الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة جيلالي ليابس سيدي بلعباس
كلية الحقوق والعلوم السياسية
19 مارس 1962
مخبر قانون المؤسسة

شهادة مشاركة

يشهد السيد عميد كلية الحقوق والعلوم السياسية بجامعة جيلالي ليابس سيدي بلعباس

بأن الدكتور(ة): ذبيح سفيان - جامعة المسيلة -

قد شارك (ت) في الملتقى الوطني حول " الأمان في العصر الرقمي - إستراتيجية الأمن السيبراني بالجزائر في ظل رهانات التحول الرقمي- " المنعقد يوم 27 ماي 2025 بمداخلة عنوانها « الأطر القانونية والمؤسساتية للأمن السيبراني في الجزائر».

عميد الكلية

مديرة المخبر

أ.د. صابونجي فاطيمة
مديرة مخبر بحث
"قانون المؤسسة"

الممسوحة ضوئيا بـ CamScanner

الرئاسي 24-181 المؤرخ في 5 جوان 2024 مدرسة وطنية عليا في الأمن السيبراني تهدف إلى تلبية الحاجة المتزايدة للخبراء في هذا المجال وتقديم برامج تعليمية متطوّرة تغطي أحدث التقنيات وأساليب الحماية، ممّا يعكس التزام الجزائر الجدي بتعزيز قدراتها في مواجهة التّهديدات السيبرانيـــة،عن طريق التّعامل مع البرامج والمعطيات الإلكترونية بذكاء وحذر وتبني إستراتيجية فعّالة للدفاع عن العالم الرّقمي الّذي أصبحنا نعيش فيه وتعزيز الثّقة به.

- **فما مدى نجاعة وفعالية الآليات القانونية، التقنية والهيكلية المعتمدة من قبل الجزائر في تحقيق الأمن السيبراني ومواجهة تحدّيات الإجرام الإلكتروني المتزايدة، والتي تغذّيها التكنولوجيا الجديدة وعلى رأسها الذكاء الاصطناعي، وما هي الرّهانات المستقبلية في هذا المجال؟**

أهداف الملتقى

- التعريف بأساسيات الأمن السيبراني.
- تبيان دوره الحاسم في مواجهة التهديدات السيبرانية وتعزيز الثقة بالعالم الرقمي.
- تسليط الضوء على إستراتجية الجزائر في بلوغ الأمن السيبراني من خلال ما إتخذته هذه الأخيرة من تدابير تشريعية، تقنية وهيكلية مع تشجيعها للتعاون الدولي.
- فهم معيقات تحقيقه في ظل التحديات الرقمية الآنية والمستقبلية وإستكشاف رهاناته وأفاقه.

محاور الملتقى

- **المحور الأول:** مفهوم الأمن السيبراني وأهميّته في تعزيز الثّقة بالعالم الرّقمي.
- **المحور الثاني:** الإطار التشريعي والمؤسساتي للأمن السيبراني في الجزائر.
- **المحور الثالث:** التعاون الدولي والمساعدة القضائية في مجال الأمن السيبراني.
- **المحور الرابع:** إشكالات الأمن السيبراني والتحدّيات المستقبلية لتحقيقه في ظل رهانات التّحول الرقمي.

الإشكاليـــــــة

في عصرنا الرقمي، حيث تتدفق المعلومات عبر الإنترنت بلا توقف، أصبح البحث عن الأمن السيبراني ليس فقط ضرورة بل مطلباً أساسياً لمواجهة الجرائم السيبرانية التي تهدّد كيان الدّولة وسيادتها نظراً لطبيعتها الخاصّة التي تجعل منها غالباً جرائم منظّمة وعابرة للحدود، حيث اقتحمت التّهديدات السيبرانية جميع مناحي الحياة، فهي الوحش الّذي خلّفته التكنولوجيا المتقدّمة والثورة المعلوماتية، المدمّر لمختلف القطاعات الحياتية الاقتصادية منها والاجتماعية والسياسية وحتى الشخصيّة إلى درجة أنّنا نعيش اليوم زمن الاستعمار السيبراني بكافة أشكاله، لما يحويه من انتهاكات للخصوصية وأعمال القرصنة والتجسس وسرقة المعطيات، ومن هنا كان لا بدّ من حماية المعلومات والبيانات المتداولة عبر الشبكة العنكبوتية من العبث والتبديل والتخريب، من خلال توفير الآليات والوسائل اللاّزمة لذلك في ظل إستراتيجية مضبوطة.

فالأمن السيبراني هو الدرع الرقمي الّذي يحمي عالمنا المتّصل بالإنترنت، فيقوّي مناعتنا الرقمية، ويحافظ على هويتنا الإلكترونية وعلى خصوصيتنا وأمان بياناتنا ويضمن استمرارية هياكلنا ومؤسساتنا.

ومع التوجّهات الحديثة للجزائر نحو بناء مجتمع معلوماتي وإنشاء حكومة إلكترونية وتكثيف الاعتماد على أدوات تكنولوجيا المعلومات والاتصالات، أدركت الأجهزة الأمنية الجزائرية أنه يتوجّب عليها تأمين هذه المعلومات بشدّة لأنّ تداولها وإدارتها إلكترونياً عبر شبكة الإنترنت يجعلها عرضة لخطر الاختراقات المعلوماتية، والتي تعدّ اليوم من أهم التحدّيات الجـــديدة التي على السياسة الأمنية الوطنية مواجهتها وهذا ما سعت إليه الجزائر منذ سنة 2004، إذ بادر المشرّع الجزائري إلى سنّ ترسانة من النّصوص التشريعيّة استهدف من خلالها أساساً إدراج في منظومته القانونية الجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات واستحداث تدابير إجرائية خاصّة لمكافحة الجرائم الإلكترونية، كما لجأ من جهة أخرى إلى إنشاء هياكل مؤسساتية لمجابهة الجريمة السيبرانية، وشجّع على التعاون الدولي في مجال جمع المعلومات والأدلة وتبادل المجرمين بين الدول والمساعدة القضائية بصفة عامّة. هـــذا علاوة على إنشاء بـموجـب المـرسـوم

جامعة جيلالي ليابس – سيدي بلعباس –
كلية الحقوق والعلوم السياسية

(19 مارس 1962)

تنظم بالتعاون مع
مخبر "قانون المؤسسة"
وفي إطار مشروع بحث
"التنظيم القانوني للمؤسسة وتحديات الثورتين الصناعيتين الرابعة والخامسة"

ملتقى وطني حول

الأمان في العصر الرقمي
– إستراتيجية الأمن السيبراني بالجزائر في ظل رهانات التحوّل الرقمي–

يوم الثلاثاء 27 ماي 2025
قاعـة المحاضرات (الجناح البيداغوجي)
حضوري/ عن بعد

الممسوحة ضوئيا بـ CamScanner

تنظيم الملتقى

الرئيس الشرفي للملتقى: أ.د بوزياني مراحي، رئيس جامعة جيلالي ليابس سيدي بلعباس.

الرئيس العلمي للملتقى: أ.د طيب ابراهيم ويس، عميد كلية الحقوق والعلوم السياسية، 19 مارس 1962، جامعة سيدي بلعباس.

رئيسة الملتقى الوطني: د. بن تركية لبندة أدبية، أستاذة محاضرة أ.

رئيسة اللجنة العلمية: د. بن تركية لبندة أدبية، أستاذة محاضرة أ.

أعضاء اللجنة العلمية

أ.د صابونجي نادية، مديرة مخبر "قانون المؤسسة".

أ.د شايب صورية، مديرة مخبر "المرافق السومية والتنمية".

أ.د بردان رشيد، مدير مخبر "النشاط العقاري".

أ.د إدريس خوجة نصيرة، رئيسة المجلس العلمي.

د. طلحة نورة، نائب العميد المكلفة بمابعد التدرج والبحث العلمي.

أ.د فرعون محمد، نائب العميد المكلف بالبيداغوجيا.

أ.د برقوق يوسف، رئيس قسم الحقوق.

د. غريب نوح، رئيس قسم العلوم السياسية.

