مجلة البحوث في العقود وقانون الأعمال
Research in Contracts and Business Law Review
مجلة علمية دولية محكمة متخصصة في مجال العقود وقانون الأعمال
Approved Scientific International Review Specializing in Contracts and Business Law
تصدرعن مخبرالعقود وقانون الأعمال، كلية الحقوق
Edited by the Contracts and Business Law Laboratory in college of law
جامعة الاخوة منتوري قسنطينة 1
University of brother's Mentouri Constantine1
ISSN: 2543-392X E-ISSN: 2716-8913

إشهاد بنشر مقال

المرجع/ 117-2025

تشهد الاستاذة الدكتورة قسوري فهيمة رئيسة تحرير مجلة البحوث في العقود وقانون الأعمال الصادرة عن مخبر العقود وقانون الاعمال كلية الحقوق جامعة الاخوة منتوري قسنطينة1 (الجزائر) أن :

الأستاذ(ة) : مقري صونيا جامعة محمد بوضياف المسيلة (الجزائر)

والأستاذ(ة) : بن لعامر وليد جامعة محمد بوضياف المسيلة (الجزائر)

قد نشر(ت) مقال موسوم : **" المنظومة الوطنية لأمن الأنظمة المعلوماتية كآلية مؤسساتية لمكافحة الجريمة المعلوماتية وفقا للمرسوم الرئاسي رقم 20-05 ."**

ضمن العدد التسلسلي 26 / مجلد 10 عدد02 / ديسمبر 2025 من مجلة البحوث في العقود و قانون الأعمال.

https://www.asjp.cerist.dz/en/PresentationRevue/610

سلم هذا الإشهاد بناء على طلب المعني(ة) لاستعماله في حدود ما يسمح به القانون.

قسنطينة(الجزائر) في :18 ديسمبر 2025

رئيسة التحرير

مجلة البحوث في العقود وقانون الأعمال

Research in Contracts and BusinessLaw Review

مجلة علمية دولية محكمة متخصصة في مجالي العقود و قانون الأعمال

Approved Scientific International Review
Specializing in Contracts and Business Law

تصدر عن مخبر العقود وقانون الأعمال

Edited by the Contracts and Business Law Laboratory

جامعة الإخوة منتوري قسنطينة1 الجزائر

العدد 02 المجلد 10 العدد التسلسلي 26

ديسمبر 2025

Brother Mentouri University
Constantine 1 (Algeria)
Volume:10/ N°: 02 / Issue number:26
December 2025

ISSN 392-2543X

الإيداع القانوني ديسمبر 2018

هيئة إدارة المجلة/
مدير المجلة : أ.د/ بن حملة سامي جامعة قسنطينة1

رئيس التحرير: أ.د/ قسوري فهيمة جامعة باتنة1

سكرتير المجلة : د/ عبد الدايم هاجر جامعة قسنطينة 2

تقديم العدد التسلسلي الرابع والعشرين (المجلد 10 ، العدد02 التسلسلي 26)

بسم الله الرحمن الرحيم

والصلاة والسلام على سيدنا محمد خاتم الأنبياء والمرسلين

نتشرف أن نقدم لكم هذا العدد الجديد من مجلة البحوث في العقود وقانون الأعمال، والذي يتضمن مجموعة من المقالات والدراسات العلمية المتخصصة، والتي تعد مكسبا تضيفه جامعتنا لدولتنا، يواكب المستجدات التشريعية ويعالج قضايا ومسائل في مختلف الفروع القانونية.

ويتضمن هذا العدد أساتذة أكفاء وباحثين من جامعات وطنية من كليات الحقوق، حرصوا على تقديم مادة علمية موثوقة للطلبة والأساتذة القانونيين، إذ أنه لا يمكن الرقي بالبحث العلمي في الجامعة الجزائرية دون أن تتضافر الجهود للباحثين الأوفياء لأخلاقيات البحث العلمي.

وإننا نأمل أن يكون هذا العمل إضافة نوعية للمكتبة القانونية الجزائرية، ومكسبا علميا للطلبة والأساتذة، كما نتطلع أن يساهم هذا العدد في مواكبة المستجدات والتطورات التي يشهدها المجال القانوني.

عراب مريم
كلية الحقوق
جامعة وهران 2 محمد بن أحمد -الجزائر

فهرس المحتويات

التقديم للعدد التسلسلي 25(المجلد 10 عدد 01)			
	اسم ولقب المؤلفين	عنوان المقال	الجامعة	الفهرس
01	احمد طلعت علي حامد	إصابات العمل والأمراض المهنية في إطار التشريع العمالي الفلسطيني	جامعة تيسمسيلت (الجزائر)	24-06
02	بن شرطيوة سناء	إستراتيجية المدن الذكية بين آليات التنفيذ و التفعيل	جامعة الاخوة منتوري قسنطينة 1 (الجزائر)	39-25
03	مكيديش أحلام غانية	الأسس القانونية والقضائية لعدم الادارية المتعلقة المشروعية في القرارات برخص ومخططات التعمير	جامعة طاهري محمد بشار(الجزائر)	60-40
04	جحنيط خديجة	الإيجاب الالكتروني في التشريع الجزائري : دراسة تحليلية للمفهوم و الأحكام القانونية	جامعة محمد البشير الإبراهيمي –برج بوعريريج (الجزائر)	75-61
05	ياسمين يحي إبراهيم شعار فريال كريكو	الاخطار بالشبهة كآلية للتعاون الدولي في اطار الوقاية من جريمة غسيل الاموال في ظل القانونين الفلسطيني والجزائري	جامعة الاخوة منتوري قسنطينة 1 (الجزائر) جامعة الاخوة منتوري قسنطينة 1 (الجزائر)	93-76
06	لمياء حدرباش	الاطار القانوني لانشاء شبابيك الصيرفة الاسلامية في الجزائر	جامعة محمد لمين دباغين سطيف 2(الجزائر)	94- 114
07	ساكري زبيدة	التجميعات الاقتصادية: المفهوم و المميزات	جامعة باتنة 1 الحاج لخضر (الجزائر)	128-115
08	مقري صونيا بن لعامر وليد	المنظومة الوطنية لأمن الأنظمة المعلوماتية كآلية مؤسساتية لمكافحة الجريمة المعلوماتية وفقا للمرسوم الرئاسي رقم 20-05	جامعة محمد بوضياف المسيلة (الجزائر) جامعة محمد بوضياف المسيلة (الجزائر	150-129

مجلة البحوث في العقود وقانون الأعمال

09	بن حبيلس آمنة	خصوصية أحكام انتقال حيازة العقار الى الخلف بين ثبوت حق الملكية وحماية الحيازة	جامعة الاخوة منتوري قسنطينة 1 (الجزائر)	170-151
10	أماني بلعلمي	دراسة التأثير الوسيلة القانونية للجماعات المحلية لحماية البيئة	جامعة جيجل (الجزائر)	188-171
11	عائشة كاملي	دراسة تحليليّة للمادّة الثّانية (2) من القانون 22 – 23 المتضمّن القانون الأساسي للمقاول الذّاتي	جامعة العربي بن مهيدي- أم البواقي (الجزائر)	207-189
12	حداد ياسر قرماط أحمد الأمين	دور التحول الرقمي في حماية النظام التنافسي للمؤسسات	جامعة الإخوة منتوري قسنطينة 1 (الجزائر) جامعة الإخوة منتوري قسنطينة 1 (الجزائر)	223-208
13	رحوي فاطمة الزهراء	عقود السياحة الإلكترونية كآلية لتعزيز السياحة المستدامة في الجزائر	المدرسة العليا الإدارة الإعمال تلمسان (الجزائر)	245-224
14	بن حمود لطيفة	مستجدات التسوية الادارية للعقارات غير المطالب بها- وفقا للمادة 166 من قانون المالية لسنة 2025-	جامعة الإخوة منتوري قسنطينة 1 (الجزائر)	264 -246
15	يونس أكرم بولسينة هشام	مشروعية اللجوء إلى التحكيم التجاري الدولي في العقود الإدارية	جامعة باجي مختار عنابة (الجزائر) جامعة باجي مختار عنابة (الجزائر)	278-265
16	غضبان نور اليقين بن لشهب أسماء	نشاط المرقي العقاري مهنة مقننة بصدور القانون 04/11	جامعة الإخوة منتوري قسنطينة1 (الجزائر) جامعة الإخوة منتوري قسنطينة 1(الجزائر)	290-279

مجلة البحوث في العقود وقانون الأعمال

17	إيمان رتيبة شويطر	الحجز التحفظي كوسيلة من وسائل حماية الحق	جامعة الإخوة منتوري قسنطينة1 (الجزائر)	291-307
18	بوحملة صلاح الدين	السكوت الملابس و أثره في إبرام عقود التجارة الإلكترونية: دراسة في التباين الفقهي حول حجيته كقبول	المدرسة العليا للتسيير و الاقتصاد الرقمي - القليعة- (الجزائر)	308-320
19	بن زردة محمد علي خوادجية سميحة حنان	دور الموثق في تحقيق الامن القانوني و حماية الأطراف المتعاقدة	جامعة الاخوة منتوري قسنطينة1 جامعة الاخوة منتوري قسنطينة1	321-332
20	**Dich Touria**	**Harmonizing Contract Theory with Blockchain-Enabled Smart Contracts**	Algiers University 1 (Algeria)	333-364
21	**Hadji Ibtissem**	**Investment incentives and economic advancement in light of the developments of law No. 22-18**	University of Constantine 1 Mentouri Brothers (Algeria)	365-388
22	**Zakaria Tertag**	**Le droit à l'information en matière de l'environnement The right to information in environmental matters**	University of Constantine 1 Mentouri Brothers (Algeria)	389-406
23	**MANSOURI TOURIA**	**Settlement of Medical Disputes in the Field of Social Security under lgerian Legislation. (A comparative Study Between the Former Law No. 83/15 and the New Law No. 08/08)**	Djilali Al-Yabis University - Sidi Bel Abbes (Algeria),	407-422
24	**SOUILEM Said**	**The role of terms and conditions in agricultural investment contracts in achieving food security**	University of Ghardaïa (Algeria),	423-447

