنفيذ الفعلي. وتجسيد هذا المبدأ وبث معنى الحياة فيه يقتضي بالإضافة إلى النص عليه تأكيداً لوجوده تحديد الأفعال التي تعتبر محظورة على الأشخاص وبيان العقوبات الواجبة التوقيع عند إتيانها، وهذا التحديد هو بعينه موضوع القسم الخاص من قانون العقوبات، والذي يعد مرآة تعكس ظروف الزمان والمكان التي وضعت فيها نصوصه وبمثابة الصدى لحضارة المجتمع الذي تحكمه وترجمة لنظمه الاقتصادية والسياسية وظروفه. وتكفي مطالعة نصوص القسم الخاص للوقوف على حالة المجتمع الذي تطبق فيه هذه النصوص فهو يتضمن توصيف الجرائم كل على حدة عن طريق بيان الأركان الخاصة بكل جريمة من الناحية المادية والجزاءات المقررة لها.

فقد تضمن القسم الخاص من قانون العقوبات 15/04 في المواد 394 مكرر إلى 394 مكرر 07 القسم السابع على المساس بأنظمة المعالجة الآلية للمعطيات سواء للشخص الطبيعي أو للشخص المعنوي. فعاقب المشرع على كل تخريب لمحتويات نظام المعالجة الآلية للمعطيات أو إعاقه تشغيله، وتخريب الحماية الفنية للمعطيات التي تتمثل في الإجراء الوقائي للمحافظة على خصوصية البيانات المتناقلة عبر الشبكات وبالأخص عبر الانترنت والوصول إلى سرية الرسائل الالكترونية والبيانات المتناقلة ولايد من التعرض للاعتداءات الواردة على المعلوماتية.

-جريمة الدخول والبقاء غير المشروع في أنظمة المعالجة الآلية للمعطيات عن طريق الغش

وهذا ما نصت عليه 394 مكرر بنصها "يعاقب بالحبس من ثلاثة أشهر إلى سنة 1 وبغرامة من 50000 دج إلى 200000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من 6 أشهر إلى سنتين والغرامة من 50000 إلى 300000 دج".

وقسمها المشرع إلى جريمة بسيطة وأخرى مشددة فحسب الفقرة الأولى يكون النشاط الإجرامي في الدخول إلى نظام المعالجة الآلية للمعطيات أو في جزء منه، وهو يمثل ظاهرة معنوية تتمثل في اختراق

العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات ولا يدخل في نطاق الجريمة الدخول إلى برنامج منعزل عن نظام المعالجة الآلية للمعطيات، كما لا تقوم الجريمة إذا اقتصر دور المحرم المعلوماتي على مجرد قراءة للشاشة دون الدخول إلى داخل النظام.

أما البقاء فيتخذ السلوك الإجرامي وهو التواجد داخل النظام ضد إرادة من له الحق في السيطرة على النظام¹ والوصول إلى نظام غير مصرح به للدخول إليه والدخول إلى البرنامج فعلا. والركن المعنوي يتمثل في العلم والإرادة ولا يتحقق إذا كان دخول الجاني أو بقاءه مسموحا به داخل النظام أو مشروع أو وقع في خطأ يتحقق بموجبه دخول في النظام وجهله حظر الدخول. أما المشددة ومتى ترتب على الدخول أو البقاء غير المشروع محو أو تعديل للبيانات التي يحتويها النظام وهذه النتيجة اعتبرها المشرع ظرفا مشددا وهي عمدية.

- جريمة إدخال أو إزالة أو تعديل لمعطيات بطريق الغش في نظام المعالجة الآلية

ونصت عليها المادة 394 مكرر 1 من قانون العقوبات وهي تشمل كل عمليات الإدخال أو التعديل أو الحذف والمحو لمعطيات التي يتضمنها نظام المعالجة الآلية بطريق الغش سواء إتلافها أو تخريبها بهدف تعطيل النظام المعلوماتي كليا أو جزئيا مثل نشر فيروسات. والمحو في جريمة اختراق النظم المعلوماتية يقصد به إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل أو تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة³². ونصت المادة "يعاقب بالحبس من 06 أشهر إلى ثلاث سنوات وبغرامة من 500000 دج إلى 4000000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها النظام."

- جريمة نشر أو تصميم أو تجميع أو الاتجار في معطيات مخزنة

وهي المنصوص عليها في المادة 394 مكرر 2 وهي جريمة الاعتداء العمدي على سلامة المعطيات الموجودة داخل النظام ذاته ضد النشاطات، والمشرع يوفر الحماية الموجودة داخل النظام ذاته ضد النشاطات الإجرامية وهي تتعلق بالمعطيات أو البيانات داخل النظام. ونصت عليها في المادة 3 و 4

¹ بدري فيصل، مرجع سابق، ص 164.

³ عبد الفتاح بيومي حجازي، مرجع سابق، ص 383.

و8 من اتفاقية الدولية للإجرام المعلوماتي ويتمثل الركن المادي في أفعال الإدخال أو الحو أو التعديل وتلاعب في المعطيات التي يتضمنها نظام المعالجة وإدخال معطيات جديدة وموضوع الجريمة هو الاعتداء على معطيات في نظام المعالجة أي البيانات التي أدخلت لمعالجتها وإزالة جزء من المعطيات المسجلة على الدعامات الموجودة داخل النظام أو تحطيم تلك الدعامات. والتعديل هو تغيير المعطيات الموجودة واستبدالها بمعطيات جديدة.

وهي من أكثر الجرائم وقوعا في العالم الافتراضي فاعتبر المشرع في المادة 394 مكرر 2 بنصه كل من يقوم عمدا وبطريق الغش تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلّة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم أي كل عمليات اصطناع برنامج مخصص لارتكاب فعل الغش المعلوماتي وكذا حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم. وتضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بعقوبات أشد طبقا لنص المادة 394 مكرر 3 واعتبرها ظرف تشديد. وهي جريمة عمدية فيها صورة القصد الجنائي بعنصره العلم والإرادة وعلمه أن نشاطه بالإدخال والحو والتعديل يترتب عليه التلاعب بالمعطيات وليس له الحق في ذلك.

-الجريمة المعلوماتية المرتكبة من الشخص المعنوي

كرس المشرع الجزائري ابتداء من سنة 2004 بموجب تعديل قانون العقوبات بالقانون رقم 04-15 صراحة مبدأ المسؤولية الجنائية للأشخاص المعنوية إذ نصت المادة 51 مكرر : "باستثناء الدولة والجماعات المحلية الخاضعة للقانون العام يكون الشخص المعنوي مسؤولا جزائيا عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه الشرعيين عندما ينص القانون على ذلك. إن المسؤولية الجزائية للشخص المعنوي لا تمنع مساءلة الشخص الطبيعي كفاعل أصلي أو كشريك في نفس الأفعال".

حيث نصت المادة 18 مكرر على مايلي: "العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات و الجنح:

الغرامة التي تساوي مرة(1) إلى خمس(5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

واحدة أو أكثر من العقوبات التكميلية الآتية

- حل الشخص المعنوي.
 - غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس سنوات.
 - الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات.
 - المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز خمس سنوات.
 - مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.
 - نشر أو تعليق حكم الإدانة.
 - الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس سنوات وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبةه."
- وهي المنصوص عليها في المادة 394 ككرر 4 وشدّد عقوبة الغرامة في جريمة الاعتداء على نظام المعالجة الآلية وهي الغرامة التي تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي -جريمة تكوين جمعية أشرار لغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وهي المنصوص عليها في المادة 394 مكرر 5 وتتمثل في التحضير أو الإعداد لارتكاب جرائم معلوماتية مع توفر القصد الجنائي وحسب نص المادة "فكل من شارك في مجموعة أو في اتفاق تألّف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها".
- جريمة المساس بحمة الحياة الخاصة بأية تقنية خاصة:

وهي المنصوص عليها في المادة 303 مكرر بموجب التعديل لقانون العقوبات 23/06 حيث يعاقب بالحبس من 06 أشهر إلى ثلاث سنوات وبغرامة من 50000 دج إلى 300000 دج كل من تعمد المساس بحمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه أو بالتقاط أو تسجيل أو نقل صورة في مكان خاص بغير إذن صاحبها أو رضاه.

وباعتبار أن الشروع في الجنح يكون بنص قانوني فقد أدرج المشرع في المادة 394 مكرر 7 على أنه "يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة

ذاتها ". كما نص المشرع على العقوبات التكميلية والمتعلقة بمصادرة الأجهزة والبرامج والوسائل المستخدمة وكذا إغلاق المواقع التي تكون محلا لجريمة من الجرائم وإغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكيها وفق ما نصت عليه المادة 394 مكرر 6.

خاتمة:

الحقيقة أن الجريمة المعلوماتية في تزايد يوما بعد يوم وان مجالات وقوعها كثيرة ومخاطرها عديدة نظرا لطبيعة استخدامها في المعاملات الاقتصادية والمالية والدولية والاعتماد عليها في تسير شؤون الأفراد يوميا ومن شأن ذلك أن يضيف أبعادا غير مسبقة على الخسائر والأضرار التي تنجم عن هذه الجرائم وفقد الثقة في المعاملات الالكترونية. وللإشارة فان المشرع الجزائري لم يكتف بمكافحة الجريمة المعلوماتية بنصوص قانون العقوبات فقط وإنما هناك نصوص في قوانين خاصة كالملكية الفكرية وحقوق المؤلف وغيرها. وعليه أقدم الاقتراحات التالية:

- تكثيف الجهود الوطنية و رسم إستراتيجية واضحة المعالم للقضاء على هذه الجريمة و نشر الوعي في جميع المرافق و الأوساط التعليمية على جميع المستويات بآثار الإجرام المعلوماتي على مصالح الدولة و وزعزعة الاستقرار السياسي والاجتماعي والحياة الخاصة للفرد.

- عقد دورات تكوينية للقضاة ولأعوان القضاء ولضباط الشرطة القضائية حتى يتمكنوا من فهم العديد من التقنيات من أجل تبادل الخبرات وإنشاء محاكم متخصصة لهذه الظاهرة الإجرامية.

- توسيع آليات التعاون الدولي فيما يخص التحقيق وتسليم المجرمين و تعزيز الجهود الدولية وإبرام اتفاقية للدول العربية خاصة بمكافحة الإجرام المعلوماتي والإسراع في تجسيد مشروع الحكومة الالكترونية لما من فوائد في تطويق الجريمة وعدم استفحالها أكثر فأكثر والاستفادة من خبرات الدول السباقة في مكافحة هذه الجرائم.

الجريمة المعلوماتية بين ضيق النص التجريمي و إتساع السلوك الإجرامي

أ/ مريم عثمان

كلية الحقوق والعلوم السياسية

جامعة خنشلة

د/ بوقرة العمري

كلية الحقوق والعلوم السياسية

جامعة المسيلة

مقدمة:

بالرغم من الإيجابيات الكثيرة للأنترنت إلا انه مع مرور الوقت بدأت السلبيات في الظهور فكشفت الاختبارات والحوادث عن ظهور نوع جديد من الجرائم هو الجرائم المعلوماتية، الناتجة عن جرائم الحاسب الآلي والانترنت والتي غيّرت مفهوم الجريمة العادية، بما يفرض تغيير السياسة الجنائية لمكافحتها، وإذا كانت عملية التجريم والعقاب هي أهم أدوات السياسة الجنائية، فإن فعالية هذه الأدوات تتحدّد بمدى امتداد النص التجريمي وشموليته لمختلف السلوكات الإجرامية التي يمكن أن تشكل جريمة ما، وبذلك فمحاولة المشرع الجزائري الإحاطة بالجريمة المعلوماتية لا تكون له فاعلية إلا إذا استوعب النص التجريمي لها مختلف الأفعال التي تشكّلها، وأمام إتساع الهوة بين السلوكات الإجرامية الموجودة وبين الجرائم التي تتبناها المشرع الجنائي في إطار محدود يعجز عن مواكبة التطور اللا متناهي لأساليب إرتكاب الجرائم المعلوماتية، جاءت فكرة البحث في موضوع الجريمة المعلوماتية بين ضيق النص التجريمي وإتساع السلوك الإجرامي، ومن هذا المنطلق، كانت إشكالية الدراسة تتمثل في السؤال المحوري الآتي:

ما مدى كفاية النصوص التجريبية المتعلقة بالجرائم المعلوماتية في التشريع الجزائري في ظل إتساع السلوك الإجرامي لهذه الجرائم؟ وإجابة على التساؤل الرئيسي تطرح الأسئلة الفرعية التالية:

- ما مدى ضيق النص التجريمي في قانون العقوبات ؟

- ما مدى ضيق النص التجريمي في القوانين الخاصة ؟

- إلى أي مدى إتّسع السلوك الإجرامي للجرائم المعلوماتية ؟

لتبرز بذلك أهمية الدراسة من خلال أهمية تحقيق التوازن بين السلوكات الإجرامية الموجودة وبين النصوص التجريبية القائمة، كإستراتيجية للحد من جرائم المعلوماتية التي أصبحت واقعا بل هاجسا

يهدّد بدوره كل من الدول، وذلك تزامنا مع فرض الانترنت لنفسها كساحة نموذجية للإجرام تتحدى كل الأجهزة الأمنية والقضائية بثغرات قانونية وفراغ تشريعي، ومحاولة لتحقيق أهداف الدراسة والمتمثلة في التعرف على الجرائم المعلوماتية الموجودة في التشريع الجزائري وكيفية تعامل السياسة الجنائية معها كجريمة قائمة، إضافة إلى تحديد السلوكات الإجرامية المتطورة التي تشكل جريمة معلوماتية لم يتم مواكبتها بعد، وللإجابة على الإشكالية المطروحة وتحقيقا للأهداف المسطرة اتبعنا المنهج الوصفي في عملية الوصف الدقيق والموضوعي لكل من الجرائم المعلوماتية، وكذا المنهج التحليلي لتحليل القواعد القانونية الواردة في كل من قانون العقوبات وبعض القوانين الخاصة بقانون الملكية والأدبية، لتحديد الفجوة بين التجريم الموجود والتجريم الذي يفترض أن يوجد، وذلك من خلال التعرض لضيق النص التجريمي للجرائم المعلوماتية في المبحث الأول، واتساع السلوك الإجرامي لها ضمن المبحث الثاني.

المبحث الأول: ضيق النص التجريمي في الجرائم المعلوماتية

حاول الفقهاء إعطاء تعريف الجريمة المعلوماتية من خلال اتجاهاين، أحدهما يعرفها تعريفا واسعا والآخر تعريفا ضيقا كما فعل الفقيه merwe الذي عرّفها بأنها: الفعل غير المشروع الذي يتورط في إرتكابه الحاسب الآلي، وكذا عرّفها محمد أمين الشوابكة تعريفا ضيقا كذلك على أنها: نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الكمبيوتر أو تلك التي يتم تحويلها عن طريقه¹، فإلى أي مدى قد أثرت هذه التعاريف الضيقة للجريمة المعلوماتية على ضيق النص التجريمي في قانون العقوبات و في القوانين الخاصة.

المطلب الأول: ضيق النص التجريمي في قانون العقوبات بعد أن تنبّه المشرع الجزائري لمكافحة الجريمة المعلوماتية حاول تجريم بعض السلوكات الإجرامية المكوّنة لها ضمن القسم السابع مكرر، والذي عنوانه بالمساس بأنظمة المعالجة الآلية لمعطيات، وذلك ابتداء من المادة 394 مكرر إلى 394 مكرر 08، لذا كان لابد من التطرق لمفهوم نظام المعالجة الآلية للمعطيات، وبيان السلوك المجرم طبقا لهذه المواد.

أولا مفهوم نظام المعالجة الآلية للمعطيات يعتبر نظام المعالجة الآلية للمعطيات الشرط الأولي للبحث في توافر أو عدم توافر أي جريمة من جرائم الإعتداء على نظام المعالجة الآلية، لذا يكون من

¹ محمد أمين الشوابكة، جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان، 2007، ص 08.

اللازم تحديد معناه، ومدى إشتراط المشرع الجزائري لوجود حماية فنية حتى يجرّم الإعتداء على نظام المعالجة للمعطيات.

1- تعريف نظام المعالجة الآلية للمعطيات: ذكر مجلس الشيوخ الفرنسي في إقتراحه لتعريف نظام المعالجة الآلية للمعطيات بأنه كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط، والتي تربط بينها مجموعة من العلاقات والتي عن طريقها تتحقق نتيجة معينة وهي معالجة المعطيات، على أن يكون هذا المركب خاضعا للحماية الفنية¹، في حين عرّفها المشرع الجزائري بأنها كل نظام أو مجموعة من الأنظمة منفصلة كانت أو متصلة بعضها البعض أو المرتبطة والتي يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين²، ليتوافق هذا التعريف مع التعريف الذي جاءت به الإتفاقية الدولية للإجرام المعلوماتي المبرمة ببودابست 2001³، وهو ما يؤكد أن نظام المعالجة الآلية للمعطيات يتطلب عنصرين أولهما وجود عناصر مادية يتكون منها المركب، وثانيهما وجود علاقة تربط بين هذه العناصر المختلفة وتوحيدها لتحقيق هدف واحد ومحدد، وبذلك فلا يتوافر هذا النظام ولا تقع الجريمة إذا وقع الاعتداء على عنصر بمفرده كالاعتداء على برامج معروضة للبيع، كما لا يقع الاعتداء أيضا إذا وقع على النظام خارج ساعات تشغيله العادية أو كانت أحد عناصره في حالة عطل.⁴

2- مدى ضرورة التلازم بين الحماية الفنية والحماية الجزائية توجد وسائل فنية تواجه الاعتداء على نظام المعالجة الآلية للمعطيات، وتضع حدا لمختلف عمليات السطو والتخريب والقرصنة، وذلك عن طريق إعداد برمجيات الانترنت ووضعها على الشبكة لوضعها في موقف دفاعي عن النظام⁵، وهي ما تسمى الحماية الفنية التي لا يتطلبها الرأي الغالب في الفقه الفرنسي والذي يرى أنها ليست شرطا ضروريا لأن وجودها لا يكون له سوى دور واحد وهو إثبات سوء النية، فمن قام بانتهاك

¹ مسعود خثير، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، الجزائر، 2010، ص 109.

² جمال براهمي، مكافحة الجرائم الإلكترونية في التشريع الجزائري، المجلة النقدية، ص 126.

³ الاتفاقية الأوروبية لمكافحة الإجرام المعلوماتي ببودابست سنة 2001.

⁴ مسعود خثير، مرجع سابق، ص 110.

⁵ علي نايت عمر، الملكية الفكرية في إطار التجارة الإلكترونية، مذكرة ماجستير، تخصص القانون الدولي

للأعمال، جامعة مولود معمري تيزي وزو، 2014، ص 61.

النظام والدخول إليه بطريقة غير مشروعة فإن ذلك يدخل في إثبات القصد الجنائي، أما المشرع الجزائري فإن المبدأ المستقر هو مبدأ الشرعية، وعليه فإن عدم ذكر المشرع وعدم إشتراطه لشرط الحماية الفنية يعني أنه أراد إستبعاد هذا الشرط صراحة، ومن الناحية العملية فإن غالبية أنظمة المعالجة الآلية للمعطيات تتمتع بنظام حماية فنية يساعد خاصة على إثبات أركان الجريمة لاسيما الركن المعنوي.¹

ثانيا: الجرائم المعلوماتية في قانون العقوبات

تأخذ هذه الجريمة صورتين من صور الإعتداء هما:

1- الإعتداء على نظام المعالجة الآلية للمعطيات

تتحقق هذه الجريمة في صورتين:

*الصورة البسيطة للإعتداء على نظام المعالجة الآلية للمعطيات: ويتم ذلك في شكل الدخول أبقاء غير المرخص بهما.

- الدخول غير المرخص به: يتضح هذا السلوك من خلال المادة 394 مكرر من قانون العقوبات²، أين يتحقق السلوك المادي بمجرد الدخول إلى المنظومة باستعمال الوسائل الفنية أو التقنية، وذلك بغض النظر إن كان الدخول إلى النظام بأكمله أو إلى جزء منه، وتوقع العقوبة المقررة سواء كانت الجريمة تامة أو كان السلوك مجرد شروع في إرتكابها، فالمشرع لا يشترط لقيام الجريمة تحقق النتيجة بل المهم أن يكون الدخول عن طريق الغش أي غير مشروع، بمعنى أن لا يكون الدخول صدفة.³

¹ مختارية بوزيدي، ماهية الجريمة المعلوماتية، أعمال الملتقى الوطني آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري 29 مارس 2017، مركز جيل البحث العلمي، ص13.

² المادة 394 مكرر من القانون رقم 16-02 المؤرخ في 19 جوان 2016، المعدل والمتمم للأمر 66-156 المؤرخ في 08 جوان 1966 المتضمن قانون العقوبات تنص على: يعاقب بالحبس من ثلاث أشهر إلى سنة وبغرامة من 50000 دج إلى 100000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك.

³ نجية شيخ، حول مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم القانونية والسياسية، المجلد 09، العدد 02، جوان 2018، ص690.

- **البقاء غير المرخص به** : قد يتخذ النشاط الإجرامي سلوكا آخر هو البقاء داخل النظام، و يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، وقد يكون البقاء مقترنا بعملية الدخول أو مستقلا عنها، كما في حالة تحقق الدخول صدفة إلى النظام والبقاء عمدا به، وذلك متى تجاوز المتدخل المدة المسموح بها داخل النظام.¹

***الصورة المشددة للإعتداء على نظام المعالجة الآلية للمعطيات** بإستقراء نص المادة 394 مكرر2-3 من قانون العقوبات نجد أنهما قد نصت على طرفين تشدد بهما عقوبة الدخول والبقاء ويتمثل هذان الطرفان في حالة ما إذا نتج عن الدخول أو البقاء غير المشروع محو أو تعديل البيانات التي يحتويها النظام أو عدم قدرة النظام على تأدية وظيفته، ويكفي لقيام الطرف المشدد أن تكون هناك علاقة سببية بين الدخول أو البقاء غير المشروع وبين النتيجة التي تحققت وهي محو النظام.²

ثانيا تجريم الإعتداء على معطيات نظام المعالجة الآلية بعد أن تَفطن المشرع إلى ما قد يصيب معطيات نظام المعالجة الآلية عند الدخول والبقاء بها جرّم الإعتداء على هذه المعطيات كمايلي:

1- **تجريم الاعتداء على المعطيات الداخلية للنظام**: تنص المادة 394 مكرر1 من قانون العقوبات الجزائي على أن يعاقب بالحبس من 6 أشهر إلى 3 سنوات وبغرامة من 500000 دج إلى 2000000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية للمعطيات أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها،³ ويقصد بالمعطيات محل جريمة الإعتداء بمفهوم هذه المادة، تلك المعلومات التي يحتويها النظام وتشكل جزء منه، ليلاحظ من خلال المادة أن المشرع قد حصر حالات الإعتداء في:

***إدخال معطيات جديدة** وهي عبارة عن تعليمات بلغة ما توجه إلى كيان الحاسوب بغرض الوصول إلى نتيجة معينة تمثل هدف الجاني.⁴

***الحو وهو إزالة معطيات مسجلة وتخطيمها.**

¹ بدرة عمارة، الحماية الجنائية للمعلومات الإلكترونية دراسة في القانون 04-15، مجلة البحوث القانونية

والسياسية، العدد 02، جامعة مولاي الطاهر بسعيدة، 2014، ص 439

² مسعود خثير، مرجع سابق، ص 119.

³ المادة 394 مكرر 1 من القانون رقم 16 -02، سابق الذكر.

⁴ زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، 2011، ص 54.

*التعديل وهو تغيير المعطيات الموجودة داخل النظام و إستبدالها بمعطيات أخرى. ويكفي لقيام الجريمة توافر واحدة فقط من هذه الحالات¹.

2- تجريم الإعتداء على المعطيات الخارجية للنظام:

نص المشرع الجزائي على هذه الجريمة في المادة 394 مكرر² من قانون العقوبات، وكس بموجبها حماية جزائية للمعطيات في حد ذاتها، دون أن يشترط أن تكون المعلومة داخل النظام أو أن تكون قد تمت معالجتها آلياً، ويتمثل محل الجريمة في هذه الحالة في المعطيات سواء كانت مخزنة في أشرطة أو أقراص أو معالجة آلياً أو مرسلّة عن طريق منظومة معلوماتية مادامت قد تستعمل في ارتكاب الجرائم² التي حددها المشرع كمايلي:.

*تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلّة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

*حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.³

وبذلك فإن أي تلاعب في المعطيات الخارجية للنظام سواء كانت يمكن أن ترتكب بها الجريمة أو محصل عليها من جريمة يعتبر جريمة في حد ذاته حسب المادة 394 مكرر².

المطلب الثاني: ضيق النص التجريمي في القوانين الخاصة

لم يقتصر تجريم المشرع الجزائي على السلوك المقرّر كجريمة ضمن قانون العقوبات، بل إمتد هذا التجريم إلى بعض القوانين الخاصة، منها قوانين الملكية الأدبية والفنية ومنها بعض القوانين الخاصة الأخرى.

أولاً: التجريم في قانون الملكية الأدبية والفنية: حاول المشرع من خلال الأمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة حماية مختلف المصنفات الأدبية والفنية بما فيها المصنفات الرقمية، التي شكلت نقطة تقاطع بين جرائم الاعتداء على حق المؤلف وجرائم المعلوماتية التي وردت بهذا القانون

¹ نجية شيخ، مرجع سابق، ص 693 .

² مختارية بوزيدي، مرجع سابق، ص 18

³ زبيحة زيدان، مرجع سابق، ص 56.

وعليه ماهي شروط إضفاء الأمر 03-05 حمايته على المصنفات الرقمية؟، وكيف جرّم الإعتداء عليها ؟

أولا: شروط إضفاء الحماية الجزائية المقررة بموجب الأمر 03-05: حتى يتم إضفاء الحماية الجزائية على المصنفات التقليدية لابد من توافر شرط شكلي وهو الوجود أي التعبير عن المصنف وتثبيته على دعامة مادية وشرط موضوعي وهو شرط الابتكار، فإلى أي مدى يمكن القول بضرورة توافر الشرطين في المصنفات الرقمية حتى يمكن إعتبار الإعتداء عليها جريمة معلوماتية وفقا للأمر 03-05 ؟

- شرط الوجود: لا يمكن أن تنصب الحماية على شيء مستقبلي أو على مجرد الأفكار بل لابد أن يفرغ المصنف في صورة مادية يبرز فيها إلى الوجود ويكون معدا للنشر، لا أن يكون مظهر التعبير عن الفكرة قد بلغ الغاية من الوضع المستقر، وتحسيدا لهذا الوجود فرض المشرع عملية الإيداع القانوني كشرط شكلي لتقرير الحماية بنصه على ضرورة الإيداع في المادة 07 من الأمر 16/96 المتعلق بالإيداع القانوني بقولها: تخضع للإيداع القانوني..... وبرامج الحاسوب بكل أنواعها أو قواعد المعطيات وذلك مهما تكن الدعامة التي تحملها وتقنية الإنتاج والنشر والتوزيع.¹

- شرط الابتكار: يعرف الابتكار بأنه تمييز المصنف بطابع أصلي، إما في الإنشاء أو في التعبير، أي أنه يتسم بطابع يبرز شخصية صاحبه سواء في المضمون أو جوهر الفكرة أو في مجرد الطريقة التي اتبعها لعرض هذه الفكرة، وقد اختلفت الآراء حول ضرورة وجود الابتكار في برامج الكمبيوتر، مابين مؤيد ومعارض، لكن المشرع الفرنسي أوجب ضرورة توافر ذلك، أما المشرع الجزائري فلم يكن النص واضحا ولكن يستفاد ذلك من مضمون النص، فإشارة المشرع إلى عبارة الأصالة تعتبر قرينة مباشرة على وجوب و إشمال برامج الكمبيوتر على نوع من الأصالة تبرز من خلالها شخصية المؤلف،² وتتحقق شروط الحماية بسط المشرع حمايته على المصنفات الرقمية تحت نطاق حق المؤلف وتماشيا مع إتفاقية

¹ المادة 07 من الأمر 96-16 المؤرخ في 2 جويلية 1996، المتعلق بالإيداع القانوني، الجريدة الرسمية رقم 41 المؤرخة في 03 جويلية 1996.

² مسعود خثير، مرجع سابق، ص84.

برن الدولية حددها بمدة 50 سنة ابتداء من مطلع السنة الميلادية التي تلي نشر المصنف، وهو ما يعتبر مبالغاً فيه مقارنة بالمشروع المصري الذي حدّد مدة الحماية بـ 25 سنة فقط.¹

ثانياً: الجرائم الواردة في الأمر 03-05: تنقسم الجرائم الواردة في الأمر 03-05 المتعلقة بحقوق المؤلف والحقوق المجاورة إلى جرائم تقليد وجرائم التعامل بالمصنفات المقلدة.

1- جريمة التقليد: جاء النص عليها في المواد 151/ف1، 155، 154، 2 من الأمر 03-05، لتتكون بذلك من ركنين مادي ومعنوي كأى جريمة يتمثلان في:

الركن المادي: يتمثل الركن المادي لجريمة التقليد في قيام الجاني بأحد أفعال التقليد المنصوص عليها قانونياً على مصنف محمي، ليمثل هذا النشاط طبقاً للمادة 151/ف1 في الإعتداء على حق من الحقوق الأدبية أو المعنوية وذلك من خلال الكشف غير المشروع عن البرنامج، كأن يتم الكشف عن برنامج في الوقت أو بطريقة يرى المؤلف أنها غير مناسبة، أو المساس بالبرنامج عن طريق تعديله أو تغييره أو إضافة فيه أو حذف جزء منه دون موافقة صاحبه، ويلاحظ أن المشروع لم يجرم الإعتداء على أهم حق من الحقوق المعنوية، ألا وهو حق الأبوة أو ما يعرف بحق المؤلف في نسبة مؤلفه إليه، كما يتمثل النشاط المادي أيضاً في الإعتداء على الحقوق المالية عن طريق عملية النسخ دون موافقة المؤلف أو صاحب البرنامج²، وذلك بإستثناء الحالة التي يتم فيها إستنساخ نسخة واحدة إذا كان الغرض من ذلك هو:

*الاستنساخ بغرض استعمال برنامج الحاسوب للغرض الذي اكتسب من أجله، ووفقاً للشروط التي كانت قائمة عند اكتسابه، وفي هذا تدعيماً لحق المؤلف عندما يتجاوز التعاقد معه حدود التعاقد. عندما يكون النسخ تعويضاً لنسخة مشروعة الحياة من البرنامج وذلك بغرض التوثيق أو خشية ضياعه أو تلفه أو عدم صلاحيته للاستعمال.³

¹ عبد الهادي بن زبطة، حماية برامج الحاسوب في التشريع الجزائري، الطبعة الأولى، دار الخلدونية، الجزائر، 2007، ص56.

² صالح شنن، الحماية الجنائية لبرامج الحاسوب في التشريع الجزائري، المجلة الأكاديمية للبحث القانوني، العدد 01، جامعة عبد الرحمان ميرة، بجاية، 2010، ص65.

³ المادة 52 من الأمر 03-05 المؤرخ في 19 جويلية 2003، المتعلقة بحق المؤلف والحقوق المجاورة، الجريدة الرسمية رقم 44 المؤرخة في 23 جويلية 2003، ص10.

كما أكد المشرع في المادة 154 من الأمر 03-05 أنه يعتبر مرتكباً لجريمة التقليد كل من يشارك بعمله أو بالوسائل التي يجوزها للمساس بحق المؤلف أو صاحب البرنامج¹، فضلاً على إعتبره عدم دفع المكافئة المستحقة عمداً للمؤلف أحد جرائم التقليد، وذلك رغم كونها في الأصل إخلالاً بالمسؤولية العقدية المترتبة عن العقد وليست جريمة.

الركن المعنوي: لا يكفي لقيام جريمة التقليد وجود ركن مادي بل لابد من علم وإرادة الجاني أثناء قيامه بأي اعتداء، وإن كان المشرع لم ينص على ذلك صراحة، والقصد المتطلب في هذه الحالة هو القصد العام وليس الخاص، فيكفي أن يعلم الجاني أنه يعتدي على برنامج شخص آخر وأن تتجه إرادته لذلك.²

2- جريمة التعامل بالبرامج المقلدة: لقيام هذه الجريمة لابد من توافر ركنين هما:

الركن المادي: يتمثل الركن المادي لهذه الجريمة في التعامل ببرنامج مقلد، أي التعامل ببرنامج مشابه للبرنامج الأصلي تم الوصول له عن طريق المحاكاة بين البرنامج الأصلي والنسخة المقلدة، وتتمثل صور هذا التعامل في:

- استيراد أو تصدير نسخ مقلدة.

- بيع نسخ مقلدة. لا يشترط أن تتكرر عمليات البيع حتى تقوم الجريمة.

- تأجير مصنف مقلد أو عرضه للتداول.³

الركن المعنوي: يتمثل الركن المعنوي في القصد الجنائي العام، والذي يقتضي أن يكون الجاني عالماً بأن عما يبيعه أو يتداوله أو يؤجره أو يستورده أو يصدره برنامج مقلد مع إتجاه إرادته لذلك، وهو قصد مفترض يفتر تواجده بمجرد توافر الركن المادي لهذه الجريمة. وإن كان توافر الركن المادي يعتبر قرينة بسيطة على توافر القصد الجنائي قابلة لإثبات العكس، وخاضعة لتقدير محكمة الموضوع دون رقابة من محكمة النقض.⁴

¹ المادة 154 من الأمر 03-05 المتعلق بحق المؤلف والحقوق المجاورة، سابق الذكر.

² مسعود خثير، مرجع سابق، ص 96.

³ نجية شيخ، مرجع سابق، ص 696.

⁴ صالح شننن، مرجع سابق، ص 67.

ثانيا: **التجريم في بعض القوانين الخاصة الأخرى** إضافة إلى الجرائم التي تضمنتها القوانين السابقة حاول المشرع التوسيع نوعا ما من الجرائم المعلوماتية في بعض القوانين الخاصة .

1- قانون رقم 2000-03 مؤرخ في 05 غشت سنة 2000، يحدد القواعد العامة المتعلقة لبريد والمواصلات السلوكية واللاسلكية: وتتمثل الجرائم المعلوماتية التي نص عليها المشرع الجزائري ضمن هذا القانون في:

- فتح أو تحويل أو تخريب البريد أو انتهاك سرية المراسلات أو المساعدة على ارتكاب هذه الأفعال من قبل:

- كل شخص يقوم بتقديم خدمة البريد السريع الدولي أو كل عون يعمل لديه وفي إطار ممارستهم لمهامهم،

- كل شخص مرخص له بتقديم خدمة مواصلات سلوكية ولاسلكية.

- كل عامل لدى متعاملي الشبكات العمومية للمواصلات السلوكية واللاسلكية وأثناء ممارستهم لمهامهم وغيرهم.

- إنشاء أو استغلال شبكة عمومية للمواصلات السلوكية واللاسلكية دون رخصة أو مواصلة ممارسة النشاط.

- إنشاء أو استغلال شبكة عمومية للمواصلات السلوكية واللاسلكية دون رخصة أو مواصلة ممارسة النشاط خرقا لقرار التعليق أو سحب هذه الرخصة.

- إنشاء أو العمل على إنشاء شبكة مستقلة دون ترخيص.

- إشهار بغرض بيع تجهيزات أو معدات للمواصلات السلوكية واللاسلكية دون الحصول على الاعتماد المسبق.

- تحويل أو العمل على تحويل أو استغلال خطوط المواصلات السلوكية واللاسلكية المحوثة.¹

2- قانون التأمينات: تضمن قانون التأمينات من خلال المادة 6 مكرر 01 منه¹ التي تضمنت الجريمة الإلكترونية من خلال هيئات الضمان الاجتماعي في نصوص قانونية عديدة، تخص البطاقة

¹ ورودة شرف الدين وسامية بولجرف، الجوانب الموضوعية والإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري، مجلة المنار للبحوث والدراسات القانونية والسياسية، العدد 03، ديسمبر 2017، ص 33.

الإلكترونية التي تسلم للمؤمن له اجتماعيا مجانا بسبب العلاج، وهي صالحة في كل التراب الوطني، وكذلك الجزاءات المقررة في حالة الإستعمال غير المشروع، أو حالة ما يقوم الشخص عن طريق الغش بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا².

3- القانون رقم 09-04 المؤرخ في 5 أوت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهم: أكد المشرع الجزائري في المادة 2 على أنه يقصد بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية، كما تحدث المشرع الجزائري في الفصل الرابع من قانون رقم: 09-04، المؤرخ في 5 أوت سنة 2009، في المادتين 10 و11، على أنه من بين التزامات مقدمي الخدمات مساعدة السلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وب حفظ المعطيات المتعلقة بحركة السير ووضعها تحت تصرف السلطات المذكورة . ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين، وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق، بينما فصلت المادة 11 في إجراء حفظ المعطيات المتعلقة بخط السير، دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في المادة 11 من نفس القانون، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة 6 أشهر إلى خمس 5 سنوات وبغرامة من 50000 دج إلى 500000 دج. ويعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات³، وما يمكن ملاحظته أن هذا القانون ركز على التدابير الوقائية لمكافحة الجرائم المعلوماتية أكثر من تركيزه على عملية التجريم.

¹ المادة 6 مكرر 1 من القانون 08-01 المؤرخ في 23 جانفي 2008 المتعلق بالتأمينات، الجريدة الرسمية رقم 04 المؤرخة في 25 جانفي 2008.

² نجية الشيخ، مرجع سابق، ص 699.

³ وردة شرف الدين وسامية بولجرف، مرجع سابق، ص 36.

المبحث الثاني: إتساع السلوك الإجرامي في الجرائم المعلوماتية

عرّف أصحاب الإتجاه المؤسّع الجريمة المعلوماتية بأنها سلوك إجرامي يتم في محيط أجهزة الكمبيوتر، وقد عرّفها الفقيهان credo /michel بأنها سوء إستخدام الحاسب أو جريمة الحاسب تسهل إستخدام الحاسب كأداة لارتكاب الجريمة، بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحساب المجني عليه أو بياناته، كما تمتد لتشمل الاعتداءات المادية على جهاز الحاسب ذاته، وكذا الاستخدام غير المشروع لبطاقات الإئتمان بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكوّنات المادية والمعنوية للحاسب¹، لذا قد تدخل ضمن الجريمة المعلوماتية العديد من السلوكات الإجرامية التي قد لا تستوعبها النصوص التجريمية السابقة والتي تشكّل إما إعتداء على المكوّنات المادية أو المعنوية للحاسب، وإما إستخدام الحاسب كأداة لارتكاب الجريمة.

المطلب الأول: الإعتداء على مكوّنات الحاسب قد يكون الإعتداء إما على مكوّنات الحاسب المادية، كما قد يتعلق بمكوّنات الحاسب المعنوية.

أولاً: الإعتداء على المكوّنات المادية للحاسب تتحقق هذه الحالة إذا كانت أجهزة الحاسب المادية من أجهزة ومعدات وكابلات وشبكات ربط وآلات و شرائط خام من التي تسجل عليها البرامج والمعطيات هي محلا لهذه الجريمة وبالتالي لا تثير هذه الحالات أية مشكلة في ضيق النص التجريمي لأنها تتمتع بالحماية الجنائية للنصوص التقليدية باعتبارها من الأموال المنقولة التي تخضع سرقته وإتلافها لنصوص التجريم التقليدية²، وبذلك فإن الإعتداء على الكيان المادي يخضع لأحكام صور الإعتداء على شيء مادي كأحكام السرقة و الإتلاف والنصب وخيانة الأمانة، ليتمكن تصور إستخدام الأساليب التقليدية لارتكاب عدة جرائم يكون محلها المكوّنات المادية للحاسب مثل سرقة الدعامة المادية وما تحتويها من برامج وبيانات أو سرقة البطاقة الممغنطة التي تستخدم لسحب النقود من الحاسب، وكذا إتلاف البرامج والبيانات عن طريق تدمير الدعامات التي تحويها، سواء بإحراقها أو تفجيرها.

¹ سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، العدد 07، جامعة محمد خيضر بسكرة، ص 276.

² الشاذلي فتوح و عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، لبنان، 2003، ص 36.

ثانيا: الإعتداء على المكونات المعنوية للحاسب عند الإعتداء على الكيان المعنوي تكون النصوص التجريبية عاجزة عن حمايته بصورة فعالة لأن لهذا الكيان طابعا خاصا¹ تكون فيه مكونات الحاسب المعلوماتية الغير مادية مثل البرامج المستخدمة، البيانات والمعطيات المخزنة في ذاكرة الحاسب محلا أو موضوعا للجريمة، حيث من المتصور أن يقوم أحد الأشخاص بالإعتداء على برنامج الحاسب أو أنيدعي ملكيته أو يقوم بسرقة أو يقلده أو يتلفه أو يعطله أو يقوم بإفشاء محتوياته، أما البيانات فيستطيع العبث بها، تحريفها وتزويرها ونسخها²، وبالنسبة لهذا النوع من الجرائم فهي قد أخذت الحظ الأوفر من نسبة التجريم في التشريع الجزائري، لاسيما في قانون العقوبات، غير أن اتساع الهوة بين تطور مستوى الجرائم المعلوماتية الواقعة على المكونات المعنوية للحاسب ودرجة ثبات النص التجريبي، أفرزت وجود فراغ تشريعي لاسيما بالنسبة لبعض السلوكات الإجرامية البارزة والتي من بينها:

- **تعديل البرنامج:** الهدف الرئيسي من تعديل هذه البرامج يتمثل في اختلاس النقود و تكثر هذه الجرائم في مجال الحسابات، ومن أمثلة ذلك قيام مبرمج بأحد البنوك الأمريكية بإدارة الحسابات بتعديل برنامج بإضافة دولار واحد على كل حساب يزيد عن عشرة دولارات و قام بقيد المصاريف الزائدة في حساب خاص به أطلق عليه اسم Zzwick و حصل على إثر ذلك على مئات الدولارات كل شهر و كان من الممكن أن يستمر هذا العمل الإجرامي لولا أن البنك أراد بمناسبة تأسيس شركة جديدة للدعاية أن يكافئ أول و آخر عميل له ليكتشف عدم وجود ما يدعى Zzwick. وهناك نظام آخر يسمى سلامي Salami و يتم الاختلاس بموجب هذا النظام باستقطاع مبالغ زهيدة و على فترات زمنية طويلة و متباعدة من خلال صفقات عديدة يترتب عليها تحقيق فائدة كبيرة.

- **التلاعب في البرنامج:** يأخذ التلاعب في البرنامج عدة أشكال فقد يتم عن طريق استعمال القنبلة المنطقية أو عن طريق قيام أحد المبرمجين بزرع برنامج فرعي غير مسموح به في البرنامج الأصلي

¹ محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة لبنان، 2004، ص 163.

² الشاذلي فتوح و عفيفي كامل عفيفي، مرجع سابق، ص 36.

يسمح له بالدخول غير المشروع في العناصر الضرورية لأي نظام معلوماتي، و يصعب اكتشاف هذا البرنامج لصغره و دقته¹.

-التلاعب في البرامج التشغيلية: التلاعب هنا قد يأخذ وجهين:

الوجه الأول: المصيدة: وتعني أن أي برنامج يتضمن عند إعدادة أخطاء و عيوب قد لا تكتشف كلها أو بعضها إلا عند الإستعمال، أين يستطيع المبرمج القيام بتصحيحها عن طريق الولوج للبرنامج من خلال ما يعرف بالمداخل المميزة التي يجب أن يستبعد المبرمج بمجرد الإنهاء من التصحيح النهائي للبرنامج، إلا أنه قد يعتمد وبسوء قصد إلى الإبقاء عليها لاستخدامها للولوج في البرنامج في أي وقت.

الوجه الثاني: إصطناع برنامج وهمي: القصد منه هو التخطيط لمراقبة وتنفيذ ارتكاب جرائم الغش المعلوماتي التي تأتي الصدفة في الغالب وراء إكتشافها².

-إتلاف ومحو المعلومات: قد يهدف الجاني من خلال ارتكابه الجريمة المعلوماتية إلى إتلاف المعلومات المخزنة بالنظام المعلوماتي. ويتخذ الإتلاف عدة صور فقد يتم عن طريق طرق الإتلاف العادية كالحريق أو الضرب أو السرقة أو عن طريق استبدال أو محو المعلومات، و يشكل استبدال المعلومات نوع من جرائم الغش أو التزوير المعلوماتي و هو على درجة كبيرة من الخطورة لأنه في حالة نجاحه يستمر لوقت طويل قبل اكتشافه و يتولد عنه مكاسب كبيرة بمجرد استبدال رقم بآخر أو إحلال رقم مكان آخر، فمثلا هناك مجموعة من المستخدمين الإداريين استطاعوا خلال سنوات قليلة مضاعفة روايتهم عن طريق النظام المعلوماتي.

أما محو المعلومات فهو من أسهل طرق الإتلاف كون أنه من خصائص الجرائم المعلوماتية قدرة الجاني على محو آثار جريمته في فترة وجيزة جدا لا تتعدى الضغط على زر بسيط في لوحة المفاتيح أو البرنامج عن طريق الفأرة، فمثلا قام شخصان باختلاس مبلغ يقدر ب 61000 دولار مرسله من

¹ سفيان سوير، جرائم المعلوماتية، مذكرة ماجستير تخصص العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بلقايد تلمسان، 2011، ص42.

² الشاذلي فتوح و عفيفي كامل عفيفي، مرجع سابق، ص41.

شركات التأمين إلى إحدى المراكز الجامعية عن طريق محو الحسابات القائمة في سجلات النظام المعلوماتي الخاص بالمركز و جعلها غير قابلة للتحصيل.¹

المطلب الثاني: إستخدام الحاسب كأداة لإرتكاب الجريمة

إن كانت صعوبة توسيع نطاق التجريم تطرح نفسها في جرائم الاعتداء على الكيان المعنوي للبرامج، فإن هذه الصعوبة تطرح أكثر عندما يكون الحاسب الآلي أداة لارتكاب وتسهيل إرتكاب مختلف الجرائم التقليدية، أين يستلزم الأمر إصدار قانون يتعلق بالجرائم التقليدية المرتكبة بواسطة الحاسب سواء تعلقت بالإعتداء على الأموال أو كانت تشكل إعتداء على الأشخاص، والتي من بينها على سبيل المثال لا الحصر الجرائم التالية:

أولاً: إستخدام الحاسب كأداة لإرتكاب جريمة إعتداء على الأموال

تمثل هذه الجرائم في جملة الجرائم التي تستهدف أموال الأشخاص والمؤسسات، والتي من بينها:

1- جرائم إساءة إستخدام البطاقة الائتمانية: أدى إدخال النظام المعلوماتي في مجالات عمليات البنوك إلى ظهور هذا النوع الجديد من الجرائم المعلوماتية. و تعد من أخطر الجرائم المعلوماتية لاسيما في المجتمعات التي تتسم نظمها البنكية بدرجة عالية من التطور و الحداثة، و يتخذ هذا النوع من الجرائم المعلوماتية صورتين. تتمثل الأولى في إساءة استخدام العميل البطاقات الائتمانية و ذلك عن طريق عدم احترام العميل المصدر إليه البطاقات الائتمانية شروط العقد المبرم بينه و بين البنك، كأن يستعمل بطاقة ائتمانية انتهت مدة صلاحيتها أو بطاقة تم إلغاؤها أو الشراء بأكثر من قيمتها...إلخ، وأما الصورة الثانية تتمثل في إساءة استخدام الغير البطاقات الائتمانية كأن يقوم سارق استعمال البطاقة الائتمانية للحصول على السلع و الخدمات أو سحب مبالغ مالية بموجبها من أجهزة التوزيع الآلي أو السحب بإستخدام بطاقات مزورة.²

2 - جرائم التجارة الإلكترونية: بعد أن إنتشرت التجارة الإلكترونية وإتاحتها للعديد من المزايا لرجال الأعمال عن طريق تجنيبهم مشقة السفر لتنفيذ عمليات البيع والشراء، أفرز ذلك نوعاً من الصعوبة لاسيما في ظل غياب مستندات ورقية بخط اليد يمكن من خلالها التمييز بين الرسالة الأصلية والرسالة المستنسخة، وهو ما سبب إحتمال إرتفاع جرائم تزوير الرسائل الإلكترونية عبر

¹ سفيان سوير، مرجع سابق، ص 45

² سفيان سوير، نفس مرجع، ص 37.

الأنترنت، فضلا على إمكانية الوفاء بنوع آخر من النقود يعرف بالنقود الورقية -DIGITAL MONEY، مما أدى إلى تطور أساليب الإعتداء، إضافة إلى عمليات السطو والقرصنة.¹

3- جرائم القمار وغسيل الأموال: من الجرائم التي ترتكب بواسطة الحاسب جرائم القمار وغسيل الأموال، إذ يمنح الراغب في ممارسة القمار خصوصية أكثر تتداخل غالبا مع جريمة غسيل الأموال بتوفير عدة مميزات منها السرعة الشديدة وتغطي الحواجز الحدودية بين الدول وتفادي القوانين التي تضعها هذه الدول لإعاقة النشاط، مما يعطيها قدر كبير من السرية²، وخاصة في تسهيل ارتكاب جرائم غسيل الأموال التي يقصد بها أساسا نقل أموال مستمدة من مصدر غير مشروع بهدف تظهيرها، فهي جملة العمليات ذات الطبيعة الاقتصادية والمالية التي تؤدي إلى إدخال أموال ناتجة من أنشطة غير مشروعة ضمن دائرة الإقتصاد الرسمي³، وهو الأمر الذي يسهل إرتكابه في المجال المعلوماتي على أساس أن وجود كمية هائلة من الأموال قد تكون قابلة للحركة عبر النظام المعلوماتي في زمن قصير للتجاوز بذلك حدود الدولة وكذا قوانينها.

4- جرائم السرقة والسطو على أموال البنوك:

أصبحت البنوك والمصارف هي هدف لمحتربي التلاعب واختراق شبكات الانترنت والذين يتلاعبون في كشوف حسابات العملاء ونقل الأرصدة من حساب لآخر، وقد تكون بصورة ثانية كإضافة بضعة أرقام أو أصفار إلى رقم ما في هذا الحساب. جاءت ثورة المعلومات في النصف الثاني من القرن العشرين لكي تفرض على العالم تحديات كثيرة ولدها التطور العلمي والثورة الهائلة في مجال التكنولوجيا والمعلومات والاتصالات وصناعة الالكترونيات والتعامل مع نظم متقدمة للخبرة والذكاء الاصطناعي⁴، لتتم جرائم السطو على أعمال البنوك عن طريق استخدام الحاسب الآلي للوصول غير المشروع للبنوك وتحويل الأموال من الحسابات الخاصة بالعملاء إلى حسابات أخرى⁵.

¹ خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، مصر، 2009، ص121.

² صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجستير تخصص قانون دولي للأعمال، جامعة مولود معمري تيزي وزو، 2013، ص47.

³ خالد ممدوح إبراهيم، مرجع سابق، ص130.

⁴ فتيحة رصاع، الحماية الجنائية للمعلومة على شبكة الأنترنت، مذكرة ماجستير في القانون العام، جامعة أبي بكر بلقايد تلمسان، 2012، ص84.

⁵ يوسف صغير، ص48.

ثانيا: استخدام الحاسب كأداة لإرتكاب جريمة إعتداء على الأشخاص

تعدد صور استخدام الحاسب كأداة لإرتكاب جرائم الإعتداء على الأشخاص، لذا يمكن التعرض لبعض هذه الصور كمايلي:

1 جرائم السب والقذف: تعد جرائم السب والقذف من أكثر الجرائم انتشارا، فالقذف هو إسناد واقعة محدّدة تستوجب عقاب من تنسب إليه أو إحتقاره إسنادا علنا عمديا يفيد نسبة الأمر إلى الشخص على سبيل التوكيد، أما السب فهو خدش شرف شخص واعتباره عمدا دون أن يتضمن ذلك إسناد واقعة معينة إليه، مع ضرورة توافر العلانية في كليهما،¹ وهو ما يجعل المنظومة المعلوماتية مجالا خصبا لارتكاب هذه الجرائم لما تحقّقه من تسهيل علانية السب والقذف.

2- جريمة الإرهاب الإلكتروني: في عصر الازدهار الالكتروني و في زمن قيام حكومات الكترونية، تبدل نمط الحياة وتغيرت معه أشكال الأشياء وأنماطها ومنها ولا شك أنماط الجريمة والتي قد يحتفظ بعضها باسمها التقليدي مع تغيير جوهري أو بسيط في طرق ارتكابها، ومن هذه الجرائم الحديثة في طرقها والقديمة في اسمها جريمة الإرهاب الإلكتروني والتي أخذت أشكال حديثة تتماشى مع التطور التقني، ويتغير تطور الأساليب التي يحاول المفسدين الوصول بها إلى أهدافها، فقد غدا الإرهاب الإلكتروني هو السائد حاليا . وأصبح اقتحام المواقع وتدميرها وتغيير محتوياتها والدخول على الشبكات والعبث بمحتوياتها بإزالتها أو بالاستيلاء عليها أو الدخول على شبكات الاتصالات أو شبكات المعلومات بهدف تعطيلها عن العمل أطول فترة ممكنة أو تدميرها نهائياً أصبح هو أسلوب الإرهاب حالياً في محاولة الوصول إلى أغراضهم،² وكان أول استخدام لكلمة الإرهاب الإلكتروني في فترة الثمانينات في دراسة "Barrycollin" التي خلص فيها إلى صعوبة تعريف ظاهرة الإرهاب التكنولوجي بدقة، وأيضا الأساليب والحلول المطلوبة لمواجهته وكذا تحديد دور الكمبيوتر و الأنترنت في العمل الإرهابي، ل يتميز بذلك الإرهاب الإلكتروني الذي يعرف بأنه كل " عدوان أو تخويف أو تهديد مادي أو معنوي باستخدام الوسائل الإلكترونية، الصادر من الدول أو الجماعات أو الأفراد على الإنسان سواء في دينه أو نفسه أو عرضه، أو عقله، أو ماله بغير حق، وبالتالي فلكي ينعت شخصا ما بأنه إرهابيا، وليس فقط مخترقا، فلا بد وأن تؤدي الهجمات التي

¹ خالد ممدوح إبراهيم، مرجع سابق، ص 125.

² فتيحة رصاع، مرجع سابق، ص 77.

يشنها إلى عنف ضد الأشخاص أو الممتلكات، أو على الأقل تحدث أذى كافيا من أجل نشر الخوف والرعب¹، وذلك عن طريق استخدام الوسائل التالية:

***التسلل:** يشمل هذا الفعل كل الاختراقات للمواقع الرسمية للمؤسسات الحكومية أو المواقع الشخصية أو اختراق البريد الإلكتروني أو الاستيلاء على الأرقام السرية للمستخدمين، وتتم هذه العملية عن طريق تشغيل برنامج إلكتروني صغير يعرف باسم "حصان طروادة" في الحاسب الآلي للتجسس على كل ما يقوم به صاحبه، حيث يقوم هذا البرنامج بتسجيل كل بياناته السرية..

***الإغراق بالرسائل الإلكترونية:** تتم هذه العملية عن طريق إرسال عدد كبير من الرسائل الإلكترونية ذات الحجم الكبير غير المفيدة دفعة واحدة وفي وقت متقارب قصد التأثير على السعة التخزينية للحواسيب الآلية المستهدفة، ما يؤدي إلى توقفها عن العمل بسبب امتلاء منافذ الإتصال وكذا قوائم الانتظار، الأمر الذي ينتج عنه انقطاع الخدمة التي توفرها هذه الحواسيب.

*- **نشر الفيروسات الإلكترونية:** يقصد بالفيروسات الإلكترونية برامج خارجية صنعت عمدا بغرض تغيير خصائص الملفات التي تصيبها، لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب وما شابهها من عمليات يكون الغرض منها إلحاق الضرر بحاسوب أو السيطرة عليه².

***إنشاء مواقع أنترنت:** يقوم الإرهابيون بإنشاء و تصميم مواقع لهم على شبكة المعلومات العالمية لنشر أفكارهم والدعوة إلى مبادئهم، بل تعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية، فقد أنشئت مواقع لتعليم صناعة المتفجرات، وكيفية اختراق وتدمير المواقع، وكيفية الدخول إلى المواقع المحجوبة، وطريقة نشر الفيروسات، ومن بين المواقع الإلكترونية التي تم تصميمها من بعض التنظيمات الإرهابية، موقع النداء: وهو الموقع الرسمي لتنظيم القاعدة، بعد أحداث 11 سبتمبر³.

3- جرائم المخدرات والمخدرات الرقمية: بعد أن ظهرت مخاوف جديدة من مواقع السوء - المواقع المنتشرة على الانترنت والتي لا تتعلق بالترويج للمخدرات وتشويق النشء لاستخدامها بل تتعداه إلى

¹ وهيبة بشريف، أساليب الجريمة الإلكترونية: مسار الانتقال من الإرهاب التقليدي إلى الإرهاب الإلكتروني في ظل المجتمع المعلوماتي، مجلة الحوار الثقافي بجامعة مستغانم، العدد 2018، 01، ص 64.

² توفيق مجاهد، جريمة الإرهاب الإلكتروني في ضوء أحكام الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، مجلة العلوم القانونية والسياسية، العدد 03، ديسمبر 2018، ص 85.

³ وهيبة بشريف، مرجع سابق، ص 65.

كيفية زراعة وصناعة المخدرات بكافة أصنافها وأنواعها وبأبسط الوسائل المتاحة¹، تطور الأمر إلى ظهور ما يعرف بالمخدرات الرقمية التي يتم فيها تحويل المادة المخدرة والمؤثرة في النواحي العقلية والنفسية، من شكلها المادي أو السائل أو الغازي، إلى شكل جديد من خلال تحميل هذه المخدرات في أوعية رقمية على شكل أسطوانات أو ملفات، بحيث يشكل الملف أو الأسطوانة الجرعة المخدرة، بما يكون لها من تأثير قد يعادل التأثير نفسه الذي تحدثه المخدرات التقليدية في عمل الدماغ والتفاعلات الكيميائية والعصبية، وفي الحالة النفسية والعصبية، وقد تكون دافعا في كثير من الحالات لتعاطي المخدرات الحقيقية التقليدية²، لأنها تحدث حالة من السعادة والحاجة إلى تناول الخمر، كما تعمل على تحسين مهارات التصوّر والتخيّل، حيث وبعد محاولة الاستغناء عنها يفقد الضحية توازنه النفسي ويصبح بالتالي عرضة للاختيار العصبي³.

خاتمة:

بعد دراسة الجريمة الإلكترونية بين ضيق النص التجريمي واتساع السلوك الإجرامي، يمكن القول أنه رغم عمل المشرع على وضع نصوص تجريمية لمكافحة الجريمة الإلكترونية سواء في قانون العقوبات أو في قانون الملكية الأدبية والفنية والقانون 04-09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، ومحاولته توسيع نطاق التجريم ليشمل الشروع في ارتكاب هذه الجرائم والاتفاق الجنائي على ارتكابها، إلا أن تطور مستوى السلوك الإجرامي لها وارتباطه بالتطور التقني اللامنتهي، جعل هناك عدم تناسب بين المستوى التجريمي المتواجد والمستوى الإجرامي الموجود، وهو ما يدفعنا للوصول إلى الإقتراحات التالية:

* اعتماد الدقة والوضوح والحبكة القانونية عند تحديد أنماط السلوك الإجرامي والابتعاد عن التعبيرات الغامضة أو المطاطية التي تحمل أكثر من معنى أو دلالة.

* عدم الاقتصار عند التجريم والعقاب على أنماط السلوك المحظور المرتكبة حالياً بل يجب مراعاة الأبعاد المستقبلية لأن تكنولوجيا المعلومات والحواسيب في تطور سريع.

¹ فتيحة رصاع، مرجع سابق، ص 83.

² عمر عبد المجيد مصبح، الإشكالات الجزائية في تكييف المخدرات الرقمية، ص 217.

³ ياسين جبيري، المخدرات الرقمية، مجلة الشريعة والاقتصاد، جامعة الأمير عبد القادر للعلوم الإسلامية بقسنطينة،

العدد 08، ص 578.

*وضع قانون خاص بالجرائم المعلوماتية بدل تناثر أحكام تجريمها في قانون العقوبات وبعض القوانين الخاصة وذلك بالموازاة مع بع الجرائم الأقل خطورة منها كجرائم الفساد وتبييض الأموال التي لها قوانين خاصة.

الهوامش:

محمد أمين الشوابكة، جرائم الحاسوب والأنترنيت، دار الثقافة للنشر والتوزيع، عمان، 2007، ص 08.

² مسعود خثير، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، الجزائر، 2010، ص 109.

³ جمال براهمي، مكافحة الجرائم الإلكترونية في التشريع الجزائري، المجلة النقدية، ص 126.

⁴ الاتفاقية الأوروبية لمكافحة الإجرام المعلوماتي ببودابست سنة 2001.

⁵ مسعود خثير، مرجع سابق، ص 110.

⁶ علي نايت عمر، الملكية الفكرية في إطار التجارة الإلكترونية، مذكرة ماجستير، تخصص القانون الدولي للأعمال، جامعة مولود معمري تيزي وزو، 2014، ص 61.

⁷ مختارية بوزيدي، ماهية الجريمة المعلوماتية، أعمال الملتقى الوطني آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري 29 مارس 2017، مركز جيل البحث العلمي، ص 13.

⁸ المادة 394 مكرر من القانون رقم 16 - 02 المؤرخ في 19 جوان 2016، المعدل والمتمم للأمر 66-156 المؤرخ في 08 جوان 1966 المتضمن قانون العقوبات تنص على: يعاقب بالحبس من ثلاث أشهر إلى سنة وبغرامة من 50000 دج إلى 100000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك.

⁹ نجية شيخ، حول مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم القانونية والسياسية، المجلد 09، العدد 02، جوان 2018، ص 690.

¹⁰ بدرة عمارة، الحماية الجنائية للمعلومات الإلكترونية دراسة في القانون 04-15، مجلة البحوث القانونية والسياسية، العدد 02، جامعة مولاي الطاهر بسعيدة، 2014، ص 439.

¹¹ مسعود خثير، مرجع سابق، ص 119.

¹² المادة 394 مكرر 1 من القانون رقم 16 - 02، سابق الذكر.

¹³ زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، 2011، ص 54.

¹⁴ نجية شيخ، مرجع سابق، ص 693.

- 15 مختارية بوزيدي، مرجع سابق، ص18
- 16 زبيحة زيدان، مرجع سابق، ص56.
- 17 المادة 07 من الأمر 96-16 المؤرخ في 2 جويلية 1996، المتعلق بالإيداع القانوني، الجريدة الرسمية رقم 41 المؤرخة في 03 جويلية 1996.
- 18 مسعود خنير، مرجع سابق، ص84.
- 19 عبد الهادي بن زيطة، حماية برامج الحاسوب في التشريع الجزائري، الطبعة الأولى، دار الخلدونية، الجزائر، 2007، ص56.
- 20 صالح شنين، الحماية الجنائية لبرامج الحاسوب في التشريع الجزائري، المجلة الأكاديمية للبحث القانوني، العدد 01، جامعة عبد الرحمان ميرة، بجاية، 2010، ص65.
- 21 المادة 52 من الأمر 03-05 المؤرخ في 19 جويلية 2003، المتعلق بحق المؤلف والحقوق المجاورة، الجريدة الرسمية رقم 44 المؤرخة في 23 جويلية 2003، ص10.
- 22 المادة 154 من الأمر 03-05 المتعلق بحق المؤلف والحقوق المجاورة، سابق الذكر.
- 23 مسعود خنير، مرجع سابق، ص96.
- 24 نجية شيخ، مرجع سابق، ص696.
- 25 صالح شنين، مرجع سابق، ص67.
- 26 وردة شرف الدين وسامية بولجرف، الجوانب الموضوعية والإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري، مجلة المنار للبحوث والدراسات القانونية والسياسية، العدد 03، ديسمبر 2017، ص33.
- 27 المادة 6 مكرر 1 من القانون 08-01 المؤرخ في 23 جانفي 2008 المتعلق بالتأمينات، الجريدة الرسمية رقم 04 المؤرخة في 25 جانفي 2008.
- 28 نجية الشيخ، مرجع سابق، ص699.
- 29 وردة شرف الدين وسامية بولجرف، مرجع سابق، ص36.
- 30 سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، العدد 07، جامعة محمد خيضر بسكرة، ص276.
- 31 الشاذلي فتوح و عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، لبنان، 2003، ص36.

- 32 محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة لبنان، 2004، ص163.
- 33 الشاذلي فتوح و عفيفي كامل عفيفي، مرجع سابق، ص36..
- 34 سفيان سوير، جرائم المعلوماتية، مذكرة ماجستير تخصص العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بلقايد تلمسان، 2011، ص42.
- 35 الشاذلي فتوح و عفيفي كامل عفيفي، مرجع سابق، ص41.
- 36 سفيان سوير، مرجع سابق، ص 45.
- 37 سفيان سوير، نفس مرجع، ص37.
- 38 خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، مصر، 2009، ص121.
- 39 صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجستير تخصص قانون دولي للأعمال، جامعة مولود معمري تيزي وزو، 2013، ص47.
- 40 خالد ممدوح إبراهيم، مرجع سابق، ص130.
- 41 فتيحة رصاع، الحماية الجنائية للمعلومة على شبكة الأنترنت، مذكرة ماجستير في القانون العام، جامعة أبي بكر بلقايد تلمسان، 2012، ص84 .
- 42 يوسف صغير، ص48.
- 43 خالد ممدوح إبراهيم، مرجع سابق، ص125.
- 44 فتيحة رصاع، مرجع سابق، ص77.
- 45 وهيبة بشريف، أساليب الجريمة الإلكترونية: مسار الانتقال من الإرهاب التقليدي إلى الإرهاب الإلكتروني في ظل المجتمع المعلوماتي، مجلة الحوار الثقافي بجامعة مستغانم، العدد 2018، 01، ص64.
- 46 توفيق مجاهد، جريمة الإرهاب الإلكتروني في ضوء أحكام الإنفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، مجلة العلوم القانونية والسياسية، العدد 03، ديسمبر 2018، ص85.
- 47 وهيبة بشريف، مرجع سابق، ص65.
- 48 فتيحة رصاع، مرجع سابق، ص83.
- 49 عمر عبد المجيد مصباح، الإشكالات الجزائية في تكييف المخدرات الرقمية، ص217.
- 50 ياسين جبري، المخدرات الرقمية، مجلة الشريعة والاقتصاد، جامعة الأمير عبد القادر للعلوم الإسلامية بقسنطينة، العدد 08، ص578.

التنظيم القانوني للجريمة المعلوماتية

د/ محميد حميد

كلية الحقوق والعلوم السياسية

جامعة الجلفة

د/ غضبان سمية

كلية الحقوق والعلوم السياسية

جامعة المسيلة

مقدمة:

لقد شهد العالم في العصر الحديث تطورا ملحوظا مس كل المجالات الحياتية في المجتمعات، كان من أهمها المجال التكنولوجي الذي كانت بدايته بشكل مباشر بعد الثورة الصناعية، ومن أهم ما نتج عن هذا التطور التكنولوجي ظهور نظام المعلوماتية، و المتمثل في اختراع جهاز الإعلام الآلي الذي ساهم بشكل كبير و تدريجي في تطوير الجانب الاقتصادي بالدرجة الأولى ثم انتقل إلى باقي الجوانب الإدارية و الاجتماعية... الخ، لكن كل هذه التكنولوجيا المعلوماتية صاحبها للأسف مظاهر سلبية تمثلت أساسا في ظهور الجريمة المعلوماتية التي تسببت في خلق مشاكل كبيرة على مستوى الفرد و المجموعة، حيث انتهكت فيها حقوق الإنسان و حرياته من خلال المس بخصوصيات الأشخاص و التعدي على أعراضهم و ممتلكاتهم بالقذف أحيانا و التشهير أحيانا أخرى، و تعدى الأمر إلى المس بأمن القومي للبلد و نشر الأفكار السلبية وسط الشباب و تشجيعهم على اعتناق أفكار متطرفة تمس بالنظام العام و تحثهم على الانضمام الى جماعات متطرفة و قتلهم و تخريبهم أو طأنهم باسم الثورات الربيع العربي و التي مقصدها في الظاهر هو تحسين الإطار المعيشي لكن في الواقع هو تخريب الدول و تمكين المستعمر الجديد باسم الديمقراطية من احتلال الدول و نزع ثرواتها الطبيعية و بقاء شعوب هاته الدول في تخلف و فقر دائمين.

إن هذا النوع من الجرائم المعلوماتية قد بات يشكل خطرا رهيبا خاصة و أنها أصبحت تتم إما ضد الأشخاص أو ضد الأموال أو حتى ضد الحكومات، فهي جرائم عابرة للحدود و أحيانا هي جرائم معلوماتية هدفها زعزعة استقرار البلدان و الأوطان، كما أنا مموليها و منفذيها يتخذون أسماء و ألقاب مستعارة هدفهم إثارة الفتن و زرع البلبلة و الفوضى، خاصة بعد شيوع استعمال التواصل الإلكتروني المعلوماتي تحت ما بات يعرف بوسائل التواصل الاجتماعي و التي تتخذ من العولمة المعلوماتية و شيوع استعمالها مبدأ أساسيا تنطلق منه جل سمومها و أعمالها، فذاع و شاع استعمال

شبكات التواصل الاجتماعي من الفايسبوك و التويتر و استغرام..الخ، و أصبحت مجالات خصبة للتشهير أحيانا و التهديد أحيانا أخرى و الابتزاز في مرات عديدة، و هذا ما أدى إلى تكثيف الجهود الوطنية و الدولية للحيلولة دون انتشار هذه الجرائم المعلوماتية، و محاولة ردع مرتكبيها من خلال إبرام الاتفاقيات الدولية و إصدار التشريعات الوطنية و هذا أيضا ما ذهب إليه المشرع الجزائري.

كما صاحب هذا التقدم السريع في مجال المعلوماتية والتقنية واستخداماتها لخير البشرية؛ تقدم آخر مواز في مجال الجريمة المعلوماتية، فلم تصبح الجريمة مقصورة على طبقة معينة من طبقات المجتمع دون أخرى، وذلك لوضوح إجرام الفساد الذي يتورط فيه كبار المسؤولين في الدول المختلفة، علاوة على إجرام ذوي الطبقات المهمة، والذي يتورط فيه كبار المسؤولين في الشركات العملاقة، والجرائم المرتبطة بالمخدرات.

فضلا عن أنه جعل من المعلومات في متناول الجميع من خلال شبكات الإنترنت، أي شبكات المعلومات المحلية والإقليمية والعالمية، وأصبح العالم بذلك مدخرا بكم هائل من المعلومات لا تعرف الحواجز الجغرافية ولا المسافات، و بصورة يمكن معها القول بأن العالم صار أشبه بمجتمع كبير تترايط فيه الحاسبات و شبكات المعلومات، لتعلن بزوغ فجر ثورة جديدة هي الثورة المعلوماتية أو الثورة الصناعية الثالثة التي تدفع بالإنسانية إلى عصر جديد هو عصر أو مجتمع المعلومات.

و سنحاول في هذه المداخلة تعريف المعلوماتية أولا ذلك أنه لا يمكن التطرق للجريمة المعلوماتية دون معرفة المعلوماتية في حد ذاتها، ثم سيتم تعريف الجريمة المعلوماتية و توضيح خصائصها و أنواعها مع تحديد أساليب وسائل مكافحتها.

الفقرة الأولى: ماهية الجريمة المعلوماتية

إن ظهور المعلوماتية و تطبيقاتها المتعددة أدى إلى بروز مشاكل قانونية جديدة في نطاق القانون الجنائي يفرض حلها البحث في الأوضاع القانونية القائمة و مدى ملاءمتها لمواجهة هذه المشاكل، و أمام هذه المشاكل الجديدة للإجرام المعلوماتي لا يبدو القانون الجنائي التقليدي على حالته الراهنة كافيا أو فعالا بالدرجة المطلوبة، فنصوصه و النظريات و المبادئ القانونية التي يتضمنها موروثة من القرن التاسع عشر، حيث لم يكن ثمة فنيون وقتئذ، وتطبيق بعضها على الأشكال الجديدة للجرائم المعلوماتية التي تستعير من تقنيات الحاسبات و المعلومات أهم وسائلها الإجرامية، سننتقل لتعريف الجريمة المعلوماتية.

أولاً: تعريف الجريمة المعلوماتية

انقسم الفقهاء حيال تعريف الجرائم المعلوماتية الى قسمين: قسم وسع من مفهوم هذه الجرائم ليشمل كل فعل نشأ عن الاستخدام غير المشروع للتقنيات الالكترونية¹ سواء كان هدفه الاعتداء على الأموال المادية أو المعنوية، أو هدف آخر غير مشروع، وآخر ضيق في مفهومها ليقصره على الأفعال غير المشروعة الموجهة للمال الالكتروني².

فقد عرفت الجريمة المعلوماتية على أنها: "كل سلوك غير مشروع يرتكب باستخدام الحاسب، كما عرفت على أنها: كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية بهدف الاعتداء على الأموال المادية أو المعنوية".³

وواضح من التعريف الأول أنه أدخل في مفهوم الجريمة المعلوماتية كل التصرفات غير المشروعة التي لها علاقة بالحاسوب، أي كانت هاته العلاقة، وأي كان دور الحاسوب فيها، سواء أكان وسيلة أو موضوعاً لها، أما التعريف الثاني فقد حصرها في تلك الجرائم التي تستهدف الأموال المادية أو المعنوية.

وهناك من عرفها مع تضيق في مفهومها فقد نص على أنها: "تلك الأفعال غير المشروعة الموجهة ضد الأموال المعلوماتية، كما عرفت على أنها تلك الأفعال غير المشروعة التي تحوي بصفة حصرية: الغش المعلوماتي، التزوير المعلوماتي، المساس بالمعطيات أو البرامج، العرقلة، إعادة نسخ البرامج".

¹ - إبراهيم بلبالي، الجريمة الالكترونية بين وضوح معالم وأهداف التجريم وصعوبة التصنيف والتطبيق مداخل في الملتقى الدولي حول التنظيم القانوني للإنترنت و الجريمة الالكترونية المنعقد يومي 27 و 28 أبريل 2009، كلية الحقوق و العلوم السياسية جامعة الجلفة، ص 03.

² - سهر لطفى، تقرير حول ندوة الجرائم الاقتصادية المستحدثة المنعقدة في: 20-21/04/2001 مجلة حق المؤلف بين الواقع والقانون، مركز الدراسات القانونية، جامعة القاهرة، دار النشر هاني، 1990، ص، 129، نقلاً عن: قارة أمال: الجريمة المعلوماتية، مذكرة مقدمة لنيل درجة الماجستير كلية الحقوق بن عكنون جامعة الجزائر، 2001/2002 ص 17.

³ - إبراهيم بلبالي، المرجع السابق. ص 03.

فهذان التعريفان وما يحذو حذوهما يخرجان من دائرة الجرائم المعلوماتية تلك الأفعال غير المشروعة التي لا يكون أحد العناصر المبينة في التعريف الثاني موضوعا لها، مما أطلق عليه في التعريف الأول منهما اسم الأموال المعلوماتية.

ويقصد بالجريمة المعلوماتية أيضا كل سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة إجرامية محله معطيات الحاسوب، فالسلوك يشمل الفعل الإيجابي والامتناع عن الفعل، وهذا السلوك غير مشروع باعتبار المشروعية تنفي عن الفعل الصفة الإجرامية، ومعاقب عليه قانونا، لأن إسباغ الصفة الإجرامية لا يتحقق في ميدان القانون الجنائي إلا بإرادة المشرع، ومن خلال النص على ذلك حتى ولو كان السلوك مخالفا للأخلاق.¹

وهو ما ذهب إليه خبراء متخصصون من بلجيكا بقولهم أن جريمة الكمبيوتر هي: "ل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية".²

بينما ذهب رأي آخر إلى أنها: "كل فعل أو امتناع عمدي ينشأ عن نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة في الحاسب، أو التي تحوّل عن طريقه"³، أو "نّها سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها".⁴

¹ - حكيم سياب، السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية، كلية الحقوق جامعة سكيكدة. مداخلة في الملتقى الدولي حول التنظيم القانوني للإنترنت و الجريمة الالكترونية المنعقد يومي 27 و 28 أبريل 2009، كلية الحقوق و العلوم السياسية جامعة الجلفة. ص 05

² - عفيفي كامل عفيفي. "جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة"، منشورات الحلبي الحقوقية، بيروت، 2003، ص 32.

³ - يونس عرب. "موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والإنترنت، الجزء الأول، الطبعة الأولى"، منشورات إتحاد المصارف العربية، القاهرة، 2001، ص 213.

⁴ - أنظر ذلك: الدكتور علي عبد القادر القهوجي. "الحماية الجنائية لبرامج الحاسب"، بحث منشور بمجلة الحقوق للبحوث القانونية والاقتصادية، التي تصدرها كلية الحقوق، جامعة الإسكندرية، العدد 24، الصادر عام 1992، ص 172.

في حين أن منظمة التعاون الاقتصادي والتنمية OCDE وضعت التعريف التالي للجريمة المعلوماتية، هي: "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية".¹

و نحن نميل إلى التوسع في مفهوم الجرائم المعلوماتية لتشمل كل تلك الجرائم التي إما يكون الهدف فيها الكمبيوتر، أو يستعمل فيها فقط كوسيلة مسهلة، و لقد سمى قانون العقوبات الجزائري في تعديله بالقانون رقم 04-15 ما يطلق عليه المفهوم الضيق للجرائم المعلوماتية سماه بالمساس بأنظمة المعالجة الآلية للمعطيات²، كما إن القانون الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها الذي اعتمدته مجلس وزراء العدل العرب في دورته التاسعة عشرة، بالقرار رقم 495-د19 - 2003/10/8، واعتمدته مجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم 417- د 2004/21، وسع من مفهوم الجرائم الالكترونية لتشمل تلك الجرائم التقليدية المرتكبة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها، وخصوصاً تلك الجرائم الخطيرة التي تمس أمن الدولة، أو المؤسسات العسكرية أو الاقتصادية بها، أو تلك الجرائم الإرهابية، أو الاتجار بالجنس البشري أو المخدرات.³

ثانياً: خصائص الجريمة المعلوماتية

تتصف الجريمة المعلوماتية بمجموعة من الخصائص تميزها عن غيرها من الجرائم التقليدية، باعتبارها جريمة تتصف بالتكنولوجية التقنية الرقمية، وهي مرتبطة بالتبادل و التواصل المعلوماتي، أي كونها مرتبطة بتكنولوجيات المعلوماتية التي ظهرت في القرن الحالي، في سياق الجريمة وظروف ارتكابها باستخدام الحاسوب ومن خلال شبكة الإنترنت، حدد بعض الخبراء أن لأفعالها خصائص متفردة، لا تتوافر في أي من أفعال الجرائم التقليدية، لا في أسلوبها ولا في طريقة ارتكابها ولا وسيلة ارتكابها، والتي نوجزها في الآتي:

¹ - هشام محمد فريد رستم. "قانون العقوبات ومخاطر تقنية المعلومات"، مكتبة الآلات الحديثة، أسبوط، مصر، 1994، ص 34.

² - الأمانة العامة لرئاسة الحكومة: الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية العدد 71 لسنة 2004 الصادرة بتاريخ 10 نوفمبر 2004م ص 11.

³ - إبراهيم بلبالي، المرجع السابق. ص 04.

1-الحاسوب هو أداة ارتكاب الجرائم المعلوماتية: حيث أن كافة الجرائم المعلوماتية -يكون الحاسب الآلي هو الأداة لارتكابها، فلا يمكن تسمية هذه جريمة أو وصفها بجريمة معلوماتية دون استخدام الحاسوب، لأنه هو وسيلة الإجرام في هذا الصنف، وبالتالي وسيلة تنفيذ الجريمة أيا كان نوعها.

2-الجرائم ترتكب عبر شبكة الإنترنت: حيث تعد شبكة الإنترنت في معظم الجرائم المعلوماتية¹، هي حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم، كالبنوك والشركات الصناعية وغيرها من الأهداف، التي ما تكون غالبا الضحية لتلك الجرائم، وهو ما دعا معظم تلك الأهداف إلى اللجوء إلى نظم الأمن المعلوماتية، في محاولة منها لحماية نفسها من تلك الجرائم، أو على الأقل لتحد من خسائرها عند وقوعها ضحية لها.²

3-الجريمة المعلوماتية لا حدود جغرافية لها: حيث أن شبكة الإنترنت ألغت أي حدود جغرافية فيما بين الدول، فيمكن التحدث بين أشخاص ليس في بلدان مختلفة، وإنما في قارات مختلفة وفي نفس الوقت على شبكة من خلال الدردشة، وعليه فإن أي جرائم ترتكب عبر شبكة الإنترنت فإنها تتخطى حدود الدولة التي ارتكبت فيها لتتعدى أثارها كافة البلدان على مستوى العالم، بالإضافة إلى خصائص أخرى وهي:

أ-سهولة ارتكاب الجريمة ذات الطابع التقني كلما زادت درجة التقنية، وصعوبة كشفها لقدرة الجاني على تدمير الأدلة المتعلقة بها في وقت قصير.

ب-صعوبة كشفها نظرا لإمكانية ارتكابها من مسافات بعيدة وفي نطاق دولي واسع مما يثير مشكلة القانون الواجب التطبيق في حالة كشفها.

ت-تحتاج إلى خبرة فنية عالية المستوى حتى يسهل الوصول إلى تلك الجرائم ومعرفة كل عناصرها وكل ما يتعلق بها.

¹ - نشير هنا إلى أنه يوجد بعض أنواع جرائم المعلوماتية التي لا تستخدم فيها شبكة الإنترنت، مثال ذلك سرقة موظف ما مرخص له باستعمال حاسوب مؤسسة ما لبيانات موجودة على ذلك الجهاز، إذ لا حاجة في هذه الحالة إلى شبة الإنترنت.

² - حكيم سياب، السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية، المرجع السابق.

ث-قد تتعدد إغراض الجريمة المعلوماتية من جوسسة، إلى تدمير المعلومات و البيانات... الخ.¹
د-لا تشمل الجريمة المعلوماتية جرما واحدا، بل هناك أنواع كثيرة من هذه الجرائم (ضد الأشخاص،
ضد الأموال... الخ)²
و-قد تكون الجريمة المعلوماتية في حد ذاتها أداة أو عملية يتم من خلالها الإعداد أو القيام بالكثير
من الجرائم التقليدية.
ي-إحجام العديد من الشركات عن الإبلاغ عن الجرائم المعلوماتية لتي تقع عليها حفاظا على
سمعتها ومكانتها الاقتصادية.

ثالثا: مبدأ الشرعية والجريمة المعلوماتية

ويعني هذا المبدأ أنه لا جريمة ولا عقوبة إلا بنص قانوني، كما نصت على ذلك المادة الأولى من
قانون العقوبات الجزائري³، أي أن مصدر الصفة غير المشروعة للفعل هو نص القانون، ويقال لهذا
النص "نص التجريم"، وبالتالي فإن القاضي لا يستطيع أن يسبغ الصفة الإجرامية على فعل ما لم يجد
سندا لذلك التجريم في قانون العقوبات والقوانين المكملة له، فإذا لم يجد لا يمكنه إضفاء صفة الجريمة
عليه قياسا على فعل آخر يشبهه ولو بلغ من الخطورة ما بلغ.
ومن الانتقادات التي وجهت لهذا المبدأ أنه لا يحقق حماية كافية للمجتمع، في مواجهة أفعال قد
تكون بالغة الخطورة في ذاتها، دون أن يرد نص مكتوب بتجريمها، ففي مثل هذه الحالات يجب على
القاضي أن يحكم بالبراءة لعدم تجريم الفعل مهما كانت خطورته الاجتماعية أو الأخلاقية، وتزيد
أهمية هذا النقد عندما نلاحظ أن المشرع لا يستطيع أن يحصر مسبقا كل ما يصلح من الأفعال محلا
للتجريم، وأن تطور الحياة وتقدم وسائل التقنية الحديثة ومهارة بعض الأفراد في إساءة استخدامها

¹ - نبيل صقر، جرائم الكمبيوتر و الانترنت في التشريع الجزائري، دار الهلال للخدمات الإعلامية، (د. ط)،
2005، ص 121

² -عمر دمانة، مفهوم الجريمة الإلكترونية و أساليب مكافحتها في ظل التشريع الجزائري، جامعة عمار ثليجي،
الأغواط مداخلة في الملتقى الدولي حول التنظيم القانوني للأنترنت و الجريمة الالكترونية المنعقد يومي 27 و 28 أبريل
2009، كلية الحقوق و العلوم السياسية جامعة الجلفة.

³ - لا جريمة ولا عقوبة أو تدابير أمن بغير قانون قانون العقوبات الجزائري.

يخلق كل يوم مخاطر جديدة وأفعال ضارة بالمجتمع ومنافية للأخلاق يضمن مبدأ الشرعية لمرتكبيها الإفلات من العقاب لمجرد أن المشرع قد أغفل النص على تجريمها.¹ وعليه فإن الجرائم المعلوماتية في الدول التي لم تسن لها قوانين خاصة يجد مرتكبوها إفلاتاً من العقاب بسبب عدم النص عليها، وحتى الدول التي سنت لها قوانين فإنه نظراً لطبيعة هذه الجرائم المتكاثرة والمسرعة في التطور تبعاً لتطور التقنيات الالكترونية تواجه فيها تلك الجرائم الإلكترونية غير المشمولة في القانون صعوبة في تطبيقها.

الفقرة الثانية: أنواع وأشكال الجريمة المعلوماتية وطبيعتها.

سنستطرق في هاته الفقرة الى انواع و أشكال الجريمة المعلوماتية، ثم الى طبيعتها

1-أنواع و أشكال الجريمة المعلوماتية

من الصعوبة تماماً حصر أنواع الجريمة المعلوماتية، حيث أن أشكالها متعددة، وهي تزداد تنوعاً وتعداداً كلما أوغل العالم في استخدام الحاسب الآلي وشبكة الإنترنت²، فمن المعروف أن أكثر تلك الجرائم يكون من ضمن أهدافها الأساسية الحصول على المعلومات الإلكترونية، التي تكون إما محفوظة على أجهزة الحاسبات الآلية وإما منقولة عبر شبكة الإنترنت، وأخرى يكون هدفها هو الاستيلاء على الأموال، وثالثة تستهدف الأفراد أو الجهات بعينها، وأخيراً جهاز الحاسب الآلي كهدف لها نلخصها فيما يلي:

أ-المعلومات: ثمة العديد من الجرائم التي ترتكب بهدف يتعلق بالمعلومات، ويتمثل هذا الهدف بالحصول على المعلومات أو تغييرها أو حذفها نهائياً، هذا حسب درجة أهمية الهدف (المعلومات)، فمعظم تلك الجرائم التي يكون الهدف منها المعلومات هي في الأغلب الأعم الجرائم الاقتصادية، وتكون بغرض الحصول على مزايا، أو مكاسب اقتصادية، فالحرب الاقتصادية لا تقل في ضراوتها وشدتها حالياً عن الحرب العسكرية، إلا أنها تتم باستخدام الحاسب الآلي وعبر شبكة الإنترنت.

¹ - إبراهيم بلبالي، المرجع السابق، ص 05.

² - جميل عبد الباقي الصغير. "القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي"، الطبعة الأولى، دار النهضة العربية، القاهرة، 1992
حكيم سياب، السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية، المرجع السابق، ص 10.

ب-**الاستيلاء على الأموال:** تستهدف أكثر تلك الجرائم تحديدا عناصر الذمة المالية، ويكون الطمع وراء ارتكابها، والحصول والاستيلاء على تلك الأموال، وفكرة المكسب السريع التي تحرك مرتكبيها، وقد ترتكب أحيانا لمجرد قهر نظام منشأة (مؤسسة) مثلا، وتخطى حواجز الحماية، أو بدافع الانتقام من صاحب تلك المنشأة أو أحد عناصرها.

ت-**الأشخاص أو الجهات:** معظم الجرائم التي ترتكب في مجال المعلوماتية تستهدف إما أشخاص وإما جهات بعينها، وغالبا ما تكون تلك الجرائم هي جرائم مباشرة، ترتكب في صورة ابتزاز أو تهديد أو تشهير، أو هي جرائم غير مباشرة ترتكب في صورة الحصول على البيانات، أو المعلومات الخاصة بتلك الجهات أو الأشخاص، وذلك لاستخدام تلك المعلومات والبيانات بعد ذلك في ارتكاب جرائم مباشرة.

ث-**أجهزة الحاسب الآلي:** وعندما يكون الهدف من ارتكاب تلك الجرائم هو أجهزة الحاسب الآلي، فالغالب يكون الهدف هو تخريب أنظمة تلك الأجهزة نهائيا، أو على الأقل تعطيلها لأطول فترة ممكنة، ومعظم تلك الجرائم تتم بواسطة استخدام الفيروسات.

2-**الطبيعة القانونية لجرائم المعلوماتية:**

هي من الجرائم المستحدثة نتيجة التطور الهائل في مجال التقنية العالية، فهي جرائم تكتنفها صعوبات ترجع لطبيعتها الخاصة، وهذا لأنها جرائم تطال المعلومات التي أختلفت القفه في تحديد مفهومها وطبيعتها ولأنها محور هذه الجرائم سميت جرائم المعلوماتية، وتقول الدكتورة هدى قشقوش كمحاولة لتحديد الطبيعة الخاصة لجرائم المعلوماتية "يجب أن نعترف أننا بصدد ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي، ففي معظم حالات ارتكاب الجريمة ندخل في مجال المعالجة الإلكترونية للبيانات"¹، وحول الوضع القانوني للمعلومات وهل يمكن اعتبارها قيمة قابلة للاستثمار وتصبح محلا للاعتداءات فإن للفقهاء اتجاهين:

أ-**الاتجاه الأول:** المعلوماتية لها طبيعة من نوع خاص: يرى الفقهاء التقليدي أن للمعلومات طبيعة خاصة، فهي تتمتع بحماية قانونية لاعتراف الفقهاء والقضاء بوجود اعتداء يجب قاب عليه عند الاستلاء غير المشروع على معلومات الغير، وقد انتهى الفقهاء إلى وجود حق ذو طبيعة خاصة على

¹ - محمود احمد عبانة - محمد معمر الرازي - جرائم الحاسوب وأبعادها الدولية - دار الثقافة للنشر والتوزيع

المعلومات المستولى عليها إذ الأصل ان الاشياء القابلة للاستحواذ والممكن الاستئثار بها هي التي يكون لها قيمة مادية.¹

ب- الاتجاه الثاني: المعلومات مجموعة مستحدثة من القيم: يرى الفقه الحديث ان المعلومات عبارة عن مجموعة من القيم المستحدثة ويرجع الفضل في ذلك للأستاذين: catala و Vivant²، وهذا لان التطور العلمي والتكنولوجي يقتضي حماية قانونية للمعلومات التي تطورها اضفي عليها قيمة اقتصادية متمثلة في قيمتها التجارية التي جعلتها سلعة تباع وتشترى مثل بنوك المعلومات والمعلومات المتبادلة بين الشركات.³

ج- جرائم المعلوماتية جرائم اموال: من الجرائم التي يستخدم فيها الحاسب الالي في الجريمة المعلوماتية، تزيف العملة التزوير في محركات رسمية الاختلاس والدخول غير المشروع للبيانات والمعلومات المخزنة على الحاسب او الجرائم الواقعة على الحاسب الالي بمشتملاته المادية والمعنوية في الحالتين هي جرائم اموال لان موضعها دائما مال.⁴

د- جرائم المعلوماتية جرائم و أشخاص: يستخدم الحاسب الالي في الجريمة المعلوماتية في ارتكاب جرائم يكون محلها الشخص مثل جرائم الدم والقدح والتحقيق وجرائم افشاء الاسرار التجارية او الشخصية وجرائم التهديد والابتزاز.

و- جرائم المعلوماتية جرائم امن وجرائم مخلة بالثقة العامة والآداب العامة⁵: حيث أن جرائم امن الدولة تنقسم الى قسمين: جرائم تمس امن الدولة الخارجي من تجسس واتصال مع العدو لأغراض غير مشروعة واخرى تمس امن الدولة الداخلي من اثاره للفتن والمساس بالوحدة الوطنية وهناك جرائم تمس الثقة العامة والآداب العامة مثل نشر صور اباحية او اقتنائها بقصد توزيعها

1 - أحمد خليفة الملط - الجرائم المعلوماتية - دار الفكر الجامعي 2006، ص 106

2 - محمد على العريان-الجرائم المعلوماتية -دار الجامعة الجديدة للنشر 2004، ص 50

3 - د/ احمد خليفة الملط - المرجع السابق ص 109

4 - أسامة احمد المناعسة -جلال محمد الزغبى-جرائم الحاسب الآلي والانترنت دراسة تحليلية مقارنة -دار وائل

للنشر والتوزيع 2001

5 - أسامة أحمد المناعسة، جلال محمد الزغبى، المرجع السابق، ص 99

ي- جرائم المعلوماتية جرائم اقتصادية: لأنها جرائم تخالف السياسة الاقتصادية القائمة على دعم الثقة والائتمان ومنها تزوير البنكوت والأوراق المالية وتزييف العملات المتداولة فتلحق الضرر بالمركز الاقتصادي للدولة.

الفقرة الثالثة: أنواع الجريمة المعلوماتية و اصنافها.

لم يعد الحاسب الالى مجرد وسيلة للبحث والاستفادة بل اصبح ايضا اداة لارتكاب جرائم تختلف باختلاف محلها والمتمثلة في:

أولاً:-الجرائم الواقعة على النظام المعلوماتي¹

و تتمثل هاته الجرائم في:

1-الاعتداء على المكونات المادية لنظام المعلوماتي: ويتم الاعتداء على الاجهزة والمعدات الملحقة بها من اسطوانات وشرائط ممغطة وكابلات..... فتكون محلا للسرقة او الاتلاف العمدي.

2 / الاعتداء على المكونات المنطقية (البرامج) للنظام المعلوماتي:

أ -الجرائم الواقعة على البرامج التطبيقية: نسبتها تقدر بحوالي 15% من مجموع حالات الجرائم المعلوماتية والغالب فيها قيام المجرم المعلوماتي بتعديل البرنامج والتلاعب فيه للحصول على اكبر استفادة مالية

ب -الجرائم الواقعة على برامج التشغيل:هي البرامج المسؤولة عن عمل النظام المعلوماتي ومن الجرائم الواقعة عليها المصيدة والمتمثلة في تضمين اي برنامج عند اعداده من طرف المبرمجين اخطاء وعيوب تشكل ممرات و فواصل تمكن من احداث التعديلات والولوج لداخل البرنامج و جريمة اضافة او تصميم برنامج وهمي من طرف المبرمجين من خلال برنامج تشغيل النظام المعلوماتي².

3 / الاعتداء على المعلومات المدرجة بالنظام المعلوماتي:

أ / جريمة التلاعب في المعلومات بطريقة مباشرة: هي ادخال معلومات بمعرفة المسؤول عن القسم المعلوماتي المسندة اليه وظيفة المحاسبة والمعاملات المالية ويتم بعدة صور: ضم مستخدمين غير موجودين بالعمل، اختلاس النقود.....

¹ - أ.د فتوح الشاذلي، عفيفي كامل عفيفي، المرجع السابق، ص 38 و ما بعدها.

² - محمد علي العويان، المرجع السابق، ص 79

- جريمة التلاعب بطريقة غير مباشرة: في المعلومات على مستوى الشرائط المغنطة فيتم التلاعب عن بعد باستخدام الجاني لكلمة السر او مفتاح الشفرة..... للحصول على المال
ب / جريمة اتلاف المعلومات : لما تشكله المعلومات المخزنة بالنظام المعلوماتي من اهمية للجنة فهم يقومون بمحاولة الاستلاء عليها بواسطة استبدالها بالتزوير او بمحو المعلومات المتعلقة بالجريمة.¹
ثانيا - الجرائم الواقعة باستخدام النظام المعلوماتي:

1 / الجرائم الواقعة على الاشخاص الطبيعية:

أ - الجرائم الواقعة على حقوق الملكية الفكرية :

تتمثل في السطو على بنوك المعلومات الموجودة في برامج نظام معلوماتي اخر او تخزين هذه المعلومات على نظام معلوماتي معين ثم يستخدمها من خزنها او يفرط فيها دون اذن صاحبها وهذا يتضمن انتهاك مزدوج لحقوق هذا الشخص فهو من جهة اعتداء على القيم المالية للمعلومة ومن ناحية اخرى اعتداء على حقوقه المعنوية لما للمعلومات من قيمة ادبية ومالية

ب - الجرائم التي تمس بالأخلاق وسمعة الاشخاص:

قامت شبكة الانترنت بتحديد مواقع اباحية تقوم بعرض صور وفيديو لمناظر غير اخلاقية لافساد الاخلاق والمبادئ الدينية فهي مشكلة عالمية تحاول الدول مقاومتها والحد من اثارها² اضافة للمواقع المستخدمة للمساس برموز الشعوب سواء كانت فكرية او سياسية او دينية فتشوه سمعة الاشخاص للحصول على ما لهم

ج - الجرائم الواقعة على حرمة الحياة الخاصة:

تتم بقيام شخص يعمل في النظام المعلوماتي باعداد ملف لشخص اخر بدون علمه او اذنه ويمكن ان يحوي هذا النظام اسراره المكتوبة وسيرته الذاتية الا انه يمكن ان تحترق هذه المعلومات من طرف اجهزة اخرى فيتم الاطلاع عليها
الخاتمة:

إن ظاهرة الجرائم المعلوماتية، ظاهرة إجرامية مستجدة نسبياً؛ تفرع في جنباتها أجراس الخطر لثبته مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عنها، باعتبارها تستهدف الاعتداء

¹ - أحمد خليفة الملط، المرجع السابق، ص 181.

² منير محمد الجهيني، ممدوح محمد الجهيني، المرجع السابق، ص 30.

على المعطيات بدلالاتها التقنية الواسعة، (بيانات، معلومات، برامج بكافة أنواعها)، فهي جريمة تقنية تنشأ في الخفاء يقتربها مجرمون أذكاء يمتلكون أدوات المعرفة التقنية، توجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسوب، وهذا وحده -عبر دلالاته العامة- يظهر مدى خطورة الجرائم المعلوماتية، فهي تطال الحق في المعلومات، وتمس الحياة الخاصة للأفراد وتحدد الأمن القومي، والسيادة الوطنية وتشيع فقدان الثقة بالتقنية، وتحدد إبداع العقل البشري.

إن الجرائم المعلوماتية من أخطر الجرائم، فالشخص الذي يرتكبها هو مجرم غير تقليدي له مميزاته الخاصة، وهي جرائم يصعب اكتشافها وإذا ما اكتشفت يصعب إثباتها، وما يزيد من خطورة هذه الجرائم أن للضحية دور مهم فيها، وأنها جرائم ناغمة شديدة الإغراء للمجرمين وأنها جرائم عابرة للحدود وجرائم فادحة الأضرار.

هذا الأمر جعل المشرع الجزائري يتصدى لمحاربة هذه الجرائم، إذ نص عليها في قانون العقوبات إثر تعديل سنة 2004، وقد صنفها إلى ثلاثة أنواع: جريمة الدخول أو البقاء غير المصرح بهما وجريمة التلاعب بالمعطيات وجريمة التعامل في معطيات غير مشروعة، ورغبة من المشرع الجنائي في حماية أكبر للمعطيات ومنها ما يتعلق بقطاع البنوك فقد جرم الاتفاق الجنائي على ارتكاب إحدى الجرائم السابقة إذا تجسد بأعمال مادية، كما جرم الشروع في تلك الجرائم كما فرض عقوبات تكميلية عليها، وشدد من عقوبة الشخص المعنوي الذي يرتكبها، كما شدد العقوبة إذا طال هذا الاعتداء الجهات العامة في الدولة.

لقد أدى التطور التكنولوجي إلى ظهور المعلوماتية التي هي عبارة عن مال معنوي، ذو قيمة مالية و اقتصادية كبيرة تخضع للسرية والانتشار والاستثمار، وقد قامت هذه الثورة المعلوماتية بتحطيم كل الحدود الجغرافية والسياسية عن طريق الأنترنت فجعلت العالم عبارة عن قرية صغيرة و إلى جانب هذا فقد جلبت المعلوماتية جرائم تحولت إلى ظاهرة عالمية يصعب التحقق منها والحكم عليها، فمن الصعب التنبؤ بهذه الجرائم أو محاكمة منفذيها بسبب عدم توفر أدلة مادية لها في الغالب أو شهود ضد مرتكبيها، وتقنيات الأنظمة المعلوماتية في تطور كبير ومستمر و جرائمها ترتكب من قبل الباحثين عن الثراء أو من مؤسسات تبحث عن معلومات وأخبار أو من حكومات غايتها المعلومات الاقتصادية والسياسية، فهذه الجرائم قد يكون النظام المعلوماتي طرفا فيها أو هدفا لتنفيذها و لما هذه الجريمة المستحدثة من طبيعة خاصة فهي تثير صعوبات قانونية في تطبيق النصوص

الجنائية التقليدية مثل قواعد الاجراءات الجنائية في التحقيقات الخاصة باستنباط الأدلة و الإثبات فيها، وكذلك صعوبة تكييف طبيعة المال المعلوماتي و ملكيته.....

و من خلال النتائج السابقة و التي أظهرتها الدراسة نلخص لبعض التوصيات للإسهام في إثراء الفكر الجنائي المعلوماتي و حقول البحث العلمي و هي تتمثل في:

أولاً: ضرورة تخلي المشرع العقابي عن حرفية النص الجنائي التقليدي، و تبني مفهوم أشمل للمال و المنقول ليشمل الأموال المعلوماتية المعنوية و هذا بإصدار قوانين تشمل هذه الأموال غير المحمية و التي أصبحت تشكل نواة المجتمع الإلكتروني الحديث

ثانياً: ضرورة تحديث نصوص قانون العقوبات لمواجهة ظاهرة الإجرام المعلوماتي، حيث تعرف الجريمة المعلوماتية على نحو واسع و تحدد عقوبتها.

ثالثاً: ضرورة استهلال نصوص قانون العقوبات بنص يجرم و يعاقب على فعل الدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه بدون إذن سواء نجم عنه ضرر أم لا

رابعاً: ضرورة التنسيق الدولي المتكامل لحل مشكلات الاختصاص القانوني و القضائي التي تثيرها جرائم الأنترنت العابرة للحدود

خامساً: وضع اتفاقيات دولية تكون مصدر أساسي للتشريعات الجنائية الداخلية فتستمد منها ضوابط نصوصها التجريبية لتحقيق تنظيم جنائي شامل

سادساً: ضرورة تدريب و تأهيل أفراد الضابطة العدلية العاملين في الإدعاء العام و القضاء على كيفية التعامل مع هذا النوع من الجرائم.

المراجع:

- أسامة احمد المناعسة -جلال محمد الزغي-جرائم الحاسب الآلي والانترنت دراسة تحليلية مقارنة -دار وائل للنشر والتوزيع 2001.
- أحمد خليفة الملط - الجرائم المعلوماتية -دار الفكر الجامعي 2006.
- إبراهيم بلبالي، الجريمة الالكترونية بين وضوح معالم وأهداف التجريم وصعوبة التصنيف والتطبيق، مداخلة في الملتقى الدولي حول التنظيم القانوني للأنترنت و الجريمة الالكترونية المنعقد يومي 27 و 28 أبريل 2009، كلية الحقوق و العلوم السياسية جامعة الجلفة.

- حكيم سياب، السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية، كلية الحقوق جامعة سكيكدة. مداخلة في الملتقى الدولي حول التنظيم القانوني للإنترنت و الجريمة الالكترونية المنعقد يومي 27 و 28 أبريل 2009، كلية الحقوق و العلوم السياسية جامعة الجلفة.
- جميل عبد الباقي الصغير. "القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي"، الطبعة الأولى، دار النهضة العربية، القاهرة، 1992.
- سهير لطفي، تقرير حول ندوة الجرائم الاقتصادية المستحدثة المنعقدة في 20-21/04/2001 مجلة حق المؤلف بين. الواقع والقانون، مركز الدراسات القانونية، جامعة القاهرة، دار النشر هايتي، 1990.
- قارة أمال: الجريمة المعلوماتية، مذكرة مقدمة لنيل درجة الماجستير كلية الحقوق بن عكنون جامعة الجزائر، 2001/2002.
- عفيفي كامل عفيفي. "جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة"، منشورات الحلبي الحقوقية، بيروت، 2003.
- علي عبد القادر القهوجي، 'الحماية الجنائية لبرامج الحاسب"، بحث منشور بمجلة الحقوق للبحوث القانونية والاقتصادية، التي تصدرها كلية الحقوق، جامعة الإسكندرية، العدد 24، الصادر عام 1992.
- هشام محمد فريد رستم. "قانون العقوبات ومخاطر تقنية المعلومات"، مكتبة الآلات الحديثة، أسيوط، مصر، 1994.
- نبيل صقر، جرائم الكمبيوتر و الانترنت في التشريع الجزائري، دار الهلال للخدمات الإعلامية، (د.ط)، 2005.
- عمر دمانة، مفهوم الجريمة الإلكترونية و أساليب مكافحتها في ظل التشريع الجزائري، جامعة عمار ثليجي، الأغواط مداخلة في الملتقى الدولي حول التنظيم القانوني للإنترنت و الجريمة الالكترونية المنعقد يومي 27 و 28 أبريل 2009، كلية الحقوق و العلوم السياسية جامعة الجلفة.
- محمود احمد عبابنة -محمد معمر الرازي -جرائم الحاسوب وأبعادها الدولية -دار الثقافة للنشر والتوزيع 2005.
- محمد على العريان-الجرائم المعلوماتية -دار الجامعة الجديدة للنشر 2004.

- يونس عرب. "موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والإنترنت، الجزء الأول، الطبعة الأولى"، منشورات إتحاد المصارف العربية، القاهرة، 2001.

- الأمانة العامة لرئاسة الحكومة: الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية العدد 71 لسنة 2004 الصادرة بتاريخ 10 نوفمبر 2004.

خصوصية المجرم المعلوماتي

أ/يرمش مراد

أستاذ مساعد (أ) - كلية الحقوق والعلوم السياسية- جامعة المسيلة

مقدمة:

إن الجريمة المعلوماتية ذات خصائص منفردة خاصة بها لا تتوافر في أي من الجرائم التقليدية في أسلوبها وطريقة ارتكابها، حيث أنه لم يكن لارتباط الجريمة المعلوماتية بالحاسب الآلي أثره على تمييز الجريمة عن غيرها من الجرائم التقليدية فحسب، وإنما له اثره في تمييز المجرم المعلوماتي عن غيره من المجرمين العاديين، فالجرم المعلوماتي تتميز شخصيته بخصائص وتختلف عن مرتكب الجريمة التقليدية، وهذا مرده إلى تميز شخصية المجرم المعلوماتي بالتقدم في مجال إستخدام الحاسب الآلي، لأن محور إرتكاب الجريمة المعلوماتية هو المجرم المعلوماتي، فهو يرتكب الجريمة في حدود مالهديه من قدرات تمكنه من إرتكابها. والإشكالية المطروحة في هذا المقام تكمن في الوقوف على تحديد خصوصية المجرم المعلوماتي في الجريمة المعلوماتية على اعتبار أنها جريمة مستحدثة ظهرت بظهور الشبكة المعلوماتية وماهي خصائص وأصناف المجرم المعلوماتي التي تميزه عن المجرم في الجريمة التقليدية؟ وللإجابة على هذه الإشكالية تم تقسيم الدراسة إلى محورين:

المحور الأول: خصائص المجرم المعلوماتي.

المحور الثاني: أصناف المجرم المعلوماتي

المحور الأول: خصائص المجرم المعلوماتي

تتوافر لدى المجرم المعلوماتي مجموعة من الخصائص والسمات التي تميزه عن المجرم في الجرائم التقليدية، فالجرم المعلوماتي يتمتع بقدر كبير من الذكاء يميزه عن غيره من المجرمين، وإتصافه بسمات معينة جعلت منه محلا من العديد من الأبحاث والدراسات، فقد إختلفت الدراسات في تحديد هذه الخصائص.

سنتطرق في هذا المحور إلى أهم السمات والخصائص التي يتميز بها المجرم المعلوماتي.

أولاً: يتمتع المجرم المعلوماتي بالذكاء والمهارة والمعرفة

المجرم المعلوماتي يتمتع بقدر لا يستهان به من المهارة بتقنيات الحاسب والإنترنت، فبعض مرتكبي الجريمة المعلوماتية من المتخصصين في مجال معالجة المعلومات ألياً، فتنفيذ هذه الجريمة يتطلب قدراً من المهارة لدى الفاعل التي يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة التي إكتسبها في مجال تكنولوجيا المعلومات.¹

فالمجرم المعلوماتي لا يمكن أن ينتمي لفئة المجرمين الأغبياء، فإذا كان من يسرق منزلاً أو من يسرق سيارة يعتبر منخفض الذكاء في كثير من الأحيان، أما من يستعين بالحاسوب في السرقة من أموال بنك أو شركة فإنه يتميز بالمستوى المرتفع الذكاء حتى يمكنه أن يتغلب على كثير من العقبات التي تواجهه في إرتكاب الجريمة.²

فالبعض من الفقه تحفظ حيال رسم صورة عامة للمجرم المعلوماتي متسمة بصفة الذكاء، إستناداً في ذلك أن بعض أنماط الجريمة المعلوماتية مثل إتلاف الحاسب الآلي أو تدميره كلياً أو جزئياً، أو سرقة المعلومات المخزنة داخل الحاسب الآلي، لا تحتاج في مرتكبها أن يكون على قدر كبير من الذكاء.³

ثانياً: يتمتع المجرم المعلوماتي بالقدرة على التكيف الإجتماعي

إن المجرم المعلوماتي لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به، بل أنه إنسان متكيف إجتماعياً، فهو أصلاً مرتفع الذكاء ويساعده على ذلك التكيف، فالذكاء في نظر الكثيرين ماهو سوى القدرة على التكيف، ولا يعني ذلك التقليل من شأن المجرم المعلوماتي، بل إن خطورته الإجرامية قد تزيد إذا زاد تكيفه الإجتماعي مع توافر الشخصية الإجرامية لديه.⁴

وهنا يكمن الاختلاف بين المجرم المعلوماتي والمجرم التقليدي، من حيث أن المجرم المعلوماتي يحيا وسط المجتمع ويمارس عمله في المجال المعلوماتي أو غيره من المجالات الأخرى.

فالمجرم المعلوماتي يتكيف ويتأقلم مع المجتمع الذي ينتمي إليه ويعيش فيه، فهو قبل كل شئ إنسان متكيف إجتماعياً، وهذا ماساعده على التميز بالسمات والصفات السابقة خاصة الذكاء.⁵

ثالثاً: المجرم المعلوماتي يبرر إرتكابه جرمته

يوجد شعور لدى مرتكب الإجرام المعلوماتي أن مايقوم به لا يدخل في عداد الجرائم، أو بمعنى آخر أنه لا يمكن لهذا الفعل أن يتصف بعدم الأخلاقية وخاصة في الحالات التي يقف فيها السلوك عند حد

قهر نظام الحاسوب وتخطي الحماية المفروضة عليه، حيث يميز مرتكبو هذه الجرائم بين الإضرار بالأشخاص، الأمر الذي يعدونه غاية في الأخلاقية وبين الإضرار بمؤسسة أو جهة في إستطاعتها إقتصاديا تحمل نتائج تلاعبهم.⁶

ويبدو أن هؤلاء الأشخاص لا يدركون أن سلوكهم يستحق العقاب، فالإستخدام المتزايد للأنظمة المعلوماتية قد أوجد مناخا نفسيا موائما لتصور إستبعاد فكرة الخير والشر وقد ساهم في ذلك عدم وجود إحتكاك مباشر بالأشخاص، ومالا شك فيه أن هذا الإستبعاد في العلاقة الثنائية بين الفاعل والمجني عليه يسهل المرور إلى الفعل غير المشروع، ويساعد على إيجاد نوع من الإقرار الشرعي الذاتي بمشروعية هذا الفعل.⁷

غير أنه لا يعني عدم الشعور بعدم أخلاقية الأفعال الإجرامية المعلوماتية لدى فئة كبيرة من مرتكبيها ينفي وجود مجرمين يرتكبون الإجرام المعلوماتي وهم على علم وإدراك بعدم مشروعية وأخلاقية هذا الفعل، فهناك فئة لديها إتجاه إجرامي خطير وسوء نية واضح وهم على إدراك بخطورة أفعالهم.⁸

المحور الثاني: أصناف المجرم المعلوماتي

إن التسارع الرهيب والمذهل في مجال التقنيات الرقمية الحديثة وبظهور شبكة الأنترنت و إنتشارها الواسع، ساهم في تغيير وتطوير أنواع الجرائم وأفرز أنماطا مستحدثة من الظواهر الإجرامية حملت معها طائفة جديدة من المجرمين، حيث ان مرتكبو الجريمة المعلوماتية يتميزون بابتكار أساليب ووسائل لخرق الحواجز الأمنية في هذا العالم الرقمي نومن هذا المنطلق سنتطرق إلى أهم الطوائف أو فئات المجرم المعلوماتي.

أولا: فئة صغار السن في الجريمة المعلوماتية

إن هذه الفئة يطلق عليها البعض تسمية صغار نوابغ المعلوماتية، ويصفهم بأنهم الشباب البالغ المفتون بالمعلوماتية والحاسوب، والحقيقة أن من بين أفراد هذه الفئة من هم دون سن الأهلية، وهم مولعون بالحاسوب والإتصالات، وقد تعددت أوصافهم في الدراسات المسحية، وشاع في الدراسات التقنية (المتلعثمين)، ويثير مجرمو المعلوماتية من هذه الفئة جدلا واسعا، حيث يمكن تقسيم الإتجاهات التقديرية لطبيعة هذه الفئة ومدى خطورة أفرادها إلى ثلاثة إتجاهات، هي:⁹

الإتجاه الأول: وهو إتجاه لا يرى إسباغ أي صفة جرمية على هذه الفئة، ولا يرى ضرورة تصنيفهم ضمن الطوائف الإجرامية لمجرمي المعلوماتية، إستنادا أن هؤلاء المتلثمين لديهم ببساطة ميل للمغامرة والتحدي ورغبة في الإكتشاف، إضافة أنهم لا يقدرّون ولا يدركون نتائج أفعالهم التي يقومون بها.

الإتجاه الثاني: هذا الإتجاه يناصر هذه الفئة ويعتبرها ممن تقدم خدمة لأمن المعلومات ووسائل الحماية، ويصف أفرادها بالأخيار وأحيانا بالأبطال الشعبيين، وينسب اصحاب هذا الإتجاه إلى هذه الفئة الفضل في كشف الثغرات الأمنية في تكنولوجيا المعلومات.

الإتجاه الثالث: يرى أصحاب هذا الإتجاه أن مرتكبي الجرائم المعلوماتية من هذه الطائفة، يصنفون ضمن مجرمي المعلوماتية كغيرهم دون تمييز، إستنادا إلى أفعالهم المتمثلة في إتهام الأنظمة وإختراق الحواجز الأمنية في البيئة الإلكترونية تعد أفعالا خطيرة من الناحية العملية، بل أن أفعالهم تتعدى الحواجز الجغرافية ولا تقف عند دولة ما.¹⁰

ثانيا: فئة المخترقون في الجريمة المعلوماتية

هذه الفئة هم قراصنة المعلومات وهم عادة مبرمجون من أصحاب الخبرة، يهدفون إلى الدخول إلى الأنظمة المعلوماتية غير المسموح لهم بالدخول إليها وكسر الحواجز الأمنية المحيطة بهذه الأنظمة، وفي مجال تصنيف القراصنة هناك صنفين هما:

1- القراصنة الهواة (الهاكرز) HACKERS

تضم هذه الطائفة الأشخاص الذين يستهدفون من أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها، كسر الحواجز الأمنية الموضوعة لهذا الغرض، وذلك بهدف إكتساب الخبرة أو بدافع الفضول أو لمجرد إثبات القدرة على إختراق هذه الأنظمة.¹²

فالمقصود بالهاكر من يستخدم الحاسوب وشبكة الأنترنت لاختراق نظم الأمن والشبكات، بغرض الدخول غير المصرح به، ورغم قدرته على الإختراق إلا أنه غير مؤد، فهو لا يقوم بالإختراق بغرض التخريب أو الإيذاء، لأنه يرى أن الأنترنت أو العالم الافتراضي تؤمن له أعنى الأماكن سرية وحصانة بغرض الإطلاع على التقنية، إذ أنه لا يقيم أهمية لحواجز الشفرات وكلمات المرور دون أن يتلف أو يخرب أي شيء.¹³

فهؤلاء القراصنة أو ما يطلق عليهم بالهاكرز يرون في إختراق الأنظمة المعلوماتية تحديا لقدراتهم الذاتية، وهذه الطائفة غالبا ماتكون من هواة الحاسوب، فيقومون بأعمالهم هذه لمجرد إظهار أنهم

قادرين على إقتحام المواقع الأمنية أحيانا أو لمجرد ترك بصماتهم التي تثبت وصولهم إلى تلك المواقع أحيانا أخرى.¹⁴

والسمة المميزة لهذه الفئة هي تبادلهم للمعلومات فيما بينهم وتحديد التشارك في وسائل الاختراق واليات نجاحها، وإطلاع بعضهم البعض على مواطن الضعف في نظم الكمبيوتر والشبكات، حيث تجري عمليات التبادل فيما بينهم وبشكل رئيسي عن طريق النشرات الإعلامية الإلكترونية ومجموعات الأخبار.¹⁵

2- القراصنة الكراكرز CRACKERS

الكراكرز هم أشخاص يقومون بالتسلل إلى نظم المعالجة الآلية للإطلاع على المعلومات المخزنة فيها، لإلحاق الضرر أو العبث بها وسرقتها وذلك بدافع التحدي الإبداعي، تتراوح أعمارهم بين (25-40 عام).¹⁶

فالكراكرز يعبر عن المخترق ذي النوايا الإجرامية، بحيث يقوم بما هو سئ، وما يشكل جريمة كإتلاف أو التخريب أو الإرهاب أو الابتزاز أو العدوان على الأموال بالإحتيال والسرقة وغيرها، فهذا النوع من الإعتداء يعكس ميولا إجرامية، ويكشف عن الرغبة في إحداث التخريب.¹⁷

هذه الفئة تعكس إعتداءاتهم ميولا إجرامية خطيرة تنبئ عن رغبتها في إحداث التخريب، ويتميز أصحاب هاته الفئة بقدراتهم التقنية الواسعة وخبراتهم في مجال أنظمة الحاسوب والشبكات وهم أكثر خطورة، فقد يحدثون أضرارا كبيرة.¹⁸

ثالثا: فئة المحترفون في الجريمة المعلوماتية

تعد هذه الفئة من أخطر الفئات التي ترتكب الجرائم، لأن الهدف الذي تقوم عليه هذه الفئة ينحصر في إرتكاب الفعل الإجرامي وهذا هو مصدر الخطورة لدى هذه الفئة، فهم يرتكبون أنواع الجرائم المختلفة وبأساليب مختلفة، وذلك بحكم أنهم يكونون على درجة كبيرة من المهارة والإتقان والغرض دائما هو الكسب أو الحصول على فائدة مادية أو معنوية.¹⁹

وتتميز فئة المحترفون في الجريمة المعلوماتية بسعة الخبرة والإدراك الواسع للمهارات التقنية، كما تتميز بالتنظيم والتخطيط للأنشطة التي ترتكب من قبل أفراد هذه الفئة، ولذلك فإنها تعد الأخطر من بين مجرمي التقنية، حيث تهدف إعتداءاتهم إلى تحقيق الكسب المادي لهم، أو للجهات التي كلفتهم وسخرتهم لإرتكاب جرائم الحاسوب، كما تهدف إعتداءات بعضهم إلى تحقيق أغراض سياسية، أو التعبير عن موقف فكري أو فلسفي.²⁰

ويلاحظ أن الأضرار التي تترتب على هذه الأفعال تكون دائما بالغة الضرر، لأنه على من الخطورة التي ترتبها فئة صغار نوابغ المعلوماتية إلا أنها ليست دائما مؤثره، لأن أغلب الظن يكون قصد هذه الفئة هو إثبات التفوق العلمي.²¹

ويمكن تقسيم هذه الفئة إلى مجموعات متعددة تبعا لتخصصهم بنوع معين من الجرائم، أو تبعا للوسيلة المتبعة من قبلهم في ارتكاب الجرائم مثل طائفة محترفي التجسس الصناعي، أو طائفة مجرمي الإحتيال والتزوير.²²

وتعد أخطر جرائم هذه الفئات جريمة التجسس سواء في المجال الصناعي أو التجاري أو في المجال السياسي أو العسكري، لأن المعلومات التي يحصلون عليها من أي من الجهات المختصة أو من الدول يكون لها بالغ الأثر بالإضرار بتلك الدولة.²³

خاتمة:

وفي الأخير يمكن القول أن هذه أبرز خصائص وأصناف المجرم المعلوماتي في الجريمة المعلوماتية، ومع ذلك فإن هذه الخصائص والأصناف غير ثابتة لدى الفقهاء والباحثين، لأن السلوك الإجرامي والدوافع لإرتكاب الجريمة المعلوماتية قد تتغير وتتحوّل بسرعة من العبث أو التحدي والتغلب على الأنظمة المعلوماتية إلى تدميرها أو حيازتها للقيام بعمليات الابتزاز، أو إستعمالها في الحصول على الأموال، ولذلك فإن الدافع إلى إرتكاب الجريمة المعلوماتية لا يتوقف عند هذه الخصائص والأصناف، لأننا نجد في كل جريمة جديدة دوافع جديدة، بل نجد أن الجريمة الواحدة لها دوافع متعددة خاصة إذا إشتبك فيها أكثر من شخص أو أكثر من جهة بحيث يسعى كل منهم لتحقيق أهدافه الخاصة.

الهوامش:

- 1-صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة الحصول على شهادة الماجستير في القانون الدولي للأعمال، كلية الحقوق، جامعة مولود معمري - تيزي وزو، 2012/2013، ص33.
- 2-عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2006، ص84.
- 3-حاتم عبد الرحمان الشحات، الإجرام المعلوماتي، دار النهضة العربية، القاهرة، 2003، ص88.
- 4-عبد الفتاح بيومي حجازي، مرجع سابق، ص86.

- 5- هروال هبة نبيلة، جرائم الأنترنت-دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة أبي بكر بلقايد- تلمسان، 2013/2014، ص48.
- 6- نائلة عادل محمد قورة، جرائم الحاسب الآلي الإقتصادية، منشورات الحلبي، الطبعة الأولى، 2005، ص ص58-59.
- 7- الشوا سامي، الغش المعلوماتي ظاهرة إجرامية مستحدثة، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، القاهرة، 1993، ص525.
- 8- نھلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع عمان الأردن، 2010، ص79.
- 9- محمد طارق عبد الرؤوف الخن، جريمة الإحتيال عبر الأنترنت، منشورات الحلبي، لبنان، الطبعة الأولى، 2011، ص188.
- 10- نھلا عبد القادر المومني، مرجع سابق، ص82.
- 11- تركي بن عبد الرحمان المويشير، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، جامعة نايف للعلوم الأمنية، الرياض، 2012، ص43.
- 12- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، (النظام القانوني لحماية المعلوماتي)، دار الجامعة الجديدة، الإسكندرية، 2009، ص180.
- 13- محمد طارق عبد الرؤوف الخن، مرجع سابق، ص185.
- 14- نھلا عبد القادر المومني، مرجع سابق، ص83.
- 15- عبدا لصبور عبد القوي علي المصري، المحكمة الرقمية والجريمة المعلوماتية، مكتبة القانون والإقتصاد، الرياض، الطبعة الأولى، 2012، ص55.
- 16- رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي، لبنان، الطبعة الأولى، 2012، ص97.
- 17- محمد طارق عبد الرؤوف الخن، مرجع سابق، ص186.
- 18- يونس عرب، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والأنترنت، الجزء الأول، منشورات إتحاد المصارف العربية، الطبعة الأولى، 2000، ص286.
- 19- أيمن عبد الحفيظ، الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، ص34.
- 20- محمد طارق عبد الرؤوف الخن، مرجع سابق، ص187.

- 21- خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2009، ص148.
- 22- محمد طارق عبد الرؤوف الخن، مرجع سابق، ص187.
- 23- خالد ممدوح إبراهيم، مرجع سابق، ص149.

تطور الجريمة المعلوماتية

ط.د/ مشان عبد الكريم

كلية العلوم الاقتصادية

جامعة المسيلة

ط.د/ سبيع جميلة

كلية الحقوق والعلوم السياسية

جامعة تيزي وزو

مقدمة:

بدأت الجريمة ببدء الحياة نفسها وتطورت معها، متخذة أبعادا جديدة في صورها وأحجامها وأسلوب ارتكابها وهي تتصل في بعدها المعاصر إتصالا وثيقا بما يشهده العالم من تطور هائل في حركة التصنيع، ووسائل النقل السريع وكذلك حرية إنتقال الأشخاص والأموال.

وهذه العوامل أدت الى تطور الظاهرة الإجرامية في العصر الحديث تطورا ملحوظا ومذهلا؛ سواء في شخصية مرتكبيها أو أسلوب ارتكابها مع استخدام آخر ما توصلت إليه العلوم التقنية والتكنولوجية، وقد تميز القرن العشرين باختراعات هائلة على المستوى التقني لعل من أهمها ظهور الحاسوب الإلكتروني ووجود ما يعرف بالإنترنت؛ وتعني شبكة الشبكات أي ربط شبكات الحاسوب الموجودة ببعضها البعض. وقد نشأت الانترنت نشأة عسكرية عام 1969 من أجل وزارة الدفاع الأمريكية ” البنتاجون ” ثم سرعان ما تحول استخدامه إلى المجال التعليمي سنة 1972 حيث أتيح استخدامه من قبل الجامعة. وأخذت استخدامات الانترنت تتطور فيما بعد.

ورغم الإيجابيات التي وفرتها النظام المعلوماتي في شتى الميادين إلا أنه لا يخلو من بعض المخاطر لأن المعلومة باعتبارها علم للمعالجة الآلية للمعطيات أصبحت تُثير عدة مشكلات من الناحية القانونية؛ فقد تكون محلا. للاعتداء كارتكاب الجرائم عن بعد، فالجريمة المعلوماتية هي نوع مستحدث من أنواع الجرائم الحديثة عامة التي ظهرت بالتزامن مع ثورة التكنولوجيا والاتصالات، حيث تمتاز باعتمادها الكامل على الصورة الإلكترونية لذلك فإنها تقتزن اقترانا وثيقا بالتكنولوجيا، كما يمكن وصفها أيضاً بأنها جريمة تقليدية ترتكب بطرق تكنولوجية أو إلكترونية حديثة، ومن الجدير بالذكر أن لهذا النوع من الجرائم تعريفات متعددة يصعب حصرها ولكن يمكن الإجماع على أنها عمل غير مشروع ولا أخلاقي يُرتكب من قبل أشخاص متخصصين يمتنعون الإجرام الإلكتروني بواسطة الحاسوب قد يتخلله حذف أو نسخ أو التسلل إلى معلومات سرية غير مخول بالوصول إليها، كما

يشمل أيضاً إلحاق الضرر بجهاز الآخر ومعلوماته، وبذلك تدخلت التشريعات من أجل التصدي لمثل هذه الظواهر ومعاقبة مرتكبيها انطلاقاً من مبدأ الشرعية وفقاً لأحكام مواد قانون العقوبات، وكغيرها من الجرائم قد مر تطورها التاريخي بعدة أسباب وعدة مراحل وهو ما سنحاول دراسته من خلال تقسيم البحث الى مبحثين يتضمن الاول الاسباب التي أدت لبروز الجريمة المعلوماتية، في حين تضمن المبحث الثاني المراحل التي مرت بها الجريمة المعلوماتية.

المبحث الاول: أسباب الجريمة المعلوماتية

لاشك أن فئات مرتكبي الجريمة المعلوماتية تختلف عن مرتكبي الأفعال الإجرامية التقليدية، لذا من الطبيعي أن نجد نفس الاختلاف في الأسباب والعوامل التي تدفع في ارتكاب الفعل غير المشروع ومن بين الاسباب التي تؤدي لارتكاب الجريمة المعلوماتية يمكن أن نذكر.

المطلب الأول: غاية التعلم

وبأني في مقدمة أسباب الجريمة المعلوماتية، غاية التعلم والتي تتمثل في استخدام الكمبيوتر والإمكانات المستحدثة لنظم المعلومات وهناك أمل الريح وروح الكسب التي كثيراً ما تدفع إلى التعدي على نظم المعلومات بالإضافة إلى الدوافع الشخصية والمؤثرات الخارجية التي قد تكون سبباً في ارتكاب الجريمة المعلوماتية.

يشير الأستاذ ليفي مؤلف كتاب قراصنة الأنظمة HACKERS إلى أخلاقيات هؤلاء القراصنة والتي تتركز على مبدئين أساسيين

- 1- أن الدخول إلى أنظمة الكمبيوتر يمكن أن يعلمك كيف يسير العالم.
 - 2- أن جمع المعلومات يجب أن تكون غير خاضعة للقيود.
- وبناء على هذين المبدئين فإن أجهزة الكمبيوتر المعنية ما هي إلا آلات للبحث، والمعلومات بدورها ما هي إلا برامج وأنظمة معلومات.

ومن وجهة نظر هؤلاء القراصنة فإن جميع المعلومات المفيدة بوجه عام يجب أن تكون غير خاضعة للقيود وبعبارة أخرى أن تتاح حرية نسخها وجعلها متناسب مع استخدامات الأشخاص.

ويري هؤلاء القراصنة إغلاق بعض نظم المعلومات وعدم السماح بالوصول إلى بعض المعلومات وخاصة بعض المعلومات السرية التي تخص الأفراد.

ويعلق قراصنة الأنظمة أنهم يرغبون في الوصول إلى مصادر المعلومات والحاسبات الإلكترونية والشبكات بغرض التعلم.

وقد لاحظ كل من "ليفي" و "لاندريس" أن قراصنة الأنظمة لديهم الاهتمام الشديد بأجهزة الكمبيوتر وبالتعلم ويدخل العديد منهم في أجهزة الكمبيوتر على أنهم محترفين ويختار بعض القراصنة الأنظمة لتعلم المزيد عن كيفية عمل الأنظمة.

ويقول "لاندريس" أن هؤلاء القراصنة يرغبون في البقاء مجهولين حتى يتمكنوا من الاستمرار في التواجد داخل الأنظمة لأطول وق ممكن. ويكرس البعض منهم كل وقته في تعلم كيفية اختراق المواقع الممنوعة والتقنيات الأمنية للأنظمة حيث تتفاوت معرفتهم عن الأنظمة والبرمجة إلى حد بعيد. وكتب أحد قراصنة الأنظمة يقول يكتشف قراصنة الأنظمة نقطة ضعف أمنية فيحاولون استغلالها لأنها موجودة بهدف عدم تخريب المعلومات أو سرقتها، أعتقد أن نقوم به يشبه قيام شخص باستكشاف أساليب جديدة للحصول على المعلومات من المكتبة فيصبح في غاية الإثارة والانهماك. وينبغي ألا نستعين بكفاءة الشبكات التي يتعلم من خلالها القراصنة حرفتهم.

وهم يقومون بالفعل بالبحث واكتشاف الأنظمة والعمل من خلال الجماعة وتعليم بعضهم البعض. حيث ذكر أن قراصنة الأنظمة أنه ينتمي إلى مجموعة بحث مهمتها استخراج كميات كبيرة من المعلومات وتعلم أكبر قدر منها.

ويسعى أعضاء القراصنة إلى التخصص والتعاون في المشاريع البحثية وتقاسم البرامج والأخبار وكتابة المقالات وتعريف الآخرين بمجالات اختصاصهم ويدع قراصنة الأنظمة نظاماً خاصاً لمجال المعرفة الذي يجذبهم ويعلمهم التفكير ويسمح لهم بتطبيق ما تعلموه في أنشطة هادفة وإن لم تكن قانونية

دائمة

المطلب الثاني: سعي إلى الربح

أشارت إحدى المجالات المتخصصة في الأمن المعلوماتي securite informatique إلى الرغبة في تحقيق الثراء من بين العوامل الأساسية لارتكاب الجريمة المعلوماتية حيث أشارت أن 43% من حالات الغش المعلن عنها قد بوشرت من أجل اختلاس الأموال.

- 23% من أجل سرقة المعلومات.

- 19% أفعال اتلاف.

- 15% سرقة وقت الآلة؛ أي الاستعمال غير المشروع للحاسب الآلي لأجل تحقيق أغراض شخصية.

لذا نجد أن الدافع لارتكاب الجريمة المعلوماتية يمكن أن تكون سببه مجرد سداد الديون المستحقة أو مشاكل عائلية راجعة للنقود أو ادمان ألعاب القمار أو المخدرات لذا فإن بيع المعلومات المختلصة هو نشاط متسع للغاية ويمكن أن نبين في هذا المجال واقعة استيلاء مبرمج يعمل لدى إحدى الشركات الألمانية على 22 شريطاً ممغنطاً تحوي معلومات هامة بخصوص عملاء وإنتاج هذه الشركة حيث هدد السارق ببيعها للشركات المنافسة ما لم تدفع له فدية مقدارها 200.000 دولار.

بعد أن قامت الشركة بتحليل الموقف وقدرت أن الخسائر التي يمكن أن تنشأ عن إفشاء محتواها تفوق بكثير المطلب المطلوب فقد فضلت دفع المبلغ من أجل استرداد الشرائط المسروقة.

كذلك أيضاً دفعت الرغبة بمستخدم يعمل بشركة التأمين كي يحتفظ بوظيفته التي سبق وأن فصل منها إلى احتجاز الذاكرة المركزية الخاصة بالشركة كرهينة لديه، حيث هدد المختلس رئيسه في العمل بأنه إذا حاول أن يلغي بطاقة أجرته من ذاكرة الحاسب الآلي فإن هذه الأخيرة سوف تدمر تلقائياً عن طريق ما يعرف بالقنابل المنطقية.

المطلب الثالث: الإثارة والمتعة والتحدي

يدرك القراصنة شيئاً عن أساسيات الكمبيوتر وأن هذا الأمر يمكن أن يكون ممتعاً، حيث جاء على لسان أحد القراصنة ما يأتي كانت القرصنة هي النداء الأخير الذي يبعثه دماغه فقد كنت أعود إلى البيت بعد يوم ممل آخر في المدرسة، وأدير تشغيل جهاز الكمبيوتر، وأصبح عضواً في نخبة قرصنة الأنظمة، كان الأمر مختلفاً برمته حيث لا وجود لعطف الكبار وحيث الحكم هو موهبتك فقط. في البدء كنت أسجل أسمى في لوحة النشرات Bulletin Board الخاصة حيث يقوم الأشخاص الآخرون الذين يفعلون مثلي بالتزرد على هذا الموقع، ثم أتصفح أخبار المجتمع وأتبادل المعلومات مع الآخرين في جميع أنحاء البلاد.

وبعد ذلك أبدأ عملية القرصنة الفعلية، وخلال ساعة واحدة يبدأ عقلي بقطع مليون ميل في الساعة وأنسي جسدي تماماً بينما أنتقل من جهاز كمبيوتر إلى آخر محاولاً العثور على سبيل للوصول إلى هدي. لقد كان الأمر يشبه سرعة العمل في متاهة إلى جانب الاكتشاف الكبير لإعداد ضخمة من المعلومات. وكان يرافق تزايد سرعة الأدرينالين الإثارة المحظورة بفعل شيء غير قانوني. وكل خطوة

أخطوها كان يمكن أن تسقطني بيد السلطات. كنت على حافة التكنولوجيا واكتشاف ما وراءها، واكتشاف الكهوف الإلكترونية إلى لم يكن من المفترض وجودي بها⁽¹⁾ وذكرت Jutian Dibbell بأنها تعتقد بأن المتعة تكمن في المخاطر التي ترتبط بعملية القرصنة وذكرت قائلة "أن التكنولوجيا تستسلم من الدراما المليئة بالمغامرات وأن قراصنة الأنظمة يعيشون في عالم لا يعتبرون فيه العمل السري سوى لعبة يلو بها الأطفال.

المطلب الرابعالدوافع الشخصية

إن الدافع لارتكاب جرائم الكمبيوتر يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح، ويميل مرتكبوا جرائم نظم المعلومات إلى إظهار تفوقهم ومستوي ارتقاء براعتهم لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبوا هذه الجرائم لديهم شغف الآلة، وغالباً ما يجدون الوسيلة إلى تحطيمها⁽²⁾

ويتزايد شيوع هذا الدافع لدى فئات صغار السن من مرتكبي الكمبيوتر الذين يمضون وقتاً طويلاً أما حواسيهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الكمبيوتر وشبكات المعلومات وإظهار تفوقهم على وسائل التكنولوجيا، الأمر الذي دفع بالعديد من الفقهاء إلى المناداة بعدم مساءلة مرتكبي جرائم الحاسب الآلي الذي يتمثل باعتهن في إظهار تفوقهم، واعتبار أعمالهم غير منظوية على نوايا آثمة.

وقد أمكن الكشف في بعض الأحوال عن أن مجرد إظهار شعور جنون العظمة وهو الدافع لارتكاب فعل الجريمة المعلوماتية وفي هذا الشأن نجد المحلل أو المبرمج المعلوماتي وهو مفتاح سر كل نظام قد ينتابه إحساس بالإهمال⁽³⁾

¹ حول قراصنة أنظمة الكمبيوتر، راجع: دروئي إي. دينغ، ورقة مقدمة للمؤتمر القومي الثالث عشر لأمن الكمبيوتر، مرجع سابق، ص. 11

² يميل القراصنة إلى التحدي وإلى معرفة تفاصيل تكنولوجيا الكمبيوتر ويبدو أن ولعهم بالكمبيوتر يدفعهم إلى ارتكاب الجرائم وفي هذا الخصوص يحدثنا الدكتور Perey Black أستاذ علم النفس بجامعة نيويورك أن القراصنة يملكونهم جميعاً شعور بالبحث عن القوة ويؤدي ارتكابهم للجرائم بواسطة الكمبيوتر إلى تعويضهم عن الإحساس بالدونية.

³ د/ عبد العالي الديري، دوريات - مفاهيم استراتيجية - الجريمة المعلوماتية، تعرفها أسبابها خصائصها.

وقد يندفع تحت تأثير الرغبة القوية من أجل تأكيد قدراته الفنية لإدارة المنشأة إلى ارتكاب الجريمة المعلوماتية، ومن ثم يجد ترضية من خلال الإفصاح عن شخصيه أمام العامة.

المبحث الثاني: المراحل التي مرت بها الجريمة المعلوماتية

الجريمة المعلومات كغيرها من الجرائم مر تطورها بعدة مراحل تاريخية أدت لبروزها على ماهي عليه اليوم. وذلك من خلال.

المطلب الأول: مرحلة الستينيات

شيوخ استخدام الحواسيب في الستينيات على السبعينات اقتضت المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر، وترافقت هذه النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم مجرد شئ عابر أم ظاهرة إجرامية مستحدثة، وأن الجدل حول ما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في بيئة أو مهنة الحوسبة، ومع تزايد استخدام الحواسيب الشخصية في السبعينات ظهرت عدد من الدراسات المسحية والقانونية التي اهتمت بجرائم الكمبيوتر وعالجت عددا من قضايا الجرائم الفعلية، وبدأ الحديث عنها بوصفها ظاهرة إجرامية لا مجرد سلوكيات مرفوضة. من شيوخ استخدام الكمبيوتر في الستينيات ومن ثم السبعينات: ظهرت أول معالجة لجرائم، بظهور استخدام الكمبيوتر وربطه بالشبكة في الستينيات إلى السبعينيات الكمبيوتر في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر و التجسس المعلوماتي، وشكلت موضوع التساؤل إذا ما كانت هذه الجرائم مجرد حالة عابرة أم ظاهرة إجتماعية إجرامية مستجدة ؟ وهل هي جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في مجال المعلوماتية؟، فبقيت محصورة في إطار السلوك اللاأخلاقي دون النطاق القانوني ومع توسع الدراسات تدريجيا⁽¹⁾.

خلال السبعينات بدأ الحديث عنها كظاهرة إجرامية جديدة وترافقت هذه النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم شئ عابر أم ظاهرة إجرامية مستحدثة، وإن الجدل حول ما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في بيئة أو مهنة الحوسبة، ومع تزايد استخدام الحواسيب الشخصية في السبعينات ظهرت عدد من الدراسات المسحية والقانونية

¹ يونس عرب، جرائم الكمبيوتر والانترنت، إيجاز في المفهوم والنطاق، ورقة عمل مقدمة الى مؤتمر الامن العربي، تنظيم المركز للدراسات والبحوث الجنائية، ابو ظبي، ايام 10-12/02/2002، ص 8.

التي إهتمت بجرائم الكمبيوتر وعالجت عددا من قضايا . الجرائم الفعلية، وبدأ الحديث عنها بوصفها ظاهرة إجرامية لامجرد سلوكيات

المطلب الثاني: مرحلة الثمانينيات

في الثمانينيات حيث طفا على السطح مفهوم جديد لجرائم الكمبيوتر والانترنت وإرتبطت بعمليات إقتحام نظام الكمبيوتر عن بعد وأنشطة نشر وزرع الفيروسات الإلكترونية التي تقوم بعملية تدميرية للملفات أو البرامج. وقد شاع إصطلاح "الهكرز" المعبر عن محققي النظم، لكن الحديث عن الدوافع لإرتكاب هذه الأفعال ظل محظورا في رغبة المحترفين تتجاوز أمن المعلومات وإظهار تفوقهم التقني، ولكن هؤلاء المفلمرون أصبحوا أداة إجرام، وظهور المجرم المعلوماتي المتفوق المدفوع بأغراض إجرامية خطيرة القدرة على إرتكاب أفعال تستهدف الاستيلاء على المال أو التجسس أو الاستيلاء على البيانات السرية والاقتصادية الاجتماعية والسياسية والعسكرية، لكن بتزايد خطورة هذه الممارسات أصبح من الضروري إعادة تصنيف الفاعلين وتحديد طوائفهم خاصة بعد تحول الجريمة من مجرد مغامرة و إبداء التفوق إلى أفعال تستهدف التجسس والاستيلاء⁽¹⁾

المطلب الثالث: مرحلة التسعينيات

شهدت فترة التسعينات تناميا هائلا في حقل الجرائم التقنية وتغيرا في نطاقها ومفهومها، وكان ذلك بفعل ما أحدثته شبكة الإنترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكات المعلومات، التي تقوم على فكرة تعطيل نظام تقني ومنعه من القيام، فظهرت أنماط جديدة كأنشطة إنكار الخدمة بعمله المعتاد، وأكثر ما مورست ضد مواقع الإنترنت التسويقية الناشطة والهامة التي يعني انقطاعها، ونشطت جرائم نشر الفيروسات عبر مواقع الإنترنت لما تسهله من خدمة لساعات خسائر مالية بالملايين من انتقالها إلى ملايين المستخدمين في ذات الوقت، وظهرت أنشطة الرسائل والمواد الكتابية المنشورة على الإنترنت أو المرسلة عبر البريد الإلكتروني، المنطوية على إثارة الأحقاد أو المساس بكرامة واعتبار الأشخاص أو المستهدفة الترويج لمواد أو أفعال غير قانونية وغير مشروعة (جرائم المحتوى الضار)

⁰¹ الجريمة الالكترونية في التشريع الجزائري، دراسة مقارنة - مذكرة مكملة لشهادة الماستر في الحقوق، كلية الحقوق، جامعة محمد خيضر، بسكرة، 2015/2016، ص17.

ذلك أن خطر انتهاك أمن وسلامة الكمبيوتر مستمرة مدى استمرارية هذه التحصينات. وقد يكون الكمبيوتر في مجال ارتكاب الجرائم هدفا للجريمة، أو أداة لارتكابها أو مسرحا لها، وقد يكون الكمبيوتر دورا رئيسيا في حقل اكتشاف الجريمة.⁽¹⁾

الخاتمة:

من خلال ما سبق ذكره يمكن القول بأن الجريمة الالكترونية قد مر تطوره بعدة مراحل بداية من مرحلة الستينيات، حينما اقتضت المعالجة على مقالات ومواد تتنافس وتلائم البيانات مرور بمرحلة الثمانينات حينما طفا على السطح مفهوم جديد لجرائم الكمبيوتر والانترنات، وصولا لمرحلة التسعينات التي شهدت تناميا هائلا في حقل الجرائم التقنية وتغيرا في نطاقها ومفهومها، ومن ثمّة فالجريمة الالكترونية ظاهرة اجتماعية مستجدة نسبيا تفرع في جوانبها أجراس الخطر..

¹ يونس عرب، جرائم الكمبيوتر والانترنت، إيجا ز في المفهوم والنطاق، المرجع السابق. ص. 47.

وسائل التحقيق الجنائي في الجرائم الرقمية

أ.د/ حسينة شرون

كلية الحقوق والعلوم السياسية

جامعة بسكرة

أ/ زينب خذير

كلية الحقوق والعلوم السياسية

جامعة غرداية

مقدمة:

شهد عصر المعلوماتية تطورا ملحوظا فيما يخص وسائل التحقيق الجنائي وكان ذلك تزامنا مع حركة الجريمة وتطور أساليب ارتكابها، فبعد أن كانت وسائل التحقيق تتميز بالعنف والتعذيب بغية الوصول إلى الدليل أصبحت في مرحلة لاحقة تتميز بالطابع العلمي وذلك بالاستعانة بالأساليب العلمية واستخدام الانترنت، ويرجع ذلك إلى حدوث طفرة علمية في مجال تكنولوجيا المعلومات والاتصالات واستخدام الوسائط الالكترونية في شتى مجالات الحياة، فكلما اكتشف العلم شيئا حديثا وجد هذا الاكتشاف طريقه إلى مجال الإثبات الجنائي، هذا التطور العلمي أدى إلى ظهور أنماط جديدة من الجرائم لم تعهد من قبل فالجرم والجريمة في تجدد مستمر مع العصر الأمر الذي يستوجب معه تحديث الأنظمة والتعليمات والجهات الأمنية المختصة بمعالجة القضايا الناتجة عن ظهور هذه الجرائم واستحداث وتطوير أساليب التحقيق فيها.

ولعل بروز ظاهرة الجرائم الرقمية تشكل في حد ذاتها تحديا حقيقيا للسياسات الجنائية السائدة وأجهزتها التشريعية والتنفيذية والقضائية في كشف هذا النمط من الجرائم والوصول إلى دليل جنائي رقمي عن طريق تطوير القواعد القانونية الخاصة بالبحث والتحري واستخدام طرق وأساليب حديثة من أجل إثبات هذا النوع من الجرائم وهو ما عمل عليه المشرع الجزائري حين أدرج قواعد و نصوص قانونية توسع من الإختصاص القضائي لوكلاء الجمهورية وقضاة التحقيق، وتعزيز صلاحيات الضبطية القضائية بوضع آليات جديدة خاصة بالبحث والتحري تدعم الآليات العامة من أجل الوصول إلى الدليل الرقمي.

وعلى ضوء ما تقدم نجد أن الإشكالية التي يجب معالجتها من خلال هذه الدراسة هي:
فيما تتجسد الوسائل القانونية المتبعة للتحقيق في الجريمة الرقمية؟

وتتجلى أهمية هذا الموضوع في حادثة الموضوع واعتماد الجهات المكلفة بالتحقيق إلى جانب الإجراءات العامة إجراءات تحقيق مستحدثة تتناسب وطبيعة الجريمة المعلوماتية وأيضاً استخدام وسائل تقنية لاستخلاص الدليل الرقمي، كما منح المشرع للجهات المكلفة بالتحقيق صلاحيات واسعة من خلال تعديل قانون الإجراءات الجزائية وكذا القانون 04/09 السالف الذكر والمرسوم الرئاسي 261/15.

والهدف المتوخى من هذه الدراسة هو إثبات حقيقة وقوع الجريمة في العالم الافتراضي ومعرفة الكيفية التي نفذت بها والظروف التي واكبت ارتكابها ذلك أن الغاية الأساسية من التحقيق هو الكشف عن الحقيقة و التنقيب عن الأدلة وجمعها في إطار التقييم القانوني لها.

- كذلك توضيح الطابع الخاص الذي تكتسيه الآليات العامة للتحقيق ومدى نجاعة الآليات الخاصة في كشف غموض الجرائم الرقمية و الحصول على دليل رقمي و توضيح مدى اختلاف التحقيق في هذه الجرائم عن الجرائم التقليدية.

وبغرض الإجابة على الإشكالية المطروحة أعلاه، تطلب منا إعداد هذا المقال الاعتماد على المنهج التحليلي من خلال تحليل بعض المفاهيم القانونية المتعلقة بالموضوع وكذلك شرح المواد ذات الصلة به منها بعض المواد في قانون الإجراءات الجزائية وكذا القانون 04/09، والمرسوم الرئاسي رقم: 261/15.

عند قيام المحقق بالتحقيق في جريمة ما عليه أن يلتزم في ذلك بقوانين وتشريعات وقواعد فنية في سبيل الكشف عن الحقيقة والوصول إلى الجاني فالحقق يتبع الإجراءات المحددة والمحكومة باللوائح المنظمة والقواعد الفنية للتحقيق، كما يتبع أساليب متغيرة كل أسلوب منها يعالج حالة معينة في ظروف معينة، فالحقق يدرس الحالة ويقرر الأسلوب المناسب من خلال دراسته لقضية التحقيق، بالتالي فهو يحتاج لعدة وسائل مادية وطرق والأساليب لضبط الجريمة وجمع الأدلة بهدف إثبات وقوعها ونسبتها إلى الجاني، وهذه الوسائل قد تكون مادية أو إجرائية وينبغي في ذلك إتباع منهج محدد، لذلك سيتم من خلال هذا المقال التطرق إلى منهج التحقيق الجنائي في الجريمة الرقمية (المحور الأول) و إلى الوسائل المادية للتحقيق (المحور الثاني) ثم الوسائل الإجرائية (المحور الثالث).

المحور الأول: منهج التحقيق الجنائي في الجرائم الرقمية.

التحقيق الجنائي له قواعد قانونية وأخرى فنية، تتمثل الأولى في تلقي المحقق البلاغ عن وقوع الجريمة متبعاً في ذلك الإجراءات اللازمة للكشف عن غموضها وضبط الفاعل وتقديمه للمحاكمة أما

القواعد الفنية للتحقيق الجنائي فتتمثل في تلك التي تحكم المحقق منذ تلقيه البلاغ حتى ضبط المتهم، وحتى يتمكن من التوصل إلى هذه النتيجة عليه أن يتبع منهجا أو أسلوبا محددا في التحقيق يتمثل في تحديد خطة عمل وتكوين فريق متكامل.

أولا: تحديد خطة عمل التحقيق الجنائي في الجرائم الرقمية.

بعد استكمال جمع المعلومات اللازمة عن الواقعة الإجرامية يبدأ المحقق معتمدا على تلك المعطيات المتوفرة لديه بتحديد خطة عمل مناسبة وفريق عمل للتحقيق في الحادثة ولا بد أن تكون هذه الخطة قد اكتملت في ذهن المحقق بمجرد انتهائه من معاينة موقع الحادث واتضحت لديه الصورة الأولية عن الحادث¹.

1/ تحديد خطة العمل المناسبة للتحقيق الجنائي في الجرائم الرقمية:

يتم التخطيط للتعامل مع حوادث الحاسب الآلي وشبكة الانترنت على ثلاث مستويات مختلفة يبنى كل مستوى منها على الآخر².

أ/ تخطيط استراتيجي للتحقيق الجنائي في الجرائم الرقمية:

وهو تخطيط بعيد المدى يهتم بحماية البنية التحتية لشبكات الحاسوب الوطنية، من خلال تحديد مصادر الخطر المحتملة التي قد تمثل تهديدا لها وتحديدها، ويهتم بوضع تصورات على درجة من المرونة تكون كفيلة بالتصدي لهذا النوع من الجرائم قبل وقوعها وضبطها والحد من آثارها في حال وقوعها، ويتم هذا التخطيط على مستوى واضعي السياسات الأمنية، حيث يهدف بشكل عام إلى منع هذا النوع من الجرائم من الوقوع داخل إقليم الدولة، والحد من قابلية الحواسيب والشبكات الوطنية من التعرض للهجوم، ومن ثم السيطرة على الحوادث إن وقعت وضبطها والحد من آثارها.

ب/ تخطيط تكتيكي للتحقيق الجنائي في الجرائم الرقمية:

ينبثق من الخطة الإستراتيجية ويتم على مستوى الجهات الرسمية وغير الرسمية التي لها علاقة بتقنية المعلومات ويدعم غايات وأهداف الخطة الإستراتيجية للتعامل مع جرائم الحاسوب والانترنت، ويمتاز

¹ حسن طاهر داود، "جرائم نظم المعلومات"، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ط1، 2000، ص 231.

² حسين بن سعيد الغافري، "التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت"، موقع المنشاوي للدراسات والبحوث على الموقع www.minshaw.com أطلع عليه بتاريخ: 2019/02/01، ص 6.

بأن له طابع تفصيلي أكثر من التخطيط الإستراتيجي، والخطط التكتيكية الخاصة بالتعامل مع جرائم الانترنت يجب أن تتضمن إجراءات مسبقة التحديد على درجة عالية من التفصيل والوضوح للتحقيق في هذه الجرائم.

ج/ خطة العمل في التحقيق الجنائي في الجرائم الرقمية:

ويقصد به التخطيط الذي يقوم به المحقق لتحديد الأسلوب الأمثل في التعامل مع حادث بعينه، وذلك في الإطار العام للإجراءات الواردة في الخطة التكتيكية وبما يتناسب مع خصوصية ظروف وملابسات الحادث.

2/ متركزات خطة العمل في التحقيق الجنائي في الجرائم الرقمية:

تعد من أهم الأمور التي يجب على المحقق أخذها بعين الاعتبار كمتركزات تساعد في تحديد خطة العمل المناسبة للتحقيق في أي جريمة من الجرائم الرقمية والانترنت¹.

أ/ حجم ونوع الحادث التي يكون المحقق بصدد التحقيق فيه يرتبط به تحديد حجم ونوع فريق التحقيق، فجرائم الانترنت منها الصغير ومنها الكبير ولكل جريمة مهما كان حجمها، طبيعتها الفنية الخاصة التي تفرض على أعضاء فريق التحقيق امتلاك مهارات فنية خاصة تعتبر ضرورية للتعامل مع هذا النوع من الجرائم، وهو أمر يجب مراعاته عند اختيار أعضاء الفريق.