د. زوقار عبد القادر، نائب رئيس قسم الحقوق المكلف بالتدريس والتعليم.

د. لبوخ محمد، نائب رئيس قسم العلوم السياسية المكلف بالتدريس والتعليم.

أ.د كراجي مصطفى، جامعة سيدي بلعباس.

أ.د صمود سيد أحمد، جامعة سيدي بلعباس.

أ.د محي الدين عبد المجيد، جامعة سيدي بلعباس.

أ.د بن دريس حليمة، جامعة سيدي بلعباس.

أ.د نزار كريمة، جامعة سيدي بلعباس.

أ.د صاري نوال، جامعة سيدي بلعباس.

أ.د شهيدي محمد سليم، جامعة سيدي بلعباس.

أ.د مكاوي أمال، جامعة سيدي بلعباس.

أ.د منصور بختة، جامعة سيدي بلعباس.

أ.د ولهاسي سمية بدر البدور، جامعة سيدي بلعباس.

أ.د بودالي محمد، جامعة سيدي بلعباس.

أ.د بودلال فطومة، جامعة سيدي بلعباس.

أ.د حلوش أمال، جامعة سيدي بلعباس.

أ.د كريم كريمة، جامعة سيدي بلعباس.

أ.د كريم زينب، جامعة سيدي بلعباس.

أ.د شنة زواوي، جامعة سيدي بلعباس.

أ.د مقدم توفيق، جامعة سيدي بلعباس.

أ.د دريسي أمينة، جامعة سيدي بلعباس.

أ.د زعزوعة فاطمة، جامعة عين تموشنت.

أ.د قردودو جميلة، جامعة عين تموشنت.

د.هواري سعاد، جامعة سيدي بلعباس.

د.شريف مريم، جامعة سيدي بلعباس.

د. حجاج يمينة، جامعة سيدي بلعباس.

د. وافي خديجة، جامعة سيدي بلعباس.

د. ناصر بدرية، جامعة سيدي بلعباس.

د. عكو فاطمة الزهرة، جامعة سيدي بلعباس.

د. صحبي محمد أمين، جامعة سيدي بلعباس.

د. مسلم عبد الرحمن، جامعة سيدي بلعباس.

د. وسواس فاطمة الزهراء، جامعة سيدي بلعباس.

د. شيورو نورية، جامعة سيدي بلعباس.

د. صنور فاطمة الزهرة، جامعة سيدي بلعباس.

د. حطاب كمال، جامعة سيدي بلعباس.

د. لورد نعيمة، جامعة سيدي بلعباس.

د. بلحسيني حمزة، جامعة سيدي بلعباس.

د. جندولي فاطمة زهرة، جامعة سيدي بلعباس.

د. بن جبارة عباس، جامعة سيدي بلعباس.

د. ختتر حياة، جامعة سيدي بلعباس.

د. بن قراش كلثوم، جامعة سيدي بلعباس.

د. خنير فريدة، جامعة سيدي بلعباس.

د. غراف ياسين، جامعة سيدي بلعباس.

د. حرير أحمد، جامعة سيدي بلعباس.

د. مالح صورية، جامعة سيدي بلعباس.

د. بوعناد فاطمة الزهرة، جامعة سيدي بلعباس.

د. مالح سعاد، جامعة سيدي بلعباس.

د. مصطفاي صافية، جامعة سيدي بلعباس.

د. باي عمر راضية، جامعة سيدي بلعباس.

د. كرمة محمد، جامعة سيدي بلعباس.

د. تريش رحمة، جامعة عين تموشنت.

د. بليدي سميرة، جامعة عين تموشنت.

رئيس اللجنة التنظيمية: أ.د مقدم توفيق، جامعة سيدي بلعباس.

أعضاء اللجنة التنظيمية

د. باي عمر راضية، نائب رئيس قسم الحقوق المكلفة بما بعد التدرج والبحث العلمي

أ.د عبار عمر، نائب رئيس قسم العلوم السياسية المكلف بما بعد التدرج والبحث العلمي.

د. رمضوم نورة، جامعة سيدي بلعباس.

د. قوسطو شهرزاد، جامعة سيدي بلعباس.

ط.د بومالة كنزة، جامعة سيدي بلعباس.

ط.د بن مالك وفاء، جامعة سيدي بلعباس.

ط.د بنابي أسامة، جامعة سيدي بلعباس.

ط.د بن شعيب يوسف - ط.د بومسيف عبد القادر، جامعة سيدي بلعباس.

ط.د بن ضياف محمد الأمين - ط.د بن عزوز محمد، جامعة سيدي بلعباس.

ط.د بلقايدي فاطمة الزهراء - ط.د شنان إيمان، جامعة سيدي بلعباس.

ط.د بوالعراس سمنون - ط.د العجيل بشير الهادي هيثم، جامعة سيدي بلعباس.

افتتاح أشغال الملتقى الوطني:

رابط الجلسات:

http://meet.google.com/azm-cmqy-emi

- 9:00 -9:05 تلاوة آيات بينات من القرآن الكريم.
- 9:05 -9:10 النشيد الوطني.
- 9:10-9:15 كلمة السيد الأستاذ الدكتور **بوزياني مراحي**، مدير جامعة جيلالي ليابس- سيدي بلعباس-.
- 9:15 -9:20 كلمة السيد الأستاذ الدكتور **طيب إبراهيم ويس**، عميد كلية الحقوق والعلوم السياسية 19 مارس 1962، جامعة جيلالي ليابس- سيدي بلعباس-.
- 9:20 -9:25 كلمة السيدة الأستاذة الدكتورة **صابونجي نادية**، مديرة مخبر "قانون المؤسسة"، كلية الحقوق والعلوم السياسية 19 مارس 1962، جامعة سيدي بلعباس.
- 9:25 -9:30 كلمة السيدة الدكتورة **بن تركية لبندة أدبية**، رئيسة الملتقى، كلية الحقوق والعلوم السياسية 19 مارس 1962، جامعة سيدي بلعباس.

الجلسة الأولى برئاسة: أ.د. بودلال فطومة

- 9:30-9:40 د. **منصوري نورية**، دكتوراه في القانون، "الفضاء الرقمي بين الحريّة والرّقابة: الأمن السيبراني كمدخل لإعادة تشكيل الثقة القانونية"، جامعة سيدي بلعباس.
- 9:40-9:50 د. **فواز العابد**، أستاذ محاضر أ، "الأمن السيبراني (مقاربة مفاهيمية)"، جامعة خميس مليانة.
- 9:50-10:00 د. **صالحي نصيرة**، أستاذة محاضرة أ، "الأمن السيبراني والأمن المجتمعي في الجزائر"، جامعة خنشلة.

الممسوحة ضوئيا بـ CamScanner

- 10:10-10:00 د. بوحفص حنان، دكتوراه في القانون، "الأمن السيبراني كركيزة أساسية لتحقيق التحول الرقمي: نحو بيئة رقمية آمنة". جامعة عين تموشنت.

- 10:20-10:10 د. تيغلت فرحات كمال، دكتوراه في القانون، "الإطار المفاهيمي للجريمة السيبرانية"، جامعة تيزي وزو.

- 10:30-10:20 د. كرمة محمد، أستاذ محاضر ب، "خصوصية الجريمة الإلكترونية من حيث القواعد الإجرائية والموضوعية". جامعة سيدي بلعباس.

- 10:40-10:30 د. نيار سليمان، أستاذ محاضر ب، "مكافحة الجريمة السيبرانية في الجزائر – دراسة في السياسات التشريعية والمؤسسات المسؤولة-"، جامعة بسكرة.

- 10:50-10:40 أ.د. شنة زواوي، أستاذ، "الإجرام الإلكتروني في ظل المبادئ الجزائية الراسخة – توافق أم قصور-"، جامعة سيدي بلعباس.

- 11:00-10:50 د. سعدون فاطمة، دكتوراه في الحقوق، "الإطار التشريعي الجنائي للأمن السيبراني في الجزائر"، جامعة الجزائر 01.