472-448	University of Cheikh larbi tebessi (Algeria)	**Unfair Terms in Standard Contracts: A Comparative Legal Analysis of Algerian, French, and Arab legislations**	**Hillel Chaoua**	25

مجلة البحوث في العقود وقانون الأعمال
The Journal of Research in Contracts and Business Law
المجلد 10/ العـدد: 02 (2025)، ص 129–150

المنظومة الوطنية لأمن الأنظمة المعلوماتية كآلية مؤسساتية لمكافحة الجريمة المعلوماتية وفقا للمرسوم الرئاسي رقم 20–05

the National System for Information Systems Security as an Institutional Mechanism to Combat Cybercrime According to Presidential Decree No. 20-05

مقري صونيا*[1] ، بن لعامر وليد[2]

[1] جامعة محمد بوضياف المسيلة (الجزائر)، sonia.makri@univ-msila.dz مخبر الدراسات والبحوث في القانون الاقتصادي والأسرة والتنمية الإدارية

[2] جامعة محمد بوضياف المسيلة (الجزائر)، walid.benlameur@univ-msila.dz مخبر الحوكمة والقانون

تاريخ الاستلام: 2025/06/28 تاريخ القبول: 2025/11/22 تاريخ النشر: 2025/12/18

ملخص:

في ظل التغيرات التي شهدها العالم في الآونة الأخيرة من استعمال مطرد لتكنولوجيا الاعلام والاتصال وتحولات رقمية متسارعة، ظهر نوع جديد من الجرائم التي أصبحت تشكل خطراً على أمن الأفراد والمؤسسات وحتى على السيادة الوطنية إنها الجريمة المعلوماتية. وبغية مكافحة هذه الأخيرة عملت الجزائر على إيجاد اطار مؤسساتي وتشريعي فعال للتصدي لهذا النوع من الجرائم، و هذا ما تم فعلا من خلال صدور المرسوم الرئاسي رقم 20–05 الصادر في 20 جانفي 2020، الذي أنشأ المنظومة الوطنية لأمن الأنظمة المعلوماتية ، وبالتالي فإن الهدف من هذه الدراسة هو الوقوف على مدى فعالية هذه المنظومة وتعزيز قدرة الدولة من أجل الوقاية من الجريمة المعلوماتية.

وبذلك تعد المنظومة الوطنية خطوة فعالة نحو فضاء رقمي آمن، لكنها مازالت تفتقر إلى قوانين شاملة للأمن المعلوماتي تكمل أحكام المرسوم الرئاسي 20–05 تتضمن الأحكام التجريمية والعقابية و التدابير الإدارية والفنية، كما أن غياب استرتيجية مفصلة للأمن المعلوماتي أدى إلى ضعف فعاليتها وهذا ما يجعل تدخلاتها محدودة الأثر في بعض القطاعات.

الكلمات المفتاحية: الأمن المعلوماتي – الجريمة المعلوماتية – المجلس الوطني لأمن الأنظمة المعلوماتية – المرسوم الرئاسي رقم 20–05 – المنظومة الوطنية.

ABSTRACT:

In light of recent global developments marked by the increasing use of information and communication technologies and rapid digital transformations, a new type of crime has emerged—cybercrime—which poses a serious threat to the security of individuals, institutions, and even national sovereignty. In response, Algeria has sought to establish an effective institutional and legislative framework to combat this form of crime. This effort materialized with the

* المؤلف المرسل.

issuance of Presidential Decree No. 20-05, dated January 20, 2020, which established the National System for the Security of Information Systems.

The aim of this study is to assess the effectiveness of this system and explore how it strengthens the state's capacity to prevent cybercrime. The National System thus represents a significant step toward a secure digital environment. However, it still lacks a comprehensive legal framework for information security that would complement the provisions of Decree No. 20-05particularly in terms of criminalization, penalties, and administrative and technical measures. Furthermore, the absence of a detailed information security strategy has weakened its overall effectiveness, limiting its impact in certain sectors.

Keywords: Information Security – Cybercrime – National Council for the Security of Information Systems – Presidential Decree No. 20-05 – National System.

مقدمة:

بعد التطور التكنولوجي الهائل الذي عرفه العالم في العقود الأخيرة من الزمن، صاحبه ظهور ما يسمى بالمجتمع الرقمي، أين أضحت تكنولوجيا المعلومات والاتصالات ضرورة لا غنى عنها في شتى الميادين الاقتصادية، الاجتماعية، السياسية.....الخ.

هذا الاستخدام المفرط للوسائط الرقمية صاحبه تنام مرعب لظاهرة باتت عالمية إنها "الجريمة المعلوماتية" التي أصبحت تشكل خطرا لا يستهان به خاصة في ظل صعوبة اثبات وتتبع مجرميها أو مرتكبيها بالوسائل التقليدية.

وفي هذا الإطار، وعلى غرار باقي الدول الأخرى، شهدت الجزائر ارتفاعا في عدد الجرائم المعلوماتية (السيبرانية) التي استهدفت الأفراد والمؤسسات على حد السواء وحتى البنى التحتية للدولة. وهذا ما دفع الجزائر إلى اتخاذ جملة من الإجراءات القانونية والمؤسساتية الهادفة إلى تعزيز أمن الأنظمة المعلوماتية، وهذا ما تم فعلا حيث أنشأت منظومة وطنية تهدف إلى مكافحة الجريمة المعلوماتية بكل أشكالها، وتأمين فضائها السيبراني بموجب المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية كآلية مؤسساتية تنظيمية حديثة هدفها حماية النظام المعلوماتي من التهديدات السيبرانية.

وعليه، فإن الهدف من هذه الدراسة هو الوقوف على مدى فعالية هذه المنظومة في مواجهة الجريمة المعلوماتية، وكذا دراسة وتحليل الإطار القانوني والتنظيمي لهذه المنظومة، خاصة في ظل البيئة الرقمية وما تفرضه من تحديات وصعوبات.

ومن هذا المنطلق يمكننا طرح الإشكالية التالية: **إلى أي مدى شكل المرسوم الرئاسي رقم 20-05 بشأن المنظومة الوطنية لأمن الأنظمة المعلوماتية آلية فعالة في مكافحة الجريمة المعلوماتية في الجزائر؟**

وللوقوف على هذا الموضوع تطرح العديد من التساؤلات الفرعية على قدر كبير من الأهمية تتعلق أساسا بتحديد تعريف للجريمة المعلوماتية وخصائصها وأركانها، وكذا تعريف أمن النظام المعلوماتي ومعاييره، بالاضافة إلى دراسة المنظومة الوطنية لأمن الأنظمة المعلوماتية وفقا للمرسوم التنفيدي رقم 20-05 ومكوناتها. ومن أجل الإحاطة بكل الجوانب القانونية للموضوع، فقد اعتمدت في هذه الدراسة على المنهج الوصفي وذلك من خلال تقديم وصف كامل للجريمة المعلوماتية وتبيان خصائصا وأركانها، والمنهج التحليلي من خلال تحليل النصوص القانونية المتعلقة بالجريمة المعلوماتية وكذا المنظومة الوطنية لأمن الأنظمة المعلوماتية. للإجابة على كل التساؤلات المطروحة قسمنا موضوع الدراسة إلى محورين:

المحور الأول: الإطار المفاهيمي والنظري للجريمة المعلوماتية وأمن الأنظمة المعلوماتية

المحور الثاني: دور المنظومة الوطنية لأمن الأنظمة المعلوماتية في مكافحة الجريمة المعلوماتية

المحور الأول: الإطار المفاهيمي والنظري للجريمة المعلوماتية وأمن الأنظمة المعلوماتية

بعد ما شهده العالم من ثورة رقمية هائلة في العقود الأخيرة والتي مست مختلف المجالات، هذا ما صاحبه سعي الدول وفي نفس الوقت إلى حماية أنظمتها المعلوماتية من الهجمات والتهديدات السيبرانية أو ما يعرف بالجريمة المعلوماتية التي نمت وتطورت بشكل سريع، وهذا ما يتطلب الوقوف على مفهوم هذه الجريمة الحديثة ، وكذلك التعريف بأمن النظام المعلوماتي.

أولا: مفهوم الجريمة المعلوماتية

عند محاولة الكشف عن مفهوم مصطلح معين، فإنه يتم التطرق إلى ابراز كل ما من شأنه إزالة الغموض والإبهام عنه، وجعله في متناول كل من يهتم بالإلمام به، وبذلك سنقوم بتعريف الجريمة المعلوماتية من الناحية الفقهية، بالتطرق إلى مختلف الآراء الفقهية حول المقصود بهذه الجريمة، ثم إلى التعريف التشريعي لها، وللخوض فيها أكثر وأكثر يستلزم دراسة خصائصها وأركانها.

1- تعريف الجريمة المعلوماتية:

من خلال هذا العنصر سنحدد المفاهيم الخاصة بموضوع الجريمة المعلوماتية من خلال التطرق إلى التعريف اللغوي والإصطلاحي.

1-1- التعريف اللغوي للجريمة المعلوماتية:

تعني (**الجريمة**) لغة الذنب، ونقول جرّم وأجرم واجترام بمعنى ادعى عليه بذنب لم يقترفه. أما المعلوماتية (**الإلكترونية**) فهي ترجمة للمصطلح الفرنسي information بمعنى المعالجة الآلية للمعطيات، ويعود هذا المصطلح إلى فليب داريفوس والذي قصد به العلم الذي يربط المعلومات والحاسوب والاتصالات [1]. وذهب البعض إلى القول أنه ليس من السهل وصف المعلومة بدقة فقط يمكن إدراك أثرها، والمعلومة عبارة عن مجموعة من المفاهيم والحقائق التي لا يجوز تأويلها أو تفسيرها لا عن طريق الأفراد أو عن طريق الأنظمة الإلكترونية [2].