ب/ بعض الظروف المحيطة بالحادث تمثل عوامل مهمة يجب مراعاتها عند وضع خطة العمل، لما يترتب عليها من قرارات على درجة كبيرة من الأهمية تتعلق بالتحقيق، ومن هذه العوامل:

- مدى أهمية الأجهزة الحاسوبية والشبكات المتضررة لعمل المنظمة أو المؤسسة.

- مدى حساسية البيانات التي قد تكون محل الجريمة الحاسوبية.

- المتهمون المحتملون.

- اطلاع الرأي العام على الجريمة أم لا.

- مستوى الإختراق الأمني الذي تسبب فيه الجاني.

- مستوى المهارة الفنية التي يتمتع بها الجاني.

ج/ طبيعة مسرح الجريمة تفرض الأسلوب الأمثل للفتيش بحثاً عن الأدلة التي تكون موجودة فيه والذي يعتبر من أهم خطوات عملية التحقيق وعدم نجاح المحقق في تحديد هذا الأسلوب قد يؤدي

¹ حسين بن سعيد الغافري، المرجع السابق، ص 6.

إما إلى عدم الحصول على أية نتائج أو الحصول على كم كبير من النتائج التي لا فائدة منها، فقائد فريق التحقيق مسؤول عن تحديد حجم المهمة ونوع الأدلة التي يتم البحث عنها بحسب نوع الجريمة، وكذلك تحديد أنسب الطرق لتنفيذ عملية التفتيش وما يتبع ذلك من توزيع للأدوار والواجبات على فريق التحقيق.

د/ تعيين الأشخاص الذين سيتم استجوابهم، وتحديد النقاط التي يجب استيضاحهم بشأنها، وكذلك تقدير مدى الحاجة إلى الاستعانة ببعض الأشخاص من ذوي الاختصاصات الفنية التي يتطلبها التحقيق ولا تتوافر ضمن أفراد التحقيق.

ثانيا: تكوين فريق التحقيق الجنائي في الجرائم الرقمية:

إن التحقيق في قضايا نظم المعلومات عادة ما يكون أكبر من أن يتولاه شخص واحد بمفرده، حتى وإن كانت المضبوطات مجرد حاسب شخصي واحد، فمن الأفضل أن يتعاون عدة أشخاص في إنجاز مهمة التحقيق و العثور على الأدلة¹؛ فهناك محققون جنائيون ذوو خبرة طويلة، وهناك أخصائيون في الحاسب الآلي والشبكات ذو معرفة واسعة، ولكنه من النادر أن يوجد شخص واحد يمتلك مهارات عالية في الاثنين معا، لاسيما وأن عالم الحاسوب والشبكات عالم متعدد ومتشعب وعلى درجة كبيرة من التعقيد وسرعة التطور، ولذلك كان من الضروري أن يستعين المحقق بخبراء في هذا المجال بحسب ما تفرضه ظروف كل قضية وملاساتها.

كما أن التحقيق في هذه الجرائم قد يتطلب الاستعانة ببعض خبراء مسرح الجريمة التقليدية، مثل خبير البصمات وخبير التصوير الذين يعتبرون من الخبراء الأساسيين في معظم أنواع الجرائم. وعلى هذا الأساس يمكن تقسيم فريق التحقيق في هذا النوع من الجرائم إلى فئتين هما:

الفئة الأولى من المحققين الجنائيين في الجرائم الرقمية:

وتمثل الأشخاص الذين يتصل عملهم مباشرة بجرائم الحاسب الآلي والانترنت ولا يمكن التحقيق في أي جريمة تنتمي إلى هذه النوعية من الجرائم إلا بهم، ووجودهم ضروري في مسرح الجريمة ويمكن تحديد أعضاء هذه الفئة على النحو التالي:²

¹ حسن طاهر داود، المرجع السابق، ص 223.

² حسين بن سعيد الغافري، المرجع السابق، ص 7.

- 1- **قائد الفريق أو المحقق الرئيسي:** يشترط فيه أن يكون له خبرة طويلة في مجال التحقيق الجنائي، ولديه معرفة بالطبيعة الخاصة بجرائم الحاسب الآلي والانترنت يتولى السيطرة الكاملة على مسرح الجريمة، وتوزيع المهام على الفريق والإشراف على قيامهم بأعمالهم، والتنسيق مع الجهات ذات العلاقة، واتخاذ كافة القرارات المتصلة بالتحقيق.
- 2- **محقق جنائي:** شخص أو أكثر بحسب ظروف الجريمة، لديه خبرة ومعرفة بوسائل وأساليب التحقيق وإجراءاته، مع إلمامه بطبيعة جرم الحاسوب والانترنت وكيفية التعامل مع الأدلة الرقمية فيتولى التفتيش عن الأدلة وأخذ إفادة الأشخاص ذوي العلاقة في مسرح الجريمة.
- 3- **خبير حاسب آلي وشبكات:** شخص أو أكثر بحسب الظروف يجمع بين المعرفة بعلوم الحاسوب والشبكات وبين الإلمام بإجراءات التحقيق الجنائي وأساليبه وكيفية التعامل مع مسرح الجريمة ويكون مسؤول عن رفع وتحريز الأدلة الجنائية الرقمية بالطريقة الفنية المناسبة التي لا تؤثر على سلامة الدليل وصلاحيته لإقامة الدعوى والعرض على المحكمة.
- 4- **خبير تدقيق حسابات متخصص في المراجعة المحاسبية وعلى درجة من الخبرة في التعامل مع الأنظمة البرمجية المستخدمة في المؤسسات المصرفية والآليات المختلفة التي يتم بواسطتها تبادل النقد الإلكتروني، ويعمل مع خبير الحاسب الآلي والشبكات على تحديد أسلوب الجريمة وما إذا كان هناك تلاعب في الأنظمة المتضررة بالإضافة إلى تقدير الخسائر المادية الناتجة عن الجريمة.**
- 5- **خبير تصوير** يتولى تصوير مسرح الجريمة كما هو متبع في جميع الجرائم فيعمل على تصوير كل المواقع داخل مسرح الجريمة وخارجه وتصوير أدلة الجريمة بالتصوير الفوتوغرافي والفيديو¹.
- 6- **خبير بصمات:** لرفع البصمات من مسرح الجريمة كإجراء عام في معظم الجرائم مع التركيز على المكونات المادية للحواسيب والشبكات المتضررة أو المشتبه بوجود صلة لها بالجريمة، خاصة لوحة المفاتيح والفأرة، وذلك بعد اتخاذ الاحتياطات الفنية اللازمة من قبل خبير الحاسوب.
- 7- **خبير رسم تخطيطي:** يقوم بعمل رسم تخطيطي (كروكي) لمسرح الجريمة بطريقة فنية دقيقة مستخدماً مقياساً مناسباً للرسم، بما يوضح تقسيماته وأماكن تواجد الأدلة والأشخاص فيه.

الفئة الثانية:

¹ حسن طاهر داود، المرجع السابق، ص 224.

وهي تمثل الأشخاص الذين قد يتطلب ظروف مسرح الجريمة تواجدهم، إلا أن دورهم ليس وثيق الصلة بالطبيعة الخاصة لجرائم الحاسب الآلي، وقلما يخلوا مسرح أي جريمة مهما كان نوعها من وجودهم، مثل أفراد حماية وتأمين المسرح وأفراد القبض وأفراد التحريات وغيرهم، وتحديد الأعضاء نوعا وكما متروك لتقدير المحقق على ضوء المعلومات المتوفرة لديه عن الجريمة، وحسب ما تفرضه طبيعة مسرح الجريمة وحجمها وظروفها.

المحور الثاني: الوسائل المادية للتحقيق الجنائي في الجرائم الرقمية

ويقصد بالوسائل المادية تلك الأدوات الفنية التي غالبا ما تستخدم في بيئة نظم المعلومات والتي يمكن باستخدامها يتم تنفيذ إجراءات وأساليب التحقيق المختلفة والتي تثبت وقوع الجريمة وتحدد شخصية مرتكبها، وفي الغالب ما تكون الجرائم التي تقع بواسطة شبكة الانترنت تكون أصعب في الإثبات وتستدعي تدخل الجهات الأمنية أكثر من جرائم النظم الأخرى التي تعلن عنها المؤسسات والتي يكون فيها المجرم غير خاضع للنظام الداخلي للمؤسسة ولا يعمل لديها ومن هنا جاء التركيز على الجرائم التي ترتكب عن طريق شبكة الانترنت وبالرغم من أن الشبكات الأخرى لها نفس الخصائص ومن أهم هذه الوسائل نذكر:

أولا: عناوين (IP¹ و MAC² والبريد الإلكتروني وبرامج المحادثة)

عنوان الانترنت (IP) هو المسؤول عن تراسل حزم البيانات عبر الانترنت وتوجيهها إلى هدفها، ويشبه إلى حد كبير العنوان على مغلف رسائل البريد التقليدي بعد وضعها بصندوق البريد، وهو يتيح للموجات والشبكات المعنية بنقل الرسالة، يوجد عنوان (IP) بكل جهاز مرتبط بالانترنت ويتكون من أربعة أجزاء والجزء الواحد يتكون من ثلاث خانات، فيكون المجموع اثنا عشر خانة كحد أقصى حيث يشير الجزء الأول من اليسار إلى المنظمة الجغرافية، والجزء الثاني لمزود الخدمة والثالث لمجموعة الحاسبات الآلية المرتبطة، والرابع يحدد الحاسب الآلي الذي تم الاتصال منه، وفي حالة وجود أي مشكلة أو أي أعمال تخريبية فإن أول ما يجب أن يقوم به المحقق هو البحث عن رقم الجهاز وتحديد موقعه لمعرفة الجاني الذي قام بتلك الأعمال غير القانونية، ويمكن لمزود خدمة

¹ هو مختصر ل: internet protocol adresse

² هو مختصر ل: media access control

الانترنت أن يراقب المشترك، كما يمكن للشركة التي تقدم خدمة الاتصال الهاتفي أن تراقبه أيضا إذا توفرت لديها أجهزة وبرامج خاصة لذلك، توجد أكثر من طريقة لمعرفة عنوان (IP) الخاص بجهاز الحاسب الآلي في حال الوصول المباشر، منها في حالة العمل على نظام تشغيل windows بكتابة winipcfg في أمر التشغيل ليظهر مربع حوار يبين فيه عنوان (IP) مع ملاحظة أنه قد يتغير كلما تم الاتصال بالانترنت مرة أخرى وفي حالة استخدام أحد برامج المحادثة كأداة للجريمة فإنه يتطلب تحديد هوية المتصل، كما تحدد رسالة البريد الإلكتروني عنوان شخصية مرسلها حتى لو لم يدون معلوماته في خانة المرسل شريطة أن تكون تلك المعلومات التي وضعت في مرحلة إعداد البريد الإلكتروني معلومات صحيحة، كما يمكن الاستعانة بعنوان MAC الذي يحدد أرقام كروت الشبكة MAC للتعرف على عنوان (IP) بشكل صحيح والذي بدوره يحدد شخصية المتصل.

ثانيا: البروكسي Proxy

يعمل البروكسي كوسيط بين الشبكة ومستخدمها، بحيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لإدارة الشبكة وضمان الأمن وتوفير خدمات الذاكرة الجاهزة cache memory، يتلقى مزود البروكسي عبر الانترنت طلبا من المستخدم بحيث يبحث عن الصفحة المطلوبة ضمن ذاكرة كاش cache المحلية المتوفرة فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل، فإذا كانت كذلك بالفعل أعادها إلى المستخدم بدون الحاجة إلى إرسال الطلب إلى الشبكة العالمية، أما إذا لم يجد مزود البروكسي الصفحة المطلوبة ضمن ذاكرة cache فإنه يعمل كمزود زبون ويرسل الطلب إلى الشبكة العالمية بحيث يستخدم أحد عناوين (IP)¹، وأهم مزايا مزود البروكسي أن cache المتوفرة لديه يمكن أن تحتفظ بتلك العمليات التي تمت عليها مما يجعل دورها قوي في الإثبات عن طريق فحص تلك العمليات المحفوظة بها والتي تخص المتهم والموجودة عند مزود الخدمة.

ثالثا: برامج التتبع

تقوم هذه البرامج بالتعرف على محاولات الاختراق التي تمت ومن قام بها وإشعار الجهة المتضررة بعملية الاختراق، ومن الأمثلة على تلك البرامج، برنامج hack tracer v 1,2 وهو مصمم

¹ بن فريدة محمد، "الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية"، شهادة الدكتوراه، جامعة الجزائر، كلية الحقوق، الجزائر، 2015، ص 170.

للعمل في الأجهزة المكتبية web وساكنة في خلفية سطح المكتب وعندما يرصد أي محاولة للقرصنة أو اختراق جهاز الحاسب الآلي يسارع بإغلاق منافذ الدخول أمام المخترق ثم يبدأ في عملية مطاردة تستهدف إقضاء أثر مرتكب عملية الاختراق حتى يصل إلى الجهاز الذي حدثت العملية من خلاله¹.

ويتكون البرنامج من شاشة رئيسية تقدم للمستخدم بيان شامل بعمليات الاختراق التي تحدث ضد جهازه، وتحمل اسم الحدث event وتاريخ حدوثه، وعنوان (IP) الذي تمت من خلاله، واسم الشركة المزودة لخدمة الانترنت المستضيفة للمخترق، وأرقام مداخلها ومخارجها على شبكة الانترنت ومعلومات أخرى²، وفور حدوث أي محاولة للاختراق تظهر أمام المستخدم شاشة أخرى صغيرة مصحوبة بتحذير صوتي ويظهر على الشاشة عنوان (IP) الخاص به ويمكن للمستخدم الإختيار ما بين أربعة أوامر موجودة في هذه الشاشة الفرعية منه report it والأمر الثاني هو trace it، وبمجرد الضغط على هذا الأمر تظهر شاشة أخرى وعليها إسم الدولة التي تمت منها محاولة الاختراق وعلى المستخدم أن يضغط على أمر next حتى يقوم البرنامج باستكمال عملية إقضاء الأثر، وبعدها تظهر شاشة ثالثة عليها خريطة العالم وخط طويل ممتد من المدينة التي تمت منها محاولة الاختراق إلى المدينة التي يقيم فيها المستخدم ويوجد أسفل الخريطة مجموعة من الأوامر هي:

- الأمر الأول map وبالضغط عليها تظهر خريطة عليها خط سير محاولة الاختراق.
- والأمر الثاني هو trace وبالضغط عليه يظهر إسم الشركة المستضيفة وعنوان (IP) ورقم المنفذ port أو البوابة الخاصة بها.
- وهناك أمر network وبالضغط عليه تظهر البيانات الكاملة للشبكة التي تتبعها الشركة المستضيفة للمخترق بما فيها أرقام التليفونات والفاكسات الخاصة بها وآخر تحديث قامت به في جهاز الخدمة الخاص بها.
- وهناك أمر registrant ويقدم معلومات الشركة المستضيفة، ثم أمر إقضاء الأثر وتحديث المعلومات ويظهر على شكل دائرة عليها خطان متقاطعان، ويمكن الحصول على هذا البرنامج من

¹ سليمان مهجع العنزي، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003، ص 100.

² سليمان مهجع العنزي، المرجع نفسه، ص 101.

موقع www.zdnet.com كما يمكن تحديد جهة مرسل الرسائل عن طريق البريد الإلكتروني باستخدام برامج تتبع مصدر الرسائل.

رابعا: نظام كشف الاختراق¹ IDS

وهذه الفئة من البرامج تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الإعلام الآلي أو الشبكة مع تحليلها بحثا عن أي إشارة قد تدل على وجود مشكلة تهدد أمن الحاسوب أو الشبكة، ويتم ذلك من خلال تحليل رزم البيانات أثناء انتقالها عبر الشبكة ومراقبة بعض ملفات نظام التشغيل الخاص بتسجيل الأحداث فور وقوعها في جهاز الحاسب الآلي أو الشبكة ومقارنة نتائج التحليل بمجموعة من الصفات المشتركة للإعتداءات على الأنظمة الحاسوبية.

خامسا: أدوات الضبط في الجريمة الرقمية.

تعد هذه الأدوات من الوسائل المادية التي تساعد في ضبط الجريمة، وإثبات وقوعها والمحافظة على الأدلة، ونسبتها إلى الجاني، لتقديمها إلى هيئة التحقيق من هذه الأدوات برامج الحماية، أدوات المراجعة auditing، أدوات مراقبة المستخدمين للشبكة، أدوات التنصت على الشبكة، التقارير التي تنتجها نظم أمن البيانات، مراجعة قاعدة البيانات، برامج النسخ الاحتياطي والتسجيل.

سادسا: الأدوات المساعدة بالتحقيق في الجرائم الرقمية.

يجب على المحقق إختيار ما يناسبه من الأدوات التي تساعد في التحقيق لأنه يحتمل أن الجاني قد قام بتشفير البرامج أو غير كلمات المرور أو أخفى تلك المعلومات أو غير فيها أو قام بإتلاف أدوات الحفظ الخارجية أو دمر المعلومات بأدوات الجريمة مثل الفيروسات وغيرها ولذا يحتاج إلى أدوات مساعدة كأدوات استرجاع المعلومات من الأقراص التالفة، وبرامج كسر كلمة المرور، وبرامج الضغط وفك الضغط، برامج البحث عن الملفات العادية والمخفية وبرامج تشغيل الحاسب وبرامج نسخ البيانات، كما يتطلب استخدام برامج منع الكتابة على القرص الصلب بعد ارتكاب الجريمة وذلك من أجل حماية مسرح الجريمة، كما يمكن عن طريق برامج استرجاع الملفات استعادة الملفات التي قام الجاني بحذفها نهائيا من الحاسب الآلي.

سابعا: أدوات فحص ومراقبة الشبكات.

¹ هو مختصر ل: intrusion detection system

يمكن أن يستخدم المحقق عدد من الأدوات في فحص البروتوكول TCP/IP وذلك لمعرفة المشاكل المتعلقة بالشبكات والعمليات التي تعرضت لها ومن بين تلك الأدوات نذكر.

- أداة ARP التي تحدد مكان الحاسب الفيزيائي على الشبكة ومعرفة رقم كرت الشبكة عند تعيين عنوان (IP).

- برنامج Visual route 5,3 a: يلتقط هذا البرنامج أي عملية فحص عملت ضد الشبكة ويقوم هذا البرنامج برسم خط يوضح مسار الهجوم بين مصدره والجهة التي استهدفها.

- أداة tracer: يرسم مسار بين جهازين بإظهار كل التفاصيل عن مسار الرزم والعناوين التي زارها الجاني وتحديد الوقت ويمكن معرفة مكان الخلل والمشاكل التي تعرض لها الشبكة والإختراقات التي حصلت بها.

- أداة netstat تعمل على فحص حالة الاتصال الحالي للبروتوكول TCP/IP كعرض جميع الاتصالات الحالية ومنافذ التنصت والعناوين بصورة رقمية¹.

المحور الثالث: الوسائل الإجرائية للتحقيق الجنائي في الجرائم الرقمية

ويقصد بهذه الوسائل تلك الإجراءات التي من خلالها يتم تنفيذ طرق و أساليب التحقيق التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها.

أولاً: اقتفاء الأثر في الجريمة الرقمية.

في جرائم نظم المعلومات يتم التركيز على اقتفاء الأثر أكثر من التركيز على الشهود في الجريمة التقليدية، فاقفاء الأثر هو فحص جهاز الحاسوب الخاص بالضحية أو المجرم بحثاً عن دليل للإدانة سواء كان بريداً إلكترونياً أو سجل لغرف المحادثة أو غيرها من الأدلة، فتقصي الأثر هو أكثر ما يخشاه المجرم المعلوماتي، فكثير من الوثائق التي يتم نشرها في المواقع الخاصة بالمخترقين تحمل نصائح أولها هي "قم بمسح آثارك COVER YOUR TRACKS" فلو لم يقوم المخترق بمسح آثاره فإنه سيتم القبض عليه حتى ولو قام بالاختراق بشكل سليم.

ثانياً: الإطلاع على عمليات النظام المعلوماتي وأسلوب حمايته.

يجب على المحقق أن يطلع على النظام المعلوماتي ومكوناته من شبكات وتطبيقات وخدمات تقدم للعملاء والإطلاع على عمليات النظام المعلوماتي، كقاعدة البيانات وإدارتها وخطة تأمينها ومعرفة

¹ سليمان مهجع العنزي، المرجع السابق، ص 104.

موارد النظام، والمستفيدين، والملفات، والإجراءات وغيرها ويجب على المحقق معرفة نوعية برامج الحماية وأسلوب عملها والاستفادة من التقارير التي تنتجها.

ثالثا: الاستعانة بالذكاء الصناعي في التحقيق في الجرائم الرقمية.

أثبتت تقنيات الحاسب الآلي نجاحها في جمع الأدلة الجنائية وتحليل القرائن واستنتاج الحقائق، كما يمكن الاستعانة بالذكاء الاصطناعي من خلال حصر الحقائق والاحتمالات والأسباب والفرضيات، ومن ثم استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسب الآلي وفق برامج صممت خصيصا لهذا الغرض، تعتمد على نظرية الاحتمالات وذلك بإعطاء كافة الاحتمالات ثم أكثر الاحتمالات وصولا إلى الاحتمال الأقوى مع إعطاء الأسباب¹.

رابعا: التوقيف خلال فترة التحقيق في الجرائم الرقمية.

تعد وسيلة مهمة من وسائل التحقيق وهو ما يعرف بالحبس الإحتياطي وهو سلب حرية المتهم مدة من الزمن تحددها مقتضيات التحقيق ومصلحته وفق ضوابط حددها القانون وقد ينتهي بالإفراج أو الإدانة، إذ تحقق هذه الوسيلة عدد من الأغراض كبقاء المتهم في متناول سلطة التحقيق للمحافظة على أدلة الجريمة عن محاولة المتهم إخفائها أو طمسها، ومنع التواطؤ بالحيلولة بين اتصال المتهم بباقي شركائه في ارتكاب الجريمة، و بغل يده عن تجهيز شهود نفي مزيفين أو من تهديد شهود الإثبات².

خامسا: إظهار الحقائق في الجريمة الرقمية.

قد تلجأ الجهة المتضررة إلى التبليغ عن جرائم نظم المعلومات أو أن الجهات الأمنية تتحرك عند تلقيها معلومات تشير إلى وقوع جريمة أو ضبط أفراد متلبسين، أو توفر معلومات من خلال النشر على شبكة الانترنت تشير إلى انتشار فيروسات أو وقوع عمليات اختراق، أو قرصنة، فيقوم المحقق بالإجراءات التي تتبع تلقي البلاغ من التأكد من صحة البلاغ، والتحفظ على مكان الجريمة وتأمينه، وتحديد أطراف الجريمة وكل من له صلة بها، وحصر الشهود ومنع مغادرتهم، وحصر الأدلة ورفع الآثار، ويلزم على المحقق إظهار مجموعة من الحقائق في مرحلة جمع الاستدلالات وإثباتها في محضره نظرا لأهميتها في تحديد الجريمة ورسم خطوات البحث في المجهول على النحو التالي:

¹ محمد الأمين البشري، التحقيق في الجرائم المستحدثة، دار الحامد للنشر والتوزيع، الأردن، ط1، 2014، ص 126.

² سليمان مهجع العنزي، المرجع السابق، ص 106.

1- التثبت من توافر أركان الجريمة الرقمية.

إن تحقق وقوع الجريمة المعلوماتية يكون بتوافر ركنين أساسيين وهما الركن المادي¹ ويقصد به الواقعة أو الضرر المادي للجريمة ويتمثل في نشاط الفاعل والنتيجة التي يحققها وعلاقة السبب بينهما، أما الركن المعنوي فيقصد به الإرادة التي اقترن بها الفعل المرتكب ويأخذ صورة القصد الجنائي في الجريمة المتعمدة² وصورة الخطأ غير المقصود بذلك على محقق جمع الاستدلالات أن يظهر أولاً وجود هذه الأركان ثم الجزم بوجود أو عدم وجود الجريمة.

أ- تحديد مكان الجريمة ووصفه

إن التوصل إلى الجاني له أهمية كبيرة في نجاح عملية البحث عن مكان الجريمة الذي توجد فيه الآثار والأدلة الجنائية المتصلة بها، ونتيجة لذلك يعتمد كثير من الجناة إدراكاً منهم لهذه الحقائق إلى نقل هدف الجريمة من مكان إتمام الجريمة وإلقائه في مكان آخر لتضليل المحقق وتعقيد عملية البحث.

ب- تحديد وقت وقوع الجريمة

يتضمن تحديد وقت الجريمة تحديد تاريخ وساعة وقوعها ويتم ذلك من خلال أقوال المجني عليه أو المبلغ أو الشهود وقد يتم عن طريق الخبراء والمتخصصين وهو عنصر هام لتحديد مسؤولية المتهم في ارتكاب الجريمة عند مناقشته عن خط سيره والأماكن والأشخاص الذين كان بصحبته في الفترة المعاصرة لارتكاب الجريمة واكتشاف مدى صدق البلاغ وصحة شهادة الشهود كما أن الوقت في بعض الجرائم يعد ظرفاً مشدداً.

ج- تحديد أسلوب ارتكاب الجريمة الرقمية:

الأسلوب هو الكيفية المتغيرة في طريقة الوصول إلى الهدف والتي سلكها الجاني في ارتكاب جرمته، وللأسلوب أهمية كبيرة في تحديد خطة البحث عن الجاني فلكل مجرم أسلوبه الإجرامي الذي لا يغيره إلا نادراً فمن الأسلوب يستطيع المحقق حصر قطاعاً محدداً من المجرمين يركز البحث عن الجاني بينهم

¹ أنظر أكثر براهيمى جمال، "مكافحة الجرائم الالكترونية في التشريع الجزائري"، المجلة النقدية، جامعة مولود معمري، تيزي وزو، العدد 02، 2016، ص 131.

² أنظر أكثر بن فردية محمد، المرجع السابق، ص 90.

ويكون التسجيل الجنائي مفيدا في تحديد أسلوب ارتكاب الجريمة ومعرفة مجرمين اعتادوا ارتكاب الجرائم المشابهة للجريمة المرتكبة.

د- تحديد أداة ارتكاب الجريمة الرقمية:

يقع على الباحث عبء التفتيش وضبط الأداة التي ارتكبت بها الجريمة الرقمية فهو أمر جوهري لتحديد شخص الجاني ومن هذه الأدوات برامج التنصت على الشبكات، أقراص بدء التشغيل وغيرها.

2- إيضاح الظروف المحيطة بالجريمة الرقمية:

يجب على المحقق إيضاح الظروف التي تحيط بالجريمة الرقمية، ومعرفة ما فيكون بعضها سابقا على وقوع الجريمة مثل سوء سمعة المتهم وسلوكه والشكاوى والمشكلات السابقة التي حدثت بالمؤسسة، والبعض الآخر قد يكون معاصرا لارتكاب الجريمة مثل مكان وجود المتهم حال الجريمة وساعة ارتكاب الجريمة وكذلك هناك ظروف تكون لاحقة على ارتكاب الجريمة مثل تصرفات وسلوك من تحوم حولهم الشكوك على ارتكاب الجريمة¹.

3- تحديد دوافع الجريمة الرقمية:

تعد دوافع الجريمة من الأمور المهمة التي يسعى المحقق لكشفها وتتمثل في السبب والوقائع المادية التي حدثت فأثرت في نفسية الجاني مما أدى إلى بروز الدافع على ارتكابه للجريمة وهو أمر نفسي داخلي مرتبط أساسا بمجموعة من الغرائز الإنسانية وتوجه السلوك لإشباعها وتحديد الدافع في بعض الجرائم يشكل دليلا على ارتكاب الجريمة، كما أن تحديد السبب يكفل حصر دائرة البحث في عدد من الأشخاص كما يحصر للمحقق طرق الكشف عن الجريمة وعدم وضوح السبب ودوافع الجريمة يعد دليل نفي قد يشير إلى براءة من تحوم حوله الشبهات واستبعاده من قائمة الإتهام.

وهناك عدة عوامل تساعد المحقق في تحديد سبب الجريمة نذكر منها.

- نوع الجريمة: غالبا ما يحدد سبب ارتكابها فجريمة سرقة الأقراص يكون سببها الحصول على المعلومات، وجريمة تدمير المعلومات سببها الانتقام.

¹ سليمان مهجع العنزي، المرجع السابق، ص 109.

- المعاينة تشكل عاملا هاما لكشف سبب الجريمة فمعاينة مسرح الجريمة يسفر عن اكتشاف الجريمة، فمثلا وجود بعض البرامج المزروعة كالفيروسات تشير في حد ذاتها إلى أن الدوافع من وراء هذه الجريمة هو الإنتقام أو العدوانية.

- أهل الخبرة: أحد أعوان الباحث الذين يرشدونه كثيرا عن الأسباب المحتملة لوقوع الحادث ومثال ذلك تقصي آثار الجاني وأساليبه والأدوات التي استخدمها قد يحدد سبب الجريمة¹.

سادسا: إتباع القواعد الفنية لكشف الجريمة

يقوم المحقق في سبيل الكشف عن الجريمة بالإجراءات اللازمة المتمثلة في المعاينة والتفتيش وانتداب الخبراء وسماع الشهود واستجواب أطراف الجريمة وجمع التحريات ويجب على المحقق أمام الأدلة الضخمة التي أمامه أن يقوم بـ:

- مراعاة الاحتمالات الشائعة في الجرائم: كاحتمال عدم وجود جريمة أصلا أو احتمال كذب البلاغ أو تصويره على غير حقيقته أو أن الجريمة وقعت فجأة ونتيجة لظروف عارضة.

- تقدير احتمالات وقوع الجريمة: ويقصد بها الخطوات التي يتصور المحقق أن الجريمة قد سارت فيها منذ مرحلة نشوء أسبابها والتفكير فيها والتحضير لها ثم تنفيذها معتمدا في تلك على الأدلة والوقائع التي جمعها كما يترتب عليه استبعاد عدد من الوقائع.

- فحص الاحتمالات: بعد حصر المحقق الاحتمالات التي يمكن أن تقع على أساسها الجريمة، وذلك في ضوء مدلولات الأدلة والحقائق التي استنتجها منها وما استبعده من احتمالات وما استخلص من تصورات لكيفية ارتكاب الجريمة يقوم بعدها بفحص كل احتمال من هذه الاحتمالات متبعا في ذلك القواعد الفنية رسم خطة البحث والبدء بالاحتمال الأقوى، وعدم التشبث باحتمال واحد، وعدم التعجل للوصول إلى نتيجة إيجابية من فحص الاحتمال².

الخاتمة:

إن التحقيق في الجريمة الرقمية يختلف تماما عن نظيره في الجرائم المعروفة في العالم التقليدي وتتجلى هذه الخصوصية في عدم إمكانية تطبيق أحكام الجرائم التقليدية على الجرائم المرتكبة في العالم

¹ محمد الأمين البشري، التحقيق في الجرائم المستحدثة، المرجع السابق، ص 124.

² سليمان مهجع العنزي، المرجع السابق، ص 111.

الافتراضي بأصلها وإنما تأخذ طابع خاص وذلك نظرا للطابع المستحدث لهذه الجريمة المتسمة بالتشعب.

أيضا هذه الخصوصية للجرائم المرتكبة عبر الإنترنت جعلت مختلف الدول و الهيئات والمنظمات الدولية و الإقليمية تدرك مدى خطورتها ومدى التحديات التي تفرضها عليها مما أدى بها إلى المسارعة من أجل وضعها في إطار قانوني يمكن من خلاله وضع طرق ناجعة وفعالة لمكافحةها.

لذلك خالصنا إلى جملة من النتائج نذكر منها ما يلي على سبيل المثال لا الحصر:

1- إن مفهوم الجرائم المعلوماتية ينصرف إلى الأفعال التي تشكل اعتداء على نظم المعالجة الآلية للمعطيات التي تستهدف البيئة الإلكترونية وعليه فإن محل الجريمة التقليدية يختلف تماما عن محل الجريمة الرقمية الذي يكون في شكل افتراضي.

2- من بين الوسائل التي تساعد المحقق في التحري عن الجرائم الإلكترونية هي عناوين الانترنت، كبروتوكول الانترنت IP الموجودة بكل جهاز مرتبط بالانترنت و الذي يساعد على تحديد مكان الحاسب الآلي.

3- المحقق في الجريمة المعلوماتية يجب أن يكون على معرفة ودراية بالجوانب الفنية وكذا التقنية للحاسب الآلي والانترنت.

4- توسيع دائرة إختصاص كل من قضاة التحقيق وضباط الشرطة القضائية في مجال متابعة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والبيانات.

5- تفتيش المنظومة المعلوماتية من أصعب إجراءات البحث و التحري عن الجريمة ومرتكبيها، الأمر الذي يتطلب خبرة واسعة وكفاءة عالية من قبل القائمين به، كما يتطلب في الوقت نفسه تعاونا دوليا فعالا لمحاصرة هذه الجرائم و ملاحقة مرتكبيها، لأن التفتيش في البيئة الافتراضية يختلف كثيرا عن مفهومه التقليدي وإن كانت تحكمه في بعض جوانبه القواعد المألوفة في قانون الإجراءات الجزائية مثل تفتيش المساكن و المجال الذي توجد فيه أجهزة الإعلام الآلي.

6- المعالجة في الجريمة الإلكترونية أقل أهمية منها في الجرائم العادية، لقلة الآثار المادية بينما الخبرة تعتبر من أهم إجراءات التحقيق في الجرائم الإلكترونية وهذا ما تستدعيه طبيعة هذه الجريمة، كونها تعتمد بالدرجة الأولى على وسائل مستحدثة.

07- كما أضاف المشرع في تعديله وسيلة جديدة والمتمثل في التسرب وهو إجراء خطير سبقته إليه بعض التشريعات منها التشريع الفرنسي وهو يهدف للكشف عن الجرائم الخطيرة والمتورطين فيها

وتحديد هويتهم ومناطق نشاطهم والوسائل التي يستعملونها وضبط كل ماله علاقة بهذه الجرائم من أدلة أو قرائن.

وبناء على هذه النتائج نستخلص مجموعة من الاقتراحات نذكر منها ما يلي:

1-إنشاء دورات تكوينية لتدريب و تأهيل قضاة التحقيق وضباط الشرطة القضائية في مجال نظم المعلوماتية والحواسيب، لان دور القاضي مهم في توجيه مسار القضايا، فإذا كان القاضي غير ملم بالجوانب التقنية الحديثة للحاسب الآلي و الانترنت، فانه لا يستطيع تقدير مدى خطورة المجرم المعلوماتي، وعليه يصدر أحكام غير متكافئة مع الجريمة المرتكبة.

2-نقترح إدراج المراسلات الالكترونية صراحة ضمن إجراء اعتراض المراسلات التي أضحت وسيلة فعالة في ارتكاب الجرائم الخطيرة في قانون الإجراءات الجزائية ليتماشى مع جاء في به المشرع في القانون 04/09 السالف الذكر.

3-دعوة المشرع إلى تعديل المادة 56 مكرر 18 من القانون 22/06 المعدل و المتمم لقانون الإجراءات الجزائية و جعلها تسمح لضباط الشرطة القضائية المسؤول عن عملية التسرب أو العون المتسرب الإدلاء بشهادته عن طريق الشاشة الالكترونية مع إمكانية تغيير الصوت والصورة.

قائمة المصادر و المراجع:

أولاً: المصادر

1. القانون رقم: 09-04، المؤرخ في: 05/08/2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام الآلي والإتصال ومكافحتها، ج.ر عدد 47، الصادرة في: 2009/08/16.

2. الأمر رقم: 66-155 المؤرخ في: 08/06/1966، المتضمن قانون الإجراءات الجزائية الجزائري، ج.ر عدد 48، الصادرة في: 10/06/1966، المتمم حسب آخر تعديل له بالأمر رقم: 17-07، المؤرخ في: 17/03/2017.

3. الأمر رقم: 66-156، المؤرخ في: 08/06/1966، المتضمن قانون العقوبات الجزائري، ج.ر عدد 49، الصادرة في: 11/06/1966، المتمم حسب آخر تعديل له بالأمر رقم: 16/02، المؤرخ في: 19/06/2016.

4. المرسوم الرئاسي رقم: 15-261، المؤرخ في: 2015/10/08، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر عدد 53، الصادرة في: 2015/10/08.
5. المرسوم التنفيذي رقم: 348/06 المؤرخ في: 2006/10/05 المتعلق بالتنظيم القضائي، ج.ر عدد 63 الصادرة بتاريخ: 2006/10/08، المعدل والمتمم بالمرسوم رقم: 267/16.
6. إتفاقية بودابست لمكافحة الجرائم المعلوماتية والموقعة في العاصمة المجرية بودابست في 23 نوفمبر 2001 المتعلقة بالإجرام الفضائي.

ثانيا: الكتب

1. محمد الأمين البشري، التحقيق في الجرائم المستحدثة، دار الحامد للنشر والتوزيع، الأردن، ط1، 2014.
2. حسن طاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ط1، 2000.

ثالثا: البحوث الجامعية

أ- أطروحات الدكتوراه

1. بن فردية محمد، "الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية"، شهادة الدكتوراه، جامعة الجزائر، كلية الحقوق، الجزائر، 2015.

ب- مذكرات الماجستير

1. سليمان مهجع العنزي، "وسائل التحقيق في جرائم نظم المعلومات"، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العالية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003.

رابعا: الملتقيات

1. محمد الأمين البشري، "التحقيق في جرائم الحاسب الآلي"، (مؤتمر القانون والكمبيوتر والانترنت)، مجلد 3، الفترة من 01 إلى 03 ماي 2000.

خامسا: المجالات:

- براهيمي جمال، "مكافحة الجرائم الالكترونية في التشريع الجزائري"، المجلة النقدية، جامعة مولود معمري، تيزي وزو، العدد 02، 2016.

القواعد الإجرائية الحديثة لمواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

د/ بن خليفة إلهام

أستاذة محاضرة (أ) - كلية الحقوق والعلوم السياسية

جامعة الشهيد حمة لخضر - الوادي

مقدمة:

يرى بعض الفقه¹ بأنّ القواعد الإجرائية التقليدية أو المتعلقة بالتحريات والتحقيقات، تبدو قاصرة إزاء ملاحقة مرتكب الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، لما تتطلبه هذه الأخيرة من إجراءات خاصة تتناسب والطبيعة التقنية للدليل إثباتها والذي اكتسبها من الطبيعة التقنية لهذه الجريمة، ذلك أن الدليل أثر يُؤلّد أو حقيقة تنبعث من نوع الجريمة المرتكبة، إذ يتطلب الأمر دائماً تحقيق تناغم بين الدليل وطبيعة الجريمة التي يُولد منها، لذلك نجد أنّ أجهزة العدالة الجنائية سوف تتعامل في ممارستها لحق المجتمع في الدفاع عن كيانه ضد الإجرام مع أشكال مستحدثة من الأدلة تُصعّب مهمتها في إثبات هذه الجريمة وهي الأدلة في الشكل الإلكتروني أو كما يُطلق عليها الأدلة الرقمية أو الإلكترونية الأمر الذي دفع بالمتجمع الدولي إلى حتّ الدول على وضع تدابير وإجراءات تتناسب مع طبيعة الجرائم التقنية وطبيعة أدلتها.

ولقد أوردت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي صادقت عليها الجزائر سنة 2014² مجموعة من الإجراءات الخاصة تلتزم الدول الأطراف بأنّ تتبناها في تشريعاتها الداخلية، وتُطبقها على الجرائم المنصوص عليها في الاتفاقية وعلى أيّ جريمة أخرى ترتكب بواسطة تقنية

¹ انظر ذلك في: د/ أيمن رمضان محمد أحمد، الحماية الجنائية للتوقيع الإلكتروني، رسالة دكتوراه، (منشورة)، دار النهضة العربية، القاهرة 2011، ص: 262، ود خيرت علي محرز، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، القاهرة 2012، ص: 09.

² مرسوم رئاسي رقم 14-252 مؤرخ في 13 ذي القعدة عام 1435 الموافق 8 سبتمبر سنة 2014 يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المخررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، منشور في الجريدة الرسمية للجمهورية الجزائرية، العدد 57، المؤرخة في: 4 ذو الحجة عام 1435 الموافق 28 سبتمبر سنة 2014، ص: 04 ومايليها.

المعلومات وعلى جمع الأدلة في الشكل الإلكتروني؛ وتتمثل هذه الإجراءات في التحفظ العاجل على البيانات المخزنة والتحفيز العاجل والكشف العاجل لبيانات المرور وأمر تسليم المعلومات والتجميع الفوري لبيانات المرور واعتراض معطيات المحتوى.

ويلاحظ أن الإجراءات الواردة في الاتفاقية العربية قد أوردتها المشرع الجزائري في قوانينه الوطنية من قبل أن يتم وضع هذه الاتفاقية سنة 2010، ولقد نص على بعض منها في قانون الإجراءات الجزائية، والباقي في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الاتصال والإعلام ومكافحتها¹، وتتمثل هذه الإجراءات في المراقبة الإلكترونية والتسرب واعتراض المراسلات السلكية واللاسلكية وحفظ المعطيات المتعلقة بحركة السير.

والإشكالية المطروحة في هذا الصدد تتمثل في هل الإجراءات القانونية المستحدثة كافية بذاتها لمواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال؟ ولقد قسمنا البحث في هذه الإشكالية إلى محورين كما يلي:

المحور الأول: القواعد الإجرائية الحديثة في قانون الإجراءات الجزائية

المحور الثاني: القواعد الإجرائية الحديثة في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المحور الأول: القواعد الإجرائية الحديثة في قانون الإجراءات الجزائية

في إطار إصلاح المنظومة التشريعية والقضائية، وضمناً لفعالية وسرعة التحقيق في القضايا المتعلقة بالجرائم المستحدثة، استحدث المشرع الجزائري في قانون الإجراءات الجزائية إجراءات جديدة تتمثل في التسرب واعتراض المراسلات السلكية واللاسلكية وذلك بموجب القانون رقم 06-22 المعدل لقانون الإجراءات الجزائية² وسنتناول بالتفصيل هذه الإجراءات في النقاط التالية:

¹ قانون رقم 04/09 مؤرخ في 14 شعبان عام 1430 هـ الموافق 05 غشت سنة 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والمنشور في الجريدة الرسمية للجمهورية الجزائرية، العدد 47، المؤرخة في 25 شعبان عام 1430 هـ الموافق 16 غشت 2009، ص: 05 وما يليها.

² قانون 06-22 مؤرخ في 29 ذي القعدة 1427 الموافق 20 ديسمبر 2006، يتم الأمر 66-156 المؤرخ في 18 صفر 1386 الموافق 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، منشور في الجريدة الرسمية للجمهورية الجزائرية، العدد 84، الصادرة بتاريخ 4 ذي الحجة 1427 الموافق 24 ديسمبر 2006، ص: 04 وما يليها.

أولاً: التسرب

نص المشرع الجزائري على التسرب في المواد من 65 مكرر 11 إلى 65 مكرر 18، وسنعرّج عن مفهومه وشروطه كما يلي:

أ- مفهوم التسرب:

عرّف المشرع الجزائري التسرب في المادة 65 مكرر 12 كما يلي: (يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه بارتكابهم جنائية أو جنحة بإيهاهم أنّه فاعل معهم أو شريك لهم أو خاف). وعرفه الفقه¹ بأنه تقنية من تقنيات التحري والتحقيق الخاصة تسمح لضابط أو عون الشرطة القضائية بالتوغل داخل جماعة إجرامية وذلك تحت مسؤولية ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرب بهدف مراقبة أشخاص مشتبه فيهم، وكشف أنظمتهم الإجرامية وذلك بإخفاء الهوية الحقيقية، وتقديم المتسرب على أنّه فاعل أو شريك.

ويرى البعض² أنّ هذه العملية عملية معقّدة، نظرًا لكونها تنطوي على أنّ القائم بها يربط علاقات ضيقة مع المجرمين مع حفاظه على السر المهني من أجل تحقيق الغرض النهائي من العملية، وأنها تتطلب الاضطرار للمشاركة المباشرة في نشاط المجموعات الإجرامية من أجل قبوله بينهم. والتسرب في نطاق الجريمة المتصلة بتكنولوجيات الإعلام والاتصال يمكن أن يُتصور في دخول المتسرب للنظام المعلوماتي واشتراكه في محادثات الدردشة أو حلقات النقاش مستخدمًا في ذلك أسماء أو صفات مستعارة أو وهمية، ويظهر بمظهر عادي كأنّه منهم.

ب- شروط التسرب:

ينطوي إجراء التسرب على المساس بالحريات الفردية وحقوق الإنسان لذا نجد أن المشرع الجزائري وضع له ضوابط أو شروط تكون بمثابة ضمانات يتعين مراعاتها عندما تقتضي ضرورة التحقيق للقيام بمثل هذا الإجراء وتمثل هذه الشروط فيما يلي:

¹ عبد الرحمن خلفي، محاضرات في قانون الإجراءات الجزائية، دار الهدى، الجزائر 2010، ص: 74-75.

² رشيدة بوك، جرائم الاعتداء على نظم المعالجة الآلية للمعطيات، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت 2012، ص: 434.

1- أن تتم هذه العملية بإذن من وكيل الجمهورية المختص إقليمياً أو من طرف قاضي التحقيق بعد إخطار وكيل الجمهورية، وهو ما جاء في المادة 65 مكرر 11.

2- يجب أن يكون الإذن مكتوباً ومسبباً، وإذا خلا من هذا الشرط فإنّ التسرب قد يقع تحت طائلة البطلان، ويجب أن يتضمن التسيب العناصر التي يستند إليها القاضي الأمر به، مع ذكر الجريمة موضوع التسرب، وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، وهو ما ورد في الفقرات الأولى والثانية من المادة 65 مكرر 15.

3- يجب ألاّ تتجاوز المدة المطلوبة لعملية التسرب الأربعة أشهر، والتي يمكن تجديدها حسب مقتضيات التحري والتحقيق، والتجديد يكون بإذن مكتوب ومسبب ويكون بنفس المدة وهي ألاّ تتجاوز أربعة أشهر، كما يجوز للقاضي الذي أمر بالتجديد أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة، وهو ما حدده المشرع في الفقرات الثالثة والرابعة والخامسة من المادة 65 مكرر 15.

4- يشترط المشرع كذلك في المادة 65 مكرر 13 وجود تقرير مسبق يحره ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب يتضمن العناصر الضرورية لمعينة الجرائم غير تلك التي تُعرض المتسرب للخطر، وذلك من أجل أن يطلع القاضي بشكل مُفصل عن ظروف القضية ومتطلباتها.

5- وحسب المشرع الجزائري وطبقاً للمادة 65 مكرر فإنّ إجراء التسرب، يتخذ في حال التحقيق أو التحريّ في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد.

ج- آثار التسرب:

تترتب عن القيام بعملية التسرب عدة آثار تتمثل في:

1- تسخير الوسائل المادية والقانونية:

حسب نص المادة 65 مكرر 14 فإنه يُمكن لضباط وأعوان الشرطة القضائية المرخص لهم بإجراء عملية التسرب، وكذا الأشخاص الذين يسخروهم لهذا الغرض دون أن يكون مسؤولين جزائياً القيام بما يأتي:

- اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد وأموال أو منتجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.
- استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال، وهذا يعني أن المتسرب سوف يقوم باستخدام وسائل غير مشروعة، فمثلاً في إطار جريمة التزوير في المحررات الإلكترونية كتزوير جواز للسفر البيومتري، فإنه يحتاج لاصطناع هذا المحرر إلى جهاز خاص يحوزه دون المرور على الإدارة المختصة لإبقاء أعماله ضمن السرية المطلوبة¹.

2- الإعفاء من المسؤولية الجنائية:

تُعتبر عملية التسرب خارج الإذن أو السماح بها قانوناً أفعالاً مجرمة، وعليه يمكن اعتبار القيام بها في إطار القانون سبباً من أسباب الإباحة وفقاً لنص الفقرة 01 من المادة 39 من قانون العقوبات الجزائي، ويترتب على ذلك إعفاء المتسرب من المسؤولية الجزائية عن الأعمال غير المشروعة التي يقوم بها في إطار هذه العملية القانونية، وهو ما ورد صراحة في المادة 65 مكرر 14 والمادة 65 مكرر 17.

3- إحاطة العملية بالسرية التامة:

يستشف أثر إحاطة العملية بالسرية التامة من المادتين 65 مكرر 16 و65 مكرر 18 ويستفاد من النصين ما يلي:

- وجوب عدم إظهار الهوية الحقيقية للمتسرب في أي مرحلة كانت عليها الدعوى العمومية، وإذ تراءى للقاضي سماع المتسرب فإنه لا يُكشف عن هويته، بل يسمع ضابط الشرطة القضائية الذي تُجرى عملية التسرب تحت مسؤوليته دون سواه.
- أنّ المشرع يعاقب بالحبس من سنتين إلى 05 سنوات وبغرامة من 50.000 دينار جزائري إلى 200.000 دينار جزائري كل من كشف عن هوية المتسرب.
- أنّه إذا أدى الكشف عن الهوية إلى أعمال عنف ضد المتسربين أو أزواجهم أو أبنائهم أو أصولهم المباشرين، فتُشدّد العقوبة لتصبح سجن من 05 سنوات إلى 10 سنوات والغرامة من 200.000 دينار جزائري إلى 500.000 دينار جزائري.

¹ رشيدة بوكري، المرجع السابق، ص: 438.

ثانيا: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

نص المشرع الجزائري على إجراء الاعتراض في المواد 65 مكرر 5 إلى 65 مكرر 10 من قانون الإجراءات الجزائية، والسؤال المطروح ماذا يُقصد بالاعتراض، وما هي أحكامه؟

أ- مفهوم اعتراض المراسلات:

لم يضع المشرع الجزائري تعريف لإجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، ويعرف البعض¹ الاعتراض بأنه عملية مراقبة سرّية المراسلات السلوكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه في ارتكابهم أو مشاركتهم في ارتكاب الجريمة.

إذ تتم المراقبة عن طريق الاعتراض أو التسجيل أو النسخ للمراسلات والتي هي عبارة عن بيانات قابلة للإنتاج أو التوزيع أو التخزين أو الاستقبال أو العرض.

أمّا تسجيل الأصوات والتقاط الصور فيقصد بها تسجيل المحادثات الشفوية التي يتحدث بها الأشخاص بصفة سرّية أو خاصة في مكان عام أو خاص، وكذلك التقاط صورة لشخص أو عدة أشخاص يتواجدون في مكان خاص².

يتبيّن أنّ إجراءات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور هي عبارة عن إجراءات تتخذ دون علم أصحابها في أيّ مكان من الأماكن العامة أو الخاصة، وهي إجراءات تنطوي على المساس بسرية المراسلات والاتصالات وحرمة الحياة الخاصة، وهي من ضمن حقوق الإنسان التي كفلتها الدساتير والتشريعات العقابية، ويُقصد من ذلك أن السلطات القضائية يجوز لها أن تعترض وتسجل وتلتقط كل المراسلات المرسلة عبر الاتصالات إن كانت ضرورة التحقيقات تستدعي ذلك³، وعلى حد قول الفقه القانوني الحديث⁴ يمكن تغليب مصلحة المجتمع في التصدي للجريمة عن المصلحة الفردية في الخصوصية والسريّة لغاية تحقيق الأمن والعدالة والسلامة لهذا الفرد.

¹ عبد الرحمن خلفي، المرجع السابق، ص: 72.

² نفس المرجع، ص: 73.

³ Christiane Féral – Schuhl, Cyberdroit, le droit à l'épreuve de l'internet, Quatrième édition, Dalloz, Paris 2006, p: 660.

⁴ زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر 2011، ص: 158.

وتكمن أهمية إجراء الاعتراض في كون أنّ التكنولوجيات المعلوماتية قادرة على نقل كميات ضخمة من البيانات في شكل نصوص أو صور أو أصوات، فإنّها في المقابل تُقدم إمكانيات واسعة لارتكاب الجرائم، والتي تأخذ شكل بثّ محتوى غير قانوني كمستند يحتوي على بيانات مزورة، إذ أنّ مثل هذه الجرائم تفترض النقل والاتصال، وعليه فمن غير الممكن تحديد الوقت الفعلي لهذه البيانات غير المشروعة إلّا من خلال اعتراض محتوى المستند، وإن لم يتم تدارك هذه البيانات بالاعتراض سوف تقع الجريمة تامة، وبذلك يعد الاعتراض من أهم الإجراءات التقنية اللازمة لتعقب الدليل في الجريمة المتصلة بتكنولوجيات الإعلام والاتصال والمحافظة عليه¹.

ب- أحكام اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

أورد المشرع الجزائري عدة قيود حال القيام بهذا الإجراء تتمثل في:

- 1- يجب أن تتخذ هذه الإجراءات حيال جرائم محددة على سبيل الحصر، وهي التي ذكرناها سابقا بمناسبة البحث في التسرب وهو ما أورده المشرع الجزائري في المادة 65 مكرر5.
- 2- ضرورة أن تتم هذه الإجراءات بناءً على إذن مكتوب من وكيل الجمهورية المختص إقليمياً أو من قاضي التحقيق وتحت مراقبته المباشرة في حالة فتح تحقيق قضائي، وهذا وفقاً للمادة 65 مكرر5؛ وحسب المادة 65 مكرر7 فإنّه يجب أن يتضمن الإذن المكتوب كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة، والجريمة التي تُبرر اللجوء إلى هذه التدابير ومدتها.
- 3- يجب أن يكون الإذن لمدة أقصاها 04 أشهر قابلة للتجديد، حسب مقتضيات التحري والتحقيق، حيث أنّ التجديد يكون بإذن مكتوب ومتضمن العناصر السابقة ومدة التجديد وهو ما جاء في الفقرة الأخيرة من المادة 65 مكرر7.
- 4- إمكانية الدخول إلى كل الأماكن العامة والخاصة بغير علم أصحابها وموافقتهم وفي كل وقت وهو ما أشار إليه المشرع في المادة 65 مكرر5.

¹ د/ هلال عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية اتفاقية بودابست الموقعة في 23 نوفمبر 2001، دار النهضة العربية، القاهرة 2006، ص: 271- 272.

5- يمكن للقائم بالاعتراض المأذون به أن يُسخر كلّ عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلوكية أو اللاسلوكية للتكفل بالجوانب التقنية للعملية، وهو ما جاء في المادة 65 مكرر8.

6- حسب المواد 65 مكرر9، و65 مكرر10 فإنّ القائم بالاعتراض يحزر محضراً بعد الانتهاء من هذه العملية يُضمن فيه محتوى العملية والترتيبات التقنية المتخذة، ويذكر فيه تاريخ وساعة بداية ونهاية العملية، ويقوم بنسخ المراسلات أو المحادثات أو الصور المسجلة والمفيدة في إظهار الحقيقة في محضر يودع بالملف وتنسخ وترجم المكالمات التي تتم باللغة الأجنبية عند الاقتضاء بمساعدة مترجم يُسخر لهذا الغرض.

المحور الثاني: القواعد الإجرائية الحديثة في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

من بين الإجراءات الحديثة التي نصت عليها الاتفاقيات والتشريعات الداخلية إجرائي المراقبة الإلكترونية، والتزامات مقدمي الخدمات، وفيما يلي نبحث في مفهوم وأحكام كل إجراء طبقاً لقانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها كما يلي:

أولاً: إجراء المراقبة الإلكترونية

استحدثت المشرع إجراء المراقبة الإلكترونية بموجب قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فماذا يقصد بهذا الإجراء؟ وما هي أحكامه التي تراعي المصالح المحمية؟

أ- مفهوم إجراء المراقبة الإلكترونية:

لم يتعرّض المشرع الجزائري لتعريف المراقبة الإلكترونية، ولقد تصدى الفقه لذلك وعرفها بأنها مراقبة شبكة الاتصالات¹، أو هو العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع بيانات

¹ La Cybersurveillance: " est la surveillance des réseaux des télécommunications ..." Maximilien dosté Amégée, la cybersurveillance et le secret professionnel, paradoxes ou contradictions? Mémoire D.E.A Université Paris, Nanterre, 2002, p:50.

مشار إليه في: رشيدة بوكري، المرجع السابق، ص:370.

أو معلومات عن المشتبه فيه، سواء أكان شخصاً أو مكاناً أو شيئاً حسب طبيعته مرتبط بالزمن (التاريخ، الوقت) لتحقيق غرض أمني أو لأيّ غرض آخر¹.

يتبين من التعريفين أنّ إجراء المراقبة الإلكترونية هو من إجراءات جمع الدليل في الشكل الإلكتروني عن المشتبه فيه، ويقوم به مراقب ذي كفاءة تقنية عالية في المجال الإلكتروني، ويستخدم في هذه المراقبة التقنية الإلكترونية عبر شبكة الانترنت.

والشيء المراقب هو شبكة الانترنت، حيث يُراقب من خلالها الاتصالات الإلكترونية للمشتبه فيه التي تتم عن طريق الانترنت، كمراسلاته مثلاً عبر البريد الإلكتروني، والجدير بالذكر أن شرطة أمريكا الشمالية تعد قائمة بالأشخاص المشتبه بهم والمبحوث عنهم توضع في ملف مركزي وترسل إلى مئات المواقع، حيث تسمح هذه التقنية بالوضع اليومي للصور في الواجهة، مما تساعد جهات البحث في عملية المراقبة، كما أنّ هذه الطريقة تستلهم رجال التحريات الأولية لأنّها بكل بساطة تنشر عبر الانترنت آراء للبحث؛ كما يراقب القائم بإجراء المراقبة الإلكترونية البيانات غير المشروعة.

ويتطلب مصطلح "يراقب" في المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية أن يكون مطبقاً فقط على الاتصالات التي يتم التقاطها أثناء بثها وليس الحصول على اتصالات سلكية أو الكترونية مخزنة، أي أنّ المراقبة هي اكتساب معطيات في الزمن الفعلي أثناء البث بين أطراف الاتصال، فالذي يطلّع لاحقاً على نسخة من اتصال مخزن لا يعد مراقباً للاتصال².

وتعني التقنية الإلكترونية المستخدمة في المراقبة مجموعة الأجهزة المتكاملة مع بعضها بغرض تشغيل مجموعة من البيانات المتعلقة بالمجرمين وفق برنامج موضوع مسبقاً لتحديدهم من أجل ضبطهم وتفتيشهم وجمع الأدلة قبلهم لإثبات إدانتهم وتقديمهم للمحاكمة³، وهناك العديد من هذه التقنيات

¹ مصطفى محمد مرسى، المراقبة الإلكترونية عبر شبكة الانترنت، مرجع سابق، ص192، مشار إليه في: نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية 2007، ص:198.

² للاطلاع أكثر انظر: د/ عمر محمد بن يونس، الإجراءات الجنائية عبر الانترنت في القانون الأمريكي، (دون دار النشر)، (دون بلد النشر)، 2005، ص:366 وما يليها.

³ د/ مصطفى محمد مرسى، المراقبة الإلكترونية عبر شبكة الانترنت، مرجع سابق، ص:205، مشار إليه في: نبيلة هبة هروال، المرجع السابق، ص، ص: 200-201.

أكدت التجارب في الولايات المتحدة الأمريكية أثرها الفعال في الرصد المبكر للاعتداءات المحتملة، كما أنها تستخدم على المستوى الدولي لمكافحة الجرائم عبر الوطنية.

ب- أحكام المراقبة الإلكترونية:

يحمي المشرع الجزائري على غرار التشريعات الأخرى الحق في الخصوصية وما يتفرع عنه من حرية المراسلات وسرية الأحاديث الخاصة وذلك عن طريق تجريمه لكل سلوك من شأنه الاعتداء على حرمة الحياة الخاصة في المادة 303 مكرر من قانون العقوبات والتي جاء فيها أنه: (يعاقب بالحبس 06 أشهر إلى ثلاث سنوات وبغرامة من 50.000 دينار جزائري إلى 300.000 دينار جزائري، كل من تعمد المساس بجرمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك:

1- بالتقاط أو تسجيل أو نقل المكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.

2- بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه...

ويشمل مصطلح المراسلات، الاتصالات السلكية واللاسلكية مثل المحادثات التليفونية سواء التي تتم في الهاتف الثابت أو الهاتف المحمول، وكذا الاتصالات الإلكترونية التي تشمل معظم اتصالات الانترنت بما في ذلك مراسلات البريد الإلكتروني¹.

غير أنّ المشرع الجزائري أباح الاعتداء على هذه الحرمة بسبب وقاية أفراد المجتمع من خطورة بعض الجرائم، وذلك في المادتين 3 و4 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ومن خلال استقراء هذه المواد نجد أن المشرع أحاط هذه الإباحة ببعض الضمانات القانونية الفعالة لحماية الحرية الفردية، وحماية حق الإنسان في سرية اتصالاته بمختلف أنواعها وتمثل هذه الضمانات في:

1- إباحة المراقبة بإذن القانون:

نصت المادة 03 من القانون السابق الذكر على إباحة المراقبة الإلكترونية كما يلي: (مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، ووفقاً للقواعد المنصوص عليها في قانون الإجراءات الجزائية، وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها...).

¹ للاطلاع أكثر على الموضوع، انظر: د/ عمر محمد بن يونس، المرجع السابق، ص: 361 وما يليها.

يُلاحظ من خلال هذا النص أنّ المشرع عندما يقول وفقاً للقواعد المنصوص عليها في قانون الإجراءات الجزائية، وفي هذا القانون، فإنه يقصد بذلك بالنسبة للقانون الأول، وهو الرجوع للشروط المنصوص عليها بصفة عامة في إجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، التي تعتبر كما سبق الذكر عبارة عن مراقبة سرية ولكنها تكون في إطار المراسلات السلكية واللاسلكية أما المراقبة الإلكترونية المنصوص عليها في هذا القانون فهي مراقبة الاتصالات الإلكترونية.

وهذا ما يؤدي إلى القول أنّ مراقبة الاتصالات الإلكترونية لا يسمح بها إلا في إطار الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ولا تكون في باقي الجرائم الخطيرة المحددة على سبيل الحصر، والمذكورة آنفاً حيث يمكن فيها فقط مراقبة الاتصالات السلكية واللاسلكية أي الاعتراض. ولهذا فإننا نرى أن يُعدل المشرع الجزائري المادة 65 مكرر 5 لتشمل جميع الاتصالات سواء أكانت إلكترونية أو تليفونية، وفيما يخص المراقبة المنصوص عليها في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، يحذف موادها ويحيل بشأنها إلى الاعتراض المنصوص عليه في قانون الإجراءات الجزائية وهذا حتى لا تكون هناك ازدواجية في النصوص ويكون التشريع الداخلي متوافق مع الاتفاقية العربية لمكافحة تقنية المعلومات التي صادقت عليها الجزائر، لأنها تنص في المادة 39 فقط على اعتراض معلومات المحتوى التي تثبت عن طريق الاتصالات بواسطة تقنية المعلومات، ويدخل في مفهوم تقنية المعلومات وفقاً للفقرة "01" من المادة الثانية من نفس الاتفاقية أنّها تشمل جميع المدخلات والمخرجات المرتبطة بالمراسلات سواء السلكية أو اللاسلكية وسواء عن طريق الشبكة.

وفيما يتعلق بالقانون الثاني فيقصد به الرجوع إلى المادة 05 من ذات القانون، والتي تقضي بالأحكام الموالية.

2- الضرورة الملحة المرخصة لإجراء المراقبة الإلكترونية:

بالرجوع إلى نص المادة 04 السابقة الذكر ووفقاً للمناقشات التي دارت خلال الأعمال التحضيرية لهذا القانون¹ يتضح أنّ ضابط الوقاية من وقوع بعض الجرائم يعتبر السند الشرعي المبرّر للمراقبة، ومن قبيل ذلك أن تكون هناك معلومات كافية تنذر باحتمال اعتداء على منظومة معلوماتية على

¹ انظر ج.م.ر الفقرة التشريعية السادسة، الدورة العادية الرابعة، الجلسة العلنية المنعقدة يوم السبت 27 يوليو 2009، السنة الثالثة، رقم 122، ص: 14-24، انظر ذلك في: رشيدة بوكري، المرجع السابق، ص: 374.

نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو أن هناك معلومات تنتقل فضائياً تنذر بوقوع اعتداء على أمن الدولة، وفي هذه الحالة يتم الترخيص بالمراقبة الإلكترونية.

3- حصر القيام بالإجراء في جرائم إلكترونية معينة:

تنص المادة 4 الفقرة الأولى الحالات التي تتيح اللجوء إلى عملية مراقبة الاتصالات الإلكترونية، وهي كالتالي: (يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 03 أعلاه في الحالات الآتية:

أ- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة، أو الاقتصاد الوطني.

ج- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

د- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة...).

يستنتج من هذه الفقرة مبدئياً أن الحالات التي تجوز فيها أو يرخّص فيها القيام بالمراقبة هي تلك الجرائم التي تمس بالمصالح الأساسية في الدولة والجرائم الموصوفة بأفعال إرهابية أو تخريبية والماسة بأمن الدولة كما يرخّص بالمراقبة في حالة عدم الحصول على دليل إدانة وحالة المساعدة القضائية المتبادلة.

وما يلاحظ في المادة أنّ الفقرة الأولى "أ" لم تحدد إن كانت تلك الجرائم ترتكب بواسطة تقنية المعلومات، أم ترتكب كجريمة تقليدية.

ويلاحظ أيضاً وفقاً للفقرة الأولى "ج" و"د" أنّ المراقبة تكون في كل الجرائم سواء أكانت عادية أو إلكترونية، والمهم هو عدم تمكن جهات التحقيق من الوصول إلى نتيجة سواء أكانت للإدانة أو للتبرئة. وكما أنّها تكون لكل الجرائم في إطار المساعدة القضائية المتبادلة، إذ لم تحدد أيّ الجرائم التي تسمح فيها بالمراقبة في إطار المساعدة القضائية الدولية المتبادلة.

وعليه ما يمكن استنتاجه هو أنّ المراقبة الإلكترونية يمكن أن تتم في كل الجرائم، ولهذا ينبغي على المشرع التحديد بطريقة أوضح.

4- لا يتم إجراء المراقبة إلا بإذن السلطة القضائية:

وحتى يكون إجراء المراقبة الإلكترونية مشروعًا أو مباحًا يجب أن تكون عن طريق إذن مكتوب من السلطة القضائية وهو ما ورد في الفقرة الثانية من المادة 4 السابقة الذكر.

وجاء في الفقرة الثالثة والرابعة من نفس المادة على أنّ الحالة المنصوص عليها في البند "أ" من الفقرة الأولى من هذه المادة فإنّ النائب العام لدى مجلس قضاء الجزائر هو من يمنح الإذن بالمراقبة لمدة 06 أشهر قابلة للتجديد لضباط الشرطة القضائية التابعين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها - والمنصوص عليها في المادة 13 من نفس القانون -، ويمنح هذا الإذن على أساس تقرير مكتوب يبين فيه طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها، وتُحصر هذه الأغراض في تجميع وتسجيل معطيات ذات صلة بالجرائم الإرهابية والاعتداءات على أمن الدولة، فإن لم تكن المراقبة لهذا الغرض فإنّ القائم بالمراقبة يقع تحت طائلة العقوبات المنصوص عليها في المادة 303 مكرر من قانون العقوبات السابقة الذكر.

ثانيا: التزامات مقدمي الخدمات

لما كان الدليل في الشكل الإلكتروني يمتاز بأنه سريع التبخر أو التعديل، حثّت اتفاقية الاتفاقية العربية لتقنية المعلومات، على ضرورة أن تتبنى الدول الأعضاء في تشريعاتها الداخلية إجراء التجميع الفوري للمعطيات المتعلقة بحركة المرور، ويلزم بهذا التجميع مزودي الخدمات، بمعنى أن يقوم هذا الأخير بجمع المحتويات المتعلقة بالاتصال في فترة الإنتاج وتجميعها لحظة النقل عبر الاتصال¹.

ولقد نص المشرع الجزائري على هذا الإجراء في المواد 10 و 11 و 12 من الفصل الرابع من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تحت عنوان التزامات مقدمي الخدمات، حيث يلتزمون بمساعدة السلطات في تجميع وتسجيل المعطيات وحفظ المعطيات المتعلقة بحركة السير، حيث تُقرر المواد السابقة تحملهم المسؤولية في حالة الإخلال بالتزاماتهم؛ وقبل التطرق للتفصيل في هذه الالتزامات والمسؤولية نتطرق في البداية إلى تعريف المصطلحات الخاصة بالتزامات مقدمي الخدمات في النقاط التالية:

¹ د/ هلاي عبد الاله أحمد، المرجع السابق، ص: 248.

أ- مفهوم التزام مقدمي الخدمات بحفظ المعطيات المتعلقة بحركة السير:

يقتضي التعرض لالتزامات مقدمي الخدمات بحفظ المعطيات المتعلقة بحركة السير ضرورة فهم معنى مقدم الخدمات ومعنى المعطيات المتعلقة بحركة السير وهو ما نشرحه كما يلي:

1- مفهوم مقدمي الخدمات:

نصت المادة الأولى "د" من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على تعريف مقدم الخدمات كما يلي:

(1- أي كيان عام أو خاص يقدم لمستهلمي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات،

2- أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستهملها).

ولقد حرصت المذكرة التفسيرية لاتفاقية بودابست على أن تُوضح أن تعريف مقدم الخدمة ينطبق على كل من يقوم بخدمات الاتصال أو خدمات معالجة البيانات أو خدمات تخزين البيانات، ويستوي في ذلك أن تكون الجهة التي تقدم الخدمة عامة أو خاصة، كما يستوي أن تكون الخدمة مقدمة لمجموعة من المستخدمين يشكلون جماعة مغلقة أو أنها مقدمة للجمهور، كذلك يستوي أن تكون الخدمة مقابل رسوم أو بالجمان، كما ينسحب هذا التعريف أيضًا ليشمل الأشخاص الذي يعرضون خدمة الاستضافة أو التخزين المؤقت أو الربط بالشبكة، ويخرج من نطاق هذا التعريف مقدم المحتوى، كالشخص المتعاقد مع المقدم على إنشاء موقع له على الشبكة العالمية دون أن يقوم هذا الشخص المتعاقد بأي خدمات أخرى كخدمات الاتصال أو المعالجة أو التخزين¹.

2- مفهوم المعطيات المتعلقة بحركة السير:

كذلك المعطيات المتعلقة بحركة السير أورد المشرع الجزائري تعريفها في الفقرة "هـ" من المادة رقم 02 من القانون السابق الذكر، كما يلي: (أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءًا في حلقة اتصالات توضح مصدر الاتصال والجهة المرسل إليها والطريق الذي يسلكه ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة)، أيضًا هذا التعريف نفسه الوارد في الفقرة "د" من المادة رقم 1 من اتفاقية بودابست، ولم يرد تعريف لها في الاتفاقية العربية.

¹ نفس المرجع، ص، ص: 47-48.

وتشير المذكرة الايضاحية لاتفاقية بودابست إلى أنّ بيانات المرور هذه تُشكل طائفة من البيانات المعلوماتية الخاضعة لنظام قانوني معين، وأنّ هذه البيانات تنشأ عن طريق أجهزة الحاسب في سلسلة من الاتصالات من أجل توجيه الاتصال من منبعه أو أصله إلى مكان وصوله، وعلى ذلك فهي من ملحقات الاتصال في حد ذاته، كما أوضحت هذه المذكرة أنّ البيانات المتعلقة بالمرور تشمل عدة طوائف، وهي منشأ أو أصل الاتصال ويُشير إلى رقم الهاتف وعنوان بروتوكول الانترنت IP، وكذلك مكان الوصول الذي يُشير إلى جهاز الاتصال الذي تتجه إليه الاتصالات المرسله، وأيضاً خط السير ووقت الاتصال وفقاً لتوقيت غرينتش والتاريخ وطول أو حجم الاتصال أو المدة أو الفترة، ناهيك عن نوع الخدمة مثل نقل ملف أو بريد إلكتروني أو بريد آني أو لحظي، وتُبين فضلاً عن ذلك، أنّ هذه الطوائف من البيانات، قد لا تكون متاحة من الناحية الفنية، إلا أنّها تكون متاحة عن طريق مقدمي الخدمات¹.

ب- التزامات مقدمي الخدمات:

تتمثل التزامات مقدمي الخدمات في مساعدة السلطات طبقاً للمادة 10 من ذات القانون وفي حفظ المعطيات المتعلقة بحركة السير وفقاً للمادة 11، ويُضيف المشرع في المادة 12 التزامات أخرى خاصة بمقدمي خدمة الانترنت، ومردّد هذه الالتزامات أنّه مثلاً في المراسلة بالبريد الإلكتروني والتي يتم استقبالها بواسطة مقدم الخدمات الخاص بالمرسل إليه، والتي لم يطلع عليها بعد، فإنّها تستقر في حالة تخزين إلكتروني، ففي هذه المرحلة فإنّ النسخة من الاتصال المخزنة تتواجد فقط كإجراء أو وسيط مؤقت في انتظار استقبال المرسل إليه من مزود الخدمة، وبمجرد استلام المرسل إليه المراسلة بالبريد الإلكتروني فإنّ موقف مزود الخدمة يتراوح بين أمرين: إمّا أن يقوم بمسح تلك الرسالة، أو أن يقوم بتخزينها² في حال طلب السلطات لتلك الرسالة، وعليه فيقوم بالتجميع والتسجيل والحفظ وتقديمها لهذه السلطات لتساعدتها في كشف الحقيقة المبتغاة، وهو ما نتناوله بالدراسة كما يلي:

1- مساعدة السلطات:

وفقاً للمادة 10 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها فإنّ مزود الخدمات يلتزم بما يأتي:

¹ نفس المرجع، ص: 49 وما يليها.

² رشيدة بؤكر، المرجع السابق، ص: 447.

- تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، بحيث أنه لما كان مزود الخدمات بإمكانه مراقبة ومعرفة جميع الخطوات التي يتبعها المستخدم إذ يتاح له معرفة المواقع التي زارها والمعلومات التي خزنها وكل الاتصالات التي أجراها، ومن ثم فإنه مُلزم بتمكين جهات التحقيق من كل المعلومات التي تبحث عنها¹، وذلك بتجميعها أو تسجيلها.
- وضع المعطيات التي يتعين عليهم حفظها وفقاً للمادة 11 من ذات القانون تحت تصرف السلطات المكلفة بالتحريات القضائية.
- الحفاظ على السرية، إذ يتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها.

2- حفظ المعطيات المتعلقة بحركة السير:

- تنص المادة 11 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على: (مع مراعاة طبيعة ونوعية الخدمات يلتزم مقدموا الخدمات بحفظ:
- أ- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.
 - ب- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.
 - ج- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.
 - د- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.
 - هـ- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ" من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه...).
ويُفهم من ذلك أنّ إجراء الحفظ يتم بعد قيام مقدمي الخدمات بإجراء التجميع والتسجيل ثم الحفظ ليُقدم في النهاية إلى يد السلطات المكلفة بالتحريات القضائية؛ وتكتسي هذه الإجراءات أهمية بالغة

¹ زبيحة زيدان، المرجع السابق، ص: 154.

من حيث كونها أداة تنقيب وتحري مفيدة من أجل تحديد مصدر الاتصال ومآله عن طريق أرقام الهاتف، كما توفر بيانات مرتبطة بالساعة والتاريخ والمدة المتعلقة بأنواع الاتصالات غير المشروعة¹. ويُعتبر إجراء الحفظ إجراءً وقائيًا، إذ حدّده المشرع الجزائري في نفس المادة من ذات القانون في فقرتها الثالثة بمدة سنة، ابتداءً من تاريخ التسجيل؛ ويأتي تحديد هذه المدة احترامًا للحق في الخصوصية، إذ يُلزم مقدم الخدمات بمسح المعطيات التي يتم حفظها.

3- التزامات خاصة بمقدمي خدمة الانترنت:

يُلزم المشرع الجزائري وفقًا للمادة 12 من قانون السابق الذكر مقدمي خدمة الانترنت إلى جانب الالتزام بالحفظ المنصوص عليه في المادة 11 بما يلي:

(أ- التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن.

ب- وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها).

يفهم من ذلك أنّ المشرع الجزائري، قد فرّق في الالتزام بين مقدمي الخدمات السلوكية واللاسلكية، حيث يقع على عاتقهم الالتزامات المنصوص عليهم في المادتين 10 و11، وبين مقدمي خدمات الاتصالات الإلكترونية أو اتصالات الشبكة إذ يقع على عاتقهم التزامات المواد 10 و11 و12.

ج- مسؤولية مقدمي الخدمات عن إخلالهم بالالتزامات القانونية المفروضة عليهم:

يتحمل مقدمو الخدمات المسؤولية الجنائية، وتطبق عليهم العقوبات المنصوص عليها في قانون العقوبات إذا لم يلتزموا بكتمان السرّ بل أفشوا كل أسرار التحري والتحقيق، كما يتحملون المسؤولية الجنائية عن إخلالهم بالتزام الحفظ، حيث تطبق على الشخص الطبيعي وفقًا للفقرة الرابعة من المادة 11 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها عقوبة الحبس من 06 أشهر إلى 05 سنوات وغرامة من 50.000 دينار جزائري إلى 500.000 دينار جزائري، وهذا مع عدم الإخلال بالعقوبات الإدارية، إذ أنّ مقدمي الخدمات يتعاملون مع هيئات وتفرض عليهم هذه الأخيرة عدة التزامات تُقيّد في دفتر الشروط، وفي حال إخلالهم بها تطبق عليهم

¹ د/ هلاي عبد اللاه أحمد، المرجع السابق، ص: 259.

جزاء كسحب الرخصة إضافة إلى عقوبات إدارية أخرى¹، وتطبق على الشخص المعنوي طبقاً للفقرة الأخيرة من ذات المادة الغرامة وفقاً للقواعد المقررة في قانون العقوبات.

الخلاصة:

إن القواعد الإجرائية التقليدية القائمة تبدو قاصرة على استخلاص الدليل في الشكل الإلكتروني ومواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مما يترتب عليه إفلات الكثير من الجناة من العقاب، مما دفع بالمشروع الجزائري إلى تكريس قواعد إجرائية حديثة تتماشى وتتواءم مع الطبيعة التقنية للجريمة والدليل الناتج عنها، لذلك سنّ قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الذي نص فيه على قواعد إجرائية حديثة تجمع بين هدف الوقاية وذلك بالرصد المبكر للاعتداءات المحتملة، وهدف المواجهة بالتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها، ونص على إجراءات أخرى في قانون الإجراءات الجزائية، وذلك قبل أن توضع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سنة 2010؛ وتوصلنا من خلال بحثنا في هذه الإجراءات إلى ما يلي:

- أنّ الإجراءات المنصوص عليها سنة 2006 في قانون الإجراءات الجزائية الجزائري وضعت لمواجهة بعض الجرائم محددة على سبيل الحصر من بينها جرائم الاعتداء عن نظم المعالجة الآلية وهي جرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المنظمة عبر الحدود الوطنية، وتمثل في اعتراض المراسلات السلوكية واللاسلكية، وتسجيل الأصوات والتقاط الصور والتسرب.
- أنّ الإجراءات المنصوص عليها في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها هي المراقبة الإلكترونية وإلزام مقدمي الخدمات بالمساعدة في التحريات القضائية عن طريق جمع وتسجيل المعطيات وكذا إلزامهم بحفظ المعطيات المتعلقة بحركة السير وإلزام مقدمي خدمة الانترنت بالتدخل الفوري لسحب المعطيات لمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن ووضع ترتيبات تقنية لمنع الدخول لمعطيات مخالفة للنظام العام أو الآداب العامة.

¹ رشيدة بوكور، المرجع السابق، ص: 452.

- أنّ القواعد الإجرائية الحديثة تنطوي على المساس بحريات وحقوق الإنسان الأساسية التي ضمنتها الدساتير في مختلف دول العالم حيث حُصت بحماية القوانين العقابية عن طريق تجريم كل سلوك من شأنه الاعتداء عليها.
- أنّ القواعد الإجرائية الحديثة سمحت الدول باتخاذها على الرغم مما تنطوي عليه، إذا كانت لها فائدة في إظهار الحقيقة ومن شأنها الوصول إلى مرتكب الجريمة الحقيقي لتحمي باقي أفراد المجتمع من إجرامه.
- أنّ إجراء اعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات والتقاط الصور هو مراقبة على المحادثات الهاتفية.
- أنّ إجراء المراقبة الإلكترونية هو مراقبة على الاتصالات الإلكترونية أي مراقبة شبكة الاتصالات (الانترنت).
- أنّ المشرع الجزائري يسمح بمراقبة المحادثات الهاتفية بالنسبة لجرائم محددة على سبيل الحصر من بينها جرائم الاعتداء على نظم المعالجة الآلية للمعطيات.
- أنّ المشرع الجزائري يسمح بمراقبة الاتصالات الإلكترونية في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
- أنّ المشرع لا يسمح بمراقبة الاتصالات الإلكترونية بالنسبة لباقي الجرائم المحددة على سبيل الحصر السابقة الذكر.
- أنّ كل من المشرع الجزائري ألزم مقدمي الخدمات بحفظ المعطيات لمدة سنة ثم إزالتها احتراماً للحق في الخصوصية.

وبناء على هذه النتائج نقدم التوصية التالية:

- نقدم اقتراح للمشرع الجزائري بأن يدخل تعديلين الأول على إجراء اعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية في المادة 65 مكرر 5 يكون بحذف الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ويستبدلها بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حيث تضم هذه الجرائم، كل الجرائم المعلوماتية بما فيها الجريمة موضوع البحث، والتي اقترحنا إدخالها ضمن قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وأن يضيف للفقرة الثانية عبارة الإلكترونية لتصبح هذه الفقرة كما يلي: (.... - اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية

واللاسلكية والإلكترونية...); والتعديل الثاني يكون على إجراء المراقبة المنصوص عليه في المادة 3 و4 من قانون الوقابة من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث يحال في هذه المراقبة إلى إجراء الاعتراض المنصوص عليه في قانون الإجراءات الجزائية، أما الحالات التي تدعو إلى المراقبة فلا تلغي بل تبقى كما هي، وهذا حتى نتفادى ازدواجية النصوص إذا ما عدّلنا إجراء الاعتراض بالطريقة التي سبق شرحها في قانون الإجراءات الجزائية، ويترتب على ذلك بأن يلغى مصطلح المراقبة ويعوض بالاعتراض، لأن الاعتراض في مفهومه يعني المراقبة.

الجوانب الإجرائية لمواجهة الجريمة المعلوماتية في التشريع الجزائري

د/ مهدي رضا

كلية الحقوق والعلوم السياسية

جامعة المسيلة

د/ رفاف لخضر

كلية الحقوق والعلوم السياسية

جامعة برج بوعرييج

مقدمة:

نتيجة للثورة التقنية والتطور الهائل في مجال الإعلام الآلي وتكنولوجيات الإعلام والاتصال ، ظهرت مخاطر وتهديدات جديدة في الساحة العالمية تسمى الجرائم السيبرانية مما يجعل من حماية المعلومات في الفضاء الإلكتروني أمرا حتميا يتطلب تسخير مختلف الوسائل المادية والقانونية المتاحة والممكنة لضمان أمن نظم المعلومات وحمايتها.

فمعظم دول العالم تفتنت لهذا الخطر وسلكت طريق حماية قواعد المعطيات من خلال إيجاد منظومة قانونية متكاملة بهدف حماية الحقوق والحريات من جهة، وتوفير مجموعة من الإجراءات والتدابير الوقائية التي تستخدم للحماية من جرائم الحاسوب والإنترنت، ومهددات استخدام التقنية التي قد تطل إياها البيانات الشخصية المتصلة بالحياة الخاصة، أو سرية المعلومات أو سلامتها أو توفرها، أو قد ترتبط بأجهزة الحاسوب نفسها كأن تطالها السرقة أو استخدام أجهزة الحاسوب وشبكات المعلومات كوسيط في ارتكاب الجرائم العادية الأخرى....

طبقا لهذه النظرة قام المشرع الجزائري منذ سنة 2004 بسن مجموعة من القوانين تهدف إلى الوقاية وإلى قمع الاستعمال غير القانوني لتكنولوجيات الإعلام والاتصال من خلال القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتمم لقانون العقوبات، والقانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية ومكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، إضافة إلى القانون رقم 15-04 المؤرخ في الفاتح فبراير 2015 الذي يحدد القواعد العامة للتوقيع والمصادقة الالكترونيتين (فيما يتعلق بتأمين التبادلات الالكترونية مقرروا بالأحكام الجزائية بالمواد من 66 الى 75) كما أسند المشرع الجزائري مكافحة الجرائم السيبرانية ولاسيما المساس بالأنظمة الآلية لمعالجة المعطيات إلى الأقطاب الجزائية المتخصصة.

أما على المستوى الدولي، وإن كانت الجزائر صادقت على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة في 21 ديسمبر 2010 بموجب المرسوم الرئاسي 14-252 المؤرخ في 08 سبتمبر 2014 إلا أنها لم تنضم بعد إلى اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية «اتفاقية بيدابست»¹ التي فتحت للتوقيع عليها في 23 نوفمبر 2001 ودخلت حيز التنفيذ في الفاتح جويلية 2004، ولم تصادق لحد الآن كذلك على اتفاقية الاتحاد الافريقي حول الأمن السيبراني وحماية المعطيات الشخصية المحررة بمالابو بغينيا الاستوائية في 26 و 27 جوان 2014. من خصائص الجريمة المعلوماتية الخفاء و التستر فهي مستترة عادة ما لم يتم التبليغ عنها للجهات المختصة بالتحقيق و تحريك الدعوى الجنائية حسب القواعد و الأنظمة المعمول بها، و الصعوبة التي تواجه أجهزة الأمن و المحققين في الجريمة المعلوماتية هي صعوبة اكتشاف هذه الجرائم بواسطة الأشخاص العاديين و هنا يظهر دور الأجهزة الأمنية في رصد حركة مرتكبي هذه الجرائم و اكتشافها⁽²⁾.

لقد وضع المشرع الجزائري بالموازاة مع نصوص قانون العقوبات قواعد إجرائية في عدة نصوص وقوانين خاصة الهدف منها السهر على تنفيذ هذه النصوص ووضع إطار إجرائي متعلق بالاختصاص وكذا طرق الإثبات وخاصة إجراءات التفتيش والمصادرة وعليه نتساءل، فيما تتمثل القواعد الإجرائية التي وضعها المشرع الجزائري للحد من الجريمة الالكترونية؟

المحور الأول: الجوانب الإجرائية المنصوص عليها في قانون الإجراءات الجزائية.

انطلاقا من فكرة خصوصية الجريمة الالكترونية أو جرائم المساس بأنظمة المعالجة الآلية للمعطيات فقد تناولها المشرع الجزائري في قانون الإجراءات الجزائية عن طريق مجموعة من النقاط يمكن اجمالها في ما يلي:

¹ هي اتفاقية مفتوحة للانضمام إليها لجميع دول العالم وليس فقط للدول الأوروبية.

² محمد أمين البشري، التحقيق في الجرائم المستحدثة، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الامنية، الرياض، الطبعة الاولى، 2004.

أولاً- إحداث المحاكم الجزائية ذات الاختصاص الموسع التي أجاز لها تمديد اختصاصها للنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من خلال المواد: 37 و 40 و 329 من قانون الإجراءات الجزائية.

ثانياً- تمديد الاختصاص الإقليمي لضباط الشرطة القضائية لمعانة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إلى كامل الإقليم الوطني من خلال المادة 16 منه. ⁽¹⁾

ثانياً - قواعد استثنائية في التفتيش ومن بين هذه الإجراءات الاستثنائية في التفتيش نذكر ما يلي:

1 جواز التفتيش في المحلات السكنية وغير السكنية وفي كل ساعات الليل والنهار لمعانة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بناءً على إذن مسبق من وكيل الجمهورية المختص وهو ما نصت عليه المادة 47 من قانون الإجراءات الجزائية.

2 إمكانية قيام ضباط الشرطة القضائية بالتفتيش داخل المساكن دون حضور المشتبه فيه ودون شهود حسب نص المادة 45 الفقرة الأخيرة.

3 إمكانية قيام ضباط الشرطة القضائية بتفتيش مسكن أي شخص يحتمل أن يحوز أوراقاً أو أشياء لها علاقة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات دون حضور صاحب المسكن حسب نص المادة 45 فقرة الأخيرة من قانون الإجراءات الجزائية.

وتجدر الإشارة إلى أن هذه القواعد الاستثنائية المنصوص عليها في المادة 45 لا تعفي من اتخاذ التدابير اللازمة لضمان احترام السر المهني عندما تجري التفتيش في محلات يكون أصحابها ملزمون باحترام السر المهني، كما أن جميع هذه الإجراءات الاستثنائية تستوجب الحصول على إذن مسبق من وكيل الجمهورية عندما يتعلق الأمر بحالة تلبس أو بتحقيق ابتدائي.

رابعاً- إمكانية استعمال أساليب خاصة للتحري في جرائم المساس بأنظمة المعالجة الآلية للمعطيات ويتعلق الأمر بـ:

-اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

-التقاط وتثبيت وبث وتسجيل الكلام والتقاط الكلام والتقاط صور الأشخاص في الأماكن الخاصة.

¹-الجمعية المعلوماتية، المجلة القضائية، العدد الأول: 2010، ص 55.

وجاءت جميع هذه الصلاحيات الاستثنائية مشروطة بإذن السلطة القضائية كما نص القانون على أن الإذن نفسه ينبغي أن يتضمن الضوابط التي تحول دون التعسف في استعماله.

خامسا - التسرب:

نصت المادة 65 مكرر 11 من قانون الإجراءات الجزائية على التسرب كوسيلة لمعاقبة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وإيقاف مرتكبيها وذلك من خلال قيام ضابط أو عون الشرطة القضائية أو الأشخاص الذين يتم تسخيرهم لغرض التسرب بإيهام المشتبه فيه أنهم يشتركون معه في ارتكاب الجريمة كفاعلين أصليين أو شركاء أو بإخفاء متحصلات الجريمة.

سادسا- إمكانية تمديد فترة الحجز للنظر:⁽¹⁾

نص قانون الإجراءات الجزائية على إمكانية تمديد فترة التوقيف للنظر المحددة بـ 48 ساعة مرة واحدة عندما يتعلق بالتحري في جرائم المساس بأنظمة المعالجة الآلية للمعطيات في حالات التلبس. سابعاً-ولقد نص القانون 02-15 المؤرخ في 23 جويلية 2015 المعدل للقانون 66-155 المتضمن قانون الإجراءات الجزائية والذي استحدث المادة: 35 مكرر على أنه يمكن للنيابة العامة الاستعانة في المسائل الفنية بمساعدين متخصصين وهذا لتعزيز قدرة النيابة في معالجة القضايا ذات الطابع التقني و هم خبراء يمكن الاستعانة برأيهم وخبرتهم في التحريات الأولية و خلال مختلف مراحل الدعوى.

المحور الثاني: القواعد الإجرائية المنصوص عليها في القانون 04-09.

لقد جاء القانون 04-09 المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، جاء بقواعد للوقاية من الجرائم الافتراضية ودعم وسائل مكافحتها من خلال وضع ترتيبات تسمح برصدها المبكر وجمع الأدلة عنها ومن المفيد أن نشير هنا إلى أن القواعد الوقائية هي التي دعت إلى وضع قانون خاص بدلا من إصدار نص مكمل لقانون الإجراءات الجزائية،ويمكن تلخيص الأحكام التي أوردها القانون الجديد فيما يلي:

¹ - قانون الإجراءات الجزائية الجزائري.

أولا- الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

عرف القانون 09-04 الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في المادة 02 منه بأنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الالكترونية.

كما عرف المنظومة المعلوماتية على أنها نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المترابطة، ويقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين. أما المعطيات المعلوماتية فعرفها المشرع الجزائري على أنها أي عملية عرض وطرح الوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل المنظومة المعلوماتية تؤدي وظيفتها.

وعرف الاتصالات الالكترونية والتي تكون في غالب الأحيان هي المعرضة للقرصنة لأنها تشكل أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية.

ثانيا- وضع قواعد خاصة تميز مراقبة الاتصالات الالكترونية:

نصت المادتين الثالثة و الرابعة من قانون 09-04 على الحالات التي تميز هذا النوع من المراقبة وهي:

1- الوقاية من جرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، ويتعلق الأمر هنا بمراقبة وقائية تنطلق من كون الإرهاب تهديدا خطيرا ودائما وقد أحاط المشرع هذه العملية الاستثنائية بضمانات خاصة إذ نص على أن إساءة استعمال المعلومات المتحصل عليها في هذا الإطار تنجر عنه المسائلة الجزائية كما أخضعها لإذن يصدره النائب العام لدي مجلس قضاء الجزائر وفق شروط خاصة ولفترة 06 أشهر قابلة للتجديد.

2- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

3- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.

4- في إطار تنفيذ طلبات التعاون القضائي الدولي.

5- تضمن قواعد إجرائية خاصة بتفتيش المنظومات المعلوماتية وحجز المعطيات المعلوماتية:

6- نصت المواد من 05 إلى 09 على هذه القواعد وفقا للمعايير العالمية المعمول بها في هذا الشأن دون الإخلال بما تضمنه قانون الإجراءات الجزائية من مبادئ عامة.

-إلزام مقدمي الخدمات بمساعدة السلطات المكلفة بإجراء التحريات القضائية: المادة 10 من قانون 04-09.

-قواعد تلزم مقدمي الخدمات بحفظ المعطيات الخاصة بحركة السير للرجوع إليها إذا اقتضت التحريات ذلك وقد يترتب عن الإخلال بهذه الالتزامات عقوبة جزائية في حالة ما إذا أدى ذلك إلى عرقلة حسن سير التحريات القضائية: منصوص عليه في المادة: 11 منه.

-إنشاء هيئة وطنية لتنشيط وتنسيق عمل السلطات المكلفة بمكافحة الجريمة الافتراضية ومدها بالمساعدة والاستشارة اللازمة، والتي أحال إنشائها إلى التنظيم (المادة 14) والمتمثلة في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وقد تم إنشاء هذه اللجنة بموجب المرسوم الرئاسي رقم 15-261، الصادر بتاريخ 08 أكتوبر 2015 ، وهذه اللجنة تسير من طرف لجنة مديرة مكونة من وزير العدل رئيسا والوزير المكلف بالداخلية، والمدير العام للأمن الوطني وكذا قائد الدرك الوطني و ممثل عن وزارة الدفاع الوطني، وكذا ممثل عن رئاسة الجمهورية بالإضافة إلى قاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء والمعروفين باهتمامهم بمجال المعلوماتية، بالإضافة إلى أعضاء من الضبطية القضائية والمتخصصين في هذا المجال.

-توسيع الولاية القضائية للمحاكم الجزائية لتختص بالنظر في الجرائم المرتكبة خارج الإقليم الوطني سواء كان مرتكبها مواطنا جزائريا أم أجنبيا عندما تستهدف مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني وفق ما نصت عليه المادة 15.

-النص على مبادئ المساعدة القضائية الدولية المتبادلة وكيفية تبادل المعلومات واتخاذ الإجراءات التحفظية لجمع الأدلة(المادتين 16 -17) مع إخضاع التعاون الدولي لقيود عدم المساس بالسيادة الوطنية والنظام العام وجواز التعاون بشرط المحافظة على سرية المعلومات المبلغة و هو ما نصت عليه المادة 18 من ذات القانون.

-القانون 03-2000 المؤرخ في 05 أوت 2000 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية (1).

¹ - المجلة القضائية للمحكمة العليا، مرجع سابق، ص 66.

وقد وضع هذا القانون القواعد التي تنظم مختلف شبكات المواصلات السلكية واللاسلكية مهما كانت الوسيلة المستعملة سواء أسلاك بصرية أو لاسلكي كهربائي أو أجهزة أخرى كهربائية مغناطيسية وهذا في المواد 08 إلى 21 منه.

-المرسوم التنفيذي رقم: 98-256 المؤرخ في 25 أوت 1998 المعدل والمتمم للجزء التنظيمي من الأمر 75-89 المؤرخ في 30-12-1975 المتضمن قانون البريد والمواصلات الذي نص علي:
- تعريف خدمات الانترنت.

- شروط ممارسة مقدمي الخدمة ومستضيفي المواقع لنشاطهم.
- واجباتهم اتجاه السلطات العمومية.
- مسؤوليتهم عن محتوى الصفحات التي يطورونها أو يستضيفونها.
- واجباتهم اتجاه زبائنهم ومنها على الخصوص أخبار المستعملين بمسؤولياتهم عن محتوى الصفحات التي ينتجونها.

على قدر ما تقدمه تقنيات المعلومات والاتصالات من تسهيلات للأفراد والمجتمعات على حد سواء فقد زعزعت سكينتهم بهذا النوع الجديد من الجرائم التي تتميز بطبيعة فنية وعلمية معقدة وتعتبر من أكثر الجرائم التي عرفها العالم الحديث خطورة نظراً لما تسببه من خسائر مادية ومعنوية كبيرة وأمام خطورة وخصوصيات الجرائم المعلوماتية، كان لا بد من وضع آليات حماية لردعها فعلى المستوى الوطني والدولي أصدرت تشريعات خاصة تراعي خصوصية هذه الجريمة المستحدثة العابرة للحدود الوطنية وعلى مستوى المؤسسات والهيئات استحدثت آليات تنظيمية وتقنية معقدة لحماية المعلومات، وبالإضافة إلى هذه الآليات على مستخدمي تقنيات المعلومات والاتصالات التحلي بالوعي والأخلاقيات واحترام قواعد الاستخدام السليم في هذا المجال :

- تجنب الإساءة للآخرين (التجسس، إرسال الفيروسات، توزيع الملفات غير الأخلاقية على الآخرين).

- الإخلاص في العمل وعدم الانحياز في الأفكار.
- احترام أملاك الآخرين وحقوق الملكية الفكرية.
- الالتزام بالحفاظ على السرية وأخلاقيات وقوانين الخدمة فيما يخص الموظفين اللذين يستخدمون الانترنت.

- احترام خصوصية الآخرين.

- استخدام أجهزة وأنظمة الإعلام الآلي في الإطار المسموح به.
- التقيد بإجراءات الحماية واحترام القوانين التي تحدد الشروط والقواعد المطبقة في مجال الأمن المعلوماتي واستغلال الانترنت.

وحتى نتمكن من تعزيز دور الآليات القانونية المتاحة لمواجهة الجريمة المعلوماتية فانه يتعين تحيين التشريعات الجزائية القائمة لمواجهة الجرائم المعلوماتية وذلك بتقرير الجرائم وتحديد العقوبات المناسبة لها بغية حماية النظام المعلوماتي، خاصة أمام تزايد العمل بما يسمى قادة البيانات في جل المؤسسات والهيئات العمومية منها والخاصة، وظهور أنماط جديدة من الجرائم المعلوماتية والتي أصبحت تهدد سلامة المواطنين وامن الدول ومنها ظاهرة الإرهاب المعلوماتي، وكذا ظاهرة التجسس المعلوماتي على الدول ورؤسائها من خلال اختراع برامج التجسس والتي تكون موضوعة بالأساس داخل أجهزة الحاسب الآلي والهواتف الذكية، وهي الظاهرة التي ظهرت في وثائق ويكيليكس المنشورة والتي أثارت ضجة إعلامية كبيرة .

وإيجاد أدلة إثبات جديدة تتلاءم مع طبيعة هذه الجرائم وذلك لعدم ملائمة أدلة الإثبات التقليدية في القانون الجنائي لإثباتها، وهذا باعتماد الدليل الرقمي في إثبات الجريمة الالكترونية والتي هي لغة الأرقام واستحداث فرق أو هيئات متخصصة في متابعة هذه الجرائم والكشف عنها وهو الأمر الذي يحتاج إلى إمكانيات بشرية ومادية تبدأ من الجامعة باستحداث فروع متخصصة في البرامج ومجابهة ظاهرة القرصنة، وكذا عقد المؤتمرات والأيام الدراسية لتسليط الضوء على هذه الظاهرة وتبادل الآراء بين المختصين في مجال التكنولوجيا وكذا رجال القانون والقضاء، بالإضافة إلى تكوين رجال القضاء في مجال الجريمة الالكترونية وكيفية عمل البرامج ومعالجة المعطيات .

واعتماد الدقة والوضوح عند سن القوانين مع الأخذ بعين الاعتبار المسائل التقنية، وعدم حصر محل الجريمة الالكترونية في نظام المعالجة الآلية للمعطيات بل ضرورة دراسة باقي نواحي هذه الجريمة، لان المعالجة الآلية للمعطيات تعتبر جزئ من الجريمة المعلوماتية وليس كلها.

وعدم الاقتصار عند التجريم والعقاب على أنماط السلوك المخطور المرتكبة حالياً بل يجب مراعاة الأبعاد المستقبلية لتكنولوجيا المعلومات والحواسيب في تطور سريع بل يكاد يكون تطورا يوميا خاصة أمام ظهور عصابات في الإعلام الآلي مهمتها إيجاد برامج وفيروسات وأصبحت تنشط على المستوى العالمي وليست أي دولة في منأى عن هذه الظاهرة.

ضرورة إعطاء مفهوم أوسع للمال والمنقول بحيث تشمل المال المعلوماتي وهذا حتى تشمل النصوص التقليدية أو صياغة نصوص قانونية خاصة بها.

تدريس مواد الأنظمة المعلوماتية في المعاهد والجامعات وخاصة طلبة الحقوق، لتسليط الضوء عليها من خلال الدراسات والبحوث.

محاولة الاستفادة من إمكانيات المجرم المعلوماتي وهذا بتنفعيل دوره من خلال العمل للنفع العام.

ضرورة تكثف التعاون الدولي وهذا بعقد المؤتمرات والملتقيات الدولية من اجل مواجهة هذه الظاهرة العابرة للحدود.

التدابير الإجرائية الخاصة لمواجهة جريمة المساس بأنظمة المعالجة الآلية للمعطيات

د/ والي عبد اللطيف

أ/ عمارة عمارة

كلية الحقوق والعلوم السياسية

كلية الحقوق والعلوم السياسية

جامعة المسيلة

جامعة المسيلة

مقدمة:

أضحى التقدم الإلكتروني وسوء استخدامه يشكل خطرا كبيرا من شأنه المساس بالمعالجة الآلية للمعطيات و أنظمتها، و ذلك إما بتغيير المعلومات أو محاولة ذلك عن طريق الغش أو المساس بها بأي شكل من الأشكال.

و نتيجة لذلك تدخل المشرع الجزائري في قانون العقوبات بتجريم كل فعل من شأنه المساس بالمعالجة الآلية للمعطيات.¹ و رتب على ذلك جملة من العقوبات تطبق وفق إجراءات سواء منها ذات الطابع العام أو الخاص.

ونركز في هذه الورقة البحثية على اجراءات المتابعة لهذه الجريمة التي أقرها قانون الإجراءات الجزائية خاصة تلك الميكانيزمات الاجرائية الخاصة و المستحدثة لمتابعة بعض الجرائم الخاصة كالفساد وتبييض الأموال و تمويل الإرهاب و الجريمة المنظمة... و منها جريمة المساس بأنظمة المعالجة الآلية للمعطيات.

و عليه تقسم الدراسة إلى عنصرين أساسيين:

أولاً: التدابير الاجرائية الخاصة على مستوى التحقيق الابتدائي

ثانياً: التدابير الاجرائية الخاصة على مستوى التحقيق القضائي

المطلب الأول: التدابير الاجرائية الخاصة على مستوى التحقيق الابتدائي

إن قيام جريمة المساس بأنظمة المعالجة الآلية للمعطيات يعتمد في التنفيذ على مجرمين محترفين أو غير محترفين يسخرون في سبيل ذلك تقنيات فنية و مهارات مركزة و لعل ما ساعدهم هو الثورة التكنولوجية الكبيرة التي أدت إلى تطور غير مسبوق في وسائل المواصلات و الاتصالات التي أدت إلى تقليص المسافات بين أجزاء العالم المختلفة² و سهولة الاطلاع و الحصول على بعض المعطيات. كل ذلك دفع بالمشرع إلى اخضاع هذه الجريمة إلى أساليب تحري خاصة تتميز بالدقة العالية وتعتمد

على التطور التكنولوجي مما جعلها تشكل استثناء على الاجراءات العادية لمتابعة الجريمة بشكل عام. وتمثل هذه الاجراءات الخاصة فيما يلي:

الفرع الأول: الاختصاص المحلي للضبطية القضائية

يتمتع ضباط الشرطة القضائية على اختلاف انتمائهم بالعمل خارج اختصاصهم المحلي المحدد قانونا و بالتالي لهم اختصاص وطني يمتد إلى كامل التراب الوطني وذلك للبحث والتحري عن مرتكبي جريمة المساس بأنظمة المعالجة الآلية للمعطيات بحيث تنص المادة 16 من قانون 06-22³: "غير أنه فيما يتعلق ببحث ومعاينة جرائم المخدرات و الجريمة المنظمة عبر الحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات... يمتد اختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني."

كما أنه يمكن للضبطية القضائية ما لم يعارض ذلك وكيل الجمهورية أن يمددوا عبر كامل الإقليم الوطني عمليات مراقبة الأشخاص الذين يوجد ضدهم مبرر مقبول أو أكثر يحمل على الاشتباه فيهم بارتكاب الجرائم المبينة في المادة 16 من قانون الإجراءات الجزائية أو مراقبة وجهة نقل أشياء أو أموال أو متحصلات من ارتكاب هذه الجرائم أو قد تستعمل في ارتكابها، وهذا حسب نص المادة 16 مكرر من القانون 06-22.

و يعمل ضباط الشرطة القضائية تحت اشراف النائب العام لدى المجلس القضائي و الذي تم تمديد الاختصاص إليه ويعلم وكيل الجمهورية المختص إقليميا بذلك في جميع الحالات. كما نصت المادة 17 من الأمر رقم 15-02⁴ على أنه عند مباشرة تحقيقات وتنفيذ الانابات القضائية فإنهم يتلقون الأوامر و التعليمات من الجهة القضائية التي يتبعونها مع مراعاة أحكام المادة 28 من قانون الإجراءات الجزائية ولهم في ذلك طلب مساعدة القوة العمومية في تنفيذ مهمتهم، كما يمكنهم توجيه نداء للجمهور قصد تلقي معلومات أو شهادات من شأنها مساعدتهم في التحريات الجارية.

و يمكنهم أيضا بناء على إذن مكتوب من وكيل الجمهورية المختص إقليميا أن يطلبوا من أي عنوان أو لسان أو سند إعلامي نشر إشعارات أو أوصاف أو صور تخص أشخاصا يجري البحث عنهم أو متابعتهم مع الأخذ بعين الاعتبار الحفاظ على حياة الناس الخاصة و حماية حقوقهم المكفولة دستوريا.

الفرع الثاني: تفتيش المساكن والتوقيف للنظر

أولاً: تفتيش المساكن

من المعلوم أن تفتيش المساكن لا يتم إلا بحضور المشتبه فيه غير أنه في جريمة المساس بأنظمة المعالجة الآلية للمعطيات و الجرائم الأخرى المنصوص عليها في نص المادة 45 من القانون 06-22 لا تستوجب حضور المشتبه فيه أو من ينوبه أو شاهدين، و ينطبق الأمر على صاحب المسكن الذي يشتبه في حيازته أوراقا أو أشياء لها علاقة بالأفعال الإجرامية. والمشرع في هذا المجال أحاط هذا الإجراء بضمانة تتمثل في الحصول على إذن مكتوب صادر من وكيل الجمهورية مع الحفاظ على السر المهني وكذا جرد الأشياء و حجز المستندات و السعي للحفاظ على ذلك.

كذلك عندما يتعلق الأمر بمتابعة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فإنه يجوز إجراء التفتيش و المعاينة والحجز في كل ساعة من ساعات النهار أو الليل و بالتالي الخروج على الميقات المحدد للتفتيش من الساعة الخامسة صباحا إلى الثامنة مساء حسب نص المادة 47 من قانون 06-22 و بالتالي فالتفتيش صحيحا مادام قد تم بناء على إذن مسبق من وكيل الجمهورية المختص.

و إذا كان الشخص الذي يتم تفتيش مسكنه موقوفا للنظر أو محبوسا و قد تعذر نقله لمخاطر قد تمس بالنظام العام أو لاحتمال فراره أو اختفاء الأدلة خلال المدة اللازمة لنقله يمكن أم يجري التفتيش بموافقة وكيل الجمهورية المسبقة أو قاضي التحقيق وبحضور شاهدين مسخرين أو بحضور ممثل يعينه صاحب المسكن محل التفتيش⁵.

ثانيا: التوقيف للنظر

يعتبر التوقيف للنظر من الاجراءات السالبة للحرية يأمر به بوضع المشتبه به في أماكن خاصة بذلك لمدة زمنية محددة للأسباب يقتضيها البحث و التحري من طرف ضابط الشرطة القضائية⁶. ومدة التوقيف للنظر 48 ساعة غير أنه إذا تعلق الأمر بجريمة المساس بأنظمة المعالجة الآلية للمعطيات فقد أعطى المشرع للضبطية القضائية سلطة تمديد هذه المدة مرة واحدة وهذا حسب الأمر رقم 02-15-07 وذلك بعد تقديم الشخص إلى وكيل الجمهورية الذي يقوم باستجوابه ويجوز له بإذن كتابي أن يمدد حجزه إلى مدة لا تتجاوز 48 ساعة أخرى بعد فحص المشتبه فيه وفق ما نصت عليه المادة 65 من الأمر رقم 02-15.

كما قرر المشرع مجموعة من الحقوق للموقوف للنظر لعل أهمها تلك التي تتعلق بحق زيارة محاميه بعد انقضاء نصف المدة القصوى المنصوص عليها في المادة 51 من الأمر 02-15 وتتم الزيارة في غرفة

خاصة توفر الأمن وتضمن سرية المحادثة وعلى مرأى ضباط الشرطة القضائية على ألا تتجاوز مدة الزيارة ثلاثين (30) دقيقة.

و عند انقضاء مدة التوقيف للنظر يتم وجوبا اجراء فحص طبي إذا ما طلب مباشرة أو بواسطة محاميه أو عائلته من طرف طبيب يتم اختياره و إذا تعذر ذلك يعين له ضابط الشرطة القضائية طبيبا. وترفق شهادة الفحص الطبي مع الملف و هذا حسب المادة 51 مكرر 1 من الأمر 15-02.

و نص المشرع على مختلف الضمانات و الضوابط التي تحكم سماع أقوال الموقوف للنظر والمحاضر المعدة لذلك وكذا أماكن التوقيف⁸.

الفرع الثالث: اعتراض المراسلات و تسجيل الأصوات و التقاط الصور و التسرب

أولا: في اعتراض المراسلات و تسجيل الأصوات و التقاط الصور

يعد مبدأ الحق في حرمة المكالمات و المحادثات الخاصة أكثر الحقوق تعرضا للاعتداء نظرا للتطور الهائل للوسائل والتقنيات المتعلقة بالتنصت و التسجيل و بالتالي التعدي على الحياة الخاصة و سرية المكالمات⁹.

و إذا تعلق الأمر بجرمة المساس بأنظمة المعالجة الآلية للمعطيات سمح المشرع للضبطية القضائية باعتراض المراسلات والتقاط الصور وتسجيل الكلام المتفوه به سواء في أماكن عامة أو خاصة و حتى داخل المنزل ويدون علم الشخص الذي له الحق على المسكن و دون رضاه¹⁰. و نظرا لخطورة هذا الإجراء ومساسه بجرمة الحياة الخاصة للأفراد خاصة فقد أحاطه المشرع بجملة من الضمانات تتمثل في:

-إذا دعت الضرورة لاتخاذ هذا الإجراء خاصة في الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات يجب الحصول على إذن مكتوب من طرف وكيل الجمهورية يتضمن معلومات تتعلق بالإجراء المراد اتخاذه سواء تعلق الأمر باتصال أو التقاط صور و كذا الأماكن المقصودة سواء سكنية أو غيرها بالإضافة إلى الجريمة المبررة لذلك.

و تكون مدة الإذن محددة بأربعة أشهر قابلة للتجديد مع التزام ضابط الشرطة القضائية بالحفاظ على السر المهني و هذا حسب المواد 65 مكرر 5 و 65 مكرر 6 و 65 مكرر 7 من قانون 22-06.

كما أن لضابط الشرطة القضائية تسخير أي عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو هيئة خاصة مكلفة بالمواصلات السلوكية و اللاسلوكية للتكفل بالجوانب التقنية¹¹.

و بعد الانتهاء من العملية يحضر ضابط الشرطة القضائية المأذون له أو المناب محضرا عن كل عملية اعتراض أو تسجيل المراسلات و كذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط و التثبيت و التسجيل الصوتي أو السمعي البصري، و يذكر بالمحضر تاريخ و ساعة بداية هذه العمليات و الانتهاء منها وتنسخ و تترجم المكالمات التي تتم باللغة الأجنبية عند الاقتضاء بمساعدة مترجم يسخر لهذا الغرض طبقا لنص المادة 65 مكرر 9 و 65 مكرر 10 من القانون رقم 06-22. و هذا المحضر يودع في ملف المتهم.

ثانيا: في التسرب

لمتابعة جريمة المساس بأنظمة المعالجة الآلية للمعطيات أوجد المشرع آلية التسرب الذي يعتبر تقنية من تقنيات البحث والتحقيق بموجبها يقوم ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرب بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، و يتم ذلك بإخفاء الهوية الحقيقية بإيهاهم بأنه فاعل أو شريك¹².

و هو الاجراء المنصوص عليه في الفصل الخامس من قانون الاجراءات الجزائية تحت عنوان: في التسرب¹³ بموجب المواد 65 مكرر 11 إلى 65 مكرر 17. و تتيح عملية التسرب لضابط الشرطة القضائية أن يستعمل هوية مستعارة و يرتكب عند الضرورة الجريمة التي يتابعها دون أن تشكل هذه الأفعال تحريضا على ارتكاب الجريمة. كما يمكن للضابط اقتناء أو حيازة أو نقل أو تسليم أو اعطاء مواد أو أموال أو منتجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها. كما يمكن أن يوضع تحت تصرف مرتكبي الجريمة وسائل ذات طابع قانوني أو مالي و كذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال دون أن يتابع جزائيا من يسخر للقيام بالتسرب. وقد أحاط المشرع الجزائري هذا الاجراء وربط تطبيقه بشروط تتمثل في:

- الحصول على اذن مكتوب و مسبب و يشمل هذا الاذن على الجريمة التي تبرر اللجوء إلى هذا الاجراء و هوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته. كما يحدد الاذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق.

و إذا تم تجاوز المدة أو عدم التمديد يمكن العون المتسرب مواصلة العملية دون أن يكون مسؤولاً جزائياً، على ألا يتجاوز ذلك مدة أربعة (4) أشهر. كما أوجب القانون عدم اظهار الهوية الحقيقية لضابط أو عون الشرطة القضائية الذين باسروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الاجراءات، وإذا ما تم الكشف عن هويتهم فإن من يكشف عن هوية الضابط أو أعوان الشرطة القضائية يتم متابعته جزائياً وفق العقوبات المقررة في المادة 65 مكرر 16 من القانون رقم 22-06.

و بعد الانتهاء من عملية التسرب يتم تحرير محضر يتضمن تقريراً عن هذه العملية من طرف ضابط الشرطة القضائية، كما يجوز سماعه كشاهد عن العملية. هذا الاجراء رغم كونه يحمل في طياته تحريضا على ارتكاب جريمة ربط المشرع تطبيقه في حدود ضيقة و جرائم محددة منها جريمة المساس بأنظمة المعالجة الآلية للمعطيات و هذا ما يبرر حرص المشرع على مكافحتها بشتى الطرق.

المطلب الثاني: التدابير الاجرائية الخاصة على مستوى التحقيق القضائي

نظرا لكون جريمة المساس بأنظمة المعالجة الآلية للمعطيات تنسم بطابع الخطورة سواء على الأفراد أو المجتمع فقد خصها المشرع بإجراءات خاصة في المتابعة من طرف النيابة العامة و قاضي التحقيق بحيث خول المشرع باتخاذ تدابير جديدة وخاصة إضافة إلى السلطات العادية التي تشترك فيها مختلف الجرائم. و كما أعطى المشرع للضبطية القضائية سلطات استثنائية، كذلك منح المشرع هذه السلطات في فترة التحقيق القضائي و يظهر ذلك على النحو التالي:

الفرع الأول: الاختصاص المحلي لقاضي التحقيق

تعمل النيابة العامة في حدود الاختصاص المحلي المقرر لها قانوناً غير أنه فيما يتعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و بعض الجرائم الأخرى المحددة قانوناً يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم¹⁴، كما أعطى المشرع لقاضي التحقيق اختصاص محلي واسع يمتد إلى دائرة اختصاص محاكم أخرى و ذلك عن طريق التنظيم في بعض الجرائم و منها الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات حسب نص المادة 40 من القانون رقم 14-04 و قد حدد المرسوم التنفيذي رقم 06-348¹⁵ تمديد الاختصاص المحلي لبعض المحاكم و وكلاء الجمهورية و قضاة التحقيق في جرائم المساس بأنظمة المعالجة الآلية للمعطيات و بعض الجرائم المحددة في القانون على النحو التالي:

- يمتد الاختصاص المحلي لمحكمة سيدي احمد و وكيل الجمهورية و قاضي التحقيق بها إلى محاكم المجالس القضائية ل: الجزائر و الشلف و الأغواط و البليدة و البويرة و تيزي وزو و الجلفة و المدية و المسيلة و بومرداس و تيارزة و عين الدفلى.

- يمتد الاختصاص المحلي لمحكمة قسنطينة و وكيل الجمهورية و قاضي التحقيق بها إلى محاكم المجالس القضائية ل: قسنطينة و أم البواقي و باتنة و بجاية و بسكرة و تبسة و جيجل و سطيف و سكيكدة و عنابة و قالمة و برج بوعريج و الطارف و الوادي و خنشلة و سوق أهراس و ميلة.

- يمتد الاختصاص المحلي لمحكمة ورقلة و وكيل الجمهورية و قاضي التحقيق بها إلى محاكم المجالس القضائية ل: ورقلة و أدرار و تامنغست و إيليزي و تندوف و غرداية.

- يمتد الاختصاص المحلي لمحكمة وهران و وكيل الجمهورية و قاضي التحقيق بها إلى محاكم المجالس القضائية ل: وهران و بشار و تلمسان و تيارت و سعيدة و سيدي بلعباس و مستغانم و معسكر و البيض و تيسمسيلت و النعامة و عين تيموشنت و غليزان.

و علاوة على ذلك يختص رئيس المجلس القضائي الذي تقع في دائرة اختصاصها بالفصل بموجب أمر في الإشكالات التي قد تثار.

الفرع الثاني: سلطة قاضي التحقيق في تفتيش المساكن و التوقيف للنظر

فضلا عن سلطة الضبطية القضائية في تفتيش المساكن و التوقيف للنظر المرتبطة بالجريمة الماسة بأنظمة المعالجة الآلية للمعطيات فإن لقاضي التحقيق سلطة منح إذن التفتيش بحيث تتم إجراءات التفتيش تحت إشرافه المباشر كما يمكنه عند الاقتضاء الانتقال إلى عين المكان للسهر على احترام القانون، كما أن الجرائم التي تكتشف و لم يرد ذكرها في إذن القاضي فإن إجراءات متابعتها تبقى صحيحة، كما خول القانون لقاضي التحقيق إذا تعلق الأمر بالجريمة الماسة بأنظمة المعالجة الآلية للمعطيات القيام بأي عملية تفتيش أو حجز ليلا أو نهارا و في أي مكان و على امتداد التراب الوطني و له أن يأمر باتخاذ أية تدابير تحفظية، إما تلقائيا أو بناء على تسخير من النيابة العامة، أو بناء على طلب من ضباط الشرطة القضائية مع التزامه بالحفاظ على السر المهني كما أن تفتيش صاحب المسكن الموقوف للنظر أو المحبوس إذا تعذر نقله إلى مكان التفتيش لسبب من الأسباب المحددة قانونا، يجري التفتيش بناء على الموافقة المسبقة لوكيل الجمهورية أو قاضي التحقيق. كل هذه الإجراءات و السلطات لوكيل الجمهورية منصوص عليها بموجب المواد 44 إلى 47 مكرر من قانون 22-06.

لقاضي التحقيق صلاحيات أيضا تتمثل في إمكانية انتقاله إلى دوائر اختصاص المحاكم المتاخمة لدائرة الاختصاص التي يزاول فيها مهام وظيفته لمتابعة تحرياته إذا ما تطلب ذلك مقتضيات التحقيق ويجب عليه أن يحضر وكيل الجمهورية بالدائرة التي ينتقل إليها، و يذكر في المحضر الأسباب التي اقتضت هذا الانتقال، كما يحيط النائب العام علما به حسب ما نصت عليه المادة 573 من قانون الإجراءات الجزائية، و إذا حضر قاضي التحقيق لمكان الحادث فإنه يقوم بإتمام أعمال ضباط الشرطة القضائية و له أن يكلف أحد ضباط الشرطة القضائية بمتابعة تلك الإجراءات، و يرسل قاضي التحقيق عند انتهاء الإجراءات جميع أوراق التحقيق إلى وكيل الجمهورية ليتخذ الاجراء اللازم بشأنها.

و إذا وصل وكيل الجمهورية و قاضي التحقيق إلى مكان الحادث في وآن واحد جاز لوكيل الجمهورية أن يطلب من قاضي التحقيق الحاضر افتتاح محضر تحقيق قانوني.

الفرع الثالث: سلطة قاضي التحقيق في اعتراض المراسلات و تسجيل الأصوات و التقاط الصور و التسرب

أولا: سلطة قاضي التحقيق في اعتراض المراسلات و تسجيل الأصوات و التقاط الصور
كما تم الإشارة إليه فإن اعتراض المراسلات و تسجيل الأصوات و التقاط الصور يقوم بها ضباط الشرطة القضائية بناء على إذن مكتوب من طرف وكيل الجمهورية غير أنه في حالة فتح تحقيق قضائي تتم هذه العمليات بناء على إذن من قاضي التحقيق و تحت مراقبته المباشرة مما يضمن ضمانات قانونية من طرف رجال القضاء من شأنها حماية الحياة الخاصة¹⁶. و بناء على هذا الإذن يجوز له أن يسمح بتنفيذ هذه العمليات بالدخول إلى المساكن و المحلات و غيرها حتى دون رضی المشتبه فيه طبقا لنص المادة 65 مكرر 5 و ما بعدها من قانون 06-22. كما يستنتج من هذه النصوص أن قاضي التحقيق لا يباشر هذه الإجراءات بنفسه بل هي مخولة لضباط الشرطة القضائية، الشيء الذي يطرح صعوبة في تطبيق الاجراء كون ضباط الشرطة القضائية تابعين لوكيل الجمهورية.

و يبقى قاضي التحقيق مرتبط بالإجراءات المتعلقة بالحبس المؤقت خاصة في حالة التمديد¹⁷ و كذا الرقابة القضائية و إجراءات تنفيذها¹⁸.

ثانيا: سلطة قاضي التحقيق في التسرب

تتمثل سلطة قاضي التحقيق في تنفيذ هذه الآلية في الإذن الذي يمنحه بعد اخطار وكيل الجمهورية إذا اقتضت ضرورة البحث و التحري أو التحقيق في الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات و الجرائم الأخرى المنصوص عليها قانونا. و تتم عملية التسرب تحت رقابته وفق ما تم الإشارة إليه حسب المادة 65 مكرر 11 من قانون 06-22، كما يمكن لقاضي التحقيق الذي رخص بإجراء عملية التسرب أن يأمر في أي وقت وقفها قبل انقضاء المدة المحددة بحسب المادة 65 مكرر 15 من قانون 06-22.

و الرخصة الخاصة بالتسرب لا تودع في ملف الاجراءات إلا بعد الانتهاء من عملية التسرب وهذا ما يشكل مساسا بحق الدفاع في الاطلاع على ملف الاجراءات. غير أن هدف المشرع من هذا الاجراء هو محاولة ابقاء عملية التسرب سرية وحفاظا على نجاح هذه العملية خاصة وأن ضابط الشرطة القضائية لا يكشف عن هويته الحقيقية، ويبقى تطبيق هذه الاجراءات استثناء على اجراءات التحقيق العادية دفعت اليه طبيعة الجريمة وخطورتها.

وفيما يتعلق بباقي الاجراءات فان متابعة الجريمة الخاصة بأنظمة المعالجة الآلية للمعطيات تبقى خاضعة للإجراءات العادية سواء فيما تعلق بتقادم الجريمة أو العقوبة حسب الوصف الجنائي لهذه الجريمة وحسب المقدار وجسامة العقوبة.

خاتمة:

من خلال استعراض مختلف الاجراءات الخاصة المتعلقة بمتابعة الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات خاصة تلك المتعلقة بالتسرب واعتراض المراسلات وتسجيل الأصوات والتقاط الصور التي يأمر بها وكيل الجمهورية أو قاضي التحقيق نجدها تشكل مساسا بجريمة الحياة الخاصة، خاصة اذا أمر بها وكيل الجمهورية باعتباره غير قابل للرد وبالتالي يبقى الاجراء الذي يقوم به. كما أن الجرائم التي يتم اكتشافها بمناسبة تنفيذ هذه الاجراءات تتم متابعتها وتعتبر اجراءاتها صحيحة مما يطرح مشكلة الدفاع في الاطلاع عليها كما يواجه صعوبة في الاطلاع على هذه العمليات خاصة التسرب لأن الرخصة لا تودع في الملف إلا بعد الانتهاء من تنفيذ هذه الاجراءات. وتبقى مشكلة تصادم هذه الاجراءات مع حقوق الاشخاص وحرمة حياتهم الخاصة المكفولة دستوريا غير أن ما يخفف من حدة هذه الاجراءات هو تعلقها بجرائم خطيرة ومحاط تنفيذه بضمانات قانونية.

الهوامش:

- 1- القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم بالقانون رقم 06-23 المؤرخ في 20 ديسمبر سنة 2006.
- 2- علاء الدين شحاتة، التعاون الدولي لمكافحة الجريمة، ايتراك للنشر والتوزيع، الطبعة الأولى، 2000، ص 09.
- 3- القانون رقم 06-22 المؤرخ في 20 ديسمبر سنة 2006.
- 4- الأمر رقم 15-02 المؤرخ في 23 يوليو سنة 2015 المعدل والمتمم لقانون الاجراءات الجزائية.
- 5- أنظر أحكام المادة 47 مكرر من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006.
- 6- عبد الله أوهائية، ضمانات الحرية الشخصية أثناء مرحلة البحث التمهيدي، دار هومة الطبعة الأولى بدون سنة، ص 164.
- 7- أمر رقم 15-02 المؤرخ في 23 يوليو 2015.
- 8- للتفصيل أكثر أنظر المادة 52 من الأمر 15-02.
- 9- أشرف حامد عبد الشافعي، الحماية الجنائية لحق الخصوصية، رسالة دكتوراه غير منشورة، جامعة القاهرة كلية الحقوق، 2012 - 2013، ص 61.
- 10- أنظر أحمد شوقي الشلقاني، مبادئ الاجراءات الجزائية في التشريع الجزائري الجزء الثاني، الطبعة الرابعة، ديوان المطبوعات الجامعية الجزائر سنة 2008، ص 157.
- 11- أنظر لتفصيل هذه الاجراءات، علي أحمد عبد الزعبي، حق الخصوصية في القانون الجنائي -دراسة مقارنة- الطبعة الأولى، سنة 2006، المؤسسة الحديثة للكتاب، لبنان، ص 533 وما بعدها.
- 12- خلفي عبد الرحمان، محاضرات في قانون الاجراءات الجزائية، دون طبعة، دار الهدى عين مليلة، 2012، ص 75.
- 13- القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006.
- 14- المادة 37 من القانون رقم 04-14 المؤرخ في 10 نوفمبر سنة 2004 يعدل ويتمم قانون الاجراءات الجزائية.

- 15- مرسوم تنفيذي رقم 06-348 المؤرخ في 05 أكتوبر سنة 2006، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.
- 16- عبد المالك بن ذياب، حق الخصوصية في التشريع العقاب الجزائي، رسالة ماجستير غير منشورة، جامعة الحاج لخضر باتنة كلية الحقوق، 2012-2013، ص 155.
- 17- راجع المواد 123 إلى المادة 125 مكرر من الأمر رقم 15-02 المؤرخ في 23 يوليو سنة 2015 يعدل ويتمم قانون الاجراءات الجزائية.
- 18- أنظر سلطة قاضي التحقيق في الرقابة القضائية المادة 125 مكرر 01 وما بعدها من الأمر رقم 15-02 السابق.

مراقبة الاتصالات الالكترونية ودورها في مواجهة الجريمة المعلوماتية

د/ يحيى لعللى

كلية الحقوق والعلوم السياسية

جامعة باتنة 1

ط.د/ سويح دنيا زاد

كلية الحقوق والعلوم السياسية

جامعة باتنة 1

مقدمة:

ادى الاستخدام المتزايد لتقنية الانترنت الى التطور السريع والانتشار لتكنولوجيا الاتصال والتحول الى عصر المعلوماتية في مجالات الادارة، وقد تولد عن ثورة الاتصالات وتكنولوجيا المعلومات العديد من التطبيقات التي اثرت بدرجة كبيرة على عدد من اوجه انشطة الحياة، كظهور الحكومة الالكترونية، التعليم عن بعد، التقاضي الالكتروني⁽¹⁾

كما وجدت الادارة الإلكترونية التي اولت اهتماما كبيرا باستخدام شبكات الاتصالات الالكترونية في نشاطاتها، وذلك للفوائد التي تقدمها هذه الاخيرة من تبسيط للإجراءات داخل المؤسسات، مما ينعكس على ايجابية الخدمات التي تقدم للمواطنين الى جانب تحقيق السرعة والسهولة في انجاز المعاملات الادارية⁽²⁾، غير ان انتشار استعمال شبكة المعلوماتية خاصة في حال عدم تأمين الاتصالات او انتهاك حق الخصوصية والاطلاع على البيانات والوصول الى المعلومات السرية، يكون له الاثر السلبي في وجود سلوكيات غير مشروعة، ويزيد من حدة ذلك اذا ما تم تجميع المعلومات والربط بينها واستكمالها، يمكن ان تظهر جوانب بمجرد كشفها وظهورها فان ذلك يضر بمصالح بعض الافراد وبأمن واستقرار الدولة نفسها.⁽³⁾

وادراكا لقصور القوانين الجنائية في ما تتضمنه من نصوص التجريم التقليدية، كان من الضروري على الدول من بينها الجزائر، تعديل النصوص القانونية التي توفر الحماية الكافية للحد من مخاطر انماط جديدة الجرائم، وهي الجرائم المرتبطة بتقنية المعلوماتية المتطورة او ما يعرف بالجريمة الالكترونية، التي

1 - خالد ممدوح ابراهيم، لوجستيات التجارة الالكترونية، دار الفكر الجامعي، طبعة 1، الاسكندرية، 2008، ص، 95.

2 - سعيد غالب ياسين، نظم المعلومات الادارية، دار اليازوري العلمية، طبعة، الاردن، 2009، ص، 204.

3 - خالد ممدوح ابراهيم، مرجع سابق، ص، 99.

اصبحت تعرف انتشارا واسعا على الصعيد الوطني والدولي، والعمل كذلك على استحداث اجراءات وآليات أكثر فاعلية تساعد في مواجهة هذه الجرائم او على الاقل التخفيف من حدتها، كما هو الحال بالنسبة لإجراء مراقبة الاتصالات الالكترونية الذي يلعب دورا كبيرا في التصدي للجريمة المعلوماتية ان ما تم التقييد بها وفقا للنصوص المعمول بها، مما ادى باهتمام المشرع الى ضرورة مواجهة هذا النوع من الجريمة، وهذا ما سنحاول توضيحه في هذه الورقة البحثية من خلال الاشكالية التي تتمثل في: ما دور مراقبة الاتصالات الالكترونية في مواجهة الجريمة المعلوماتية؟ هذه الاشكالية نحاول الاجابة عليها وفقا للعناصر التالية:

اولا: مفهوم الجريمة المعلوماتية.

ثانيا: مراقبة الاتصالات الالكترونية في مواجهة الجريمة المعلوماتية.

اولا- مفهوم الجريمة المعلوماتية.

ارتبطت الجريمة المعلوماتية بنظم الاتصالات عن بعد الذي يقوم على التراسل وبث كل انواع البيانات والمعلومات عن طريق الرسائل الالكترونية، لغرض التواصل بالمعلومات التي تشمل نصوص وصور ومعلومات من موقع الى موقع آخر⁽¹⁾،

والمعلوماتية اليوم فهي تعني التعامل مع المعطيات بواسطة وسائل الكترونية التي تقود الى تغيير في الاوليات واعطاء الامكانات التي تؤثر بدورها في مجرى طبيعة ما يمكن تحقيقه⁽²⁾، كما ادرجت منظمة اليونسكو في مفهوم المعلوماتية الفروع العلمية والتقنية والهندسية وأساليب الإدارة الفنية المستخدمة في تداول معالجة المعلومات وتطبيقاتها، اذ تشمل الحاسبات الآلية ووسائل الاتصالات وشبكات المعلومات والبيانات والمعلومات التي يمكن تخزينها ومعالجتها واسترجاعها ونقلها بواسطة هذه الحاسبات أو شبكات المعلومات، وهذه الجريمة تقوم على اساس العلاقة بين المعلومات وبين التقنية الحديثة التي تستخدم في معالجة هذه المعلومة⁽³⁾.

1 - عامر ابراهيم قنديلجي، إيمان فاضل السموراني، شبكات المعلومات والاتصالات، دار المسيرة للنشر والتوزيع، طبعة 2، عمان، 2012، ص، 89.

2 - سمير دنون، العقود الالكترونية في اطار تنظيم التجارة الالكترونية، المؤسسة الحديثة، طبعة 1، لبنان، 2012، ص، 86.

3 - سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2013، ص، 12.

1- تعريف الجريمة المعلوماتية: ان التقنية الحديثة اخترعت لتسهيل حياة الافراد وساعدت المجتمعات المعاصرة في التواصل الحضاري والثقافي، الا ان اساءة استخدام معطياتها ساهم في بروز الجريمة الالكترونية وتحدياتها التي عبرت الحدود، وهددت الامن الوطني والدولي بسبب الانشطة الاجرامية المنظمة والفردية⁽¹⁾، لذلك تعددت تعريفات الجريمة المعلوماتية واصبح من العسير معرفة ما اذا كانت الجرائم المعلوماتية المستحدثة تعتبر من قبيل الحقيقة او الخيال، واصبح من الصعوبة تحديد تعريف معين لها خشية حصرها في مجال ضيق، وخاصة لعدم الاتفاق على وضع مصطلح معين للدلالة على هذه الظاهرة الاجرامية⁽²⁾، ومن بين تعريفاتها:

* الجريمة المعلوماتية هي كل فعل اجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية⁽³⁾.

* الجريمة الالكترونية ترتكب بمهدف تحقيق عوائد مالية ضخمة جراء اعمال غير شرعية في الاقتصاد الدولي عبر شبكة الانترنت، وقد تكون هادفة الى التخريب والاضرار بالغير، او سلوك مناف للأخلاق وغير مشروع يرتبط بالمعالجة الآلية للبيانات او نقلها، اذ يمكن حصر مجالها في نوعين النوع الاول يقع على جهاز الكمبيوتر والوسائل الالكترونية نفسها وما يشملها من انظمة وبرامج ، والنوع الثاني يتعلق بالجرائم التي تتخذ الوسائط الالكترونية وسيلة لتحقيق مآربها الجرمية⁽⁴⁾،

كما تناولت الاتفاقيات الدولية والتشريعات الوطنية الجريمة المعلوماتية انطلاقا من جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مثل الاتفاقية الخاصة بالإجرام المعلوماتي بودابست في 23-11-2001 التي نصت في المادة (11)، " تقوم كل دولة طرف بالاتفاقية بإقرار هذه الاجراءات التشريعية وغيرها من الاجراءات الاخرى، كلما كان ذلك ضروريا، لإصدار نص تشريعي او قانوني بانها تشكل جرائم بموجب القانون الوطني المحلي الخاص بها عند ارتكاب عن قصد، من حيث المساعدة، او التحريض على ارتكاب اية جريمة من الجرائم النصوص عليها وفقا للمواد من 2-10 الخاصة بالاتفاقية بقصد ارتكاب مثل هذه الجريمة." فالاتفاقية جرمت كل فعل اتفاق في جرائم

1 - سمير دنون، مرجع سابق، ص، 89.

2 - محمد علي سالم، حسون عبید هجيج، الجريمة المعلوماتية، مجلة جامعة بابل، المجلد 14، عدد، 6-7، كلية القانون، جامعة بابل، موقع: <https://www.iasj.net/iasj?func=fulltext&aId=3748>

3 - عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، الاسكندرية، 2006، ص، 2.

4 - سمير دنون، مرجع سابق، ص، 90.

المساس بأنظمة المعالجة الآلية للمعطيات في عبارة من حيث المساعدة، واعتبرت ذلك من قبيل الجريمة المعلوماتية.

وفيما يتعلق بالمشروع الجزائري فق تبنى مصطلح المساس بأنظمة المعالجة الآلية للمعطيات للدلالة على هذه الجريمة في المادة (02) من القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، اذ نصت على انه يقصد في مفهوم هذا القانون ما يأتي:

- الجرائم المتصلة بتكنولوجيات الاعلام والاتصال جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات في المواد من 394 مكرر الى 394 مكرر 7 ، واي جريمة اخرى يسهل ارتكابها عن طريق منظومة معلوماتية او نظام اتصالات الكترونية.
- منظومة معلوماتية وهي أي نظام منفصل او مجموعة من الانظمة المتصلة ببعضها البعض او المرتبطة يقوم واحد منها او اكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.
- معطيات معلوماتية وهي كل عملية عرض للوقائع او المعلومات او المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها مقدمو الخدمات سواء كان عام او خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/ او نظام للاتصالات، واي آخر يقوم بمعالجة او تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة او لمستعمليه.

2- اشخاص الجريمة المعلوماتية: تقوم الجريمة المعلوماتية كغيرها من الجرائم على طرفين، يمثل الطرف الاول الجانب والطرف الثاني يمثل المجني عليه، الا انهم يختلفون نوعا ما عن اطراف باقي الجرائم، ويمكن تحديد اشخاص الجريمة المعلوماتية بالآتي:⁽¹⁾

1-المجرم المعلوماتي: يرتبط المجرم المعلوماتي بامتلاكه لمهارات تقنية عالية تستخدم في نظام الحاسبات الآلية، وهذه الشخصية تجعل منه شخصا يتسم بسمات خاصة تضاف الى الصفات الاخرى التي يجب ان تتوفر في المجرم العادي، فالاجرام المعلوماتي يعد اجرام الاذكياء بالمقارنة مع التقليدي الذي يميل الى استخدام العنف، وقد يكون مرتكب الفعل الجرمي المعلوماتي فاعلا اصليا او شريكا، وصفة الفاعل الاصلي في الجريمة المعلوماتية غالبا ما تكون احد العاملين او المستخدمين في منشأة تدار

1 - محمد علي سالم، حسون عبيد هجيج، مرجع سابق، ص، ص، 88، 90.

بالنظام المعلوماتي بصرف النظر عن المستفيد من وراء ارتكاب مثل هذه الافعال، ولما كان هذا النوع من الاجرام يستلزم الدقة والتنفيذ للعمليات غير المشروعة فانه يستلزم كذلك مشاركة او مساعدة اشخاص اخرين سواء اكانوا فنيين ام مجرد وسطاء وقد يكون هذا الاشتراك سلبيا يتمثل بالامتناع بيد انه في الغالب الاعم يتمثل بالمساعدة الفنية والمادية وخصوصا عندما تستلزم اليات الابتكار لمخادعة الحاسب الالي الاستعانة بمجموعة من الوسطاء او الشركاء والمؤتمنين على اسرار اسطوانات الحاسبات الالية اذ يؤدي هؤلاء الدور الرئيسي في نجاح العملية غير المشروع.

ب- المجني عليه: وهو الشخص الذي تلحقه اضرار معينة من جراء حدوث الجريمة المعلوماتية، وقد يكون المجني عليه اما شخص طبيعي او معنوي يتمثل في مؤسسات وقطاعات مالية وشركات ضخمة، الاي ال ان المعلومات المجردة تعد في الوقت الراهن من اهم المصالح المستهدفة بعد الاموال، خصوصا اذا كانت المعلومات ذات اهمية بالغة وكان هدف الجرم المعلوماتي الحصول على مقابل وعوض عن طريق المقايضة غير المشروعة لهذه المعلومات، سواء كانت مخزنة بالحاسوب ام مدخلة في بنوك المعلومات.

معنى ذلك ان المجني عليه في الجريمة المعلوماتية هو كل شخص تعرض لاعتداء او انتهاك لحق من حقوقه او لخصوصية حياته واعماله بواسطة المعلومات والبيانات التي تم اختراقها واستخدامها من الغير بواسطة الكمبيوتر وشبكة الانترنت، مما يؤثر على نتائج المعلومات والتسبب في خسائر على صعيد المؤسسات العامة والافراد، ومن اهم الجرائم المرتبطة بالمعلوماتية نتناول:⁽¹⁾

* **سرقة المعلومات عبر الوسائل الالكترونية:** تتم السرقة في المجال الالكتروني للمعلومات والبرامج المخزنة في الوسائل الالكترونية، كالحصول على الاسرار الصناعية لمواد ما.

* **التجسس بالوسائل الالكترونية:** يهدف من ورائه الى الحصول على المعلومات الاستراتيجية عبر استعمال الشبكة بطريقة غير قانونية والدخول الى انظمة الدول والحكومات والمنظمات، للحصول على ما لديها من معلومات خاصة بنظامها واسرارها الداخلية والخارجية.

* **التفخيخ الالكتروني:** يكون بإدخال وظائف خفية في مرحلة تصميم او نقل او صيانة النظم المعلوماتية يؤدي بعد ذلك وظائف مشبوهة وغير مشروعة لصالح من وضع البرامج.

1 - سمير دنون، مرجع سابق، ص، ص، 91.95.

* الابتزاز بالوسائل الالكترونية: عن طريق التعرض لسرية المعلومات المخزنة في الاجهزة الالكترونية، والتي تتعلق بالأشخاص او الشركات او المنظمات، استغلالها في عملية الابتزاز والتهديد بنشرها في الوسائل الاعلامية والالكترونية قصد التشهير والاضرار.

ومع تنوع اشكال الجرائم عبر الانترنت، الا انها تجتمع في عنصر واحد وهو الحاجة الى عملة ورقية لتسهيل انشطة التبادل التجاري المشروع وغير المشروع عبر اجهزة الكمبيوتر المتصلة بالشبكة، اضافة الى ذلك فقد اضيفت العديد من انتهاكات التي تدخل في جرائم الاعتداء على الشبكة الالكترونية، نظرا لسهولة ارتكاب مثل هذا النوع من الجرائم، وسهولة اخفاء معاملها وصعوبة تتبع مرتكبيها بسبب التقنية العالية التي يستخدمونها في ذلك والتي تصل الى حد الاحترافية والتخصص.

ثانيا- مراقبة الاتصالات الالكترونية ودورها في مواجهة الجريمة المعلوماتية.

سعيًا منه لمواكبة التطورات الاجرامية في مجال تكنولوجيا الاعلام والاتصال، عمد المشرع الجزائري الى تعديل العديد من القوانين الوطنية، يتضح ذلك من خلال صدور القانون رقم 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، والذي تم فيه تحديد الحالات التي تسمح باللجوء الى مراقبة الاتصالات الالكترونية، كما تضمن قانون العقوبات في الباب السابع منه عنوان المساس بأنظمة المعالجة الآلية للمعطيات، سعيًا منه لضمان الحماية الجنائية للمعاملات الالكترونية، وتم في اطار ذلك انشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، من خلال المرسوم الرئاسي رقم 15-261 المؤرخ في اكتوبر 2015، الذي يحدد تشكيلة وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.

وحتى نكون بصدد نظام معلوماتي لا يشترط ان يتوفر فيه حجم معين ولا تعدد او قلة للعناصر المادية المكونة له او التي هي باتصال به، كما ان الشخص الذي يقوم بارتكاب هذه الجريمة يعتبر غريبا لأن ذلك النظام المعلوماتي ليس ملك له، وعليه فان المساس بنظم المعالجة الآلية للمعطيات المعلوماتية يعتبر هو الآخر وسيلة تؤدي الى ارتكاب الجرائم ضد الاشخاص والحريات الفردية في محيط المعلوماتية بالأخص مع وجود شبكة الانترنت.

والمشرع لم ينص صراحة على المعلوماتية وشبكة الانترنت في قانون العقوبات كوسيلة لارتكاب اي نوع من جرائم الاعتبار، الا اننا نلمس ذلك من خلال العبارات التي توحى بالمعنى كالصيح او التهديد او الكتابة او المنشورات او الاعلانات موضوع الجريمة، هاته الاخيرة التي اصبح فيها

استخدام شبكة الانترنت ونظام المعلوماتية آلية سهلة وبسيطة لاخترق اي معلومات وبيانات، وبالتالي فان السب او القذف او الاهانة باستخدام التقنية المستحدثة التي تعتمد على الشبكة المفتوحة، تقتزن بضرورة توافر الانظمة المعلوماتية الجديدة مثل الهاتف المحمول او مختلف الانواع الاخرى من الاجهزة الالكترونية التي تكون مزودة بشبكة الانترنت وهي تمثل جرائم معلوماتية. ومن اجل مواجهة الجريمة المعلوماتية والحد من آثارها، حاول المشرع الجزائري اصدار قوانين عامة وخاصة وهياكل للتصدي لهذا النوع من الجرائم، مثل القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في القانون رقم 09-04 ، ووضع بموجب هذا القانون ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية، سعيا منه للحفاظ على النظام العام ومستلزمات التحريات والتحقيقات القضائية الجارية

1- مراقبة الاتصالات الالكترونية: حاول المشرع الجزائري في الدستور المعدل والمتمم لسنة 2016 من وضع جملة من البيانات التي تكفل حماية البيانات الخاصة بالأشخاص الطبيعيين خلال عملية المعالجة الآلية للمعطيات، اذ نصت المادة (46) منه على انه " لا يجوز انتهاك حرمة المواطن الخاصة، وحرمة حياته الخاصة بحميها القانون، سرية المراسلات والاتصالات الخاصة بكل اشغالها مضمونة. لا يجوز باي شكل المساس بهذه الحقوق دون امر معلل من السلطة القضائية، ويعاقب القانون على انتهاك هذا الحكم. حماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق اساسي يضمنه القانون ويعاقب على انتهاكه." والملاحظ ان المشرع الجزائري الوحيد في اغلب الدساتير العربية الذي تطرق لحرمة البيانات الخاصة من المعالجة الالكترونية ، بحيث تكتفي جلها بتكريس الحماية الدستورية للمراسلات بكل اشكالها فقط، وخول السلطة القضائية استثناء في اطار قرارا معلل بأن تتبع اجراءات تمس البيانات الشخصية بالنظر الى خطورة بعض الجرائم المعلوماتية المحددة حصرا في تسجيل الاتصالات الالكترونية ⁽¹⁾

1 - أمحمدي بوزينة امنة، اجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية، دراسة تحليلية لاحكام قانون الاجراءات الجزائية وقانون الوقاية من جرائم الاعلام، الملتقى الوطني، آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، مركز جيل البحث العلمي، الجزائر العاصمة، 29 مارس 2017، ص، 73.

ومن اجل ذلك وضع المشرع بموجب القانون رقم 04-09، ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية، سعيا منه للحفاظ على النظام العام ومستلزمات التحريات والتحقيقات القضائية الجارية⁽¹⁾

أ- حالات مراقبة الاتصالات الالكترونية: حددت المادة (04) من القانون رقم 04-09 الحالات التي يسمح فيها باللجوء الى المراقبة الالكترونية وحصرها في :

- * الوقاية من الأفعال الموصوفة بجرائم الإرهاب او التخريب او الجرائم الماسة بأمن الدولة.
- * توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام او الدفاع الوطني او مؤسسات الدولة او الاقتصاد الوطني.
- * مقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول الى نتيجة تهم الأبحاث الجارية دون اللجوء الى المراقبة الإلكترونية.
- * تنفيذ طلبات المساعدة القضائية الدولية المتبادلة، استنادا الى اذن مكتوب من السلطة القضائية المختصة.

ومن اجل السير الحسن لآلية مراقبة الاتصالات، وضمان تحقيق الاغراض التي اوجدتها عد المشرع الى وضع عدة ضمانات، تحقق الممارسة الفعلية لهذه الرقابة منها: ⁽²⁾.

- وضع آلية اقرار المراقبة الالكترونية تحت سلطة القضاء: نص المشرع في الفقرة الثانية من المادة (04) من القانون رقم 04-09 على انه " لا يجوز اجراء عمليات المراقبة، الا بإذن مكتوب من السلطات القضائية المختصة." وعندما يتعلق الامر بجرائم الاهاب او التخريب او الجرائم الماسة بأمن الدولة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية اذنا لمدة 6 اشهر قابلة للتجديد على اساس تقرير يبين الترتيبات التقنية المستعملة والاعراض الموجهة له.

1 - المادة 03 من القانون رقم 04-09 مؤرخ في 14 شعبان 1430 الموافق 5 اوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، جريدة رسمية ، عدد 47، بتاريخ 16 اوت 2009.

2 - محمدي بوزينة امينة، مرجع سابق، ص، ص، 74، 75.

- تحديد تقنيات الرقابة الالكترونية وحدود استعمال المعطيات المتحصل عليها: ارتبطت هذه التقنيات بتجميع وتسجيل معطيات ذات صلة بالحالات الواردة على سبيل الحصر السابقة ، والتقنيات التكنولوجية التي يمكن استعمالها في اطار المراقبة الالكترونية تتمثل في اعتراض المراسلات الالكترونية ، تسجيل الاصوات، التقاط الصور، تفتيش المنظومات المعلوماتية وحجزها، كما هو محدد في المادة (65) من القانون رقم 19-15 المعدل والمتمم لقانون العقوبات.

- سن عقوبات لإفشاء معلومات ذات طابع شخصي ناتجة عن المراقبة الالكترونية: نظرا لإمكانية اطلاع الموظفين القائمين على عمليات المراقبة الالكترونية على المعلومات ذات الطابع الجرمي او ذات الطابع الشخصي، فانهم ملزمون باحترام السر المهني وفي حال استغلال عمليات المراقبة لأغراض شخصية او كل تجاوز لحدود المراقبة الالكترونية، نحو انتهاك الحزمة الخاصة للأفراد او افشاء مستندات ناتجة عن التفتيش واطلاع الغير عليها بصفة غير قانونية.

ولضمان الحماية الجنائية للمعاملات الالكترونية، تم انشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، من خلال المرسوم الرئاسي رقم 15-261 المؤرخ في اكتوبر 2015، والذي يحدد تشكيلة وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، تتولى ممارسة اختصاصاتها الحصرية في مجال مراقبة الاتصالات تحت رقابة قاض مختص⁽¹⁾، ويخضع الموظفون الذين يدعون الى الاطلاع على معلومات سرية الى اداء اليمين امام المجلس القضائي قبل تنصيبهم، وهم ملزمون بالسر المهني⁽²⁾.

2- تفتيش المنظومات المعلوماتية: اشار المشرع الى انه يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في قانون الإجراءات الجزائية والحالات السابقة المنصوص عليها في القانون رقم 09-04، الدخول بغرض التفتيش ولو عن بعد الى:⁽³⁾

* منظومة معلوماتية او جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

* منظومة تخزين معلوماتية.

1 - المادة 41 مرسوم رئاسي رقم 15-261 مؤرخ في 24 ذي الحجة 1436 الموافق 8 اكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، جريدة رسمية، عدد 53، بتاريخ 8 اكتوبر 2015، ص، ص، 16، 17.

2 - المرجع نفسه، المادة 28 .

3 - المادة 05 من القانون رقم 09-04، مرجع سابق.

وان وجدت في الحالة الأولى اسباب تدعو للاعتقاد بان المعطيات المبحوث عنها مخزنة في منظومة معلوماتية اخرى وان هذه المعطيات يمكن الدخول اليها، انطلاقا من المنظومة الأولى يجوز تمديد المنظومة او جزء منها بعد اعلام السلطة القضائية المختصة مسبقا اما ان كانت المعطيات المبحوث عنها مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، يختلف الأمر على الحالة الأولى، لأن الحصول عليها يكون مرتبط بطلب المساعدة من السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل، وهذا ما يثير اشكالية القانون الواجب التطبيق، طالما ان ذلك يتعدى حدود اقليم الدولة.

ومن اجل تسهيل اجراءات المراقبة اشارت الفقرة الاخيرة من المادة (05) الى اجراء آخر يتمثل في اللجوء الى الاشخاص المؤهلين كالخبراء والتقنيين في الاعلام الآلي وفن الحاسوب لإجراء عمليات التفتيش على المنظومة المعلوماتية وتزويد السلطات المكلفة بالمعطيات التي تحتاجها لعملية التفتيش.

3- حجز المعطيات المعلوماتية: اكدت المادة (06) من القانون رقم 09-04، انه عندما تكتشف السلطة التي تبشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم او مرتكبيها وانه ليس من الضروري حجز كل المنظومة يتم نسخ المعطيات محل البحث والمعطيات اللازمة لفهمها على دعامه تخزين الكترونية تكون قابلة للحجز والوضع في احرارز وفقا للقواعد المقررة في قانون الاجراءات الجزائية.

واذا استحال اجراء الحجز وفقا لأسباب تقنية، يتعين عللا السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول الى المعطيات التي تحتويها المعلوماتية والى نسخها، والتي تكون موضوعة تحت تصرف الاشخاص المرخص لهم باستعمال هذه المنظومة، وتحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، الا في الحدود الضرورية للتحريات والتحقيقات القضائية⁽¹⁾.

الى جانب ذلك اشارت المادة (10) من القانون رقم 09-04، على انه يتعين على مقدمي الخدمات كتمان سرية المعلومات التي ينجزونها بطلب من المحققين والمعلومات المتصلة بها تحت طائلة

1 - محمدي بوزينة امانة، مرجع سابق، ص، 77.

العقوبات المقررة لإفشاء اسرار التحري والتحقيق، وحدد القانون المدة اللازمة لحفظ المعطيات بسنة واحدة من تاريخ التسجيل، والزمت المادة (12) على مقدمي الخدمات التزامات خاصة: ¹
*التدخل الفوري لسحب المعطيات المخالفة للقانون وتخزينها او منع الدخول اليها باستعمال وسائل فنية وتقنية.

