الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد –الطارف
كليّة الحقوق والعلوم السياسية
قسم الحقوق

مذكرة بعنوان:

الأمن السبيراني في التشريع الجزائري

مقدمة لاستكمال متطلبات الحصول على شهادة ماستر أكاديمي في تخصص: قانون أعمال

إعداد الطالب(ة):
- بركـــان سارة
- هوشي بشرى

إشراف الأستاذة:
خضار فايزة

لجـنـة الـمناقـشـة

الاسم واللقب	الرتبة	الهيئة المستخدمة	الصفة
بركات عماد الدين	أستاذ محاضر–أ-	الشاذلي بن جديد -الطارف	رئيسا
خضار فايزة	أستاذ محاضر–ب-	الشاذلي بن جديد -الطارف	مشرفاً ومقرراً
نويري محمد الامين	أستاذ محاضر-أ-	الشاذلي بن جديد -الطارف	ممتحنا

السنة الجامعية: 2025/2024

الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

Minister de L'enseignement Supérieur

Et de La Recherche Scientifique

Université el tarf

Faculté de Droit et des Sciences Politiques

Département de Droit

جامعة الشاذلي بن جديد

UNIVERSITE CHADLI BENDJEDID

ⵜⴰⴳⵍⴷⵉⵜ ⵜⴰⵣⵣⴰⵢⵔⵉⵜ ⵜⴰⵎⴰⵡⴰⵙⵜ ⵜⵉⵎⵓⵔⴰⵙⵜⵉⵏⵜ

ⵜⴰⵙⴷⴰⵡⵉⵜ - ⵜⵉⵣⵣⵓⵔⵉⵜ ⵏⵜⵉⵙⵙⵉⵙⵉⵍⵜ

ⵜⴰⵙⵙⵓⵔⵉⵜ ⵜⵉⵏⵜ ⵜⵎⵓⵔⴰⵙⵜ ⵏⵜⵉⵙⵙⵉⵙⵉⵍⵜ

ⵜⵎⵓⵔⴰⵙⵜ

ج ع: القرار الوزاري رقم 1082 المؤرخ في 27 ديسمبر 2020 المحدد للقواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

تصريح شرفي
خاص بالالتزام بقواعد النزاهة العلمية

أنا الممضي أدناه،

السيد (ة): ..... مهدي ديشري .....

الحامل لبطاقة التعريف الوطنية رقم: ..... 119970647011200005 .....

الصادرة بتاريخ: ..... 06/2021 .....

عن دائرة: ..... القالة ولاية الطارف .....

المسجل بقسم: ..... الحقوق والعلوم السياسية .....

والمكلف بإنجاز مذكرة تخرج ماستر عنوانها:

..... الأحزاب السياسية في التشريع الجزائري .....

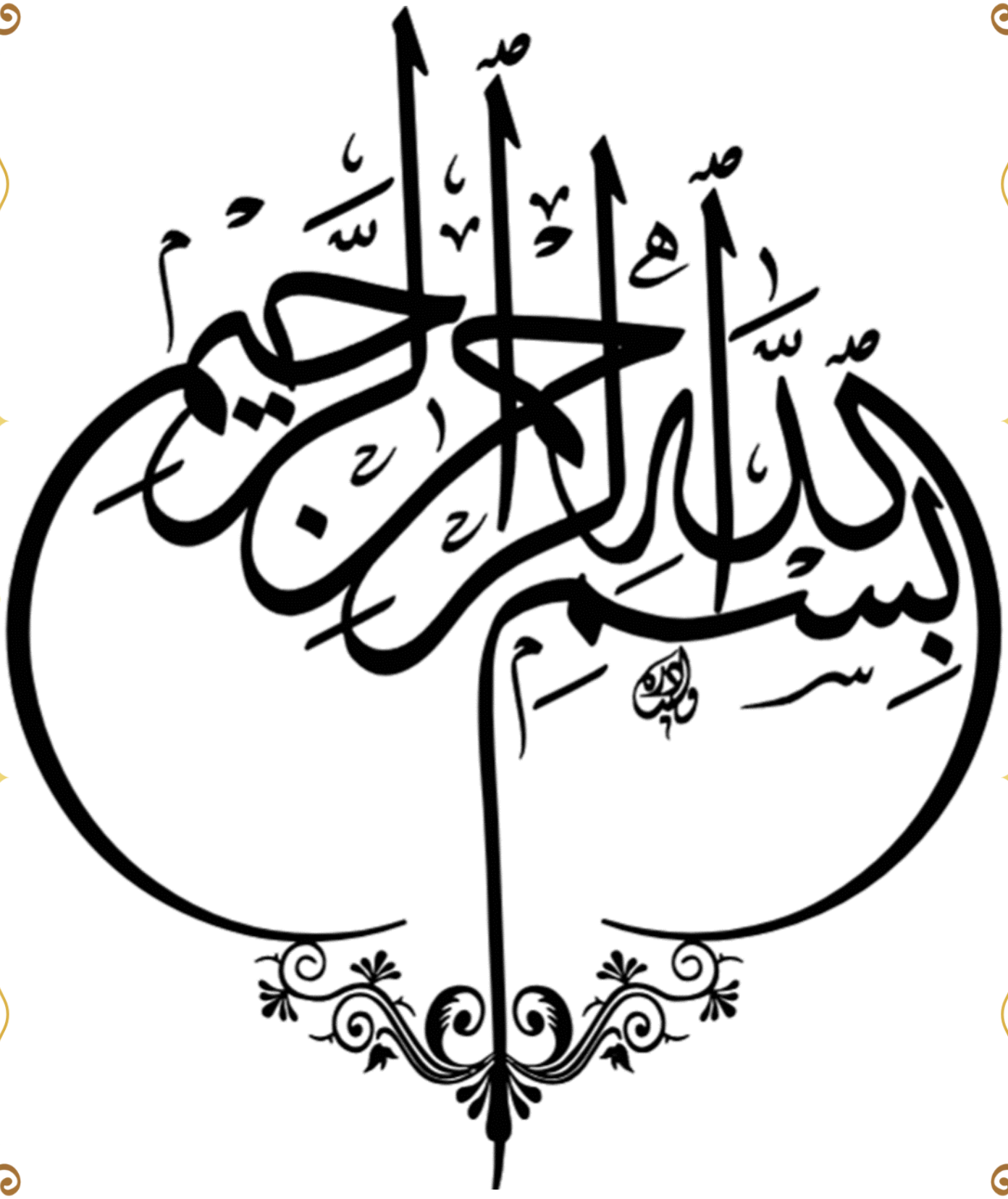
.....

أصرح بشرفي أني التزمت بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المنهجية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: 11/06/2025

إمضاء المعني

Houcha


بسم الله الرحمن الرحيم

شكر و عرفان

قال تعالى "ولئن شكرتم لأزيدنكم"

الحمد لله حمدا كثيرا طيبا مباركا، الذي أعاننا ووفقنا على إنجاز هذه المذكرة فلك الحمد ربي حتى ترضى.

نتقدم بالشكر في هذا المقام أولا إلى الاستاذة القديرة الدكتورة خضار فايزة لقبولها مهمة الإشراف على مذكرة تخرجنا هذه وعلى كل النصائح القيمة والتوجيهات المفيدة التي تعكس خبرتها في ميدان البحث العلمي وتفانيها في أداء الرسالة النبيلة التي خصها الله بها فلك منا استاذتنا الفاضلة أسمى عبارات الامتنان والشكر.

كما نتقدم بالشكر إلى كل أعضاء لجنة المناقشة المحترمين الدكتور بركات عماد الدين والدكتور نويري محمد الأمين الذين يستكرمون بتقييم هذه المذكرة

على جهودهم في قرائتها وتصويبها وتحملهم عناء المناقشة مع الامتنان لهم عن كل الانتقادات البناءة التي ستكون بلا شك سراجا منيرا في درب العلم الطويل.

كما نتقدم بالشكر لكل أستاذتنا بداية من الذين علمونا ابجديات العلم الى غاية الذين وصلوا بنا لنيل شرف هذه المرتبة.

الشكر لكل من ساندنا وصبر علينا من اهلونا واحبابنا.

قائمة المختصرات

Liste des abréviations

List of shortcuts

الاختصار	معنى الاختصار
ص	الصفحة
ص ص	الصفحة من إلى
د.ط	دون طبعة
د.س.ن	دون سنة نشر
ج ر ج ج	الجريدة الرسمية للجمهورية الجزائرية

مـقـدمـة

يعرف مجال الاتصالات وتقنيات المعلومات نهضة علمية عظيمة و تطورا مهولا وقد ألقى هذا التطور ظلاله على كافة ميادين الحياة البشرية، وذلك لما يوفره من امتيازات بتقليصه للجهد والوقت والتكلفة والدقة في تحقيق النتائج، وهذا ما جعل هذا المجال يصبح محلا للاهتمام من طرف الأفراد والدول، وجعل التطور فيه مقياس لتطور الأمم وقوتها إلا أنه وعلى الرغم من الانعكاسات الإيجابية لهذا التطور فإن الأخطار المصاحبة له لاسيما مع ربط مختلف أجهزة الحاسب ومنظومة المعلومات بالشبكة العالمية الانترنت أضحت تشكل تهديدا حقيقيا على الأمن القومي و خصوصية الافراد، وهو ما جعل الدول تكرس مجهوداتها لضمان أمنها السيبراني.

ويعتبر الامن السبيراني من أهم المواضيع المطروحة على المستوى الوطني والدولي وذلك لما يحققه من مكاسب في حالة الحفاظ عليه وتأمين الوسائل اللازمة لتحقيقه وقد عرفت الدولة الجزائرية ان الحفاظ على هذا النوع من الأمن أصبح ضرورة وذلك بالنظر إلى كمية المعلومات والبيانات التي باتت منتشرة في هذا الفضاء لاسيما أمام اتجاهها نحو الخدمات الالكترونية وتبنيهما سياسة الحكومة الرقمية منذ حوالي ثلاث عقود من الزمن من جهة، وزيادة انتشار استعمال هذه التقنيات من طرف الأفراد من جهة أخرى.

وبعد أن أضحى التحدي الحقيقي الذي تواجهه الدولة هو حماية هذه المعلومات والبيانات وكيفية الوقاية ومكافحة الهجمات السيبرانية، و خاصة مع ازدياد نسبة التطور في وسائل تكنولوجيا الاعلام و الاتصال الذي فاقت قدراته تصورات العقل البشري كاستخدام تقنيات الذكاء الاصطناعي، اصبح لابد من الاهتمام بوضع الترتيبات اللازمة لتدعيم البنية الأساسية للأنظمة الرقمية وذلك من خلال الاهتمام بالجانب التقني والفني وذلك من خلال توفير الإمكانيات المادية التي تساهم في الحد من مخاطر الهجمات السيبرانية وبناء قدرات تقنية رقمية عن طريق استعمال برمجيات وتطبيقات وأنظمة الحماية الفيروسية، واستخدام تقنيات الدفاع السيبراني بإنشاء طبقات متعددة من الحماية ضد هذه التهديدات المحتملة، إلا أن الاهتمام بهذه الجوانب لن يكون له فعالية كبيرة ما لم توجد منظومة تشريعية تكفل تحديد آليات موضوعية تحدد فيها القواعد الأساسية التي يجب مراعاتها عند التعاطي في المجال السيبراني وتشمل أساليب للحد من الأفعال التي من شأنها أن تمس بالأمن السيبراني.

وفي سبيل تحقيق الأهداف الموضوعية فإنه لابد من استحداث آليات إجرائية خاصة يتم انتهاجها للكشف عن هذا النوع من الأفعال لما تنطوي عليه من خصوصية تجعل الأساليب التقليدية غير قادرة على التصدي لها، ضف إلى ذلك وجوب استحداث مؤسسات توكل لها بعض المهام حسب مجال اختصاصها في سبيل تفعيل وتعزيز الآليات الموضوعية وهو ما تفطن له المشرع الجزائري وبدأ في تشكيل ترسانة قانونية وتشريعية في مجالات مختلفة تسعى للوصول إلى تحقيق فضاء سيبراني آمن، بداية من أعلى تشريع في الدولة وهو الدستور، والذي أقر حماية الأفراد في

هذا المجال وجعله من بين الحقوق الأساسية التي تقع على جميع السلطات والهيئات العمومية أن تكفل ضمانها وتحقيقها وهو ما يظهر جليا في نص المادة 47 منه.

وقد جاء المشرع كذلك بالعديد من النصوص الجديدة والتعديلات للنصوص القديمة لتكريس هذه الحقوق للأشخاص وتحقيق الأمن السيبراني في الدولة بصفة عامة، إلا أنه لم يعطي مفهوما صريحا للأمن السيبراني إلا بموجب القانون رقم 18-04 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية في مادته العاشرة والتي عرفته على أنه مجموع الأدوات والسياسات ومفاهيم الأمن والآليات الأمثلية والمبادئ التوجيهية وطرق تسيير المخاطر والأعمال والتكوين والممارسات الجيدة والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الالكترونية، ضد أي حدث من شأنه المساس بتوفر وسلامة وسرية البيانات المخزنة أو المعالجة أو المرسلة وهو التعريف الذي جاء مطابقا للتعريف الوارد في الاتفاقية الدولية للمواصلات السلكية واللاسلكية.

أهمية الدراسة:

إن أهمية البحث في موضوع "**الأمن السيبراني في التشريع الجزائري**" تبرز من حيث كونه من المواضيع الحديثة التي تحظى باهتمام كبير على المستويين الدولي والوطني، حيث نجد أن معظم إن لم نقل جل دول العالم ومن بينها الجزائر تسعى لتحقيق الأمن السيبراني وذلك بمكافحة الجريمة السيبرانية.

كما أنه يعالج مواضيع الساعة، فكل جزئية تحمل في طياتها العديد من المستجدات سواء على المستوى القانوني وحتى المؤسساتي على الصعيدين الدولي وحتى الوطني، الأمر الذي دفع بالعديد من الباحثين وعلى وجه الخصوص في مجال القانون إلى عقد ملتقيات وطنية ودولية حول هذا الموضوع.

ومن جهة أخرى فإن للبحث في هذا الموضوع إثراء للجانب القانوني وبالتالي الخروج عن المواضيع المتكررة المتعارف عليها في مجال القانون بعرض نظرة أو تأطير المشرع الجزائري لهذا الموضوع مواكبين آخر تعديلات القوانين المرتبطة بموضوع الدراسة.

كما أن هذا الموضوع سيساهم في إثراء المكتبة بمرجع يضاف إلى قائمة المراجع السابقة في هذا الموضوع على الرغم من قلتها، فأغلب المؤلفات في هذا الموضوع في شكل مقالات.

أهداف الدراسة:

إن البحث في أي موضوع جاد ومهم لا محالة يراد من وراءه تحقيق هدف أو بالأحرى مجموعة من الأهداف، لذلك فإن بحثنا في موضوع "**الأمن السيبراني في التشريع الجزائري**"، يرجى من وراءه تحقيق الأهداف الآتية:

- جمع متفرقات من المنظومة القانونية الجزائرية المتعلقة بالجريمة السيبرانية؛

- عرض الإطار المؤسساتي الذي يساهم بشكل كبير في تطبيق القوانين ومكافحة الجرائم السيبيرانية وبالتالي تحقيق الأمن السيبراني؛
- تكملة الدراسات السابقة باعتبارها موجزة وفي شكل مقالات؛
- تحيين الدراسات السابقة بآخر تعديلات القوانين المرتبطة بموضوع الدراسة؛
- إزالة الغموض واللبس حول كل ما يتعلق بالأمن السيبراني من خلال عرض مختلف الآليات القانونية والمؤسساتية التي تهدف إلى تحقيقه؛
- إثراء المكتبة الجامعية بهذه الدراسة الأكاديمية التي يمكن القول عنها أنها دراسة قانونية موضوعية في موضوع لم يلق حظه من الدراسة بطريقة مفصلة.