2-2- التعريف الإصطلاحي للجريمة المعلوماتية:

تباينت آراء الفقهاء حول تعريف محدد للجريمة المعلوماتية لإختلافهم للزاوية التي ينظر إليها، كما تعرضت مختلف التشريعات المقارنة لهذه الجريمة واختلفت في تسمياتها.

أ-التعريف الفقهي للجريمة المعلوماتية:

لم يتفق الفقه الجنائي على تسمية واحدة للجريمة المعلوماتية، فهناك من يطلق عليها تسمية الجريمة الإلكترونية، والبعض الآخر جرائم الكمبيوتر والإنترنت، في حين يطلق آخرون تسمية الجرائم المستحدثة، حتى أن هناك من يطلق عليها الجرائم الإلكترومعلوماتية [3]. هذا التعدد في تسميات الجريمة المعلوماتية، صاحبه تعدد في التعريفات الخاصة بها، فهناك من عرفها على أنها الإستخدام السيئ لأجهزة الحاسوب بشكل غير قانوني مؤداه ارتكاب جريمة معاقب عليها بقوانين تتعلق بجرائم الشبكات وتكنولوجيا المعلومات، تتصف بإدخال بيانات مزورة في نظام جهاز الحاسوب واساءة استخدام مخرجاته، كما أن تجهيزات وبرمجيات الحاسوب تكون محل اعتداء كالتخريب والتعديل في بياناته [4]. وهناك من عرفها على أنها كل اعتداء ضار بالآخرين عبر الوسائط الإلكترونية كشبكات الإتصال الهاتفية، الكمبيوتر، شبكة الإنترنت، أو الإستخدام غير المشروع للبيانات الإلكترونية [5].

حتى أن الفقه المعاصر أصبح يطلق على هذه الجرائم وصفاً جديداً وهو جرائم أصحاب الياقات (white collor crimme) ، وهي جرائم ترتكب من طبقة اجتماعية عالية في المجتمع من أجل الحصول على منفعة شخصية بطرق غير مشروعة، ونظرا للامكانيات المتوفرة لديها يصعب اكتشافها من قبل السلطات المختصة [6].

ب- التعريف القانوني للجريمة المعلوماتية:

مع الإنتشار الواسع للجريمة المعلوماتية وتخطيها للحدود الوطنية للدول، أصبح لزاما التصدي لهذه الظاهرة التي أصبحت تهدد الأمن المعلوماتي والوطني في نفس الوقت، الأمر الذي أدى إلى ادخال مثل هذه الجرائم في نطاق الأفعال المجرمة وتخصيص عقوبات تحد من تفاقمها وتوسعها. وبالتالي تعديل العديد من الدول لتشريعاتها سواء وطنية أو دولية [7]، وهو ما قام به المشرع الجزائري من خلال تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، حيث أضاف القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات في المواد من 394 مكرر إلى 399 مكرر 7 [8].

كما أصدر المشرع الجزائري القانون رقم 09-04 المؤرخ في 5 غشت 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي اصطلح تسميتها بالجرائم المتصلة بتكنولوجيا لإعلام والاتصال وعرفها من خلال المادة 02/ أ على أنها جرائم تمس بأنظمة المعالجة الآلية للمعطيات الوارد ذكرها في قانون العقوبات، كما يدخل في مفهوم هذه الجريمة الجرائم المرتكبة باستخدام نظام الاتصالات الإلكترونية أو باستخدام منظومة معلوماتية [9].

يتضح من خلال التعريف السابق للجريمة المعلوماتية أن المشرع الجزائري قد وسع من دائرة التجريم لتشمل جرائم معلوماتية أخرى يمكن اكتشافها في المستقبل [10]. ذلك أنه تبنى معيار دور النظام المعلوماتي لتحديد معالم الجريمة، حتى أن المشرع عند تعريفه للمنظومة المعلوماتية في المادة 02/ ب قد اشترط ضرورة الترابط بين مكونات النظام أو بين الأنظمة فيما بينها [11].

أما باقي التشريعات العربية فنجد أن البعض منها قد أعطى تعريفاً للجريمة المعلوماتية من خلال القوانين المتعلقة بمكافحة جرائم تقنية المعلومات، كما فعل كل من المشرع الكويتي والسعودي، فالمشرع الكويتي ركز في تعريفه على الوسائل المستعملة في ارتكاب الجريمة سواء من جهاز الحاسوب أو شبكة الإنترنت وغيرها من الوسائل في نص المادة الأولى من القانون رقم 63 لسنة 2015 المتعلق بمكافحة جرائم تقنية المعلومات [12]. وهو نفس التعريف الذي جاء به نظام مكافحة الجرائم المعلوماتية السعودي رقم م/ 17 لسنة 2006 من خلال المادة الأولى [13].

2- خصائص الجريمة المعلوماتية:

تتميز الجريمة المعلوماتية بخصائص غير عادية تجعلها تختلف بشئ كبير عن الجرائم التقليدية، هذا ما أدى بنا إلى دراسة اهم خصائصها في النقاط التالية:

2-1- الجريمة المعلوماتية عابرة للدول والقارات: تتسم الجريمة المعلوماتية بطابع دولي، وهذا بفضل الشبكة العنكبوتية التي جعلت العالم في حالة اتصال دائم، فمن خلال ما يسمى بالنظام المعلوماتي ترتكب العديد من الجرائم كالإحتيال المعلوماتي وسرقة الأموال والقرصنة [14]. وتمتد هذه الجرائم إلى خارج حدود مرتكبيها أي إلى دولة أخرى، وهذا من شأنه أن يثير عدة اشكالات قانونية كالاختصاص والإجراءات والتحري وما إلى ذلك من النقاط التي يمكن أن تثيرها الجرائم العابرة للحدود [15].

2-2- الجريمة المعلوماتية صعبة الإثبات: تتسم الجريمة المعلوماتية بالخفاء ذلك أنها تستهدف المعنويات لا الماديات، فالجاني لا يترك أثراً مادياً يمكن أن نتابعه من خلاله عكس الجرائم التقليدية، ضف إلى ذلك أن اجراءات التحقيق تحتاج إلى معرفة كبيرة بتقنية المعلومات، ففي الأمر الغالب يتم اكتشاف الجريمة صدفة، ذلك أن الجاني لا يترك أثراً مادياً لأنها جرائم لا عنف فيها تتم بتغيير أو محي أرقام وبيانات من سجلات مخزنة في ذاكرة الكمبيوتر [16]. كما أن الجرائم التي تم الكشف عنها هي أقل بكثير من الجرائم التي لم يكشف عنها وهذا راجع لعدة أسباب نذكر منها:

- اعتمادها على الذكاء في ارتكابها.
- أنها تتطلب خبرة فنية من الصعب على المحقق التعامل معها.
- صعبة الاحتفاظ الفني بآثارها إن وجدت [17].

2-3-الجريمة المعلوماتية سهلة الوقوع: لا تحتاج الجريمة المعلوماتية لأي مجهود عضلي لارتكابها بل تتطلب تفكيرا عمليا مدروسا قائما على المعرفة التقنية بالحاسب الآلي، وهذا عكس الجرائم التقليدية التي تحتاج إلى مجهود عضلي للقيام بها [18].

2-4- الجريمة المعلوماتية تقع أثناء المعالجة الآلية للبيانات: وهو الشرط الجوهري الذي ينبغي توافره لتحقق الجريمة المعلوماتية، فإذا تخلف انتفت الجريمة، وتقع هذه الأخيرة في مرحلة من مراحل تشغيل نظام المعالجة الآلية للبيانات، أي عند مرحلة ادخال البيانات أو أثناء معالجتها أو اخراجها [19]. ولقد حاول مجلس الشيوخ في فرانسا وضع تعريف محدد للمعالجة الآلية للمعطيات، إلا أنه عدل عن ذلك بإعتبار أنها تخضع للتطور السريع، لذلك فإن أي تعريف لها سيكون غير كاف [20].

2-5-الجريمة المعلوماتية قليلة المخاطرة: بالنظر لعدم وجود مواجهة مباشرة مع المجني عليه ومع الشرطة، كما يحدث في العادة في الجرائم التقليدية، فإن الجريمة المعلوماتية قليلة المخاطرة [21].

2-6-امتناع المجني عليه عن التبليغ في الجريمة المعلوماتية: تتميز الجريمة المعلوماتية بعدم الإبلاغ عنها من طرف الضحية أو المجني عليه. وهذا راجع إلى أن هذه الجرائم تمس خصوصية الأفراد، كما تمس الأشخاص المعنوية كالشركات حيث أنها تتخوف من أن تؤدي أعمال التحقيق التي تقوم بها إلى احتجار حواسيبها وهذا ما يؤدي إلى خسائر مادية جراء ذلك التحقيق [22].

2-7-خصوصية مجرم المعلومات في الجريمة المعلوماتية: يتميز المجرم المعلوماتي بقدر كبير من الذكاء المعلوماتي والعلم التكنولوجي، خاصة إذا تعلقت الجريمة بسرقة معلومات مشفرة [23]. وتم تصنيف مجرمي المعلومات إلى ثلاثة أصناف، الصنف الأول المخترقين (الهاكرز) وهو الشخص البارع في استخدام جهاز الحاسوب، بإمكانه استخدام حسابات الآخرين بطرق غير قانونية. أما الصنف الثاني المحترفون وهو الأكثر خطورة يسعى البعض منهم إلى الدخول إلى حسابات البنوك والبعض الآخر لتحقيق أغراض سياسية، وبالنسبة للصنف الثالث وهم الحاقدين ليس لديهم أي هدف لارتكاب الجريمة وإنما للانتقام [24].