- 11:10-11:00 أ.د. نزار كريمة، أستاذة، "جريمة الابتزاز الرقمي، التداعيات وسبل الوقاية"، جامعة سيدي بلعباس.

الجلسة الثانية برئاسة: أ.د. نزار كريمة

- 11:20-11:10 أ.د. بودلال فطومة، أستاذة، "دور القضاء الدستوري في الرقابة على أدوار ومسؤوليات الأمن السيبراني"، جامعة سيدي بلعباس.

- 11:30-11:20 أ.د. لوني فريدة، أستاذة، "الأمن السيبراني المؤسساتي في الجزائر –السياسات والتحديات-"، جامعة البويرة.

- 11:40-11:30 أ.د. فرعون محمد، أستاذ، "مخاطر الأمن السيبراني في ظل التحول الرقمي"، جامعة سيدي بلعباس.

- 11:50-11:40 ط.د. بومالة كنزة، د. بن تركية ليندة أدبية، أستاذة محاضرة أ، "التعاون الدولي لمكافحة الجريمة السيبرانية"، جامعة سيدي بلعباس.

- 12:00-11:50 د. تيراوي محمد أمين، أستاذ محاضر ب، "الآليات التشريعية الوطنية لمكافحة الجرائم السيبرانية- دراسة في الواقع والتحديات-"، المركز الجامعي تيبازة.

- 12:10-12:00 د. قادري نور الهدى، دكتوراه في القانون، "القطب الجزائي الوطني كآلية جزائية ردعية لمكافحة الجرائم السيبرانية"، جامعة سيدي بلعباس.

- 12:20-12:10 د. باهة فاطمة، أستاذة محاضرة أ، "المنظومة القانونية لمكافحة الجريمة السيبرانية في الجزائر: بين قصور النص وتحديات الواقع الرقمي"، جامعة تيارت.

- 12:30-12:20 د. صحبي محمد أمين، أستاذ محاضر أ، "حماية البيانات الصحية للمرضى في التشريع الجزائري"، جامعة سيدي بلعباس.

- 12:45-12:30 مناقشة.

- 13:00-12:45 إستراحة.

الجلسة الثالثة برئاسة: د. بن تركية ليندة أدبية

- 13:10-13:00 أ.د. شهيدي محمد سليم، أستاذ، "آليات الوقاية من الجريمة الإلكترونية ومكافحتها في التشريع المقارن"، جامعة سيدي بلعباس.

- 13:20-13:10 د.وسواس فاطمة الزهراء، أستاذة محاضرة أ، "التوازن بين الأمن السيبراني للدولة وحقوق الخصوصية للمواطنين: مقاربة وتحديات"، جامعة سيدي بلعباس.

- 13:30-13:20 د. بن عزة محمد حمزة، أستاذ محاضر أ، "مدى فعالية النصوص القانونية في تعزيز الأمن السيبراني في الجزائر"، جامعة عين تموشنت.

- 13:40-13:30 د. كتاب زاهية، دكتوراه في القانون، "تعزيز التعاون الدولي في التصدّي للاحتيال الرقمي- نظرة على دور الاتفاقيات الدولية والإقليمية-"، جامعة مستغانم.

- 13:50-13:40 د.حطاب كمال، أستاذ محاضر أ، "خصوصية التفتيش في البيئة المعلوماتية"، جامعة سيدي بلعباس.

- 14:00-13:50 د.محمودي سميرة، أستاذة محاضرة أ، "أثر الإرهاب الإلكتروني على أمن واستقرار الدول"، جامعة بجاية.

- 14:10-14:00 د. مرين يوسف، أستاذ محاضر أ، "البعد الإستراتيجي للإرهاب السيبراني وتداعياته على الأمن الوطني – من أجل جزائر صامدة سيبرانياً-"، المركز الجامعي إليزي.

الممسوحة ضوئيا بـ CamScanner

- 14:20-14:10 د. رسولي أسماء، أستاذة محاضرة أ، "دور التعاون الدولي في مجال مكافحة الجريمة السيبرانية في تعزيز الأمن السيبراني "، جامعة قسنطينة 03.

- 14:30-14:20 د. بن تركية ليندة أديبة، أستاذة محاضرة أ، "الذكاء الاصطناعي في خدمة الأمن السيبراني – بين الفعالية التقنية والمخاطر والتحديّات المستقبلية–"، جامعة سيدي بلعباس.

الجلسة الرابعة برئاسة: أ.د. مقدم توفيق

- 14:40-14:30 د. بصيلة نجيب، أستاذ محاضر ب، "السيادة الوطنية بين أخلاقيات الذكاء الاصطناعي والأمن السيبراني من مقاربة الأطر الإستراتيجية للاستقلالية الرقمية"، جامعة سعيدة.

- 14:50 -14:40 د. مجدوب عبد الحليم، أستاذ محاضر أ، "دور الذكاء الاصطناعي في تعزيز الأمن السيبراني"، المركز الجامعي مغنية.

- 15:00-14:50 د. قيصران هناء، أستاذة محاضرة ب، "تهديدات تقنية ChatGpt على الأمن السيبراني"، المركز الجامعي بريكة.

- 15:10-15:00 ط.د. تركي عبد الرحيم، د. بيوش محمد العربي، أستاذ محاضر أ، "تحديات الأمن السيبراني في المؤسسات المالية"، جامعة الوادي.

- 15:20-15:10 د. مسعودي آمنة، أستاذة محاضرة ب، "رهانات دور المشرع الجزائري في مجال حماية الأطفال من الجريمة الإلكترونية"، جامعة شلف.

- 15:30-15:20 د. طحرور فيصل، أستاذ محاضر أ، "حماية المعلومات والوثائق الإدارية في ظل الأمر 21-09 المتعلق بحماية المعلومات والوثائق الإدارية"، جامعة سطيف 02.

- 15:40-15:30 د. سالمي عائشة، أستاذة محاضرة أ، "الاستثمار في الأمن السيبراني ودوره في حماية اقتصاد المعرفة"، جامعة سيدي بلعباس.

- 15:50-15:40 د. سكماكجي هبة فاطمة الزهراء، أستاذة محاضرة أ، "الأمن الرقمي القانوني ومسألة حماية الحقوق والحريات الرقمية بين حتمية استخدام البيئة الرقمية واستشراف مخاطرها المرتقبة –تجربة جزائر نموذجاً–"، جامعة قسنطينة 01.

- 16:00-15:50 ط.د. ولد علي إبراهيم، د. ذوبب العيد، أستاذ محاضر أ، "الجزائر وتحديات الأمن السيبراني المستقبلية"، جامعة الأغواط.

- 16:10-16:00 د. نبيح سفيان، أستاذ محاضر ب، "الأطر القانونية والمؤسساتية للأمن السيبراني في الجزائر"، جامعة المسيلة.

- 16:20-16:10 د. عزوز ابتسام، أستاذة محاضرة ب، "الإجرام السيبراني في التشريع الجزائري"، جامعة سكيكدة.

- 16:30-16:20 د. بوحبل فيصل ، دكتوراه في القانون، "البعد الإستراتيجي التقني والمؤسساتي في مواجهة الجريمة الإلكترونية في الجزائر: ضرورة لتحقيق الأمن السيبراني الوطني"، جامعة جيجل.

- 16:40-16:30 د. عثماني علي، أستاذ محاضر أ، ط.د. الذيب محمد، "الإطار التشريعي للأمن السيبراني بالجزائر"، المركز الجامعي أفلو.

- 16:50-16:40 ط.د. كريم آيات فاطمة الزهراء، د. باهة فاطمة، أستاذة محاضرة أ، "العدالة عبر الحدود: المساعدة القضائية والتعاون الدولي في مواجهة تهديدات الأمن السيبراني"، جامعة تيارت.