أسباب اختيار الموضوع:

لقد شجعت العديد من المستجدات القانونية والأحداث الراهنة على عملية البحث في هذا الموضوع، دون أن ننسى الأسباب الشخصية التي ساهمت إلى حد كبير في اختيار هذه الدراسة دون سواها من المواضيع، وفيما يلي عرض لهذه الأسباب:

- **الأسباب الذاتية:**

إن البحث في أي موضوع لابد أن ينطلق من إرادة ذاتية ورغبة شخصية في خوض غماره والاستمتاع بالبحث في جزئياته وتفاصيله، ولعل السبب الأبرز يكمن في ميولنا الشخصية لمثل هذا النوع من المواضيع التي تتميز بالحداثة، إضافة إلى أن الموضوعات التي تثير الاهتمام للبحث فيها هي تلك التي لا تحظى بالدراسة بالرغم من أهميتها، ومن هذا المنطلق كانت الرغبة جامحة للخوض فيه على الرغم من الصعوبات التي تحيط به.

- **الأسباب الموضوعية:**

إن البحث في موضوع **الأمن السيبراني في التشريع الجزائري** يرجع للأسباب الموضوعية التالية:

- إن هذا الموضوع يعد من المواضيع الحيوية خاصة في ظل الجهود الدولية والداخلية لمكافحة الجرائم السيبرانية؛
- حداثة موضوع الدراسة حيث يعد موضوع الساعة ومصدر اهتمام مختلف دول العالم و من بينها الجزائر؛
- بالإطلاع المتواضع على مختلف المؤلفات التي تعالج موضوع **الأمن السيبراني في التشريع الجزائري**، لمسنا عدم تفصيلها وإيجازها.

إشكالية الدراسة:

ينطلق الإشكال الرئيسي للدراسة من أن العالم يشهد العديد من التطورات التكنولوجية خاصة في ظل انتشار ما يعرف بالذكاء الاصطناعي، الأمر الذي أدى إلى زيادة معدلات الجرائم السيبرانية والتي بات من الضروري وضع إستراتيجيات من أجل مواجهتها، وهذا ما عملت عليه الدولة الجزائرية وذلك من خلال تدعيم الترسانة القانونية و تحيينها و السهر على تطبيق هذه القوانين والتصدي لهذه الجرائم، وقد تمحور الإشكال الرئيسي لهذا الموضوع فيما يلي:

- **ما مدى فعالية المنظومة القانونية والمؤسساتية الجزائرية في تحقيق الأمن السيبراني؟**

ويتفرع عن هذه الإشكالية الرئيسية التساؤلات الفرعية الآتي ذكرها:

- هل تحقيق الأمن السيبراني مرتبط بقانون العقوبات أم أنه متشعب في قوانين متفرقة؟
- كيف تم تكييف القواعد الإجرائية للحد من التهديدات الواقعة على الامن السبيراني؟

منهج الدراسة:

بحكم أن موضوع الدراسة يثير العديد من الإشكالات النظرية وخاصة العملية المتنوعة والمتشابكة والمعقدة أيضا، الأمر الذي يدفعنا للاعتماد على المناهج الآتية لدراسة هذا الموضوع:

- **المنهج الوصفي:**

لقد كان استعمال هذا المنهج ضروريا لتوضيح عدة مفاهيم وتحديد معانيها ومدلولاتها للوقوف على مقاصدها وأهميتها كجزء فاعل في موضوع الدراسة.

- **المنهج التحليلي:**

لقد كان للمنهج التحليلي دور بارز في هذه الدراسة كونها تستلزم التعرض للنصوص القانونية التي تحتاج في الغالب إلى تحليلها وتمحيصها والمقابلة بينها والاجتهاد لمحاولة الوصول لمقصودها.

الدراسات السابقة:

لقد سبق للمؤلف الطيبي البركة ضمن أطروحة الدكتوراه الموسومة بـ: الحماية الجنائية لنظام المعالجة الالية للمعطيات– دراسة مقارنة–، تخصص قانون جنائي، جامعة احمد دراية ادرار، كلية الحقوق والعلوم السياسية، قسم الحقوق، الموسم الجامعي 2021/2020، أن تعرض لأكثر الجرائم المرتكبة في الفضاء الرقمي المنصوص عليها في قانون العقوبات، وقد كان هذا المؤلف اللبنة الأولى التي انطلقت منها الدراسة، لتتوسع الدراسة أكثر لتشمل جرائم أخرى.

كما تم الاعتماد أيضا على أطروحة دكتوراه للأستاذ عثماني رضوان، مكافحة جرائم المعلوماتية في القانون الجزائري والدولي، أطروحة دكتوراه في العلوم، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة وهران2، محمد بن احمد، 2024/2023، لكن وعلى الرغم من العلاقة الظاهرة بين هذه الدراسة وموضوع المذكرة إلا أنها شكلت فقط جزء من الموضوع،كما أنها لم تشمل بالدراسة آخر تعديلات قانون العقوبات.

صعوبات البحث:

لكل بحث علمي صعوبات تعترض سبيل القائم به، ومن أهم الصعوبات التي واجهت الباحث في سبيل الإحاطة بهذه الدراسة ما يلي:

- غياب الدراسات العلمية الأكاديمية في موضوع **الأمن السيبراني في التشريع الجزائري**؛

- صعوبة البحث، كونه يشكل حلقة وصل بين عدة قوانين متفرقة، لذلك كان من غير السهل تجميع المعلومات المتعلقة بكل قانون على حدى؛

- تشتت جزئيات موضوع البحث بين عدة نصوص قانونية مختلفة.

التقسيم العام لخطة البحث:

قسّم موضوع الدراسة وفقا لخطة ثنائية تفصيلها كما يلي:

- الفصل الأول: الاليات القانونية الموضوعية لتحقيق الامن السبيراني

- المبحث الأول: الاليات الموضوعية لتحقيق الامن السبيراني في قانون العقوبات

- المبحث الثاني: الاليات الموضوعية لتحقيق الامن السبيراني في القوانين الخاصة

- الفصل الثاني: الاليات القانونية الإجرائية والهيكلية لتحقيق الامن السبيراني

- المبحث الأول: الاليات الإجرائية لتحقيق الامن السبيراني

- المبحث الثاني: الاليات الهيكلية لتحقيق الامن السبيراني

الفصل الأول: الآليات القانونية الموضوعية لتحقيق الامن السبيراني

اصبح الامن السبيراني هاجسا لجميع الدول من دون استثناء خاصة تلك التي اتجهت نحو الاعتماد على تقنيات تكنولوجيات الاعلام و الاتصال في ميادين نشاطها، و لهذا فقد اطلقت العديد من المبادرات على المستوى الدولي لدعم الامن السبيراني كمبادرات الاتحاد الدولي للاتصالات و الاتحاد الأوروبي والتي كان لها دور كبير في إرساء قواعد موضوعية لحماية الدول والأشخاص من الاعتداءات في المجال السبيراني، وقد تأثرت التشريعات الداخلية بهذه المبادرات و منها التشريع الجزائري، وان كان الجانب المدني لم يحظى باهتمام المشرع تاركا إياه للفقه في تأسيس المسؤولية المدنية الناجمة عن التهديدات السبيرانية والاثار المترتبة عنها فان الجانب الجزائي كان له نصيب وفير، اذ سن المشرع الجزائري العديد من النصوص بغرض تحقيق الامن السبيراني بداية من تعديل قانون العقوبات في سنة 2004 بموجب القانون رقم 04-15 والذي جاء بالقواعد الجزائية العامة لحماية أنظمة المعالجة الالية للمعطيات و الذي تلته العديد التعديلات التي حاول بها المشرع إعطاء نوعا من الحماية بالنسبة للاخطار الناجمة عن استعمال الفضاء السبيراني، من جهة أخرى تم تشريع العديد من القوانين الخاصة لتعزيز الامن السبيراني، و من هذا المنطلق سنتناول الامن السبيراني في قانون العقوبات (المبحث الأول) ثم نتطرق الى الامن السبيراني في القوانين الموضوعية الخاصة (المبحث الثاني).

المبحث الأول: الاليات الموضوعية لتحقيق الامن السبيراني في قانون العقوبات

يعتبر قانون العقوبات الشريعة العامة لتحقيق الردع العام ووسيلة لمحاربة الأفعال غير المشروعة والمجرمة بصفة عامة، و لما كانت حماية الامن السبيراني تتطلب تحديد الأفعال التي من شأنها أن تشكل خطرا وتهديدا للأشخاص او لمصالح الدولة او هياكلها بغرض محاربتها وردعها فقد حدد قانون العقوبات مجموعة من الجرائم يهدف من خلالها إلى حماية المعلومات والمعطيات وهي الاحكام التي جاء بها القانون رقم 04-15[1] وهي تعد بمثابة قواعد خاصة بتحقيق الامن السبيراني كما جاء بفئة اخرى من الجرائم يهدف من خلالها الى حماية الافراد والدولة من الانتهاكات ويتحقق بها الامن السبيراني بطريقة غير مباشرة.

المطلب الأول:

حماية أنظمة المعالجة الالية للمعطيات كآلية لتحقيق الامن السبيراني

ان تفاقم الاعتداءات على الأنظمة المعلوماتية خاصة مع ضعف الحماية الفنية استدعى تدخلا تشريعيا صريحا وقد استدرك المشرع الجزائري الفراغ القانوني[2] وأقر عقوبات ردعية لتلك الاعتداءات، وهذا بموجب القانون رقم 04 - 15 المتعلق بتعديل قانون العقوبات وذلك باستحداثه للقسم السابع مكرر من خلال المواد 394 مكرر إلى 394 مكرر 7.

الفرع الأول:

مفهوم أنظمة المعالجة الالية للمعطيات

من خلال استقراء القسم السابع مكرر الذي جاء تحت عنوان "**المساس بانظمة المعالجة الالية للمعطيات**" نجد ان المشرع الجزائري تطرق الى النظام المعلوماتي[3]، دون إعطاء تعريف شامل لنظم المعالجة الالية للمعطيات، تاركا ذلك للفقه وقد اكتفى بتحديد صور هذه الجرائم والعقوبات المقررة لها، الا انه ما يفهم من المعطيات المعالجة آليا هي عمل البرامج والبيانات الموجودة في الكمبيوتر وعلى شبكة الانترنت[4].

---

[1] القانون رقم 04-15 المعدل والمتمم لامر رقم 66-156 المؤرخ في 10-11-2004 والمتضمن قانون العقوبات، ج ر ج ج العدد 71.

[2] امال قارة، "الحماية الجزائية للمعلوماتية في التشريع الجزائري"، ط 2، دار هومة، الجزائر، 2007، ص 100.

[3] عرفت المادة 02 الفقرة ب من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر ج ج العدد 47 المؤرخة في 23-08-2009، النظام المعلوماتي على انه: نظام منفصل او مجموعة من الأنظمة المتصلة ببعضها البعض او المرتبطة يقوم واحد منها او أكثر بمعالجة اليه للمعطيات تنفيذا لبرنامج معين.

[4] زيدان زيبحة، "الجريمة المعلوماتية في التشريع الجزائري والدولي"، دار الهدى، طبعة 2011، الجزائر، ص 48.

ولعل من اهم التعريفات المعتمدة في الفقة لتعريف نظام المعالجة الالية للمعطيات هو التعريف المقترح من مجلس الشيوخ الفرنسي والذي عرفه على أنه: "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، والتي تتكون كل منها من الذاكرة والبرامج و المعطيات وأجهزة الادخال والاخراج وأجهزة الربط، و التي تربط بينها مجموعة من العلاقات والتي عن طريقها تتحقق نتيجة معينة وهي معالجة المعطيات، على ان يكون هذا المركب خاضع لنظام الحماية الفنية"[1].

ومن ثمة يمكن القول ان تعريف نظام المعالجة الالية للمعطيات يعتمد على عنصرين أولهما يتضمن العناصر المادية والمعنوية التي يتكون منها المركب وكمثال عن ذلك: الذاكرة، البرامج، المعطيات، أجهزة الربط والتي تم ذكرها على سبيل المثال لا الحصر نظرا للتطور التقني في هذا المجال، والثاني يتضمن العلاقات التي تربط بين هذه العناصر وتوحدها نحو تحقيق هدف واحد محدد وهو المعالجة الالية للمعطيات[2]؛ أي لابد من وجود ترابط وصلة بين وحدات النظام وتوحدها او تحاول توحيد جهودها نحو تحقيق الهدف المقصود وعلى هذا فان المساس بمكونات مادية المعزولة او معنوية معزولة لا تشكل جريمة إلا إذا كانت هده المكونات تشارك في تطبيقات فعلية داخل نظام كامل أو لها القدرة على ذلك ويكون لها دورا في تحقيق الغاية الأساسية وهي معالجة المعطيات[3].

وعلى هذا فان جرائم الاعتداء المتعلقة بالمعالجة الالية للمعطيات لا تقوم اذا كان الاعتداء واقعا على برامج معروضة للبيع، او على جهاز حاسب لم يدخل الخدمة او عنصر مودع بالمخازن او على قطع الغيار أو على الأجهزة التي مازالت في حالة التجربة و الأنظمة التي خرجت من الخدمة تماما[4]. وعلى العكس من ذلك فان الجريمة تقع اذا وقع الاعتداء على النظام خارج ساعات تشغيله العادية واذا كانت احد عناصره في حالة عطل كما تقع الجريمة أيضا اذا وقع الاعتداء على عنصر يشكل جزءا من أنظمة متعددة[5].

اما بخصوص وجوب خضوع لنظام الحماية الفنية الذي جاء به هدا التعريف فهو محل جدل فقهي ذلك انه بالرجوع إلى النصوص المتعلقة بجرائم الاعتداء على انظمة المعالجة الآلية للمعطيات في التشريع الجزائري فانها لا تتضمن شرط الحماية الفنية وتطبيقا للمبادئ العامة المستقرة في تفسير القانون الجنائي أنه لا يجوز تقييد النص المطلق،

---

[1] علي عبد القادر قهوجي، "الحماية الجزائية لبرامج الكمبيوتر"، د ط، المكتبة القانونية، القاهرة، 1999، ص 120.

[2] مسعود خثير، "الحماية الجنائية لبرامج الكومبيوتر (أساليب وثغرات)"، دار الهدى، طبعة 2010، الجزائر، ص 109.

[3] الطيبي البركة، الحماية الجنائية لنظام المعالجة الالية للمعطيات– دراسة مقارنة، رسالة دكتوراه تخصص قانون جنائي، جامعة احمد دراية ادرار– الجزائر، كلية الحقوق والعلوم السياسية، قسم الحقوق، سنة 2021، ص 29.

[4] أمال قارة، المرجع السابق، ص ص 102، 103.

[5] مسعود خثير، المرجع السابق، ص 110.

أو تخصيص النص العام، إلا إذا وجد نص يجيز ذلك فإن عدم ذكر المشرع الشرط الحماية الفنية يعني أن المشرع أراد استبعاده، هذا فضلا عن حاجة كل أنظمة المعالجة الآلية للمعطيات سواء كانت تتمتع بحماية فنية أم لا إلى الحماية الجزائية[1].

الفرع الثاني:

صور جريمة المساس بانظمة المعالجة الالية للمعطيات

باستقراء الفصل السابع مكرر من قانون العقوبات المتضمن الجرائم المتعلقة بالمساس بانظمة المعالجة الالية للمعطيات يتضح أن الركن المادي لهذه الجريمة يتجلى في صورتين، الأولى متمثلة في الإعتداءات على نظام المعالجة الآلية وهذه الأخيرة تحتوي على نوعين من الإعتداء الأول وهو الدخول والثاني هو البقاء غير المشروع في نظام المعالجة الآلية في حين تنطوي الصورة الثانية على الاعتداء على المعطيات سواء داخل النظام او خارجه.