* وضع الترتيبات التقنية لحصر امكانيات الدخول الى الموزعات التي تحتوي معلومات مخالفة للنظام العام واخبار المشتركين لديهم بوجودها

الخاتمة:

وخلاصة لما سبق ذكره في هذه الورقة البحثية، فان المشرع الجزائري حاول في نصوصه القانونية قدر المستطاع الامام بكل الجوانب الاجرائية والموضوعية لمواجهة الجريمة المعلوماتية التي اصبحت من القضايا الشائكة، اذ تحتاج الى تكثيف الجهود من اجل مواجهتها في مجال تحقيق الامن السيبراني كمصطلح جديد يتعلق بجرائم تكنولوجيا الاعلام والاتصال ومكافحتها، وذلك عن طريق تنظيم الملتقيات الوطنية وتحسيس الأفراد بأهمية اليقظة في التحكم في التكنولوجيات الحديثة، وترقية مستوى تكوينهم في مجال امن وحماية المعلومة، والتنبيه بمخاطر سوء استعمالها اضافة الى توسيع اشراك فواعل جديدة بوسعها المساهمة في صيانة عقيدة الدفاع الوطني وضرورة تكوين اشخاص مؤهلين ومتخصصين في مجال الامن السيبراني، واجراء مؤتمرات علمية لمناقشة كل الاشكاليات التي تطرأ في هذا المجال، الى جانب الاستفادة من تجارب الدول الرائدة في مجال تحقيق الامن السيبراني والتعرف على افضل التقنيات العالمية المنتهجة في مكافحة الجرائم الإلكترونية من قرصنة وتحسس واعتماد سياسة وقائية لنشر لزيادة الوعي المجتمعي بمختلف المخاطر والتهديدات التي تفرضها الثورة التكنولوجية الحديثة.

قائمة المراجع:

أ- الكتب

- 1- خالد ممدوح ابراهيم، لوجستيات التجارة الالكترونية، دار الفكر الجامعي، طبعة 1، الاسكندرية ، 2008 ،

1 - المرجع نفسه، ص، 78.

- 2- سعيد غالب ياسين، نظم المعلومات الادارية، دار اليازوري العلمية، طبعة، الاردن، 2009،
- 3- عامر ابراهيم قنديلجي، ايمان فاضل السمورائي، شبكات المعلومات والاتصالات، دار المسيرة للنشر والتوزيع، طبعة 2، عمان، 2012
- 4- سمير دنون، العقود الالكترونية في اطار تنظيم التجارة الالكترونية، المؤسسة الحديثة، طبعة 1، لبنان، 2012
- 5- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، الاسكندرية، 2006.

ب- الرسائل العلمية

- 1- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير ، علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2013.

ج- المؤتمرات العلمية

- 1- أمحمدي بوزينة امنة، اجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية، دراسة تحليلية لأحكام قانون الاجراءات الجزائية وقانون الوقاية من جرائم الاعلام، الملتقى الوطني، آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، مركز جيل البحث العلمي، الجرائر العاصمة، 29 مارس 2017، ص، 73.

د- القوانين والمراسيم

- 1- القانون رقم 09-04 مؤرخ في 14 شعبان 1430 الموافق 5 اوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، جريدة رسمية ، عدد 47، بتاريخ 16 اوت 2009.
- 2- مرسوم رئاسي رقم 15-261 مؤرخ في 24 ذي الحجة 1436 الموافق 8 اكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، جريدة رسمية، عدد 53، بتاريخ 8 اكتوبر 2015.

مراقبة المراسلات والاتصالات الإلكترونية كأسلوب للتحري والتحقق في الجرائم المعلوماتية

د/ روابح فريد

كلية الحقوق والعلوم السياسية- جامعة سطيف

مقدمة:

يسعى قانون الإجراءات الجزائية إلى الكشف عن حقيقة الجريمة ومرتكبيها بوصول المحققين ورجال القضاء إلى المعلومات المتعلقة بالوقائع الجرمية وأدلتها والأشخاص الضالعين فيها، وهو ينظم حسب ما تقتضيه حماية المصلحة العامة للمجتمع كيفية وحدود المساس بالحقوق والحريات الفردية خاصة ما يتعلق بسرية وخصوصية مراسلاته واتصالاته الإلكترونية المضمونة دستورياً وتشريعياً. حيث لا تعتبر هذه الحماية مطلقة، لأن إطلاقها يمكن أن يكون عائقاً في كشف الجرائم ومرتكبيها، وبالتالي يمكن أن تزول الحماية الجزائية عن خصوصية المراسلات والاتصالات الإلكترونية إذا استخدمت لأغراض مكافحة الجريمة أو البحث والتحري عنها وعن أدلتها.

فإن أهمية الإنترنت كوسيلة تقنية متطورة ومتسارعة للاتصال وتبادل المعلومات بين بلدان العالم في مختلف قطاعاتها ومؤسساتها وبين الأفراد، فالجرائم المرتكبة بواسطة الإنترنت والشبكات الرقمية في تطور مستمر مع التقدم التكنولوجي فقد أصبح المجرمون وجماعات الإجرام يستغلون الإنترنت في مختلف أنشطتهم، كالإعلان عن المخدرات، والإتجار بها عبر الإنترنت والتمويه والتستر على جرائمهم، وكذا تبادل الرسائل فيما بينهم⁽¹⁾.

وتدليلاً للصعوبات التي تطرحها مسألة البحث عن الجريمة المعلوماتية ومكافحتها استحدثت المشرع الجزائري أساليب خاصة للتحري والتحقق فيها، من بينها أسلوب مراقبة الاتصالات الإلكترونية، ونظم أحكامها في المواد 65 مكرر 5 إلى 65 مكرر 10 من ق إ ج، وفي قانون الوقاية من جرائم تكنولوجيا الإعلام والاتصال ومكافحتها.

(1) عادل عبد الجواد محمد الكردوسي، التعاون الأمني العربي ومكافحة الإجرام المنظم عبر الوطني، مكتبة الآداب، القاهرة، الطبعة الأولى 2005 ص 190.

تتمحور الإشكالية الرئيسية التي يُناقشها البحث حول مدى فعالية أسلوب مراقبة المراسلات والاتصالات الإلكترونية في التحري والتحقيق عن الجريمة المعلوماتية؟ حيث تُقاس فعالية الإجراء بمدى احترام شروط استخدامه وتنفيذه، وعليه تُناقش الإشكالية ضمن مبحثين:

المبحث الأول: التعريف بمراقبة المراسلات والاتصالات الإلكترونية كأسلوب خاص للتحري والتحقيق
المبحث الثاني: شروط مراقبة المراسلات والاتصالات الإلكترونية أثناء التحري والتحقيق

المبحث الأول: التعريف بمراقبة الاتصالات الإلكترونية كأسلوب خاص للتحري والتحقيق
تبيّن في هذا المبحث مفهوم التراسل والاتصال الإلكتروني، ومفهوم المراقبة الإلكترونية المنصّب عليه ومدي مشروعية ذلك في القانون الجزائري مُقارنةً بتشريعات بعض الدول.

المطلب الأول: تعريف مراقبة الاتصالات الإلكترونية وتقنياتها:

الفرع الأول: تعريف مراقبة المراسلات والاتصالات الإلكترونية:

أولاً: مفهوم المراسلات والاتصالات الإلكترونية:

(أ) في بعض الدول الأوروبية: في فرنسا حسب مفهوم المادة 32 من قانون البريد والمواصلات، فالإتصالات الإلكترونية هي كل وسيلة تُستعمل في إرسال أو استقبال أو نقل لإشارات أو علامات للكتابة أو الصورة أو الصوت، أو تسجيل مهما كانت طبيعته، عبر الأسلاك أو الألياف البصرية أو الراديو كهربية أو أيّة وسيلة كهرومغناطيسية⁽¹⁾. وُحُدّت طبيعة المراسلات السلكية واللاسلكية في المادة 15-226 من قانون العقوبات، بأنّها كل أنواع الاتصالات التي تتمّ عن بُعد سواء كانت عن طريق الهاتف أو الفاكس أو البريد الإلكتروني والإنترنت والأقمار الصناعية⁽²⁾.

وفي بلجيكا يأخذ قانون العقوبات في المواد 259 مُكرّر فقرة 1 و 314 مُكرّر فقرة 1 من بالمفهوم الواسع، الذي قضت به محكمة النقض البلجيكية بأنّه يشمل كل ما يتمّ ذكره سواء شفاهة أو ليس

(1) Frédéric DESPORTES, Laurence LAZERGES-

COUSQUER, Traité de procédure Pénale, 3e éd, ECONOMICA, Paris, 2009, p 1367.

(2) Code Pénal, Annotation par Yves MAYAUD, Code Pénal, éd DALLOZ, n° 108, Annotation de jurisprudence et bibliographie par Yves MAYAUD. Paris Cedex 2011, p 820.

شفاهة، وسواء مباشرة أو عن بُعد وجميع الأشكال الحديثة لخدمات الإتصال عبر شبكة الإعلام الآلي، ووسائل الإتصال السلكي واللاسلكي التي تشمل أجهزة الإرسال المتمثلة في العناصر الصوتية من خلال هاتف ثابت أو خلوي (GSM) أو الحاسوب، والإشارات الإلكترونية للنصوص أو الصور مثل البريد الإلكتروني وغيره⁽¹⁾.

(ب) في الجزائر: يتضح مفهوم المراسلات والاتصالات الإلكترونية من خلال عدّة قوانين:

1. في قانون البريد والاتصالات الإلكترونية 18-04⁽²⁾ عرّف المشرع الاتصالات الإلكترونية في المادة 10 منه بقوله " يُقصد بالاتصالات الإلكترونية في مفهوم هذا القانون، كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها، عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية ". وكان يُصطلح عليها " الاتصالات السلكية واللاسلكية " في قانون قانون البريد والمواصلات السابق الملغى 032000⁽³⁾. وهو ذاته التعريف الذي ورد ضمن المادة الثالثة من قانون حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي 18-07 المؤرخ في 10 يونيو 2018⁽⁴⁾. وعرّفت الفقرة 16 من نفس المادة 10 المذكورة أعلاه، خدمة الإتصال الإلكتروني للجمهور بأنها " كل خدمة تتمثل كلياً أو أساساً في تزويد الجمهور بالاتصالات الإلكترونية، وكذا الخدمات التي تستعمل قدرات شبكات الاتصالات الإلكترونية والتي تتطلب زيادة على خدمة الاتصالات الإلكترونية القاعدية وظائف المعالجة أو التخزين ". كما عرّفت " الإنترنت " الفقرة 5 من نفس المادة بأنها شبكة معلوماتية عالمية تتشكل من مجموعة شبكات وطنية وإقليمية وخاصة، موصولة فيما بينها عن طريق بروتوكول الاتصال (IP) لتُقدم واجهة موحدة لمستعملها.

(¹) Christian De VALKENEER, KAMINSKI Dan, " Au croisement de la recherche proactive et des écoutes téléphoniques: construction et danger du mutualisme légistique ", Revu de droit pénal et de criminologie, année 83 Mars 2003 Bruxelles,, p 311 - 312.

(²) قانون رقم 18-04 المؤرخ في 10 مايو 2018 ج ر، 27 في 13 مايو 2018.

(³) قانون رقم 2000-03 المؤرخ في 5 غشت 2000، ج ر 48 بتاريخ 6 غشت 2000.

(⁴) ج ر، عدد 34 بتاريخ 10 يونيو 2018.

2 في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها رقم 09-04⁽¹⁾ عرّفتُ الفقرة (د) من المادة الثانية منه "الاتصالات الإلكترونية" بأنها "أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صورة أو أصوات أو معلومات مُختلفة بواسطة أية وسيلة إلكترونية". وأُضيفت عبارة "بما في ذلك وسائل الهاتف الثابت والنقال" بموجب المادة 5 من المرسوم الرئاسي 261.15 مؤرخ في 8 أكتوبر 2015 يُحدّد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال⁽²⁾.

ثانياً: الحماية القانونية للمراسلات والاتصالات الإلكترونية:

(أ) التشريع الفرنسي: من بين أنواع الحماية القانونية نذكر الحماية الجزائية بنصّ المادة 226-15 من قانون العقوبات، للاتصالات الإلكترونية الهاتفية السلكية منها واللاسلكية، والاتصالات التي تتمّ عبر شبكات الإعلام الآلي (Télématiques). وذلك ضدّ كافة أنواع أفعال الإعتراض لهذه الاتصالات، حيث يُمكن أن تكون الجريمة قائمة عند بداية المكالمة أو عند إرسال المراسلة أو عند وصولها، مثلاً عن طريق الدخول في الخط عبر خط آخر، أو عن طريق التطفل على صندوق البريد الإلكتروني المؤمن بالرقم السري⁽³⁾.

(ب) في التشريع الجزائري: تتظاهر عدّة قوانين لحماية سرية وخصوصية الاتصالات الإلكترونية من بينها:

1. قانون البريد وتلاصقات الاتصالات الإلكترونية: تُلزم المادة 119 مُتعاملي الاتصالات الإلكترونية باتخاذ التدابير التي من شأنها أن تضمن سرّية المكالمات والمعلومات التي يحوزونها عن مشتركهم، وألاًّ يسمحوا بوضع أي ترتيبات بغرض اعتراض الاتصالات أو مراقبة المكالمات الهاتفية والوصلات والمحادثات والمبادلات الإلكترونية دون إذن مسبق من السلطة القضائية. ويجب عليهم أن يُطّلعوا أعوانهم على الإلتزامات التي يخضعون لها والعقوبات التي يتعرضون لها في حالة عدم احترامهم لهذه الأحكام. كما تُلزم المادة 160 المتعاملين في شبكات الاتصالات الإلكترونية وكذا مستخدميهم

(1) ج ر، عدد 47 بتاريخ في 16 غشت 2009.

(2) ج ر عدد 53 بتاريخ 8 أكتوبر 2015.

(3) Jean PRADEL; Michel DANTI-JUAN, Manuel de droit pénal spécial, éditions Cujas, n° 03, Paris, 2004, p 209.

باحترام سرية المراسلات الصادرة عن طريق الاتصالات الإلكترونية وشروط حماية الحياة الخاصة والمعلومات الإسمية للمشاركين. وتناولتها أحكام جزائية في المواد 164. 166.

2. في قانون العقوبات: يكفل المشرع لهذا النوع من المراسلات والاتصالات حماية جزائية في سريتها وخصوصيتها، حيث أنّ اعتراضها أو الاطلاع عليها أو تحويلها يُعتبر جنحة اعتداء على حرمة الحياة الخاصة طبقاً للمواد 303 مكرر. 303 مكرر، ويمكن أن تُشكّل جنحة المساس بأنظمة المعالجة الآلية للمعطيات بالمواد 394 مكرر إلى 394 مكرر من ق ع ج. حيث عُرِفَت جرائم تكنولوجيا الإعلام والاتصال في الفقرة (أ) من المادة 2 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنّها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى تُرتكب أو يُسهّل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية. وكذلك يُجرّم عدم قيام مُقدّم خدمات الإنترنت، لالتزامه بالتدخل وسحب أو تخزين أو حجب محتويات تُشكّل جرائم، وعدم وضع الترتيبات التقنية التي تسمح بالسحب والتخزين (الم 394 مكرر 8). بالإضافة إلى جريمة الإرهاب الإلكتروني في المواد 87 مكرر 11 و 87 مكرر 12 ق ع ج⁽¹⁾.

3. في قانون الوقاية من جرائم تكنولوجيا الإعلام والاتصال ومكافحتها (2) يتضمّن هذا القانون الكثير من الأحكام التي فيها حماية لسرية وخصوصية الأفراد، مثل المادة 3 منه التي نصّت على أنّه يجب مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات عند وضع الترتيبات التقنية لمراقبة الاتصالات الإلكترونية وتسجيلها وتجميعها عندما يقتضيها ضرورات التحريات والتحقيقات القضائية الجارية، أو يقتضيها الحفاظ على النظام العام. والمادة 4 التي أوجبت أن تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة (أ) في إطار احترام الحياة الخاصة للغير تحت طائلة العقوبات. كما أنّ المادة 27 من المرسوم الرئاسي 15-261 المنظم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، ألزمت مُستخدمي الهيئة بالسر

(1) أضيفت المواد 87 مكرر 11 و 87 مكرر 12 و 394 مكرر 8 بالقانون 02-16 في 19 يونيو 2016، ج ر، عدد 37 لسنة 2016.

(2) قانون 04-09 المؤرخ في 05 غشت 2009، ج ر، عدد 47 مؤرّخة في 16 غشت 2009.

المهني وواجب التحفظ، حيث يؤدّون يمينًا يُقسمون فيه على كتمان سرية المعلومات التي يُحصلونها أثناء تنفيذ مراقبة الاتصالات الإلكترونية.

ثالثًا: مفهوم مراقبة المراسلات والاتصالات الإلكترونية

يتمّ هذا النوع من المراقبة عن طريق اعتراض المراسلات والاتصالات الإلكترونية بالتقاطها أو الاطلاع عليها أو تسجيلها أو نقلها، حيث يُعرّف اعتراض الاتصالات هنا بأنه إدخال تدابير تقنية مُغلّطة في خط أحد المشتركين لتسجيل المكالمات عن طريق البحث عن مصدر الإتصال من خلال عنوان (IP) في جهاز الحاسب الآلي الذي يجري منه الإتصال بالموقع ولا يُعتبرُ اعتراضًا للمراسلة الإلكترونية مُجرّد ربط الإتصال بشبكة الإنترنت (Se connecter) وقراءة ما يمكن لأي مُتصل قراءته دون إحداث تعديلات مُسبقة بتدابير تقنية مُغلّطة، وهو يُشبه تعريف اعتراض المكالمات الهاتفية ولذلك اتفق الفقه والقضاء على تطبيق أحكام هذا الأخير على الإتصالات والمراسلات بواسطة الإنترنت⁽¹⁾. وتناولت اتفاقية بودابست للجرائم الإلكترونية 23 نوفمبر 2001 في المادتين 20 و21 أحكام تجميع ومراقبة البيانات أثناء الزمن الفعلي، وهي البيانات التي تتم أثناء التراسل وتبادل الاتصالات من خلال نظام المعالجة الآلية للمعطيات، حيث تشير عبارة "مراقبة الإتصالات" في هذه النصوص إلى شبكات الإتصالات التقليدية التي تكون بنيتها الأساسية هي الكابل بما في ذلك نظام الهاتف أو الألياف البصرية والهاتف النقال باستخدام نُظم شبكات الأقمار الصناعية الخاصة، وشبكات الحاسوب التي تتخذ الطابع العالمي⁽²⁾.

الفرع الثاني: تقنيات مراقبة المراسلات والاتصالات الإلكترونية:

أولاً: حفظ مُعطيات حركة السير (Conservation des données de trafic)

في إطار الانترنت يكون مُزوّد خدمات الانترنت (ISP) هو المسيطر على مُخرجات حركة البرامج فهو الذي يسمح بدخولنا إلى الإنترنت (Log in) والتمتع بخدماتها. ولمعرفة زمن الدخول إلى الإنترنت من قبل مرتكب الجريمة لا يتم اللجوء إلى حاسوب المستخدم في العادة، وإنما يتم اللجوء

(1) Myriam QUEMENER, Yves CHARPNEL, Op cit, p169,245.

(2) أنظر أنظر عمر مُحمّد بن يونس، الإتفاقية الأوروبية حول الجريمة الافتراضية (المذكرة التفسيرية)، منشورات الإتحاد الأوروبي، الطبعة الأولى المجرّبة 2005، ص166، 163، 161.

إلى مزود خدمات الانترنت. وتفيد مخرجات حركة البرامج في إطار جرائم الانترنت كونها تُساهم في ربط السلطات بالجرم المعلوماتي بالسرعة الكافية.

يُعتبر حفظ البيانات أداة تحقيق جديدة في إطار جرائم الحاسوب والجرائم المرتبطة بها، حيث تكون البيانات محلاً للتلاعب، مما يؤدي بالدليل إلى الضياع بسهولة من خلال الإهمال في التخزين، أو التلاعب العمدي أو الحذف المصمم بتدمير الدليل، أو الحذف الروتيني للمعلومات التي لم تعد لها حاجة. ولذلك يجب أن يكون المسؤول عن حفظ البيانات جديرًا بالثقة وله سمعة مهنية جيدة، يُمكن معه تأمين مصداقية البيانات استنادًا إلى أمر حفظ البيانات. كما أنّ الكم الهائل من التراسل والاتصالات يمكن أن يؤدي إلى تداخل المعطيات، فيُصبح تحديد مصدر الإتصال أو جهة إرساله مهم جدًا لمعرفة هوية مرتكبي الجريمة، ولهذا فحفظ حركة البيانات المتعلقة بالإتصال هو أمر لازم لأنه هو الذي يسمح بتتبع الإتصال ومعرفة مصدره، فيكون هذا الإجراء أفضل من التفتيش والضبط المعلوماتي⁽¹⁾.

أ) في الجزائر وبهدف مساعدة السلطات القضائية المكلفة بالتحري والتحقيق، يقوم مقدّمو الخدمات بحفظ مُعطيات حركة السير بتسجيلها والإحتفاظ بالتسجيلات المدة سنة من تاريخ التسجيل. وهي المعطيات التي عرّفها الفقرة(هـ) من المادة2 من قانون الوقاية من جرائم تكنولوجيا الإعلام والإتصال، بأنّها " أي مُعطيات متعلقة بالإتصال عن طريق منظومة معلوماتية تُنتجها هذه الأخيرة باعتبارها جزءًا من حلقة اتصالات، توضح مصدر الإتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الإتصال ونوع الخدمة". ونصّت المادة11 على الالتزام المفروض على مُقدّمي خدمات الإنترنت بحفظ معطيات حركية السير وبيّنت أنواعها.

ب) وفي فرنسا تفرض المادة34 من قانون البريد والاتصالات الإلكترونية على مُوردي خدمات الإنترنت التزامًا بحفظ المعطيات غير المشروعة من أجل تقديمها عند الحاجة إلى السلطات القضائية والمصالح المكلفة بمحاربة الإرهاب، دون أن يُنشئوا ملفات أو قوائم إسمية لمستخدمي الشبكة، ولا القيام بحفظ الاتصالات التي تتم بواسطة الرسائل القصيرة ال (SMS) أو عن طريق ال (e-mail). كما أنّ قانون مكافحة الإرهاب 2006-64 المؤرخ 23 جانفي 2006 يوسّع هذا

(1) عمر مُحمّد بن يونس، " الدليل الرقمي "، (المؤتمر الدولي الثاني لقانون الانترنت، مالطا من 27 إلى 31 نوفمبر 2006)، منشورات المنظمة العربية للتنمية الإدارية بجامعة الدول العربية، 2006، ص8.

الإلتزام بالحفظ إلى مقاهي الإنترنت والأشخاص الذين يُورَدون لربائتهم خدمة الإنترنت كالفنادق وشركات الطيران بصفة مجانية أو بمقابل عبر اللاسلكي (WIFI). وصدر في فرنسا أيضًا مرسوم خاص بهذا الإجراء وهو المرسوم 358-2006 المؤرخ في 24 مارس 2006 يتعلق بحفظ مُعطيات الإتصال الإلكتروني، يُحدّد بالتفصيل أنواع المعطيات التي يجب حفظها، وهي التي حصرتها المادة (1L34) من هذا القانون⁽¹⁾.

(ج) وفي اتفاقية بودابست لجرائم الإنترنت لسنة 2001، نصّت على هذا الإجراء المادة 16 وكيفية الحصول على حفظ مُعجّل لبيانات حاسوب مُحدّدة أثناء قيام إجراء جنائي مُحدّد ضمن الإختصاص الوطني للسلطات القضائية. حيث عرّفت الاتفاقية في المادة الأولى فقرة (b) حركة البيانات (Traffic data) بأنّها: " صنفٌ من بيانات الحاسوب التي تُشكل محلاً لنظام قانوني مُحدّد، حيث يتم تولّد هذه البيانات من الحواسيب عبر تسلسل حركة الإتصالات لتحديد مسلك وشكل الإتصالات من مصدرها إلى الجهة المقصودة". وتشمل حركة البيانات خاصّةً "المصدر" الذي يُشير إلى رقم الهاتف أو عنوان الـ (IP) بروتوكول الإنترنت (Internet Protocol)، و" الوجهة المقصودة " أي الإشارة التي يتم إرسال الإتصال إليها، و"نوع الخدمة التي يحتويها" أثناء الإتصال مثل البريد الإلكتروني أو المراسلات الفورية.

ويتطلب حفظ البيانات أن توضع هذه البيانات في هيئة مخزنة ومحمية من أي شيء يمكن أن يتسبّب في تغيير أو تعيب معالمها الفعلية والإستمرار في تأمينها من التعديل والتدمير والحذف. لكن لا يعني حفظ البيانات تجميدها بخاصية منع الدخول إليها مثلاً، وأن لا يكون هناك مجال لنسخها، وأن لا يتم الإستعانة بها ولو بشكل مشروع. وتُحدّد الفقرة الثانية من المادة 16 من اتفاقية بودابست الحد الأقصى لمدة الحفظ بـ 90 يوماً للسماح للسلطات المختصة باتخاذ الإجراءات الضرورية للكشف عنها⁽²⁾.

(¹) Myriam QUEMENER, Yves CHARPNEL, Op cit, p 176.

(²) أنظر عمر مُحمّد بن يونس، عمر مُحمّد بن يونس، الجريمة الافتراضية، المرجع السابق، ص 55-57. 124، 128، 130.

ثانيًا: التسرب الرقمي (Infiltration numérique)

التسرب الرقمي هو تسلل معلوماتي يسمح بالدخول بطريقة احتيالية مُخادعة في مُنتدى حوار، أو على المواقع. وهو يُعدُّ من تقنيات التحري الإستثنائية التي لا يجب أن تُستخدم إلا من طرف مُحققين مؤهلين خصيصًا مركزين أو جهويين، في إطار التحري والتحقيق عن الجريمة المنظمة المنصوص عليها في المادة 73-706 من ق إ ج ف فقط. وفي القانون رقم 297-2007 المؤرخ في 5 مارس 2007 المتعلق بالوقاية من الإجرام، عدّلت المادة (35 III) منه قانون الإجراءات الجزائية الفرنسي من أجل السماح لضباط الشرطة القضائية المؤهلين خصيصًا للقيام بالتسرب بغرض تسهيل مُعانة بعض الجرائم التي تُرتكب بواسطة وسائل الإتصال الإلكتروني وجمع أدلتها وكشف مرتكبيها. وتُتيح المادة 73-706/1 من ق إ ج ف لضباط الشرطة القضائية المتخصصين أثناء التحريات أو بموجب إنابة قضائية، باتخاذ إجراء التسرب الإلكتروني لمعانة وكشف الجرائم المقررة بالمواد 225-4-1 إلى 225-9-4 والمواد 225-5 إلى 225-12 والمواد 225-1 إلى 225-12 من قانون العقوبات الفرنسي خاصة منها الجرائم المتعلقة بتصوير مشاهد الشذوذ الجنسي الخلية وجرائم الدعارة، واستخدام القصر لأغراض جنسية والإتجار بالرقيق عبر الإنترنت. وكذلك تسمح المادة 73-706-47-3 من ق إ ج ف، بالتسرب المعلوماتي من أجل المعانة وجمع الأدلة وكشف مرتكبي الجرائم المنصوص عليها في المواد 8227 إلى 24227 من قانون العقوبات الفرنسي عندما تُرتكب هذه الأخيرة باستعمال وسائل الإتصال الإلكتروني. فهذه الأحكام تسمح لضباط الشرطة القضائية أثناء التحريات أو التحقيق الابتدائي أن يُشارك بإسم مُستعار في التراسلات الإلكترونية، وأن يكون في اتصال إلكتروني مع الأشخاص المشتبه فيهم ارتكابهم جرائم جنسية. أو بناءً على طلب استعجالي في جريمة استخراج أو حيازة أو حفظ مضمون غير شرعي للمعطيات، بشرط أن لا تُشكل هذه الأعمال تحريضًا على الجريمة. وتُحدّد المواد (D47-8,9,11) من ق إ ج ف، إطارًا صارمًا لضباط الشرطة القضائية المؤهلين خصيصًا لاستخدام أسلوب التسرب في شبكات الإنترنت. ويجب لتنفيذه إذن مُسبب من السلطات القضائية تُذكر فيه الجريمة وهوية المتسرب والضابط المسؤول عن العملية، ومُدتها⁽¹⁾.

(¹) Myriam QUEMENER, Yves CHARPNEL, Cybercriminalité – Droit pénale appliqué, éd ECONOMICA, 2010, p180. 181

ثالثاً: التقاط المُعطيات (Captation des données à distance):

من ضمن صور الاعتراض والمراقبة في مجال الاتصالات الإلكترونية، توجد المراقبة عن طريق أسلوب الإلتقاط عن بُعد للمعطيات عبر أنظمة المعالجة الآلية، نصّ عليها مشروع قانون التوجيه والبرمجة في الأمن الداخلي الفرنسي. والذي يسمح لضباط الشرطة القضائية المنتدبين في إنابة قضائية أن يقوموا بدون رضا المعني، بوضع تدابير تقنية بغرض الدخول في أي حيز كان إلى مُعطيات الإعلام الآلي، وتسجيلها والإحتفاظ بها ونقلها مثلما هي معروضة على الشاشة للمستخدم. حيثُ يسمح هذا الإجراء بوضع حضان الطراودة بدون علم المشتبه فيه، حيث يُستعمل بضمانات إجرائية صارمة وخاصة تحت رقابة القاضي. وهي لا تُطبّق إلا في الجرائم الخطيرة المرتكبة في إطار العصابات، وهذه المراقبة يمكن أن تدوم (8) أشهر، أي (4) أشهر قابلة للتجديد مرة واحدة، قابلة للتنفيذ في أية لحظة⁽¹⁾. ويمكن للسلطة التي تقوم بالتفتيش في منظومة معلوماتية استعمال التقنيات اللازمة لحجز المعطيات عن طريق منع الوصول إلى المعطيات التي تحتويها منظومة معلوماتية أو نسخها طبقاً لما نصّت عليه المادة 7 من القانون 04.09.

رابعاً: فتح المُعطيات المُشفرة (Mise en clair des données chiffrées):

بصدور القانون 2001-62 المؤرخ في 15 نوفمبر 2001 المتعلّق بالأمن أصبحت المواد 1230 إلى 230-5 من ق إ ج الفرنسي تُرخص لقاضي التحقيق استخدام تقنيات فك الرسائل المشفرة. حيث متى كان هذا الإجراء ضرورياً لإظهار الحقيقة، بإمكان قاضي التحقيق تعيين أي شخص طبيعي أو معنوي مُنحصص مؤهل لتنفيذ العملية التقنية التي تسمح بالحصول على الصيغة المجانية أو المفتوحة (Claire) للمعلومات أو مُعادلة فك الشفرة في حالة استخدام تقنية التشفير (Cryptage, Chiffrement) وقرارات قاضي التحقيق بهذا الشأن غير قابلة للطعن. ومن أمثلة هذا الإجراء أنّه عندما يجري التحري أو التحقيق في جرائم مُعاقب عليها بالحبس المُدّة تُساوي أو تتجاوز السنتين، يُمكن لقاضي التحقيق استخدام الوسائل المشمولة بأسرار الدفاع الوطني، بموجب تسخيرة موجهة إلى الديوان المركزي لمكافحة جرائم تكنولوجيا الإعلام (OCLCTIC) حيث يقوم هذا الديوان بإحالة الطلب أو التسخيرة إلى هيئة تقنية خاضعة لأسرار الدفاع الوطني ومُعينة بموجب مرسوم. ونفس الإجراءات تُتبع في حالة قطع أو توقيف العملية. ويتم إرسال نتائج

(1), Myriam QUEMENER, Yves CHARPNEL, Op cit -182.

العملية من طرف الديوان إلى السلطات القضائية التي تُحرّر محضراً بالإستلام يُضم إلى ملف الإجراءات، حيث يُمكن الإطلاع على هذه المعلومات المرتبطة بأسرار الدفاع الوطني من قبل الأطراف لمناقشتها في طعونهم⁽¹⁾.

المطلب الثاني: مشروعية مراقبة الإتصالات الإلكترونية:

الفرع الأوّل: مشروعية مراقبة الإتصالات الإلكترونية في قوانين بعض الدّول الأوروبية:
أولاً: في بلجيكا: صدر قانون 30 أبريل 1994 المعدّل في 10 جوان 1998 يتعلّق بحماية الحياة الخاصّة ضدّ التنصّت والإستخبارات وتسجيل المحادثات والإتصالات السلكية واللاسلكية الخاصّة وغيرها من الأفعال يُجيز لقاضي التحقيق ووكيل النيابة لدى الملك اتّخاذ إجراءات مثل التنصّت والتسجيل بموجب المواد 90ter إلى 90monies من قانون التحقيقات الجنائية، والتقاط الصور بموجب المادة 88 مُكرّر، والتعرّف على هوية الإتصالات السلكية واللاسلكية الخاصّة بالمادة 46 مُكرّر من نفس القانون. وبعد صدور قانون الإجرام المعلوماتي لسنة 2000 أضاف المشرّع البلجيكي أشكالاً جديدة من الجرائم التي تُبرّر اتّخاذ الإجراءات المتعلّقة بالإتصالات السلكية واللاسلكية والإلكترونية بواسطة وسائل الإعلام الآلي. ثمّ صدر قانون 6 جانفي 2003 المتعلّق بالأساليب الخاصّة للتّحري، فوسّع من سلطات التحقيق وسمح بالتنصّت المباشر من طرف قاضي التحقيق⁽²⁾.

ثالثاً: في فرنسا: أصبح لتكنولوجيات الحديثة للإعلام والاتصال قيمة إثباتية في المجال الجنائي نظراً لما للعالم الافتراضي عالم المعلوماتية من آثار وبصمات من خلال تبادل المعطيات، حيث أنّ أحكام قانون 1991 المتعلّقة باعتراض المراسلات والاتصالات السلكية واللاسلكية تُطبّق على جرائم المعلوماتية والإنترنت لكشف مُستخدميها من المجرمين، مثل مُتتديات الدردشة انطلاقاً من العنوان

(1) Ibid,p175-176.

(2) Bertrand RENARD; Caroline VANDRESSE, La Belgique ou l'incrimination de l'organisation criminelle comme soutien des techniques d'enquête. Sous la direction de Maria LUISA CESONI, Criminalité organisée – des représentations sociales aux définitions juridiques, L.G.D.J paris, George éditeur Genève, Bruylant Bruxelles 2004.p 479.

(IP) المرتبط بالحاسوب أو (URL) المرتبط بالموقع، حيث هناك إمكانية للإلتقاط عن بُعد لمعطيات مُعالجة آليًا سواء الظاهرة على الشاشة أو المكتوبة بلوح المفاتيح (Clavier) الخاصين بالشخص المعني أو في إطار إجراءات التفتيش والحجز داخل منظومة معالجة آلية للمعطيات طبقًا للمادة 97 من ق إ ج⁽¹⁾. ثم ابتداءً من سنة 2000 تدعّمت الإجراءات الجزائية بوسائل وأساليب جديدة للتحريّ والتحقق للحصول على الأدلة الرقمية، فصدر قانون التوجيه والبرمجة من أجل الأمن الداخلي في 18 مارس 2003، وقانون الإلتئمان في الإقتصاد الرقمي في 21 جوان 2004، وقانون تكييف جهاز القضاء مع الإجرام في 9 مارس 2004 جاءت بأساليب حديثة لفاعلية وسرعة التحريات. كحفظ المعطيات غير المشروعة (Conservation des données de trafic)، وشرطة الإنترنت (Cyber patrouilles)، واعتراض الاتصالات الإلكترونية (L'interception des communication électronique). بالإضافة إلى الأساليب الإجرائية التقليدية التي ظلت قابلة للتطبيق في مجال جرائم الإنترنت⁽²⁾.

الفرع الثاني: مشروعية مراقبة الاتصالات الإلكترونية في القانون الجزائري:

أولاً: في قانون الإجراءات الجزائية: عند تعديل قانون الإجراءات الجزائية بالقانون 06-22 كرسّ المشرّع ضمن المواد 65 مُكرّر 5 إلى 65 مُكرّر 10 المراقبة الإلكترونية عن طريق اعتراض ونقل وتسجيل المراسلات التي تتم بواسطة وسائل الإتصال السلكية والسلكية وتشمل إتصالات الهاتف الثابت والهاتف النقال والاتصالات الإلكترونية عبر الشبكة الرقمية والإنترنت وتسجيل والتقاط ونقل الأحاديث والصور، ونظّم شروط استخدامها في التحقيقات الجنائية. وهي التي أشار إليها قانون الوقاية من الفساد ومكافحته⁽³⁾ بموجب المادة 56 عند نصّه أنّه « من أجل تسهيل جمع الأدلة المتعلقة بالجرائم المنصوص عليها في هذا القانون يمكن اللجوء إلى أساليب التحريّ الخاصّة كالترصد الإلكتروني...على النحو المناسب بإذن من السلطة القضائية المختصة...».

(1) SOPHIE Sontag Koenig, Technologies de l'information et de la communication et défense pénale, éd mare et martin, Paris, 2015, p 181-183

(2) Myriam QUEMENER, Yves CHARPNEL, Op cit, p 169.

(3) قانون رقم 06-01 المؤرخ في 20 فيفري 2006، ج ر عدد 14 في 08 مارس 2006. المتعم بالأمر 10-05 المؤرخ في 26 غشت 2010، ج ر عدد 14 في 01 سبتمبر 2010.

ثانياً: في قانون الوقاية من جرائم تكنولوجيايات الإعلام والاتصال ومكافحتها⁽¹⁾ بهذا القانون نظم المشرع الجزائري مراقبة الاتصالات الإلكترونية التي تتم عبر الإنترنت والشبكات الرقمية، حيث جعلت المادة 3 من بين مجالات تطبيقه مراقبة الاتصالات الإلكترونية عن طريق وضع الترتيبات التقنية وتجميع وتسجيل محتواها في حينها. وخصّص في المادة 4 فصلاً مستقلاً بعنوان مراقبة الاتصالات الإلكترونية والحالات التي تسمح بها. وأنشأ في فصله الخامس بموجب المادتين 13 و 14 الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال. ويّين المرسوم الرئاسي رقم 261.15 تشكيلة وتنظيم وكيفية سير الهيئة. حيث نصّت المادة 4 من المرسوم على مهام الهيئة ومن أهمّها ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة. ونصّت المادة 21 « بأنّه تُكلّف الهيئة حصرياً بمراقبة الاتصالات الإلكترونية وتسجيل محتواها في حينها والقيام بإجراءات حجز وتفتيش داخل منظومة معلوماتية تحت سلطة قاض مُختصّ، ووفقاً للأحكام المنصوص عليها في المادة 4 من القانون 04.09»

وتُكلّف بتنفيذ عمليات مراقبة الاتصالات الإلكترونية مصلحة داخل هذه الهيئة تُسمّى مديرية المراقبة والوقاية واليقظة الإلكترونية. حيث طبقاً للمادة 11 من المرسوم الرئاسي تُكلّف مديرية المراقبة والوقاية واليقظة الإلكترونية على الخصوص بتنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية من أجل الكشف عن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بناءً على رُخصة مكتوبة من السلطة القضائية وتحت رقابتها طبقاً للتشريع الساري المفعول، وإرسال المعلومات المحصّل عليها من خلال المراقبة الوقائية، إلى السلطات القضائية ومصالح الشرطة القضائية، المختصة، وتنفيذ طلبات المساعدة القضائية الأجنبية في هذا المجال.

المبحث الثاني: شروط مراقبة الاتصالات الإلكترونية أثناء التحري والتحقيق

(1) قانون 04-09 المؤرخ في 05 غشت 2009، ج ر، عدد 47 مؤرّحة في 16 غشت 2009، ص 6.

حتى يكون أسلوب مراقبة الاتصالات الإلكترونية مُنتجًا وفعالاً في تحقيق أهدافه الإجرائية بالكشف عن حقيقة الجريمة ومُرتكبها، ينبغي أن يستجيب لشروطه القانونية من ناحية إجراءات ترخيصه وإجراءات تنفيذه.

المطلب الأول: شروط ترخيص مراقبة الاتصالات الإلكترونية

الفرع الأول: الشروط الموضوعية لترخيص المراقبة الإلكترونية:

أولاً: الجريمة موضوع الإجراء:

أ) أنواع الجرائم موضوع المراقبة الإلكترونية: تركزت تدابير المراقبة الإلكترونية في القانون الجزائري كأسلوب من أساليب التحري والتحقيق على أنواع مُحددة على سبيل الحصر من الجرائم الخطيرة في المادة 65 مُكرّر 5 من قانون الإجراءات الجزائية وهي جرائم نظم المعالجة الآلية للمعطيات وجرائم والإرهاب، والمتاجرة بالمخدرات، وتبييض الأموال وجرائم الفساد وجرائم الصرف، والجريمة المنظمة عبر الوطنية. ويرجع للقاضي مُصدر الإذن، تقدير مدى توفر الوصف الجنائي في الأفعال محل التحري والتحقيق كمبرر وشرط موضوعي لاتخاذ إجراء المراقبة الإلكترونية.

وُحدّد حالات اللجوء إلى مراقبة الاتصالات الإلكترونية كذلك بموجب المادة 4 من قانون الوقاية من جرائم تكنولوجيا الإعلام والاتصال 04-09 في قسمين، أولهما كمراقبة إدارية تدخل في إطار الضبط الإداري للوقاية من جرائم الإرهاب والتخريب والمساس بأمن الدولة والنظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني. والثاني يدخل في إطار الإجراءات الجزائية للضبط أو التحقيق القضائي وله حالتان: حالة مُقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة في الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية. وحالة تنفيذ طلبات مُساعدة قضائية دولية مُتبادلة.

وبموجب المادة 26 من المرسوم الرئاسي رقم 15-261 المؤظم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال، يجب تحت طائلة العقوبات الجزائية ألا تُستخدم التسجيلات والمعطيات لأغراض أخرى غير تلك المتعلقة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومُكافحتها وذلك وفقاً للأحكام المنصوص عليها في القانون 04-09. ولهذا الغرض رخصت المادة 30 من نفس المرسوم للقضاة القيام بتفتيش مكان أو هيكل بلغ إلى علمهم

أنه يجوز أو يستعمل تجهيزات موجهة لمراقبة الاتصالات الإلكترونية، وفي حالة مُعانة أفعال جزائية تُخطر النائب العام المختص للقيام بالمُتابعة المحتملة.

(ب) **مقتضيات وضرورات التحري والتحقيق:** مثل أي إجراء تطفلي يجب أن يكون إعتراض المراسلات الإلكترونية ضروريًا لإظهار الحقيقة، وهذا الشرط نصّت عليه المادة 8 § 2 من الإتفاقية الأوروبية لحقوق الإنسان⁽¹⁾.

. في فرنسا يُشترط مبدأ الضرورة بالنسبة لاعتراض الاتصالات صراحةً بنص المادة 95.706 فقرة 1 من ق إ ج ج، حيث يتعيّن على قاضي الحريات والحبس أن يقوم بتقديره والتأكد منه في طلب وكيل الجمهورية. ومسألة تقدير الضرورة لاتخاذ إجراء اعتراض الاتصالات السلكية واللاسلكية ترجع إلى قاضي الحريات والحبس، حيث يجب أن يتضمّن الإذن بالإعتراض جميع العناصر التي تسمح بالتعرّف على الإتصال، والجريمة التي تُبرّر الإجراء، وكذا المدة التي يجري فيها المادة (100-1)⁽²⁾.

. في الجزائر نصّت عليه المادة 65 مكرّر 5 من ق إ ج فقرّت أنه لا يتمّ اللجوء إلى هذه المراقبة إلا إذا دعت إلى ذلك ضرورات التحري والتحقيق الابتدائي في جرائم مُحدّدة على سبيل الحصر ومن بينها أفعال الجريمة المعلوماتية. وكذلك نصّت المادة 3 من القانون 04.09، بأنّه لا يتمّ اللجوء إلى مراقبة الاتصالات الإلكترونية إلا إذا استدعت ذلك **مقتضيات ومستلزمات التحريات** أو التحقيقات القضائية الجارية وفقًا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون. كما حصرت المادة 4 من نفس القانون مراقبة الاتصالات الإلكترونية بمجالات مُحدّدة من بينها في الفقرة (ج) حالة مُقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهمّ الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

وتُعتبر مسألة تقدير ضرورة اللجوء إلى هذه العمليات من عدمه حسب المادة 65 مكرّر 5 من ق إ ج ج متروكةً دائمًا لتقدير القاضي الذي أصدر الإذن سواء قاضي التحقيق أو وكيل الجمهورية. غير أنّ

(1) Serge GUINCHARD; Jaque BUISSON, procédure pénale, éd Litec n°6, Paris, 2010, p 1121.

(2) Frédéric DESPORTES, Laurence LAZERGES-COUSQUER, Op cit, p 1367.

القانون لا يُلزم القاضي بتسبيب إذن المراقبة، لذا فإنّه يصعب التأكد من توفر هذا الشرط الموضوعي.

ثانيًا: صفة الشخص محل المراقبة:

أ) **ضرورة ارتباط الشخص بالجريمة:** في التشريع المصري نظرًا لعموم نص المادتين 95 و 206 من قانون الإجراءات الجنائية فمن الفقه من يعتبر سلطة القاضي واسعة بعموم النص إذ يملك أن يمدّ المراقبة لغير المتهم متى كان في تلك المراقبة فائدة في إظهار الحقيقة⁽¹⁾. وهناك رأي فقهي آخر يستلزم أن يكون المتهم طرفًا في الحديث الذي تجري مُراقبته، وأنّه لا يُمكن إهدار الحماية الدستورية والقانونية لحرمة وسريّة الحياة الخاصّة لشخص لم يُتهم بجريمة، وليس له شأن بملف متابعته. لأنّ هذا الإجراء استثنائي، والإتهام المبني على الدلائل الجديّة القوية هو الذي يُبرّر اللجوء إلى هذا الإستثناء والتسلل إلى الحياة الخاصّة للفرد، من أجل الكشف عن حقيقة الجريمة. كما أنّ الإستثناء لا يجوز التوسع في تفسيره⁽²⁾. فكل شخص له علاقة بالجريمة محل التحقيق سواء كان شاهدًا أو مشتبهًا فيه يمكن أن يخضع لاعتراض مراسلاته السلوكية واللاسلكية، حتى ولو لم يكن يوجد ضده أي اشتباه لمشاركته في الجريمة، فالمررّ الوحيد لاتخاذ الإجراء هو مبدأ الضرورة، وهو يخضع لتقدير القاضي أمام غرفة التحقيق، أو قاضي الحكم⁽³⁾.

ب) **إستثناء بعض الأشخاص من إجراء المراقبة الإلكترونية:** في فرنسا كرس القانون حماية إجرائية لبعض الوظائف، بأن يقع إجراء اعتراض المراسلات تحت طائلة البطلان إذا خالف أحكام هذه الحماية. مثل حماية المحامين وحقوق الدفاع في الفقرة الثانية من المادة 100-7 من ق إ ج ف التي ألزمت قاضي التحقيق قبل اتخاذ إجراء اعتراض مراسلات المحامي في مكتبه أو بيته بإعلام النقيب. والمادة 100-5 قرّرت أنّه لا يجوز وصف المكالمات التي يقوم بها المحامي ويصب موضوعها في مُمارسة حقوق الدفاع، مع إستثناء وحيد هو وجود قرائن على مساهمة المحامي نفسه في الجريمة.

(1) محمود أحمد طه، التعدي على حق الإنسان في سريّة اتصالاته الشخصية بين التجريم والمشروعية، دار النهضة العربية، القاهرة، الطبعة الثانية 1999، ص 196.

(2) ياسر الأمير فاروق محمد، مراقبة الأحاديث الخاصّة في الإجراءات الجنائية، رسالة دكتوراه، ج القاهرة، 2008، ص 543.

(3) Serge GUINCHARD; Jaque BUISSON, Op Cit, p 1120.

وكذلك حماية لأعضاء البرلمان نصّت المادة 100-7 من ق إ ج على أنّه لا يُمكن إجراء اعتراض الاتصالات الهاتفية لعضو البرلمان في مكتبه أو بيته إلا بعد إخطار رئيس الهيئة من طرف قاضي التحقيق.

. في الجزائر لم يأت المشرّع بمثل هذه الإستثناءات الصريحة بل اكتفى في المادة 65 مكرر 1/6 بالنّص على ضرورة عدم المساس بالسّر المهني إذا تعلّق الأمر بتنفيذ هذه العمليات في أية أماكن يوجد بها أشخاص مُلزمون بالسّر المهني، مثل السّر المهني للمحامي والطبيب والمثوق⁽¹⁾.

كما نصّت المادة 3 من القانون 04.09 على ضرورة مراعاة مراقبة الإتصالات الإلكترونية للأحكام القانونية التي تضمن سرّية المراسلات والاتصالات. وألّزمت المادة 27 من المرسوم الرئاسي 261.15، مُستخدمي هذه الهيئة بالسّر المهني وواجب التحفّظ. كما يتضمّن اليمين الذي يؤدّونه القسم على كتمان الأسرار والمعلومات التي يطلّعون عليها أثناء قيامهم بمهامهم والتي من بينها مراقبة الإتصالات الإلكترونية.

الفرع الثاني: الشروط الإجرائية لترخيص المراقبة الإلكترونية (الإذن القضائي بالمراقبة):

تعلّق الشروط الإجرائية لترخيص المراقبة الإلكترونية في اعتراض المراسلات السلكية واللاسلكية والإلكترونية، بالإذن القضائي الذي يُرخص استخدامها. نصّت عليه كافة التشريعات المقارنة ومنها التشريع الجزائري في المادة 65 مكرر 5 من ق إ ج وذلك في فقرتها الأولى «يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي...»، وفي فقرتها الأخيرة « في حالة فتح تحقيق قضائي تتم العمليات المذكورة بناءً على إذن من قاضي التحقيق وتحت رقابته المباشرة ». كما نصّت المادة الرابعة من القانون 04-09، أنّه لا يتمّ اللجوء إلى مراقبة الإتصالات الإلكترونية إلا بإذن الجهات القضائية المختصة، وتُحيل المادة الثالثة في ذلك إحالة عامّة على قانون الإجراءات الجزائية.

أولاً: السلطات المختصة بإصدار الإذن بالمراقبة:

(أ) في التشريع الفرنسي: في ظل قانون 10 جويلية 1991 كانت المادة 100 من ق إ ج ف، وما بعدها من ق إ ج ف لا تسمح باعتراض المراسلات إلا أثناء التحقيق الابتدائي، ثمّ جاء قانون 9 مارس 2004 يسمح بتطبيقه أثناء التحريات الأولية في أفعال الإجرام المنظم عندما تقتضي ذلك

(1) جمال نخيمي، إثبات الجريمة على ضوء الاجتهاد القضائي . دراسة مقارنة . دار هومة للطباعة والنشر والتوزيع، الجزائر، 2011، ص 446.

ضرورات التحقيق في التلبس أو التحقيق الأولي (المادة 706-95 ق إ ج ف) ⁽¹⁾. وهي المذكورة على سبيل الحصر في المادة 706-73 ق إ ج ويجوز لقاضي التحقيق بموجب أمر مُسبّب وبعد إخطار وكيل الجمهورية أن يأذن بالإلتقاط عن بُعد لمعطيات معلوماتية وتسجيلها وحفظها ونقلها، مثلما هي ظاهرة على شاشة الحاسوب أو مثلما تمّ كتابتها بأحرف الجهاز (الم 706-102 ق إ ج) ⁽²⁾.

وترجع سلطة اتخاذ إجراء اعتراض المراسلات السلكية واللاسلكية والإلكترونية، في الجريمة المنظمة لقاضي الحريات والحبس بالمحكمة ذات الاختصاص الشامل (TGI) بطلب من وكيل الجمهورية المختص. أمّا بالنسبة للمجالات الأخرى، في الجنايات وفي الجناح التي تُساوي أو تزيد عقوبتها عن سنتين حبس، فقاضي التحقيق هو الذي له سلطة اتخاذ الإجراء (المادة 100 ق إ ج ف) أو في إطار التحقيق التكميلي لقضاة غرفة التحقيق أو محكمة الجناح أو محكمة الجنايات طبقاً للمواد (المادتان 205، 283 ق إ ج ف) ⁽³⁾.

ب) في التشريع الجزائري يُمكن اللجوء إلى المراقبة الإلكترونية بجميع أنواعها في كلتا مرحلتَي التحريات الأولية والتحقيق القضائي الابتدائي، ومن ثمّ يصدرُ الإذن من قاضي التحقيق في إطار التحقيق الابتدائي. ومن وكيل الجمهورية في إطار التحقيق الأولي وتحقيقات التلبس، وهنا يجدر التنبيه أنّ النسخة العربية لنص الفقرة الأولى من المادة 65 مكرّر 5 من ق إ ج سقطت منها عبارة « التحقيقات الأولية » التي وردت في النسخة الفرنسية لنفس المادة حيث تنص أنّه تُطبق هذه الإجراءات في مرحلة التحريات سواء في التحقيقات الأولية أو تحقيقات التلبس.

وما لم يُخطر قاض التحقيق بملف الدعوى لا يحقّ له إصدار إذن بإجراء عمليات اعتراض المراسلات عندما يتعلق الأمر بوجود دلائل على الجرائم المنصوص عليها في المادة 65 مكرّر 5 ق إ ج ج بأنّها

(1) Jean PRADEL , " Le crime organisé après la loi française du 09 Mars 2004 dite loi de Perben II ", Rrevue de droit pénal et de criminologie, éd la charte, Bruxelles, n° 02, 2005. p151.

(2) Frédéric DESPORTES, Laurence LAZERGES-COUSQUER, Op Cit, p 1367.

(3) Serge GUINCHARD; Jaque BUISSON, Op Cit, p 1121.

سُتَرَكِبُ مُسْتَقْبَلًا⁽¹⁾. وإذا تعلّق موضوع المراقبة بجرائم الإرهاب والتخريب وأمن الدولة يصدر الإذن عن النائب العام لمجلس قضاء الجزائر إلى الهيئة الوطنية للوقاية من الجريمة الإلكترونية المذكورة في المادة 13 من القانون 04-09، بناءً على تقرير يُبيّن طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها. وتدخل جرائم المعلوماتية والجرائم الأخرى التي يُسمح فيها بمراقبة الاتصالات الإلكترونية داخلة في اختصاص الأقطاب القضائية الجزائرية بموجب المواد 37، 40، 329، 37، 40، 329، وكذلك الاختصاص الإقليمي الموسّع لضباط الشرطة القضائية في المراقبة بالمادة 16 مُكرّر ق إ ج.

ثانيًا: مضمون الإذن

يجب أن يكون الإذن باعتراض الاتصالات الإلكترونية مكتوبًا يتضمّن جميع العناصر التي تبين حقيقة الاتصال المعترض، بحيث ينبغي التحديد الدقيق لنوع الجريمة التي تُبرّر الإجراء، والتحديد الواضح والمفصّل لجهاز الكمبيوتر الخاضع للمراقبة وطبيعة المعطيات المراد التقاطها أو اعتراضها و المدة (المادة 65 مُكرّر 7).

ويزيد القانون الفرنسي عن القانون الجزائري بضرورة تسبب الإذن. فالقانون الفرنسي وقر إمكانية المراقبة الحقيقية لاحترام مبدأ الضرورة والملاءمة في اتخاذ هذا الإجراء عن طريق اشتراط أن يكون الأمر أو الإذن المرخص للإجراء مُسبّبًا. وهو الشرط الذي تنصّ عليه المادة 706-1/97 من ق إ ج ف⁽²⁾. لأنّ الملاءمة لا تنتج فقط عن توافر الشروط القانونية لتطبيق الإجراء، بل تخضع للسلطة التقديرية للقاضي حالةً بحالة. والمشرّع أخضع هذه الملاءمة للمراقبة القضائية عن طريق فرض تسبب الإذن⁽³⁾. فعندما يكون الإذن بالإعتراض غير مُسبب يصعب مراقبة مدى توافر هذا الشرط. وتجاهل هذا الشرط ينبغي أن يُرتّب البطلان.

(1) فوزي عمار "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية" مجلة العلوم الإنسانية، جامعة منتوري قسنطينة، عدد 33 جوان 2010 ص 242.

(2) Joceline LEBLOIS-HAPPE, Autorisation et contrôle des écoutes téléphoniques, rôle du JLD " Actualité Juridique Pénal, n° 6/2008, juin 2008, p 284-285.

(3) Frédéric DESPORTES, Laurence LAZERGES-COUSQUER, Idem, p 1378 - 1379.

ينبغي على المشرّع الجزائري أن يُظيف شرط التسبب بالنسبة للمراقبة التي تتمّ بواسطة التقاط أو اعتراض الاتصال الإلكتروني لأنّ الدستور⁽¹⁾ أرسى بموجب الفقرة الثالثة من المادة 39 ضمانات تسبب الأمر القضائي في الإجراءات التي تتضمنّ المساس بجرمة الحياة الخاصة وقرّر الجزاء الجنائي على انتهاكها. وهذا احترامًا لما نصّت عليه الفقرة الثانية من نفس المادة 39 وهو ضمان سرّية المراسلات والاتصالات الخاصة للأفراد بكلّ أشكالها.

لكن إذا تمّت مراقبة الاتصالات الإلكترونية عن طريق أسلوب التسرّب الرقمي فإنّه يُشترط تسبب الإذن لأنّ المشرّع اشتراطه تحت طائلة البطلان بالنسبة لأحكام التسرّب في المادة 65 مكرّر 15 ق إ ج ج.

ثالثًا: مُدّة مراقبة الاتصالات الإلكترونية:

. في فرنسا تُحدّد المادة 95.706 من ق إ ج مُدّة المراقبة ب (15) يومًا قابلة للتجديد مرّة واحدة وفق نفس الشروط الشكلية والزمنية، على أن تتمّ عملية الاعتراض تحت إشراف الأمانة العامة لوزارة العدل التي تتكفل بالتنسيق بين مختلف الإدارات المختصة في مجال اعتراض المراسلات⁽²⁾.

. في الجزائر حدّدتها القواعد الخاصة للمراقبة الإلكترونية في المادة 65 مكرّر 7 قانون الإجراءات الجزائية بمُدّة (4) أشهر قابلة للتجديد. أمّا القانون 09-04 فلم يشترط المُدّة في غير حالة الجرائم الإرهابية والتخريبية والماسّة بأمن الدولة، بالتالي تخضع لنفس المُدّة التي نصّت عليها المادة 65 مكرّر 7 ق إ ج، لكن إذا تعلّق موضوع المراقبة بجرائم الإرهاب والتخريب وأمن الدولة فقد حدّدت المادة 4 فقرة 5 من القانون 09-04 مُدّة الإذن الذي يمنحه النائب العام لمجلس قضاء العاصمة للهيئة الوطنية للوقاية من الجريمة الإلكترونية هي (6) أشهر قابلة للتجديد وذلك على أساس تقرير يبيّن طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

(1) دستور 28 نوفمبر 1996 الصادر بموجب المرسوم الرئاسي رقم 438.96 بتاريخ 7 ديسمبر 1996 المصادق عليه في استفتاء 28 ديسمبر 1996. المعدّل بالقانون رقم 16-01 المؤرّخ في 6 مارس 2016 م، ج ر عدد 14 في 07 مارس 2016.

(2) Myriam QUEMENER, Yves CHARPNEL, Op cit, p 169.

المطلب الثاني: شروط تنفيذ مراقبة الاتصالات الإلكترونية:

الفرع الأول: الجهات المُكلّفة بتنفيذ مراقبة الاتصالات الإلكترونية:

بمقتضى المادة 65 مكرّر 8 ق إ ج ج يتمّ تنفيذ إذن المراقبة من طرف ضابط الشرطة القضائية سواء في إطار مهامه الأصلية أثناء التحقيقات الأولية أو في إطار الإنابة القضائية أثناء التحقيق الابتدائي، كما يمكن للقاضي الذي أصدر إذن المراقبة أن يُسَخَّر كل عون مُؤَهَّل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصّة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات المداورة في المادة 65 مكرّر 5 أعلاه.

أولاً: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال:

طبقاً للمادة 13 من القانون 04.09 المتعلّق بالوقاية من جرائم تكنولوجيا الإعلام والاتصال، أنشئت الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته، وحدّدت مهامها المادة 14 ومن بين مهامها أنّها تُكلّف بمُساعدة السلطات القضائية ومُصالح الشرطة القضائية في التحريات التي تُجرّيها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والاتصال، بما في ذلك تجميع المعلومات وإنجاز الخبرات.

وتحتسّد نظام الهيئة بالمرسوم الرئاسي رقم 261.15 المتعلّق بتشكيل وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، حيث نصّت المادة الرابعة من هذا المرسوم الرئاسي أنّ هذه الهيئة تمارس مهامها تحت رقابة السلطة القضائية وطبقاً للتشريع الساري المفعول لاسيما قانون الإجراءات الجزائية.

وطبقاً للمادة 11 من نفس المرسوم تُكلّف هذه الهيئة حصريّاً عن طريق مديرية المراقبة والوقاية واليقظة الإلكترونية بتنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية " من أجل الكشف عن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بناءً على رُخصة مكتوبة من السلطة القضائية وتحت رقابتها طبقاً للتشريع الساري المفعول"، هو يتمثل خاصّة في المواد 65 مكرّر 5 إلى 65 مكرّر 10 من قانون الإجراءات الجزائية.

ونصّت المادة 21 من نفس المرسوم « قصد الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة تُكلّف الهيئة حصريّاً بمراقبة الاتصالات الإلكترونية وتسجيل مُحتواها في حينها والقيام بإجراءات حجز وتفتيش داخل منظومة معلوماتية تحت سُلطة قاض

مُختَصّ، ووفقًا للأحكام المنصوص عليها في المادة 4 من القانون 09-04، المتعلّق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال».

يعمل في هذه الهيئة مُستخدمون تقنيون، وتزوّد الهيئة بضباط وأعوان للشرطة القضائية من المصالح العسكرية للإستعلام والأمن الوطني والدرك الوطني، ويمكن أن تستعين الهيئة بخبراء وموظفين مُختصّين من الوزارات المعنية بتكنولوجيا الإعلام والاتصال. وتتكوّن الهيئة من عدّة مصالح مُبيّنة في المادة 6 من المرسوم، من بينها مُديرية المراقبة والوقاية واليقظة الإلكترونية، وهي المصلحة المكلفة بتنفيذ عمليات مراقبة الاتصالات الإلكترونية، تتوفر على مركز العمليات التقنية ومُلاحقات جبهوية ووحدات تتبعها، تقوم بتنفيذ عمليات المراقبة على مُستواها.

ثانيًا: مُقدّموا خدمة الاتصالات الإلكترونية:

. في الجزائر يخضع تنفيذ المراقبة عن طريق اعتراض الاتصالات الإلكترونية في الجزائر لنفس أحكام التصنت والتقاط الأصوات والصور في قانون الإجراءات الجزائية، ويُضيف قانون مكافحة جرائم تكنولوجيا الإعلام والاتصال في مجال مراقبة أو اعتراض الاتصالات الإلكترونية بعض الأحكام الإجرائية التي تُمثّل صورًا للمراقبة الإلكترونية في مجال الإنترنت أو إجراءات تنفيذية مُكمّلة لاعتراض المراسلات الإلكترونية، تمثلت في تقديم المساعدة للسلطات القضائية للتحرّي والتحقيق من طرف مُقدمي خدمات الاتصال الإلكتروني، وذلك بحفظ مُعطيات حركة السير الإلكتروني، وحجز واستعمال مُعطيات الإعلام الآلي. حيث تُلزم المادة 10 من قانون مكافحة جرائم تكنولوجيا الإعلام والاتصال مُقدمي خدمات الاتصال الإلكتروني بتقديم المساعدة للسلطات المكلفة بالتحريات والتحقيقات القضائية لتجميع وتسجيل المعطيات المتعلقة بمُحتوى الاتصالات في حينها، وذلك بوضع المعطيات التي يتعيّن عليهم حفظها وفق المادة 11 من نفس القانون تحت تصرّف السلطات المذكورة، مع التزامهم بواجب كتمان السر تحت طائلة عقوبات إفشاء أسرار التحري والتحقيق.

وتُعرّف الفقرة (د) من المادة 2 من هذا القانون « مقدّم الخدمات » بأنه: أيّ كيان عام أو خاص يُقدم لمستخدمي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات. وأيّ كيان آخر يقوم بمعالجة أو تخزين مُعطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستخدميها. . في فرنسا تتم المساعدة التي يُقدّمها مُزودو خدمات الاتصال الإلكتروني، في إطار التسخيرة المعلوماتية، فبغرض تجميع عناصر الأدلة الرقمية، يمكن للقضاة أو ضباط الشرطة القضائية اتخاذ

العديد من إجراءات التحري في شكل تسخيرة، من خلال فرض الإلتزام على أي شخص بتقديم خدمة نظرًا لما يملكه هذا الشخص من وسائل تقنية أو خبرات غير متوفرة لدى السلطات القضائية. مثل التسخيرة التي تنصّ عليها المواد 1.60 و 1.1.77 و 3.99 و 4.99 من قانون الإجراءات الجزائية، والتي تسمح بتسخير الأشخاص المختصّين والإدارات والمصالح أثناء تحقيقات التلبس أو التحقيق الأولي، من أجل الإطلاع على ملفات يجوزونها تتضمن معطيات رقمية أو في منظومات المعالجة الآلية، عن طريق الإنترنت أو وسائل الإتصال الإلكترونية. وتسمح المادة 1/120 لضابط الشرطة القضائية أن يدخل عن طريق شبكات الإعلام الآلي أو الإنترنت إلى بعض الهيآت العمومية والأشخاص المعنوية الخاصة، ويضع تحت تصرّفه المعلومات التي تفيد في كشف الحقيقة، والتي يمكن نقلها أو تحويلها في شكل رقمي. وتنصّ المادة 2.1.77 من ق إ ج ف على أنّه بإمكان ضابط الشرطة القضائية بإذن من وكيل الجمهورية والإذن المسبق لقاضي الحريات والحبس، أن يُسخر بعض المؤسسات والأشخاص من أجل أن يضعوا تحت تصرّفهم المعلومات المتحصل عليها عن طريق شبكات الإتصال المعلوماتية والإنترنت في أقرب الآجال. وهذا تحت طائلة العقوبات المقرّرة بالمادة 2.121 من قانون العقوبات⁽¹⁾. وقانون مكافحة الإرهاب والمراقبة عبر الحدود رقم 642006 وسّع من نطاق مراقبة الاتصالات الإلكترونية في مجال جرائم الإرهاب، إلى الأشخاص الذين يقدمون بصفة مهنية خدمة عمومية للإتصال عبر شبكة الإنترنت مثل مقاهي الإنترنت وموردي خدمة (WIFI)⁽²⁾.

الفرع الثاني: التدابير المتخذة أثناء وبعد عملية المراقبة:

أولاً: التقيّد بمضمون الإذن ومنع تحويل الإجراءات:

إذا كان موضوع الإجراء هو المراقبة الصوتية والبصرية للأشخاص، فلا يمكن أن تكون له أهداف أخرى من غير المنصوص عليها في مادّة المراقبة الصوتية والبصرية. أي أنّه في الترخيص بوضع الترتيبات التقنية من أجل التقاط أو بث أو تثبيت أو تسجيل الكلام والصور، لا يمكن استغلال فرصة الدخول إلى مكان خاص بمُناسبة وضع ترتيبات التنصّت، والقيام بعمليات تفتيش وحجز، وهو ما يُسمّى بمبدأ منع تحويل الإجراءات (détournement de procédure) فلا إجراء

(1) Myriam QUEMENER, Yves CHARPNEL, Op cit, p 173-174.

(2) Marie-Hélène GALMARD, Op cit, p 14-15.

عملية تفتيش لا مانع من إصدار إذن بإجراء التفتيش بشكل مُستقل، وفق شروطه الخاصة به. وبالنسبة للحالة العكسية فيمكن وضع الترتيبات التقنية للتنصّت بمناسبة تنفيذ إذن بالتفتيش، لكن شريطة أن يتمّ التفتيش فعلاً⁽¹⁾.

وفي الجزائر بيّنت المادّة 9 من قانون مكافحة جرائم تكنولوجيا الإعلام والاتصال 04.09 حدود استعمال المعطيات المتحصل عليها أثناء المراقبة أو التفتيش المعلوماتي مُقرّرةً أنّه تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون إلّا في الحدود الضرورية للتحريات أو التحقيقات القضائية وفي الحالة العكسية حالة اكتشاف جرائم أخرى غير مذكورة في إذن المراقبة، نصّت المادّة 65 مكرّر 2/6 على عدم ترتّب البطالان للإجراءات العارضة.

ثانيًا: تحرير محاضر المراقبة:

من أهمّ ضمانات المهّم في عملية المراقبة الإلكترونية أن يتمّ تنفيذها تحت السلطة والرقابة المستمرة للقاضي من خلال وجوب تحرير محاضر العمليات والنسخ والوصف والتدابير الاحتياطية بعد انتهاء عملية المراقبة.

أ) **محضر العمليات:** عن هذه العملية من طرف ضابط الشرطة القضائية المكلف بها، يدرج في ملف الإجراءات، ويكون لمحامي المتهم الخاضع للمراقبة الإطلاع عليه من أجل مُناقشته أو إنكار مضمونه والمطالبة بإجراء خبرة على الصوت المسجل أو الصور الملتقطة. حيث يُدوّن في هذا المحضر جميع مُجريات سير عملية وضع الترتيبات التقنية، وكل مرحلة من مراحل عمليات الالتقاط والتثبيت والتسجيل الصوتي أو المرئي، ويوجد فيه تاريخ وساعات بداية ونهاية الإجراء (المادّة 65 مكرّر 9).

في عمليات الاعتراض والتسجيل والالتقاط، لا يتم انتظار بلوغ مرحلتها النهائية لتحرير محضر بشأنها، فعلى قاضي التحقيق أو وكيل الجمهورية بحكم مراقبته المباشرة للعمليات وضابط الشرطة القضائية المنتدب لإجراء العمليات تحرير محاضر عن كل مرحلة على حدة، إذ يُحرّر بشكل منفصل محضر الترتيبات التقنية ومحضر الدخول إلى المساكن ومحضر الالتقاط ومحضر التثبيت ومحضر التسجيل الصوتي أو محضر التسجيل السمعي البصري، ومحضر عملية الاعتراض ومحضر تسجيل

(¹) Frédéric DESPORTES, Laurence LAZERGES-COUSQUER, Op Cit, p 1379.

المراسلات. وإذا كانت المكالمات التي تم اعتراضها أو التسجيلات الصوتية أو السمعية البصرية بلغة أجنبية تتم ترجمتها بمساعدة مترجم يتم تسخيرها لهذا الغرض.

ويجب أن تُبنى عملية حفظ الدليل الرقمي على أسس علمية، وتحديث أسلوب تحرير المحاضر في هذا الشأن، بحيث يجب ألاّ يتخذ المحضر المظهر التقليدي فقط. فيجب مثلاً التذكير بضرورة الارتباط بالخبرة وتحديد الخبرة في تحرير محضر ضبط الدليل العلمي⁽¹⁾.

ويثير هذا الإجراء بعض الصعوبات فيما لو كان ضابط الشرطة القضائية أثناء تنفيذ المراقبة تحصل على عناصر مهمة تفيد في الكشف عن الحقيقة فبادر بإرسالها إلى قاضي التحقيق. فلو وجد قاضي التحقيق نفسه مضطراً لإجراء استجواب مع المتهم فهل يلتزم بإطلاع المحامي على ملف التحقيق ومن ثمّ إفساد تحقيقه؟ فبعض قضاة التحقيق يقومون بسحب محضر الوصف من ملف الإجراءات، أو سحب الإنابة القضائية كاملة نسختها الثانية⁽²⁾.

وتقضي المادة 25 من المرسوم المتعلق بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بأنه تُسجل الاتصالات الإلكترونية التي تكون موضوع مراقبة وتُحرّر وفقاً للشروط والأشكال المنصوص عليها في ق.إ.ج. وتُسلم التسجيلات والمحزرات إلى مصالح الشرطة والسلطات القضائية المختصة التي تحتفظ دون سواها بهذه المعطيات أثناء المدة القانونية المنصوص عليها في التشريع الساري المفعول.

(ب) محضر النسخ والوصف: تأكيداً على ضمانات صحة التسجيلات المأخوذة للمكالمات، قرّر المشرع الفرنسي بموجب المادة 4.100 فقرة 1 بأنّ كل عملية اعتراض أو تسجيل يجب أن تكون موضوع محضر للوصف، يقع على عاتق قاضي التحقيق أو ضابط الشرطة القضائية المنتدب أو وكيل الجمهورية بحسب الإطار الإجرائي. حيث يُدوّن فيه تاريخ وساعة البداية والنهاية لكل عملية، ثم وصف المكالمات التي تفيد في إظهار الحقيقة. ويجب إدراج هذا المحضر ووثيقة الإنابة القضائية في

(1) أنظر عمر مُحمّد بن يونس، "الدليل الرقمي"، المرجع السابق، ص 11.

(2) Jean PRADEL, " Un exemple de restauration de la légalité criminelle – le régime des interceptions de correspondances émises par la voie des télécommunications (commentaire de la loi n° 91-646 du 10 juillet 1991), Recueil Dalloz 1992, Chroniques, p 49.

ملف التحقيق بعد تنفيذ الإعتراض، من أجل تمكين الدفاع من الإطلاع عليها. وتكون لضابط الشرطة القضائية السلطة التقديرية، بأن يصف فقط المحادثات المفيدة في إظهار الحقيقة⁽¹⁾. وفي الجزائر وطبقاً للمادة 65 مكرر 10/1 من ق إ ج ينتقي ضابط الشرطة القضائية من هذه التسجيلات ما يكون مفيداً في إظهار الحقيقة وينسخه ويصفه، أي يُفرغه بنقله إلى معطيات كتابية، ويجرّر محضراً مُستقلاً عن هذا النقل ولو بالتلخيص والإختصار لمضمون التسجيلات، ويودع المحضر بدوره في ملف الإجراءات. وإذا كانت الإتصالات قد تمت بلغة أجنبية، تُرجم وجوباً إلى اللغة العربية، بمساعدة ترجمان مسجل بجدول المترجمين المقبولين لدى المحاكم. كما يجوز الإستعانة بخبراء وذوي الإختصاص في حالة اشتغال المراسلة على رموز أو ألغاز.

ج) اتخاذ تدابير احتياطية بعد انتهاء عملية المراقبة:

1) وضع التسجيلات في أحرار مُقفلة: يعتبر هذا الإجراء من الضمانات الأساسية في تنفيذ عمليات المراقبة الإلكترونية، قبل تقديم الدليل المتحصل عليه من تسجيل المكالمات إلى المحكمة، والغرض منه هو التأكد من سلامة الأشرطة والدعامات الإلكترونية ومنع تغييرها أو التلاعب فيها بالحذف أو الإضافة، غير أنه لم يرد النصّ عليه في القانون الجزائري، ويُمكن إخضاعه للأحكام العامة المتعلقة بالمضبوطات الناتجة عن التفتيش.

لكن في فرنسا نصّت عليه المادة 100.706/2 من ق إ ج الفرنسي بالنسبة لالتقاط الصور والأصوات. وحسب التعليمات التطبيقية (CRIM 04-13 G1 du 2 Septembre 2004) يجب الإحتفاظ بالأشرطة الأصلية للتسجيل في أحرار محتومة. بخلاف الأمر بالنسبة للتنصّت الهاتفية، وتفادياً لاضطرار اللجوء إلى كسر الأختام عن الحرز بحضور المتهم المراقب يقوم قاضي التحقيق باستنساخ نسخة ثانية من الشريط، من أجل الرجوع إليها كلما اقتضى الأمر، والسماح بالإطلاع عليها وفحصها من طرف محامي المتهم المراقب إذا كان يريد مناقشتها، أو

(1) Jean PRADEL, " Un exemple de restauration de la légalité criminelle: le régime des interceptions de correspondances émises par la voie des télécommunications ", Op cit, p49.

فحص مدى شرعيتها وصحتها،⁽¹⁾. ويجب تحريز الأشرطة المغناطيسية التي تحتوى تسجيلات جميع المكالمات التي تم اعتراضها، حفاظاً على صحتها ومطابقتها للحقيقة وهذا الضبط والتحريز لا يمنع استعمال نسخة من التسجيلات في إجراءات أخرى⁽²⁾.

(2) إتلاف التسجيلات: حمايةً للأسرار والحياة الخاصة، ألقت القوانين على عاتق كل من يشارك في عملية المراقبة واجب التحفظ بشأن نتائجها بعد الانتهاء من الإجراء، وتحقيق الغرض المقصود من المراقبة باستخدامها كدليل في الملف الإجرائي. بضرورة إتلاف جميع أشرطة التسجيل الأصلية ونسختها. نصّت على هذا الإجراء المادة 102.706 ق إ ج الفرنسي. بتقريرها أنّ التسجيلات السمعية أو السمعية البصرية يجب أن يتم إتلافها وتخطيطها تحت إشراف وعناية وكيل الجمهورية أو النائب العام عند انقضاء أجل تقادم الدعوى العمومية. مع تحرير محضر الإتلاف. والحكم نفسه ينطبق على التسجيلات الهاتفية بموجب المادة 95.706 ق إ ج ف، بالإحالة إلى المادة 6.100 من نفس القانون. فبمجرد الإنتهاء من استخدام التسجيلات المستمدة من اعتراض المراسلات السلكية واللاسلكية يجب إتلافها⁽³⁾. ويكون الإحتفاظ بالتسجيلات محدوداً بفترة زمنية معينة وهي ميعاد تقادم الدعوى العمومية إذا لم يتم استخدامها، حيث يتوجب إتلافها أو محوها عند انقضاء هذه المدة وتحرير محضر بهذا الإتلاف من طرف وكيل الجمهورية أو النائب العام (المادة 6.100 ق إ ج ف)⁽⁴⁾. ونفس الإجراء نصّت عليه المادة 113 من المسطرة الجنائية المغربي التي ألزمت به قاضي التحقيق وقضاة النيابة⁽⁵⁾. ولم ينصّ المشرع الجزائري على هذا الإجراء رغم أهميته.

(1) Code De Procédure Pénale, Annotation de jurisprudence et bibliographie par Jean François RENUCCI, éd DALLOZ, n° 50, Paris Cedex 2009, p 1219.

(2) Serge GUINCHARD; Jaque BUISSON, Op Cit, p1123-1125.

(3) Jean PRADEL, " Un exemple de restauration de la légalité criminelle – le régime des interceptions de correspondances émises par la voie des télécommunications ", Op cit, p49.

(4) Serge GUINCHARD; Jaque BUISSON, Op Cit, p1124.

(5) قانون المسطرة الجنائية وفق آخر التعديلات، إعداد و تقديم، المحمّد لفروجي، مطبعة النجاح الجديدة، الدار البيضاء، ط (2) 2012، ص 69.

خاتمة:

في مجال الإجرام المعلوماتي الذي يستخدم المنظومة المعلوماتية وشبكات الاتصال والانترنت كوسيلة أو يتخذها هدفاً إجرامياً، ظهرت أهمية المراقبة الإلكترونية للمراسلات والاتصالات الإلكترونية كأسلوب إجرائي للتحقيقات الجنائية واستنباط الدليل الرقمي الذي تأكدت مشروعته في الإثبات الجنائي رغم قداسة الحياة الخاصة وحرية سرية المراسلات والاتصالات، وهذا تغليباً لمصلحة المجتمع في حمايته من الإجرام الإلكتروني والسراني الخطير، مما جعل معظم تشريعات الدول تُكرّس المراقبة الإلكترونية باعتبارها من أكفأ الأساليب الإجرائية، ومن بينها التشريع الجزائري الذي نظمها في قانون الإجراءات الجزائية وقوانين أخرى، بتحديد شروط ترخيصها وتنفيذها التي تضمن نجاحها وفعاليتها. حيث أدّت مُناقشته في هذا البحث إلى الخروج بالتوصيات التالية بخصوص قانون الإجراءات الجزائية الجزائري:

1. أن يُضاف شرط التسبب بالنسبة للإذن بالمراقبة التي تتمّ بواسطة التقاط أو اعتراض الاتصال الإلكتروني.
2. أن يُوسّع من مجال استخدام هذه الأسلوب، ويحصر سلطة اتخاذه في قاضي التحقيق فقط.
3. ضرورة النصّ على إجراء إتلاف تسجيلات المراقبة وتحرير محضر الإتلاف بعد الانتهاء من استخدامها.
4. النصّ علماً السماح لضباط الشرطة القضائية المؤهلين خصيصاً لاستخدام أسلوب التسرّب في شبكات الإنترنت.

المراجع:

الكتب والمقالات والأطروحات:

1. محمود أحمد طه، التعدي على حق الإنسان في سرّية اتصالاته الشخصية بين التجريم والمشروعية، دار النهضة العربية، القاهرة، الطبعة الثانية 1999.
2. عادل عبد الجواد مُحمّد الكردوسي، التعاون الأمني العربي ومكافحة الإجرام المنظم عبر الوطني، مكتبة الآداب، القاهرة، الطبعة الأولى 2005.

3. عمر مُحمَّد بن يونس، الإتفاقية الأوروبية للجريمة الافتراضية. مذكرة تفسيرية، منشورات الإتحاد الأوروبي، 2005.
 4. عمر مُحمَّد بن يونس، "الدليل الرقمي"، منشورات المنظمة العربية للتنمية الإدارية بجامعة الدول العربية، 2006.
 5. جمال جرجس تاووضروس، الشرعية الدستورية لأعمال الضبطية القضائية، النسر الذهبي للطباعة، مصر، 2006.
 6. جمال نجيمي، إثبات الجريمة على ضوء الإجتهد القضائي . دراسة مُقارنة . دار هومة، الجزائر، 2011.
 7. فوزي عمارة "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية" مجلّة العلوم الإنسانية، جامعة منتوري قسنطينة، عدد 33 جوان 2010 .
 8. ياسر الأمير فاروق محمّد، مراقبة الأحاديث الخاصّة في الإجراءات الجنائية، رسالة دكتوراه، ج القاهرة، 2008.
 9. يوسف الشيخ، حماية الحق في حرمة الأحاديث الخاصّة دراسة مقارنة في تشريعات التنصت وحرمة الحياة الخاصّة، دار الفكر العربي، القاهرة، الطبعة الأولى 1998.
- النصوص القانونية:**
1. الدستور الجزائري المصادق عليه في استفتاء 28 نوفمبر 1996 المعدّل بالقانون 01-16 في 2016/03/06
 2. قانون الإجراءات الجزائية الجزائري في ضوء الممارسة القضائية، احسن بوسقيعة، بيري، 2018
 3. قانون العقوبات الجزائري في ضوء الممارسة القضائية، إشراف احسن بوسقيعة، بيري، الجزائر 2018
 4. قانون الوقاية من جرائم تكنولوجيا الإعلام والاتصال ومكثفتها، 04-09 المؤرخ في 05 غشت 2009.
 5. قانون الوقاية من الفساد ومكافحته 01-06 المؤرخ في 20/02/2006، ج ر 14 في 2006/03/08

6. قانون البريد والاتصالات الالكترونية رقم 04.18 في 2018/05/10، ج ر، 27 في 2018/05/13

7. قانون حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي 07.18

8. قانون المسطرة الجنائية وفق آخر التعديلات، إعداد، محمد لفروجي، مطبعة النجاح، الدار البيضاء، 2012

9. المرسوم الرئاسي 261.15 المؤرخ في 8 أكتوبر 2015 المتعلق بتشكيل وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، ج ر 53 في 08 أكتوبر 2015.

Ouvrages et articles :

01– Bertrand RENARD; Caroline VANDRESSE, La Belgique ou l'incrimination de l'organisation criminelle comme soutien des techniques d'enquête. Sous la direction de Maria LUISA CESONI, Criminalité organisée – des représentations sociales aux définitions juridiques, L.G.D.J paris, George éditeur Genève, Bruylant Bruxelles 2004.

02– Christian De VALKENEER, KAMINSKI Dan, " Au croisement de la recherche proactive et des écoutes téléphoniques: construction et danger du mutualisme légistique ", Revu de droit pénal et de criminologie, année 83 Mars 2003 Bruxelles.

03– Frédéric DESPORTES, Laurence LAZERGES– COUSQUER, Traité de procédure Pénale, 3^e éd, ECONOMICA, Paris, 2009.

04– Jean PRADEL; Michel DANTI-JUAN, Manuel de droit pénal spécial, éditions Cujas, n° 03, Paris, 2004.

05– Jean PRADEL, " Un exemple de restauration de la légalité criminelle – le régime des interceptions de correspondances émises par la voie des télécommunications (commentaire de la loi n° 91-646 du 10 juillet 1991) ", Recueil Dalloz 1992, Chroniques, p 49.

- 06**–Jean PRADEL , " Le crime organisé après la loi française du 09 Mars 2004 dite loi de Perben II ", Revue de droit pénal et de criminologie, éd la charte, Bruxelles, n° 02, 2005.
- 07**–Joceline LEBLOIS-HAPPE, Autorisation et contrôle des écoutes téléphoniques, rôle du JLD " Actualité Juridique Pénal, n° 6/2008, juin 2008.
- 08**–Marie-Hélène GALMARD, Vers une nouvelle approche du phénomène terroriste ? Apport de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives aux contrôles transfrontaliers ", Revue pénitentiaire et de droit pénal, n°1, janvier/mars, 2007.
- 09**–Myriam QUEMENER, Yves CHARPNEL, Cybercriminalité – Droit pénale appliqué, éd ECONOMICA, 2010.
- 10**–Sontag Koenig SOPHIE, Technologies de l'information et de la communication et défense pénale, éd mare et martin, Paris, 2015.
- 11**–Serge GUINCHARD; Jaque BUISSON, procédure pénale, éd Litec n° 6, Paris, 2010.

Lois:

1. Code De Procédure Pénale, Annotation de jurisprudence et bibliographie par Jean François RENUCCI, éd DALLOZ, n° 50, Paris Cedex 2009.
2. Code Pénal, Annotation de jurisprudence et bibliographie par Yves MAYAUD. éd DALLOZ, n° 108, Paris Cedex 2011.

إجراء التفتيش وضبط الأدلة في الجريمة المعلوماتية

د/ جلول فواز

كلية الحقوق والعلوم السياسية

جامعة المسيلة

ط.د/ بوعاية كمال

كلية الحقوق - جامعة الجزائر 1

مقدمة:

بالرغم من المزايا الهائلة التي تحققت وتحقق كل يوم بفضل تقنية المعلومات على جميع الأصعدة وفي شتي ميادين الحياة المعاصرة، إلا أنه وفي مقابل ذلك صاحبها جملة من الانعكاسات السلبية الخطيرة نتيجة استخدام التقنية المتطورة والانحراف عن الأغراض المتوخاة منها تبدت في تفشي طائفة من الظواهر الإجرامية المستحدثة ألا وهي ظاهرة الجرائم المعلوماتية. (1)

ومما لا شك فيه أن أهم مميزات الجريمة المعلوماتية أنها أصعب الجرائم إثباتا وذلك لكون أن القائم على هذه الجريمة يلجأ إلى استعمال تقنيات حديثة ومتطورة يصعب على غيره التعامل معها، هذا من ناحية.

ومن ناحية أخرى تعتبر الجرائم المعلوماتية أقل عنفا من الجرائم التقليدية بالنظر إلى أنها لا تحتاج أدبي مجهود عضلي بل تعتمد بدرجة كبيرة على الدراية الذهنية والتفكير العلمي المدروس والقائم على معرفة تقنيات الحاسب الآلي.

ومن الواضح أن المشرع الجزائري يكون قد سارع إلى تدارك نوعنا ما النقص وسد الفراغ القائم بخصوص التحقيق القضائي إثر التطور الذي عرفته الجريمة (2)، حيث نجد أن المشرع الجزائري خرج عن القواعد العامة المتعلقة بالتحقيق بما فيها إجراء التفتيش وضبط الأدلة كاستثناء وخصوصية الجريمة المعلوماتية.

وعليه نطرح الإشكال التالي: كيف عالج المشرع الجزائري إجراء التفتيش وضبط الأدلة في مجال الجرائم المعلوماتية؟

ونتيجة لذلك، سنحاول الإجابة على هذه الاشكالية من خلال محورين، نتطرق في (المحور الأول) إلى إجراء التفتيش في الجرائم المعلوماتية، في حين نتطرق في (المحور الثاني) للإجراء الضبط في الجرائم المعلوماتية، وهو ما سوف نوضحه في العرض التالي:

المحور الأول: التفتيش في الجرائم المعلوماتية.

التفتيش في الجريمة المعلوماتية يقع على نظم الحاسوب والانترنت وهو إجراء يهدف للبحث عن الأدلة المادية والمعنوية التي تثبت ارتكاب الجريمة ونسبتها إلى مرتكبيها. وعلمية سنحاول من خلال هذا المحور بيان المقصود بالتفتيش في الجرائم المعلوماتية (الفرع الأول)، مروراً ببيان أهمية التفتيش في الجرائم المعلوماتية (الفرع الثاني)، وصولاً إلى بيان ضوابط التفتيش في الجرائم المعلوماتية (الفرع الثالث) وذلك على الآتي:

الفرع الأول: تحديد المقصود بالتفتيش.

يعرف التفتيش بصفة عامة بأنه "إجراء من إجراءات التحقيق تقوم به سلطة حددها القانون يستهدف البحث عن الأدلة المادية لجريمة تحقق وقوعها في محل خاص يتمتع بالحرمية بغض النظر عن إرادة صاحبه." (3)

وباستقراء فحوى هذا التعريف يتبين بأن إجراء التفتيش ينطبق على الجرائم التي تترك آثار مادية فقط، ونتيجة لذلك فإنه لا يوجد معوقات تعترض هذا لإجراء لاعتبار أنه سوف يتم البحث فيه عن الأدلة المادية الملموسة.

ونتيجة لذلك، يختلف التفتيش في نظم الحاسوب والشبكات عنه في الجرائم التقليدية، بحيث يتم إجراء التفتيش في أشياء مادية وأخرى معنوية تفيد في كشف الحقيقة (4) وهو ما سوف نشير إليه في الفرع الثاني من المحور الثاني المتعلق بالأشياء التي تكون محل للتفتيش والضبط في نفس الوقت.

الفرع الثاني: أهمية التفتيش في الجرائم المعلوماتية.

إن التفتيش سواء كان في العالم المادي أو الافتراضي يعبر من بين إجراءات التحقيق وذو الأهمية الكبيرة في كشف الأسرار وتوضيح معالم ومسار التحقيق، وهذه الأهمية إما تتعلق بالواقعة المراد إثباتها أو بطرق أخرى نستعرضها كالآتي:

أولاً- بالنسبة للواقعة المراد إثباتها: إن التفتيش مادياً كان أم افتراضياً يكشف عن عدة أمور تتعلق بالواقعة محلّه وهي:

1- ثبوت وقوع الجريمة وتوافر أركانها وشروطها.

1- ثبوت الوقت الحقيقي للواقعة ومكانها.

ثانيا- الأهمية بالنسبة للأطراف: إن التفتيش يساعد على التحقيق في الكشف عن عدة أمور تتعلق بأطراف الجريمة نذكر منها:

- 1- تحديد الدافع الحقيقي لارتكاب الجريمة.
- 2- تحديد شخصية الجاني وخطورته الإجرامية من خلال الإطلاع عن أعماله وقدراته في فك الشفرات وأساليبه في استخدام شبكات الاتصال والتعامل الفني معها.
- 3- تحديد عدد الجناة من خلال التفتيش النظام المعلوماتي وما يعتمد عليه من أدوات وأجهزة استخدمت في مكان الجريمة.

وعليه فإن هذه الأهمية التي يكتسبها التفتيش تتحقق سواء في الجرائم التقليدية من خلال التفتيش العادي أو من خلال التفتيش الأنظمة المعلوماتية وما تحتويه من برامج وأساليب فنية نظرا لما تسفر عنه من أدلة تساعد في كشف الحقيقة كالأدوات والأجهزة الالكترونية المستخدمة في ارتكاب الجريمة والبرامج والمعلومات التي يتم التلاعب من خلالها. (5)

والجدير بالذكر، أن القانون رقم 04/90 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما بموجب مادته الخامسة (05) ينص على أنه يجوز للسلطات القضائية المختصة الدخول بغرض التفتيش ولو عن بعد إلى:

- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.
- منظومة معلوماتية. (6)

الفرع الثالث: ضوابط التفتيش في الجرائم المعلوماتية.

يختلف التفتيش في مجال الجرائم المعلوماتية عن التفتيش العادي، فالأول يستهدف جهاز الكمبيوتر (الحاسوب) بمكوناته المادية والمعنوية ولمباشرة إجراءات التفتيش وفق أحكام القانونية ينبغي مراعاة بعض الضوابط والقواعد الشكلية والموضوعية حتى يقع إجراء التفتيش صحيحا وسنكلم عن هذه الضوابط من خلال التالي:

أولا- الضوابط الشكلية للتفتيش في الجرائم المعلوماتية.

يعد إجراء التفتيش من الإجراءات التي فيها خرق وتعدّي على الحقوق والحريات الأفراد ولذلك وضعت غالبية التشريعات الجنائية المقارنة ضمانات يتم من خلالها الموازنة بين حق الفرد في المحافظة على حقوقه وحرياته من الانتهاك وحق المجتمع في القبض على الجناة ومعاقتهم.

وتطبيق تلك الضمانات في مجال التفتيش على نظم المعلوماتية قد تتحول إلى مشكلات تعيق تحقيق الهدف من إجراءات التفتيش بدلا من كونها ضمانات في مجال التفتيش التقليدي. وعليه سوف نحاول من خلال هذه الجزئية عرض أهم الشروط الشكلية التي يتطلبها إجراء التفتيش في مجال الجرائم المعلوماتية وهو ما سيتم إيضاحه في العناصر التالية:

1- الحصول على إذن مسبق من قبل السلطة القضائية المختصة:

يعتبر وجوب الحصول على إذن مسبق لقيام بعملية التفتيش من قبيل الشروط الواجب الالتزام بها حتى لا يقع التفتيش باطلا ومن بين البيانات التي يجب أن يتضمنها إذن التفتيش:

- أن يكون مكتوب وصادر من وكيل الجمهورية أو قاضي التحقيق.
- أن يتضمن الإذن بيان وصف الجريمة موضوع البحث عن الدليل بشأنها وعنوان الأماكن المقصودة بالتفتيش.(7)

والجدير بالذكر، أنه تنجز هذه العمليات تحت الإشراف المباشر للقاضي الذي أذن بها والذي يمكنه عند الإقتضاء أن ينتقل إلى عين المكان للسهر على احترام أحكام القانون، كما أنه إذا إكتشفت أثناء هذه العمليات جرائم أخرى غير تلك الجرائم التي وردت في إذن القاضي فإن ذلك لا يكون سببا بطلان الإجراءات العارضة.

"2- ميقات التفتيش في الجرائم المعلوماتية:

وضع المشرع الجزائري بموجب قانون الاجراءات الجزائية قاعة عامة تم من خلالها تحديد الميقات الذي يجوز فيه دخول المساكن وتفتيشها وهو ما بين الساعة الخامسة صباحا والساعة الثامنة مساء.(8)

وفي مقابل ذلك، أورد المشرع الجزائري إستثناءا يرد على هذه القاعدة أين يجوز دخول المساكن وتفتيشها في أي وقت من اليوم ليلا ونهارا ودون الحاجة للتقيد بالمقيات القانوني المقرر في المادة 1/47 ق إ ج وذلك في بعض الجرائم التي وردت على سبيل الحصر ومن بينها الجرائم المعلوماتية التي يطلق عليها المشرع الجزائري وصف الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

والجدير بالملاحظة، أن الغرض من تمديد الميقات القانوني للتفتيش يتمثل في الإسراع في الإجراء والقيام به خارج الميقات هو المحافظة على الدليل نظرا للطبيعة الخاصة لهذا النوع من الجرائم التي يستفيد فيها الجاني من التطور التكنولوجي ومن ثمة عرقلة سير التحقيق، وذلك لكون أن أدلة الجرائم المعلوماتية هي عبارة عن كيانات غير مادية مما ينتج عنها إمكانية إخفاء أدلتها بسرعة غير متوقعة

هذا إذا ما وصل إلى علم الجاني مسبقا الوقت الذي سيتم فيه تفتيش أنظمتة وهو ما دفع بالمشرع الجزائري إلى إضافة الجرائم المعلوماتية ضمن الجرائم التي تستثنى من مجال قيد المدة الزمنية السابقة الذكر. (9)

3- بالنسبة لحضور صاحب المسكن أثناء عملية التفتيش في الجرائم المعلوماتية:

باستقراء فحوى المواد 82 و 83 من قانون الإجراءات الجزائية الخاصة بخصوص حضور أشخاص معينين لعملية التفتيش والتي تحيلان إلى المادة 45 من ق إ ج، حيث يعفي المشرع الجزائري قاضي التحقيق من وجوب الالتزام بقاعدة الحضور المنصوص عليها في المادتين 82 و 83 ق إ ج فعلى سبيل المثال تنص المادة 82 ق إ ج على أنه "إذا حصل التفتيش في مسكن غير المتهم استدعى صاحب المنزل الذي يجري تفتيشه ليكون حاضرا وقت التفتيش فإذا كان ذلك الشخص غائبا أو رفض الحضور أجرى التفتيش بحضور اثنين من أقاربه أو أصهاره الحاضرين بمكان التفتيش فإن لم يوجد أحد منهم فبحضور شاهدين لا تكون ثمة بينهم وبين سلطات القضاء أو الشرطة تبعية." (10)

وعلى قاضي التحقيق أن يلتزم بمقتضيات المادتين 45 و 47 ق إ ج ولكن أن يتخذ مقدا جميع الإجراءات اللازمة لضمان احترام سر المهنة وحقوق الدفاع.

بالإضافة لما سبق ذكره، يشترط أيضا للتفتيش في الجرائم المعلوماتية دون غيرها من الجرائم الأخرى ضرورة الاستعانة بخبراء الحاسب الآلي يستعين بهم في معاينة مسرح الجريمة أو القيام بعمليات التفتيش أو الضبط وفحص آثار الجريمة لا تشكل خلافا أو قانونيا، كما ينبغي البحث عن أسلوب خاص يجمع بين الخبرة الفنية والكفاءة المهنية للقيام بإجراءات التحقيق مع الاشخاص ذوي العلاقة بجرائم الحاسب الآلي. (11)

ثانيا- الضوابط الموضوعية للتفتيش في الجرائم المعلوماتية.

تتمثل الشروط الموضوعية التي يلزم تحقيقها لإجراء التفتيش في سبب التفتيش المتمثل في وقوع الجريمة ونسبة ارتكابها إلى المتهم، إضافة إلى ضرورة أن ينصب التفتيش على محل يحتمل العثور فيه على أدلة الجريمة، وآخر يفترض لكي يكون التفتيش صحيحا أن تكون له غاية تتمثل في أن يكون التفتيش بغرض العثور على الآثار والأشياء التي يمكن أن تفيد في كشف الحقيقة (12)، نستعرضها على النحو التالي:

1- سبب التفتيش:

يمكن حصر الشروط الموضوعية المتعلقة بسبب التفتيش فيما يلي:

- أن يكون التفتيش بصدد جريمة من الجرائم المعلوماتية واقعة بالفعل سواء كانت جنائية أو جنحة.
- ارتكاب شخص أو عدة أشخاص معينين لإحدى الجرائم المعلوماتية أو المشاركة فيها.
- توافر أدلة قوية أو قرائن على وجود أشياء أو أجهزة أو معدات معلوماتية أو إلكترونية تفيد في كشف الحقيقة. (13)

2- محل التفتيش في الجريمة المعلوماتية:

في الجرائم التقليدية فإن التفتيش يمكن أن ينصب على شخص المتهم أو غيره أو مسكنه أو ما في حكمه لكن في الجرائم المعلوماتية فإن محل التفتيش هو كل المكونات النظام المعلوماتي سواء كانت مادية أو معنوية وكذلك شبكات الاتصال الخاصة به بالإضافة إلى الأشخاص الذين يستخدمون الكمبيوتر محل التفتيش.

3- الغاية من التفتيش:

لا بد من توافر لدى سلطات التحقيق أسباب كافية على أنه يوجد في مكان أو لدى شخص المطلوب تفتيشه أدوات استخدمت في الجريمة المعلوماتية أو أشياء متحصل منها أو مستندات إلكترونية يحتمل أن تكون لها فائدة في إجلاء الحقيقة لدى المتهم أو غيره. (14)

المحور الثاني: ضبط الأدلة في الجرائم المعلوماتية.

يعد الضبط إجراء من إجراءات التحقيق القضائي ودليل إثبات في الجريمة التي يباشر التحقيق بشأنها والتحفظ عليها، والضبط هو الغاية من التفتيش ونتيجته المباشرة ولذلك يتعين عند إجرائه أن تتوفر فيه نفس القواعد التي تطبق على إجراء التفتيش.

وعليه سنحاول من خلال هذا المحور بيان المقصود بالضبط في الجرائم المعلوماتية (الفرع الأول) مروراً ببيان الأشياء التي تكون محل ضبط في الجرائم المعلوماتية (الفرع الثاني)، وصولاً إلى بيان الصعوبات التي تواجه الضبط في الجرائم المعلوماتية (الفرع الثالث) وذلك على الآتي:

الفرع الأول: بيان المقصود بالضبط في الجرائم المعلوماتية.

يعرف الضبط بأنه وضع اليد على أي شيء يتصل بالجريمة التي وقعت من أجل كشف الحقيقة وعن مرتكبيها، والهدف الذي يسعى إليه سلطة التحقيق من أجل القيام بالتفتيش وهو ضبط الأدلة

والوثائق والأشياء التي تفيد في الكشف عن الجريمة لذلك ينبغي التقيد بالقواعد الإجرائية التي تحدد الأماكن التي يجوز تفتيشها والأشخاص الذين يجري تفتيشهم. (15)

الفرع الثاني: الأشياء محل الضبط في الجرائم المعلوماتية.

تتمثل جملة الأشياء التي يتم ضبطها في مجال الجرائم المعلوماتية والتي تكون لها قيمة في مجال الإثبات الجزائي في نوعان هي مكونات ذات قيمة مادية (أولا)، وأخرى ذات قيمة معنوية (ثانيا) نوضحها كالآتي:

أولا- ضبط المكونات ذات القيمة المادية في الجرائم المعلوماتية.

يشمل ضبط المكونات ذات القيمة المادية في مجال الجرائم المعلوماتية ما يلي:

1- ضبط جهاز الكمبيوتر ومكوناته الرئيسية والفرعية.

لا يثير ضبط جهاز الكمبيوتر ومكوناته الرئيسية والفرعية أية مشكلات تعيق إجراءات التحقيق وعليه لا يوجد خلاف بين فقهاء القانون في إمكانية ضبطها طالما أن الهدف والغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في إظهار الحقيقة خاصة وأن المكونات التي سيتم ضبطها هي في حقيقتها مكونات مادية. (16)

هذا وتتمثل المكونات المادية التي يمكن أن تخضع للضبط والمتعلقة بجهاز الكمبيوتر ومكوناته الرئيسية والفرعية في:

أ- الورق: كثير من الجرائم الواقعة على المال أو على جسم الإنسان تترك خلفها قدرا كبيرا من الأوراق والمستندات الرسمية منها والخاصة إلا أو وجود أجهزة الحاسب الآلي يجعل كثيرا من المعلومات يتم حفظها في الحاسب الآلي مما قلل حجم الأوراق والملفات ومع ذلك نجد الكثيرين يقومون بطباعة المعلومات لأغراض المراجعة أو التأكد من الشكل العام للمستند أو الرسالة موضوع الجريمة.

والجدير بالذكر، أن أجهزة الحاسب الآلي والطابعات المتطورة ذات السرعة الفائقة تطبع قدرا كبيرا من الأوراق في وقت قصير وعليه يعتبر الورق من الأدلة المادية التي ينبغي الإهتمام بها في البحث والتفتيش مسرح الجريمة والورق أربعة أنواع هي: الأوراق التحضيرية، أوراق تالفة تتم طباعتها للتأكد وأوراق أصلية تتم طباعتها والاحتفاظ بها كمرجع ولأغراض تنفيذ الجريمة، أوراق أساسية وقانونية محفوظة في الملفات العادية أو دفاتر الحسابات وتكون لها علاقة بالجريمة خاصة عند تقليدها ببياناتها لتنفيذ جرائم المعلوماتية. (17)

ب- وحدات المدخلات: تستعمل هذه الوحدات لإدخال المعلومات أو المعطيات المراد معالجتها من الوسط الموجودة عليه إلى ذاكرة الحاسوب وتشمل على لوحة المفاتيح والفارة (18)، بالإضافة إلى القلم الضوئي ونظام القراءة الضوئية للحروف ونظام قراءة الحروف المغناطيسية.

ج- وحدة المعالجة المركزية: تعتبر هذه الوحدة بمثابة العقل والمفكر المسيطر على عمل باقي الوحدات المكونة لجهاز الحاسوب وتشمل على الوحدات الآتية:

- وحدة الحساب والمنطق وتتمثل هي الأخرى في مجموعة من الدوائر الإلكترونية والمسجلات.
- وحدة التحكم وما تستعين به من مسجلات وسماعات منطقية.
- وحدة المخرجات وما تشمله من وسائط كالشاشة والطابعة والرسم والمصغرات الفيلمية.
- وحدة التخزين الثانوية وتشمل الأقراص مغناطيسية بأنواعها المرنة والصلبة والأشرطة المغناطيسية. (19)

د- وحدة الذاكرة: وهي الوحدة التي يتم بموجبها عملية تخزين المعلومات الواردة للجهاز وتنقسم بدورها إلى ثلاثة وحدات هي: وحدة الذاكرة الرئيسية، وحدة الذاكرة المساعدة، وحدات الإخراج.

ثانيا- ضبط المكونات ذات القيمة المعنوية في الجرائم المعلوماتية.

بالنسبة للمكونات المعنوية للحاسوب فإن ضبطها يثير مشكلة وخلاف بين فقهاء القانون، حيث هناك من يرى بأن إجراء الضبط لا يصلح إلا على الأشياء المادية أما الأشياء المعنوية والمتمثلة في برامج وبيانات الحاسب المعالجة فإن هذه الأخيرة لا تصلح بأن تكون محلا للضبط وذلك للاعتبار أن النصوص القانونية المتعلقة بالضبط يكون مجال تطبيقها الأشياء المادية فقط ومن بين التشريعات التي أخذت بهذا الاتجاه التشريع الألماني. (20)

وكحل لهذه المشكلة قدم أصحاب هذا الاتجاه حلا يمكن من خلاله تجاوز هذا الإشكال وذلك عن طريق التدخل التشريعي لتوسيع دائرة الأشياء التي يمكن أن ترد عليها الضبط لتشمل البيانات الإلكترونية وبرامج الحاسب الآلي وذلك بإضافة عبارة البيانات والبرامج المعالجة عن طريق الحاسوب إلى النص القانوني الذي ينص على التفتيش والضبط. (21)

في حين هناك اتجاه يرى فيه أصحابه بأنه لا مانع من إمكانية ضبط مكونات الحاسب الآلي المعنوية وحجتهم في ذلك أن الهدف والغاية من التفتيش كما ذكرنا سابقا هو ضبط الأدلة المادية التي تفيد

في كشف الحقيقة وعلية فإنهم يرون بأن هذا المفهوم يمتد ليشمل البيانات الإلكترونية وقاعدة البيانات.(22)

أما عن موقف المشرع الجزائري في هذه المسألة فإنه أخذ بمبدأ جواز وإمكانية التفتيش والضبط لأنظمة الحاسوب وما يؤكد على ذلك المواد 47 و84 من قانون الإجراءات الجزائية، فعلى سبيل المثال تنص المادة 84 من ق إ ج على أنه "إذا إقتضى الأمر أثناء إجراء التحقيق وجوب البحث عن مستندات فإن لقاضي التحقيق أو ضابط شرطة قضائية المنوب عنه وحدهما الحق في الإطلاع عليها قبل ضبطها، وعلى قاضي التحقيق أن يتخذ مقدا جميع الإجراءات اللازمة لضمان احترام كتمان سر المهنة وحرية الدفاع ويجب على الفور إحصاء الأشياء والوثائق المضبوطة ووضعها في أحرز محتومة".(23)

ومن جانب آخر، لا يجوز فتح هذه الاحراز والوثائق إلا بحضور المتهم مصحوبا بمحاميه أو بعد إستدعائهما قانونا كما يستدعى أيضا كل من ضبطت لديه هذه الأشياء بحضور هذا الإجراء ولا يجوز لقاضي التحقيق أن يضبط غير الأشياء والوثائق النافعة في إظهار الحقيقة أو التي قد يضر إفشاؤها بسير التحقيق ويجوز لمن يعينهم الأمر الحصول على نفقتهم وفي أقصر وقت على نسخة أو صورة فوتوغرافية لهذه الوثائق التي بقيت مضبوطة إذا لم تخل دون ذلك مقتضيات التحقيق.

الفرع الثالث: الصعوبات التي تواجه عملية الضبط في الجرائم المعلوماتية.

عملية ضبط البيانات المعالجة إلكترونيا تعترضها عدة صعوبات يمكن إجمالها كالآتي:

- 1 - حجم الشبكة التي تحتوي على المعلومات المعالجة إلكترونيا والمطلوب ضبطها.
- 2 - وجود بيانات في شبكات أو أجهزة تابعة لدولة أجنبية.
- 3 - يشمل الضبط أحيانا إعتداء على حقوق الغير أو على حرمة حياتهم الخاصة وعليه يجب إتخاذ ضمانات اللازمة لحماية هذه الحقوق والحريات.(24)

خاتمة:

بعد استعراضنا بالبحث والدراسة لموضوع التفتيش وضبط الأدلة في مجال الجرائم المعلوماتية كإجراء من إجراءات التحقيق القضائي اتضح لنا جليا التحول الذي مس مجال التحقيق القضائي فقد تأثر هذا الأخير بالتطور التكنولوجي وبالخصوص تطبيقات التقنيات الإلكترونية هذا من جهة.

ومن جهة أخرى، قمنا من خلال هذه المداخلة بعرض وإبراز أعمال التفتيش وضبط الأدلة في الجرائم المعلوماتية وتوصنا إلى أن قواعد التفتيش والضبط في الجرائم المعلوماتية لا تختلف بكثير عن الجرائم التقليدية الأخرى.

وعليه نقترح بعض التوصيات:

1- لقد أصبحت الجريمة المعلوماتية من بين أهم قضايا الإجرام الأكثر خطورة والأمر الذي يتطلب الإلمام بكافة القواعد الإجرائية والموضوعية لمواجهتها بشكل فعال خاصة وأن القواعد الإجرائية والنصوص القانونية المقررة لمتابعة الجرائم التقليدية لا تتلاءم وطبيعة هذا النوع من الإجرام، ذلك أن جهات التحقيق لا بد أن تكون مؤهلة للتحقيق في الجريمة المعلوماتية حتى يمكن استيعاب واقعة التحقيق والتعامل مع مفردات الجريمة سيما وأن المجرم الذي ارتكب الجريمة والذي يحقق معه ليس بالمجرم العادي.

2- وعلى هذا الأساس نري بأنه من ضروري تكيف إجراءات المتابعة وخصوصية الجرائم المعلوماتية بما فيها التحقيق، بالإضافة إلى ضرورة التركيز على رفع مستوى والتأهيل للقائمين على الجهات القضائية والأمنية المختصة بالتحقيق الابتدائي والقضائي في هذه الجرائم.

الهوامش:

1- موسى مسعود أرحومة، الاشكاليات الاجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، مداخلة في إطار المؤتمر المغاربي الأول حول الجريمة المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، خلال الفترة 28-29/10/2009، ص 2.

2- زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، 2011، ص 115.

3- سامي حسني الحسني، النظرية العامة للتفتيش في القانون المصري، دار النهضة العربية، القاهرة، 1982، ص 244.

4- على حسن محمد الطوالة، التفتيش الجنائي على النظم الحاسوب والانترنت، عالم الكتب الحديث، الاردن، الطبعة الاولى، 2004، ص 12.

5- مانع سلمي، التفتيش كإجراء للتحقيق في الجرائم المعلوماتية، مجلة العلوم الإنسانية، جامعة محمد خيضر، بسكرة، الجزائر، العدد 22، جوان 2011، ص 230.

- 6- أنظر المادة 05 من قانون رقم 04/09 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، ج.ر.ج.ج، العدد 47، 16 أوت 2009.
- 7- زبيحة زيدان، المرجع السابق، ص 133.
- 8- أنظر المادة 01/47 من قانون الإجراءات الجزائية.
- 9- فايز محمد راجح غلاب، الجرائم معلوماتية في القانون الجزائري واليميني، أطروحة دكتوراه في الحقوق، فرع القانون الجنائي والعلوم الجنائية، جامعة الجزائر 1، السنة الجامعية 2010/2009، ص 329-330.
- 10- أنظر المواد 82 و 83 من قانون الإجراءات الجزائية.
- 11- محمد الأمين البشري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2004، ص 122.
- 12- فايز محمد راجح غلاب، المرجع السابق، ص 317.
- 13- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الاسكندرية، الطبعة الأولى، 2009، ص 209.
- 14- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الطبعة الأولى، 2006، ص 385-386.
- 15- خالد عياد الحلبي، احراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، الاردن، الطبعة الاولى، ص 168.
- 16- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، الطبعة الثانية، 2000، ص 353.
- 17- محمد الأمين البشري، المرجع السابق، ص 117.
- 18- نخلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، الاردن، الطبعة الاولى، 2008، ص 25.
- 19- علي حسن محمد الطوالة، المرجع السابق، ص 140.
- 20- المرجع نفسه، ص 146.
- 21- فايز محمد راجح غلاب، المرجع السابق، ص 343-344.

- 22- المرجع نفسه، ص 344.
- 23- أنظر المادة 84 من قانون الإجراءات الجزائية.
- 24- يوسف صغير، الجريمة المرتكبة عبر الانترنت، رسالة ماجستير، جامعة مولود معمري، تيزي وزو، كلية الحقوق والعلوم السياسية، 2013، ص 87.

إجراءات التحقيق الجنائي في الجريمة الالكترونية

د/ بلعيد جميلة

كلية الحقوق والعلوم السياسية - جامعة المسيلة

مقدمة:

وصف المفكرون الثورة المعلوماتية بالثورة الصناعية الثانية مقارنة بتلك التي تحققت في أواخر القرن التاسع عشر، إذ انعكست الثورة المعلوماتية والتكنولوجية بصفة إيجابية على الكثير من جوانب الحياة المعاصرة والاعتماد شبه كلي في بعض الدول على شبكة المعلوماتية والحواسيب في كل القطاعات العامة أو الخاصة، لكن ذلك لم يمنع ظهور بعض الجوانب السلبية للثورة التكنولوجية أهمها الجرائم الالكترونية التي تمثل تهديدا جديا لأنظمة الدول القانونية والسياسية والاجتماعية، وأضحت تهدد الاستقرار والأمن الداخلي للدول والأمن الدولي بصفة عامة. فالجرائم الالكترونية تعتبر أخطر الجرائم وأعقدها لاعتمادها على الاحترافية والتقنية (le professionnalisme et la technologie de pointe) والفضاء الافتراضي غير المرئي وانتشارها السريع مع صعوبة الكشف عليها أو التحري عليها، وهو الأمر الذي حتم على مشرعي الدول تكييف القوانين حسب هذه الآليات والتقنيات المستحدثة بدل التقنيات التقليدية للجريمة التقليدية الكلاسيكية من حيث الحصول على الإثبات الالكتروني أو الدليل الالكتروني والتحقيق والتحري من أجل ضبط المجرمين وقيام الدليل على ارتكابهم للجريمة. ضمن هذا المسعى قام المشرع الجنائي الجزائري بالتدخل من أجل تعديل قانون العقوبات على غرار معظم دول العالم، تحت تأثير ضرورة التعاون والتنسيق في آليات مواجهة الجريمة المنظمة والعابرة للحدود وعلى رأسها الجريمة الالكترونية وذلك بموجب القانون رقم 15/04 المؤرخ في 2004/11/10¹ باستحداث المواد من 394 مكرر الى 394 مكرر 7، واستحداث القانون

¹ قانون رقم 04-15 المؤرخ في 2004/11/10 الذي يعدل ويتمم الأمر رقم 156/66 الذي يتضمن قانون العقوبات، الجريدة الرسمية العدد 71 الصادرة بتاريخ 2004/11/10 وذلك باستحداث القسم السابع مكرر خاص بالجرائم الماسة بالمعالجة الآلية للمعطيات.

رقم 04/09 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة بالوقاية المتصلة بتكنولوجيات الإعلام والاتصال¹.

أمام هذه التعديلات والتغيرات الجذرية لمسار التحقيق والتحري صبط الجريمة الالكترونية وذلك تحت تأثير التغير المتسارع والهائل على مستوى العالم، نطرح الإشكالية التالية: ماهى الجهات التي تختص بالتحقيق والتحري الجنائي في قانون العقوبات الجزائري، وما هي إجراءاتها التي فرضت نفسها أمام جهات التحقيق خاصة أن الجريمة هي افتراضية احترازية عابرة للحدود والقارات؟؟ للإجابة على هذه الإشكالية قسمنا دراستنا إلى محورين أساسيين:

أولا. التعديلات القانونية الجذرية المستحدثة من طرف المشرع الجنائي الجزائري لمواجهة الجرائم الالكترونية وإجراءات التحقيق الالكتروني
ثانيا. السلطات المكلفة بالتحقيق الجنائي في الجرائم الالكترونية وتشجيع التعاون الدولي في مجال الجرائم الالكترونية

أولا. التعديلات القانونية الجذرية وإجراءات التحقيق الخاصة المستحدثة من طرف المشرع الجنائي لمواجهة الإجرام الالكتروني

تدخل المشرع الجنائي الجزائري بالقيام بتعديلات جذرية في قانون العقوبات وقانون الإجراءات الجزائية وإصدار بعض القوانين الخاصة (1) وإجراءات تحقيق خاصة فرضت نفسها (2).

1/ التعديلات القانونية الجذرية المستحدثة وإجراءات التحقيق الخاصة المستحدثة من المشرع الجنائي الجزائري لمواجهة الجريمة الالكترونية

نميز هنا بين التعديلات المستحدثة من طرف المشرع الجزائري فيما يخص الاعتراف بالجريمة الالكترونية وتعديل مختلف القوانين ذات الصلة (أ)، والنص على إجراءات تحقيق خاصة بها (ب)

أ/ تعديل قانون العقوبات: عدل المشرع الجنائي الجزائري قانون العقوبات باستحداث القسم السابع مكرر منه وذلك بأن كرس ثمان مواد حدد من خلالها الأفعال الماسة بنظم المعالجة الآلية للمعطيات وما يقبلها من جزاء أو عقوبة، وهى الجرائم التي تهدف إلى الإضرار بمعلومات الحاسب الآلي ووظائفه سواء بالمساس بسريرتها أو بالمساس بسلامة محتوياتها أو بتعطيل قدرة وكفاءة الأنظمة بشكل يمنعها

¹ قانون رقم 04/09 المؤرخ في 05/أوت/2009 المتضمن القواعد الخاصة بالوقاية المتصلة بتكنولوجية الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47 الصادرة بتاريخ 16/أوت/2009.

من أداء وظيفتها وهي لا تخرج عن الأشكال الثلاثة التالية: 1/ الاعتداء على المعطيات الداخلية للنظام (المادة 394 مكرر 1 من قانون العقوبات)، 2/ الاعتداء على المعطيات الخارجية للنظام، 3/ جرائم الاعتداء على سير نظام المعالجة الآلية ونظرا للطابع الخطير لهذه الجريمة فقد جرم المشرع الجزائي كل من الاشتراك والشروع في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية وجعل العقوبة عليها هي العقوبة المقررة على الجريمة ذاتها¹.

ب/ تعديل قانون الإجراءات الجزائية: تدخل المشرع الجنائي مرة أخرى فقام بتعديل قانون الإجراءات الجزائية الصادر بموجب الأمر رقم 66-155 وذلك بموجب رقم القانون رقم 06—22 المؤرخ في 20 ديسمبر 2006² ثم بالقانون رقم 15-02 المؤرخ في 23 جويلية 2015 ثم بالقانون رقم 17-07 المؤرخ في 27 مارس 2017 بأن خص الفصل الرابع الذي ورد تحت عنوان "في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور"، إذ تم النص في المادة 65 مكرر 5 على بعض إجراءات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد والتي يجوز بشأنها لوكيل الجمهورية المختص أن يأذن بما يلي: - اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، - وضع الترتيبات التقنية، دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام..."" وهي إجراءات تفصل فيها لا حقا عند دراسة مهام وكيل الجمهورية ودوره كسلطة إشراف ومراقبة لعمليات التحقيق الخاصة بالجرائم الالكترونية.

ج/ إصدار قوانين خاصة بالوقاية المتصلة بتكنولوجية الإعلام والاتصال

¹ براهمي جمال: التحقيق الجنائي في الجرائم الالكترونية، أطروحة لنيل درجة الدكتوراه في العلوم، تخصص القانون، كلية الحقوق والعلوم السياسية جامعة مولود معمري تيزي وزو، نوقشت في 2018/06/27.

² أمر رقم 66-155 المؤرخ في 8 يونيو 1966 الذي يتضمن قانون الإجراءات الجزائية معدل ومتمم بالقانون رقم القانون رقم 06—22 المؤرخ في 20 ديسمبر 2006 ثم بالقانون رقم 15-02 المؤرخ في 23 جويلية 2015 ثم بالقانون رقم 17-07 المؤرخ في 27 مارس 2017 .

نذكر هذه القوانين على سبيل المثال لا الحصر وهي: القانون رقم 2000-03 المؤرخ في 5 أوت 2000 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية¹ والقانون رقم 09-04 القانون رقم 09-04 المؤرخ في 05/أوت/2009 المتضمن القواعد الخاصة بالوقاية المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والذي تضمن بعض الإجراءات الخاصة بالجرائم الالكترونية وكيفية مراقبتها والتحقيق فيها ومجموعة من المراسيم الرئاسية مثل المرسوم الرئاسي رقم 183/04 المؤرخ في 26 جوان 2004 يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي²، والرسوم الرئاسي رقم 15-261 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام ومكافحتها³، وقرار وزاري مؤرخ في 14/04/2017 يتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي⁴.

2- إجراءات تحقيق خاصة تفرض نفسها لمواجهة تعقيدات الجريمة الالكترونية

من هذه الإجراءات نجد:

أ/ اعتراض المراسلات: وهي المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية - وضع الترتيبات التقنية دون موافقة المعنيين ، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه

¹ قانون رقم 2000-03 المؤرخ في 5 أوت 2000 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، الجريدة الرسمية، العدد 48، الصادرة في 06/أوت/2000

² المرسوم الرئاسي رقم 183/04 المؤرخ في 26 جوان 2004 يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني، الجريدة الرسمية، العدد 49، الصادرة في 27/جوان/2004.

³ مرسوم رئاسي رقم 15-261 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام ومكافحتها، الجريدة الرسمية العدد 53 ل 8 أكتوبر 2015.

⁴ قرار وزاري مؤرخ في 14/04/2017 يتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، الجريدة الرسمية العدد، 36، الصادرة، بتاريخ 03 جويلية 2007.

به بصفة خاصة أو سرية...¹ " أين خص إجراء من إجراءات التحقيق في الجرائم الالكترونية وهو التسرب الالكتروني (l'infiltration électronique)².

إن اعتراض المراسلات التي تتم عن طريق الاتصالات السلكية واللاسلكية يشكل مساسا صارخا لحرمة الحياة الخاصة على الرغم من جدارته وفائدته في الكشف عن العديد من الجرائم الالكترونية وهي حرمة الحياة الخاصة التي كفلتها معظم الدساتير في العالم³ ومن اجل خلق نوعا من التوازن بين مقتضيات حماية المصلحة العامة وتلك الخاصة بحماية المصلحة الخاصة تم فرض مجموعة من القيود وهي: ضرورة الحصول على إذن من السلطة القضائية المختصة ، وهو الإذن المكتوب والمسبب الذي يمنحه عادة وكيل الجمهورية أثناء التحقيق الابتدائي أو قاضي التحقيق أثناء مرحلة التحقيق القضائي وإلا كان الإجراء باطلا وهو ضمان لمشروعية هذا الإجراء⁴، يضاف إلى ذلك وجوب تسبيب اللجوء إلى اعتراض المراسلات.

ب/ **التسرب:** بحيث نصت المادة 65 مكرر 11 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 على التسرب الذي تضمنه الفصل الخامس من قانون الإجراءات الجزائية بنصها على انه عندما تقتضي ضرورة التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر

المادة 65 مكرر 5 من القانون رقم 06/22 المؤرخ في 22/ديسمبر/2006 لذي يعدل ويتمم الأمر رقم 155/66 الذي يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية العدد 84 الصادرة بتاريخ 2006/12/24، المعدل والمتمم

² تعرف المادة 65 مكرر 12 من قانون الإجراءات الجزائية التسرب على انه " قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جنابة أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف. يسمح لضابط أو عون الشرطة القضائية أن يستعمل هوية مستعارة وأن يرتكب عند الضرورة الأفعال المذكورة في المادة 65 مكرر 14 أدناه، ولا يجوز تحت طائلة البطلان، أن تشكل هذه الأفعال تحريضا على ارتكاب جرائم ".

³ المادة 2/46 من القانون رقم 01/16 المؤرخ في 6 مارس 2016 يتضمن نص التعديل الدستوري لسنة 2016، ج،ر العدد 14 المؤرخة في 7 مارس 2016.

⁴ غير أنه استثناء لهذه القاعدة عندما يتعلق الأمر بالوقاية من الأفعال الإرهابية أو التخريب أو الجرائم الماسة بأمن الدولة، يكون النائب العام لدى مجلس قضاء الجزائر العاصمة هو المختص بمنح الإذن لإجراء عملية المراقبة حسب ما تنص عليه الفقرتين 6 و 7 من المادة 4 من القانون رقم 04/09 السابق الذكر.

5 والتي من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يجوز لوكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب.."

اذ يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية و تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهاهم أنه فاعل معهم أو شريك لهم، ويسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض، هوية مستعارة¹. يحزر ضابط الشرطة القضائية المكلف بالتسرب تقريراً يتضمن العناصر الضرورية لمعانة الجرائم غير تلك التي قد تعرض للخطر أمن الضابط أو العون المتسرب. يجب أن يكون الإذن المسلم حسب المادة 65 مكرر 11 مكتوباً ومسبباً وذلك تحت طائلة البطلان وتذكر فيه الجريمة التي تبرر اللجوء إلى هذا الإجراء، و هوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، ويحدد هذا الإذن مدة عملية التسرب التي لا يجوز أن تتجاوز أربعة (4) أشهر².

ت/ **التفتيش الإلكتروني:** يجوز للسلطات القضائية المختصة وكذا لضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية الدخول بغرض التفتيش، لو عن بعد منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة، وكذا تفتيش منظومة تخزين معلوماتية³.

ث/ **حجز المعطيات المعلوماتية:** عندما تكشف السلطة التي تباشر التفتيش في منظومة معلوماتية معلومات مخزنة تكون مفيدة للكشف عن الجرائم أو مرتكبيها وليس من الضروري حجز كل المنظومة تقوم بنسخ المعطيات محل البحث لتحليلها وفهمها⁴. كما يمكن الحجز عن طريق منع الوصول إلى المعلومات التي تحتويها المنظومة المعلوماتية إذا استحال إجراء الحجز لأسباب تقنية⁵.

المادة 65 مكرر 12 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، مرجع سابق.¹

المادة 65 مكرر 15 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، مرجع سابق.²

المادة 5 من القانون رقم 09-04 يتضمن القواعد الخاصة بتكنولوجيات الإعلام والاتصال ومكافحتها، نفس المرجع.³

المادة 6 من القانون رقم 09-04 يتضمن القواعد الخاصة بتكنولوجيات الإعلام والاتصال ومكافحتها، نفس المرجع.⁴

مادة 7 من القانون رقم 09-04 يتضمن القواعد الخاصة بتكنولوجيات الإعلام والاتصال ومكافحتها، نفس المرجع.⁵

* **المعاينة الالكترونية:** تتم المعاينة في الجرائم الالكترونية كأى جريمة أخرى عن طريق الانتقال إلى مسرح الجريمة، بحيث نميز هنا بين الانتقال المادي والافتراضي، فإذا كانت الجريمة هي الاعتداء على الحاسب الآلي أو الأشرطة أو الأقراص المغنطة هنا في هذه الحالة يكون الانتقال إلى مسرح الجريمة لمعاينة والحجز على الأشياء التي تعتبر أدلة لوقوع الجريمة.

أما إذا كانت الجريمة واقعة على مكونات غير مادية للأجهزة الالكترونية أو بواسطتها كتلك الواقعة على برامج الحاسوب فيكون الانتقال الكترونياً أي الانتقال عبر الانترنت في إطار أعمال المراقبة والتفتيش نص القانون رقم 09-04 على التزامات مقدمي الخدمات في تقديم المساعدة المكلفة بالتحريات القضائية وبوضع المعطيات التي يتعين عليهم حفظها تحت تصرف السلطات¹، وبعد المعاينة الالكترونية يمكن تحرير محضر بذلك.

ثانياً. السلطات المكلفة بالتحقيق الجنائي في الجرائم الالكترونية وإجراءات التعاون الدول في مجال الجريمة الالكترونية

1/ السلطات المكلفة بمراقبة الجرائم الالكترونية

أ/ السلطة المركزية المتمثلة في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام ومكافحتها

أنشأ المرسوم الرئاسي رقم 15-261 هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها²، والتي تعتبر سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى وزير العدل³، والتي استحدثت تطبيقاً للمادة 13 من القانون رقم 09-04 المؤرخ في 05/أوت/2009 المتضمن القواعد الخاصة بالوقاية المتصلة بتكنولوجية الإعلام والاتصال ومكافحتها.

أ - 1 تشكيل الهيئة: تتكون من:

المادة 10 من القانون رقم 09-04 يتضمن القواعد الخاصة بتكنولوجيات الإعلام والاتصال وكافحتها، نفس المرجع.¹

مرسوم رئاسي رقم 15-261 يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة² بتكنولوجيات الإعلام ومكافحتها، المرجع السابق

³ المادة 2 من المرسوم رقم 15-261 مرجع سابق ذكره،

لجنة مديرة، مديرية عامة، مديرية للمراقبة الوقائية واليقظة الالكترونية، مديرية للتنسيق التقني، مركز للعمليات التقنية، ملحقات جهوية¹. يرأس اللجنة المديرية وزير العدل وتشكل من الأعضاء الآتية: الوزير المكلف بالداخلية، الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال، قائد الدرك الوطني، المدير العام للأمن الوطني، ممثل رئاسة الجمهورية، ممثل عن الدرك الوطني²، ويؤهل القضاة وضباط الشرطة القضائية التابعون للهيئة أثناء ممارستهم لمهامهم أو بمناسبة، طبقا للشروط والكيفيات المنصوص عليها في التشريع الساري المفعول، ولا سيما قانون الإجراءات الجزائية بتفتيش أي مكان أو هيكل أو جهاز بلغ إلى علمهم انه يجوز و/أو يستعمل وسائل أو تجهيزات موجهة لمراقبة الاتصالات الالكترونية. وفي حالة معاينة أفعال يمكن وصفها جزائيا تخطر الهيئة النائب العام المختص للقيام بالتابعات المحتملة³. تتولى الهيئة مراقبة الاتصالات الالكترونية تحت مراقبة قاض مختص، باستثناء الحالات المنصوص عليها في قانون الإجراءات الجزائية⁴.

أ- 2 مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام ومكافحتها

تقوم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال باقتراح الإستراتيجية الوطنية الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وتنسيق وتنشيط عمليات الوقاية من الجرائم الالكترونية ومساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية، وضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة تحت سلطة القاضي المختص وكذا تسجيل وتجميع وحفظ المعطيات الرقمية وتحديد مسارها ومصدرها من أجل استعمالها في الإجراءات القضائية،

وكذا السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها، تطوير التعاون مع المؤسسات والهيئات الوطنية

¹ المادة 6 من المرسوم رقم 15-261، مرجع سابق.

² المادة 7 من المرسوم الرئاسي رقم 15-261 نفس المرجع السابق

³ المادة 30 من المرسوم الرئاسي رقم 15-261، مرجع سابق

⁴ المادة من المرسوم رقم 15-261 مرجع سابق

المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، المساهمة في تكوين المحققين المختصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال، المساهمة في تحديث المعايير في مجال اختصاصها¹.

ب/ **الجهات القضائية:** حسب المادة 5 من القانون رقم 04-09² فيجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه³ الدخول بغرض التفتيش ولو عن بعد، إلى: أ) منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها، ب- منظومة تخزين معلوماتية، وفي الحالة المنصوص عليها في الفقرة "أ" من هذه المادة إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعلومات يمكن الدخول إليها انطلاقاً من المنظومة الأولى فيجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقاً بذلك

***وكيل الجمهورية:**

يقوم وكيل الجمهورية بالإشراف ومراقبة جميع عمليات المراقبة التقنية التي يقوم بها ضباط الشرطة القضائية والتي يأذن بها وكيل الجمهورية بالمختص بإذن مكتوب. عدل المشرع الجنائي الجزائري أحكام المادة 37 من قانون الإجراءات الجزائية وذلك بإضافة فقرة ثانية نصت على مايلي: "...يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات...."⁴

¹ المادة 4 من المرسوم رقم 15-261 مرجع سابق ذكره ،

² المادة 5 من القانون رقم 04-09 يتضمن القواعد الخاصة بتكنولوجيات الإعلام والاتصال وكافتحتها، نفس المرجع السابق.

³ التي تنص انه يمكن القيام بمهام المراقبة الإلكترونية للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة...."

⁴ المادة 37 من القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للامر رقم 66-155 المتضمن قانون الإجراءات الجزائية المعدل والمتمم.

***قاضي التحقيق:** كما تم تمديد الاختصاص المحلي لقاضي التحقيق إلى دائرة المحاكم الأخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات¹.

ت -ضباط الشرطة القضائية: منح لهم التعديل الجديد لقانون الإجراءات الجزائية² صلاحية القيام بإجراءات مراقبة المنظومات الالكترونية عن طريق اعتراض المراسلات وتسجيل الأصوات والتقاط صور بواسطة وسائل الاتصال السلكية واللاسلكية وتحت المراقبة المباشرة لوكيل الجمهورية، يظهر ذلك من خلال الإذن الذي يجب أن يكون مكتوبا متضمنا لكل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سكنية أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير. يسلم الإذن مكتوبا لمدة أقصاها أربعة(4) أشهر قابلة للتجديد حسب مقتضيات التحقيق ضمن نفس الشروط الشكلية والزمنية³. كما يجوز لوكيل الجمهورية أو ضباط الشرطة القضائية الذي أذن له ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينييه أن يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات⁴ المذكورة في المادة 65 مكرر 5⁵. ويجوز ضباط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص محضرا عن كل عملية اعتراض وتسجيل المراسلات وكذا عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري، ويذكر بالمحضر تاريخ وساعة هذه العمليات والانتهاؤها منها⁶. يصف أو ينسخ ضابط الشرطة القضائية المأذون له أو المناب المراسلات أو الصور أو المحادثات المسجلة والمفيدة في

¹ المادة 40 من القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للامر رقم 66-155 المتضمن

قانون الإجراءات الجزائية المعدل والمتمم

² القانون رقم 06-22 المؤرخ في 20/ديسمبر 2006

³ المادة 65 مكرر 7 من القانون رقم 06-22 المؤرخ في 20/ديسمبر 2006، مرجع السابق.

⁴ المادة 65 مكرر 8 من القانون رقم 06-22 المؤرخ في 20/ديسمبر 2006 ن مرجع سابق.

⁵ تنص المادة 65 مكرر 5 من القانون رقم 06-22 المؤرخ في 20/ديسمبر 2006، مرجع السابق "على أنه:

"إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للوطنية أو الجرائم الماسة بأنظمة معالجة الآلية للمعطيات أو جرائم تبييض الأموال...."

⁶ المادة 65 مكرر 9 من القانون رقم 06-22 المؤرخ في 20/ديسمبر 2006.

إظهار الحقيقة في محضر يودع بالملف. كما تنسخ وترجم المكالمات التي تتم باللغات الأجنبية عند الاقتضاء بمساعدة مترجم يسخر لهذا الغرض¹.

ث- الأقطاب الجزائية المتخصصة

حدد المشرع الجزائري أربع محاكم جزائية ذات اختصاص موسع ومدد اختصاصها الإقليمي بموجب المرسوم التنفيذي رقم 06-348 المؤرخ في 5 أكتوبر 2006 الذي يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقاضي التحقيق². وهي محكمة سيدي محمد، محكمة قسنطينة، محكمة ورقلة، محكمة وهران، حيث أعطيت مهمة الفصل في الجرائم المعقدة والخطيرة إلى الأقطاب الجزائية المتخصصة.

2- التعاون الدولي وإجراءات تحقيق جديدة تفرض نفسها ومدى اعتمادها من المشرع الجنائي الجزائري

نميز في هذه الجزئية التعاون الدولي في مجال التشريع (أ) والتعاون في مجال المساعدة القضائية الدولية (ب)، والتعاون والمساعدة الأمنية المتبادلة بين الدول (ج)

أ- **التعاون الدولي في مجال التشريع:** هناك قناعة دولية بضرورة مواجهة الجريمة الالكترونية بصفة جماعية بواسطة التعاون التشريعي بين الدول وتسهيل التعاون وتكريس إجراءات الملائمة والتنسيق والتوحيد في بعض الإجراءات التي من شأنها الكشف والحصول على الدليل الالكتروني وتعقب المجرمين نظرا لكون الجريمة عابرة للوطنية ولتعقيد مسارها وتشعبه. ويعتبر التعاون بين الدول في مجال التشريع من أنجع الحلول لمواجهة الجريمة الالكترونية وتجاوز العقبات التي تعيق عملية المكافحة. يمكن أن نميز الجهود المبذولة على المستوى الدولي، التنسيق التشريعي في إطار منظمة الأمم المتحدة، وفي إطار منظمة التعاون والتنمية الاقتصادية (OCDE) والجهود المبذولة على المستوى الجهوي تتمثل في جهود الاتحاد الأوروبي وعلى مستوى الدول العربية والإفريقية.

المادة 65 مكرر 10 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006¹

² مرسوم تنفيذي رقم 06-348 المؤرخ في 5 أكتوبر 2006 يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقاضي التحقيق، الجريدة الرسمية، العدد 63 المؤرخة في 08 أكتوبر 2006.

ب- التعاون في مجال المساعدة القضائية الدولية

يقصد بالمساعدة القضائية الدولية كل إجراء قضائي تقوم به دولة من شأنه تسهيل عملية المتابعة والمحكمة الجزائية في دولة أخرى بخصوص جريمة من الجرائم¹، حيث تزايد في الآونة الأخيرة أهمية التعاون الدولي في مجال مواجهة ومكافحة الجريمة المنظمة العابرة للوطنية بصفة عامة والجريمة الالكترونية على وجه الخصوص، بما تثيره هذه الجريمة من صعوبة في إثباتها وتقفي أثار المجرمين المحترفين غير المرئيين الذين ينشطون وبكثافة داخل العالم الافتراضي، وكذا في ظل عالميتها وتشتت عناصرها بين الدول²، وضمن هذا المسعى أبرمت الجزائر العديد من الاتفاقيات الثنائية ومتعددة الأطراف تهدف إلى تشجيع التعاون الدولي، وتكريس تنسيق تبادل المعلومات في الجرائم العابرة للوطنية. وتعتبر الاتفاقية الأوروبية حول الجريمة الالكترونية في 2001 مثال يمكن الالتزام بأحكامها لإقرارها عدة إجراءات مستحدثة منها إجراءات تم تميمها واعتمادها في الجرائم التقليدية والالكترونية بما يمكن أن نعبر عليه بثمين الإجراءات التقليدية للتعاون القضائي الدولي (أ-1) و إجراءات أخرى مستحدثة للقضاء على العقبات البيروقراطية (أ-2).

أ-1 تامين الإجراءات التقليدية للتعاون القضائي الدولي،

* **تبادل المعلومات:** يعتبر هذا الإجراء من بين أهم وسائل التعاون الدولي على المستوى الإجرائي بالاتصال المباشر بين الأجهزة الأمنية والقضائية بين الدول، ويمكن أن يتم تبادل المعلومات بشكل عفوي حسب ما نصت عليه المادة 26 من الاتفاقية السابق ذكرها، كقيام السلطات القضائية في دولة من تلقاء نفسها بتقديم معلومات مفيدة ومهمة للتحقيقات. ولتفادي التعقيد والبيروقراطية التي تتسم بها الطرق الرسمية الدبلوماسية نصت المادة 37 / 3 من الاتفاقية الأوروبية حول الجريمة الالكترونية على انه: "في حالة الطوارئ أو الاستعجال كما هو عليه الحال بالنسبة للتحقيق في الجرائم الالكترونية يمكن إرسال طلبات تبادل المعلومات مباشرة من قبل الهيئات القضائية أو الأمنية في الدولة التي قدمت الطلب إلى الهيئات القضائية أو الأمنية التي تحوز على المعلومات في الدولة المطلوب منها.

المادة 329 من قانون الإجراءات الجزائية¹

². براهمي جمال، مرجع سابق، ص 315

نص المشرع الجزائري على هذا الإجراء في المادة 17 من القانون رقم 09-04 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الذي أُنشئ الهئية الوطنية المتصلة بتكنولوجيات الإعلام والاتصال التي تتكون من خبراء متخصصين في هذا المجال.

فمن أجل تطوير تبادل المعلومات وتقويته وتدعيمه يجب العمل على تسهيله بأكبر قدر ممكن من الوسائل وبالتالي حبذا لو يتم تشجيع التواصل وتبادل المعلومات شفها في حالة الاستعجال القصوى على أن يتم تأكيده فيما بعد كتابة و عبر البريد الالكتروني أو موقع السلطة القضائية أو الأمانة للبلد باستعمال مواقع الكترونية آمنة من أجل تفعيل هذا التبادل ومسايرة السرعة الفائقة التي تتميز بها الجريمة الالكترونية، ولهذا لم يغفل المشرع الجزائري على النص على هذا الإجراء المهم جدا في المادة 17 من القانون رقم 09-04 الذي يتضمن القواعد الخاصة بتكنولوجيات الإعلام والاتصال ومكافحتها بحيث أجاز للسلطات المعنية الاستجابة لطلبات المساعدة الرامية إلى تبادل المعلومات ولو باستعمال مختلف وسائل الاتصال السريعة في حالة الاستعجال في إطار الاتفاقيات الدولية ذات الصلة وبالاعتماد على مبدأ التعامل بالمثل (Le principe de réciprocité)، والذي أرفقه بإنشاء الهئية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام ومكافحتها والتي تشكل من خبراء ومتخصصين في مجال مكافحة الجريمة الالكترونية.

***نقل الإجراءات:** يقصد بهذا الإجراء قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية على إقليمها بخصوص جريمة ارتكبتها على إقليم دولة أخرى ولمصلحة هذه الأخيرة متى توافرت شروط معينة أهمها التجريح المزدوج، وشرعية الإجراءات المطلوب اتخاذها بمنظور قانون الدولة المطلوب منها، ويتم نقل الإجراءات وفق وسائل جديدة ودقيقة وفورية وتم هجران الوسائل التقليدية المتمثلة في نقل الوثائق الخطية والمختومة عبر القنوات الدبلوماسية.

***استحداث منصب قاضي الاتصال (Magistrat de liaison):** استحدث مجلس الاتحاد الأوروبي "قاضي الاتصال" وهي تقنية تسمح لكل دولة عضو بتعيين هيئة قضاة وطنية يكون اختصاصها الإشراف على عملية المساعدة القضائية الدولية والتنسيق المباشر والفوري مع

نظيرتها الأجنبية¹ في هذا المجال، وقد ذهبت فرنسا إلى أبعد من ذلك إذ قامت بتعيين قضاة اتصال تعمل مع دولة ليست عضوة في الاتحاد الأوروبي وهي الجزائر².

***تبادل الإنابة القضائية الدولية:** وهو إجراء تتقدم به دولة ما إلى أخرى يتضمن طلب إجراء قضائي من إجراءات الدعوى الجزائية في إقليمها نيابة عنها، ويهدف هذا الإجراء إلى تسهيل الإجراءات الجنائية بين الدول بما يضمن إجراءات تحقيق لازمة للمتهمين وتقديمهم للمحاكمة، وكذا التغلب على عقبة السيادة الوطنية، والتي تشترط فيها الاتفاقيات والمعاهدات الدولية ضمان السرعة والفعالية من خلال تعيين سلطة مركزية وهي عادة وزارة العدل ترسل إليها الطلبات مباشرة لاختصار الوقت وتسريع الإجراءات.

لم يذكر المشرع الجزائري الإنابة القضائية، بما يعني ترك المجال لأحكام الإنابة القضائية الواردة في الاتفاقيات الدولية، التي يمكن أن نذكر منها الاتفاقية المبرمة بين الجزائر وفرنسا في مجال الإنابة القضائية المبرمة في 1962/08/28 التي نصت على أن البلدين يتعاونان لتقديم المعونة والمساعدة القضائية التي تطلبها كل دولة.

***تسليم المجرمين:** لم تعد الحدود الجغرافية للدول تشكل حاجزا أمام مرتكبي الجريمة بسبب التطور الحاصل في مجال تكنولوجيات الاتصال و ما سبب ذلك من عبور الجريمة لحدود دول كثيرة في ظرف لحظة من الزمن، ولأن النشاط الإجرامي لم يعد مقتصرًا على إقليم دولة واحدة بل يشمل إقليم عدة دول حيث لا يمكن متابعة الدولة لمجرميها وتجاوز حدودها للقبض على المجرمين الفارين، ولذلك تم إيجاد آلية تسليم المجرمين كآلية قضائية للتعاون بين الدول. واعترف المشرع الجزائري بأهمية هذا الإجراء كأحد تدابير المساعدة القضائية وجعله مبدأً دستوري بنصه في المادة 82 من الدستور: مبدأ جواز تسليم شخص بناء على قانون تسليم المجرمين وتطبيقاً له. ونص على هذا الإجراء في المادة 694 وما يليها من قانون الإجراءات الجزائية.

¹ كما تعمل هيئة قضاة الاتصال بمساعدة السلطات القضائية والأمنية في بلدها الأصلي على فهم التشريعات الوطنية للدول الأخرى.

² براهمي جمال مرجع سابق، ص 320

أ-2 إجراءات مستحدثة لمواجهة العالم الافتراضي وتذليل العقبات البيروقراطية

وهناك إجراءات مستحدثة للقضاء على العقبات البيروقراطية والبطء والتعقيد تم بالتالي والتخلي على الطرق الدبلوماسية التي تتسم بالبطء والتعقيد واعتماد إجراءات أكثر تقنية ودقة منها:

* طلب الحفظ العاجل للمعطيات المخزنة (la conservation rapide des données stockées):

تعتبر هذه التقنية تقنية مستحدثة للتعاون القضائي الدولي في مجال مكافحة الجرائم المرتكبة عبر وسائل الإعلام والاتصالات الالكترونية وذلك بموجب المادة 29 من الاتفاقية الأوروبية لعام 2001 لتمكين أية دولة طرف في الاتفاقية من المطالبة بحفظ البيانات المخزنة في أجهزة الحاسوب الموجودة في أراضي الدولة المطلوب منها على وجه السرعة خلال الفترة اللازمة لتقديم طلب المساعدة المتبادلة بغرض القيام بالتفتيش أو الدخول بأية طريقة مماثلة لضبط أو الحصول أو الكشف عن هذه البيانات¹. وهو بمثابة تدبير احترازي تحفظي سريع لحفظ المعلومات والبيانات والاحتفاظ بدليل قيام الجريمة، وتفاذي تخريبها من المجرم خاصة إذا كان يعلم بوجود إجراءات تحقيق ومتابعة ضده.

* طلب الكشف العاجل عن البيانات المحفوظة: (Divulgence rapide des données conservées)

هو بمثابة إجراء مكمل للإجراء الأول المتمثل في الحفظ والذي نصت عليه المادة 30 من الاتفاقية الأوروبية المذكورة أعلاه بحيث تلتزم بموجب الدولة المطلوب منها حفظ بيانات المرور المتعلقة بأي بث أو اتصال عبر أجهزة الحاسوب التابعة لها، والتي تبين أن هذا البث أو الاتصال انتقل من مورد خدمات دولة ثالثة بأن تكشف على وجه السرعة إلى الدولة مقدمة الطلب أكبر نسبة ممكنة من البيانات المارة حتى يمكن الكشف عن مرود الخدمة، ولا يمكن للدولة الطرف الموجه إليها هذا الطلب رفض الإفصاح عن البيانات إلا إذا كانت الجريمة سياسية، أو من شأنه الإخلال بسيادة الدولة أو بأمنها أو نظامها العام أو بمصالحها السياسية.

* طلب الدخول لغرض التفتيش والضبط والكشف عن البيانات المخزنة (L'accès aux données pour perquisitionner, saisir, divulguer, les données stockées)

براهمي جمال مرجع سابق، ص 325¹

نصت المادة 31 من الاتفاقية الأوروبية حول الجريمة الالكترونية على هذا الإجراء والتي أجازت لكل دولة طرف أن تطلب من دولة أخرى طرف السماح لها بإجراء تفتيش أو الدخول بأية طريقة مماثلة للكشف عن البيانات المحفوظة بواسطة شبكة المعلومات داخل النطاق المكاني للدولة الطرف في الاتفاقية

* تبادل المساعدة لجمع البيانات في الوقت الحقيقي (L'entraide dans la collecte en temps réel de données relatives au trafic)¹

لم ينص المشرع الجزائري بشكل صريح على هذه الإجراءات الجديدة للتعاون القضائي إلا ما نجده في نص المادة 16 من القانون رقم 04-09 المتعلق بالوقاية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والتي جاءت عامة في النص على جمع الأدلة على الشكل الالكتروني بنصها: "في إطار التحريات والتحقيقات القضائية الجارية لمعانة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن للسلطات المختصة تبادل المساعدات القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكتروني".

ج/ التعاون والمساعدة الأمنية المتبادلة بين الدول: يتجلى هذا التعاون في إطار المنظمة الدولية للشرطة الجنائية (INTERPOL) وهي أكبر شبكة لتبادل المعلومات الأمنية على المستوى الدولي وشاركت في إحباط عدة عمليات إجرامية خطيرة عبر العالم². تضاف إليها شرطة الانترنت الويب الدولية (IWP) والتي أنشئت في الولايات المتحدة الأمريكية³، كما يساهم (EUROPOL) في تنسيق أمني وذلك في إطار الاتحاد الأوروبي. وكذا منظمة الشرطة الجنائية الإفريقية متكون من قوات الشرطة ل 41 دولة افريقية بمبادرة من الجزائر.

¹ ألزمت الاتفاقية الأوروبية حول الجريمة الالكترونية في مادتها 35 كل دولة طرف في الاتفاقية نقطة اتصال وطنية تعمل 24 ساعة / 24 ساعة وطيلة أيام الأسبوع، تكون مهمتها توفير المساعدة المباشرة والفورية في مجال التحقيقات والمتابعات المتعلقة بالجرائم الالكترونية للسلطات القضائية التابعة للدول الأطراف الأخرى.

² باشرت السلطات الأمنية الجزائرية، فتم فتح تحقيق منذ صدور القانون رقم 04-09 في أكثر من 800 جريمة تورط فيها جزائريون وأجانب. ١

³ والتي تتكون من متخصصين وسلطات إنفاذ القانون والمؤسسات الحكومية وضباط شرطة ومتخصصين فنيين من 61 دولة عبر العالم.

خاتمة:

فرض التطور الهائل في مجال الاتصالات السلكية واللاسلكية التي تستعمل العالم الافتراضي ظاهرة عالمية خطيرة تتمثل في الإجرام الإلكتروني الذي يعتبر من أعقد الجرائم وتشعبها وانتشارها بسرعة البرق عبر المنظومة المعلوماتية الإلكترونية العالمية بما حتم على مشرعي الدول التعاون والتنسيق سواء في المجال القضائي أو الأمني في مراحل التحقيق ومتابعة المجرمين والقضاء القبض عليهم عبر حدود وأمكنة جغرافية متعددة لدول المختلفة. أمام الإجرام الخطير والمنظم الذي يتحدى أعنى وأقوى المنظومات القانونية الدولية وجد المشرع الجنائي الجزائري نفسه مجبرا على اعتماد آليات التنسيق والتعاون التقني والخبراتي وضرورة قبول وتلقي المساعدة القضائية والأمنية المتبادلة لمواجهة الجريمة الإلكترونية الافتراضية، وقد حققت في ذلك تقدما كبيرا من خلال التعديلات الكثيرة التي مست قوانين كثيرة ذات الصلة والتي لا يزال يبقى أمامها الكثير يحسده التطور المتسارع والهائل لتقنيات ودقة التكنولوجيات المستعملة في الجريمة التي تمس كل المجالات أبرزها: المجال الأمني، والأخلاقي، والمجتمعي والاقتصادي، المالي.... الخ.

قائمة المراجع والمصادر:

أولا. الرسائل الجامعية

1- براهيم جمال: التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل درجة الدكتوراه في العلوم، تخصص القانون، كلية الحقوق والعلوم السياسية جامعة مولود معمري تيزي وزو، نوقشت في 2018/06/27.

ثانيا. النصوص التشريعية والتنظيمية

أ/ النصوص التشريعية

أ-1- الدستور:

أ-2- قانون رقم 01/16 المؤرخ في 6 مارس 2016 يتضمن نص التعديل الدستوري لسنة 2016، ج، ر العدد 14 المؤرخة في 7 مارس 2016.

- أمر رقم 66-155 المؤرخ في 8 يونيو 1966 الذي يتضمن قانون الإجراءات الجزائية معدل ومتمم بالقانون رقم القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 ثم بالقانون رقم 15-02 المؤرخ في 23 جويلية 2015 ثم بالقانون رقم 17-07 المؤرخ في 27 مارس 2017 .

- قانون رقم 04-15 المؤرخ في 10/11/2004 الذي يعدل ويتمم الأمر رقم 156/66 الذي يتضمن قانون العقوبات، الجريدة الرسمية العدد 71 الصادرة بتاريخ 10/11/2004 وذلك باستحداث القسم السابع مكرر خاص بالجرائم الماسة بالمعالجة الآلية للمعطيات.

- قانون رقم 04/09 المؤرخ في 05/أوت/2009 المتضمن القواعد الخاصة بالوقاية المتصلة بتكنولوجية الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47 الصادرة بتاريخ 16/أوت/2009.