17:30-16:50 -

مناقشة واختتام فعاليات الملتقى الوطني

الممسوحة ضوئيا بـ CamScanner

جامعة جيلالي اليابس بسيدي بلعباس

ملتقى وطني بعنوان:

"الأمان في العصر الرقمي"

-استراتيجية الأمن السيبراني بالجزائر في ظل رهانات التحول الرقمي-

يوم 27 ماي 2025م

مداخلة تندرج ضمن المحور الثاني الموسوم ب :

الإطار التشريعي والمؤسساتي للأمن السيبراني بالجزائر

عنوان المداخلة:

الأطر القانونية والمؤسساتية للأمن السيبراني في الجزائر

- الاسم واللقب :سفيان ذبيح
- الرتبة العلمية :دكتور
- التخصص: قانون خاص
-الرتبة العلمية: أستاذ محاضر قسم "ب "
- الجامعة :محمد بوضياف (المسيلة)
- البريد الالكتروني: debih.soufiane@univ-msila.dz
- عضو مخبر النظام القانوني للعقود والتصرفات في القانون الخاص (جامعة خميس مليانة).

ملخص:

تتناول هذه المداخلة دراسة الأطر القانونية والمؤسساتية التي وضعها المشرع الجزائري لمكافحة الجرائم السيبرانية وتحقيق الأمن السيبراني، هذا وقد حاولنا من خلالها الإجابة على إشكالية تتمحور حول الاستراتيجية التي رصدتها الجزائر لمجابهة الجرائم السيبرانية والوقاية منها؟

وللإجابة على هاته الاشكالية اعتمدنا في مداخلتنا على كلّ من المنهجين الوصفي والتحليلي كونهما الأنسب لمثل هذه الدراسات، وقد خرجنا من خلال دراستنا لهذا الموضوع بمجموعة من النتائج والتوصيات والتي أدرجناها في نهايتها.

الكلمات المفتاحية: الجريمة الالكترونية-مواجهة الجريمة الالكترونية-الوقاية من الجرائم الالكترونية.

Abstract:

This paper examines the legal and institutional frameworks established by the Algerian legislature to combat cybercrime and achieve cybersecurity. Through this paper, we attempt to answer a question centered around the strategy Algeria has adopted to confront and prevent cybercrime.

To address this question, we relied on both descriptive and analytical approaches, as they are the most appropriate for such studies. Through our study of this topic, we concluded with a set of findings and recommendations, which we include at the end

Key words:
Cybercrime - Combating Cybercrime - Preventing Cybercrime.

مقدمة:

من نتائج الثورة التكنولوجية التي شهدها العالم في العقد الأخير انتشار وتعميم استعمال أجهزة الإعلام الآلي وكذا الهواتف الذكية في جميع الميادين، فإن كانت إيجابيات معلومة وملموسة لدى الجميع فإنّ ما نتج عنه من ممارسات غير مشروعة غير خفي بدوره؛ حيث أنتج نوعا جديدا جديد من الجرائم حديثة النشأة لم تعهد قبل لدى المجتمعات، تتميز عن غيرها بخصوصية الوسيلة والمجرم معا؛ فخصوصية الوسيلة تتمثل في كون الإعلام الآلي هو الوسيلة المستعملة، أمّا خصوصية المجرمين فتتمثل في كونهم أناسا مختصين يصعب تتبعهم والعثور عليهم، كما يصعب نسب الأعمال المجرمة إليهم، بل أبعد من ذلك فقد أصبحت الشبكة العنكبوتية مجالا وميدانا جديدا لحروب اصطلح عليها بالحروب السيبرانية، والتي تعبر عن الهجمات التي تشن على الأجهزة المرتبطة بالشبكة العنكبوتية بشكل عام.

وتماشيا مع هذه التطورات وبالتحديد هذه الجرائم سعت معظم الدور لمجابهتها عن طريق تحديث منظوماتها التشريعية من جهة، واستحداث مؤسسات وهيئات تعنى بالوقاية من هذه الجرائم ومكافحتها وكل ذلك في سبيل تحقيق ما بات يعرف بالأمن السيبراني، والجزائر كغيرها من البلدان ليست بمنأى عن هذه التحولات، خاصة بعد المسعى الذي تبنته الدولة ألا وهو رقمنة جميع الإدارات العامة والمرافق فيها، مما قد يشكل خطرا على بيانات المواطنين من جهة وبيانات مؤسسات الدولة والخواص من جهة أخرى، حيث قامت باستحداث هيئات خاصة بمكافحة الجرائم السيبرانية والوقاية منها، كما أصدرت قانونا خاصا بهذا الصنف من الجرائم وهو القانون رقم: 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1]، والذي اعتمد تسمية الجريمة المعلوماتية لهذا النوع من الجرائم.

وعليه وانطلاقا مما سبق واستنادا عليه فقد تمحورت الإشكالية التي حاولنا الإجابة عنها في مداخلتنا هاته حول الاستراتيجية المتبعة من قبل الجزائر في سبيل تحقيق الأمن السيبراني ونصها كالتالي:

-**الإشكالية:** ما هي الاستراتيجية التي تبنتها الجزائر في سبيل تحقيق الأمن السيبراني؟

وللإجابة على هاته الإشكالية اعتمدنا في مداخلتنا هاته كلّا من المنهجين الوصفي والتحليلي كونهما الأنسب لمثل هاته الأبحاث، كما قسمناها إلى محورين؛ تناولنا في الأول دراسة الإطار المفاهيمي للأمن السيبراني، واستعرضنا في الثاني الآليات القانونية والمؤسساتية التي رصدتها الدولة الجزائرية في سبيل تحقيق الأمن السيبراني.

[1]- القانون رقم 09-04 المؤرخ في 14 شعبان 1430هـ الموافق ل 5 غشت 2009م المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر ج ج د ش، العدد رقم 47 الصادرة بتاريخ 25 شعبان 1430هـ الموافق ل16 غشت 2009م.

المحور الأول: مفهوم الأمن السيبراني

سنتطرق في هذا المحور لدراسة الإطار المفاهيمي للأمن السيبراني؛ وذلك بتحديد ماهيته، من جهة وتحديد ماهية الجرائم السيبرانية من جهة أخرى؛ لأنّ مفهوم الأمن السيبراني إنّما وجد أصلا لمجابهتها والحد منها.

أولا-ماهية الأمن السيبراني:

1-تعريف الأمن السيبراني: مصطلح الأمن السيبراني هو مصطلح مركب من شقين: "أمن" و "سيبراني"؛ وإن كان معنى الأول مفهوما فمعنى الثاني يحتاج إلى مزيد بيان؛ فهو يتمحور أساسا حول مفهوم الأمن متعدد الأبعاد؛ كالأمن المرتبط بالإعلام الآلي، والأمن المرتبط بالشبكة العنكبوتية لحمايتها من الهجمات السيبرانية، والتي يمكن أن يكون مصدرها إمّا فردا أو مؤسسات أو حتى حكومات[2].

هذا ويمكن تعريف الأمن السيبراني انطلاقا من أهدافه بأنّه النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصال والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج، ولا تتحول الأضرار إلى خسائر دائمة، أمّا تعريفه من الناحية الإجرائية فيتمحور حول حماية شبكات الكمبيوتر والمعلومات التي تحتويها من الاختراق ومن الضرر الخبيث أو التعطيل[3].

وعلى العموم فإنّ إعطاء تعريف دقيق للأمن السيبراني يجب أن يرتكز على مجموعة من العناصر تتمثل في: التكنولوجيا، الأحداث، الاستراتيجيات والعمليات والأساليب، الإنسان، المرجع الأمني[4].

2-مميزات الأمن السيبراني: بالرجوع للعناصر التي تم إيرادها سابقا فإنّ الأمن السيبراني يجب أن يتميز بما يلي[5]:

---

[2]- حاتم بن عزوز، مناني حليمة، الأمن السيبراني والجرائم الالكترونية في الدول ما بعد الحداثية-الولايات المتحدة الأمريكية أنموذجا-مجلة الرسالة للدراسات الإعلامية، مج6، العدد 2، جوان 2022م، ص581.

[3]- بارة سميرة، الأمن السيبراني في الجزائر-السياسات والمؤسسات-المجلة الجزائرية للأمن الإنساني، العدد 4، جويلية 2017م، ص257.

[4]- المرجع نفسه، ص257.

[5]- المرجع نفسه، ص258.