أولا: الاعتداءات على أنظمة المعالجة الالية

1- فعل الدخول: ويقصد بالدخول هنا الدخول الالكتروني عن طريق الأساليب والوسائل التقنية المتاحة كالدخول إلى مركز النظام المعلوماتي والاطلاع على المعلومات ولم يحدد المشرع الجزائري الطريقة التي يتم بها الدخول وعليه فان الجريمة تتحقق بأي وسيلة[2].

ويذهب الفقه الفرنسي إلى أن الدخول له مدلول معنوي، حيث يشبه الدخول إلى النظام بمثابة الدخول في ذاكرة الإنسان، كما أن له مدلول مادي يتمثل في كون الشخص قد حاول الدخول أو دخل بالفعل إلى النظام المعلوماتي، و وفقا لذلك يستوي أن يكون التعدي مباشراً أو غير مباشر، كما ان هذه الجريمة تقوم بغض النظر عن صفة الفاعل، سواء كان يعمل في مجال الأنظمة، أم لا علاقة له بها، وسواء كان يستطيع الاستفادة من النظام أم لا، وحتى ولو لم تكن للجاني القدرة الفنية على تنفيذ العمليات على النظام و إنما يشترط ألا يكون من أولئك الذين لهم حق الدخول إلى هذا النظام ويتحقق الدخول غير المشروع كذلك متى كان مخالفاً لإرادة صاحب النظام، أو من له حق السيطرة عليه، كتلك الأنظمة المتعلقة بأسرار الدولة أو دفاعاتها، أو تتضمن بيانات شخصية تتعلق بحرمة الحياة الخاصة بحيث لا يجوز الاطلاع عليها[3].

---

[1] علي عبد القادر القهوجي، المرجع السابق، ص 123.

[2] رامي حليم، "جرائم الاعتداء على أنظمة المعالجة الالية للمعطيات"، مجلة دراسات وأبحاث، جامعة الجلفة، المجلد 01، العدد 01، 2009، ص 343.

[3] خثير مسعود، المرجع السابق، ص 115.

كما تقوم الجريمة سواء تم الدخول الى النظام كله او جزء منه فقط، ولا يشترط لقيامها التقاط او حصول الفاعل على المعلومات الموجودة داخل النظام او البعض منها،أي انها تقوم بغض النظر عن نتيجة الفعل[1].

كما ان المشرع الجزائري لم يحدد ما اذا كان الدخول غير المشروع يؤدي او ينتج عنه انتهاك أجهزة وسائل الحماية تاركا ذلك للسلطة التقديرية للقاضي، كما انه لم يتطرق لفعل الاعتراض غير المشروع لعملية نقل المعلومات واعطى في المقابل مفهوما موسعا لفعل الدخول الدخول عن طريق الغش الى نظام المعالجة الالية ليمتد ويشمل الالتقاط غير المشروع والاعتراض غير المشروع للمعلومات اثناء انتقالها باعتبارها تمثل انتهاكا لاتصال معلوماتي بين النظم المختلفة اثناء عملها وبهذا فهو يندرج ضمن نص المادة 394 مكرر من قانون العقوبات[2].

2- فعل البقاء: تم تعريف البقاء على انه كل تواجد غير عادي كالاتصال بواسطة الشبكة المعلوماتية بنظام بالدخول و النظر فيه، أي في المعطيات التي يتضمنها و غيرها من التصرفات غير المسموح بها و التي تشكل بدورها بقاء احتيالي[3]، وعلى العموم يقصد بالبقاء هو التواجد داخل النظام المعلوماتي ضد إرادة من له حق السيطرة على هذا النظام[4]. ويتحقق فعل البقاء سواء كان مستقلا عن فعل الدخول غير المشروع وذلك في الحالة التي يكون الدخول مسموحا به ومع ذلك لايقطع الفاعل الاتصال مع ادراكه أن وجوده داخل النظام والبقاء فيه غير مشروع، أو كان مقترنا بفعل الدخول غير المشروع، أي يكون الفاعل غير مصرح له بالدخول ومع ذلك يدخل إلى النظام ليبقى فيه بعد ذلك[5] ويتحقق في هذا الغرض الإجماع المادي لجريمتي الدخول والبقاء غير المشروع في النظام[6].

وإذا كان الإتجاه الغالب في الفقه يعتبر جريمة الدخول او البقاء سلوك مجرد أي أنها تبدأ وتنتهي بانتهاء السلوك المكون لها دون أن تتطلب أي نتيجه اجراميه إلا أن الفقه لم يتفق على كون هذه الجريمة وقتية أو مستمرة أو متتابعة

---

[1] عائشة نايري، الجريمة الالكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الإداري، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة احمد دراية- ادرار، سنة 2017، ص 28.

[2] الطيبي البركة، المرجع السابق، ص164.

[3] أمال قارة، المرجع السابق، ص 111.

[4] سامي منصور، "الاعمال الاجرامية التي تستهدف الأنظمة المعلوماتية"، د ط، دار المنشورات الحقوقية، بيروت، لبنان، د ت ن، ص 52.

[5] بسمة مامن، "جرائم المساس بانظمة المعالجة الالية للمعطيات في التشريع الجزائري"، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، المجلد 09، العدد 01، 2022، ص 480.

[6] مسعود خثير، المرجع السابق، ص117.

الأفعال[1]، والرأي الراجح أن هذه الجريمه مستمرة، فالجريمه تستمر كلما زادت مدة البقاء غير المشروع داخل النظام المعلوماتي[2].

وفي هذا الصدد تثور اشكالية زمن نهاية جريمة الدخول وبداية جريمة البقاء، اين ذهب رأي من الفقه إلى أن جريمة الدخول تتحق منذ اللحظة التي يتم الدخول فيها فعلا إلى البرنامج، ويبقى مدة قصيرة من الزمن داخله، وبعد تلك اللحظة تبدأ جريمة البقاء وتنتهي بانتهاء حالة البقاء، ويذهب رأي ثاني إلى تحديدها من اللحظة التى يعلم فيها الفاعل أن بقاءه داخل النظام غير مشروع، فيما يذهب رأي أخر وهو الرأي الراجح أن جريمة البقاء تبدأ منذ اللحظة التي بدأ فيها الجاني التجوال داخل النظام، ويستمر في التجول داخله بعد انتهاء الوقت المحدد، أي منذ علم الجاني أنه ليس له حق الدخول، فإذا دخل و ظل ساكنا تبقى الجريمة جريمه دخول إلى النظام، أما إذا بدأ في التجوال فإن جريمة البقاء داخل النظام تبدأ من تلك اللحظة لأنه يتجول في نظام يعلم مسبقا أن مبدأ دخوله واستمراره فيه غير مشروع، ومنذ تلك اللحظة تبدأ جريمة البقاء داخل النظام[3].

بالنسبة إلى الركن المعنوي فإن جريمة الدخول او البقاء تعد من الجرائم العمدية بحيث يكفي فيها توفر القصد العام، ويكفي أن يعلم الفاعل أنه قد دخل إلى نظام ليس له حق الدخول فيه، أو تعمد البقاء فيه رغم انتهاء مده حقه في البقاء فيه ولوكان الدخول مشروعا، أما إذا انتفى علمه فإن الجريمة لا تقوم، كأن يجهل وجود حظر الدخول، او كان يعتقد خطأ أنه مسموح له الدخول فيه. فإذا توافر القصد الجرمي بعنصرية العلم والإرادة، فإنه لا يتأثر بالباعث على الدخول أو البقاء، فيظل القصد الجرمي قائما حتى ولو كان الباعث من الدخول او البقاء الفضول أو التنزه او اثبات القدرة على الانتصار على النظام[4].

والواضح أن المشرع الجزائري لم يكتف بتجريم الدخول أو البقاء غير المشروعين في النظام المعلوماتي بل تجاوز ذلك إلى تجريم مجرد المحاولة وذلك حسب نص المادة 394 مكرر غير ان ما يمكن اثارته في هذا الاطار هوما يتعلق بفكرة الإثبات وما من شأنه اعطاء تصور يفيد بان هناك شروع أو محاولة طالما أن الجريمة في حد ذاتها تطرح اشكالا في الإثبات[5]

[1] امال قارة، المرجع السابق، ص112.
[2] بسمة مامن، المرجع السابق، ص 481.
[3] مسعود خثير، المرجع السابق، ص 117.
[4] علي عبد القادر قهوجي، المرجع السابق، ص 137.
[5] زيدان زيبحة، المرجع السابق، ص 51.

هذا بالنسبة لجريمة الدخول إلى النظام أو البقاء فيه في صورتها البسيطة أما إذا نتج عن الدخول أو البقاء غير المشروع حذف او تغيير المعطيات المنظومة فإن المشرع اعتبر هذه النتيجة ظرفا مشددا تضاعف فيه العقوبة وكذلك هو الشأن في حاله ترتب عن هذه الأفعال تخريب نظام اشتغال المنطومة ويكفي لتوافر هذا الظرف المشدد أن تكون هناك علاقة سببية بين الدخول أو البقاء غير المشروع وبين النتيجة التي تحققت[1].

وإذا كانت الجريمة على هذه الصورة تهدف أساسا إلى حماية نظام المعالجة الألية للمعطيات بصورة مباشرة، إلا أنها تحقق ايضا وبصورة غير مباشرة حماية المعطيات او المعلومات ذاتها.

ثانيا: الاعتداءات على المعطيات

وفر المشرع الجزائري الحماية الجزائية للمعطيات سواء كانت هذه المعطيات داخل النظام وهو ما نص عليه بالمادة 394 مكرر1 أو كانت هذه المعطيات خارج نظام المعالجة وهو ما نصت عليه المادة 394 مكرر 2 .

1- الاعتداءات على المعطيات داخل النظام:

تعتبر جريمة الاعتداء على سلامة المعطيات ثاني جريمة ينص عليها التشريع الجزائري بعد جريمة الدخول و البقاء وهذه الجريمة تطال المعلومات أو البرامج المخزنة داخل النظام المعلوماتي[2].

ويمكن تعريف هذا النوع من الاعتداءات بأنه كل فعل او نشاط يقوم به الجاني في نظام الحاسوب من شأنه الدخول او الازالة أو التعديل في المعطيات المتعلقة بنظام الحاسوب، كما يطلق عليه القرصنة المعلوماتية لأن هدف الجاني فيها هو تحقيق النظام المعلوماتي لنتائج ومعطيات غير تلك التي كان يجب أن يحققها[3].

وينحصر النشاط الاجرامي لهذه الجريمة في أفعال الادخال و المحو و التعديل، ويكفي توافر احداهما لقيام الجريمة، ويعد القاسم المشترك في هذه الافعال انطوائها على تلاعب في المعطيات التي يتضمنها نظام المعالجة البيانات بادخال معطيات جديدة غير صحيحة أو محو أو تعديل[4]، وعليه فإن النشاط الإجرامي لهذه الجريمة ينصب على المعطيات والتي أصبحت رموزا و اشارات وليست المعلومات في حد ذاتها باعتبارها أحد عناصر المعرفة، كما يقتصر على المعطيات الموجودة داخل النظام والتي تشكل جزءا منه وبناء عليه فالجريمة لا تحقق إذا وقع النشاط الاجرامي على المعطيات خارج النظام سواء قبل دخولها أم بعد خروجها[5].

---

[1] انظر المادة 394 مكرر االفقرة 02 و03 من القانون 04-15، المصدر السابق.

[2] رامي حليم، المرجع السابق، ص 344.

[3] سمير بودواب- فؤاد لديوي، جرائم المساس بانظمة المعالجة الالية للمعطيات، مذكرة شهادة ماستر، تخصص قانون جنائي وعلوم جنائية، جامعة 20 اوت 1955، سكيكدة، جوان 2024، ص25.

[4] علي عبد القادر قهوجي، المرجع السابق، ص 143.

[5] مسعود خثير، المرجع السابق، ص 123.

أ- الادخال: يقصد بفعل الادخال اضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خاليه ام كان يوجد عليها معطيات من قبل، وقد يكون بادخال معطيات وهمية الى النظام المعلوماتي بقصد التشويش على صحة البيانات القائمة.

ب-المحو : يقصد به إزالة كل او جزء من المعطيات الموجودة داخل النظام او نقل وتخزين المعطيات إلى المنطقة الخاصة بالذاكرة، ويعتبر المحو جريمة إتلاف طالما وقع ثمة اتلاف او تخريب للشيء موضوع الجريمة و تعطيله ايا كانت الوسيله المستخدمة[1].

ج- التعديل: يقصد بفعل التعديل تغيير المعطيات الموجودة داخل نظام واستبدالها بمعطيات أخرى، ويتحقق فعل المحو والتعديل عن طريق برامج غريبة تتلاعب في المعطيات سواء بمحوها كليا او جزئيا أو تعديلها.

وهذه الأفعال المتمثلة في الادخال و المحو و التعديل وردت على سبيل الحصر، فلا يقع تحت طائلة التجريم أي فعل آخر غيرها حتى ولو تضمن اعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات ، وبهذا فانه لا يخضع لتلك الجريمة فعل نسخ المعطيات أو فعل نقلها أو التنسيق أو التقريب فيما بينهما، لأن هذه الأفعال لا تنطوي لا على ادخال و لا على تعديل بالمعنى السابق[2].

وللإشارة فإن المشرع الجزائري لم يتعرض إلى جريمة الاعتداء القصدى على النظام التي تداولتها العديد من التشريعات ولاسيما التشريع الفرنسي الذي نص على معاقبه كل من عطل او افسد نشاط ووظائف المعالجة الألية للمعطيات[3].

2- الاعتداء على المعطيات خارج النظام

تعد المحافظة على البيانات والمعلومات من اكبر تحديات الأمن السيبراني، وتعتبر الاعتداءات الواقعة عليها من أخطر الجرائم وأكثرها ضررا، خاصة إذا تعلقت هذ المعطيات بأمن الدولة أو الحياة الخاصة ولهذا حرص المشرع الجزائري على مكافحة هذه الجريمة وفرض عقوبات ردعية لها من خلال نص المادة 394 مكرر 2 من قانون العقوبات[4].

---

[1] بسمة مامن، المرجع السابق، ص 485.

[2] امال قارة، المرجع السابق، ص 122.

[3] مسعود خثير، المرجع السابق، ص 120.

[4] محمد خليفة، "الحماية الجنائية لمعطيات الحاسب الالي في القانون الجزائري والمقارن"، ط 3، دار الجامعة الجديدة، الإسكندرية، مصر، د ت ن، ص193.

ويمكن تعريف هذه الجريمة والتي يطلق عليها جريمة التعامل مع المعطيات غير المشروعة على أنها كل أشكال و أنواع التعامل الواقعة و الواردة على معطيات الحاسب الالي السابقة لعملية استعمال هذه المعطيات ارتكاب جريمة ما، بداية من تخطيط المعطيات والبحث فيها وتجميعها وصولا إلى نشرها، من أجل جعلها في متناول الغير أو الإتجار بها[1].

وقد حرص المشرع على توفير الحماية الجزائية للمعطيات في حد ذاتها لانه لم يشترط أن تكون داخل نظام معالجه الية المعطيات أو ان يكون قد تم معالجتها اليا، فمحل الجريمة هو المعطيات سواء كانت مخزنة كأن تكون مخزنة على أشرطة أو أقراص أو تلك المعالجة آليا أو تلك المرسلة عن طريق منظومة معلوماتية ما دامت قد استعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات[2].