3- أركان الجريمة المعلوماتية:

تتطلب الجريمة المعلوماتية لقيامها تحقق أركانها، وبما أنها جريمة ترتكب عبر الفضاء الرقمي، مما يجعلها تنفرد بخصوصيات، إلا أن ذلك لا يعني عدم وجود تشابه بينها وبين الجريمة المرتكبة في العالم المادي، فتشترك بوجود الفعل غير المشروع، فمن خلال هذا التشابه سنتطرق إلى الأركان التي تقوم عليها هذه الجريمة:

3-1-الركن الشرعي للجريمة المعلوماتية: استنادا إلى مبدأ الشرعية الوارد ذكره في نص المادة الأولى من القانون رقم 04-15 من قانون العقوبات السالف ذكره، لا يمكن تجريم أي فعل بدون وجود نص قانوني وعقاب مترتب على اتيان فعل غير مشروع. وفي هذا الإطار خصص المشرع الجزائري القسم السابع مكرر تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات" في المواد من 394 إلى 394 مكرر 8 أين عالج كل أنواع الاعتداءات على الأنظمة المعلوماتية [25].

كما جاء القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ليحد من وقوع الجرائم المعلوماتية وذلك بفرض ترتيبات تقنية لمراقبة الاتصالات الإلكترونية والقيام بكل اجراءات التفتيش داخل المنظومة المعلوماتية [26].

وعلى الصعيد الدولي فقد أبرمت العديد من الاتفاقيات الدولية، أشهرها اتفاقية بودابست الصادرة عن المجلس الأوربي عام 2001، التي وضعت اطار عام لحماية المعلومات، وبفضلها أصدرت العديد من التشريعات الداخلية بما يتوافق وأحكام الاتفاقية وضرورة التعاون الدولي في سبيل مكافحة الجريمة المعلوماتية [27].

3-2 -الركن المادي للجريمة المعلوماتية: يتطلب السلوك المادي في الجريمة المعلوماتية وجود بيئة رقمية واتصال بشبكة الإنترنت، كما يتطلب ايضا نتيجة وعلاقة سببية [28]. بالنسبة للسلوك الإجرامي هو ذلك الفعل الذي جرمه القانون (سلوك ايجابي) كتعمد اختراق شبكة معلومات غير مصرح بالولوج إليها، أو الإمتناع عن فعل يأمر به القانون (سلوك سلبي) كإغفال مهندس معلومات بالمؤسسة لتطوير وتحديث نظم حماية البيانات مما تسبب في اختراقها وسرقة معلوماتها.

أما النتيجة فهي الضرر الناتج عن السلوك الإجرامي، سواء كان الضرر مادياً أو معنوياً [29]. والجامع بين السلوك الإجرامي والنتيجة هي العلاقة السببية وهي اساس الركن المادي للجريمة وبها تقوم المسؤولية الجنائية.

3-3-الركن المعنوي للجريمة المعلوماتية: يعد الركن المعنوي من أهم أركان الجريمة المعلوماتية فلا يمكن تصور وجودها دون توافره إلى جانب الركن المادي [30]، ويعرفه البعض على أنه الحالة النفسية للجاني التي تربط بين ماديات الجريمة وشخصية الجاني، حيث يسميه البعض الركن الشخصي [31].

كما يمكن تعريفه بأنه العلم بمكونات الجريمة وإرادة ارتكابها، لذلك فإن هذا الركن يتضمن عنصرين أساسيين هما العلم والإرادة، فالعلم هو إدراك الأمور على نحو مطابق للواقع، أما الإرادة فهي الإتجاه نحو تحقيق السلوك الإجرامي، وبذلك وفي إطار هذا الركن تتوافر كافة مقومات المسؤولية الجنائية (من علم وإدراة آثمة) مع تقرير العقاب الذي يبنى على هذه المقومات[32].

ومن أجل تحديد التكييف القانوني المناسب للجريمة نميز بين ما إذا كان القصد عمدياً أو غير عمدي، فبالنسبة للقصد العمدي نكون أمام جريمة عمدية بعنصريها (العلم والإرادة الآثمة)، كتعمد الإختراق غير المشروع لمنصة ما، وأوضح قضية على ذلك تصميم عصابة مكونة من ثلاث أشخاص في مصر لموقع يشبه موقع بعض المصارف، حيث قاموا بإرسال رسائل عشوائية إلى عملاء حقيقيين بواسطة البريد الإلكتروني، ليدخلوا بياناتهم المصرفية على الموقع المزيف، ثم بعد ذلك تم التعرف على بياناتهم السرية ليتم الاستيلاء على أموالهم.

أما بالنسبة للقصد غير العمدي (جريمة غير عمدية)، فقد تكيف الواقعة بأنها خطأ غير مقصود من المستخدم بسبب عيب في أنظمة الحماية الخاصة بالشبكة، ومن هنا تنتفي المسؤولية الجنائية للشخص. لذلك نجد أن القضاء الأمريكي قد اتجه إلى ضرورة توافر العلم والإرادة الصريحة لتحقق القصد الجنائي في جرائم الإنترنت، ويعتبر العلم بمثابة القصد الجنائي الخاص الذي يطبق عليه الظرف المشدد للعقوبة، في حين اكتفى القضاء الفرنسي في جرائم الإنترنت بإثبات سوء النية [33].

أما الشروع في الجرائم المعلوماتية فهناك من التشريعات من عاقب عليها بنفس عقوبة الجريمة التامة رغبة من المشرع من حماية مصالح المعتدى عليها، كالتشريع الفرنسي في المادة 19 من قانون العقوبات لسنة 1988 [34]. في حين عاقب

المشرع الفلسطيني على الشروع في الجرائم المعلوماتية نصف عقوبة الجريمة التامة (المادة 49 من قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية) [35].

وبالنظر للانتشار المتزايد للجرائم المعلوماتية والتهديدات المستمرة في استعمال تكنولوجيا الاتصال، هذا ما دفع العديد من الدول إلى الإهتمام بأمن المعلومات بهدف حماية الأنظمة المعلوماتية للاشخاص والحكومات من حيث المفهوم والمعايير في العنصر الموالي من هذه الدراسة.

ثانيا: مفهوم أمن الأنظمة المعلوماتية

أولت العديد من دول العالم اهتماماً بمجال الأمن المعلوماتي ومنها الجزائر التي تعرضت للعديد من الهجمات الإلكترونية، التي مست بشكل مباشر حياة كل من المتعاملين مع الوسائط الإلكترونية بما في ذلك مؤسسات الأعمال التي انعكست على مصالحهم [36]، بل أن الأمر تعدى إلى المستوى الفردي، حيث أصبح كل شخص يمتلك جهازه الخاص به لأداء أعماله وتصفح شبكة الإنترنت [37]، وبالتالي فإن أمن نظم المعلومات ليس حلاً اختيارياً وانما ضرورة ملحة، لذلك وجب التعريف به وبيان معاييره.

1- تعريف أمن نظم المعلومات:

نتعرض من خلال هذا العنصر للتعريف الفقهي والقانوني لأمن نظم المعلومات:

1-1- التعريف الفقهي لأمن نظم المعلومات: حسب وكالة الأمن القومي الأمريكي يعرف أمن نظم المعلومات بأنه حماية نظام المعلومات من أي تعديل غير مرخص لهذه المعلومات أثناء معالجتها أو حفظها أو نقلها، أو من أي وصول غير مرخص إلى المعلومات، بما في ذلك كل الإجراءات الضرورية لمواجهة وكشف المخاطر والإعتداءات [38]. أما من الناحية التقنية فيعرف على أنه التدابير الوقائية والإجراءات المستخدمة لصيانة المعلومات كالأجهزة والبيانات والبرمجيات، كما يشير أمن المعلومات إلى دخول أطراف غير مخول لها باستخدام النظام إلى موارد المنشأة [39].

2-1- التعريف القانوني لأمن نظم المعلومات: عرف قانون الأونسترال النموذجي بشأن التجارة الإلكترونية نظم المعلومات في نص المادة 6/02 بأنه النظام الذي يستعمل لإنشاء رسائل البيانات أو ارسالها أو تخزينها أو تجهيزها على أي وجه آخر [40].

كما عرفت معاهدة بودابست الدولية لسنة 2001 نظم المعلومات بأنها كل معالجة آلية للمعطيات سواء بواسطة آلة بمفردها أو مع آلات مرتبطة بها تنفيذاً لبرنامج معين [41].

يتضح من تعريف اتفاقية بودابست أن محل الجريمة هو النظام المعلوماتي الذي يحتوي على مكونات مادية وأخرى منطقية ووسائل ادخال واخراج ومعالجة المعلومات، هذه المكونات قد تكون منفردة أو متصلة بأجهزة مماثلة عن طريق شبكة الإنترنت وبدون تدخل الإنسان [42].

أما المادة 01/ ب من القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والإتصال ومكافحتها السالف ذكره، فقد عرفت المنظومة المعلوماتية بأنها كل معالجة آلية للمعطيات سواء بواسطة مجموعة من الأنظمة المرتبطة ببعضها البعض، أو بواسطة نظام متصل لوحده تنفيذاً لبرنامج معين [43].

يتضح من التعاريف السابقة بأن نظام أمن المعلومات ما هو إلا تدابير واجراءات تتخذها المؤسسة لحماية أصولها الإلكترونية من كل استخدام غير مصرح به (السرقة، التزوير، الإستخدام غير المشروع أو القانوني، التخريب.....) وذلك باستعمال وسائل تقنية تضمن الحماية. لذلك فإن الهدف من نظام المعلومات هو منع انتشار المعلومات وتعديلها وتغييرها بطريقة غير قانونية، وكذا منع انتشارها غير الشرعي للموارد المعلوماتية للشبكات [44].