أ-طابع متعدد التخصصات الاجتماعية والتقنية،

ب-شبكة خالية من الحجم،

ج-درجة عالية من التغيير والترابط، وسرعة التفاعل.

3-أهداف الامن السيبراني: يهدف الامن السيبراني إلى تحقيق مجموعة من الأهداف يمكن ايجازها فيما يلي[6]:

أ-الهدف الأول للأمن السيبراني هو حماية الأنظمة الحاسوبية من الوصول غير الشرعي لها، أو العبث بالمعلومات أثناء التخزين أو المعالجة أو النقل، وإلى الحماية ضد تعطيل خدمة المستخدمين الشرعيين.

ب-تحسين مستوى حماية المعلومات وضمان استمرارية تدفقها وتشغيلها.

ج-ضمان انسيابية آمنة للمعلومات وانتقال مشروع ومصرح ومرخص للملفات والبيانات.

د-استرداد البيانات المسربة في أسرع وقت في حالة حدوث خرق للأنظمة الأمنية السيبرانية.

4-أبعاد الأمن السيبراني: بالنسبة لأبعاد الأمن السيبراني فإنّها تتنوع بين البعد العسكري (الدفاعي) المرتبط بالأمن القومي، وكذا البعدين السياسي والاقتصادي، إلى جانب البعد الاجتماعي طبعا.

ثانيا-ماهية الجرائم السيبرانية:

سنتطرق لدراسة ماهية الجرائم السيبرانية وذلك بتعريفها وتبيان خصائصها وأنواعها، وكذا أنماطها.

1-تعريف الجرائم السيبرانية:

أ-التعريف الفقهي للجرائم السيبرانية: في حقيقة الأمر لا يوجد تعريف موحد لمصطلح الجريمة السيبرانية؛ حيث يختلف تعريفها من فقيه لآخر وكذا من قانون لآخر، بل حتى من حيث تسميتها؛ حيث نجد أنّ هناك من يسميها بالجريمة المعلوماتية وذهب آخرون إلى تسميتها بالجريمة الالكترونية، وعلى العموم فإنّه يمكن الوقف على تعريف لها من خلال تعريف كلّ من المصطلحين

[6]- حميدي حياة وطايلب نسيمة، مدخل مفاهيمي حول الأمن السيبراني، مجلة مدار للدراسات الاتصالية الرقمية، مج2، العدد 2، نوفمبر 2022م، ص ص 8، 9.

أو بالأحرى المصطلحات التي تتركب منها؛ وهي كل من مصطلح جريمة ومصطلح السيبرانية، وهو ما سنتناوله فيما يلي:

أ-1-الجريمة: تُعرف الجريمة في نطاق القانون الجنائي العام بأنّها سلوك الفرد عملا كان أو امتناعا يواجه المجتمع بتطبيق عقوبة جزائية، وذلك بسبب الاضطرابات التي يحدثه في النظام الاجتماعي، وهو التعريف الذي يستند على عناصر الجريمة إلى جانب بيانه لأثرها (السلوك، والسلوك غير المشروع وفق القانون الإرادة الجنائية وأثرها العقوبة أو التدبير الذي يفرضه القانون)، هي الأوصاف التي تميز بين الجريمة عموما، وبين الأفعال المستهجنة في نطاق الأخلاق أو الجرائم المدنية أو التأديبية[7].

أ-2-السيبرانية: كلمة سيبراني:(cyber) تعني الإلكترونية، وقد أُصطلح على أن تُطلق كلمة "سيبراني" على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية، وشبكة الإنترنت، ومثلًا عندما نقول الفضاء السيبراني، فهذا يعني الفضاء الإلكتروني(Cyberspace) ، فهذا يعني كل ما يتعلق من قريب أو بعيد بشبكات الحاسوب، والإنترنت، والتطبيقات المختلفة (كالوتسآب، والفيس بوك، ...الخ)، وكل الخدمات التي تقوم بتنفيذها (كتحويل الأموال عبر النت، والشراء أون لاين، وغيرها من آلاف الخدمات في جميع مجالات الحياة على مستوى العالم).

وعليه وبالجمع بين المصطلحين يمكن القول بأنّ الجريمة السيبرانية هي مجموعة الأفعال والسلوكيات الإيجابية والسلبية التي يجرمها القانون والتي تكون وسائل الاتصال الحديثة المرتبطة بشبكة الانترنت أداة لها.

هذا وقد حاول الفقهاء تعريف هذا الصنف من الجرائم؛ لتظهر بذلك عديد التعريفات تختلف حسب منطلق ونظرة الفقيه لها، إلّا أنّها تشترك عموما في كون هذه الجرائم تتم بواسطة وسائل حديثة، ومن بين هذه التعريفات نذكر التعريف الذي يرى بأنّها:"؛ فمنهم من مجموعة من المخالفات القابلة للارتكاب على شبكات الاتصال بصفة عامة وعلى شبكات الانترنت بصفة خاصة، وهو ما أدى لظهور مفهوم التكنولوجيا الحديثة للإعلام والاتصال (NTIC) أي تكنولوجيا العالم الرقمي والتي تشمل عولمة المعلوماتية واستحداث دعامات رقمية حديثة للمعلومات"[8].

ب-التعريف القانوني للجرائم السيبرانية: عرف المشرع الجزائري الجرائم التي تتم بواسطة الأجهزة الالكترونية بشكل عام وذلك من خلال نص المادة الثانية من القانون رقم: 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وقد اصطلح المشرع الجزائري على تسميتها مصطلح: "الجرائم المتصلة بتكنولوجيات الإعلام

---

[7]- سوير سفيان، جرائم المعلوماتية، مذكرة ماجستير، تخصص العلوم الجنائية وعلم الاجرام، كلية الحقوق والعلوم السياسية، جامعة تلمسان، 2011/2010م، ص9.

[8]- بن دعاس فيصل، إشكالات الجريمة المعلوماتية في التشريع الجزائري، محاضرة في إطار التكوين المحلي المستمر للقضاة، مجلس قضاء قسنطينة،2011/2010م، ص 2.

والاتصال"؛ حيث عرفها بموجب أحكام هذه المادة كما يلي: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأيّ جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية"[9]، مطلقا عليها تسمية "المنظومة المعلوماتية"، وهي أيّ نظام منفصل أو مجموعة من الأنظمة المتصلة مع بعضها البعض أو مترابطة، يقوم واحد منها أو أكثر معالجة الآلية للمعطيات تنفيذا لبرنامج معين[10].

حيث جرم المشرع الجزائري الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثر الدولة الجزائرية بالثورة المعلوماتية وما صاحبها من ظهور لأشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل، وهذا ما دفع بالمشرع الجزائري إلى تعديل قانون العقوبات (الأمر رقم: 66-156) بموجب القانون رقم: 04-15 المؤرخ في: 10نوفمبر 2004 م؛ حيث أفرد له القسم السابع مكرر وعنونه ب :المساس بأنظمة المعالجة الآلية للمعطيات، والذي تضمن بدوره 08 مواد من المادة 394مكرر وحتى المادة (394مكرر مكرر07)[11].

2-خصائص الجريمة السيبرانية: تتميز الجريمة السيبرانية عن غيرها من الجرائم الأخرى بمجموعة من الخصائص سواء تعلق الأمر بالوسائل التي تستعمل في ارتكابها، أو بالمجرم الذي يقوم بها، وسنستعرض فيما يلي كلّا منها:

أ-خصائص الجريمة السيبرانية: تنطوي الجريمة السيبرانية على مجموعة من الخصائص، وفيما يلي بيانها[12]:

أ-1-الجريمة السيبرانية ترتكب عبر شبكة الانترنت: فهي حلقة الوصل الرئيسية بين كافة الأهداف المحتملة لتلك الجرائم، كالبنوك والشركات وغيرها من الأهداف التي تكون غالبا الضحية لتلك الجرائم.

---

[9]- انظر: المادة الثانية من القانون رقم: 09-04 المؤرخ في: 2009/08/5، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج ج د ش، العدد رقم47.