وقد جرم المشرع بموجب المادة الفقرة الأولى من المادة 394 مكرر2 من قانون العقوبات مجموعة من الافعال تكون صالحة لارتكاب الجرائم المنصوص عليها في نفس القسم وذلك انها افعال تشكل جزء لا يتجزأ من التحضير لارتكاب احدى هذه الجرائم وتبرز نية الفاعل بالتحضير لها [3]وقد حصر هذه الافعال في التصميم، البحث، التجميع، التوفير، النشر، الاتجار كما جرم بموجب الفقرة الثانية من المادة 394 مكرر 2 من قانون العقوبات أفعال الحيازة، الافشاء، النشر، الاستعمال، بغض النظر عن الغرض من هذه الأفعال التي ترد على المعطيات المتحصل عليها من احدى الجرائم الواردة في القسم السابع مكرر من قانون العقوبات سواء كان الهدف منها المنافسة غير المشروعة، الجوسسة الارهاب ، التحريض على الفسق .. الخ.

ويتحقق الركن المعنوي في هذه الجرائم بالإضافة الى القصد العام المتمثل في العلم و الإرادة القصد الجنائي الخاص و المتمثل في نية الغش[4].

---

[1] عبد العزيز بودراع، خصوصية الجرائم الماسة بانظمة المعالجة الالية للمعطيات، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر، سنة 2011، ص68.

[2] امال قارة، المرجع السابق، ص 123.

[3] عزيزة رابحي، الاسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، سنة 2017، ص 60.

[4] أمال قارة، المرجع السابق، ص ص 123، 126.

الفرع الثالث:

الجزاءات المقررة لجرائم المساس بانظمة المعالجة الالية للمعطيات

نص المشرع الجزائري على مجموعة من العقوبات لهاته الجرائم الماسه بالانظمة المعالجه الالية للمعطيات إذ نص على عقوبات أصلية وأخرى تكميلية كما نص على عقوبة الاشخاص المعنوية كما بالاضافة الاشتراك والشروع في الجريمة.

أولا: العقوبات الأصلية

بالنسبة للعقوبات الأصلية فسيتم تقسيمها وفق هذه الدراسة إلى عقوبات تطبق على الشخص الطبيعي وأخرى على الشخص المعنوي، وهذا ما سيتم تفصيله من خلال ما يلي:

1-بالنسبة للشخص الطبيعي : اعتمد المشرع أثناء وضعه لهاته الجرائم على معيار أساسه الخطورة الجرمية بحيث اتبع مبدأ الهرمية في التدرج في سلم العقوبات، فنص على جريمة الدخول أو البقاء في صورتيها البسيطة والمشددة، تم نص على جريمة الإعتداء العمدى على المعطيات بإعتبارها أشد خطوره من سابقتها باعتبارها تستهدف المعطيات الموجودة داخل النظام، بما في ذلك البيانات والبرامج وغيرها والتي تعتبر بمثابة المحرك الاساسي لهذا النظام والقلب النابض لنظام المعطيات وأي اعتداء عليها سيؤدي لامحالة إلى وقف النظام أو تعطيله وتغيير وجهة سيره[1]، وقد شدد المشرع بموجب آخر تعديل لقانون العقوبات 06/24 في العقوبات المقررة لهذه الجرائم.

أ- عقوبة الدخول أو البقاء داخل النظام:

* **الصورة البسيطة للجريمة:** حدد المشرع العقوبة بالحبس من 06 أشهر إلى سنتين والغرامة من 60.000 دج إلى 200.000 دج[2].

***الصورة المشددة للجريمة:** حدد المشرع العقوبة بضعف العقوبة المقررة للصورة البسيطة في حال ما إذا أدى فعل الدخول أو البقاء إلى حذف او تغيير معطيات المنظومة كما جعل العقوبة من سنة إلى ثلاث سنوات والغرامة من 100.000 دج إلى 300.000 دج إذا أدت الأفعال لتخريب نظام اشتغال المنظومة[3].

---

[1] مسعود خثير، المرجع السابق، ص 126.

[2] المادة 394 مكرر من القانون 24-06 المؤرخ في 28-04-2024 المعدل والمتمم للامر رقم 66-156 المتضمن قانون العقوبات، ج ر ج ج، ع 30.

[3] المادة 394 مكرر من قانون 24-06 المصدر نفسه.

ب- عقوبة الإعتداء العمدي على المعطيات:

حدد المشرع الجزائري عقوبة الإعتداء العمدي على المعطيات داخل النظام بالحبس من سنة إلى 3 سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج[1].

من جهة أخرى حدد المشرع عقوبة الاعتداء العمدي على المعطيات خارج النظام أو ما يطلق عليه جريمة التعامل غير الشرعي مع المعطيات بالحبس من سنة إلى 5 سنوات والغرامة من 1.000.000 دج إلى غاية 5.000.000 دج[2].

كما حدد المشرع العقوبة من سنتين إلى 10 سنوات والغرامة من 700.000 دج الى 2.000.000 دج إذا استهدف الجرائم المنصوص عليها في هذا القسم الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.

2- العقوبات المقررة بالنسبة للشخص المعنوي:

مبدأ مساءلة الشخص المعنوى وارد في المادة 12 من الإتفاقية الدولية للإجرام المعلوماتي، بحيث يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا او شريكا أو متدخلا كما يسأل عن الجريمة التامة أو الشروع فيها كل ذلك بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة أجهزته او ممثليه القانونيين أو الحائزين على تفويض سلطات عندما ينص القانون على ذلك[3].

ثانيا: العقوبات التكميلية

نصت المادة 394 مكرر من قانون العقوبات على العقوبات التكميلية التي يحكم بها إلى جانب العقوبات الأصلية والمتمثلة في:

1- **المصادرة:** وهي عقوبة تكميلية تشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة المعلوماتية مع مراعاة حقوق الغير حسن النية.

2- **اغلاق المواقع:** والأمر يتعلق بالمواقع التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية.

3- **اغلاق المحل أو مكان الإستغلال:** إذا كانت الجريمة قد ارتكبت بعلم مالكها ومثال ذلك اغلاق المقصى الإلكتروني الذي ترتكب فيه مثل هذه الجرائم بشرط توافر عنصر العلم لدى مالكه[4].

---

[1] المادة 394 مكرر 1 من 24-06 المصدر السابق.

[2] المادة 394 مكرر 2 24-06 المصدر نفسه.

[3] انظر المادة 51 مكرر من القانون 24-06 المصدر نفسه.

[4] امال قارة، المرجع السابق، ص 128.

– **المشاركة:** اقر المشرع نفس العقوبة المقررة للجريمة داتها لكل من شارك في مجموعة او في اتفاق تالف بغرض الاعداد لجريمة او اكثر من الجرائم المنصوص عليها في هذا القسم و كان هذا التحضير مجسدا بفعل او عدة أفعال مادية[1].

– **الشروع:** نص المشرع الجزائري على معاقبة الشروع في الجرائم المنصوص عليها في القسم المتعلق بالمساس بانظمة المعالجة الالية للمعطيات و ذلك بنفس العقوبات المقرر للجنحة ذاتها[2].

المطلب الثاني:

النصوص التقليدية كآلية لتحقيق الامن السبيراني

ألقى التطور العلمي لاسيما في مجال تكنولوجيا الاتصالات ضلاله على كل بقاع المعمورة واختلف اسلوب الحياة عما كان عليه وتطور النمط المعيشي كانعكاس ايجابي لهذا التطور، إلا أنه في المقابل تم استغلاله سلبا وأصبح وسيلة وفضاءا جديدين لارتكاب الجرائم، فكان على المشرع أن يواكب هذا التطور بدوره من أجل حماية مصالح الدولة وأمنها وحماية الأفراد واموالهم من جهة أخرى في خضم هذه الثورة التكنولوجية وذلك بتطوير المفهوم التقليدي للجرائم إلى الصورة الحالية والتي أصبحت ترتكب من خلال عالم افتراضي متشابك ومتداخل في جميع أنحاء العالم في محاولة منه لتحقيق أكبر قدر ممكن من الأمن السيبراني وهو ما سنتطرق إليه على النحو التالي:

الفرع الأول:

الجرائم الواقعة على أمن الدولة في الفضاء السيبراني

تهدد الجرائم السيبرانية أمن الدولة ومصالحها على كل المستويات سواء على المستوى السياسي او الاقتصادي أو العسكري، وهنا تكمن خطورة هذا النوع من الجرائم لاسيما تلك المتعلقة بالإرهاب والتجسس.

أولا: الجرائم الموصوفة بأفعال إرهابية أو تخريبية

ترتبت عن ثورة وسائل الاتصالات و تقنية المعلومات بروز مصطلح الإرهاب الالكتروني او ما يطلق عليه الإرهاب الرقمي و ذلك بعد زيادة خطورة الجرائم الإرهابية و تعقيدها بعد ان أصبحت تعتمد على التكنولوجيات الحديثة و وسائل الاتصال المتطورة و هو الامر الذي دعا ثلاثين دولة الى توقيع على اول اتفاقية دولية لمكافحة

[1] المادة 394 مكرر 05 من القانون 04-15 المصدر السابق.

[2] المادة 394 مكرر 07 من القانون 04-15 المصدر نفسه.

الاجرام المعلوماتي في العاصمة المجرية بودابست عام 2001، عقب الهجمات الإرهابية التي تعرضت لها الولايات المتحدة الامريكية في الحادي عشر من شهر سبتمبر من العام نفسه[1].

ولعل من بين ابرز مظاهر الإرهاب الالكتروني استعمال الشبكة المعلوماتية في تبادل المعلومات الإرهابية و نشرها و انشاء مواقع إرهابية الكترونية و تدمير المواقع و البيانات الالكترونية و النظم المعلوماتية و استغلال هذه الأخيرة في التجسس بالإضافة الى التهديد و الترويع الالكتروني[2].

كما أصبحت المجموعات الإرهابية تستخدم تقنية المعلومات لتسهيل الاشكال النمطية من الأعمال الإجرامية، فيتم استخدام الوسائل المتقدمة مثل الإتصالات و الأنترنت للتنسيق وبث الأخبار المغلوطة وتوظيف بعض صغار السن وتحويل بعض الأموال في سبيل تحقيق أهدافهم، كما يقومون باستغلال وسائل تكنولوجيا الإتصال لاستغلال المؤيدين لأفكارهم وجمع الأموال لتمويل برامجهم الإرهابية لا سيما أمام سهولة استخدام هذه التقنيات[3].

والمشرع الجزائري وبمناسبة تعديله لقانون العقوبات سنة 2016 بموجب القانون رقم 16-02[4]اعتبر استخدام تكنولوجيا الإعلام والإتصال لارتكاب الأفعال المنصوص عليها في المادة 87 مكرر 11 جناية يعاقب عليها بالسجن من 05 سنوات إلى 10 سنوات وبغرامة من 100.000 دج إلى 500.000 دج وقد حصر نطاق استخدام تكنولوجيا اللإعلام والإتصال في هذه المادة من حيث السلوك المجرم في الجزائريين أو المقيمين في الجزائر الذين يقومون بالسفر أو محاولة السفر إلى دولة أخرى أو كل من يقوم بتمويل أو تنظيم هذه العملية أو جمع أو توفير أموال بأي وسيلة وذلك بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الاعداد لها أو المشاركة فيها أو التدريب بخصوصها[5]. والملاحظ أن المشرع ربط محل تحقيق الغرض من السلوك اجرامي بدولة أخرى غير الجزائر.

---

[1] علي عدنان الفيل، "الاجرام الالكتروني (دراسة مقارنة)"، منشورات زين الحقوقية، العراق، ط1، 2011، ص 49.

[2] المرجع نفسه، ص 52.

[3] فاطمة اخلاص بن عزوز، وهيبة سالمي، الاليات القانونية لمكافحة الجرائم الماسة بالامن الالكتروني، مذكرة ماستر في الحقوق تخصص القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، سنة 2020، ص 23.

[4] لقانون رقم 16-02 المؤرخ في 19 يونيو 2016 المتمم للامر رقم 66-156 والمتصمن قانون العقوبات، ج ر ج ج ع 37 المؤرخة في 22 يونيو 2016.

[5] انظر المادة 87 مكرر 11 من القانون رقم 16-02، المصدر نفسه.

كما أقر نفس العقوبة لمن يستخدم تكنولوجيا الاعلام والإتصال لتجنيد الأشخاص لصالح إرهابي أو جمعية أو تنظيم أو جماعة منظمة يكون غرضها أو تقع أنشطتها تحت القسم المتعلق بالجرائم الموصوفة بأفعال إرهابية أو تخريبية أو بتنظيم شؤونها أو يدعم أعمالها أو أنشطتها و ينشر أفكارها[1].

ثانيا: جرائم الخيانة والتجسس

تعد كلا من أفعال الخيانة والتجسس من الجرائم الخطيرة التي حرص المشرع الجزائري على محاربتها ورصد لها عقوبات زجرية كبيرة تصل حتى عقوبة الاعدام وذلك لمساس هذه الأفعال بأمن الدولة ومصالحها الحيوية، وعلى الرغم من التمييز الفقهي بين الجريمتين إلا أن المشرع الجزائري نص عليهما في نفس القسم الأول من الفصل المتعلق بالجنايات والجنح ضد امن الدولة في المواد من 61 إلى 64 من قانون العقوبات. وباستقراء هذه المواد نجد أن المشرع اعتمد معيار عملي للتفرقة بين الجريمتين والمتمثل في الجنسية، فجنسية الجاني هي الضابط الذي يفصل بين الجريمتين[2] إذ تعتبر الجريمة خيانة إذا كان الجاني جزائريا أو عسكري أو بحار في خدمة الجزائر وتكون الجريمة تجسسا إذا كان الجاني أجنبيا[3].ولا يختلف المفهوم التقليدي والحديث في الجريمتين إلا من حيث الأداة وهي تكنولوجيا المعلومات[4] والإتصال إلا أنه وبالرغم من هذا الإختلاف تبقى العقوبة واحدة في الحالتين.

وبعدم تقدير المشرع الجزائري وتحديده للوسيلة المستعملة في ارتكاب هذه الجرائم بذكر عبارة "بأي وسيلة كانت" فإن الجريمة تقوم في حالة تحقق الركن المادي لها بغض النظر عن الوسيلة المستعملة فيها سواء وسيلة تقليدية كالرسائل والمنشورات أو باستعمال الوسائل الحديثة المبنية على تقنية المعلومات ونظام الاتصالات الالكترونية، وحسنا فعل المشرع خاصة أمام التطور الهائل لهذه الوسائل، والتي استطاعت اختراق كل الحواجز وتمكنت من الاطلاع على اسرار الدول بدون أن تتلقى أي رصد لهذا الاختراق.

---

[1] انظر المادة 87 مكرر 12 من القانون رقم 16-02، المصدر السابق.

[2] لامية عيساني- فطيمة كعال، جريمتي الخيانة والتجسس في أصل القضاء العسكري الجزائري، مذكرة ماستر، تخصص جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق جامعة العربي بن مهيدي، أم البواقي، 2021/2020، ص 60.

[3] انظر المادة 64 من الامر 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات.

[4] عبد الحليم بن بادة- محمد سعد بوحدة، مداخلة بعنوان: جريمة التجسس الإلكتروني نمط جديد من التهديدات السيبرانية الماسة بأمن دول المنطقة- دراسة سياسية قانونية، الملتقى الدولي الأول الموسوم بامن المعلومات في الفضاء الالكتروني الرهانات والتحديات في شمال افريقيا، المنعقد يومي 17 و18 فيفري 2022، كلية الحقوق والعلوم السياسية، جامعة غرداية، ص5.

ففي مجال أنظمة الاتصالات فإن الأقمار الصناعية أصبحت وسيلة في يد الدول المتطورة تكنولوجيا لمراقبة العالم[1]، و تتجلى خطورة هذه التقنية بالنظر إلى احتكارها من طرف بعض الدول المتطورة فقط و صعوبة تفادي الانكشاف لهذه الأقمار التي تستفيد من حرية الملاحة الفضائية لاسيما و أن الفضاء الخارجي لا يخضع لسيادة دولة معينة و عدم إمكانية التحجج بفكرة السيادة لإبطال عمل تلك الأقمار[2]،كما أن التطور التكنولوجي في مجال هواتف النقالة زاد من إمكانية استعمال هذه الأجهزة كوسيلة فعالة للتجسس[3].