- قانون رقم 03-2000 المؤرخ في 5 أوت 2000 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، الجريدة الرسمية، العدد 48، الصادرة في 06/أوت/2000 - مرسوم رئاسي رقم 183/04 المؤرخ في 26 جوان 2004 يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني، الجريدة الرسمية، العدد 49، الصادرة في 27/جوان/2004. - مرسوم رئاسي رقم 15-261 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام ومكافحتها، الجريدة الرسمية العدد 53 ل 8 أكتوبر 2015.

ب/النصوص التنظيمية

- قرار وزاري مؤرخ في 14/04/2017 يتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، الجريدة الرسمية العدد، 36، الصادرة، بتاريخ 03 جويلية 2007.

مرسوم تنفيذي رقم 06-348 المؤرخ في 5 أكتوبر 2006 يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقاضي التحقيق، الجريدة الرسمية، العدد 63 المؤرخة في 08/أكتوبر 2006/.

إجراءات التحقيق الخاصة بالجرائم الإلكترونية

ط.د/ تباني السعيد

كلية الحقوق والعلوم السياسية - جامعة المسيلة

مقدمة:

نظرا للتطور الذي يشهده العالم في مجال الحاسوب وتقنيات الحاسب الآلي وتعدد البرامج، لا سيما في مجال الجريمة الإلكترونية أدى بجل التشريعات الجنائية (العقابية) إلى تبني سياسة قمعية تهدف إلى تحديث وفعالية الآليات الرقابية في هذا المجال.

ونظرا لخصوصية الجريمة في المجال الإلكتروني سواء من ناحية طبيعتها أو الوسائل المستعملة في ارتكابها نتج عنه تبني إجراءات بحث وتحقيق خاصة.

ولعلّ المشرع الجزائري مواكبة منه لهذه التطورات الحاصلة في هذا المجال لجأ إلى تعديل قانون الإجراءات الجزائية تماشيا مع ذلك الطرح. المتمثلة في القانون 06-22 المتضمن تعديل قانون الإجراءات الجزائية الجزائري. حيث استحدث إجراءات تحقيق خاصة بالجرائم بصفة عامة ومنها الجرائم الإلكترونية. فما هي هذه الإجراءات؟ وما المقصود بالتسرب الإلكتروني؟ وما المقصود باعتراض الرسائل؟

هذا ما سنتطرق إليه طبقا لخطة من مطلبين:

المطلب الأول: التسرب الإلكتروني.

قسم إلى فرعين المقصود بالتسرب الإلكتروني.. كفرع أول.

الضوابط التي تحكم التسرب الإلكتروني... كفرع ثاني.

المطلب الثاني: اعتراض المراسلات وتسجيل الاصوات والتقاط الصور.

قسم إلى فرعين مفهوم بالاعتراض والمراقبة الإلكترونية كفرع أول.

القيود الواردة على الاعتراض والمراقبة الإلكترونية كفرع ثاني.

المطلب الأول: التسرب الإلكتروني

التسرب تقنية جديدة بالغة الخطورة على أمن الضبطية القضائية حيث يتطلب جراً وكفاءة ودقة في العمل، نص عليها المشرع الجزائري في التعديل الحاصل في قانون الإجراءات الجزائية لسنة 2006 م. (1)

إذ أصبحت الطرق التقليدية لاستخلاص الدليل بخصوص هذا النوع من الإجرام يحتاج إلى تقنيات جديدة تتناسب مع طبيعة هذه الجريمة. (2)

حيث يعد التسرب من إجراءات البحث والتحقيق التي أرستها جميع التشريعات لمواجهة الجرائم الإلكترونية.

أما المشرع الجزائري فقد تبني بدوره هذا الإجراء، مباشرة عقب مصادقة الجزائر على إتفاقية منظمة الأمم المتحدة المتعلقة بالجريمة المنظمة. (3)

الفرع الأول: تعريف التسرب

يعرف التسرب بأنه تقنية من تقنيات التحري والتحقيق الخاصة تسمح لضابط أو عون شرطة قضائية بالتوغل داخل جماعة إجرامية وذلك تحت مسؤولية ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرب، بهدف مراقبة أشخاص مشتباه فيهم، وكشف أنشطتهم الإجرامية، وذلك بإخفاء الهوية الحقيقية، وتقديم المتسرب نفسه على أنه فاعل أو شريك. (4)

وبالرجوع إلى قانون الإجراءات الجزائية لا سيما القانون 22/06 في المادة 65 مكرر 12 منه التي جاء بها ما يلي: " يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف. (5)

هو نفس التعريف الذي تبناه المشرع الفرنسي في المادة 706-81 من قانون الإجراءات الجزائية التي تنص:

« un officier ou un agent de police judiciaire spécialement habilité, et agissant sous la responsabilité d'un officier de police judiciaire chargé de cordonner l'opération. (6)

وعلى ذلك فالتسرب نوع من استعمال الحيلة لضبط الجناة وتقديمهم للسلطة القضائية بشرط أن لا ترقى الحيلة إلى درجة العمل غير المشروع أو التحريض على الجريمة، حيث لا يجوز البحث عن

الحقيقة بطرق غير مشروعة حيث يقوم التسرب المنظم على مجموعة من الشروط سنستعرضها لاحقا.
(7)

بالإضافة إلى ذلك كون عملية التسرب عملية معقدة تتطلب أحيانا من العون أو ضابط الشرطة القضائية المساهمة المباشرة في نشاط الخلية الإجرامية التي تم التسرب إليها وذلك بارتكاب أفعال محظورة قصد تحقيق الهدف المقصود من عملية التسرب برمتها.

لذلك جرد المشرع الجزائري الضابط أو العون المتسرب من المسؤولية الجنائية عن كافة الأفعال غير المشروعة التي قد تقدم على ارتكابها أثناء عملية التسرب. (8)

وعلى هذا فالمشرع أجاز عملية التسرب في بعض الجرائم البالغة الخطورة والمنصوص عليها على سبيل الحصر في المادة 65 مكرر 05 وهي:

جرائم المخدرات- الجريمة المنظمة- جريمة تبييض الأموال- الإرهاب- الجرائم المتعلقة بالتشريع الخاصة بالصرف- الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

ويمكن تصور عملية التسرب في الجرائم الإلكترونية في ولوج ضابط أو عون الشرطة القضائية إلى العلم الافتراضي ومشاركته في محادثات أو دردشة أو نقاش مباشر حول تقنيات اختراق شبكات الاتصال أو بث الفيروسات أو انخراطه في مجموعة نوادي الهاكر، مستخدما أسماء وصفات مستعارة وهمية ظاهر فيها بمظهر عادي وطبيعي كما لو كان واحدا منهم قصد استدراجهم والكشف عنهم وعن أعمال الإجرامية. (9)

فالتسرب نظام من أنظمة التحري والتحقيق الخاصة التي تتيح لضباط وأعوان الشرطة القضائية اختراق الجماعات الإجرامية تحت مسؤولية ضابط الشرطة القضائية آخر مكلف بالتنسيق في عملية التسرب تحت رقابة ومصدر الإذن بذلك لوكيل الجمهورية أو قاضي التحقيق بهدف مراقبة أشخاص مشتباه فيهم وكشف أنشطتهم الإجرامية. (10)

الفرع الثاني: ضوابط والشروط التي تحكم التسرب في الجرائم الإلكترونية

إن عملية التسرب عملية معقدة وخطيرة، حيث من خلالها يكون المتسرب فردا من جماعة إجرامية قصد الحصول على المعلومات التي تساعد في الوصول إلى الحقيقة. (11)

وعلى هذا الأساس تتم عملية التسرب وفقا لشروط محددة ومنصوص عليها في قانون الإجراءات الجزائية وهي في مجملها:

- يجب أن يتم التسرب بمناسبة جرائم محددة على سبيل الحصر ويجب أن تتم هذه الإجراءات بمناسبة جريمة في تلبس أو أثناء التحقيق الابتدائي. (12)

وهذا ما سنتطرق إليه على النحو التالي:

1/ الضوابط الشكلية أو الشروط الشكلية:

تقتضي هذه الشروط شكل معيناً منصوص عليها قانوناً ومنها:

- يجوز لقاضي التحقيق المختص عند اقتضاء التحقيق بأن يأذن بإجراءات عملية التسرب، ويجب أن يكون هذا الإذن مكتوباً ومسبباً حتى يكون قانونياً، وعلى هذا يستبعد الإذن الشفاهي، حيث لا يجوز للضابط أو عون الشرطة القضائية الخوض في عملية التسرب من تلقاء نفسه دون الحصول على إذن مسبق من طرف الجهات القضائية المختصة حسب المادة 65 مكرر 11 ق إ ج. والمتمثلة في وكيل الجمهورية قبل افتتاح التحقيق أو قاضي التحقيق على أن تتم العملية تحت الرقابة المباشرة للجهة الصادرة للإذن. (13)

ولا يكفي أن يصدر الإذن من الجهة المختصة فلا بد أن يكون مكتوباً طبقاً للمادة 65 مكرر 15 ق إ ج والتي جاء فيها ما يلي: " يجب أن يكون الإذن المسلم تطبيقاً للمادة 65 مكرر 11 أعلاه مكتوباً ومسبباً وذلك تحت طائلة البطلان. (14)

بالإضافة إلى أنه يجب أن يكون الإذن لمدة أقصاها 4 أشهر، قابلة للتجديد مرة واحدة لنفس الفترة حسب مقتضيات البحث والتحري وإلا كان باطلاً حيث يجوز لوكيل الجمهورية في أي وقت يراه مناسباً أن يوقف عملية التسرب وهذا ما تقرره المادة 65 مكرر 17. (15)

كما يشترط في الإذن جملة من البيانات التي يتوقف على تحديدها صحة أو بطلان الإجراءات كاسم الضابط التي تتم العملية تحت إشرافه ومسؤوليته.

2/ الضوابط الموضوعية (الشروط الموضوعية):

بالإضافة إلى الشروط والضوابط الشكلية في عملية التسرب والمتمثلة في الإذن الصادر من السلطة المختصة فإن هناك شروط موضوعية تنصب على موضوع عملية التسرب ذاتها حيث أحاط المشرع عملية التسرب بضمانات موضوعية وهي:

• أن يكون الإذن ممنوح لضابط الشرطة القضائية مسبباً مبرراً وهذا ما أشار إليه المشرع في المادة 65 مكرر 15 ويتمثل عنصر التسيب في المبررات والحجج التي أقنعت الجهات القضائية

المتخصصة لمنح الإذن بإجراء عملية التسرب وكذلك الدوافع والأسباب التي جعلت ضباط الشرطة القضائية يلجأ إلى هذه العملية والمتمثلة عادة في ضرورة التحقيق في هذه الجريمة.

• أن يتعلق الإذن بالجرائم المذكورة في نص المادة 65 مكرر 05 أي بمعنى آخر أن ينصب الإذن في عملية التسرب على نوع محدد من الجرائم المنصوص عليها طبقاً للمادة 65 مكرر 05 المذكور آنفاً وهذه الجرائم هي:

(جرائم المخدرات - الجريمة المنظمة العابرة للحدود الوطنية - الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

جريمة تبييض الأموال - الإرهاب - الجرائم المتعلقة بالتشريع الخاصة بالصرف - وكذا جرائم الفساد.....). (16)

وعلى هذا يجوز للضباط أو الأعوان الذين يعملون في عملية التسرب استعمال هوية مزورة ولا يجوز بحال من الأحوال إبراز وإظهار الهوية الحقيقية لأي منهم طبقاً للمادة 65 مكرر 16 " لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الذين يباشرون عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات. (17)

* الحماية القانونية لمنفذ عملية التسرب:

نتيجة لخطورة عملية التسرب فقد كفل القانون حماية قانونية خاصة للمتسرب ولأولاده حيث جعل المتسرب بمنأى عن تحمل المسؤولية الجنائية عن الجرائم التي يكون قد ارتكبها عرضاً أثناء تنفيذه للمهام الموكلة إليه، ومنع الكشف عن هويته الحقيقية وسمح له بأخذ هوية مستعارة، ورتب على مخالفة هذه الإجراءات عقوبات جزائية. (18)

وتتضاعف هذه العقوبات عند إفشاء هذا الكشف لهوية المتسرب إلى جروح أو أحوال أفراد عائلته للضرب أو الجرح أو عرض حياته للخطر قد يتضاعف في حالة الوفاة أي ضرورة حماية المتسرب يميز له مواصلة النشاط الموكل إليه دون تحمله لأي مسؤولية بشرط إخبار الجهة المصدرة للإذن. (19) وعلى هذا فالمرشح قصد حماية الشخص المتسرب سواء كان ضابط شرطة قضائية أو أحد أعوان الشرطة القضائية إحاطة جملة من الضمانات:

- الحماية الجزائية لهوية المتسرب: أي تجريم كل فعل ويعاقب على كل فعل يؤدي إلى كشف الهوية الحقيقية للمتسرب بعقوبة إلى 5 سنوات حبس ويغرامة مالية 500.00 دج إلى 200.000 دج. (20)

- الإعفاء من المتابعة الجزائية لا يمكن متابعة المتسرب متى كان الإجراء (الإذن بالتسرب) وفقا للشروط المطلوبة قانونا.

- عدم سماع المتسرب كشاهد وهو أمر طبيعي للحفاظ على سلامته وعدم الكشف عن هويته.

(21)

المطلب الثاني: اعتراض المراسلات - تسجيل الأصوات والتقاط الصور

اعتمدت العديد من الدول إلى تبني عملية اعتراض ومراقبة الاتصالات الإلكترونية ضمن إجراءات التحري والتحقيق الجنائي، وذلك من خلال قوانينها ولا سيما قانون الإجراءات الجزائية. وكان المشرع الفرنسي سابقا في هذا المجال من خلال قانون الإجراءات الجزائية لعام 1991 ثم المشرع الأمريكي في 2000.

ونظرا لنجاعة هذا الإجراء في تعقب الدليل وإثبات الجرائم الإلكترونية لم يتخلف المشرع الجزائري عن هاته الدول بل تدخل بموجب قانون الإجراءات الجزائية 22/06 المؤرخ في 2006/09/20 المعدل والمتمم فاستحدث هذا الأخير في الفصل الرابع تحت عنوان اعتراض المراسلات وتسجيل الأصوات والتقاط الصور. (22)

الفرع الأول: مفهوم الاعتراض والمراقبة الإلكترونية

عرفت لجنة خبراء البرلمان الأوروبي في اجتماعها بسترسبورغ في 2006/10/06 لدراسة أساليب التحري التقنية وعلاقتها بالإرهاب عملية اعتراض المراسلات بأنها " عملية سرية المراسلات السلوكية واللاسلكية وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة حول الأشخاص المشتبه فيهم في ارتكابهم أو مشاركتهم في ارتكاب الجريمة. (23)

وقد اقتبس المشرع الجزائري هذا التعريف بشيء من التفصيل في المادة 65 مكرر 5 من قانون الإجراءات الجزائية التي جاء فيها >> بأنها اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلوكية واللاسلكية وهذه المراسلات عبارة عن بيانات قابلة للتخزين- الاستقبال والعرض وهذا بإعادة صياغة المادة 100 من قانون الإجراءات الجزائية الفرنسي. (24)

Art (100): “... les autorités judiciaires peuvent intercepter, enregistrer et transcrire des correspondances émises par la voie des télécommunications ... »

شرح المفاهيم والمصطلحات:

مفهوم اعتراض المراسلات:

هي عملية سرية المراسلات السلوكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع أدلتها والمعلومات حول الأشخاص المشتبه في ارتكابهم أو مشاركتهم في الجريمة. (52)

حيث تتم المراقبة عن طريق الاعتراض - التسجيل - أو النسخ والتي هي عبارة عن بيانات قابلة للإنتاج أو التوزيع أو التخزين أو الاستقبال أو العرض.

مفهوم تسجيل الأصوات والتقاط الصور:

يقصد بها تسجيل المحادثات الشفوية التي يتحدثها الأشخاص بصفة سرية أو خاصة في مكان عام أو خاص، وكذلك التقاط صور الشخص أو عدة أشخاص يتواجدون في مكان خاص.

كما عرفت المادة 02 فقرة (و) من القانون 04/09 الاتصالات الإلكترونية بأنها >> أي ترسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صورا أو أصواتا أو معلومات مختلفة بواسطة أية وسيلة إلكترونية. (26)

الفرع الثاني: القيود الواردة على عملية الاعتراض والمراقبة الإلكترونية

ضمن المشرع ضابط الشرطة القضائية من اختصاصات بالغة الخطورة فيها مساسا بالحريات الفردية تتمثل في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور وأحاطها بضمانات وشروط سوف نتطرق لها كالتالي: (27)

حيث تتم المراقبة عن طريق هذه الآلية كما يمكن التفرقة بين اعتراض المكالمات الهاتفية وبين وضع الخط الهاتفية تحت المراقبة.

فيكون اعتراض المكالمات الهاتفية دون رضا المعني بينما وضع الخط لهاتف تحت المراقبة برضا صاحب الشأن. (28)

لا تتم هذه الإجراءات صحيحة إلا باحترام مجموعة من الشروط الواردة في نص المادة 65 مكرر 5 من ق إ ج وهي:

1/ يجب أن تتم هذه المراقبة واعتراض المراسلات بمناسبة جرائم محدودة على سبيل الحصر وهي (جرائم المخدرات - الجريمة المنظمة العابرة للحدود الوطنية - الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات. جريمة تبيض الأموال - الجرائم الإرهابية - جرائم الصرف - وكذا جرائم الفساد). (29)

2/ الحصول على إذن السلطة القضائية المختصة قيد المشرع عملية اعتراض أو مراقبة المراسلات بشرط الحصول على إذن مكتوب ومسبب من الجهات القضائية المختصة المتمثلة في وكيل الجمهورية أثناء مرحلة التحقيق الابتدائي أو قاضي التحقيق في مرحلة التحقيق القضائي وإلا كان هذا الإجراء باطلا فالسلطة القضائية وحدها المختصة في هذا الشأن وهو يعد بمثابة ضمانات لازمة لمشروعية الإجراء. (30)

واستثناء على هذا الاختصاص وطبقا لمادة 04 من الأمر 09/04 وللوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الماسة بأمن الدولة فالنائب العام لدى مجلس قضاء الجزائر هو صاحب الاختصاص الأصلي في منح الإذن لمدة 06 أشهر قابلة للتجديد. (31)

إلا أنه يطرح التساؤل على لي أساس جاء هذا الاستثناء هل على أساس طبيعة الجريمة أو خطورتها رغم أن الجرائم المتعلقة بعملية الاعتراض المنصوص عليها من المادة 65 مكرر 5 كلها خطيرة -فما جدوى هذا الاستثناء؟

3/ كما يجب أن يتضمن الإذن كل العناصر التي تسمح بالتعرف على الاتصالات المراد التقاطها والأماكن المقصودة والجريمة المبررة لهذه الإجراءات ومدتها.

4/ يجب أن يكون هذا الإجراء لمدة أقصاها أربعة (04) أشهر قابلة للتجديد حسب مقتضيات التحري والتحقيق.

- كما على ضابط الشرطة القضائية وكل شخص تحت سلطته وهم بصدد مراقبة الاتصالات أو التبادلات بين الأشخاص موضع الاشتباه ويكتشفون صدفة حالات إجرامية جديدة لا تتعلق بمحل الإذن فعليهم ضبطها وعرضها على النيابة العامة.

5- كما يجوز لضابط الشرطة القضائية إصدار تسخيرة لكل عون مؤهل لدى مصلحة أو هيئة عمومية أو خاصة مكلفة بوسائل الاتصال والعمليات التقنية وأن يحضر محضر على ذلك يبين فيه تحديد تاريخ وساعة بداية هذه العمليات والانتهاؤها منها. (32)

الخلاصة:

الملاحظ من أن المشرع قد وسع من اختصاصات ضابط الشرطة القضائية وقاضي التحقيق في مجال البحث والتحري عن الجرائم وذلك مسايرة لكافة التشريعات المقارنة الأخرى. ورغم أن هذه العمليات تتم جلها بإذن من وكيل الجمهورية أو قاضي التحقيق فإن هذه الإجراءات تعد خطيرة على الحياة الفردية الحقوق والحريات حيث أنه في بعض الأحيان يبدو انتهاك حرمة الحياة الخاصة جليا لاسيما في مرحلة التحقيق والتحري. وتبدوا جلية أكثر في حالة انتهاء التحقيق بدون إدانة للجاني،

- ولهذا ندعو المشرع إلى تضيق هذا الاختصاص كأن يطلب من وكيل الجمهورية هذا الإجراء من قاضي التحقيق متى رأى ذلك لازما.
- إنشاء هيئات أخرى تحارب الجريمة في هذا المجال وتفعيل الأجهزة الخاصة في هذا المجال - كهيئة مكافحة الفساد - والهيئة الوطنية للوقاية من الجريمة المعلوماتية.
- منح ضمانات أكثر فعالية للهيئات الإدارية ولاسيما في مجال مكافحة الفساد حيث أصبحت بعض الهيئات خوفا من المتابعة القضائية الطويلة تنأى بنفسها عن التبليغ عن هذه الجرائم.
- إقامة ندوات توعية ولاسيما في مجال الفساد.

المراجع:

- (1) عبد الرحمان خلفي - الإجراءات الجزائية في التشريع الجزائري المقارن - دار بلقيس - الجزائر - 2015 - ص 103.
- (2) براهيم جمال - التحقيق الجنائي في الجرائم الإلكترونية - أطروحة لنيل شهادة الدكتوراه تخصص القانون - جامعة مولود معمري - تيزي وزو - نوقشت بتاريخ 2018/06/27 - ص 87.
- (3) براهيم جمال - المرجع نفسه - ص 88.
- (4) عبد الرحمان خلفي - المرجع السابق - ص 103-104.
- (5) أحمد لعور / نبيل صقر - موسوعة الفكر القانوني - قانون الإجراءات الجزائية نصا وتطبيقا - دار الهدى - الجزائر - 2015 - ص 52.
- (6) براهيم جمال - المرجع السابق - ص 89.

- (7) عبد الله أو هاببية- شرح قانون الإجراءات الجزائية الجزائري- التحري والتحقيق- دار هومة- الجزائر- 2015- ص320.
- (8) براهيمي جمال- المرجع السابق- ص90.
- (9) براهيمي جمال- المرجع نفسه- 91.
- (10) رابح وهيبة- التسرب في قانون الإجراءات الجزائية الجزائري- مقال منشور في مجلة البحوث في الحقوق والعلوم السياسية- جامعة ابن خلدون تيارت- العدد الخامس- 20 أبريل 2017- ص288.
- (11) رابح وهيبة- المرجع نفسه- ص289.
- (12) عبد الرحمان خلفي- المرجع السابق- ص105.
- (13) براهيمي جمال- المرجع السابق- ص91-92.
- (14) أنظر المادة 15 مكرر ق إ ج.
- (15) عبد الله أو هاببية- المرجع السابق- ص321.
- (16) براهيمي جمال- المرجع السابق- ص92.
- (17) أحمد لعور/ نبيل صقر- المرجع السابق- ص53.
- (18) رابح وهيبة- المرجع السابق- ص292.
- (19) رابح وهيبة- المرجع نفسه- ص292-293.
- (20) أنظر المادة 15 مكرر 16 ق إ ج.
- (21) رحامية عماد الدين- المتابعة الجزائية لجرائم الفساد والعقوبات المقررة لها في ظل القانون 01/06 المتعلقة بالوقاية من الفساد- مقال منشور بمجلة الفقه والقانون- العدد التاسع- يوليو 2013- ص6.
- (22) براهيمي جمال- المرجع السابق- ص93-94.
- (23) براهيمي جمال- المرجع نفسه- ص94.
- (24) براهيمي جمال- المرجع نفسه- ص95.
- (25) سامية بولافة / مبروك ساسي- الأساليب المستحدثة في التحريات الجزائية- مقال منشور بمجلة الباحث للدراسات الأكاديمية- العدد التاسع- جوان 2016- ص18.

(26) المادة 02 من القانون 04/09- الصادر في 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها- ج ر عدد 47 بتاريخ 2009/08/16- ص05.

(27) عبد الرحمان خلفي- المرجع السابق- ص100

(28) عبد الرحمان خلفي- المرجع نفسه- ص101.

(29) عبد الرحمان خلفي- المرجع نفسه- ص102.

(30) براهيمي جمال- المرجع السابق- ص93-94.

(31) أنظر الفقرة 6- 7 من المادة 04 من القانون 04/09- المرجع السابق- ص05.

(32) سامية بولافة/ مبروك ساسي- المرجع السابق- ص09.

التفتيش وضبط الأدلة كآليتين فعاليتين للتحقيق في الجرائم المعلوماتية

ط.د/ كرازدي سارة

كلية الحقوق والعلوم السياسية

جامعة المسيلة

مقدمة:

إن التطور الحاصل على الساحة الدولية في مجال تكنولوجيا المعلومات و ما حققه من آثارا إيجابية ومن إنجازات وتطورات في المجال الرقمي أصبح يعتمد عليه في الكثير من قطاعات الحياة، إلا أنه في الوقت نفسه مهد لظهور أنواع جديدة من الجرائم المعلوماتية بالغة الخطورة، حيث شكلت اعتداءات على الحياة الخاصة للأفراد وتسببت في خسائر فادحة في إقتصاديات الدول، لكون المجرم إستغل هذه التقنيات و الأساليب الحديثة لارتكاب هذه الجرائم دون ترك آثار للكشف عن هوية مرتكبها ومعرفة مصدرها، كما مكنته من اقتراف الجرائم في أي مكان و زمان في الوقت نفسه.

هذه الجرائم المعلوماتية تجمع بين ذكاء المجرم (الذكاء الإنساني) وذكاء الأجهزة الرقمية (الذكاء الاصطناعي)، لذلك فإن هذا التطور التكنولوجي يجب أن يواكبه تطور لقوانين العقوبات و قوانين الإجراءات الجزائية من أجل كبح جماح الجرائم المستحدثة التي ترتكب عبر الوسائط الإلكترونية، كما يجب العمل على تطوير وسائل الإثبات الجزائية بما يتوافق والحقائق العلمية، فالقانون يجب أن لا ينفصل عن الواقع.

إن الإثبات عموما يهدف إلى تبيان التطابق بين الشكل القانوني والوقائع المعروضة، حيث يتم استخدام وسائل معينة (الأدلة) لغرض الإثبات أو النفي، وتثير مسألة الإثبات في مجال تكنولوجيا المعلومات (الحاسوب والانترنت) مشكلات في جمع الأدلة الجنائية، باعتبار الجرائم المعلوماتية غير مرئية حيث يمثل انعدام الدليل المرئي عقبة كبيرة أمام كشف الجرائم، وقد يشكل تشفير البيانات المخزنة إلكترونيا أو المنقولة عبر الانترنت صعوبة أمام إثباتها، كما أن سهولة محو الدليل تعد من أهم الصعوبات التي تعترض طرق الوصول إلى أدلة الإثبات الجنائي في مجال الجرائم المعلوماتية، و من بين هذه الوسائل التفتيش و ضبط الأدلة.

و في هذا الصدد و بناء على ما سبق يمكن طرح الإشكالية التالية:

ما هي الإجراءات المتبعة في التفتيش و ضبط الأدلة لمحاربة الجرائم المعلوماتية؟

و هذا ما سنحاول الإجابة عليه من خلال المبحثين التاليين:

المبحث الأول: التفتيش في الجرائم المعلوماتية.

المبحث الثاني: ضبط الأدلة في الجرائم المعلوماتية.

المبحث الأول: التفتيش في الجرائم المعلوماتية.

باعتبار التفتيش من أهم آليات التحقيق ألا أنه من أخطر الحقوق التي منحت للمحقق لكونه يمس بالحريات التي تكفلها وتصورها الدساتير، فإن مختلف التشريعات تقيد هذا الحق و من بينها التشريع الجزائري الذي وضع له عدة ضوابط سواء فيما يتعلق بالسلطة المختصة بمباشرة، أو التي تأذن بإجرائه، أو الحالات التي تجوز فيها مباشرته وشروط اتخاذه، وكل هذا يمثل ضمانات الحرية الفردية و حرمة المسكن.

يقع التفتيش على محل منح له القانون حرمة خاصة باعتباره مستودع السر، وقد يكون المحل شخص أو مسكن أو محل ألحقه القانون في حكم المسكن، ويباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أدلة أو أشياء يكون كشفها مفيدا لإظهار الحقيقة، و قد نصت عليه العديد من المعاهدات و الاتفاقيات من بينها اتفاقية بودابست التي تناولت إجراء التفتيش، أي تفتيش البيانات في المادة 19 منها.

المطلب الأول: تعريف التفتيش المعلوماتي.

يجمع الفقه الجنائي على أن التفتيش هو إجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة، تحقق وقوعها في محل يتمتع بحرمة، وذلك وفقا للضمانات والقيود القانونية المقررة، من أجل هذا فإن تفتيش نظم المعالجة الآلية يعد من أخطر المراحل حال إتخاذ الإجراءات الجزائية ضد مرتكب الجريمة المعلوماتية، لكون محل التفتيش فيها هو نظام المعالجة الآلية ذو الطابع غير المادي، ولا يعدو أن يكون إلا معلومات إلكترونية ليس لها أي مظهر مادي محسوس في العالم الخارجي.

لا يختلف معنى التفتيش في الجريمة التقليدية عن الجريمة المعلوماتية، وبالتالي يقصد به بأنه ذلك الإجراء الذي يدخل ضمن إجراءات التحقيق الابتدائي أو القضائي الغرض منه البحث عن أدلة

الإثبات المرتكبة، وكل ما يفيد للوصول إلى الحقيقة في متابعة أي شخص يشتبه في أنه مرتكب الجريمة.¹

فقد نص قانون الإجراءات الجزائية الجزائري رقم 04/09 في المادة 05 فقرة 01 بأنه "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه الدخول بغرض التفتيش ولو عن بعد إلى:
-منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.
-منظومة تخزين معلوماتية".

المطلب الثاني: شروط تفتيش الجرائم المعلوماتية.

يعتبر التفتيش انتهاك على الحق في الخصوصية الفردية، ومن ثم يعد التفتيش أحد مظاهر تقييد الحريات الإنسانية، لذا عمدت الدول على إحاطته بالضمانات القانونية حتى لا يتم إساءة استخدامه و هذا ما سنتناوله :

الفرع الأول: الشروط الموضوعية لتفتيش الجرائم المعلوماتية.

يشترط أن يتوافر للتفتيش في النظم المعلوماتية مجموعة من القواعد الموضوعية و هي :
أولاً- أسباب تفتيش النظم المعلوماتية: لقد تناول المشرع الجزائري سبب التفتيش في أكثر من نص منها المادة (44) من قانون الإجراءات الجزائية والتي نصت على ما يلي " : لا يجوز لضباط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء تفتيش إلا بإذن مكتوب صادر من وكيل الجمهورية أو قاضي، التحقيق مع وجوب الاستظهار بهذا الأمر قبل الدخول إلى المنزل والشروع في التفتيش"².

وعليه لكي يعتبر التفتيش في مجال الجريمة المعلوماتية مشروعاً، لابد من توافر شروط محددة حصراً والتي نوردتها فيما يلي:

¹ بلعليات إبراهيم، أركان الجريمة و طرق إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الجزائر، ط 1، 2006، ص214.

² المادة 44 الفقرة 2 من ق.إ.ج.ج.

- وجوب وقوع جريمة معلوماتية سواء كانت جنائية أو جنحة، وبالتالي تستبعد المخالفات نظرا لقلة أهميتها باعتبارها لا تصل إلى درجة المساس بحريات الأشخاص أو انتهاك لحرمان منازلهم¹.
- اتهام شخص أو أشخاص معينين بارتكاب الجريمة أو المشاركة فيها.
- توافر أمارات قوية أو قرائن على وجود أجهزة معلوماتية تفيد في كشف الحقيقة لدى المتهم أو غيره².

ولذلك فلا يجرى التفتيش إلا إذا توافرت لدى قاضي التحقيق أسباب كافية مقنعة، أي تواجد أدوات أو أشياء استعملت في ارتكاب الجريمة أو متحصلة منها، أو مستندات إلكترونية يحتمل أن يكون لها فائدة في التفتيش عن الحقيقة سواء لدى المتهم المعلوماتي أو غيره والتي تتواجد في المكان أو عند الشخص المراد تفتيشه³.

ثانياً - محل تفتيش النظم المعلوماتية: يقصد بمحل التفتيش المستودع الذي يحتفظ فيه الشخص بالأشياء التي تتضمن سره، ومحل التفتيش في الجرائم المعلوماتية هو نظام المعالجة الآلية بكل مكوناته المادية والمعنوية وشبكات الإتصال، وحكم تفتيش هذه المكونات يتوقف على طبيعة المكان الموجود فيه، فيما إذا كان من الأماكن العامة أو من الأماكن الخاصة، وتكمن أهمية التفرقة هنا في أن هذه الكيانات في الأماكن الخاصة يكون لها حكم تفتيش المساكن بنفس الضمانات المقررة قانونا سيما إشتراط الإذن بالتفتيش من السلطات القضائية المختصة وهو ما نصت عليه المادة 44 من قانون الإجراءات الجزائية فيما يتعلق بالإذن المكتوب، وهذه الضمانة خاصة بجميع الجرائم بما فيها الجرائم المعلوماتية، أما التفتيش الواقع على مكونات الحاسوب الموجودة في الأماكن العامة فإن أغلب

¹ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي الإسكندرية، الطبعة الأولى، 2009، ص، ص، 211-210.

² هلال عبد الله أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة، طبعة الأولى، دار النهضة العربية، القاهرة، 1997، ص. 115.

³ طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتي، د. ط، دار الجامعة الجديدة، الإسكندرية، د.س.ن، ص 405.

التشريعات تميز لرجال الضبطية دخول المحال العامة المفتوحة للجمهور كمقاهي الإنترنت من أجل مراقبتها والتأكد من إحترامها للأخلاق والآداب العامة بكل سهولة دون حاجة لإذن بالتفتيش.¹ كما تطرق المشرع الجزائري لتفتيش المنازل في نص المادتين (82-83) من قانون الإجراءات الجزائية، والتي تتضمن تفتيش منزل المتهم أو غير المتهم، فعلى قاضي التحقيق عند مباشرة التفتيش في هذه الحالة أن يلتزم بالشروط الواردة في المادتين (45-47) من نفس القانون واللذان تناولتا أحكاما في مجال التفتيش، حيث يوجب على ضابط الشرطة القضائية أو قاضي التحقيق مراعات قواعد معينة وكما شملت المادتين على قواعد خاصة بكيفية التعامل مع الأوراق أو المستندات.²

ثالثا-السلطة المختصة بتفتيش النظم المعلوماتية: الأصل أن تقوم بإجراء تفتيش نظم الحاسب الآلي سلطة التحقيق الأصلية المتمثلة في قاضي التحقيق والنيابة العامة، إلا أنه يجوز لضباط الشرطة القضائية أن يقوموا بهذا الإجراء بناء على تفويض صادر من السلطة المختصة، وهذا ما سنبينه تبعا.

1_ إجراء تفتيش النظم المعلوماتية بمعرفة سلطة التحقيق الأصلية:

المشرع الإجرائي المصري أناط الاختصاص بالتفتيش كإجراء تحقيق للنيابة العامة كسلطة أصلية ولقاضي التحقيق في حالات خاصة³، وهذا عكس ما قضى به المشرع الجزائري حيث جعل سلطة تحقيق الأصلية من اختصاص قاضي التحقيق باعتباره مختص بإجراء كل التحقيقات بما فيها التفتيش، لكن في كل الحالات التي يقوم فيها بهذا الإجراء لابد من إخطار وكيل الجمهورية الذي له الحق في مرافقته⁴، واستثناء يجوز لوكيل الجمهورية أن يقوم ببعض إجراءات التحقيق، لأن الاختصاص الأصل بمباشرته يعود لقاضي التحقيق وحده دون سواه.⁵

التشريع الجزائري أكد بأن يكون قاضي التحقيق مختصا سواء من ناحية الاختصاص المكاني أو النوعي، فيحدد اختصاصه محليا إما بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في

¹ علي حسن محمد الطوالة، التفتيش الجنائي على نظم الحاسوب و الإنترنت، عالم الكتب الحديثة، الأردن، 2004، ص 7 .

² المواد 45، 47 من ق.إ.ج.ج.

³ هلالي عبد الله أحمد، مرجع سابق، ص 133 .

⁴ المواد 79 ، 82 من ق.إ.ج.ج.

⁵ المواد 56-1، 59-1، 117-1 من ق.إ.ج.ج.

ارتكابهم الجريمة أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان القبض قد حصل لسبب آخر، كما يجوز تمديد الاختصاص المحلي إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم وذلك في جرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية وغيرها، بالإضافة إلى ذلك يجب أن يتوافر الاختصاص النوعي المتمثل في نوع الجريمة التي يختص بها المحقق بالتفتيش، وبالنسبة للقانون الجزائري نجد أن قاضي التحقيق يختص بإجراء التحقيقات بما فيها التفتيش في الجنايات والجناح المتلبس بها¹.

2_ إجراء تفتيش النظم المعلوماتية بمعرفة ضباط الشرطة القضائية:

إن ضباط الشرطة القضائية المنتدب الذي يختص في الجريمة التقليدية هو نفسه الذي يختص في الجريمة المعلوماتية، ويتحقق إجراء التفتيش نظم المعلوماتية بمعرفة ضباط الشرطة القضائية²، في الحالات التالية هي:

أ_ التفتيش بناء على إذن قضائي بإجرائه: باعتبار أن قاضي التحقيق غير ملزم في كل الحالات بمباشرة التفتيش، فإنه يجوز له أن يندب أحد ضباط الشرطة القضائية للقيام بهذا الإجراء وهذا ما يسمى بالإنبابة القضائية، لذلك فلا يجوز لضباط الشرطة القضائية القيام بإجراء التفتيش إلا بعد حصوله على إذن من السلطة المختصة³.

وقد حدد المشرع الجزائري الاختصاص المكاني لضباط الشرطة القضائية ويكون ذلك إما بمكان وقوع الجريمة، أو بمكان إقامة المتهم، أو بمكان القبض عليه، وكما مدد اختصاصهم في حالة الاستعجال إلى كافة دائرة الاختصاص المجلس القضائي الملحقين به، ومدد أيضا بالنسبة لبعض الجرائم الخطيرة منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إلى كامل الإقليم الوطني⁴.

ب - التفتيش بناء على حالة التلبس بالجريمة: لا يختلف التفتيش في حالة التلبس في نظم الحاسب الآلي عن الجريمة التقليدية، لذلك يجوز لضباط الشرطة القضائية المنتدب في أحوال التلبس

¹ المادة 40 من ق.إ.ج.ج .

² طارق إبراهيم الدسوقي عطية، مرجع سابق، ص 428 .

³ راجع المادة 44 من ق.إ.ج.ج و المادة 40 من الدستور الجزائري .

⁴ راجع المادة 16 من ق.إ.ج.ج .

بالجنايات والجنح المعلوماتية تفتيش نظم الحاسب الآلي¹، هذا ما تضمنته نص المادة (44) من قانون الإجراءات الجزائية الجزائري.

ج - التفتيش بناء على موافقة المتهم: يجب أن تكون الموافقة من طرف صاحب الشأن بالتفتيش صريحة ومكتوبة بخط يده، فإذا كان لا يعرف الكتابة يذكر ذلك في المحضر ويذكر فيه هذه الموافقة؛ أما بخصوص جرائم الحاسب الآلي فإنه لا توجد نصوص قانونية مشابهة تخص تفتيش نظم المعلوماتية بناء على موافقة المتهم سواء في مصر أو في القانون المقارن، لذلك فإن هذا الفراغ يمكن تغطيته بالقواعد التقليدية².

الفرع الثاني: الشروط الشكلية لتفتيش الجرائم المعلوماتية.

إلى جانب الضوابط الموضوعية لتفتيش نظم الحاسب الآلي، هناك ضوابط أخرى ذات طابع شكلي يجب مراعاتها والأخذ بها أثناء القيام بالتفتيش، والتي تتمثل فيما يلي:

أولا- الأشخاص المطلوب حضورهم أثناء التفتيش: المشرع الجزائري من التشريعات الإجرائية التي أوجبت ضرورة حصول إجراء التفتيش المتعلق بالمساكن وملحقاتها بحضور المشتبه فيه عندما يتم تفتيش مسكنه من طرف الضبطية القضائية، وإن تعذر ذلك بإمتناعه عن حضور التفتيش أو كان هاربا يتم هذا الإجراء بحضور شاهدين من غير الموظفين الخاضعين لسلطة ضابط الشرطة القضائية القائم بالتفتيش، إلا أنه وبموجب التعديل الذي أحقه على قانون الإجراءات الجزائية بالقانون 22/06 إستثنى تطبيق هذه الشروط (حضور المشتبه فيه أو الشاهدين عندما يتعلق الأمر بالجرائم المعلوماتية)³.

ثانيا- تحديد ميعاد التفتيش المعلوماتي: يعتبر ميعاد التفتيش أحد أهم الضمانات الشكلية، بحيث لا يجوز إجراؤه خارج الأوقات المحددة قانونا ما عدا في الأحوال الاستثنائية المقررة قانونا، فلا يجوز البدء في التفتيش قبل الساعة الخامسة صباحا ولا بعد الساعة الثامنة مساء، إلا إذا طلب صاحب المنزل ذلك، أو وجهت نداءات من الداخل، أو في الحالات الاستثنائية التي أقرها القانون⁴، منها

¹ طارق إبراهيم الدسوقي عطية، مرجع سابق، ص 437 .

² هلاي عبد الله أحمد، مرجع سابق، ص 162 .

³ المادة 45 من قانون الإجراءات الجزائية.

⁴ المادة 47 من ق.إ.ج.ج.

الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والتي يجوز إجراء التفتيش فيها في كل ساعة من ساعات الليل والنهار بناء على إذن مسبق من وكيل الجمهورية المختص، ذلك لأن المكونات المعنوية للحاسب الآلي وشبكة الاتصال قد تكون عرضة لإخفاء أو تغيير أو تدمير أو تلاعب بالبيانات المخزنة والتي تعتبر أدلة إلكترونية لإظهار الحقيقة، مما قد يؤدي بالجاني في ظرف ثواني إلى إفساد هذه الأدلة وعرقلة عمل التحقيق، لذلك استوجب هذا الأمر على التشريعات الحديثة إضافة الجريمة المعلوماتية، كما حددته أيضا معاهدة بودابست في المواد 19 و 31 منها.

المطلب الثالث: التفتيش في البيئة الرقمية.

يتكون النظام المعلوماتي من مكونات مادية ومكونات منطقية، كما أن له شبكات إتصالات سلوكية ولا سلوكية على المستوى المحلي والدولي فهل تخضع هذه المكونات للتفتيش؟

الفرع الأول: تفتيش المكونات المادية للنظم المعلوماتية.

يكون التفتيش في هذه الحالة حسب المكان الذي تتواجد فيه الأشياء المراد تفتيشها، فإذا كانت أماكن خاصة مثل المساكن ولواحقها فإن التفتيش هنا يخضع للأحكام التي تطبق على تفتيش المساكن، والتي تم النص عليها في المادة 64 من ق إ ج ج، غير أن المادة 47 من نفس القانون والتي جاء بها القانون رقم 06/22 المعدل والمتمم لقانون الإجراءات الجزائية استثنت خضوع التفتيش للضمانات المنصوص عليها في المادة 64 سالف الذكر، إذ خولت لجهة التحقيق أو من أنابته القيام بالتفتيش في أي ساعة من ساعات الليل أو النهار وفي المحلات السكنية وغير السكنية بإذن من وكيل الجمهورية المختص في بعض الجرائم ومن بينها الجريمة المعلوماتية.¹

الفرع الثاني: تفتيش المكونات المعنوية للنظم المعلوماتية.

هناك اختلاف في جواز تفتيش المكونات المعنوية للتفتيش فهناك رأي يرى بجواز تفتيشها على غرار المشرع الكندي حين أجاز ضبط أي شيء بمعنى حتى لو كان غير مادي، لكن يشترط توفر الشروط الشكلية والموضوعية المذكورة آنفا، و هناك رأي يرى بعدم جواز تفتيش إلا ما هو مادي على اعتبار أن التفتيش يهدف للحصول على أدلة مادية.²

¹ نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات (دراسة مقارنة)، دار الفكر الجامعي، الإسكندرية، 2007، ص 237.

² على حسن الطويلة، مرجع سابق، ص 31.

الفرع الثالث: تفتيش شبكات المنظومة المعلوماتية:

يكون التفتيش هنا في أماكن مجهزة وبعيدة عن الموقع الفعلي للتفتيش، ونميز هنا بين حالتين: الحالة الأولى إذا كان حاسب المتهم متصلاً بنهاية طرفية داخل الإقليم الوطني فإن التفتيش لا يطرح أي إشكال إذ أجاز المشرع تمديد التفتيش لنظم المعلومات المتصلة بالحاسوب الذي يجري تفتيشه أي الشبكة وما يتصل بها، وتسجيل كل البيانات اللازمة كأدلة إثبات لإدانة المتهم أمام المحكمة، كما نصت على ذلك المادة 05 من القانون 04/09.

الحالة الثانية يطرح الإشكال في حالة اتصال جهاز المتهم بجهاز أو نهاية طرفية خارج الدولة، لأن تمديد التفتيش هنا يعتبر مساساً بسيادة الدولة، لذلك أجاز المشرع الجزائري تمديد التفتيش خارج إقليم الوطني لكن بمساعدة السلطات الأجنبية المختصة و طبقاً للمعاهدات الدولية المبرمة في هذا الشأن، وهذا ما يجعل التفتيش يخضع لمبدأ المعاملة بالمثل¹.

المحور الثاني: ضبط الأدلة في الجرائم المعلوماتية.

إن النتيجة الطبيعية التي ينتهي إليها التفتيش هي ضبط الأدلة التي يتم الحصول عليها أثناءه، فالضبط إذن هو غاية التفتيش القريبة والأثر المباشر الذي يسفر عنه الإجراء، والأساس القانوني للضبط هو العلاقة التي تربط بينه وبين الأشياء المتعلقة بالجريمة التي يشملها التحقيق والتي تفيد في كشف الحقيقة ما كان منها ضد المشتبه فيه أو ما كان في مصلحته.

المطلب الأول: تعريف ضبط الأدلة.

يقصد بالضبط في قانون الإجراءات وضع اليد على شيء مرتبط بجريمة تمت ويفيد في كشف الحقيقة عنها وعن مرتكبها، وهو من حيث طبيعته القانونية قد يكون من إجراءات الاستدلال أو التحقيق، فإذا كان الشيء في حيازة شخص واقتضى الأمر تجريدته من حيازته وقت ضبطه كان الضبط بمثابة إجراء تحقيق، أما إذا كان نزع الشيء قد تم دون الاعتداء على حيازة قائمة، فيكون الضبط بمثابة إجراء استدلال².

¹ نبيلة هبة هروال، مرجع سابق، ص 240 .

² خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط 1، 2011، ص 168 .

الشرط اللازم لصحة الضبط أن يكون الشيء مفيد في كشف الحقيقة فكل ما يحقق هذا الهدف يصبح ضبطه كما أن الضبط لا يرد إلا على الأشياء، أما الأشخاص فلا يصلحوا محلاً للضبط، وإنما المصطلح الأصح هو القبض والقبض يختلف تماماً عن ضبط الأشياء.¹

يترتب على هذا الارتباط بين التفتيش والضبط، أن الضبط لا يجوز أن يقع على شيء إلا بوصفه دليلاً من أدلة الجريمة التي يجري التفتيش بشأنها، ولذلك فإنه يباشر ضبط ما يتعلق بها من أدلة سواء كانت أنه ما دام التفتيش يستهدف ذات الحقيقة فيتعين أن يباشر ضبط ما يتعلق بها من أدلة سواء كانت للإدانة أم للبراءة، لأن ما يضبط الحالتين يحقق العدالة الجنائية، لذلك يقول فوستان هيلي: "إنه لما كان التفتيش يباشر للكشف عن الحقيقة، سواء كان في إدانة المتهم أو براءته فإنه ينبغي ألا يقتصر الضبط على الأشياء التي تؤدي إلى إدانة المتهم دون غيرها، بل أنه يتعين أن ينصب أيضاً على الأشياء التي تفيد الحقيقة أياً كانت أدت إلى تبرئة المتهم".²

لقد تعودت جهات التحقيق في الجرائم التقليدية أن يقع الضبط على الأشياء المادية فقط بوصفها أدلة مادية للجريمة التي يجري التفتيش بشأنها، لكن في مجال الجرائم المعلوماتية الطبيعية العلمية المعقدة للدليل الرقمي الذي يوجب التفتيش عنه وضبطه لإثبات هذا النوع من الجرائم ليس كالدليل التقليدي.

المطلب الثاني: مدى صلاحية ضبط أدلة الجرائم المعلوماتية.

ثمّة صعوبة لاعتبار مكونات الحاسب الآلي من الأشياء التي يمكن ضبطها وبالأخص ضبط الشبكة الإلكترونية والمكونات المعنوية للحاسب الآلي التي تشمل محتوى أنظمة المعالجة الآلية للمعطيات. في هذا الشأن تدخل المشرع الجزائري بموجب القانون 09 / 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال، أين إستحدثت المادة 06 التي تنص على أنه " عندما تكتشف السلطة التي تبأشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في

¹ عبد الله حسين على محمود، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات، ص 397 .

² مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة القاهرة، الطبعة الأولى، 2009، ص 209.

أحراز وفق القواعد المقررة في قانون الإجراءات الجزائية.."، وإلى جانب الشرع الجزائري نجد المشرع الفرنسي قام بإدخال تعديل على قانون الإجراءات الجزائية بموجب قانون الأمن الداخلي 2003 / 239 أين إستحدثت الفقرة الثالثة من المادة 57 التي تنص على المعطيات التي يتم بلوغها في ظل الشروط المنصوص عليها ويتعين نسخها على دعامات التخزين المعلوماتية ويتم تحريرها في أحراز محتومة وفق الشروط المنصوص عليها في هذا القانون¹.

الفرع الأول: ضبط المكونات المادية للحاسب الآلي: إن ضبط المكونات المادية للحاسب الآلي وملحقاته الذي يشمل على جهاز الحاسوب ومكوناته الأساسية والثانوية لا تثير أية صعوبة، لأن الضبط يرد على أشياء مادية كالدعامة المادية للبرامج والأسطوانات والأشرطة²، ومن المكونات المادية التي تكون محلا للضبط ما يلي: وحدة المعالجة المركزية، لوحة المفاتيح والشاشة والفأرة، والأقراص والأشرطة المغناطيسية التي يقوم البعض بتخزينها في البنوك أو في مراكز التوثيق الحكومية الأمنية، ولوحة الدوائر الإلكترونية، وأجهزة الاتصال عبر شبكة الانترنت كأجهزة المودم³. وباعتبار أنه لا خلاف حول ضبط مكونات الحاسب الآلي المادية ومواجهتها إجرائيا بالنصوص التقليدية، فإنه توجد بعض التشريعات تضمنت صراحة النص على تفتيش المكونات المادية، ومن هذه التشريعات قانون المنافسة الكندي والقانون الإنجليزي الصادر في عام 1990 والذي يطلق عليه قانون إساءة استخدام الحاسب⁴.

الفرع الثاني: ضبط المكونات المعنوية للحاسب الآلي: تكمن المشكلة في الأشياء المعنوية للحاسب الآلي التي تتضمن البرامج والبيانات، ويثور التساؤل إلى مدى صلاحيتها كمحل للضبط، حيث أن

¹ لقد كان هذا التعديل إستجابة لإتفاقية بودابست لعام 2001 التي نصت على ضبط الدليل الرقمي في الفقرة الثالثة من المادة 19 من القسم الرابع منها بإعتبارها أنه من سلطة كل دولة طرف أن تتخذ الإجراءات التالية: أن تضبط نظام الكمبيوتر أو جزء منه أو المعلومات المخزنة على أي وسيط من وسائط التخزين الخاصة بالكمبيوتر وأن تحافظ على سلامة تلك المعلومات المخزنة.

² عفيفي كامل عفيفي، جرائم الكمبيوتر، وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت - لبنان، 2007، ط 2، ص 373.

³ عبد الله حسين على محمود، مرجع سابق، ص، ص 398-399.

⁴ هلاي عبد الله أحمد، مرجع سابق، ص 199.

بعض الفقهاء يتجه إلى اعتبارها لا تصلح كمحل للضبط، وهذا ما ذهب إليه الفقه الألماني و اللوكسمبرجي، أما البعض الآخر من الفقهاء يرون إمكانية تطوير النصوص التقليدية للضبط على البرامج والبيانات المخزنة، لكون الغاية من التفتيش تتحقق بضبط الأدلة المادية التي تفيد في كشف الحقيقة، ومن هذا الاتجاه الفقه الكندي الذي يرى أن غرض الضبط لم يقتصر بضبط الأشياء المادية المحسوسة، بل تطور إلى أغراض أخرى منها الحصول على المعلومات والبيانات وضبطها للوصول إلى الأدلة، اذا فالإشكال يقع على الأدلة المعنوية (برامج الحاسب الآلي و بياناته).

أولاً- برامج الحاسب الآلي: إن الأمر يتعلق بكيفية ضبط الأدلة في حالة استخدام الوسائل الفنية في نسخ أو إتلاف البرنامج كالفيروسات مثل حصان طروادة، مع قلة خبرة وتدريب الضبطية القضائية وسلطة التحقيق في جمع الأدلة في مجال الفني والتقني وهذا من الناحية الأولى، ومن الناحية الثانية تتمثل في قيام عملية ضبط الوسائل التقنية بواسطة الأنظمة والشبكات المعلوماتية الكبيرة، حيث يؤدي الضبط إلى عزل النظام المعلوماتي بالكامل عن دائرته لفترة زمنية يمكن أن تطول أو تقصر والذي يسبب خسائر وأضرار بالجهة مستخدمة النظام، وكذلك ينتج عن ذلك عدم مبادرة مستخدمي النظام المعلوماتي استعدادهم للتعاون ومساعدة سلطة التحقيق لما يمثله الضبط لهم من الاعتداء على حقوق الآخر.¹

ثانياً- بيانات الحاسب الآلي: لقد نظم المشرع الجزائري القواعد الخاصة بضبط البيانات المعلوماتية وفقا للقانون رقم 04/09 تحت تسمية "حجر المعطيات المعلوماتية"، حيث قضت المادة (06) من نفس القانون على نسخ المعطيات محل البحث، وكذلك المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية التي تكتشفها السلطات المختصة عند القيام بالتفتيش في المنظومة المعلوماتية، وتكون هذه المعطيات تفيد إظهار الحقيقة وقابلة للحجز، وتوضع في الأحراز مع وجوب قيام السلطة المختصة بحماية سلامة المعطيات المخزنة في المنظومة المعلوماتية، كما يجوز استخدام الوسائل التقنية وفقا لما يستهدفه التحقيق لتشكيل أو إعادة تشكيل هذه المعطيات بشرط عدم المساس بمحتوى المعطيات، أما المادة (07) من نفس القانون نصت على أنه حالة استحالة إجراء الحجز وفقا لما نصت عليه المادة (06) ، أما المادة (08) تعلقت بالمعطيات التي يشكل محتواها جريمة، فعلى السلطة المباشرة بالتفتيش أن تصدر أمر بتكليف أي شخص مؤهل فنيا وتقنيا لاستخدام الوسائل

¹ عفيفي كامل عفيفي، مرجع سابق، ص 374 .

التقنية المناسبة من أجل منع الإطلاع على محتوى هذه المعطيات، أما المادة (09) من نفس القانون، فيتضح من خلالها أن المعلومات المتحصل عليها عن طريق المراقبة وفقا لهذا القانون، لا يجوز استخدامها إلا في الحدود الضرورية التي يقتضيها التحري أو التحقيق القضائي، وذلك تحت طائلة العقوبات التي نص عليها التشريع المعمول به.¹

الفرع الثالث: ضبط الرسائل ومراقبة الاتصالات الإلكترونية: لقد عمدت الدول إلى حماية هذه الأسرار الشخصية عن طريق إرساء نصوص دستورية تضمن عدم الاعتداء على خصوصية المراسلات، ومن بينها الدستور الجزائري الذي تضمن منع الإطلاع على المراسلات سواء كانت بريدية أو برقية أو هاتفية وذلك في نص المادة (39) من الدستور الجزائري التي تنص على أنه: "سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة"²، و من بين هذه مراسلات:

أولا- البريد الإلكتروني: يقصد بالبريد الإلكتروني استخدام شبكات الانترنت من أجل نقل الرسائل بدلا من الطرق التقليدية، وباعتبار أن استعماله سهل أضحى من أكثر وسائل الانترنت استعمالا في الوقت الحالي، وأهم مسائل تتعلق بالبريد الإلكتروني هو وجوب المحافظة على سرية، وهو ما أدى إلى وضع برامج تشفير خاصة به، ولقد ساعد ذلك على ظهور التوقيع الإلكتروني في تيسير عملية التراسل عبر البريد الإلكتروني، و ضبط البريد الإلكتروني الذي يحتوي على برامج متخصصة لكتابة وإرسال واستعراض وتخزين الرسائل الإلكترونية، و هذه الرسائل لا يختلف التعامل معها عن التعامل مع الرسالة الورقية، إذ بمقدور المستخدم أن يطرحها جانبا أو يرد عليها أو ينقلها إلى شخص آخر أو يحفظها في ملف خاص.³

وبالرجوع إلى النصوص القانونية يلاحظ بأن القانون الجزائري استحدث مصطلحات تقنية جديدة في نصوص قانونية جديدة تتلاءم مع ضبط الرسائل الإلكترونية في العديد من الجرائم في حالة التلبس أو التحقيق الابتدائي، ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وهذه النصوص

¹ المواد 6-9 من القانون رقم (09-04) المؤرخ في 05-08-2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ومكافحتها.

² المادة 39 من الدستور الجزائري.

³ عفيفي كامل عفيفي، المرجع السابق، 355 .

خصت عن النصوص التقليدية بجوانب تقنية تجيز بمقتضاها لقاضي التحقيق أو ضابط الشرطة القضائية المناب له باعتراض المراسلات وتسجيل الأصوات والتقاط الصور¹.

ثانياً_ التنصت والمراقبة الإلكترونية لشبكات الحاسب الآلي:

يقصد بمراقبة المحادثات وتسجيلها والتنصت عليها بأنها إجراء من إجراءات التحقيق، تباشرها السلطة المختصة للبحث عن أدلة إثبات الجريمة ضد شخص نسبت إليه ارتكابها أو لديه أدلة تتعلق بها، وكانت هذه الجريمة على درجة من الخطورة لاتخاذ مثل هذا الإجراء الاستثنائي، وبالرغم من الجدل المثار حولها إلا أنها مسموح بها تحت ظروف معينة في جميع الدول تقريباً، فالقانون الفرنسي الصادر في 1991/07/10 يجيز اعتراض الاتصالات البعيدة، و في الولايات المتحدة الأمريكية يجوز اعتراض الاتصالات الإلكترونية بما فيها شبكات الحاسوب بشرط الحصول على إذن بالتفتيش من القاضي و في هولندا أجاز المشرع للقاضي التحقيق ان يأمر بالتنصت على شبكات الاتصالات إذا كانت هناك جرائم خطيرة²، وهو ما أخذ به المشرع الجزائري في المواد 65 مكرر 5 و مكرر 10 كما تم النص عليها سابقاً.

المطلب الثالث: أساليب حجز المعطيات المعلوماتية.

لقد اعتمد المشرع في حجز المعطيات المجرمة على أسلوبين متماثلين في نسخ المعطيات أو حجبتها (تجميدها):

الفرع الأول: نسخ المعطيات الرقمية.

إن المعطيات الرقمية المعلوماتية المجمعة يمكن نسخها على "جميع دعائم التخزين" هذا الذي يناسب تسمية الحجز المعلوماتي الذي هو غير متعارض مع الضبط المادي التقليدي لدعائم التخزين المعلوماتية المستخرجة من نفس مكان التفتيش، أي بدل حجز القطع الصلبة التي تتضمن المواد الممنوعة، فيتم مثلاً نسخ المواد التي تحتاج إلى فك شفرتها لكي يتم التعرف على محتوياتها، أو نسخ البيانات التي يتم وضعها في إطار برمجية تحوي قنبلة زمنية موقوتة، وهنا نجد أسلوب النسخ يصلح

¹ المواد من 65 مكرر 5 - 65 مكرر 10 من الباب الثاني من الكتاب الأول في الفصل الرابع تحت عنوان "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من القانون 06-22 المؤرخ في 20 ديسمبر 2006، يتضمن قانون الإجراءات الجزائية الجزائري المعدل والمتمم.

² عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الاثبات الجنائي، دار الجامعة الجديدة، مصر، 2010، ص164.

تماماً أن ينتج عنه دليل رقمي مقبول أمام القضاء¹، وهذا ما قضت به المادة 06 من قانون 04/09 بنصها "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث... على دعامة تخزين إلكترونية تكون قابلة للحجز..." أما الفقرة الثالثة من نفس المادة فقد أجاز المشرع استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل المعطيات المبحوث عنها من أجل جعلها قابلة للاستغلال لأغراض التحقيق شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

الفرع الثاني: الحجز عن طريق منع الوصول إلى المعطيات.

تناولت المادة 07 من قانون 04/09 الاستحالة التقنية لإجراء الحجز بنسخ المعطيات الرقمية محل البحث وكذا المعطيات اللازمة لفهما على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحرار، فأوجب المشرع على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة ل:

- منع الوصول إلى المعطيات التي تحويها المنظومة المعلوماتية. - منع نسخ تلك المعطيات.²

الخلاصة:

من خلال ما قدمناه في عرضنا هذا يتضح أن الجرائم المعلوماتية كانت ومازالت محلاً للخلاف الفقهي والقضائي، بالنظر إلى قيمة المعلومات وطبيعتها غير المادية، وكذلك من حيث إجراءات التحقيق من التفتيش والضبط التي قد تكون حتى عن بعد وغيرها من الإجراءات المتبعة، و نرى ان اجراء التفتيش و ضبط الأدلة يلعب دورا هاما في هذا النوع من الجرائم المستحدثة نظرا للتطور التكنولوجي الحاصل، للوصول الى الأدلة الالكترونية التي تثبت الجريمة وتدين المتهم، و تظهر هذه الالهية من خلال النص عليها في المعاهدات الدولية منها معاهدة بودابست و كذا تكريسها من قبل المشرع الجزائري في الدستور و في قانون الإجراءات الجزائية.

¹ فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، دار الفكر والقانون، مصر، طبعة 2010، ص 636.

² المادة 7 من القانون 04-09.

أما بخصوص التشريع الجزائري، فإن الإثبات الجنائي في مجال الجرائم المعلوماتية لا يزال قاصرا، بحيث لم يتضمن الاستثناء الخاص بوقت التفتيش والأشخاص المطلوب حضورهم ضمن القانون 04/09 لسنة 2009.

من خلال هذا البحث نخلص الى بعض التوصيات:

— على المشرع الجزائري تضمين الاستثناء الخاص بوقت التفتيش والأشخاص المطلوب حضورهم في القانون 04/09

— ان يتم التكوين الجيد للقائمين بعملية التفتيش في المجال المعلوماتي باعتباره مجالا جديدا على الساحة الجزائرية.

— تكوين الخبرات للقضاة وضباط الشرطة القضائية في هذا المجال.

قائمة المراجع:

القوانين.

— الدستور الجزائري.

— قانون الإجراءات الجزائية المعدل و المتمم.

الكتب.

1_ بلعليات إبراهيم، أركان الجريمة و طرق إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الجزائر، ط1، 2006.

2_ خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط1، 2011 .

3_ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي الإسكندرية، الطبعة الأولى، 2009.

4_ طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتي، د. ط، دار الجامعة

الجديدة، الإسكندرية، د.س.ن.

5_ عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الاثبات الجنائي، دار الجامعة الجديدة، مصر، 2010 .

- 6_ عبد الله حسين على محمود، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات.
- 7_ عفيفي كامل عفيفي، جرائم الكمبيوتر، وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، ط2 ، منشورات الحلبي الحقوقية، بيروت - لبنان، 2007.
- 8_ علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب و الإنترنت، عالم الكتب الحديثة، الأردن، 2004 .
- 9_ فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، دار الفكر والقانون، مصر، طبعة 2010 .
- 10_ مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة القاهرة، الطبعة الأولى، 2009.
- 11_ نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات (دراسة مقارنة)، دار الفكر الجامعي، الإسكندرية، 2007 .
- 12_ هلاي عبد الله أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة، طبعة الأولى، دار النهضة العربية، القاهرة، 1997 .

الجرائم الماسة بنظام المعالجة الآلية للمعطيات وأطر مكافحتها في قانون العقوبات الجزائري

د/ قسمية محمد

كلية الحقوق والعلوم السياسية

جامعة المسيلة

مقدمة:

لما أخذت الجرائم على عاتقها تعزيز دولة القانون، التي تعد الشرط الضروري لكل تقدم، ولما كان إصلاح العدالة يقع في قلب وطلبة كل مشروع للتجديد الوطني على أن تمنح أولوية تنفيذه في إطار عمل السلطات القانونية، تم التفكير في القيام بتكييف التشريع الوطني مع الحقائق المترتبة عن التحولات الاجتماعية و الاقتصادية التي تشهدها الجزائر و مع التزاماتها الدولية، وقد اعتبر أن ترجمة الأحكام الملائمة لمختلف الاتفاقيات الدولية المرتبطة بها الجزائر في المجال الجزائي يتم التكفل بها بشكل منتظم ضمن القانون الوطني (الداخلي).

وفي هذا الإطار تم الإشارة إلى التكفل بأشكال جديدة للإجرام، والتي تم التأكيد على أنها مستحدثة بموجب تعديل قانون الإجراءات الجزائية سنة 2006 الذي تضمن إجراءات خاصة بتلك الجرائم على سبيل الحصر، وضمن هذا المسعى يمكن التطرق إلى جريمة المساس بأنظمة المعالجة الآلية للمعطيات، إذ أن المشرع الجزائري كغيره من التشريعات نظر إلى جريمة المساس بأنظمة المعالجة الآلية للمعطيات كجريمة من الجرائم السيبرانية، وعلى الرغم من صعوبة مكافحتها ميدانيا لخصوصيتها إلا أن المشرع استحدث نصوص لتوفير الحماية الجزائية للمعطيات المعلوماتية (معطيات الحاسب الآلي) وكان ذلك بموجب القانون 04-15 المؤرخ في 10-11-2004 الذي تم الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر 66-156 المتضمن قانون العقوبات بقسم سابع مكرر تحت عنوان "المساس بأنظمة المعالجة المعطيات" والذي استحدث ثمانية مواد من المادة 394 مكرر إلى 394 مكرر7، وكانت هذه الالتفاتة من المشرع الجزائري بسبب تطور المعاملات

الالكترونية، وبالتالي أصبح المجال الكتروني مسرحا لبعض الجرائم، منها جريمة المساس بأنظمة المعالجة الآلية للمعطيات.

لذا يثار التساؤل حول: ما المقصود بنظام المعالجة الآلية للمعطيات؟ هل جريمة المساس بأنظمة المعالجة للمعطيات متعددة الصور أم لا، أم لها صورة واحدة فقط؟ وإذا كانت لها عدة صور هل هناك أحكام مشتركة بين تلك الصور؟.

للإجابة على هذه التساؤلات يمكن الاعتماد على المحورين الآتيين كمايلي:

المحور الأول: مفهوم نظام المعالجة الآلية للمعطيات وصوره:

المشرع الجزائري لم يضع تعريفا لنظام المعالجة الآلية للمعطيات وهذا ما يدفعنا إلى البحث عن ذلك في الفقه.

أولا: تعريف نظام المعالجة الآلية للمعطيات

قدمت الاتفاقية الدولية الأوروبية للإجرام المعلوماتي تعريفا للنظام المعلوماتي في مادتها الأولى على النحو التالي: "يقصد بمنظومة الكمبيوتر أي جهاز أو مجموعة من الأجهزة المتصلة ببعضها البعض أو ذات صلة بذلك , و يقوم إحداها أو أكثر من واحد منها تبعا للبرنامج بعمل معالجة آلية للبيانات".

و في هذا الشأن، يقصد ببيانات الكمبيوتر "أي عملية عرض للوقائع أو المعلومات أو المفاهيم بشكل مناسب لعملية المعالجة داخل منظومة الكمبيوتر بما في ذلك البرنامج المناسب لجعل منظومة الكمبيوتر تؤدي وظائفها".

هذا التعريف هو نفسه الذي تبناه المشرع الجزائري في القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في المادة الثالثة منه في الفقرة ب منها التي عرفت المنظومة المعلوماتية بأنها: " أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين ". و يؤخذ على هذا التعريف أنه خاص بالنظام المعلوماتي بينما فكرة المعالجة الآلية أوسع من فكرة المعالجة المعلوماتية.

و من خلال هذا التعريف يستخلص أن نظام المعالجة الآلية للمعطيات يقوم على عنصرين:
- مركب يتكون من عناصر مادية ومعنوية مختلفة مرتبطة نتيجة علاقات توحيدها نحو تحقيق هدف محدد.

- خضوع النظام للحماية.

وبالرجوع إلى التشريع الجزائري نجد أن النصوص المتعلقة بجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات جاءت خالية من شرط الحماية، وهذا ما يعني توجه إرادة المشرع إلى استبعاد هذا الشرط لتشمل الحماية الجنائية كل الأنظمة سواء كانت تتمتع بحماية فنية أم لا(1).

ثانيا: صور الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

سعى المشرع الجزائري من خلال تعديل قانون العقوبات لعام 2004 إلى حماية المصالح المتعلقة بمعطيات الحاسب الآلي، وهو ما يتم التطرق إليه فيما يلي:

1- جريمة الدخول أو البقاء غير المصرح بهما بصورتها البسيطة: جرم المشرع الجزائري ذلك في المادة 394 مكرر من قانون العقوبات في فقرتها الأولى من قانون العقوبات، ولعل جريمة الدخول أو البقاء غير المصرح بهما في أنظمة المعالجة الآلية للمعطيات هي من أهم جرائم المعطيات والجرائم المعلوماتية عموما، ذلك أن أغلب جرائم المعطيات لا يمكن ارتكابها إلا بعد الدخول للنظام، لهذا كانت جريمة الدخول هي الباب والحد الفاصل بين الجاني وبين ارتكابه لمختلف جرائم المعطيات الأخرى، لذا حرص المشرع على تجريم كل تواجد غير مشروع داخل أنظمة المعالجة الآلية للمعطيات فجرم الدخول غير المصرح به وكذا البقاء بغير تصريح سواء تم ذلك في كل النظام أو جزء منه، كما تتحقق الجريمة سواء أدى هذا التواجد أو لم يؤدي إلى نتائج معينة.

ويتمثل السلوك الإجرامي في جريمة الدخول والبقاء غير المصرح بهما في نشاط إجرامي إما في فعل الدخول إلى نظام المعالجة الآلية للمعطيات أو في جزء منه، وإما في فعل البقاء في هذا النظام أو في جزء منه، ولقد سبق بيان مفهوم نظام المعالجة الآلية للمعطيات، لذا يمكن التطرق فقط لمفهوم الدخول و البقاء.

ويقصد بالدخول هنا هو الولوج إلى المعلومات والمعطيات المخزنة داخل النظام و هو إذا ذو طبيعة معنوية وليست مادية، ولم يحدد المشرع الجزائري الوسيلة المتبعة في الدخول إلى النظام لذلك تقع الجريمة أيا كانت الوسيلة المستعملة في ذلك، و يستوي أن يتم الدخول مباشرة أم بطريقة غير مباشرة كما هو الحال في الدخول عن بعد عن طريق شبكات الاتصال سواء كانت محلية أو عالمية.

وينصرف معنى الدخول في إطار المعلوماتية ليشمل كافة الأفعال التي تسمح بالولوج إلى نظام معلوماتي، ويتحقق الدخول غير المصرح به إلى جهاز الكمبيوتر بالوصول إلى المعلومات والبيانات المخزونة داخل نظام الكمبيوتر دون رضا المسؤول عن النظام أو المعلومات الذي يحتوي عليها. فقد يتم الدخول باستعمال أجهزة خاصة تمكنه من كسر شفرة قاعدة المعطيات أو أن يستخدم الشفرة الصحيحة الخاصة بشخص آخر مأذون له بالدخول، وقد يتم ذلك عن طريق استخدام تقنية "أبواب المصيدة" حيث يقوم واضعو البرامج بترك فواصل في البرامج أثناء إعدادها تسمى أبواب المصيدة تستخدم في إضافة ما يحلو لهم من أوجه التلاعب ويتم ذلك أثناء قيامها بالمعالجة النهائية على اعتبار أن هذا الشيء عادي إذ يمكن لمهندسي الحاسب أن يقوموا باكتشاف هذه الفواصل من أجزاء داخلية للصيانة.

و يستوي أن يتم الدخول إلى قواعد البيانات كلها أو إلى جزء فقط من نظام التشغيل، وتحقق الصورة الأخيرة إذا تمكن الجاني من كسر شفرة بعض قواعد البيانات أو مواقع المعلومات دون أن يتمكن من اختراق كل مواقع النظام.

و لا عبرة في هذه الجريمة بصفة مرتكب الفعل الإجرامي فقد يكون مسؤولاً عن العمال والصيانة وقد يكون شخصاً منبث الصلة عن النظام الداخل فيه وتوصل إلى الدخول عن طريق حاسب آلي آخر موجود في مكان آخر بواسطة الدخول إلى شبكة المعلومات، وقد عبرت عنه المادة 394 مكرر من قانون العقوبات بقولها "كل من يدخل أو يبقى".

و بذلك يكفي أن يكون الجاني من الأشخاص الذين ليس لهم الحق في الدخول إلى النظام أو كان دخوله مخالفاً لشروط الدخول التي نص عليها القانون أو الاتفاق أو مخالفاً لإرادة من له حق السيطرة على النظام، كما هو الحال إذا كان القانون يفرض سرية معينة بالنسبة لبعض الأنظمة مثل أسرار الدولة أو السرية المتعلقة بالمعلومات الذاتية أو الاسمية أو سرية المهنة كما يكون الدخول غير مشروع إذا كان من له الحق السيطرة على النظام قد وضع بعض القيود للدخول إليه و لم يحترم الجاني تلك القيود، أو إذا كان يتطلب ضرورة دفع مبلغ من النقود و تم الدخول دون دفع ذلك المبلغ (2). و على ذلك لا تتوفر الجريمة إذا تم الدخول إلى عنصر لا علاقة له بنظام المعالجة الآلية للمعطيات كالدخول إلى برنامج منعزل عن غيره من العناصر، أو أن يقتصر الشخص على مجرد قراءة الشاشة. كما يقصد بالبقاء، التواجد داخل ذلك النظام ضد إرادة من له الحق في السيطرة على النظام، وقد يتحقق فعل البقاء مستقلاً عن فعل الدخول عندما يكون الدخول مرخصاً به وفقاً لشروط معينة،

خاصة ما تعلق منها بالوقت المرخص به أي مدة الدخول، فإذا استهلك الشخص ثم زاد عليه فهنا يتحقق فعل البقاء بطريق غير مشروع وكذلك في حالة الدخول إلى نظام المعالجة الآلية عن طريق الصدفة أو الخطأ وهنا يجب على الشخص أن يقطع وجوده داخل النظام فوراً، فإذا بقي فيه فإنه يعد مرتكباً لفعل البقاء بطرق غير مشروع في النظام.

كما يتحقق هذا الفعل مستقلاً عن فعل الدخول إذا ما سمح للشخص الإطلاع على معلومة دون السماح له بطبعتها، فإن قام بذلك فإنه يكون مرتكباً لفعل البقاء بطريق الغش، هذا ويمكن أن يتحقق فعل البقاء وفعل الدخول معاً إذا لم يرخص للشخص الدخول إلى نظام المعالجة الآلية للمعطيات.

وقد يكون البقاء غير المشروع حقاً لاحقاً على دخول قد تم بوجه مشروع، ويتحقق ذلك بتجاوز شخص النطاق الزمني أو الغرض المصرح له في الاتصال بنظام المعلومات.

فجريمة البقاء عن طريق الغش داخل نظام المعالجة الآلية للمعطيات يشكل عادة التابع المنطقي لجريمة الدخول غير الشرعي للنظام، لكن الجريمتين قد تتفرقا بحيث تظهر فقط جريمة البقاء داخل النظام عن طريق الغش، إذا كان الشخص قد دخل النظام بطريقة شرعية.

وبالرجوع إلى نص المادة 394 مكرر من قانون العقوبات نجد أنه يكفي لقيام جرمي الدخول والبقاء غير المصرح بهما مجرد الدخول أو البقاء داخل نظام المعالجة الآلية للمعطيات ولا يتطلبان حدوث نتيجة معينة كالوصول إلى معطيات أو التلاعب بها.

أما عن طبيعة هذه الجريمة فإنه على الرغم من أن الاتجاه الغالب في الفقه يعتبر جرمي الدخول أو البقاء ذات سلوك مجرد إلا أنهم لم يتفقوا على كون هذه الجريمة مستمرة أو وقتية أم متتابعة الأفعال. فذهب رأي إلى اعتبار كل من جريمة الدخول و جريمة البقاء مستمرة، بينما ذهب رأي آخر إلى اعتبارها متتابعة الأفعال، كما ذهب رأي ثالث إلى أن جريمة الدخول جريمة وقتية ذات أثر ممتد بينما جريمة البقاء مستمرة (3).

ومالاً شك أن القصد الجنائي المطلوب في هذه الجريمة هو القصد العام، فطالما توافر عنصر علم الجاني بأن فعله يدخل في تكوين جريمة الدخول أو البقاء في نظام للمعالجة الآلية للمعطيات الخاصة بالغير دون أن يكون له الحق في ذلك، وطالما توافر عنصر الإرادة الحرة بأن كان دخول الجاني لنظام المعالجة الآلية للمعطيات بإرادته وليس بمحض الصدفة البحتة فإن أركان الجريمة متوفرة.

ومن ثم لا يتوافر القصد الجنائي إذا كان الدخول أو البقاء قد تم عن طريق الخطأ، وتطبيقا لذلك ينتفي القصد الجنائي إذا ثبت أن الجاني قد دخل على قواعد المعطيات مصادفة وأنه كان وليد الخطأ، و لم يكن فعله كاشفا عن توافر هذا القصد. ومن الأمثلة أيضا إذا كان الدخول على النظام يتم بموجب اشتراك وكان قد سبق للشخص الدخول بوجه مشروع، غير أنه قد انتهت مدة اشتراكه وكان يجهل ذلك، ومن القرائن الدالة على توافر القصد هي استخدام وسائل خداعية في تحقيق الدخول أو البقاء في النظام، إذا كان الدخول على النظام يتطلب شفرة أو بطاقة معينة فقام الجاني بسرقة هذه البطاقة أو بكسر هذه الشفرة، فإذا توافر القصد الجنائي بعنصره العلم و الإرادة بالمعنى السابق فإنه لا عبرة بالبواعث على الدخول أو البقاء، فيظل القصد الجنائي قائما حتى لو كان الباعث هو الفضول أو حب الاستطلاع أو إثبات القدرة على التغلب على قيود النظام أو أن يكون الغرض هو الاستفادة من المعلومات والبيانات التي تحتويها النظام.

أما عن القصد الخاص فلا يبدو من خلال نص المادة 394 مكرر من قانون العقوبات أن المشرع الجزائري يتطلب وجود نية خاصة لدى الجاني حتى تقوم جريمة الدخول أو البقاء غير المصرح بهما، ذلك أن القصد الخاص هو علم وإرادة ينصرفان إلى وقائع خارجة عن أركان الجريمة أي إلى وقائع لا تدخل ضمن عناصرها، وأن لفظ الغش و إن حمل معنى الاحتيال فهو لا يدل إلا على معنى واحد هو أن الجريمة عمدية لا أكثر (4).

وبخصوص العقوبات المترتبة عن صورة الدخول أو البقاء غير المصرح بهم نصت الفقرة الأولى من المادة 394 مكرر على عقوبة أصلية تتمثل في الحبس من 3 أشهر إلى سنة والغرامة من خمسين ألف (50.000) إلى مئة ألف (100.000) دينار جزائري، هذا بالنسبة للشخص الطبيعي، أما بالنسبة للشخص المعنوي فإن العقوبة المقررة بموجب المادة 394 مكرر 4 من قانون العقوبات الجزائري فهي الغرامة المضاعفة 5 مرات على ما هو مقرر للشخص الطبيعي، وعليه تكون الغرامة المقررة على الشخص المعنوي بالنسبة لهذه الجريمة تتراوح بين مائتان وخمسون ألف (250.000) و(500.000) خمسمائة ألف دينار جزائري.

2- الصورة المشددة (الحذف أو التغيير أو التخريب كنتيجة للدخول أو البقاء غير المصرح بهما):

لقد سعى المشرع الجزائري إلى حماية المعطيات وإتاحتها في الصورة المشددة لجريمة الدخول أو البقاء غير المصرح بهما من خلال الفقرتين الثانية والثالثة من المادة 394 مكرر من قانون العقوبات. فبالرجوع إلى نص المادة السابقة نجد أن المشرع و إن كان لا يتطلب نتيجة معينة لقيام جريمة الدخول أو البقاء غير المصرح بهما إلا أنه قد ضاعف العقوبة إذا أدى ذلك إلى نتائج معينة تتمثل في محو أو تعديل المعطيات التي يحتويها النظام كما شدد العقوبة إذا أدت الجريمة السابقة إلى تخريب نظام تشغيل المنظومة وجعله غير صالح لأداء وظائفه.

وبكفي لتوافر هذا الظرف المشدد وجود علاقة سببية بين الدخول أو البقاء غير المصرح بهما وبين النتيجة الضارة سواء محو أو تعديل المعطيات التي يحتويها النظام، أما عدم صلاحية النظام للقيام بوظائفه فإنه يعني عدم قدرته على تنفيذ المعالجة الآلية للمعطيات بأن يصبح غير قابل للاستخدام، ومثال ذلك محو بعض أوامر التشغيل الذي يترتب عليه تعطيل النظام.

كما أنه بالرجوع إلى نص المادة 394 من قانون العقوبات في فقرتيها الثانية والثالثة نجد أن النتيجة المشددة التي يتطلبها المشرع الجزائري لا يشترط أن تكون مقصودة، فيكفي أن تكون على سبيل الخطأ غير العمدية الذي يأخذ صورة الإهمال أو عدم الاحتراز أو الرعونة.

فالظرف المشدد هنا ظرف مادي يكفي أن توجد بينه وبين الجريمة العمدية الأساسية وهي جريمة الدخول أو البقاء غير المصرح بهما علاقة سببية للقول بتوافره، إلا إذا أثبت الجاني انتفاء تلك العلاقة كأن يثبت أن تعديل أو محو المعطيات أو عدم صلاحية النظام للقيام بوظائفه يرجع إلى القوة القاهرة أو الحادث المفاجئ.

وبالنسبة لفعلي التعديل والإزالة فلا يمكن تطبيق الظرف المشدد إلا إذا قصد الجاني النتيجة المشددة لأن ذلك يقع مباشرة تحت طائلة المادة 394 مكرر 1 من قانون العقوبات المتعلقة بجريمة التلاعب بالمعطيات، أما بالنسبة لتخريب نظام المعالجة الآلية للمعطيات فهو يتعلق بنتيجة لا تقع إلا عمدية على الإطلاق في القانون الجزائري.

وبخصوص العقوبات شددت الفقرة الثانية والثالثة من المادة 394 مكرر من قانون العقوبات من عقوبة جريمة الدخول أو البقاء غير المصرح بهما إذا نجم عن هذا الدخول أو البقاء تخريب لنظام تشغيل نظام المعالجة الآلية للمعطيات أو حذف أو تغير المعطيات، ففي هذه الحالة الأخيرة ترفع

العقوبة إلى ضعف تلك المقررة للجريمة في صورتها البسيطة فتصبح الحبس من ستة (6) أشهر إلى سنتين و الغرامة من مئة ألف (100.000) إلى أربعمئة ألف (400.000) دينار جزائري. أما في حالة ما إذا أدت الجريمة إلى تخريب النظام إشغال المنظومة فإن العقوبة تكون الحبس من ستة (6) أشهر إلى سنتين والغرامة من خمسين ألف (50.000) إلى ثلاثمئة ألف (300.000) دينار جزائري، هذا بالنسبة للشخص الطبيعي، أما عن الشخص المعنوي فتشدد العقوبة إلى خمسة أضعاف ما هو مقرر للشخص الطبيعي فتتراوح في قانون العقوبات الجزائري ما بين مئتان وخمسون ألف (250.000) دينار جزائري وسبع مئة وخمسون ألف (750.000) دينار جزائري (5).

3- الجرائم الماسة بسلامة المعالجة الآلية للمعطيات (الإدخال، التعديل، الإزالة عن طريق الغش)

لقد قام المشرع الجزائري بتأمين الحماية اللازمة لضمان سلامة معطيات الحاسب الآلي من خلال تجريمه لبعض الأفعال التي تشكل تلاعبا بتلك المعطيات، و قد وردت بنص المادة 394 مكرر 1 من قانون العقوبات و تتمثل في الإدخال، التعديل، الإزالة عن طريق الغش.

و لا يشترط اجتماع تلك الصور، بل يكفي أن يصدر من الجاني إحداها فقط لكي يتوفر الركن المادي، سواء كان ذلك بإضافة معطيات جديدة أو محوها أو تعديل معطيات موجودة من قبل.

وهذا يعني أن النشاط الإجرامي في هذه الجريمة إنما يرد على محل أو موضوع محدد هو المعطيات التي تمت معالجتها آليا والمتواجدة داخل نظام أو تشكل جزءا منه، بمعنى أن الجريمة لا تقوم بالنسبة للمعلومات التي لم يتم إدخالها إليه أو تلك التي دخلت و لم تتخذ حيالها إجراءات المعالجة الآلية، كما لا تقوم الجريمة بالنسبة للمعطيات الموجودة خارج النظام كأن تكون مفرغة على قرص أو شريط ممغنط خارج النظام.

و فيما يلي بيان الأفعال التي تعد تلاعبا في المعطيات:

فالإدخال، يقصد به إضافة معطيات جديدة على الدعامات الخاصة بها سواء كانت خيالية أم كان يوجد عليها معطيات من قبل، ويتحقق هذا الفعل في القرض الذي يستخدم فيه الحامل الشرعي لبطاقات السحب الممغنطة التي يسحب بمقتضاها النقود من أجهزة السحب الآلي وذلك عندما يستخدم رقمه الخاص والسري للدخول لكي يسحب مبلغا من النقود أكثر من المبلغ الموجود في حسابه، كما يتحقق فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب كفيروس مثلا لإضافة معطيات جديدة.

أما التعديل، يتحقق بكل نشاط من شأنه أن يحقق غاية الجاني من ذلك، فإذا كانت غاية الجاني من التعديل أن يحصل مثلاً على مستند أو محرر يخالف المحرر الأصلي المحفوظ في ذاكرة الحاسب الآلي فإن ذلك من الممكن أن يتحقق إما بحذف معطيات فقط أو بإضافة معطيات أو بالفعلين معاً، فالتعديل إذا لا يكون إلا بوسائل مدروسة ومحددة النتائج من قبل الجاني، أي أن الجاني في التعديل يحدد الهدف ثم يختار من بين الوسائل المتاحة تلك التي يراها مناسبة للوصول إلى غايته. أما الإزالة، فهي مرحلة لاحقة على عملية إدخال المعطيات فالإزالة تفترض الوجود السابق لعملية الإدخال.

هذا وإن الأفعال المتمثلة في " الإدخال والتعديل والإزالة " وردت على سبيل الحصر، فلا يقع تحت طائلة التجريم أي فعل آخر غيرها ولو تضمن اعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات، فلا يخضع لتلك الجريمة فعل نسخ المعطيات أو نقلها، لأن كل تلك الأفعال لا تنطوي لا على إدخال و لا على تعديل بالمعنى السابق.

ومما لا شك أن جريمة التلاعب بمعطيات الحاسب الآلي جريمة عمدية لا بد لقيامها من توافر القصد الجنائي العام بأن يكون الجاني على علم بكافة العناصر المكونة للركن المادي للجريمة، فيقوم بإدخال أو إزالة أو تعديل على معطيات الحاسب الآلي مع علمه بأن ذلك يؤدي إلى تغيير في حالة المعطيات و تتجه إرادته إلى إحداث تلك النتيجة، و عليه فهذه الجريمة من جرائم الخطيرة تتحقق بمجرد الإدخال أو التعديل أو الإزالة و لو لم يترتب عن ذلك أي ضرر، و تنتفي هذه الجريمة إذا تمت الأفعال السابقة عن طريق الخطأ.

أما عن القصد الجنائي الخاص فلا يتطلب المشرع نية خاصة في هذه الجريمة، ويستشف ذلك من عدم نص المادة 394 مكرر 1 من قانون العقوبات على نية خاصة لدى الجاني، أما لفظ الغش لا يدل على ذلك وإنما يعني توافر القصد الجنائي العام (6).

وبخصوص العقوبات تضمنت المادة 394 مكرر 1 من قانون العقوبات عقوبتي الحبس والغرامة لجريمة التلاعب بمعطيات الحاسب الآلي فتتراوح مدة الحبس من 6 أشهر إلى 3 سنوات، أما الغرامة فتتراوح ما بين خمسمائة ألف ومليون دينار جزائري (7).

وبالنسبة للشخص المعنوي، تتمثل العقوبة الأصلية المقررة للشخص المعنوي في غرامة تقدر بخمسة أضعاف ما هو مقرر للشخص الطبيعي فتتراوح ما بين مليونين وعشرة ملايين دينار جزائري.

4- الجرائم الهامة بجميع مصالح المعطيات

جرم المشرع الجزائي طائفة من الأفعال تصب كلها في التعامل في معطيات صالحة لأن ترتكب بها إحدى جرائم المعطيات، فان لم ينجح ذلك في ردع الجناة، فقد حرص المشرع على التقليل من الضرر الذي يمكن أن تسببه تلك الجرائم قدر الإمكان، فقام بتجريم أشكال من التعاملات في المعطيات التي يتم الحصول عليها من إحدى الجرائم، وذلك بموجب نص المادة 394 مكرر2 من قانون العقوبات، وهذا ما يمكن تبينه فيما يلي:

أ- التعامل في معطيات صالحة لارتكاب الجريمة: نصت الفقرة الأولى من المادة 394 مكرر2 من قانون العقوبات على طائفة من الأفعال تمثل كافة أشكال التعامل في معطيات الحاسب الآلي التي تصلح لارتكاب إحدى جرائم المعطيات التي سبق الحديث عنها.

والمقصود بالتعامل هنا كل سلوك له علاقة بإعداد وإنتاج المعطيات غير المشروعة والتي تبدأ بتصميم المعطيات والبحث فيها وتجميعها وصولاً إلى توفيرها أو نشرها أو الاتجار فيها أي جعلها في متناول الغير وتحت تصرفه وستتطرق هذه الأفعال فيما يلي:

***التصميم:** هو أول حلقة في سلسلة التعامل في المعطيات، و يعني القيام بابتداع وإيجاد معطيات صالحة لارتكاب الجريمة و يتم هذا العمل عادة من طرف المختصين في هذا المجال كأن يقوم مصمم برنامج بتصميم برنامج اختراق.

***البحث:** يعني على الأرجح البحث في كيفية تصميم هذه المعطيات وإعدادها، و ليس مجرد البحث عن المعطيات، لأن الأصل أن البحث عن الوسيلة التي يمكن أن ترتكب بها الجريمة لا يعد جريمة. ***التجميع:** هو القيام بجمع العديد من المعطيات التي يمكن أن ترتكب بها جريمة الدخول غير المصرح به أو جريمة التلاعب.

***التوفير:** يعني تقديم المعطيات واثاحتها لمن يريد، أي جعلها في متناول الغير وتحت تصرفه، وهذا الفعل معاقب عليها أيضا في التشريع الفرنسي ومنصوص عليه في اتفاقية بودابست لسنة 2001. ***النشر،** يقصد به إذاعة المعطيات محل الجريمة وتمكين الغير من الإطلاع عليها عبر مختلف وسائل النشر.

***الاتجار:** هو تقديم المعطيات للغير بمقابل، ولا يشترط أن يكون هذا المقابل نقديا بل قد يكون عينيا أو قد يتمثل في خدمات أو غير ذلك، والفرق بين هذا السلوك وسلوك التوفير هو أن هذا الأخير قد يكون بدون مقابل.

ب- التعامل في معطيات متحصلة من جريمة: تتحقق جريمة التعامل في معطيات متحصلة من جريمة بأحد الأفعال التالية: "الحيازة - الإفشاء - النشر - الاستعمال" والتي تنطرق لها فيما يلي:

***الحيازة:** تقوم الحيازة بسيطرة الجاني على المعطيات المتحصلة من إحدى جرائم المعطيات، ويكفي للقول بتوافر السيطرة عدم وجود عقبات واقعية تحول بين الشخص وبين التمتع بهذه المعطيات.

***الإفشاء:** لقد جرم المشرع الجزائري إفشاء المعطيات المتحصلة من جرائم المعطيات، و الذي يقوم بالإفشاء، هنا ليس شخصا مؤمنا على هذه المعطيات وإنما هو شخص تحصل على هذه المعطيات بطريقة غير مشروعة وأراد المشرع أن يمنعه من إفشائها ونشرها سعيا لتضييق انتشارها.

***النشر:** أراد المشرع أن يضيق إلى حد كبير من دائرة الأشخاص الذين يمكن أن يطلعوا على هذه المعطيات فجرم نشر المعطيات المتحصلة من إحدى جرائم المعطيات، وهذا الفعل هو الوحيد المشترك بين صوري جريمة التعامل في معطيات غير مشروعة.

***الاستعمال:** جرم المشرع هذا السلوك بصفته أخطر سلوك يمكن أن يقع على المعطيات المتحصلة من جرائم المعطيات، ويشمل هذا التجريم كل استعمال للمعطيات مهما كان الهدف منه، وهو ما عبرت عنه المادة 394 مكرر 2 من قانون العقوبات في فقرتها الثانية بقولها "أو استعمال لأي غرض كان"، ومن أمثلة ذلك استخدام كلمة عبور تم الحصول عليها إثر دخول غير مصرح به (8).

ومما لا شك حسب نص المادة 394 مكرر 2 من قانون العقوبات أن جريمة التعامل في معطيات غير مشروعة هي جريمة عمدية تتطلب توافر القصد الجنائي العام لدى الجاني و يتجلى ذلك من خلال عبارة "عمدا" و عبارة "عن طريق الغش".

فلا بد للجاني إذا أن يعلم بأنه يقوم بالتعامل في معطيات غير مشروعة، ويتحقق ذلك بعلمه بأن من شأن المعطيات التي يتعامل فيها أن تستعمل في ارتكاب الجريمة و هذا بالنسبة لجريمة التعامل في معطيات صالحة لارتكاب الجريمة، أو بعلمه بأن من شأن تعامله في المعطيات المتحصلة من الجريمة أن تزيد من الضرر المترتب عنها بالنسبة لجريمة التعامل في معطيات متحصلة من الجريمة.

ولابد للجاني أن يعلم أيضا بالصفة غير مشروعة للمعطيات، أي أنه يمكن أن يرتكب بها جريمة أو أنها متحصلة من جريمة، فإذا قام رغم ذلك بالتعامل في هذه المعطيات بإرادته الحرة المختارة تقوم الجريمة في حقه.

أما بالنسبة للقصد الجنائي الخاص، فإن كان واضحا أن جريمة التعامل في معطيات متحصلة من جريمة لا تتطلب توفر القصد الجنائي الخاص كون الصفة غير المشروعة لهذه المعطيات ثابتة مما يجعل القصد العام كافيا لقيام الجريمة فلا يسأل الفاعل عن القصد الخاص من التعامل في هذه المعطيات (9).

المحور الثاني: الأحكام المشتركة بين جرائم المعطيات

من استقراء المواد من 394 مكرر 3 إلى 394 مكرر 7 من قانون العقوبات نجد أن المشرع قد وضع أحكاما مشتركة بين جميع جرائم المعطيات، منها ما يتعلق بالجريمة ومنها ما يتعلق بالعقوبة، لذا يمكن أن نميز بين نوعين من الأحكام المشتركة كمايلي:

أولا: الأحكام المشتركة المتعلقة بالجريمة، منها

* العقاب على الاتفاق الجنائي، إذ يعاقب المشرع الجزائري على الإشتراك في الإتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها.

* العقاب على الشروع، إذ نص المشرع صراحة في المادة 394 مكرر 7 من قانون العقوبات على العقاب على الشروع في ارتكاب إحدى جرائم المعطيات بنفس العقوبة المقررة للجريمة المرتكبة، رغبة من المشرع في عدم السماح بإفلات مجرمي المعلوماتية من العقاب.

ثانيا: الأحكام المشتركة المتعلقة بالعقوبة، منها:

* إضافة للعقوبات الأصلية المقررة لجرائم المعطيات، فقد قرر المشرع عقوبات تكميلية أيضا لهذه الجرائم. فبخصوص المصادرة، تطرقت إليها المادة 394 مكرر 6 من قانون العقوبات بنصها: "مع الاحتفاظ بحقوق الغير حسن النية بحكم بمصادرة الأجهزة و البرامج و الوسائل المستخدمة".

وبخصوص الغلق، نصت المادة 394 مكرر 06 على عقوبة تكميلية أخرى هي عقوبة الغلق، و تشمل هذه العقوبة المواقع التي تكون محلا لجريمة من الجرائم الماسة بالمعطيات، بالإضافة إلى مكان الاستغلال إذا ارتكبت الجريمة بعلم مالكيها، وذلك دون الإخلال بحقوق الغير حسن النية.

و لا يقصد المشرع بالمواقع التي تكون محلا للجريمة تلك المواقع التي تتضمن أنظمة المعالجة الآلية للمعطيات التي تم الاعتداء عليها بالدخول غير المشروع أو بالتلاعب بمعطياتها، لأن هذه المواقع هي الضحية في تلك الجرائم، وإنما يقصد بها المواقع التي استعملت في ارتكاب الجريمة، إذ أن هناك مواقع تقدم خدمات تسمح بالدخول غير المصرح به لمختلف الأنظمة أو تسمح بالتلاعب

بالمعطيات، كما أن هناك مواقع تقوم بتعليم كيفية تصميم المعطيات غير المشروعة و توفرها و تنشرها و تتاجر فيها و ما إلى ذلك من أشكال التعامل.

و تقع عقوبة الغلق أيضا على المحل أو مكان الاستغلال، و هو المكان الذي استعمله الجناة في ارتكاب جريمتهم و كان يحوي الأجهزة التي استعملت في عملية الدخول غير المصرح به أو في عملية التلاعب بالمعطيات أو في التعامل في معطيات غير مشروعة، بأن كانت تحوي هذه الأخيرة أو يتم التعامل فيها بواسطة هذه الأجهزة داخل المحل، و يمكن أن يحوي هذا المحل أو المكان المعطيات الصالحة لارتكاب الجريمة أو المعطيات المتحصلة منها دون أن تحوي أجهزة ما، و هذا لم تحدد المادة 394 مكرر 6 مدة الغلق.

* تشديد عقوبة الشخص المعنوي، إذ بالنسبة للجرائم الماسة بمعطيات الحاسب الآلي نجد أن المشرع قد شدد من عقوبة الشخص المعنوي، إذ جعل لها حداً واحداً هو الحد الأقصى لما هو مقرر عادة لعقوبة الشخص الطبيعي و المتمثل في 5 أضعاف الحد الأقصى للغرامة المقررة للجريمة، و بذلك لا يكون للقاضي السلطة التقديرية في تحديد العقوبة، لذلك تقدر الغرامة في جريمة الدخول أو البقاء غير المصرح بهما بخمسمائة ألف (500000) دينار جزائري في حين تقدر بعشرة ملايين (10) دينار جزائري في جريمة التلاعب في المعطيات و تبلغ قيمة الغرامة في جرائم التعامل في معطيات غير مشروعة خمسة و عشرون مليون (25) دينار جزائري.

والحكمة من مضاعفة الغرامة المقررة على الشخص المعنوي تتمثل في أنها لا تطبق لوحدها على الشخص الطبيعي، وإنما تطبق عادة إلى جانب عقوبة سالبة الحرية، لهذا تقتضي الحكمة عدم المساواة بين الغرامة التي تطبق وحدها على الشخص المعنوي وبين تلك التي تطبق بالإضافة إلى عقوبة سالبة للحرية على الشخص الطبيعي.

و ما تجدر الإشارة إليه في هذا الصدد أن المسؤولية الجزائية للشخص المعنوي لا تستبعد مسؤولية الأشخاص الطبيعيين بصفتهم فاعلين أو شركاء في نفس الجريمة.

* تشديد عقوبة الاعتداء على الهيئات العامة، إذ رتب المشرع عقوبة مشددة على جرائم المعطيات إذا كان موضوع النتيجة الإجرامية بعض الهيئات العامة، وذلك بمضاعفة العقوبة المقررة للاعتداء على معطيات و أنظمة أشخاص القانون الخاص ويرجع المبرر في ذلك إلى أهمية و حساسية المعطيات المتعلقة بالمصالح العليا للدولة و ما تتطلبه من ضمانات أكبر لحمايتها هذا من جهة، ومن جهة أخرى فإن الاعتداء على المعطيات المتعلقة بالهيئات المذكورة بالمادة 394 مكرر 4 من قانون

العقوبات يعكس جرأة و خطورة الفاعل، كما يحمل أبعادا سياسية قد تحدد سيادة الدولة ويتعلق الأمر بالمعطيات التابعة لمؤسسات الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام. وقد خص المشرع مؤسسة الدفاع الوطني بالذكر نظرا لأهمية هذه المؤسسة و دورها في الحفاظ على سلامة التراب الوطني والأمن العام و رد الاعتداءات الداخلية و الخارجية التي تهدف للإطاحة بنظام الدولة.

وبتطبيق العقوبة المشددة التي نص عليها المشرع يضاعف الحد الأدنى و الأقصى لكل من عقوبتي الحبس والغرامة المنصوص عليهما، فتكون العقوبة في جريمة الدخول أو البقاء غير المصرح بهما الحبس من 6 أشهر إلى سنتين والغرامة من مائة ألف إلى مائتي ألف دينار جزائري و إذ تترتب على تلك الجريمة تخريب النظام تكون العقوبة الحبس من سنة إلى أربع سنوات والغرامة من مائة ألف إلى ثلاثمائة ألف وتكون العقوبة الحبس من سنة إلى 4 سنوات و الغرامة من مائة ألف إلى مائتي ألف دينار جزائري إذا تترتب على الدخول أو البقاء حذف أو تغيير للمعطيات.

أما بالنسبة لجريمة التلاعب بالمعطيات فتصبح العقوبة الحبس من سنة إلى 6 سنوات والغرامة من مليون إلى أربعة 4 ملايين دج، أما في جريمة التعامل في معطيات غير مشروعة فتكون العقوبة المشددة الحبس من 4 أشهر إلى 6 سنوات و الغرامة من مليونين إلى 10 ملايين دينار جزائري، هذا بالنسبة للشخص الطبيعي، أما إذا ارتكبت الجريمة من طرف شخص معنوي فتضاعف العقوبة مرتين الأولى إلى 5 مرات عما هو مقرر للشخص الطبيعي لأن الجريمة ارتكبت من طرف شخص معنوي و الثانية تضاعف فيها تلك العقوبة إلى ضعفين لأنها ارتكبت ضد إحدى الهيئات العامة، فتشدد بذلك العقوبة إلى 10 أضعاف ما هو مقرر للشخص الطبيعي، و عليه تكون عقوبة جريمة الدخول أو البقاء غير المصرح بهما هي مليون دينار جزائري وإذا أدى ذلك إلى تخريب النظام تصبح مليون و خمسة مائة دينار جزائري في حين تصبح أربع مائة ألف دينار جزائري إذا تترتب على ذلك حذف أو تغيير لمعطيات المنظومة، أما بالنسبة لجريمة التلاعب بالمعطيات فتقدر الغرامة بعشرين مليون دينار جزائري، و عن جريمة التعامل في معطيات غير مشروعة فتكون الغرامة خمسين مليون دينار جزائري (10).

الخاتمة:

من خلال دراسة جريمة المساس بأنظمة المعالجة الآلية للمعطيات، يمكن القول أن المشرع ميز هذه الجريمة عن بقية الجرائم لخطورتها ولخصوصيتها، وكل هذا جعل المشرع الجزائري يتدارك الأمر سنة

2006 بتعديله لقانون الإجراءات الجزائية، ويجعل سلطة اتخاذ الإجراءات الخاصة بهذه الجريمة من صلاحيات وكيل الجمهورية وقاضي التحقيق، ومن بين تلك الإجراءات (تمديد التفتيش في غير الأوقات العادية، تمديد الوقف للنظر، اعتراض الصور والمراسلات تمديد الاختصاص خارج الاختصاص العادي)، كما نص على الإطار القانوني الذي يحكم مكافحة تلك الجرائم، كنصه على بيان صور كل جريمة وأركانها والعقوبات المترتبة في حال ارتكابها.

ولعل المشرع الجزائري أراد من خلال هذه الإجراءات الخاصة مواكبة دول العالم المتقدمة من خلال المصادقة على الاتفاقيات الدولية في هذا الشأن، بهدف التضييق على المجرمين من جهة، والحد من التوسع الإجرامي الخطير، على الرغم من أن البعض من الفقهاء يقول فيها مساس بالحرية الشخصية. وعلى الرغم مما سبق يتضح أنه على الرغم من وجود ركن شرعي خاص بالجريمة، بمعنى وجود نص قانوني ينص على الأفعال المكونة لهذه الجريمة، وينص على العقوبات المترتبة في حال ارتكابها، إلا أن هذا الجهد التشريعي يبقى مفعوله نسبي، لذا يمكن إبداء بعض الاقتراحات في هذا الشأن، منها:

- تنظيم دورات تكوينية لرجال القضاء ومساعديه، لاسيما القضاة والمحامين للتعريف بهذه الجرائم والتعريف بفنيتها، لأنه في أغلب الأحيان على الرغم من أن الوقائع تشكل جريمة المساس بأنظمة المعالجة الآلية للمعطيات، إلا أنها تكيف بأنها جريمة، وهذا راجع إلى حداثة هذه الجريمة.
- تعديل قانون العقوبات بوضع تعريف خاص لهذه الجريمة، بدل الاكتفاء ببيان الأفعال المكونة لهذه الجريمة فقط، وكذا النص على إعادة تكييفها من جنحة إلى جناية.
- تكوين رجال ضبطية قضائية متخصصين في مجال مكافحة هذه الجريمة، ليكونوا قادرين على كشف ماديات الجريمة.
- تفعيل أدلة الإثبات الحديثة وتطويرها لتسهيل التحري وملاحقة الفاعلين.
- تشجيع التأليف في مجال شرح هذه الجريمة، لاسيما من الناحية القانونية لسد الفراغ الحالي.

قائمة المراجعين:

- (1)- خروبي عفاف، الحماية الجنائية لمعطيات الحاسب الآلي، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الدفعة الثامنة عشر، الفترة التكوينية 2007-2010، ص 16-18.
- (2)- خروبي عفاف، المرجع السابق، ص 19-21.
- (3)- خروبي عفاف، المرجع السابق، ص 21-22.

- (4)-الدكتور أشرف شمس الدين، الحماية الجنائية، للمستند الإلكتروني، دار النهضة العربية، القاهرة، 2006، ص 45.
- (5)-يوسف دلاندة، قانون العقوبات، دار هومة للطباعة والنشر والتوزيع، 2006، ص275،276.
- (6)-خروبي عفاف، المرجع السابق، ص25-27.
- (7)-أحسن بوسقيعة، قانون العقوبات في ضوء الممارسة القضائية، منشورات بيرتي، الجزائر، 2005-2006، ص 185.
- (8)-أ، محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة،الإسكندرية،2008، ص204،201، 210،209.
- (9)-يوسف دلاندة، المرجع السابق، ص 276.
- (10)-خروبي عفاف، المرجع السابق، ص35-39.

جريمة الإرهاب الالكتروني

ط.د/ بدراني أحمد
كلية الحقوق والعلوم السياسية
جامعة غرداية

د/ بوقرين عبد الحليم
كلية الحقوق والعلوم السياسية
جامعة الأغواط

مقدمة:

الإرهاب الآن هو الهاجس الذي تعيشه جميع الدول ويتخوف منه الأفراد، حتى أصبح جزءاً من الحياة اليومية ولا يكاد يمر يوم دون أن تقع عملية إرهابية في مكان ما من العالم، وأصبحت أنباء وأخبار الإرهاب تحتل الصدارة في وسائل الإعلام، وتحظى بجذب إنتباه الناس على اختلاف مستوياتهم الثقافية ومواقع وجودهم على ظهر الأرض بحيث بعد الثورة الرقمية ظهر نوعاً جديداً من الإرهاب وهو الإرهاب الالكتروني، بحيث يعتبر من أخطر أنواع الإرهاب في العصر الحاضر لاتساع نطاق استخدام التكنولوجيا الحديثة في العالم، وقد أخذ يقرع أجراس الخطر في السنوات الأخيرة لتنبيه الحكومات والأفراد بحجم المخاطر والخسائر الناجمة عنه، بوصفه اعتداء سافراً على الأفراد وعلى الأمن القومي والسيادة الوطنية للدول، وزعزعة استقراره، فقد مكن التوسع في استخدام الانترنت التنظيمات لإرهابية من التحرك بمرونة عالية وإبراز دورها وإدارة إمكانيات من مختلف أنحاء العالم إذ أصبحت الانترنت منبراً للجماعات والأفراد لنشر الإرهاب والعنف والكراهية ووسيلة للاتصال بين الإرهابيين أو بمؤيديهم أو المتعاطفين معهم، لذا يعتبر الإرهابيون الجدد أن التقنية الالكترونية من أفضل لأسلحة الناعمة في أداء العمل الإرهابي.

يتمتع هذا النوع من الإرهاب بمجاذبية خاصة عند الجماعات الإرهابية وذلك لأن الانترنت مجال مفتوح وواسع ليس لها حدود، ولا يتوقف الأمر عند حد استخدام التنظيمات الإرهابية لوسائل التقنية الحديثة في تنفيذ مخططاته التخريبية، بل يتعداه إلى أبعد من ذلك بحيث أدى التطور المتنامي للظاهرة الإرهابية إلى شبكات دولية إلى البحث في أحدث التقنيات والاختراعات العلمية لتسخيرها كوسيلة وكهدف يخدم مشروعاته الإجرامية، لذا من الأهمية مكان دراسة هذا النوع الجديد من الإرهاب من كافة الجوانب وبحث طرق مكافحته، وعلى هذا الأساس نطرح الإشكالية التالية: ما مفهوم الإرهاب الالكتروني؟ وما هو موقف المشرع الجزائري منه؟.

ولقد كان لظهور شبكة المعلومات (الإنترنت) دور كبير في تنفيذ الإرهابيون لعملياتهم المدمرة تلك وللوقوف على هذه الظاهرة بشكل يتناسب مع موضوع بحثنا، فإننا سوف نقوم بتقسيم بحثنا على النحو الآتي:

المبحث الأول: مفهوم الإرهاب الإلكتروني

المبحث الثاني: موقف المشرع الجزائري من الإرهاب الإلكتروني

المبحث الأول: مفهوم الإرهاب الإلكتروني

سنتناول في هذا المبحث تعريف الإرهاب الإلكتروني وخصائصه في المطلب الأول، وفي المطلب الثاني: صور الإرهاب الإلكتروني، والمطلب الثالث: أشكال الإرهاب الإلكتروني.

المطلب الأول: تعريف وخصائص الارهاب الالكتروني

سنتناول في هذا المطلب تعريف الإرهاب الإلكتروني في الفرع الأول وخصائصه في الفرع الثاني

الفرع الأول: تعريف الارهاب الالكتروني

لقد تعدت تعاريف الإرهاب وإختلفت وتباينت في شأنه الإجهادات، ولم يصل المجتمع الدولي حتى الآن إلى تعريف جامع مانع متفق عليه للإرهاب، ويرجع ذلك إلى تنوع أشكاله ومظاهره، وتعدد أساليبه وأنماطه، وإختلاف وجهات النظر الدولية والإتجاهات السياسية حوله، وتباين العقائد والإيديولوجيات التي تعتنقها الدول إتجاهه، فما يراه البعض إرهاباً يراه الآخر عملاً مشروعاً.

قامت بعض القوانين الجنائية الوطنية بتعريف الإرهاب، كما تم تحديد المراد من هذا المصطلح في الإتفاقيات الإقليمية تعريف الإرهاب :عرفت المادة 87 مكرر من قانون العقوبات الأفعال التي تعد إرهابية أو تخريبية بأنها كل فعل يستهدف أمن الدولة وسلامتها وتتلخص هذه الأفعال في جرائم الشيء العمومي، والتي يكون الهدف منها:

__ بث الرعب وخلق جو إنعدام الأمن سواء كان الإعتداء معنوياً أو جسدياً.

__ التجمهر وعرقلة حركة المرور.

__ الإعتداء على رموز الأمة ونش القبور __.الاعتداء على وسائل المواصلات والملكيات العمومية والخاصة والاستحواذ عليها بغير قانون.

__ تعريض صحة الإنسان والحياة، أو البيئة للخطر ببث مواد محظورة في الماء أو الجو، أو باطن الأرض.

__ عرقلة عمل السلطات العمومية أو حرية ممارسة العبادة والحريات العامة وسير المؤسسات المساعدة للمرفق العام.

__ عرقلة سير المؤسسات العمومية أو الإعتداء على حياة أعوانها، أو ممتلكاتهم، أو عرقلة تطبيق القوانين والتنظيمات، وما يلاحظ أن هذا المفهوم واسع وغير محدد نظرا للمظاهر المختلفة للأعمال الإرهابية لذلك اختلفت المفاهيم وكان من الصعب وضع تعريف شامل للإرهاب¹.

أما تعريف الارهاب حسب القانون المصري:- هو كل استخدام للقوة أو العنف أو التهديد أو الترويع يلجأ اليه الجاني تنفيذا لمشروع اجرامي فردي أو جماعي بمهدف الاخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر اذا كان من شان ذلك ايذاء الاشخاص أو القاء الرعب بينهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر. أو الحاق الضرر بالبيئة أو بالاتصالات أو بالمواصلات أو بالأموال أو المباني أو بالأماكن العامة أو احتلالها أو الاستيلاء عليها أو منع أو عرقلة ممارسة السلطات العامة أو دور العبادة أو معاهد العلم أو تعطيل تطبيق الدستور أو القوانين أو اللوائح².

أما بالنسبة للاتفاقيات العربية لمكافحة الارهاب فقد عرفت الارهاب:- هو كل فعل من أفعال العنف أو التهديد به أيا كانت دوافعه أو أغراضه يقع تنفيذا لمشروع اجرامي فردي أو جماعي من أجل القاء الرعب بين الناس أو ترويعهم بايذاء أو الحاق الضرر بالبيئة أو بالمرافق العامة أو الخاصة أو تعريض الموارد الوطنية للخطر.

وفي ضوء التعاريف السابقة يمكن تعريف الارهاب الالكتروني بشكل عام بأنه:- العدوان او التخويف او التهديد المادي او المعنوي الصادر من الدول أو الجماعات أو الافراد على الانسان في دينه أو نفسه أو عرضه أو ماله أو عقله بغير حق باستخدام الموارد المعلوماتية والوسائل الالكترونية بشتى صنوف العدوان وصور الفساد.

¹ - رفد عيادة الهاشمي، الإرهاب الإلكتروني. بدون دار النشر، بدون بلد، بدون سنة، بدون طبعة.

² - أمين حسين، "الإرهاب الإلكتروني أخطر معارك حروب الفضاء": من الموقع: تم تصفحه يوم 28-12-2018 على الساعة 14:12 <http://alwatan.com/details/166324> تاريخ النشر: 2017/01/14.

فالإرهاب الإلكتروني يعتمد على إستخدام الإمكانيات العلمية والتقنية، وإستغلال وسائل الاتصالات والشبكات المعلوماتية من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم¹.

الفرع الثاني: خصائص الإرهاب الإلكتروني

مما لا شك فيه أن الإرهاب الإلكتروني ينفرد بعدد من الخصائص التي يختص بها دون سواه، ويتميز بها عن غيره من الظواهر الإجرامية الأخرى، كما يسعى إلى تحقيق جملة من الأهداف والأغراض غير المشروعة.

يتميز الارهاب الالكتروني بعدة خصائص وسمات:

أولاً: الارهاب الالكتروني لا يحتاج عند ارتكابه الى العنف والقوة بل يتطلب حاسب الي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة.

ثانياً: يتميز الارهاب الالكتروني بانه جريمة اراهبية متعددة الحدود وعابرة للدول والقارات وغير خاضعة لنطاق اقليمي محدود.

ثالثاً: صعوبة اكتشاف جرائم الارهاب الالكتروني ونقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مثل هذه الجرائم.

رابعاً: صعوبة اثبات في الارهاب الالكتروني نظراً لسرعة غياب الدليل الرقمي وسهولة اتلافه وتدميره.

خامساً: يتميز الارهاب الالكتروني بانه يتم بتعاون أكثر من شخص على ارتكابه.

سادساً: مرتكب جريمة الارهاب الالكتروني يكون من ذوي الاختصاص في مجال تقنية المعلومات أو من شخص لديه على الأقل قدر من المعرفة والخبرة في التعامل مع الحاسب الالي والشبكة المعلوماتية.

المطلب الثاني: صور الإرهاب الإلكتروني

فمن خلال الشبكة المعلوماتية تستطيع المنظمات والجماعات الإرهابية نشر أفكارها المتطرفة، والدعوة لمبادئها المنحرفة، والسيطرة على وجدان الأفراد واستغلال معاناتهم من أجل تحقيق أغراضهم غير المشروعة والتي تتعارض مع مصلحة المجتمع.

¹ - رفد عيادة الهاشمي، الإرهاب الإلكتروني. بدون دار النشر، بدون بلد، بدون سنة، بدون طبعة.

ويستخدم الإرهابيون الشبكة العالمية للمعلومات الانترنت بشكل يومي لنشر أفكارهم الهدامة ولتحقيق أهدافهم السيئة، ومن الممكن إبراز أهم استخداماتهم للشبكة في ما يلي: سنتناول في هذا المطلب الإتصال والتخفي في الفرع الأول جمع المعلومات الإرهابية في الفرع الثاني، وفي الفرع الثالث: التخطيط والتنسيق للعمليات الإرهابية، و الفرع الرابع: الحصول على التمويل².

الفرع الأول: الإتصال والتخفي

تستخدم الجماعات والمنظمات الإرهابية المختلفة الشبكة العالمية للمعلومات في الإتصال والتنسيق فيما بينهم نظرا لقلّة تكاليف الاتصال والوسائل للاستخدام الشبكة مقارنة بالوسائل الأخرى، كما توفر الشبكة للإرهابيين فرصة ثمينة في الاتصال للتخفي وذلك عن طريق البريد الالكتروني أو المواقع والمنتديات وغرف الحوار الالكتروني حيث وضع رسائل مشفرة تأخذ طابعاً لا يلفت الانتباه، فمن دون أن يضطر الإرهابي الإفصاح عن هويته كما أنها لا تترك أثراً واضحاً يمكن أن يدل عليه.

الفرع الثاني: جمع المعلومات الإرهابية

تمتاز الشبكة المعلوماتية بوفرة المعلومات الموجودة فيها، كما أنها تعتبر موسوعة إلكترونية شاملة متعددة الثقافات ومتنوعة المصادر وغنية بالمعلومات الحساسة التي يسعى الإرهابيون للحصول عليها كمواقع المنشآت النووية، ومصادر توليد الطاقة، وأماكن القيادة والسيطرة والاتصالات ومواعيد الرحلات الجوية والمعلومات المختصة بسبل مكافحة الإرهاب؛ نظراً لما تحتويه من معلومات تفصيلية مدعمة بالصور الضوئية

الفرع الثالث: التخطيط والتنسيق للعمليات الإرهابية

العمليات الإرهابية عمل على جانب التعقيد والصعوبة فهي تحتاج الى تخطيط محكم وتنسيق شامل وتعتبر الشبكة العالمية للمعلومات وسيلة اتصال بالغة الأهمية للجماعات الإرهابية حيث تتيح لهم حرية التخطيط الدقيق والتنسيق الشامل لشن هجمات إرهابية محددة في جو مريح، وبعيداً عن أعين الناظرين مما يسهل على الإرهابيين ترتيب تحركاتهم وتأقيت هجماتهم.

² - أيمن حسين، "الإرهاب الالكتروني أخطر معارك حروب الفضاء": من الموقع: تم تصفحه يوم 28-12-2018 على الساعة 12:14 <http://alwatan.com/details/166324> تاريخ النشر: 2017/01/14.

الفرع الرابع: الحصول على التمويل

من خلال الشبكة المعلوماتية العالمية وعن طريق الاستعانة ببيانات إحصائية منتقاة من المعلومات الشخصية التي يدخلها المستخدمون على الشبكة المعلوماتية من خلال الاستفسارات والاستطلاعات الموجودة على المواقع الالكترونية يقوم الإرهابيون بالتعرف على الأشخاص ذوي المشاعر الرقيقة والقلوب الرحيمة ومن ثم استجداؤهم بدفع تبرعات مالية لأشخاص اعتباريين يكونون واجهة لهؤلاء الإرهابيين، ويتم ذلك بواسطة رسائل البريد الالكتروني أو من خلال مساحات الحوار الالكترونية بطريقة ذكية وأسلوب مخادع بحيث لا يشك المتبرع بأنه سيساعد إحدى التنظيمات الإرهابية¹.

الفرع الخامس: التعبئة وتجنيد الإرهابيين

تستخدم الجماعات والمنظمات الإرهابية الشبكة المعلوماتية العالمية في نشر ثقافة الإرهاب والترويج لها، وبث الأفكار والفلسفات التي تنادي بهم كما تسعى جاهدة الى توفير اكبر عدد ممكن من الراغبين في تبني أفكارها ومبادئها ومن خلال الشبكة المعلوماتية تقوم التنظيمات الإرهابية بتكوين قاعدة فكرية لمن لديهم ميول واستعداد للانخراط في الأعمال التدميرية والتخريبية مما يوفر لديها قاعدة ممن تجمعهم نفس الأفكار والتوجهات فيسهل تجنيدهم لتنفيذ عمليات إرهابية في المستقبل إن استقدام عناصر جديدة داخل التنظيمات الإرهابية يحافظ على بقائها واستمرارها لذا فإن الإرهابيين يقومون باستغلال تعاطف بعض أفراد المجتمع مع قضاياهم، فيجتذبونهم بأسلوب عاطفي وعبارات حماسية براقعة، وذلك من خلال غرف الحوار والمنتديات والمواقع الالكترونية¹.

¹ - إيهاب شوقي، الإرهاب الالكتروني و جرائمه، من الموقع:

<http://www.anntv.tv/new/showsubject.aspx?id=121062> (د.ت.ن) تم تصفحه يوم 27-12-2018. على الساعة 18.30.

¹ - إيهاب شوقي، الإرهاب الالكتروني و جرائمه، من الموقع:

<http://www.anntv.tv/new/showsubject.aspx?id=121062> (د.ت.ن) تم تصفحه يوم 27-12-2018. على الساعة 18.30.

الفرع السادس: التدريب الإرهابي الإلكتروني

تحتاج العمليات الإرهابية الى تدريب خاص ويعد التدريب من أهم هواجس التنظيمات الإرهابية وقد أنشئت معسكرات تدريبية سرية كما ظهر بعضها في وسائل الإعلام لكن مشكلة معسكرات التدريب الإرهابية أنها دائماً معرضة للخطر ويمكن اكتشافها ومداومتها في أي وقت لذا فإن الشبكة المعلوماتية بما تحتوه من خدمات ومميزات أصبحت وسيلة مهمة للتدريب والتخطيط والتنفيذ كما قامت بعض الجماعات الإرهابية بإنتاج أدلة إرشادية للعمليات الإرهابية وهذه الأدلة يمكن نشرها عبر الشبكة المعلوماتية لتصل الى الإرهابيين في مختلف أنحاء العالم وغني عن البيان ما تشتمل عليه الشبكة المعلوماتية من كم هائل من المواقع والمنتديات والصفحات التي تحتوي على كتيبات وإرشادات تبين كيفية تصنيع القنابل والمتفجرات والمواد الحارقة والأسلحة

الفرع السابع: إصدار البيانات الإلكترونية

تقوم المنظمات الإرهابية باستخدام الشبكات المعلوماتية في نشر بياناتها الإرهابية المختلفة وذلك عن طريق المواقع الإلكترونية أو بواسطة رسائل البريد الإلكتروني أو من خلال منتديات الحوار وساحاته وقد ساعدت القنوات الفضائية التي تسارع في الحصول على مثل هذه البيانات الإرهابية ومن ثم تقوم بنشرها عبر وسائل الإعلام في مضاعفة انتشار تلك البيانات ووصولها الى مختلف شرائح المجتمع وتأخذ البيانات الصادرة من قبل التنظيمات الإرهابية اتجاهات متنوعة فتارة ترسم أهدافاً وخططاً عامة للتنظيم الإرهابي، وأحياناً تكون للتهديد والوعيد لشن هجمات إرهابية معينة في حين تصدر معلنة عن تبني تنفيذ عمليات إرهابية محددة، كما تصدر تارة أخرى بالنفي أو التعليق على أخبار وتصريحات صادرة من جهات أخرى².

المطلب الثالث: أشكال الإرهاب الإلكتروني

سنتناول في هذا المطلب إنشاء المواقع الإرهابية الإلكترونية في الفرع الأول تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية في الفرع الثاني، وفي الفرع الثالث: السيناريوهات المحتملة للإرهاب الإلكتروني في عصر المعلومات.

² - عبد الرحمن بن عبد الله السند، وسائل الإرهاب الإلكتروني وحكمها في الإسلام وطرق مكافحتها من الموقع:

http://shamela.ws/browse.php/book-1244/page-20 (د.ت.ن) تم تصفحه يوم 27-

2018-12 على الساعة 12.45.

الفرع الأول: إنشاء المواقع الإرهابية الإلكترونية

يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على الشبكة العالمية للمعلومات الانترنت لبث أفكارهم الضالة والدعوة الى مبادئهم المنحرفة ولإبراز قوة التنظيم الإرهابي، وللتعبئة الفكرية وتجنيد إرهابيين جدد، ولإعطاء التعليمات والتلقين الإلكتروني، وللتدريب الإلكتروني من خلال تعليم الطرق والوسائل التي تساعد على القيام بشن هجمات إرهابية، فقد أنشأت مواقع إرهابية إلكترونية لبيان كيفية صناعة القنابل والمتفجرات والأسلحة الكيماوية الفتاكة ولشرح طرق اختراق البريد الإلكتروني وكيفية اختراق وتدمير المواقع الإلكترونية والدخول الى المواقع المحجوبة، ولتعليم طرق نشر الفيروسات ونحو ذلك.

والموقع عبارة عن معلومات مخزنة بشكل صفحات وكل صفحة تشتمل على معلومات معينة تشكلت بواسطة مصمم الصفحة باستعمال مجموعة من الرموز تسمى لغة تحديد النص الأفضل (hyber text mark up language html) ولأجل رؤية هذه الصفحات يتم طلب استعراض شبكة المعلومات العالمية (www browser) ويقوم بحل رموز (html) وإصدار التعليمات لإظهار الصفحات المكتوبة وإذا كان الحصول على مواقع افتراضية أو وسائل إعلامية كالقنوات التلفزيونية والإذاعية صعباً بالنسبة للإرهابيين فإن إنشاء مواقع خاصة بهم على الشبكة العالمية للمعلومات الانترنت، لخدمة أهدافهم وترويج أفكارهم الضالة أصبح سهلاً وممكناً، ولذا فإن معظم التنظيمات الإرهابية لها مواقع إلكترونية وهي بمثابة المقر الافتراضي لها¹.

إن الوجود الإرهابي النشط على الشبكة المعلوماتية متنوع ومراوغ بصورة كبيرة فإذا ظهر موقع إرهابي اليوم فسرعان ما يغير عنوانه الإلكتروني غداً ثم يختفي ليظهر مرة أخرى بشكل جديد وتصميم مغاير وعنوان إلكتروني مختلف، بل تجد لبعض المنظمات الإرهابية الآف المواقع حتى تضمن انتشاراً أوسع، وحتى لو تم منع الدخول على بعض هذه المواقع، أو تعرضت بعضها للتدمير تبقى المواقع الأخرى، ويمكن الوصول إليها، ومن الأمثلة على بعض المواقع الإلكترونية التي قام بإنشائها وتصميمها بعض التنظيمات الإرهابية ما يأتي:

¹ - عبد الرحمن بن عبد الله السند، وسائل الإرهاب الإلكتروني وحكمها في الإسلام وطرق مكافحتها من الموقع: <http://shamela.ws/browse.php/book-1244/page-20> (د.ت.ن) تم تصفحه يوم 27-12-2018 على الساعة 12.45.

- موقع النداء: وهو الموقع الرسمي لتنظيم القاعدة بعد أحداث الحادي عشر من سبتمبر عام 2001، ومن خلاله تصدر البيانات الإعلامية للقاعدة².

- ذروة السنام: وهي صحيفة الكترونية دورية للقسم الإعلامي لتنظيم القاعدة.

- صوت الجهاد: وهي مجلة نصف شهرية يصدرها ما يسمى بتنظيم القاعدة في جزيرة العرب ، وتتضمن مجموعة من البيانات والحوارات مع قادة التنظيم ومنظريه.

- البتار: وهي مجلة عسكرية إلكترونية متخصصة تصدر عن تنظيم القاعدة، وتختص بالمعلومات العسكرية والميدانية والتجنيد.

وقد وجد الإرهابيون غايتهم في تلك الموارد المعلوماتية والوسائل الالكترونية التي جلبتها حضارة التقنية في عصر المعلومات، فأصبح للمنظمات العديد من المواقع على الشبكة العالمية للمعلومات، وصارت تلك المواقع من أبرز مظاهر وأشكال الإرهاب الالكتروني¹.

الفرع الثاني: تدمير المواقع والبيانات الالكترونية والنظم المعلوماتية

تقوم التنظيمات الإرهابية بشن هجمات إرهابية الكترونية من خلال الشبكة المعلوماتية؛ بقصد تدمير المواقع والبيانات الالكترونية والنظم المعلوماتية، وإلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها، وتستهدف الهجمات الإرهابية في عصر المعلومات ثلاثة أهداف أساسية غالباً، وهي الأهداف العسكرية والسياسية والاقتصادية، وفي عصر ثورة المعلومات تجدد الأهداف الثلاثة نفسها وعلى رأسها مراكز القيادة والتحكم العسكرية، ثم مؤسسات المنافع كمؤسسات الكهرباء والمياه، ومن ثم تأتي المصارف والأسواق المالية؛ وذلك لإخضاع إرادة الشعوب والمجتمعات الدولية.

إن عملية الاختراق الإلكتروني تتم عن طريق تسريب البيانات الرئيسة والرموز الخاصة ببرامج شبكة الإنترنت وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود شخص المخترق في الدولة التي يتم اختراق مواقعها فالبعد الجغرافي لا أهمية له في الحد من الاختراقات المعلوماتية، ولا تزال نسبة

²- شيريهان نشأت المنيري، "مخاطر جرائم الانترنت على استقرار النظام الدولي"، مجلة السياسة الدولية، من الموقع

<http://www.siyassa.org.eg/NewsQ/2450.aspx>، (د.ت.ن) تم تصفحه يوم، 01-02-

2017. على الساعة 09.56.

¹- عبد الرحمن بن عبد الله السند، وسائل الإرهاب الإلكتروني وحكمها في الإسلام وطرق مكافحتها من الموقع:

<http://shamela.ws/browse.php/book-1244/page-20> (د.ت.ن) تم تصفحه يوم 20-

2018-12 على الساعة 12.45.

كبيرة من الإختراقات لم تكتشف بعد بسبب التعقيد الذي يتصف به نظم تشغيل الحاسب الآلي والشبكات المعلوماتية.

ومن الممكن تصور هجوم إلكتروني على احد المواقع الإلكترونية بقصد تدميرها وشلها عن العمل، حيث يمكن أن يقوم الإرهابيون بشن هجوم مدمر لإغلاق المواقع الحيوية على الشبكات المعلوماتية، وإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات، ومحطات توليد الطاقة والماء، ومواقع الأسواق المالية بحيث يؤدي توقفها عن العمل إلى تحقيق آثار تدميرية تفوق ما تحدثه القنابل والمتفجرات من آثار.

إن من الوسائل المستخدمة حالياً لتدمير المواقع ضخ مئات الآلاف من الوسائل الالكترونية -e-mail من جهاز الحاسوب الخاص بالمدمر إلى الموقع المستهدف؛ للتأثير على السعة التخزينية للموقع، فتشكل هذه الكمية الهائلة من الوسائل المستخدمة الالكترونية ضغطاً يؤدي في النهاية إلى تفجير الموقع العامل على الشبكة².

وتشتيت البيانات والمعلومات المخزنة في الموقع، فتنتقل إلى جهاز المعتدي أو تمكنه من حرية التجول في الموقع المستهدف بسهولة ويسر، والحصول على كل ما يحتاجه من أرقام ومعلومات وبيانات خاصة بالموقع المعتدى عليه، وتعد الفيروسات من اخطر آفات الشبكة المعلوماتية والفيروس عبارة عن برنامج حاسوبي يلحق ضرراً بنظام المعلومات والبيانات ويقدر على التضاعف والانتشار والانتقال من جهاز إلى آخر².

الفرع الثالث: السيناريوهات المحتملة للإرهاب الإلكتروني في عصر المعلومات:

لقد قام خبراء الجرائم الالكترونية والأمن المعلوماتي بوضع أكثر من سيناريو محتمل للهجمات الإرهابية، وأودعها في البحوث والدراسات والتقارير التي تعالج هذه المسألة، ويمكن تقسيم هذه السيناريوهات إلى ما يأتي:

² - شيريهان نشأت المنيري، "مخاطر جرائم الانترنت على استقرار النظام الدولي"، مجلة السياسة الدولية، من الموقع <http://www.siyassa.org.eg/NewsQ/2450.aspx>، (د.ت.ن) تم تصفحه يوم، 01-02-2017. على الساعة 09.56.

أولاً- استهداف النظم العسكرية:

تستهدف هذه النوعية من الهجمات عادة الأهداف العسكرية غير المدنية، والمرتبطة بشبكات المعلومات ويعد هذا السيناريو من أخطر السيناريوهات المحتملة التي قد تعصف بمجتمعنا المعاصر، وتبدأ المرحلة الأولى من هذا السيناريو باختراق المنظومات الخاصة بالأسلحة الاستراتيجية، ونظم الدفاع الجوي والصواريخ النووية¹.

ثانياً- استهداف محطات توليد الطاقة والماء:

أصبح الاعتماد على شبكات المعلومات وخصوصاً في الدول المتقدمة من الوسائل المهمة لإدارة نظم الطاقة الكهربائية ويمكن للهجمات على مثل هذا النوع من شبكات المعلومات أن تؤدي إلى نتائج خطيرة، وخصوصاً في ظل اعتماد الإنسان المعاصر على الطاقة الكهربائية فإن شبكات المعلومات المرتبطة بشكل مباشر أو غير مباشر بشبكات الطاقة الكهربائية تعتبر من الأهداف الأولى التي قد يستهدفها الإرهاب الإلكتروني.

ثالثاً- استهداف البنية التحتية الاقتصادية

أصبح الاعتماد على الشبكات المعلوماتية شبه مطلق في عالم المال والأعمال مما يجعل هذه الشبكات نظراً لطبيعتها المترابطة وانفتاحها على العالم هدفاً مغرياً للمجرمين والإرهابيين، ومما يزيد من إغراء الأهداف الاقتصادية والمالية هو أنها تتأثر بشكل ملموس بالإنطباعات السائدة والتوقعات والتشكيك في صحة هذه المعلومات، أو تخريبها بشكل بسيط يمكن أن يؤدي إلى نتائج مدمرة وإضعاف الثقة في النظام الاقتصادي.

¹ عمارة. عمارة التدابير الوقائية والجرائية من جريمة تبييض الأموال وتمويل الارهاب، الملتقى الوطني الثالث حول الجريمة المنظمة وسياسة مكافحتها في الجزائر، جامعة مسيلة.

² حسن بن سعيد بن سيف الغافري، الإرهاب الإلكتروني. من الموقع:

http://www.ita.gov.om/ITAPortal_AR/Pages/Page.aspx?NID=1&PID=9&LID=5

،(د.ت.ن)، تم تصفحه يوم 28-12-2108، على الساعة 13.30.

رابعاً- استهداف نظم المواصلات

ويتضمن هذا السيناريو اختراق نظم التحكم بخطوط الملاحة الجوية والبرية والبحرية، وإحداث خلل في برامج هبوط الطائرات وإقلاعها؛ مما قد ينجم عنه حصول تصادم فيما بينها، أو تعطيل نظم الهبوط فلا تستطيع الطائرات الوصول إلى مدرج مطار من المطارات، كما يحتمل تمكن قراصنة المعلومات من السيطرة على نظم التحكم بتسيير القطارات، وتغيير مواعيد الإنطلاق بحيث تسود الفوضى أو تتصادم هذه القطارات فيما بينها وكذا بالنسبة للسفن والناقلات والغواصات البحرية.

خامساً- استهداف نظم الاتصالات

ويشمل هذا السيناريو اختراق الشبكات المعلوماتية والشبكة الهاتفية الوطنية، وإيقاف محطات توزيع الخدمة الهاتفية وقد تمارس سلسلة من الهجمات على خطوط الهواتف المحمولة ومنع الإتصال بين أفراد المجتمع، ومؤسساته الحيوية الأمر الذي ينشر حالة من الرعب والفوضى، وعدم القدرة على متابعة تداعيات الهجمات الإرهابية المعلوماتية ولا يتوقف الأمر عند هذا الحد فقط بل هناك العديد من الأهداف الأخرى التي يمكن للمجرمين والإرهابيين المتمكنين من خلالها أن يشيعوا الفساد²، وينشروا الفوضى فهناك على سبيل المثال شبكات المعلومات الطبية والتي يمكن من خلال مهاجمتها واختراقها، ومن ثم التلاعب بها حصول خسائر بشرية، ومن أمثلة ذلك في العالم الغربي ما قام به أحد المجرمين من الدخول إلى سجلات المستشفيات والتلاعب بملفات المرضى بشكل أدى إلى حقن هؤلاء بأدوية وعلاجات كانت مميتة بالنسبة لهم، وما إلى ذلك يمكن لها أن تحدث آثاراً مدمرة على الصعيد الاجتماعي¹

²-رغد عيادة الهاشمي، مرجع سابق، ص43.

المبحث الثاني: موقف المشرع الجزائري من الإرهاب الإلكتروني

حاول المشرع الجزائري، إصدار قوانين عامة وخاصة وهياكل وأجهزة للتصدي للجرائم الإلكترونية، ويعود أسباب الاهتمام بتنظيم جرائم الانترنت من جهة تطور تكنولوجيا الإعلام، الذي أدى إلى اتساع نطاق الجريمة الإلكترونية فهي أصبحت لا تقتصر على جريمة واحدة وإنما إتسعت إلى عدة جرائم ترتكب عن طريق الهاتف وعن طريق الكمبيوتر، ولا ترتكب هذه الجريمة من طرف شخص طبيعي فقط بل تعدت إلى الشخص المعنوي ومن جهة أخرى كون القانون الجنائي التقليدي غير قادر على استيعاب الجرائم الإلكترونية الحديثة ضيف إلى ذلك المحافظة على مبدأ الشرعية الجنائية، متكلا على تعزيز التعاون بين الجهات القانونية والخبراء المتخصصين في المعلوماتية زيادة على التعاون الدولي لمكافحةها، وعليه خصصنا هذا المبحث إلى، القوانين العامة الموضوعية المنظمة للجريمة الإلكترونية (المطلب الأول)، القوانين الخاصة وآليات مكافحة الإرهاب الإلكتروني: (المطلب الثاني).

المطلب الأول: تجريم الارهاب الالكتروني

تفطن المشرع لخطورة الارهاب الالكتروني فعدل قانون العقوبات ونص على تجريمه حيث جاء في المادة 87 مكرر: (قانون رقم 16 - 02 مؤرخ في 19 يونيو سنة 2016) يعاقب بالسجن المؤقت من 5 سنوات على 10 سنوات بغرامة مالية من 100.000 دج إلى 500.000 دج، كل جزائري أو أجنبي مقيم بالجزائر بطريق شرعية أو غير شرعية، يسافر أو يحاول السفر إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو تديرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها.

يعاقب بنفس العقوبة كل من:

- يوفر أو يجمع عمدا أموالا بأي وسيلة و بصورة مباشرة أو غير مباشرة، بقصد استخدامها أو مع علمه بأنها ستستخدم في تمويل سفر أشخاص إلى دولة أخرى بغرض ارتكاب الأفعال المذكورة في فقرة الأولى من هذه المادة،
- قام عمدا بتمويل أو تنظيم سفر أشخاص إلى دولة أخرى، لغرض ارتكاب أفعال إرهابية أو تديرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها أو تسهيل ذلك السفر،
- يستخدم تكنولوجيايات الإعلام والاتصال لارتكاب الأفعال المذكورة في هذه المادة.

ففي هذه الحالة يحاول المشرع قطع الطريق على الجماعات الارهابية عن طريق تجريم بعض الاعمال التي تعد في عرف القانون الجنائي اعمال تحضيرية لا يعاقب عليها القانون، مثل مساعدة شخص على السفر للانظام الى جماعة ارهابية عن طريق استعمال وسائل الاعلام والاتصال.

بينما جاء جاء في المادة 87 مكرر 12 انه " يعاقب بالسجن من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 100.000 دج إلى 500.000 دج كل من يستخدم تكنولوجيايات الإعلام والاتصال لتجنيد الأشخاص لصالح إرهابي أو جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها أو تقع أنشطتها تحت طائلة أحكام هذا القسم أو ينظم شؤونها أو يدعم أعمالها أو أنشطتها أو ينشر أفكارها بصورة مباشرة أو غير مباشرة".

ويحاول المشرع من خلال هذه الجريمة منع استعمال تكنولوجيايات الإعلام والاتصال لغرض تجنيد أو تدريب شخص لصالح إرهابي أو جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها أو تقع أنشطتها في دائرة ارتكاب أفعال إرهابية أو تديرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها.

المطلب الثاني: الاحكام الاجرائية لمكافحة الارهاب الالكتروني

الفرع الاول: تنظيم إجراءات التفتيش الإلكتروني

نظم المشرع تفتيش المنظومات المعلوماتية بواسطة القانون 04/09 السالف الذكر حيث جاءت فيه إجراءات التفتيش وحجز المعطيات المعلوماتية¹.

وبالرجوع الى نص المادة 5 من القانون 04/09 نجد أن المشرع قد اجاز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد إلى كل منظومة معلوماتية أو جزء منها وكذا المعطيات المخزنة فيها وكل منظومة معلوماتية..، وقد حددت المادة 2 من القانون 04/09 المقصود بالمنظومة المعلوماتية على أنها " أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم وأحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذاً لبرنامج معين"،.

¹ - كما نظمت اتفاقية بودابست السالفة الذكر إجراءات التفتيش في بيئة الأعمال الإلكترونية، ينظر المادة 19 من الاتفاقية.

وتشترط المادة الأولى الفقرة الرابعة من قانون 04/09 السالف الذكر ان يتم التفتيش بإذن قضائي حيث جاء فيها "لا يجوز إجراء عمليات في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة¹.

ويتوجب على السلطة القائمة على التفتيش والحجز السهر على سلامة المعطيات، ويجوز لها عند الضرورة إستعمال الوسائل التقنية قصد جعلها قابلة للإستعمال لأغراض التحقيق شرط ألا يؤدي ذلك إلى المساس بمضمون هذه المعطيات².

الفرع الثاني: حفظ المعطيات

الزم المشرع مقدمي الخدمات بتقديم المساعدة اللازمة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات عند إجرائها، وبوضع المعطيات التي يتعين عليهم حفظها، ولا يتعلق الأمر بكل المعطيات وإنما يلتزم مقدمو الخدمات بحفظ المعطيات التالية:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة ؛
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال ؛
- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال ؛
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها ؛
- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

أما بالنسبة للنشاطات المتعلقة بالإتصالات الهاتفية فإنه يتوجب على مقدم هذه الخدمة بحفظ المعطيات التالية:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة ؛

¹ - أما إذا تعلق الأمر بالتفتيش الإلكتروني في جرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، فإن الإذن بمنح من طرف النائب العام لدى مجلس قضاء الجزائر... ينظر المادة 4 الفقرة الأخيرة من قانون 04/09 السالف الذكر.

² - ويمكن للجهة القائمة على التفتيش والحجز الاستعانة بالوسائل التقنية المناسبة للحيلولة دون الوصول إلى المعطيات إلى تحتويتها المنظومة المعلوماتية ومنع فسحها أو استعمالها أو الإطلاع عليها أو تحريكها أو إتلافها، وهو ما يستخلص من المادة 7 و8 من قانون 04/09.. ينظر أيضا.. زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهادي عين ميلة الجزائر، 2012، ص 152.

- المعطيات التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه¹. وإلى جانب التزامات مقدمي الخدمات بحفظ البيانات والمعطيات يتوجب عليهم أيضاً تسليم البيانات التي تكون مجوزتهم للسلطات المختصة عند طلبها منهم وأشارت المادة 5 من القانون 04/09 أنه يجوز لسلطة التفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية قصد مساعدتهم وتزويدهم بالمعلومات التي يطلبونها منهم...

الفرع الثالث: التعاون الدولي لمكافحة الارهاب الالكتروني

بالرجوع إلى التشريع الجزائري نجد أن هذا الأخير قد تنبه إلى أهمية التعاون الدولي والمساعدة القضائية الدولية، فسمح في إطار التحريات أو التحقيقات القضائية بخصوص الجرائم الواقعة في بيئة الأعمال الإلكترونية وبالتحديد تلك المتعلقة بأنظمة المعالجة الألية للمعطيات، والتي تعتبر في موضوعنا جرائم واقعة على وسائل ومتطلبات المعاملات التجارية الإلكترونية، سمح للسلطات المختصة بتبادل المساعدة القضائية الدولية بخصوص جمع الأدلة الإلكترونية، بل يمكن في حالة الاستعجال قبول طلبات المساعدة القضائية إذا وردت عن طريق وسائل الإتصال الإلكتروني، وذلك بقدر ما توفره هذه الوسائل من شروط تضمن أمنها وصحتها².

أولاً: تبادل المعلومات ونقل الاجراءات بين الدول

جاء في المادة 17 من قانون 04/09 المتعلق بالوقاية من جرائم تكنولوجيا الاعلام الاتصال أنه تتم الإستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقاً للاتفاقية الدولية ذات الصلة والاتفاقيات الثنائية ومبدأ المعاملة بالمثل.

¹ - غير أن مدة الحفظ غير مطلقة فهي محددة بسنة واحدة ابتداءً من تاريخ التسجيل... ينظر المادة 11 من نفس القانون.

² - وذلك مع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل... ينظر المادة 16 من القانون 04/09 السالف الذكر.

اما فيما يتعلق بنقل الاجراءات ويتم ذلك عن طريق قيام دولة باتخاذ إجراءات جنائية بمناسبة جريمة معينة قد ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة وذلك بناء على إتفاقية مبرمة بينهما¹. وبالرجوع إلى المادة 17 من قانون 04/09 نجد أن المشرع قد أشار إلى هذا الإجراء تحت عنوان تبادل المعلومات واتخاذ الإجراءات التحفظية، وتذكر المادة أن هذا الإجراء يتم وفق للإتفاقيات الدولية ذات الصلة والاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل.

ثانيا: الإنابة القضائية على المستوى الدولي

الإنابة القضائية الدولية هي طلب إحدى الدول من دولة أخرى اتخاذ إجراء من إجراءات الدعوى الجزائية للفصل في مسألة معروضة على السلطة القضائية لدى الدولة صاحبة الطلب²، ومن هذه الإجراءات طلب إجراء التفتيش والضبط والمعاينة، وتتم هذه الإجراءات وغيرها عن طريق إرسال ملف الدعوى ومحاضر الإستدلالات ويكون ذلك عبر القنوات الدبلوماسية بوزارة الخارجية ثم سفارة الدولة متلقية الطلب³.

وقد نظم المشرع إجراءات الإنابة القضائية في المواد 721 و722 من قانون الإجراءات الجزائية حيث جاء في المادة الأولى أنه في حالة المتابعات الجزائية غير السياسية في بلد أجنبي تسلم الإنابات القضائية الصادرة من السلطة الأجنبية بالطريق الدبلوماسي⁴، وتنفيذ الإنابات القضائية وفقاً للقانون الجزائري ومبدأ المعاملة بالمثل.

¹ - حيث نلمس عديد الإتفاقيات التي أقرت هذا النوع من المساعدات كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية واتفاقية الامم المتحدة لمكافحة الجريمة المنظمة سنة 2000، والأمثلة أيضا ما جاء في اتفاقية التعاون القانوني والقضائي لمجلس التعاون الخليجي سنة 2003.

² - ومن هنا تظهر أهمية الإنابة القضائية الدولية إذ تسهل الإجراءات القضائية بين الدول ولذلك لتعذر ممارسة الأعمال القضائية خارج إقليم الدولة علما أن الجرائم الإلكترونية عموما تتطلب هذا النوع من الإجراءات... ينظر، شول بن شهرة، الحماية الجنائية للتجارة الإلكترونية، رسالة دكتوراه، جامعة محمد خيضر بسكرة، ص 380.

³ - ونظرا لبطء القنوات الدبلوماسية فإن الدول عادة ما تبرم اتفاقيات في هذا الشأن حيث يتم ارسال الطلبات مباشرة إلى وزارة العدل.

⁴ - اذا رأت الحكومة الأجنبية في دعوى جنائية تحقق في الخارج أنه من الضروري طلب إرساب أدلة الاثبات أو مستندات توجد تحت يد السلطات الجزائرية..، تقدم طلب عنها بالطريق الدبلوماسي ويحجب هذا الطلب على أن

الخاتمة:

مما سبق يتضح لنا أن العالم دولا وشعوب أصبح أمام تحد كبير، فلم يعد الإرهاب لالالكتروني يقتصر على ما نشاهده من هجمات الكترونية، ومن إساءة استخدام لوسائل التواصل الاجتماعي مثل فيسبوك وتويتر ومدونات ووتس آب وغيرها بل سوف يستحدث ما هو اشد وانكأ ضررا منها، و عليه فإن مكافحة الإرهاب الالكتروني تعد مسؤولية مشتركة تتطلب أعلى درجات التعاون و التنسيق بين الدول، و الاستعداد الكامل لتبادل المعلومات الاستخباراتية والأمنية بأسرع ما يمكن بين الأجهزة المعنية و عبر وسائل آمنة، مع ضرورة تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمواجهة هذا المشكلة وبخاصة الإنتربول لمواجهة كافة أشكال جرائم الإرهاب الالكتروني.

نستنتج من خلال ما سبق أن الإرهاب الالكتروني يشكل تهديدا أمنيا الكترونيا عابرا للحدود، خاصة بزيادة استخدام التكنولوجيا المتطورة في مختلف المجالات، من خلال استخدامها بشكل سلبي من طرف الجماعات الإرهابية وقيامها بهجمات واعتداءات الكترونية على مختلف القطاعات الحيوية للدولة، مما ينتج عنها خسائر فادحة تمس بجميع الميادين خاصة الأمني منها. هذا ما يوجب على المجتمع الدولي اتخاذ كافة التدابير اللازمة لمواجهة هذه الأخطار أو الحد منها.

وفي هذا الإطار يمكننا رصد مجموعة من التوصيات لمواجهة الإرهاب الالكتروني وتحقيق امن واستقرار الدول:

- ضرورة إيجاد تعريف جامع شامل مانع للإرهاب ومن ثم الإرهاب الالكتروني.
- العمل على مواجهة أسباب الإرهاب وتحقيق رفاهية الشعوب عامة والشباب خاصة.
- تطوير تقنيات مراقبة شبكة الانترنت وتعزيز إجراءات الأمن والحراسة للمواقع الرسمية.
- زيادة التكامل التعاون الثنائي والدولي لمكافحة ظاهرة الإرهاب الالكتروني لتسليم المجرمين وتحقيق أمن واستقرار الدول.
- العمل على انشاء جهاز خاص لمواجهة هذه الجرائم
- العمل على تخصص القضاء

تلتزم برد الاوراق والمستندات في أقصر أجل، ذلك ما لم تحل اعتبارات خاصة دون اجابته، ينظر المادة 273 من قانون الاجراءات الجزائية.

قائمة المراجع:

أولاً: الكتب

- 1- رفد عيادة الهاشمي، الإرهاب الإلكتروني. بدون دار النشر، بدون بلد، بدون سنة، بدون طبعة.
- 2- زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهادي عين ميله الجزائر، 2012،
- 3- شول بن شهرة، الحماية الجنائية للتجارة الإلكترونية، رسالة دكتوراه، جامعة محمد خيضر بسكرة.

ثانياً: المجلات العلمية

- 2- سليمان مبارك، الإرهاب الإلكتروني و طرق مكافحته، جامعة خنشلة، العدد: 08 ج / 01 جوان. 2017.

ثالثاً: المداخلات

- 1- عمارة. عمارة التدابير الوقائية والجزائية من جريمة تبييض الأموال وتمويل الارهاب، الملتقى الوطني الثالث حول الجريمة المنظمة وسياسة مكافحتها في الجزائر، جامعة مسيلة
- 2- بوحادة سارة، أثر الإرهاب الإلكتروني على أمن واستقرار الدول، المدرسة الوطنية العليا للعلوم لسياسية - الجزائر.

رابعاً- مواقع الكترونية

- 1- أيمن حسين، "الإرهاب الإلكتروني أخطر معارك حروب الفضاء": من الموقع: تم تصفحه يوم 2018-12-28 على الساعة 12:14 <http://alwatan.com/details/166324> تاريخ النشر: 2017/01/14.
- 2- إيهاب شوقي، الإرهاب الإلكتروني و جرائمه، من الموقع: <http://www.anntv.tv/new/showsubject.aspx?id=121062> (د.ت.ن) تم تصفحه يوم يوم 2018-12-27 على الساعة 18.30.
- 3- عبد الرحمن بن عبد الله السند، وسائل الإرهاب الإلكتروني وحكمها في الإسلام وطرق مكافحتها من الموقع: <http://shamela.ws/browse.php/book-1244/page-20> (د.ت.ن) تم تصفحه يوم 2018-12-27 على الساعة 12.45.

4- حسن بن سعيد بن سيف الغافري، الإرهاب الإلكتروني. من الموقع:

http://www.ita.gov.om/ITAPortal_AR/Pages/Page.aspx?NID=1&PID=9&LID=5

،(د.ت.ن)، تم تصفحه يوم 28-12-2108، على الساعة 13.30.