[10]- نشناش منية، الركن المفترض في الجريمة المعلوماتية، مداخلة ضمن فعاليات الملتقى الوطني الموسوم ب: الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة بسكرة ،2016/2015م، ص2.

[11] - عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن دار الجامعة الجديدة ، كلية الحقوق جامعة الإسكندرية ، 2006 ، ص27 .

[12] - ياسمينة بونعارة، الجريمة الالكترونية، مجلة المعيار، المجل د20، العدد 39، جامعة الأمير عبد القادر للعلوم الإسلامية، 2015م، ص7.

أ-2-الجريمة السيبرانية عابرة للحدود: وهو ما يعني أن مساحة مسرح الجريمة لم تعد محلية، بل أصبحت عالمية، الأمر الذي خلق العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب تطبيقه بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام.

أ-3- صعوبة إثبات الجريمة السيبرانية: نظرا لارتكابها في الخفاء إلى جانب ارتفاع الخسارة الناجمة عن الجرائم السيبرانية مقارنة بالجرائم التقليدية، فقد أكدت" انتل سكيوريتي"، الشركة العالمية المتخصصة في تقنيات حماية وأمن المعلومات، أنّ قطاعات الأعمال العالمية تتكبد خسائر سنوية تصل إلى 400 مليار دولار أمريكي، وأوضحت الشركة أن الهجمات السيبرانية أصبحت اقتصادا متناميا قائما بذاته تبلغ قيمته ما بين (2إلى 3 ترليون دولار سنويا)، أو ما يشكل 15 إلى 20% من القيمة الاقتصادية الناتجة عبر الإنترنت ، وقد تكبدت شركة بريطانية خسائر بلغت 1.3مليار دولار بسبب هجوم إلكتروني واحد، وخسر مصرفين في الخليج 45 مليون دولار في ساعات قليلة، وأعلنت الهند عن تعرض308371 موقعا إلكترونيا للاختراق بين عامي 2011 و 2013.

أ-4-قلة الإبلاغ عن وقوعها: حيث يرجع ذلك لسببين؛ الأول هو الخشية والخوف من التشهير، لذلك نجد أن معظم جرائم الانترنت تم اكتشافها بالصدفة، أو بعد فترة طويلة من ارتكابها، والثاني هو عدم اكتشاف الضحية للجريمة، مما يعني أن الجرائم التي حدثت ولم يتم اكتشافها هي أكثر بكثير من الجرائم التي تم كشف الستار عنها[13].

ب- خصائص المجرم المعلوماتي: يعد المجرم السيبراني مجرما لارتكابه فعل إجرامي يتطلب توقيع العقاب عليه، وكل ما في الأمر أنّه ينتمي إلى طائفة خاصة من المجرمين تقترب في سماتها من جرائم ذوي الياقات البيضاء، وإن كانت حسب رأي الفقيه Parker لا تتطابق معها، فالمجرم السيبراني من ناحية ينتمي في أكثر الحالات إلى وسط اجتماعي متميز، كما أنّه يكون على درجة من العلم والمعرفة، هذا ويتفق مجرمو السيبرانية مع ذوي الياقات البيضاء في كون أن الفاعل في الحالتين يبرر جريمته كونه لا ينظر إلى سلوكه باعتباره جريمة أو فعل يتنافى مع الأخلاق، ويتميز المجرم السيبراني بالإضافة إلى ذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من

[13] - ياسمينة بونعارة، الجريمة الالكترونية، مرجع سابق، ص8.

المجرمين، ويرمز إليها الأستاذ(باركر Parker) بكلمة S.K.R.A.M وهي تعني: (المهارة Skills) ،(المعرفة Knowledge)، (والوسيلة Resources) (والسلطة Anthority)، (الباعث Motives)[14].

3-أنواع الجرائم السيبرانية: اختلف الفقهاء في تحديد أنواع الجرائم السيبرانية وذلك لصعوبة حصر هذه الأنواع بصفة دقيقة بالنظر لحداثة ظهور هذه الجريمة وعدم وجود تعريف عام متفق عليه لها، وتحديد مجالها، وكذا بالنظر للتطور التكنولوجي في كل صوره للارتباط الوثيق بينهما، إلى جانب تعدد تقسيماتها؛ حيث تقسم إلى طوائف مختلفة تتميز كل منها بسمات خاصة؛ وذلك بالنظر إلى اختلاف المعيار المعتمد في هذه التقسيمات، وسنحاول فيما يلي إبراز أهم المعايير التي تقسم الجرائم الالكترونية على أساسها:

أ-هناك من قسم الجرائم السيبرانية إلى ثلاث طوائف حسب الفئة المستهدفة: وتتمثل هذه الطوائف في[15]:

أ-1-جرائم الحاسب الآلي الاقتصادية،

أ-2-جرائم الحاسب الآلي التي تنطوي على الاعتداء على حرمة الحياة الخاصة،

أ-3-أخيرا جرائم الحاسب الآلي التي تهدد المصالح القومية أو السلامة الشخصية للأفراد.

ب-وهناك من قسمها بالاعتماد على معيار أنماط السلوك المختلفة: والتي تمثل الجريمة المعلوماتية ومدى اتفاقها أو اختلافها مع القواعد التي تحكم القانون الجنائي إلى ثلاث طوائف رئيسية[16]:

ب-1-الدخول والاستعمال غير المصرح بهما لنظام الحاسب الآلي،

ب-2-تتمثل في طائفة الاحتيال المعلوماتي وسرقة المعلومات،

ب-3-الطائفة الأخيرة تتمثل في الجرائم التي يساعد الحاسب الآلي على ارتكابها والأفعال التي تساعد على ارتكاب جرائم الحاسبات الآلية.

يلاحظ على هذه التقسيمات أو بعضها لم تراع بعض أو كل خصائص هذه الجرائم وموضوعها والحق المعتدى عليه لاعتمادها على معيار واحد للتقسيم متناسية معايير أخرى، هذا

---

[14]- ينظر: سوير سفيان، جرائم المعلوماتية، مرجع سابق، ص 23.

[15]- ينظر: المرجع نفسه، ص33.

[16]- ينظر: المرجع نفسه، ص33.

ويرى البعض من الفقهاء أنه يجب مراعاة في كل محاولة لتقسيم الجرائم السيبرانية اعتباران: الأول يرتكز على التطور المستمر الذي يطرأ على الجريمة المعلوماتية بصفة عامة، والثاني يرتكز على الجريمة السيبرانية أي ما يدخل في إطار هذه الجرائم وما يخرج منه[17].

ومراعاة لهذين الاعتبارين ذهب الفقه الراجح إلى تقسيم الجرائم السيبرانية إلى طائفتين رئيسيتين بالاعتماد على محل الجرائم السيبرانية التي تنصب على معطيات الحاسوب وتطال الحق في المعلومات، بالإضافة إلى الاعتماد على الدور الذي يقوم به الحاسب الآلي في الجريمة إذ يستخدم لاقترافها وسائل تقنية تقتضي استخدام الحاسب الآلي، حيث تتمثل:(الطائفة الأولى في الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي)، أمّا (الطائفة الثانية تتمثل في الجرائم المعلوماتية الواقعة على النظام المعلوماتي)[18].

4-أنماط الجرائم السيبرانية: يمكن إجمال أخطر التهديدات السيبرانية التي تواجهها الدول فيما يلي[19]:

أ-تعطيل الخدمة،

ب-إتلاف المعلومات أو تعديلها،

ج-التجسس على الشبكات،

د-تدمير الأصول والمعلومات.

---

[17] - ينظر: سوير سفيان، جرائم المعلوماتية، مرجع سابق، ص33.

[18]- للمزيد من الاطلاع انظر سوير سفيان، جرائم المعلوماتية، المرجع نفسه، ص33 وما بعدها (المبحث الثالث الموسوم ب: أنواع الجرائم المعلوماتية).

[19]- بارة سميرة، الأمن السيبراني في الجزائر-السياسات والمؤسسات-مرجع سابق، ص260.