2- معايير أمن المعلومات:

من أجل تحقيق الحماية اللازمة للمعلومات، من الضروري توفير مجموعة من المعايير الأساسية للأمن المعلوماتي والمتمثلة في:

2-1-السرية أو الموثوقية: ويطلق عليها أيضا تسمية الخصوصية وتعني المحافظة على المعلومات من أن يقرأها ويفهمها غير الأشخاص المخول لهم فقط. فعند إرسال رسالة سرية فإنه يستوجب أن لا يراها إلا المرسل والمرسل إليه فقط. حتى وإن استطاع شخص آخر الإطلاع عليها فإنه يجب أن تكون غير مفهومة بالنسبة إليه [45]. ويمكن تحقيق ذلك باستعمال عدة معرقلات كبصمة الابهام، الصوت، اسم المستخدم، كلمة السر [46]، بالاضافة إلى تشفير البيانات الذي يساعد على حماية سرية المعلومات أثناء ارسالها أو تخزينها أو ارسالها بتحويلها إلى خوارزميات رياضية معقدة يصعب فكها [47].

2-2- السلامة: ونقصد بها أن مضمون المعلومات صحيح، لم يتم العبث به، أو لم يتم تعديله، وأن المعلومة هي المعلومة الأصلية دون نقصان أو زيادة، إضافة إلى دقة الأنظمة المعالجة لها من التلاعب أو التغيير غير الملاخص به، وهذا من شأنه أن يولد الثقة لدى المتعاملين مع المعلومات [48].

2-3- الوفرة: وتعني أن تكون المعلومة قابلة للوصول إليها في أي وقت يحتاجها المستخدم، لأن عدم توفر المعلومة عند الحاجة إليها يشكل خطراً بالنسبة لمستعملي النظام، لذلك لابد من اللجوء إلى الوسائل التي تمكن من المحافظة على إتاحة المعلومات وتخزين البيانات بشكل دوري [49].

المحور الثاني: دور المنظومة الوطنية لأمن الأنظمة المعلوماتية في مكافحة الجريمة المعلوماتية

وفقاً لما يتطلبه العصر التكنولوجي من ضرورة تحقيق أمن المعلومات والبيانات، حيث يسعى كل مستفيد من الخدمة الإلكترونية من أفراد وشركات إلى حمايتها من كل اعتداء خاصة في ظل تنامي الجرائم المعلوماتية بشتى أنواعها [50]. أصدر المشرع الجزائري في 20 من يناير 2020 مرسوماً رئاسياً تحت رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية لاسيما المادة الثالثة التي تضمنت تشكيلة المنظومة من مجلس وطني لأمن الأنظمة المعلوماتية والذي يدعى في صلب النص " المجلس"، ووكالة لأمن الأنظمة المعلوماتية تدعى في صلب النص " وكالة" [51]. لذلك نسعى من خلال هذا المحور إلى بيان مهام وتشكيلة كل من المجلس والوكالة.

أولا: المجلس الوطني لأمن الأنظمة المعلوماتية

استحدث المشرع الجزائري بموجب المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية السالف ذكره، مجلساً وطنياً لذلك سنتطرق إلى مهامه وتشكيلته وطرق سيره وفق مايلي:

1- تشكيلة المجلس الوطني لأمن الأنظمة المعلوماتية:

يعد المجلس الوطني لأمن الأنظمة المعلوماتية أحد مكونات المنظومة الوطنية يترأسه وزير الدفاع الوطني أو ممثله ويتكون من ممثل عن: رئاسة الجمهورية، الوزير الأول. وتشكيبة وزارية متنوعة تضم الشؤون الخارجية، الشؤون الداخلية، العدل، الطاقة، المالية، الاتصلات، التعليم العالي، ويستعين المجلس بأي مؤسسة أو شخص من شأنه أن يساعده في أعماله [52]. وحتى يقوم المجلس بآداء مهامه على أكمل وجه، فإنه يتوفر على أمانة تقنية يسيرها أمين عام توضع تحت تصرف سلطة رئيس المجلس تقوم بعدة مهام من بينها: العمل على إعداد مشروع النظام الداخلي للمجلس والتنسيق مع الوكالة، كما تقوم بجمع الوثائق والمعلومات لتحضير أشغال المجلس الوطني من أي ادارة أو مؤسسة أو هيئة [53].

وتعتبر هذه المهمة من أخطر المهام التي منحت للأمانة التقنية لأنه بموجبها ستتمكن من الاطلاع على معلومات تمس حرمة وخصوصية الحياة الخاصة للأفراد، لذا من المفروض أن ترفق هذه المهمة بآليات لحماية تلك الحرمة تضمن لها عدم انتهاكها باسم القانون [54].

2- مهام المجلس الوطني لأمن الأنظمة المعلوماتية:

يتولى المجلس الوطني عدة مهام تضمنها المرسوم التنفيذي رقم 20-05 في مادته 04 كالبت في الاستراتيجية التي تم اقتراحها من قبل الوكالة، كما يدرس المجلس مخطط عمل الوكالة ويقرر في نشاطاتها ويوافق عليها. كما يتولى الموافقة على اتفاقيات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في مجال الأنظمة المعلوماتية، لأن التعاون في هذا المجال ضرورة بالنظر إلى التطور المخيف في للإجرام الإلكتروني.

كذلك من مهام المجلس الموافقة على تصنيف الأنظمة المعلوماتية [55]، والتي تتعدد فعلى سبيل المثال نجد نظم المعلومات الإدارية وتتعلق بالأنظمة المسؤولة عن تقديم المعلومات الضرورية للإدارة حتى تتمكن من تحديد المشكل وحله، كما أن هناك أنظمة دعم القرار وهي التي تسمح بإتخاذ القرار المناسب لحل الاشكال المطروح وخلق فرص للتطوير والابتكار من أجل الحصول على أفضل النتائج [56]. كما يقترح المجلس مدى ملائمة الإطار الهيكلي أو التنظيمي الخاص بأمن الأنظمة المعلوماتية، ويبدي رأيه في أي مشروع نص تشريعي أو تنظيمي له علاقة بأمن الأنظمة المعلوماتية [57].

3- سير عمل المجلس الوطني لأمن الأنظمة المعلوماتية:

يتولى المجلس الوطني لأمن الأنظمة المعلوماتية المصادقة على نظامه الداخلي [58]، حيث يجتمع بناء على استدعاء من رئيسه كلما دعت الضرورة إلى ذلك [59]. كما يخول لرئيس المجلس إعداد جدول أعمال اجتماعات المجلس، مع ارسال

الاستدعاءات وجدول الأعمال إلى أعضاء المجلس قبل خمسة أيام على الأقل من تاريخ انعقاد الاجتماع، مع امكانية تبليغ جدول الأعمال خلال يوم انعقاد الجلسة في حالة الاستعجال.

ويتخذ المجلس قراراته بالأغلبية مع وآراء وتقارير ترجيح صوت الرئيس في حالة تساوي عدد الأصوات، تدون نتائج أشغال اجتماعات المجلس في محضر، حيث تتوج أعماله بقرارات وتوصيات وآراء وتقارير، وتسجل اعتمادات سير المجلس في ميزانية وزارة الدفاع الوطني [60].

ثانيا: وكالة أمن الأنظمة المعلوماتية:

بداية كان المشرع التونسي الأسبق في انشاء الوكالة الوطنية للسلامة المعلوماتية وذلك بموجب القانون الصادر في 2004 المتعلق بالسلامة المعلوماتية، حيث يهدف هذا القانون إلى تنظيم مجال السلامة العمومية وضبط القواعد العامة لحماية النظم المعلوماتية والشبكات، تعمل الوكالة تحت اشراف الوزارة المكلفة بتكنولوجيا الاتصال، أما التنظيم الإداري وطرق تسييرها فيكون بمقتضى أمر[61].

أما المشرع الجزائري فقد تبنى وكالة أمن الأنظمة المعلوماتية من خلال المرسوم الرئاسي رقم 20-05 ضمن المادة 17 واعتبرها مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي مقرها بالجزائر.

1- مهام وكالة أمن الأنظمة المعلوماتية:

حسب المادة 18 من المرسوم الرئاسي رقم 20-05 [62]، يوكل للوكالة عدة مهام تتعلق بتحضير وتنسيق الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، كما أنها تقترح طريقة اعتماد مزودي التدقيق ضمن نفس المجال. وبما أن مقدمي خدمات الإنترنت لهم دور في تسهيل عملية الحصول على معلومات بخصوص الجرائم المعلوماتية، فإن الوكالة تعمل على فحص الإمضاء الإلكتروني واجراء تحقيقات رقمية في حالة حدوث هجمات أو جرائم معلوماتية التي تستهدف المؤسسات الوطنية، كما ألزمها القانون بالسهر على جمع وتحليل كل المعطيات، واعداد وتحديث المرجعيات والإجراءات والأدلة العلمية وكذلك تقديم توصيات تسمح بتأمين منشآت المؤسسات الوطنية، ومن خلال المعلومات التي تحصلت عليها بالتعاون والتشاور مع الهياكل المتخصصة في هذا المجال يمكن للوكالة أن تطلب من- الهيئات والمؤسسات والمتعاملين المزودين بنظام اعلام- أي معلومة أو وثيقة تفيدها في القيام بمهامها بموجب هذا المرسوم [63].

وبالتالي " **فالوكالة** " في سبيل متابعة التطور التقني المرتبط بنشاط المؤسسات، بإمكانها تقديم المشورة والمساعدة ومرافقة المؤسسات والإدارات والهيئات العامة والخاصة من أجل وضع استراتيجية لأمن أنظمتها المعلوماتية، كما أنه بإمكانها اقتراح تدابير التطوير والبحث والمشاركة في التظاهرات العلمية المتعلقة بأمن الأنظمة المعلوماتية وتقديم توجيهات تتعلق بتكوين أعوان المؤسسات العمومية في نفس الميدان، كما أنه بإمكانها اقتراح مشاريع اتفاقيات التعاون والإعتراف المتبادل مع الهيئات الدولية، واقتراح مشاريع قوانين أو تنظيمات في مجال أمن الأنظمة المعلوماتية بعد موافقة المجلس ولتعزيز ثقافة تأمين الأنظمة المعلوماتية يمكنها إبرام مشاريع شراكة بعد موافقة المجلس، هذا ما يسمح لها بإعداد تقارير دورية عن نشاطها واعداد وتحيين حالات الخلل والنقص الموجود في الأنظمة المعلوماتية [64].