ضف الى ذلك استعمال الموجات و الترددات لاسيما ما يطلق عليه بالترددات السرية الدولية في التجسس على قنوات التلفزيون أو شركات الاتصال[4]أما أكثر وسيلة استعمالا للتجسس هي الانترنت و الكمبيوتر و يستعمل في هذا النوع من التجسس برامج خارجية للتجسس بواسطة الانترنت أو دس وحدات ناقلة للبيانات داخل جهاز الكمبيوتر[5]،و هذا ما تصدي له المشرع في المواد من 394 مكرر الى 394 مكرر 8 من قانون العقوبات إلا أنه في حالة كان الغرض من المساس بأنظمة المعالجة الألية للمعطيات هو الخيانة أو التجسس و تحقق اركان هذه الجرائم فإنه هذه الأخيرة تطبق باعتبار هذه الجرائم منصوص عليها بعقوبات أشد طبقا للمواد 32 و 394 مكرر 3 من قانون العقوبات.

وما يجدر التنويه له أنه و بالرغم من أن المشرع الجزائري في هذه الجرائم وسع في الوسائل المستعملة في هذه الجرائم واعتبر تقنيات المعلومات ووسائل الاتصال الحديثة من الوسائل التي تستعمل فيها إلا انه و حرصا منه على تحقيق أكبر حماية ممكنة للأمن السبيراني و الذي يلعب دورا هاما في أمن الدولة أدرج بموجب أخر تعديل لقانون العقوبات وفقا للقانون 06/24 أدرج المواد 63 مكرر و 63 مكرر1 واللتان نصتا على معاقبة كل من يقوم بتسريب معلومات أو وثائق سرية تتعلق بالأمن الوطني أو الدفاع الوطني أو الاقتصاد الوطني عبر وسائل التواصل الاجتماعي بعقوبة تصل حتى السجن المؤبد في حال ارتكاب الفعل من طرف جزائري لفائدة دولة أخرى أو أحد عملائها.

---

[1] الهام بن خليفة– جمال غريسي، التجسس الالكتروني كجريمة ماسة بأمن الدولة في التشريع الجزائري، مجلة دفاتر السياسة والقانون، جامعة ورقلة، المجلد 14، العدد 01، 2022، ص 164.

[2] عبد الحليم بن بادة، محمد سعد بوحادة، المرجع السابق، ص11

[3] المرجع نفسه، ص10.

[4] فتيحة خالدي، "تاثير التجسس الالكتروني على الحق في الخصوصية المعلوماتية"، مجلة البحوث في الحقوق والعلوم السياسية، جامعة تيارت، المجلد 07، العدد 01، سنة 2021، ص308.

[5] عبد الحليم بن بادة، ب محمد سعد بوحادة، المرجع السابق، ص12.

الفرع الثاني:

الجرائم الواقعة على الافراد في الفضاء السبيراني

تسبب الجرائم الواقعة على الأشخاص أضرار للضحايا سواء من الناحية المادية أو المعنوية، وإذا كانت الوسائط الإلكترونية وسيلة لارتكاب هذه الجرائم عبر الفضاء السبيراني فإن انعكاساتها تكون أشد وطأة وهذا راجع لسرعة واتساع رقعة انتشارها وذلك بزيادة عدد المستقبلين أو المطلعين، وهذا ما جعل المشرع الجزائري يتدخل لحماية الأشخاص بصفاتهم العادية أو بصفاتهم المرتبطة بوظائفهم أو لسنهم وحاجتهم للحماية، وذلك إما بالتأكيد على هذه الوسائط كوسيلة لارتكاب الجريمة تارة أو سن عقوبات لردع استعمال هذه الوسائط كجريمة مستقلة تارة أخرى.

أولا: جرائم الإساءة

إن الحماية التي أولاها المشرع الجزائري للحماية من الإساءة عبر الوسائط الإلكترونية عبر قانون العقوبات تهدف الى فرض الهيبة اللازمة لمؤسسات الدولة وتمكينهم من ممارسة مهامهم بكل أريحية من جهة وتهدف الى حماية وصون شرف الأشخاص وكرامتهم.

إذ نجد ان المشرع الجزائري أدرج بمناسبة تعديله لقانون العقوبات لسنة 2020[1] المادة 149 مكرر 3 والتي سعى من خلالها فرض حماية لممرضي الصحة و موظفي و مستخدمي الهياكل والمؤسسات الصحية أثناء تأدية مهامهم أو بمناسبتها من كل اعتداء يمس مهنيتهم أو بالسلامة المعنوية لهم وذلك عن طريق تسجيل مكالمات أو أحاديث أو التقاط صور أو فيديوهات أخبار أو معلومات ونشرها أو أن تسجل المكالمات والأحاديث باستعمال وسيلة لها القدرة على التسجيل سواء كان هاتفا ذكيا أو آلة تسجيل[2] وذلك على موقع أو شبكة إلكترونية أو في مواقع التواصل الاجتماعي أو بأي وسيلة أخرى[3].

أما بالنسبة لجرائم الإساءة ضد الأفراد العاديين عبر الوسائط الإلكترونية فإنه بالرغم من نص المشرع على هذه الجرائم لاسيما جرائم السب والتهديد والقذف إلا أنه لم يأت بأحكام جديدة تتوافق مع طبيعة الجرائم السيبرانية

---

[1] بموجب القانون 20-01 المؤرخ في 30 يوليو 2020 المعدل والمتمم للامر رقم 66-156 المتضمن قانون العقوبات، ج ر ج ج العدد 44.

[2] كريم بوزيان، "الحماية الجزائية لمستخدمي الصحة في ظل قانون العقوبات لسنة 2020"، مجلة الدراسات القانونية والمقارنة، جامعة المدية، المجلد 07، العدد 01، سنة 2020، ص 2027.

[3] أنظر المادة 149 مكرر 3 من القانون 20-01 المصدر السابق.

مكتفيا بالنصوص التقليدية[1] من حيث الأركان، والتي يمكن أن يتم اسقاطها على هاته الجرائم في حال ارتكابها عبر شبكة الإنترنت بواسطة الخدمات المتاحة للشبكة وبالامكان الإطلاع عليها من طرف المستخدمين ومستعملي الشبكة فور التعرف على عنوان الموقع ذلك ان نشرها يصبح مفترضا[2]، إلا أنه ومن حيث العقوبة فإن المشرع الجزائري في آخر تعديل له لقانون العقوبات بموجب القانون 06/24 ضاعف العقوبات المقررة لهذه الجرائم عندما ترتكب أو يسهل ارتكابها استعمال تكنولوجيات الإعلام والاتصال[3].

أما إذا كانت طريقة الإرسال من قبل المراسلات الخاصة والتي يمكن للمجني عليه وحده رؤية أو سماع ما وجه إليه فإن الجريمة لا تقوم لانتفاء ركن العلنية الذي تقوم عليه[4] جرائم القذف والسب في حين تقوم في باقي الجرائم إذا توافرت أركانها مثل التهديد.

وما يمكن إثارته حول هذه الجرائم المرتكبة عبر الفضاء السيبراني هو صعوبة إثبات اسناد الفعل للجاني في الكثير من الأحيان كحالة غلق الحساب أو عدم اتاحته في مرحلة التحقيق كما أثار إشكالية الاختصاص القضائي وكذا تكييف الأفعال الذي يختلف من بلد الى آخر[5].

ثانيا: الجرائم الماسة بحرمة الحياة الخاصة

يعد الحق في الحياة الخاصة أحد أبرز الحقوق الملازمة لحياة الأفراد، لما لها من أثر عظيم في تحقيق كرامتهم الإنسانية ويشمل الحق في الحياة الخاصة حرمه المسكن، سرية الاتصالات وحماية حياته من أي تدخل خارجي، وهذا الحق كرسته المواثيق الدولية المتعلقة بحقوق الإنسان باعتبار هذا الحق من الحقوق الأساسية له، كما سعت التشريعات الداخلية لتكريس هذا الحق وهو ما فعله المشرع الجزائري بدءا بتوفير الحماية الدستورية له وذلك بضمان هذا الحق دستوريا ومن ثم توفير الحماية الجزائية له وذلك من خلال قانون العقوبات. وبازدياد التطور العلمي في مجال تكنولوجيا الإعلام والاتصال ازدادت حاجة الأفراد لهذه الحماية نظرا للاستعمال الشائع لهذه التقنيات وسهولتها مما يجعلهم يتداولون كمية كبيرة من البيانات والمعلومات الشخصية لاسيما الصور الشخصية والأحاديث وبالمقابل

---

[1] مهدي رضا، "الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة إيليزا للبحوث والدراسات، المركز الجامعي اليزي، المجلد 06، العدد 02، سنة 2021، ص 117.

[2] زيدان زيبحة، المرجع السابق، ص 83.

[3] أنظر المادة 333 مكرر 6 من 24-06 المصدر السابق.

[4] عبد الصمد بودخيل، جريمة القذف على مواقع الانترنت، مذكرة ماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة مولاي الطاهر-سعيدة، سنة 2020، ص 18.

[5] زيدان زيبحة، المرجع السابق، ص 83.

عجزت الانترنت عن توفير الأمان اللازم والسرية التامة للحفاظ على ما يتداول عبرها، ومن جهة أخرى فإن تطور وسائل الاتصال الحديثة جعلها وسيلة للمساس بحرمة الحياة الخاصة نظرا للقدرات الكبيرة التي تتمتع بها هذه الأجهزة.

وحتى يضمن المشرع الجزائري ممارسة الحق المنبثق من القواعد الدستورية والقانونية المتعلقة به اتجه إلى تجريم الأفعال والتي من شأنها أن تضر سلامة المصالح الفردية والجماعية المتصلة به[1]. وذلك من خلال تعديله لقانون العقوبات بموجب القانون رقم 06-23[2]، ولعل هذه الجرائم تجد مجالها الخصب في البيئة الرقمية لسهولة القيام بالفعل المادي لها، وهذا ما جعل المشرع يتدخل في التعديل بموجب القانون 24-06 مصيفا لأحكام جديدة وخاصة تتلائم مع طبيعة المجال السبيراني ولاسيما الانتشار الواسع لهذه الجرائم عبره في الآونة الأخيرة، إذ أضاف أحكاما جديدة متعلقة بالتجريم و أحكاما أخرى متعلقة بالعقوبات سواء الأصلية أو المكملة.

إذ جرم المشرع الجزائري كل التقاط أو حصول على صور أو فيديوهات أو رسائل الكترونية أو أي معلومات خاصة لأي شخص بغض النظر عن الطريقة المستعملة و القيام بعد ذلك بإذاعتها أو نشر محتواها دون إذن صاحبها ورضاه، بل إن الجريمة تقوم حتى في حالة التهديد بذلك حتى بدون إتمام الفعل بالنشر أو الإذاعة[3]، وأقر عقوبة الحبس من سنة إلى 5 سنوات والغرامة من 100.000 دج إلى 500.000 دج كما جرم استعمال الصور الالكترونية للغير أو تحويرها أو نقلها أو نسخها، أو نشرها قصد الاضرار به وشدد في العقوبة إذ جعلها بالحبس من 3 سنوات إلى 7 سنوات.

وبتجريم الأفعال المتعلقة بنشر الصور والرسائل الالكترونية يكون قد أضفى حماية للأشخاص عند استعمال وسائل الاتصال الالكترونية باعتبار الاعتداء على الصور الشخصية والمحادثات من أخطر أنواع الانتهاكات التي يمكن أن تقع على الحياة الخاصة[4]، ويسبب في بعض الأحيان أضرار وخيمة للشخص الذي يكون ضحية هذه الأفعال،كما أن الاعتماد على النصوص التقليدية لاسيما المادة 303 مكرر كان غير كاف ذلك ان قيام الجريمة

[1] فتيحة حزام، "الحق في الحياة الخاصة بالبيئة الرقمية دراسة مقارنة"، مجلة الدراسات القانونية المقارنة، جامعة الشلف، المجلد 08، العدد 01، 2022، ص634.

[2] قانون 06-23 المؤرخ في 30 ديسمبر 2006 المعدل والمتمم للامر رقم 66-156 المتضمن قانون العقوبات، ج ر ج ج العدد 84.

[3] انظر المادة 333 مكرر 4 من قانون 24-06 المصدر السابق.

[4] كوثر مختاري، الاعتداء على الحياة الخاصة على شبكات التواصل الاجتماعي، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2018، ص36.

مقيد بمعيار موضوعي يتعلق بالمكان الذي التقطت فيه هذه الصورة ولا تقوم الجريمة الا إذا كان هذا المكان خاصا[1]، وهو ما لا يتلائم مع طبيعة هذه الجريمة في البيئة السبيرانية.

من جهة أخرى فإن نقل هذه الصور يمكن شخص آخر الإطلاع عليها كإرسال صور لشخص من أحد حسابات شبكات التواصل الاجتماعي إلى حساب شخص آخر بغرض الإضرار بصاحبها و هو ما يشكل خطر كبيرا على خصوصية الشخص و انعكاسا سلبيا عليه لما لهذا الفعل من تأثير في تشويه سمعته أو استغلال لهذه الصورة لأغراض غير مشروعة أو حتى استغلال هذا الشخص بواسطة ابتزازه أو تهديده[2].

كذلك استحدث المشرع الجزائري في هذا التعديل فعل التحوير الصور، ويكون هذا الفعل بإجراء تعديلات وتغيرات على الصور كإحداث تغييرات على ملامح الشخص أو إضافة أشخاص إلى الصور وهو من أخطر الأفعال التي يمكن أن تضر بالأشخاص، ذلك أن هذه التعديلات يمكن لها تغيير هذه الصورة بشكل سيء للفرد ويظهرها عكس الحقيقة وهو ما قد يؤدي إلى خلق انطباعات خاطئة لدى الجمهور عن هذا الشخص[3].

من ناحيتها المراسلات تعتبر ترجمة مادية لأفكار شخصية ولآراء خاصة لا يجوز لغير مصدرها ومن توجه إليه الإطلاع عليها وفي حالة الإطلاع عليها من قبل الغير يعتبر انتهاكا لحرمة المراسلات وبالتالي انتهاكا لحرمة الحياة الخاصة، ذلك أن الرسالة قد تكون مستودعا لسر الإنسان وخصوصياته[4] لهذا حرص المشرع الجزائري على حماية هذه المراسلات من كل التقاط أو تسجيل أو نقل بدون إذن صاحبها أو رضاه بموجب المادة 303 مكرر من قانون العقوبات وإذا كان الأمر يتعلق بإذاعة أو نشر محتوى رسائل الكترونية فإن المشرع خصها بحماية خاصة وجعلها لها عقوبات أكثر ردع بموجب المادة 303 مكرر 04 من نفس القانون.

وقد شدد القانون العقوبة عن هذه الأفعال وجعلها مضاعفة في حال صاحبتها ممارسة ضغوطات على منفعة مادية أو خدمة أو أي مقابل آخر مباشر أو غير مباشر[5].

كما أن المشرع ونظرا لطبيعة العلاقة الناشئة عن الزواج والخطبة فإنه أقر عقوبة كبيرة بالحبس من 05 إلى 10 سنوات والغرامة من 500.000 دج إلى 1.000.000 دج لكل زوج أو خاطب أو خاطب أو مخطوبة يقوم

---

[1] عباسية زروقي، "جرائم الاعتداء على الحياة الخاصة عبر شبكات التواصل الاجتماعي وآليات الحماية"، مجلة القانون والعلوم السياسية، المركز الجامعي النعامة، المجلد 08، العدد 02، 2022، ص15.

[2] العيد زروال، عثمان نغزة، جريمة انتهاك الحياة الخاصة عبر الانترنت، مذكرة ماستر، تخصص قانون الإعلام الآلي والانترنت، كلية العلوم السياسية والحقوق، جامعة محمد البشير الإبراهيمي، سنة 2022، ص34.