5- شيريهان نشأت المنيري، "مخاطر جرائم الانترنت على استقرار النظام الدولي"، مجلة السياسة الدولية، من الموقع:

<http://www.siyassa.org.eg/NewsQ/2450.aspx>،(د.ت.ن) تم تصفحه يوم،
2017-02-01. على الساعة 09.56.

مواجهة جريمة الإرهاب الالكتروني في ظل القانون رقم 16 - 02 المتتم للأمر رقم 66 - 156 المتضمن قانون العقوبات

د/ مسعودان فتيحة

كلية الحقوق والعلوم السياسية- جامعة بجاية

مقدمة:

ساهمت الثورة التكنولوجية الحديثة في تجاوز الحدود وتقريب المسافات وزيادة حرية التواصل بين الشعوب وتسهيل الحصول على الخدمات وغير ذلك من الانعكاسات الايجابية، غير أنّ لهذه الثورة التكنولوجية آثارا سلبية حيث أدت التطورات التكنولوجية التي يشهدها العالم اليوم في كل مجال إلى ظهور ما يسمى بالجريمة المعلوماتية، والتي تتخذ عدّة صور من بينها جريمة الإرهاب الالكتروني، والتي تعتبر من الجرائم الخطيرة التي تهدد سلامة العالم وسلامة الدولة وكيانها.

ومنه لم تعد الدول تقتصر على محاربة الإرهاب في صورته التقليدية والتي لا تزال موجودة إلى يومنا هذا، وإتّما كان لزاما عليها العمل من أجل محاربة جريمة الإرهاب الالكتروني، حيث سعت جل الدول إلى تكريس مثل هذه السياسة في قوانينها ومن بينها القانون الجزائري، حيث كرست ذلك بموجب تعديل قانون العقوبات سنة 2016 بإدراج بعض المواد تناولت الإرهاب الالكتروني ومنه نطرح السؤال الآتي: كيف عالج المشرع الجريمة جريمة الإرهاب الالكتروني في ظل القانون رقم 16 - 02 المتتم للأمر رقم 66 - 156 والمتضمن قانون العقوبات؟.

وللإجابة على الإشكال المطروح تم تقسيم موضوع الدراسة إلى محورين: المحور الأول نتعرض فيه لتعريف الإرهاب الالكتروني، والمحور الثاني ندرس فيه مظاهر وصور جريمة الإرهاب الالكتروني والعقوبات المقررة لها وفقا للقانون رقم 16 - 02.

المحور الأول: تعريف الإرهاب الالكتروني

تستدعي دراسة جريمة الإرهاب الالكتروني التطرق أولا لتعريف الإرهاب الالكتروني، فنتطرق من خلال هذا المحور إلى تعريف فقهاء القانون للإرهاب الالكتروني (فقرة أولى) وتعريف المشرع الجزائري للإرهاب الالكتروني (فقرة ثانية).

الفقرة الأولى: تعريف فقهاء القانون للإرهاب الإلكتروني

عرّف فقهاء القانون الإرهاب الإلكتروني بعدّة تعاريف نذكر بعضها في الآتي:

- لإرهاب الإلكتروني هو خرق للقانون يقدم عليه فرد من الأفراد، أو تنظيم جماعي بهدف إثارة اضطراب خطير في النظام العام عن طريق شبكات المعلومات العالمية للانترنت⁽¹⁾.
 - الإرهاب الإلكتروني هو الاستخدام العدائي و العدواني غير المشروع للانترنت بهدف ترهيب الحكومة و المدنيين أو قسم من هم في إطار السعي إلى تحقيق أهداف سياسية أو اجتماعية⁽²⁾.
 - الإرهاب الإلكتروني هو الاستخدام غير الأمثل للشبكة العالمية بما يؤدي إلى ترهيب المواطنين بشكل خطير أو يسعى إلى زعزعة الأمن والاستقرار أو تفويض المؤسسات السياسية أو الدستورية أو الاقتصادية أو الاجتماعية لأحدى الدول أو المنظمات الدولية في إطار السعي إلى تحقيق أهداف سياسية أو اجتماعية⁽³⁾.
 - الإرهاب الإلكتروني هو العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق بشتى صنوفه وصور الإفساد في الأرض⁽⁴⁾.
 - الإرهاب الإلكتروني هو اعتداء على شخص ما وإصابته بأذى فعلي أو ذعر أو تهديد، فمن الممكن اقتحام صفحة المستشفيات وتهديد حياة المرضى عن طريق تغيير برنامج العلاج، وتهديد الاقتصاد باقتحام مواقع البورصة العالمية كما يمكن أيضا التدخل في نظام الاتصالات كالكهرباء والمياه، بل والسيطرة على نظام المواصلات والطائرات وبذلك تهديد بلد بأكملها وشبكات الأمن و إغلاقها⁽⁵⁾.
- يستشف من خلال التعريفات المذكورة آنفا أن الإرهاب الإلكتروني لا يكاد يختلف في مضمونه وجوهره عن الإرهاب بصورة عامة من حيث القصد الجرمي للجاني ما عدا طريقة تنفيذ الفعل أو العمل الإرهابي، فالإرهاب في صورته التقليدية يكون عن طريق استعمال العنف والقوة الفعلية ممثلة بالأسلحة النارية والمتفجرات وغيرها من صور الأعمال الإرهابية الأخرى، أما الإرهاب الإلكتروني فيكون عن طريق استخدام شبكة الانترنت للوصول إلى الأهداف التي يسعى إليها الإرهابي لتجنيد الأشخاص للانحياز مع الجماعات أو العناصر الإرهابية أو نشر الدعاية لتلك الجماعات المسلحة أو التعرض للقيام بعمليات مسلحة ضد الدولة أو ضد جماعات معينة⁽⁶⁾.

حيث استغلت المجموعات الإرهابية التطور الكبير الذي حققته تكنولوجيا المعلومات وشبكة الانترنت في أعمالها الإرهابية من خلال الولوج إلى المعلومات الحكومية والتأثير فيها لتحقيق أهدافها وإيديولوجيتها العدائية الأمر الذي أدى إلى زيادة عدد الأصوات المطالبة بمكافحة الإجرام عبر الانترنت، وهو ما تحقق سنة 2001 عندما أبرمت اتفاقية بودابست الأولى لمكافحة الإجرام عبر الانترنت⁽⁷⁾.

والإرهاب الإلكتروني يهدف إلى تحقيق جملة من الأهداف غير مشروعة تتمثل في نشر الخوف والرعب بين الأشخاص والدول والشعوب المختلفة، الإخلال بالنظام العام والأمن المعلوماتي وزعزعة الطمأنينة، تعريض سلامة المجتمع وأمنه للخطر، إلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها و الإضرار بوسائل الاتصالات وتقنية المعلومات أو بالأموال والمنشآت العامة والخاصة، تهديد السلطات العامة والمنظمات الدولية وابتزازها، الانتقام من الخصوم، الدعاية و الإعلان وجذب الانتباه وإثارة الرأي العام، وجمع الأموال والاستيلاء عليها⁽⁸⁾.

الفقرة الثانية: تعريف المشرع الجزائري للإرهاب الإلكتروني

المشرع الجزائري لم يعرف الإرهاب الإلكتروني إلا أنه قام بتعريف فعل الإرهاب وكذلك جريمة تمويل الإرهاب حيث عرف الإرهاب بموجب المادة 87 مكرر من الأمر رقم 95 - 11 المؤرخ في 25 فيفري 1995 المعدل والمتمم للأمر رقم 66 - 156 المتضمن قانون العقوبات، حيث نصت المادة السالفة الذكر على أنه: " يعتبر فعلا إرهابيا أو تخريبيا، في مفهوم هذا الأمر، كل فعل يستهدف أمن الدولة والوحدة الوطنية والسلامة الترابية واستقرار المؤسسات وسيرها العادي عن طريق أي عمل غرضه ما يأتي:

- بث الرعب في أوساط السكان وخلق جو انعدام الأمن من خلال الاعتداء المعنوي أو الجسدي على الأشخاص أو تعريض حياتهم أو حريتهم أو أمنهم أو المس بممتلكاتهم،
- عرقلة حركة المرور أو حرية التنقل في الطريق و التجمهر أو الاعتصام في الساحات العمومية
- الاعتداء على رموز الأمة والجمهورية ونش أو تدنيس القبور،

- الاعتداء على وسائل المواصلات والتنقل والملكيات العمومية والخاصة والاستحواد عليها أو احتلالها دون مسوغ قانوني،
- الاعتداء على المحيط أو إدخال مادة أو تسريبها في الجو أو في الباطن أو إلقاءها عليها أو في المياه بما فيها المياه الإقليمية من شأنها جعل صحة الإنسان أو الحيوان أو البيئة الطبيعية في خطر،
- عرقلة عمل السلطات العمومية أو حرية ممارسة العبادة والحريات العامة وسير المؤسسات المساعدة للمرفق العام،
- عرقلة سير المؤسسات العمومية أو الاعتداء على حياة أعوانها أو ممتلكاتهم أو عرقلة تطبيق القوانين والتنظيمات⁽⁹⁾.

فالمشرع الجزائري قد عرّف بموجب هذه المادة المقصود من الإرهاب وما هي صوره وحالته إلا أنّه لم يتطرق إلى ذكر الإرهاب الإلكتروني، إلّا أنّ ما يمكن قوله وهو إسقاط هذه المادة على الإرهاب الإلكتروني بمعنى أنّه كلما ارتكبت هذه العمليات بواسطة وسيلة نكون أمام جريمة الإرهاب الإلكتروني، حيث تختلف فقط الجريمة من حيث طريقة ارتكابها.

أما جريمة تمويل الإرهاب فقد عرّفها المشرع الجزائري في المادة 3 من القانون رقم 05 - 01 والتي تنص: " تعتبر جريمة تمويل للإرهاب، في مفهوم هذا القانون، كل فعل يقوم به كل شخص بأية وسيلة كانت، مباشرة أو غير مباشرة، وبشكل غير مشروع وبإرادة الفاعل، من خلال تقديم أو جمع الأموال بنية استخدامها كلياً أو جزئياً، من أجل ارتكاب الجرائم الموصوفة بأفعال إرهابية أو تخريبية، المنصوص عليها بالمواد 87 مكرر إلى 87 مكرر 10 من قانون العقوبات⁽¹⁰⁾.

إضافة إلى ما ذكرته المادة السالفة الذكر يمكن أن تتم عملية تمويل الإرهاب دون علم ورغبة الممول حيث من خلال الشبكة المعلوماتية العالمية وعن طريق الاستعانة ببيانات إحصائية سكانية منتقاة من المعلومات الشخصية التي يدخلها المستخدمون على الشبكة المعلوماتية من خلال الاستفسارات والاستطلاعات الموجودة على المواقع الإلكترونية يقوم الإرهابيون بالتعرف على الأشخاص ذوي المشاعر الرقيقة والقلوب الرحيمة ومن ثم يتم استجداؤهم لدفع تبرعات مالية لأشخاص اعتباريين يكونون واجهة لهؤلاء، ويتم ذلك بواسطة رسائل البريد الإلكتروني أو من خلال ساحات الحوار

الالكترونية، بطريقة ذكية وأسلوب مخادع، إذ لا يشك المتبرع بأنه سيساعد أحد التنظيمات الإرهابية⁽¹¹⁾.

وفي سبيل تحقيق العصابات الإرهابية مشاريعها وأهدافها تستخدم الجماعات والمنظمات الإرهابية الشبكة المعلوماتية العالمية في نشر ثقافة الإرهاب والترويج لها وبت الأفكار الفلسفات التي تنادي بها، كما تسعى جاهدة إلى توفير أكبر عدد ممكن من الراغبين في تبني أفكارها ومبادئها ومن خلال الشبكة المعلوماتية تقوم التنظيمات الإرهابية بتكوين قاعدة فكرية لدى من لديهم ميول واستعداد للانخراط في الأعمال التدميرية والتخريبية مما يوفر لديها قاعدة ممن تجمعهم الأفكار والتوجهات نفسها فيسهل تجنيدهم لتنفيذ هجمات إرهابية يحافظ على بقائها واستمرارها فيجذبونهم بأسلوب عاطفي وعبارات حماسية براقية، وذلك من خلال غرف الحوار والمنتديات والمواقع الالكترونية⁽¹²⁾.

كما يمكن تعريف جريمة تمويل الإرهاب وفقا لما ذكرته المادة 3 من القانون رقم 15 - 06 والمتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب حيث نصت المادة السالفة الذكر على أنه: "يعتبر مرتكبا لجريمة تمويل الإرهاب ويعاقب بالعقوبة المقررة في المادة 87 مكرر 4 من قانون العقوبات، كل من يقدم أو يجمع أو يسير بإرادته، بطريقة مشروعة أو غير مشروعة، بأي وسيلة كانت، بصفة مباشرة أو غير مباشرة، أموالا بغرض استعمالها شخصا، كليا أو جزئيا، لارتكاب أو محاولة ارتكاب جرائم موصوفة بأفعال إرهابية أو مع علمه أو علمه بأنها ستستعمل..."⁽¹³⁾.

المحور الثاني: مظاهر وصور جريمة الإرهاب الالكتروني والعقوبات المقررة لها وفقا للقانون رقم 16-

02

لجريمة الإرهاب الالكتروني مجموعة من المظاهر والصور، وهو ما نراه في الفقرة الأولى من هذا المحور، كما يترتب على الجريمة السابقة الذكر مجموعة من العقوبات قد تطرق إليها المشرع الجزائري بموجب تعديل قانون العقوبات بالقانون رقم 16 - 02 وهو ما نتعرض له في الفقرة الثانية من هذا المحور.

الفقرة الأولى: مظاهر وصور جريمة الإرهاب الالكتروني وفقا للقانون رقم 16 - 02

تستنتج من خلال تحليل المواد 87 مكرر 11 والمادة 87 مكرر 12 والمادة 394 مكرر 8 من القانون رقم 16 - 02 بعض الصور والمظاهر التي تكيف على أنها جريمة إرهاب الكتروني وتتمثل في الآتي:

أولا: ارتكاب أفعال إرهابية أو تديرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها

تأتي جريمة الإرهاب الإلكتروني في عدّة صور ومن بينها ارتكاب الفعل الإرهابي أو التدبير له أو التدريب على ارتكابه أو المشاركة في ارتكابه، حيث يعاقب كل من قام بارتكاب فعل من الأفعال المذكورة سواء كان مرتكب الجريمة جزائري أو أجنبي مقيم في الجزائري بطريقة شرعية أو غير شرعية وكان ارتكابها ذلك باستخدام تكنولوجيات الإعلام والاتصال بالعقوبة المقررة للإرهاب الإلكتروني⁽¹⁴⁾.

ثانيا: السفر أو محاولة السفر من أجل ارتكاب الأفعال الإرهابية المذكورة في الفقرة الأولى من المادة 87 مكرر 11

وتعتبر جريمة إرهاب الكتروني كل شخص جزائري أو أجنبي مقيم في الجزائر بصورة شرعية أو غير شرعية يسافر أو يحاول السفر إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها⁽¹⁵⁾.

ثالثا: توفير أو جمع أموالا في تمويل سفر أشخاص للقيام بأعمال إرهابية

يعتبر من مظاهر أو من صور الإرهاب الإلكتروني توفير أو جمع الأموال بصورة عمدية وبأية وسيلة كانت وسواء كان ذلك بصورة مباشرة أو غير مباشرة بقصد استعمالها أو مع علمه بأنّها ستستخدم في تمويل سفر أشخاص إلى دولة أخرى بهدف ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها⁽¹⁶⁾.

كما تعتبر أيضا القيام بصورة عمدية بتنظيم أو تمويل سفر أشخاص إلى دولة أخرى ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها أو تسهيل ذلك السفر مظهر من مظاهر الإرهاب الإلكتروني⁽¹⁷⁾.

رابعا: استخدام تكنولوجيات الإعلام والاتصال في تجنيد الأشخاص لتحقيق أعمال إرهابية

يعتبر من جرائم الإرهاب الإلكتروني وفقا لقانون العقوبات الجزائري استخدام تكنولوجيات الإعلام والاتصال في سبيل تجنيد أشخاص لصالح إرهابي، أو جمعية، أو تنظيم، أو جماعة، أو منظمة يكون الغرض منها أو تقع أنشطتها تحت أعمال إرهابية وفقا لقانون العقوبات المعدل سنة 2016 أو ينظم شؤونها، أو يدعم أعمالها أو أنشطتها، أو ينشر أفكارها بصورة مباشرة أو غير مباشرة⁽¹⁸⁾.

حيث تجند الجماعة الإرهابية من خلال الانترنت عناصر إرهابية جديدة تساعدهم على تنفيذ أعمالهم الإرهابية، وهم في ذلك يعتمدون على فئة الشباب خصوصا ضعاف العقل والفكر فتعلن

الجماعة الإرهابية عبر مواقعها على الانترنت حاجتها إلى عناصر انتحارية كما لو كانت تعلن عن وظائف شاغرة للشباب، مستخدمة في ذلك الجانب إلى الجهاد وحثهم إلى الاستشهاد في سبيل الفوز بالجنة⁽¹⁹⁾.

فالمواقع الالكترونية تتيح للجماعات الإرهابية قدرا كبيرا من التحكم في المعلومات والرسائل الإعلامية التي تريد توجيهها، وتتيح لها مرونة توجيه الرسائل لفئات من الجمهور المستهدف، ورسم صورة ذهنية عن الجماعة وعن أعدائها⁽²⁰⁾.

وإضافة إلى الصور المذكورة أضاف المشرع الجزائري صورة أخرى تعتبر مظهرا من المظاهر المعاقب عليها بصدد جرائم الإرهاب الالكتروني، وهي معاقبة مقدمو خدمات الانترنت في حالة الامتناع رغم اعذارهم من طرف الهيئة الوطنية المكلفة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته أو عن طريق صدور أمر أو حكم قضائي عن التدخل الفوري لسحب أو تخزين المحتويات التي يتيح الاطلاع عليها أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا، أو الامتناع عن وضع ترتيبات تقنية تسمح بسحب أو تخزين المحتويات التي تتعلق بجرائم الإرهاب المنصوص عليها قانونا أو لجعل الدخول إليها غير ممكن⁽²¹⁾.

الفقرة الثانية: العقوبات المقررة لجريمة الإرهاب الالكتروني وفقا للقانون رقم 16 - 02

تترتب على جريمة الإرهاب الالكتروني مجموعة من الآثار منها توقيع العقوبة على مرتكبيها، وتحليل مواد قانون رقم 16 - 01 المتمم لقانون العقوبات يتبين أنّ العقوبات المقررة لجرائم الإرهاب الالكترونية تتراوح ما بين العقوبات السالبة للحرية والغرامة المالية، وهذا ما سنراه من خلال هذه الفقرة في الآتي:

أولاً: السجن المؤقت

كل جزائري أو أجنبي مقيم بالجزائر، بطريقة شرعية أو غير شرعية، يسافر أو يحاول السفر إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو تديرها أو الأعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها، و كل من يوفر أو يجمع عمدا أموالا بأي وسيلة وبصورة مباشرة أو غير مباشرة بقصد استخدامها أو مع علمه بأنها ستستخدم في تمويل سفر أشخاص إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو تديرها أو الأعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها، وكل من قام عمدا بتمويل أو تنظيم سفر أشخاص إلى دولة أخرى بغرض

ارتكاب أفعال إرهابية أو تديرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو تلقي تدريب عليها أو تسهيل ذلك السفر، وكان ارتكاب الأفعال المذكورة باستخدام تكنولوجيات الإعلام والاتصال لارتكاب الأفعال السالفة الذكر، بالسجن المؤقت من خمس (5) سنوات إلى عشر (10) سنوات، وهو ما نصت عليه المادة 87 مكرر 11 من القانون 16 - 02.

ويعاقب بنفس العقوبة مستخدم تكنولوجيات الإعلام والاتصال من أجل تجنيد الأشخاص لصالح إرهابي أو جمعية أو منظمة يكون غرضها أو تقع أنشطتها تحت طائلة أحكام هذا القسم أو ينظم شؤونها أو يدعم أعمالها أو أنشطتها أو ينشر أفكارها بصورة مباشرة أو غير مباشرة، وهو ما نص عليه المشرع الجزائري بموجب المادة 87 مكرر 12 من القانون رقم 16 - 02.

ثانيا: عقوبة الحبس

يمكن التوقيع بصدد جرائم الإرهاب الإلكتروني بعقوبة الحبس وهي عقوبة مقررة لمقدمي خدمات الانترنت، حيث عرفت المادة 2 فقرة د من القانون رقم 09 - 04 مقدمو خدمات الانترنت على أنهم أي كيان كان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و أو نظام للاتصالات أو أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعملها" (22).

فمقدم خدمات الانترنت الذي لا يقوم رغم اعذاره من الهيئة الوطنية المكلفة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، أو صدور أمر، أو حكم قضائي بالتدخل الفوري بسحب أو تخزين المحتويات التي يتيح الاطلاع عليها، أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا أو بوضع ترتيبات تقنية تسمح بسحب أو تخزين المحتويات التي تتعلق بالجرائم المنصوص عليها قانونا أو لجعل الدخول إليها غير ممكن قانونا، يعاقب بالحبس من سنة إلى ثلاثة سنوات (23).

ثالثا: الغرامة المالية

إضافة إلى توقيع العقوبة على الشخص المرتكب لجريمة الإرهاب الإلكتروني بسلب حريته بالحكم عليه بالسجن المؤقت والحبس المؤقت، يمكن علاوة على ذلك أن يقوم القاضي بالحكم على المجني بغرامة مالية تتراوح بين 100.000 دج إلى 5000.000 دج، وهذه العقوبة توقع على كل جزائري أو أي شخص أجنبي مقيم بالجزائر سواء بطريقة شرعية أو غير شرعية يسافر أو يحاول

السفر إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو الإعداد لها أو التدريب على ارتكابها أو لتلقي تدريب عليها أو تديرها أو المشاركة فيها، كما تطبق أيضا على كل من قام عمدا بتمويل أو تنظيم سفر أشخاص إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو تديرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو تلقي تدريب عليها أو تسهيل السفر من أجل القيام بها، كما تطبق على كل من يوفر أو يجمع عمدا أموالا بأي وسيلة وبصورة مباشرة أو غير مباشرة بقصد استخدامها أو مع علمه بأنها ستستخدم في تمويل سفر أشخاص إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو الإعداد لها أو التدريب على ارتكابها أو لتلقي تدريب عليها أو تديرها أو المشاركة فيها، وعلى كل من يستخدم تكنولوجيات الإعلام والاتصال لتجنيد الأشخاص لصالح إرهابي أو جمعية أو منظمة يكون غرضها أو تقع أنشطتها تحت طائلة أحكام هذا القسم أو ينظم شؤونها أو يدعم أعمالها أو أنشطتها أو ينشر أفكارها بصورة مباشرة أو غير مباشرة" (24).

وقد تكون العقوبة المالية تتراوح من 2.000.000 دج إلى 10.000.000 دج، وتطبق هذه العقوبة على مقدمي خدمات الانترنت الذين يمتنعون عن القيام بالتدخل الفوري بسحب أو تخزين المحتويات التي يتيح الاطلاع عليها أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا، أو الامتناع عن وضع ترتيبات تقنية تسمح بسحب أو تخزين المحتويات التي تتعلق بالجرائم المنصوص عليها قانونا أو لجعل الدخول إليها غير ممكن رغم اعذارهم من طرف الهيئة الوطنية المكلفة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، أو صدور أمر أو حكم قضائي يلزمه بذلك وهو ما نصت عليه المادة 394 مكرر 8 من القانون رقم 16 - 02 (25).

خاتمة:

تعتبر جريمة الإرهاب الإلكتروني من الجرائم الخطيرة التي تهدد أمن الدولة وسلامتها وحتى الأمن العالمي، وجريمة الإرهاب لم تعد تعتمد على الأسس التقليدية فقط، وإنما ظهر إلى الواقع ما يعرف بالإرهاب الإلكتروني أين تتم العمليات الإرهابية بمختلف صورها عن طريق وسائل الإعلام والاتصال، ما دفع بالدول الاهتمام بمثل هذه الجريمة بعقد العديد من المؤتمرات والاتفاقيات، وهو ما دفع التشريعات الوطنية الانتباه إلى مثل هذه الجريمة وإدراجها ضمن قوانينها الداخلية مثلما عليه

المشرع الجزائري، حيث تطرق إلى مثل هذه الجريمة بموجب القانون رقم 16 - 02 ومنه توصلنا إلى مجموعة من النتائج والتوصيات نتطرق لها في الآتي:

أولا: النتائج

1. رغم المحاولات العديد من طرف أساتذة القانون لوضع تعريف للإرهاب الإلكتروني فضلا عن محاولة بعض المنظمات الدولية والإقليمية لكن هذه الجهود لم تنجح في وضع تعريف محدد له إذ لا يوجد حتى اليوم تعريف متفق عليه دوليا للإرهاب الإلكتروني لا بل حتى الإرهاب التقليدي، وذلك لأسباب تتعلق بتباين المصالح واختلاف المعايير والقيم بين الدول.
2. يعتبر الإرهاب الإلكتروني هاجسا يخيف العالم ولذلك سعت العديد من الدول إلى اتخاذ التدابير والإحترازا لمواجهة الإرهاب الإلكتروني ومن بينها الدولة الجزائرية، إلا أنّ هذه الجهود قليلة ولا تزال بحاجة إلى المزيد من الجهود المبذولة لمواجهة هذا السلاح الخطير.
3. يتميز الإرهاب الإلكتروني من غيره من أنواع الإرهاب بالطريقة العصرية المتمثلة في استخدام الموارد المعلوماتية والوسائل الإلكترونية التي جلبتها الحضارة التقنية في عصر المعلومات، لذا فإن الأنظمة الإلكترونية والبنية التحتية المعلوماتية هي هدف الإرهابيين.
4. إنّ توظيف الدول والحكومات للتكنولوجيا في محاربة الإرهاب يوازيه توظيف الإرهاب نفسه لذات التكنولوجيا في استهداف مواقع ذات الدول والحكومات سواء بسواء أو بدرجات متفاوتة تفاوت الاحتكام على هذه التكنولوجيا وتفاوت القدرة على توظيفها.
5. قلة النصوص القانونية الحديثة التي تواجه كافة الجرائم المعلوماتية، غير أنّ هذا لا يجب أن يؤدي إلى بقاء المحقق الجنائي وأسلوب التحقيق جامدا، وإثما وجب أن يتطور ويتمشى مع ما يتناسب مع هذه الجرائم من أجل مواجهتها.

ثانيا: التوصيات

1. ضرورة التدخل التشريعي لمواجهة القصور في التشريعات والقوانين الحالية في مواجهة مشكلة الإرهاب الإلكتروني.
2. تأهيل القائمين على أجهزة تنفيذ القانون لتطوير معلوماتهم في مجال تكنولوجيا المعلومات من خلال تدريب القائمين بالضبط والخبراء وسلطات التحقيق والقضاة وتأهيلهم على التعامل مع هذا النوع من الأدلة في الإثبات وتقديرها حتى يتم التمكن من ضبط الدليل.

3. حث الدول للإسراع بالانضمام إلى الاتفاقيات الدولية الخاصة بمكافحة جرائم الإرهاب عبر الإنترنت.
4. فرض الدولة رقابة كافية دون المساس بالحقوق في الخصوصية لمنع الدخول على بعض المواقع التي تبث الفكر الإرهابي والتي تتناسب مع المجتمع العصري من خلال اقتراح إنشاء برنامج على الحاسب أو تصميمه.

قائمة المراجع:

1. محمد عبد الله منشاوي، جرائم الإنترنت من منظور شرعي وقانوني، مطبعة جامعة الملك فهد، الرياض، 1423 هـ، ص.11.
2. ذياب البدانية، جرائم الحاسب الدولية، بحث مقدم إلى أكاديمية نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 1998، ص.22.
3. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي والانترنت، الهيئة العربية للدراسات الأمنية والتدريب، الرياض، المملكة العربية السعودية، 1422 هـ، ص.22.
4. بالكر محمد، ن مرزوق عنتر، "البعد الإلكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب"، مجلة العلوم الاجتماعية و الإنسانية، جامعة الجزائر 1، المجلد 9، العدد 1، 2018، ص.33.
5. محمد مهد الألفي، تشريعات مكافحة جرائم الإرهاب الإلكتروني، الأحكام الموضوعية و الأنماط، ص.11.
6. إسراء طارق جواد كاظم الجابري، جريمة الإرهاب الإلكتروني، دراسة مقارنة، جزء من متطلبات الحصول على شهادة الماجستير في القانون العام، كلية الحقوق، جامعة النهدين، ص.24.
7. فرانك بولتز، أسس مكافحة الإرهاب، ترجمة: هشام الحناوي، المكتب العربي للمعارف، القاهرة، ص.216.
8. عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، المنعقد بالقاهرة في المدة من 2 - 4 يونيو، 2008، ص.76.

9. أمر رقم 95 - 11 مؤرخ في 25 رمضان 1415 الموافق 25 فبراير 1995 يعدل ويتمم الأمر رقم 66 - 156 المؤرخ في 8 يونيو 1966 والمتضمن قانون العقوبات، ج.ر.ع.11، مؤرخة في 29 رمضان 1415 هـ.
10. قانون رقم 05 - 01 مؤرخ في 27 ذي الحجة 1425 هـ الموافق 6 فبراير 2005، يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، ج.ر.ع.11، مؤرخة في 30 ذي الحجة 1425 هـ الموافق 9 فبراير 2005م.
11. صالح السدلان، أسباب الإرهاب والعنف والتطرف، دار روز للطباعة، الجزائر، 1999، ص.104.
12. محمد المتولي، التخطيط الاستراتيجي في مكافحة الإرهاب، مطابع جامعة الكويت، 2008، ص. 300.
13. قانون رقم 15 - 06 مؤرخ في 25 ربيع الثاني 1436 هـ الموافق 15 فبراير 2015 م، يعدل ويتمم القانون رقم 05 - 01 المؤرخ في 27 ذي الحجة 1425 الموافق 6 فبراير 2005 والمتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، ج.ر.ع.8 مؤرخة في 25 ربيع الثاني 1436 هـ الموافق 25 فبراير 2015م.
14. أنظر المادة 87 مكرر 11 من القانون رقم 16 - 02، قانون رقم 16 - 02 مؤرخ في 14 رمضان 1437 هـ الموافق 19 يونيو 2016 م، يتمم الأمر رقم 66 - 156 المؤرخ في 18 صفر 1386 هـ الموافق 8 يونيو 1966 م والمتضمن قانون العقوبات، ج.ر.ع.4 مؤرخة في 17 رمضان 1437 هـ الموافق 22 يونيو 2016م.
15. أنظر المادة 87 مكرر 2/11 من القانون رقم 16 - 02، المرجع السابق.
16. أنظر المادة 87 مكرر 11، المرجع نفسه.
17. أنظر المادة 87 مكرر 12، المرجع نفسه.
18. محمد سيد سلطان، قضايا قانونية في أمن المعلومات وحماية البيئة الالكترونية، دار ناشري للنشر الالكتروني، 2004، ص.13.
19. محمد سيد سلطان، قضايا قانونية في أمن المعلومات وحماية البيئة الالكترونية، دار ناشري للنشر الالكتروني، 2004، ص.13.

- Debray Stéphan, internet face aux substances illicites: 20. complice de la cyber criminalité ou outil de prévention ?, DESS média électronique & internet, Université de paris, 8.2002-2003, p 13.
21. أنظر المادة 394 مكرر 8 من القانون رقم 16 - 02، المرجع السابق.
22. القانون رقم 09 - 04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ع. 47. مؤرخة في 25 شعبان 1430 هـ الموافق 16 غشت 2009 م.
23. أنظر المادة 394 مكرر 8 من القانون رقم 16 - 02، المرجع السابق.
24. أنظر المادة 87 مكرر 11، المرجع نفسه.
25. أنظر المادة 394 مكرر 8، المرجع نفسه.

صعوبات الإثبات الجنائي في الجريمة المعلوماتية

د/ الطيب بلواضح

أستاذ محاضر (أ) - كلية الحقوق والعلوم

السياسية- جامعة المسيلة

ط.د/ الذهبي خليفة

كلية الحقوق والعلوم السياسية

جامعة المسيلة

مقدمة:

لا شك أن المتغيرات الجديدة التي يشهدها العالم الحديث كالعولمة و التطور السريع في مجال التكنولوجيا وفي أنظمة المعلومات وشبكات الاتصالات المختلفة، صاحبها بعض المشكلات الأمنية الخطيرة من ذلك ظهور ما يسمى بالإجرام المعلوماتي، فرغم ما توفره هذه التقنيات الحديثة من تسهيلات إلا أن لها الأثر الكبير في تمهيد الطريق إلى بروز أشكالاً جديدة من الجرائم، لا سيما بعد ربط هذه الأجهزة المتطورة بالشبكة العالمية للانترنت التي تخوّل للمجرم التقنية العالية والأسلوب الحديث الذي يساعده للقيام بالجريمة دون أن يترك أثراً لفعليته التي قد يقع ضحيتها العديد من الأفراد في عدة مناطق مختلفة من هذا العالم وفي وقت وجيز.

و تعتبر الجريمة المعلوماتية ظاهرة حديثة تنفذ بعدة أساليب تتطور وتتغير بتطور التقنيات والتكنولوجيا إلى أن وصلت لما هي عليه اليوم بحيث أصبحت تشكل خطراً محدقاً على الدول والأفراد لذلك فقد أصبح هذا الموضوع من المسائل الأكثر اهتماماً من طرف المشرعين نظراً للخطورة الناجمة عن هذه الظاهرة وما تسببه من مضار على المستوى السياسي والاقتصادي والاجتماعي.

إن ثورة الاتصالات وتكنولوجيا المعلومات إقترنت بظهور هذه الظاهرة الإجرامية الجديدة التي تتميز عن السلوك الإجرامي التقليدي من عدة أوجه لا سيما وأنها ترتكب من مجرم معلوماتي يوصف بالسرعة والدكاء والمهارة من جهة، كما أنها في حد ذاتها تعتبر جريمة سريعة التنفيذ ومتطورة بتطور الوسائل التكنولوجية المستعملة في ارتكابها.

كل ذلك جعل حصر هذه السلوكيات وتجريمها عملاً مضنياً لا سيما في ظل التشريعات الجزائية التقليدية التي أثبتت عجزها عن مواكبة ملاحقة وتجريم هذه الظواهر المستحدثة.

وهو الأمر الذي يستوجب على المشرع ذكاء خارقا يفوق ذكاء هؤلاء المجرمين ودقة متناهية في تشريع النصوص العقابية الرادعة لمثل هؤلاء الجناة كل ذلك في إطار احترام مبدأ الشرعية العقابية والإجرائية واحترام الاتفاقيات والمعاهدات الدولية في هذا الشأن.

و من هذا المنطلق سعى المشرع الجزائري لمكافحة هذه الجريمة، وتجسد ذلك بوضوح من خلال التطرق للجريمة المعلوماتية في عدة نصوص قانونية من ذلك ما ورد في قانون العقوبات من مواد تتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات ثم التعديلات الأخيرة التي وردت في إطار القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، إضافة إلى مصادقة الجزائر وانضمامها لعدة اتفاقيات دولية تعاونية بهدف مكافحة هذه الاشكال من الجرائم.

إن ما يميز هذه الجرائم أنها غير ملموسة كما أنها قد تحدث من أي مكان سواء داخل اقليم الدولة أو خارجه لذلك فإن أهم الصعوبات التي تواجهها الانظمة الامنية أو القضائية هي مسألة اثبات هذه الجريمة، خاصة وان القواعد التقليدية المعروفة في الاثبات الجنائي لم تعد مجدية لإثبات هذا النوع الجديد من الاجرام.

ومن هذا المنطلق ارتأينا معالجة موضوع الاثبات الجنائي في الجريمة المعلوماتية لما له من أهمية في التأكد من وقوع هذه الجريمة ومركبيها و تحديد مكانها وزمانها وما يلعبه دور الاثبات في تبصير الجهات الامنية ومساعدتهم في ملاحقة الجناة من جهة وكذا تبصير رجال القضاء لتشخيص الفاعل وإدانته بناء على أدلة وقرائن وحجج لا تقبل اثبات العكس، إضافة إلى معرفة الاليات والمعطيات الحديثة المعتمدة في إثبات الجريمة وصولا لمعاقبة الجاني في ظل محاكمة عادلة من شأنها ردع الجناة ومكافحة هذه الظواهر المستفحلة حديثا.

إن هذا النقاش يدفعنا لطرح الاشكالية التالية: ماهي صعوبات الاثبات الجنائي في الجريمة المعلوماتية؟
إن الإجابة على هذا الاشكال تقتضي طرح التساؤلات الفرعية التالية:

- ما مفهوم الجريمة المعلوماتية وخصائصها ؟
- ما هي الاجراءات المتبعة في إثبات هذه الجريمة ؟
- ما هي أهم المعوقات التي تواجه الاثبات الجنائي ؟
- وما مدى نجاعة وفعالية النظام العقابي الجزائري في الحد من هذا النوع من الجرائم؟

ولتسليط الضوء على هذا الموضوع والإجابة على إشكالية الدراسة والتساؤلات المرتبطة بها نقترح تقسيم العمل إلى مبحثين تُخصص الأول لمفهوم الجريمة المعلوماتية فنتعرف على تعريفها وأنواعها وخصائصها وأركانها، ثم نتعرض في المبحث الثاني إلى معرفة الاجراءات المتبعة في إثبات الجريمة المعلوماتية ونعرج على أهم الصعوبات والمعوقات التي تواجه الاثبات المتعلقة بهذا النوع من الجرائم. وحوصلة لدراسة وتحليل الإشكالية السالفة الذكر سنتوصل حتمًا إلى نتائج جوهرية حول تقييم ومدى نجاعة وفعالية النظام العقابي الجزائي في الحد من الظواهر والسلوكيات الاجرامية الحديثة وسنقرن هذه النتائج باقتراحات ذات صلة سيتم إدراجها ضمن الخاتمة، وسنعالج هذه الدراسة من خلال خطة ثنائية من مبحثين، نتناول في المبحث الأول: ماهية الجريمة المعلوماتية، أما في المبحث الثاني فننتطرق للاثبات الجنائي في الجريمة المعلوماتية.

المبحث الأول: ماهية الجريمة المعلوماتية

مما لا شك فيه أن ظهور الاجرام المعلوماتي إرتبط ارتباطاً وثيقاً بالتكنولوجيا الحديثة والتطورات الهائلة والكبيرة في مجال الاتصالات التي يتصف بها عصرنا الحالي الذي اقل ما يقال عنه انه العصر الالكتروني أو الرقمي فالجميع يستخدم الحاسوب والتقنيات الحديثة والوسائل العصرية في الاتصالات كل ذلك ساهم في ظهور حركة إجرامية من نوع خاص تتطلب معطيات وطرق معقدة لإثباتها¹. إن معرفة ماهية هذه الجريمة تتطلب منا ضبط تعريفها وخصائصها² وأنواعها وأركانها وهو ما سنتعرف عنه من خلال هذا المبحث وهذا ما سنفصله من خلال المطلبين الأول والثاني.

المطلب الأول: مفهوم الجريمة المعلوماتية

يعتبر مصطلح الجريمة المعلوماتية من المصطلحات الجديدة التي تم تداولها في العصر الحديث وهذا بعد الثورة التكنولوجية والتطور المذهل الذي شهدته شبكات المعلومات والاتصالات وأنظمة الإعلام الآلي، وما صاحبه من ظهور لسلوكيات جديدة مجرمة تهدد أمن الافراد والدول³، لذلك سنخصص

¹ نمديلي رحيمة، خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة، مداخلة في اعمال المؤتمر الدولي الرابع عشر المتعلق بالجرائم الإلكترونية، طرابلس 24، 25 مارس 2017.

² نمديلي رحيمة، المرجع نفسه.

³ محمد الامين البشري، تأهيل المحققين في جرائم الحاسب الآلي وشبكات الانترنت، الحلقة العلمية "الانترنت والإرهاب" كلية التدريب، قسم البرامج التدريبية بالتعاون بين جامعة نايف العربية للعلوم الامنية وجامعة عين شمس، القاهرة 2008.

هذا المطلب في معرفة دلالة المصطلح المذكور - الجريمة المعلوماتية - ثم نتعرف عن خصائصها وأنواعها وذلك من خلال ما يتقدم من فروع.

الفرع الأول: تعريفها

يتحدد مفهوم الجريمة المعلوماتية من الدلالة اللغوية والاصطلاحية للمصطلح في حد ذاته، ومع ذلك فقد حظي نظرا لحدائته بالاهتمام الواسع مما أدى إلى ورود العديد من التعاريف منها: أن الجريمة المعلوماتية " هي التي يستخدم فيها الحاسب الآلي كوسيلة لارتكابها، وهي سلوك غير مشروع يتعلق بالمعالجة الآلية للبيانات أو بنقلها"¹.

وقد عرفها المشرع الجزائري " بأنها جرائم المساس بأنظمة المعالجة الآلية للمعلومات أو تلك التي يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية "².

ومما سبق ذكره يمكن القول بأن الجريمة المعلوماتية هي عبارة عن تنفيذ العمل الاجرامي باستخدام التقنية الالكترونية في مجال تكنولوجيا الإعلام والاتصال الحديثة.

الفرع الثاني: خصائصها

إن هذا النوع من الاجرام يتسم بطبيعة خاصة تميزها عن تلك الجرائم التقليدية وعليه فان خصائص الجريمة المعلوماتية تتمثل فيما يلي:

- إن الجريمة المعلوماتية تتخطى الحدود الجغرافية للدولة.
- يتميز مرتكبيها بالمهارة والذكاء والاحترافية في تنفيذ الجريمة.
- تتميز بالسرعة في تنفيذ العمل الاجرامي.
- الجريمة المعلوماتية مغرية ولا تتطلب أي جهد يذكر.
- صعوبة إكتشافها وإثبات دليل وقوعها³.

الفرع الثالث: أنواعها

1 دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير، كلية الحقوق، شعبة القانون الجنائي، جامعة منتوري قسنطينة 2012، 2013.

2 تعرض المشرع الجزائري لهذا النوع من الجرائم من خلال المواد 394 مكرر الى 394 مكرر 07 من قانون العقوبات.

3 نمديلي رحيمة، المرجع السابق.

لا يمكن بأي حال من الاحوال حصر أنواع الجرائم المعلوماتية لتنوعها واختلافها باختلاف الزاوية التي ينظر منها لهذا الفعل المجرم فقد يكون النظام المعلوماتي أو البرنامج التابع له هو نفسه محل الجريمة أو قد يكون الحاسب هو أداة الجريمة ووسيلة تنفيذها فتقع هذه الجرائم على الاشخاص أو على الاموال أو على أمن الدولة، وبذلك سنذكر بعض التقسيمات التي تظهر في الواقع منها ما يلي:

أولاً: الجرائم الواقعة على الانظمة والبرامج المعلوماتية:

قد تستهدف هذه الجرائم المكونات المادية للنظام في حد ذاته أي تلك الجرائم التي تقع على الاجهزة والمعدات المستخدمة وهي جرائم ذات طبيعة تقليدية كالسرقة والإتلاف العمدي وغيرها، كما قد تستهدف هذه الجرائم البرامج التطبيقية كالمساس بها وتعديلها بالزيادة أو النقصان من ذلك التحويلات البنكية وغيرها أو أن يقع الفعل المجرم على برامج التشغيل المسؤولة عن عمل النظام المعلوماتي فيتم اختراقها والدخول إلى جميع المعطيات فيها، وقد يتم الفعل المجرم أيضا على المعلومة الالية في حد ذاتها فيتم التلاعب فيها أو استبدالها أو إتلافها من ذلك جرائم الغش أو التزوير المعلوماتي¹.

ثانياً: الجرائم الواقعة بواسطة الانظمة المعلوماتية:

قد يستخدم النظام المعلوماتي كأداة أو وسيلة لتنفيذ الاعمال الاجرامية سواء على الاشخاص أو الاموال أو امن الدولة في حد ذاته. من ذلك جريمة التهديد والملاحقة والمضايقة عن طريق الرسائل الالكترونية وجرائم القذف والسب والمساس بالكرامة عن طريق وسائل الاتصال ضد الأشخاص وكذلك جرائم التحويل الالكتروني غير المشروع للأموال والقرصنة وخرق الحسابات البنكية والقمار وغسيل الاموال عبر شبكة الانترنت وترويج المخدرات وغيرها من الجرائم الماسة بالأموال². أما تلك الواقعة على امن الدولة فمثالها جرائم الارهاب المعلوماتي والجرائم المنظمة والتجسس الالكتروني وغيرها من الجرائم التي تستهدف أمن الدولة واستقرارها.

1 جدي نسيم، جرائم المساس بأنظمة المعالجة الالية للمعطيات، مذكرة لنيل شهادة الماجستير، كلية الحقوق، تخصص القانون الجنائي، جامعة وهران، 2013، 2014.

2 جدي نسيم، المرجع نفسه.

المطلب الثاني: أركان الجريمة المعلوماتية

من المستقر عليه أن لكل جريمة ركن شرعي يتمثل في النص العقابي المجرم للفعل وركن مادي يتمثل في إتيان الجاني للفعل المجرم وركن معنوي يتمثل في القصد الجنائي وهو نية الجاني بإرادته الحرة للقيام بالجريمة، وباعتبار ان الجريمة المعلوماتية لها طبيعة خاصة ومتميزة عن الجريمة التقليدية فانه يتعين توضيح هذه الاركان بنوع من التفصيل من خلال ما يتقدم من فروع.

الفرع الأول: الركن الشرعي للجريمة المعلوماتية

الركن الشرعي للجريمة بصفة عامة يتمثل في تلك النصوص والمواد التي تجرم الفعل المعين وتضع له عقوبة مناسبة وهو ما يعبر عنه بمبدأ الشرعية العقابية على أساس أن " لا جريمة ولا عقوبة ولا تدابير أمن إلا بنص ". ويعتبر هذا الركن جوهر المتابعة الجزائية إذ يلعب دورا هام في تحديد الجرم وعقابه وتظهر أهمية هذا الركن خاصة في هذه الجرائم المستحدثة اذ يتطلب على المشرع مواكبة المتغيرات التي فرضها هذا العصر وما يشهده من تطور في الوسائل التكنولوجية وما صاحب ذلك من سلوكيات مجرمة¹.

مما لا شك فيه أن النصوص العقابية التقليدية عاجزة عن وضع حد لخطورة هذا النوع من الجرائم التي انتشرت بسرعة رهيبية وذلك لقصور قواعدها عن متابعة وملاحقة الجناة ومرد ذلك الضعف التشريعي في هذا المجال، إذ لا نجد في هذه النصوص ما يلم بتحريم كل السلوكيات الاجرامية الحديثة. إن الجناة في مجال الجريمة المعلوماتية يتميزون بالذكاء والدهاء والمهارة في تنفيذ جرائمهم دون أن يتركوا لها أثرا أو دليلا، الامر الذي يستدعي من أن يكون مسن النصوص العقابية يتصف أيضا بدقة تفوق دقة مرتكب الفعل حتى تؤدي هذه النصوص دورها وفعاليتها على أحسن وجه وتساهم في ردع ومعالجة المشكلة، وبذلك فان للنص القانوني دورا وقائيا لمنع هذا النوع من الجرائم حتى قبل وقوعها لأنه يقع حائلا دون ارتكاب الفعل، وهو ما يعبر عنه بالحماية الجزائية.

ولقد اعتمد المشرع الجزائري على استراتيجية مزدوجة لمواكبة الجريمة المعلوماتية، بحيث قام من جهة بتعديل العديد من القوانين الوطنية بما فيها التشريعات الجزائية (العقوبات و الاجراءات) وجعلها

1 برة سعيدة، الجريمة الالكترونية في التشريع الجزائري، دراسة مقارنة، مذكرة لنيل شهادة الماستر، كلية الحقوق، تخصص القانون الجنائي، جامعة محمد خيضر بسكرة، 2015، 2016.

تتجاوب مع التطورات الاجرامية في مجال تكنولوجيا الإعلام والاتصال وقام من جهة ثانية باستحداث قوانين أخرى خاصة أكثر انسجاما مع الطبيعة المميزة للجريمة الالكترونية. وبذلك فقد سارع المشرع الجزائري إلى تدارك الفراغ القانوني الحاصل في هذا المجال فقام بتعديل قانون العقوبات مستحدثا فيه بعض النصوص التي جرم من خلالها الأفعال المتصلة بالمعالجة الآلية للمعطيات، وحدد لكل فعل منها ما يقابله من جزاء، وقام إلى جانب ذلك بسن قواعد اجرائية جديدة تتعلق بالتحقيق تماشى مع الطبيعة المميزة لهذه الجرائم، وذلك من خلال تعديله لقانون الاجراءات الجزائية، ويبقى السؤال المطروح يدور حول مدى كفاية وفعالية هذه النصوص في الحد من هذه الظواهر المتنامية والمتجددة.

الفرع الثاني: الركن المادي للجريمة المعلوماتية

القاعدة العامة تقتضي أن لكل جريمة ركن مادي ويعد هذا الأخير المظهر الخارجي للجريمة أو كيانها المادي أو بمعنى آخر هو سلوك الجاني المادي الملموس الذي ينتج أثره في العالم الخارجي وقد يكون الركن المادي فعلا معينا أو امتناع عن أداء فعل معين، والركن المادي للجريمة المعلوماتية يتطلب وجود سلوك أو نشاط في ظل وجود بيئة رقمية وإتصالات بالانترنت، كما يتطلب معرفة بداية النشاط والشروع فيه ونتيجته، ومثال ذلك تجهيز الحاسوب وتحميل برامج للاختراق أو اعداد برنامج للقيام بالجرم أو اعداد برامج لبث الفيروسات وغيرها¹.

إن الجرائم المعلوماتية تتخذ عدة أشكال تتعدد بتنوع صور الاعتداء على الإعلام الآلي والتي يمكن إجمالها في صورتين أساسيتين وهما الاعتداءات على أنظمة المعالجة الآلية للمعطيات وكذا الاعتداءات على منتجات الإعلام الآلي.

فالصورة الأولى تتمثل في الدخول والبقاء غير المشروع في نظام المعالجة الآلية وتنطوي تحته أفعال الدخول والعرقلة والتعطيل، وكذلك أفعال الإدخال والحو والتعديل، أما الصورة الثانية فتحتوي على فعل التزوير المعلوماتي، وللإشارة فإن المشرع الجزائري لم يستحدث نصا خاصا بالتزوير المعلوماتي إذ أخضعه للنصوص العامة ولم يتبنى الإتجاه الذي تبنته التشريعات التي عملت على توسيع مفهوم المحرر ليشمل كافة صور التزوير الحديث.

الفرع الثالث: الركن المعنوي للجريمة المعلوماتية

1 بكرة سعيدة، المرجع نفسه.

لا يكفي لقيام الجريمة توافر الركن المادي فقط وإنما يجب فضلا عن ذلك توافر الركن المعنوي الذي يعبر عنه أحيانا بالركن الادبي والخطيئة والإذئاب والخطأ بمعناه الواسع، ويعني الصلة النفسية التي تربط بين النشاط الاجرامي ونتائجه من جهة وبين الفاعل الذي صدر منه النشاط بحيث يمكن القول أن السلوك هو بسبب ارادة الفاعل¹.

والركن المعنوي للجريمة المعلوماتية يعني نية وقصد الانحراف في استخدام الاجهزة الالية الرقمية بطريقة غير مشروعة لأهداف تخريبية، ويتطلب قيام معظم الجرائم المعلوماتية قصد خاص الذي يعني وجود نية إضافية في الجاني كالغش مثلا غير أن ما يميز الركن المعنوي للجرائم المعلوماتية بمختلف أشكالها هو صعوبة إثباته.

المبحث الثاني: الاثبات في الجريمة المعلوماتية

إن إثبات أي جريمة يعتمد أساسا على الاجراءات الأولية والتحقيقات التي على ضوءها يمكن التوصل إلى اكتشاف ملاسبات الجريمة مما يسهل على القضاء اثباتها ومن ثمة ادانة المتهم. إن طبيعة الجريمة المعلوماتية تتطلب أساليب غير تقليدية لاكتشاف الدليل وإثبات الجرم فجمع الأدلة في مثل هذه الجرائم يتطلب وقفة من قبل المشرع والقضاء لاتخاذ مجموعة من الخطوات الاصلاحية لمواجهةها، على اعتبار ان عالم تقنية المعلومات واسع لا يحده حد وان الوسائل المستعملة في ارتكاب الجريمة المعلوماتية متنوعة ومتشعبة².

مما لا شك فيه أن الجرائم المعلوماتية التي لم تُكتشف هي أكثر بكثير من تلك التي كُشف الستار عنها، لأنها عادة ما يتم اكتشافها عن طريق الصدفة، بل وبعد وقت طويل من ارتكابها، ولعل ذلك يرجع إلى صعوبة إجراءات التحقيق في هذا النوع من الجرائم وإلى عدة معطيات أخرى من ذلك اخفاء الجريمة وسهولة وسرعة محو أو تدمير أدلة ومعالم الجريمة والضخامة البالغة لكمية البيانات المراد فحصها على الشبكة، وتبرز الصعوبات كذلك في مسائل جمع الأدلة من المعاينة والتفتيش والضبط

1 عبد القادر عدو، مبادئ قانون العقوبات الجزائري، القسم العام، نظرية الجريمة، الطبعة الثانية، دار هومة، الجزائر 2013.

2 ثنيان ناصر آل ثنيان، اثبات الجريمة الالكترونية، رسالة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير، تخصص السياسة الجنائية، كلية الدراسات العامة، قسم العدالة الجنائية، جامعة نايف العربية للعلوم الامنية، الرياض، 2012.

وغيرها من الإجراءات فضلاً عن الطابع العالمي الذي تمتاز به هذه الجرائم لكونها من الجرائم التي تتجاوز عنصري الزمان والمكان.

ومن هذا المنطلق ستعرض من خلال هذا المبحث إلى اجراءات المتبعة في الاثبات الجنائي للجرمة المعلوماتية ثم نتطرق إلى أهم الصعوبات المطروحة التي تعترض سبيل رجال الامن والقضاء في اثبات هذا النوع من الجرائم.

المطلب الأول: إجراءات الاثبات في الجريمة المعلوماتية

لا شك أن للإثبات أهمية بالغة في هذا المجال، على أساس أن الدليل هو عصب الواقعة أي أنه النتيجة التي حققتها وسائل الإثبات وهذا الأخير يقصد به تلك القواعد المتعلقة بالبحث عن الأدلة وإقامتها أمام القضاء وبالتالي فالإثبات هو تلك الاسباب المنتجة لليقين والحقيقة¹.

ومن هذا المنطلق فالإثبات الجنائي في الجريمة المعلوماتية يتجسد في تلك الأدلة التي تؤكد وقوع السلوك الإجرامي، والتي من شأنها تحقيق حالة اليقين لدى القاضي ليتوصل إلى البراءة أو الإدانة في مواجهة المتهم، فالإثبات الجنائي في مجال مكافحة الجريمة المعلوماتية له عدة إجراءات تنطلق من مرحلة التحري وجمع الأدلة ثم التفتيش والخبرة في هذا المجال، مع أن لهذه الجرائم خصوصيتها التي تميزها عن إجراءات الإثبات في الجرائم التقليدية وهذا ما سنفصله من خلال ما يتقدم من فروع.

الفرع الأول: التحري وجمع الأدلة

من الصعب الإبلاغ عن الجرائم المعلوماتية في حينها لما تتطلبه من مهارات فنية لكشفها، إلا أن أي إخبار عن جريمة سواء كان فاعلها مجهولاً أم معلوماً ينبغي أن يتضمن على الأقل معلومات أولية عن الجريمة مثل تحديد محل الجريمة ومكان وقوعها ونوعها، وهي عناصر مهمة وضرورية لمساعدة رجال الضبطية القضائية في أي إخبار متعلق بجرائم تقنية المعلومات، بحيث تمكنهم من تحديد معالم الجريمة ووضع خطة عمل لمواجهتها².

1 ثنيان ناصر آل ثنيان، المرجع نفسه.

2 محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت، رسالة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير، تخصص السياسة الجنائية، كلية الدراسات العليا، قسم العدالة الجنائية جامعة نايف العربية للعلوم الامنية، الرياض، 2004.

هذا ويتم الاستعانة في الكشف عن هذا النوع من الجرائم بوضع برمجيات حاسوبية معينة كما يتم الحصول على المعلومات من موقع ارتكاب الجريمة بعد أن يتم إكتشافه باستخدام البرمجيات الحديثة، أو من خلال الحصول على المعلومات عن طريق رصد البيانات المنقولة من وإلى الموقع، وفي إطار التحري عن هذه الجريمة لا بد من التحفظ على الأجهزة وملحقاتها والمستندات الموجودة وغيرها من الأشياء التي يعتقد ان لها صلة بالجريمة، إضافة إلى اثبات الطريقة التي تم بواسطتها اعداد النظام والعمليات الالكترونية مع الحفاظ على البيانات من المحو والتبديل.

الفرع الثاني: التفتيش

يعتبر التفتيش إجراء من إجراءات التحقيق ويُقصد به البحث عن جسم الجريمة والأداة المستعملة في ارتكابها وكل ماله علاقة بها أو بفاعلها، والتفتيش في عالم تقنية المعلومات لا بد أن يكون محله الكيانات المادية والمعنوية أيضاً فالأولى مثل البحث في المكونات المادية للحاسوب أو ما يتصل به من اجهزة ويمكن في هذه الصورة ان نطبق القواعد العامة للتفتيش. أما التفتيش في الكيانات المعنوية فهو الامر الذي يطرح اشكالا وصعوبة لان التفتيش محله بيانات غير محسوسة وهذا الامر فيه قصور تشريعي واضح في معظم التشريعات اذ لم ترد النصوص واضحة وصريحة على جواز تفتيش المكونات المعنوية هذا من جهة ومن جهة اخرى فتفتيش هذه البيانات يتطلب مهارة خاصة¹.

الفرع الثالث: الخبرة

يقوم المحقق الجنائي في مجال كشف الجريمة المعلوماتية وفاعلها باتخاذ بعض الاجراءات والوسائل والتي من ضمنها الاستعانة بأهل الخبرة وذلك تحقيقاً لمبدأ هام وهو مبدأ التخصص نظراً لكون الخبرة هي تقدير مادي أو ذهني يُبديه أصحاب الفن أو الاختصاص في مسألة فنية لا يستطيع القائم بالتحقيق معرفتها ومعلوماته الخاصة سواء أكانت تلك المسألة الفنية متعلقة بشخص المتهم أو بجسم الجريمة أو المواد المستعملة في ارتكابها أو آثارها².

1 براهيمى جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراة في العلوم، كلية الحقوق والعلوم السياسية، قسم القانون العام، جامعة مولود معمري تيزي وزو، 2018.

2 براهيمى جمال، المرجع نفسه.

ونظراً للطبيعة الخاصة التي تتميز بها الجرائم المعلوماتية خاصة وأنها مرتبطة بمسائل فنية وعلمية بحتة أصبح من اللازم الاستعانة بالخبراء والمختصين الذين ينبغي أن تكون لديهم خبرة علمية وكفاءة فنية عالية في حقل أو أكثر من حقول تقنية المعلومات ونظمها ووسائلها لأن تصدي المحقق لفحص شيء وإبداء الرأي فيه دون أن تتوافر لديه المعرفة اللازمة يجعل قراره معيباً يضر بمصلحة التحقيق ويعوق الوصول إلى الحقيقة.

المطلب الثاني: صعوبات الإثبات في الجريمة المعلوماتية

إن صعوبات الإثبات الجنائي في هذه الجرائم منها ما هو متصل بالجريمة في حد ذاتها ومنها ما هو متعلق بالجهات المتضررة من الجرم، هذا من جهة ومن جهة أخرى قد ترجع الصعوبة لأسباب متعلقة بجهات التحقيق¹ أو للواقع التشريعي الخاص بهذا النوع من الجرائم، وهي الصعوبات التي سنأتي على بيانها من خلال الفروع الآتية.

الفرع الأول: المعوقات المرتبطة بالجريمة والمتضرر منها

إن الجريمة المعلوماتية في حد ذاتها لها خاصية عن باقي الجرائم وهو الأمر الذي يؤدي إلى ظهور عدة معوقات تتعلق بها وبضحايا هذه الجرائم من ذلك ما يلي:

● المعوقات المتعلقة بالجريمة المعلوماتية:

- سرعة اختفاء آثار الجريمة وغياب الدليل المرئي الممكن فهمه بالقراءة بفضل مهارة تركيبها في استخدام التقنيات وبرامجها.
- صعوبة الوصول إلى الدليل المثبت للجريمة بسبب إحاطته من طرف الجناة بوسائل حماية تمنع الوصول إلى الحقيقة.
- سهولة محو الدليل أو تدميره في زمن وجيز يصعب معه كشف الجريمة.
- ضخامة حجم المعلومات والبيانات وإمكانية خروجها عن نطاق إقليم الدولة.
- عدم استخدام الجاني المعلوماتي جهازه الخاص بل يلجأ إلى مقاهي الانترنت التي لا تتقيد بأي ضوابط أو أنظمة أمنية وهو ما يمنع التعرف على مستخدم الجهاز ومصدره.

● المعوقات المتعلقة بالمتضرر من الجريمة:

1 بكرة سعيدة، المرجع السابق.

- عدم إدراك الضحية خطورة الجرائم المعلوماتية مع غياب التوعية لإرشاد المستخدمين إلى خطورتها لا سيما اذا تعلق الامر بالمؤسسات المختلفة.
- عدم الابلاغ عن الجرائم المعلوماتية في حينها لعدم اكتشافها أو بسبب عدم رغبة الجهات المتضررة في الظهور كضحية لهذه الجرائم خوفا من نعتها بالإهمال أو قلة الخبرة أو عدم أخذ الاحتياطات اللازمة لحماية معلوماتها.
- عدم تركيز الشركات والمؤسسات على الجانب الامني في تقديم الخدمات المعلوماتية واهتمامها بتبسيط الاجراءات وتسهيل استخدام البرامج والخدمات الالكترونية.

الفرع الثاني: المعوقات المرتبطة بجهات التحقيق

- مما لا شك فيه أن للتحقيق الامني أو القضائي أهمية بالغة في اثبات الجريمة وكشفها إلا ان هناك بعض المعوقات المتعلقة بجهات التحقيق نوجزها فيما يلي:
- عدم مهارة المحقق في استخدام جهاز الكمبيوتر وعدم تمكنه من استعمال تقنيات الاتصالات الحديثة بالإضافة إلى عدم الاهتمام بمتابعة المستجدات في مجال الجرائم الالكترونية.
 - عدم توفر الاجهزة والبرامج المناسبة للتحقيق وعدم التنسيق بين المحققين في هيئات التحقيق والعاملين في مجال المعلومات والأنظمة الالكترونية والحاسوب.
 - عدم التخصص في مجال التحقيق لإثبات الجرائم المعلوماتية ومواكبة التقنيات العالمية الحديثة.

الفرع الثالث: المعوقات المرتبطة بالواقع التشريعي

مما لا شك فيه أن عالم تقنية المعلومات عالم متطور ومتسارع بشكل مذهل، نظرا للابتكارات الجديدة في هذا المجال لذلك يجب توافر اطلاع دائم وكاف على هذا العالم اللامتناهي، كي تتمكن الجهات التشريعية بكشف كل مستجد في مجال تقنية المعلومات حتى تعمل بدورها على سد الثغرات في مجال التشريعات الالكترونية، ومع كل ذلك تظهر عدة مسائل على الصعيدين الوطني والدولي تعيق الاثبات في مجال الجرائم المعلوماتية¹.

إن مسألة الواقع التشريعي يمكن أن نعالجها من خلال قانون العقوبات بمفهومه الواسع وكذا قانون الاجراءات الجزائية، فالأول يتصدى للظواهر الاجرامية فيحدددها ويضع العقوبات الرادعة لكل منها،

1 براهيمي جمال، المرجع السابق.

أما الثاني فيحدد القواعد الاجرائية والضمانات التي ينبغي أن تحترمها الجهات المعنية وصولاً إلى محاكمة عادلة، وتبرز اشكالية التشريع في مدى نجاعة وكفاية النصوص التقليدية لوضع حد لهذه الظواهر المتجددة والمتنامية التي حتمت على المشرع ضرورة تعديل هذه النصوص أو إضافة نصوص جديدة لتشمل كافة الجرائم المعلوماتية أو استحداث أقسام جديدة للجرائم الالكترونية على غرار الأقسام التقليدية.

كما أن الطبيعة الخاصة للجريمة المعلوماتية تطرح عدة اشكالات تتعلق باختصاص الاقليمي على أساس أن هذه الجريمة قد تقع في مكان ما في العالم وتنتج آثارها في أماكن أخرى خارج اقليم الدولة وهو ما يدعو إلى التعاون الدولي غير ان الصعوبة تطرح حول اختلاف منظور الدول للجريمة وتفاوت دول العالم في هذا المجال وصعوبة توحيد الجهود لمكافحة الجرائم المعلوماتية، ولعل من أبرز المنظمات الدولية التي عملت في هذا الشأن الاتحاد الدولي للاتصالات التابع للأمم المتحدة.

وعلى هذا الاساس ينبغي على المشرع إصدار تشريع خاص ومستقل لهذه الجرائم يحدد هذا النوع من الجرائم ويضع عقوبات خاصة وملائمة للجريمة، فضلاً عن وضع إجراءات جزائية تنسجم مع طبيعة هذا النمط من الجرائم، مع ضرورة تشجيع التعاون الدولي لمواجهة هذا الخطر المحدق.

الخلاصة:

من خلال هذه الدراسة نخلص إلى أنه على الرغم من الايجابيات العديدة التي أحدثتها ثورة التطور التكنولوجي في تسهيل نقل وتبادل المعلومات، إلا أن هناك خشية متزايدة من تنامي الحروق والسلبات والأعراض الجانبية لهذه الشبكات واستغلالها لارتكاب وتعميم أعمال وأفعال تتقاطع مع القوانين ومع الاعراف والأخلاق والآداب.

امتازت التعريفات الواردة للجريمة المعلوماتية بالتعدد ومع ذلك يمكن إيجازها في أنها سلوك غير مشروع ضار بالمجتمع يرتكب باستخدام الحاسب الآلي، لهذه الجريمة أنواع وخصائص تميّزها عن باقي الجرائم التقليدية كما تقوم على ركن مادي ومعنوي وآخر شرعي يتمثل في النص العقابي المستحدث. إن الجريمة المعلوماتية تطل الحقوق وتمس حرمة الحياة الخاصة للأفراد وتهدد الأمن الوطني وتؤدي إلى فقدان الثقة بالتقنية وغيرها من مفاصل الحياة العامة المختلفة.

من بين الاشكالات المتعلقة بهذه الجريمة مسألة الاثبات الجنائي للجريمة في حد ذاتها ومعرفة زماها ومكانها ومرتكبها.

اهتمت جل التشريعات بهذه المسألة لما لها من أهمية خاصة في مواجهة ومكافحة هذا النوع من الجرائم، فرتبت عدة إجراءات قانونية وطرق حديثة ومواكبة للجريمة كل ذلك بهدف إثبات الدليل الجنائي.

لا شك أن هناك عدة صعوبات ومعوقات تعترض سبيل المحققين قصد كشف معالم الجريمة وتشخيص الجناة وبسط الرقابة وصولاً لمحاكمة عادلة، من بين هذه المعوقات ما يتصل بالجريمة في حد ذاتها من حيث الطبيعة والأشخاص ومنها ما يتعلق بنوع التحقيقات التي تتطلبها هذه الجرائم المتطورة ومنها ما يتعلق بالنص العقابي الذي يجعل المشرع متأهباً لمواكبة هذه الجرائم المتنامية والتي لم يرد النص على تجريمها في النصوص التقليدية.

ومن هذا المنطلق نكون قد أجبنا من خلال هذه الدراسة على الإشكالية المطروحة ونؤكد في الختام بأن النظام العقابي للجريمة المعلوماتية في التشريع الجزائري يحتاج إلى تطوير مستمر لمواكبة مكافحة هذا النوع من الجرائم التي تتميز بالحدثة والتنامي.

أما الاقتراحات التي يمكن لنا إثارتها حول هذا الموضوع فارتأينا طرح ما يلي:

- تكثيف التكوين لرجال الأمن والقضاء لا سيما في المجال الإلكتروني وفقاً للمعايير الحديثة حتى نكون أمام جهات أمنية وقضائية تمتاز بالمهارة والدقة، كل ذلك قصد السيطرة على هذه الجرائم المتطورة وكشف مرتكبيها.
- تطوير التشريعات العقابية لمكافحة هذا النوع من الجرائم حتى تكون النصوص الجزائية قابلة للتطبيق محلياً وعالمياً على الجرائم المعلوماتية ومرتكبيها.
- ضرورة تهيئة الهياكل التنظيمية والسياسات المتعلقة بمواجهة الجرائم الإلكترونية.
- وضع معايير أمنية للنظم والتطبيقات والبرامج واعتمادها من طرف المؤسسات والأفراد.
- استحداث آليات عالمية فعالة للمراقبة والإنذار في هذا المجال.
- نشر الوعي العام المساند للتحويل الإلكتروني من جهة والتنبيه عن المخاطر التي يسببها للجمهور وضرورة التبليغ عن هذه المخاطر عند حدوثها حتى تسهل السيطرة عليها.
- الاستفادة من التجارب الأجنبية والعربية في مجال مكافحة الجريمة المعلوماتية، دراسة وتبادلاً للمعلومات والخبرات مع تحقيق التواصل بين الدول العربية في هذا المجال.
- إنشاء هيئات متخصصة في التحقيق والإثبات الجنائي في مجال الجرائم المعلوماتية.

- ضرورة إصدار تشريع خاص ومستقل لهذا النوع من الجرائم توضح فيه الجريمة وما يلائمها من عقوبة بالإضافة إلى إصدار تشريع اجرائي ينسجم مع طبيعة هذا النمط من الجرائم.
- السعي في عقد الاتفاقيات التعاونية ذات العلاقة بمكافحة هذه الجرائم مع الدول العربية والأجنبية.

المبادئ التي تحكم مقبولية الأدلة الجنائية الرقمية أمام القضاء الجزائي

ط.د/ طاهري عبد المطلب

كلية الحقوق والعلوم السياسية - جامعة الأغواط

مقدمة:

شهدت العقود القليلة الماضية غزوا تكنولوجيا كبيرا لكافة نواحي الحياة وفي مختلف المجالات الاقتصادية والاجتماعية والثقافية، وهو ما نتج عنه تغيرا جذريا في حياة الإنسان، حيث أصبح يعتمد بشكل كبير على ما أفرزته التكنولوجيا الحديثة من أجهزة الحواسيب والهواتف الذكية وحتى شبكات الاتصال السلكية واللاسلكية، وأصبح من السهل جدا وفي لمح البصر نقل البيانات ومعالجتها وتخزينها في ظرف قياسي.

إلا أنه هناك من حاول استغلال هذا التطور في الجانب السلبي، وأصبح يعتمد على التكنولوجيا في ممارسات غير شرعية تدخل ضمن نطاق الجرائم المنصوص عليها بموجب قانون العقوبات، وهو ما حتم على جهات التحقيق والحكم بالاعتماد على نوع جديد من الأدلة تتماشى وطبيعة الجريمة المرتكبة، ألا وهي الأدلة الجنائية الرقمية،

ولضمان حقوق الأفراد وحرياتهم أثناء عملية استخلاص الأدلة الجنائية الرقمية التي تتطلب طرق وأساليب تقنية وفنية معقدة، عمد المشرع إلى استحداث قواعد موضوعية وإجرائية تنظم اللجوء لعمليات الإثبات بالأدلة الجنائية الرقمية، وأرسى مجموعة من المبادئ والأسس المتعلقة بمدى مقبولية الأدلة الجنائية الرقمية أمام الجهات القضائية الجزائية (موضوع مداخلتنا).

ومنه وبناء على ما سبق ذكره، سنعالج في هذه المداخلة مبادئ وأسس قبول الأدلة الجنائية الرقمية أمام القضاء الجزائي وفق الخطة التالية:

أولاً: مبدأ مشروعية الأدلة الجنائية الرقمية

ثانياً: مبدأ يقينية الأدلة الجنائية الرقمية

ثالثاً: مبدأ مناقشة الأدلة الجنائية الرقمية

أولاً: مبدأ مشروعية الأدلة الجنائية الرقمية

أخذ المشرع الجزائري بضابط مشروعية الأدلة الجنائية كقاعدة أساسية عامة تسري على جميع الأدلة الجنائية مهما كان نوعها، فلا يعقل للقاضي أن يعتمد في تكوين عقيدته وحرثته في الاقتناع إلا إذا كان الدليل الذي يعتمد عليه مشروعاً بصفة أولى¹.

لذا فإنه من الواجب اتفاق القواعد الإجرائية المتعلقة باستخلاص الأدلة الجنائية الرقمية مع القواعد القانونية والأنظمة المعمول بها، بهدف الحفاظ على حقوق الأفراد وحررياتهم من تعسف جهات التحقيق المنوط بها جمع الأدلة الجنائية، كما يجب التنبيه على أن مشروعية الأدلة الجنائية لا تقتصر فقط على مجرد المطابقة مع القواعد القانونية التي ينص عليها المشرع فحسب، بل يجب أيضاً مراعاة تطابقها مع ما نصت عليه المواثيق والاتفاقيات الدولية المتعلقة بحقوق الإنسان وقواعد النظام العام².

1- أسس قيام مشروعية الأدلة الجنائية الرقمية

يقوم مبدأ مشروعية الأدلة الجنائية عموماً على أساسين رئيسيين وهما:

أ) مشروعية وجود الأدلة الجنائية الرقمية

يقصد بمشروعية وجود الأدلة الجنائية الرقمية أن يكون الدليل الجنائي الرقمي معترفاً به، بمعنى أن القانون يميز للقاضي الاستناد إليه لتكوين عقيدته للحكم بالإدانة³، ويختلف مفهوم مشروعية وجود الأدلة الجنائية الرقمية بحسب نظام الإثبات الجنائي المتبع في كل دولة، فبالنسبة للدول التي تتبع نظام الإثبات الحر القانون لا يلزم القاضي في تكوين اقتناعه بأدلة جنائية محددة، بل له الحرية المطلقة في الاعتماد على أي دليل يراه مناسباً لتكوين اقتناعه حتى ولو لم يكن منصوصاً عليه في القانون، لذا ففي الدول التي تتبع نظام الإثبات الحر مثل الجزائر وفرنسا فإن مشروعية الأدلة الجنائية الرقمية لا

¹ كمال محمد عواد، الضوابط الشرعية والقانونية للأدلة الجنائية (في الفقه الإسلامي والقانون الوضعي)، الطبعة الأولى، دار الفكر الجامعي، مصر، 2011، ص 165.

² أحمد عبد اللاه هلال، "حجية المخرجات الكمبيوترية في المواد الجنائية (دراسة مقارنة)"، في بحوث مؤتمر القانون والكمبيوتر والإنترنت، المجلد الثاني، الطبعة الثالثة، جامعة الإمارات العربية المتحدة، الإمارات العربية المتحدة، 2004، ص 429.

³ خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2011، ص 235.

تثير أي إشكال على اعتبار أن المشرع في هذه الحالة ليس مطالب بتحديد أدلة الإثبات بناتا لأن الأصل في الأدلة مشروعية وجودها، بخلاف الدول التي تتبع نظام الإثبات المقيد مثل الولايات المتحدة الأمريكية وبريطانيا، التي يحدد المشرع فيها على سبيل الحصر الأدلة الجنائية التي يجوز للقاضي الاعتماد عليها في الإثبات، كما يحدد المشرع أيضا القوة الثبوتية لكل دليل جنائي على حدا، ويقتصر دور القاضي في هذه الحالة فقط على فحص الدليل والتأكد من توافر شروط مقبوليته أمام القضاء¹.

ب) مشروعية الحصول على الأدلة الجنائية الرقمية

من بين أهم القواعد العامة المتعلقة بالإثبات الجنائي (الحر) القاضي له الحرية المطلقة في إقامة اقتناعه على أي دليل يراه مناسباً، لكن هذه القاعدة ليست مطلقة لهذا الحد، وإنما وُضعت لها العديد من الضوابط والشروط خوفاً من أن يتسبب القاضي بالمساس بحقوق الأفراد وحرياتهم، وعلى هذا أساس إن قبول الأدلة الجنائية الرقمية متوقف على أن يتم الحصول عليها بطريقة مشروعة، وذلك من خلال أن تكون الإجراءات المتبعة في استخلاص الأدلة الجنائية الرقمية قد تمت بشكل قانوني²، انطلاقاً من توافقها مع القواعد والشروط العامة المتعلقة بصحة إجراءات التحقيق.

❖ ضوابط مشروعية الحصول على الأدلة الجنائية الرقمية

وتتمثل هذه القواعد في قواعد الموضوعية مثل أن يكون الإجراء الذي يستهدف استخلاص الأدلة الجنائية الرقمية عملاً إرادياً صادراً من شخص له صلاحية القيام به بناء على سبب معين، زيادة على ذلك يجب أن يكون المحل الذي يرد عليه الإجراء محدداً أو قابلاً للتحديد وأن يكون مشروعاً، وأما بالنسبة للقواعد الشكلية فيجب الالتزام باحترام كيفية مباشرة تنفيذ هذا الإجراء وفق ما نص عليه القانون³، وهذه القواعد الإجرائية يؤدي إلى بطلان جميع إجراءات التحقيق، وبالتالي بطلان الدليل الناتج عنها ولا تصلح في الأخير لأن تكون أدلة جنائية يبنى عليها الحكم بالبراءة أو بالإدانة.

❖ الحصول على الأدلة الجنائية الرقمية والحق في الخصوصية

¹ المرجع نفسه، ص 237.

² كمال محمد عواد، المرجع السابق، ص 167.

³ المرجع نفسه، ص 167 – 168.

إن الحديث عن مشروعية الحصول على الأدلة الجنائية يحتم علينا التطرق إلى مسألة الحق في الخصوصية في العالم الرقمي انطلاقاً من أن الإجراءات المتخذة في سبيل استخلاص الأدلة الجنائية الرقمية تؤدي في الأخير إلى المساس بحقوق الإنسان وحرياته¹، هذا الحق الذي برز بشكل كبير في عصرنا الحالي في ظل تزايد الاعتماد الإنسان على التكنولوجيا الحديثة في مختلف المجالات، إلا أن المجتمع الدولي وخصوصاً المشرع الجزائري قد نظم وكرس مبدأ حماية الحياة الخاصة في العالم الرقمي من أي مساس واستثنى من ذلك الإجراءات التي تكون في صالح التحقيق.

وعلى المستوى الدولي، تضمنت العديد من الاتفاقيات والمواثيق الدولية مبدأ حماية الحياة الخاصة للفرد، وذلك مثل ما نصت عليه المادة 12 من الإعلان العالمي لحقوق الإنسان على أنه: "لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات".

كما نصت أيضاً المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسة على أنه: "لا يجوز تعريض أي شخص على نحو تعسفي أو غير قانوني لتدخل في خصوصياته، أو شؤون أسرته أو بيته أو مراسلاته، ومن حق كل شخص أن يحميه القانون من مثل ذلك التدخل".

وأما على المستوى الداخلي فقد اجتهد المشرع الجزائري على حماية الحياة الخاصة للفرد في البيئة الرقمية من أي مساس قد يطرأ، حيث نصت المادة 46 من الدستور الجزائري² على أنه: "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون. سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة. لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية. ويعاقب القانون على انتهاك هذا الحكم. حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه".

¹ معتصم خيس مشعشع، "إثبات الجريمة بالأدلة العلمية"، مجلة الشريعة والقانون، العدد 56، جامعة الإمارات العربية المتحدة، الإمارات العربية المتحدة، 2013، ص 34.

² القانون رقم 16-01 المؤرخ في 2016/03/06، المتعلق بالتعديل الدستوري الجزائري، الجريدة الرسمية رقم 14، الصادرة في 2016/03/07.

وبالنسبة لقانون العقوبات الجزائري¹، فقد نصت المادة 303 مكرر على ما يلي: "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 50.000 دينار جزائري إلى 300.000 دينار جزائري، كل من تعمد المساس بجرمة الحياة الخاصة للأشخاص، وبأية تقنية خاصة كانت وذلك بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه..."، ومن جهة أخرى قام المشرع الجزائري أيضا في قانون العقوبات بتجريم الأفعال التي تستهدف المساس بالبيانات الشخصية التي تدخل ضمن مفهوم "المعطيات" من خلال المواد 394 إلى 394 مكرر 7.

ولم يكتف المشرع أيضا بهذا بل نظم طرق لجوء المساس بالبيانات الشخصية من قبل جهات التحقيق والقضاء لاستخلاص الأدلة الجنائية الرقمية وذلك من خلال القانون 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما²، وأيضاً القانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي³.

ثانيا: مبدأ يقينية الأدلة الجنائية الرقمية

¹ الأمر رقم 66-156 المؤرخ في 08/06/1966، المتضمن قانون العقوبات، الجريدة الرسمية رقم 49، الصادرة بتاريخ 11/06/1966، المعدل والمتمم.

² القانون رقم 04-09 المؤرخ في 16/08/2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، الجريدة الرسمية رقم 47، الصادرة بتاريخ 16/08/2009، ص 5.

³ القانون رقم 07-18 المؤرخ في 10/06/2018، المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، الجريدة الرسمية رقم 34، الصادرة بتاريخ 10/06/2018، ص 11.

يعرف اليقين بأنه: "حالة ذهنية أو عقلانية تؤكد وجود الحقيقة، ويتم الوصول إلى ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من وقائع الدعوى، وما ينطبع في ذهنه من تصورات واحتمالات ذات درجة عالية من التوكيد، والتي وصل إليها القاضي في حكمه تستبعد إمكانية تطرق أي شك أو ريب تجاه تلك المحصلة النهائية"¹، والمقصود باليقين الذي يبنى عليه حكم القاضي بالإدانة ليس هو اليقين الشخصي فحسب، وإنما هو اليقين القضائي الذي يمكن أن يصل إليه الكافة².

لذا، فاليقين في مجال الأدلة الجنائية الرقمية هو بأن تكون غير قابلة للشك حتى يمكن الحكم بالإدانة، وذلك بأنه لا مجال لدحض قرينة البراءة وافتراض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين³، ويمكن الوصول إلى اليقين في هذه الحالة من خلال ما يعرض من الأدلة الرقمية بمختلف أنواعها وأشكالها، وما ينطبع في ذهنه من تصورات واحتمالات بالنسبة لها أن يحدد قوتها الاستدلالية على صدق نسبة الجريمة المعلوماتية إلى شخص معين من عدمه⁴.

وفي حالة عدم قدرة أدلة الإدانة على إحداث القطع أو اليقين يترتب عليه استمرار حالة البراءة التي يكفي لتأكيد وجودها حينئذ مجرد الشك في ثبوت تلك الإدانة، انطلاقاً من أن الحكم بالإدانة يستوجب اليقين بوجود هذه الإدانة، وذلك لأنها إثبات على خلاف الأصل الذي لا يمكن إثبات عكسه إلا بمقتضى حالة من اليقين تتساوى في نتائجها مع تلك المسلم بوجودها نتيجة لمبدأ افتراض البراءة⁵.

وانطلاقاً من الطابع العلمي والتقني الذي تتميز به هذا النوع من الأدلة تم وضع قواعد أساسية تحكم يقينية الأدلة الجنائية الرقمية، وذلك باستعمال وسائل تقنية تمكن من فحصه والتأكد من سلامته وصحة الإجراءات المتبعة في الحصول عليه⁶:

¹ كمال محمد عواد، المرجع السابق، ص 304.

² المرجع نفسه، ص 304.

³ علي حسن محمد الطويلة، التفتيش الجنائي على نظم الحاسوب والانترنت (دراسة مقارنة)، الطبعة الأولى، عالم الكتب الحديث، الأردن، 2004، ص 190.

⁴ المرجع نفسه، ص 190.

⁵ أحمد عبد اللاه هلايلي، المرجع نفسه، ص 740.

⁶ خالد عياد الحلبي، المرجع السابق، ص 249.

1) تقييم الأدلة الجنائية الرقمية من حيث سلامتها من العبث

يعتبر مبدأ سلامة الأدلة الجنائية الرقمية من أهم المبادئ المتبعة نظرا للطبيعة العلمية والتقنية التي تتميز بها، وكذا سهولة إتلافها أو تغيير محتواها، لذا وجب على المختصين إتباع مجموعة من الطرق أهمها استعمال عملية التحليل التناظري الرقمي، التي تعتبر من بين الوسائل المهمة للكشف عن مصداقية الأدلة الجنائية الرقمية، من خلال القيام بعملية مقارنة الدليل (الأصلي) المقدم للقضاء بالنسخة المستخرجة¹.

وفي حالة عدم الحصول على النسخة الأصلية للدليل الجنائي الرقمي، أو في حالة وقوع تعديل أو إتلاف النسخة الأصلية، فيمكن في هذه الحالة التأكد من سلامة هذا الدليل من العبث من خلال استخدام عمليات حسابية خاصة تسمى بالخوارزميات (برامج خاصة)، أو باللجوء إلى نوع آخر من الأدلة الجنائية الرقمية الذي يطلق عليه باسم الدليل الجنائي الرقمي المحايد، وهو دليل لا علاقة له بموضوع الجريمة، ولكنه يساهم في التأكد من مدى سلامة الدليل الجنائي الرقمي².

2) تقييم الأدلة الجنائية الرقمية من حيث السلامة الفنية لإجراءات استخلاصه

تعتبر عملية التحقق من السلامة الفنية لإجراءات استخلاص الأدلة الجنائية الرقمية عملية مهمة جدا لتفادي أي أخطاء تقنية قد تشكل في سلامة الأدلة المستخلصة، وهي عبارة عن اختبارات تقنية متبعة من قبل خبراء متخصصون بهدف التأكد من سلامة إجراءات الحصول على الدليل الجنائي الرقمي³، ومضمونها الأساسي التأكد من دقة الوسائل والأدوات المستخدمة على عرض كافة البيانات المتعلقة بالأدلة⁴.

ثالثا: مبدأ مناقشة الأدلة الجنائية الرقمية

يعتبر مبدأ مناقشة الأدلة الجنائية عموما من أهم المبادئ التي تحكم مقبولية الأدلة الجنائية أمام الجهات القضائية الجزائية، يقصد بمناقشة الأدلة الجنائية: "أن القاضي لا يمكن أن يؤسس اقتناعه إلا

¹ المرجع نفسه، ص 249.

² ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2006، ص 125.

³ المرجع نفسه، ص 127.

⁴ خالد عياد الحلبي، المرجع السابق، ص 250.

على العناصر الإثباتية التي طرحت في جلسات المحاكمة، وخضعت لحرية مناقشة أطراف الدعوى"¹، وقد نص عليها المشرع الجزائري من خلال المادة 2/212 من قانون الإجراءات الجزائية² بقولها: "...ولا يسوغ للقاضي أن يبيّن قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه".

فبالرغم من الحرية التي منحتها المشرع الجزائري للقاضي باعتماده لأي دليل يراه مناسبا، إلا أنه مجبر بموجب هذا المبدأ الاعتماد على الأدلة الجنائية التي طرحت بجلسة المرافعة، وملزم أيضا بإتاحة أطراف الدعوى العمومية الإطلاع على الأدلة المقدمة لمناقشتها في الجلسة³. كما يستند مبدأ مناقشة الأدلة الجنائية على قواعد مرتبطة بها أهمها: شفعية المرافعات والمواجهة بين الخصوم، فهي تلزم جميع أطراف الدعوى أن تناقش الأدلة المعروضة في جلسة محاكمة حضورية بطريقة شفوية (صوت مسموع) مع مواجهة أدلة كل خصم للآخر، وفي النهاية يتسنى للقاضي تكوين اقتناعه من خلال هذه المواجهة⁴.

ويترتب على الإخلال بضابط المناقشة بطلانها وعدم الاعتداد بها، لأن ذلك يعد من قبيل حرمان أطراف الدعوى العمومية من الإطلاع على الأدلة وإبداء دفعهم، وهو ما يشكل اعتداء صريحا للمبادئ المقررة في سبيل الوصول إلى محاكمة عادلة⁵. وعليه تطبيقا لما تم ذكره سابقا، يجب على القاضي عرض جميع الأدلة الجنائية الرقمية أمام أطراف الدعوى العمومية في الجلسة مهما كان نوعها وشكلها، ونظرا للطبيعة العلمية والتقنية لهذا النوع من الأدلة، فإنه يستوجب إظهارها إما عن طريق شاشات الحاسب الآلي أو طباعتها⁶.

¹ نصر الدين مروك، محاضرات في الإثبات الجنائي (النظرية العامة للإثبات الجنائي)، الجزء الأول، دار هومة، الجزائر، 2003، ص 637.

² الأمر رقم 66-155 المؤرخ في 08/06/1966، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية رقم 48، الصادرة بتاريخ 10/06/1966، المعدل والمتمم.

³ نصر الدين مروك، المرجع السابق، ص 458.

⁴ كمال محمد عواد، المرجع السابق، ص 362.

⁵ المرجع نفسه، ص 398.

⁶ أحمد عبد اللاه هلاّلي، المرجع السابق، ص 748.

خاتمة:

انطلاقاً مما تمت دراسته سابقاً، يمكن أن نخلص إلى أنه بالرغم من حرية الإثبات الجنائي التي منحها المشرع الجزائري للقاضي فيما يخص اعتماده لأي دليل يراه مناسباً لتكوين عقيدته، إلا أنه قد وضع

العديد من الضوابط والشروط التي تضمن عدم انحراف عملية الإثبات، خصوصا فيما يتعلق بالأدلة التي تكتسي طابعا علميا وتقنيا مثل الأدلة الجنائية الرقمية. إن مناقشة الدليل الجنائي الرقمي أثناء جلسة المحاكمة والتحقق من يقينته، تتطلب مؤهلات تقنية ومعارف فنية، وكذا سلامته الفنية من العبث، وسلامة الإجراءات المتبعة في استخلاصه، وهو ما يستوجب التأهيل التقني والفني للقضاة للتعامل مع هذا النوع من الأدلة الجنائية. ومن جهة أخرى، اجتهد المشرع الجزائري في تأسيس إطار قانوني عام يحفظ حقوق وحريات الأفراد خصوصا وأن عملية الإثبات بالأدلة الجنائية قد تمس العديد من الحقوق اللصيقة بالفرد، لعل أهمها الحق في الحياة الخاصة، حيث قام المشرع بتعديل قانون العقوبات واستحدث قواعد إجرائية تهدف إلى تنظيم عمليات استخلاص الأدلة الجنائية الرقمية، خصوصا وأن تطور التكنولوجيا أدى إلى اعتماد هذا النوع من الأدلة حتى في إثبات الجرائم التقليدية الأخرى ولم تعد مقتصرة على إثبات الجريمة المعلوماتية فقط.

قائمة المراجع:

الكتب:

- كمال محمد عواد، الضوابط الشرعية والقانونية للأدلة الجنائية (في الفقه الإسلامي والقانون الوضعي)، الطبعة الأولى، دار الفكر الجامعي، مصر، 2011.
- نصر الدين مروت، محاضرات في الإثبات الجنائي (النظرية العامة للإثبات الجنائي)، الجزء الأول، دار هومة، الجزائر، 2003.
- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2011.
- علي حسن محمد الطوالة، التفتيش الجنائي على نظم الحاسوب والانترنت (دراسة مقارنة)، الطبعة الأولى، عالم الكتب الحديث، الأردن، 2004.
- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2006.

المقالات:

- أحمد عبد اللاه هلايلي، "حجية المخرجات الكمبيوترية في المواد الجنائية (دراسة مقارنة)"، في بحوث مؤتمر القانون والكمبيوتر والإنترنت، المجلد الثاني، الطبعة الثالثة، جامعة الإمارات العربية المتحدة، الإمارات العربية المتحدة، 2004.
- معتصم خميس مشعشع، "إثبات الجريمة بالأدلة العلمية"، مجلة الشريعة والقانون، العدد 56، جامعة الإمارات العربية المتحدة، الإمارات العربية المتحدة، 2013.

النصوص القانونية:

- القانون رقم 16-01 المؤرخ في 2016/03/06، المتعلق بالتعديل الدستوري الجزائري، الجريدة الرسمية رقم 14، الصادرة في 2016/03/07.
- القانون رقم 09-04 المؤرخ في 2009/08/16، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، الجريدة الرسمية رقم 47، الصادرة بتاريخ 2009/08/16.
- القانون رقم 18-07 المؤرخ في 2018/06/10، المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، الجريدة الرسمية رقم 34، الصادرة بتاريخ 2018/06/10.
- الأمر رقم 66-155 المؤرخ في 1966/06/08، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية رقم 48، الصادرة بتاريخ 1966/06/10، المعدل والمتمم.
- الأمر رقم 66-156 المؤرخ في 1966/06/08، المتضمن قانون العقوبات، الجريدة الرسمية رقم 49، الصادرة بتاريخ 1966/06/11، المعدل والمتمم.

القيمة الإثباتية للدليل الجنائي الإلكتروني

د/ طيب عمور محمد

أستاذ محاضر (أ) - كلية الحقوق والعلوم السياسية

جامعة حسبية بن بوعلي - الشلف

مقدمة:

تتسم الجريمة المعلوماتية بكونها خفية ومستترة، فقد تتم بحضور المجني عليه دون أن يتفطن لوقوعها إلا بعد فترة زمنية قد تطول، لأن الجاني ينفذ جريمته بدقة متناهية، مثل نشر الفيروسات، سرقة الأموال أو البيانات الخاصة، قرصنة بطاقات الائتمان، إتلاف البيانات، التجسس، وغيرها من الجرائم الإلكترونية، ومما يصعب من اكتشاف هذا النوع من الجرائم إحجام الكثير من ضحايا الجريمة المعلوماتية وخاصة المصارف من الإبلاغ عن وقوع تلك الجرائم، خوفاً من أن يسيء الإعلان السلبي إلى سمعة الضحايا، فحين تعلن شركة أن متسللين وصلوا إلى خوادمها قد يفقد الزبائن الثقة بها، وقد تكون التكاليف والعواقب أكبر بكثير حتى من الخسائر الناجمة عن الهجوم المتسلل.

ومن هنا كان إثبات الجريمة المعلوماتية أمراً بالغ الصعوبة، يتطلب مهارات فنية وتقنية عالية، وترجع صعوبة إثبات هذا النوع من الجرائم إلى عدم وجود آثار مادية خارجية تدل على وقوع الجريمة أو مرتكبها، كما أن أغلب من يقوم بارتكاب هذا النوع من الجرائم يحيطون أنفسهم بجملة من التدابير التقنية والأمنية للوقاية تصعب على الأجهزة الأمنية العثور على الأدلة الرقمية، وذلك بتشفير البيانات المخزنة بأرقام سرية، أو ترميزها، مما يجعل الوصول إليها وفهمها في غاية الصعوبة، كما يسهل على الجاني التخلص من أدلة الإدانة بمحوها في زمن قياسي لا يتطلب أكثر من ثوان معدودة..

الإشكالية: ومن هنا تتساءل عن القيمة الإثباتية للدليل الجنائي الإلكتروني

المحور الأول: موقف التشريع من الإثبات الجنائي بالدليل الرقمي

تذهب جل التشريعات المقارنة إلى قبول الأدلة الرقمية في الإثبات الجنائي، وهذا موقف بعض التشريعات.

أولاً: موقف التشريع الأنجلوسكسوني:

1- موقف التشريع الأمريكي: من بين القواعد المتعلقة بالإثبات في القانون الأنجلوسكسوني قاعدة استبعاد شهادة السماع (the hearsay rule) وقاعدة الدليل الأفضل (the best Evidence rule). وهذا يثير مسألة قبول الأدلة الرقمية في الإثبات الجنائي لتعارضها مع هاتين القاعدتين:

الأدلة الرقمية مستثناة من قاعدة استبعاد الأدلة السماعية: تضمنت القواعد الفيدرالية الأمريكية نصاً يعتبر السجلات والبيانات المنظمة بدقة بيّنة مقبولة أمام المحاكم الجنائية استثناءً للبيئة السماعية، وبناءً على تلك القواعد تعدّ التقارير والمعلومات والبيانات المحفوظة في أي شكل، وكذلك الوقائع والأحداث والآراء ونتائج التحاليل المنقولة بواسطة أصحاب المعرفة والخبرة في نطاق الأنشطة والممارسات المنظمة بيّنة مقبولة أمام المحاكم الجنائية لكونها بيانات أكثر دقة ومحفوظة بأسلوب علمي يختلف عن غيرها من الأدلة السماعية، والأدلة الجنائية الإلكترونية من هذا القبيل لكونها معدّة بعمليات حسابية دقيقة لا يتطرق إليها الشك ويتم حفظها آلياً بأسلوب علمي⁽¹⁾.

مع العلم أن قبول الدليل الرقمي كاستثناء من قاعدة شهادة السماع لا ينطبق على جميع أنواع سجلات الحاسوب، حيث تمّ تقسيم هذه السجلات من قبل وزارة العدل الأمريكية - تأسيساً على الأحكام القضائية للمحاكم الاتحادية الأمريكية - إلى ثلاثة فئات⁽²⁾:

الفئة الأولى: السجلات التي تمّ إنشاؤها بواسطة الحاسوب دون تدخل الإنسان: مثل سجلات المكالمات الهاتفية، سجلات البريد الإلكتروني، السجلات المصرفية الإلكترونية، وغيرها. وهذه الفئة لا

(1) انظر: د/محمد الأمين البشري، الأدلة الجنائية الرقمية مفهومها ودورها في الإثبات، ص128، 129.

(2) See: United States Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, July 2002. Printed in 2015. P148-152.

يمكن اعتبارها شهادة سماعية؛ لأنها تتمّ دون قسم، ولا يمكن إخضاعها للاستجواب، وشرط قبول هذه السجلات الحاسوبية في الإثبات هو التأكد بأن الجهاز يعمل بشكل صحيح.

الفئة الثانية: السجلات المحفوظة في الحاسب الآلي والتي تم إنشاؤها بواسطة التدخل المباشر للإنسان: ويشمل هذا النوع البريد الإلكتروني الشخصي، سجلات المحاسبة، وسجلات المعاملات التجارية المدخلة من قبل الأشخاص، سجلات غرف الدردشة، وغيرها. وهذه الفئة تعتبر شهادة سماع، إلا أنها مقبولة أمام القضاء كاستثناء من قاعدة عدم قبول البيئة السماعية، ويشترط للاعتماد على هذا النوع في الإثبات الجنائي التأكد من نسبة هذه المستندات للمتهم.

الفئة الثالثة: السجلات المختلطة: وهذا النوع مزيج من الفئتين الأولى والثانية، حيث تمّ حفظ جزء من السجلات بواسطة الإنسان، والجزء الآخر تم إنشاؤه بواسطة الحاسوب، وهذه الفئة جزء منها يعتبر شهادة سماع، ويشترط للاعتماد على الأدلة الرقمية المتولدة من هذه الفئة شرطان: الأول: توفر شروط صحة الشهادة السماعية المنصوص عليها في القانون الإثبات الفدرالي، والشرط الثاني هو التأكد من أن الحاسوب كان يعمل بشكل صحيح.

الأدلة الرقمية مستثناة من قاعدة الدليل الأفضل: يقصد بالدليل الأفضل وفق تعريف وزارة العدل الأمريكية: "أنه لإثبات مضمون كتابة أو سجل أو صورة فإن أصل الكتابة أو التسجيل أو الصورة يكون مطلوباً".

وقد اشترطت المادة 1002 من قانون الإثبات الفدرالي الأمريكي المعدلة بتاريخ 26 أبريل 2011 توفرّ النسخة الأصلية لتقديمها أمام القضاء حيث نصت على أنه: "مطلوب أصل الكتابة، والتسجيل، أو الصورة من أجل إثبات مضمونها ما لم تنص القواعد أو قانون اتحادي على خلاف ذلك". وهذه المادة تثير إشكالا متعلقا بقبول المستندات الإلكترونية في الإثبات؛ لأنها تؤدي من الناحية النظرية إلى استبعاد الأدلة الرقمية من الإثبات الجنائي، بسبب أن هذه الأدلة غالبا ما يتمّ تقديمها للقضاء على هيئة مستندات معالجة باستخدام الحاسوب، والأصل في الدليل الإلكتروني أنه مجرد إشارات ونبضات مغنطة لا ترى بالعين المجردة، وهذا ما يجعل الأدلة الإلكترونية مجرد صورة طبق الأصل، وبالتالي فهي مجرد مستندات ثانوية، وهذا ما يتعارض مع قاعدة تقديم الدليل الأفضل.

وقد تدخلّ المشرع الأمريكي لإضفاء طابع النسخة الأصلية على المخرجات الحاسوبية تماشيا مع التطور التكنولوجي، حيث قام بتوسيع مفهوم الكتابة والتسجيل والصورة ليشمل الحروف والأرقام والكلمات التي تم كتابتها أو تسجيلها أو تخزينها في أي شكل من الأشكال، حسب الفقرات: (أ)،

ب، ج) من القاعدة 1001 من قانون الإثبات الفيدرالي، وبذلك تعتبر هذه الكتابة أو التسجيل أو الصورة المخزنة في جهاز الحاسوب في صورة كهرومغناطيسية نسخاً أصلية ولا تتعارض مع قاعدة الدليل الأفضل.

واعتبرت الفقرة (د) من القاعدة 1001 من قانون الإثبات الفيدرالي أن النسخة المطابقة للأصل لها ذات حجية الأصل، سواء كانت عبارة عن كتابة أو تسجيل أو صورة في أي شكل كانت، إذا كانت تعكس بدقة المعلومات المتواجدة بالمستند الأصلي. وذهبت الفقرة (هـ) من القاعدة 1001 من ذات القانون إلى أن النسخة المطابقة للأصل هي التي يتم إنتاجها ميكانيكياً أو فوتوغرافياً أو كيميائياً أو إلكترونياً أو عن طريق أي وسيلة تقنية أخرى مساوية تستنسخ الأصل بدقة.

2- موقف التشريع البريطاني: نظم قانون البوليس والإثبات الجنائي لسنة 1984⁽¹⁾ مسألة قبول مخرجات الحاسوب والإنترنت كأدلة إثبات في المواد الجنائية، وخوّلت المادة 20 منه المتعلقة بـ "تمديد صلاحيات الاستيلاء على المعلومات الحاسوبية" السلطات المختصة بالتفتيش الدخول إلى المباني للحصول على أي معلومات موجودة في الكمبيوتر بعد الحصول على إذن قضائي مسبب. وأوجبت المادة 78 من ذات القانون على السلطات القضائية استبعاد جميع الأدلة التي تم الحصول عليها بطريقة غير مشروعة.

ونصت المادة 69 من ذات القانون - التي تم إلغاؤها - على الشروط التي يجب توفرها في الأدلة الحاسوبية لاعتمادها في الإثبات وهي:

- ألا يوجد أساس معقول للاعتقاد أنّ البيان خاطئ أو غير دقيق بسبب الاستعمال الخاطئ للحاسوب.

- يجب أن تكون جميع المكونات المادية للحاسوب تعمل بشكل صحيح، وإذا لم يكن يعمل بشكل صحيح فيجب إثبات أن ذلك لم يؤثر على الوثائق أو دقة محتوياته.

- أيّ من الشروط المحددة في متطلبات القبول المتعلقة بالموضوع يجب أن تخضع لتقدير المحكمة. ويلاحظ أنه قبل إلغاء المادة 69 من قانون البوليس والإثبات الجنائي كان من الضروري إثبات أن الكمبيوتر كان يعمل بشكل صحيح، ولم يستخدم بشكل خاطئ قبل التطرق لإمكانية قبول الدليل

(1) Police and Criminal Evidence Act 1984.

الناتج عن الكمبيوتر، وبعد إلغاء هذه المادة أصبح وجود الدليل الرقمي في جهاز الحاسوب قرينة على أن الجهاز كان يعمل بشكل سليم، وبالتالي يمكن التعويل على هذا الدليل في الإثبات، ويقع عبء إثبات العكس على المتهم.

كما أجازت المادة 133 من قانون العدالة الجنائية لسنة 2003⁽¹⁾ للمحكمة قبول نسخة من المستند إذا كان الأصل غير متوفر، بغض النظر عما إذا كانت تلك الوثيقة لا تزال قائمة أو لا، بشرط التأكد من صحتها، وهذا من شأنه أن ينطبق على المعلومات المخزنة في الأجهزة الإلكترونية.

3- موقف التشريع الكندي: اعتبر قانون الإثبات الكندي أن المستندات الإلكترونية تعتبر أفضل الأدلة، حيث نصت المادة 1.31 فقرة (1) على أن الوثيقة الإلكترونية⁽²⁾ تعتبر أفضل الأدلة في حالة موثوقية نظام السجلات الإلكتروني. كما اعتبرت الفقرة (2) من المادة سائلة الذكر أن الوثيقة الإلكترونية المطبوعة تعتبر أفضل الأدلة إذا كانت واضحة ومنظمة واستخدمت كوثيقة للمعلومات المسجلة أو المخزنة فيها.

واشتطت المادة 3.31 لقبول الوثيقة الإلكترونية المخزنة في الحاسوب كدليل إثبات موثوق:
أ- أن يكون الحاسوب يعمل بشكل صحيح، وإذا لم يكن يعمل بشكل صحيح فيشترط ألا يؤثر العطل على سلامة الوثيقة الإلكترونية، وأنه لا توجد أسباب أخرى معقولة للشك في موثوقية نظام السجلات الإلكترونية.

ب- إذا ثبت أن الوثيقة الإلكترونية المقدمة تم تسجيلها أو تخزينها من قبل الطرف الخصم.
ج- إذا ثبت أن الوثيقة الإلكترونية تم تسجيلها أو تخزينها في المسار العادي للأعمال التي يقوم بها شخص ليس طرفاً في الدعوى ولا يخضع لسلطة الطرف الذي يسعى إلى تدخله.

ثانياً: موقف التشريع اللاتيني: لا يشير اعتماد الأدلة الرقمية في الإثبات الجنائي أي مشكلة في التشريعات ذات الصبغة اللاتينية التي يسود فيها نظام الإثبات الحرّ أو نظام الأدلة المعنوية، وفي ظل هذا النظام لا يقيد القاضي بأدلة معينة يجب عليه الاعتماد عليها في الحكم، بل يترك له مطلق الحرية

(1) Criminal Justice Act 2003.

(2) يقصد بالوثيقة الإلكترونية في قانون الإثبات الكندي حسب المادة 8.31: "البيانات التي يتم تسجيلها أو تخزينها على أي وسيط أو عن طريق نظام كمبيوتر أو جهاز مماثل آخر، والتي يمكن قراءتها أو مشاهدتها من قبل شخص أو نظام كمبيوتر أو جهاز مماثل آخر. ويتضمن الأشياء المعروضة، أو المطبوعة أو أي إخراج آخر من تلك البيانات".

في أن يبني اقتناعه من أيّ دليل يطرح عليه في الجلسة، وأن يقدّر قيمته الإثباتية، بشرط أن يتمّ الحصول عليه بطريق مشروع، وأن يسبب قراره تسبباً منطقياً معقولاً ينسجم مع ظروف القضية وملايساتها.

ثالثاً: موقف التشريع الجزائري من الإثبات الجنائي بالدليل الرقمي

لقد تبوّى المشرّع الجزائري نظام الإثبات المعنوي، وفي ظل هذا النظام لا يرسم القانون طرقاً محددة للإثبات يُقَيّدُ بها القاضي الجنائي، بل يترك حرية الإثبات لأطراف الخصومة في أن يقدموا ما يرون أنه مناسب لإثبات دعواهم، كما يترك للقاضي الحرية في أن يبني قناعته من أيّ دليل يطرح أمامه في الدعوى، وأن يُقدّر قيمة كل دليل، بحسب ما يرتاح إليه ضميره، فالمبدأ السائد في الإثبات الجنائي هو حرية الإثبات، وهذا ما كرّسته المادة 212 من قانون الإجراءات الجزائية، التي تساوي بين الدليل العلمي بصفة عامة و بين باقي الأدلة الأخرى من حيث قوّتها الإثباتية، فقد ورد في هذه المادة بأنه: «يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعاً لاقتناعه الخاص»، كما يستفاد ذلك أيضاً من نص المادة 307 من ق إ ج التي جاء فيها: «إن القانون لا يطلب من القضاة أن يقدموا حساباً عن الوسائل التي بها وصلوا إلى تكوين اقتناعهم، ولا يرسم لهم قواعد بما يتعين عليهم أن يخضعوا لها، على الأخص تقدير تمام أو كفاية دليل ما...».

وقد خلت مواد القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها من بيان طرق إثبات الجريمة المعلوماتية، وفي ذلك إشارة إلى تطبيق القواعد العامة في الإثبات، وأن الجرائم المعلوماتية شأنها شأن جميع الجرائم من حيث طرق إثباتها.

ويتميز نظام الأدلة المعنوية بالدور الفعال للقاضي تجاه الدليل، ويظهر هذا الدور الإيجابي من ناحيتين: فمن ناحية، فإن القاضي حرّ في أن يستعين بجميع طرق الإثبات في الكشف عن الحقيقة، ومن ناحية أخرى فإن القاضي الجنائي حرّ في وزن الأدلة المطروحة في الدعوى، فيأخذ منها ما يرتاح إليه ضميره، وي طرح ما لا يطمئن إليه، دون أن يلزمه المشرّع بأدلة محددة.

ومع أن القانون قد اعترف للقاضي بسلطة واسعة في تقدير الدليل، فإنه قيّده بمجموعة من القواعد حتى لا يُطلق له العنان بحيث يكون لتصوراته دخلاً في النتيجة التي توصل إليها، فاشتراط في الدليل أن يتمّ الحصول عليه بطرق مشروعة، وأن يطرح في الجلسة لمناقشته من الخصوم، وأن يكون واضحاً

غير مشوب بالغموض والإبهام، وأن يتم تسبيب الأحكام، وأي مخالفة لهذه الشروط قد تهدر قيمة الدليل وتشوب الحكم بالبطلان.

وفي هذا السبيل يمكن للقاضي أن يلجأ إلى الخبرة الإلكترونية، حيث تعتبر الخبرة الفنية ضرورة لا غنى عنها في تحصيل الدليل الرقمي ونسبته إلى المتهم نظرا للطابع الفني الخاص للجريمة الإلكترونية، لذا اهتم المشرع الجزائري بتنظيم أعمال الخبرة، وأجاز «الجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع فني أن تأمر بنذب خبير إما بناء على طلب النيابة العامة وإما من تلقاء نفسها أو من الخصوم»⁽¹⁾.

ورغم أن مسألة الرجوع إلى الخبرة أمرٌ جوازيٌّ متروكٌ لتقدير المحكمة، إلا أنها كثيرا ما تجدد نفسها مضطرة إلى الرجوع إلى آراء الخبراء، لمساعدتها في فهم الأدلة الرقمية وتقديرها، باعتبارها مسألة فنية بالغة التعقيد، ذات طبيعة فنية خارجة عن تكوين القاضي وتخصّصه، تتطلب مهارة فنية تُجيد التعامل مع هذا النوع من الأدلة الرقمية، وبدونها يتعذر كشف الدليل وفهمه، وهذا ما أكدته المحكمة العليا في إحدى قراراتها بقولها: «إن الخبرة عملية فنية قد يلجأ إليها القاضي الجزائري إذا وجد نفسه أمام مشكلة تتطلب معرفة خاصة، لذلك يقتضي المنطق والعدالة أن لا يفصل في أمور فنية بحجة تصعب عليه معرفتها بدون أن يستشير رأي أهل الخبرة»⁽²⁾.

وإدراكا من المشرع الجزائري لأهمية الخبرة الفنية في التعامل مع هذا النوع من الجرائم نصّ في الفقرة 4 من المادة 5 من قانون 04-09 على أنه: «يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محلّ البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها».

ولا تخرج القواعد القانونية المنظمة للخبرة في مجال الجريمة الإلكترونية عن القواعد القانونية التي تحكم الخبرة عموما، والتي نظمها المواد من 143 إلى 156 من قانون الإجراءات الجزائية، ولا يتسع المقال هنا لذكرها.

(1) المادة 143/1 ق إ ج. كما نصت المادة 147 على أنه: "يجوز لقاضي التحقيق ندب خبير أو خبراء".

(2) قرار رقم: «47487» صادر عن الغرفة الجنائية الثانية بتاريخ 1988/02/23، المجلة القضائية، عدد 1 لسنة 1992، ص 193.

وتطرح هنا مشكلة تعامل القاضي مع هذه الخبرة الفنية، فهو من جهة دليل فني خارج عن تخصصه لا يمكن أن يفصل فيه دون آراء أهل الخبرة، ومن جهة ثانية فإن الخبرة كغيرها من أدلة الإثبات تخضع لتقدير محكمة الموضوع، وهنا يتعين على القاضي الموازنة بين الخبرة الفنية والاقتناع القضائي، وذلك بأن يميّز بين أمرين: الأول: القيمة العلمية القاطعة للدليل، والأمر الثاني: الظروف والملايسات التي وجد فيها الدليل، فتقدير القاضي لا يتناول الأمر الأول، وذلك لأن قيمة الدليل تقوم على أسس علمية دقيقة، ولا حرية للقاضي في مناقشة الحقائق العلمية الثابتة، أما الظروف والملايسات التي وجد فيها هذا الدليل فإنها تدخل في نطاق تقديره، فهذا من طبيعة عمله⁽¹⁾.

والقاضي وإن كان كامل السلطة في تقدير القوة الإثباتية لعناصر الدعوى، وهو الخبير الأعلى في كل ما يستطيع أن يفصل فيه بنفسه، إلا أنه لا يسوغ له أن يستند في دحض ما قاله الخبير الفني إلى معلومات شخصية، بل يتعين عليه إذا لم يقتنع بتقرير الخبير الفني أن يستعين بخبراء آخرين، لكونه من المسائل الفنية التي لا يصلح للقاضي أن يحلّ فيها محلّ الخبير. فالقاضي لا يملك المنازعة في أمر فني قائم على أصول علمية ثابتة، كما هو الحال بالنسبة للدليل الرقمي، وتطبيقاً لذلك قضت المحكمة العليا في إحدى قراراتها بأنه: «إذا كان قضاة الموضوع غير مُقَيَّدِينَ برأي الخبير فإنه لا يسوغ لهم أن يستبعدوا بدون مبرر نتائج الخبرة الفنية التي انتهى إليها الطبيب في تقريره»، وأكدت ذلك بقولها: «ليس لقضاة الاستئناف أن يفصلوا في أمور فنية بحجة خلافاً لرأي أهل الخبرة دون أن يُبَيَّنُوا في قضائهم أسباب ذلك»⁽²⁾. وعلى هذا استقرّ قضاء محكمة النقض المصرية التي جاء في إحدى قراراتها بأنه: «من المقرر أنه متى تعرضت المحكمة لرأي الخبير الفني في مسألة فنية بحجة فإنه يتعين عليها أن تستند في تفنيده إلى أسباب فنية تحمله وهي لا تستطيع في ذلك أن تحلّ محلّ الخبير فيها»⁽³⁾. كما قضت بأنه: «لا يسوغ للمحكمة أن تستند في دحض ما قال به الخبير الفني إلى معلومات شخصية، بل يتعين عليها إذا ما ساورها الشك فيما قرره الخبير في هذا الشأن أن تستجلى

(1) انظر: د/ هلال عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية. دراسة مقارنة. بحث مقدم لمؤتمر

القانون والكمبيوتر والإنترنت، في الفترة من 1-3 ماي 2000. نشر جامعة الإمارات العربية، الطبعة الثالثة،

2004. ج2 ص724. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، ص22.

(2) قرار صادر بتاريخ 15/05/1984 عن الغرفة الجنائية الثانية، القسم الأول، الطعن رقم: «28616». المجلة

القضائية للمحكمة العليا، العدد الأول لسنة 1990، ص272.

(3) الطعن رقم «1237» لسنة 43 ق. جلسة 1974/1/27. س25. ص74.

الأمر بالاستعانة بغيره من أهل الخبرة لكونه من المسائل الفنية البحتة التي لا يصح للمحكمة أن تحلّ محلّ الخبير فيها»⁽¹⁾.

أما الظروف والملابسات التي وجد فيها الدليل فهي مسألة خاضعة لتقدير القاضي، وهو غير ملزم بآراء الخبراء إذا لم يقتنع بنتائجها، فتقرير الخبير هو من جملة الأدلة المعروضة على المحكمة خاضع للمناقشة، وهذا ما قرره المحكمة العليا في عدة قرارات لها، فقد قضت بأنه: «إن الخبرة كغيرها من أدلة الإثبات خاضعة لتقدير قضاة الموضوع»⁽²⁾، وأكدته في قرار آخر بقولها: «إن تقرير الخبرة لا يقيد لزوما قضاة الموضوع وإنما هو كغيره من أدلة الإثبات قابل للمناقشة والتمحيص ومتروك لتقديرهم وقناعتهم»⁽³⁾. وتطبيقا لذلك يمكن للقاضي أن يطرح الدليل الرقمي - رغم قطعيته من الناحية العملية - إذا رأى أنه لا يتسق منطقيا مع ظروف الواقعة وملابساتها.

والقاضي وإن كان يملك كامل السلطة التقديرية في تقدير حجية الدليل الرقمي وهو الخبير الأعلى في الدعوى، إلا أنه غالبا ما يجد نفسه مضطرا إلى التسليم بما خلص إليه الدليل الرقمي باعتباره من طبيعة فنية لا يستطيع القاضي البتّ فيها بمعزل عن رأي الخبير الرقمي، كما أن الدليل الرقمي غالبا ما يكون هو الدليل الوحيد المتاح في الدعوى، وهو ما يحتّم على القاضي - من الناحية العملية - الأخذ بما خلص إليه التقرير م نتائج واعتمادها كأساس لبناء اقتناعه الشخصي متى لمّس فيه التّزاهة والموضوعية التي تجعله يصدر حكمه وهو مطمئن، طالما أن الأمر يتعلق بدليل فني مبني على أسس علمية دقيقة لا تختمل في الغالب أي مجال للظن والتخمين.

المحور الثاني: شروط قبول الأدلة الرقمية في الإثبات الجنائي

رغم أن الدليل الرقمي هو دليل من جملة الأدلة التي تخضع للسلطة التقديرية للقاضي، من حيث قبوله وقوّته، إلا أن ذلك مقيد بمجموعة من الضوابط التي يجب مراعاتها عند الاعتماد عليه في أحكام الإدانة، يمكن تلخيصها في ثلاثة شروط:

(1) الطعن رقم «1542» لسنة 40 ق. جلسة 1971/1/31. ص 22. ص 119.

(2) قرار صادر بتاريخ 22 جانفي 1981 عن القسم الثاني للغرفة الجنائية الثانية في الطعن رقم: «22641». ذكره جيلالي بغدادي، الاجتهاد القضائي، ج 1 ص 357.

(3) قرار صادر بتاريخ 04 ديسمبر 1988 عن الغرفة الجنائية الأولى في الطعن رقم: «30093». ذكره جيلالي بغدادي، الاجتهاد القضائي، ج 1 ص 358.

الشرط الأول: يقينية الدليل الرقمي: يتعين على القاضي أن يتأكد من يقينية الأدلة الرقمية وعدم قابليتها للشك حتى يمكنه الحكم بالإدانة، فالأحكام الجنائية يجب أن تُبنى على الجزم واليقين لا على الظن والاحتمال، والمتهم بريء حتى تثبت إدانته.

ولا مجال لدحض قرينة البراءة وافتراض عكسها إلا عندما يصل اقتناع القاضي إلى حدّ الجزم واليقين، ويمكن التوصل إلى ذلك من خلال ما يعرض من مخرجات كمبيوترية، سواء كانت مخرجات ورقية تنتجها الطابعات، أو مخرجات إلكترونية كالأقراص المضغوطة، والمستندات، والصور، وأفلام فيديو، وغيرها من الأشكال الإلكترونية التي تتوافر عن طريق الوصول المباشر، أم كانت مجرد عرض لهذه المخرجات المعالجة بواسطة الكمبيوتر، ويصل القاضي إلى يقينية المخرجات الكمبيوترية عن طريق نوعين من المعرفة: أولهما المعرفة الحسية التي يدركها بواسطة حواسه من خلال معاينة هذه المخرجات وفحصها، وثانيهما المعرفة العقلية التي يقوم بها القاضي من خلال الربط بين هذه المخرجات والملايسات التي أحاطت بها⁽¹⁾.

والدليل الرقمي وإن كان مفيدا في الكشف عن الجريمة، إلا أنه قد يعصف بحقوق الأفراد إذا لم يحسن استخدامه، ولذلك يجب مراعاة الضوابط الفنية والقانونية عند استخلاصه حتى يمكن قبوله أمام القضاء، ويجب على المحكمة أن تتأكد من أصالة الدليل الرقمي وسلامته من العبث والتغيير منذ أن تضع عليه السلطة المختصة بالتفتيش يدها وحتى عرضه على المحكمة، وفي سبيل ذلك عليها أن تطرح مجموعة من الأسئلة التي يتعين على أجهزة الضبط القضائي الإجابة عليه، وقد عدّ تقرير صادر عن المعهد الوطني للعدالة التابع لوزارة العدل الأمريكية هذه الأسئلة، ومنها⁽²⁾:

- ما هي الأدلة التي تشير إلى وقوع جريمة إلكترونية؟
- ما هو التسلسل الزمني لوقوع الجريمة؟
- ما هي الأضرار المقدرة؟
- من هو المشتبه به في ارتكابه الجريمة؟ وما هي الدلائل على ذلك؟

(1) انظر: د/ هلاي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، ج2 ص741، 742.

(2) see: Alberto R. Gonzales, Regina B. Schofield, David W. Hagy, Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors, National Institute of Justice, U.S. Department of Justice, Special report, JAN. 2007. NCJ 211314. P15, 16.

- متى وقع الحادث لأول مرة؟ ومتى تمّ اكتشافه؟

- ما هي الإجراءات التي تمّ اتخاذها لتحديد البيانات وجمعها وحفظها وتحليلها؟ وهل هذه الإجراءات كفيلة بالمحافظة على الأدلة الرقمية دون تغيير؟ وينبغي أن تتضمن الإجابة على هذا السؤال وصف دقيق للحالة التي كانت عليها الأدلة الرقمية قبل جمعها وتخزينها، وتحديد جميع الأدوات أو الوسائل المستخدمة في جمعها، وتوثيق التاريخ والوقت الذي تمت فيه عملية الضبط توثيقاً دقيقاً ومتسلسلاً، مع ذكر المكان الذي عثر فيه على الأدلة الرقمية، مع الأخذ بعين الاعتبار أن هذه الأدلة قد تكون موجودة في أكثر من موقع في وقت واحد.

- من هي الجهة التي قامت بضبط الدليل الرقمي والتعامل معه؟ وهنا ينبغي توثيق اسم ووظيفة كل فرد تعامل مع الأدلة الرقمية منذ ضبطها وحتى تسليمها للقضاء.

- ما هي أنواع الأدلة الرقمية التي تمّ جمعها من قبل سلطات التفتيش؟ ويتعيّن هنا ذكر نوع الجهاز الذي ضبط فيه الدليل الرقمي، ورقمه التسلسلي، ولمن تعود ملكيته، وهل كان استخدامه قاصراً على شخص معين أم جهاز مشترك؟ وهل كان الوصول إلى المعلومات محمياً بكلمة مرور؟

الشرط الثاني: خضوع الدليل الرقمي للمناقشة: لا يمكن للقاضي أن يؤسّس اقتناعه إلا على عناصر الإثبات التي طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى، حيث نصت المادة 2/212 ق إ ج على أنه: «... لا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضورياً أمامه». ويتربّب على الإخلال بهذا الشرط بطلان الحكم المبني على دليل لم يطرح للمناقشة، أو لم تُنحَ فرصة لإبداء الرأي فيه⁽¹⁾.

والدليل الرقمي شأنه شأن بقية أدلة الإثبات الجنائي يجب أن يكون ضمن أوراق ملف الدعوى الموضوعة تحت نظر القاضي، وأن يتاح للخصوم الاطلاع عليه ومناقشته في الجلسة إذا أرادوا، كما يمكن للقاضي طلب مثول الخبير الرقمي إلى جلسة المحكمة لمناقشته فيما توصل إليه من نتائج، ليتمكن من تحديد القوة الاستدلالية للدليل الرقمي.

وبغية تمكين المحكمة وأطراف الخصومة من مناقشة الدليل الرقمي يجب تهيئة قاعة المحكمة بالأجهزة والوسائل المناسبة لعرض الأدلة الرقمية، وأن يكون القضاة والمدعي العام وأطراف الخصومة على دراية

(1) انظر: د/ مروك نصر الدين، محاضرات في الإثبات الجنائي، مرجع سابق، ج1 ص457، 458.

بالمسائل الفنية ذات الصلة، نظرا لما يتطلبه هذا النوع من الأدلة من الإلمام بالتكنولوجيا المتخصصة التي تتميز بالدقة والتعقيد، ويمكن استدعاء الشهود والخبراء الفنيين لمناقشتهم في كيفية تحصيل هذه الأدلة ومدى مصداقيتها.

الشرط الثالث: مشروعية الدليل الرقمي: يتعين على القاضي الجنائي أن يستقي قناعته في الحكم من خلال أدلة مشروعة، ولا يمكن الاستناد إلى أدلة غير مشروعة تم الحصول عليها بطرق مخالفة للدستور أو لقانون العقوبات أو قانون الإجراءات الجزائية أو مخالفة لقواعد الآداب والسلوك، ويجب طرحها نهائيا، لأن ما بني على الباطل فهو باطل⁽¹⁾.

والدليل الرقمي كغيره من الأدلة الأخرى يجب أن يتم تحصيله بطريقة مشروعة حتى يمكن الاعتماد عليه في الحكم، والأدلة الجنائية التي يتم الحصول عليها بطرق غير مشروعة يجب أن تكون مستبعدة سواء كانت أدلة تقليدية أم أدلة رقمية، ولا يمكن أن تؤسس عليها أحكام الإدانة، ولا عبء بالدليل الرقمي إذا كان وليد إجراءات باطلة، كأن يتم تحصيله عن طريق تفتيش لم يستوف إجراءاته القانونية، أو نتج عن مراقبة إلكترونية لم تراعى فيها الضوابط الإجرائية المنصوص عليها في القانون.

وقد أوصى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات المنعقد في ريو دي جانيرو بالبرازيل في الفترة بين 4-9 أكتوبر 1994 بشأن جرائم الكمبيوتر في التوصية الثانية المتعلقة بالشق الإجرائي بأنه ينبغي: "لتجنب تعسف السلطات الرسمية، فإن القيود التي ترد على حقوق الإنسان عن طريق رجال السلطة العامة، لا يمكن أن تكون مقبولة إلا في الحالة التي تكون فيها مرتكزة على قواعد قانونية واضحة ودقيقة وملتزمة مع المعايير الدولية لحقوق الإنسان. إن الانتهاكات غير المشروعة لحقوق الإنسان التي يرتكبها رجال السلطة العامة، يمكن أن تبطل الدليل المتحصل عليه، بالإضافة إلى تقرير المسؤولية الجنائية لرجل السلطة العامة الذي انتهك القانون".

(1) انظر: د/ ممدوح خليل بحر، نطاق حرية القاضي الجنائي في تكوين قناعته الوجدانية، ص355؛ أغليس بوزيد، تلازم مبدأ الإثبات الحر بالاقتناع الذاتي للقاضي الجزائي، ص83.

المحور الثالث: موقف الفقه من الإثبات الجنائي بالدليل الرقمي

تذهب معظم الآراء الفقهية ذات الصبغة اللاتينية إلى القول بحجية المخرجات الحاسوبية في الإثبات الجنائي إذا تمّ تحصيلها بطريق مشروع، ففي فرنسا نجد أن مناقشة مسألة اعتماد هذا النوع من الأدلة الجنائية لا يبدو مسألة ملحة أو عاجلة في نظر الفقهاء هناك، فالأساس هو حرّية الإثبات وحرية القاضي في تقدير الأدلة⁽¹⁾.

ولا يختلف الرأي الفقهي في ألمانيا عما هو سائد في فرنسا، إذ يذهب الفقهاء الألمان إلى قبول الدليل الناتج عن الحاسبات الآلية في الإثبات الجنائي تطبيقاً للفقرة الثانية من المادة 224 من قانون الإجراءات الجنائية التي تعطي للمحكمة حرّية اختيار الأدلة وتقدير قيمتها الإثباتية، وهذا يعني أن تكون مخرجات الحاسب بأنواعها المختلفة من مطبوعات أو بيانات أحد المصادر التي تقبلها المحكمة⁽²⁾.

كما ذهب الفقه في الدول الأنجلوسكسونية إلى الإقرار بحجية الأدلة الرقمية في الإثبات الجنائي، ويرى الفقيه الأمريكي (إدوارد وايز (Edward wise) أن الصعوبات الحقيقية في الولايات المتحدة الأمريكية نابعة من عدم الألفة مع تكنولوجيا الحاسب الآلي أكثر من كونها صعوبات قانونية، ولذلك فليست هناك حاجة ماسة إلى سنّ تشريعات بخصوص التعامل مع مقبولة السجلات المعالجة بواسطة الحاسبات الآلية⁽³⁾.

والدليل الرقمي وإن كان مفيداً في الكشف عن الجريمة، إلا أنه قد يعصف بحقوق الأفراد إذا لم يحسن استخدامه، ولذلك يجب مراعاة الضوابط الفنية والقانونية عند استخلاصه حتى يمكن قبوله أمام القضاء، ويجب على المحكمة إذا ما أرادت قبول هذا النوع من الأدلة أن تتأكد بنفسها من مصداقيتها وذلك بمراعاة ما يلي:

أ - التأكد من أنه تم استخلاص الدليل ضمن ضمانات قانونية إجرائية تضمن سلامة وصحة ودقة هذا الاستخلاص.

ب - أن يتم التأكد من حجية هذا الدليل بإجراء اختبارات الثقة.

(1) انظر: د/ هلاي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، ص 722.

(2) المرجع نفسه، ص 723.

(3) المرجع نفسه، ص 729.

ج - أن يتم استخلاص الدليل طبقاً لمبادئ المشروعية الإجرائية والقانونية.

المحور الرابع: موقف القضاء من الإثبات الجنائي بالدليل الرقمي:

أولاً: موقف القضاء الأنجلوسكسوني:

1- موقف القضاء الأمريكي: يذهب القضاء الأمريكي إلى صحة الاعتماد على الأدلة الرقمية في الإثبات الجنائي إذا ما تمّ تحصيلها بطريقة مشروعة، واستجابت لمعايير النزاهة، واعتبرت المحاكم أن الشروط العامة المتعلقة بالتفتيش تنطبق على تفتيش الأجهزة الإلكترونية، يظهر ذلك من عديد أحكامها القضائية، ومن ذلك الحكم الذي أصدرته الدائرة السابعة لمحكمة الاستئناف الأمريكية بتاريخ 1997/6/4 في قضية فرانك ويتاكر (Frank R. Whitaker) المتهم بالتجارة بالمخدرات بالاشتراك مع متهمين آخرين، وتتلخص وقائع القضية في عبور رجال الضبط القضائي على ملفات تحتوي على أسماء متعاملين في التجارة بالمخدرات تحت أسماء مستعارة أثناء تفتيشهم لجهاز حاسوب تعود ملكيته لأحد المتهمين يدعى فروست (Frost) بعد حصولهم على إذن قضائي، فتم إدانة المتهم الأول Whitaker بالحبس لمدة 180 شهراً بناءً على هذا الدليل الإلكتروني. فدفع المتهم بأن المحكمة أخطأت في قبول مطبوعات سجلات الكمبيوتر ضده لأنها غير موثقة بشكل صحيح، حيث تم التلاعب بالبيانات عن طريق إدخال اسمه إلى قاعدة البيانات من طرف المتهم الثاني (Frost)، وهذا يتضمن انتهاكاً لحقوقه الواجبة في محاكمة عادلة بموجب التعديل الخامس للدستور. رفضت محكمة الاستئناف هذا الطعن وذهبت إلى صحة الاعتماد على مخرجات الحاسوب في الإثبات الجنائي إذا تم تحصيلها بطريقة مشروعة، وقالت بأن محكمة المقاطعة لديها سلطة تقديرية واسعة في تحديد الأدلة المقبولة، وأن الأدلة الحاسوبية لا تتعارض مع قاعدة تقديم الدليل الأفضل عملاً بالقاعدة 1001 من قانون الإثبات الفدرالي التي تعتبر البيانات المخزنة في جهاز الكمبيوتر أو جهاز مماثل أو أي مطبوعة أو إخراج آخر يعكس البيانات بدقة هو مستند أصلي⁽¹⁾.

(¹) U.S. V. WHITAKER 127 F.3d 595 (7th Cir. 1997). Appeal No. 96-1352.

انظر تفاصيل الحكم على الرابط: <http://caselaw.findlaw.com/us-7th-circuit/1233418.html>

غير أن القضاء الأمريكي لم يستقرّ على رأي واحد حول كيفية التعامل مع الملفات الموجودة في أجهزة التخزين الرقمية، ووصل إلى استنتاجات مختلفة حول ما إذا كان ينبغي أن يعامل جهاز الكمبيوتر أو أي جهاز تخزين آخر كحاوية مغلقة واحدة أو ينبغي أن يعامل كل ملف على أنه حاوية مغلقة منفصلة يحتاج كل منها إلى إذن خاص بالتفتيش.

فذهبت بعض الأحكام القضائية إلى أن قرص الكمبيوتر الذي يحتوي على ملفات متعدّدة هو حاوية واحدة لأغراض التعديل الرابع للدستور، ومن ذلك الحكم الصادر عن الدائرة الخامسة لمحكمة الاستئناف الأمريكية في قضية (United States v. Runyan) بتاريخ 2001/12/10، وتتلخص وقائع القضية في عثور أجهزة التفتيش على مواد إباحية خاصة بالأطفال في جهاز المتهم أثناء تفتيش بعض الملفات، رأت المحكمة أن الشرطة لم تتجاوز نطاق البحث الخاص عندما فحصت ملفات إضافية موجودة على القرص، وأن قرص الحاسوب يشبه الحاوية المغلقة⁽¹⁾.

وهذا ما أكدته الدائرة التاسعة لمحكمة استئناف الولايات المتحدة الأمريكية في قضية جيبيرسن (United States V. Giberson) بتاريخ 2008 المتهم بجرمة حيازة مواد إباحية خاصة بالأطفال، وتتلخص وقائع القضية في اكتشاف شرطة المرور لولاية لاس فيغاس بتاريخ 24 فبراير 2003 أن المتهم يستخدم وثائق هوية مزورة، وبالتحقيق معه وجد أنه محلّ متابعة قضائية حيث صدرت بحقه ثلاثة أوامر بالاعتقال متعلقة بمخالفات مروية واستخدام هويات مزورة والتهرب من دفع نفقات الحضانة، فاستصدرت سلطات التحقيق إذنا بتفتيش منزله.

وخلال عملية البحث اكتشف ضباط التفتيش جهاز كمبيوتر على مكتب في غرفة نوم Giberson موصول بطابعة، وبجانب الطابعة بطاقات هوية وشهادات ميلاد وبطاقات ضمان اجتماعي مزورة، في ظروف تشير إلى احتمال أنه تم إنشاؤها وطباعتها من الكمبيوتر، فاستصدر الضباط إذنا ثانياً بالتحفظ على جهاز الكمبيوتر وتحريره وإرساله لمختبر الطب الشرعي، وأثناء البحث في ملفات الكمبيوتر عن الملفات المزورة تم اكتشاف غير مقصود لصور إباحية للأطفال، فتم

(1) UNITED STATES v. RUNYAN. 275 F.3d 449 (5th Cir.

2001).Decided: December 10, 2001. Nos. 00-10821, 01-11207.

انظر تفاصيل الحكم على الرابط: [http://caselaw.findlaw.com/us-5th-](http://caselaw.findlaw.com/us-5th-circuit/1018338.html)

circuit/1018338.html

استصدار إذن ثالث بالتفتيش موجّه نحو الصور الإباحية للأطفال، فتم العثور على 700 صورة إباحية للأطفال، قدمت المستخرجات الحاسوبية كأدلة اتّهام عن جنائية التزوير وحيازة صور إباحية للأطفال وأدين المتهم بالسجن لمدة 60 شهرا.

تقدم المتهم بالطعن في الحكم أمام الدائرة التاسعة لمحكمة استئناف الولايات المتحدة الأمريكية، بحجة أن الموظفين المكلفين بإنفاذ القانون تجاوزوا إذن التفتيش الأول عندما استولوا على جهاز الكمبيوتر الخاص به بصورة غير قانونية، وأنه كان ينبغي أن يقتصر التفتيش على الملفات المحتمل أن تكون موجودة في الأماكن المحددة في مذكرة تفتيش، وأنهم تجاوزوا نطاق مذكرة التفتيش الثاني عندما بحثوا عن المواد الإباحية في الحاسوب. وهذا يتعارض مع التعديل الرابع للدستور الأمريكي الذي يحمي الخصوصية والمصالح الدستورية الهامة الأخرى⁽¹⁾، وأنه لا يمكن تفتيش الكمبيوتر إلا بإذن قضائي صريح.

رفضت محكمة الاستئناف الطعن ورأت أن أجهزة الكمبيوتر مثل صناديق صغيرة وشراط الكاسيت يمكن أن تكون مستودعات للوثائق والسجلات، وأجهزة الكمبيوتر لا تشكل استثناء من المبدأ العام الذي يميز الاستيلاء على وثائق معينة بحثا عن وعاء من المحتمل أن يحتوي على تلك الوثائق، والضباط لم يتجاوزوا نطاق مذكرة التفتيش عندما استولوا على جهاز الكمبيوتر، وقالت أنه لا يوجد أي سبب يسمح للضباط بالبحث عن الوثائق المذكورة في مذكرة التفتيش في غرفة كاملة من خزائن حفظ الملفات أو مكتبة الشخص ولا يسمح له بالبحث في الحاسوب. ورأت أنه في ظل التقنيات المتوفرة لم يكن من الممكن إجراء عملية بحث عن وثائق هوية مزورة بطريقة من شأنها أن تجنب احتمال اكتشاف الصور الإباحية للأطفال⁽²⁾.

(1) ينص التعديل الرابع للدستور الأمريكي على أنه «لَا يَجُوزُ الْمَسَاسُ بِحَقِّ النَّاسِ بِأَنْ يَكُونُوا آمِنِينَ فِي أَشْخَاصِهِمْ وَمَنَازِلِهِمْ وَمُسْتَنْدَاتِهِمْ وَمُقْتَنِيَاتِهِمْ مِنْ أَيْ تَفْتِيشٍ أَوْ اخْتِجَازٍ غَيْرِ مَعْقُولٍ، وَلَا يَجُوزُ إِصْدَارُ مُذَكَّرَةٍ بِهَذَا الْخُصُوصِ إِلَّا بِوُجُودِ سَبَبٍ مَعْقُولٍ مُعَزَّزٍ بِالْيَمِينِ أَوْ التَّوَكُّيدِ، وَتُبَيَّنُ بِالتَّخْلِيدِ الْمَكَانَ الْمُرَادَ تَفْتِيشُهُ، وَالْأَشْخَاصَ أَوْ الْأَشْيَاءَ الْمُرَادَ اخْتِجَازُهَا».

(2) United States v. GIBERSON, United States Court of Appeals, Ninth Circuit. 527 F.3d 882 (9th Cir. 2008). Decided: May 30, 2008. No. 07-10100.

في حين ذهبت أحكام قضائية أخرى إلى أنه يجب التعامل مع ملفات الكمبيوتر الفردية على أنها كيانات منفصلة في سياق التفتيش، وتطبيقاً لذلك رفضت الدائرة العاشرة لمحكمة الاستئناف الأمريكية في قضية كاري (United States v. Carey) السماح بالقيام بعمليات تفتيش شاملة في القرص الصلب لجهاز الكمبيوتر في حالة عدم وجود مذكرة بذلك، وقالت: "إن المحقق توسّع بصورة جائرة وتجاوز نطاق بحثه عندما تخلى عن البحث عن أدلة تتعلق بالمخدرات للبحث عن أدلة على المواد الإباحية"⁽¹⁾.

2- موقف القضاء البريطاني: قبل القضاء البريطاني الاعتماد على المخرجات الحاسوبية في الإثبات الجنائي على أساس أنها شهادة مباشرة وليست استثناء من قاعدة شهادة السماع، يظهر ذلك من بعض الأحكام القضائية التي عرضت عليه، ومن بينها قضية (R v Wood) التي حدثت سنة 1983 وتتلخص وقائعها في سرقة بعض المعادن، وبتفتيش جهاز الكمبيوتر الخاص بالمتهم عثر فيه على مستند خاص بالتركيب الكيميائي للمواد المسروقة، وقد قدّمت ورقة مستخرجة من الكمبيوتر كدليل إثبات، فقررت المحكمة قبولها، وقالت إن هذه الورقة تصلح كدليل للإثبات وفقاً للشرعية العامة، ولا تعتبر من قبيل البيّنة السماعية، وعلى المحكمة التأكد من صحة هذه الوثيقة بالرجوع إلى الخبراء الكيميائيين، واستطلاع رأي خبراء البرمجة الحاسوبية للتأكد من أن جهاز الكمبيوتر كان يعمل بشكل سليم⁽²⁾.

انظر تفاصيل الحكم على الرابط: <http://caselaw.findlaw.com/us-9th-circuit/1491017.html>

(¹) United States v. CAREY, United States Court of Appeals, Tenth Circuit. 172 F.3d 1268 (10th Cir. 1999). Decided: April 14, 1999, No. 98-3077.

انظر تفاصيل الحكم على الرابط: <http://caselaw.findlaw.com/us-10th-circuit/1317424.html>

(²) R v Wood (1983) 76 Cr (1982) 76 Cr App R 23. See: Law Reform Commission, consultation paper: documentary and electronic Evidence first published December 2009. P176.

ثانيا: موقف القضاء الفرنسي: يذهب القضاء الفرنسي إلى قبول الأدلة الرقمية في الإثبات الجنائي شريطة أن يتم مراعاة مبدأ الشرعية في تحصيلها، أما إذا تم الحصول على هذه الأدلة بطرق غير مشروعة فقد استقرّ القضاء الفرنسي على أن الأفراد العاديين غير مخاطبين بقاعدة استبعاد الأدلة غير المشروعة، وأن تطبيق هذه القاعدة قاصر على الأعمال التي يباشرها رجال السلطة العامة، وقد صدرت بهذا الخصوص عديد الأحكام القضائية، من ذلك الحكم الصادر في 2013/11/27 عن محكمة النقض الفرنسية في قضية Gilbert المتهم بالتهرب الضريبي واستخدام أموال الشركة وخيانة الأمانة وغسيل الأموال والتزوير، حيث قدّمت بيانات حاسوبية تدين المتهم تم الحصول عليها بطريقة غير مشروعة بسرقتها من حاسوبه الشخصي دون إذن قضائي، فصدر حكم قضائي عن دائرة التحقيق في محكمة الاستئناف في باريس القسم 2 بإحالة المتهم إلى المحاكمة. فتقدم المتهم بالظعن في هذا الحكم أمام محكمة النقض مؤسسا شكواه على أنّ الملفات التي قدّمت كأساس للمحاكمة تم الحصول عليها بطريقة غير مشروعة، وهو ما يتعارض مع قانون الإجراءات الجنائية سيما المادتين 60-2 و 77-1، ومع أحكام المادة 8فقرة 1 من الاتفاقية الأوروبية لحقوق الإنسان. تم قبول الظعن من طرف محكمة النقض، وجاء في قرارها: "عندما يتمّ الحصول على الأدلة بطريقة غير مشروعة من طرف سلطة عامة فإن ذلك يتعارض مع الحق في الخصوصية المحمي بموجب المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان، وتحديدًا الحق في حماية البيانات الشخصية، ومع قانون الإجراءات الجنائية خصوصا المادتين 60-2 و 77-1 الذي يوجب الحصول على إذن قضائي، في حين إذا تم جمعها بطريقة غير مشروعة من قبل الأفراد العاديين فإنها تكون مقبولة في الإثبات بشرط أن لا تتدخل السلطات العامة بشكل مباشر أو غير مباشر في إنتاجها أو تصنيفها"⁽¹⁾.

ثالثا: موقف القضاء المصري: يتجه القضاء المصري إلى الاعتماد على الدليل الرقمي في الإثبات الجنائي إذا ما اقتنع به القاضي، تأسيسا على مبدأ الإثبات الحرّ الذي يعطي القاضي سلطة واسعة في وزن الأدلة وتقدير قيمتها الإثباتية لا يقيّده في ذلك سوى ضميره، ومن الأحكام الحديثة المتعلقة بذلك الحكم الصادر عن محكمة النقض المصرية بتاريخ 2012/11/28 في القضية المتعلقة بجريمة

(1) Arrêt n° 13-85042 du 27 novembre 2013. Cour de cassation –
Chambre criminelle. Publié au bulletin des arrêts-Chambre criminelle, n°
9. Novembre 2013. P456-459.

سب وتعمد إزعاج وتعدي على حرمة الحياة الخاصة باستخدام الإنترنت، وتتلخص وقائع القضية في قيام المتهم بنقل صور خاصة بالمجني عليهما بغير رضاها باستخدام الحاسب الآلي الخاص بالشركة محلّ عمله عبر شبكة المعلومات الدولية، وتعتمد إزعاج ومضايقة المجني عليهما باستعمال أجهزة الاتصالات حيث قام بإرسال رسائل إلى البريد الإلكتروني الخاص بالغير عبر البريد الإلكتروني الخاص به يتضمن عبارات سب، وقد تمّ إدانته بعشرين ألف جنيه والمصاريف القضائية، وألزمته بأن يؤدي للمدعي بالحقوق المدنية مبلغ خمسة آلاف جنيه وواحد على سبيل التعويض المدني المؤقت.

قام المتهم بالطعن في الحكم بحجة أنّ الحكم المطعون فيه قد شابته القصور في التسبب والإخلال بحق الدفاع، ذلك بأنه لم يدلّل على توافر أركان الجريمة، ولم يعرض لدفاعه بانتفاء صلته بها، لأنه لم يرسل أية رسائل من الحاسب الآلي الخاص به، وإنما تم إرسالها من الشركة التي يمثلها المجني عليه ومن موقعها الذي يستخدمه جميع العاملين بها، وليس الشخص الوحيد الذي يستخدم ذلك الجهاز.

رفضت محكمة النقض هذا الطعن ورأت أنّ الأدلة التي استند إليه حكم الإدانة - ومنها تقرير الفحص بقسم المساعدات الفنية من وزارة الداخلية إدارة مكافحة جرائم الحاسب الآلي وشبكة المعلومات - أدلة سائغة من شأنها أن تؤدي إلى ما رتبّه الحكم عليها، وقالت في حيثيات حكمها: "إنّ ما يثيره الطاعن في هذا الخصوص ينحلّ إلى جدل موضوعي حول سلطة محكمة الموضوع في تقدير الدليل، وهو مما تستقلّ به، ولا يجوز مجادلته فيه أو مصادرة عقيدته بشأنه أمام محكمة النقض... كما أنّ لمحكمة الموضوع كامل الحرّية في تقدير القوّة التدلّيلية لتقرير الخبر المقدم إليها والفصل فيما يوجه إليه من اعتراضات، وما دامت المحكمة قد اطمأنت إلى ما جاء به فلا يجوز مجادلتها في ذلك" (1).

خاتمة:

من خلال الدراسة تبين لنا أنه لا خلاف بين التشريعات المقارنة في قبول الأدلة الجنائية الإلكترونية في الإثبات الجنائي، رغم اختلافهم في الشروط الواجب توفرها في هذا الدليل حتى يكتسب حجّيته

(1) الطعن رقم «567» لسنة 82 ق. جلسة 2012/11/28. تم مشاهدته بتاريخ 2015/10/11 على موقع

المحاميين العرب على الرابط:

<http://www.mohamoon.com/montada/Default.aspx?Action=Display&ID=117044&Type=3>

الإقناعية، ولا يختلف الأمر في التشريع الجزائي الذي اعتنق مذهب الإثبات الحر الذي يعطي القاضي الجنائي حرية واسعة في تقدير قيمة الأدلة عموما ومنها الدليل الإلكتروني، غير أنه لما كان الدليل الإلكتروني ذا صبغة فنية، فإنه يمكن للقاضي الجنائي اللجوء إلى الخبرة الفنية في ضبط الدليل الإلكتروني وفهمه، لكنه يبقى هو صاحب السلطة التقديرية في تقييم الدليل الإلكتروني والاعتماد عليه من عدمه، بشرط أن يسبب قراره تسببا منطقيا معقولا.

إشكالية الحصول على الدليل الجنائي في الجرائم المعلوماتية

ط.د/ فلاك مراد

كلية الحقوق والعلوم السياسية

جامعة أم البواقي

مقدمة:

إن التطور المدهش للإنترنت، أدى إلى نشوء جرائم ناتجة عن ذلك الاستخدام، و هذه الجرائم قد تقع على الإنترنت نفسه أو قد تقع بواسطته، بحيث يصبح أداة في يد الجاني يستخدمه ليحقق أغراضه الإجرامية نظرا لظهور مشكلة جرائم الكمبيوتر كمسكلة أمنية، وقانونية واجتماعية، فإن خبراء الأمن المعلوماتي وصانعي السياسات الحكومية ومسوقي الكمبيوتر، والأفراد المهتمين بهذا الموضوع في حاجة إلى تغيير نظرهم تجاه جرائم الكمبيوتر، لا لأنها مشكلة وطنية فقط، وإنما كمسكلة عالمية، وتتطلب الإجراءات الوطنية تعاوننا في مجالي القطاع العام والخاص، فبخصوص القطاع الخاص الالتزام بإجراءات الوقاية، وبخصوص القطاع العام تنفيذ الإجراءات اللازمة لمكافحة الجريمة وبوجه عام.

واعتبارا لهذا الازدياد السريع للجرائم الإلكترونية، فقد ذهبت جل الدول إلى وضع تشريعات جنائية خاصة لمكافحة الجرائم الإلكترونية، هذه الظاهرة المستحدثة في علم الإجرام ومن هذه الدول الولايات المتحدة الأمريكية و فرنسا وهولندا و الاتحاد الأوروبي؛ هذا الأخير الذي وضع اتفاقية حول جرائم الكمبيوتر سنة 2000.

وكما هو الحال في كل دول العالم استفحلت الجريمة الإلكترونية في الجزائر خلال العقود الأخيرة، وأصبح القضاء الجزائري في محك حقيقي، عندما وضعت أمامه قضايا تتعلق بالجرائم الإلكترونية. ونظرا لهذا التطور الذي عرفته الجريمة في الجزائر، قام المشرع الجزائري بتعديل قانون بموجب قانون العقوبات رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتمم للأمر رقم 66-156 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى المادة 394 مكرر 7.

لكل هذه الأسباب كان لابد من الاشتغال على وسائل الإثبات و تطويرها، بحيث أصبح ما يعرف بالإثبات الإلكتروني أو الرقمي، متجاوزا تلك الإثباتات التقليدية و استبدال الملفات الورقية بالأسطوانات الضوئية أو الأقراص الممغنطة.

هنا يمكن طرح الإشكال على الشكل التالي: ما هي آليات الحصول على الدليل في الجرائم الإلكترونية؟ و إلى أي حد يمكن قبول الأدلة الرقمية كوسائل إثبات؟ و ما هي الصعوبات التي يطرحها الحصول على الدليل الإلكتروني؟

وللإجابة عن الإشكال سوف نتبع التصميم التالي:

المطلب الأول: ماهية الدليل في الجريمة الإلكترونية.

المطلب الثاني: الإجراءات التقليدية للحصول على الدليل الإلكتروني.

المطلب الأول: ماهية الدليل في الجريمة الإلكترونية

بعد الإثبات الجنائي بالأدلة الرقمية من أبرز تطورات العصر الحديث، و التي جاءت لتلائم الثورة العلمية و التكنولوجية و التقنية في عصرنا الحالي، و التي تطور معها الفكر الإجرامي الذي صاحب ظهور ما يعرف بالجريمة الإلكترونية ألقى على عاتق القائمين على مكافحة الجريمة في الدولة عبئا شديدا و مهاما جسيمة تفوق القدرات المتاحة لهم و فق أسس و قواعد و إجراءات البحث الجنائي و الإثبات الجنائي التقليدي، نظرا لعدم كفاية و عدم ملائمة هذه النظم التقليدية في إثبات تلك الجرائم سواء من الناحيتين القانونية أو التقنية، الشيء الذي ألزم على المشرع أن يتدخل بقوانين تتناسب مع مثل هذه الجرائم.

فكانت هذه التطورات التي عرفت المعلومات كقيلة لتجعل الإثبات الجنائي يتأثر من جراء الجرائم التي أفرزتها هذه الثورة المعلوماتية، الأمر الذي جعل من طبيعة الإثبات بالوسائل التقليدية أمر متجاوز، ولعل هذه الطبيعة غير المرئية للأدلة المتحصلة من الوسائل الإلكترونية تلقى بظلالها على الجهات التي تتعامل مع الجرائم التي تقع بالوسائل الإلكترونية حيث تصعب قدرتهم على فحص واختبار البيانات محل الاشتباه خاصة في حالات التلاعب في برامج الحاسوب، ومن ثم فقد يستحيل

عليهم الوصول إلى الجناة¹. فمن المعلوم أن جهات التحري والتحقيق اعتادت على الاعتماد في جمع الدليل على الوسائل التقليدية للإثبات الجنائي التي تعتمد على الإثبات المادي للجريمة ولكن في محيط الإلكترونيات فالأمر مختلف، فالمتحري أو المحقق لا يستطيع أي منهما تطبيق إجراءات الإثبات التقليدية على المعلومات المعنوية.

أولاً: ماهية الدليل الرقمي

يقصد بالإثبات إقامة الدليل على وقوع الجريمة و على نسبتها إلى المتهم، أي إثبات الوقائع، فليس هناك من شك في أن وصول القاضي الجنائي إلى حكم يعبر عن الحقيقة في الواقعة المطروحة عليه، ليس بالأمر الهين، لذلك فالقاضي ملزم بإقامة الدليل على وقوع هذه الجريمة و على مسؤولية المتهم عنها. و هذا يستلزم على القاضي أن يستعين بوسائل تعيد أمامه تفاصيل حدوث الجريمة، و هذه الوسائل هي وسائل الإثبات، ومن هنا تأتي مسؤولية الدليل في المسائل الجنائية هذا من ناحية، أما من ناحية أخرى فعملية الإثبات الجنائي في الجرائم الرقمية تركز على الدليل الرقمي باعتباره الوسيلة الوحيدة و الرئيسية لإثبات الجريمة، و هو محور اهتمام بحثنا. بداية نشير إلى أن الأدلة الإلكترونية المستخرجة من الأنترنت، قد تكون مستخرجات ورقية يتم إنتاجها عن طريق الطابعات (les imprimantes)، أو مستخرجات لا ورقية لكنها إلكترونية كالأقراص الممغنطة أو أسطوانات الفيديو أو الأقراص الضوئية و غيرها من الأشكال غير التقليدية، إضافة أن هناك نوع ثالث يتمثل في عرض المستخرجات المعالجة بواسطة الحاسوب². وعموما يُعرف الدليل الرقمي بأنه: هو الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ و تطبيق القانون³. كما يمكن تعريف الدليل الإلكتروني بأنه: هو تلك المعلومات التي يقبلها المنطق و العقل و

¹ - أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية الإسكندرية، 2009، ص25.