وفي سبيل مواجهة الجرائم المعلوماتية ومكافحة المجرمين، عمدت العديد من الدول إلى تأمين أنظمتها المعلوماتية من خلال تشريعاتها، فمثلا نجد المشرع المصري قد قام بإنشاء المجلس الأعلى للمجتمع الرقمي وذلك بموجب قرار رئيس الجمهورية رقم 511 لسنة 2022، والذي أوكلت له عدة مهام من بينها اعتماد اجراءات وآليات خاصة بالتغييرات الهيكلية لبناء مجتمع رقمي [65].

أما في فرنسا فنجد أنها قد أوجدت عدة آليات لمكافحة الجريمة المعلوماتية، من بينها إنشاء الوكالة الوطنية لأمن الأنظمة المعلوماتية Agence nationale de la sécurité des systèmes d'information، بموجب المرسوم رقم 2009-834 [66]، حيث تضمنت المادة 03 وما بعدها على بعض المهام المخولة للوكالة، من بينها أنها تقوم بجميع التدابير اللازمة لحماية الأنظمة المعلوماتية [67].

وفي نفس السياق أسست المملكة المتحدة البريطانية مركزاً لحماية منظومتها المعلوماتية في 01/ أكتوبر/ 2016 حيث أطلقت عليه تسمية المركز الوطني لأمن المعلوماتية NCSC الذي يملك قدرات دفاعية إلكترونية متطورة لحماية الفضاء الرقمي، حيث يلعب المركز دوراً هاماً في تحليل التهديدات الإلكترونية وفهمها وكشفها من أجل دعم جهود الدولة في تطوير مهارة أمن المعلوماتية والتصدي للجرائم المعلوماتية التي تستهدف الأمن المعلوماتي البريطاني [68].

2- تنظيم وسير وكالة أمن الأنظمة المعلوماتية:

تتولى لجنة توجيه إدارة وكالة أمن الأنظمة المعلوماتية، كما يسيرها مدير عام ويعمل تحت سلطته مديريات ومصالح تقنية وإدارية بالإضافة إلى مركز وطني عملياتي لأمن الأنظمة المعلوماتية [69].

1-2- لجنة التوجيه:

يعين رئيس لجنة التوجيه في وزارة الدفاع الوطني طبقا للتنظيم المعمول به [70].

أ- تشكيلة لجنة التوجيه:

تتكون من ممثلين من مختلف الوزارات: وزارة الدفاع، الوزارة المكلفة بالشؤون الخارجية، الوزارة المكلفة بالداخلية، الوزارة المكلفة بالعدل والمالية والطاقة، الوزارة المكلفة بالتغليم العالي، الوزارة المكلفة بالصناعة والتجارة، الوزارة المكلفة بالاتصالات، بالإضافة إلى عدة سلطات كسلطة ضبط البريد والإتصالات الإلكترونية، السلطة الوطنية للتصديق الإلكتروني، السلطة الحكومية للتصديق الإلكتروني، الهيئة الوطنية لحماية البيانات ذات الطابع الشخصي، مصالح الأمن. والمدير العام على سبيل الاستشارة.

أما مصالح الوكالة فتعهد إلى أمانة لجنة التوجيه [71]، على أن يتم تحديد القائمة الإسمية لأعضاء لجنة التوجيه بقرار من وزير الدفاع الوطني وذلك بناء على اقتراح من السلطات التي ينتمون إليها. وفي حالة غيابهم لا يحق لأعضاء لجنة التوجيه انتداب من يمثلهم [72].

ب- مهام لجنة التوجيه:

يعهد إلى لجنة التوجيه عدة مهام كدراسة عناصر الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية والبرامج السنوية قصد تنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، وتحديد الوسائل اللازمة للاستجابة للحاجات الوطنية في مجال أمن الأنظمة المعلوماتية. كما تعمل اللجنة على ضبط الوسائل اللازمة لترقية البحث ضمن نفس المجال.

كما من شأنها التداول في كل المسائل المتعلقة بتنظيم وسير الوكالة، التسيير المالي للسنة الماضية وكذا البيانات المتعلقة بالإيرادات والنفقات وكل ما يتعلق بتكوين وتوظيف المستخدمين ومرتبات مستخدمي الوكالة وكذا الموافقة على النظام الداخلي للوكالة [73].

ج- سير عمل اللجنة:

بناء على استدعاء من رئيسها تجتمع لجنة التوجيه في دورة عادية أربع مرات في السنة، ويمكنها أن تجتمع في دورة غير عادية حسب ما يقرره نظامها الداخلي كلما استدعت الضرورة ذلك [74]. ويتم تدوين أعمال لجنة التوجيه في محضر ويرسل في شكل تقرير إلى وزير الدفاع الوطني [75].

2-2- المدير العام لوكالة أمن الأنظمة المعلوماتية:

طبقا للتنظيم المعمول به في وزارة الدفاع الوطني يتم تعيين المدير العام، وتنهى مهامه بنفس الطريقة [76]. يعمل المدير العام على تنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، كما ينفذ كل البرامج الموضوعة من طرف لجنة التوجيه. وبالتالي فهو المسؤول عن سير عمل الوكالة وفقا للتشريع المعمول بهما، ويكلف في نفس الإطار بإعداد برنامج عمل الوكالة وعرضها على لجنة التوجيه للموافقة عليها، كما يعمل على تحضير مشروع الميزانية وعرضه على لجنة التوجيه للمداولة والتنفيذ.

من مهامه أيضا إبرام الصفقات والعقود والاتفاقيات التي لها صلة بمهام الوكالة، إذا هو المتصرف بإسمها يمثلها أمام الهيئات القضائية، كما يخوله القانون ممارسة السلطة السلمية على مستخدمي الوكالة الوطنية لأمن الأنظمة المعلوماتية، وكذا الأمر بصرف ميزانية الوكالة وإعداد التقرير السنوي المتعلق بنشاطات الوكالة وإرساله إلى المجلس [77].كما يقترح المدير العام بعد موافقة لجنة التوجيه النظام الداخلي للوكالة وهذا بناء على قرار من وزير الدفاع الوطني [78].

3-3- اللجنة العلمية للوكالة:

تختار لجنة التوجيه أعضاء اللجنة العلمية (10 أعضاء) من بين الأساتذة والباحثين في مجال الأنظمة المعلوماتية لمدة ثلاث سنوات قابلة للتجديد. على أن يتم انتخاب رئيس اللجنة العلمية من طرف زملائه الأعضاء، أما أمانة اللجنة العلمية فتعهد إلى مصالح الوكالة [79].

يقدم المدير العام استشارته للجنة العلمية في كل مسألة ذات طابع علمي والمندرجة ضمن مهام الوكالة والتي تتعلق بنشاطات البحث والتطوير في مجال أمن الأنظمة المعلوماتية.

كما يوكل للجنة ابداء توصياتها حول طرق تنفيذ مشاريع البحث والتطوير والمشاركة في التظاهرات العلمية المتعلقة بأمن الأنظمة المعلوماتية، تجانس المشاريع والبرامج المقترحة من المدير العام للوكالة. وكذا نشاطات التكوين العلمي وإعادة

التأهيل لفائدة مستخدمي الوكالة، وكذلك المستخدمين المكلفين بأمن الأنظمة المعلوماتية في الإدارات والمؤسسات والهيئات العمومية وكل المسائل ذات الطابع العلمي التي يعرضها عليها المدير العام للوكالة، على أن تتم مصادقة اللجنة العلمية خلال الدورة الأولى على نظامها الداخلي[80].

تستطيع اللجنة العلمية الاستعانة بأي كفاءة أو خبرة مفيدة في مجال أمن الأنظمة المعلوماتية [81]. على أن يحدد سير الوكالة ومهامها وصلاحياتها بموجب قرار من وزير الدفاع الوطني [82].

خاتمة:

استحدث المشرع الجزائري من خلال المرسوم الرئاسي رقم 20-05 منظومة وطنية لأمن الأنظمة المعلوماتية كآلية مؤسساتية هدفها وضع استراتيجية شاملة ومتكاملة للأمن المعلوماتي بواسطة أجهزة عليا في الدولة والمتمثلة في المجلس الوطني للأمن المعلوماتي ووكالة أمن الأنظمة المعلوماتية. وتعتبر المنظومة خطوة هامة نحو بناء هيكل تنظيمي يعنى بالتهديدات المعلوماتية أو ما يعرف بالجرائم المعلوماتية. ومن هذا المنطلق يمكننا تبني مجموعة من النتائج المتعلقة بموضوع الدراسة والمتمثلة في:

– يصعب ايجاد تعريف شامل جامع للجريمة المعلوماتية، ويعود السبب في ذلك من جهة إلى تنوع أساليب ارتكابها والتطور السريع في وسائل تقنية المعلومات، وظهور أشكال جديدة لهذه الجرائم من جهة أخرى. لذلك فإنه يستحسن وضع تعريف عام وشامل لها تحسبا للتطور التقني في المستقبل ويمكن أن نعرفها بأنها كل اعتداء غير مشروع معاقب عليه قانونا، يرتكب بواسطة أشخاص أو شخص يتمتع بقدرات فنية عالية ودرجة من الذكاء، ويرتكز على مجموعة من العناصر التي لها تأثير على طبيعة الأفعال الإجرامية والمتصلة اتصالاً وثيقاً بجهاز الكمبيوتر، ومن أمثلتها الإحتيال عبر الإنترنت، سرقة حسابات البطاقات الإئتمانية سرقة الهوية.