[3] رشيد شميشم، "الحق في الصورة"، مجلة البحوث والدراسات العلمية، جامعة المنيعة، العدد الثالث، ديسمبر 2009، ص11.

[4] كوثر مختاري، المرجع السابق ص41.

[5] انظر المادة 333 مكرر 4 من قانون 24-06 المصدر السابق.

بإذاعة أو نشر صورة خادشة للطرف الآخر سواء ارتكب الفعل أثناء قيام الرابطة الزوجية أو الخطوبة أو بعد انتهاء هذه الرابطة

بالإضافة إلى العقوبات الأصلية أقر المشرع الجزائري عقوبات تكميلية جديدة لهذه الجرائم والمتمثلة في:

- مصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب هذه الجرائم، والأموال المتحصلة منها.
- إغلاق الموقع الالكتروني أو الحساب الالكتروني الذي ارتكبت بواسطته الجريمة أو جعل الدخول إليه غير ممكن.
- إغلاق محل أو مكان الاستعمال إذا كانت الجريمة ارتكبت بعلم مالكه.[1]

الفرع الثالث:

الجرائم الواقعة على الاموال في الفضاء السبيراني

لم تقتصر أساليب الإساءة واستخدام الثورة التقنية على الاعتداء على أمن الدول والاعتبار للأشخاص بل تعدتها للذمة المالية للأشخاص، هذه الأخيرة التي تكفلت التشريعات القانونية بحمايتها[2]، إلا أن اختلاف الطبيعة القانونية للمال المعلوماتي طرح عدة إشكالات من حيث مدى إمكانية تطبيق النصوص التقليدية المتعلقة بجرائم الأموال على هذا النمط المستحدث من الجرائم، خاصة أمام تقيد القاضي الجزائري بمبدأ الشرعية الجزائية والذي يمنعه من تجريم أفعال لم ينص عليها القانون[3].

فالمال المقصود بمحل الاعتداء في جريمة السرقة التقليدية مثلا هو كل شيء قابل أن يكون محلا للسرقة بشرط أن تكون له قيمة سواء تجارية أو مادية أو أدبية[4]، أما المال المعلوماتي فيقصد به الحاسوب بكل مكوناته وهو يعتبر مجموعة من الكيانات التي تسمح بدخول المعلومات ومعالجتها وتخزينها واسترجاعها عند الطلب، ويتكون من كيان مادي وكيان معنوي، فأما الكيان المادي فهو يضم الأجهزة المادية المختلفة وهي جهاز الإدخال وجهاز الإخراج ووحدات التشغيل المركزية، ولا يحتاج هذا الكيان لنصوص خاصة لحمايتها جزائيا لاحتوائها من النصوص التقليدية إلا أن المشكل يثور حول الكيان المعنوي الذي يشمل البرامج المختلفة التي تتحقق من خلالها قيام الحاسب بوظائفه المختلفة بالإضافة إلى المعلومات المطلوب معالجتها[5].

---

[1] المادة 333 مكرر 7 من قانون 24-06 المصدر السابق.

[2] محمد أمين الشوابكة، "جرائم الحاسوب والانترنت (الجريمة المعلوماتية)"، دار الثقافة للنشر والتوزيع، ط 1، الأردن، 2009، ص136.

[3] أمين طعباش، "الحماية الجنائية للمعاملات الالكترونية"، مكتبة الوفاء القانونية، مصر، ط1، 2015، ص107.

[4] أحسن بوسقيعة، الوجيز في القانون الجزائري الخاص، ط 10، دار هومة للنشر والتوزيع، الجزائر، د ت ن، ص267.

[5] آمال قارة، المرجع السابق، ص15.

فالنظرة التقليدية لجرائم الأموال تحصر محل الجريمة على الأشياء المادية، نظرا لشيوع هذه الأخيرة وندرة الأشياء غير المادية (المعنوية) في الماضي، إلا أنه بعد التطور المتزايد للأشياء المعنوية والتي أصبحت أكبر عددا، ويفوق بعضها في قيمته الأشياء المادية استدعى الأمر إعادة النظر في حصر الأموال في الأشياء المادية والبحث عن معيار آخر حتى يمكن اسباغ صفة المال على الأشياء المعنوية[1].

ومن هذه الأشياء المعنوية ذات القيمة الاقتصادية العالية برامج الحاسب الآلي، والتي تكون عادة مثبتة على دعامة أو حامل مثل الأقراص أو الشرائط الممغنطة من البلاستيك أو أي مادة أخرى فإذا وقع الاعتداء على الدعامة في هذه الحالة يكون واقعا على شيء مادي مما يصلح تكيفه حسب النشاط الإجرامي بإحدى جرائم الأموال والتي يتطابق نموذجها مع هذا النشاط، أما إذا وقع اعتداء على شيء معنوي فلابد أن تثبت له صفة المال أولا[2].

وفي هذا الصدد ظهر اتجاهين:

الاتجاه الأول: الاتجاه المعارض لإعطاء المعلومات والبرامج وصف المال

يرى هذا الاتجاه أن المعلومات لا يمكن أن تكون محلا لجريمة السرقة لأنها ليست مالا وهذا بالتسليم بالطبيعة الذاتية للمعلومة وهذا الرأي هو نتيجة لتطبيق المنهج التقليدي الذي يضفي وصف المال على الشيء المادي وحده[3].

ويستند هذا الرأي إلى أن المعلومة في حالتها المجردة والفكرة في حد ذاتها لا تقبل التملك والاستئثار وأن تداولها والانتفاع بها من حق الكافة دون تمييز ومن ثم لا يمكن أن تكون محلا للملكية الفكرية، ويفرق البعض بين المعلومات والبيانات التي لم يتم معالجتها الكترونيا على اعتبار عنصرها الأساسي هو الدلالة لا الدعامة التي تجسدها فلها طبيعة غير مادية ولا سبيل لاختلاسها أما البيانات التي تمت معالجتها فتتحد في كيان مادي يتمثل في نبضات أو إشارات الكترونية ممغنطة يمكن تخزينها على وسائط معنية ونقلها واستغلالها وإعادة انتاجها فضلا عن إمكانية تقديرها كميا وقياسها، بمعنى أن المعالجة تحول المعلومات من أموال معنوية إلى أموال مادية وبالنتيجة خضوعها للنصوص التقليدية لجرائم الأموال كما يفرق هذا الاتجاه بين سرية المعلومة وعدم سريتها ذلك أن الحصول عليها إذا

[1] مسعود خيثر، المرجع السابق، ص37.

[2] آمال قارة، المرجع السابق، ص16.

[3] طعباش أمين، المرجع السابق، ص117.

كانت غير سرية يعد من قبيل الحصول على جهد الآلة بغير مقابل وبغير رضا صاحب الحق في اقتضائه مقابل ذلك لأن جهد الآلة ما هو إلا خدمة نتاج لقاء مقابل مادي[1].

الاتجاه الثاني: الاتجاه المؤيد لإعطاء المعلومات والبرامج وصف المال

يرى جانب من الفقه الحديث إلى اعتبار الشيء مالا ليس بالنظر إلى كيانه المادي وإنما على أساس ماله من قيمة أو منفعة اقتصادية وذلك ما يتجسد في المعلومة[2].

ويستند هذا الجانب من الفقه على أن المعلومات صالحة لأن تكون محلا للاعتداء عليها طالما كانت هذه المعلومات تعكس الرأي الشخصي لصاحبها ولا تتوقف عن نطاق المعلومات العامة وهذا يعني أنها من الحقوق اللصيقة بشخصية صاحبها فالمعلومات باعتبارها نتاجا ذهنيا لمن يعطيها شكل المعلومة فهي تعد محور العلاقات مثل تلك التي تنشأ بين المالك وبين ما يملك، فيكون له نقلها أو إيداعها وحفظها وتأجيرها وبيعها وما دامت البرامج في جوهرها معلومات معالجة بطريقة ما ولها قيمة اقتصادية فإنه يجب معاملتها على أنها مال[3]. وسنحاول فيما يلي تطبيق بعض النصوص التقليدية المتعلقة بجرائم الأموال على المعلومات.

اولا: بالنسبة لجريمة السرقة

طبقا للمادة 350 من قانون العقوبات "**كل من اختلس شيئا غير مملوك له يعد سارقا**"، لم يشترط المشرع الجزائري أن يكون الشيء موضوع الجريمة ماديا، مما يجعل وقوع الجريمة السرقة على شيء معنوي أمرا لا يصطدم بمبدأ شرعية الجرائم والعقوبات[4] خاصة وأن المشرع الجزائري جرم فعل اختلاس الكهرباء على الرغم أنه ليس له طبيعة مادية[5].

إلا أن تطبيق جريمة السرقة على برامج الحاسب الآلي والمعلومات بصفة تصادفه العديد من العقبات فالجاني وإن كان يدخل في ذمته ما استولى عليه من برامج إلا أنه في نفس الوقت لم تخرج هذه البرامج و المعلومات من ذمة صاحبها الشرعي إذ تظل رغم مباشرة الأفعال عليها تحت حيازة صاحبها في حين أن جريمة السرقة تقتضي نقل حيازة المال موضوع الاختلاس والسرقة من حيازة المجني عليه إلى الجاني، ضف إلى ذلك صعوبة تصور فعل الاختلاس

---

[1] مسعود خيثر، المرجع السابق، ص41.

[2] طعباش أمين، المرجع السابق، ص120.

[3] آمال قارة، المرجع السابق، ص17، 18.

[4] سارة عرفة–سليمة طابون، تكليف الجريمة الالكترونية في التشريع الجزائري مذكرة ماستر، تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، سنة 2021 ص13.

[5] انظر المادة 350 فقرة 2 من القانون 06-23، المصدر السابق.

الذي هو من طبيعة مادية على شيء معنوي والمتمثل في المعلومات[1] وهو ما أدى إلى ظهور جدال فقهي حول الكثير من صور التي يتم بها فعل الاختلاس في مجال المعاملات الالكترونية كصورة الالتقاط الذهني للبيانات وذلك ببقاء المعلومات في ذاكرة الإنسان اثر مطالعتها بالبصر أو بعد وصولها إلى الإذن، فعلى الرغم من أن بعض الفقه اعتبر أن هذا الفعل تحت طائلة العقاب بالسرقة على الرغم من صعوبة اثباته إلا أن البدء في قبول وجود جرائم تتمثل ماديتها في محض نشاط ذهني من شأنه فتح المجال أمام التسلل إلى دخائل الفرد والعقاب على ما يدور في الأذهان أو يعيش بالصدور من الأفكار والآراء وهو أمر ليس مقبول.

كما اعتبر اغلبية الفقه بأن الموجات والاشعاعات المنبعثة من الأجهزة المعلوماتية حال تشغيلها وإن صلحت بسبب تجسدها في صورة مادية كهرومغناطيسية لأن تكون محلا للسرقة إلا أن التقاطها لا يتحقق به معنى إنتزاع أو سلب الحيازة فلا تقع بذلك جريمة السرقة لانتقاء أحد عناصر ركنها المادي[2].

وفي هذا الصدد قضت محكمة باريس فيما يتعلق بالاختلاس الناتج عن الالتقاط غير المشروع الوارد بقضية قناة تلفزيونية في فرنسا، أن جريمة السرقة لا تتوافر عناصرها كون التوصيل غير المشروع لالتقاط برامج هذه القناة لم يكن من شأنه أن يغل يد المالك أي صاحب البرنامج[3].

كذلك المعلومات والبيانات المخزنة الكترونيا ثار جدل حول مدى قابليتها للسرقة لانتقاء الصفة المادية لهذه البيانات وفي هذا الشأن أدانت محكمة النقض الفرنسية المتهم بالسرقة ليس لقيامه بالتصوير، وإنما لاستيلائه على المستند الأصلي أثناء المدة اللازمة لاستنساخه، وبذلك تكون حافظت على شرط توافر الصفة المادية في محل السرقة.

ثانيا: بالنسبة لجريمة النصب

يعرف الاحتيال في نطاق المعلوماتية على أنه كل سلوك احتيالي يرتبط بعملية التحسيب الإلكتروني بهدف كسب فائدة أو مصلحة مالية[4]، وقد تطرق المشرع الجزائري الى جريمة النصب في نص المادة 372 من قانون العقوبات إلا أنه لم يتطرق الى النصب الواقع في مجال المعاملات الإلكترونية وعلى الرغم من إجماع غالبية الفقه على صلاحية المكونات المادية وكذا البرامج والبيانات بأن تكون محل جريمة النصب بشرط أن تكون على دعامات مادية

[1] علي عبد القادر القصوجي، المرجع السابق، ص95.
[2] آمال قارة، المرجع السابق، ص23، 25.
[3] طعباش أمين، المرجع السابق، ص129.
[4] محمد الأمين الشوابكة، المرجع السابق، ص 180.

فتكون هذه الأخيرة محلا أو موضوعا للجريمة نظرا لطبيعتها المادية، فإنه تم الاختلاف حول مدى صلاحية المعلومات الموجودة على الأجهزة أو الموجودة على الدعامات المادية وليست الدعامة ذاتها لان تكون محلا لجريمة النصب[1].

وقد حصر المشرع الجزائري محل الجريمة في الأموال أو المنقولات أو سندات تصرفات أو أوراقا مالية أو وعودا أو مخالصات أو البراء من التزامات[2]، و في هذا الصدد قد تم الانقسام على النحو التالي:

الاتجاه الأول: الاتجاه المعارض لصلاحية المعلومات كمحل جريمة النصب

وأسس هذا الفريق رأيه على أساس عدم وجود نشاط مادي ملموس يحصل به التسليم والاستلام ولعدم ترتب على الفعل حرمان المجني عليه من حيازة هذه البرامج والبيانات التي تبقى تحت سيطرته التامة[3]، كما يرى البعض أن جريمة النصب لا تقوم إلا إذا خدع شخص شخصا مثله وأن يكون المخدوع مكلفا بمراقبة البيانات وعلى ذلك لا يمكن خداع الحاسب الآلي بوصفه آلة ومن ثم عدم إمكانية تطبيق النص الجنائي الخاص بالنصب على الوقائع لافتقاره أحد العناصر اللازمة لتطبيقه[4].

الاتجاه الثاني: الاتجاه المؤيد لصلاحية المعلومات كمحل جريمة النصب

وقد استدل أصحاب هذا الرأي على أن خداع النظام المعلوماتي لسلب مال الغير تتحقق به الطرق الاحتيالية بمفهومها ككذب تدعمه أعمال مادية أو وقائع خارجية سائدة وهي إبراز وتقديم المستندات المعلوماتية التي تدخل الى النظام المعلوماتي[5]، كما استدل رأي آخر الى أن المعيار الأساسي لجريمة النصب يتمثل في المحاولة التدليسية وذلك باستخدام أساليب فنية من قبل الجاني أثناء تشغيل الجهاز، ويرجع ذلك الى الطبيعة الذاتية الخاصة لهذه الجريمة في نطاق المعاملات الإلكترونية[6]، ففي المجال المعلوماتي تتوافر الخبرة الفنية وتتنوع الأساليب التكنولوجية في خداع النظام المعلوماتي وكيفية الحصول على الهوية واختلاسها وإنتحال صفة صاحبها للحلول محله في العمليات الإلكترونية

[1] مسعود خثير، المرجع السابق، ص 56.
[2] أنظر المادة 372 من الامر 66-156 المصدر السابق.
[3] علي عبد القادر القهوجي، المرجع السابق، ص 34.
[4] طعباش أمين، المرجع السابق، ص 154.
[5] مسعود خثير، المرجع السابق، ص 57.
[6] طعباش أمين، المرجع السابق، ص 153.

وباختلاس الهوية يمكن الحصول على المستخرجات والنتائج العمليات الأولية[1]، كما أن الطبيعة المعلوماتية لجرائم الحاسب الآلي لا تضيف جديد في مجال النصب التقليدي إلا مجرد الوسيلة المستخدمة.