المحور الثاني: الآليات التي تبناها المشرع الجزائري لتحقيق الأمن السيبراني

في إطار مكافحة الجرائم السيبرانية رصد المشرع الجزائري مجموعة من النصوص القانونية التي تنظم هذا الجرائم، ولأنّ مكافحة هذا الصنف من الجرائم يتطلب أطرا مؤسساتية فقد استحدث المشرع الجزائري مجموعة من المؤسسات التي تعمل حصرا على تحقيقه، وسنستعرض في هذا المحور كلّا من الأطر القانونية والمؤسساتية التي رصدها المشرع الجزائري لتحقيق الأمن السيبراني.

أولا-الآليات القانونية التي تبناها المشرع الجزائري لتحقيق الأمن السيبراني:

بالنسبة للآليات القانونية التي رصدها المشرع الجزائري لمكافحة الجرائم الالكترونية فتتمثل في النصوص القانونية التي تضمنها التشريع العقابي بشكل عام، وكذا النصوص الواردة في بعض القوانين الخاصة، وسنستعرض في هاته السانحة كلّا منهما:

1-طرق مواجهة الجريمة المعلوماتية في التشريع العقابي الجزائري: بالرجوع إلى التشريع العقابي الجزائري بشكل عام والمتمثل في كل من قانون العقوبات وكذا قانون الإجراءات الجزائية نجد أنّ المشرع قد رصد مجموعة من النصوص القانونية لمواجهة هذا النوع المستجد من الجرائم، بعضها عام والآخر خاص، وفيما يلي عرض موجز لكل منهما:

أ-القواعد الموضوعية المقررة لمواجهة الجريمة الالكترونية في قانون العقوبات الجزائري:

أ-1-تجريم الاعتداء على نظام المعالجة الآلية للمعطيات: حيث يتخذ الاعتداء على نظام المعالجة الآلية للمعطيات صورًا:

أ-1-1-الصورة البسيطة للاعتداء على نظام المعالجة الآلية للمعطيات: بدورها هذه الصورة تنقسم إلى قسمين، الدخول غير المرخص به وقد نصت عليه المادة 394 مكرر من قانون العقوبات الجزائري[20]، والبقاء غير المرخص؛ والذي يقصد به الدخول إلى النظام والاستمرار في التواجد داخله وذلك دون إذن صاحبه، رغم علمه بأن بقاءه فيه غير مرخص؛ حيث ساوى المشرع الجزائري في المادة 394 مكرر من قانون العقوبات[21].

---

[20]- تنص المادة 394 مكرر من قانون العقوبات الجزائري على ما يلي:" يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك".

[21]- سوّى المشرع الجزائري في المادة 394 مكرر من قانون العقوبات بين كل من جريمتي الدخول غير المرخص به والبقاء غير المرخص به، وهو ما تأكد بتطبيق الجزاء نفسه على السلوكين وهي عقوبة الحبس من ثلاثة أشهر إلى سنة، وغرامة مالية من 50.000 دج إلى 100.000 دج (انظر: المادة 394 مكرر من القانون رقم: 23- 06 مؤرخ في 20 ديسمبر2006 ، المتضمن قانون العقوبات، ج ر ج ج د ش عدد84 ، صادر بتاريخ 20 ديسمبر2006 ، معدل ومتمم).

وبالرجوع للمادة 394 من قانون العقوبات الجزائري نجد أنّه قد تطرق إلى الدخول ثم البقاء وكأنّه يصنف الأولى على أنّها جريمة وقتية والثانية على أنّها جريمة مستمرة.

أ-1-2-الصورة المشدّدة للاعتداء على نظام المعالجة الآلية للمعطيات: وهو ما تضمنته المادة 394 مكرر من قانون العقوبات في فقرتها الثانية؛ والتي شدد فيها المشرع الجزائري من عقوبة الدخول والبقاء بدون ترخيص في نظام المعالجة الآلية، وذلك بنصها على أن تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظومة بعقوبة الحبس من 6 أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج"، وبالتالي فقد، حددت المادة ظرفين لتشديد عقوبة الدخول والبقاء بدون ترخيص في نظام المعالجة الآلية؛ الأول في حالة الدخول أو البقاء مع محو أو تعديل في البيانات التي يحتويها النظام، والثاني في حالة ترتب عن الدخول أو البقاء تخريب نظام اشتغال المنظومة وإعاقته عن أداء وظيفته[22].

أ-2-تجريم الاعتداء على معطيات نظام المعالجة الآلية: يأخذ الاعتداء على معطيات نظام المعالجة الآلية ثلاثة أشكال، تتمثل في الاعتداء على المعطيات الداخلية للنظام والاعتداء على المعطيات الخارجية للنظام، وكذا الاعتداء على سير نظام المعالجة الآلية (المواد 393مكرر، 394 مكرر1، 2، 3)[23].

ب-القواعد الاجرائية المقررة في قانون الإجراءات الجزائية الجزائري لمكافحة الجرائم المعلوماتية: إلى جانب القواعد الموضوعية وضع المشرع الجزائري مجموعة من القواعد الإجرائية

---

[22] - انظر المادة 394 مكرر الفقرة 2 من قانون العقوبات الجزائري رقم: 23- 06.

[23] - نصت المادة 394 مكرر1 على أن: "يعاقب بالحبس من قانون العقوبات أنه 6 أشهر إلى 3 سنوات وبالغرامة من 500.000دج وإلى 2000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية، أو أزال أو عدّل بطريقة الغش المعطيات التي يتضمنها"، أمّا المادة تنص المادة 394 مكرر 02 من قانون العقوبات الجزائري على أنه:" يعاقب بالحبس من شهرين إلى 3 سنوات، وبغرامة من1.000.000 إلى 5000.000 دج، كل من يقوم عمدا أو عن طريق الغش بما يلي:

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

- حيازة أو إفشاء أو نشر أو استعمال لأيّ غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

أمّا المادة 393مكرر، فقد نصت على مسألة الاعتداء على النظام بتخريبه؛ والذي من شأنه أن يعيب عملية سير النظام المعلوماتي، ولاسيما باستعمال برامج القنابل المعلوماتية وبرامج الفيروسات، ومهما يكن فإنّ الأفعال الماسة بالسير الحسن لنظام المعالجة قد تتخذ عدة صور، لاسيما منها أفعال التخريب، التعطيل والإفساد، إلّا أنّه حبذا لو خصص المشرع الجزائري بندا خاصا ومستقلا لهذا النوع من الاعتداء الذي يقع على سير النظام، ولاسيما أن القاضي الجزائي يكتفي بالتفسير الضيق للنص، وذلك لرفع الحرج عليه.

في إطار مكافحة هذه الجرائم دائما، والمتمثلة في: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور[24] كإجراء نص عليه المشرع الجزائري في القانون رقم: 06-22 المعدل لقانون الإجراءات الجزائية، والذي أحاطه المشرع الجزائري بمجموعة من الضمانات القانونية التي تحد من تعسف سلطات الاستدلال والتحري وتصون الحقوق والحريات العامة والحياة الخاصة للأفراد[25]، وكذا إجراء التسرب[26].

2-مواجهة الجريمة المعلوماتية إطار القانون رقم: 09-04 في الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها: وضع المشرع الجزائري في هذا القانون مجموعة من التدابير التي قصد من ورائها الوقاية من هذه الجرائم ومكافحتها، وهي على شقين؛ تدابير وقائية وأخرى إجرائية:

أ-التدابير الوقائية: بالرجوع للمادة الرابعة من القانون رقم: 09-04 نجد أنّ المشرع قد حدد من خلالها الحالات التي يجوز فيها لسلطات الأمن القيام بمراقبة المراسلات الإلكترونية، وهي أربع، وفيما يلي تفصيلها:

-الوقاية من الأفعال التي تحمل وصف جرائم الإرهاب والتخريب وجرائم ضد أمن الدولة،

-عندما تتوفر معلومات عن احتمال وقوع اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام لضرورة التحقيقات والمعلومات القضائية،

-حين يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية،

-في إطار تنفيذ طلبات المساعدات القضائية الدولية المتبادلة.