– تتميز الجريمة المعلوماتية بخصائص تختلف بشئ كبير عن الجرائم التقليدية، من بين هذه الخصائص أنها من الجرائم الجرائم العابرة للحدود، صعبة الإثبات، سهلة الوقوع من حيث عدم احتياجها لأي مجهود عضلي، وأنها تقع أثناء المعالجة الآلية للبيانات، كما أن الشئ الذي يميزها هو إمتناع المجني عليه عن التبليغ نظراً لأنها تمس خصوصية الأفراد والأشخاص المعنوية على حد سوا، وكذا خصوصية المجرم المعلوماتي من حيث تمتعه بالدراية الكافية بالمجال الإلكتروني.

– عالج المشرع الجزائري كل أنواع الاعتداءات على الأنظمة المعلوماتية في قانون العقوبات رقم 04-15 القسم السابع مكرر تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات" في المواد من 394 إلى 394 مكرر 8، كما فرض القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ترتيبات تقنية لمراقبة الاتصالات الإلكترونية والقيام بكل اجراءات التفتيش داخل المنظومة المعلوماتية قصد الحد من وقوع الجرائم المعلوماتية.

– يبدو التقارب واضحاً بين تعريف المشرع الجزائري للمنظومة المعلوماتية في المادة 01/ ب من القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والإتصال ومكافحتها السالفة الذكر وتعريف معاهدة بودابست الدولية، وهذا ما يدل على أن المشرع الجزائري قد استمد التعريف من المعاهدة.

– خول المشرع الجزائري لوزارة الدفاع الوطني بإعتبارها هيئة عليا وطنية مهام أمن الأنظمة المعلوماتية بموجب المرسوم الرئاسي رقم 20-05 وذلك من خلال المجلس الوطني لأمن الأنظمة المعلوماتية ووكالة أمن الأنظمة المعلوماتية تضم تشكيلة ثلاثية مكونة من لجنة التوجيه، مدير عام ولجنة علمية خول لها البت في الهجمات المعلوماتية التي يكون هدفها المؤسسات.

– يتضح التداخل جلياً في الصلاحيات المخولة لكل من المجلس والوكالة خاصة فيما يتعلق بإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية.

– ضعف فعالية المنظومة الوطنية لأمن الأنظمة المعلوماتية وهذا راجع إلى غياب استراتيجية وطنية شاملة للأمن المعلوماتي، وهذا ما يحد من تدخلاتها في حالة التهديدات المعلوماتية.

من خلال هذه النتائج يمكننا تقديم بعض التوصيات والمتمثلة أساسا في :

– على المشرع الجزائري أن يستحدث تعريف قانوني خاص بهذا النوع من الجرائم أي الجرائم المعلوماتية، لأهميتها وخطورتها من جهة وتزايدا ارتكابها من جهة أخرى.

– سن تشريع شامل لأمن الأنظمة المعلوماتية يكمل أحكام المرسوم الرئاسي رقم 20-05.

– سن تشريع خاص بمكافحة الجرائم المعلوماتية مع ضرورة ارفاقه بالآليات المؤسساتية والإجرائية التي تسهل تلك المكافحة.

– منحت للأمانة التقنية مهمة جمع الوثائق والمعلومات لتحضير أشغال المجلس الوطني من أي ادارة أو مؤسسة أو هيئة وتعتبر هذه المهمة من أخطر المهام، لأنه بموجبها ستتمكن من الاطلاع على معلومات تمس حرمة وخصوصية الحياة الخاصة للأفراد، لذا من المفروض أن ترفق هذه المهمة بآليات لحماية تلك الحرمة تضمن لها عدم انتهاكها باسم القانون.

– من أجل مواجهة التهديدات العابرة للحدود لابد من تفعيل آليات التعاون الدولي والإقليمي.

– إعداد استراتيجية وطنية شاملة للأمن المعلوماتي نحدد من خلالها الأهداف والإجراءات المتبعة في حالة التهديدات المعلوماتية.

– على الجزائر إبرام اتفاقيات دولية ومحاولة الاستفادة من تجارب باقي الدول بهدف تحسين آليات مواجهة الجريمة المعلوماتية بشتى أنواعها.

قائمة المراجع:

أولا– باللغة العربية:

أ) النصوص القانونية:

1– النصوص القانونية الوطنية:

– القانون رقم 04-15 المؤرخ في 27 رمضان عام 1425 هـ الموافق لـ 10 نوفمبر 2004، المعدل والمتمم للأمر 66-156 المؤرخ في 18 صفر عام 1386 هـ الموافق لـ 8 يونيو سنة 1966، المتضمن قانون العقوبات، الجريدة الرسمية عدد 71،المؤرخة في 27 رمضان عام 1425 هـ الموافق لـ 10 نوفمبر سنة 2004 م.

– القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 هـ الموافق لـ 5 غشت 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47 المؤرخة في 25 شعبان عام 1430 هـ الموافق لـ 16 غشت سنة 2009 م.

– المرسوم الرئاسي رقم 20-05 المؤرخ في 24 جمادي الأولى عام 1441 الموافق لـ 20 جانفي سنة 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية عدد 04، المؤرخة في أول جمادي الثانية عام 1441 هـ الموافق لـ 26 جانفي 2020 م.

2– النصوص القانونية الأجنبية:

– قانون الأونسترال النموذجي بشأن التجارة الإلكترونية مع دليل تشريع 1996 ومع المادة الإضافية 5 مكرر بصيغتها المعتمدة عام 1998، منشورات الأمم المتحدة نيويورك، 2000، المنشور في الموقع الإلكتروني: www.unictral.org>texts>electcom

– القانون عدد 5 لسنة 2004، مؤرخ في 3 فيفري 2004، المتعلق بالسلامة المعلوماتية، نقلا عن الموقع الإلكتروني لتعذر الحصول على الجريدة الرسمية: https://legislation-securité.th

– نظام مكافحة الجرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم م/ 17 في 8 ربيع الأول 1428 هـ الموافق لـ 26 مارس 2007 م، المنشور على الموقع الإلكتروني: https://law.boe.gov-sa

– قانون مكافحة جرائم تقنية المعلومات الكويتي رقم 63 لسنة 2015 الصادر يوم الأحد 25 رمضان 1436 هـ الموافق لـ 12 يوليو 2015 م، العدد 1244 السنة الحادية والستون.

– قرار بقانون رقم 10 لسنة 2018، بشأن الجرائم الإلكترونية، المنشور على الموقع الإلكتروني لتعذر الحصول على الجريدة الرسمية: maqam.najah.edu/législation

– قرار رقم 511 لسنة 2022، الجريدة الرسمية عدد 42 مكرر (أ) في 24 أكتوبر سنة 2022.

ب) الكتب:

– أيمن عبد الله فكري، الجرائم المعلوماتية (دراسة مقارنة في التشريعات العربية والأجنبية)، مكتبة القانون والاقتصاد، الطبعة الأولى، الرياض، 2014.

– ذيب بن عياض القحطاني، أمن المعلومات، مكتبة الملك فهد الوطنية، الرياض، 2015.

– شريف حسين محمد، القانون الواجب التطبيق على الجريمة الإلكترونية، دكتوراه، كلية الحقوق، قسم القانون الدولي الخاص، جامعة عين شمس، 2016.

– عبد الصبور عبد القوي على مصري، المحكمة الرقمية والجريمة المعلوماتية (دراسة مقارنة)، مكتبة القانون والاقتصاد، الطبعة الأولى، الرياض، 2012.

– محمود مدين، فن التحقيق والإثبات في الجرائم الإلكترونية، المصرية للنشر والتوزيع، الطبعة الأولى ،2020.

– ميرفت محمد حباية، مكافحة الجريمة الإلكترونية، دراسة مقارنة في التشريع الجزائري والفلسطيني، دار اليازوري للنشر والتوزيع، عمان، 2023.

ج) الرسائل والأطروحات الجامعية

– خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية (دراسة مقارنة)، أطروحة دكتوراه مقدمة لنيل شهادة الدكتوراه الطور الثالث (ل م د)، تخصص: القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة أدرار، 2021.

د) المقالات :

– آمن حمراني، سهيلة بضياف، أمن المعلومات في الجزائر: الإجراءات والتحديات، المجلة الجزائرية للأمن والتنمية، المجلد 09، العادد 16، جانفي 2020.

– حسين فريجة، الجرائم الإلكترونية والإنترنت، دار المنظومة، مجلة المعلوماتية، العدد السادس والثلاثون، السعودية، أكتوبر 2011،

– حنان مهداوي، التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري، مجلة الفكر القانوني والسياسي، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف 2، المجلد السادس، العددالثاني، 2022.

– حمزة خضري، حمزة عشاش، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، المجلد 06، العدد 2، جوان 2020.

– دمان ذبيح عماد، بهلول سمية، الآليات القضائية لمكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، العدد 13، جانفي 2020.

– عبد الحكيم مولاي براهيم، الجرائم الإلكترونية، دار المنظومة، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور بالجلفة، العدد 23، المجلد الثاني، الجزائر، 2015.

– شريهان ممدوح حسن، الجرائم المعلوماتية وسبل مواجهتها على المستويين الوطني والدولي، المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية، جامعة الشقراء، المملكة العربية السعودية، العدد الواحد والعشرون (كانون الثاني)، 2020، ص 07.

– نوفيل حديد، كريبط حنان، أمن المعلومات ودوره في مواجهة الإعتداءات الإلكترونية على نظام ومعلومات المؤسسات، المؤسسة، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة الجزائر 3، العدد 3، 2014.

– نوفيل حديد، مسوس كمال، مقاربات حماية أنظمة معلومات المؤسسة من الإعتداءات الإلكترونية، المؤسسة، جامعة الجزائر، العدد 5، 2016.

– هدية أحمد زعتر، الاشكاليات القانونية للجرائم المعلوماتية العابرة للحدود وسبل مواجهتها، مجلة البحوث القانونية والاقتصادية، جامعة المجمعة، المملكة العربية السعودية، العدد 84، يونية 2023.