بقيت مسألة خضوع فعل الاحتيال المعلوماتي للتجريم بواسطة النص التقليدي محل جدل وحتى على المستوى الوطني لم يتم حسم هذه المسألة فهناك من يرى أن سكوت المشرع الجزائري عن استحداث نصوص تتعلق بالنصب المعلوماتي فإنه يساير بذلك الاتجاه التقليدي المعارض لقيام جريمة النصب في هذه الأفعال[2]، وأن جريمة النصب على الكمبيوتر لا تتفق مع طبيعة النشاط الإجرامي في جريمة النصب حتى وإن اتفق ذلك مع طبيعة البرامج والمعلومات[3] في حين يرى جانب آخر أنه لا يوجد ما يحول دون وقوع البرامج والبيانات تحت طائلة نص المادة 372 من قانون العقوبات سواء باعتبارها أموالا أو منقولات[4].

ولعل تدخل المشرع في هذا المجال أصبح لازما من أجل وضع حد لعمليات النصب عبر الفضاء السيبراني والتي عرفت في الآونة الأخيرة تفشي كبير وذلك بالاعتماد على طرق متعددة لاسيما سرقة هويات متسوقي المتاجر الالكترونية او بطاقاتهم الائتمانية و استعمال بياناتهم الشخصية في عمليات شراء عبر الانترنت مما ينجر عنه تحمل تكاليف سلع و خدمات على عاتق أصحابها الفعليين، و زيادة خطر قرصنة بطاقات الدفع الالكتروني و المعطيات الشخصية لاسيما عبر الرسائل الالكترونية مجهولة المصدر و المواقع المزيفة و التطبيقات الالكترونية او البرمجيات غير الموثوقة [5].

---

[1] عمر أبو الفتوح عبد العظيم الحطامي، "الحماية الجنائية للمعلومات المسجلة إلكترونيا"، دراسة مقارنة، د.ط، دار النهضة العربية، القاهرة، 2010، ص 645.

[2] طعباش أمين، المرجع السابق، ص 154.

[3] مسعود خثير، المرجع السابق، ص 59.

[4] آمال قارة، المرجع السابق، ص 31.

[5] الدليل الارشادي الخاص بالتجارة الالكترونية جانفي 2024، الموقع الرسمي لوزارة البريد والمواصلات السلكية واللاسلكية mpt.gov.dz تاريخ الاطلاع 01-06-2025 الساعة 05:03.

المبحث الثاني: الاليات الموضوعية لتحقيق الامن السيبراني بموجب القوانين الخاصة

استحدث المشرع الجزائري العديد من النصوص الجديدة منها التي يهدف من خلاله الى تحقيق الامن السيبراني بالنظر الى موضوع الحماية و هو المعطيات ذات الطابع الشخصي و ذلك من خلال القانون رقم 18-07 و الذي خطى بها خطوة جبارة في مجال حماية الافراد و خصوصياتهم عند معالجة بيناتهم الشخصية، و الكثير من النصوص الأخرى يهدف من خلالها الى تحقيق الامن السيبراني ونتطرق لاهمها وهي تلك المتعلقة بمجال الاتصالات الالكترونية، مجال الملكية الفكرية و مجال التوقيع و التصديق الاكترونيين

المطلب الاول:

حماية المعطيات ذات الطابع الشخصي كآلية لتحقيق الامن السيبراني

لقد أفرز التطور العلمي والتكنولوجي الذي يعد أحد مظاهر العصر الحديث ثورة في الاتصالات والمعلومات، وأتاح فرصة جديدة للإطلاع على المعلومات وتبادلها وهو ما صاحبه خطورة الانتهاك غير المشروع للبيانات الشخصية، فسارعت الجهود الدولية والوطنية لإيجاد قواعد تفرض التوازن بين حاجات المجتمع لجمع وتخزين ومعالجة البيانات الشخصية وحماية هذه البيانات من التهديدات والاستعمال الغير المشروع لها، وهو ما دفع المشرع الجزائري للسعى الى وضع إطار قانوني لحماية هذه المعطيات وإرساء القواعد اللازمة لضمان احترام الحياة الخاصة للأشخاص وهو ما كرسه في القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

الفرع الأول:

المبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي

قبل الخوض في المبادئ الأساسية التي سنها المشرع الجزائري في الباب الثاني من القانون رقم 18-07 فانه يتعين ابراز مفهوم المعطيات ذات الطابع الشخصي وكذا مفهوم معالجة هذه المعطيات حتى يمكننا حصر نطاق هذا القانون.

ومن جهة أخرى فإن مقتضيات الأمن السبراني تفرض اعتماد قواعد واضحة لما يعتبر بيانات شخصية بغية تأمين الحماية اللازمة وقد عرفها المشرع الجزائري على أنها كل معلومة بغض النظر عن دعامتها متعلقة بشخص

معرف أو قابل للتعريف بصفة مباشرة أو غير مباشرة، لا سيما بالرجوع الى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية[1].

وعلى ذلك فإن المعطيات ذات الطابع الشخصي هي كل معلومة تدل على الشخص مباشرة أو عن طريق معالجتها أو تحليلها سواء كانت على دعامة ورقية أو إلكترونية أو غيرها ما عدا تلك المعلومات المتعلقة بالحياة العامة[2].

كما أورد المشرع تعريف معالجة البيانات ذات الطابع الشخصي وذلك انطلاقا من نوعية العمليات التي تطال البيانات مع المساواة بين اليدوي منها والآلي، مشيرا الى أمثلة عن هذه العمليات وذلك على النحو التالي: كل عملية أو مجموعة عمليات منجزة بطرق أو بوسائل آلية أو بدونها على معطيات ذات طابع شخصي، مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو الملاءمة أو التغيير أو الاستخراج أو الاطلاع أو الاستعمال أو الإيصال عن طريق الإرسال أو الشراء أو أي شيء آخر من أشكال الإتاحة أو التقريب أو الربط البيني وكذا إغلاق أو التشفير أو المسح أو الإتلاف[3].

وأشار المشرع الجزائري أيضا الى بيانات وصفها بالحساسة كفئة من البيانات الشخصية بشكل عام، نظرا لارتباطها المباشر بحقوق إنسانية وحريات أساسية تقرها مواثيق دولية وقوانين أساسية كالدساتير[4]. وهذا التعريف جاء على النحو التالي: هي معطيات ذات طابع شخصي يبين الأصل العرقي أو الاثني أو الأراء السياسية أو القناعات الدينية أو الفلسفية أو الانتماء النقابي للشخص المعني أو تكون متعلقة بصحته، بما في ذلك معطياته الجينية[5]. وهي نفسها التي عرفها الفقه بأنها البيانات الشخصية التي تبنى على العرق أو الأصل أو الانتماءات الدينية أو الفلسفية أو السياسية أو الحياة الصحية أو الجنسية أو البيانات المتعلقة بالملاحقات الجنائية والإدانات[6].

---

[1] المادة 03 من القانون رقم 18-07 المؤرخ في 10-06-2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر ج ج عدد 34 المؤرخة في 10-06-2018.

[2] محمد العيداني، يوسف زروق، "حماية المعطيات الشخصية في الجزائر على ضوء القانون رقم 18-07"، مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي تندوف، العدد 5، ديسمبر 2018، ص 119.

[3] أنظر المادة 03 من القانون 18-07 المصدر السابق.

[4] خليفة بوداود، السعيد بوزيان، "معالجة المعطيات ذات الطابع الشخصي بين الضمانات القانونية الدولية والداخلية،" مجلة البحوث والدراسات، جامعة الوادي، المجلد 20، العدد 02، سنة 2023، ص 109.

[5] المادة 03 من القانون رقم 18-07 المصدر السابق.

[6] حليمة علاني، الحماية الجنائية للمعطيات الشخصية في التشريع الجزائري، مذكرة تخرج لاستكمال متطلبات نيل شهادة ماستر، جامعة قاصدي مرباح، كلية الحقوق والعلوم السياسية، تخصص قانون جنائي، سنة 2019، ص 15.

أما فيما يخص المبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي والتي نص عليها قانون 18-07 فهي تتمثل في الموافقة المسبقة ونوعية المعطيات بالإضافة الى الإجراءات المسبقة عن المعالجة.

أولا: الموافقة المسبقة

وهو ما نصت عليه المادة 07 من قانون 18-07 والتي علقت معالجة المعطيات ذات الطابع الشخصي على الموافقة الصريحة للشخص المعني[1] ويشترط في هذه الموافقة أن تكون صادرة من هذا الأخير أوممثله الشرعي ويستوي الأمر أن تكون بطريقة يدوية أو إلكترونية[2].

كما يمكن للشخص المعني التراجع عن موافقته في أي وقت، وعلى الرغم أن المشرع حث على ضرورة الحصول على موافقة الشخص المعني على عملية معالجة معطياته الشخصية إلا أنه استثنى بعض الحالات والتي لا تستلزم موافقته وهي في الحالات التي تكون فيها هذه المعالجة ضرورية لاحترام التزام قانوني يخضع له المسؤول عن المعالجة[3] أو الشخص المعني أو حماية حياة هذا الأخير أو لتنفيذ عقد يكون طرفا فيه أو تنفيذ إجراءات سابقة للعقد، أو للحفاظ على مصالحه الحيوية في حالة عدم قدرته على التعبير عن رضاه من الناحية البدنية أو القانونية، كما أقر صراحه على إمكانية ذلك في حالة تنفيذ مصلحة الصالح العام أو المسؤول عن المعالجة وكذا تحقيق مصلحه مشروعه بشرط مراعاة مصلحة الشخص المعني وحقوقه وحرياته الأساسية[4]، والملاحظ أن المشرع وحفاظا على حدود حرية الشخص وحقوقه أورد هذه الحالات على سبيل الحصر لا على سبيل المثال لتصبح أي حالة خارج ما ذكرته هذه المادة هو انتهاك صريح وتعدي على المعطيات الشخصية التي أصبحت محمية بموجب هذا القانون[5].

وتعزيزا لهذه الحماية فقد حصر الأشخاص الذين لهم الحق في الإطلاع على هذه المعطيات وجعلها حكرا على كل من المسؤول عن المعالجة والمرسل إليه[6]. وذلك في إطار انجاز الغايات المرتبطة مباشرة بمهامهم[7].

---

[1] عرفت المادة 03 من القانون 18-07 الشخص المعني على أنه: كل شخص طبيعي تكون المعطيات المتعلقة بذات الطابع الشخصي المتعلقة به موضوع معالجة.

[2] المادة 03 من القانون 18-07 المصدر نفسه.

[3] عرفته المادة 03 من القانون 18-07 على أنه: شخص طبيعي أو معنوي عمومي أو خاص أو أي كيان أخذ يقوم بمفرده أو بالإشتراك مع الغير بتحديد الغايات من معالجة المعطيات ووسائلها.

[4] انظر المادة 07 من القانون 18-07 المصدر نفسه.

[5] محمد العيداني، يوسف زروق، المرجع السابق، ص 121.

[6] عرفته المادة 03 من القانون 18-07 المصدر السابق، على أنه: شخص طبيعي أو معنوي أو السلطة العمومية أو المصلحة أو أي كيان آخر يتلقى معطيات ذات طابع شخصي.

[7] انظر المادة 07 من القانون 18-07 المصدر نفسه.

وفي نفس السياق المتعلق بالموافقة على معالجة المعطيات فإنه إذا تعلق الأمر بطفل فإن هذه العملية مرهونة بموافقة ممثله الشرعي أو ترخيص من القاضي المختص عند الاقتضاء، كما يمكن للقاضي الأمر بالمعالجة حتى من دون موافقة الممثل الشرعي للطفل إذا استدعت المصلحة الفضلى للطفل ذلك، ويمكن للقاضي العدول عن هذا الترخيص في أي وقت[1].

ثانيا: نوعية المعطيات:

سن المشرع الجزائري مبادئ تتعلق بالمعطيات محل المعالجة في حد ذاتها، إذ اشترط أن تكون معالجة بطريقة مشروعة ونزيهة وأن تكون مجمعة لغايات محددة ومشروعة وأن لا تعالج لاحقا بطريقة تتنافى مع هذه الغايات وأن تكون ملائمة ومناسبة لهذه الغايات بالإضافة الى صفتها وكمالها وتحينها، وحفظها بشكل يسمح بالتعرف على الأشخاص المعنيين خلال مدة لا تتجاوز المدة اللازمة لإنجاز الأغراض التي من أجلها تم جمعها ومعالجتها[2].

وقد تم اسناد معالجة المعطيات ذات الطابع الشخصي المتعلقة بالجرائم والعقوبات وتدابير الأمن الى كل من السلطة القضائية والسلطات العمومية والأشخاص المعنويين الذين يسيرون مصلحة عمومية ومساعدي العدالة في إطار اختصاصاتهم القانونية[3]، وقد منع المشرع الاستناد على المعالجة الآلية للمعطيات ذات الطابع الشخصي المتضمنة تقييم بعض الجوانب الشخصية في تأسيس الأحكام القضائية والقرارات المنشئة لأثار قانونية تجاه شخص[4].

ثالثا: الإجراءات المسبقة عن المعالجة:

يلزم للقيام بمعالجة المعطيات ذات الطابع الشخصي ضرورة مراعاة مجموعة من القواعد الإجرائية لضمان حماية حقوق وحريات الشخص المعني وتأمين رقابة فعالة على مختلف المعالجات مما جعل المشرع يخضعها لتصريح مسبق أمام السلطة الوطنية أو لترخيص منها إلا في حالة نص القانون على خلاف ذلك[5].

---

[1] انظر المادة 08 من القانون 18-07 المصدر السابق.

[2] انظر المادة 09 من القانون 18-07 المصدر نفسه.

[3] انظر المادة 10 من القانون 18-07 المصدر نفسه.

[4] انظر المادة 11 من القانون 18-07 المصدر نفسه.

[5] يزيد بوحليط، عبد الرحمان فطناسي، "الحماية الإدارية والجزائية في مجال المعطيات ذات الطابع الشخصي على ضوء القانون 18-07"، مجلة أبحاث قانونية وسياسية، جامعة جيجل، المجلد 06، العدد 02، ديسمبر 2021، ص 60.

1- التصريح: يودع التصريح المسبق لدى السلطة الوطنية مقابل الحصول على وصل في أجل 48 ساعة، ويمكن المسؤول من المعالجة وبمجرد استلامه الوصل وتحت مسؤوليته المباشرة في أعماله[1] ويتضمن التصريح المودع لدى السلطة الوطنية إلتزاما بإجراء المعالجة وفقا للقانون 18-07[2].

كما حدد القانون الحالات التي لا تستوجب إلزامية التصريح وتتمثل في المعالجات التي يكون الغرض منها فقط مسك سجل مفتوح ليطلع عليه الجمهور أو كل شخص يثبت أن له مصلحة مشروعة في ذلك، وقد ميز قانون 18-07 بين نوعين من التصريح[3]:

- ✓ التصريح العادي: الذي يستوجب أن تتوفر فيه كل البيانات المذكورة في المادة 14.
- ✓ التصريح البسيط: وهو الذي أجازته المادة 15 عندما يظهر أن المعالجة لا تشكل أي خطر للإضرار بحقوق وحريات الأشخاص المعنيين وحياتهم الخاصة، إذا اشترطت أن يتضمن فقط البيانات الستة الأولى من المادة 14 على أن تحدد السلطة الوطنية قائمة بأصناف المعالجات الآلية وغير آلية الخاضعة للتصريح المبسط[4].