² - عبد الفتاح بيومي حجازي، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت، دار الكتب القانونية مصر 2006، ص 81.

³ - أمير فرج يوسف، مرجع سابق، ص29.

يعتمدها العلم، يتم الحصول عليها بإجراءات قانونية و علمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي و ملحقاتها و شبكات الاتصال، و يمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة¹.

ولذا بالاستفادة مما سبق يمكن تعريف الدليل الرقمي بأنه: مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التي يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية.

ثانياً: أنواع الدليل الإلكتروني

إن التعريف بالدليل الرقمي يحتم علينا تحديد أنواعه و أشكاله حتى يتسنى فهم الهيئة التي يتخذها للحكم على قيمته القانونية فيما بعد، بحيث يمكن تقسيم الدليل الرقمي لنوعين رئيسين هما:

1 - أدلة أعدت لتكون وسيلة إثبات

وهذا النوع من الأدلة الرقمية يمكن إجمالها فيما يلي:

- السجلات التي تم أنشاؤها بواسطة الآلة تلقائياً، وتعتبر هذه السجلات من مخرجات الآلة التي لم يساهم الإنسان في إنشائها مثل سجلات الهاتف وفواتير أجهزة الحاسب الآلي.
- السجلات التي جزء منها تم حفظه بالإدخال وجزء تم إنشاؤه بواسطة الآلة ومن أمثلة ذلك البيانات التي يتم إدخالها إلى الآلة و تتم معالجتها من خلال برنامج خاص، كإجراء العمليات الحسابية على تلك البيانات.

2- أدلة لم تعد لتكون وسيلة إثبات

وهذا النوع من الأدلة الرقمية نشأ دون إرادة الشخص، أي أنها أثر يتركه الجاني دون أن يكون راغباً في وجوده، ويسمى هذا النوع من الأدلة بالبصمة الرقمية، وهي ما يمكن تسميته أيضاً بالآثار المعلوماتية الرقمية، وهي تتجسد في الآثار التي يتركها مستخدم الشبكة المعلوماتية بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الآلة أو شبكة المعلومات العالمية².

وتبدو أهمية التمييز بين هذين النوعين فيما يلي:

¹ - هشام محمد رستم: الجوانب الإجرائية للجرائم المعلوماتية . مكتبة الآلات الحديثة أسبوط 1994، ص 31

² - عبد الفتاح بيومي حجازي ، مرجع سابق ، ص 84.

- النوع الثاني من الأدلة الرقمية هو الأكثر أهمية من النوع الأول لكونه لم يُعد أصلاً ليكون أثراً لمن صدر عنه، ولذا فهو في العادة سيتضمن معلومات تفيد في الكشف عن الجريمة ومرتكبها.

- يتميز النوع الأول من الأدلة الرقمية بسهولة الحصول عليه لأنه أُعد أصلاً لأن يكون دليلاً على الوقائع التي يتضمنها، في حين يكون الحصول على النوع الثاني من الأدلة بإتباع تقنية خاصة لا تخلو من صعوبة وتعقيد.

- لأن النوع الأول قد أُعدَّ كوسيلة إثبات لبعض الوقائع فإنه عادة ما يُعتمد إلى حفظه للاحتجاج به لاحقاً وهو ما يقلل من إمكانية فقدانه، و على عكس النوع الثاني حيث لم يُعد ليحفظ ما يجعله عرض للفقدان لأسباب منها فصل التيار الكهربائي عن الجهاز مثلاً.

ثالثاً: أشكال الدليل الإلكتروني

يتخذ الدليل الرقمي ثلاثة أشكال رئيسة هي:

1 - **الصور الرقمية:** وهي عبارة عن تجسيد الحقائق المرئية حول الجريمة، وفي العادة تقدم الصورة إما في شكل ورقي أو في شكل مرئي باستخدام الشاشة المرئية، والواقع أن الصورة الرقمية تمثل تكنولوجيا بديلة للصورة الفوتوغرافية التقليدية و هي قد تبدو أكثر تطوراً ولكنها ليست بالصورة أفضل من الصور التقليدية .

2 - **التسجيلات الصوتية:** وهي التسجيلات التي يتم ضبط وتخزينها بواسطة الآلة الرقمية، وتشمل المحادثات الصوتية على الانترنت والهاتف الخ.

3- **النصوص المكتوبة:** وتشمل النصوص التي يتم كتابتها بواسطة الآلة الرقمية، ومنها الرسائل عبر البريد الإلكتروني، والهاتف المحمول، والبيانات المسجلة بأجهزة الحاسب الآلي، الخ.

رابعاً: خصائص الدليل الإلكتروني

يتميز الدليل الجنائي الإلكتروني عن الدليل الجنائي التقليدي بعدة خصائص يمكن رصد مجملها فيما يلي:

- الأدلة الرقمية تتكون من بيانات و معلومات ذات هيئة إلكترونية غير ملموسة، لا تدرك بالحواس العادية، بل يتطلب إدراكها الاستعانة بالأجهزة و المعدات و الأدوات الآلية (hardware) ، و استخدام نظم برمجية حاسوبية (software)¹.

¹ - محمد عادل ريان، جرائم الحاسب الآلي وأمن البيانات، بيروت، 2002، ص 43.

- الأدلة الرقمية ليست أقل من الدليل المادي فحسب، بل تصل إلى درجة التخيلية في شكلها و حجمها و مكان تواجدها غير المعلن.

- يمكن استخراج من الأدلة الرقمية الجنائية نسخ مطابقة للأصل ولها ذات القيمة العلمية و الحجية الثبوتية الشيء الذي لا يتوفر في أنواع الأدلة (الأخرى التقليدية)، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد، و التلف، و التغيير، عن طريق نسخ طبق الأصل من الدليل¹.

- يتميز الدليل الرقمي بصعوبة محوه أو تحطيمه، إذ حتى في حالة محاولة إصدار أمر بإزالة ذلك الدليل فمن الممكن إعادة إظهاره من خلال ذاكرة الآلة التي تحتوى ذلك الدليل.

المطلب الثاني: الإجراءات التقليدية للحصول على الدليل الإلكتروني.

على الرغم من وجود تشابه كبير بين التحقيق في جرائم الإنترنت وبين التحقيق في الجرائم الأخرى فهي جميعاً تحتاج إلى إجراءات تتشابه في عمومها مثل المعاينة والتفتيش والشهادة و الخبرة بالإضافة إلى جمع الأدلة، كما أنها تشترك في كونها تسعى إلى الإجابة على الأسئلة المشهورة لدى المحقق، ماذا حدث؟ وأين؟ ومتى؟ وكيف؟ ومن؟ ولماذا؟.

وتظل الجرائم المتعلقة بشبكة الإنترنت تمتاز عن غيرها من الجرائم ببعض الخصائص وهذا بالطبع يستدعي تطوير أساليب التحقيق الجنائي وإجراءاته بصورة تتلاءم مع هذه الخصوصية، وتمكن المحقق من كشف الجريمة والتعرف على مرتكبيها بالسرعة والدقة اللازمين للتحقيق في هذا النوع من الجرائم يستدعي الرجوع إلى عدد كبير من السجلات التي يجب الاطلاع عليها مثل الكتيبات الخاصة بأجهزة الحاسب الآلي، وملفات تسجيل العمليات الحاسوبية، بالإضافة إلى الاطلاع على كم كبير من السجلات عن خلفية المنظمة وموظفيها.

ومما لا شك فيه أن هذه الجرائم غيرت أسلوب عمل أجهزة البحث و التحقيق، و فرضت عليه التعامل مع مسرح جريمة غير معتاد يقع في عالم افتراضي، وفي بيئة تقنية تتطلب مهارات و قدرات و تقنيات خاصة قد لا تتوفر معظم هذه الأجهزة مما فرض عليها كذلك تخصيص فرق متخصصة و متكونة في مجال تقنيات المعلومات ورصدها لمكافحة هذه الجرائم.

¹ - هشام محمد رستم ، مرجع سابق ، ص 36.

فعلى المستوى الإجرائي تشكل الإجراءات التقليدية من معاينة وتفتيش والاستماع إلى الشهود و ندب الخبراء أساس عمل أجهزة البحث و التحقيق قصد الحصول على الأدلة الجنائية، للثبوت من الجريمة و ضبط مرتكبيها و تقديمهم للمحاكمة.

ويعتد كل من المعاينة و التفتيش و الشهادة من أحد وسائل جمع الأدلة ولكل منها قواعده يتم إتباعها، وستتناول كل واحدة على النحو التالي:

أولاً: المعاينة

يرى البعض أن أهمية المعاينة تتضاءل في الجريمة المعلوماتية، وذلك لندرة تخلف آثار مادية عند ارتكاب الجريمة المعلوماتية، كما أن طول فترة الوقوع بين وقوع الجريمة و ارتكابها و بين اكتشافها يكون له تأثير سلبي على الآثار الناجمة عنها سواء بسبب العبث أو المحو أو التلف لتلك الآثار¹. ويقصد بالمعاينة أنها "رؤية العين لمكان أو شخص أو أي شيء لإثبات حالته و ضبط كل ما يلزم لكشف الحقيقة"، و يقصد بها كذلك أنها "إثبات مادي و مباشر لحالة الشخص و الأشياء والأمكنة ذات صلة بالحادث"².

كما يقصد بالمعاينة الكشف الحسي المباشر لإثبات حالة شيء أو شخص، وتتم إما بانتقال المحقق إلى مكان آخر أو بجلب موضوع المعاينة إلى مقره كما في معاينة العملات المزورة أو الأشياء و الأسلحة و الأوراق التي استخدمت في اقتراف الجريمة أو مكان و آثار الجريمة أو الكشف عن المجني عليه لإثبات آثار الجريمة من ضرب أو جرح أو قتل أو فحص المدعى عليه لإثبات حالته المرضية أو ما تعرض له من ضرب و تعذيب

فالمعاينة وسيلة بواسطتها يتمكن القاضي من الإدراك المباشر للجريمة ومرتكبها وقد تشمل النتائج المادية التي تخلفت عنها أو إثبات حالة الأماكن أو الأشياء أو الأشخاص التي لها علاقة بالجريمة أو إثبات الوسيلة التي استخدمت في ارتكابها أو المكان الذي وقعت فيه الجريمة³.

و تتم المعاينة بأية حاسة من الحواس، مثل المس و السمع و البصر و الشم والتذوق. والمعاينة قد تكون شخصية فتتصب الملاحظة على شخص، ويستوي أن تتناول المعاينة المجني عليه أو المتهم كما

¹ - عبد الفتاح مراد ، شرح جرائم الكمبيوتر و الانترنت ، دار الكتب والوثائق المصرية ، 2005، ص 65.

² - هشام محمد رستم ، مرجع سابق ، ص 39.

³ - عبد الفتاح بيومي حجازي ، مرجع سابق ، ص 92.

إذا كان الغرض منها إثبات أثار الإكراه بالجني عليه في جريمة السرقة، وقد يكون موضوع المعاينة شخصا على قيد الحياة. وفي الجرائم المعلوماتية تكون فرصة الحصول على الدليل الإلكتروني ضئيلة مقارنة مع الجرائم الأخرى.

أما الجهة التي أسندت إليها المهمة الخاصة بإجراء المعاينة فهي الشرطة القضائية التي عليها في حال علمها بارتكاب جريمة أو جنحة أن تخبر بها النيابة العامة و أن تنتقل في الحال إلى مكان ارتكاب الجريمة من أجل إجراء المعاينة كما ينبغي على الشرطة القضائية أن تحافظ على الأدلة القابلة للاندثار و التحفظ على مكان الجريمة و المحافظة على كل ما قد يوصل إلى الحقيقة¹.

وفي كل الأحوال عند تلقي بلاغ عن وقوع جريمة إحدى الجرائم الإلكترونية و التأكد من صحة الخبر و البيانات المتضمنة في الخبر، يتم الانتقال إلى مسرح الجريمة من أجل المعاينة، و مسرح الجريمة المعلوماتية يختلف عن المسرح الخاص بالجريمة التقليدية كالقتل و السرقة.

وإن كانت الجريمة واردة في كل الجرائم، إلا أن أهميتها تتضاءل في بعض الجرائم مثل جريمة التزوير المعنوي و جريمة السب فإن المعاينة فيها غير ذات جدوى، أما معاينة الجريمة التقليدية و الاطلاع على مسرح الجريمة فيها فيكون ذات أهمية متمثلة في تصور كيفية وقوع الجريمة و ظروف ملابس ارتكابها، إلا أن إجراء المعاينة في الجريمة الإلكترونية يتقيد بعدة ضوابط أهمها²:

- تصوير الحاسب الآلي والأجهزة الطرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ و مكان التقاطها.
- قطع التيار الكهربائي من موقع المعاينة لشل فاعلية الجاني من القيام بأي فعل من شأنه التأثير أو محو الآثار.
- إخطار الفريق الذي سيتولى المعاينة قبل موعدها بوقت كافٍ حتى يستعد من الناحية الفنية و العملية، و ذلك لكي يضع الخطة المناسبة لضبط أدلة الجريمة حال معاينتها.
- التحفظ على مستندات الإدخال و المخرجات الورقية للحاسب ذات صلة بالجريمة.

¹ - محمد عادل ريان ، مرجع سابق ، ص 46.

² - عبد الفتاح بيومي حجازي ، مرجع سابق ، ص 93.

- عدم نقل أي مادة معلوماتية مسرح الجريمة قبل إجراء اختبار التأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال لقوى مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة.

ثانياً: التفتيش

عرفت الأنظمة الجنائية في مراحل تطورها أنواعاً من الإجراءات تنطوي على انتهاك لحقوق الفرد الأولية في سبيل تتبع الجناة ومحاکمتهم ومنها القبض والتفتيش فإذا ما تخلت يد العدالة عن التعرض لحقوق الأفراد أصبحنا إزاء فوضى إجرامية.

ويعتبر التفتيش إجراء من إجراءات التحقيق، يهدف إلى البحث عن أشياء تتعلق بالجريمة، وكل ما يفيد بصفة عامة في كشف الحقيقة، سواء تعلق بالأشخاص أو بالأماكن. وللتفتيش شروط موضوعية تتعلق ب¹:

أ- بسببه: وقوع جريمة بالفعل تعد جنابة أو جنحة، وإن يوجه اتهام إلى الشخص المراد تفتيشه أو تفتيش مسكنه.

ب- الغاية منه: ضبط أشياء تفيد في كشف الحقيقة.

والشروط الشكلية تتحدد بـ:

أ- أن يكون الأمر بالتفتيش مسبباً.

ب- حضور المتهم أو من ينيبه أو الغير أو من ينيبه التفتيش.

ج- تحرير محضر بالتفتيش.

ويثور السؤال عن إمكانية التفتيش وفقاً للضوابط السابقة والغاية منه في مجال الجرائم الإلكترونية ؟ والغرض من هذا السؤال يتضح من أن التفتيش بالمعنى التقليدي يهدف إلى حفظ أشياء مادية تتعلق بالجريمة وتفيد في كشف الحقيقة، بينما البيانات الإلكترونية ليس لها بحسب جوهرها مظهر مادي ملموس في العالم الخارجي. ومع ذلك فيمكن أن يرد التفتيش على هذه البيانات غير المحسوسة عن طريق الوسائط الإلكترونية لحفظها وتخزينها كالأسطوانات والأقراص الممغنطة، ومخرجات الحاسب.

ولهذا فقد أجاز الفقه والتشريعات التي صدرت في هذا المجال إمكانية أن يكون محل لتفتيش البيانات المعالجة آلياً، والمخزنة بالحاسب الآلي، ثم ضبطها والتحفيز عليها، أو ضبط الوسائط الإلكترونية التي

¹ - منى الأشقر، القانون والانترنت " تحدي التكيف والضبط "، بيروت، الناشر ش م م مصر، 2008، ص 70.

سجلت عليها هذه البيانات .والتفتيش في هذه الحالة يخضع لما يخضع له التفتيش بمعناه التقليدي من ضوابط وأحكام فالتفتيش أو البحث في الشبكات الإلكترونية يسمح باستخدام الوسائل الإلكترونية للبحث في أي مكان عن البيانات أو الأدلة المطلوبة¹.

ومحل التفتيش وما يتبعه من ضبط يشمل: البرامج أو الكيانات المنطقية Les logiciels ، البيانات المسجلة في ذاكرة الحاسب أو في مخرجاته - السجلات المثبتة الاستخدام نظام المعالجة الآلية للبيانات - دفتر يومية التشغيل وسجل المعاملات - السجلات الخاصة بعمليات الدخول إلى نظام المعالجة الآلية للبيانات، ويتعلق بها من سجلات كلمات السر، ومفاتيح الدخول، ومفاتيح فك الشفرة. ونظرا لكون التفتيش يتضمن تقييداً للحرية الفردية ويمثل اعتداء على حرمة الحياة الخاصة فيجب أن تتوفر فيه الضمانات القانونية اللازمة لصحته ومنها أن يتم صدور أمر قضائي مسبب بشأنه وأن يباشره الشخص أو الجهة المختصة (النيابة العامة، أو الشرطة القضائية). وبحسب الأصل يجب أن يصدر إذن التفتيش مكتوباً إلا أن هذا الشرط يحمل بعض المخاطر أحيانا وذلك في حالة ما إذا كان البحث عن أدلة الجريمة يستدعي أن يتم التفتيش في مكان آخر في نظام معلوماتي آخر غير الذي صدر بشأن الإذن المكتوب. صدر والمخاطر تتمثل في إمكانية قيام الجاني بتدمير، أو محو البيانات، أو نقلها، أو تعديلها، خلال الفترة التي يراد الحصول على إذن مكتوب بشأنها. ولمواجهة هذه المخاطر، يرى البعض أن الإذن الأول بالتفتيش في مكان ما يجب أن يتضمن الإذن بتفتيش أي نظام معلوماتي آخر يوجد في أي مكان غير مكان البحث². ويشتر امتداد الإذن بالتفتيش إلى أماكن أو أنظمة أخرى، غير الواردة في الإذن الأول بعض المشكلات، يتعلق أولها برفض صاحب المكان أو النظام الآخر مباشرة التفتيش لديه، يرى البعض في هذه الحالة عدم استمرار أو امتداد البحث لديه إلا في حالتي التلبس، أو رضائه بالتفتيش. ويرى البعض أنه في حالة امتداد الاختصاص، فيمكن أن يصدر الأمر بالإمداد شفوياً من قاضي

¹ - أمير فرج يوسف، مرجع سابق، ص33.

² - سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، د. ط، دار الكتب القانونية مصر، 2012، ص113.

التحقيق، تحقيقا للسرعة المطلوبة، ثم يصدر فيما بعد الإذن المكتوب، وفي جميع الأحوال يجب أن يكون الإذن مسببا، لتتمكن الجهة القضائية من مراقبة مدى مشروعيته¹. و عموما فالتفتيش في الجرائم المعلوماتية يكون محله كل مكونات الحاسب الآلي سواء كانت مادية أو معنوية، وكذلك شبكات الاتصال الخاصة به، بالإضافة إلى الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش و تشمل جميع مكوناته، و يستلزم تفتيش الحاسب الآلي مجموعة من الأشخاص لديهم الخبرة و المهارة التقنية .

ثالثا: الخبرة

الخبرة هي الوسيلة التي من خلالها تستطيع سلطة التحقيق أو المحكمة تحديد التفسير الفني للأدلة أو الدلائل بالاستعانة بالمعلومات العلمية، فهي في حقيقتها ليست دليلا مستقلا عن الدليل القولي أو المادي وإنما هي تقييم فني لهذا الدليل. فهي في مجملها تقرير صادر عن الخبير في أمر من الأمور المتعلقة بالجريمة.

والعنصر المميز للخبرة عن غيرها من إجراءات الإثبات كالمعانة والشهادة والتفتيش هو الرأي الفني للخبير في كشف الدلائل أو تحديد قيمتها التدليلية في الإثبات والذي يتطلب معارف علمية أو فنية خاصة لا تتوافر سواء لدى المحقق أو القاضي².

وإذا كان القانون قد أخذ في الاعتبار ضرورة توافر الأركان الشكلية والموضوعية في الخبرة فإن الأمر يستدعي أن يقوم القضاء بالاستعانة بخبراء مصنفين في هذا الشأن مما هو مندرج في قائمة المحكمة، وهو ما يطلق عليه نظام جدول الخبراء الذي يتميز به النظام القانوني الفرنسي، دون نظيره الأنجلوأمريكي، فحين يندب القاضي في هذا النظام خبيرا فإنه يقوم بذلك مستعينا بجدول الخبرة المعد في كل محكمة.

على إن هذا الأمر غير مقيد للقاضي، وإنما يجوز للقاضي ندب خبير من خارج الجدول، وإن كان القضاء الفرنسي يستلزم في هذه الحالة ضرورة أن يقوم القاضي بتسبيب قراره هنا وإلا ترتب البطلان على قرار ندب الخبير. أضف إن القانون يتطلب إجراءات شكلية أخرى في الخبير ينبغي

¹ - عائشة بن قارة مصطفى ، حجية الدليل الالكتروني في مجال الإثبات الجنائي ، دار الجامعة الإسكندرية ، 2010، ص76.

² - سامي جلال حسين ، مرجع سابق ، ص 114.

توافرها كحلف الخبير اليمين ... الخ، وهذه كلها إجراءات يترتب على مخالفتها البطلان إن لم يقيم الخبير بمראعاتها.

ولكن السؤال المطروح هنا يتمثل في مدى إمكانية قيام القضاء باللجوء إلى الخبرة حين اعتراض قضائه موضوعاً من موضوعات الانترنت؟ لا سيما وهو يواجه قاعدة خطرة تتمثل في حداثة موضوع العالم الافتراضي أو الرقمي ككل، مما يعني إن ما يمكن أن يردد كنتيجة للخبرة يمكن أن يكون غير الذي سوف يتقرر مستقبلاً، ناهيك عن كونه يمكن أن يكون مثار جدل في الفترة المعاصرة. على إن مثل هذا القول لا يعفي في الحقيقة القضاء من ضرورة الاستعانة بالخبرة التقنية بحسب ما هو متاح. إن الخبرة التقنية في مجال الانترنت والعالم الافتراضي لا تشمل بالضرورة تلك النوعية من الخبرة الدارسة، فدراسات الحاسب الآلي والانترنت لا ترتبط بمنهج دراسي أو بحثي معين أو حتى مدة زمنية يقضيها المرء دارساً في الجامعات والمعاهد المتخصصة، وإنما ترتبط بمهارات خاصة وبموهبة استعمال الحاسوب والانترنت والتعامل مع تقنية المعلومات، إذ إن أمر مبرمجي نظم التشغيل حتى الآن مثل Bill Gates لم يكن تحصيله العلمي يتجاوز المرحلة الثانوية، وذات الأمر ينطبق على عتاة الهاكرز ومخترقي الأنظمة فإن أعمارهم لا تتجاوز مرحلة التعلم الثانوي والسنوات الجامعية الأولى في أحسن الأحوال¹.

ومن هذا المنطلق تتميز الخبرة في مجال تكنولوجيا المعلومات عن الخبرة في أي فرع آخر من الفروع التي يمكن أن تكون محلاً للخبرة أمام القضاء. وللخبرة في المجال التقني أنواع أهمها²:

1 - الخبرة الخاصة: وهذه تعد أقوى أنواع الخبرات على الإطلاق لكونها تنطلق من مفهوم السعي إلى خلق فرص منافسة حقيقية بين المنظمات الخاصة. وهي تضم في جنباتها الخبرة الفردية التي تعد أقوى وأهم مظاهر الخبرة السائدة في مجال تكنولوجيا المعلومات/الانترنت، ويكفي هنا أن نذكر إن المؤسسات الكبرى المتخصصة في الحاسب الآلي والانترنت تسعى بكل جهودها إلى الاستعانة العقدية بأشخاص أثبتوا كفاءتهم في مجال الحاسوب والانترنت. حتى عصاة القانون منهم فهناك اتجاه اقتصادي يحاول جاهداً إثبات عدم جدوى التخلص من هؤلاء بمعايبتهم وفقاً للقانون، وإنما يلزم اللجوء إلى الحلول الاقتصادية لكي يمكن أن يظلوا عاملين في إطار الأهداف الاقتصادية، بل إن من

¹ - عائشة بن قارة مصطفى ، مرجع سابق ، ص 78.

² - سامي جلال حسين ، مرجع سابق ، ص 115.

الدول ما تسعى جاهدة إلى محاولة التعرف على قرصنة تحولوا مع مرور الوقت إلى رموز وطنية جراء تحركاتهم عبر الانترنت.

2 -المؤسسات التعليمية: لما كانت الانترنت تعد أحد منتجات العلم في حركته التقنية، فإنه يمكن القول وبحق إن أقوى مظاهر الخبرة التي يمكن الاستعانة بها لمواجهة الجريمة في العالم الافتراضي يمكن أن تكون من خلال المؤسسات التعليمية، فهذه الأخيرة تعد مصدر دعم متكامل لمؤسسات الدولة ككل , وهذه المؤسسات تعتمد منهج علمي غير تجاري هدفها بالتأكيد تطوير العلم ليقضي على المشكلات التي تواجه البشرية، كما إن التفكير العلمي لا يمكن تجنبه في رصده للظاهرة الإنسانية. ولقد قامت عدة مؤسسات تعليمية بتكوين قاعدة خبرة كبيرة فيها لتكون على أهبة الاستعداد لمواجهة الجريمة عبر الانترنت، ومن ذلك دراسات الحاسب الآلي التي تتطور بشكل فائق في جامعة ستانفورد، كذلك معهد التكنولوجيا في ماساشوستس الذي قدم للبشرية خبراء على درجة عالية من التفوق.

3 -جهات الضبط القضائي: شرعت بعض الدول في إعداد أجهزة متخصصة للخبرة في الإجرام عبر الانترنت. وعلى رأس تلك الدول الولايات المتحدة التي تجاوز نشاطها في هذا المجال الإطار الدولي الممثل في منظمة الإنتربول. وكان آخر نشاط مؤسسي في هذا الإطار هو ذلك الفرع الجديد الذي تأسس في المباحث الفيدرالية الأمريكية FBI أطلق عليه المعمل الإقليمي الشرعي للحاسوب. أساليب عمل الخبير التقني:

للخبير التقني في سبيل تحري الحقيقة أن يقوم بكل ما يمكنه من التوصل إليها. وهو في إطار القيام بعمله عليه أن يستخدم الأساليب العلمية التي يقوم عليها تخصصه وليس للمحكمة أن ترفض تلك الأساليب ما لم يكن رفضها لها مسببا بشكل منطقي وإلا تعرض حكمها للنقض. وهناك أسلوبان لعمل الخبير التقني¹:

الأول: القيام بتجميع وتحصيل لمجموعة المواقع التي تشكل جريمة في ذاتها، كما هو الشأن في التهديد Intimidation أو النصب Fraud أو السب Defamation أو جرائم Infringement of copyrights وبث صور فاضحة بقصد الدعاية للتحريض على ارتكاب جرائم الدعاية والرقيق الأبيض ودعاية الأطفال وغيرها. ثم القيام بعملية تحليل رقمي لها

¹ - مني الأشقر , مرجع سابق , ص 78.

لمعرفة كيفية إعدادها البرمجي ونسبتها إلى مسارها الذي أُعدت فيه، وتحديد عناصر حركتها، وكيف تم التوصل إلى معرفتها، ومن ثم التوصل في النهاية إلى معرفة بروتوكول الانترنت IP الذي ينسب إلى جهاز الحاسوب الذي صدر عنه هذه المواقع.

الثاني: القيام بتجميع وتحصيل لمجموعة المواقع التي لا يشكل موضوعها جريمة في ذاته، وإنما تؤدي حال تتبع موضوعها إلى قيام الأفراد بارتكاب جرائم. كما هو الحال في المواقع التي تساعد الغير على التعرف على جرعات المخدرات والمؤثرات العقلية التي تناسب وزن الإنسان بادعاء أنه إذا تم تتبع التعليمات الواردة فيها فلن يصاب الشخص بحالة إدمان، وأيضا كيفية زراعة المخدرات بعيدا عن أعين الغير (ويطلق عليه في هذه الحالة الفضولي) وأيضا كيفية أعداد القنابل وتخزينها، وكيفية التعامل مع القنابل الزمنية وتركيبها والقيام بفكها وحفظها، وكذلك القيام بتحديد مسار الدخول على مواقع دعارة من أماكن متفرقة دون لزوم القيام بالدخول من مكان ثابت، ومثل هذا الأمر جائز الحدوث كما لو كان مرتكب الجريمة مشتركا لدى مزود في مدينة مختلفة عن تلك التي يقيم فيها ويقوم بالولوج إلى الانترنت من محل أقامته .

كذلك يحق للخبير أن يطلع على شهادات وأقوال الجناة في الصحف وأمام الجهات الرسمية والشعبية، إذ أن كثيرا ما يكون في مثل هذه الأقوال عوامل مساعدة لخبرته، فيمكن من خلالها التعرف على أسلوب عمل مرتكب الجريمة المعلوماتية والتعامل معه على أساس أقواله، ومعلوم إن الكونجرس الأمريكي قد استدعى أحد كبار هكرة العالم الافتراضي، بل أخطرهم على الإطلاق، وهو "كيفين ميتنيك"، لكي يدلي بشهادته كهacker عن كيفية ارتكابه للاختراق ورأيه في إعداد تشريع يحظر الاختراق. ولقد تضمنت شهادته العديد من الأمور التي كانت خافية على رجال التشريع والقانون¹.

رابعا: الشهادة

يقصد بالشهادة بأنها: "تقرير الشخص لما يكون قد رآه أو سمعه بنفسه أو أدركه على وجه العموم بالحواس.

و يقصد بالشاهد في جرائم المعلوماتية بأنه الشخص الفني صاحب الخبرة المعلوماتية و التخصص في تقنية و علوم الحاسب الآلي و شبكاته،و يطلق على هذا النوع من الشهود مصطلح الشاهد

¹ - عائشة بن قارة مصطفى ، مرجع سابق ، ص 80.

المعلوماتي "témoin" "informatique le" تميزا له عن الشاهد التقليدي. ويشمل الشاهد في الجرائم المعلوماتية عدة طوائف أهمها¹:

1- القائم على تشغيل الحاسب الآلي: و هو المسئول عن تشغيل الحاسب الآلي و المعدات المتصلة به و يجب أن تكون لديه الخبرة الكبيرة في استخدام الجهاز، كما يجب أن تكون لديه معلومات عن قواعد كتابة البرامج

2 المبرمجون: و هم الأشخاص الذين يأخذون على عاتقهم كتابة البرامج، و ينقسمون إلى فئتين: *الفئة الأولى: هم مخططو البرامج التطبيقية و يقومون بالحصول على خصائص النظام المطلوب *الفئة الثانية: وهم مخططو برامج النظم و يقومون باختيار و تعديل و تصحيح برامج النظام الحاسب الداخلية و إدخال أي تعديلات أو إضافات لها

3 مهندسو الصيانة و الاتصالات: و هم المسئولون عن أعمال الصيانة الخاصة بتقنيات الحاسب و مكوناته و شبكات الاتصال المتعلقة به.

4 المحللون: وهم الأشخاص الذين تأتي على عاتقهم مهمة التحليل الخاصة ببيانات نظام معين إلى وحدات مفصلة و استنتاج العلاقة الوظيفية منها، كما يقومون كذلك بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات و استنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسب الآلي.

5- مديرو النظم: وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية.

6- طاقم عمليات البيانات: الذي يعد البيانات بالصورة التي يستطيع الكمبيوتر قراءتها (شريط أو اسطوانة).

7- مهندس الصيانة الإلكترونية: الذي يقوم على صيانة الجهاز الأصلي والتأكد من عمله بصورة صحيحة.

يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات سعيا عن أدلة الجريمة بداخله، والسؤال الذي يطرح نفسه هل يلتزم الشاهد بطبع الملفات والإفصاح عن كلمات المرور والشفرات؟ هناك اتجاهان في هذا الصدد:

¹ - سامي جلال حسين , مرجع سابق , ص 118.

الاتجاه الأول: ويرى أنه ليس من واجب الشاهد وفقا للالتزامات التقليدية للشهادة أن يقوم بطبع ملف البيانات أو الإفصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة ويميل إلى هذا الاتجاه الفقه الألماني حيث يرى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسب على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب , وكذلك لا يجوز في تركيا إكراه الشاهد لحمله على الإفصاح عن كلمات المرور السرية أو كشف شفرات تشغيل البرامج المختلفة¹.

الاتجاه الثاني: ويرى أنصار هذا الاتجاه أن من بين الالتزامات التي يتحمل بها الشاهد القيام بطبع ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة حيث يرى اتجاه في الفقه الفرنسي أن القواعد العامة في مجال الإجراءات تحتفظ بسلطانها في مجال الإجراءات المعلوماتية ومن ثم يتعين على الشهود من حيث المبدأ الالتزام بتقديم شهادتهم (المواد 62، 109، 138 من قانون الإجراءات الجنائية الفرنسية) ومن ثم يجب عليهم الإفصاح عن كلمات المرور السرية التي يعلمونها، ولكن رفض إعطاء المعلومات المطلوبة غير معاقب عليه جنائيا إلا في مرحلة التحقيق والمحاكمة².

خاتمة:

ختاما يكمن القول أن تسارع إيقاع التقدم التكنولوجي والتقني الهائل، وظهور الفضاء الإلكتروني ووسائل الاتصالات الحديثة كالفاكس والإنترنت وسائر صور الاتصال الإلكتروني عبر الأقمار الصناعية كانوا وسيلة استغلها مرتكبو الجرائم الإلكترونية، في تنفيذ جرائمهم التي لم تعد تقتصر على إقليم دولة واحدة، بل تجاوزت حدود الدول، وهي جرائم مبتكرة ومستحدثة تمثل ضربا من ضروب الذكاء الإجرامي، استعصى إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية.

ومن حيث ما يرتبط بمشاشة نظام الملاحقة الإجرائية التي تبدو قاصرة على استيعاب هذه الظاهرة الإجرامية الجديدة، سواء على صعيد الملاحقة الجنائية في إطار القوانين الوطنية أم على صعيد الملاحقة الجنائية الدولية، مما أوجب تطوير البنية التشريعية الجنائية الوطنية بذكاء تشريعي ماثل تعكس فيه الدقة الواجبة علي المستوى القانوني وسائر جوانب وأبعاد تلك التقنيات الجديدة، بما

¹ - أمير فرج يوسف، مرجع سابق، ص41.

² - محمد عادل ريان، مرجع سابق، ص 58.

يضمن في الأحوال كافة احترام مبدأ شرعية الجرائم والعقوبات من ناحية، ومبدأ الشرعية الإجرائية من ناحية أخرى، وتتكامل فيه في الدور والهدف مع المعاهدات الدولية.

النتائج:

هناك العديد من النتائج التي توصلت إليها الدراسة، علما أن ماتم التوصل إليه من نتائج الآن ربما يتغير مستقبلا بحكم طبيعة الجريمة الالكترونية المرتبطة بالتقنية التي تتطور بشكل كبير، والنتائج هي:

- يعد الإثبات من أهم التحديات التي تواجه الأجهزة الأمنية ويزداد الإثبات صعوبة في الجرائم المعلوماتية، وفي حال اكتشاف وقوع هذه الجريمة والإبلاغ عنها فإن إثباتها أمر يحيط به الكثير من الصعاب، مما يستلزم الكثير من الجهد والخبرة الفنية.

- تواجه طرق التحقيق في إثبات الجريمة الالكترونية صعوبات متعددة، حيث تستدعي في المقام الأول اكتشاف الجريمة الالكترونية ومحلها وبيئتها ثم الإبلاغ عنها، واخذ إذن الجهات المختصة قبل القيام بالمعاينات والتفتيش للمواقع، وذلك للبحث عن الدليل الرقمي الالكتروني بالطرق الفنية.

- تمثل الشهادة أهمية كبيرة في إثبات الجريمة الالكترونية في المواد الجزائية فهي ترد على وقائع مادية وترشد القاضي إلى تحري قيمتها، حيث يكون للشهادة أثناء التحقيق اثر كبير فيما يتعلق بالبراءة والإدانة، كما لها أهميتها في الكشف عن الأدلة التي تساعد على إثبات الجريمة الالكترونية.

-لم تنص اغلب التشريعات والقوانين على الدليل الالكتروني أو الرقمي ومنهم المشرع الجزائري، الذي بدوره لم ينص على الدليل الالكتروني في قوانينه، علما انه يعتبر المساهم الأول في سبيل مواجهة الجرائم الالكترونية، وهذا يعتبر قصورا من طرف مختلف التشريعات والقوانين.

-إن محل الدليل الالكتروني ونطاق العمل به هو الجريمة الالكترونية، غير انه يصلح كذلك لإثبات الجرائم التقليدية التي تم ارتكابها عن طريق تقنية الحاسب الآلي.

-قصور اغلب التشريعات من الناحية الإجرائية فيما يخص إجراءات الحصول على الدليل الالكتروني واقتصارها على القواعد العامة والإجراءات التقليدية.

الاقتراحات:

على ضوء هذه النتائج المتوصل إليها يمكن وضع جملة من التوصيات أهمها:

- فيما يتعلق بمعاينة الجريمة الالكترونية، فيجب تحديد أجهزة الحاسب الآلي الموجودة في مكان المعاينة وتحديد موقعها بأسرع وقت ممكن، وفي حالة وجود شبكة اتصالات يجب البحث عن خادم

الملفات بهدف تعطيل الاتصالات لمنع تخريب الأدلة المتحصل عليها ,مع تصوير الأجهزة الموجودة وبصفة خاصة الأجهزة الخلفية.

- على الدولة أن تعمل على تبني جهازاً خاصاً للخبرة الجنائية للجريمة المعلوماتية، يتكون أعضاؤه من فريق متخصص فنياً في التقنية المعلوماتية، على أن يتم إعادة النظر في القواعد التقليدية للخبرة، لأن إثبات الجريمة المعلوماتية يتطلب قواعد خاصة للتعامل مع الأدلة في هذه الجرائم، لأن البحث عنها يتم داخل نظام اليكتروني معقد، يسهل فيه محو الأدلة إذا ما تم التعامل الأولي مع الجهاز بشكل خاطئ..

- يجب فحص كل ماتحويه سلة المهملات في الجهاز ورفع البصمات التي قد تكون لها دلالة على مرتكب الجريمة ,بالإضافة إلى ضرورة القيام بحفظ كل المستندات الخاصة بالإدخال والإخراج والتي قد تكون على صلة بالجريمة.

- أهمية التنسيق المستمر بين الجهات القضائية والأمنية من جهة والجهات ذات العلاقة بالتكنولوجيا من جهة أخرى لمسايرة مايستجد في هذا المجال.

- ضرورة النص صراحة على الأدلة الالكترونية كأدلة إثبات في المجال الجنائي والاعتراف لها بحجية قاطعة وكذلك النص على وسائل التأكد من سلامة الدليل الالكتروني التي تعتبر شرطاً لقبوله.

-العمل على عقد المزيد من الندوات العلمية و المؤتمرات حول العلاقة بين المعلوماتية و القانون، وتبني خطة واسعة للتدريب و رفع مستوى الكفاءة المعلوماتية في القطاع الوظيفي للدولة، وتخصيص دورات تدريبية مكثفة، للقضاة و رجال النيابة العامة لرفع مستوى الكفاءة لديهم في استخدام التقنية المعلوماتية.

المصادر والمراجع:

- أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية الإسكندرية، 2009.

-عبد الفتاح بيومي حجازي، الدليل الجنائي و التزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية مصر 2006.

- هشام محمد رستم , الجوانب الإجرائية للجرائم المعلوماتية, مكتبة الآلات الحديثة أسبوط مصر1999.

- عبد الفتاح مراد , شرح جرائم الكمبيوتر و الانترنت , دار الكتب والوثائق المصرية , 2005.
- محمد عادل ريان، جرائم الحاسب الآلي وأمن البيانات، بيروت، 2002.
- منى الأشقر، القانون والانترنت ” تحدي التكيف والضبط ”، بيروت، الناشر ش م م، مصر، 2011.
- سامي جلال فقي حسين , الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي, د.ط , دار الكتب القانونية مصر, 2012.
- عائشة بن قارة مصطفى , حجية الدليل الالكتروني في مجال الإثبات الجنائي , دار الجامعة الإسكندرية , 2013.

إجراءات الإثبات في الجريمة المعلوماتية

ط.د/ فراحتية أكرم

كلية الحقوق والعلوم السياسية

جامعة المدية

ط.د/ كباهم سامي

كلية الحقوق والعلوم السياسية

جامعة خميس مليانة

مقدمة:

إن التطور التكنولوجي الذي يشهده العالم قد انعكس أثره على الجرائم التي تمخضت عنه؛ بحيث تميزت هذه الجرائم بطبيعة خاصة من حيث الوسائل التي ترتكب بها ومن حيث المحل الذي تقع عليه ومن حيث الجناة الذين يرتكبونها؛ وهو ما يجعل إجراءات المتابعة فيها في منتهى الصعوبة. ولما كان القانون وليد بيئة اجتماعية كان لابد له من مسايرة هذا التطور الذي انعكس أثره على قانون العقوبات والذي بدوره انعكس أثره أيضا على قانون الإجراءات الجزائية تلقائيا باعتباره القانون الإجرائي لقانون العقوبات خاصة في مجال الإثبات الذي تأثر بدوره بالتطور الهائل الذي لحق الأدلة الجزائية بسبب تطور طرق ارتكاب الجريمة الأمر الذي يتعين معه تغيير النظرة إلى طرق الإثبات الجزائي.

وفي ظل الأهمية الكبيرة لعملية الإثبات في مجال الجنائي حيث أن الدليل هو الذي على أساسه يبنى الحكم، ولعل هذه الأهمية تزداد أكثر في الجريمة المعلوماتية نظرا لحدائث القوانين التي تعالج هذا النوع من الجرائم وكذا صعوبة الإثبات نظرا لوجود اشخاص محترفين في هذا المجال، لذلك يستلزم الإثبات في مجال الجريمة المعلوماتية إجراءات تختلف عن تلك الموجودة في الجرائم العادية. فما هي إجراءات الحصول على الدليل الإلكتروني من أجل إثبات الجريمة المعلوماتية، وما هي المشكلات التي تعترض قبول هذه الأدلة؟.

وللإجابة على هذه الإشكالية إعتدنا على الخطة التالية:

المحور الأول: إجراءات الحصول على الدليل الإلكتروني في الجريمة المعلوماتية

المحور الثاني: مشكلات قبول الدليل الإلكتروني في الجريمة المعلوماتية

المحور الأول: إجراءات الحصول على الدليل الإلكتروني في الجريمة المعلوماتية

أولاً: التفتيش

التفتيش في مدلوله القانوني بالنسبة للجرائم المعلوماتية لا يختلف عن مدلوله السائد في فقه الإجراءات الجزائية رغم اختلاف المحل التي يقع عليه التفتيش.

ويقصد به إجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة وتشكل جناية أو جنحة والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم بارتكابها¹.

ويثير موضوع التفتيش الذي يقع على نظم الحاسب الآلي مسائل عديدة للبحث كمدى صلاحية الكيانات المعنية في هذه الوسائل كمحل يرد عليه التفتيش، وحكم تفتيش الوسائل التي تتصل مع بعضها البعض وتقع في أماكن عامة أو خاصة، وضوابط هذا التفتيش.

1/مدى صلاحية الكيانات المعنية كمحل يرد عليه التفتيش:

إذا كان التفتيش كوسيلة إجرائية يستهدف الحصول على دليل مادي يساعد في إثبات الجريمة فإن البعض قد شكك في مدى صلاحيته للبحث عن أدلة الجريمة في الكيانات المعنية للحاسب الآلي وهو ما حدا ببعض التشريعات بأن تنص صراحة على أن التفتيش يتم بالنسبة لأنظمة الحاسب الآلي مثل ذلك قانون إساءة استخدام الحاسب الآلي في إنجلترا الصادر في سنة 1990 حيث نص أن إجراءات التفتيش تشمل أنظمة الحاسب الآلي².

وهناك تشريعات أخرى قد أجازت تفتيش أي "شيء" له علاقة بالأفعال الإجرامية مثلما هو الحال بالمشروع الجزائري.وعلى ضوء ذلك فإن تفتيش المكونات المعنية للحاسبات الآلية يدخل في عداد الأشياء التي جاء النص عليها عاما دون تقييد.

¹ د. هلاي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، د.س.ن، ص 73 وما بعدها.

² Wasik (martin) , computer crimes and other crimes against information technology in the United Kingdom- rev, inter, De, Dr, Panal 1993,P,640

ثم إن نظرة الفقه في الكثير من دول العالم إلى مصطلح " الأشياء " التي ترد عليها جرائم الاعتداء على المال نظرة واقعية، بحيث أن هذا المصطلح لا يجب أن يظل جامدا عند معناه الحرفي وإنما يجب أن يؤخذ بأكثر شمولية من معناه المادي حتى أن بعض الفقه في فرنسا¹ ذهب إلى أن برامج الحاسبات الآلية المتمثلة في النبضات والإشارات والذبذبات الالكترونية المغناطيسية أو الكهرومغناطيسية لها كيانها المادي الملموس؛ فالشيء يكون محلا للحماية الجنائية بالنظر إلى القيمة التي يتمتع بها والتي قد تتمثل في منفعة مالية أو اقتصادية ولا فرق بين الأشياء المادية والأشياء المعنوية من حيث المنفعة التي قد يحصل عليها صاحبها؛ بل إن بعض الأشياء المعنوية قد تكون لها قيمة اقتصادية تعلق بكثير على الأشياء المادية؛ كالأسرار التجارية والصناعية².

وعلى ضوء هذه الآراء الفقهية؛ وعلى النحو الذي قننه المشرع الجزائري صراحة في إمكانية وقوع التفتيش على مساكن أشخاص يظهر أنهم يحوزون على أشياء لها علاقة بالأفعال الجنائية فإن التفتيش يرد على الكيانات المعنوية في الحاسبات الآلية، بحسب أن هذه الكيانات المعنوية وإن كانت غير مادية إلا أنها في نطاق الأشياء المادية³.

ويتربط على ذلك أنه يمكن تفتيش نظام معلومات الحاسب ووسائط أو أوعية حفظ وتخزين البيانات المعالجة آليا كالاسطوانات والأقراص والأشرطة الممغنطة ومخرجات الحاسب، ويدخل في هذا التفتيش أيضا المحتويات المخزنة في الوحدة المركزية للنظام والتي يمكن عزلها ككيان قائم بذاته⁴.

ثانيا: ضوابط التفتيش الذي يقع على نظم ومكونات الحاسب الآلي

¹ Sagros "Pierre" et masse "Michel" le droit penal et l'informatique 1
journée d'étude du 15 Novembre 1982 publication à l'institut de
science criminelle de la faculté IV- P 25

² Gautal (Jean – Louis), la protection penale des logiciel " le droit
criminel face aux technologie nouvelles de la communication " P 254 et
255

³ د. هلاي عبد الله أحمد، تفتيش نظم الحاسب الآلي، المرجع السابق، ص 89

⁴ هشام محمد فريد رستم، قانون العقوبات ومخاطر التقنية المعلومات، مكتبة الآلات الحديثة، سنة 1992، ص 69.

لقد تطورت طرق التفتيش بحيث أنها أصبحت لا تقف - فقط - عند ضبط الأدوات المادية المستخدمة في ارتكاب الجريمة أو ضبط جسم الجريمة الذي يحقق نموذجها القانوني، وإنما يمكن لهذه الطرق كذلك أن تتعامل مع الجرائم التي ترتكب بالوسائل الالكترونية خاصة الحاسب الآلي، أو تقع عليه، فيمكن تبعا لذلك تسجيل البيانات المعالجة آليا بعد تحويلها من نبضات أو ذبذبات أو إشارات أو موجات كهرومغناطيسية إلى أشياء محسوسة تسجل وتخزن على وسائل معينة، وعلى هذه الوسائل يرد التفتيش أو الضبط¹.

ويخضع التفتيش لشروط مقيدة يجب مراعاتها تحت طائلة البطلان.

إذ تنص المادة 44 من قانون الإجراءات الجزائية بعد تعديله بالقانون رقم 06 - 22 على عدم جواز إجراء التفتيش من قبل ضابط الشرطة القضائية إلا بإذن مكتوب من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهار هذا الأمر قبل الدخول إلى المنزل والشروع في التفتيش.

ثم تنص المادة 45 على القيود التي يتعين على ضابط الشرطة القضائية احترامها أثناء فترة التفتيش بصفة عامة لكن أضاف التعديل وتم نص المادة 45 بأن رفع القيود الواردة فيها فيما يتعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، إلا ما تعلق منها بالحفاظ على السر المهني وكذا جرد الأشياء وحجز المستندات.

كما أجاز في نص المادة 47 إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل دون احترام الأوقات المذكورة في الفقرة الأولى في المادة 47 من قانون الإجراءات الجزائية، إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات غير أنه يشترط أن يكون مصحوبا بإذن مسبق من وكيل الجمهورية المختص أو قاضي التحقيق.

غير أن المشرع لم يتطرق إلى المحل الذي يرد عليه التفتيش بصفة مدققة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات. ذلك أن التفتيش هنا يقع على نظام معلومات الحاسب أو الوسائط أو أوعية حفظ وتخزين البيانات المعالجة الكترونيا كالاسطوانات والأقراص والأشرطة الممغنطة ومخرجات الحاسب

Jean P, spreutels, les crimes informatiques et d'autres crimes dans les ¹ domaines de la technologie informatique en Belgique - rev - inter de- dr pen 1993 - P 170.

ويدخل في هذا التفتيش أيضا المحتويات المخزنة في الوحدة المركزية للنظام والتي يمكن عزلها ككيان قائم بذاته¹.

والملاحظ أن المشرع الجزائري عندما عدل نصوص المواد المتعلقة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات قد خص حسب رأبي على الحاسبات الآلية داخل الدولة وحتى لو اتصلت مع بعضها البعض فيكون ذلك عن طريق شبكة محلية.

لكن يطرح التساؤل هنا في حالة ما إذا اتصلت بحاسبات أخرى خارج الدولة عن طريق الربط الشبكي بين أجزاء العالم المختلفة؛ ومنها شبكة الانترنت.

ففي حالة وقوع جريمة في نظم الحاسب الآلي داخل الدولة الجزائرية فيجوز هنا لوكيل الجمهورية أو قاضي التحقيق إصدار الإذن بالتفتيش

لكن هذا الإذن بالتفتيش لا ينفذ إلا على الحاسب الآلي الذي صدر من أجله، ويترتب على ذلك أنه إذا كان الحاسب المراد تفتيشه يتصل بحاسب آخر لم يصدر بالنسبة له إذن بالتفتيش لا يمكن أن يمتد إليه التفتيش حتى لو كان يحتوي على الجريمة.

إلا إذا أمر قاضي التحقيق هنا في إذنه بالتفتيش أن يمتد على مستوى التراب الوطني بكامله حسب الفقرة الأخيرة من نص المادة 47.

لكن في حالة الإذن بالتفتيش على حاسب واحد معين، يتعين استصدار إذن جديد بالتفتيش للحاسب الثاني إذا تبين أنه متصل عن طريق شبكة داخلية بالحاسب الذي أذن التفتيش فيه.

لكن هناك حالة أخرى أكثر تعقيدا تواجه التفتيش على الحاسب الآلي وذلك عندما يقوم بعض الجناة بتخزين بياناتهم في أنظمة حاسبات آلية تقع خارج الدولة الجزائرية مستخدمين في ذلك الاتصالات البعيدة أو مواقع خارج الجزائر مستهدفين عدم إمكان الوصول إليها وفي هذه الحالة فإن تفتيش هذه الحاسبات التي تقع خارج حدود الدولة لضبط جريمة تتصل بحاسبات

آلية داخل الدولة أمر قد يتعذر القيام به بسبب تمسك كل دولة بسيادتها، غير أنه يمكن اتخاذ هذا الإجراء عن طريق اتفاقات خاصة تعقد بين الدول المعنية.

¹ د. هشام رستم، المرجع السابق، ص 69

وكتطبيق لهذا الإجراء فقد حدث في ألمانيا أثناء إجراءات التحقيق عن جريمة غش وقعت في بيانات حاسب آلي، ذلك أنه قد تبين وجود اتصال بين الحاسب الآلي المتواجد في ألمانيا وبين شبكة اتصالات في سويسرا حيث يتم تخزين بيانات المشروعات فيها، وعندما أرادت سلطات التحقيق الألمانية ضبط هذه البيانات، فلم تتمكن من ذلك إلا عن طريق التماس المساعدة الذي

تم بالتبادل بين الدولتين¹ ولقد أدرك المجلس الأوروبي مشكلة التفتيش التي قد تثار بالنسبة للجرائم التي ترتكب بالوسائل الالكترونية في أكثر من دولة فأصدر التوصية رقم R 9513 التي أكد فيها على وجود قصور على مستوى التعاون الدولي بالنسبة لإجراء التفتيش عبر الحدود

Perquisition transfrontière

لكن الجزائر لحد الآن لم تنضم إلى أي من المعاهدات أو الاتفاقيات الخاصة بجريمة المعلوماتية.

ثانيا: الخبرة

الخبرة هي الوسيلة لتحديد التفسير الفني للأدلة بالاستعانة بالمعلومات العلمية؛ فهي في حقيقتها ليست دليلا مستقلا عن الدليل المادي وإنما هي تقييم في هذا الدليل.

وقد أجاز المشرع للمحقق الاستعانة بخبير متخصص في المسألة موضوع الخبرة.

فقد نصت المادة 143 قانون الإجراءات الجزائية في فقرتها الأولى على أنه يجوز لكل جهة قضائية تتولى " التحقيق أو تجلس للحكم إذا تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما بناء على طلب النيابة أو الخصوم أو من تلقاء نفسها.

وبالنظر إلى الطبيعة الخاصة بالجرائم المعلوماتية فإن إمطة اللتام عنها قد يحتاج إلى خبرة فنية تظهر الحاجة إليها منذ بدء مرحلة التحري عن هذه الجرائم، ثم تستمر هذه الحاجة في مرحلتي التحقيق والمحاكمة نظرا للطابع الفني الخاص بأساليب ارتكابها والطبيعة المعنوية محل الاعتداء².

وبالعودة لنص المادة 146 نجد أن المشرع يفرض على الجهة القضائية الآمرة بندب الخبير تحديد مهمة الخبير بدقة وهذا يعود بنا إلى ضرورة تأهيل سلطات التحقيق أو الحكم في الجرائم المعلوماتية لنجاح الهدف المتوخى من التحقيق في هذا النوع المستحدث من الجرائم.

¹ Mohrenschlager " Manfred" op.cit , P 351 www.anablawinfo.com

² د. هشام رستم، المرجع السابق، ص 137

كما تجدر الإشارة على أنه يجب على القاضي اختيار الخبراء ذوي الإمكانات العلمية والمقدرة الفنية الحالية فلا يكفي مجرد الحصول على شهادة علمية، إذ يجب مراعاة الخبرة العلمية فالوسائل الالكترونية متعددة وشبكات الاتصال بينها متنوعة فطبيعتها الفنية تجعلها موزعة على تخصصات فنية وعلمية دقيقة¹ على القاضي في رأيي أن يتناول في أمر ندب الخبير المسائل التالية:

1. تركيب الحاسب الآلي، طرازه، نوعه، نظام تشغيله، الأنظمة الفرعية التي يستخدمها.
2. بيئة الحاسب أو الشبكة من حيث طبيعتها، تركيزها، توزيعها وكذلك نمط ووسائل الاتصالات.
3. المكان المحتمل لأدلة الإثبات وشكلها وهيئتها.
4. الآثار الاقتصادية والمالية المترتبة عن الجريمة المعلوماتية.
5. كيفية عزل النظام المعلوماتي دون إتلاف الأدلة أو الأجهزة أو تدميرها.
6. إمكانية نقل أدلة الإثبات لأوعية أو وسائط مادية كالأوراق أو الاسطوانات على إن تكون مطابقة لما هو مسجل في الحاسب الآلي أو النظام أو الشبكة.

ثالثاً: اعتراض المراسلات السلوكية واللاسلكية والمراقبة الالكترونية

تجدر الإشارة إلى أن تأثير التطور العلمي لا يقف عند مضمون الدليل وإنما يمتد هذا التأثير كذلك إلى الإجراءات التي يترتب عليها الحصول على هذا الدليل، ولذلك فانه يجب أن تكون هذه الإجراءات المتطورة ذات طبيعة مشروعة لكي تحافظ على شرعية الأدلة المتولدة منها. وانطلاقاً من أهمية حماية الحياة الخاصة نجد الدستور في نص المادة 39 ينص " لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، يحميها القانون، سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة".

وتبعاً لذلك نظم سبل الرقابة عليها وحدد السلطة التي تملك ذلك والإجراءات التي يتم إتباعها حيال هذه المراقبة.

¹ د. هشام رستم، المرجع السابق، ص 140 و 141

وإذا كانت شبكات الحاسب الآلي تستخدم خطوط الهاتف وتستعين بجهاز معدل الموجات "modem" والذي يستطيع تحويل الإشارات الرقمية المستخدمة بواسطة الحاسب على موجات تناظرية تنقل مع الموجات الصوتية خلال خطوط الهاتف، وبذلك فانه يتبين وجود علاقة بين المراسلات التي تتم بالطرق التقليدية وتلك التي تتم بالوسائل الالكترونية بحيث يمكن القول أن هناك تنصتا ومراقبة الكترونية تتم على شبكات الحاسب الآلي¹.

ومن ثمة لا يجوز التنصت عليها أو الاطلاع على الأسرار التي تحتويها إلا بذات الطرق التي ينص عليها قانون الإجراءات الجزائية، فلا يستطيع الشخص اختراق صندوق البريد الالكتروني أو الدخول إلى أنظمة الحاسب الآلي المخزنة به الرسائل البريدية الالكترونية وضبطها إلا عن طريق إتباع إجراءات قانونية محددة في القانون ومن قبل أشخاص مخولين قانونا بذلك.

وقد اختلف الفقه في تكييف إجراء اعتراض المراسلات السلكية واللاسلكية، فذهب رأي إلى أنها تعد تفتيشا وبالتالي تخضع لقيوده، واستند في ذلك إلى أن هذه المراقبة تتفق مع التفتيش في أن الهدف منها هو البحث وضبط ما يفيد الوصول إلى الحقيقة، ولا أهمية لأن يكون الشيء المضبوط ماديا أم معنويا، وهي ذات الغاية من المراقبة والتنصت فهي البحث عن دليل معين².

في حين ذهب رأي آخر إلى التفرقة بين التفتيش والمراقبة، واعتبر الأول إجراء غايته العثور على الأدلة المادية وضبطها بوضع اليد عليها لمصلحة العدالة، أما الثانية فليس لها كيان مادي ملموس والقول بأن الرسائل الالكترونية أو الحديث في التلفون يندمج في كيان مادي يمكن ضبطه، فأسلاك التلفون أو التسجيل ليس دليلا في حد ذاته وإنما هي وسيلة أو أداة لسماع الحديث ولا تتأثر طبيعته بوسيلة أو أداة الحصول عليه³.

والرأي عندي أن التفتيش واعتراض المراسلات إجراءان مختلفان ذلك أن المشرع الإجرائي قد أفرد أحكاما خاصة لكل واحد منهما نظرا لاختلاف المحل الذي يقع على كل منهما، فالأخير يقع على

¹ د. هلاي عبد الله، تفتيش نظم الحاسب الآلي، المرجع السابق، ص 221

² د. رؤوف عبيد، مبادئ الاجراءات الجنائية في القانون المصري، دار الجيل للطباعة، الطبعة السادسة عشر، 1985 ص 358.

د. أحمد فتحي سرور، مراقبة المكالمات التلفونية، المجلة الجنائية القومية، ما بين 1963 ص 147

³ د. عبد المهيمن بكر، المرجع السابق ص 352، 353

حرمة الحياة الخاصة بمطلق القول، أما الأول فقد يمس مصادفة هذه الحياة الخاصة حتى وإن تمت على كيانات معنوية، فليس معنى أنه يتصور وقوع التفتيش على كيان معنوي وأن المراقبة تتم دائما على كيانات معنوية أن نسوي بينهما من حيث تأثيرهما على حرمة الحياة الخاصة بما قد لا يتوافر بالنسبة للتفتيش.

وقد تدخل المشرع الفرنسي في 10 جويلية 1991 بإصدار قانون يفرض الرقابة على الاتصالات عن بعد بما في ذلك شبكات تبادل المعلومات¹ بعد اختلاف الفقه بشأن ضبط الأشياء المعنوية من مكونات الحاسب الآلي عن طريق التنصت أو اعتراض المراسلات إذ اعتبر جانب من الفقه أن قانون الإجراءات الجزائية عندما نص على إصدار إذن بضبط " أي شيء " فانه يشمل بذلك بيانات الحاسب المعنوية.

أما الجانب الآخر للفقه فاقترح مواجهة هذا القصور التشريعي بالنص صراحة على اعتراض المراسلات ويجب أن يشمل المواد المعالجة عن طريق الحاسب الآلي.

وعلى ضوء هذا القانون فإن المشرع الإجمالي الفرنسي خص إصدار قرار المراقبة بقاضي التحقيق (المادة 1/110) وله أن يندب مأمور الضبط القضائي للقيام به، ولا يأذن بالمراقبة إلا إذا كانت هناك ضرورة تستوجبها ظروف كشف الحقيقة وكانت هناك استحالة في الوصول إليها بطرق البحث والتنقيب العادية م (1/100) وتطلب هذا القانون كذلك في الجريمة المراد ضبطها بهذه الوسيلة أن تكون جناية أو جنحة معاقب عليها بالحبس الذي يزيد عن سنتين (م 2/100) وكذلك حدد ميعادا زمنيا للمراقبة مدته أربعة أشهر في حدها الأقصى وتكون قابلة للتجديد، وانه يتعين أن يتم التسجيل وتفريغ التسجيل تحت سلطة قاضي التحقيق ورقابته (م100).

وقد خاض المشرع الجزائري في تعديله الأخير لقانون الإجراءات الجزائية بالقانون رقم 06-22 المؤرخ ب20 ديسمبر 2006 في نص المادة 14 المتممة للباب الثاني من الكتاب الأول من الأمر رقم 66 - 155 بفصل الرابع تحت عنوان " اعتراض المراسلات وتسجيل الأصوات والتقاط الصور " بالمواد 65 مكرر 5 إلى المادة 65 مكرر 10.

¹ Francillon (Jacques) , les crimes et d'autres crimes dans le domaine de la technologie informatique en France – Rev.inter. De. Dr. P en 1993 P303

إذ خول لوكيل الجمهورية أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم محددة على سبيل الحصر في نص المادة 65 مكرر 5 ومن بين هذه الجرائم جرائم المساس بأنظمة المعالجة الآلية للمعطيات. فيسمح الإذن بالدخول إلى المحلات

السكنية أو غيرها ولو خارج المواعيد المنصوص عليها في المادة 47 من قانون الإجراءات الجزائية بغير رضا أو حتى علم الأشخاص الذين لهم حق على تلك الأماكن وتنفيذ عمليات المراقبة هنا تكون تحت المراقبة المباشرة لوكيل الجمهورية.

والإذن بالمراقبة أو التنصت أو اعتراض المراسلات محددة بميعاد 4 أشهر كحد أقصى قابلة للتجديد المادة 65 مكرر 7.

كما خول لقاضي التحقيق الإذن أيضا بوضع هذه الترتيبات في حالة فتح تحقيق قضائي وتتم العمليات تحت مراقبته المباشرة. كما أجاز المشرع في نص المادة 65 مكرر 8 تسخير كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية أو اللاسلكية للتكفل بالجوانب التقنية للعمليات السابقة المذكورة في نص المادة 65 مكرر 5.

وفي الأخير على ضابط الشرطة القضائية تحرير محضر عن أي عملية اعتراض أو تسجيل أو وضع ترتيبات تقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري ويذكر تاريخ بداية هذه العمليات والانتهاء منها، كما يودع أي تسجيل أو اعتراض أو نسخ تم أثناء عملية المراقبة ويودعها بالملف.

المحور الثاني: مشكلات قبول الأدلة المتحصلة عن الوسائل الالكترونية

يسيطر على الإثبات الجزائي في قانون الإجراءات الجزائية مبدأ حرية القاضي في الاقتناع ذلك أن نص المادة 212 من قانون الإجراءات الجزائية تنص على جواز إثبات الجرائم بأي طريق من طرق الإثبات ماعدا الأحوال التي ينص عليها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص، ولا يوجد نص خاص في القانون يقيد مبدأ الإثبات الجنائي في مواد الجريمة المعلوماتية فتخضع بذلك للقواعد العامة في الإثبات.

والقاضي وعلى الرغم من أنه يتمتع بالحرية في تكوين عقيدته إلا أنه ملزم بتسبيب حكمه وبيان الأدلة التي استمد منها اقتناعه، فليست الحرية أن نطلق له العنان لكي يقتنع بما يحلو له، وإنما هو حر - فقط - في استخلاص الحقيقة من مصدر مشروع، فهناك طرق للإثبات نص عليها قانون الإجراءات الجزائية والتي تعد مشروعة وهي التي يجوز له استخلاص الحقيقة منها.¹ وعلى ضوء هذه الطبيعة الخاصة بالإثبات الجنائي نتناول تقدير القاضي لأدلة الإثبات الالكترونية في هذا المبحث ونقسمه إلى مطلبين الأول: مشكلات قبول الأدلة المتحصلة عن الوسائل الالكترونية وفي مطلب ثان تقدير هذه الأدلة في ضوء الأدلة العلمية.

أولاً: مشكلات قبول الأدلة المتحصلة عن الوسائل الالكترونية

بالنظر إلى الطبيعة الخاصة التي تتميز بها الأدلة المتحصلة من الوسائل الالكترونية وما قد يصاحب الحصول عليها من خطوات معقدة، فإن قبولها في الإثبات قد يثير العديد من المشكلات، ذلك أنه يمكن التلاعب فيها وتغيير الحقيقة التي يجب أن تعبر عنها. ولذلك فإن المشكلات التي تثيرها هذه الأدلة ليس بسبب أنها قد تصلح لتكون طرق إثبات أم لا؟ وإنما المشكلة التي تتعلق بها تتحدد في: كيفية ضمان مصداقية هذه الأدلة ومدى تعبيرها بالفعل عن الحقيقة التي تهدف إليها الدعوى العمومية في هذا النوع من الجرائم.

1/: مدى قبول التسجيلات ومخرجات الوسائل الالكترونية كأدلة إثبات.

¹ د. رمسيس بهنام، الإجراءات الجنائية تأصيلاً وتحليلاً، منشأة المعارف، طبعة 1984 ص 698

تذهب التشريعات المقارنة إلى قبول مصادر المعلومات الخاصة بالحاسب الآلي أو المتحصل عليها من أنظمتها مثل مخرجات نظام المعالجة الآلية للمعطيات، والبيانات المسجلة على دعائم ممغنطة أو المخزنة داخل نظام المعالجة الآلية كأدلة يقوم عليها الإثبات الجنائي¹.

وهذه الأدلة المتحصلة من الوسائل الالكترونية تخضع للسلطة التقديرية للقاضي الجزائي، فإن استراح إليها ضميره ووجدتها كافية ومنطقية فيمكنه أن يستمد اقتناعه بسبب حكمه بالاعتماد عليها. وفي الجزائر فإن المخرجات المتحصلة من الوسائل الالكترونية كأدلة إثبات يسودها مبدأ حرية القاضي في تكوين اقتناعه، فهو يتناول حجية الأدلة الالكترونية ضمن مسألة قبول الأدلة المتحصلة على الآلة أو ما يسمى بالأدلة العلمية والتي تقبل كطرق إثبات حسب نص المادة 212 من قانون الإجراءات الجزائية.

ولكن قبول الأدلة المتحصلة من الوسائل الالكترونية في ظل القواعد الأنجلوأمريكية يثير عدة مشاكل ذلك أنها تعتنق مبدأ الإثبات بالشهادة التي تتعلق بالواقعة محل الإثبات ولذلك فإن قبول المستندات المطبوعة لمخرجات الوسائل الالكترونية وهي عبارة عن إشارات الكترونية ونبضات ممغنطة، يمثل مشكلة أمام القضاء في هذا النظام، إذ لا يمكن للمحلفين أو القاضي من مناظرة الأدلة المتولدة منها ووضع أيديهم عليها وهذا يجعلها بمثابة أدلة ثانوية وليست أصلية².

2/: شروط قبول مخرجات الوسائل الالكترونية كأدلة إثبات في المواد الجزائية.

إن الأدلة المتحصلة عن الوسائل الالكترونية توجس خيفة القضاء من عدم تعبيرها عن الحقيقة نظرا لما يمكن أن تخضع له طرق الحصول عليها من التعرض للتزيف والتحريف والأخطاء المتعددة وسرعة إتلافها أو تغييرها ولم يقيد المشرع الجزائري أي شروط بخصوص هذه الأدلة بل تركها للقاضي. وأرى أنه على القاضي لقبول هذه الأدلة كأساس تشيد عليه الحقيقة في الدعوى العمومية سواء أكان الحكم الصادر فيها بالإدانة أم بالبراءة يجب توافر بعض الشروط أهمها:

1. أن تكون هذه الأدلة يقينية:

وهذا يستوجب أن تقترب نحو الحقيقة الواقعية قدر المستطاع وأن تتبعد عن الظنون والتخمينات، فلا محل لدحض مبدأ أن الأصل في الإنسان البراءة بالنسبة لهذه الأدلة إلا بتعيين مثله أو أقوى منه ذلك

¹ د. هلاي عبد الله، المرجع السابق، ص 212 وما بعدها.

² د. هشام رستم، المرجع السابق، ص 173

أن هذه المخرجات الالكترونية أو أقراص ممغنطة أو مصغرات فيلمية تخضع لتقدير القاضي الجزائي، ويجب أن نستنتج منها الحقيقة بما يتفق مع اليقين ويتعد عن الشك والاحتمال. والقاضي يمكنه أن يصل إلى يقينية المخرجات عن طريق المعرفة العلمية بما يقوم به من استقراء واستنتاج ليصل إلى الحقيقة وهذا ما يفرض على القاضي تأهيلا متخصصا في هذا المجال.

2. يتعين مناقشة مخرجات الوسائل الالكترونية تطبيقا لمبدأ شفوية المرافعة:

إذا كانت مخرجات الوسائل الالكترونية تعد أدلة إثبات قائمة في أوراق الدعوى في الجريمة المعلوماتية، فإنه يجب مناقشتها أما الخصوم إذ تنص المادة 212 في فقرتها الثانية على أنه لا يسوغ للقاضي أن يبنى قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه. فعلى القاضي الاجتهاد في الحكم في الجرائم المعلوماتية وعدم الاعتماد على رأي الغير، إلا إذا كان الغير من الخبراء، وقد ارتاح ضميره إلى التقرير المحرر منه وقرر الاستناد إليه ضمن حكمه بناء عليه يكون متولدا من عقيدته وليس من تقرير الخبير.

3. يجب أن تكون الأدلة المتحصلة من الوسائل الالكترونية مشروعة:

وتترتب على ذلك أن إجراءات جمع الأدلة المتحصلة من الحاسب الآلي إذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليها، فإنها تكون باطلة ولا تصلح لأن تكون أدلة تبنى عليها الإدانة في المواد الجزائية.

ومن أمثلة ذلك استخدام الغش ومخالفة القيود الواردة في قانون الإجراءات الجزائية من أجل الحصول على الأدلة الالكترونية.

ثانيا: تقدير أدلة الإثبات المتحصلة عن الوسائل الالكترونية:

تنوع نظم الأدلة الجزائية في الإثبات، بين التي تأخذ بنظام الأدلة القانونية في الإثبات وأخرى تعتنق الإثبات الحر القائم على حرية القاضي الجزائي في تكوين اقتناعه وتلك التي تجمع بين النظامين بما يسمى النظام المختلط.

ففي نظام الأدلة القانونية يتقيد القاضي في الإثبات بأدلة يحددها له المشرع مقدما ويقدر له قيمتها في الإثبات، فيتقيد القاضي بأن يستمد اقتناعه من هذه الأدلة دون غيرها¹.

¹ د. سعيد عبد اللطيف، اثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، دار النهضة العربية، ط 1999،

أما في نظام الأدلة الاقتناعية فإن القاضي لا يقيدده المشرع بأدلة إثبات معينة وإنما يترك له حرية الإثبات وفقا للسلطة التقديرية في تقدير الدليل ويترب عن ذلك أن للقاضي الجزائي قبول أي دليل يمكن أن يتولد منه اقتناعه¹.

وعلى الرغم من سيادة هذا النظام الأخير للإثبات الجنائي في جل التشريعات، منها الجزائر إلا أن المشرع قد طبق في إثبات بعض الجرائم نظام الأدلة القانونية عندما نص على تقييد سلطة القاضي في الإثبات بأدلة معينة ومثال ذلك إعطاء حجية كاملة لبعض المحاضر كمحاضر الحجز والمعاينة الجمركية التي تكون صحيحة إلى أن يطعن فيها بالتزوير² ومحاضر أخرى أعطاه المشرع حجية نسبية فتكون صحيحة إلى أن يثبت العكس وهنا ينتقل عبء الإثبات من النيابة إلى المتهم ومثال ذلك الاعترافات والتصريحات في المحاضر الجمركية³.

وتقييد سلطة القاضي في إثبات بعض الجرائم بأدلة معينة ومثال ذلك المادة 341 من قانون العقوبات والتي نصت على وسائل إثبات محددة لإثبات جريمة الزنا، وهذه الحجية وتلك القيود التي ترد على ذلك حرية القاضي في الاقتناع ليس المقصود منها افتراض ارتكاب المتهم للوقائع التي تنص على إعطائها الحجية ولكنها تعفي القاضي من إعادة التحقيق فيها. ويظل القاضي هو مالك السلطة التقديرية لهذه الأدلة ليستمد منها اقتناعه ويظل المتهم بريئا إلى حين إثبات عكس ذلك بالأدلة الكافية.

وإذا كان التطور العلمي قد أفرز ثورة الاتصالات عن بعد وجاءت للبشرية بتكنولوجيا جديدة نراها في مختلف مناحي الحياة، كالتجارة الالكترونية، وشبكات الاتصال العالمية (الانترنت) والتحويلات المصرفية الالكترونية، والنقود الالكترونية وحلول الثورة الرقمية محل الأوراق والكتابة والتوقيعات التقليدية يطرح التساؤل هنا حول الآثار التي ترتبت على ثورة الاتصالات ومدى تأثيرها في الإثبات الجزائي بالاعتماد على الأدلة العلمية الالكترونية ومدى تقييد سلطة القاضي في الاقتناع.

¹ د. عبد الرؤوف مهدي، حدود حرية القاضي في تكوين عقيدته، مؤسسة العين للطباعة ص 12 و 13

² د. حسن بوسقيعة، المنازعات الجمركية، دار هومة، ط 2005، ص 191.

³ غ.ج 2 ملف 73553 قرار 12-06-1992 وايضا غ.ج.م ق 3 ملف 89323 قرار 8-11-92 ص 52 و 53

فقد وفرت التقنية العلمية طرقا دقيقة لجمع الأدلة بحيث يمكن أن يساهم العلم في صنع الدليل بحيث أن هذا الدليل قد يتمتع بقوة علمية يصعب إثبات عكسها، مثلما هو الحال بالنسبة للبصمة الوراثية، وبصمة قزحية العين... الخ.

كما وفرت التقنية العلمية بالمقابل الوسائل الكافية لخلق جرائم أشد تعقيدا زادت من تعقيد الدليل وطرق الوصول إليه، وخلق عناصر تكوينية في الجرائم تغير مفهومها التقليدي كالشيكات الالكترونية مثلا التي تؤثر بدورها في جريمة الشيك ذلك إثباته يعتمد على مسائل فنية لإثبات الشيك كورقة تجارية.

وظهور الكيانات غير المادية التي تكون محلا في جريمة خيانة الأمانة والتي يتطلب البحث فيها عن العقد الذي تسلم الجاني هذا الكيان غير المادي بموجبه.

وتغير مفهوم المستند في جرائم التزوير بظهور المستندات الالكترونية وتغير طرق الإثبات في هذه الجرائم خاصة بعد ظهور التوقيع الالكتروني وتمتعه بالحجية في الإثبات في الكثير من التشريعات وإذا كانت الغلبة في إثبات الجرائم الالكترونية للخبرة، فان ذلك سيزيد من أهمية الدليل العلمي في الإثبات الجزائي ويزيد بذلك أهمية دور القاضي في هذا الإثبات بحيث يظل القاضي متمتعا بسلطة تقديرية في تقدير هذه الأدلة حسبنا أنها قد لا تكون مؤكدة على سبيل القطع¹.

Jean Pierre , essai de synthèse et libre de cloture le droit des preuves au ¹ defi de la modernité. Op.Cit. P 144

أو قد تكون أمارات أو دلالات، أو قد يحوطها الشك، فهنا تظهر أهمية هذه السلطة التقديرية التي يجب أن يتمتع بها القاضي كما تظهر أهمية تأهيل وتكوين القاضي في هذا النوع من الجرائم لأنه من خلال ذلك يستطيع إظهار مواطن الضعف في هذه الأدلة ويستطيع تفسير الشك لصالح المتهم.

فالدليل مهما تقدمت طرقه وعلت قيمته العلمية أو الفنية في الإثبات، فإنه يحتاج إلى قاض يتمتع بسلطة تقديرية، لأن هذه السلطة التقديرية تكون لازمة لتنقية الدليل من الخطأ أو الغلط أو الغش، وهي تكون ضرورية أيضا لكي تجعل الحقيقة العلمية حقيقة قضائية، فالحقيقة تحتاج إلى دليل.

الخاتمة:

لقد بات من المحتتم على دول العالم مواكبة التطور التكنولوجي الحاصل في العالم الافتراضي الجديد الذي صارت المعلومة فيه سيدة دون منازع ومصدرا للقوة، المعرفة، السلطة والمال، بل وأكثر من هذا صارت معيارا لتطور الشعوب ونموها.

وإزاء التطور العلمي الهائل فإن مرايا المعلوماتية جلبت معها أيضا مخاطر جمة طوعها المجرم المعلوماتي وصارت سلاحا لا يستهان به لممارسة نشاطاته الإجرامية وبهذا ظهرت طائفة جديدة من الجرائم المستحدثة، إضافة إلى إمكانية ارتكاب الجرائم التقليدية بطريقة حديثة، وباتت القوانين الجزائية، الموضوعية منها والإجرائية قاصرة عن مواجهة الجرائم المرتكبة باستخدام الحاسب الآلي.

وقد تبين لنا من خلال دراسة لهذا البحث قصور قواعد الإجراءات الجزائية في مواجهة الإجرام المعلوماتي، كفشلها في مجال الضبط والتحري، التحقيق، تفتيش النظام المعلوماتي استنباط الأدلة وإثبات الجريمة المعلوماتية وصعوبة إثبات الجرائم الالكترونية بالنظر إلى طبيعة الدليل الذي يتحصل منها، إذ قد يكون هذا الدليل غير مرئي وقد يسهل إخفاؤه أو تدميره، وقد يكون متصلا بدول أخرى فتكون هناك صعوبة للحصول عليه نظرا لتمسك كل دولة بسيادتها. كما وأن هذا الإثبات قد يحتاج إلى معرفة علمية وفنية قد لا تتوافر لضباط الشرطة القضائية والقضاة.

مكانة الدليل الإلكتروني في الإثبات الجزائي

د/ بن حميدوش نور الدين

كلية الحقوق والعلوم السياسية

جامعة المسيلة

ط.د/ رحموني عبد الرزاق

كلية الحقوق والعلوم السياسية

جامعة المسيلة

مقدمة:

أدى التطور الهائل في علم البرمجيات، والتقدم المتسارع للتقنية والأنظمة المعلوماتية، خصوصا من ناحية أتمة وآنية الاتصالات، إلى بروز نمط جديد من الجريمة تتعدى في صورها وأشكالها الجرائم التقليدية المعروفة، إذ أن مرتكبها يمتاز بالدكاء والاحترافية، وحسن استعمال تقنيات الشبكة الإلكترونية، خاصة إذا علمنا أن الانترنت أصبحت تشكل قوة اجتماعية واقتصادية وسياسية في المجتمعات المعاصرة.

إذ اعتبر تقرير صادر عن الأمم المتحدة حول شبكة الانترنت، أن الحصول على خدمة الانترنت يعتبر حق من حقوق الإنسان الأساسية¹، وقد نتج عن هذا التطور بروز نمط جديد من الجرائم تدعى بالجرائم المعلوماتية وأخطر ما فيها هي خصائصها إذ أنها جرائم تتعدى الحدود الجغرافية للدول كونها تقع في حيز افتراضي غير محدود، الأمر الذي يثير عدة إشكالات منها الاختصاص في الزمان والمكان، كما أنها جريمة يصعب الكشف عنها أو تتبعها إلا بالطرق التقنية والتكنولوجية المعقدة التي تتطلب الخبرة والاحترافية، ضف إلى ذلك خصوصية دليل الإثبات الذي يعد الفيصل في قيام الجريمة من عدمها، ونظرا للطبيعة الخاصة التي تتميز بها الدليل الرقمي عن غيره، إلا أنه يشير العديد من الإشكالات الخاصة فيما يتعلق بمشروعية وحجية ومصادقته ومدى قبوله قضائيا.

الإشكالية التالية:

¹ جريدة لوس أنجلوس تايمز، مقال منشور في موقع الإلكتروني

<https://latimesblogs.latimes.com/technology/2011/06/united-nations-report-internet-access-is-a-human-right.html> 22:22 على الساعة: بتاريخ:

2019/02/12

تكتسب قواعد الإثبات أهمية بالغة، إذ من شأنها أن تشكل حماية قانونية للشخص في حد ذاته في التحقيقات الجنائية، ولعل موضوع الدليل الإلكتروني على وجه الخصوص يعد من الموضوعات التي تطرح عدة إشكالات قانونية وذلك للطبيعة الخاصة والغير المألوفة. هذا ما يقودنا لطرح الإشكالية التالية: ما المقصود بالدليل الإلكتروني وما دوره في الإثبات وما حجته؟

وللإجابة على هذه الإشكالية نعتمد الخطوة التالية:

المحور الأول: مفهوم الدليل الإلكتروني

أولاً: تعريف الدليل الإلكتروني

ثانياً: الطبيعة القانونية للدليل الإلكتروني

المحور الثاني: حجية الإثبات بالدليل الإلكتروني في المادة الجزائية

أولاً: شرعية الإثبات بالدليل الإلكتروني

ثانياً: سلطة القضاء في الأخذ بالدليل الإلكتروني

المحور الأول: مفهوم الدليل الإلكتروني

إن الدليل الإلكتروني من الأدلة ذات الخصوصية، في طبيعة البيئة الافتراضية التي يستخلص منها، ما يستلزم استعراض المقصود بالدليل الإلكتروني.

أولاً: تعريف الدليل الإلكتروني:

1- اصطلاحاً:

الدليل هو ما يلزم من العلم به على الشيء الآخر، وغايته أن يتوصل العقل إلى التصديق اليقين بما كان يضمن في صحته، بمعنى أنه الطريقة التي يستعين بها القاضي للحصول على الحقيقة التي يستدل بها.¹

2- فقهيًا:

تعددت التعريفات الفقهية للدليل الإلكتروني إذ تباينت بين النظرة القانونية للتعريف، والنظرة التقنية البحتة له.

¹ منصور عمر المعاينة، الأدلة الجنائية والتحقيق الجنائي، طبعة 01، دار الثقافة والنشر والتوزيع، الأردن، 2007، ص 18.

فهناك من عرفه على أنه: (معلومات يتقبلها المنطق والعقل ويعتمد بها العلم، يتم الحصول عليها بإجراءات قانونية وعليه، وذلك بترجمة البيانات الرقمية والحسابية المخزنة في الأجهزة وملاحقتها أو في شبكات الاتصال، حيث يمكن استخدامها في أي مرحلة من مراحل الجنائي، أو المحاكمة لإثبات حقيقة أو فعل أو شيء له علاقة بجريمة أو جان أو مجني عليه)¹.

كما عرفه البعض بأنه: (كل البيانات التي يمكن إعدادها أو تخزينها في شكل رقمي، بحيث تمكن الحاسوب من إنجاز مهمة ما)².

وعامة فإن دليل الجنائي معنى يدرك من مضمون واقعة تؤدي لثبوت الإدانة أو ثبوت البراءة ويتم ذلك باستخدام الأسلوب العقلي، وإعمال المنطق في وزن وتقدير تلك الواقعة فيصبح المعنى المستمد منها أكثر دقة ودلالة على الإدانة أو البراءة.³

ومما سبق يمكن تعريف الدليل الإلكتروني: بأنه الدليل المأخوذ من أجهزة الحاسوب ويكون في شكل مجالات أو نبضات ممغنطة أو كهربائية يمكن تجميعها أو تحليلها باستخدام برامج وتطبيقات تكنولوجية خاصة، وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال أو الرسوم، وذلك من أجل اعتماده أمام أجهزة إنفاذ القانون.⁴

ثانيا: الطبيعة القانونية للدليل الإلكتروني

يثار التساؤل على موقع الدليل الإلكتروني من بين الأدلة الجنائية الأخرى.

1- الدليل الإلكتروني هو دليل مادي:

إذ يرى هذا الاتجاه من الفقه، أن الدليل الإلكتروني ما هو إلا مرحلة متقدمة من الأدلة المادية، والتي يستطيع الإنسان إدراكها بحواسه الطبيعية.⁵

¹ المرجع نفسه، ص 26.

² عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، مصر، 2010، ص 47.

³ محمد مأمون سلامة، الإجراءات الجنائية في التشريع المصري، دار النهضة العربي، القاهرة، ب. س. ن، ص 199.

⁴ نضال ياسين الحاج حمو، دور الدليل الإلكتروني في الإثبات الجنائي، مجلة جامعة تكريت للعلوم القانونية، مجلد 01، عدد 19، ب. س. ن، ص 43.

⁵ محمود نجيب حسني، شرح قانون الإجراءات الجنائية، طبعة 02، دار النهضة العربية، سنة 1988، ص 410-411.

فهي إما تكون في شكل كتابة أو رسم على مخرجات ورقية، وإما أن تكون إلكترونية كالأشرطة والأقراص الممغنطة وغيرها من الأشكال الإلكترونية غير التقليدية¹، وإما أنها تتمثل في عرض مخرجات المعالجة بواسطة حاسوب على شاشة العرض.²

2- الطبيعة الخاصة للدليل الإلكتروني:

أي أن للدليل الإلكتروني طبيعة خاصة تميزه عن باقي الأدلة الجنائية، فهو دليل جديد يضاف لأنواع الأدلة الجنائية المعروفة.³

وهو الرأي الراجح لأن الأدلة الإلكترونية تتمتع بخصائص وسمات تجعلها تتميز عن الأدلة الجنائية الأخرى -القانونية، المادية، الفنية والقولية- سواء من حيث البيئة التي تنبعث منها وهي العالم الافتراضي المبني على كيفية المعنوية غير المادية⁴.

- كما يمتاز الدليل الإلكتروني بجملة من الخصائص نوجزها فيما يلي:

يستخلص الدليل الإلكتروني من البيئة متطورة تشمل أصناف عدة من بيانات رقمية وبرمجية مما جعله يتميز بعدة خصائص:

❖ الدليل الإلكتروني ذو طبيعة مزدوجة:

إذ يتطلب إدراك هذا الدليل الاستعانة بأجهزة ومعدات وبرمجيات حاسوبية فهو ينطبق عليه ما ينطبق على الأدلة العلمية.⁵

كما أنه دليل تقني من بيئة خاصة هي البيئة الرقمية التقنية، التي لها جرائمها الخاصة بها، فلا وجود للدليل الإلكتروني خارج بيئة تقنية أو إلكترونية.¹

¹ محمد عمر بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، د. دارنشر، سنة 2006، ص 98.

² Ecoghan Casey ,Digital,Evidence and computer Crime Forensic Science,computer and the internet,second edition academic press an imprint of Elsevier,London,2004, p06

³ هلاي عبد الإله أحمد، حجية المخرجات الكمبيوترية في الإثبات الجنائي، دار النهضة العربية، القاهرة 1988، ص 21.

⁴ نضال ياسين الحاج حمو، المرجع السابق، ص 55.

⁵ عائشة بن قارة مصطفى، مرجع سابق، ص 63.

❖ الدليل الإلكتروني دليل صعب الإتيلاف:

وتعد هذه الخاصية مميزة للدليل الإلكتروني عن غيره من الأدلة التقليدية حيث يمكن استرجاعها بعد محوها وإصلاحها بعد تلفها وإظهارها بعد إخفائها مما يؤدي إلى صعوبة التخلص منها، وحتى وإن سعى الجاني لمحو الدليل فإن ذلك سيشكل دليلا آخر لإدانته، إذ يتم تسجيل هذا الفعل داخل الحاسوب.²

❖ الدليل الإلكتروني دليل متطور ومتعدد الأشكال:

فقد يتخذ الدليل الرقمي أشكالا مختلفة، فهو يشمل كافة أشكال وأنواع البيانات الإلكترونية الممكنة، كما هو الشأن في حالة الرقابة على شبكات الانترنت والخادم، كما يمكن أن يكون صورا ثابتة أو متحركة، أو مزودة بنظام للتسجيل السمعي البصري، أو مخزنة في البريد الإلكتروني، فهذه الأمور كلها تستوجب تطورا علميا وتكنولوجيا³.

المحور الثاني: حجية الإثبات بالدليل الإلكتروني في المادة الجزائية

أولا: شرعية الإثبات بالدليل الإلكتروني

01- في التشريعات المقارنة:

تذهب جل التشريعات المقارنة إلى قبول الدليل الإلكتروني، المتحصل عليه من أنظمة البرمجة الآلية أو مخرجات أنظمة المعالجة الآلية للبيانات المكتوبة، على الشاشات، أو البيانات المسجلة على دعائم مغمطة، أو مخرجات أنظمة المعالجة، كأداة يقوم عليها الإثبات الجزائي، إلا أن هذه الأدلة المتحصل عليها من هذه الوسائل السالفة الذكر تخضع لسلطة القاضي الجزائي التقديرية ومدى اقتناع القاضي بها، كما أن مدى قبول هذه الأدلة قضائيا يختلف من نظام قانوني لآخر.⁴

¹فتحى محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، طبعة 01، دار النشر والقانون مصر، ص 650.

²Ecoghan Casey, o.p, cit, p08

³فتحى محمد أنور عزت، مرجع سابق، ص 653.

⁴ياسين الحاج هو، مرجع سابق، ص 38.

ففي فرنسا مثلاً تم تناول حجية مخرجات الأنظمة الآلية ضمن ما يسمى بالأدلة العلمية التي يجب أن تتوفر فيها شروط معينة ومقررة لها سلفاً حتى تقبل كوسيلة من وسائل الإثبات.¹

02- موقف المشرع الجزائري:

لقد أخذ المشرع الجزائري بمبدأ الإثبات الجنائي الحر كأصل، والذي نص عليه صراحة في المادة 212 من قانون الإجراءات الجزائية²، على أنه: (يجوز إثبات الجرائم بأي طريق من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعاً لاعتقائه الخاص). لكن ما لبث المشرع أن تدارك تأخره في هذا المجال بسنّه القانون 04-15 الذي يهدف لتوفير الحماية الجزائية للأنظمة المعلوماتية³، وأساليب معالجة المعطيات إذ تطرق المشرع الجزائري إلى تحريم الأفعال والأعمال التي تمس بأنظمة المعالجة الآلية للمعطيات من خلال المواد 394 مكرر إلى 394 مكرر 07.⁴

ثم جاء القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والذي احتوى قواعد للوقاية من الجرائم الافتراضية ودعم وسائل مكافحتها، من خلال وضع ترتيبات تسمح برصدها المبكر وجمع أدلة عنها.⁵ وبين هذا القانون أن الدليل الإلكتروني يخضع في ضبطه إلى القواعد العامة المطبقة على باقي الأدلة الجزائية، وهذا ما أشارت إليه المادة 06 من نفس القانون.⁶

¹ أحمد ضياء الدين محمد خليل، مشروعية الدليل في المواد الجنائية، دراسة تحليلية مقارنة لنظريتي الإثبات والمشروعية في مجال الإجراءات الجنائية، أطروحة دكتورا كلية الحقوق، جامعة عين شمس، القاهرة، 1986، ص 239.

² الأمر 66-155 مؤرخ في 08 يونيو 1966 المعدل والمتمم، المتضمن قانون الإجراءات الجزائية.

³ قانون رقم 04-15 ماضي في 10 نوفمبر، الجريدة الرسمية عدد 71 مؤرخة في 10 نوفمبر 2004، ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات.

⁴ المواد من 394 مكرر إلى 394 مكرر 07

⁵ قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن

القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته ومكافحتها، جريد رسمية عدد 47.

⁶ نص المادة 06 من القانون 09-04.

ثانيا: سلطة القضاء في الأخذ بالدليل الإلكتروني

01- شروط إعمال الدليل الإلكتروني قضائيا:

إن الدليل الإلكتروني عامة يخضع لمبدأ الإثبات لأن الأصل هو مشروعية وجودها، وهو الأمر الذي أخذ به المشرع الجزائري،¹ وهو نص عليه صراحة في المادة 212 من قانون الإجراءات السالفة الذكر في هذا النظام لا تعني استعمال وسائل غير قانونية فردية الإثبات هي مقيدة بضوابط المشروعية التي يجب أن لا تخالف المبادئ العامة في الإثبات وإلا ترتب على هذه المخالفة عدم مشروعية الدليل ومنه عدم قبوله وبطلانه.²

لذلك وبقبول هذه الأدلة جزئيا يجب أن تتوفر على بعض المواصفات منها:

- أن يكون الدليل واقعي غير خيالي، ويتعد عن الشك والتخمين.
- يجب مناقشة الدليل أمام الخصوم، تطبيقا لمبدأ الوجاهية، وهو ما نصت عليه المادة 212 من قانون الإجراءات المدنية والإدارية في فقرتها الثانية وهو الأمر الذي يدعم مبدأ الحرية الإثبات ويعمق من قناعة القاضي له.
- يجب أن تكون عملية استخلاص الدليل مشروعة، ويسمح بها القانون، وإلا عدت باطلة لا يقيد بها قضائيا.

02- سلطة القاضي في قبول الدليل:

مهما تعددت طرق استخلاص الدليل وقيمتة القضائية فإنها تبقى خاضعة لسلطة القاضي وقناعته،³ إلا في الحالات التي ينص القانون على أدلة معينة، كمحاضر الحجز والمعاينة الجمركة التي تتمتع بالحجية الكاملة⁴

كما أن على القاضي أن يبني قناعته على عنصرين هما:

¹ خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، طبعة 01، دار الثقافة للنشر والتوزيع، الأردن، 2011.

² عائشة بن قارة، مرجع سابق، ص 186 - 187

³ عبد الرؤوف مهدي، حدود حرية القاضي في تكوين عقيدته، محاضرات القيت على طلبة دراسات عليا علوم جنائي، 2000، ص13.

⁴ حسن بوسقيعة، المنازعات الجمركية، دار هومة، سنة 2005، ص190.

أ- عنصر ذاتي: والذي يعني ارتياح القاضي واطمئنانه إلى الحكم الذي حكم به على سبيل الجزم واليقين لا على سبيل الشك والظن.

ب- عنصر موضوعي: ويعني أن هذا الاطمئنان يتركز على أساس المنطق والعقل في قبول هذا الدليل¹.

أما فيما يتعلق بحكم البراءة فإنه يكفي ظن القاضي ببراءة المتهم، لأن الأصل براءة الإنسان ما لم يثبت إدانته، وكذا عملاً لقاعدة أن الشك يفسر لمصلحة المتهم، وهو ما أكدته المشرع الجزائري بدوره في جميع دساتيره إذ نص في المادة 56 من دستور 1996 المعدل والمتمم، على أن كل شخص يعتبر بريئاً حتى تثبت إدانته، في إطار محاكمة عادلة تؤمن له الضمانات اللازمة للدفاع عن نفسه.² لذلك ومما سبق فإن توفر الدليل الإلكتروني لا يعني أن القاضي ملزم به، بل يبقى دليل إثبات كما في الأدلة التقليدية، وللقاضي السلطة التقديرية معتمداً على ظروف وملابسات القضية، إما الأخذ به أو تركه³.

الخاتمة:

لقد تناولنا في ورقتنا البحثية مفهوم الدليل الإلكتروني، وكذا شروط الأخذ به وإعماله قضائياً وكذلك نطاق سلطة القاضي الجزائري بالأخذ به من عدمه، كما أدرك المشرع الجزائري أهمية هذا النوع من الأدلة، إذ عمل على استحداث قواعد موضوعية وأخرى إجرائية جديدة تتماشى مع خصوصية الجريمة المعلوماتية وأدلتها وانطلاقاً من عجز القواعد الإجرائية التقليدية في التعامل مع الأدلة الجنائية الرقمية.

كما خالصنا في بحثنا إلى مجموعة من النتائج نوجزها في مايلي:

- ينفرد الدليل الإلكتروني بمجموعة من السمات والخصائص التي تميزه عن باقي الأدلة التقليدية الأخرى.

¹ مفيدة سويدان، نظرية الاقتناع الذاتي للقاضي الجنائي، أطروحة دكتوراه، جامعة القاهرة، 1985، ص 116.

² القانون رقم 16-01 المؤرخ في 06 مارس 2016 الجريدة الرسمية رقم 14 المؤرخة في 7 مارس 2016، المتضمن تعديل دستور 1996.

³ عائشة بن قارة، مرجع سابق، ص 247.

- حتى يكون للدليل الإلكتروني حجية في الإثبات، يجب أن يستخلص وفق الطرق والأساليب المنصوص عليها قانوناً وإلا كان باطلاً لا يعتد به.
- يجب مناقشة الدليل الإلكتروني أمام جميع أطراف الدعوى تطبيقاً لمبدأ الوجاهية.
- العمل على رفع كفاءة رجال الضبطية القضائية وكذا القضاة عامة، على التعامل مع الطبيعة الخاصة للدليل الإلكتروني.
- استحداث مخبر جنائي خاص بالجرائم الإلكترونية.
- ضرورة تعزيز التعاون الدولي في مجال مكافحة هذا النوع من الجرائم، وكذا تبادل الخبرات التقنية في مجال استخلاص الدليل وطرق معالجته.

قائمة المراجع:

أولاً: باللغة العربية

أ- القانون:

- 01- دستور 28 نوفمبر 1996، منشور بموجب المرسوم الرئاسي رقم 438-96، مؤرخ في 7 ديسمبر 1996، ج.ر.ج.د.ش، عدد 76، لسنة 1996، المعدل والمتمم.

02- القوانين:

- الأمر 66-155 مؤرخ في 08 يونيو 1966 المعدل والمتمم، المتضمن قانون الإجراءات الجزائية.
- قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته ومكافحتها، جريد رسمية عدد 47.
- قانون رقم 04-15 ماضي في 10 نوفمبر 2004 الرسمية عدد 71 مؤرخة في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات.

- القانون رقم 16-01 المؤرخ في 06 مارس 2016 الجريدة الرسمية رقم 14 المؤرخة في 7 مارس 2016.
- ب-الكتب:**
- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجيدة، مصر، 2010.
- محمد مأمون سلامة، الإجراءات الجنائية في التشريع المصري، دار النهضة العربي، القاهرة، ب. س.ن.
- محمود نجيب حسني، شرح قانون الإجراءات الجنائية، طبعة 02، دار النهضة العربية، سنة 1988
- هلاي عبد الإله أحمد، حجية المخرجات الكمبيوترية في الإثبات الجنائي، دار النهضة العربية، القاهرة 1988.
- فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، طبعة 01، دار النشر والقانون مصر.
- محمد عمر بن يونس، الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، دون دار نشر، سنة 2006.
- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، طبعة 01، دار الثقافة للنشر والتوزيع، الأردن، 2011.
- منصور عمر المعاينة، الأدلة الجنائية والتحقيق الجنائي، طبعة 01، دار الثقافة والنشر والتوزيع، الأردن، 2007.
- احسن بوسقيعة، المنازعات الجمركية، دار هومة، سنة 2005.
- ج- الأطروحات والمحاضرات الجامعية:**
- مفيدة سويدان، نظرية الاقناع الذاتي للقاضي الجنائي، أطروحة دكتوراه، جامعة القاهرة، غير منشورة. د.س.ن.

- عبد الرؤوف مهدي حدود حرية القاضي في تكوين عقيدته، محاضرات القيت على طلبة دراسات عليا علوم جنائي، 2000

- أحمد ضياء الدين محمد خليل، مشروعية الدليل في المواد الجنائية، دراسة تحليلية مقارنة لنظريتي الإثبات والمشروعية في مجال الإجراءات الجنائية، أطروحة دكتورا كلية الحقوق، جامعة عين شمس، القاهرة، 1986

ح- المجالات والمقالات:

- نضال ياسين الحاج حمو، دور الدليل الإلكتروني في الإثبات الجنائي، مجلة جامعة تكريت للعلوم القانونية، مجلد 01، عدد 19، ب. س.

خ- مواقع الأنترنت:

- مقال منشور في موقع الإلكتروني لجريدة لوس أنجلوس تايمز
latimesblogs.latimes.com على الساعة: 22:22 بتاريخ: 2019/02/12.

ثانيا: باللغة الأجنبية

- EcoghanCasey ,Digital,Evidence and computer Crime
Forensic Science,computer and the internet,second edition
academic press an imprint of Elsevier,London,2004.

مدى خضوع الدليل الرقمي للقواعد المقررة للإثبات الجنائي

ط.د/ بومسلة عبد القادر

جامعة سوسة

تونس

د/ راجي خضر

كلية الحقوق والعلوم السياسية

جامعة الاغواط

مقدمة:

إن التطور العلمي الرهيب الذي يشهده العالم اليوم، وذلك راجع لإستخدام التقنيات التكنولوجية في كل مجالات الحياة، بل وتم استعمال هته التقنيات التكنولوجية حتى في ارتكاب الجرائم، مما أدى إلى ظهور ما يسمى بالجريمة المعلوماتية والتي بذل الفقه جهودا لوضع لها التعريف المناسب، فمنهم من يعرفها بأنها: "كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر كبير لازما لارتكابه من ناحية وملاحقته من ناحية أخرى"، والبعض الآخر يعتبرها: "الجريمة التي تتم باستخدام الحاسب الآلي، أو تلك التي تقع على الحاسب الآلي ذاته" أو هي كل سلوك إجرامي يتم بمساعدة الكمبيوتر¹.

فجريمة الأمس ليست كجريمة اليوم، هذا ما استوجب توفير الحماية القانونية اللازمة وإيجاد نظام عقابي متكامل لمرتكب الجريمة المعلوماتية، بحيث أصبح هذا النوع من الجرائم يرتكب في وسط افتراضي غير مؤلفو، لا يشبه الوسط التقليدي للجرائم التقليدية، وهو ما استتبع ظهور طائفة جديدة من الأدلة تتماشى وطبيعة الوسط الذي ترتكب فيه الجريمة المعلوماتية وهي الأدلة الرقمية، ويمكن تعريف هذا الأخير بأنه: "كل بيانات يمكن إعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسوب من انجاز مهمة ما" أو هو "الدليل الذي نجد له أساسا في العالم الافتراضي ويقود إلى الجريمة" ويرى جانب آخر من الفقهاء بأنه: " معلومة مخزنة في أجهزة الحاسوب وملحقاته من ديسكات وأقراص مرنة وغيرها من وسائل تقنية المعلومات كالتابعات والفاكس أو متنقلة عبر

¹ لبيض عادل و نزلي بشرى، إثبات الجريمة الإلكترونية، مذكرة مقدمة لاستكمال متطلبات شهادة الماستر، تخصص قانون جنائي، كلية الحقوق، جامعة قاصدي مرباح ورقلة، 2017/2018، ص 09.

شبكات الاتصال والتي يتم تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة بهدف إثبات وقوع الجريمة ونسبتها إلى مرتكبها"¹.

وتماشيا مع ما قدمناه فضلنا طرح الإشكالية التالية: إلى أي مدى يمكن اعتبار الدليل الرقمي دليلا مقبولا في إثبات الجريمة المعلوماتية ؟

وللإجابة على الإشكالية المطروحة قمنا بتقسيم دراستنا وفقا للخطة التالية:

المبحث الأول: القيمة القانونية للدليل الرقمي في الإثبات

المطلب الأول: مشروعية الدليل الرقمي

المطلب الثاني: حجية الدليل الرقمي في أنظمة الإثبات

المبحث الثاني: حجية الدليل الرقمي أمام القاضي الجزائي

المطلب الأول: الطبيعة العلمية للدليل الرقمي

المطلب الثاني: أثر الطبيعة العلمية للدليل الرقمي على الاقتناع الشخصي للقاضي

المبحث الأول: القيمة القانونية للدليل الرقمي في الإثبات

لا يمكن للقاضي الجنائي أن يصدر الحكم بناء على علمه الشخصي في مجال الإثبات إلا بعد إخطائه بوقائع الدعوى والتي تطرح أمامه في شكل أدلة، والأدلة هي الوسيلة التي يستقي منها قناعته، أما بالنسبة للدليل الرقمي في مجال الجريمة الإلكترونية فقد لا يعبر في بعض الأحيان على الحقيقة نظرا لما يتعرض له ممن تزيف وتخريب، هذا ما يثير مسألة مشروعية الأخذ به، إذ أنه وبوجه عام يستلزم في الدليل الجنائي أن يكون مشروعا من حيث وجوده ومن حيث الحصول عليه، هذا ما سوف يتم التطرق إليه من خلال مشروعية الدليل الرقمي (المطلب الأول) وحجيته في أنظمة الإثبات (المطلب الثاني).

المطلب الأول: مشروعية الدليل الرقمي

حكم الإدانة لا يتم إصداره بمجرد وجود أدلة تثبت وقوع الجريمة، بل يجب أن تكون لهته الأدلة قيمة قانونية أي بمعنى خضوعها للقواعد المقررة للإثبات الجنائي، وزيادة على ذلك فإن القانون يفرض

¹ حنان ربحان مبارك المضحكي، الجرائم المعلوماتية، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، 2014، ص34.

على القاضي بأن يلتزم بعدم قبول أي دليل تم الحصول عليه بطريقة غير مشروعة، وهذه المسألة تقع على عاتق القاضي الجنائي بعد عملية البحث عن الدليل وقبل إخضاعه لتقديره، وهذا من أجل حماية حقوق الأفراد وحرياتهم، والمقصود بمشروعية وجود الدليل الرقمي: "أن يكون الدليل معترفا به بمعنى أن يجيز القانون للقاضي الاستناد إليه لتكوين عقيدته للحكم بالإدانة"¹.

وما يجب لفت الانتباه إليه هو أن الدليل الرقمي لا يكون مشروعاً ولا يتم الأخذ به من طرف القاضي الجنائي، إلا إذا أجريت له عملية البحث والتنقيب وإقامته أمام القضاء في إطار ما وضعه القانون من أحكام والتي تعمل على تحقيق العدالة بين الدولة والمتهم²، ففي حالة الحصول على الدليل خارج هذه القواعد القانونية فلا يعتد به مهما كانت دلالاته وقوته نظراً لعدم مشروعيته، ومن الأمثلة في هذا الصدد الحصول على نظام معلوماتي باطل أثناء القيام بعملية التفتيش³، فتشريعات مختلف الدول تعمل جاهدة على ضبط وتحديد مختلف وسائل إجراءات تحصيل أدلة الإثبات، وإخضاعها لمبدأ الشرعية فيلجأ إليها القاضي الجنائي أثناء تكوين اقتناعه الشخصي كمعيار لتحديد مدى مشروعية الدليل المستند عليه في ذلك، ومنه نتوصل إلى أن هناك ارتباط وثيق بين مشروعية الدليل وشرعية الإجراء الموصل إليه فوجود الأول متوقف أساساً على وجود الثاني ولذلك لا يمكن غنى أي منها على الآخر⁴.

فلا يمكن إضفاء طابع المشروعية على الدليل الرقمي إلا إذا تم الحصول عليه بطرق مشروعة، هذا القيد يحظى بأهمية كبيرة نتيجة للتطور الهائل المتعلق بتطوير التقنية لكي تعمل في بيئة الرقابة، ونذكر على سبيل المثال المراقبة الالكترونية المستحدثة بموجب القانون رقم 09-04، فإذا كانت المراقبة

¹ خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان، الطبعة الأولى، 2011، ص 235.

² أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الالكترونية، دار الجامعة العربية، مصر، بدون طبعة، 2015، ص 206.

³ رشيدة بوكور، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، لبنان، الطبعة الأولى، 2012، ص 489.

⁴ هنية عميروش، أثر الدليل العلمي على اقتناع القاضي الجزائري، المجلة الأكاديمية للبحث القانوني، المجلد 16، العدد 02، 2017، ص 248.

الإلكترونية تفيد في الكشف عن الجريمة وإقامة الدليل على المتهم فإنها في نفس الوقت قد تمس بحريات الأفراد إذا لم يحسن استخدامها¹.

المطلب الثاني: حجية الدليل الرقمي في أنظمة الإثبات

المعيار الذي على أساسه يمكن تحديد موقف القوانين المقارنة فيما يتعلق بسلطة القاضي الجنائي في مدى قبول الدليل الإلكتروني كدليل لإثبات الجريمة المعلوماتية متوقف على حسب طبيعة نظام الإثبات السائد في الدولة، بحيث تنقسم هذه النظم إلى ثلاثة:

الفرع الأول: نظام الإثبات المقيد

في ظل هذا النظام لا يمكن قبول الدليل الرقمي من طرق القاضي الجنائي ما لم يتم النص عليه من قبل المشرع، حيث يتوجب على هذا الأخير تحديد هذا النوع من الأدلة مسبقا وبدقة، والقاضي الجنائي يتوجب عليه الأخذ بهذه الأدلة متى توافرت فيها شروط قبول الدليل الرقمي، من شرط مشروعيته وشروط مناقشته وشروط بلوغ القاضي درجة اليقين².

ومن بين الدول التي تأخذ بهذا النظام الو.م.أ، بريطانيا، كندا، استراليا... أي الدول ذات النظام الأنجلوسكسوني، حيث يتم طبقا لهذا النظام تحديد أدلة الإثبات المتاحة وقيمتها وقوتها في الإثبات من طرف المشرع، فالقاضي يكون مقيدا في حكمه بالاستناد على الأدلة المنصوص عليها في التشريع المعمول به، فإذا لم يتوفر الدليل لا يمكن للقاضي الحكم بالإدانة بغض النظر عن اقتناعه واعتقاده الشخصي، بل يحكم باستبعاد الدليل حتى لو اقتنع بأن المتهم مدان³.

¹ القانون رقم 09-04، المؤرخ في 14 شعبان 1430 الموافق ل 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر العدد 47، الصادرة في 16 أوت 2009.

¹ سامي جلال حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، درا الكتب القانونية، مصر، بدون طبعة، 2011، ص91.

³ سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، كلية الحقوق، جامعة باتنة، 2013، ص209.

إلا أن نظام الإثبات المقيد في ظل هذا التطور التكنولوجي يتعارض مع طبيعة الجريمة المعلوماتية والأدلة الناتجة عنها، هذا ما جعل الدول التي تنتهج هذا النظام قد بدأت تغير من حدته وأظهرت بعض الاستثناءات والليونة في هذا المجال وذلك بتغير نظرتها تجاه الدليل الرقمي¹.

الفرع الثاني: نظام الإثبات الحر

يأخذ بهذا النظام فرنسا واسبانيا وإيطاليا... ومعظم الدول العربية، أي دول النظام اللاتيني، ويقصد بنظام الإثبات الحر أن لجميع أطراف الدعوى الجنائية الحرية في اللجوء إلى كافة طرق الإثبات المتاحة للاستدلال على صحة ادعاءاتهم، فلسلطة الإتهام الحرية في اللجوء إلى أية وسيلة لإثبات وقوع الجريمة ونسبتها للمتهم، وللمتهم الحرية في إثبات براءته بأية وسيلة، وللقاضي السلطة التقديرية في قبول كل أدلة الإثبات أو طرحها، كما أن له أن يتحرى الحقيقة بنفسه وبممكنه في ذلك الاستعانة بكل وسائل الإثبات²، وبالتالي فإن للقاضي الدور الفعال في سير الدعوى الجنائية على عكس النظام المقيد الذي يتم فيه تحديد الأدلة مسبقا من طرف المشرع.

إذا فهذا النظام يصلح فيه الأخذ بالدليل الرقمي دون وجود أي عائق في الغالب، على أساس أنه يقوم على الحرية في الإثبات الجنائي³، وهو النظام الذي أخذ به المشرع الجزائري ويظهر ذلك في تكريس سلطة القاضي في قبول كل الأدلة للإثبات هذا ما تم النص عليه من خلال الفقرة الأولى المادة 212 من قانون الإجراءات الجزائية والتي جاء فيها: "يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص"⁴.

¹ بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم تخصص قانون عام، كلية الحقوق، جامعة الجزائر 01 بن يوسف بن خدة، 2018/2017، ص 238.

² بن فردية محمد، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة دكتوراه علوم تخصص قانون عام، كلية الحقوق، جامعة الجزائر 01 بن يوسف بن خدة، 2015، ص 204.

³ لبيض عادل و نزلي بشرى، المرجع السابق، ص 63.

³ المادة 212 الفقرة الأولى، من الأمر رقم 66-155 المؤرخ في 18 صفر 1386 الموافق ل 8 جوان 1966، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم، ج ر العدد 47 المؤرخة في 9 جوان 1966.

الفرع الثالث: النظام المختلط

إن هذا النظام مزج بين النظامين السابقين فهم يقوم على تحديد أدلة الإثبات سلفاً من قبل المشرع، بحيث يتقيد القاضي بهذه الأدلة المحددة سابقاً، ويحدد قيمة وحجية كل من تلك الأدلة، كما أنه يقوم على إعطاء حرية للقاضي في تقدير الأدلة الموجودة في القضية المطروحة أمامه، وفيما يتعلق بالدليل الرقمي من ناحية مبدأ تحديد الأدلة مسبقاً، فبالنسبة للتشريعات التي لم تنص عليه باعتباره دليلاً مستحدثاً لجرمة مستحدثة، إلا أن هذه التشريعات في إطار مواكبة التكنولوجيا وتماشياً مع هذا النوع المستحدث من الأدلة والجرائم، فقد قامت بوضع استثناءات حتى تضم هذا الدليل في تشريعاتها.

وبالنسبة لمبدأ حرية القاضي الجنائي لا يثير إشكالا باعتبار أن كل الأدلة الجنائية خاضعة لحرية وتقدير القاضي الجنائي، والدليل الرقمي يعتبر دليل من أدلة الإثبات الجنائي فهو خاضع لحرية القاضي وتقديره واقتناعه كغيره من الأدلة، أي للقاضي دور إيجابي في ظل هذا النظام¹.

المبحث الثاني: حجية الدليل الرقمي أمام القاضي الجزائي

أصبحت الأدلة الرقمية حجة يعول عليها القاضي الجنائي كأدلة يؤسس عليها أحكامه إما ببراءة المتهم أو بإدائته في العديد من القضايا خاصة في القضايا المتعلقة بالجرائم المعلوماتية هذا راجع لطبيعتها العلمية، إذ يعد قبول الدليل الرقمي الإجراء الأول الذي يمارسه القاضي، ولهذا الأخير الحر في الأخذ بالأدلة الرقمية.

ومنه سوف نبحث في هذا المبحث عن الطبيعة العلمية للدليل الرقمي وأثرها على اقتناع القاضي وذلك من خلال المطلبين التاليين.

المطلب الأول: الطبيعة العلمية للدليل الرقمي

الدليل الرقمي لا تختلف قيمته ولا تزيد حجته عن غيره من الأدلة، وبطبيعة الحال هذا أثر من آثار حرية القاضي الجنائي في الاقتناع، وعليه يؤسس القاضي اقتناعه على الدليل الرقمي كما يمكنه إبعاده، وبالتالي لا يجوز مطالبة القاضي أو إلزامه بالاقتناع بالدليل الرقمي حتى ولو لم تكن في الدعوى أدلة غيره.

¹ سامي جلال حسين، المرجع السابق، ص 93.

وبما أن الدليل الرقمي يعتبر تطبيق من تطبيقات الدليل العلمي، نظرا لما يتميز به من موضوعية وحياد وكفاءة، مما يجعل اقتناع القاضي الجنائي أكثر جزما وبقينا، حيث يساعده على التقليل من الأخطاء القضائية، والتوصل بدرجة كبيرة نحو الحقيقة¹.

فالمسمات التي يتمتع بها الدليل الرقمي تدفع إلى الاعتقاد بأنه بمقدار اتساع مساحة الأدلة العلمية ومن بينها الدليل الرقمي بمقدار ما يكون تضاؤل دور القاضي الجنائي في التقدير، خاصة أمام نقص الثقافة الفنية للقاضي، حيث يصبح الدور الكبير للخبير الذي يسيطر على العملية الإثباتية، وهذا الأمر لا يثير أي مشكل خاصة إذا قلنا بأن نظام الإثبات السائد يقوم على التوازن بين الإثبات العلمي والاقتناع القضائي، حيث يتم العمل بالإثبات العلمي في إطار مبدأ الاقتناع القضائي².

المطلب الثاني: أثر الطبيعة العلمية للدليل الرقمي على الاقتناع الشخصي للقاضي

بالنسبة لمسألة اقتناع القاضي فقد كرسها المشرع الجزائري من خلال نص المادة 307 من قانون الإجراءات الجزائية³، والفقهاء قد اختلفوا في تحديد مدلولها، إلا أنها تتفق على أنها تعني بأن القاضي بإمكانه أن يستحضر عقيدته ضد أي دليل يراه مناسبا ويطمئن إليه، وهذه الأدلة قد تكون من طرف الخصوم أو النيابة العامة أو من القاضي بنفسه، والتي عن طريقها تتكون قناعة هذا القاضي، وما تجدر الإشارة إليه أن هذه الحرية الممنوحة للقاضي الجنائي ليست بهدف توسيع سلطته، وإنما

¹ شهرزاد حداد، الدليل الإلكتروني في مجال الإثبات الجنائي، مذكرة مكتملة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي للأعمال، كلية الحقوق، جامعة العربي بن مهيدي أم البواقي، 2016/2017، ص 84.

¹ عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، مصر، بدون طبعة، 2010، ص 246.

³ المادة 307 من الأمر رقم 66-155، المرجع السابق، والتي جاء في فحواها: " يتلو الرئيس قبل مغادرة المحكمة قاعة الجلسة التعليمات الآتية التي تعلق فضلا عن ذلك بحروف كبيرة في أظهر مكان من غرفة المداولة، إن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم، ولا يرسم لهم قواعد بما يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت وتدبر، وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم و أوجه الدفاع عنها ولم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم: هل لديكم اقتناع شخصي؟ "

لصعوبة الحصول على الدليل في المواد الجزائية خاصة فيما يتعلق بالأدلة العلمية ومنها الدليل الإلكتروني¹.

إن الدليل الرقمي يخضع بطبيعة الحال إلى تقدير القاضي الجنائي وإلى اقتناعه، ومنه فإن الدليل الرقمي قائم على أمرين مهمين وهما القيمة العلمية التي تيمت عبها كما سبق توضيحها، والأمر الثاني هو الظروف والملابسات التي وجد فيها هذا الدليل، فتقدير القاضي لا ينصب على الأمر الأول لأن قيمة الدليل تقوم على أسس علمية دقيقة وبالتالي ليس للقاضي الحرية في مناقشة الحقائق العلمية الثابتة، أما الظروف والملابسات التي وجد فيها الدليل فإنها تدخل في نطاق تقديره الذاتي وهي من صميم وظيفته القضائية، بحيث يكون في مقدوره أن يطرح مثل هذا الدليل رغم قطعيته إذا تبين له بأنه لا يتفق مع ظروف الواقعة وملابساتها، حيث تولد الشبهة لدى القاضي ومن ثم يقضي في إطار تفسير الشك لصالح المتهم².

فليس القاضي ملزم بالحكم بموجب الدليل الرقمي مباشرة بمجرد توافره سواء بالإدانة أو البراءة دون البحث في ظروف وملابسات الدليل، فالدليل الرقمي ليس آلة معدة لتقرير اقتناع القاضي بخصوص مسألة غير مؤكدة، بل إنه مهما على شأن الأدلة العلمية والرقمية في مسألة الإثبات الجنائي تبقى السلطة التقديرية للقاضي في تكوين اقتناعه من هذه الأدلة وذلك من أجل ضمان سلامة الأدلة من أي شيء قد يمتنع من الوصول إلى الحقيقة، فسلطته التقديرية تحول له القدرة على تفسير الشك لصالح المتهم مع استبعاد الأدلة التي تم الحصول عليها بطريقة غير مشروعة³.

الخلاصة:

لقد صار من الواضح اليوم أن هناك ارتباط وثيق بين تطور تكنولوجيا المعلومات وطرق ارتكاب الجريمة المعلوماتية وإثباتها، ولكن مع الأسف فأغلب التشريعات والقوانين لم تنص على الدليل الرقمي ومن ضمنهم المشرع الجزائري، علما أن الدليل الرقمي يعتبر المساعد الأول في سبيل مكافحة الجريمة المعلوماتية لأن محل العمل به يكون في هذا النوع من الجرائم، ومن النتائج كذلك المتوصل إليها أن

¹ أشرف عبد القادر قنديل، المرجع السابق، ص 221.

² فتحي محمد أنور عزة، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، دار الفكر القانوني للنشر والتوزيع، مصر، الطبعة الأولى، 2010، ص 596.

³ نعيم سعيداني، المرجع السابق، ص 222.

طبيعة الجريمة المعلوماتية تتطلب أساليب غير تقليدية في التحقيق لاكتشاف الدليل الرقمي، وذلك يستدعي إجراءات سريعة في هذا المجال لأن الدليل الرقمي غير مادي ويمكن التخلص منه من قبل مرتكبي هذه الجرائم، فالإثبات في الجريمة المعلوماتية يعد من أهم التحديات التي تواجه الجهات الأمنية ويستلزم الكثير من الجهد والخبرة الفنية.

على ضوء هذه النتائج المتوصل إليها يمكن وضع جملة من التوصيات والتي يمكن تعدادها فيما يلي:

- سد الفراغ التشريعي في مجال الجريمة المعلوماتية ولاسيما فيما يتعلق بطرق إثباتها، على أن يكون هناك تعديل قانوني شاملا للقواعد الموضوعية والإجرائية، مستمدين هذا التعديل من المجتمع المحلي وعدم استيراده جاهزة حرصا على فعاليته.
- إنشاء قاعدة بيانات لجرائم المعلومات من حيث أساليبها وأنواعها وطرق إثباتها للرجوع إليها عند الحاجة.
- ضرورة العمل على التنسيق الدائم والمستمر بين الجهات الأمنية والقضائية من جهة والجهات ذات العلاقة بالتكنولوجيا من جهة أخرى للإطلاع ومسايرة ما يستجد وتكوين ثقافة معلوماتية للقضاة ورجال الأمن في هذا المجال.
- خلق جهاز خاص داخل الشرطة متخصص بالبحث والتحري عن هذا النوع من الجرائم.
- ضرورة التعاون الدولي في مجال الجريمة المعلوماتية وجمع الأدلة الرقمية، وذلك بوضع تشريع دولي خاص بمكافحة هذه الجريمة باعتبارها من الجرائم العابرة للحدود.

قائمة المراجع:

1 / النصوص القانونية:

- الأمر رقم 66-155 المؤرخ في 18 صفر 1386 الموافق ل 8 جوان 1966، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم، ج ر العدد 47 المؤرخة في 9 جوان 1966.
- القانون رقم 09-04، المؤرخ في 14 شعبان 1430 الموافق ل 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر العدد 47، الصادرة في 16 أوت 2009.

2/ الكتب:

- أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الالكترونية، دار الجامعة العربية، مصر، بدون طبعة، 2015.
- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان، الطبعة الأولى، 2011.
- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، لبنان، الطبعة الأولى، 2012.
- سامي جلال حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، دار الكتب القانونية، مصر، بدون طبعة، 2011.
- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، مصر، بدون طبعة، 2010.
- فتحي محمد أنور عزة، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، دار الفكر القانوني للنشر والتوزيع، مصر، الطبعة الأولى، 2010.

3/ المقالات:

- هنية عميروش، أثر الدليل العلمي على اقتناع القاضي الجزائري، المجلة الأكاديمية للبحث القانوني، المجلد 16، العدد 02، 2017.

4/ الرسائل الجامعية:

الأطروحات:

- بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم تخصص قانون عام، كلية الحقوق، جامعة الجزائر 01 بن يوسف بن خدة، 2018/2017.
- بن فردية محمد، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة دكتوراه علوم تخصص قانون عام، كلية الحقوق، جامعة الجزائر 01 بن يوسف بن خدة، 2015.

المذكرات:

- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، كلية الحقوق، جامعة باتنة، 2013.

- شهرزاد حداد، الدليل الإلكتروني في مجال الإثبات الجنائي، مذكرة مكملة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي للأعمال، كلية الحقوق، جامعة العربي بن مهيدي أم البواقي، 2017/2016.

- لبيض عادل و نزلي بشرى، إثبات الجريمة الإلكترونية، مذكرة مقدمة لاستكمال متطلبات شهادة الماستر، تخصص قانون جنائي، كلية الحقوق، جامعة قاصدي مرباح ورقلة، 2018/2017.

مدى اقتناع الشخصي القاضي الجزائري بالأدلة الجنائية الحديثة

د/ حمادي محمد رضا

كلية الحقوق والعلوم السياسية

جامعة أدرار

ط.د/ قنقارة سليمان

كلية الحقوق والعلوم السياسية

جامعة بشار

مقدمة:

تهدف التشريعات الإجرائية إلى أن يصيب القاضي في حكمه سواء بالإدانة أو البراءة، و الحقيقة القضائية لا تكتشف فوراً أو بسهولة و إنما هي ثمرة البحث الذي تمارسه الجهات المختصة منذ وقوع الجريمة وذلك عن طريق إقامة الدليل على وقوعها، ومع التطور التكنولوجي الذي يشهده العالم والذي انعكست آثاره على جميع مجالات الحياة ومنها الميدان الجنائي حيث استفاد المجرمين من التقنيات المتطورة في ارتكاب الجرائم لهذا كان من الضروري إيجاد وسائل حديثة جديدة تساعد في الكشف عن الجرائم الذي بات يخطط قبل ارتكابه للجريمة في أنه لا يترك آثار مادية تدل عليه لذلك سعت أجهزة البحث و التحقيق في الاستعانة بالوسائل العلمية في إثبات الجريمة على المجرم. والدليل له تأثير على القاضي باعتبار أن هناك تلازم لا يمكن إغفاله بين القاضي والأدلة في خضم عملية الإثبات فالأدلة هي وسائل إظهار الحقيقة وهنا يطرح الإشكال: ما مدى تأثير أدلة الإثبات الجنائية الحديثة على الاقتناع الشخصي للقاضي الجزائري؟.

و للإجابة على هذه الإشكالية اقترحنا الخطة في مبحثين حيث تناولنا في المبحث الأول مبدأ اقتناع القاضي الجزائري، والمبحث الثاني تطرقنا فيه إلى القوة الإقناعية للدليل الحديث.

المبحث الأول: مبدأ اقتناع القاضي

إن الهدف الأسمى الذي يسعى إليه القضاء بصفة عامة و القاضي بصفة خاصة هو أن يصيب في حكمه سواء كان بإدانة المتهم أو براءته حيث يعد الحكم بناء على اقتناع القاضي، والذي يعتبر من أهم الآثار المترتبة على القاعدة العامة للإثبات في القانون الجنائي، ومؤداه أن القاضي في المواد الجنائية يبني حكمه على اقتناعه الشخصي في ترجيحه للأدلة المعروضة أمامه حيث يتمتع بكامل الحرية في تقديرها دون أن يخضع لرقابة المحكمة العليا مادام الدليل الذي استند إليه القاضي سائعا

ومتفقا مع الأدلة المقدمة في الدعوى فهو يباشر سلطته ضمن ضوابط ومعايير يقاس من خلاله مدى سلامة تقديره.

المطلب الأول: تعريف مبدأ الاقتناع الشخصي للقاضي الجزائري

الفرع الأول: التعريف الفقهي

تعددت الآراء حول تعريف الاقتناع الشخصي للقاضي الجزائري ومنها:
عرف الفقيه ليوني جيوفاني: " بأن الاقتناع الحر للقاضي لا معنى له أكثر من أنه سلطة القاضي وواجبه في أن يستمد من أي مصدر وسيلة إثبات الوقائع و أن يقدرها دون أن يقيده في ذلك أحدا أو قيда ما ".¹ وعرفه محمود مصطفى بأنه "التقدير الحر المسبب لعناصر الإثبات في الدعوى وهو البديل عن نظام الأدلة القانونية".²

كما عرفه كمال جوهرى أنه: "حالة ذهنية جوهرية، وهي محصلة عملية علمية منطقية تستريها وقائع القضية الجنائية " في نفس القاضي فتتنشط ذاكرته لتستدعي " القواعد القانونية " ذات الوقائع النموذجية المرشحة للتطابق مع وقائع القضية و توقف طبيعة هذه الحالة نتيجة عملية المطابقة بين الواقعتين، فقد تكون ارتياح ضمير القاضي و إذعانه أو تسليمه بدون أدنى شك بثبوت الوقائع من جانب المتهم وثبوت مسؤوليته عنها وقد تكون الشك في ذلك وأخيرا قد تكون ارتياح ضميره و إذعانه وتسلمه بعد حدوثها أو عدم مسؤولية المتهم عنها مطلقا".³

الفرع الثاني: التعريف القضائي

أولاً: حسب اجتهاد القضاء المقارن: من خلال قرار محكمة النقض المصرية الصادر بتاريخ 1980/05/08 و الذي جاء فيه أن القاضي الجزائري كامل الحرية في أن يستمد اقتناعه من أي دليل يطمئن إليه من الأدلة التي تقدم له في الدعوى، بالإضافة إلى هذا فإن القضاء الفرنسي أخذ بمبدأ الاقتناع الشخصي للقاضي الجزائري و يستشف ذلك من عدة قرارات محكمة النقض الفرنسية

¹ ليوني جيوفاني، مبدأ الاقتناع و المشاكل المرتبطة به، مجلة القانون و الاقتصاد، ترجمة لرئيس بنهام، سنة 1994، ص 923.

² محمود محمود مصطفى، الإثبات في المواد الجنائية في القانون المقارن، الجزء الأول، مطبعة جامعة القاهرة و الكتاب الجامعي، القاهرة، سنة 1977، ص 03.

³ الجوهري كمال عبد الواحد، تأسيس اقتناع القاضي و المحاكم الجنائية العادلة، دار محمود للنشر والتوزيع، القاهرة، سنة 1999، ص 14.

بأن قاضي الموضوع له الحرية في تقدير أدلة الإثبات التي تتم مناقشتها وتحديد قيمة كل دليل، كما أضافت أن تقرير الخبرة يخضع كباقي أدلة الإثبات الأخرى للسلطة التقديرية لقاضي الموضوع¹.
ثانيا: **حسب الاجتهاد القضائي الجزائري:** و يتمثل في قرارات المحكمة أين جاء في قرارها: " لقضاة الموضوع السلطة المطلقة في تقدير أدلة الإثبات بدون معقب مادام ما استندوا إليه له أصل ثابت في أوراق الدعوى "².

- ومن خلال هذه التعريفات فإن الاقتناع الشخصي للقاضي الجزائري يتميز بخاصيتين³:
 - أنه حالة ذهنية غير ملموسة تكمن في أعماق القاضي لأنه من تقييم ضميره الذي يخضع بدوره لمؤثرات مختلفة وقد يخطأ في تقديره للأمور ومن ثم لا يمكنه الوصول إلى اليقين القاطع في جميع الأحوال.
 - أنه يقوم على الاحتمال وهذا الاحتمال يقوم على درجة كبيرة من اليقين و التأكد وهي مرحلة سابقة لصدور الحكم الجزائري.

المطلب الثاني: نطاق تطبيق قاعدة الاقتناع الشخصي للقاضي

إن نطاق تطبيق مبدأ الاقتناع الشخصي للقاضي الجزائري يشمل مجالين في إطار القانون الجزائري، فهو يشمل كافة أنواع المحاكم الجزائية من جهة و شمولية تطبيق مبدأ في كافة مراحل الدعوى من جهة أخرى.

فقد استقر الفقه و القضاء على أن مبدأ الاقتناع الشخصي يطبق أمام جميع أنواع القضاء الجنائي من محاكم الجنايات ودون تمييز بين القضاة والمحلفين حيث لم يفرق المشرع الجزائري بينهما في محكمة الجنايات فقد نصت المادتين 284 من قانون الإجراءات الجزائية بأن يقسم المحلفين بأن يصدروا قراراتهم طبقا لضمائرهم واقتناعهم الشخصي.

¹ عمورة محمد، سلطة القاضي الجزائري في تقدير أدلة الإثبات الجزائية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق و العلوم السياسية جامعة أبو بكر بلقايد تلمسان، السنة الجامعية 2009-2010، ص 39.

² المحكمة العليا، قرار صادر يوم 1982/01/05، الغرفة الجنائية الأولى، طعن رقم 25814، مشار إليه لدى:

جيلالي بغدادي، الاجتهاد القضائي في المواد الجزائية، الجزء الأول، الطبعة الأولى، سنة 2002، ص 16.

³ مروت نصر الدين، محاضرات في الإثبات الجزائي، النظرية العامة للإثبات الجنائي، الجزء الأول، دار هومة للطباعة والنشر والتوزيع، الجزائر، ص 622.

و المادة 307 من قانون الإجراءات الجزائية في فقرتها الأخيرة، هل لديكم اقتناع شخصي ؟؟ أمام محكمة الجناح و المخالفات فتطبيق أحكام المادة 212 من ق.إ.ج الجزائري "...على القاضي أن يصدر حكمه تبعا لاقتناعه الخاص " أي أن المشرع الجزائري تبنى شمولية مبدأ الاقتناع الشخصي أمام كل جهات قضاة الحكم وما يمكن التنبيه إليه أن قاعدة الاقتناع الشخصي أمام كل جهات قضاة الحكم وهذا ما يظهر بوضوح من خلال نص المادة 307 من ق.إ.ج الجزائري¹.

المطلب الثالث: مبررات مبدأ الاقتناع الشخصي للقاضي الجزائري

إن الهدف من مبدأ الاقتناع الشخصي للقاضي الجزائري هو الوصول إلى الحقيقة و الواقع الإجرامي باستعماله جميع وسائل الإثبات التي تؤدي إلى تكوين اقتناعه و بالتالي هو ملزم بأن يؤسس حكمه بالإدانة على الجزم و اليقين دون الاعتماد على الشك، لكن يثور الإشكال حول السبب و الباعث الذي دفع بالمشرع الجزائري أن يقتصر حكم الإدانة على الجزم و اليقين دون حكم البراءة مما أدى إلى فقدان الثقة في مدى نجاعته كمبدأ من مبادئ الإثبات. و يرجع الأصل في إرساء هذه القاعدة إلى مبررات ألزمت تقرير الاحتكام للضمير الحي للقاضي و نوجزها في:

أولاً: صعوبة الإثبات في المواد الجزائية

ذلك أن الجريمة و طرق و أساليب ارتكابها تطورت بصورة مروعة ذلك أن المجرم لم يعد الشخص الهمجي البدائي الذي يقوم بارتكاب الجريمة دون احتراس، بل بالعكس إنه يحاول المجرم جاهدا طمس معالم الجريمة و الأدلة التي تقود إلى كشفها خاصة مع تطور الأساليب الإجرامية، ورغم كل ما تقوم به مصالح الشرطة من مجهودات و ما تستعين به من وسائل تقنية و تكنولوجية، وعلمية و بيولوجية لاكتشاف الجريمة².

بالإضافة إلى أن الإثبات في المواد الجنائية يختلف عن غيره من قواعد الإثبات فعلى سبيل المثال فالإثبات في القانون المدني ينصب على أعمال قانونية على عكس القانون الجزائي الذي ينصب الإثبات فيه على واقعة مادية وهذا الأمر الذي يستدعي طرق الإثبات في القانون الجنائي، الذي هو أوسع بكثير مما هي عليه في القانون المدني التي تكون علة سبيل الحصر.

¹ مارك نصر الدين، مرجع سابق، ص 635.

² مارك نصر الدين، مرجع سابق، ص 625.

ثانيا: طبيعة المصالح التي يحميها القانون الجزائي

على العكس مما هو عليه الحال في القانون المدني الذي يقوم بحماية مصالح خاصة وذات طابع مالي، فإن القانون الجنائي يقوم بحماية كيان المجتمع و المصالح الأساسية لأفراده من أي اعتداء عليها ولذلك فهو يضع النص التجريمي لتحذير الأفراد من الإقدام على الجريمة و يقرر جزاءا على ذلك و هي أهداف يستحيل أن تحقق إذا كان القاضي مقيدا باستعمال نوع أو عدد معين من أدلة الإثبات أو في تقديرها، بل إنها تستلزم أن يخول القضاة إثبات الجريمة و الخطورة الإجرامية بكل الوسائل كي يتوجهوا إليها بالعقوبة أو التدبير اللازم حسبما تقتضيه المصلحة الاجتماعية¹.

كما أن وجود قرينة البراءة كحماية للمتهم ومقتضيات مصلحة المجتمع في مكافحة الجريمة وكشف حقيقتها تستلزم قبول جميع أدلة الإثبات ومنح سلطة للقاضي في تقديرها و ذلك تحقيقا للتوازن بين مصلحة المجتمع و مصلحة المتهم².

كما يمكن أن نضيف إلى هذا تطور الوسائل العلمية الحديثة في الإثبات فإذا كان العلم قد أحدث العديد من أساليب الإثبات و أمد سلطات التحقيق بوسائل علمية حديثة و متطورة، فإن إخضاع هذه الوسائل العلمية الحديثة و المتطورة إلى اقتناع القاضي يعد كضمان لما قد يرافق هذه الوسائل من أخطاء تترتب عليها أضرار كبيرة في حالة التسليم بها دون تقدير قيمتها الفعلية، بالإضافة إلى ما تنطوي عليه من اعتداء على الحريات الشخصية³، كما أن هذه الأدلة لا تقبل بطبيعتها إخضاع القاضي لأي قيود بشأنها بل ينبغي أن يترك الأمر في تقديرها لمحض سلطة القاضي⁴، فمهما تقدمت طرق جمع الأدلة ومهما علت قيمتها العلمية أو الفنية في الإثبات فإنها تحتاج إلى قاض يتمتع بسلطة

¹ مارك نصر الدين، مرجع سابق، ص 625.

² زبدة مسعود، الاقتناع الشخصي للقاضي الجزائي، مذكرة مقدمة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق والعلوم السياسية جامعة الجزائر، سنة 1983/1984، ص 42، 43.

³ فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة - دراسة مقارنة -، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، سنة 2006، ص 101.

⁴ صالح يحيى رزق ناجي، سلطة القاضي في تقدير أدلة الإثبات الجنائية الحديثة، دراسة مقارنة، منتدى مكتب السوري للمحاماة و الاستشارات القانونية www.syrianlanlaw.org/vb/showthread.php?t=781

تقديرية لان هذه السلطة التقديرية تكون لازمة لتفقيّة هذه الأدلة من الغلط أو الخطأ أو الغش، وهي تكون ضرورية أيضا لتجعل الحقيقة العلمية حقيقة قضائية¹.

ثالثا: الدور الإيجابي للقاضي الجزائي

إذا كان دور القاضي المدني هو دور حيادي أي لا يتدخل في الخصومة، أي ينظر إلى مدى توافر الأدلة التي يتطلبها القانون في الواقعة المعروضة عليه وبناء على ذلك يصدر حكمه فيها، أي له دور سلبي، فإنه على العكس من ذلك فإن القاضي الجنائي له دور إيجابي في الخصومة². و تكمن مظاهر هذا الدور الإيجابي في البحث عن الحقيقة وكشفها من خلال المرحلتين الأساسيتين للدعوى، وهما مرحلة التحقيق الابتدائي ومرحلة المحاكمة بحيث أنه في مرحلة التحقيق الابتدائي يتم جمع الأدلة وتمحيصها لتحديد مدى كفايتها لإحالة المتهم على المحكمة المختصة أما في مرحلة المحاكمة فإن القاضي يقوم بمناقشة الأدلة المعروضة في القضية حيث يقوم بتوجيه الأسئلة لمن يشاء، كما له وفي إطار استظهار الحقيقة أن يأمر بالقيام بأي إجراء من شأنه أن يمكنه للوصول إلى غايته ولا معقب عليه في ذلك³.

ويورد البعض أن من عناصر الوظيفة القضائية عنصر يسمى تمتع القاضي الجزائي بالسلطة التقديرية، إذ بدون هذه السلطة يتحول القاضي إلى آلة توضع فيها الوقائع من جهة فتخرج من الجهة الأخرى مغلفة بنص قانوني ينطبق عليها تمام الانطباق، فتقدير الأدلة هي مسألة تتعلق بمجوهرة العدالة وهي في أساسها وإن قامت على قواعد العقل والمنطق إلا أنها تبقى ذات حس إنساني لا يمكن تصوره في أية آلة مهما دقت تقنياتها⁴.

المبحث الثاني: القوة الإقناعية للوسائل الحديثة

لا ريب في أن استخدام الأساليب الحديثة للحصول على دليل يحمل بين طياته نوعا من الوسائل التي تشكل اعتداء على الحياة الخاصة ونوعا آخر من الوسائل التي تشكل انتهاكا و اعتداء على

¹ حسين بن سعيد الغافري، سلطة القاضي الجنائي في قبول الأدلة المستخرجة من الإنترنت، منتديات القانون

العماي [http:// www.omanlrgal.net /vb/showthread.php ?t=56](http://www.omanlrgal.net/vb/showthread.php?t=56)

² مراد بلوهي، الحدود القانونية لسلطة القاضي الجزائي في تقدير الأدلة، مذكرة مقدمة لنيل شهادة الماجستير تخصص علوم جنائية، كلية الحقوق و العلوم السياسية جامعة الحاج لخضر باتنة، سنة 2010/2011، ص 27.

³ مراد بلوهي، مرجع سابق، ص 27.

⁴ مرجع نفسه، ص 27-28.

سلامة الفرد الجسدية وفي الحقيقة أن معيار قبول أية وسيلة علمية مستمدة في مجال الإثبات الجنائي لإظهار الحقيقة يركز أساسا على عدم إهدارها لحرية الفرد أو كرامته الإنسانية، الأمر الذي قد يزيد من القاضي الجنائي لكي يوازن بين ما هو مشروع وما هو غير مشروع¹.

المطلب الأول: رقابة القاضي الجنائي في قبول الدليل المستمد من الوسائل الحديثة

لا يكون الدليل الجنائي مقبولا في عملية الإثبات إلا إذا جرت عملية البحث عنه أو الحصول عليه في إطار المشروعية، وفي الحدود التي رسمها القانون بطريقة تكفل تحقيق التوازن بين حق الدولة في العقاب، وحق المتهم في أن لا تشمل طريقة الحصول على هذه الأدلة أي اعتداءات على حضانة جسم الفرد أو على حرته، إلا بالقدر الضروري وفي الحدود التي رسمها القانون².

وبما أن الإثبات الجنائي يعتمد على الوسائل العلمية الحديثة فإنه يجب الاعتماد على النظم و الشكل القانوني في تلك الوسائل وهذا لا يتم إلا إذا تم البحث عن هذه الأدلة في إطار إجراءات اتسمت بالشرعية دون انتهاك حقوق الأفراد التي أقرها القانون لهم³.

الفرع الأول: مشروعية تحصيل الدليل

أولا: ماهية مشروعية تحصيل الدليل

يعتبر مبدأ الشرعية الجنائية أو ما يعرف بمبدأ احترام القانون من الأصول الدستورية الكبرى في نظام الدول الديمقراطية وهو يعني التزام الحاكم والمحكوم بالقواعد القانونية التي تصدرها السلطة المختصة، وهذا المبدأ يميز بين دولة القانون عند الدولة البوليسية أو الدكتاتورية، ونعتبر الشرعية الجنائية فرع من ذلك الأصل العام ومفادها أن لا جريمة ولا عقوبة إلا بنص، إذ لا يمكن توجيه اتهام لشخص ما لارتكابه فعلا معينا ما لم يكن منصوص على تجريم هذا الفعل في القانون، كذلك لا يمكن توقيع العقوبة ما لم تكن محددة من قبل⁴.

و بالرغم من أن هذه القاعدة تمثل إحدى الركائز الأساسية التي تقوم عليها كل التشريعات الجنائية إلا أنها لا تكفي وحدها لحماية حرية الإنسان، وفي حالة القبض عليه أو حبسه أو اتخاذ الإجراءات

¹ بن بلاغة عقيلة، حجية أدلة الإثبات الجنائية الحديثة، مذكرة مقدمة لنيل شهادة الماجستير فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق جامعة الجزائر 1، السنة الجامعية 2011/2012، ص 115.

² فاضل محمد زيدان، مرجع سابق، ص 242.

³ بن بلاغة عقيلة، مرجع سابق، ص 43.

⁴ مارك نصر الدين، مرجع سابق، ص 519.

اللازمة لمحاكمته، لذلك كان من الضروري تدعيم هذه القاعدة الدستورية بقاعدة ثانية تحكم تنظيم الإجراءات التي تتخذ ضد المتهم بطريقة يضمن بها احترام الحقوق و الحريات الفردية، وهذه القاعدة سميت بالشرعية الإجرائية أو قاعدة مشروعية الدليل وهي تعني كـ "ضرورة اتفاق الإجراء مع القواعد القانونية و الأنظمة الثابتة في وجدان المجتمع المتحضر"¹.

وبما أن قاعدة مشروعية الدليل الجنائي تعني ضرورة اتفاق الإجراء مع القواعد القانونية نجد أن المشرع الجزائري نص على هذه في المادة 59 من الدستور بقوله: "لا يتابع أحد، ولا يوقف أو يحتجز إلا في الحالات المحددة بالقانون و طبقاً للأشكال التي نص عليها"، و ترتيباً على ما تقدم فإن قاعدة مشروعية الدليل الجنائي تغاير قاعدة الشرعية الجنائية، ولكن تظل هذه الأخيرة هي الأصل الذي تتفرع منه كل القواعد.

ثانياً: قيمة الدليل غير مشروع في الإثبات

لقد أثار هذا التساؤل جدلاً فقهيًا كبير انقسم على إثره على ثلاث اتجاهات²:

الاتجاه الأول: تزعمته محكمة النقض المصرية و جانب من الفقه إذ يرون أن الأصل في الإنسان البراءة و لا تحتاج المحكمة لإثباتها بل كل ما تحتاجه هو التشكيك في الإدانة، بالإضافة إلى أن بطلان دليل الإدانة الناتج عن إجراء غير مشروع وضع كضمان لحرية المتهم و بالتالي لا يمكن قلب أثره عليه.

الاتجاه الثاني: تزعمه جانب من الفقه، ينتقد الرأي الأول و حجته في ذلك أنه مخالف لمبدأ شرعية الدليل، إضافة إلى أنه لا يحق للقضاء أن يقرر قاعدة الغاية تبرر الوسيلة كمبدأ قانوني صحيح، وإذا اعتمدنا على هذا القول فإنه يحدث إثبات البراءة بكل الوسائل و يصبح التزوير، وشهادة الزور كلها أمور مشروعة لإثبات البراءة وهذا كلام يرفضه كل عاقل.

الاتجاه الثالث: هو اتجاه توفيقى، إذ يؤيد رأي محكمة النقض المصرية لكن في حدود معينة، إذ أنه فرق بين ما إذا كانت وسيلة الحصول على الدليل تعد في حد ذاتها جريمة جنائية فإنه لا يمكن الاعتداد به، لأن القول بغير هذا يعني الدعوة لارتكاب بعض الجرائم و إخراجها من دائرة العقاب، وهذا لا يجوز أما إذا كانت وسيلة الحصول على الدليل مجرد مخالفة لقواعد الإجراءات، هنا

¹ بن بلاغة عقيلة، مرجع سابق، ص 44.

² مروك نصر الدين، مرجع سابق، ص 522، 525 .

يمكن الاستناد إلى هذا الدليل لأن الغاية من تقرير البطلان ترجع إلى من قام بالإجراء الباطل و منه لا يصح أن يضار المتهم بذلك.

الفرع الثاني: التزام القاضي بحماية الحقوق الشخصية

لكي يكون الدليل محل التقدير سليماً قانونياً، و مقبولاً أن يكون مستمد من إجراءات مشروعة باعتبار أن شرعية الإثبات الجنائي تستلزم عدم قبول أي دليل كان البحث عنه أو الحصول عليه قد تم بطرق غير مشروعة، كما يجب أن يراعي في الدليل عدم انتهاك الحقوق للأفراد وضماناتهم التي أقرها لهم ومن أهم هذه الضمانات مراعاة حقوق الدفاع ومقتضيات الحفاظ على الكرامة الإنسانية¹.

فتكمن مهمة القاضي هنا التأكد من أن لا يكون استخدام الوسائل العلمية الحديثة يمثل أي اعتداء على الحريات الفردية كما يجب على القاضي التأكد من توفير بعض الشروط التي يجب أن يتميز بها الأساليب الفنية الحديثة وهذا ما سنحاول توضيحه².

أولاً: مبدأ احترام حقوق الدفاع

إن الاعتماد على الوسائل العلمية الحديثة عادة ما يصطدم بعقبة أساسية هي الضمانات المقررة للمتهم، حيث أنه و من المبادئ المسلم بها عدم المساس بحرية الأفراد إلا في الأحوال التي يحددها القانون، لذلك وجب التوازن بين الحق في الحصول على الدليل ومعرفة الحقيقة و بين حقوق الأفراد واحترام كرامتهم الإنسانية واعتبارات العدالة³.

ولا شك أن حق الدفاع من أهم الحقوق الأساسية للإنسان، وهو وثيق الصلة بالخصومة القضائية إذ يعتبر أحد مفترضات المحاكمة المؤسسة على إجراءات مشروعة، وغياب هذا الحق يؤدي بطبيعة الحال إلى تزييف الحقائق، الأمر الذي سيضلل القضاء ويوجب عنه الثقة⁴.

ثانياً: مبدأ الكرامة البشرية⁵

¹ فاضل محمد زيدان، مرجع سابق، ص 244، 245.

² بن بلاغة عقيلة، مرجع سابق، ص 54.

³ مرجع نفسه، ص 58.

⁴ شهيرة بولحية، حق المتهم في الدفاع أمام القضاء الجنائي، مجلة المنتدى القانوني، كلية الحقوق، جامعة محمد خيضر بسكرة، العدد الخامس، ص 90، 91.

⁵ بن بلاغة عقيلة، مرجع سابق، ص 55.

تتمثل مهمة القاضي في قبول الدليل في البحث عن نوع المساس الذي يمكن يحدثه استخدام الأساليب الفنية الحديثة على حقوق المتهم الأساسية حتى يحول ذلك دون الاعتداء على الكرامة الإنسانية و حقوق الدفاع.

فالتطور العلمي في مجال الكشف عن الجريمة الكثير من الوسائل الحديثة التي تهدف إلى إمكانية فحص المتهم بعد ارتكاب الحادث بحثا عن الحقيقة، مما قد يؤدي بالمساس و الاعتداء على حقوق المتهم، لأنه يهدف إلى حماية الأفراد من تعسف السلطة.

وإذا كانت هذه الأخيرة تملك وسائل عديدة تساعده في الكشف عن الحقيقة وتمكنها من الوقوف على المعطيات الصحيحة لوقائع النزاع إلا أن ذلك يجب أن يبقى محدودا ولا يمكن أن يكون ذلك على حساب حقوق الإنسان، هذه الحقوق التي تكفلها الدساتير المختلفة، وبما أنه في بعض الأحيان قد تقتضي الضرورة إجراء كشوف طبية، وتحليل عينة من دم المتهم وفي ذلك مساس واضح بسلامة الجسد، فإن جانب من الفقه يرى أن القاعدة العامة هي عدم إخضاع المريض للتجارب دون رضاه، إلا أن هذه القاعدة ليست مطلقة، فالصالح العام قد يدفع المشرع لإخضاع الأفراد لتدابير معينة فيها مساس بكيانهم ورغم هذا الاعتداء إلا أن الغاية هي الكشف عن الحقيقة.

ومن هنا ينشأ التعارض بين المصالح و الحقوق، وفي هذه الحالة يجب على السياسة الشرعية التوفيق بين هذين الاعتبارين المتعارضين.

ولذلك يمكن لنا القول بأن استخدام هذه الوسائل الحديثة قد جعل القاضي في موقع التقويم، فعليه أن يقبل من هذه الوسائل ما يراه إنسانيا، ويرفض ما قد ينال من الحق في الكرامة الإنسانية.

المطلب الثاني: سلطة القاضي الجنائي في تقدير الدليل الحديث

إن سلطة القاضي في تقدير الأدلة محكومة بمبدأ حرية القاضي الجنائي في الإقناع، وإن هذا المبدأ يؤدي إلى نتيجتين أولهما حرية القاضي في قبول الدليل، وثانيهما أن الدليل يخضع إلى التقدير المطلق للقاضي الجنائي أي أن القاضي يمكن أن يبني اقتناعه الذاتي أو يؤسس حكمه على أي عنصر من عناصر الإثبات¹.

¹ عبد الحكيم فودة، حجية الدليل الفني في المواد الجنائية و المدنية، دار الفكر الجامعي، الإسكندرية، سنة 1996،

ولذلك فإن السعي لتقريب الحقيقة القضائية من الحقيقة الواقعية يجعل القضاة يلجئون إلى الاستعانة بأهل الاختصاص، لفصل النزاعات عندما تعرض عليهم مسائل فهمها خاصة بعد التطور العلمي الذي شهدته البشرية، و ظهور طرق جديدة تعتمد على وسائل فنية حديثة¹.