ثانيا: باللغة الأجنبية

- Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « agence nationale de la sécurité des systèmes d'information », NOR : PRMD091478D, JOR n° 156 du 8 juillet 2009, Texte n° 3.

الهوامش

[1] ميرفت محمد حبايبة، مكافحة الجريمة الإلكترونية، دراسة مقارنة في التشريع الجزائري والفلسطيني، دار اليازوري للنشر والتوزيع، عمان، 2023، ص 29.

[2] شريهان ممدوح حسن، الجرائم المعلوماتية وسبل مواجهتها على المستويين الوطني والدولي، المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية، جامعة الشقراء، المملكة العربية السعودية، العدد الواحد والعشرون (كانون الثاني)، 2020، ص 07.

[3] شريف حسين محمد، القانون الواجب التطبيق على الجريمة الإلكترونية، دكتوراه، كلية الحقوق، قسم القانون الدولي الخاص، جامعة عين شمس، 2016، ص 18.

[4] عبد الصبور عبد القوي على مصري، المحكمة الرقمية والجريمة المعلوماتية (دراسة مقارنة)، مكتبة القانون والاقتصاد، الطبعة الأولى، ، الرياض، 2012، ص 44.

[5] محمود مدين، فن التحقيق والإثبات في الجرائم الإلكترونية، المصرية للنشر والتوزيع، الطبعة الأولى، ،2020، ص 28.

[6] شريف حسين محمد، المرجع السابق، ص 25.

[7] دمان ذبيح عماد، بهلول سمية، الآليات القضائية لمكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، العدد 13، جانفي 2020، ص 141.

[8] القانون رقم 04-15 المؤرخ في 27 رمضان عام 1425 الموافق لـ 10 نوفمبر 2004، المعدل والمتمم للأمر 66-156 المؤرخ في 18 صفر عام 1386 هـ الموافق لـ 8 يونيو سنة 1966، المتضمن قانون العقوبات، الجريدة الرسمية عدد 71،المؤرخة في 27 رمضان عام 1425 هـ الموافق لـ 10 نوفمبر سنة 2004 م.

[9] القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـ 5 غشت 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47 المؤرخة في 25 شعبان عام 1430 هـ الموافق لـ 16 غشت سنة 2009 م.

[10] خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية (دراسة مقارنة)، أطروحة دكتوراه مقدمة لنيل شهادة الدكتوراه الطور الثالث (ل م د)، تخصص: القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة أدرار، 2021، ص 12.

[11] ميرفت محمد حبايبة، المرجع السابق، ص 39.

[12] قانون مكافحة جرائم تقنية المعلومات الكويتي رقم 63 لسنة 2015 الصادر يوم الأحد 25 رمضان 1436 هـ الموافق لـ 12 يوليو 2015 م، العدد 1244 السنة الحادية والستون.

[13] نظام مكافحة الجرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم م/ 17 في 8 ربيع الأول 1428 هـ الموافق لـ 26 مارس 2007 م، المنشور على الموقع الإلكتروني: https://law.boe.gov-sa.

[14] حسين فريجة، الجرائم الإلكترونية والإنترنت، دار المنظومة، مجلة المعلوماتية، العدد السادس والثلاثون، السعودية، أكتوبر 2011، ص 2.

[15] عبد الحكيم مولاي براهيم، الجرائم الإلكترونية، دار المنظومة، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور بالجلفة، العدد 23، المجلد الثاني، الجزائر، 2015، ص 214.

[16] حنان مهداوي، التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري، مجلة الفكر القانوني والسياسي، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف 2، المجلد السادس، العددالثاني، 2022، ص 1062.

[17] عبد الصبور عبد القوي على مصري، المرجع السابق، ص 51.

[18] المرجع نفسه، الصفحة نفسها.

[19] حنان مهداوي، المرجع السابق، ص 1063.

[20] حسين فريجة، المرجع السابق، ص 3.

[21] عبد الصبور عبد القوي على مصري، المرجع السابق، ص 47.

[22] خضرة شنتير، المرجع السابق، ص 17.

[23] عبد الحكيم مولاي براهيم، المرجع السابق، ص 214.

[24] حنان مهداوي، المرجع السابق، ص 1063.

[25] القانون رقم 04-15، المتضمن قانون العقوبات، سالف الذكر.

[26] حمزة خضري، حمزة عشاش، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، المجلد 06، العدد 2، جوان 2020، ص 173.

[27] هدية أحمد زعتر، الاشكاليات القانونية للجرائم المعلوماتية العابرة للحدود وسبل مواجهتها، مجلة البحوث القانونية والاقتصادية، جامعة المجمعة، المملكة العربية السعودية، العدد 84، يونية 2023، ص 78.

[28] شريف محمد حسين، المرجع السابق، ص 32.

[29] هدية أحمد زعتر، المرجع السابق، ص 79.

[30] شريهان ممدوح حسين، المرجع السابق، ص 14.

[31] شريف حسين محمد، المرجع السابق، 45.

[32] حنان مهداوي، المرجع السابق،ص 1066.

[33] هدية أحمد زعتر، المرجع السابق، ص 81.

[34] المرجع نفسه، ص 82.

[35] قرار بقانون رقم 10 لسنة 2018، بشأن الجرائم الإلكترونية، المنشور على الموقع الإلكتروني لتعذر الحصول على الجريدة الرسمية: maqam.najah.edu/législation.

[36] نوفيل حديد، كريبط حنان، أمن المعلومات ودوره في مواجهة الإعتداءات الإلكترونية على نظام ومعلومات المؤسسات، المؤسسة، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة الجزائر 3، العدد 3، 2014، ص 197.

[37] ذيب بن عياض القحطاني، أمن المعلومات، مكتبة الملك فهد الوطنية، الرياض، 2015، ص 95.

[38] نوفيل حديد، مسوس كمال، مقاربات حماية أنظمة معلومات المؤسسة من الإعتداءات الإلكترونية، المؤسسة، جامعة الجزائر، العدد 5، 2016، ص 35.

[39] المرجع نفسه، ص 179.

[40] قانون الأونسترال النموذجي بشأن التجارة الإلكترونية مع دليل تشريع 1996 ومع المادة الإضافية 5 مكرر بصيغتها المعتمدة عام 1998، منشورات الأمم المتحدة نيويورك، 2000، المنشور في الموقع الإلكتروني: www.unictral.org>texts>electcom

[41] أيمن عبد الله فكري، الجرائم المعلوماتية (دراسة مقارنة في التشريعات العربية والأجنبية)، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض، 2014، ص 24.

[42] المرجع نفسه، ص 25.

[43] القانون رقم 09-04 المؤرخ في 14 شعبان عام1430 الموافق لـ 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47 مؤرخة في 25 شعبان عام 1430 هـ الموافق لـ 6 غشت سنة 2009 م.

[44] نوفيل حديد، كريبط حنان، المرجع السابق، ص 198.

[45] ذيب بن عياض القحطاني، المرجع السابق، ص 91.

[46] نوفيل حديد، كريبط حنان، المرجع السابق، ص 199.

[47] آمن حمراني، سهيلة بضياف، أمن المعلومات في الجزائر: الإجراءات والتحديات، المجلة الجزائرية للأمن والتنمية، المجلد 09، العدد 16، جانفي 2020، ص 180.

[48] ذيب بن عياض القحطاني، المرجع السابق، ص 93 و94.

[49] نوفيل حديد، كريبط حنان، المرجع السابق، ص 199.

[50] خضرة شنتير، المرجع السابق، ص 183.

[51] المرسوم الرئاسي رقم 20-05 المؤرخ في 24 جمادي الأولى عام 1441 الموافق لـ 20 جانفي سنة 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية عدد 04، المؤرخة في أول جمادي الثانية عام 1441 هـ الموافق لـ 26 جانفي 2020 م.

[52] المادة 05 من المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.

[53] المادة 09/ 1 من المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر..

[54] خضرة شنتير، المرجع السابق، ص 183.

[55] المادة 4/ 1،2،3،4،5،6 من المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.

[56] خضرة شنتير، المرجع السابق، ص 184.

[57] المادة 4/ 8،7 من المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.

[58] المادة 11 من المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.

[59] المادة 12 من المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.

[60] المواد 13، 14، 15، 16 من المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.

[61] القانون عدد 5 لسنة 2004، مؤرخ في 3 فيفري 2004، المتعلق بالسلامة المعلوماتية، نقلا عن الموقع الإلكتروني لتعذر الحصول على الجريدة الرسمية: https://legislation-securité.th.

[62] المادة 18 من من المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.

[63] المادة 19 من من المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.

[64] المادة 18 من من المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.

[65] قرار رقم 511 لسنة 2022، الجريدة الرسمية عدد 42 مكرر (أ) في 24 أكتوبر سنة 2022.

[66] Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « agence nationale de la sécurité des systèmes d'information », NOR : PRMD091478D, JOR n° 156 du 8 juillet 2009, Texte n° 3.

[67] Article 3 du décret n° 2009-834 portant création d'un service à compétence nationale dénommé « agence nationale de la sécurité des systèmes d'information », Op.cit.

[68] خضرة شنتير، المرجع السابق، ص 190.

[69] المادة 20 من من المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.

[70] المادة 21 من من المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.

[71] المادة 21 من من المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.

[72] المادة 23 من من المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.

[73] المادة 24 من من المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.

[74] المادة 25 من من المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.

[75] المادة 26 من من المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.

[76] المادة 27 من من المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.

[77] المادة 28 من من المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.

[78] المادة 30 من من المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.

[79] المادة 31 من من المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.

[80] المادة 32 من من المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.

[81] المادة 33 من من المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.

[82] المادة 34 من من المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، سالف الذكر.