ب-التدابير الإجرائية: أضاف المشرع الجزائري إلى جانب التدابير الوقائية الواردة في القانون الخاص رقم: 04-09 إجراءات جديدة تدعم تلك المنصوص عليها في قانون الإجراءات الجزائية خاصة تلك المتعلقة بمكافحة الجريمة الإلكترونية، يمكن إجمالها والتي تتمثل في:

-جواز التفتيش ولو عن بعد للمنظومة المعلوماتية أو لجزء منها من طرف الجهات القضائية المختصة وضباط الشرطة القضائية،

-إمكانية تمديد آجال التفتيش بإذن من السلطة المختصة،

---

[24]- أشار المشرع الجزائري إلى ظروف وكيفية اللجوء هذا الاجراء في المادة 65 مكرر 5 من قانون الإجراءات الجزائية.

[25]- تتمثل هذه الضمانات في: ترخيص السلطة القضائية ومراقبتها، وضرورة الاعتراض لإظهار الحقيقة مع مراعاة السر المهني، ومراعاة الجرائم التي يجوز فيها الاعتراض ومدته، وتحرير محضر حول عملية الاعتراض (انظر: براهيمي جمال، مكافحة الجرائم الالكترونية في التشريع الجزائري، المجلة النقدية، العدد 11، الرقم 2، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، 2016م، ص 141).

[26]- انظر المواد المادة 65 مكرر 11 وما بعدها من القانون رقم: 06-22 المتضمن تعديل قانون الإجراءات الجزائية الجزائري الصادر بموجب الأمر رقم: 66-155.

-إمكانية الاستعانة بالسلطات الأجنبية المختصة للحصول على المعطيات محل البحث المخزنة في منظومة معلوماتية موجودة خارج الإقليم الوطني، وذلك طبقا للاتفاقيات الدولية ومبدأ المعاملة بالمثل، طبقا للمادة 05 من القانون رقم: 09-04،

-السماح للسلطات الجزائرية المختصة باللجوء إلى التعاون المتبادل مع السلطات الأجنبية في مجال التحقيق وجمع الأدلة للكشف عن الجرائم المتصلة بتكنولوجية الإعلام والاتصال عبر الوطنية ومرتكبيها، وذلك عن طريق تبادل المعلومات أو اتخاذ تدابير احترازية في إطار الاتفاقيات الدولية ومبدأ المعاملة بالمثل.

ثانيا-الآليات المؤسساتية التي تبناها المشرع الجزائري لتحقيق الأمن السيبراني: في إطار مكافحة ومحاربة الجرائم السيبرانية استحدث المشرع الجزائري مجموعة من الأطر المؤسساتية التي تعنى بهذا الشأن، وفيما يلي عرض موجز لها:

1-مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني: تم إنشاء هذا المركز سنة 2008م ومقره ببئر مراد رايس بالجزائر العاصمة، والهدف من إنشائه هو تأمين منظومة المعلومات لخدمة الأمن العمومي ويعتبر بمثابة مركز توثيق[27].

2-المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني: وهو مؤسسة عمومية ذات طابع إداري تحت الوصاية المباشرة لوزارة الدفاع الوطني[28].

3-الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: أنشئت هذه الهيئة بموجب القانون رقم: 09-04 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها هذه الهيئة تعرف في صلب القانون ب: "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال"؛ اهتمت هذه الهيئة بمهام متعددة، أهمها:

أ -تفعيل التعاون القضائي والأمني والدولي وإدارة وتنسيق العمليات الوقائية،

ب-المساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية في حالة الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني.

4-المصلحة المركزية لمكافحة الجريمة المعلوماتية: وهي مصلحة تابعة لمديرية الأمن الوطني، تم إنشاؤها سنة 2011م[29].

5-السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي: تم استحداثها تجسيدا للمبادئ الدستورية وتكريسا لمبدأ حماية حقوق الانسان والحفاظ على الحياة الخاصة والكرامة الانسانية، تسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي لأحكام القانون رقم: 07-

---

[27]- بارة سميرة، الأمن السيبراني في الجزائر-السياسات والمؤسسات-مرجع سابق، ص270.

[28]- المرجع نفسه، ص270.

[29]- المرجع نفسه، ص270.

18 وضمان عدم انطواء استعمال التكنولوجيات الاعلام والاتصال على أي خطر تجاه حقوق الاشخاص والحريات العامة والحياة الخاصة ومن أجل ذلك فإنّها تقوم بعديد المهام والواجبات نذكر منها:

أ-تلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي، وتمنح التراخيص عند الاقتضاء.

ب-إعلام الاشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباهم.

ج-تقديم الاستشارات للأشخاص والكيانات التي تلجا لمعالجة المعطيات ذات الطابع الشخص ي واعلام اصحابها بمآلها .

د-الترخيص بنقل المعطيات ذات الطابع الشخص ي نحو الخارج وفقا للشروط المنصوص عليها في هذا القانون، سيما المادتين: 44-45.

6-المنظومة الوطنية لأمن المنظومة المعلوماتية: استجابة لمتطلبات العصر التكنولوجي أصبح من الضروري حماية الانظمة المعلوماتية وبناء على ذلك تم اصدار مرسوم رئاس ي سنة 2020م تحت رقم: 05-20 من أجل وضع منظومة وطنية لأمن الانظمة المعلوماتية موضوعة لدى وزارة الدفاع الوطني، وتعد هذه المنظومة اداة الدولة واطارها التنظيمي ووسيلتها لإعداد استراتيجيتها في مجال امن الأنظمة المعلوماتية، وتشتمل على:

أ-المجلس الوطني لأمن الانظمة المعلوماتية: والذي يتكلف بإعداد الاستراتيجية الوطنية لأمن تلك الانظمة والموافقة عليها وتوجيها.

ب-وكالة أمن الانظمة المعلوماتية: تتكلف بتنسيق تنفيذ تلك الاستراتيجية، كما تتكفل بإجراء تحقيقات في حالة حدوث هجمات الكترونية، بالإضافة الي جمع وتقييم المعطيات، وتقديم المشورة للهيئات العمومية بالإضافة إلى مهام أخرى تتعلق بالأمن الالكتروني للمؤسسات العمومية.

خاتمة:

سعت الدولة الجزائرية لحماية مؤسساتها ومواطنيها من مخاطر الجرائم التي تتم عبر الفضاء السيبراني وذلك باعتماد سياسة منظمة تتمثل في استحداث نصوص قانونية تنظم هذا الصنف من الجرائم، كما قامت بإنشاء مؤسسات وهيئات متخصصة في هذا الشأن، ونظرا لتزايد مخاطر الهجمات السيبرانية والتي أججتها تطبيقات الذكاء الاصطناعي فقد قامت الدولة بافتتاح مدرسة عليا للذكاء الاصطناعي وذلك لتكوين إطارات متحكمة في تقنياته، وكل ذلك في إطار تحقيق الأمن السيبراني.

ومن النتائج التي خرجنا بها من خلال دراستنا لهذا الموضوع نذكر:

-تحقيق الأمن السيبراني من خلال تبني استراتيجيات محكمة بات ضرورة ملحة للدول.

-الفضاء السيبراني أصبح ميدانا لنوع جديد من الحروب،

- فرض الفضاء السيبراني تحديات جديدة على دول العالم دون استثناء، كما أوجد معايير جديدة للقوة خاصة في عصر الذكاء الاصطناعي.

- فرضت الهجمات السيبرانية وعمليات الجوسسة على دول العالم إعادة النظر في فكرة السيادة الكاملة، حيث أنّ الدول الضعيفة في هذا المجال لا تعد سيادتها كاملة.

وانطلاقا من هاته النتائج نقترح ونقدم التوصيات التالية:

-تحديث المنظومة القانونية بما يتلاءم مع التحديات المستقبلية خاصة بعد ظهور الذكاء الاصطناعي على الخط وتأجيجه للهجمات السيبرانية.

-عقد اتفاقيات مع الدول المتطورة في المجال وإرسال بعثات علمية للوقوف على خبراتها ونقلها.

-التحديث المستمر للمؤسسات والهيئات بالوسائل المادية والإطارات البشرية المتخصصة.