الفرع الأول: نطاق سلطة القاضي في تقدير الدليل الحديث

بالرغم من الأدلة الجنائية تخضع لمبدأ تكافؤ الأدلة إلا أن سلطة القاضي الجنائي في تقدير الأدلة العلمية الحديثة، لا نقول أنها تقيّد أو تحد من هذه السلطة، إلا أنه يجب على القاضي الجنائي أن يراعي هذه الأدلة باعتبارها مسائل علمية دقيقة، ومراعاة ذلك يكون ضمن مجالين أساسيين:

- القيمة العلمية للدليل

- الظروف و الملابسات التي وجد فيها الدليل

وسلطة القاضي في التقدير تحد إطارها في المجال الثاني دون الأول على اعتبار أنه لا مجال لمناقشة الحقائق العلمية الثابتة، لأنها أمور علمية دقيقة لا اعتراض عليها على عكس الظروف التي وجد بها الدليل فإنها تدخل في نطاق تقديره الذاتي إذ أن هذه من طبيعة عمله².

أولاً: التزام القاضي بالحقائق و الأصول الفنية و العلمية الثابتة

لقد قطع التقدم التقني و العلمي خطوات هائلة في المجال الجنائي لذلك كان من الضروري أن يلجأ القاضي إلى الاستعانة بأهل الخبرة، لفصل النزاعات عندما تعرض عليه مسائل يستعصى عليه فهمها، فمن المنطقي أن ثقافة القاضي مهما كانت واسعة فلا يمكن أن تستوعب جميع المشاكل التي تعرض على القضاة خاصة بعد التطور الذي شهدته البشرية، وظهور وسائل فنية حديثة مما جعل اللجوء إلى الخبرة ضرورية.

1/ مفهوم الخبرة:

أ/ تعريف الخبرة: هي عبارة عن استشارة فنية يستعين بها قاضي التحقيق لتقدير المسائل الفنية التي يحتاج تقديرها إلى معرفة فنية أو إدارية علمية لا تتوفر لدى قاضي التحقيق بحكم تكوينه³.

¹ بن بلاغة عقيلة، مرجع سابق، ص 59.

² بن بلاغة عقيلة، مرجع سابق، ص 60.

³ مرجع نفسه، ص 60.

ولقد نص المشرع الجزائري على الخبرة في المواد من 143 إلى 156 إجراءات جزائية حيث نصت المادة 143 على أنه: "جهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع في أن تأمر بئب خبير إما بناء على طلب النيابة العامة أو من تلقاء نفسها أو من الخصوم"، و إذا رأى قاضي التحقيق أنه لا موجب للاستجابة لطلب الخبرة فعليه أن يصدر في ذلك أمرا مسببا في خلال 30 يوم من تاريخ استلامه الطلب".

ب/ الخبرة تتناول الوقائع المادية الفنية دون القانونية: لا تجوز للقاضي أن يستعين في المسائل القانونية بأهل الخبرة، لأن القاضي يتكفل بالقانون إذ أنه لا يستطيع أن يستعين بخبير للحصول على نص يطبق على النزاع إلا أنه إذا فعل ذلك يكون قد أدخل بواجباته و عرض حكمه للبطلان. ولقد أصبحت الخبرة تحتل مكانا هاما، في العمل القضائي باعتبارها طريقا مهما من طرق إثبات الحقوق في المنازعات التي تنظر أمام القضاء، لاسيما في مواجهة التطور التقني في شتى المجالات مما يؤكد بأن اللجوء إلى الخبرة أمر ضروري خاصة إذا تعلق الأمر بالمسائل الفنية البحتة التي يلتزم القاضي بتعيين خبير لفهم معطيات النزاع¹.

و هو ما نصت عليه المادة 146 من قانون الإجراءات الجزائية الجزائري: "يجب أن تحدد دائما في قرار نئب الخبراء مهمتهم التي لا يجوز أن تهدف إلا إلى فحص مسائل ذات طابع في". ولهذا فإن ما يصل إليه الخبير من إثبات الواقعة يمثل وجهة نظرا فنية محضة و يجب أن تقتصر بوجهة نظر قانونية، لكي تكتسب وجهة نظره قيمة فعلية في مجال الإثبات².

ومن ثم مهمة الخبير، هي المساهمة في تقديم الدليل العلمي الذي يعتبر نتيجة الاختبارات التي يقوم بها الخبير، إذ يقدم التفسير العلمي أو الاستنتاج المنطقي لها، ولهذا اعتبرت مهمة الخبير مكملة للتحقيق الجنائي.

مما يؤكد أن اللجوء إلى الخبرة أصبح أمرا حتميا بشأن المسائل الفنية البحتة باعتبارها تساهم في إنارة طريق القاضي للوصول و الكشف عن الحقيقة و أداء رسالته.

ج/ أداء الخبير لمهمته: يشرع الخبير في أداء مهمته بمجرد تسليمه لأمر تعيينه و الجدير بالذكر أنه يقوم بمهمته تحت مراقبة قاضي التحقيق و هذا ما نصت عليه المادة 143 فقرة 03 من ق.إ.ج.

¹ بن بلاغة عقيلة، مرجع سابق، ص 61.

² فاضل زيدان، محمد، مرجع سابق، ص 317.

ويجب على الخبير أثناء القيام بمهمته أن يبقى على اتصال مع قاضي التحقيق أن يحيطه بكل التطورات التي يقوم بها، ويجوز للخبير وفي إطار مهمته أن يتلقى أقوال الأشخاص غير المتهمين ولكن على سبيل المعلومات، غير أنه يجوز للخبراء الأطباء المكلفين بفحص المتهم أن يوجه إليه الأسئلة اللازمة لأداء مهماته بغير حضور قاضي التحقيق ومحامي المتهم، وقد أجازت المادة 152 من القانون ق.إ.ج للأطراف أن يطلبوا من قاضي التحقيق تكليف الخبير المعين لإجراء أبحاث معينة أو سماع أي شخص معين يمكنه إفادتهم بالمعلومات. وتجدر الإشارة أن رغم يتمتع به قاضي التحقيق من مهام يبقى مجرد مساعد لقاضي التحقيق¹.

2/ الرقابة القانونية للرأي الفني:

إن الاستعانة بالخبير هو أمر متروك لتقدير القاضي، وهو الذي يقدر لزوم هذا الإجراء أو عدم لزومه، ولا معقب عليه في ذلك متى كان رفضه لطلب تعيين الخبير قائما على أسباب مبررة²، إلا أنه تجدر بنا الإشارة إلى أنه لا يمكن للقاضي أن يحل نفسه محل الخبير في مسألة معينة لا يستطيع الوصول فيها إلى نتائج حاسمة باعتبار أن القاضي يفقه المسائل القانونية لكن عمله لا يسع المسائل الفنية و التقنية وهو ما يؤدي بالضرورة إلى ندب أهل الخبرة أما بالنسبة للمسائل الفنية الأخرى التي يمكن للقاضي أن يقوم بتقديرها اعتمادا على تجاربه وخبراته والتي لا تثير تقديرها خلافات فإنه يمكن الفصل فيها دون الاستعانة بالخبير³.

وإذا كان للقاضي التقدير والسلطة الكاملة في رقابة تقدير الخبير و استمداد اقتناعه منه، فإن لهذه السلطة حدود فالقاضي لا يمكنه استعمال هذه السلطة بصورة تعسفية وإنما عليه أن يتحرى مدى جدية متبعا في ذلك أساليب الاستدلال المنطقي التي يقرها العلم⁴.

وعليه واستنادا لمبدأ الإقناع الشخصي للقاضي الجزائي فإن رأي الخبير يخضع لتقدير القاضي الذي له أن يقرر بنفسه الحقيقة التي يقتنع بها، ويزن تقرير الخبرة مع الأدلة الأخرى المتوفرة في الدعوى، ثم

¹ أحسن بوسقيعة، التحقيق القضائي، الطبعة السادسة، دار هومه للنشر والتوزيع، الجزائر، سنة 2006، ص

115 - 116.

² بن بلاغة عقيلة، مرجع سابق، ص 63.

³ بلوحي مراد، مرجع سابق، ص 72.

⁴ بن بلاغة عقيلة، مرجع سابق، ص 64.

يقدر قيمته الثبوتية وهو الأمر الذي أكدته المحكمة العليا حيث قضت: "أن تقدير الخبرة ليس إلا عنصر من عناصر الإقناع يخضع لمناقشة الأطراف ولتقدير قضاة الموضوع"¹.

وفي الأخير يمكن القول أن التزام القاضي برأي الخبير لا ينقص من مبدأ الإقناع القاضي فالقاضي هو الذي انتدب الخبير ووثق فيه وراقب أداء مهمته للتأكد من مدى جديته. فمهمة القاضي الرقابة القانونية للرأي الفني وتطبيقا لذلك فالقاضي له مطلق الحرية في الأخذ برأي الخبير كله أو جزء منه وقد يستبعده كلياً إذا رأى أن في إظهار الحقيقة وسيلة أخرى أو ندب خبير آخر².

ثانياً: تقدير القاضي للظروف و الملابسات التي وجد فيها الدليل³

إن التزام القاضي الجنائي بالحقائق والأصول العلمية لا يسلب منه سلطة الرقابة القانونية على كل عناصر الدعوى.

فإذا كان القاضي الجنائي لا يملك الحرية في مناقشة الحقائق العلمية الثابتة لقيامها على أسس مؤكدة و دقيقة فإنه وفيما يخص طريقة الحصول على الدليل و الظروف التي وجد فيها، فإنه تدخل ضمن الاختصاص الأصيل للقاضي الجنائي و تخضع أيضاً لمبدأ تكافؤ الأدلة، إذ يمكن للقاضي هنا أن يستبعد أي دليل علمي وجد أنه لا يتناسب مع ظروف الواقعة و ملابساتها.

ومن هنا يمكن القول أن الاستعانة بمعطيات التطور العلمي في مجال كشف الجريمة لم ينل من بدأ حرية القاضي في تكوين عقيدته، إذ يبقى للقاضي الحرية في تقدير القوة التدليلية لأدلة الدعوى المعروضة عليه، وأخذ ما هو مناسب و طرح ما لم يقتنع به، حتى لو كان دليل علمي يقوم على مبادئ و أسس دقيقة و يمكن توضيحه في المثال التالي.

ففي جريمة اغتصاب أنثى أثبت الدليل الفني و الطبي أن المجني عليها قد تم فعلاً اغتصابها، إذا وجدت الحيوانات المنوية على السرير و الملابس، كما وجدت آثار داخل جسمها و أعضائها الجنسية، فبالرغم من وجود هذا الدليل القاطع الذي لا يمكن للقاضي أن يرفضه، إلا أن رفضه مستند في ذلك إلى سلطته التقديرية ورقابته القانونية وذلك عندما رأى وجود الدليل لا يتناسب مع ظروف الواقعة و ملابساتها.

¹ بلوحي مراد، مرجع سابق، ص 76.

² بن بلاغة عقيلة، مرجع سابق، ص 64.

³ بن بلاغة عقيلة، مرجع سابق، ص 66 - 67.

إذا يجب على القاضي أولاً: التحقق من عدم رضا المجني عليها، إذ أن العنصر الجوهري في هذه الجريمة هو ارتكابها على خلاف إرادة الأنثى. ثانياً: أن يبحث القاضي عن عدم وجود علاقة سابقة بين المجني عليها والجاني. ثالثاً: بحث سمعة المجني عليها، وهو يتطلب بيان عفتها.

وفي الحقيقة لا يمكن لأحد أن ينكر ما أحدثه العلم من تطور في مجالات الإثبات باعتبار أن الدليل العلمي يمكنه أن يتوصل إلى ما يؤكد وقوع الجريمة كما يؤكد وجود علاقة بينهما وبين المتهم، إلا أنه قد يوجد في الدعوى ما جعل القاضي يقتنع ولو احتمالاً يدعو إلى الشك بأن شخصاً آخر قد ارتكب الجريمة، مما يؤكد ضرورة إعطاء القاضي سلطة تقدير الدليل العلمي، وعدم التسليم بصفة مطلقة و إفساح الحرية للقاضي في تكوين اقتناعه إما بالتيقن من ارتكاب المتهم للجريمة فيحكم بالإدانة أو الاقتناع أو الشك بعدم إسنادها إليه فيحكم ببراءته.

الفرع الثاني: الشروط التي ترد على القاضي في تكوين اقتناعه

أولاً: أن يكون اقتناع القاضي مبني على الجزم واليقين

لكي تكون قناعة القاضي سليمة في تقديرها للأدلة، يجب أن تكون النتيجة التي توصل إليها تتفق مع العقل والمنطق، و تكون مطابقة للنموذج المنصوص عليه في القانون وهو ما يطلق عليه بالحقيقة القضائية، و التي يشترط فيها أن تتفق مع الحقيقة الواقعية¹.

فحرية القاضي الجنائي أن لا يبني حكمه على مجرد الظن و التخمين بل يجب التأكد و بشكل جازم مبني على اليقين بأن المتهم المائل أمامه هو من قام بارتكاب الفعل المجرم، فالحقيقة لا يمكن توافرها إلا باليقين لا مجرد الظن و الاحتمال².

و باعتبار أن هذا الشرط ما هو إلا نتيجة مترتبة و منطقية على قاعدة الأصل في الإنسان البراءة فالأحكام الصادرة بالبراءة يجب أن تبقى إلا على حجج قطعية الثبوت تفيد الجزم و اليقين فإذا ما ثار في نفس القاضي نوع من الشك و جب عليه أن يفسره لمصلحة المتهم. فالدليل اليقيني هو الذي

¹ العربي شحطة عبد القادر، نبيل صقر، الإثبات في المواد الجزائية على ضوء الفقه و الاجتهاد القضائي، دار الهدى لنشر و التوزيع، عين ميلة الجزائر، سنة 2006، ص 34.

² محمد ناجي عبد الحكيم هاشم، الإثبات الجنائي ومدى حرية القاضي في تكوين عقيدته، مجلة المحاماة، دار الطباعة الحديثة، العددان التاسع و العاشر، سنة 1991، ص 146.

يجسد حقيقة الواقعة أمام المحكمة تأكيداً لا يدخلها في حقيقته شك، فتقتنع بحدوث الواقعة كما دل عليها الدليل¹.

ثانياً: أن يفسر الشك لمصلحة المتهم

بالرغم من أن الدليل العلمي قد أحدث تطوراً هائلاً في مجال الإثبات الجنائي مما يجعله مقبولاً أمام المحكمة إلا أنه قد يوجد في الدعوى ما يجعل القاضي يقتنع ولو احتمالاً يدعو إلى الشك بأن شخصاً آخر قد ارتكب الجريمة.

ولذلك فإنه يجب على القاضي أن يقتنع اقتناعاً يقينياً بارتكاب المتهم للتهمة فإذا لم يقتنع وثار لديه نوع من الشك، وجب عليه أن يقض ببراءته تطبيقاً لقاعدة أن الشك يفسر لمصلحة المتهم².

ثالثاً: تسبب الأحكام³

من المقرر أن القاضي الجنائي السيادة التامة في تكوين اقتناعه أي أنه حر في أن يستمد من أي مصدر يطمئن إليه ضميره مادام مطروح على بساط البحث في الجلسة.

فالقاضي لا يكون ملزماً بتسبب اقتناعه و بيان العناصر التي كونت هذا الاقتناع، إذا أنه لا يكفي بإعلانه لاقتناعه بصدق الدليل أو عدم صدقه، و الجدير بالذكر في هذا المقام أن إعفاء القاضي من تسبب اقتناعه، لا يعفيه من تسبب أحكامه فتسبب الاقتناع يتطلب بيان تفاصيل تقدير القاضي للأدلة و تحديد مدى تأثير كل منها على ضميره و تحليل الطريقة التي كون بها اقتناعه، أما تسبب الأحكام فهو إثبات وجود الواقعة الإجرامية.

وهذا ما استقر عليه قضاء المحكمة العليا: "أن قناعة القضاة مشروطة بضرورة تسبب قرارهم دون تناقض مع العناصر الموجودة بملف الدعوى و المناقشات التي دارت حولها أمامهم".

¹ بن بلاغة عقيلة، مرجع سابق، ص 68.

² مروك نصر الدين، مرجع سابق، ص 609.

³ بن بلاغة عقيلة، مرجع سابق، ص 70.

الخاصة:

إن دراسة لموضع تأثير الأدلة الجنائية الحديثة على الاقتناع الشخصي للقاضي الجزائي توصلنا إلى النتائج التالية:

- القاضي يستمد قناعته من أي دليل معروض أمامه دون أن يكون مقيد بتكوين قناعته بدليل معين.
- إن الاستعانة بالوسائل الحديثة لم ينل من مبدأ حرية القاضي في تكوين اقتناعه، ذلك أنه يبقى للقاضي الحرية في تكوين قناعته وتقدير القوة التدليلية لأدلة الدعوى المعروض عليه حتى لو كان دليل علمي يقوم على مبادئ وأسس دقيقة، فالقاضي له أن يرفض الدليل المادي إذا رأى أنه لا يتناسب مع الواقعة المعروضة عليه.
- ضرورة الاستعانة بخبير في المسائل التي لا يستطيع القاضي الوصول فيها إلى نتائج حاسمة، وتجدر الملاحظة إلا أن رأي القاضي يخضع لتقدير القاضي وله أن يقتنع بما أو أن يقرر رأي خبير آخر في هذه الحالة، وهذا ما أكدته المحكمة العليا في العديد من المسائل.

إن الاستعانة بالأدلة الحديثة قد تحمل بين طياته في بعض الأحيان انتهاك لأقدس حق من الحقوق الفردية هو الاعتداء على حصانة الجسم وحرية، لكن القانون شرع هذا القيد راعية لحق آخر تملكه الجماعة.

مكافحة الجرائم المعلوماتية الماسة بالأخلاق والآداب العامة وأولويات السياسة الجنائية للدولة

د/ عبد الحليم بوشكيوه
كلية الحقوق والعلوم السياسية - جامعة جيجل

مقدمة:

شبكة الإنترنت سلاح ذو حدين، فهي شبكة مفتوحة مليئة بما هو مفيد؛ إلا أنها بالمقابل مليئة بكل ما هو مناف للأخلاق والآداب العامة، أخلاق وآداب اختلفت التشريعات الجنائية التقليدية في تجريمها وذلك لاختلاف مفاهيم الأخلاق والآداب من مجتمع إلى آخر باختلاف الثقافات والقيم والعادات.

فالمجتمعات الغربية مثلا لا يوجد بها نقاش حول خطورة المواد الإباحية عموما، مع الاتفاق على خطر هذه المواد على الصغار؛ أما في المجتمعات الإسلامية يمكن القول أن هناك اتفاقا على حرمة المواد الإباحية سواء بالنسبة للصغار أو الكبار، وإن كانت على الصغار أشد خطرا؛ ورغم هذا الاتفاق فإن الكثير من الدول الإسلامية لم تتخذ بعد الإجراءات اللازمة لحماية الأخلاق والآداب العامة من الانتهاك الواقع عليها عبر الانترنت رغم خطورة الأمر.

وكنموذج لذلك الخطر: المواقع الجنسية الإباحية التي غزت شبكة الإنترنت، فهي تشكل خطرا حقيقيا على النمو الأخلاقي والتنشئة الاجتماعية السوية للأطفال، وتزيد من انتشار الجرائم الجنسية كما هو ملاحظ في السنوات الأخيرة، وهذا كله ينعكس سلبا على الدولة وما تسعى إلى تحقيقه من الاستقرار والتنمية والتقدم.

ولا تنحصر الجرائم الماسة بالأخلاق والآداب العامة على المواقع الإباحية فقط، بل تتضمن أشكالا أخرى كمواقع القذف والتشهير، وكذا الاعتداء على الحياة الخاصة للآخرين، وغيرها. وقد يبدو أن هذه المشكلة هي مشكلة إقليمية خاصة بدول الشرق المسلمة فقط، على أساس أن دينهم وعاداتهم وتقاليدهم ترفض ذلك وتحرمه؛ إلا أن الواقع خلاف ذلك، فهذه المشكلة - في

معظم جوانبها - عالمية تعاني منها كل الدول حتى الغربية، وتحاول بكل الوسائل - خاصة القانونية - إيجاد الحلول لها والحد من آثارها السلبية.

فما هي الآليات الوطنية والدولية لمكافحة الجرائم المعلوماتية الماسة بالأخلاق والآداب العامة؟ وما مدى كفايتها؟ ما هي الصعوبات التي تواجهها؟ وكيف يمكن التغلب عليها؟ خاصة في ظل أولويات السياسة الجنائية للدولة لمواجهة الجرائم المعلوماتية؟

أولا - مفهوم الجرائم المعلوماتية الماسة بالأخلاق والآداب العامة:

أ - المقصود بالجرائم المعلوماتية الماسة بالأخلاق والآداب العامة:

الأخلاق والآداب، وإن كانت تختلف في مفهومها من مجتمع لآخر، إلا أنه يمكن إيجاد مفهوم مشترك يتفق عليه الفكر الإنساني بالنظر إلى الفطرة الإنسانية السليمة، فهي: اسم جامع لكل المعاني الفاضلة والأفعال الحميدة التي ترتضيها النفس السوية وتتماشى مع الأعراف والتقاليد لكل الشعوب والأمم الحية، والتعاليم والتشريعات لكافة الديانات السماوية، وهي دستور فطري جاءت كافة الديانات لتبرزه وتحض عليه، وتضع التشريعات لتقنينه وضبط آلياته بقيم ثابتة ومثل عليا، مثل صالحة لكل زمان ومكان.

بل إن هناك من يرى أن الأخلاق هي الأساس الذي يضبط تصرفات الناس دون إجبار أو إكراه. فهي معيار للفضيلة وريب داخلي وشكل من أشكال الوعي الإنساني يقوم على ضبط سلوك الإنسان في كافة مجالات حياته وتنظيم علاقاته الممتدة مع شقيقه الإنسان وما يحيط به من بيئة ومكان وحيوان.⁽¹⁾

ولم يقدم الباحثون تعريفا خاصا بالجرائم المعلوماتية الماسة بالأخلاق والآداب العامة، وإنما أوردوا تعريفات للجرائم المعلوماتية بصورة عامة، ويذكرون الجرائم الماسة بالأخلاق والآداب العامة عندما يتطرقون لتصنيفات الجرائم المعلوماتية.

¹ - صالح بن ناصر الخرجي، الأخلاق في عصر النشر الإلكتروني والانترنت، مقال منشور على موقع: <http://www.uaec.com/articles-action-show-id-1812.htm> بتاريخ:

2017/03/15م

فعند تصنيفهم الجرائم المعلوماتية تبعاً لدور الكمبيوتر في الجريمة، اعتبرت الجرائم الماسة بالأخلاق والآداب العامة من جرائم المحتوى أو ما يعبر عنه بالمحتوى غير المشروع أو غير القانوني الذي يرمز إلى جرائم المقامرة ونشر المواد الإباحية والغسيل الإلكتروني للأموال وغيرها.

ومن بين من أخذ بهذا التقسيم الاتفاقية الأوروبية لجرائم الكمبيوتر والانترنت لعام 2001م التي أوردت أربعة طوائف رئيسية لجرائم الكمبيوتر والانترنت، سمّت الطائفة الثالثة بالجرائم المرتبطة بالمحتوى وضمنتها طائفة واحدة وهي الجرائم المتعلقة بالأفعال الإباحية واللاأخلاقية.⁽¹⁾

أما عند من يصنف الجرائم المعلوماتية تبعاً لمساسها بالأشخاص والأموال - وهو تصنيف شائع في الدراسات والأبحاث الأمريكية - فنجد أن الجرائم الماسة بالأخلاق والآداب العامة تصنف ضمن الجرائم التي تستهدف الأشخاص ومن بينها طائفة الجرائم الجنسية.⁽²⁾

وفي تصنيف آخر للأفعال الجنائية المرتكبة أثناء استخدام الانترنت أورد محمد عبد الله منشاوي صنفاً أسماه: الجرائم الجنسية والممارسات غير الأخلاقية، وقال بأنه يشمل⁽³⁾: المواقع والقوائم البريدية الإباحية؛ المواقع المتخصصة في القذف وتشويه سمعة الأشخاص؛ استخدام البروكسي للدخول إلى المواقع المحجوبة؛ إخفاء الشخصية؛ الجرائم الاقتصادية.

ويصنف محمد أمين الرومي الجرائم الماسة بالأخلاق والآداب العامة عبر الإنترنت إلى ثلاثة أنواع:⁽⁴⁾ جرائم الجنس عبر الإنترنت؛ جرائم السب والقذف عبر الإنترنت؛ جريمة التجسس عبر الإنترنت. وهناك تصنيف آخر لمنير محمد الجنيهي وممدوح محمد الجنيهي⁽¹⁾ تحت مسمى آخر وهو الجرائم والممارسات الجنسية وغير الأخلاقية وتضم: المواقع الإباحية؛ مواقع قذف وسب وتشويه سمعة الأشخاص؛ الدخول إلى المواقع المحجوبة.

¹ - يونس عرب، جرائم الكمبيوتر والإنترنت، مقال منشور على موقع الدكتور عايض المري للدراسات والاستشارات القانونية

www.lawjo.net/vb/attachment.php?attachmentid=1210&d بتاريخ:

2017/03/13

² - المرجع نفسه.

³ - محمد عبد الله منشاوي، مرجع سابق.

⁴ - محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية الإسكندرية، 2004 م، ص 130-139.

ومن التصنيفات السابقة يمكن القول بأن المقصود بالجرائم الماسة بالأخلاق والآداب العامة عبر الإنترنت: جميع الأفعال المخالفة للأخلاق والآداب العامة المرتكبة من خلال شبكة الانترنت بواسطة الكمبيوتر أو أي جهاز آلي آخر يمكن بواسطته الاتصال بالانترنت.⁽²⁾

ويمكن القول بأن أهم الأفعال المخالفة للأخلاق والآداب العامة على الانترنت والتي تشكل جريمة في القانون ما يلي: المواقع الإباحية: إنشاؤها، ارتيادها، الاشتراك فيها، الشراء منها؛ التشهير بالآخرين عبر الانترنت؛ الاعتداء على الحياة الخاصة عبر الإنترنت (التجسس عبر الإنترنت).

ب - أنواع الجرائم المعلوماتية الماسة بالأخلاق والآداب العامة:⁽³⁾

1- جرائم المواقع الإباحية:

1-1- المقصود بجرائم المواقع الإباحية:

يندرج ضمن جرائم المواقع والقوائم البريدية الإباحية جرائم ارتياد المواقع الإباحية، الشراء منها، الاشتراك فيها، أو إنشائها. وتحاول بعض هذه المواقع استدراج مرتاديها بتقديم خدمة إرسال صور جنسية مجانية يومية على عناوينهم البريدية.

أما القوائم البريدية فهي أسهل إنشاء، وغالبا مجانية ويقوم أعضاؤها من المشتركين بتبادل الصور والأفلام الخليعة على عناوينهم البريدية. ويشترك في القوائم البريدية آلاف الأشخاص الذين تصل أي رسالة يرسلها مشترك منهم إلى جميع المشتركين مما يعني كما هائلا من الرسائل والصور الجنسية التي يتبادلها مشتركو القائمة البريدية بشكل يومي.

¹ - منير محمد الجنيبي وممدوح محمد الجنيبي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، دط، 2005 م، ص 29-39

وانظر: - تركي محمد العطيان، جرائم الحاسب الآلي - دراسة نفسية تحليلية، مقال منشور على موقع أكاديمية نايف العربية للعلوم الأمنية: <http://library.nauss.edu.sa/> بتاريخ: 2017/03/16م.

² - كالهاتف المحمول الذي يمكن استخدام الجيل المتطور منه للاتصال على الانترنت.

³ - للاستزادة انظر: - محمد محمد الألفي، بعض أنماط الجرائم الأخلاقية عبر الانترنت في المجتمع العربي، مقال منشور على موقع شبكة النبأ المعلوماتية.

- سعود وصل الله سعد النقيب، جرائم الكمبيوتر والانترنت، مقال منشور على موقع أكاديمية نايف العربية للعلوم الأمنية: <http://library.nauss.edu.sa/> بتاريخ: 2017/03/16م.

ويوجد على الإنترنت آلاف المواقع الإباحية وعدد كبير جدا من القوائم الجنسية والتي أصبحت أكثر تخصصا، فهناك قوائم خاصة للشواذ من الجنسين.⁽¹⁾

وأود الإشارة إلى أن زيارة الصفحات الإباحية تبدأ بفضول وتتطور إلى إدمان وإفلاس أخلاقي ومادي وتوجه نحو الجريمة بالتقليد.

فقد أوضحت دراسة أدست (ADIST)⁽²⁾ أن المواقع الإباحية أصبحت مشكلة حقيقية وأن الآثار المدمرة لهذه المواقع لا تقتصر على مجتمع دون الآخر⁽³⁾ ويمكن أن تلمس آثارها السيئة على ارتفاع جرائم الاغتصاب بصفة عامة واغتصاب الأطفال بصفة خاصة، العنف الجنسي، فقد الأسرة لقيمها ومبادئها وتغير الشعور نحو النساء إلى الابتذال بدل الاحترام، من المودة إلى المهانة.

ولا شك أن هناك علاقة بين ارتكاب الجرائم الجنسية والنظر إلى الصور والأفلام الجنسية الفاضحة⁽⁴⁾ فلا بد من الربط بين زيارة المواقع الإباحية الخليعة والتي تضغط على الغرائز وتثيرها في مجتمعات محافظة جنسيا كالمجتمعات العربية وبين زيادة الجرائم الجنسية التي زاد عددها.⁽⁵⁾

وتشمل هذه الجريمة كذلك حض وتحريض القصر على أنشطة جنسية غير مشروعة وإفساد القصر بأنشطة جنسية عبر الوسائل المعلوماتية، وإغواء أو محاولة إغواء القصر لارتكاب أنشطة جنسية غير مشروعة، وتلقي أو نشر المعلومات عن القصر عبر الكمبيوتر من أجل أنشطة جنسية غير مشروعة، والتحرش الجنسي بالقصر عبر الكمبيوتر والوسائل التقنية، ونشر وتسهيل نشر واستضافة المواد الفاحشة عبر الانترنت بوجه عام وللقصر تحديدا ونشر الفحش والمساس بالحياء (هتك العرض بالنظر) عبر الانترنت، وتصوير أو إظهار القصر ضمن أنشطة جنسية واستخدام الانترنت لترويج الدعارة بصورة قسرية أو للإغواء أو لنشر المواد الفاحشة التي تستهدف استغلال عوامل الضعف

1 - محمد عبد الله منشاوي، المرجع السابق.

2 - المرجع نفسه.

3 - مشعل بن عبد الله القدحي، الإباحية في الانترنت والاتصالات والإعلام وأثرها على الفرد والمجتمع والأمن العام، مقال منشور على موقع أكاديمية نايف العربية للعلوم الأمنية: <http://library.nauss.edu.sa/> بتاريخ: 2017/03/16م.

4 - محمد عبد الله منشاوي، المرجع السابق.

5 - المرجع نفسه، ص 32.

والانحراف لدى المستخدم والحصول على الصور والهويات بطريقة غير مشروعة لاستغلالها في أنشطة جنسية.⁽¹⁾

وبإمعان النظر في هذه الأوصاف نجد أنها تجتمع جميعاً تحت صورة واحدة هي استغلال الانترنت والكمبيوتر لترويج الدعارة أو إثارة الفحش واستغلال الأطفال والقصر في أنشطة جنسية غير مشروعة.⁽²⁾

ويوجد على الانترنت حالياً مواقع وبرامج متخصصة في المحادثات (CHATING) المصورة تستخدم كاميرات الويب (WEB CAM) حيث يقوم بعض الشباب بتصوير مشاهد التعري أو الفاحشة أو اللواط وغيرها من المشاهد المنافية للأخلاق والآداب وذلك باستخدام تلك الوسيلة أو بكاميرات الجيل الثالث من الهواتف النقالة ثم تحميلها على الإنترنت، أو تبادلها مباشرة عن طريق البريد الإلكتروني أو غرف المحادثة، أو في الطرقات العامة باستخدام البلوتوث (BLEUTOOTH)، ثم تطور الأمر إلى تطبيقات أكثر تطوراً على الهواتف الذكية. وقد أدى انتشار مواقع المحادثة هذه إلى ظهور سلوك جديد أيضاً وهو ممارسة الفاحشة عبر الانترنت.⁽³⁾

1-2- التكييف القانوني لجرائم المواقع الإباحية:⁽⁴⁾

الأفعال المخلة بالحياء أمر مجرم في كافة القوانين العربية، بل وفي كثير من القوانين في معظم بلاد العالم، وتندرج تحت جريمة مسماها: «إتيان الأعمال الفاضحة علانية والتحريض على ممارستها».

¹ - يونس عرب، صور الجرائم الإلكترونية واتجاهات تبويبها، مقال منشور على موقع: www.ituarab.org/coe. بتاريخ: 2017/03/16م.

انظر كذلك: - عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت (الجرائم الإلكترونية)، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، ط 1، 2007م ص 133.

- يونس عرب، تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، مقال منشور على موقع: www.ituarab.org/coe بتاريخ: 2017/03/16م.

² - يونس عرب، صور الجرائم الإلكترونية واتجاهات تبويبها، المرجع السابق.

³ - ناصر بن محمد المهيزع، المواد الإباحية والانترنت، مقال منشور على موقع أكاديمية نايف العربية للعلوم الأمنية <http://library.nauss.edu.sa/> بتاريخ: 2017/03/16م.

⁴ - منير محمد الجنبهي وممدوح محمد الجنبهي، المرجع السابق، ص 32.

ويعتد من الأمور المشددة في التجريم والعقاب أمرين: العلانية أثناء ممارسة الفعل. والعلانية في التحريض على الممارسة. ومثال ذلك ما هو منصوص عليه في قانون العقوبات الجزائري من تجريم لتلك الأفعال وعقاب من يقوم بها، وذلك في المواد 333، 333 مكرر، 342، 343. ولما كانت شبكة الانترنت تعد مكانا مقصودا من الكثير من الأشخاص ومن كافة الجنسيات على مستوى العالم، وهو ما يجعلها تحمل نفس خصائص الأماكن العامة التي توفر صفة العلانية بمعنى أن كل من يقوم بفعل على شبكة الانترنت يكون بإمكان أي من مرتادي الشبكة الإطلاع عليه. وكما كانت المواقع الإباحية المنتشرة على شبكة الانترنت هي مواقع تحرض على الفسق و الدعارة لا بالإشارة و القول فقط، وإنما أكثر من ذلك فهي تحرض على ذلك بالصور وأفلام الجنس، وهو الفعل الذي تم النص على المعاقبة عليه في المادة 347 من قانون العقوبات الجزائري. بل إن المحادثات الجنسية التي تتم من خلال ما يعرف بغرف المحادثات (CHATING) تندرج تحت إتيان الأفعال الإباحية الفاضحة التي تتم علانية والتي تم النص على تجريمها طبقا للمادة 333 من قانون العقوبات الجزائري.

2 - جريمة التشهير بالآخرين عبر الانترنت:

تعد جريمة السب والقذف والتعرض للحياة الخاصة للأفراد والاعتداء على شرفهم واعتبارهم وإفشاء أسرارهم و الخوض في أغراضهم من أكبر الجرائم التي يتم تجريمها في كافة القوانين سواء في الدول العربية أو الأجنبية أيا كانت الطريقة أو الوسيلة التي تتم بها تلك الجريمة سواء تقليدية كالصحف أم حديثة باستخدام شبكة الانترنت بواسطة إنشاء مواقع خاصة بقذف وسب و التشهير سواء بشخص معين أو بدولة من الدول أو بدين من الأديان.¹ ويهدف مرتكبو هذه الجريمة إما إلى تشويه سمعة بعض الرموز الدينية أو السياسية أو الفكرية بهدف تشكيك الناس في مدى مصداقيتهم ومحاولة فض الناس من حولهم، وقد يكون الهدف محاولة ابتزاز بعض الأشخاص ماليا أو جنسيا وإذا لم يرضخوا للابتزاز يقوم الجاني بتشويه سمعتهم.⁽²⁾

¹ - للاستزادة انظر: - عبد الله بن فهد الشريف، جريمة التشهير بالآخرين عبر الانترنت، مقال منشور على موقع أكاديمية نايف العربية للعلوم الأمنية <http://library.nauss.edu.sa> بتاريخ: 2017/03/16م.

² - منير محمد الجنبهي وممدوح محمد الجنبهي، المرجع السابق، ص 35، 36.

وأَسباب ذلك التجريم هي أن الحرية والديمقراطية لا يجب أن تنطوي على الإخلال بها وتجرّيح الأشخاص في أعراضهم ومبادئهم وشرفهم ونسب أمور غير صحيحة لهم بغرض التشهير بهم ومبادئهم و الخوض في أعراضهم وفي حياتهم الخاصة التي هي ملك لهم وحدهم دون أن يكون لأي شخص آخر أن يخوض أو يتدخل فيها بأي شكل من الأشكال.

وعليه فإن جريمة القذف والسب والتشهير التي تتم عن طريق الانترنت بواسطة إنشاء مواقع أو إرسال بريد الكتروني يكون هدفها فقط قذف أو سب أو التشهير سواء بشخص أو دولة أو دين ما تقع تحت طائلة نفس النصوص القانونية التقليدية التي تجرم تلك الأفعال. ⁽¹⁾ وفي القانون الجزائري تم تجريم تلك الأفعال بالمواد: 296 - 299 - 303 مكرر - 303 مكرر 1 - 303 مكرر 3.

ومن مجموع هذه النصوص العقابية يمكن توقيع عقوبة القذف أو السب مباشرة بطريقة الهاتف أو الانترنت على من يقوم بإرسال شتائم أو يقوم بالتشهير بالغير بواسطة شبكة الانترنت، وسواء تم ذلك عن طريق إنشاء موقع خاص على الشبكة أو عن طريق إرسال بريد الكتروني للمجني عليه أو عن طريق ما يسمى بغرف المحادثات (CHATING)⁽²⁾

3 - جريمة الاعتداء على الحياة الخاصة عبر الانترنت (التجسس عبر الانترنت):

3-1- المقصود بجريمة الاعتداء على الحياة الخاصة عبر الانترنت:

ويتم ذلك عن طريق إدخال ملف تجسس⁽³⁾ إلى المجني عليه عن طريق بريده الالكتروني أو برامج المحادثة (CHATING) أو عند زيارة مواقع مجهولة تغريه بتحميل بعض البرامج والملفات المجانية ومن ضمنها ملف التجسس.

وفي حالة إصابة الجهاز بملف التجسس يقوم على الفور بفتح أحد المنافذ في جهاز الشخص المجني عليه وهذا المنفذ هو الباب الخلفي لحدوث اتصال بين جهاز الشخص المجني عليه وجهاز المخترق. والذي من خلاله يمكن للمخترق أن يسيطر على جهاز المجني عليه دون أن يشعر هو بذلك،

¹ - المرجع نفسه، ص 36، 37.

² - محمد أمين الرومي، المرجع السابق، ص 135 بتصرف.

³ - من بين ملفات التجسس ملف " حصان طروادة " Cheval de trois " الذي يرسله المخترق للمجني عليه ويقول له بأنه يحتوي على لعب مثيرة أو ملفات قيمة أو غير ذلك من الإغراءات فيخدع المجني عليه ويقوم باستقبال الملف.

انظر: - محمد أمين الرومي، المرجع السابق، ص 136.

فبإمكان المخترق فتح القرص الصلب (DISC DUR) لجهاز المجني عليه والعبث فيه كيفما يشاء سواء بالحذف أو بالإضافة، كما يمكن للمخترق معرفة كل كلمات السر المخزنة في الجهاز بداية من الاشتراك في الانترنت وحتى رقم بطاقة الائتمان. كذلك يمكن للمخترق إذا كان لدى المجني عليه ميكروفون أو كاميرا ويب (WEB CAM) أن يستمع ويرى كل ما يفعله المجني عليه في المساحة التي يغطيها الميكروفون أو الكاميرا.⁽¹⁾

3-2- التكييف القانوني لجريمة الاعتداء على الحياة الخاصة عبر الانترنت:

بالنسبة للتشريع الجزائري نجد أن قانون العقوبات يحمي الحياة الشخصية للمواطن من أي اعتداء عليها. فالمادة 303 مكرر (قانون رقم 06 - 23 مؤرخ في 20 ديسمبر 2006) تنص على أن يعاقب كل من تعمد المساس بجريمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك:

- 1 - بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.
 - 2 - بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه.
- وطبقا لهذه المادة وكذلك المادة 303 من نفس القانون⁽²⁾ يمكن القول بخضوع فعل التجسس على الأشخاص عن طريق الانترنت والعقاب عليه لهذه المادة. فكل من يمس بجريمة الحياة الخاصة لشخص أو أشخاص عن طريق الإنترنت أو بالتقاط صورا أو أحاديث موجودة على ملفات الكترونية شخصية للغير عن طريق برامج التجسس يخضع لأحكام جريمة الاعتداء على حرمة الحياة الخاصة⁽³⁾.

ولكن تبقى مشكلة الشرعية الجزائية مطروحة في هذه الجريمة وفي سابقاتها؟ إذ لا جريمة ولا عقوبة إلا بنص، وكذلك مبدأ عدم القياس والتفسير الضيق لنصوص القانون الجنائي كل هذه المسائل مطروحة لمناقشة إشكالية مدى إمكانية تطبيق النصوص الجنائية التقليدية على جرائم الانترنت الحديثة؟ وهذا ما سنتناوله في العنصر التالي.

1 - المرجع نفسه، ص 136، 137.

2 - نصت المادة 303 من قانون العقوبات الجزائري على أن: "كل من يفض أو يتلف رسائل أو مراسلات موجهة إلى الغير وذلك بسوء نية وفي غير الحالات المنصوص عليها في المادة 137، يعاقب بالحبس من شهر إلى سنة وبغرامة من 25000 دج إلى 100.000 دج أو بإحدى هاتين العقوبتين فقط".

3 - أنظر: - محمد أمين الرومي، المرجع السابق، ص 138.

ج - مدى انطباق النصوص الخاصة بالجرائم المخلة بالأخلاق والآداب العامة في التشريعات الجزائية التقليدية على الجرائم المعلوماتية

إن أكثر مسائل ظاهرة جرائم الكمبيوتر والانترنت إثارة للجدل، إلى جانب تعريفها وتحديد موضوعها أو مناهج الحماية ومحله، مسألة تحديد قائمة جرائم الكمبيوتر وتحديد أنماط السلوك الإجرامي والأفعال المكونة له وبيان القوام القانوني لهذه الجرائم، هذه المسألة أفرزت خلافا وتباينا موضوعيا لدى الفقه الجنائي في مختلف النظم القانونية اللاتينية و الجرمانية والأنجلوسكسونية حول مدى انطباق نصوص القوانين الجنائية التقليدية على هذه الجرائم؟⁽¹⁾

ومن بين هذه الجرائم الجرائم الماسة بالأخلاق والآداب العامة عبر الانترنت، إذ يثور التساؤل فيما إذا كانت النصوص التي جرم المشرع الجنائي الجزائري من خلالها الإخلال بالأخلاق والآداب العامة بصورتها التقليدية فيما إذا كانت هذه النصوص من المرونة بحيث تسمح بانطباقها على الانترنت فيما لو استخدم كوسيلة للقيام بالأفعال المخلة بالأخلاق والآداب العامة أم لا؟

لقد جرم المشرع الجزائري الإخلال بالأخلاق والآداب العامة بصورتها التقليدية (أي غير المعلوماتية). فقد نصت المادة 333 مكرر من قانون العقوبات الجزائري على أن: "يعاقب بالحبس من شهرين إلى سنتين وبغرامة من 500 إلى 200 دج كل من صنع أو حاز أو استورد أو سعى في استيراد من أجل التجارة أو وزع أو أجر أو لصق أو قام معرضا أو عرض أو شرع في العرض للجمهور أو باع أو شرع في البيع أو وزع أو شرع في التوزيع كل مطبوع أو محرر أو رسم أو إعلان أو صور أو لوحات زيتية أو صور فوتوغرافية أو أصل الصورة أو قالبها أو أنتج أي شيء مخل بالحياء".

كما نصت المادة 347 على أن: "يعاقب بالحبس من 6 أشهر إلى سنتين وبغرامة من 1000 إلى 20.000 دج كل من قام علنا بإغراء أشخاص من أي من الجنسين بقصد تحريضهم على الفسق وذلك بالإشارة و الأقوال أو الكتابة أو بأية وسيلة أخرى. ويعاقب على الشروع بالعقوبات ذاتها المقررة للجريمة التامة".

باستقراء المواد السابقة الذكر من قانون العقوبات الجزائري، نجد أن المشرع حرص على تجريم أي مادة خليعة تؤدي إلى إفساد الأخلاق، ومن ذلك تجريم عرضها في محل عام.

¹ - يونس عرب، جرائم الكمبيوتر والانترنت، المرجع السابق.

فإذا كانت مقاهي الانترنت من الأماكن العامة التي يرتادها جمهور الناس فإن عرض المواد الإباحية الخليعة داخلها (على شاشات الحاسوب الموجودة فيها) تتحقق به الجريمة طبقا لنص المادة 333 مكرر السابقة الذكر.

فكل من يصنع تلك الأشياء الخليعة ويقوم بتحميلها وعرضها على صفحات الانترنت أو يسمح بعرض تلك الأشياء المخلة بالحياء في محله تقع عليه المسؤولية الجنائية.

ومن عرض وتحليل النصوص الجزائية السابقة يمكن القول بإمكانية انطباقها في بعض جوانبها على الجرائم الماسة بالأخلاق والآداب العامة على الانترنت إلا أن هذه النصوص لا يمكن تطبيقها على هذا النوع من الجرائم عبر الانترنت استنادا إلى القياس لأن ذلك يتعارض مع مبدأ الشرعية الجنائية القاضي بأن لا جريمة ولا عقوبة إلا بنص، ومبدأ عدم القياس و التفسير الضيق لنصوص القانون الجنائي.

وهذا ما أكدته يونس عرب حين دعا إلى وضع نظرية عامة لجرائم الانترنت تختلف عن النظرية العامة للجرائم التقليدية فقال: "إن طبيعة وأبعاد ظاهرة جرائم الكمبيوتر تشير إلى تميزها في أحكام لا توفرها النظريات القائمة (التقليدية)... وهذا ما أدى إلى حسم الجدل الواسع حول مدى انطباق النصوص القائمة على هذه الجرائم لجهة وضع تشريعات ونصوص جديدة تكون قادرة على الإحاطة بمفردات ومتطلبات وخصوصية جرائم الكمبيوتر والانترنت، وهو بالتالي ما يحسم الجدل حول الحاجة إلى نظرية عامة لجرائم الكمبيوتر توقف التوصيف الجزئي والمعالجات المبسترة".⁽¹⁾

لهذا على المشرع الجزائري أن يعنى بتعديل هذه النصوص بحيث تشمل على تجريم المساس بالأخلاق والآداب العامة عبر الانترنت بما يتفق ومبدأ المشروعية الجنائية، أو يقوم بإصدار قانون خاص بهذه الجرائم. وهذا ما يتوقع إصداره في الأيام المقبلة إذ برمج البرلمان الجزائري لدورته الربيعية المقبلة التصويت على مشروع قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاتصال والمعلوماتية ومكافحتها.⁽²⁾

1 - المرجع نفسه.

2 - جلال بوعاتي، مشروع قانون الوقاية من جرائم الانترنت والاتصالات في البرلمان، إلزام متعملي الانترنت والهاتف النقال بالتعامل مع مصالح الأمن، (مقال)، جريدة الشروق اليومي الجزائرية، عدد يوم 01 مارس 2009م.

ثانيا - آليات مكافحة الجرائم المعلوماتية الماسة بالأخلاق والآداب العامة:

أ - الآليات الداخلية (الوطنية) لمكافحة الجرائم المعلوماتية الماسة بالأخلاق والآداب العامة:

يجب أولا وضع ضوابط لاستخدام الانترنت عن طريق إصدار قوانين تنظم استخدام الانترنت. وكذلك تجريم كل الأفعال الماسة بالأخلاق والآداب العامة التي تطرقنا إليها وهذا ما سعى إليه المشرع الجزائري من خلال مشروع قانون الوقاية من جرائم الانترنت والاتصالات، الذي سيعرض للمصادقة عليه خلال الدورة الربيعية للبرلمان لهذا العام 2009م.

بالإضافة إلى ترشيح (حجب) المواقع الإباحية والأخلاقية.

هناك من يقول إن الناس - في غالبيتهم - يستطيعون ضبط أنفسهم فهم بذلك يتحكمون في أنفسهم ولا حاجة للحجب ؟

وجد "كاس سانستين" بأن الدول التي تفرض قوانين صارمة في منع المواد الإباحية تنخفض في نسبة جرائم الاغتصاب والجرائم العنيفة.⁽¹⁾

كما قام باحثان من جامعة "نيوهامبشير" بأمريكا بدراسة ظاهرة تفشي الإباحية والدعارة وأثر ذلك على جريمة الاغتصاب، فوجدا أن الولايات التي تكثر فيها وسائل الدعارة والإباحية ترتفع في نسبة جرائم الاغتصاب، والعكس صحيح.⁽²⁾

لهذا ندعو إلى الإسراع في إنشاء هيئة تقنية متخصصة تقوم بترشيح وحجب المواقع المخالفة للقانون خاصة المنافية للأخلاق والآداب العامة.⁽³⁾

¹ - مشعل بن عبد الله القدهي، الإباحية في الإنترنت والاتصالات والإعلام وأثرها على الفرد والمجتمع والأمن العام، مقال منشور على موقع المنشاوي للدراسات والبحوث، ص 24 www.minshaw.com نقلا عن: - Cass R. Sunstein, « pornography and the first amendment », Duck Law jornal, September 1986.

وانظر كذلك: - موقع www.khayma.com/almslm بتاريخ: 2017/03/16م.

² - مشعل بن عبد الله القدهي، المرجع السابق.

³ - وهذا اقتداء ببعض الدول التي أنشأت أنظمة حجب، مثل ما تقوم به مدينة الملك عبد العزيز للعلوم والتقنية بالعربية السعودية. انظر: مشعل بن عبد الله القدهي، المرجع السابق ص 25.

ولكن من المهم أن يكون هناك تعاون دولي خاصة بين الدول العربية الإسلامية في وضع استراتيجيات موحدة ودعم الأبحاث ذات العلاقة، والتعاون في إنتاج حلول وبرامج خفية وتوعوية وجزائية لمكافحة هذا النوع من الجرائم، كما فعل الاتحاد الأوروبي خلال السنوات الماضية.

فقد قام الاتحاد الأوروبي برصد مبلغ 25 مليون يورو من 1999 إلى 2002م لمشروع وضع إستراتيجية فنية متكاملة لتسهيل أمر ترشيح الإنترنت على مستوى الأفراد، ومن 2002 إلى 2004م زاد الاتحاد في الميزانية المخصصة لذلك إلى 38.3 مليون يورو.⁽¹⁾ إلا أن الترشيح كان متعلقاً أساساً بحماية الأطفال فقط من المواد الإباحية.

وتقوم الصين منذ 1995 بترشيح الإنترنت لمنع الإباحية والقمار والمخدرات والعنف وبعض المواد السياسية. وقد قامت السلطات فيها في الفترة ما بين فيفري 2004 و جويلية 2004 بإجراء حملة تفتيشية على 1.8 مليون مقهى للإنترنت، أصدرت على إثره أوامر بإيقاف العمل في 18000 منها حتى يتم تصحيح أوضاعها، و بإغلاق أكثر من 1600 منها، وسجن أكثر من 224 فرداً، وفرض غرامات قدرها 12 مليون دولار على بعضها لمساهمتها في نشر أفلام الإباحية والقمار والمواد العنيفة وألعاب العنف عبر الإنترنت، ولتعريضها الصغار إلى هذه المواد.⁽²⁾

وتقوم العديد من الدول الأخرى بترشيح محتوى الانترنت طبقاً لقوانين أصدرتها لمنع المواد التي تعتبرها متنافية مع قيمها ومنها المواد الإباحية والشذوذ، ومن هذه الدول: النرويج، أستراليا، سنغافورا، كوريا الجنوبية، بريطانيا، تايلاندا، تايوان (في مؤسسات محددة مثل جامعة تايوان المركزية التي تعني بترشيح المواد الإباحية والعنيفة)، الهند، كندا، ألمانيا، إسبانيا...

وقد قامت إحدى الشركات البريطانية بتطوير بطاقة هوية ذكية تمكن القائمين على غرف الدردشة من التعرف على أعمار الزائرين وحجبهم عن بعض المنتديات المخلة بالآداب.⁽³⁾

¹ - www.europa.eu.int/information_society/programes/iap/index_en.htm

بتاريخ: 2017/03/16م.

... www.aljazeera.net/NR/exeres/ بتاريخ:

² - انظر:

2017/03/16م.

بتاريخ: 2017/03/16م. www.china.org.cn/arabic/140656.htm

بتاريخ: 2017/03/16م. www.bbc.co.uk/2/hi/asia-pasific/3943445.stm

- مشعل بن عبد الله القدهي، المرجع السابق ص36. ³

أما الدول العربية والإسلامية، فإن نظام الترشيح فيها وإن لم يعم جميع الدول استهدف بشكل أساسي المواد الإباحية ثم السياسية ثم المسيئة للدين الإسلامي و نذكر من تلك الدول: المملكة السعودية، الإمارات العربية المتحدة، إيران، اليمن، قطر، سلطنة عمان، الكويت، السودان، تونس (التي تعني بحجب المواد السياسية بشكل أساسي)، تركيا، سوريا، باكستان.

ولكن نشير إلى أن سياسة الحجب هذه رغم فعاليتها فيما يخص المواقع الإباحية إلا أنها عاجزة عن حجب مواقع الدردشة (المحادثات) وتبادل المواد الإباحية عن طريق البريد الإلكتروني فما هو الحل بالنسبة لهاتين التقنيتين؟ خاصة وأنه يمكن التقاط الصور بالكاميرات الرقمية أو كاميرات الهواتف النقالة ثم تحميلها على الانترنت وإرسالها عبر غرف الدردشة أو البريد الإلكتروني.

لهذا يجب مراقبة مقاهي الانترنت، وذلك بإنشاء ما يسمى بشرطة الانترنت أو الشرطة المعلوماتية، ومعاينة كل من يقوم أو يسمح بعرض ما يخالف الأخلاق والآداب العامة.

ومن الواجب إلزام أصحاب هذه المقاهي باستخدام البرامج المضادة لمثل هذه المواقع الإباحية (ANTI PORN)، وتحميلهم المسؤولية الجنائية في حالة المخالفة.

كل ما سبق لا يكفي للقضاء نهائياً على هذا النوع من الجرائم، فالإنترنت دخلت البيوت وغرف الأطفال الصغار، لذلك فإن الرقابة الأسرية الصارمة والوعاية، بالإضافة إلى التوعية وغرس الوازع الديني في نفوس الشباب ويمكن أن يساهم في حماية أبنائنا وبناتنا من خطر هذه الجرائم.

فمن الضروري إيجاد البدائل البناءة؛ فلا بد من وجود المحتوى العلمي المفيد والمحتوى الترفيهي الهادف والمحتوى الديني المتزن، ولا بد من توفير خدمات الانترنت الخالية من المواد التي تخدش الحياء في متناول الجميع.⁽¹⁾

إن الخطر المحتمل لجرائم الإنترنت ومن بينها الجرائم الماسة بالأخلاق والآداب العامة في البيئة العربية كبير، باعتبار أن الجاهزية التقنية والتشريعية والأدائية (استراتيجيات الحماية) لمواجهة لها ليست بالمستوى المطلوب إن لم تكن غائبة تماماً. وإدراكاً لقصور القوانين الجنائية بما تتضمنه من نصوص

¹ - محمد محمد الألفي، دور المجتمع المدني في مكافحة مظاهر العدوان الإجرامي عبر الانترنت، مقال منشور على موقع المنشاوي للدراسات والبحوث www.minshawy.com

التجريم التقليدية كان لابد من وضع قوانين وتشريعات خاصة أو العمل على تعديل تلك القوانين التقليدية من أجل ضمان توفير الحماية القانونية الفاعلة ضد هذه الجرائم.⁽¹⁾

ومن الاقتراحات المقدمة لمكافحة الجرائم الماسة بالأخلاق والآداب العامة عبر الإنترنت:⁽²⁾

* التدخل التشريعي بالنص صراحة على تجريم التشهير و الإساءة إلى الغير عبر شبكة الإنترنت و اعتبار الإنترنت ضرفا مشددا.⁽³⁾

* محو أمية الإنترنت لدى العاملين في مجال القضاء و الجهات ذات العلاقة.

* تقرير عقوبات تأديبية من طرف شبكة الإنترنت أو إدارة الموقع و ذلك مثل الحرمان المؤقت أو المؤبد من استخدام الانترنت للشخص الذي يسيء استعماله.

* تقرير تدابير احترازية للعاملين من المهنيين في مجال النت حالة إساءة استعمال المهنة.

وهناك من اقترح إيجاد أنظمة تمنع الإساءة والتشهير بالآخرين، وتعني بجرائم النشر في الإنترنت، وتشتمل تنظيم إنشاء المواقع على الشبكة العالمية وعملية إدارتها والإشراف عليها ومتابعتها وتحديد مسؤولية الناشر والمشرّف على الموقع عن كل ما يشرف فيه من خلال تقنين المشاركات وإخضاع المشرّف للمساءلة القانونية عند سماحه بنشر كل ما يخالف النظام، وفي حالة التجاوزات يمكن منعها ابتداء أو حذفها مباشرة من خلال وضع برامج لا تسمح بنشر المشاركات إلا بعد موافقة المشرّف على المتتديات في تلك المواقع، بمعنى أن تكون مسؤولية مخالفة النشر في مواقع الإنترنت مسؤولية أصحاب هذه المواقع والمشرّفين عليها، كما هو الحال في نظام المطبوعات والنشر ولجان المخالفات الصحفية التي يجرّم فيها رئيس التحرير وكاتب المقال عن كل ما ينشر في المطبوعة من أخبار غير صحيحة تسيء للآخرين في أعراضهم وسمعتهم، بحيث يكون للمتضرر من جرائم التشهير في

1 - يونس عرب، جرائم الكمبيوتر والإنترنت، مرجع سابق.

2 - عثمان سعيد المحيشي، جريمة التشهير بين الرؤية القانونية التقليدية و تقنيات العصر، و رقة عمل مقدمة إلى المنظمة العربية للتنمية الإدارية، المؤتمر الدولي لقانون الإنترنت 21-25 أوت 2005 منشور على موقع المنشاوي للدراسات والبحوث www.minshawi.com. بتاريخ: 2017/03/16م.

3 - انظر: - محمد صالح العادلي، الجرائم المعلوماتية ماهيتها صورها، مقال منشور على موقع المنشاوي للدراسات والبحوث www.minshawi.com بتاريخ: 2017/03/16م.

- يحيى بن محمد أبو مغايز، رؤية مستقبلية لدور الحكومة الالكترونية في مواجهة الجريمة المعاصرة، مقال منشور على موقع كلية نايف العربية للعلوم الأمنية <http://library.nauss.edu.sa> بتاريخ: 2017/03/16م.

الإنترنت الحق في المطالبة بالتعويض أو حجب هذه المواقع التي تسيء للغير بدون وجه حق بقوة القانون⁽¹⁾.

بينما يجزم الأستاذ محمد بن عبد الله المشوح بأن بإمكان الجهات التشريعية والقضائية والتنفيذية والرقابية فرض طوق أمني حازم والضرب بقوة على أولئك المشهرين بحقوق الناس وحرماهم وأشخاصهم⁽²⁾.

إن البعد الإجرائي لمكافحة جرائم الإنترنت ومن بينها الجرائم الماسة بالأخلاق والآداب العامة على الإنترنت - ينطوي على مشكلات و تحديات كبرى أهمها:

- الحاجة إلى سرعة الكشف خشية ضياع الدليل.⁽³⁾
- خصوصية قواعد التفتيش والضبط الملائمة لهذه الجرائم.⁽⁴⁾
- قانونية وحجية أدلة إثبات جرائم الإنترنت.⁽⁵⁾
- مشكلات الاختصاص القضائي والقانون الواجب التطبيق.⁽⁶⁾

1 - هيام المفلح، التشهير بالناس عبر النت.. جرائم استفحلت.. تبحث عن عقوبات وحلول، مقال على موقع صحيفة الرياض.

انظر: - ويكيبيديا الموسوعة الحرة، أخلاقيات الانترنت، مقال منشور على موقع الموسوعة www.ar.wikipedia.org.

2 - هيام المفلح، المرجع السابق.

3 - فهذه الجرائم لا تترك أثرا ماديا في مسرح الجريمة، كما أن مرتكبيها يملكون القدرة على إتلاف أو تشويه أو إضاعة الدليل في فترة قصيرة.

4 - التفتيش والضبط في هذا النمط من الجرائم يمتدان إلى نظم أخرى غير النظام محل الاشتباه، وهذا يخلق تحديات كبيرة أولها مدى قانونية هذين الإجراءين ومدى مساسها بحقوق الخصوصية المعلوماتية لأصحاب النظم الأخرى التي يمتد إليها التفتيش والضبط.

5 - وأدلة الإدانة ذات طبيعة معنوية، وتثير أمام القضاء مشكلات من حيث مدى قبولها وحجيتها للإثبات.

6 - كما أن اختصاص القضاء بنظر جرائم الإنترنت، وكذا القانون الواجب تطبيقه على الفعل، لا يحظى دائما بالوضوح والقبول، لأن غالبية هذه الأفعال ترتكب من قبل أشخاص من خارج الحدود أو تمر عبر شبكات وأنظمة معلومات خارج حدود الدولة. وهو ما يبرز أهمية وضع قواعد الاختصاص والقانون الواجب التطبيق خاصة بهذا النوع من الجرائم.

ويرتبط بمشكلات الاختصاص والقانون الواجب التطبيق مشكلات امتداد أنشطة الملاحقة والتحري والضبط والتفتيش خارج الحدود، وما يحتاجه ذلك إلى تعاون دولي شامل للموازنة بين موجبات المكافحة ووجوب حماية السيادة الوطنية. وهذه المشكلات كانت، ولا تزال محل اهتمام على الصعيدين الوطني والدولي.

والتعاون الدولي مهم عند التعامل مع جرائم الإنترنت، كونه سيطور أساليب متشابهة لتحقيق قانون جنائي وإجرائي لحماية شبكات المعلومات الدولية، خاصة أن هذه الجرائم هي عابرة للقارات ولا حدود لها، وفي المقابل فإن عدم التعاون الدولي سيؤدي إلى زيادة القيود على تبادل المعلومات عبر حدود الدول مما سيعطي الفرصة للمجرمين من الإفلات من العقوبة ومضاعفة أنشطتهم الإجرامية.⁽¹⁾

ب - الآليات الدولية لمكافحة الجرائم المعلوماتية الماسة بالأخلاق والآداب العامة:⁽²⁾
الدول الغربية لا تهتم بالجرائم الماسة بالأخلاق والآداب العامة⁽³⁾ إلا ما تعلق بالأطفال⁽⁴⁾ لأنها دول إباحية، ولهذا وجب أن يكون هناك تعاون إقليمي بين الدول العربية والإسلامية لمكافحة هذا النوع من الجرائم الذي يهدد أخلاق مجتمعاتها.

إن المعاهدات الدولية هي الأساس الذي يركز عليه التعاون الدولي في مكافحة جرائم الانترنت ومن بينها الجرائم الماسة بالأخلاق والآداب العامة وقد عقدت العديد من المعاهدات في هذا المجال أهمها: معاهدة بودابست لمكافحة جرائم الانترنت عام 2001م.

1 - محمد عبد الله منشاي، المرجع السابق، نقلا عن: عبد الرحمن عبد العزيز الشنيفي، أمن المعلومات وجرائم الحاسب الآلي، د ن، الرياض، ط 1، 1414 هـ، ص 113.

2 - انظر: - حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الانترنت، مقال منشور على موقع المنشاي للدراسات والبحوث السابق ذكره.

3 - فقد تم مؤخرا في أمريكا إلغاء قانون العفة في الاتصالات ليتمكن الناس من الاستمرار في أعمال الإباحية دون أية قيود قانونية.

4 - فقد تمت إدانة مجرمين في أكثر من 250 جريمة في الولايات المتحدة الأمريكية خلال فترة أربع سنوات انتهت في ديسمبر 1998م تتعلق بتغريب الأطفال في أعمال إباحية أو نشر مواقع تعرض مشاهد إباحية للأطفال.
انظر: - إلياس الهاجري، جرائم الانترنت، مقال منشور على موقع المنشاي للدراسات والبحوث السابق ذكره.

إن مهمة الكشف عن الجريمة المعلوماتية صعبة وتصبح بالغة الصعوبة حين تعبر الجريمة اختصاصات قضائية لدول متعددة ذات نظم مختلفة. فالوسائل التقليدية لم تعد كافية للمكافحة. كما أن بطء الإجراءات الرسمية قد يؤدي إلى فقدان الأدلة، ولذا تشكل متابعة وحفظ سلسلة الأدلة تحدياً كبيراً، بل حتى الجرائم المحلية قد يكون لها بعد دولي فتكون هناك حاجة لطلب المساعدة من جميع البلدان التي مرت الجريمة من خلالها.

إن المساعدة الرسمية بين الدول مرهقة لأنه يتم اللجوء إليها عملاً بمعاهدات بين البلدان المعنية، وهي تشترط في الغالب أن تكون الجريمة المعنية على درجة من الجسام، وأن تشكل جريمة في كل من البلدان الطالبة والموجه إليها الطلب.

إن فعالية التحقيق⁽¹⁾ والملاحقة القضائية في جرائم الانترنت غالباً ما تقتضي تتبع اثر النشاط الإجرامي من خلال مجموعة متنوعة من مقدمي خدمات الانترنت أو الشركات المقدمة لتلك الخدمات، وحتى ينجح المحققون في ذلك عليهم أن يتبعوا أثر قناة الاتصالات بأجهزة الحاسب الآلي المصدرة والجهاز الخاص بالضحية.

وعندما يكون مقدمو الخدمات خارج نطاق الولاية القضائية للمحقق وهو ما يحدث غالباً فإن أجهزة إنفاذ القانون تكون بحاجة إلى مساعدة من ولايات قضائية أخرى (بحاجة إلى تعاون قضائي).

وأهم صور التعاون القضائي: التعاون الأمني والمساعدة القضائية.

بالنسبة للتعاون الأمني على المستوى الدولي فمن الضروري القيام بما يلي:

- السماح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي جرائم الإنترنت وتعميمها.⁽²⁾ ومن الأمثلة على ذلك:

1 - حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، مقال منشور على موقع المنشاوي للدراسات والبحوث السابق ذكره.

2 - جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة، ط، 1998م، ص 75.

* المنظمة الدولية للشرطة الجنائية (INTERPOL) والتي من بين أهدافها التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف ومدّها بالمعلومات المتوفرة لديها على إقليمها، وخاصة بالنسبة للجرائم المتشعبة في عدة دول ومنها جرائم الإنترنت.⁽¹⁾

* وعلى المستوى العربي أنشأ مجلس وزراء الداخلية العرب المكتب العربي للشرطة الجنائية بهدف تأمين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين في حدود القوانين والأنظمة المعمول بها في كل دولة، بالإضافة إلى تقديم المعونة في مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء.⁽²⁾

- القيام بالعمليات الشرطية والأمنية المشتركة لصقل مهارات وخبرات القائمين على مكافحة تلك الجرائم المعلوماتية.

أما بالنسبة للمساعدة القضائية الدولية فإنها تتخذ عدة صور منها: تبادل المعلومات، نقل الإجراءات وفق شروط معينة أهمها التجريم المزدوج، الإنابة القضائية الدولية في سماع الشهود وإجراء التفتيش وغيرها...

ونظراً لأهمية عامل السرعة في مكافحة جرائم الإنترنت فإن تعديل الاتفاقيات التقليدية للتعاون القضائي أصبح أمراً ملحاً.⁽³⁾

¹ - ومن الأمثلة عن دور الإنتربول فيما يتعلق بالجرائم المتعلقة بالإنترنت ما حصل في الجمهورية اللبنانية عندما تم توقيف أحد الطلبة الجامعيين من قبل القضاء اللبناني بتهمة إرسال صور إباحية لقاصرة دون العشرة أعوام من موقعه على شبكة الأنترنت، وذلك إثر تلقي النيابة اللبنانية برقية من الإنتربول في ألمانيا بهذا الخصوص.
انظر - حسين بن سعيد بن سيف الغافري، المرجع السابق، نقلاً عن: جريدة النهار اللبنانية عن يوم 2001/07/19.

² - المرجع نفسه.

³ - كما أبرمت العديد من الاتفاقيات الجديدة التي ساهمت في تكريس التعاون واختصار الإجراءات في مثل هذه الجرائم منها:

- معاهدة بودبست لمكافحة جرائم الأنترنت 2001م. - المؤتمر الدولي لمكافحة الاستغلال الجنسي للأطفال 1999م بفيينا.

- معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي لعام 1999 في الفقرة 2 من المادة 30 منها. - اتفاقية الرياض للتعاون القضائي 1983، المادة 15 منها. - اتفاقية شينغين 1990 في المادة 53 منها والخاصة باستخدام الاتصالات المباشرة بين السلطات القضائية في الدول الأطراف.

أما فيما يتعلق بتسليم المجرمين فقد حرصت العديد من الدول على سن التشريعات الخاصة بتسليم المجرمين، بالإضافة إلى عقد العديد من الاتفاقيات الثنائية والإقليمية والدولية التي تعنى بعملية التسليم وأهم الاتفاقيات الدولية: الاتفاقية الأوروبية بشأن الإجرام المعلوماتي لعام 2001م، التي نصت في المادة 24 منها على أن: (تطبق هذه المادة على عملية تسليم المجرمين فيما بين الدول الأطراف بالنسبة للجرائم المنصوص عليها وفقا للمواد من 2 إلى 11، ومن هذه الجرائم: الدخول غير المشروع في البيانات (م2، م4). الجرائم المتعلقة بالأعمال الإباحية وصور الأطفال الفاضحة (م9)، الشروع والمساعدة والتحريض (م11).

إن التقدم الهائل في تكنولوجيا الإعلام الآلي وظهور أنماط جديدة من الجرائم أصبح كما هو ملاحظ في الواقع العملي يشكل عبئا ثقيلا على عاتق جميع أجهزة العدالة الجنائية سواء رجال الضبط القضائي أو رجال التحقيق أو المحاكم على مختلف درجاتها. لذلك لا بد أن تكون هذه الأجهزة على درجة كبيرة من الكفاءة والمعرفة والقدرة على كشف غموض تلك الجرائم والتعرف على مرتكبيها بسرعة ودقة متناهيين، وهذا لن يتحقق إلا بالتدريب والتكوين المستمرين.⁽¹⁾ وما من دولة يمكنها بمفردها النجاح في مواجهة هذه الجرائم بمفردها دون تعاون وتنسيق مع غيرها من الدول لتطوير أساليب الوقاية والمكافحة بأساليب تتناسب وتفيق أساليب المجرمين الذين عادة ما يمتازون بالذكاء والاحترافية.

ج- صعوبات التعاون الدولي لمكافحة الجرائم المعلوماتية الماسة بالأخلاق والآداب العامة:

ورغم جهود التعاون الدولي السابقة الذكر، إلا أن هناك صعوبات لا زالت تواجه التعاون الدولي لمكافحة جرائم الانترنت أهم هذه الصعوبات:

- تنوع واختلاف النظم القانونية الإجرائية، إذ قد تكون قانونية ومشروعة في دولة (ذات فائدة)، وغير قانونية في دولة أخرى (عديمة الفائدة).

انظر: - حسين بن سعيد بن سيف الغافري، المرجع السابق.

¹ - حسين بن سعيد بن سيف الغافري، نقلا عن: هشام فريد محمد رستم، الجرائم المعلوماتية، " أصول التحقيق الجنائي الفني"، بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة بتاريخ 2000/05/03م، المجلد 2، ط2، 2004م، ص439، 440.

- عدم وجود قنوات اتصال بين الدول يعيق الحصول على المعلومات والبيانات المتعلقة بالجريمة والمجرمين وبالتالي يعيق التصدي لهم.

- مشكلة الاختصاص في الجرائم المتعلقة بالإنترنت، وذلك على المستوى الدولي حيث يوجد اختلاف التشريعات والنظم القانونية والتي قد ينجم عنها تنازع في الاختصاص بين الدول بالنسبة لجرائم الإنترنت العابرة للحدود.

فقد يحدث أن ترتكب في إقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى استناداً إلى مبدأ الإقليمية، وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى فتدخل عندئذ في اختصاصها استناداً إلى مبدأ العينية.⁽¹⁾

كما تثار فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الإقليمية، كما لو قام الجاني ببث الصور الخليعة ذات الطابع الإباحي من إقليم دولة معينة وتم الإطلاع عليها في دول أخرى ففي هذه الحالة يثبت الاختصاص وفقاً لمبدأ الإقليمية لكل دولة من الدول التي مستها الجريمة.⁽²⁾

وهناك مشكلة التجريم المزدوج، وهو من أهم الشروط الخاصة بنظام تسليم المجرمين. لأن الكثير من الدول لا تجرم جرائم الإنترنت ومعظمها لا يجرم جرائم الإنترنت الماسة بالأخلاق والآداب العامة. وهذا يعيق تسليم المجرمين ومحاكمتهم وبالتالي يعيق التعاون الدولي في مكافحة هذا النوع من الجرائم.⁽³⁾

كما أن التعاون القضائي أو ما يسمى بالمساعدات القضائية تتم بالطرق الدبلوماسية وهذا ما يجعلها بطيئة ومعقدة، وهذا يتعارض مع طبيعة الإنترنت وجرائمها وما تتميز به من سرعة.⁽⁴⁾ وللقضاء على ما سبق ذكره من المعوقات من الضروري محاولة توحيد النظم القانونية والنظم الإجرائية في هذا النوع من الجرائم بالاتفاقيات الدولية، وتعديل النظم الداخلية لتتوافق قدر الإمكان مع النظم

1 - جميل عبد الباقي الصغير، الجوانب الإجرامية للجرائم المتعلقة بالإنترنت، المرجع السابق، ص 73

2 - حسين بن سعيد بن سيف الغافري، المرجع السابق.

3 - المرجع نفسه.

4 - المرجع نفسه بتصرف.

الأخرى ومع النصوص القانونية الدولية. وإبرام اتفاقيات دولية ثنائية أو جماعية يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الاختصاص القضائي والمساعدة القضائية وتسليم المجرمين وتدريب الإطارات، خاصة بالنسبة لجرائم الإنترنت التي تتطلب السرعة.

خاتمة:

- من أهم النتائج والاقتراحات المتوصل إليها في نهاية هذه المداخلة ما يلي:
- ضرورة مساهمة المسؤولين والتربويين والإعلاميين وخطباء المساجد والمؤسسات العلمية وكافة شرائح المجتمع في مواجهة الجرائم الماسة بالأخلاق والآداب العامة عبر الإنترنت.
- لا بد من إعطاء هذه الجريمة قدرا من الاهتمام يتناسب مع حجم الخطر الذي تشكله اتجاه المجتمع، اهتمام بدعم جهود المكافحة ماديا ومعنويا.
 - إن حماية شبكة الانترنت من التلوث الأخلاقي يستوجب ما يلي: الرقابة المستمرة على المواقع، وضع أخلاقيات للانترنت، سن قوانين تشريعية تتعلق بمحتوى هذه الشبكة العالمية، وضع مشرفين على المواقع لمراقبتها، سن تشريعات عربية خاصة بمحتويات الانترنت ومكافحة الجرائم المتعلقة بها، وضع أخلاقية عربية تحدد التعامل مع الانترنت.
 - مسؤولية ضبط أخلاقيات الانترنت تقع على المختصين في المعلوماتية ثم بأفراد المجتمع والجمعيات والهيئات المهتمة بالانترنت.
 - ترشيح وحجب المواقع المسيئة للأخلاق والمنافية للآداب.
 - استحداث الشرطة المعلوماتية وتدريبها على الوسائل الحديثة في التحقيق والكشف عن مرتكبي هذه الجرائم محليا وعربيا.
 - إنشاء خطوط خضراء للمواطنين للإبلاغ عن المواقع الإباحية ومواقع التشهير.
 - تدعيم التعاون الدولي في مجال مكافحة جرائم الانترنت الماسة بالأخلاق.
 - ضرورة نشر الوعي بين المواطنين بمخاطر المواقع اللاأخلاقية على الانترنت، وإدخال مادة أخلاقيات استخدام الانترنت ضمن المناهج الدراسية.
 - تفعيل دور المجتمع المدني في مكافحة تلك الجرائم.

الجريمة الالكترونية و أولوية حماية الحلقة الضعيفة (الطفل) في القانون الجزائري

د/ عبد المجيد صغير بيرم

كلية الحقوق والعلوم السياسية - جامعة المسيلة

مقدمة:

تتعدّد وتنوّع أشكال الحماية القانونية والاجتماعية و القضائية للفرد من طرف الحكومات في ظل اتساع رهيب للجريمة الالكترونية بفضل اتساع دائرة الاستعمال الجماهيري واسع النطاق لوسائط التواصل الاجتماعي لكونها أصبحت أكثر جماهيريّة وتمشياً مع تطلعات الكثير من المواطنين لمزيد الاطلاع والتواصل مع الغير داخل وخارج الدائرة الوطنية(المحيّة) وبالخصوص الشباب منهم، وبغض النظر، عن الجنس و السن(العمر) والمكانة و/أو الوسط الاجتماعي للفرد، وذلك كلّ بفضل التنافسية الموجودة بين مختلف شركات الهاتف الجوّال(سعرا و مساحة واسعة في مجال الاستعمال الترفيهي و التعليمي والثقافي والتوصلي بين مختلف شرائح المجتمع الواحد و المتعدد كذلك) من جانب ومن جانب ثان فقد تحوّل الاتصال الالكتروني أقلّ تكلفة ماديّة و متوفر لدى شرائح واسعة في عالمنا العربي بصفة عامة و في الجزائر بصفة خاصة، كما أن استعمالاته في الحياة اليومية للفرد أضحت لا حدود لها بفضل التنافسيّة بين أكبر منتجي الحواسب الالكترونية والهواتف الذكيّة في العالم.

تتمثل الاشكالية كالآتي: ما هي طبيعة الردع الاجتماعي و القانوني للجريمة الالكترونية الماسّة بالحلقة الضعيفة (الطفل) في ظل الأزمات الاقتصادية و الاجتماعية للدولة الوطنية؟

فضلت معالجة الاشكالية المثارة أعلاه ضمن محور واحد ضمّنته عديد العناصر رأيت ضرورة التعرّض لها بالتحليل والمناقشة و المقارنة وبعنوان رئيس: "الحماية القانونية و الاجتماعية للحلقة الضعيفة في المجتمع في القانونين الوطني و الدولي ظل الخطر الالكتروني المتزايد". وجاءت عناصر هذا المحور على النحو الآتي: - أولا: الجريمة الالكترونية: التعريف ودور قانون العقوبات في الحد من الجريمة الالكترونية؛ - ثانيا: واقع وتحديات التجربة الجزائرية في مجال محاربة الجريمة الالكترونية. وبالإضافة إلى خاتمة أوردت فيها مجموعة من الاقتراحات رأيت ضرورة المساهمة من خلالها في النقاش الدائر حول

أهمية توسيع دائرة الحماية القانونية للطفل باعتباره المستهدف رقم واحد من قبل مقترفي الاجرام الالكتروني.

-أولا: الجريمة الالكترونية: التعريف ودور قانون العقوبات في الحد من الجريمة الالكترونية.

يقف المتتبع للتطور التكنولوجي في مجال الاستخدام الالكتروني على حقيقة أنه، وبقدر ما كان لهذا التوسع للاستعمال الالكتروني بمختلف وسائطه ووسائله وأنماطه في حياة الفرد اليومية(تعلima و ترفيهها و تثقيفا و تلبية للحاجيات اليومية)،مجتمعات متطورة و نامية على حد سواء،من ايجابيات لا يصح نكرانها على الأفراد والمجتمعات الذكية،إلا أن العصابات الإجرامية بمختلف أشكالها وتنوعها(جريمة عابرة للقارات، وتجارة للمخدرات، وتجارة الرقيق الأبيض، والاتجار بالبشر، وشبكات تهريب البشر، وكذلك في مجال تمويل الإرهاب و تجنيد الأطفال) لم تترك هذا القطاع الاتصالي-الرقمي دون استعمال اجرامي منّ الحلقات الضعيفة(الطفل) في المجتمعات دون تمييز.

ومن منطلق أنه لا يمكن، وبأي حال من الأحوال، فهم مكونات الجريمة الالكترونية إلا بعد أن نقوم بتعريف لعلم الإجرام(Les Sciences criminelles ou Criminologie) الذي اختلف تعريفه من فقيه إلى فقيه ثان، كل يعرّف علم الإجرام من زاويته الخاصة، أو من منطلق إيديولوجيته،أو من قاعدة الانتماء لمدرسة اجتماعية(إسلامية أو ماركسية أو ليبرالية أو علمانية)،فضلت التقسيم الآتي لهذا الجزء من الدراسة.

1:علم الإجرام:التعريف و العلاقة بقانون العقوبات كقانون رادع.

لا يمكن لأي باحث في عالم الاجرام و/ أو في المنظومة العقابية للدولة غض الطرف عن أهمية معالجة التعاريف المختلفة لعلم الاجرام بالإضافة إلى دور قانون العقوبات المحيّن في الحد من الجريمة الالكترونية التي أصبحت انشغالا رئيسا لحكومات الدول على الصعيد العالمي.

1-1: تعريف علم الاجرام.

وقع اختياري على عديد التعاريف لعلم الاجرام أرى ضرورة وأهمية ذكرها و الكتابة بشأنها تحليلا ومقارنة وتوضيحا بغرض تعميم الفائدة البحثية و في مقدمتها تعريف الدكتور إسحاق إبراهيم منصور(أستاذ جامعي دّرس بجامعة وهران) في مؤلف أصدره بالجزائر سنة 1979¹ جاء على هذا النحو: هو"العلم الذي يدرس الجريمة كظاهرة اجتماعية احتمالية في حياة الفرد، وحتمية في حياة

¹ - اسحاق إبراهيم منصور:الموجز في علم الإجرام والعقاب،ديوان المطبوعات الجامعية، الجزائر، 1979،ص:7.

المجتمع، ويتقصى أسبابها الفردية و الاجتماعية للتوصل إلى القضاء عليها أو الحد منها". ويلتقي هذا التعريف للجريمة و تصديق المؤتمر الدولي الثاني للجرائم (باريس 1950) على تعريف مضمونه الآتي: "إن علم الاجرام هو الدراسة العلمية لظاهرة الإجرام و إن موضوعه هو دراسة أسباب الظاهرة الإجرامية وسبل علاجها"¹.

وفي الإطار ذاته يقترح علينا الدكتور محمد خلف (من جامعة بنغازي-ليبيا) تعريفاً أراه يضيف توضيحاً إضافياً لعلم الإجرام لتضمنه عناصر أساسية لمعرفة علم الاجرام جاء على هذا النحو: هو "العلم الذي يدرس الجريمة بوصفها ظاهرة فردية واجتماعية، ويكشف العوامل المسببة لها، ويعمل على تلافيها"².

ومن التعاريف التي لا يمكن لأي باحث في علم الإجرام، وبأي حال من الأحوال، غض الطرف عنها التعريف الذي ضمنه الدكتور إسحاق إبراهيم منصور في مؤلفه المذكور أعلاه أذكر تعريف الدكتور محمود نجيب حسني (في مؤلف له بعنوان: أسباب في علم الاجرام) لعلم الاجرام على أنه "العلم الذي يدرس أسباب الجريمة كظاهرة فردية واجتماعية ليحدد القوانين المنطقية التي تحكمها وتفسرها في مظاهرها المتنوعة"³.

نستشف من نص التعاريف التي اشرنا إليها أعلاه لعلم الإجرام أن الجريمة هي ظاهرة اجتماعية صرفة وذات دلالات ومفاهيم اجتماعية وأخلاقية و قانونية وجدت مع وجود المجتمعات البشرية والتجمعات السكانية، ولنا مرجع في أول جريمة ارتكبتها الإنسان (قابيل وهابيل)، وهي باقية، و متصاعدة، و متنوعة، و متعددة مع وجود البشر واختلاف مزاجه وتنشئته الاجتماعية، بل نجدها تنمو كما تنمو المجتمعات وبالتالي فإن المجتمعات الحديثة مطالبة بتفسير مسببات الفعل الإجرامي باعتبارها ذي منشأ اجتماعي. فالجريمة، وبمختلف أنواعها و مفاهيمها، كانت موجودة كما كانت محل اعلان وشبه ترويج منذ أن اكتشف العالم الإذاعة و التلفزيون والصحيفة المكتوبة، أي أنّها كانت موجودة قبل أن يكتشف الحاسوب، والهاتف الذكي، و الاتصالات عن طريق الأقمار الصناعية

¹ - محمد خلف: مبادئ علم الإجرام، الطبعة الثالثة، الشركة العامة للنشر والتوزيع والإعلان، بنغازي، ليبيا، 1978، ص: 7.

² - المرجع نفسه، ص: 17.

³ - المرجع نفسه، ص: 16.

والألياف البصريّة منذ تاريخ الانفجار العلمي في مجال الاتصالات (بداية السبعينات من القرن الماضي).

إن الفعل المجرّم (L'Acte incriminé) في أي مجتمع يعالج من باب الاحتمالية والتوقع (توقع حدوثه في أي وقت إذا ما توفرت له الظروف). وبالنتيجة فإن "الجريمة ملازمة لكل مجتمع ولا نجد مجتمعا خلوا منها مهما ارتقى في سلم الحضارة و المدنية"¹. هذا ومنذ تاريخ بزوغ مفهوم الدولة بعد انهيار الإمبراطوريات الغربية التي كانت سببا في قيام الحرب العالمية الأولى (1914-1918) على وقع الثورات الشعبية ضد الحكم الملكي الذي كان قائما على "الانتماء لتستبدل بالشرعية الديمقراطية على الانتخابات"² و انتشار أفكار دافيد إميل دوركايم (1858-1917)³ الذي اعتبر "الجريمة ظاهرة اجتماعية وضرورة حتمية في كل مجتمع وعلامة صحة من علاماته"⁴، يسجل أن الدول تسعى عبر ترسانتها القانونية إلى القضاء أو الحد من الجريمة⁵، ومن هذا المنطلق جاء في الدستور الجزائري أنه: "لا ادانة إلا بمقتضى قانون صادر قبل ارتكاب الفعل المجرّم"⁶ كما أنه: "لا يتابع أحد، ولا يوقف أو يحتجز، إلا ضمن الشروط المحددة بالقانون، وطبقا للأشكال التي نص عليها. الحبس المؤقت اجراء استثنائي يحدد القانون أسبابه ومدته وشروط تمديده. يعاقب القانون على أعمال وأفعال الاعتقال التعسفي"⁷.

¹- محمد خلف: مبادئ علم الإجرام، ص: 7.

²- محمد فاروق الباشا: التشريعات الاجتماعية (قانون العمل)، الطبعة السادسة منقحة، منشورات جامعة دمشق، 1991، ص: 32.

³- وهو أحد مؤسسي علم الاجتماع الحديث (David Émile DURKEIM) و من أهم مؤلفاته: - في تقسيم العمل؛ - تربية وعلم الاجتماع.

⁴- محمد خلف: مبادئ علم الإجرام، مرجع سابق، ص: 7.

⁵- تذكر بعض التقارير الموثوق بها صادرة عن هيئة الأمم المتحدة أن الدولة الوحيدة التي تمكنت من تقليل الجريمة في مجتمعها هي دولة اليابان بفضل اعتمادها لبرنامج وطني متكامل (اجتماعيا و اقتصاديا ورعاية للأفراد بالإضافة إلى الردع القانوني و تغليظ العقوبات على مرتكبي الأفعال المجرّمة الماسة بالأطفال و المرأة و المسنين.

⁶- المادة 58 من الدستور الجزائري لعام 2016 (القانون رقم: 16-01 المؤرخ في 06 مارس 2016، الجريدة الرسمية للجمهورية الديمقراطية، العدد: 14، التاريخ: 07 مارس 2016).

⁷- المادة 59 من الدستور الجزائري لعام 2016.

هذا وقد جاء قانون العقوبات الجزائري المعدل والمتمم مؤكداً على التوجه الدستوري القائم على الاستشراف القانوني في مجال الفعل المجرّم عبر التنقيص بصريح العبارة على أنّه: "لا جريمة ولا عقوبة أو تدابير أمن بغير قانون"¹. وبما أن الجريمة الالكترونية هي في حد ذاتها مجموعة أفعال تقع تحت طائلة المتابعة القضائية (قانون الاجراءات الجزائية) والعقاب (قانون العقوبات) يقوم بارتكابها فرد أو مجموعة أفراد الغرض منها إلحاق الضرر المادي و المعنوي بالأشخاص الطبيعيين والاعتباريين، فإن البحث في مضامينها يتطلب توضيح الآتي:

-إنّ الجريمة الالكترونية، هي وفي المقام الأول، انحراف مقصود من قبل فرد و/أو مجموعة أفراد تشكلوا في شكل عصابة أو مجموعة أشرار، واجتمعوا على استعمال ما توفره الأداة الالكترونية (حاسوب و/أو هاتف ذكي) لكي يلحقوا ضرراً مادياً و/أو معنوياً لفرد و/أو لمجموعة في مجتمع معيّن، وقد يكون الفرد و/أو المجموعة تدير الفعل المجرّم من داخل و/أو من خارج الإقليم وبالتالي فإن الجريمة الالكترونية لها خاصيّة التحرك من داخل الإقليم (الوطن - الدولة) و/أو من خارج حدود الدولة، ومن هنا تتأتى الصعوبة بالنسبة للمشرع الوطني في تعقب الجريمة الالكترونية دون المساعدة الدولية. ومن خلال ما تقدّم فإنّه يقع على عاتق المشرع الوطني توقع حدوث أفعال تدخل في خانة "الاجرام.. Le Crime" في مجتمعه و ذلك من منطلق أن الفعل الاجرامي هو في حد ذاته فعلاً غريباً، إذ أن المجتمعات لمرحلة ما قبل الحداثة (الاكتشافات العلمية التي قلبت حياة الفرد رأساً على عقب) تعرّفت، وبدورها، على أشكال إجرام فاضحة وشديدة القسوة والهمجية، وذلك قبل أن يبتكر الإنسان الهاتف السلكي واللاسلكي والكهرباء و النقل بالسكك الحديدية و النقل الجوي. فالفعل الاجرامي ليس مقتصرًا على المجتمعات الفقيرة دون المجتمعات الغنية التي قد تحقق حكوماتها وطبقتها السياسية الحاكمة لشعوبها مستويات معيشية مرموقة بالنظر لما هو متوفر لشعوب أخرى.

1-2: دور قانون العقوبات في الحد من الجريمة الالكترونية.

يعكس اهتمام الحكومات، وبالأخص في منطقتنا العربية، وبدعم من هيئة الأمم المتحدة و المنظّمات الدّولية و الإقليمية المعنية بموضوع الجريمة التي لم تعد جريمة وطنية وحسب، بل أصبحت

¹ -المادة الأولى من قانون العقوبات الجزائري المعدل و المتمم (آخر تعديل وتنظيم: القانون رقم: 16-02 المؤرخ في 19 يونيو -جوان- 2016، الجريدة الرسمية للجمهورية الجزائرية، العدد: 37، التاريخ: 22 جوان 2016).

جريمة عابرة للأوطان والسيادة الوطنية بفضل اتساع دائرة الاتصالات الحديثة التي جعلت العالم عبارة عن قرية صغيرة، رغبة كل سلطة سياسية حاكمة في توفير الشروط الموضوعية المساعدة لحماية مجتمعها من الآثار السلبية لعولمة الاتصالات على مصراعيها (الانترنت، والفيسبوك، والتويتر، والمسنجر، والسكايب، وإلى غير ذلك من المستحدثات الجديدة التي قد توفرها الشركات متعددة الجنسية في هذا المجال مستقبلا) وانفتاح الأسواق المحليّة على ما هو خارجي (سلعا، و يد عاملة من الجنسین، وتجارة مشروعة و غير مشروعة).

يقف الباحث في علم الاجرام على حقيقة التأثير والتأثر بين هذا العلم (Criminologie) الذي هو "العلم الذي يشمل جميع الأبحاث والدراسات المتعلقة بالجريمة والجرم والبيئة وأسباب الاجرام والوقاية منها وقمعها"¹ وبين العديد من العلوم الاجتماعية و النفسية و الاقتصادية و السلوكية الأخرى التي لها تأثيرها سلبا أم إيجابا في سلوك الفرد و/أو المجموعة لكون الجريمة لم تعد فعلا فرديا فقط، بل أصبحت، وفي معظم الجرائم الالكترونية الماسة بالأفراد والجماعات في المجتمع، فعلا جماعيا يقوم على تقسيم دقيق، وتوزيع وفق إمكانيات و قدرات كل فرد، وتحديد منهجيّ لتدخل كل فرد في ارتكاب الفعل المجرّم.

و لا أفتشي سرا إذا قلت أن الجرائم البشعة يحدث الكثير منها في المجتمعات الغربية المتقدمة اقتصاديا و تكنولوجيا و لديها هيئات وهياكل تكفل اجتماعي قويّة وممتدة إلى أبعد منطقة سكنية في البلد. لقد ظهرت الجريمة الالكترونية في البلدان المتقدمة التي شهدت انفجارا في الاستعمال واسع النطاق للأجهزة الالكترونية قليلة التكلفة (أسعارها أصبحت في متناول أغلب الشرائح المهنية و الاجتماعية و العمرية) حتى في أبسط الخدمات، بل وأنها انتشرت، وبشكل رهيب ومخيف، لم يسلم منها الطفل، و المرأة، و الموظف، الأمر الذي استدعى تدخل المشرع إلى تسريع وتيرة اصدار النصوص القانونية بغرض احتواء الفعل الاجرامي حتى لا يخل بالنظام الاجتماعي العام للدولة. وإنّ ما يميز المجتمعات الحديثة، ومنهم مجتمعنا الجزائري و المجتمعات العربية و بدرجات متفاوتة، أنهم يسارعون لتكييف تشريعاتهم الأساسية وفق متطلبات كل مرحلة ودون تسويق و تأخير وتأجيل.

¹- وهو التعريف الذي عرّف به الفقيه ميس فورو (Mice Foro) علم الاجرام (أورد هذا التعريف الدكتور

محمد خلف، مرجع سبقت الاشارة إليه، ص: 17).

لقد اعتقد البعض منا و لمدة طويلة أن الجريمة الالكترونية العابرة للأوطان أو السيادات الوطنية سوف لن تصل مجتمعنا الجزائري و المجتمعات العربية والشمال أفريقية، وأن لدينا مناعة تحفظ شخصيتنا الوطنية الضاربة في التاريخ والمشبعة حضاريا وثقافيا، لكن، ومع انفتاح مجتمعنا على الخارج بعد تسعينيات القرن الماضي وسيما بعد التعديل الدستوري العام 1989، بدأت رياح التأثير تحتاحنا أفرادا و مجموعات منها ما هو ايجابي، و منها كذلك ما جاء محملا بسموم الحضارة المادية الغربية القائمة على علو المصلحة الفردية(المنفعة الشخصية للفرد تعلو على مصلحة الجماعة بأي حال من الأحوال).

وإذا كان علم الاجرام يقوم على فروع علمية أساسية(العلوم الإنسانية الجنائية،وعلم النفس الجنائي، وعلم الاجتماع الجنائي،وبالإضافة إلى فروع جديدة جاءت كاستجابة لرغبة المجتمعات الحديثة استحداثها للرد على تنوع وتعدد أنواع الجريمة الالكترونية التي لم يسلم منها الطفل،فإن المشرع الوطني لم يكن له منفذا إلا تعديل وتتميم قانون العقوبات لتواكب قواعده القانونية الملزمة للأفراد والمؤسسات والشركات تحت تهديد الجزاء الجنائي في حالة اقتراف الفعل المجرم، وذلك كله بغرض القضاء أو الحد من الظاهرة الاجرامية الالكترونية على الأقل.

2: موقف المنظمات الدولية و الإقليمية من حماية الطفل في ظل التهديد الالكتروني المتصاعد.
لم يتوقف مسعى المجتمع الدولي الذي بدأ التأسيس له مباشرة بعد أن وضعت الحرب العالمية الأولى(1914-1918) أوزارها عبر الاعلان عن انشاء عصبة الأمم (La Société des nations) التي كلفت بتثبيت السلم العالمي والتأسيس لعلاقات دولية جديدة بعيدة من الحروب المدمرة والصراعات بين الدول العظمى آنذاك، بالإضافة إلى الدعوة إلى مزيد الحماية الاجتماعية للأمم و الطفل في ظل مجتمع جديد يقوم على المساواة الحقوقية والاقتصادية و الاجتماعية بين الأفراد بغض النظر عن الجنس واللون و الأصل الاجتماعي. ومن الأسئلة التي واجهت المجتمع الدولي لمرحلة ما بعد الحرب العالمية الأولى التي كبدت الشعوب خسائر مادية و بشرية جسيمة كان الطفل وقودا و ضحية: -كيف لنا كمنظمات مجتمعية أن نحمي الحلقات الضعيفة(المرأة و الطفل) من الاستغلال الاقتصادي؟ و ما هي سبل العمل على الصعيد الدولي من أجل تكريس مبدأ إن العمل ليس بسلعة؟

2-1: منظمة العمل الدولية و أشكال استغلال الطفل في ظل الخطر الالكتروني.

وكنتيجة لهذا التوجه العام المشبّع بقيم ومبادئ الحرية، والاقتصاد الاجتماعي، وأولوية حماية المرأة و الطفل، أعلن عن انشاء منظمة العمل الدولية العام 1919 (وهي منظمة ثلاثية التمثيل والتشكل - عمال وأصحاب عمل وحكومات-)، وهي المنظمة الدولية التي تمكنت، وبعد جهد معياري واسع النطاق تناول كل ما قد يعتبر سعيًا دوليًا من أجل حماية الأطفال من مختلف أشكال الاستغلال المباشر وغير المباشر وبالخصوص بعد الانتشار الواسع للجريمة الالكترونية، من إقناع ممثلي أطراف الانتاج من التصديق على أهم وأحدث اتفاقية دولية سنة 1999 عرفت باتفاقية محاربة ومقاومة أسوأ أشكال عمل الأطفال (الاتفاقية رقم: 182) المشفوعة بالتوصية رقم: 190 لعام 1999¹، وقد تحدد الهدف من اصدار الاتفاقية دفع وتشجيع ومرافقة الحكومات على امتداد العالم من أجل القضاء على مختلف أشكال الاستغلال (أسوأ أشكال العمل)، بما في ذلك الرق، وعبودية الدين، والعمل الجبري، والاستغلال لأغراض الدعارة، وكل ما قد يدخل في خانة الاتجار بالبشر. يعكس هذا الاهتمام بأولوية توفير شروط الحماية الجزائية للطفل في ظل عولمة الاقتصاد، من قبل أكبر وأهم منظمة دولية تعنى بعالم الشغل والتشغيل (للجنسين) أن مخاطر الاستعمال الالكتروني في مسائل العمل (التشغيل من بعد، وإدارة شبكات إنتاج من خارج الدولة، واتساع ابرام اتفاقيات عمل عن طريق الهاتف.. إلخ) كانت موجودة وموجودة بكثرة، لكن المخاطر قد تضاعفت، وازداد حجمها، واتسعت درجتها بعد الثورة التكنولوجية في مجال الاتصالات منذ تسعينيات القرن الماضي. هذا وقد سبق لمنظمة العمل الدولية ان أصدرت اتفاقية دولية لحماية الأمومة سنة 1952 (الاتفاقية رقم: 103) و قد تم مراجعتها سنة 2000 وتوصي بحماية الأمومة للمرأة العاملة في الشغل.

يخلص الباحث في المنظومة المعيارية الدولية في ظل انفتاح الأسواق، وبروز أشكال عمل (شغل) جديدة في ظل اتساع الرقمنة، و الاستعمال الالكتروني في مجالات كانت تدار بشكل كلاسيكي بعيدا عن الرقمنة، أنه، و من أهم التحديات التي أصبحت تواجهها مجتمعات العمل أذكر حالتين:

¹- أصدرت منظمة العمل الدولية (مؤتمر العمل الدولي-1998) الاعلان العالمي بشأن المبادئ والحقوق الأساسية في العمل تضمن مجموعة من الاتفاقيات الدولية (8) تضمنت مجموع معايير العمل في مجال القضاء على التمييز وحرية الوظيفة و القضاء على أشكال العمل الازامي و الجبري و تشغيل اطفال. الجزائر، ومن منطلق عضويتها بمؤتمرات العمل الدولية منذ سنة 1962، صدقت على معظم الاتفاقيات الدولية التي أصدرتها المنظمة.

-الأولى و تتمثل في تشغيل الأطفال و الأثر الذي تحدثه وسائط الاتصال الالكتروني من تسهيل وتيسير وهكذا تشغيل مناف للأعراف والتشريعات الاجتماعية الوطنية للدول المنضوية تحت لواء منظمة العمل الدولية؛

-والحالة الثانية والمتمثلة في مخاطر الاستعمال الالكتروني لحالات واسعة للتجار بالأطفال بغرض الاستغلال الجنسي و"دعارة الأطفال".
تتحدّد مخاطر الحالة الأولى في الآتي:

-ازدياد مخاطر الاستعمالات الالكترونية في مجال التشغيل غير المنظم بعيدا عن الرقابة الحكومية و احترام شروط التشغيل المنظم وبالخصوص ما يتعلق باستغلال الأطفال(عمالة الأطفال) في قطاعات وعرة و دون أدنى احترام لسنهم و خصوصيتهم.وهنا لا بد من الإشارة أن الاستغلال كان موجودا قبل تاريخ استفحال الثورة التكنولوجية(الاستغلال التقليدي للأطفال في أعمال شاقة إلا أن دخول المعاملات الالكترونية كآلية اتصال مضمونة و يمكن إفلات مستعملها من الرقابة الحكومية و الأمنية قد أسهم في اتساع دائرة الاستغلال للأطفال في العالم.

وفي هذا الإطار حدد تقرير صادر عن مكتب العمل الدولي التابع لمنظمة العمل الدولية بعنوان:"مستقبل خال من عمل الأطفال" سنة 2002(هذا التقرير صادر سنة 2002 و ليس سنة 2019)¹ أشكال الأعمال الخطرة التي تدخل في خانة الاستغلال:

-العمل(الشغل) الذي يؤدّيه طفل لم يبلغ الحد الأدنى للسنّ والذي تحدّده التشريعات الوطنية أو المعايير الدولية وفقا لنوع العمل المحدّد²(المشرع الجزائري سبق نظراءه على امتداد المنطقة العربية و المغربية و الافريقية في الموضوع المتعلق بتحديد سن التشغيل ب:16 سنة وربطه بالتكوين و التأهيل المهنيين-راجع نص المادة:15 من القانون رقم:90-11 المؤرخ في 21 أفريل 1990 والمتعلق بعلاقات العمل، المعدل والمتمم)؛

¹-التقرير نشرته مجلة عالم العمل، الطبعة العربية، منشورات مكتب العمل الدولي، العدد 43، أوت 2002، جنيف، سويسرا، ص:4-7.

²-المرجع نفسه، ص:7.

-العمل الخطر الذي يهدّد صحّة الأطفال الجسدية و العقلية و المعنوية، إما بسبب طبيعة هذا العمل، أو بفعل الظروف التي ترافقه¹(المشرع الجزائري منع منعاً باتاً تشغيل الأطفال بل وجّرم التشغيل دون 16 سنة الذي ربطه بالتكوين و التمهين لا بالتشغيل الكامل).

وليس سرا القول أن حالات الاستغلال للأطفال في العالم قد تضايفت منذ هذا التقرير الصادر سنة 2002 بالنظر للأزمات الاقتصادية التي هزت عديد الدول بسبب برامج الهيكلة الاقتصادية وخصوصية قطاعات واسعة من النسيج الاقتصادي العمومي بتأطير من المؤسسات المالية العالمية(صندوق النقد الدولي، والبنك الدولي، والمنظمة العالمية للتجارة) المعروفة باسم مؤسسات بروتون ودز(Les Institutions de Bretton-Woods)².

2-2: منظمة العمل العربية و أشكال استغلال الطفل في ظل الخطر الالكتروني.

سعت جامعة الدول العربية المنبثقة عن اللجنة الاقتصادية و الاجتماعية على مستوى جامعة الدول العربية منذ تاريخ تأسيسها بالقاهرة سنة 1970 إلى التأسيس لمنظومة قانونية(معياريّة) في مجال حماية الطفل في العالم العربي بالرغم من التأثير السلبي للخلافات العربية-العربية في أعمالها و إلى يومنا هذا.

ومن منطلق أن العالم العربي ليس جزيرة معزولة فقد تأثرت مجتمعاته و بدرجات متفاوتة بالنظر لخصوصية كل مجتمع وتجاربه التنموية و الاقتصادية، قلت تأثرت بالتطور التكنولوجي العابر للقطاعات والأوطان، وتفاعل الأفراد والمؤسسات والشركات و الجماعات السكانية مع هذا الوافد الجديد في حياة الفرد العربي، كل حسب ما توفر لديه من إمكانيات مادية وتسهيلات حكومية للولوج إلى أحدث الوسائط الالكترونية.

والنتيجة من كل ما ذكرته أعلاه أن ظهرت الآثار السلبية للمعاملات الالكترونية، وبفضل اتساع دائرة الاستعمال المفرط غالبا لوسائط الاتصال، على سلوك الأفراد والجماعات السكانية فبدأنا نسجل أفعالا مجرّمة بل شاذة تدخل في خانة "الاجرام" المعاقب عليه قانونا(قانون العقوبات)،بالإضافة إلى بروز أفعال جديدة لم تكن المجتمعات العربية الكلاسيكية والمحافظة في معظمها تعرفها بشكل علني، أو أنّها كانت موجودة لكنه كان يتم التستر عنها لأسباب مجتمعية و

¹-المرجع نفسه،ص:7.

²- نوري منير: السياسات الاقتصادية في ظل العولمة، ديوان المطبوعات الجامعية، الجزائر، 2010، ص:86-91.

ثقافية ودينية ومنها:- تشغيل الأطفال من هم دون السادسة عشر عمرا بل وأقل من ذلك في التجارة(الأعمال التجارية غير المشروعة بحجة حاجة عائلة الطفل لمدخل تعيل به نفسها) وأطفال المساكن(تشغيل القاصرات في البيوت) وما يلحق هذا التشغيل من حالات الاستغلال الجنسي للمراهقات؛- تشغيل الأطفال في الأعمال التجارية والصناعية و الخدمية الشاقة تحت ذريعة الحاجة الاقتصادية الملحة للعائلات.

هذا و قد تناولت دراسة أكاديمية متكاملة بعنوان:"عمل الأطفال في الدول العربية: رصد الواقع و تقييم الانجاز" أنجزتها الدكتورة ناهد رمزي (مستشار بالمركز القومي للبحوث الاجتماعية و الجنائية بجمهورية مصر العربية) نشرته مجلة العمال العرب التابعة للاتحاد الدولي للعمال العرب(دمشق- سورية) سنة 2009¹ أهم التحديات التي تواجهها الطفولة في العالم العربي الذي لم يتمكن أغلب دوله من ضبط الاحصائيات المتعلقة بالتشغيل الجبري (الجبري) على مستوى هذه الدولة أو تلك. ومن أسباب عدم دقة الاحصائيات المتعلقة بعمالة الأطفال على امتداد العالم العربي تذكر الدراسة الآتي:-عدم التزام معظم الدول العربية بالاتفاقيات والمواثيق الدولية التي وقعت عليها؛-التجاء عديد الدول العربية إلى إخفاء الحجم الحقيقي انسب الأطفال العاملين؛-وجود قطاع اقتصادي وخدمي و فلاحي وداخل نطاق الأسرة غير رسمي(يشغل و يشتغل بعيدا عن الرقابة الحكومية و أجهزتها الرقابية.

وفي ظل غياب الاحصائيات الدقيقة في علمنا العربي بشأن آثار الجريمة الالكترونية في الاخلال بتوازن المجتمع تبقى المطالبة بضرورة عناية السلطات العمومية بالمخاطر المحدقة بالمجتمعات العربية بسبب اتساع دائرة الاستعمال الالكتروني أفرادا و جماعات شريفة وغير شريفة. يسجل أن علمنا العربي يعاني مثله مثل دول ثانية في أفريقيا وآسيا وأمريكا الجنوبية و كذلك في البلدان الأوروبية التي كانت تابعة للمعسكر الشرقي قبل انهياره العام 1989-1990(ولو بدرجات متفاوتة)، فالجريمة الالكترونية بمختلف أشكالها تستهدف،وفي المقام الأول، الحلقة الضعيفة(الأطفال ثم النساء) في أي مجتمع تظهر فيه مظاهر الفشل الاقتصادي و الانحيار المجتمعي إما نتيجة الإفلاس الاقتصادي و/أو الفساد الاداري و/أو الحروب.

¹ -مجلة العمال العرب، اللسان الاعلامي المركزي للاتحاد الدولي لنقابات العمال العرب،العدد:87،دمشق، 2009.

وبالرجوع إلى الاتفاقية الدولية الصادرة عن المنظمة العالمية للعمل (Organisation Internationale du Travail) المتعلقة بمكافحة أسوأ أشكال عمل الأطفال (الاتفاقية رقم: 182 لسنة 1999) والتوصية المرافقة لها (التوصية رقم: 190 لعام 1999، فإننا نجدهما (الاتفاقية+التوصية) قد استشرفتا عبر تحديد أسوأ أشكال عمل الأطفال، بمجمل التحديات التي تشكلها مخاطر المعلوماتية الصاعدة (سنة 1999) أي قبل حوالي عقد من الزمن، على الطفل من خلال ضغوطات التشغيل التي تفرض على العائلات السماح لأطفالها الشغل في ظل ظروف جد صعبة و مقابل أجر زهيد غير كاف لسد رمق الطفل فما بالك سد حاجيات أفراد العائلة، وفي مقدمتها:

-مكافحة كافة أشكال الرق و الاتجار بالأطفال (وهي ممارسة تضاعف حجمها وازدادت درجاتها على امتداد العالم و منها عالما العربي بسبب انتشار البطالة، والعوز الاجتماعي، والتسرب المدرسي، وضعف مداخيل العائلة العربية، وغلبة النمو السكاني على درجات و نسب تتجاوز وبكثير نسب النمو الاقتصادي)، وقد يزداد الأمر تعفنا بانتشار واتساع الحروب و الأزمات الاقتصادية في مجتمعاتنا العربية؛-التجنيد القصري (الاجباري) للأطفال لاستخدامهم في الحروب و الصراعات المسلحة (العالم العربي لم يكن يعرف ظاهرة التجنيد القصري للأطفال قبل تسعينيات القرن الماضي حتى في أحلك الحروب ضد الكيان الصهيوني أو الحروب بين الدول العربية، إلا الحرب اليمنية الدائرة بينت هذا الشكل من أشكال التجنيد القصري-الاجباري-لأطفال للزج بهم في حروب داخلية بدعم وتدخل خارجي)؛

-استخدام الأطفال في التجارة الجنسية أو لإنتاج أفلام و أعمال جنسية يكون الطفل موضوعها و عنصرها (وهي اعمال أصبحت تلقى رواجا بسبب انتشار وسائل الاتصال الجديدة (يوتيوب و منسجر و فيسبوك و هي أفعال تدار الكترونيا ومن بعيد بواسطة الهاتف الذكي و هي تجارة رائجة و مضمونة الربح)؛-استخدام الأطفال في تجارة المخدرات أو انتاجها و العمل فيها (وهي أفعال منتشرة في مناطق واسعة من العالم ولم ينجو منها عالما العربي و منطقتنا المغاربية وتؤدي فيها الوسائط الالكترونية دورا رئيسا في الترويج لها وتشجيعها، بل و تبنيها في ظل صعوبة الرقابة الحكومية من جانب و غياب الوازع الأخلاقي لدى العائلات التي تقوم بتشغيل أطفالها في هكذا أعمال غير مشروعة و مجرمة قانونا و وطنيا و دوليا.

تبقى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2014 أحد أهم وأبرز اتفاقية عربية تتناول الجريمة الالكترونية في مفهومها الواسع والشامل للظاهرة الإجرامية و كفاءات لحد منها من الناحية الوقائية) لكون الوقاية من الاجرام الالكتروني ضرورة حيائية لمجتمعاتنا العربية التي لم تكن تعرف مثل هكذا أفعال يجرمه القانونين الوطني و الدولي لخطورتها على الإنسان و السلوك الحسن) والردعية(الردع القانوني و كل ما يخص تغليظ العقوبات وإعادة النظر في الهيكل العامة لقوانين الاجراءات الجزائية.

والجزائر البلد العربي و المغاربي و الأفريقي المتميز الذي عرف ثورات اقتصادية و اجتماعية وثقافية منذ تاريخ الاستقلال وإلى غاية تاريخنا هذا رغم الكبوات الظرفية التي شهدتها مجتمعا، وهي أمر عادي بالنسبة لدولة جاءت بفضل ثورة عظيمة ضد أشرس احتلال استيطاني كان يمنع على الجزائري ولمدة 132 سنة حق التمتع بأبسط الحقوق الحياتية، و كانت لسلطاتها السياسية المتعاقبة قبل وبعد تاريخ التعديل الدستوري لسنة 1989، برامج واضحة ومحددة المعالم منذ سبعينيات القرن الماضي في مجال المعلوماتية.

ومن معالم هذا البرنامج في مجال المعلوماتية انشاء أول مدرسة للإعلام الآلي بمنطقة الحراش(منطقة الخمس سكناات) على مستوى العالم العربي، كما كانت للدولة الجزائرية اتفاقيات تبادل في مجال البرمجيات و تبادل الخبرات مع دولة الهند في سنوات 1973 إلا أن هذه الأخيرة-دولة الهند- واصلت جهدها المعلوماتي إلى أن وصلت ما حققته في مجال تصدير البرمجيات واستقطاب الكفاءات الهندية المهاجرة في العالم بل وتقوم اليوم بتصدير ما لا يقل عن عشرة(10) ملايين دولار سنويا في حين تخلت الجزائر عن برنامجها المعلوماتي الطموح انطلاقا من سنة 1978 أي مباشرة مع وفاة الرئيس هواري بومدين رحمه الله.

ثانيا: واقع وتحديات التجربة الجزائرية في مجال محاربة الجريمة الالكترونية.

لا اختلاف في بلدنا الجزائر الذي سبق له أن خاض تجربة التحكم وإنتاج البرمجيات في سبعينيات القرن الماضي، أن للتكنولوجيات الحديثة اضافة نوعية للمجتمع الجزائري الراغب في التطور التقني و التكنولوجي عبر توفير الإطار التشريعي والقانوني والتنظيمي المساعد في مجالات البحث المعلوماتي بصفة عامة(بغرض التأطير التشريعي للبحث العلمي)، والتحكم التكنولوجي في كل ما يتعلق بوسائط الاتصال الجديدة بصفة خاصة سيما وأن البلد يتمتع اليوم بعشرات الجامعات التي تحتل فيها كليات التكنولوجيا الصدارة، إن كان ذلك من حيث التأطير البيداغوجي(أساتذة ومؤطرين

بيداغوجيين ومخبريين في الاختصاص) أو من حيث استقطاب الطلبة لهذا التخصص أهميته وطنيا) برامج التوسع والاستثمار في القطاعين العمومي و الخاص وكذلك المختلط) و دوليا(طالب التكنولوجيا مرحب به في جامعات الأجنبية و الأوروبية بالخصوص).

1: المشرع الجزائري والموقف من مخاطر الجريمة الالكترونية

بدأت الجزائر مشرعا وأفرادا وجماعات تتعرف على أشكال الجريمة الالكترونية بقدر اتساع استعمالها ورواجها، فالمجتمع الجزائري لم يكن يعرف الجريمة البشعة، قبل دخول البلد في الأزمة الاقتصادية على مدار سنوات 1986 و 1987 و 1988، وذلك نتيجة تكفل الدولة بانشغالات شرائح واسعة من المواطنين بغض النظر عن تواجدهم في الحواضر و/أو المناطق القروية عبر تعميم برامج التنمية الاقتصادية.

إلا أن دخول الجزائر في مرحلة جديدة بعد تاريخ التعديل الدستوري لعام 1989 ركيزتها انسحاب الدولة من النشاط الاقتصادي كمتعامل اقتصادي صاحب سلطة وسيادة عملا بأحكام دستور 1989 الذي "ترسخ أحكامه الفصل بين الدولة باعتبارها قوة عمومية والدولة باعتبارها المالك لرأسمال المؤسسات الاقتصادية التجارية"¹ بالإضافة إلى ما أفرزته الأزمة الأمنية ابتداء من سنة 1992-1993 من آثار سلبية على سكينه المجتمع أفرادا و جماعات تمثلت في بروز حالات اجرام جديدة ورهبية مست الأطفال و النساء و المسنين و المواطنين بمختلف شرائحهم، ومهنتهم، و رتبهم في الدولة لم نكن نعرفها من قبل في ظل دولة الرفاهية الكاملة على مدار ثلاثة عقود بفضل سيادة الدولة المتدخلة في النشاط الاقتصادي و الاجتماعي والثقافي دون منازع إذ أن السلطة-الدولة صاحبة الشخص المعنوي الوحيد- كانت تمارس من خلال قانون العقوبات².

إلا أن الحقبة الزمنية التي أعقبت الأزمة الأمنية وتفاعلاتها ابتداء من سنة 1992-1993 وما رافقها من إرهاب وعنف و أفعال مجرّمة شرعا وقانونا وعرفا مجتمعيها هي التي أدخلت المجتمع في دوامة عنفوية كانت محل تحكم من الناحية الأمنية لعدم انسياق شرائح واسعة من الشعب الجزائري

¹ -المجلس الاقتصادي و الاجتماعي: لجنة علاقات العمل، تقرير حول نظام علاقات العمل في سياق التعديل الهيكلي، الدورة العامة العاشرة، الجزائر، أفريل 1998، ص: 17.

² -لمزيد الاطلاع على مميزات وخصائص السلطة، أنظر: اسحق ابراهيم منصور: ممارسة السلطة وآثارها في قانون العقوبات، ديوان المطبوعات الجامعية، الجزائر، 1983، ص: 20-33.

وراء الأفكار الهدامة التي كانت تجد دعما لها من دوائر مشبوهة لا تريد الخير و الاستقرار للدولة الجزائرية.

ومن منطلق أن قانون العقوبات هو "النظام القانوني الذي يشتمل على مجموعة من القواعد الملزمة التي تفرض على المخاطبين بها تحت تهديد الجزاء الجنائي.."¹ فإن قانون العقوبات الجزائري (الأمر رقم: 66-156 مؤرخ في 8 جوان 1966 المعدل و المتمم-الجريدة الرسمية للجمهورية الديمقراطية، العدد: 49، التاريخ: 11-06-1966) قد استجابت أحكامه لواقع الأفعال المجرمة قانونا.

لكن ومع دخول الهواتف الذكية وآخر مستحدثات التكنولوجيا في مجال الانترنت و الرقمنة و الاتصالات الحديثة وجد المجتمع الجزائري نفسه أمام أفعال و سلوكات وأنشطة تدخل أصحابها في خانة المجرمين الذين يستوجب معاقبتهم، ويبد من حديد، وفق نصوص قانونية صريحة و رادعة، فكان تعديل قانون العقوبات سنة 2004 ضروريا بالنسبة لمجتمع بدأ يشعر باتساع الجريمة الالكترونية ولو أنها كانت في بداياتها سنة 2001 و إلى غاية 2004 لكون السوق الوطنية لم تكن مشبعة من ناحية وفرة الهواتف الجواله لارتفاع أسعارها من جانب، ولقلة وفرتها من جانب ثان. ومع الوفرة المالية التي أعقبت الزيادة في أسعار النفط انطلاقا من سنة 2008-2009، وشروع السلطات العمومية في تطبيق الأنظمة الخاصة بموظفي قطاع الوظيفة العامة (كافة القطاعات) بعد أن أصدرت القانون الأساسي العام للوظيفة العمومية (الأمر رقم: 06-03 المؤرخ في 15 جويلية 2006) وجدت شرائح واسعة من أفراد المجتمع الجزائري في فسحة من أمرهم (من الناحية المادية بسبب التعويضات التي تحصلت عليها)، مع ما رافق ذلك من انفتاح السوق المحلية على مصراعيها أمام كل ما هو معلوناتي (هواتف ذكية و حواسب و انترنت.. إلخ).

2: سنة 2004 والبدية الفعلية لمواجهة مخاطر الجريمة الالكترونية.

وأمام حاجة المجتمع للوسيلة الالكترونية في اتصالاته وقضاء حاجياته أفراده اليومية، ودخول الرقمنة الاقتصادية كآلية في الدفع والتسديد شيئا فشيئا في حياة الفرد الجزائري، بالإضافة إلى "دمقرطة"

¹- اسحق ابراهيم منصور: الموجز في علم الاجرام والعقاب، مرجع سابق، ص: 7.

اللجوء واستعمالات الانترنت وتيسير الوصول إليه شرع المشرع الجزائري في تعديل قانون العقوبات سنة 2004 (قانون رقم: 04-15 المؤرخ في 10 نوفمبر 2004، معدل ومتمم المر رقم: 66-156 المؤرخ في 8 جوان 1966 والمتضمن قانون العقوبات-الجريدة الرسمية للجمهورية الجزائرية، العدد: 71، التاريخ: 10 نوفمبر 2004). وهو التعديل في قانون العقوبات الذي تضمن جديدا في تغليظ العقوبات الماسة بالأشخاص و الممتلكات العمومية و الخاصة لمزيد حماية المجتمع مع التذكير أن المشرع الجزائري قد استوعب في تعديله هذا، ولو دون التصريح الواضح نصا بمسؤولية صاحب الأفعال المجرمة الصادرة عن وسيلة الكترونية أو اتصالية.

وقد انتظرنا اصدار القانون رقم: 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم الالكترونية المتصلة بتكنولوجيات الاعلام و الاتصال ومكافحتها(الجريدة الرسمية للجمهورية الجزائرية، العدد: 47، التاريخ: 16 أوت 2009) لنجد أنفسنا أمام نصوص واضحة الكتابة و المضمون.

ومن أهم الأفكار المستخلصة من قراءتنا لنصوص هذا القانوني الآتي:- وضع قواعد خاصة للوقاية من كل جريمة الكترونية و تشديد أشكال مكافحة أوجه الظاهرة الإجرامية المحدقة بالمجتمع(راجع نص المادة الأولى من القانون رقم: 09-04 السالف الذكر)؛

- تجريم الأفعال الضارة الصادرة عن أشخاص بواسطة أو عن طريق منظومة معلوماتية أو نظام اتصالات الكترونية(راجع المادة: 2 بعد التعديل) و هذا ما كنا بأمس الحاجة إليه كباحثين في الجريمة الالكترونية التي انتشرت وتعددت خيوطها و أنواعها في ظل التقنيات الجديدة؛
- تحميل مسؤولية جنائية للقناة الاتصالية التي أقترب بواسطتها، أو من خلالها، أو عبرها الفعل المجرم و هذا ما يحمل المؤسسات و الشركات و المقاولات المعنية بالاتصال الالكتروني واجب تحمل المسؤولية ؛

- تشديد الرقابة على كل ما قد يضر أمن الدولة (ارهاب و تخريب و جرائم ماسة بالدولة) من باب الوقاية وفي إطار رعاية قضائية(راجع نص المادة: 4/أ من القانون رقم: 09-04 السالف الذكر)؛

والجديد في هذا القانون يتمثل في انشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال و مكافحته و تحديد مهامه (وقاية و مساعدة و تبادل المعلومات).

وما يلاحظ من خلال نصوص القانون رقم: 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم الالكترونية المتصلة بتكنولوجيات الاعلام و الاتصال ومكافحتها حقيقة أن المشرع الجزائري لم يخص الطفل بإطار قانوني خاص به يحميها من مخاطر المعلوماتية ويكفل له الحماية الجزائية في ظل ما يواجهه أطفالنا من أفعال ابتزاز و مساومة و اعتداء غير أخلاقي من قبل أناس فقدوا إنسانيتهم و تحولوا إلى حيوانات مفترسة في حق الطفولة.

الخاتمة: إن اجتهادات المشرع الجزائري في مجال حماية أمن الدولة، و محاربة الإرهاب، و تجارة المخدرات و كذلك الاتجار بالبشر هي اجتهادات تنم عن حرص شديد على أمن و استقرار الوطن ونتمنها و نقوم بتبليغها و شرحها و الدفاع عنها في المحافل الوطنية و الدولية.

لكن ما نحن بأمس إليه هو أن يقوم المشرع الجزائري مشكورا بمبادرة اصدار قانون خاص للجريمة الالكترونية الماسة بالأطفال و النساء بالنظر للحوادث المؤلمة التي يشهدها مجتمعنا في ظل ازدياد الطيش الشبابي المتأثر بالأفلام الكارطونية، وسلسلة الألعاب الشيطانية المستقطبة للشباب من كل العمار والشرائح التي تقدم لهم القتل، الاغتصاب، والختف، و الابتزاز، و مسّ شرف الناس وكأنه بطولة.

ومن هنا يأتي دور كلية الحقوق والعلوم السياسية على مستوى جامعات الوطن في تقديم قراءات قانونية للنصوص القانونية التي من شأنها أن تسهم في اصدار قانون رادع للجريمة الالكترونية بمختلف أشكالها يكون انموذجا على الصعيد العربي و الإفريقي.

الجريمة الالكترونية في الجزائر: الواقع، المأمول وآليات المواجهة

د/ ابرادشة فريد

كلية الحقوق والعلوم السياسية

جامعة المسيلة

ط.د/ عامر هني

كلية الحقوق والعلوم السياسية

جامعة المسيلة

مقدمة:

في عالمنا المعاصر نكاد نجزم بأنه لا أحد يستطيع أن ينكر الدور الإيجابي الذي أضافته التكنولوجيا للحياة الانسانية، إذ أنها سهلت الكثير من المعاملات و طوعت العديد من الخدمات، بل لقد تعدى دورها الى حد التقريب بين الدول والشعوب واختصار المسافات، فتطورت التجارة تطورا مذهلا وأضحت مصدرا من مصادر الدخل والعمل، وبالتالي فقد ساهمت في القضاء على البطالة، وغير هذا كثير، لكن في مقابل هذا لا يمكننا أيضا أن ننكر بأن نفس هذه التكنولوجيا ساهمت في ظهور العديد من الجرائم التي اصطلح على تسميتها الجريمة المعلوماتية أو الالكترونية، لأنه بعدما كان منتظرا أن تكون هذه التكنولوجيا الرقمية في يد الانسان ولحيته ومصالحته تحولت حينما وقعت بين أيدي اشخاص وجماعات محترفة حولها عن مسارها الحقيقي والصحيح لتصبح أداة للجريمة كالقرصنة وتحويل الأموال والتهديد والابتزاز والتجسس على الحسابات والسرقة العلمية وتحويل الأموال، ونشر الرذيلة وإفساد الاخلاق، وكل هذا مشاهد في حياتنا اليومية ولم يعد خافيا على أحد...الخ.

طبعا كما نعلم أنّ الجريمة العادية في السابق كانت عبارة عن جرائم عادية ترتكب من طرف أشخاص عاديين، و في مكان وزمان محدد ومعروف، وبالتالي فإنّ أركانها هم أشخاص معروفون ومكانها معروف و محدد، لكن التطور التكنولوجي والرقمي والتقنيات العالية الجودة جعلت من ظاهرة الجريمة تتطور الى درجة أنّ الجرائم المعلوماتية صارت ترتكب في بلد ومنفذوها في بلد اخر ومن خارج الحدود وقد تكون عابرة للقارات وكل ما يساعده في تنفيذ تلك الجريمة هو جهاز كمبيوتر او حاسوب وشبكة عنكبوتية من خلالها يعمل على إيقاع وتنفيذ جرائمه من خلال مجموعة من الازرار والرموز والشفيفرات والارقام السرية التي يقوم بفكها ن طبعا فلهذه الأسباب اضطرت أجهزة الامن

والقضاء والمحققين في أي دولة الى تطوير مجموعة من الوسائل والاليات لمحاربة مثل هذه الظاهرة الخطيرة.

لابد من ضرورة وضع خطط واستراتيجيات عالمية وعلى مستوى عال من العلمية والاحترافية لمواجهة وللمحد من اخطار هذا النوع المدمر على سياسات واقتصاديات الدول، بداية من عملية سن منظومة قانونية وتشريعية تتلائم وتتكيف مع هذا النوع من الجرائم ثم سن مجموعة من الاليات التربوية والمجتمعية التي تلقن للنشأ في المدارس للتوعية من أخطار هذه الظاهرة ومن تبعاتها الدينية والدينية.

بطبيعة الحال لقد كلفت مثل هذه البرامج الوقائية ميزانيات الدولة الملايير لاسيما في عملية تكوين مختلف الاسلاك القضائية والأمنية من شرطة ودرك وجيش وحماية مدنية بهدف الجاهزية لمواجهة الظاهرة والقضاء عليها قبل استفحالها لاسيما وأنا في الجزائر أصبحنا نشهد العديد من عمليات التهديد الإلكتروني والابتزاز والتحرير والتشهير ونشر الرذيلة والمواد الاباحية وغيرها والتشهير بالأشخاص والمساس بالخصوصيات الأسرية والفردية وحتى الجماعية والخطر من هذا كله هو كشف أسرار الدولة وغيرها من الامور التي تمس بالاستقلال والسيادة الوطنية.

إنّ التحدي أصبح كبيرا وخطيرا وأساليب المواجهة لا تزال غير كافية ن وذلك لأنه كلما طورت الدولة ومختلف مؤسساتها من أليات المواجهة لهذا النوع من الجرائم كلما قام أولئك الاشخاص الذين لا هم لهم إلا مصالحهم الشخصية الضيقة من تطوير أساليبهم عبر ابتكار أساليب وتقنيات جديدة لتحقيق مآربهم وغاياتهم الدينية التي تضر بالبلد وتهدد سلامته.

اشكالية الدراسة:

هل استطاعت الجزائر عبر منظومتها الامنية والتشريعية والقانونية أن تطور و تكيف من أليات مكافحة الجرائم الالكترونية ؟

محاور الدراسة:

المحور الاول: مفهوم الجريمة الالكترونية

المحور الثاني: واقع الجريمة الالكترونية في الجزائر

المحور الثالث: اليات مكافحة الجرائم الالكترونية في الجزائر

أهداف الدراسة:

تهدف من خلال هذه الدراسة الى كشف اللثام عن خطر هذه الظاهرة العابرة للقارات والتي تعتبر أثارها وخيمة على كل مكونات الدولة والمجتمع وبالتالي سوف نسعى الى تحليل الظاهرة وإعطاء الحلول المناسبة لمواجهتها.

المحور الاول: مفهوم الجريمة الإلكترونية

(أ) تعريف الجريمة:

تعرف الجريمة عموما على أنها ذلك العمل السلبي الذي يرتكبه بعض أفراد المجتمع، وقد تدفعه لذلك أسباب ذاتية أو ظروف اجتماعية معينة.¹ ويمكن ان نعرف الجريمة بأنها سلوك فاسد ينبذه أفراد المجتمع الصالحين ويعاقب عليه القانون، نظرا لما يسببه من أضرار على ضحاياه، مثل جريمة القتل والسرقة والاعتداء الجنسي والضرب.

(ب) تعريف الجريمة الالكترونية:

الجريمة الالكترونية: هي ظاهرة حديثة ومعاصرة، ارتبطت في ظهورها بتكنولوجيا الحاسوب.²

وعرف مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين الجريمة الالكترونية في تعريف شامل: بأنها كل جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية.³ وعرفت الدكتورة هدى قشقوش الجريمة الالكترونية بأنها كل سلوك غير مشروع أو غير مسموح به قانونا، والذي يتمثل في المعالجة الالية للبيانات أو نقل هذه البيانات.⁴

¹ - كوثر فرام ومحمد العيماني، الجريمة المعلوماتية على ضوء العمل القضائي المغربي، المعهد العالي للقضاء، بحث منجز في نهاية عملية التدريب، وزارة العدل، المملكة المغربية، 2007/2009، ص ص 04، 05.

² - كوثر فرام ومحمد العيماني، مرجع سبق ذكره، ص 05.

³ - المرجع نفسه، ص 05.

⁴ - رحيمة غديلي، خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة، مداخلة مقدمة للمشاركة في فعاليات المؤتمر الدولي الرابع عشر حول الجرائم الالكترونية، يومي 24-25 مارس، مركز جيل البحث العلمي، طرابلس، لبنان، 2017، ص 99.

وعرف الفقيه ماور Mawre الجريمة الالكترونية بأنها: الفعل غير المشروع الذي يتورط الحاسب الآلي في ارتكابه.¹

ويمكن تعريف الجرائم الإلكترونية بأنها "جميع المخالفات التي تُرتكب ضد أفراد أو مجموعات من الأفراد، مع وجود دافع إجرامي للمجرم لإلحاق الضرر عمدا بسمعة الضحية، أو التسبب له في الأذى الجسدي أو النفسي، بشكل مباشر أو غير مباشر، وذلك باستخدام شبكات التواصل الحديثة مثل الإنترنت، بواسطة غرف الدردشة (الفايسبوك، الواتسب، الفايبر، الانستجرام، الماسينجر...)، البريد الإلكتروني...، والهاتف النقال من خلال الرسائل النصية القصيرة ورسائل الوسائط المتعددة.²

وتشمل الجرائم الإلكترونية أي فعل إجرامي يتم من خلال الحواسيب أو شبكات مواقع التواصل الاجتماعي، كما تضم أيضا أشكال الجرائم التقليدية التي يتم تنفيذها عبر الإنترنت. حيث نجد أن مثل تلك الجرائم قد تهدد أمن الدولة واستقرارها وأموالها العامة، وأبرزها جريمة الاختراق أو القرصنة، وانتهاك حقوق التأليف، ونشر الصور الخليعة والأفلام الاباحية، ومحاولات في استمالة الاطفال لاستغلالهم جنسيا، وحتى في الحروب الى جانب التنظيمات الارهابية، والتجارة غير القانونية (كتجارة المخدرات وتجارة الاعضاء والتجارة الجنسية)، كما تقوم بانتهاك خصوصية الآخرين من خلال استخدام معلوماتهم السرية بشكل غير قانوني..، مثل انتحال شخصية الغير للقيام بأعمال غير قانونية.³

كما تتسبب الجرائم الإلكترونية للدول بأضرار كبيرة أخرى، مثل ما يترتب عن التجسس الإلكتروني، وما يعرف لدى المجتمع الدولي بالحرب الإلكترونية، خاصة وأن هذه الظاهرة عابرة

1 - المرجع نفسه، ص98.

2 - ذياب موسى البدينة، الجرائم الالكترونية: المفهوم والاسباب، مداخلة مقدمة للمشاركة ضمن فعاليات المنتدى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، أيام 2-3-4، بكلية العلوم الاستراتيجية، عمان، الاردن، 2014، ص03.

3 - موسوعة الجزيرة- فضاء من المعرفة الرقمية، الجرائم الالكترونية...عندما تصبح التقنية وسيلة للاجرام، في الموقع الإلكتروني:

للحدود والقارات، والنظام القانوني الدولي يحاول تحميل الفاعلين المسؤولية عن أفعالهم في مثل هذا النوع من الجرائم من خلال المحكمة الجنائية الدولية.¹

جدول رقم (01): يقارن بعض نماذج الجريمة التقليدية مع الجريمة الالكترونية

الجريمة التقليدية	الجريمة الالكترونية
الاختيال	الاختيال على الشبكة، الاختيال بالمزاد الالكتروني... الخ
السطو	القرصنة على الانترنت، الحرمان من الخدمة، الفيروسات
جرائم الاطفال الجنسية	استمالة الاطفال على النت، المواقع الاباحية
غسيل الاموال	أنظمة الدفع على الشبكة
السرقه	جرائم الهوية، سرقة الملكية

المصدر: ذياب موسى البداينة، مرجع سبق ذكره، ص 07

أولاً: إحصائيات وأرقام مخيفة

لقد ازداد عدد الجرائم الالكترونية بشكل رهيب بداية من الألفية الثالثة، التي انتشرت فيها الانترنت واصبحت في متناول الصغار قبل الكبار، ولعل الارقام والاحصائيات العالمية وحتى المحلية في الجزائر تبين مدى تضاعف حجم الكارثة

تكلف الجرائم الالكترونية الاقتصاد العالمي 440 مليار دولار سنوياً، فهي تتراوح سنوياً بين 375 و575 مليار دولار.²

¹ - المرجع نفسه، ص 03.

² - رضية بوشعور الغازي وأحمد الطويل، التكلفة الاقتصادية والاجتماعية لوسائل الدفع الالكترونية- تحليل التجربة الجزائرية وآفاقها، مداخلة مقدمة للمشاركة في فعاليات المؤتمر الدولي الرابع عشر حول الجرائم الالكترونية، يومي 24-25 مارس، مركز جيل البحث العلمي، طرابلس، لبنان، 2017، ص 203.

قبل التحدث عن انتشار ظاهرة الجرائم الإلكترونية لابد من التحدث عن أخطار الاستعمال المفرط لتكنولوجيا المعلومات والاتصال على الصحة البشرية، ففي دراسات طبية ونفسية مختصة أجريت على العديد من الناس أثبتت وبالتجربة والبرهان مدى خطورتها على صحة العيون، القلب، الكبد، الكلى، الدماغ، بل إنها تؤدي في العديد من الاحيان الى العقم....الخ

إنّ هناك خطرا كبيرا من جراء استعمال الواي فاي Wi - fi على صحة الانسان بحيث يؤكد العديد من الأطباء بأنّ هذه الشبكة لاستعمال الانترنت في البيت ن تفوق إشعاعاتها حجم وقوة الاشعة السينية N ويصل مداها الى 300 متر مختربة الجدران والابواب والنوافذ.

التشريع الجزائري على الرغم من سنه للعديد من القوانين والتنظيمات التي تؤطر هذا المجال المهم من حياة الناس إلاّ انها لاتزال في غير مستوى الدول المتطورة، وغير مواكبة للجديد الحاصل على المستوى العالمي وذلك راجع بدوره الى العديد من الاسباب نذكر منها:

. نقص الخبرات والكفاءات التقنية المختصة في مجال تكنولوجيا الاعلام والاتصال
. نقص البرامج المتطورة وارتفاع ثمنها، بالإضافة الى حتمية ضرورة تحديثها كل سنة او بين الفترة والأخرين الامر الذي يجعلها غير مطلوبة، هذا على الرغم من اهميتها، كبرامج حجب المواقع الاباحية والخلاعية، حجب البرامج التي تروج للعنف والتعصب والتطرف الديني وغيرها، مثل مراقبة المؤلفات والكتب التي تدخل للبلاد

. قلة البرامج التدريبية للقضاة والشرطة والدرك على مواكبة الجديد في مجال الجريمة الالكترونية خاصة التقنيات الجديدة التي يطورها القراصنة يوما بعد يوم.

المحور الثاني: واقع الجرائم الالكترونية في الجزائر

أولا: تعريف التشريع الجزائري للجريمة الالكترونية:

الجرائم المتصلة بتكنولوجيات الاعلام والاتصال: هي جرائم المساس بأنظمة المعالجة الالية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى تتركب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.¹

¹ - قانون رقم 04-09 مؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، (الجريدة الرسمية للحكومة الجزائرية، عدد 47، الصادرة بتاريخ 16 أوت 2009)، المادة 02، ص 05.

لم تسلم الجزائر كبقية دول العالم من اضرار الجرائم الالكترونية، وذلك بالرغم من بساطة حجم التعامل الالكتروني بها مقارنة بدول أخرى، فهي مصنفة في المراتب الاولى عربيا وافريقيا من حيث الجريمة الالكترونية، بنسبة 85 %، من ضمنها حسابات المسؤولين، وهذا ما جعلها تلقى اهتمام كبير لدى تقارير المنظمات والهيئات الدولية المتخصصة في هذا الشأن، فقد سجلت فيها سنة 2016 1055 جريمة الكترونية، تورط فيها أكثر من 946 شخص، يعني بمعدل جريمة الكترونية لكل 08 ساعات، و03 جرائم الكترونية كل 24 ساعة، ورغم ذلك وجود قلة المبلغين من فئة ضحايا الجريمة الالكترونية، تخوفا من انتشار الفضيحة أو بسبب ضعف ثقافة التبليغ عندهم.¹

جدول رقم (02): يوضح احصائيات حول تطور الجريمة الالكترونية في الجزائر بين سنوات (2013-2016)

السنوات	عدد الجرائم الالكترونية في الجزائر بين سنوات (2013-2016)
2013	91
2014	246
2015	567
2016	1055

المصدر: رضية بوشعور الغازي وأحمد الطويل، مرجع سبق ذكره، ص206.

نلاحظ من خلال الجدول رقم (02) أن معدل الجريمة الالكترونية بالجزائر في تزايد مستمر منذ سنة 2013 الى غاية سنة 2016، وذلك بفارق كبير، قدر بعدد 964 جريمة الكترونية، حيث قد يرجع هذا العدد الى ارتفاع كبير في عدد مستخدمي شبكة الانترنت هذا من جهة، ومن جهة أخرى عدم فعالية الرقابة الالكترونية بالشكل الذي يخفف من حدة انتشار الجرائم الالكترونية، وكذا عدم تفعيل قانون العقوبات المتعلق بتلك الجرائم بالشكل المطلوب. ويمكن أن يكون الخلل متمثل في عدم كفاءة اليات وأجهزة الرقابة الالكترونية التي تستعملها الشرطة العلمية الجزائرية.

¹ - المرجع نفسه، ص206.

ثانيا: إحصائيات عن الدرك والشرطة حول الجرائم الالكترونية في الجزائر:

كشف رئيس مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية والحماية منها ومكافحتها، أن مصالح الدرك الوطني، عاجلت أكثر من 500 جريمة رقمية، خلال سنة 2015، منها 300 جريمة تتعلق بمواقع التواصل الاجتماعي “فيسبوك”، و 20 جريمة رقمية تعلقت باختراق مواقع رسمية لمؤسسات خاصة وعامة، استهدف مجرموها أنظمة المعالجة الآلية للمعطيات¹.

فقد سجلت مصالح الدرك الوطني والشرطة الجزائرية قرابة 2500 جريمة إلكترونية خلال سنة 2017، تنوعت بين جرائم القرصنة والابتزاز والتشهير والتحرش الإلكتروني والاحتيال والنصب، وتشير أرقام صرحت بها المصالح الامنية الجزائرية المكلفة بمكافحة الجرائم الالكترونية، منها 80 % ارتكبت عن طريق موقع التواصل الاجتماعي الفيسبوك، حيث تعرض من خلالها الضحايا الى عمليات ابتزاز وتهديد بنشر صور، أغلبها مفبركة².

وفي هذا الشأن أكد العقيد جمال بن رجم على تامين دور الدرك الوطني في حماية المواطن الجزائري من الجرائم السيبرانية، خاصة وأن معظم الجرائم تطورت وانتقلت من شكلها التقليدي الى شكلها العصري (الافتراضي)، مما استدعى ذلك المصالح الامنية الجزائرية الى تجنيد وسائل وأساليب رقمية متطورة لمكافحة الجريمة الالكترونية كما جاء على لسان بن رجم أن المجتمع الجزائري في ظل التطور الهائل الذي تشهده تكنولوجيا الاعلام والاتصال، وكذا في جميع مجالات الحياة أصبح يعاني من ارتفاع معدل الجريمة الالكترونية، والتي تسببت له في مشاكل عديدة ومختلفة أضرت بأمنه واستقراره، وهذا رغم المجهودات الكبيرة التي تبذلها المصالح المعنية في كشف مرتكبي تلك الجرائم الالكترونية وتقديمهم للعدالة، ومن بين تلك الجرائم قرصنة الانظمة المعلوماتية والمعطيات المختلفة، والقذف

¹. حسامن حريشان، 500 جريمة إلكترونية في 2015 ن جريدة الخبر أنظر موقع:

<https://www.elkhabar.com/press/article/98286>.

² - موقع ثقافة ومجتمع، الجريمة الالكترونية بالجزائر - الفضيحة أعنت أسلحة الجناة، في الموقع الالكتروني:

<https://www.dw.com,10-02-2018,pp02,03>.

والسبب والشتم، والمساس بالنظام العام واغتصاب الممتلكات العمومية والخاصة والنصب والاحتيال، وجرائم التجارة الإلكترونية والدفع الإلكتروني.¹

تُعتبر الجرائم الإلكترونية من أحدث أنواع الجرائم التي يترتب عنها آثار سلبية على الدول في مختلف القطاعات العمومية، وذلك في ظل مرحلة العولمة والتي أصبحت دول العالم فيها تمثل قرية صغيرة، لأن شبكة الانترنت ومواقع التواصل الاجتماعي قصرت المسافات واختزنت حدود وسيادة الدول، واخضرت في الوقت والجهد، حيث أصبح الفرد يتابع أخبار العام في جهاز رقمي يحمله في كف يده، وظهر ما يعرف بالتجارة الإلكترونية والتسويق السياحي. فالجزائر كبقية هذه الدول تضررت في السنوات الأخيرة من الجرائم الإلكترونية، وهي تزايد مستمر، حيث بلغت في العام الماضي حسب تصريحات المؤسسات الأمنية المعنية 1055 جريمة إلكترونية، تورط فيها أكثر من 946 شخصاً، فالجزائر ومواطنيها أصبحت مستهدفة كثيراً من قبل عصابات الجريمة الإلكترونية المنظمة من داخل وخارج الوطن، والتي تستهدف أمن واستقرار الدولة واقتصادها، مثل سرقة ونهب الأموال العمومية والخاصة.²

فقد جاء في تقارير المنظمات العالمية المتخصصة العام الماضي أن الاقتصاد العالمي خسر أكثر من 650 مليار دولار من جراء الهجمات الإلكترونية التي تستهدف الأنظمة المعلوماتية والحاسوبية لمختلف الدول بما فيها الجزائر طبعاً، ووفقاً لدراسة قدمتها شركة غارتنر المختصة بالأمن المعلوماتي، فإن دول الشرق الأوسط وشمال إفريقيا أنفقت سنة 2016 أزيد من 11.5 مليار دولار على خدمات وتقنيات المعلومات، وخاصة الاستثمار في الخدمات الداخلية وخدمات أنظمة البيانات والتجهيزات الخاصة وخدمات الاتصالات.³

فالجزائر التي تُعتبر من الدول التي قامت باقتناء تجهيزات وأنظمة معلومات متقدمة ومعقدة لتطبيق مشروع الحكومة الإلكترونية وحماية بُنيته التحتية الإلكترونية من الجرائم الإلكترونية، ولكن لا تزال

¹. مركز مكافحة الجرائم الإلكترونية بالدرك الوطني: معالجة 100 قضية تتعلق بالطفولة والمراهقين و 20 جريمة مالية خلال 2017، أنظر موقع:

<https://www.djazairress.com/echchaab/107048>

². عميرة أيسر. الجرائم الإلكترونية في الجزائر. موقع انترنت: <http://www.almayadeen.net/articles/blog/714137>.

³ -المرجع نفسه.

الفِرَق المختصة في الأمن المعلوماتي في مختلف القطاعات الأمنية تحصى الآلاف من الجرائم الإلكترونية قد تنجح في فكّ شفرات بعضها، وإحباطها قبل حدوثها وتفشل في صدّ الكثير منها. الجزائر تُعتبر من الدول التي تُسجّل نسبة الإنترنت فيها نمواً مستمراً سجّل برسم سنة 2010 أكثر من 4 ملايين مستخدم لها من بين 67 مليون مستخدم لها في إفريقيا، وكلما زاد عدد المستخدمين وتشبّعت شبكة الإنترنت الوطنية كلما تطوّرت عصابات الجريمة الإلكترونية فيها وأصبحت أكثر خطورة وتأثيراً على الفضاء الافتراضي، خاصة في ظل الجهود الكبيرة التي تبذلها في تطبيق مشروع الحكومة الإلكترونية ومحاولة تعميمه على كل القطاعات العمومية.¹

وجاء على لسان البروفيسور عبد اللطيف لديد والذي كان رئيس المنتدى العالمي للنسخة السادسة من بروتوكول الإنترنت في سنة 2010: (إنّ الجزائر لا تمتلك رقابة فعّالة وصارمة على الإنترنت، وهذا ما يضعنا أمام مُعضلة حقيقية مستقبلاً، إن لم تتحرّك أجهزة الدّولة ومُؤسّساتها المختصة من أجل وضع مُخطّط استراتيجي قومي للحدّ من تنامي نسب الجريمة الإلكترونية وتفعيل البرامج المختصة بمراقبة الإنترنت بما يحفظ حقوق الأفراد وممتلكاتهم المادية والمعنوية).²

المحور الثالث: اليات مكافحة الجرائم الإلكترونية في الجزائر

اولاً: أسباب استفحال ظاهرة الجرائم الإلكترونية

نظراً لازدياد عدد الجرائم الإلكترونية وانتشارها الهائل في دول العالم، وتفاقم حدة الاضرار التي تخلفها على مواطنيها، شرعت بعض الدول والمنظمات الدولية والإقليمية بوضع تشريعات جزائية خاصة لمكافحة جرائم الإنترنت التي تعتبر ظاهرة مستحدثة في عالم الإجرام، وقد يكون من المشاكل المشجعة أيضاً على الجريمة الإلكترونية غياب تشريع خاص يتعلق بهذا النوع من الجرائم أو عدم تفعيل مثل هذه التشريعات بالشكل المطلوب، بحيث في بعض الحالات يضطر رجال القضاء لملاحقة هذه الجرائم عن طريق تطويع نصوص قانون العقوبات الحالي، بالإضافة الى ما يتضمنه من نصوص قانونية تتعلق بجرائم السرقة والنصب وخيانة الأمانة والابتزاز والسب والتشهير وغيرها، أي تطبيق الاحكام الجزائية (العقوبات) للجريمة التقليدية على مرتكبي الجرائم الإلكترونية المماثلة لها على أرض الواقع، الأمر الذي قد يكون من السهل التحايل عليه من قبل الجناة ومحاميهم، لتنتهي الكثير من

¹ - عميرة أيسر، مرجع سبق ذكره.

² - المرجع نفسه.

هذه القضايا البراءة أو عقوبات خفيفة، بالتالي يجب على السلطة التشريعية سن تشريعات متعلقة بشكل مباشر وخصيصا بالجرائم الإلكترونية، مع شرط تطبيقها بشكل فعال وعادل على كل الجناة.¹

ثانيا: الاليات القانونية لمكافحة الجريمة الالكترونية

تمتلك الجزائر جملة من القوانين الجيدة، من شأنها الوقاية من هذه الجريمة والحد منها، شرط تطبيقها بشكل موضوعي وفعال.

1- قانون البريد والاتصالات السلكية واللاسلكية:

ويعد هذا القانون من بين القوانين الهامة جدا في مكافحة الجريمة الالكترونية، لأنه ينضم قطاع حساس، حيث ترتكب الجرائم الالكترونية في مجاله، من خلال قنوات وشبكات الاتصال التابعة له، فقد تناول الباب الرابع من هذا القانون شرطة البريد والمواصلات السلكية واللاسلكية، والذي يتفرع عليه فصلين، فالفصل الاول تطرق الى بحث ومعاينة المخالفات في المواد من 121 الى 126، فعلى سبيل المثال نصت المادة 121 على ما يلي: (علاوة عن ضباط وأعوان الشرطة القضائية، يؤهل للبحث عن مخالفات أحكام هذا القانون ومعاينتها، أعوان البريد والمواصلات السلكية واللاسلكية الذين لهم رتبة لا تقل عن رتبة المفتش والمتمتعين بصفة الموظف). أما الفصل الثاني فقد تعرض فيه المشرع الى الاحكام الجزائية في المواد من 127 الى 144، فقد نصت المادة 127 على سبيل المثال على ما يلي: (تطبيق العقوبات المنصوص عليها في المادة 137 من قانون العقوبات على كل شخص مرخص له بتقديم خدمة البريد السريع الدولي أو كل عون يعمل لديه، والذي في اطار ممارسة مهامه، يفتح أو يحول أو يخرب البريد أو ينتهك سرية المراسلات أو يساعد في ارتكاب هذه الافعال... علاوة على العقوبات المنصوص عليها في الفقرات 1 و 2 و 3 المشار اليها أعلاه، يمنع المخالف من ممارسة كل نشاط أو مهنة في قطاع المواصلات السلكية واللاسلكية أو قطاع البريد أو قطاع ذي صلة بهذين القطاعين لمدة تتراوح بين سنة الى 5 سنوات).²

¹ . <https://www.alwatanvoice.com/arabic/news/2016/06/19/936136.html>

² - قانون رقم 200-03 مؤرخ في 05 أوت 2000، يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، (الجريدة الرسمية للحكومة الجزائرية، عدد 48 الصادر بتاريخ 06 أوت 2000)، المادتين 121 و 127، ص ص 22، 23.

2- قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها:

حسب مادته الاولى يهدف هذا القانون الى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.¹

يعد هذا القانون التشريع الرئيسي والهام جدا المناط به الوقاية من الجريمة الالكترونية ومكافحتها، فقد حدد فيه المشرع الجزائري أساليب وطرق الرقابة الالكترونية وكذا تفتيش المنظومة المعلوماتية، والتزامات مقدمي الخدمة، بالإضافة الى مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته، والتعاون والمساعدة القضائية في مجال مكافحة الجريمة الالكترونية.

3- قانون العقوبات:

لقد تطرق المشرع الجزائري الى الافعال الالكترونية التي يجرمها القانون، والتي افرزتها ثورة تكنولوجيا المعلومات والاتصال التي شهدتها العالم بشكل عام والجزائر بشكل خاص، بالأخص منذ مطلع القرن الواحد والعشرين (21)، بحيث دفع هذا التطور الرقمي المشرع الجزائري الى تعديل قانون العقوبات رقم 04-15 المؤرخ في 10 نوفمبر 2004، المتمم للأمر رقم 66-15 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الالية للمعطيات، ويتضمن هذا القسم ثمانية مواد من 394 الى 07 مكرر. وفي عام 2006 عدل قانون العقوبات، حيث درس هذا التعديل القسم 7 مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الالية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الافعال، ويرجع هذا التعديل الى ازدياد خطورة الجريمة الالكترونية على الامن القومي الجزائري وعلى أمن وسلامة المجتمع الجزائري.²

ثالثا: الاليات المؤسسية الجزائرية لمكافحة الجريمة الالكترونية:

يعتبر القانون رقم 04/09 الصادر في 2009، من بين أهم التشريعات الجزائرية المناط بها مكافحة الجريمة الالكترونية، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات

¹ - قانون رقم 09-04، مرجع سبق ذكره، المادة 01، ص 05.

² - فضية عاقل، الجريمة الالكترونية واجراءات مواجهتها من خلال التشريع الجزائري، مداخلة مقدمة للمشاركة في فعاليات المؤتمر الدولي الرابع عشر حول الجرائم الالكترونية، يومي 24-25 مارس، مركز جيل البحث العلمي، طرابلس، لبنان، 2017، ص 127.

الاعلام والاتصال. فقد استحدثت المشرع الجزائري في هذا القانون هئتين هامتين للوقاية من الجرائم الالكترونية ومكافحتها، بهدف ردعها والحفاظ على سلامة المواطن منها. بالاضافة الى هيئات أخرى لم يتطرق لها.

أ)-الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته:

تتولى هذه الهيئة حسب ما نصت عليه المادة 14 المهام الآتية:¹

- 1-تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته.
- 2-مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الاعلام والاتصال، بما في ذلك تجميع المعلومات وأنجاز الخبرات القضائية.
- 3-تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الاعلام والاتصال وتحديد مكان تواجدهم.

ب)- الهيئات القضائية المتخصصة في التعاون والمساعدة الدولية في مكافحة الجريمة الالكترونية:

تختص المحاكم الجزائرية حسب ما جاء في المادة 15 من هذا القانون بالنظر في الجرائم المتصلة بتكنولوجيا الاعلام والاتصال المرتكبة خارج الاقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني.² أضف الى ذلك النظر في كل الجرائم الالكترونية المرتكبة داخل الاقليم الوطني.

ج)- المعهد الوطني للأدلة الجنائية وعلم الجرائم:

يتكون هذا المعهد من احدى عشرة (11) دائرة متخصصة في مجالات عديدة، والمتمثلة في دائرة التكوين والتعليم وتقديم المساعدات التقنية، ودائرة الاعلام الالي والالكتروني المكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة وتقدم كذلك مساعدة تقنية للمحققين في المعاينات.³

د)- المديرية العامة للأمن الوطني:

¹ -قانون رقم 04/09، مرجع سبق ذكره، المادة 14، ص08.

² - قانون رقم 04/09، مرجع سبق ذكره، المادة 15، ص08.

³ - فضيلة عاقل، مرجع سبق ذكره، ص133.

تختص هذه المديرية في مكافحة الجريمة الالكترونية من عدة جوانب، من بينها الجانب التوعوي، وذلك من خلال برمجتها لدروس توعوية في مختلف الأطوار الدراسية، وكذا المشاركة في الملتقيات والندوات الوطنية وكل التظاهرات والفعاليات العلمية التي تساهم في توعية المواطن حول مدى خطورة الجرائم الالكترونية.¹

الخلاصة:

في ختام هذه المداخلة لابد ان نشير الى حقيقة أكيدة بأنه لا سبيل للقضاء على ظاهرة الجرائم الالكترونية إلا اذا كان هناك أسلوب جماعي وتشاركي يشترك ويساهم فيه الجميع للوقاية من أخطار هذه الظاهرة الفتاكة، هذه الظاهرة التي أصبحت تهدد كل جوانب الحياة البشرية، الصحية، النفسية، المالية، الدينية، الاقتصادية، العلمية.... الخ.

طبعاً هذا الأمر سوف يتطلب إعداد منظومة متكاملة ومزدوجة، جناحها الاول الاصلاح القانوني والتشريعي، والجناح الثاني وهو الأهم وهو الاصلاح الاخلاقي والديني الذي يساهم في إعداد جيل من القادة والمدراء والمسولين القادرين على استشعار الاخطار الالكترونية ومواجهتها، و لكي يتحقق هذا فإنّ هناك مخصصات وميزانية مالية ضخمة لابد من رصدّها، لأنّه لا شيء يولد من العدم، يقول الله عز وجل إنّ الله لا يغير ما يقوم حتى يغيروا ما بأنفسهم.

قائمة المراجع:

أولاً: الوثائق الحكومية أو الرسمية

1- قانون رقم 200-03 مؤرخ في 05 أوت 2000، يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، (الجريدة الرسمية للحكومة الجزائرية، عدد 48 الصادر بتاريخ 06 أوت 2000)، المادتين 121 و 127.

2- قانون رقم 09-04 مؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، (الجريدة الرسمية للحكومة الجزائرية، عدد 47، الصادرة بتاريخ 16 أوت 2009)، المادة 02.

¹ - المرجع نفسه، ص 133.

ثانيا: الملتقيات:

- 1-البداينة ذياب موسى، الجرائم الالكترونية: المفهوم والاسباب، مداخلة مقدمة للمشاركة ضمن فعاليات الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، أيام 2-3-4، بكلية العلوم الاستراتيجية، عمان، الاردن، 2014.
- 2-بوشعور رضية الغازي والطويل أحمد، التكلفة الاقتصادية والاجتماعية لوسائل الدفع الالكترونية- تحليل التجربة الجزائرية وآفاقها، مداخلة مقدمة للمشاركة في فعاليات المؤتمر الدولي الرابع عشر حول الجرائم الالكترونية، يومي 24-25 مارس، مركز جيل البحث العلمي، طرابلس، لبنان، 2017.
- 3-نمديلي رحيمة، خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة، مداخلة مقدمة للمشاركة في فعاليات المؤتمر الدولي الرابع عشر حول الجرائم الالكترونية، يومي 24-25 مارس، مركز جيل البحث العلمي، طرابلس، لبنان، 2017.
- 4-فرام كوثر والعيماي محمد، الجريمة المعلوماتية على ضوء العمل القضائي المغربي، المعهد العالي للقضاء، بحث منجز في نهاية عملية التدريب، وزارة العدل، المملكة المغربية، 2009/2007.
- 5-عاقلي فضية، الجريمة الالكترونية واجراءات مواجهتها من خلال التشريع الجزائري، مداخلة مقدمة للمشاركة في فعاليات المؤتمر الدولي الرابع عشر حول الجرائم الالكترونية، يومي 24-25 مارس، مركز جيل البحث العلمي، طرابلس، لبنان، 2017.

ثالثا: المواقع الالكترونية

- 1-موسوعة الجزيرة- فضاء من المعرفة الرقمية، الجرائم الالكترونية...عندما تصبح التقنية وسيلة للاجرام، في الموقع الالكتروني:

<https://www.aljazeera.net/encyclopedia/conceptsandterminology>, 2015/11/13.

- 2-حريشان حسام، 500 جريمة إلكترونية في 2015 ن جريدة الخبر أنظر موقع:
<https://www.elkhabar.com/press/article/98286/500>
- 3-موقع ثقافة ومجتمع، الجريمة الالكترونية بالجزائر- الفضيحة أعتى أسلحة الجناة، في الموقع الالكتروني:

<https://www.dw.com,10-02-2018,pp02,03>.

4-مركز مكافحة الجرائم الإلكترونية بالدرك الوطني: معالجة 100 قضية تتعلق بالطفولة والمراهقين و
20 جريمة مالية خلال 2017، أنظر موقع:

<https://www.djazairess.com/echchaab/107048>

5-عميرة أيسر. الجرائم الإلكترونية في الجزائر. موقع انترنت:

<http://www.almayadeen.net/articles/blog/714137>

6- <https://www.alwatanvoice.com/arabic/news/2016/06/19> 6-

مظاهر القصور عن مواجهة الجريمة المعلوماتية- الحالة الجزائرية نموذجاً

د/ ذبيح ميلود

كلية الحقوق والعلوم السياسية- جامعة المسيلة

مقدمة:

الجريمة الإلكترونية هي كل اعتداء يستهدف نظاماً معلوماتياً بأي شكل من الأشكال ، أو هي كل سلوك سلمي أو إيجابي يتم بموجبه الاعتداء على البرامج والمعلومات للاستفادة منها بأي صورة كانت ، وعرفها المجلس الأوروبي بأنها " كل تغيير في معطيات أو بيانات أو برامج الحاسوب أو محوها أو كتابتها ، أو أي تدخل آخر في مجال إنجاز البيانات أو معالجتها ، بما يتسبب في ضرر اقتصادي أو قصد حيازة ملكية شخص آخر " ¹ ، والملاحظ من خلال هذه التعاريف أن بعضها يعرف الجريمة من خلال موضوعها ، والعض الآخر يعرفها من منطلق أهدافها ، والبعض يوسع في مدلولها ويضيق العض الآخر من هذا المدلول ، مما يعني افتقار هذه التعاريف لوحدة التعريف والتصور ، وذلك عائد ولا شك للتعقيد الذي يطبع الجريمة نفسها باعتبارها تعتمد أحدث التقنيات الإلكترونية ، وهذا انعكس بالسلب على أساليب مكافحتها ، وجعل هذه الأساليب قاصرة إلى حد بعيد عن مواجهة هذه الجريمة

ولأجل ذلك سنركز على أهم مواطن القصور عن الحد من هذه الجريمة ، بالتركيز على القصور التشريعي في منظومتنا القانونية تحديداً ، ثم تناول الأسباب الأخرى للقصور تساهم في تكبيل جهود مكافحة هذه الجريمة ضمن النقاط التالية:

أولاً : مظاهر القصور التشريعي عن مواجهة الجريمة المعلوماتية

تواجه الأجهزة الحكومية والأمنية تحديداً تحدي مكافحة الجريمة الإلكترونية بجملة من الآليات القانونية والأمنية ، غير أنها لم تفلح في السيطرة على هذه الجريمة ، ويعود ذلك إلى طبيعة الجريمة

¹ - د. سومية عكور ، الجرائم المعلوماتية وطرق مواجهتها ، قراءة في المشهد القانوني والأمني ، ورقة قدمت في الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية ، عمان - الأردن ، سنة 2014 ، ص 3 .

نفسها ، وإلى صعوبة ضبطها ومواكبة التطورات المذهلة التي تشهدها إبداعات مرتكبيها ، مما جعل جل هذه الآليات قاصرة عن الحد من هذه الجريمة ، ولعل أهم مواطن القصور تتحدد في التشريعات التي سنّها المشرع الجزائري لمحاربة هذه الجريمة ، ويتجلى هذا القصور في نصوص قانون العقوبات وقانون الإجراءات الجزائية والقوانين الخاصة ، وهو ما سنفصله كالتالي :

1- القصور في مواد قانون العقوبات

يكرس الدستور الجزائري مبدأ عدم انتهاك حرمة الإنسان ويضمن حقوقه وحرياته ، كما يضمن حرية الابتكار الفكري والعلمي والفني ، وكذا حقوق المؤلف بموجب المادة 38 والمادة 44 منه ، وتم تعديل قانون العقوبات وقانون الإجراءات الجزائية وسن قوانين خاصة تتعلق بهذه الجريمة ، وهذه التشريعات هي من ضمن مساعي المشرع لمواكبة التشريعات الدولية بخصوص مكافحة الجريمة المعلوماتية¹ ، فقد تم تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156 المتعلق بقانون العقوبات ، وتضمن هذا التعديل ثمانية مواد من المادة 394 إلى المادة 394 مكرر⁷، وتم إدخال تعديل على قانون العقوبات أيضا بموجب القانون رقم 06-03 المؤرخ في 20 ديسمبر 2006 بقصد تشديد العقوبات الخاصة بالجريمة الماسة بالأنظمة المعلوماتية بالمادة 394 مكرر²⁷، وأورد التعديل الأخير تحديدا وحصرًا للجرائم الالكترونية وهي : - الغش أو الشروع فيه في المعالجة الآلية - حذف أو تغيير المعطيات المنظمة - إدخال تعديل في نظام المعلومات - تصميم أو بحث أو تجميع أو توفير أو نشر أو اتجار - حيازة أو إفشاء أو نشر أو استعمال المعطيات - تكوين جمعيات أشرار .

وحدد قانون العقوبات المعدل والمتمم العقوبات المقررة لهذه الجرائم³، وهي تتراوح بين شهرين وثلاث سنوات حبس ، وبالغرامة من 50000 إلى مليوني دينار جزائري¹ ، بالإضافة إلى العقوبات التكميلية الممثلة في الغلق والمصادرة .

¹-فضيلة عاقللي ، الجريمة الالكترونية وإجراءات مواجهتها في التشريع الجزائري ، مركز جيل البحث العلمي ، بيروت - لبنان ، الموقع الالكتروني www.jilrc.com

² -نفس المرجع

³ - مثال ذلك مت نصت عليه المادة 394 مكرر من نفس القانون : " يعاقب بالحبس من 3 أشهر إلى سنة وبغرامة مالية من 50000 إلى 10000 دينار جزائري كل من يدخل عن طريق أو يبقى عن طريق الغش في كل جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك .

ويظهر القصور في قانون العقوبات من خلال:

- 1- غياب الصرامة والحزم في التعامل مع مرتكبي الجرائم الإلكترونية ، فالعقوبات تتراوح بين شهرين وثلاث سنوات وفرض غرامات على الجناة ، وكان الأولى هو التشدد مع الجناة للردع ، واقتصر قانون العقوبات على ذكر جملة من الجرائم وإغفال بعضها .
- 2- اعتماد التعميم في التجريم مما يعقد مهمة القاضي ويتعارض في نفس الوقت مع مبدأ شرعية الجريمة والعقوبة ، فالصياغة عامة بخصوص الركن المادي للجريمة تحديدا ، كما أن قانون العقوبات لم يعرف تعريفا دقيقا للجريمة المعلوماتية بل اكتفى بالنص على وقائع يمكن أن تسند إلى أشخاص معنويين أو طبيعيين.
- 3- لم يراع هذا القانون طبيعة الجريمة باعتبارها جريمة متغيرة ومستمرة ومتطورة بتطور الوسائل التكنولوجية².

2- القصور في مواد قانون الإجراءات الجزائية والنصوص الخاصة

ينسجم قانون الإجراءات الجزائية الجزائي المعدل مع الجرائم المستحدثة الخاصة بجرائم المعلوماتية المنصوص عليها في قانون العقوبات ، حيث أضاف هذه الجريمة إلى غيرها من الجرائم الماسة بأمن الأشخاص والمؤسسات ، فحدد إجراءات متابعة مرتكبي هذه الجرائم ، حيث نص في المادة 65 مكرر منه على إجراءات متابعة الشخص المعنوي ، وهذا بالمواد من المادة 65 مكرر 1 إلى المادة 65 مكرر 4 ، وبالفصل الرابع منه تحت عنوان " في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور " بالمواد من 65 مكرر 5 إلى المادة 65 مكرر 10 ، وتعتزض عملية المتابعة مسألة خصوصية الجريمة المعلوماتية، وتحدي شرعية التجريم والعقوبة ، وعدم مواكبة هذا القانون للتشريعات الدولية في مجال المتابعة وإثبات الجريمة .

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة ، وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 إلى 150000 دينار جزائري.

¹- انظر : المواد من 394 مكرر إلى المادة 394 مكرر 7 من القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 ، جر رقم 71 المؤرخة في 10 نوفمبر 2004

²- بن دعاس فيصل ، إشكالات الجريمة المعلوماتية في التشريع الجزائري ، ورقة قدمت بمجلس قضاء قسنطينة ، الموقع الإلكتروني ، سنة 2015 ، ص 4 faycel.bendaas@gmail.com

أما أهم النصوص الخاصة التي خصت هذه الجريمة بالعناية هو النص المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها رقم 09-04¹ ، حيث حدد المادة 2 منه هذه الجرائم ، ومراقبة الاتصالات الاليكترونية بالمادة 4 ، والقواعد الإجرائية لتفتيش المنظومات المعلوماتية بالمادة 5 ، وحجز المعطيات من المادة 6 إلى المادة 8 ، ونصت المادة 13 على إنشاء هيئة وطنية لمكافحة هذه الجريمة ، وركزت المادتان 15 ، 16 على التعاون والمساعدة القضائية الدولية .

وعلى الرغم من أن المشرع الجزائري أولى مكافحة هذه الجريمة عناية خاصة ، وأبرزت التشريعات تحكما نسبيا في هذه الجريمة إلا أن النصوص التشريعية تظل قاصرة وناقصة ومبتورة وتتصف بالعمومية ، ويظهر القصور أيضا في:

- 1- أن أغلب المصطلحات التقنية الواردة به غير واضحة ، وهذا إلى الحد الذي يقتضي وضع نصوص خاصة لهذه المصطلحات لتحديدتها وتوضيحها ز
- 2- كما أن القانون لا يبرز حقوق وواجبات المتعاملين مع الأجهزة الإلكترونية ، فتوضيح وتحديد المصطلحات يساعد على تفادي التهرب من المسؤولية الجزائية والمدنية ، ويسهل عمل القضاة في هذا المجال² .
- 3- أن هذا القانون لا يواكب التطور المذهل لأساليب ارتكاب هذه الجريمة ، وتبقى بعيدة عن التطورات التي تشهدها التشريعات الدولية ، مما يقتضي معه إجراء تعديلات على النصوص بما يتوافق مع أساليب الإجرام المعلوماتي ، وإصدار نصوص جديدة تأخذ بعين الاعتبار هذا التطور .

ثانيا : أسباب أخرى للقصور عن مواجهة الجريمة المعلوماتية

من أهم أسباب القصور التي تعيق مواجهة الإجرام المعلوماتي هي القصور في التشريعات المنفرقة الواردة في نصوص جزائية مختلفة ، وتتحدد أساسا في إجراءات التحري ، وفي تفتيش المنظومة المعلوماتية ، وفي إجراءات حجز المعطيات المعلوماتية أو في إجراءات حفظها، وكذا عدم التدقيق

¹ -انظر القانون رقم 09-04 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصالات ومكافحتها ، ج ر رقم 47 مؤرخة في 16 أوت 2009 .

- نفس المرجع ، ص 6 .²

والتفصيل في بعض النصوص ، ونموذج ذلك ما نص عليه الأمر رقم 03- 05 بخصوص جرائم الملكية الفكرية ، ومنها جريمة التقليد، كما تم سن النص والتي تستهدف الحماية الجزائية للمصنفات الأدبية والفنية ، غير أن هذه النص لا تشير إلى حماية المصنفات المنشورة على الأنترنت ، كما أن المشرع الجزائي لا يعاقب على التحميل غير الشرعي للملفات الاليكترونية من الانترنت بينما يعاقب المشرع الفرنسي على ذلك¹ .

ومن أهم الصعوبات المسجلة والتي تكبل جهود الحد من الجريمة المعلوماتية:

- 1- التراخي والإحجام عن الإبلاغ عن الجريمة .
 - 2- صعوبة إثبات الجريمة إذ تعد من العوائق التي تحد من فعالية المتابعة .
 - 3- كما تطرح مشكلة الاختصاص نفسها فأى من الجرائم يسند على المحاكم العادية وأي منها يسند إلى الأقطاب الجزائية المتخصصة .
 - 4- إشكالية التجريم المزدوج وقصور التعاون الدولي في هذا المجال .
- وللتفصيل سنتناول بالشرح أهم هذه الصعوبات والعوائق التي تعترض الحد من الجريمة المعلوماتية فيما يأتي :

1- عقبات إثبات الجريمة المعلوماتية :

من أهم العقبات التي تعترض المحققين في الجرائم الاليكترونية هو أنهم تعودوا على الاعتماد على الوسائل المعهودة التقليدية في جمع الأدلة لإثبات الجريمة من خلال الإثبات المادي ، غير أنه في مجال الجريمة الاليكترونية يختلف الأمر إذ أنه من غير الممكن تطبيق الإجراءات التقليدية على المعلومة المعنوية² ، وتحدد صعوبة الإثبات أيضا في :

- **القدرة على إخفاء الأدلة** : يلجأ مرتكبو الجرائم الاليكترونية إلى التلاعب غير المرئي في تسجيل البيانات لإخفاء أدلة إدانتهم ، فهم يحتكرون التجسس ونسخ الملفات المغفلة ، واختراق قواعد البيانات وتخريب الأنظمة، مع قدرتهم على محو الأدلة بيسر وسهولة وبالسرية المطلوبة ، ويعد تستر

- بن دعاس فيصل ، المرجع السابق ، ص 14¹

²- د. عادل عبد الناصر ، مظاهر صعوبة إثبات الجريمة الاليكترونية ، مجلة " مصريون " الاليكترونية ، الموقع

الاليكتروني: www.almasrione.com

المؤسسات المالية تحديدا على هذا الاختراق خشية فقدان الزائن الثقة بها عاملا مساعدا على إخفاء الأدلة .

- تضليل المحققين حين البحث عن الأدلة : لإعاقة الوصول إلى الدليل يوظف المجرمون كلمات السر والأسماء المستعارة والتشفير والبريد الإلكتروني بشكل يصعب معه تحديد هوياتهم ، ويتيح لهم ذلك ارتكاب جرائم القتل والتخريب والنصب دون العثور عليهم ، فهم مجرمون محترفون لهم القدرة الفائقة على تضليل ملاحقيهم¹ .

ب- عائق قلة الخبرة والتخصص :

بالنظر إلى الطبيعة غير المادية للبيانات المخزنة ومضمون في يجعل من الصعب على المحقق فك رموزها ، وحتى على فرض تحصيل الدليل الإلكتروني من الحاسوب فإن المحقق قليل الخبرة يصعب عليه فهم هذا الدليل² ، فخبرة المحقق وتخصصه عامل مهم وأساسي في تحصيل الدليل وفك رموزه ، ولأجل ذلك فإن تطعيم خبرات المحققين بالتكوين والتدريب ، واعتماد التجارب الدول المتطورة في هذا أصبح ضرورة تقتضيها مكافحة الجريمة³ .

ج- قصور وخذلان التعاون الدولي في ملاحقة المجرمين :

يتجلى التعاون الدولي في مكافحة الجريمة الإلكترونية في تبادل المعلومات بين أجهزة الشرطة ، وفي تعقب المجرمين الفارين عبر الدول ، وفي مجال المساعدة القضائية وفي تسليم المجرمين ، وفي غيرها من أشكال التعاون ، والتي تتم من خلال اتفاقيات دولية أو من خلال اتفاقيات ثنائية بين الدول ، ولم يشذ المشرع الجزائري عن هذا التوجه فقد تبنى جل أدوات التعاون منها المساعدة القضائية الدولية في هذا المجال ، وتبادل المعلومات وإجراءات الردع ، وتبادل الإنابة القضائية الدولية ، ومثال ذلك ما ورد بالمادة 16 الفقرة الأولى من القانون 04-09 " في إطار التحريات أو التحقيقات القضائية

- نفس المرجع¹.

²- الدليل الإلكتروني هو مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التي يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية . انظر : إشكالية الحصول على الدليل الإلكتروني في الجريمة المعلوماتية ، الموقع الإلكتروني : www.alkanonia.com

- د. عادل عبد الناصر ، نفس المرجع³ .

الجارية لمعينة الجرائم المشمولة لهذا القانون وكشف مرتكبيها ، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الاليكتروني " ¹ فالتعاون الدولي ضروري بل هو إلزامي في مجال الجريمة الاليكترونية ² ، فالدولة لا تستطيع وحدها مكافحة الجريمة المعلوماتية إذا كان مرتكب الجريمة يقيم في بلد ويرتكب جريمة تمس باقتصاد أو أمن دولة أخرى وهو لا يغادر موطنه ³ .

غير أن هذا التعاون تعترضه جملة من الصعوبات جعلته قاصرا على الحد من الجريمة، ومن أسباب هذا القصور عدم وجود نموذج موحد للنشاط الإجرامي ، وتنوع واختلاف النظم القانونية الإجرائية ، إضافة إلى التعارض والاختلاف بين التشريعات بين الدول ، واختلاف أساليب أجهزة التفتيش ، واختلاف شروط وإجراءات تمديد الاختصاص والإنابة القضائية ، فكل ذلك يعد عقبة أمام التحكم في الجريمة الاليكترونية بمختلف أشكالها ، وحتى تتحقق أهداف التعاون الدولي ينبغي توحيد التشريعات الإجرائية وتوحيد نظم إثبات هذه الجرائم ، وإنشاء مكاتب متخصصة لجمع المعلومات عن مجرمي المعلوماتية ، وتعاون أجهزة الدول في هذا المجال ⁴ ، فنقص التعاون الدولي من شأنه أن يخلق ثغرات يساعد على إفلات المجرمين من العقاب فتزيدهم ثقة بقدراتهم ⁵ ، فيصعب حينها ويتعقد ويتشابك الحد من هذه الجريمة .

- انظر المادة 16 ف1 من القانون رقم 09-04 المرجع السابق ¹ .

² - لقد تبلور هذا التعاون في إنشاء المنظمة الدولية للشرطة الجنائية " الأنتربول " وتتولى إقامة العلاقات بين الدول المنتمية إلى المنظمة وتبادل المعلومات بين سلطات التحقيق والقبض على المجرمين الفارين من العدالة ، كما تبلور التعاون الدولي في إنشاء المجلس الأوروبي سنة 1991 بتشكيل شرطة أوروبية تختص بملاحقة الجرائم العابرة للحدود " انظر : د. جميل عبد الباقي الصغير ، الجوانب الإجرائية المتعلقة بجرائم الانترنت ، دار النهضة العربية - القاهرة ، سنة 2001 ص 87 .

³ - أحمد مسعود مريم ، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون رقم 09-04، مذكرة

ماجستير ، جامعة قاصدي مرباح ورقلة - كلية الحقوق ، سنة 2013 ، ص 58

- د. جميل عبد الباقي الصغير ، المرجع السابق ، ص 79⁴

⁵ - رابع وهيبة ، الجريمة المعلوماتية في التشريع الجزائري الجزائري ، مجلة الباحث للدراسات الأكاديمية ، العدد الرابع ، ص 330 .

وملخص القول أن الجهود المبذولة في مجال مكافحة الجريمة المعلوماتية في الجزائر معتبرة ، ويتم التركيز بالدرجة الأولى على الجرائم التي تهدد الأمن والنظام العام على الخصوص ، غير أن هذه المساعي ليست بالفعالية والنجاعة المطلوبة في ظل القصور التشريعي والطبيعة المعقدة والمتشابكة للجريمة ، وكذا قصور التعاون الدولي والتجريم المزدوج ، مما يقتضي مراجعة النصوص التشريعية ذات الصلة ، ومواكبة الإجراءات للتطور المذهل لأدوات الإجرام الإلكتروني ، واعتماد التعاون الدولي والاستفادة من الخبرات والتجارب الدولية في هذا المجال لتفعيل أداء أجهزة مكافحة الجريمة الالكترونية .

آليات مكافحة الجريمة المعلوماتية في النظام المصرفي الجزائري

ط.د/ دبش رياض

كلية الحقوق والعلوم السياسية - جامعة سطيف 2

مقدمة:

أثر التطور السريع للتكنولوجيا في العالم على تطور الجريمة في الجزائر وباقي دول العالم، حيث سعت جل دول العالم إلى تكريس منظومة قانونية لمكافحة الجرائم المعلوماتية، وعلى اعتبار أن القطاع المصرفي يعتبر من أهم القطاعات التي تستهدفها الجرائم المعلوماتية فقد سعى المشرع الجزائري إلى تكريس مجموعة من النصوص القانونية والتنظيمية للوقاية والحد من انتشار هذه الجرائم. حيث بادر المشرع الجزائري إلى مجموعة من الإصلاحات المصرفية في مجال الجرائم المعلوماتية، خاصة في ظل الإصلاحات الاقتصادية التي تلت تكريس الحرية الاقتصادية في الجزائر، حيث كرس المشرع الجزائري قانون خاص بالنقد والقرض صادر بموجب الأمر (03-11) المعدل والمتمم، كما كرس كذلك مجموعة من النصوص التنظيمية الصادرة عن بنك الجزائر في مجال الوقاية من الجرائم الإلكترونية.

أولاً: أهمية الدراسة

يكتسي موضوع مكافحة الجرائم المعلوماتية من طرف النظام المصرفي الجزائري أهمية كبيرة في الدراسات الحديثة كون أن هذا الأخير يعد من أهم العوامل المساعدة في تطور الدول في شتى المجالات على غرار المجال الاقتصادي وكذا السياسي والاجتماعي، وعلى اعتبار أن أغلب الجرائم المعلوماتية ترتبط بالمال والأعمال وعليه فإن النظام المصرفي الجزائري يعد حلقة جوهرية في مكافحة الجرائم المعلوماتية.

ثانياً: أهداف الدراسة

تهدف الدراسة إلى توضيح مدى نجاعة أنظمة بنك الجزائر في الوقاية من الجرائم الإلكترونية وكذا عن مدى تمكين النظام المصرفي الجزائري من آليات قانونية فعالة للحد من هذه الجرائم ومكافحتها، كما تهدف الدراسة أيضاً إلى توضيح فيما إذا خصصت الدولة الجزائرية أجهزة وهيكل خاصة بالجرائم المعلوماتية.

ثالثا: أسباب اختيار الموضوع.

بالنسبة للعامل الذاتي لاختيار الموضوع فهو الميول لكل المواضيع التي تتسم بالحدثية والارتباط بالتكنولوجيا الحديثة، وخاصة ما يتعلق بالنظام المصرفي في الجزائر.

بالنسبة للعامل الموضوعي فهو يرتبط بأهمية الموضوع خاصة بعد الإصلاحات التي قام بها المشرع الجزائري لتكريس وتطوير التجارة الإلكترونية وكذا العمليات المصرفية عن بعد.

رابعا: منهجية الدراسة.

من أجل الإجابة عن الإشكالية المطروحة فقد تم الاعتماد على المنهج الوصفي التحليلي من أجل تحديد الآثار القانونية المترتبة على تكريس منظومة قانونية خاصة بمكافحة الجرائم المعلوماتية الماسة بالنظام المصرفي الجزائري.

خامسا: اشكالية الدراسة.

بما أن المشرع الجزائري قد كرس منظومة قانونية خاصة بالنظام المصرفي، وعلى اعتبار أن حماية النظام المصرفي الجزائري يحتاج إلى تكريس نظام قانوني خاص بالوقاية من كل الجرائم الماسة به، وعلى هذا الأساس يمكن طرح الإشكالية التالية:

ماهي الآليات الموضوعية والإجرائية الخاصة التي اعتمدها المشرع الجزائري في الوقاية من جرائم المعلوماتية الماسة بالنظام المصرفي الجزائري؟

سادسا: خطة الدراسة.

للإجابة عن الإشكالية المطروحة والمتعلقة بالقواعد الموضوعية والإجرائية الخاصة بمكافحة جرائم المعلوماتية الماسة بالنظام المصرفي الجزائري، سنتناول الدراسة وفق خطة مقسمة على النحو التالي:

المحور الأول: الأحكام الموضوعية المميزة للجرائم المعلوماتية الماسة بالنظام المصرفي الجزائري.

أولا: مفهوم الجريمة المعلوماتية وعلاقتها بالنظام المصرفي الجزائري.

ثانيا: أركان الجريمة المعلوماتية.

المحور الثاني: الأحكام الإجرائية الخاصة بمكافحة جرائم المعلوماتية الماسة بالنظام المصرفي.

أولا: إجراءات متابعة جرائم المعلوماتية في التشريع الجزائري

ثانيا: الأجهزة المختصة في متابعة جرائم المعلوماتية.

المحور الأول: الأحكام الموضوعية المميزة للجرائم المعلوماتية الماسة بالنظام المصرفي الجزائري.

خضع النظام المصرفي الجزائري لمجموعة كبيرة من الإصلاحات الاقتصادية، خاصة مع التحول الاقتصادي التي مرت به الجزائر، فكان قانون النقد والقرض (90-10) أول النصوص القانونية التي مهدت للحرية الاقتصادية في المجال المصرفي، لكن المشرع الجزائري قد سارع إلى تكريس قانون النقد والقرض الصادر بموجب الأمر (03-11) والذي جاء بمجموعة من الأنظمة الصادرة عن بنك الجزائر في مجال مكافحة الجرائم الإلكترونية الماسة بالنظام المصرفي، وعليه لا بد من التطرق أولاً إلى الأحكام الموضوعية المميزة للجرائم المعلوماتية والماسة بالنظام المصرفي الجزائري (أولاً).

ثم التطرق إلى الأحكام الإجرائية الخاصة بالحد ومكافحة جرائم المعلوماتية الماسة بالنظام المصرفي الجزائري وخاصة منها ما يتعلق بالجانب المعلوماتي الجانب المالي (ثانياً).

أولاً: مفهوم الجريمة المعلوماتية وعلاقتها بالنظام المصرفي الجزائري.

يكتسي القانون المصرفي أهمية بالغة بالنسبة لكل دول العالم، فهو الأداة الرئيسة التي تمكن الدولة من النهوض باقتصادها، فنجاح الدول الحديثة يقاس بمنظومتها المصرفية القوية والتي تخلو من الثغرات، خاصة في ظل تطور التكنولوجيا الحديثة من جهة وتطور جريمة قرصنة المعلومات من جهة ثانية.

تعتبر الجريمة المعلوماتية من بين الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها التي ارتبطت بتقنية المعلومات، فقد اصطلح على تسميتها بداية "بإساءة استخدام الكمبيوتر"، ثم "احتيال الكمبيوتر"، "الجريمة المعلوماتية"، بعدها "جرائم الكمبيوتر"، و"الجريمة المرتبطة بالكمبيوتر"، ثم "جرائم التقنية العالية"، إلى "جرائم الهاكرز"، "جرائم الأنترنت"، وأخيراً "السيبر كرايم".¹

ويعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها: الجريمة التي تلعب فيها البيانات الحاسوبية، والبرامج المعلوماتية دوراً رئيسياً، وقد اتجه جانب كبير من الفقهاء إلى اعتماد التعريف الذي تبنته منظمة التعاون الاقتصادي والتنمية (OCDE) للجريمة المعلوماتية في اجتماع باريس عام 1983، من أنها: كل سلوك غير مشروع، أو غير أخلاقي، أو غير مصرح به، يتعلق بالمعالجة

1 سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، ع 07، جامعة محمد خيضر، بسكرة،

أفريل 2010، ص 275.

الآلية للبيانات أو نقلها، وهو تعريف تبني أكثر من معيار، يتعلق الأول بوصف السلوك، أما الثاني فاتصال السلوك بالمعالجة الآلية للبيانات أو نقلها.¹

ثانيا : أركان الجريمة المعلوماتية:

من خلال التعريف السابق يتضح أنه لقيام الجريمة المعلوماتية توفر ركنين أساسيين هما الركن المادي وكذا الركن المعنوي، وبدون هذين الركنيين لا تقوم الجريمة.

1- الركن المادي للجريمة المعلوماتية:

تتكون الجريمة المعلوماتية كغيرها من الجرائم من الركن المادي للجريمة، والذي يفترض وجوده لقيام الجريمة، حيث يتكون هذا الركن من ثلاث عناصر نجملها كالتالي:

❖ الفعل أو السلوك غير المشروع:

يتطلب القيام بالجريمة المعلوماتية وجود جهاز الحاسوب أو الجهاز المعلوماتي وكذا الاتصال بشبكة الأنترنت أو الشبكات المحلية، وكذلك يفترض قدرة الجاني الذهنية والجسمانية على تجهيز الحاسوب، لكي يتحقق له حدوث الجريمة، فيقوم بتحميل الحاسب ببرنامج اختراق، أو يقوم بإعداد هذه البرامج بنفسه أو يقوم بإعداد برامج فيروسات تمهيدا لبثها.

أما من الناحية القانونية فإن السلوك أو الفعل غير المشروع في الجريمة المعلوماتية له عدة صور وتختلف هذه الصور للسلوك أو الفعل غير المشروع من تشريع إلى تشريع آخر، فتح أن المشرع الجزائري قد استعمل مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة ويمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي لا بد من تحقيقه حتى يمكن البحث في توافر أو عدم توافر أركان الجريمة.²

إن الركن المادي للجريمة الإلكترونية يقوم على صورتين أساسيتين:

➤ الصورة الأولى: متمثلة في الاعتداء على نظام المعالجة الآلية وهذه الأخيرة تحتوي

على نوعين من الاعتداء:

1 مليكة عطوي، الجريمة المعلوماتية، حوليات جامعة الجزائر، ع 21، جوان 2012، ص 08.

2 لورنس سعيد الحوامدة، الجرائم المعلوماتية أركانها وآلية مكافحتها دراسة تحليلية مقارنة، جامعة طيبة المملكة العربية السعودية، ص 12.

✓ **النوع الأول:** وهو الدخول والبقاء غير مشروع في نظام المعالجة الآلية وتنطوي تحت هذا النوع ثلاث أفعال هي فعل الدخول والبقاء وعرقلة أو التعطيل.

✓ **النوع الثاني:** متمثل في الاعتداء العمدي على نظام المعالجة الآلية للمعطيات وتندرج تحت هذا النوع كذلك ثلاث أفعال وهي فعل الإدخال والمحو والتعديل .

➤ **الصورة الثانية:** متمثلة في الاعتداء على منتجات الإعلام الآلي وتحتوي هذه الصورة على فعل التزوير المعلوماتي.

❖ النتيجة الإجرامية:

تعد النتيجة الإجرامية أحد أهم عناصر الركن المادي لأي جريمة، حيث تعتبر النتيجة الجرمية الأثر المباشر للسلوك الجرمي غير المشروع، وفي كثير من الأحيان لا يحدد القانون على وجه التفصيل أوصاف السلوك المحظور، بل يكفي بذكر النتيجة الجرمية، حيث يحدد أوصاف السلوك بناء على طبيعة النتيجة الجرمية.

2- الركن المعنوي للجريمة المعلوماتية:

الركن المعنوي للجريمة المعلوماتية يختلف باختلاف أشكالها، وعلى اعتبار أن الموضوع يرتبط بالجريمة المعلوماتية الماسة بالنظام المصرفي ارتأينا التعرض للركن المعنوي للجرائم المعلوماتية الماسة بالنظام المصرفي.

❖ جريمة الدخول والبقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات:

إن جريمة الدخول والبقاء غير المشروع هي جرائم عمدية تتطلب قصدا جنائيا وذلك بنص المادة 394 مكرر قانون العقوبات الجزائي التي عبرت عن القصد الجنائي بنصها "كل من يدخل أو يبقى عن طريق الغش"¹، وتعني هذه العبارة أن الفاعل له كامل العلم بأن الدخول أو البقاء غير مشروع. ولتوافر القصد الجنائي لا بد أن يكون الجاني محيطا علما بكافة عناصر الجريمة وله علم بأن الفعل الذي يقوم به ينصب على نظام المعالجة الآلية للمعطيات بما يتضمنه من معلومات وبرامج وباعتبار محل الحق الذي يحميه المشرع².

1 أنظر المادة 394 مكرر من الأمر رقم (66-156)، المؤرخ 1966/06/11، المتضمن قانون العقوبات، ج ر، العدد 49، الصادر في 1966/06/11، المعدل والمتمم.

2 منصور رحمان، القانون الجنائي للمال والأعمال، دار العلوم، الجزء الأول، عناية 2012، ص 134.

بمعنى آخر أنه اتجاه إرادة الجاني اتجهت إلى فعل الدخول أو فعل البقاء و أن الجاني يعلم بأن ليس له الحق في الدخول إلى النظام والبقاء فيه. ولا يتوافر القصد الجنائي إذا كان الجاني يعتقد أن دخوله أو بقاءه داخل النظام مسموح به أي مشروع، أو كان الجاني يجهل بوجود حظر الدخول أو البقاء.

❖ جريمة الاعتداءات على سير نظام المعالجة الآلية للمعطيات:

إن جريمة الاعتداء على سير نظام المعالجة الآلية للمعطيات هي جريمة عمدية لأن أفعال العرقلة والتعطيل من الأفعال العمدية وهذا ما يميزه عن الاعتداء غير العمدية لسير النظام الذي يعتبر ظرفا مشددا لجريمة الدخول والبقاء غير مشروع داخل النظام، وعليه فالقصد الجنائي المفترض ينتج من طبيعة الأفعال المجرمة.

❖ الاعتداءات العمدية على المعطيات:

إن جريمة الاعتداء العمدية على المعطيات جريمة عمدية يتخذ فيها القصد الجنائي بعنصرية العلم والإرادة ، فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل¹، كما يجب أن يعلم الجاني بأن نشاطه الإجرامي يترتب عليه التلاعب في المعطيات ، ويعلم أيضا أنه ليس له الحق في القيام بذلك و أنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته. ويشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجنائي العام نية الغش، لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير بل تتوافر الجريمة ويتحقق ركنها بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذلك واتجاه الإرادة إليه، وإن كان الضرر قد يتحقق في الواقع نتيجة للنشاط الإجرامي إلا أنه ليس عنصرا في الجريمة².

❖ استخدام المعطيات كوسيلة في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية:

إن هذا الاستخدام يكون عمديا وذلك الاستخدام المتمثل في التصميم أو البحث أو التجميع أو التوفير أو النشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية ، ويكون هذا الاستخدام عن طريق الغش فلذلك يتطلب القصد الجنائي العام إضافة إلى القصد الجنائي الخاص المتمثل في نية الغش.

1 بكرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر تخصص قانون جنائي، جامعة بسكرة، السنة الجامعية 2015/2016، ص50.

2 منصور رحمان، المرجع السابق، ص 162.

المحور الثاني: الأحكام الإجرائية الخاصة بمكافحة جرائم المعلوماتية الماسة بالنظام المصرفي
بعد التطرق إلى الأحكام الموضوعية لجرائم المعلوماتية عموماً، نتطرق إلى الأحكام الإجرائية الخاصة بمكافحة جرائم المعلوماتية الماسة بالنظام المصرفي الجزائري، ولذلك لا بد من التطرق إلى إجراءات متابعة جرائم المعلوماتية في التشريع الجزائري (أولاً).

ثم نتطرق مباشرة إلى الأجهزة المختصة في متابعة هذه الجرائم (ثانياً).

أولاً: إجراءات متابعة جرائم المعلوماتية في التشريع الجزائري
لتقييم نجاح النظام المصرفي الجزائري في الحد والوقاية من هذا النوع من الجرائم لا بد من تحديد الترسنة القانونية التي نظمت هذا النوع من الإجراءات بشكل عام وكذا تحديد التنظيمات الصادرة عن بنك الجزائر بشكل خاص.

1- الآليات الإجرائية المتبعة في القانون (04-14) المتضمن قانون الإجراءات

الجزائية:

❖ **توسيع اختصاص بعض الجهات القضائية وكيل الجمهورية.**

✓ **توسيع اختصاص لوكيل الجمهورية.**

حددت المادة (37) من قانون الإجراءات الجزائية الجزائري الاختصاص المحلي لوكيل الجمهورية بصفة واضحة وموضوعية، ويعرف الاختصاص المحلي بأنه "تلك الدائرة القضائية التي يستطيع فيها وكيل الجمهورية مباشرة وظيفته بصفة مباشرة طبقاً لقانون الإجراءات الجزائية".

وعليه فإن اختصاص وكيل الجمهورية وفق المادة المذكورة أعلاه لا يمكن أن يتعدى هذه الحدود، وعلى اعتبار أن جرائم المعلوماتية باعتبارها جرائم عابرة للحدود استحدث المشرع الجزائري (الفقرة الثانية من المادة 37) من قانون الإجراءات الجزائية، ووسع من الاختصاص المحلي لوكيل الجمهورية ليشمل اختصاص محاكم أخرى شرط أن يكون عن طريق التنظيم¹.

حيث تم حصر هذا التوسيع ليشمل التحري والتحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

✓ **توسيع اختصاص قاضي التحقيق.**

1 أنظر المادة 37 من الأمر رقم 66-155 المؤرخ في 08/06/1966، المتضمن قانون الإجراءات الجزائية، ج ر، العدد رقم 48 الصادر بتاريخ 10/06/1966، المعدل والمتمم.

يتحدد الاختصاص المحلي لقاضي التحقيق وفق المادة (40) من قانون الإجراءات الجزائية الجزائري الجمهورية بناء على:

- مكان وقوع الجريمة؛
- أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها؛
- أو محل القبض على أحد هؤلاء الأشخاص حتى ولو كان القبض قد حصل لسبب آخر؛

وعليه فقد أكدت الفقرة الثانية من المادة (40) أن قاضي التحقيق مختص محليا كلما تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات. وبالتالي يمتد اختصاص قاضي التحقيق لمحاكم تتجاوز اختصاصه العادي¹.

❖ إجراءات التحقيق الابتدائي.

التحقيق الابتدائي يعتبر مرحلة من مراحل سير الدعوى الجزائية، حيث يهدف إلى التثبيت من الأدلة القائمة على نسبة الجريمة إلى فاعل معين حتى لا تعرض على المحكمة إلا الدعوى المستندة إلى أسس واقعية وقانونية متينة.

✓ التفتيش في مجال الجرائم المعلوماتية.

لم يعرف المشرع الجزائري التفتيش لكن بالرجوع على الفقه نجد يعرف التفتيش بأنه "إجراء من إجراءات التحقيق التي تهدف إلى الحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحزمة المسكن أو الشخص وذلك من أجل إثبات ارتكابها أو نسبتها إلى المتهم وفقا للإجراءات القانونية المقررة².

وعليه فالتفتيش وسيلة من أجل الإثبات المادي، لكن في المقابل فإن تفتيش المعدات الإلكترونية كالحاسب الآلي وغيره يخضع إلى ضوابط موضوعية وأخرى شكلية، حيث تلخص الضوابط الموضوعية في وقوع جريمة معلوماتية ترتكب من شخص أو عدة أشخاص ولو كانوا شركاء كما أنه

1 بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، دار الخلدونية، طبعة 2017، الجزائر 2017، ص 2016.

2 المرجع نفسه، ص 218.

يشترط للتفتيش وجود دلائل كافية تؤدي إلى الاعتقاد بأنه قد ساهم بصورة فاعل أصلي أو شريك¹، وأما بالنسبة للضوابط الموضوعية فإنها ترتبط بالحريات الفردية وحمايتها من التعسف في استعمال السلطة وهي ضرورة حضور شخص أثناء عملية التفتيش كما أكدت ذلك المادة (47) مكرر التي تنص أنه إذا كان الشخص المراد تفتيش منزله موقوفا للنظر أو محبوسا في مكان آخر، فإنه لا بد أن يتم التفتيش بحضور شاهدين مسخرين وفق أحكام نفس المادة، وفي حالة مخالفة هذه الأحكام فإن البطلان هو الأثر القانوني الذي يترتب بعد ذلك.

✓ وقت إجراء التفتيش.

عكس القواعد العامة المحددة لوقت التفتيش، فإن الفقرة الثانية من المادة (47) قد سمحت بإجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني وبأي ساعة من ساعات النهار أو الليل فيما يخص جرائم الاعتداء على نظم المعطيات للمعالجة الآلية شرط الحصول على إذن مسبق من وكيل الجمهورية المختص، وهو ما يعتبر خروجاً عن قواعد التفتيش العامة المحددة في المادة (47) التي تحدد مواقيت التفتيش من الساعة الخامسة صباحاً إلى الثامنة ليلاً.²

✓ التفتيش في مجال الجرائم المعلوماتية.

بالنسبة لمحضر التفتيش المعد بخصوص جرائم المعلوماتية فإن عدة إشكالات قانونية تثار في هذه المسألة، فالجريمة غالباً ما تتجاوز حتى الإقليم الوطني، كما أن الوصول إلى الطرف الثاني يعطي الفرصة للتخلص من البيانات التي يستهدفها التفتيش.

2- الآليات الإجرائية المتبعة في القانون (04-09) المتضمن القواعد الخاصة للوقاية

من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:

✓ التعاون والمساعدة القضائية الدولية.

أشارت المادة (15) من القانون (04-09) أن المحاكم الجزائية تختص بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبياً وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني، كما أكدت

1 المرجع نفسه، ص 218.

2 بن مكي نجا، المرجع السابق، ص 221.

المادة (16) من نفس القانون أنه في إطار التحريات أو التحقيقات القضائية الجارية يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني، كما يمكن في حالة الاستعجال ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل قبول طلبات المساعدة القضائية.¹

ثانيا: الأجهزة المختصة في متابعة جرائم المعلوماتية.

✓ إنشاء الهيئات الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

نصت المادة (13) من القانون (04-09) على إنشاء هيئات وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها والتي تعتبر سلطات إدارية مستقلة لدى وزير العدل، حيث تظم الهيئة قضاة وضباط وأعوان الشرطة القضائية التابعين لمصالح الاستعلام العسكرية والدرك الوطني والأمن القومي وفقا لأحكام قانون الإجراءات الجزائية.

كما أن بنك الجزائر ممثلا في مجلس النقد والقرض، وكذا اللجنة المصرفية قد مكنهما قانون النقد والقرض الصادر بموجب الأمر (03-11) المعدل والمتمم، وتحديدًا في المادة (117) أنه بإمكانهما تبليغ المعلومات إلى السلطات المكلفة بحراسة البنوك والمؤسسات المالية في بلدان أخرى، مع مراعاة مبدأ المعاملة بالمثل، وشريطة أن تكون هذه السلطات في حد ذاتها خاضعة للسرية المهنية.²

خاتمة:

1 المرجع نفسه، ص 233.

2 أنظر المادة 117 من الأمر رقم 03-11 المؤرخ في 26/08/2003، يتعلق بالنقد و القرض، ج ر، العدد 52، الصادر في 27/08/2003. المعدل والمتمم.

وفي الأخير نخلص إلى أن سعي الحكومة والمشرع الجزائري واضح في تجسيد آليات قانونية وتنظيمية وهيكلية من أجل الوقاية من جرائم المعلومات بشكل عام وكذا الوقاية من الجرائم المعلوماتية الماسة بالنظام المصرفي الجزائري.

النتائج:

نخلص من موضوع آليات مكافحة الجريمة المعلوماتية في النظام المصرفي الجزائري إلى مجموعة من النتائج أهمها ما يلي:

- النظام المصرفي الجزائري شريك أساسي في عملية الوقاية من الجرائم المعلوماتية، كما أنه عنصر جوهري في الجرائم الماسة بالأموال والنقود بشكل خاص.
 - عملية الوقاية من جرائم المعلوماتية الماسة بالنظام المصرفي تحتاج إلى هياكل مختصة بالعمليات البنكية.
 - النظام المصرفي الجزائري بحاجة ماسة إلى تكريس منظومة قانونية خاصة بالجرائم المعلوماتية الماسة والأنظمة المصرفية.
- كما نقدم في الأخير مجموعة من التوصيات التي من شأنها الحد من الجرائم المعلوماتية:
- لا بد من حملات توعوية وتحسيسية لإبراز أهمية أنظمة الحماية، خاصة ما يتعلق بالقرصنة كونها تعتبر الجريمة الأكثر شيوعا في الجرائم المعلوماتية.
 - ضرورة تكريس منظومة قانونية خاصة بالوقاية من الجرائم المعلوماتية.

قائمة المراجع:

(1) الكتب:

1- منصور رحمان، القانون الجنائي للمال والأعمال، دار العلوم، الجزء الأول، عنابة 2012

2- أيمن بن مكي نجا، السياسة الجنائية لمكافحة جرائم المعلوماتية، دار الخلدونية، طبعة 2017، الجزائر 2017.

(2) المجلات العلمية:

1- سمية سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، ع 07، جامعة محمد خيضر بسكرة، أفريل 2010.

(3) حوليات ودراسات:

1- مليكة عطوي، الجريمة المعلوماتية، حوليات جامعة الجزائر، ع 21، جوان 2012،

2- لورنس سعيد الحوامدة، الجرائم المعلوماتية أركانها وآلية مكافحتها دراسة تحليلية مقارنة، جامعة طيبة المملكة العربية السعودية.

(4) النصوص القانونية والتنظيمية:

أ) النصوص التشريعية:

1- أمر رقم 66-155 المؤرخ في 08/06/1966، المتضمن قانون الإجراءات الجزائية،

ج ر، العدد رقم 48 الصادر بتاريخ 10/06/1966.

2- أمر رقم 66-156، المؤرخ في 11/06/1966، المتضمن قانون العقوبات، ج ر،

العدد 49، الصادر في 11/06/1966.

معوقات التحقيق في الجرائم المعلوماتية الدولية وسبل مواجهتها

د/ حيزوم بدر الدين مرغني

كلية الحقوق والعلوم السياسية

جامعة الوادي

د/ مقرووف محمد

كلية الحقوق والعلوم السياسية

جامعة المسيلة

مقدمة:

لقد كان من نتائج التطور التقني الذي عرفه المجتمع البشري ظهور صور وسلوكات هددت أمن واستقرار المجتمع الدولي وضرت بمصالح الأشخاص، وذلك بسبب ارتباط جميع المصالح الحيوية بالمعلوماتية المتطورة وما رافقه ذلك من ظهور أشكال جديدة وخطيرة من الجرائم المعلوماتية تعدت حدودها حدود الدولة الواحدة لتصل إلى جميع أنحاء العالم بفعل دهاء ونفوذ مرتكبي هذه الجرائم، مما فرض معه حتمية التعامل الدولي لمكافحةها والتي لم تعد الجهود الوطنية قادرة على مجابهتها. غير أن هذا الأمر جابهه العديد من الإشكاليات المختلفة، فمنها ما هو متعلق بطبيعة ونوعية هذه الجرائم المستحدثة والمتجدد، ومنها ما هو ذا طابع وطني ومنها ما هو ذا طابع دولي يفرض على جميع الدول الوصول معه إلى حلول لمجابهتها والعمل على حلها والتغلب عليها، وهو ما سنحاول التعرض له بشئ من التفصيل في هذه الورقة البحثية.

المحور الأول: مفهوم التعاون الدولي في مواجهة الجرائم المعلوماتية

تعتبر الجرائم المعلوماتية وبالنظر للتطور العلمي والتكنولوجي وما شهدته المجتمع الدولي من طفرة تكنولوجية جعلت العالم قرية صغيرة، من أهم الجرائم ذات البعد والصدى الدولي العابر للحدود والمتجاوزة لمبدأ القومية والسيادة المستقرة في التعامل الدولي، حيث لم تعد تعتبر الحدود ولا الاجراءات الحدودية المتبعة مهما كانت صرامتها وشدتها كفيلا بأن تقف حاجزا أمام مرتكبي هذه الجرائم المعلوماتية، حيث إمتد نشاط الممارسين لهذه الجرائم ليشمل أكثر من دولة وبالتالي أصبحت هذه الجريمة بإمتياز جريمة ذات طابع دولي وهو الأمر الذي تنبعت له الأمم المتحدة حين أفردت في

مؤتمرها العاشر لمنع الجريمة ومعاملة المجرمين حلقة عمل من إحدى أربع حلقات لدراسة وتحليل الجرائم المتعلقة بالمعلوماتية، واعتبرتها أحد أهم تحديات القرن الحادي والعشرين¹.

وبالنظر لخطورة هذا الأمر فقد أصبح التعاون الدولي من أهم المبادئ القانونية لمكافحة الجريمة المعلوماتية على الصعيد الدولي وذلك مع تعدد وتشعب أنشطتها وأشكالها وأساليب ارتكابها، ورغم أن التعاون الدولي من المفاهيم القانونية التي يصعب وضع تعريف جامع لها وذلك لمجموعة من الأسباب أهمها اختلاف الرؤى السياسية التي أثرت بشكل مباشر في الموضوع، وإتساع المجال والأشكال والصور التي يمكن لهذا التعاون أن يأخذها، وكذا للتغير السريع والمستمر التي يعرفها هذا المفهوم، وأخيرا لإرتباطه بمفاهيم الجريمة والإجرام المنظم والتي يصعب وضع تصور محدد وإطار ثابت لها².

غير أن ذلك لم يمنع من محاولة وضع تعريف له إنطلاقا من أنه يمثل إحدى السبل المستخدمة لتحقيق الدرجة العالية من الانسجام مع أهداف المجتمع الدولي في منع الجريمة والحفاظ على المجتمع وصونه ووضعه في حال أفضل وذلك عن طريق الاجراءات الجماعية القسرية أو الجهود المتضافرة³ وذلك قصد مواجهة أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية⁴.

وبالنظر لخطورة هذه الجريمة فقد وجد المجتمع الدولي تبرير مواجهتها من خلال مجموعة من الاعتبارات.

فيأتي على رأس هذه الاعتبارات أن الدول ومهما بلغت قوتها العسكرية فإنه وبسبب التقدم التكنولوجي لا تستطيع بقدراتها الذاتية مواجهة التحديات الناتجة عن ظهور أنماط جديدة من الجرائم بسبب تجاوزها لمبدأ القومية والسيادة، وعدم قدرة الحدود التقليدية على ضبطها والتي يأتي من بينها الجرائم المعلوماتية.

¹ - عقد هذا المؤتمر في فيينا بين 10 و 17 أبريل 2000.

² - علاء الدين شحاته، التعاون الدولي لمكافحة الجريمة، دار النهضة العربية القاهرة، 2000، ص 18.

³ - عبد الرحمان فتحي سمعان، تسليم المجرمين في ظل قاعد القانون الدولي، دار النهضة العربية، القاهرة، 2012، ص 511.

⁴ - أسامة المناسعة - جلال الزعبي - صابيل فاضل الهواوشة، جرائم الحاسب الآلي والانترنت، دار وائل للنشر، عمان الأردن، 2001، ص 78.

ثاني هذه الاعتبارات أن الجرائم المعلوماتية وفي غالب الأحيان يصعب على القوانين الوطنية التصدي لها ومواجهتها بمفردها، حيث أنه في أغلب الأحيان ترتكب في أكثر من بلد، وأدلتها يسهل طمسها ومحوها بسهولة وسرعة، وهو الأمر الذي يتوجب معه على الدول التعاون والتنسيق في ما بينها للوصول الى تدابير دولية مشتركة قصد التعاون في مواجهتها.

ثالث هذه الاعتبارات هو تعدد صور الجرائم المعلوماتية من جمع وتخزين البيانات على نحو غير مشروع، وإساءة استخدام هذه البيانات والافشاء غير المشروع للبيانات والاعتداء على سرية الاتصالات والمراسلات وغيرها من الصور المتطورة باستمرار، قابله إن لم نقل ضعف تشريعي وطني ودولي عدم قدرة على مجازات سرعت تطور هذه الجرائم مما يوجب وبشكل مستعجل وجدي التعاون، بداية بتجريم هذه الجرائم، ثم ملاحقة مرتكبيها وبشكل عاجل¹.

وهنا فقد توجب من أجل مكافحة فعالة للجرائم المعلوماتية وبالنظر لخطورة هذه الجرائم أن يتم هذا التعاون أولاً بصورة أمنية على إعتبار أنه أحد أهم الوسائل التي يمكن من خلالها منع الجريمة المعلوماتية أو التقليل منها، حيث أن أجهزة الأمن الوطنية لا يمكنها تعقب وملاحقة المجرمين خارج حدود دولتهم، الأمر الذي أصبحت معه الحاجة ماسة الى وجود تعاون أممي دولي كاجراء حديث هدفه التحري والتحقيق في مجال مكافحة الجريمة المعلوماتية باستخدام تكنولوجيات حديثة وذلك من خلال مجموعة من الصور كربط شبكات الاتصال والمعلومات فيما بينها من أجل سرية التواصل، وأيضاً إمكانية القيام ببعض العمليات المشتركة كتعقب المجرمين وتعقب وضبط وحفظ الأدلة ولقيام بإجراءات التفتيش العابرة للحدود وغيرها من الاجراءات المساعدة في هذا المجال².

ثاني صورة للتعاون هو التعاون القضائي ذلك أم ملاحقة مرتكبي الجرائم المعلوماتية وتقديمهم للمحاكمة تستلزم القيام بخطوات قضائية خارج حدود الدولة وهو الأمر الذي لا يمكن تحقيقه من دون التعاون القضائي الدولي، والذي يمكن أن يأخذ عدة أشكال من أهمها المساعدة القضائية الدولية والتي تنصرف الى الإجراءات القضائية التي تباشرها الدولة والتي من شأنها تسهيل المحاكمة في

¹ - محمد حماد الهيبي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2004، ص152.

² - سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الانترنت، دار النهضة العربية، القاهرة، 2013، ص415.

دولة أخرى بصدد أحد الجرائم الإلكترونية من قبيل تحليل صحف الحالة الجنائية والمساعدة في المواد الجنائية من خلال تجميع عناصر الأدلة وتقديم المعلومات والوثائق التي تطلبها السلطات القضائية في دولة أخرى وحضور الشهود الخبراء و نقل الإجراءات بموجب اتفاقيات سابقة والإجابة القضائية وغيرها من الصور التي لا تتحقق إلا بعد تقديم طلب من دولة لأخرة ومن ثم فحصه والموافقة عليه وأخيرا تنفيذ المساعدة القضائية¹.

وثالث صورة للتعاون الدولي في مجال مكافحة الجريمة المعلوماتية تتعلق بتسليم المجرمين، والذي يعتبر من أهم صور التعاون الدولي، كما انه أيضا أكثر صور الجدل وعدم الاتفاق الدولي لمساسه المباشر بالحرمة الشخصية، حيث يقوم مبدأ تسليم المجرمين على اساسى أن الدولة التي يتواجد على اقليمها المتهم بارتكاب إحدى الجرائم المعلوماتية العابرة للحدود عليها أن تقوم بمحاكمته إذا كان قانونها يسمح بذلك، و إلا فعليها تسليمه لمحاكمته في دولة أخرى تكون مختصة في ذلك²، ويكون التسليم بشروط أهمها ظان يكون التجيم مزدوج في الدولة الطالبة والمطلوب منها التسليم، وأن يشكل الفعل جريمة من الجرائم الجائز بشأها التسليم، وألا يكون الشخص المطلوب للتسليم من رعايا الدولة أو متحصل على لجوء سياسي أو تمت محاكمته على ذات الجريمة، مع المرور بإجراءات التسليم تحددها عادة الإتفاقيات الثنائية أو الجماعية، من قبيل اتفاقية " بودابست " لسنة 2001 والإتفاقية العربي لسنة 1953 واتفاقية التسليم لدول الإتحاد الأوروبي لسنة 1996، واتفاقية الأمم المتحدة لسنة 2000.

المحور الثاني: معوقات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية

من خلال ما سبق وبيننا فإن التعاون الدول في مجال محاربة الجريمة المعلوماتية يعتبر تقريبا السبيل الوحيد المتاح لمكافحة هذه الجريمة لما لها من بعد دولي كبير، إلا أن هذا التعاون تعترضه مجموعة كبيرة من المعوقات التي حالت دون الوصول إلى النتائج المرجوة منه، حيث يرجع بعض هذه المعوقات إلى النظم الداخلية وبعضها الآخر يرجع الى طبيعة النظام الدولي العالمي.

¹ - أحمد عبد الحكيم شاكور، دور الغنابة القضائية في مكافحة الجريمة، مجلة الفكر الشرطي، المجلد 17، العدد 4، 2008، ص 153.

² - جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة، 2002، ص 88.

فعن معوقات التعامل الدولي على الصعيد الداخلي، فإن أول و أهم معوق يبرز هو عدم موائمة ومواكبة ومسايرة القوانين الداخلية للتطور الحاصل على الصعيد المعلوماتي السريع التطور وخصوصا في ظل اشتراط القوانين لشرط الركن المادي في الجريمة، وهو أمر صعب التحقيق في الجريمة المعلوماتية، وبالتالي تصبح هذه الجريمة في نظر القانون شرعية لتخلف ركن من أركانها، وبالتالي عدم امكانية تطبيق النصوص القانونية على هذه الجرائم مما يصعب مكافحتها¹.

وعلى الرغم من أن العديد من الدول قد أصدرت تشريعات خاصة بها متعلقة بالجرائم المعلوماتية أو أنها صادقت على الإتفاقيات الدولية التي تجرم بعض الأفعال المعلوماتية، إلا أن هذه النصوص الوطنية والدولية ليست كافية لمكافحة كل الجرائم المعلوماتية المتطورة بشكل سريع جدا مما يقلل من جهود مكافحتها.

كل هذا يضاف إليه معوق بالغ الأهمية وهو صعوبة التحقيق في الجريمة المعلوماتية وإثباتها، حيث أن هذه الجرائم على اختلاف الجرائم العادية لا يشعر المجني عليه بارتكابها في حقه إلا بعد فترة من الزمن وبمحض الصدفة أو بعد الإستعانة بالخبراء في غالب الأحيان، يضاف لها عدم وجود الجاني في مسرح الجريمة ولا يترك أي آثار مادية يمكن إدراكها بالحواس، وحتى الدلائل والقرائن المساعدة في التحقيق يتولى مسحها أو تشفيرها أو التخلص من الجهاز المستخدم أصلا في الجريمة في زمن قياسي، بل يمكن له تحويل قرار الإدانة الموجودة على جهازه إلى أي جهاز آخر، كما يمكن كذلك القيام بالجرائم المعلوماتية عن طريق استخدام أجهزة الكترونية موجودة لدى أشخاص آخرين يجري التحكم بها عن بعد، وبالتالي يمكن أن تطل الإدانة أشخاص لا علاقة لها بالجريمة²، يضاف لها حرفة مرتكبيها واعتمادهم على الخداع والتظليل والتخفي في الإنترنت، وأيضا تحفظ وإحجام الكثير من الجهات عن التبليغ عليها تجنباً للإضرار بسمعتها ومن ثم بمركزها المالي، كالبנק والمؤسسات الإدخارية مما يشجع الجناة على ارتكاب المزيد من الجرائم، يضاف إلى كل ذلك نقص الخبرة لدى

¹ - محمد منير صالح، الجريمة المعلوماتية وطرق مواجهتها، مجلة بحوث الشرطة، أكاديمية الشرطة، القاهرة، العدد 3، 2005، ص 179.

² - أمين عبد الحفيظ، الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، مكتبة الكتب العربية، القاهرة، 2005، ص 214.

رجال التحقيق مما يعرقل عملهم، حيث أن هؤلاء تعودوا على التعامل مع الجرائم التقليدية، وليس جرائم التعقب عبر شبكة المعلومات الدولية¹.

أما عن معوقات التعامل الدولي فهو الأكثر والأهم على هذا الصعيد، فهي نابعة أساساً من المعوقات الوطنية، يضاف إليها تعارض المصالح الدولية.

وهنا يتمثل أو معوق دولي في اختلاف الرؤى الدولية حول هذا الموضوع وما يترتب عليه ذلك من مشاكل في تطبيق القانون، حيث أنه لا يوجد اتفاق بين جميع الدول حول ماهية الجرائم المعلوماتية، ومتى نكون أمام جريمة من عدمها، حيث أن أحد الإجراءات قد يكون مباحاً في دولة ما ومجرم في دولة أخرى، حيث أن كل دولة تحدد هذه الجرائم حسب اختلاف بيئتها وعاداتها وثقافتها والتطور الذي يعرفه المجال المعلوماتي فيها، وهو الأمر الذي انعكس سلباً على إجراءات التعامل الدولي في هذا المجال غداة القصور التشريعي في العديد من الدول لوضع قواعد خاصة تمثل الجرائم المعلوماتية وترك القواعد العامة تطبق عليها، وهو أمر لا يتلائم مع طبيعة هذه الجرائم، وفي ظل هذا الانقسام الداخلي وعدم التوافق الدولي على ضبط الغطار القانوني لهذه الجرائم، فإن الدول تلجأ هنا إلى حماية وتغليب مصلحتها الخاصة على مصالح الدول الأخرى، حيث تلعب هنا الاعتبارات السياسية وعدم التوافق والتناغم السياسي الدور الأبرز في مجال تفعيل التعاون الدولي من عدمه².

ثاني معوق دولي هو اختلاف القواعد الإجرائية في الدول، حيث أن من شأن تنوع وتعدد هذه القواعد أن يؤدي إلى عدم التوافق الدولي في مجال مكافحة هذه الجرائم، حيث أن بعض طرق التحري والتحقيق التي أثبتت فعاليتها في دولة ما ليس بالضرورة أن تثبت ذات الفعالية في الدول الأخرى، كالمراقبة الإلكترونية لبعض المشتبه بهم على شبكة الإنترنت، وأيضا بعض الطرق غير المشروعة أو السرية التي تنتهجها بعض الدول في هذا المجال وتتحفز عن التصريح بها أمام باقي الدول مما يزرع حالة من عدم الثقة والشك بين الدول في ما يتعلق بالإجراءات الجنائية المتبعة في ملاحقة مرتكبي الجرائم المعلوماتية³.

1 - منير محمد الجهيني - محمود محمد الجهيني، جرائم الإنترنت، دار الفكر الجامعي، الاسكندرية، 2004، ص 40.

2 - هشام عبد العزيز، تسليم المجرمين بين الواقع والقانون، دار النهضة العربية، القاهرة، 2006، ص 536.

3 - مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الإنترنت، دار الكتب والوثائق القومية، القاهرة، 2003 ص 3.

ثالث معوق هو تنازع الإختصاص القضائي بين الدول والذي يعتبر من أهم المعوقات القانونية وينصرف الى تحديد الجهة القضائية المختصة بالنظر في الجريمة المعلوماتية وخصوصا أن هذه الجريمة عابرة للحدود وترتكب في أكثر من إقليم دولة واحدة، وبالتالي تتحجج كل دولة بسلطة محاكمها للنظر في هذه الجرائم علاوة على التنازع بين جهتي التحقيق والحكم، فهل يحق للجهة التي باشرت التحقيق الحكم على المشتبه به؟ أو أنه يجب هنا تسليم المشتبه به إلى دولة أخرى لمحاكمته؟ كما يبرز هنا تنازع الإختصاص السليبي بمعنى عدم اختصاص أي من المحاكم بالنظر في هذه الجريمة وهي أمور لا يمكن الوصول إلى حل لها سوى بتظافر الجهود الدولية للوصول إلى اتفاقية عامة تنظم هذه المسائل¹.

رابع اشكالية تثور هنا، هي الإنابة القضائية الدولية وتعارضها مع مبدأ السيادة على اعتبار أن كل دولة سيدة في إقليمها وتقوم بنفسها أو عبر جهازها القضائي بالتحقيق والفصل في كل النزاعات التي تثور على اقليمها ودون أن تشاركها في ذلك أي سلطة او جهة قضائية أخرى، وهو ما يتعارض هنا وموضوع الجرائم المعلوماتية التي ترتكب في أكثر من دولة ويتطلب الأمر فيها جهدا عابرا للحدود بين الدول المختلفة وهو أمر صعب التحقيق بداية من تذرع كل دولة بمبدأ السيادة وخوفها من أن تستخدم هذه الإنابة في أنشطة غير مشروعة كالتجسس، وذلك لارتباطها المباشر بأجهزة الكمبيوتر والإنترنت داخل الدولة وما يترتب عليه من تهديد الأمن الداخلي للدولة وأيضا لإشكالية البطئ في إجراءات الإنابة ذلك أنها تكون بالطرق الدبلوماسية العادية التي تتسم بالبيروقراطية والبطئ وهو ما يجعلها تتعارض مع طبيعة الجرائم المعلوماتية التي تتميز بالسرعة وهو ما يؤثر بشكل كبير في التصدي لهذه الجرائم².

أما خامس آخر إشكالية متعلقة بالتعاون الدولي في مجال محاربة الجريمة المعلوماتية فهي خاصة ومتعلقة بتسليم المجرمين المرتكبين لهذا النوع الخاص من المجرمين، فهي تتعلق إما بإشكالية ازدواجية التسليم بمعنى أن يكون هذا الفعل المرتكب يشكل جريمة يعاقب عليها في كل من قانون الدولة طالبة والمطلوب منها تسليم هذا الشخص وألا يكون هذا الفعل مباحا في أي القانونين، ورغم فائدة هذا

¹ - نائلة عادل قورة، جرائم الحاسب الإقتصادية، منشورات الحلبي، القاهرة، 2005، ص 49.

² - حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت -دراسة مقارنة- أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة، 2007، ص 553.

الأمر إلا انه يبرز بعض العقبات أمام التعاون الدولي في هذا المجال وخصوصا أن مجال المعلوماتية واسع وبعض الدول المتطورة تبيح الكثير من الأنشطة التي تعتبر مجرمة في الدول المتخلفة، إضافة إلى أن القواعد التي تحكم هذا الموضوع هي في معظمها قواعد عامة، وبالتالي تتحفظ الدول على تسليم أشخاص ليحاكموا وفق قواعد عامة في مواضيع حساسة وهو ما يحد من إمكانية التطبيق الإتفاقيات الدولية في هذا الشأن.

يضاف إلى ذلك بروز حالات يكون فيها الشخص الواحد مطلوب امام اكثر من جهة لمحاكمته على جريمة واحدة ارتكبها في نفس الوقت ومست بمصالح العديد من الدول وقدمت هذه الأخيرة الأدلة التي تثبت قيام الشخص المطلوب بارتكاب الجريمة المعلوماتية وليس مجرد الإدعاء عليه وهو ما يطلق عليه بتزاحم الطلبات، والذي لا يشترط فيه أن يكون في نفس الوقت، ولكن يجب أن يكون الشخص المطلوب تسليمه ما يزال متواجدا على إقليم الدولة ولم تسلمه بعد إلى أي من الدول¹.

المحور الثالث: سبل مواجهة معوقات التحقيق في الجرائم المعلوماتية

انطلاقا مما تقدم وتأسيسا على أن معوقات التحقيق في الجرائم المعلوماتية تنقسم إلى قسمين، الأول ذا طابع وطني والثاني ذا طابع دولي، فإن سبل وآليات التغلب على هذه المعوقات يجب أن تكون أيضا ضمن هذه المستويات وانطلاقا من تحليل كل معوق على حدة.

فعن سبل مواجهة المعوقات على الصعيد الداخلي والمتعلقة أولا بالتدابير الموضوعية، فيجب بداية على الدول العمل على اتخاذ سياسة الإنفتاح والتعاون الدولي مع باقي الدول لأجل حماية نفسها أساسا من أخطار الجرائم المعلوماتية، انطلاقا من الطبيعة الخاصة لهذه الجرائم، ولذا على الدول بداية تبني سياسات تشريعية حديثة من شأنها الكشف المبكر عن ارتكاب أي من الأفعال الإجرامية المعلوماتية والحد من إمكانية نقل أو إتلاف الأدلة المتعلقة بتلك الأفعال الإجرامية وكفالة حفظها وتخزينها مع تجريم كل عمل من شأنه أن يعتبر إضرار أو إتلاف أو محو أو إعاقة أو تعديل أو كل ما من شأنه أن يعيق التحقيق، مع إمكانية مسائللة الأشخاص الاعتبارية عن كل ما ينشأ من جرائم معلوماتية.

¹ - أحمد عبد الله، التعاون الدولي في الإجراءات الجنائية - دراسة مقارنة بالنظام الإسلامي - أطروحة دكتوراه، كلية الحقوق، جامعة المنصورة، 2009، ص 394.

ومن هنا كان من الأحسن للدول وبالنظر الى خصوصية هذه الجرائم أن تخرجها من نطاق القانون الجنائي التقليدي والجرائم التقليدية الكلاسيكية، ذلك ان التطور الحاصل والذكاء الإلكتروني قد لا نجد له نصا قانونيا تقع تحت طائلته تلك الجرائم، وبالتالي يتوجب الأمر هنا نصوص قانونية جنائية جديدة تحرم بداية تلك الجرائم المعلوماتية وتواكب كل جديد يمكن أن يستجد فيها بما قد يسوعب أي تطور قد يحدث في المستقبل، وبالتالي لاق يأتي وقت يصبح فيه القانون عاجزا عن مواجهة هذه الجرائم التي تقف ورائها فئة محترفة تستغل الخبرة التكنولوجية لارتكاب أفعال تؤذي المجتمع¹.

كما تلعب التدابير الإجرائية الوطنية كذلك دورا مهما في مكافحة الجرائم المعلوماتية، وبالتالي يتوجب البحث في الحلول التي يتوجب الخوض فيها من أجل ان تقوم هذه التدابير بالدور المنوط بها بداية من اعتماد اجراءات ذات بعد ذات بعد عالمي يمكن من خلالها القيام بإجراءات التفتيش والتحري وفحص البيانات الإلكترونية المخزنة على مختلف الوسائط، وذلك بمناسبة مباشرة أي تحقيق متعلق بالإشتباه بموضوع جريمة إلكترونية مع الأخذ هنا بعين الاعتبار احترام خصوصيات الناس وحرمتهم الشخصية وهو امر شديد وبالغ الحساسية، يرافقه قيام الدولة باتخاذ التدابير الإدارية والتشريعي قصد ضبط وإحضار كل الأشخاص المشتبه بقيامهم بارتكاب أي نشاط إجرامي إلكتروني، سواء كانوا متواجدين داخل إقليمها أو خارجه مع ضمان التدريب الكافي واللازم لأفراد الشرطة و الأمن العاملين في هذا المجال الجديد، وأيضا إضفاء صفة الضبطية القضائية على بعض العاملين في مجال المعلومات من غير أفراد الشرطة والعاملين في مجال المعلومات كمزودي الدخول وخدمات الأنترنت، بحيث أنه وفي حال إكتشافهم لجريمة إلكترونية فلهم التحفظ على الأدلة المتعلقة بالجريمة وذلك إلى حين وصول رجال الضبطية القضائية ومباشرتهم لأعمالهم، كون هذه الأدلة يسهل التخلص منها².

كما يجب على الدول كذلك عقد اتفاقية تعاون ثنائية أو جماعية بداية مع أجهزة الشرطة في الدول الأجنبية، وذلك للتعاون في مجال الجرائم المعلوماتية التي يمكن أن تتم خارج الحدود، وأيضا على الدول تبني سياسات تشريعية مد اختصاصها الفقضي خارج اقليمها وخصوصا إذا ارتكبها أحد

1 - منير محمد الجهيني - محمود محمد الجهيني، مرجع سابق، ص 147.

2 - عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، دار النهضة العربية، القاهرة، 2004، ص 809.

مواطنيها الموجودين في دولة أجنبية أخرى، أو ارتكب في منطقة لا تخضع للسيادة كأعالي البحار مثلاً¹.

أما في ما يتعلق بسبل مواجهة المعوقات المتعلقة بالتحقيق الإلكتروني الدولي فإنه يجب البحث في كل معوق على حدة قصد الوصول الى حل.

فبداية وفي ما يتعلق باختلاف الرؤى الدولية حول هذا الموضوع، فإنه يتوجب بشكل أساسي الوصول إلى معاهدات دولية تضع وتحدد الإطار العام لمكافحة الجرائم الإلكترونية بما يتسنى بعده للدول تضمين هذه الإتفاقيات الدولية ضمن قوانينها الوطنية مما يضمن حالة من التناسق والإنسجام وتوحد أو على أقل تقدير تقارب تقارب الرؤى الدولية في ما يتعلق بمكافحة الجريمة المعلوماتية، بداية من تديد وحصر هذه الجرائم ووصولاً إلى تخفيف الفوارق بين الأنظمة العقابية الداخلية².

ثاني معوق ويتصل باختلاف القواعد الإجرائية في الدول فيمكن حله عن طريق جملة من الخطوات المتنوعة من قبيل اعتماد أجهزة أو إدارات أو أشخاص محددين يعملون كنقاط تواصل بين الدول المختلفة ومخولين باتخاذ القرارات بشكل سريع وحاسم في حال وجود أو الاشتباه بوجود جرائم معلوماتية، يضاف إليه تعزيز وتدعيم التعاون التقني بين سلكات الضبط الإداري في الدول المختلفة قصد المعالجة الجماعية لهذه الجريمة وخصوصاً في ما يتعلق بدمج الابتكارات والتطبيقات الناتجة عن تقنية المعلومات في مجال الإجراءات الجزائية المشتركة وخصوصاً في مسألة " إثبات الجريمة "، التي تعتبر العنصر الأهم في هذا الموضوع، وهو ما تنبه له الاتحاد الأوروبي على سبيل المثال، حين أصدر التوصية رقم 13/95 في 11 سبتمبر 1995، والمتعلقة بمشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات، وحث فيها الدول على مراجعة قوانينها الإجرائية والمتعلقة بتفتيش أجهزة الكمبيوتر وضبط وتحويل المعلومات التي تحتويها، مع توسيع هذه الإجراءات إلى أنظمة الكمبيوتر الأخرى والمجودة في دائرة اختصاصهم مع ضرورة كفالة حقوق الشخص محل التفتيش وإبلاغه بأن النظام كان محل تفتيش والبيانات التي تم ضبطها بما يتيح له اللجوء للقضاء من أجل استيفاء حقوقه، مع الدعوة كذلك لضع قانون إجراءات جزائية خاص بالجرائم المعلوماتية يتميز عن قانون

¹ - عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، 2002، ص 346.

² - عبد الفتاح بيومي حجازي، الأحداث والأنترنت، دار الكتب القانونية، القاهرة، 2007، ص 314.

الإجراءات العادية، مع تشكيل وحدات خاصة ومشاركة داخل الاتحاد الأوروبي لمكافحة هذه الجرائم¹.

ثالث معوق متصل بتنازع الاختصاص القضائي بين الدول فيمكن حله باعتبار الجرائم المعلوماتية تدخل ضمن الجرائم الدولية وينطبق عليها الاختصاص القضائي العالمي، بمعنى أن يعطى الحق لجميع دول العالم بملاحقة مرتكبي هذه الجرائم مهما كانت جنسيتهم، أو الدولة التي ارتكبوا فيها هذه الجريمة أو الدولة التي تضررت منها، حيث يهدف هذا المبدأ إلى التصدي للجرائم ذات البعد الدولي من خلال تجاوز مبدأ الإقليمية القوانين التي تقف حاجزا أما انعقاد الاختصاص القضائي بما يكفل هنا تجنب إفلات المجرمين من العقاب وتعزيز فكرة التضامن بين الدول، وخصوصا أن هذه الجرائم قد ترتكب في أماكن غير خاضعة لسيادة أي دولة كأعالي البحار، أو لا يعرف أصلا الدولة التي ارتكبت فيها هذه الجريمة وذلك للقدرة الفائقة على التضييل التي يتمتع بها هؤلاء المجرمين الإلكترونيين، وهو ما حاولت ان تصل له بعض الدول كالقانون العربي النموذجي بشأن مكافحة جرائم الكمبيوتر والإنترنت لسنة 2003، والذي نص في مادته ال 22 على امتداد القانون الداخلي للدولة على الجرائم المعلوماتية المرتكبة خارج حدودها إذا كانت تخل بأمنها².

رابع معوق متعلق بالإنبابة القضائية الدولية فيمكن تجاوزه من خلال مراعات مجموعة من الخطوات التي يمكن معها كفالة مبدأ سيادة الدولة، وذلك من خلال ابرام اتفاقيات دولية تتولى تنظيم هذا الموضوع، وبالتالي لا تتم الإنابة إلا وفق الأسلوب الذي حددته الإتفاقية وأن يخضع طلب الإنابة إلى التدقيق المسبق من الدولة وأن يتم تنفيذ إجراءات الإنابة بعد قبولها وفق قانون الدولة المطلوب منها الإنابة، لتعبر بداية عن أوجه التعاون بين الدولتين ولتضمن عدم استغلالها في أنشطة غير مشروعة، وهنا يتعين على الدول التغلب على اشكالية أخرى، وهي بطئ إجراءات الإتصال ومرورها عبر القنوات الدبلوماسية الرسمية وما يترتب عليه ذلك من بطئ، وهنا على الدول تفعيل آليات التواصل

¹ - عبد الرحمان فتحي سمحان، تسليم المجرمين في ظل القانون الدولي، دار النهضة العربية، القاهرة، 2012، ص375.

² - سليمان أحمد فضل، مرجع سابق، ص 437.

المباشر بين سلطات الدولة بما يتلائم مع حالة الإستعجال والضرورة التي تطبع موضوع الجرائم المعلوماتية¹.

أما خامس إشكالية متعلقة بتسليم المجرمين فيمكن التغل على صورتها، فعن الصورة الأولى والمتعلقة بازدواجية التسليم، فيمكن الوصول إلى حلها عن طريق إلزام الدول بتجريم الأفعال المنصوص عليها في الإتفاقيات الدولية التي يتم عقدها بين الدول، حيث يوفر ذلك الأساس القانوني لتحقيق شرط ازدواجية التجريم، مع إمكانية إدراج أحكام في المعاهدة الدولية المتعلقة بتسليم المجرمين تسرد الأفعال التي تتطلب أن تجرم كجرائم أو أفعال مخلة بمقتضى قوانين الدول الموقعة على الإتفاقية، أو يكون التسليم بسبب أي سلوك يتم تجريمه ويخضع لدرجة معينة من العقوبة في إحدى الدول الموقعة².

وأما الصورة الثانية والمتعلقة بإشكالية التزام في طلبات التسليم فيمكن حلها عن طريق تطبيق معيار "جسامه الفعل"، بمعنى أن تكون الأولوية في التسليم للدولة الأكثر تضررا من الفعل، وأما إذا كان الإشكال في التسليم بسبب جرائم مختلفة فإن الأولوية تعطى للدولة التي ارتكبت داخل حدودها الجريمة الأكثر خطورة، وأما إذا تساوت درجة خطورة الجرائم فإن الأولوية تعطى هنا للدولة التي قدمت طلبها أولا³.

خاتمة:

في ختام هذه الورقة البحثية والتي تناولنا فيها التعاون الدولي لمكافحة الجريمة المعلوماتية والعوائق التي تواجهها والسبل والحلول المقترحة لتجاوز هذه العوائق، فإنه يتوجب هنا بداية الوصول إلى إطار تشريعي موحد لمفهوم الجرائم المعلوماتية من أجل تحديد الأفعال التي تعتبر جريمة معلوماتية من عدمها، وذلك كخطوة أخرى في سبيل مجahتها والذي يتوجب ان يكون أساسا ذا طابع دولي من خلال العمل المتناسق والمتطابقين قوانين الدول المختلفة، بحيث لا يجد المجرمون المعلوماتيون ملاذ آمن، ثم العمل سويا على حل القضايا العالقة، كمشاكل تنازع الإختصاص والإنابة القضائية

1 - عمر سالم، الإنابة القضائية في المسائل الجنائية - دراسة مقارنة، دار النهضة العربية، القاهرة، 2001، ص 189.

2 - حسين الغافري، مرجع سابق، ص 558.

3 - عبد الغني محمود، تسليم المجرمين على أساس المعاملة بالمثل، مجلة كلية الشريعة والقانون، القاهرة، العدد 16، لسنة 1998، ص 161.

الدولية، وكل ذلك يجب أن يكون في قالب موضوعي عملي بعيدا عن النضرة المصلحية الدولية الضيقة.

قائمة المراجع:

- 1 - أسامة المناسعة - جلال الزعي - صابل فاضل الهواوشة، جرائم الحاسب الآلي والانترنت، دار وائل للنشر، عمان الأردن، 2001.
- 2 - أيمن عبد الحفيظ، الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، مكتبة الكتب العربية، القاهرة، 2005.
- 3 - أحمد عبد الحكيم شاكر، دور الغنابة القضائية في مكافحة الجريمة، مجلة الفكر الشرطي، المجلد 17، العدد 4، 2008.
- 4 - أحمد عبد الله، التعاون الدولي في الإجراءات الجنائية - دراسة مقارنة بالنظام الإسلامي - أطروحة دكتوراه، كلية الحقوق، جامعة المنصورة، 2009.
- 5 - هشام عبد العزيز، تسليم المجرمين بين الواقع والقانون، دار النهضة العربية، القاهرة، 2006.
- 6 - حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت - دراسة مقارنة - أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة، 2007.
- 7 - علاء الدين شحاته، التعاون الدولي لمكافحة الجريمة، دار النهضة العربية القاهرة، 2000.
- 8 - عبد الرحمان فتحي سمعان، تسليم المجرمين في ظل قاعد القانون الدولي، دار النهضة العربية، القاهرة، 2012.
- 9 - محمد حماد الهبتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2004.
- 10 - سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الانترنت، دار النهضة العربية، القاهرة، 2013.
- 11 - جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة، 2002.
- 12 - محمد منير صالح، الجريمة المعلوماتية وطرق مواجهتها، مجلة بحوث الشرطة، أكاديمية الشرطة، القاهرة، العدد 3، 2005.

- 13- منير محمد الجهيني - محمود محمد الجهيني، جرائم الإنترنت، دار الفكر الجامعي، الاسكندرية، 2004.
- 14- مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الإنترنت، دار الكتب والوثائق القومية، القاهرة 2003.
- 15- نائلة عادل قورة، جرائم الحاسب الإقتصادية، منشورات الحلبي، القاهرة، 2005.
- 16- عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، دار النهضة العربية، القاهرة، 2004.
- 17- عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، 2002.
- 18- عبد الفتاح بيومي حجازي، الأحداث والأنترنت، دار الكتب القانونية، القاهرة، 2007.
- 19- عبد الرحمان فتحي سمحان، تسليم المجرمين في ظل القانون الدولي، دار النهضة العربية، القاهرة، 2012.
- 20- عمر سالم، الإنابة القضائية في المسائل الجنائية - دراسة مقارنة، دار النهضة العربية، القاهرة، 2001.
- 21- عبد الغني محمود، تسليم المجرمين على أساس المعاملة بالمثل، مجلة كلية الشريعة والقانون، القاهرة، العدد 16، لسنة 1998.

مكافحة الجريمة المعلوماتية في إطار منظمة مجلس أوروبا

د/ براهيم السعيد

كلية الحقوق والعلوم السياسية - جامعة برج بوعريش

مقدمة:

أصبح العالم أمام ثورة حقيقية هي ثورة المعلومات أو العالم الرقمي، وصار الناس مختارين، وفي أحيان أخرى مضطرين للتعامل مع هذا العالم الجديد أو مجتمع المعلومات، كما يحلو للبعض أن يسميه. وبعيدا عن الاستخدامات الحميدة أو السلمية للأجهزة الإلكترونية خاصة جهاز الحاسوب، يمكن القول بأن التطور في هذا المجال، قد ترتب عليه نشوء جرائم ناتجة عن استخداماته المتعددة، وهذه الجرائم إما أن تقع على الكمبيوتر ذاته، وإما أن تقع بواسطة الكمبيوتر، حيث يصبح أداة في يد الجاني يستخدمه لتحقيق أغراضه الإجرامية، وهو الشيء الذي أدى إلى ظهور نمط جديد من الإجرام، تجسد في انتشار الجرائم المعلوماتية أو الإلكترونية، والتي تعتبر من أكبر السلبيات التي خلفتها الثورة المعلوماتية لكون هذه الجرائم تشمل في اعتدائها قيما جوهرية تخص الأفراد والمؤسسات وحتى الدول في كافة نواحي الحياة، كما أن هذه الجرائم تركت في النفوس شعورا بعدم الثقة بخصوص التعامل والاستفادة من ثمار هذه الثورة الجديدة.

ونظرا لازدياد الجرائم المتعلقة بالحاسوب، فقد شرعت أغلب الدول بوضع تشريعات جنائية خاصة لمكافحة جرائم الكمبيوتر المستحدثة على علم الإجرام، ومن هذه الدول نجد: الولايات المتحدة الأمريكية وفرنسا وباقي دول الاتحاد الأوروبي الذي وضع اتفاقية بودابست حول جرائم الكمبيوتر بتاريخ 23 نوفمبر 2001.

لقد اهتم المجتمع الدولي، بمسألة مكافحة الجريمة المعلوماتية وفي هذا الصدد نشير إلى اتفاقية بودابست التي تم التوقيع عليها بتاريخ 23 نوفمبر 2001 بشأن الإجرام الكوني أو المعلوماتي، وذلك إيمانا من الدول الأعضاء في المجلس الأوروبي والدول الأخرى الموقعة على هذه الاتفاقية بضرورة مواجهة هذا النمط الجديد من الإجرام.

ما مضمون اتفاقية بودابست؟ وما مدى كفايتها في مكافحة الجريمة الإلكترونية؟

للإجابة عن هذه الإشكالية، سنقسم البحث إلى محورين اثنين:

المحور الأول: مضمون اتفاقية بودابست

من الجهود المبذولة على المستوى الدولي، نجد اتفاقية بودابست التي حظيت باهتمام كبير من الدول الأعضاء فيها والموقعين عليها، وتعد هذه الاتفاقية الوحيدة التي تم إبرامها لمكافحة الجرائم المعلوماتية، والمعروفة بالاتفاقية الدولية لمكافحة الجرائم التي ترتكب عبر الانترنت، حيث شهدت العاصمة الجبرية بودابست في 2001/11/23 ولادة أول معاهدة دولية هدفها مكافحة جرائم الانترنت، وتقوية الجهود الدولية من اجل التعاون والتضامن في محاربة هذه الجرائم والحد منها وخاصة بعد أن أصبحت تلك الجرائم تشكل خطرا يهدد الأشخاص والممتلكات، وقد تم صياغة هذه الاتفاقية من قبل عدد كبير من الأشخاص الذين يمتلكون خبرة قانونية في مجلس أوروبا، بالتعاون مع دول أخرى وخصوصا الولايات المتحدة الأمريكية، وبعد مشاورات عديدة بين الحكومات وأجهزة الشرطة وقطاع الكمبيوتر على مستوى العالم، وهو الأمر الذي أدى في النهاية إلى التوقيع عليها من قبل 30 دولة بتاريخ 2001/11/23 وفي عاصمة المجر بودابست، وذلك لمواجهة الاستخدام غير المشروع للحاسبات وشبكات المعلومات فيما يعرف بالإجرام الكوني أو الإجرام المعلوماتي أو الجرائم المعلوماتية، وقد تناولت هذه المعاهدة الجرائم التي تعد أكثر انتشارا على مستوى العالم مثل الإرهاب الإلكتروني، وعمليات تزوير بطاقات الائتمان ودعارة الأطفال...الخ.

وعلى اثر اتساع الجهود الدولية لمكافحة الجريمة المعلوماتية، من حيث ضرورة السعي لتكوين أرضية قانونية تعمل على دعم الكفاح الدولي المشترك ضد الجريمة عبر الانترنت، وبناء على توصية مجلس الوزراء الأوروبي، وقراراته المختلفة حول المشاكل والحلول التي يمكن طرحها، وإعداد مشروعات قوانين تيسر على هديها المجموعة الأوروبية، فقد قام مجلس أوروبا، منذ ثمانينات القرن العشرين بمحاولات عدة، من أجل إعداد مشروعات عمل لمواجهة الأنشطة الإجرامية والتهديدات المحتملة كالاختراق والأنشطة الإجرامية الأخرى ذات العلاقة بالحاسوب ومن تلك المحاولات إعداد اتفاقية تتضمن في محتواها ضرورة تسهيل التعاون الدولي في الإجراءات الجنائية في الجرائم الناشئة عن استخدام الحاسوب والانترنت، ولقد تم توجيه الدعوة إلى الو م أ واليابان وكندا وجنوب إفريقيا، لكي تشارك كل منها في إعداد الاتفاقية بصفة مراقب، وذلك لكون الو م أ تحديدا ذات علاقة ومصصلحة بموضوع الجريمة عبر الانترنت، أما مشاركة كل من اليابان وكندا وجنوب إفريقيا هو الأمر الذي يجعل الاتفاقية صالحة لكي تمتد للدول غير الأعضاء في الاتحاد الأوروبي، من حيث إمكانية الدول غير الأعضاء في الاتحاد من الدخول فيها.

لقد تضمنت الاتفاقية أقساماً ثلاثة الأول: تناول مجموعة الجرائم التي تتعرض لها شبكة الإنترنت والحاسب الآلي، والثاني تناول الإجراءات الجنائية التي تتخذ في مواجهة هذه الجرائم، وتناول القسم الثالث التعاون الدولي في مكافحة هذه الجرائم بين الدول الأعضاء، وجاء في المادة الأولى من الاتفاقية تعريفات لبعض المصطلحات الحديثة في القانون الجنائي وهي «نظام معلوماتي» «بيانات معلوماتية» «مفهوم مقدم الخدمة عبر الإنترنت» «البيانات التي تمر خلال النظام المعلوماتي».

وتناولت المواد من 2- 6 الجرائم ضد سرية وسلامة وإتاحة البيانات والنظم المعلوماتية، وهي جرائم الدخول غير المشروع للنظم المعلوماتية، والاعتراض غير القانوني لهذه النظم والاعتداء على سلامة البيانات، وتناولت المادتان 7 و8 منها التزوير والغش المعلوماتي، كما تناولت المادة 9 الجرائم المتصلة بالمواد الإباحية للأطفال، وتضمنت المادة العاشرة الاعتداء على حقوق الملكية الفكرية والحقوق المجاورة، والمادة 11 تناولت الشروع والاشتراك في هذه الجرائم، وشملت الاتفاقية مسؤولية الأشخاص المعنوية عن ارتكاب هذه الجرائم، وهي مسؤولية مستحدثة في التشريع الجنائي المعاصر وأيضاً الجزاءات."

كما تناولت الاتفاقية الجوانب الإجرائية إذ أوصت الدول الأعضاء باتخاذ الإجراءات اللازمة والضرورية لضبط ونسخ الأدلة المعلوماتية، واستحداث تنظيم لإجراءات هذا الضبط وتمكين سلطات التحقيق من الحصول على نسخ من الأدلة وتفتيش وضبط البيانات المعلوماتية المخزنة آلياً، ووضع نظم لمراقبة الإنترنت والتحفظ العاجل على البيانات المعلوماتية واعتراضها

وتضمنت الاتفاقية أيضاً التعاون الدولي في مكافحة الجريمة المعلوماتية حيث نصت الاتفاقية على إمكانية التعاون الدولي في مكافحة الجرائم المعلوماتية عابرة الحدود، وذلك بتسليم المجرمين والمساعدة القضائية المتبادلة، كما نصت على إجراءات طلب المساعدة القضائية المتبادلة، وتحديد مجالات هذه المساعدة في الإجراءات الوقتية العاجلة وفي مجالات سلطات التحقيق، وختاماً فإن الانضمام إلى هذه الاتفاقية ذات أهمية قصوى من أجل التعاون الدولي لمكافحة الجرائم الإلكترونية خاصة مع تنامي جرائم الإرهاب على مستوى دول العالم.

المحور الثاني: آليات الحماية من الجريمة المعلوماتية

اتخذت العديد من الإجراءات على المستوى الأوروبي لمكافحة الجريمة المعلوماتية، ويظهر ذلك من خلال:

أ - الشق التشريعي: سنت عدد من الدول الأوروبية قوانين خاصة بجرائم الانترنت والحاسوب مثل بريطانيا وهولندا وفرنسا والدنمارك والمجر وبولندا واليابان وكندا، كما اهتمت البلدان الغربية بإنشاء أقسام خاصة بمكافحة جرائم الإنترنت، بل إنها خطت خطوة إلى الأمام وذلك بإنشاء مراكز لاستقبال ضحايا تلك الجرائم.¹

أما على مستوى الدول العربية فقد قامت الدول العربية بالتوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وذلك بتاريخ 2010/12/21، كما أدت هذه الاتفاقية كذلك لميلاد قوانين عديدة لمكافحة ما يسمى بالجرائم الإلكترونية في السعودية والأردن وقطر والإمارات والعراق وسلطنة عمان. وصارت الاتفاقية سارية المفعول بعد تصديق الرئيس المصري عليها سنة 2015 ليكتمل نصاب الدول السبع المطلوبة لسريانها.²

ب - الشق الأمني:

إن مواجهة مخاطر الجرائم المعلوماتية تعتمد بشكل كبير على تبني إستراتيجية أمنية - مجتمعية متكاملة، والتي تعمل فيها أجهزة مكافحة الجريمة الرسمية في الدولة جنباً إلى جنب مع أفراد المجتمع ومؤسسات القطاع الخاص، هو ما يمكن من خلاله مكافحة الأنشطة الإجرامية في الفضاء الإلكتروني والتقليل من مخاطرها والحد من انتشارها، وهذه الرؤية تتسق مع نتائج الدراسات التي أجريت في بلدان مختلفة من العالم حول التعامل مع جرائم الإنترنت، والتي أوضحت أهمية مشاركة العديد من المصادر والمؤسسات الخاصة في تحمل جزءاً من المسؤولية فيما يتعلق بمكافحة هذه الجرائم والسيطرة عليها وتلك المصادر تتمثل في:³

¹ - سمير سعدون مصطفى، محمود خضر سلمان، حسن كريم عبد الرحمن، الجريمة الالكترونية عبر الانترنت أثرها وسبل مواجهتها، مجلة التقني، المجلد 24، الإصدار 9، 2011، ص 49.

² - عزة مغازي، قانون الجريمة الإلكترونية.. التورنت يحملك إلى طرة، مقال منشور على موقع المنصة بتاريخ 2019/02/13 على الرابط <https://almanassa.com/ar/story/1019>، تاريخ الاطلاع 2019/02/13

³ - عبدالله بن فارع القرني، مواجهة جرائم الإنترنت: نحو إستراتيجية أمنية - مجتمعية متكاملة، مقال منشور على موقع جريدة الرياض بتاريخ 2019/02/11 على الرابط <http://www.alriyadh.com/912032> : تاريخ الاطلاع: 2019/02/11.

1. مزودو خدمة الإنترنت الذين يملكون القدرة على تحديد ما يعرف ب (Internet Protocol) (IP) للمشاركين، ما يتيح إمكانية مراقبة الأنشطة الخطرة على الإنترنت وتقييد اشتراك المستخدمين المنخرطين في تلك الأنشطة.
 2. المواطن العادي بدوره كذلك يمكن أن يساهم من خلال تحمل مسؤولية حماية نفسه من الوقوع ضحية لجرائم الإنترنت باقتنائه برمجيات الحماية من الفيروسات.
 3. المصارف التجارية وشركات البطاقات الائتمانية عليها أيضاً مسؤولية كبيرة في حماية عملائها من خلال تطبيق إجراءات وقائية ضد الاحتيال، وكذلك تنصيب برمجيات مراقبة خاصة على خوادمها لتعقب النشاطات غير المعتادة على حسابات العملاء ووضع أنظمة لتنبيه العميل على كل عملية تتم على حسابه.
 4. المحققين الخاصين الذين يعملون بالتنسيق مع أجهزة العدالة الجنائية يمكن أن يلعبوا دوراً مهماً في مكافحة جرائم الإنترنت.
- وقد قدمت شركة « فاير آي FireEye » المتخصصة في مجال التصدي للهجمات الالكترونية المتقدمة 8 إجراءات مهمة لتفادي مخاطر تزايد الهجمات الالكترونية التي تستهدف دول الخليج العربي، بعدما كشفت عن جملة من التصورات والرؤى التحليلية بشأن مشهد الهجمات الالكترونية في مناطق أوروبا والشرق الأوسط وأفريقيا، وعلى وجه الخصوص في دول مجلس التعاون الخليجي، وتمثلت هذه الإجراءات في ما يلي:¹
1. التوقع الدائم بأن تكون تلك الشركات مستهدفة.
 2. أنه من الممكن تخطي حدود الضوابط الأمنية المتوفرة لديها.
 3. التأكد دائماً من أن ليس هناك أي كيان تجاري بمنأى عن الهجمات.
 4. وضع إطار عمل خاص بالمخاطر ذات الصلة بالانترنت.
 5. الحصول على منصة استخبارات التهديدات الأنسب لتحسين قدرات الكشف عن الهجمات المحتملة.

¹ - 8 إجراءات لتفادي مخاطر تزايد الهجمات الالكترونية التي تستهدف دول الخليج العربي، مقال منشور على موقع جريدة مكة، تاريخ النشر 2016/06/01 على الرابط :

<http://makkahnewspaper.com/article/147871>، تاريخ الاطلاع: 2019/02/12.

6. إنشاء خدمة الاستجابة للحوادث الطارئة وإدارتها، والتي من شأنها تمكين الشركات من اكتشافها والتفاعل مع هجمات APT بالسرعة الممكنة.
7. تسخير التكنولوجيا المناسبة القادرة على تحديد واكتشاف هذه التهديدات الجديدة.
8. وضع خطة استجابة واضحة والعمل على تحضيرها استعدادا للتعامل مع أي حالة اختراق.

التجربة العملية لدولة استونيا لمواجهة الجريمة الالكترونية: كتحجربة عملية في مجال التصدي للإجرام الإلكتروني نذكر على سبيل المثال « إستراتيجية الأمن السيبراني (الأمن المعلوماتي (للفترة الممتدة من 2017 -2014، التي تبنتها دولة استونيا، وهي إستراتيجية تقوم بتحديد المخاطر التي تهدد الأمن المعلوماتي لدولة استونيا وتقدم التدابير اللازمة لإدارة هذه المخاطر، وتتولى وزارة الشؤون الاقتصادية والاتصالات مهمة توجيه سياسة أمن الانترنت و أيضا التنسيق ما بين الأطراف المعنية بتنفيذ بهذه الإستراتيجية والمتمثلة في وزارة الدفاع الوطني، وزارة العدل، وزارة الداخلية، وزارة الخارجية، مصالح الأمن والشرطة، الجهاز المسئول على نظام المعلومات، وزارة التعليم والبحث، ومنظمات أصحاب العمل، وتضمنت هذه الإستراتيجية ما يلي:¹

أولا -مبادئ ضمان الأمن السيبراني (الأمن المعلوماتي): (اشتملت هذه الإستراتيجية على المبادئ الأساسية التالية:

- الأمن الإلكتروني هو جزء لا يتجزأ من الأمن القومي، فهو يدعم سير العمل في الدولة والمجتمع، ويعزز القدرة التنافسية للاقتصاد والابتكار.
- الأمن الإلكتروني مكفول من خلال احترام الحقوق والحريات الأساسية، وكذلك من خلال حماية الحريات الفردية والمعلومات الشخصية.
- يتم ضمان الأمن الإلكتروني بطريقة منسقة من خلال التعاون بين القطاعين العام والخاص، مع مراعاة الترابط المتبادل بين البنية التحتية القائمة والخدمات في مجال التجارة الإلكترونية.

¹ - Estonia Cyber Security Strategy 2014-2017, Ministry of Economic Affairs and Communication, Estonia 2014, p 7-12.

- يبدأ الأمن الإلكتروني انطلاقاً من المسؤولية الفردية عن استخدام أدوات تكنولوجيات المعلومات والاتصال.
- الأولوية القصوى لضمان الأمن السيبراني هو استباق ومنع التهديدات المحتملة والتصدي بفعالية للتهديدات التي تتحقق.
- يتم دعم الأمن الإلكتروني عن طريق البحث والتطوير المكثف والقادر على المنافسة دولياً.
- يُكفل الأمن الإلكتروني عبر التعاون الدولي مع الحلفاء والشركاء.

ثانياً - الهدف العام من الإستراتيجية: الهدف العام من هذه الإستراتيجية هو زيادة قدرات الأمن السيبراني ، وتوعية السكان حول كيفية التعامل مع التهديدات السيبرانية، وبالتالي ضمان استمرار الثقة في الفضاء الإلكتروني.

ثالثاً - الأهداف الفرعية: تشتمل إستراتيجية الأمن المعلوماتي على الأهداف الفرعية التالية:

- 1- **ضمان حماية نظم المعلومات الأساسية للخدمات الهامة:** ويتم تحقيق هذا الهدف عن طريق الإجراءات التالية:
 - تأمين أو ضمان حلول بديلة للخدمات الهامة.
 - ضمان أمن البنية التحتية وخدمات تكنولوجيات المعلومات والاتصال.
 - إدارة التهديدات السيبرانية على القطاع العام والخاص.
 - تأسيس نظام وطني لرصد أمن المعلومات.
 - ضمان الاستمرارية الرقمية للدولة.
 - تعزيز التعاون الدولي في مجال حماية البنية التحتية الحيوية للمعلومات.
- 2- **تعزيز مكافحة الجرائم الإلكترونية:** وذلك من خلال:
 - تعزيز الكشف عن الجرائم الإلكترونية.
 - رفع مستوى الوعي العام اتجاه مخاطر الانترنت.
 - تعزيز التعاون الدولي لمكافحة الجريمة الإلكترونية.
- 3- **تطوير قدرات الدفاع السيبراني الوطني:** عن طريق:
 - مزامنة التخطيط العسكري والاستعداد لحالات الطوارئ المدنية.
 - تطوير الدفاع السيبراني الجماعي و التعاون الدولي.

- تطوير قدرات الدفاع السيبراني العسكري.
- ضمان مستوى عال من الوعي بشأن دور الأمن السيبراني في الدفاع الوطني.
- 4- تطوير قدرات استونيا في مجال إدارة التهديدات الأمنية الالكترونية: من خلال:
 - تكوين وتأطير جيل قادم من المتخصصين في مجال الأمن المعلوماتي.
 - المساهمة في البحوث المتعلقة بالأمن السيبراني لإيجاد الحلول الآمنة.
 - دعم وتنمية المؤسسات التي توفر الأمن السيبراني وتقديم حلول الأمن المعلوماتي الوطني.
- 5- استونيا تطور الأنشطة المشتركة بين القطاعات :عن طريق:
 - وضع إطار قانوني لدعم الأمن الالكتروني.
 - تعزيز سياسة الأمن السيبراني الدولية.
 - التعاون الوثيق مع الحلفاء والشركاء.
 - تعزيز قدرة الاتحاد الأوروبي.

خاتمة:

إن التطورات الهائلة التي عرفتتها التكنولوجيات الحديثة للإعلام والاتصال، ورغم ما وفرتة من تسهيلات في أمور حياتنا، إلا أنها في المقابل فتحت الباب على مصراعيها لتطور أدوات ووسائل وسبل تنفيذ الجرائم الالكترونية، وجعلتها أكثر تعقيدا وصارت مكافحتها تبدو صعبة المنال إذا لم تتضافر جهود جميع الأطراف الفاعلة في الساحة المعلوماتية، وأمام هذا الوضع بات لزاما على حكومات الدول الإسراع في اتخاذ الإجراءات اللازمة لتطوير آليات التصدي لمثل هذه الجرائم وتعزيز التعاون الدولي في هذا المجال.

فعالية التعاون الدولي في مواجهة الجريمة المعلوماتية

د/ وحي المختار

كلية الحقوق والعلوم السياسية - جامعة المسيلة

مقدمة:

تعتبر الجريمة المعلوماتية من الجرائم المستحدثة، لكونها ظهرت مع التطور التكنولوجي والثورة التقنية في وسائل الاتصال وارتباطها الوثيق بشبكة الانترنت، ولهذا فهي من الجرائم العابرة للحدود، حيث أصبحت تهدد سيادة الدول وتزعزع استقرارها الاقتصادي، كما تكمن خطورتها في صعوبة اكتشافها وعدم الوصول الى الدليل المادي لإدانة مرتكبيها في غالب الأحيان.

ونتيجة لهذه الإشكالات التي تطرحها هذه الجريمة، كان لابد للمجتمع الدولي مواجهتها وضرورة التعاون الدولي الفعال في سبيل الحد منها، والقضاء عليها ومعاقبة مرتكبيها، وعلى هذا الأساس تظهر أهمية التعاون الدولي في مجال التصدي للجريمة المعلوماتية والتحديات التي تقف في سبيل الوصول الى تعاون دولي فعال.

ومن هذا المنطلق تتناول هذه الورقة البحثية محورين:

المحور الاول: التعاون الدولي في مواجهة الجريمة المعلوماتية

المحور الثاني: التحديات التي تواجه التعاون الدولي

المبحث الأول: التعاون الدولي في التصدي للجريمة المعلوماتية

تعتبر الجريمة المعلوماتية إحدى القضايا التي تؤرق دول العالم، حيث تشغل بال المختصين والخبراء، وكذا الحكومات نظرا لخطورتها ونفوذها إلى جميع أنحاء العالم، متخطية جميع الحواجز باعتبارها إشارات إلكترونية، ولهذا فكل المجتمعات الدولية في حاجة إلى خبرة بعضها البعض، مما يحتم ضرورة التعاون الدولي لمواجهة ضراوتها والحد منها ومعاقبة مرتكبيها وتحقيق الردع العام بخصوص هذا النوع من الجرائم.

وعليه يتخذ التعاون الدولي عدة أوجه منها على الخصوص التعاون الدولي الأمني والتعاون الدولي القضائي وتسليم المجرمين.

المطلب الأول: التعاون الدولي الأمني

يعرّف التعاون الدولي الأمني بأنه: «تبادل العون والمساعدة وتضافر الجهود المشتركة بين طرفين دوليين أو أكثر، لتحقيق نفع أو خدمة أو مصلحة مشتركة في مجال التصدي لمخاطر الإجرام، وما يرتبط به في مجالات أخرى، مثل مجال العدالة الجنائية، ومجال الأمن أو لتخطي مشكلات الحدود والسيادة التي قد تعترض الجهود الوطنية لملاحقة المجرمين وتعقب مصادر التهديد، سواء أكانت المساعدة المتبادلة قانونية أو قضائية أو شرطية، وسواء اقتصر على دولتين أو امتدت إقليمياً أو عالمياً».¹

يتضح من خلال هذا التعريف الأهمية القصوى للتعاون الدولي في هذا المجال، وكذا الدور الذي تلعبه المنظمة الدولية للشرطة الجنائية.

الفرع الأول: أهمية التعاون الدولي الأمني وصوره

يعتبر التعاون الدولي الأمني ثمرة الجهود الدولية لتطوير العلاقات فيما بينها، ويقوم هذا التعاون على عدة أسس، كما أن له عدة صور.

أولاً: الأهمية البالغة للتعاون الأمني

تظهر أهمية التعاون الدولي الأمني في مجال التصدي للجريمة المعلوماتية من خلال المخاطر التي تلحق بالمجتمع الدولي وشعوره بها وبما يمكن أن تحدثه من آثار وخيمة على المصالح المشتركة للمجتمع الدولي، وقد استشعرت الدول أنه ليس بإمكانها وبمجهودها المنفردة مواجهة الجريمة بصفة عامة والجريمة المعلوماتية بشكل خاص، هاته الأخيرة التي أصبحت تشكل خطراً لا على سرية النظم الحاسوبية أو سلامتها أو توافرها فحسب، بل تعدت إلى البنى الأساسية الحرجة²، ومع تميزها بالعالمية فإن مواجهتها لا تتحقق في الدول المختلفة، وذلك باستحداث مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المعلوماتية وتعميمها.³

¹ - خالد بن مبارك القروي القحطاني، التعاون الأمني الدولي في مواجهة الجريمة المنظمة عبر الوطنية، أطروحة دكتوراه، جامعة نايف للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2006، ص38.

² - بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة دكتوراه، جامعة الجزائر، 2017-2018، ص64.

³ - جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 1998، ص75.

ومثال على خطورة هذه الجريمة فإن الذي يقوم بها يجمل جنسية دولية ما ويقوم بها من حواسيب موجودة في دولة أخرى، وتقع الآثار لهذه الجريمة في دولة ثالثة، وعليه من البديهي أن تقف مشاكل الحدود والولايات القضائية عقبة أمام اكتشاف هذه الجرائم ومعاينة مرتكبيها.

ثانيا: أسس التعاون الدولي الأمني

التعاون الدولي الأمني في مواجهة الجرائم المعلوماتية يجب أن يقوم على أسس معينة تكفل فعالية التصدي لهذه الجرائم بصورة فعالة، وهذه الأسس تتمثل في الآتي:¹

- 1- التعاون العلمي لبحث ظاهرة جرائم الإنترنت وتوفير المعلومات الإحصائية والبيانات اللازمة، سواء ما يتعلق بالخريطة ذاتها أو ما تعلق بمرتكبيها أو ما يتعلق بسير نظام القضاء الجنائي، وفي سبيل ذلك يجب إنشاء مركز دولي للمعلومات والبيانات الخاصة بتلك الجرائم.
- 2- التنسيق بين المؤسسات الأمنية بآلياتها المختلفة في الساحات الأمنية الدولية والإقليمية، مما يتيح معرفة الثغرات الأمنية ومحاولة سدها.
- 3- تحديد سبل التعاون في مجال التدريب والتعاون التقني وتحقيق التكامل الأمني على المستوى الدولي.
- 4- إعداد مدونة دولية تتضمن توحيد المعايير والأركان القانونية التي تقوم عليها هذه الجرائم.
- 5- وضع استراتيجية وقائية قادرة على خلق المناخ الملائم لأعمال التصدي لهذه الجرائم.

ثالثا: صور التعاون الدولي الأمني

هناك عدة صورة للتعاون الدولي الأمني، نذكر منها على الخصوص:²

- 1- ربط شبكات الاتصال والمعلومات للأجهزة الأمنية والعدالة الجنائية، لتحقيق السرعة في التحقيق والملاحقة.

¹ - عادل عبد العال إبراهيم خراشي، إشكالية التعاون الدولي في مكافحة جرائم المعلوماتية وسبل التغلب عليها، بحث منشور بمجلة كلية الشريعة والقانون بتفهننا، الإشراف بالدقهلية جامعة الأزهر، العدد 16، الجزء الأول، 2014، ص191.

² - عادل عبد العال إبراهيم خراشي، المرجع نفسه، ص194.

2- القيام ببعض العمليات الشرطية والأمنية المشتركة بين الدول، لتعقب المجرم المعلوماتي وتعقب الأدلة الرقمية وضبطها، وهذا يؤدي إلى تبادل الخبرات والمهارات بين الخبراء القائمين على مكافحة هذه الجرائم، وبالتالي وضع حد لها.¹

الفرع الثاني: جهود المنظمة الدولية للشرطة الجنائية (الإنتربول)

الإنتربول هو أكبر منظمة شرطية دولية أنشأت عام 1923، بفيينا ومقرها الرئيسي الآن مدينة "ليون" الفرنسية منذ عام 1989²، وتهدف المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعال في مكافحة الجريمة، والجريمة المعلوماتية من أهم الجرائم التي أولتها المنظمة اهتماما كبيرا، حيث أنشأت المنظمة الدولية للشرطة الجنائية عام 2004، وحدة خاصة لمكافحة الجرائم المعلوماتية، كما قامت بالتعاون مع مجموعة الدول الثمانية (G8) بوضع استراتيجية لمواجهة هذا النوع من الجرائم، تتلخص في التالي:³

1- إنشاء مركز اتصالات أمني عبر الشبكة يعمل دون توقف على مستوى مصالح الشرطة في الدول الأطراف.

2- استخدام وسائل حديثة في تلك المكافحة.

3- تزويد شرطة الدول الأطراف بكتيبات إرشادية حول الجرائم المعلوماتية، وكيفية التدريب على مكافحتها والتحقيق فيها.

¹ - سليمان أحمد فاضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، دار النهضة العربية، القاهرة، 2013، ص 45.

² - للمزيد من التفصيل حول نشأة هذه المنظمة وتطورها راجع: عبد الواحد الفار، الجرائم الدولية وسلطة العقاب عليها، دار النهضة العربية، القاهرة، 1996، ص 596 وما بعدها.

³ - عادل عبد العال إبراهيم خراشي، مرجع سابق، ص 198.

ويمكن الإشارة هنا إلى أنه تم إنشاء شرطة أوروبية في لكسمبورغ عام 1991، لتكون همزة وصل بين أجهزة الشرطة الأوروبية لملاحقة الجناة في الجرائم العابرة للحدود ومنها بطبيعة الحال الجرائم المعلوماتية، ونفس الشيء تم إنشاء منظمة الشرطة الجنائية الإفريقية.¹

المطلب الثاني: التعاون الدولي القضائي وتسليم المجرمين

نتيجة لخطورة الجريمة المعلوماتية وصعوبة تتبعها والحد منها كونها عابرة للحدود تتطلب التدخل السريع من خلال التعاون القضائي بين الدول من خلال عدة آليات كالمساعدة القضائية والإنابة القضائية وغيرها من الإجراءات، وكذلك لتفعيل ملاحقة مرتكبي الجريمة المعلوماتية أينما كانوا لا بد من تسليم المجرمين من خلال سن التشريعات اللازمة لذلك.

الفرع الأول: التعاون القضائي الدولي

إن ملاحقة مرتكبي الجرائم المعلوماتية يستلزم القيام بإجراءات خارج حدود الدولة حيث ارتكبت الجريمة أو جزء منها، وهذا يصطدم على أرض الواقع بمشاكل الحدود والولايات القضائية، وعليه لا مناص من تقديم المساعدة القضائية الدولية، وتعرف هاته الأخيرة بأنها: «كل إجراء قضائي تقوم دولة من شأنه لتسهيل جهة المحاكمة في دولة أخرى بصدد جريمة من الجرائم»²، وتتخذ المساعدة القضائية في المجال الجنائي عدة صور منها:³

أولاً: تبادل المعلومات

ويتم ذلك بواسطة تبادل البيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية بصدد النظر في جريمة ما، كما أن هناك صورة أخرى لتبادل المعلومات تتعلق بالسوابق القضائية للجنة⁴، من خلالها تتعرف الجهات القضائية بدقة على الماضي الجنائي.

¹ - منظمة الشرطة الجنائية الإفريقية (الأفريبول)، هي منظمة تسهل تبادل المعلومات بين قوات الشرطة الوطنية بخصوص الجريمة الدولية والإرهاب والمخدرات والاتجار بالأسلحة في إفريقيا، أنشئت يوم 13 ديسمبر 2015 ومقرها بالجزائر، ومكونة من قوات الشرطة لـ 41 دولة.

² - سالم محمد سليمان الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية، أطروحة دكتوراه، جامعة عين شمس، جمهورية مصر، 1997، ص 425.

³ - بدري فيصل، مرجع سابق، ص 68 وما بعدها.

⁴ - توجد لهذه الصورة عدة تطبيقات منها ما ورد في الفقرتين 6 و 7 من المادة الأولى من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية الصادرة في 14 مارس 1990 في الجلسة العامة 68 للجمعية العام

ثانيا: نقل الإجراءات

ويقصد به قيام دولة ما باتخاذ الإجراءات الجنائية بشأن جريمة ارتكبت في إقليم دولة أخرى، ولمصلحة هذه الدولة بناء على اتفاقية متى توافرت شروط معينة أهمها:¹

1- التجريم المزدوج، أي أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب منها عن ذات الجريمة.

2- أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والمطلوب منها.

3- أن تكون الإجراءات المطلوب اتخاذها من الأهمية بمكان تؤدي إلى الوصول إلى الحقيقة. وقد أقرت العديد من الاتفاقيات الدولية والإقليمية هذه الصورة، كإحدى صور المساعدة القضائية الدولية، كاتفاقية الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية²، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام 2000 في المادة (21) منها، وكذلك معاهدة المؤتمر الإسلامي لمكافحة الإرهاب لعام 1999 في المادة (9) منها.

ثالثا: الإنابة القضائية

يقصد بالإنابة القضائية الدولية اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية، تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها لضرورة ذلك للفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام بنفسها³، والهدف منها هو تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة في قضايا ممتدة خارج الحدود الوطنية.⁴

للأمم المتحدة وتقضي باتفاق أطرافها أن يقدم كل منهم للآخر أكبر قدر من المساعدة المتبادلة في التحقيقات وإجراءات المحاكمة المتعلقة بجرائم يكون العقاب عليها وقت طلب المساعدة داخلا في اختصاص السلطة القضائية طالبة المساعدة، وكذلك الفقرتان 3 و4 من المادة (08) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة لعام 2000.

1 - سالم محمد سليمان الأوجلي، مرجع سابق، ص 427.

2 - اعتمدت هذه المعاهدة بواسطة جمعية الأمم المتحدة بالقرار 48/118 بتاريخ 14 ديسمبر 1990.

3 - جميل عبد الباقي الصغير، مرجع سابق، ص 83.

4 - قرران مصطفى، الآليات الدولية لمكافحة الجريمة الإلكترونية، بحث مقدم في الملتقى الدولي حول التنظيم القانوني للإنترنت والجريمة الإلكترونية، جامعة زيان عاشور، الجلفة، 27 و28 أبريل 2008، ص 8.

تجدر الإشارة إلى أن الإنابة القضائية عرفتها الشريعة الإسلامية وهناك من المذاهب من عبر عنها بالاستنابة كالمالكية ويقصد بها كتاب القاضي إلى القاضي.¹

الفرع الثاني: التعاون الدولي بشأن تسليم المجرمين لمكافحة الجريمة المعلوماتية

تسليم المجرمين هو إجراء من إجراءات التعاون القضائي الدولي تقوم به إحدى الدول بتسليم شخص متواجد على إقليمها إلى دولة أخرى، أو إلى جهة قضائية دولية، إما بهدف محاكمته عن جريمة أتم ارتكابها، وإما لأجل تنفيذ حكم الإدانة ضده من محاكم هذه الدولة أو الجهة القضائية الدولية²، لكن هناك من يعبر عن التسليم بنقل كما هو عليه حال النظام الأساسي للمحكمة الجنائية الدولية، دلالة على أن التسليم يتم بين دولة ودولة أو جهة قضائية أخرى بناء على معاهدة أو اتفاقية، لكن بالنسبة للمحكمة الجنائية الدولية لا يتم بناء على أية معاهدة أو اتفاقية.³ ولكي يتسنى لنا الإحاطة بالتعاون الدولي بشأن تسليم المجرمين نتعرض بالدراسة إلى شروطه وصوره، ثم مظاهر هذا التعاون الدولي.

أولاً: صور التسليم

هناك ثلاث صور للتسليم من خلال الممارسة الدولية وهي:

1 - راجع بخصوص الإنابة القضائية في الشريعة الإسلامية، عادل عبد العال إبراهيم خراشي، مرجع سابق، ص 210 وما يليها.

2 - سيمان عبد المنعم، الجوانب الإشكالية في النظام القانوني لتسليم المجرمين (دراسة مقارنة)، دار الجامعة الجديدة، الإسكندرية، 2007، ص7؛

وللمزيد أنظر: محمد طلعت الغنيمي، الوسيط في قانون السلام، منشأة المعارف، الإسكندرية، 1983، ص435.

3 - تنص المادة 102 من نظام روما الأساسي على:

«لأغراض هذا النظام الأساسي

(أ) يعني "التقديم" نقل دولة ما شخصاً إلى المحكمة عملاً بهذا النظام الأساسي

(ب) يعني "التسليم" نقل دولة ما شخصاً إلى دولة أخرى بموجب معاهدة أو اتفاقية أو تشريع وطني»

1-التسليم القضائي:

وهذا الذي تكون فيه المحاكم الجهة المختصة الوحيدة والمخول لها إصدار قرا التسليم، ويعاب على النوع بطء الإجراءات وهو ما ينعكس سلبا على ما تستوجبه سرعة متابعة مرتكبي الجرائم المعلوماتية لسهولة اندثار أدلة الإثبات.¹

2-التسليم الإداري:

يعتبر هذا النوع من التسليم عملا من أعمال السيادة أو تدبيرا من تدابير السلطة التنفيذية والتي لها صلاحيات مطلقة في ذلك تبعا لاعتبارات سياسية أو إدارية أو غير ذلك من الاعتبارات، ومن إيجابيات هذا النظام السرعة في البت في طلب التسليم لأنه لا يتطلب إجراءات طويلة ومعقدة ولا يحتاج إلى نفقات مثل النظام القضائي في السابق، بالإضافة إلى أنه يساعد على تحسين العلاقات الدولية بين الدول، وعلى الرغم من ذلك فإن لهذا النظام سلبيات منها إهداره لحقوق الأفراد الدفاعية، بالإضافة إلى المجالات الدولية وكذا في الغالب يحدث هذا التسليم في إطار التعقيم والكتمان مما يعني بعده عن الأجهزة الرقابية القضائية والتشريعية.²

3-التسليم المختلط:

وهذا الأكثر رواجاً وهو يجمع بين الجانبين القضائي والإداري، كما أنه يوازي بين مصلحتين متعارضتين، مصلحة الدولة طالبة التسليم ومصلحة الشخص المطلوب تسليمه حيث يكون للسلطة القضائية حق فحص الطلب، وتمنح الشخص المطلوب تسليمه كل الضمانات القانونية للدفاع، شريطة أن لا تقحم الدولة المطلوب منها التسليم نفسها في فحص وقائع الدعوى، وتكتفي بما يرد إليها من مستندات ووثائق من الدولة الطالبة.³

¹ - قززان مصطفى، مرجع سابق، ص 9.

² - الغافري حسين بن سعيد، الجهود الدولية في مواجهة الإنترنت، بحث منشور على شبكة الإنترنت، موقع المنشاوي للدراسات والبحوث www.minshawi.com، تاريخ الاطلاع عليه 2009/02/12 الساعة 09.00، ص 22.

³ - بدري فيصل، مرجع سابق، ص 74.

ثانيا: شروط تسليم المجرمين

شروط التسليم تكاد تتفق في جميع حالات التسليم من حيث العناصر، أما من حيث الموضوع فهي محل خلاف بين الدول، وذلك بحسب حاجاتها للتسليم، واعتبارات المصالح الدولية¹، وهي كالاتي:

1- شرط التجريم المزدوج:

يقصد به أن يكون الفعل سبب التسليم مجرماً في قانون كل من الدولتين الطالبة والمطلوب إليها التسليم، وهذا الشرط يعتبر من أهم مبادئ النظام القانوني للتسليم الذي لا يتصور الخروج عليه سواء على صعيد المعاهدات الدولية أو على صعيد التشريع الوطني².

من بين المعاهدات التي كرست شرط التجريم المزدوج في مجال التسليم هي اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، إذ تنص في مادتها 16 التي تحدد الجرائم الخاضعة لنظام التسليم «...شرط أن يكون المجرم الذي يلتمس بشأنه التسليم معاقباً عليه بمقتضى القانون الداخلي لكل من الدولة الطالبة والدولة الطرف متلقية الطلب».

2- درجة جسامة الجريمة

هناك بعض التشريعات تشترط درجة معينة من الجسامة أو حد ادنى من العقوبة الموافقة لهذه الجريمة وفق تشريعاتها الداخلية، وكذا في بعض الاتفاقيات الدولية³، كما هو عليه الحال في المادة 2 من المعاهدة النموذجية بشأن تسليم المجرمين والمادة 24 من الاتفاقية الأوروبية للإجرام المعلوماتي.

3- الشروط المتعلقة بالأشخاص المطلوب تسليمهم

يمكن إنجازها في التالي:⁴

- أ - عدم جواز تسليم الرعايا.
- ب - عدم جواز تسليم اللاجئين السياسيين.
- ج - عدم جواز تسليم المحاكمين على ذات الجريمة.

1 - عادل عبد العال إبراهيم خراشي، مرجع سابق، ص 220.

2 - سليمان عبد المنعم، مرجع سابق، ص 131.

3 - المرجع نفسه، ص 205 وما بعدها.

4 - بدري فيصل، مرجع سابق، ص 76 وما بعدها.

الفرع الثالث: مظاهر التعاون الدولي في مجال التدريب على مكافحة الجريمة المعلوماتية

التدريب يعتبر أمراً مهماً من أجل كفاءة وفعالية مواجهة هذا النوع من الجرائم ويجب أن ينصب على بيان المخاطر والتهديدات ونقاط الضعف والاختراقات لشبكة المعلومات، مع تبيان مفاهيم معالجة البيانات وتحديد نوعية وأنماط الجرائم المعلوماتية، وكذا صفات المجرم المعلوماتي.¹ ومن هنا لا بد من التعاون الدولي في مجال تدريب رجال العدالة، وهو ما دعت إليه بعض الاتفاقيات الدولية، كاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام 2000²، ولأنه لا يمكن لدولة بمفردها مواجهة تحديات هذا النوع من الجرائم ما لم تعاون مع غيرها وبالخصوص في مجال التدريب، خاصة بالنسبة للدول النامية التي تفتقر لخبراء مختصين في التحري والتحقيق، بالإضافة إلى حاجتها للمساعدة التقنية.

المبحث الثاني: التحديات التي تواجه التعاون الدولي وسبل مواجهتها

إنه مع وجود هذا التطور الهائل في مجال الاتصالات ونقل المعلومات والبيانات عن طريق شبكة الإنترنت، قد يحدث أن يتم التلاعب بهذه المعطيات مما سبب خسائر وأضرار للدول والشركات والأفراد، مما حتم ضرورة التعاون الواسع بين الدول لمواجهة هذا الخطر عن طريق الاتفاقيات الدولية والإقليمية والثنائية وكذا المؤتمرات، إلا أن هناك تحديات ومعوقات تقف دون فعالية هذا التعاون وتجعله محدوداً (المطلب الأول)، وعليه لابد من البحث عن السبل الكفيلة للتغلب على الصعوبات التي تعيق التعاون الدولي، في مجال مكافحة الجريمة المعلوماتية (المطلب الثاني).

المطلب الأول: التحديات التي تواجه التعاون الدولي في مجال مكافحة الجريمة المعلوماتية

إن التعاون الدولي في مجال التصدي للجريمة المعلوماتية الذي هو مطلب كل الدول في الوقت الحالي بغية تحقيقه، إلا أن هناك صعوبات ومعوقات تقف دون تحقيقه.

الفرع الأول: تعدد صور النشاط الإجرامي واختلاف النظم القانونية الإجرائية

هناك قصور في تشريعات الدول نظراً لتعدد صور النشاط الإجرامي وعدم وجود نموذج موحد له، بالإضافة إلى تنوع واختلاف النظم القانونية الإجرائية.

¹ - المرجع نفسه، ص 84.

² - المادة 29 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام 2000.

أولاً: عدم وجود نموذج موحد للنشاط الإجرامي¹

يلاحظ البعض بأن الأنظمة القانونية المختلفة لمواجهة الجريمة المعلوماتية، ليس على توافق حول نماذج استخدام نظام المعلومات وشبكات الإنترنت الواجب تجريمها، فما يكون مباحاً في أحد الأنظمة قد يكون مجرمًا وغير مباح في نظام آخر، ويعود ذلك إلى عدة عوامل كاختلاف العادات والتقاليد والديانات والثقافات من مجتمع لآخر، وبالتالي اختلاف السياسة التشريعية².

ثانياً: تنوع واختلاف النظم القانونية الإجرائية

نظراً لاختلاف النظم القانونية الإجرائية نجد أن طرق التحري والتحقيق والمحاكمة التي تثبت فعاليتها في دولة ما، قد تكون عديمة الفائدة في دولة أخرى، أو قد لا تسمح بإجرائها كالمراقبة الإلكترونية³، بالإضافة إلى ذلك السلطات القضائية لدى الدولة الثانية قد لا تسمح باستخدام أي دليل تم الحصول عليه بطرق ترى هذه الدولة أنها غير مشروعة حتى وإن كان هذا الدليل تم الحصول عليه بشكل مشروع⁴.

الفرع الثاني: تنازع الاختصاص القضائي وإشكالات الإنابة القضائية

من أشكال التعاون الدولي في مجال مواجهة الجرائم المعلوماتية تنازع الاختصاص القضائي وكذا صعوبات الإنابة القضائية الدولية.

أولاً: تنازع الاختصاص

الجرائم المعلوماتية من أكثر الجرائم التي تثير مسألة الاختصاص على المستوى الدولي، حيث اختلاف التشريعات والنظم القانونية، فقد يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى استناداً إلى مبدأ الإقليمية، وتخضع كذلك الجريمة ذاتها لاختصاص الدولة التابع لها هذا الأجنبي وفقاً لمبدأ الاختصاص الشخصي، وقد تكون

¹ - عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، 2002، ص102.

² - جميل عبد الباقي الصغير، مرجع سابق، ص72.

³ - عادل عبد العال إبراهيم خراشي، مرجع سابق، ص237.

⁴ - الغافري حسين بن سعيد، مرجع سابق، ص52.

هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى فتدخل عندئذ في اختصاصها استنادا إلى مبدأ العينية.¹

كما أن فكرة الاختصاص القضائي تثار في حالة تأسيس الاختصاص على مبدأ الإقليمية، كما لو قام الجاني ببث الصور الخليعة ذات الطابع الإباحي من إقليم دولة معينة وتم الاطلاع عليها في دولة أخرى، ففي هذه الحالة يثبت الاختصاص وفقا لمبدأ الإقليمية لكل دولة من الدول التي مستها الجريمة.²

ثانيا: الصعوبات الخاصة بالمساعدة القضائية الدولية

من صعوبات التعاون الدولي في مواجهة الجرائم المعلوماتية المتعلقة بالإبادة القضائية، ما يعرف بإشكالية فكرة السيادة، حيث أن كل دولة عادة ما تقوم بنفسها وعبر جهازها القضائي بالفصل في كافة المنازعات التي تثار على أراضيها لاعتبارات ترتبط بفكرة السيادة. بالإضافة الى هذه الإشكالية الأولى، فإن هناك صعوبات أخرى تتمثل في بقاء الإجراءات المتعلقة بالإبادة القضائية، أي التباطؤ في الرد في مجال المساعدات القضائية المتبادلة، وهذا يتعارض مع طبيعة أعمال الإنترنت وما تتميز به من سرعة.³

الفرع الثاني: الصعوبات الخاصة بتسليم المجرمين في مواجهة الجريمة المعلوماتية

تتمثل صعوبات التعاون الدولي في مجال تسليم المجرمين في إشكاليتين هما: التجريم المزدوج والتزاحم في طلبات التسليم.

أولا: التجريم المزدوج

يعتبر التجريم المزدوج من أهم الشروط الخاصة بنظام تسليم المجرمين، فقد نصت عليه أغلب الصكوك الدولية والتشريعات الوطنية المعنية بتسليم المجرمين، وبالرغم من أهميته، إلا أنه غالبا ما يكون عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم المعلوماتية، لا سيما وأن معظم الدول لا

¹ - جميل عبد الباقي الصغير، مرجع سابق، ص73.

² - عبد الفتاح بيومي حجازي، مرجع سابق، ص52.

³ - التباطؤ في الرد قد يكون نتيجة الصعوبات اللغوية، أو الفوارق في الإجراءات، أو بسبب نقص الموظفين المدربين وغيرها من الأسباب.

أنظر في ذلك: بدرى فيصل، مرجع سابق، ص111.

تجرّم هذه الجرائم¹، بالإضافة إلى أنه توجد صعوبة فيما إذا كانت النصوص القانونية التقليدية لدى الدولة المطلوب فيها التسليم يمكن أن تنطبق على الجرائم المعلوماتية أولاً، الأمر الذي يعرقل تطبيق الاتفاقية الدولية في مجال تسليم المجرمين، ويحول بالتالي دون جمع الأدلة ومحاكمة مرتكبي الجرائم المعلوماتية².

ثانياً: التزامات طلبات التسليم³

ويقصد بالتزامات طلبات التسليم هي الحالات التي يصل فيها الدولة المطلوب منها التسليم أكثر من طلب تسليم من عدة دول تطلب ذات الشخص، سواء كان الطلب متعلق بنفس الجريمة أو بجرائم أخرى، والإشكالية المطروحة بالنسبة للجرائم المعلوماتية تتمثل في أن الشخص المطلوب تسليمه، قد يرتكب جريمة أو أكثر من الجرائم المعلوماتية تمس في نفس الوقت مصالح أساسية لأكثر من دولة، ففي هذه الحالة تتزام طلبات التسليم المقدمة من الدول المضرومة إلى الدول المطلوب إليها⁴.

ولا يشترط في التزام حجم الطلبات أن تتعاصر في وصولها إلى الدولة المطلوب إليها، بل يكفي أن تتوالى إلى الدولة المطلوب إليها، طالما أن الشخص المطلوب ما زال متواجداً على إقليمها، ولم يتم تسليمه إلى أي من الدول⁵.

المطلب الثاني: سبل التغلب على صعوبات التعاون الدولي في مجال مكافحة الجرائم المعلوماتية
بما أن الجرائم المعلوماتية من الجرائم المستحدثة التي تطورت بشكل كبير مع القصور المذهل في تكنولوجيات الإعلام والاتصال، وهذا أدى إلى القول بأنه ليست كل الدول باستطاعتها مواجهة هذا النوع من الجرائم، خاصة الدول النامية، ولهذا كان لا مناص من التعاون الدولي في هذا المجال، الذي تعترضه عدة صعوبات تحول دون فعاليته في ملاحقة مرتكبي هذه الجرائم. وعليه ما هي السبل الكفيلة للتغلب على إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية؟

1 - الغافري حسين بن سعيد، مرجع سابق، ص 53.

2 - جميل عبد الباقي الصغير، مرجع سابق، ص 91.

3 - عادل عبد العال إبراهيم خراشي، مرجع سابق، ص 247.

4 - المرجع نفسه، الصفحة نفسها.

5 المرجع نفسه، الصفحة نفسها.

الفرع الأول: سبل التغلب على تعدد صور النشاط الإجرامي واختلاف النظم القانونية الإجرائية

تسعى دول العالم إلى مواكبة التطورات خاصة ما تعلق منها بتكنولوجيات الإعلام والاتصال، وذلك بإصلاح التشريعات الجنائية ومحاولة توحيد النظم القانونية.

أولاً: معالجة إشكالية تعدد صور النشاط الإجرامي

لكي يتم التغلب على هذه الإشكالية، لا بد من توحيد النظم القانونية ولاستحالة هذا الأمر، فإنه لا مناص من البحث عن طريقة أخرى تساعد على إيجاد تعاون دولي يتفق مع طبيعة هذا النوع من الجرائم، ويخفف من غلو الفوارق بين الأنظمة القضائية الداخلية، وتتمثل هذه الوسيلة في تحديث التشريعات المحلية المعنية بالجرائم المعلوماتية، وإبرام اتفاقيات خاصة يراعى فيها هذا النوع من الجرائم¹.

ولتفعيل التعاون الدولي في هذا المجال لا بد من التركيز على العناصر التالية²:

- 1- الانضمام إلى المعاهدات الدولية التي تعمل على زيادة التعاون والتنسيق بين الجهود التي تبذلها الدول في مجال مكافحة الجرائم المعلوماتية.
- 2- إدخال تلك المعاهدات إلى حيز التنفيذ الفعلي.
- 3- العمل على وجود أكبر قدر ممكن من التطابق فيما بين قوانين الدول المختلفة.

ثانياً: سبل التغلب على إشكالية تنوع واختلاف النظم القانونية الإجرائية

بخصوص هذه الإشكالية نجد أن الكثير من المواثيق الدولية تشجع الدول الأطراف فيها على السماح باستخدام بعض تقنيات التحقيق الخاصة، الشيء الذي يخفف من الاختلاف الكبير بين النظم القانونية الإجرائية ويفتح المجال أمام تعاون دولي فعال³.

ومن الأمثلة على هذه المواثيق الدولية نجد اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية في مادتها 20، تشير إلى أن التسليم المراقب والمراقبة الإلكترونية وغيرها من أشكال المراقبة المستمرة، والتي تعتبر من أهم التقنيات المستخدمة في التصدي للجماعات الإجرامية المنظمة، بسبب الأخطار

¹ - الغافري حسين بن سعيد، مرجع سابق، ص 55.

² - عادل عبد العال إبراهيم خراسي، مرجع سابق، ص 261.

³ - المرجع نفسه، ص 264.

والصعوبات الكامنة وراء محاولة الوصول إلى عملياتها، وتجميع المعلومات وأدلة الإثبات لاستخدامها فيما بعد في الملاحقة القضائية المحلية فيها، أو الدولية في دول أطراف في سياق نظم المساعدة القانونية المتبادلة، وهو ما أكدت عليه المادة 29 من الاتفاقية الأوروبية للإجرام المعلوماتي العام 2001¹.

ومن خلال نصوص الاتفاقية الأوروبية للإجرام المعلوماتي، يلاحظ أنها قد أوجدت بعض الحلول، التي من شأنها التغلب على مشكلة اختلاف النظم الإجرائية أمام التعاون الدولي لمواجهة الجرائم المعلوماتية.²

الفرع الثاني: سبل التغلب على إشكالية الاختصاص والمساعدة القضائية

مشكلة تنازع الاختصاص بالنسبة للجريمة المعلوماتية طرحت صعوبة كبيرة بالنسبة للتعاون الدولي لمواجهة هذه الجريمة، ونفس الشيء بالنسبة للمساعدة القضائية.

أولاً: التغلب على إشكالية تنازع الاختصاص

تطرح مسألتان للتغلب على هذه الإشكالية

الأولى: تتمثل في إبرام اتفاقيات دولية ثنائية كانت أو جماعية، يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الاختصاص القضائي، بالإضافة إلى تحديث القوانين الجنائية الموضوعية منها والإجرائية، بما يتناسب والتطور الكبير الذي يشهده عالم تكنولوجيا المعلومات والاتصال.³

أما الثانية: فتتمثل في اعتبار جميع الجرائم المعلوماتية من الجرائم الدولية، وتدخل في الاختصاص القضائي العالمي، أي أن يعقد الاختصاص القضائي العالمي لأي دولة ترغب في ملاحقة مرتكبي

1 - لقد أكدت المادة 29 على سرية حفظ البيانات المعلوماتية المخزنة وأجازت لكل طرف أن يطلب من الطرف الآخر الحفظ السريع للمعلومات المخزنة عن طريق إحدى الوسائل الإلكترونية الموجودة داخل النطاق المكاني لذلك الطرف الآخر والتي ينوي الطرف الطالب للمساعدة أن يقدم طلباً للمساعدة بشأنها، بغرض القيام بالتفتيش أو الدخول بأي طريقة مماثلة وضبط أو الحصول أو الكشف على البيانات المشار إليها.

بالإضافة إلى هذا النص أشارت المادة 30 من ذات الاتفاقية إلى الكشف السريع عن البيانات المحفوظة والمساعدة المتعلقة بالخوّل إلى البيانات؛ راجع مزيداً من التفصيل حول هذه الاتفاقية: عادل عبد العال إبراهيم خراشي، مرجع سابق، ص 265 وما بعدها.

2 - بدري فيصل، مرجع سابق، ص 117.

3 - المرجع نفسه، ص 119.

الجرائم الدولية، دون اعتبار لجنسية مرتكبيها، أو المكان الذي ارتكبت فيه الجريمة، وينطلق أصحاب هذا الرأي من كون الجرائم المعلوماتية هي من الجرائم الدولية، كونها أصبحت تشكل تهديدا للسلم والأمن الدوليين¹.

ثانيا: التغلب على الصعوبات المتعلقة بالمساعدة القضائية الدولية

بالنسبة لهذه المشكلة يتطلب الأمر إيجاد وسيلة أو طريقة تتسم بالسرعة تسلم من خلالها طلبات الإنابة القضائية، كتعيين سلطة وكزية مثلا أو السماح بالاتصال المباشر بين الجهات المختصة في النظر في مقل هذه الطلبات² وبخصوص الرد على طلبات التماس المساعدة فإنه من الضروري الاستجابة السريعة على هذه الطلبات وهو ما نصت عليه أغلب الاتفاقيات والمعاهدات الخاصة بالمساعدة القضائية المتبادلة³.

أما بخصوص إشكالية السيادة كعائق أمام المساعدة القضائية فهذا لم يعد مطروحا الآن لأن غالبية الدول أصبحت منخرطة في معاهدات ثنائية أو جماعية تكرس مبدأ التعاون بين سلطاتها من أجل مكافحة الجريمة بصفة عامة والجرائم المعلوماتية بصفة خاصة.

الفرع الثاني: سبل التغلب على الإشكاليات الخاصة بتسليم المجرمين

نبحث في هذا الفرع كيفية معالجة إشكالية ازدواجية التجريم أولا ثم معالجة الإشكالية الثانية والمتمثلة في التزام في طلبات التسليم.

أولا: معالجة إشكالية التجريم المزدوج

لأجل التغلب على هذه الإشكالية ركزت الاتجاهاات والتطورات التشريعية الخاصة بتسليم المجرمين، على تحقيق التطبيق الصارم لهذا الشرط، وذلك بإدراج أحكام عامة في المعاهدات والاتفاقيات

¹ - عادل عبد العال إبراهيم خراشي، مرجع سابق، 239.

² - هذا ما أوصى به مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية الذي انعقد ببانكوك 2005، حيث أكد على ضرورة تعزيز فعالية السلطات المركزية المعنية الضالعة في مجال المساعدة القانونية المتبادلة وإقامة قنوات مباشرة للاتصال فيما بينها بغية تنفيذ الطلبات في الوقت المناسب، ونفس الأمر نصت عليه الاتفاقية الأوروبية للإجرام المعلوماتي في المادتين 27 و35:

لمزيد من التفصيل راجع: بدري فيصل، مرجع سابق، ص 119 وما بعدها.

³ - أنظر المادة 25 من الاتفاقية الأوروبية للإجرام المعلوماتي.

الدولية المعنية بتسليم المجرمين، واما بسرد الأفعال التي تتطلب أن تجرم بمقتضى قوانين الدولتين معا، أو بمجرد السماح بالتسليم لأي سلوك يتم تجريمه ويخضع لمستوى معين من العقوبة في كل دولة¹. كما أن اتفاقية الأمم المتحدة لمكافحة الفساد لعام 2003 قد أوجدت مخرجا مناسباً لما تطرحه مشكلة ازدواج التجريم، فمن خلال التزام الدول بتجريم الأفعال المنصوص عليها في الاتفاقيات التي يتم عقدها بين الدول، فإن ذلك يوفر الأساس الكافي لتحقيق شرط ازدواج التجريم²، وقد ذهبت بعض الاتفاقيات إلى التحلل من شرط ازدواج التجريم في حالة ما إذا كان الشخص المطلوب من رعايا الدولة طالبة التسليم، أو كان من رعايا دولة أخرى تقرر نفس العقوبة، مثل اتفاقية الدول العربية للتعاون القضائي³.

ثانيا: معالجة إشكالية التزام في طلبات التسليم

هناك اختلاف بين الدول من حيث تحديد ترتيب التسليم في حالة تراحم طلبات التسليم وهذا يرجع بالأساس إلى اختلاف مصالح الدول وأولوياتها مع الأطراف المتعاقدة، بل أن هذا الاختلاف موجود حتى على مستوى الدولة الواحدة⁴، لكن في واقع الأمر أن الدولة لها مطلق الحرية في تحديد أولويات التسليم، عكس ما نصت عليه الاتفاقية العربية الخاصة بالتسليم التي أعطت الأولوية لجسامة الجرم⁵، وعليه فإن التغلب على هذه الإشكالية يتطلب الأمر عقد اتفاقية دولية تتضمن وضع ضوابط موضوعية وآليات محددة، يتبعها المجتمع الدولي كأن تكون الأولوية في التسليم مثلاً للدولة التي

1 - عادل عبد العال إبراهيم خراشي، مرجع سابق، ص 558.

2 - تنص المادة 2/43 من اتفاقية الأمم المتحدة لمكافحة الفساد على أن: «في مسائل التعاون الدولي كلما اشترط توافر ازدواجية التجريم وجب اعتبار ذلك الشرط مستوفى، بصرف النظر عما إذا كانت قوانين الدولة الطرف متلقية الطلب تدرج الجرم المعني ضمن فئة الجرائم التي تدرجه فيها الدولة الطرف طالبة أو تستخدمه في تسميته نفس المصطلح الذي تستخدمه الدولة الطرف طالبة، إذا كان السلوك الذي عليه الجرم تلتبس بشأنه المساعدة، يعتبر فعلاً إجرامياً في قوانين كلتا الدولتين الطرفين».

3 - اتفاقية تسليم المجرمين المعقودة بين دول الجامعة العربية.

4 - الغافري حسين بن سعيد، مرجع سابق، ص 295.

5 - نصت المادة 13 من الاتفاقية العربية الخاصة بالتسليم على أنه: «إذا قدمت إلى الدولة المطلوب إليها عدة طلبات من دولة مختلفة بشأن تسليم متهم من أجل نفس الجريمة، فتكون الأولوية في التسليم للدولة التي أضرت الجريمة بمصالحها، ثم الدولة التي ارتكبت الجريمة على أرضها، ثم الدولة التي ينتمي إليها المطلوب تسليمه، أما إذا كانت طلبات التسليم خاصة بجرائم مختلفة فتكون الأولوية للدولة التي طلبت التسليم قبل غيرها».

أضرت الجريمة بمصالحها، ثم الدولة التي ارتكبت الجريمة على أرضيها، ثم الدولة التي ينتمي إليها المطلوب تسليمه، وإذا كانت طلبات التسليم عن جرائم مختلفة، فإن الأفضلية تعطى للدولة التي ارتكبت داخل حدودها الجرائم الأكثر خطورة، وفقا لتشريع الدولة المطلوب إليها التسلم، أما إذا تساوت في الخطورة فإن الأفضلية تكون للدولة التي قدمت الطلب أولاً¹. ومن الأمثلة على عملية التعاون الدولي لتسليم المجرمين في الجرائم المعلوماتية، نذكر عملية محطم الجليد قامت بها الشرطة الجنائية الأوروبية (يوروبول) في 14 جوان 2005، تم خلالها مداومة وتفتيش أماكن في 13 دولة أوروبية، وتم توقيف عدة أشخاص في كل من فرنسا، بلجيكا، المجر، إيسلندا، السويد، وتم تسليمهم إلى بريطانيا، حيث قام القضاء الجنائي البريطاني بإدانتهم².

¹ - عادل عبد العال إبراهيم خراشي، مرجع سابق، ص 296 وما بعدها.

² لمزيد من التفصيل عن هذه الواقعة وغيرها، راجع: عادل عبد العال إبراهيم خراشي، مرجع سابق، ص 302.

الخلاصة:

من خلال هذه الورقة البحثية المتعلقة بفعالية التعاون الدولي في مواجهة الجريمة المعلوماتية، توصلنا إلى مجموعة من النتائج أهمها:

- 1- الجريمة المعلوماتية من أخطر الجرائم المستحدثة لما يعتريها من صعوبات الإثبات وتطورها السريع ومساسها باستقرار الدول، كونها مرتبطة بالتطور الهائل في تكنولوجيات الإعلام والاتصال.
 - 2- لا يمكن لأي دولة مهما بلغت من التطور التكنولوجي من التصدي بمفردها للجريمة المعلوماتية، باعتبارها من الجرائم العابرة للحدود.
 - 3- يعد مبدأ التعاون الدولي من أهم المبادئ القانونية الدولية في مكافحة الجريمة المعلوماتية، خاصة وأنه أعطى نتائج مهمة في مكافحة الجرائم الأخرى كجرائم الإرهاب الدولي.
 - 4- بالرغم من أهمية التعاون الدولي في مواجهة الجرائم المعلوماتية، إلا أن غالباً ما تعترضه صعوبات تحد من فعاليته أهمها، تنوع واختلاف النظم القانونية الإجرائية، تنازع الاختصاص القضائي الدولي، إشكالية تسليم المجرمين، عدم وجود نموذج موحد للنشاط الإجرامي.
 - 5- بالرغم من وجود عدة اتفاقيات دولية وإقليمية تتعلق بالجرائم المعلوماتية إلا أنها غير كافية لمعالجة سائر الجرائم المعلوماتية.
- بناء على ما تقدم توصلت إلى مجموعة من الاقتراحات أهمها:
- 1- يتعين على الدول توحيد النظم القانونية المتعلقة بالجرائم المعلوماتية في محاولة لإيجاد تصور شامل لهذه الجرائم قصد محاربتها.
 - 2- ضرورة الانضمام إلى المعاهدات والاتفاقيات الدولية التي تعمل على التنسيق والتعاون من أجل مكافحة الجرائم المعلوماتية.
 - 3- اعتماد الدول للاختصاص القضائي العالمي، في سبيل مكافحة الجريمة المعلوماتية واعتبارها من الجرائم الدولية.
 - 4- تضافر الجهود الدولية الرامية لمكافحة الجريمة المعلوماتية، بغرض التوصل إلى معاهدة دولية تحت رعاية الأمم المتحدة، بغية توحيد الجهود الدولية في مجالات التجريم والولاية القضائية وتعزيز التعاون الدولي.