2- الترخيص: أعطى المشرع للسلطة الوطنية السلطة التقديرية لتقييم الأخطار التي تهدد المعطيات الشخصية في البيئة الرقمية كالنشر والاستعمال غير المرخص للمعطيات بما يضر حرمه الحياة الخاصة والحريات الأساسية للأفراد[5]، وبعد دراسة التصريح المودع لديها يمكن أن تقرر إخضاع المعالجة المعنية الى ترخيص مسبق بواسطة قرار معلل يدلي الى المسؤول عن المعالجة في أجل 10 أيام من تاريخ إيداع التصريح وهذا في حالة ما إذا تبين لها أن المعالجة المزمع القيام تشكل أخطار ظاهرة على احترام وحرية الحياة الخاصة[6].

ولا يمكن الترخيص بمعالجة المعطيات الحساسة إلا فيما يتعلق بالمصلحة العامة وتكون ضرورية لضمان ممارسة المهام القانونية أو النظامية للمسؤول عن المعالجة أو بعد موافقة الشخص المعني، وكذا في الحالات الأخرى التي ذكرها

---

[1] العيداني محمد، يوسف زروق، المرجع السابق، ص 122.

[2] انظر المادة 13 من القانون 18-07 المصدر السابق.

[3] انظر المادة 16 من القانون 18-07 المصدر نفسه.

[4] حليمة علالي، المرجع السابق، ص 21.

[5] يزيد بوحليط، عبد الرحمان فطناسي، المرجع السابق، ص 61.

[6] انظر المادة 17 من القانون 18-07 المصدر السابق.

المشرع على سبيل الحصر في المادة 18 من نفس القانون التي يمكن فيها الحصول على ترخيص لمعالجة المعطيات الحساسة، ويعتبر هذا بمثابة تفعيل للحماية وإجراء رقابي يمنع التعرض لحقوق الشخص المعني أو الإساءة له[1].

الفرع الثاني:

ضوابط عمليات المعالجة الآلية للمعطيات الشخصية

لخلق نوع من التوازن بين معالجة المعطيات الشخصية والحق في الحياة الخاصة فإنه لابد من وضع مجموعة من الضوابط لحماية الأشخاص المعنيين بمعالجة المعطيات الشخصية بمنحهم حقوقا من جهة والزام القائمين على المعالجة ببعض الالتزامات من جهة أخرى، وهو ما سار عليه المشرع الجزائري على غرار النصوص العربية والأوروبية في هذا المجال، ويبدو واضحا تأثر القوانين بالتوصيات الأوروبية لعام 1995 وانسجامها مع الأهداف المرجوة من إقرارها، لا سيما منها الحماية عبر إطار تشريعي يضمن وضوح الخطوات العملية التي تحصل في هذا المجال[2].

أولا: حقوق الشخص المعني

عالج المشرع الجزائري حقوق الشخص المعني بالمعالجة الآلية للمعطيات في الباب الرابع من القانون 18-07 حاصرا إياها فيما يلي:

1- الحق في الإعلام:

لقد أشارت أحكام المادة 32 من قانون 18-07 وجوب الإعلام المسبق لكل الأشخاص المعنيين الذين يتم الاتصال بهم لجمع المعطيات بمجموعة من العناصر، وذلك قبل القيام بهذا التجميع وليس أثنائه فالعبرة هنا هي تمكين صاحب المعطيات من اتخاذ قراره بشأن تقديمها أو عدم تقديمها[3].

كما اشترط المشرع أن يكون هذا الإعلام بصفة صريحة ودون لبس وأن يشمل العناصر المتعلقة بهوية المسؤول عن المعالجة أو ممثله القانوني والغرض من المعالجة، وكل معلومة إضافية مفيدة، أما في الحالة التي يكون فيها جمع المعلومات من خلال شبكة مفتوحة يمكن تداولها دون ضمانات السلامة وتسقط الزامية الإعلام إذا تعذر إعلام

---

[1] نزيهة بن علال،" الإطار القانوني لحماية المعطيات ذات الطابع الشخصي في الفضاء الإلكتروني في ظل القانون رقم 18-07"، مجلة دائرة البحوث والدراسات القانونية والسياسية، المركز الجامعي تيبازة، المجلد 4، العدد 2، سنة 2020، ص 61.

[2] بوداود خليفة، السعيد بوزيان، المرجع السابق 111.

[3] مبروكة بوقرة، اسيا طالبي، الحماية الجزائرية للمعطيات الشخصية في ظل القانون 07/18، مذكرة ماستر، جامعة قاصدي مرباح، ورقلة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2022/2021، ص 60.

الشخص المعني بان المعطيات المتعلقة به يمكن ان تتعرض للقراءة او الاستعمال غير المشروع [1]، كما تسقط الزامية الإعلام كذلك إذا تمت المعالجة تطبيقا لنص قانوني أو إذا تمت المعالجة حصريا لأغراض صحفية أو فنية أو أدبية[2].

2- الحق في الولوج:

إن الولوج إلى المعلومة هو في حد ذاته حق من حقوق الإنسان ويعزز إمكانية تحقيق ممارسة الحقوق ، وهذا الحق يسمح للشخص المعني أن يحصل من المسؤول عن المعالجة على المعطيات الشخصية المتعلقة به محل المعالجة والغرض من المعالجة، وفئات المعطيات، التي تنصب عليها والمرسل إليهم، كما يمكن إفادته بكل معلومة متاحة حول مصدر المعطيات[3]. كما يمكن للمسؤول عن المعالجة الاعتراض لدى السلطة الوطنية عن طلبات الولوج متى كانت تعسفية أو متكررة، كما له طلب تحديد آجال الإجابة[4].

3- الحق في التصحيح:

يقصد به أحقية الشخص بالحصول دون مقابل من المسؤول المعالج عن تحيين أو تصحيح أو غلق المعطيات الشخصية في حالات معنية وفي أجل أقصاه 10 أيام من تاريخ اخطاره ويستطيع كذلك الشخص اللجوء إلى السلطة الوطنية في حالة عدم تلقي إجابة خلال المدة المذكورة أو في حالة تلقي الرفض من طرف المسؤول عن معالجة معطياته الشخصية ،كما يحق له تبليغ الغير الذي تلقى المعطيات الشخصية بأي تحسين أو تصحيح أو إغلاق للمعطيات وفي حالة وفاة الشخص ينتقل الحق في الحالتين السابقتين للورثة[5].

وما تجدر إليه الإشارة في هذا السياق أن المشرع الجزائري لم يتطرق إلى حق النسيان المنصوص عليه في قانون حماية البيانات في الاتحاد الأوروبي، والذي يتيح للمستخدمين في ظروف معينة أن يطلبوا من محركات البحث الغاء عناوين الويب من النتائج عندما يتم البحث باستخدام أسمائهم، وأكتفي بالنص على حق المسح وهو نفسه حق المحو والذي يسمح للأشخاص بحذف بياناتهم الشخصية عندما يغادرون الخدمة أو التطبيق[6].

---

[1] انظر المادة 32 من القانون 18-07، المصدر السابق.

[2] انظر المادة 33 من القانون 18-07، المصدر نفسه.

[3] عبد السلام طوبال، منى غبولي، "الضمانات القانونية لحماية المعطيات ذات الطابع الشخصي في التدريج الجزائري"، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور بالجلفة، المجلد 05، العدد 02، جوان 2020 ص270.

[4] محمد الفيداني – يوسف زروق، المرجع السابق ص 125.

[5] انظر المادة 35 من القانون 18-07، المصدر السابق.

[6] نزيهة بن علال، المرجع السابق، ص ص63، 64.

4- الحق في الاعتراض:

يعتبر الحق في الاعتراض أحد الحقوق الأساسية التي منحها القانون 18-07 للشخص المعني بغية حماية حياته الخاصة، فهو بمثابة سلطة في مواجهة استعمال معطياته الشخصية من قبل المسؤول عن المعالجة أو من قبل الغير[1]، إذ يمكن هذا الحق للشخص المعني الاعتراض لأسباب مشروعة على معالجة المعطيات الشخصية المتعلقة به، وله الحق في الاعتراض على استعمال معطياته الشخصية لأعراض دعائية ولاسيما التجارية منها من طرف المسؤول عن المعالجة غير أن هذا الحق يبقى مقيدا لا يمكن ممارسته في الحالة التي تكون فيها المعالجة ستجيب لالتزام قانوني أو إذا كان ترخيص المعالجة قد استبعد إمكانية الشخص الاعتراض عن معالجة معطياته الشخصية[2].

ويستبعد حق الاعتراض أيضا في حالة المعالجة التي لا تخضع بتطبيق قانون 07/18 بشكل عام، ويتعلق الأمر بالحالات الواردة في المادة 06 كالمعالجة لمصلحة الدفاع والأمن الوطني أو تلك التي تكون العرض منها الوقاية من الجرائم ومتابعة مرتكبيها وقمعها وتلك التي تحتويها السجلات المتعلقة بالسوابق القضائية بالإضافة إلى بعض حالات المعالجة المتعلقة بالصحة والتي نصت عليها المادة 5 من قانون 07/18.

ولم يقيد المشرع الجزائري حق الاعتراض بنوع معين من المعالجة بل إجازه سواء في إطار المعالجة الآلية أو غير الآلية، وسواء كانت المعالجة من طرف هيئة عمومية أو خاصة[3]. إلا أنه قيده بوجود مبرر شرعي فلا يجوز ممارسة هذا الحق دون إبداء هذا المبرر ، وذلك من دون إعطاء مدلول لمصطلح المبرر المشروع و يبقى تقدير مدى مشروعية المبرر من عدمه أمرا خاضعا لقاضي الموضوع في كل حالة على حدى[4]، غير أنه يمكن للشخص المعني الاستناد إلى المادة 02 من القانون 18-07 والتي وضعت الإطار العام بحدود معالجة المعطيات ذات الطابع الشخصي والتي يجب أن تتم في ظل الاحترام للكرامة الإنسانية والحياة الخاصة والحريات العامة وألا تمس بحقوق الأشخاص وشرفهم وسمعتهم[5].

---

[1] مبروكة بوقرة، آسيا طالبي، المرجع السابق، ص20.

[2] انظر المادة 36 من القانون 18-07، المصدر السابق.

[3] حليمة علالي المرجع السابق ص24، 26.

[4] نزيهة بن علال، المرجع السابق ص64.

[5] عز الدين طباش،" الحماية الجزافية للمعطيات الشخصية في الشريع الجزائري،" المجلة الأكاديمية للبحث القانوني، جامعة بجاية، العدد 2، 2018، ص38.

5- الحق في منع الاستكشاف المباشر:

يعتبر الاستكشاف المباشر إحدى صور الإشهار الالكتروني ووسيلة تبررها حرية التجارة وهدفها الوصول إلى أكبر عدد ممكن من المستهلكين، إلا أن ذلك من شأنه المساس بحرمة الحياة الخاصة للمستهلك الالكتروني، والذي يظل دائما الطرف الضعيف في البيئة الافتراضية ولهذا جاءت هذه الأحكام في قانون 18-07 بغرض حماية هذا الشخص الذي يتم استكشافه من خطر انتهاك المورد الالكتروني للمعطيات الشخصية له في البيئة الرقمية[1]. ولهذا فإن المشرع منع الاستكشاف المباشر بواسطة آلية اتصال أو جهاز الاستنساخ البعدي أو بريد الالكتروني أو أي وسيلة تستخدم تكنولوجيا ذات طبيعة مماثلة باستعمال بيانات شخص طبيعي في أي شكل من الأشكال دون موافقته المسبقة على ذلك[2]. كما سعى لحماية كل الأشخاص المستعملين لآليات الاتصال الحديثة، لاسيما زبائن الهاتف النقال الذين تصلهم رسائل دعائية ومسابقات وهمية من دون معرفة كيفية وصول أرقام هواتفهم إلى المرسلين وبدون معرفة المرسل ولا هويته لكي يطلب منه إيقاف هذه الرسائل[3].

هذه الحقوق التي أقرها المشرع الجزائري للشخص المعني بمعالجة المعطيات ذات الطابع الشخصي إلا أنه وما يلاحظ أن المشرع لم يخص الحق في الولوج والحق في التصحيح كما فعل بالنسبة للحق في الإعلام والحق في الاعتراض باستثناءات يستبعد فيها ممارسة هذه الحقوق على عكس التوجيه الأوروبي والقانون الفرنسي اللذان أخضعا هذان الحقان لنفس الاستثناءات وخاصة في ظل صعوبة ممارستها إما بسبب طبيعة المعالجة أو بسبب تعارض هذا الولوج مع مقتضيات تشريعية أخرى[4].

من جهة أخرى وعلى الرغم من أن هذه الحقوق تعتبر انعكاسا لحق الخصوصية للشخص المعني والسياسة التي ينتهجها الموقع الالكتروني لتكريس هذا الحق، لا سيما بتحديد المعلومات الكافية عن معالجة بيانات الشخص والجهة المسؤولة عن المعالجة وكذا حقه بقبول أو الاعتراض على المعالجة أو الوصول إلى المعلومات التي تجمع عنه، إلا أنه واقعيا فمستخدم المواقع الالكترونية نادرا ما يقرأ الشروط الطويلة والبنود الغامضة التي تعرض عليه قبل إعطائه حق استخدام برنامج أو تطبيق أو منصة الكترونية ما يعني أن الموافقة التي يعطيها ليست صادرة عن إرادة حقيقية[5].

---

[1] يزيد بوحليط، عبد الرحمان فطناسي، المرجع السابق ص63.

[2] انظر المادة 37 من القانون 18-07، المصدر السابق.

[3] نزيهة بن علال، المرجع السابق ص64.

[4] مبروكة بوقرة، آسيا طالبي، المرجع السابق، ص ص18، 20.

[5] نزيهة بن علال، المرجع السابق، ص63.

ثانيا: التزامات المسؤول عن المعالجة الآلية للمعطيات الشخصية

فرض المشرع الجزائري بموجب القانون 18-07 على المسؤول عن المعالجة سواء كان شخص طبيعي أو معنوي أو أي هيئة تقوم بمفردها أو باشتراك مع الآخرين عدة التزامات نذكر منها:

1- الالتزام بسريه وسلامة المعالجة:

يلتزم المسؤول عن المعالجة وفق هذا القانون باتخاذ كل التدابير التقنية والاحترازات اللازمة من أجل حماية وتأمين المعطيات ذات الطابع الشخصي من القرصنة والتلف وكل استخدام غير مشروع خاصة إذا كانت مرسلة عبر شبكة معنية وتزيد هذه التدابير كلما زادت قيمة وأهمية هذه المعطيات[1].

وقد أوجب المشرع على المسؤول عن المعالجة وضع مجموعة من التدابير التقنية والتي تكون عن طريق استعمال مجموعة من التقنيات مثل برامج مضادة للفيروسات ومحاولة الدخول بدون إذن أو عرقلة أنظمة تعديل المعطيات وتقنية التشفير أو الترميز بالنسبة لمحاولات الاختراق، بالإضافة إلى اتخاذ تدابير تنظيمية والتي تتعلق أساسا بتنظيم الولوج أو الدخول وانتقاء وتكوين ومرافقة العمال، صيانة المعدات، إعداد نسخ احتياطية من قواعد المعطيات وحمايتها من الحرائق والسرقة وغيرها من الإجراءات[2].

أما إذا كان المسؤول عن المعالجة يستخدم مسؤولا من الباطن[3] يعمل لحسابه وجب على هذا الأخير تقديم الضمانات الكافية من سلامة وتأمين المعطيات ذات الطابع الشخصي ويجب أن يكون هذا التفويض بموجب عقد أو سند قانوني مكتوب[4]. وذلك لأغراض حفظ الأدلة[5]، ولا يخول للمعالج من الباطن التصرف الا وفقا لتوجيهات وتعليمات من المسؤول الأول عن المعالجة وهذا من أجل تحديد المسؤوليات القانونية ولكي لا تضيع حقوق الأشخاص بين المسؤول عن المعالجة والمسؤول عن المعالجة من الباطن، كما يلتزم هؤلاء بالمحافظة على السر المهني من بعد انتهاء مهامهم[6].

---

[1] محمد العيداني، يوسف زروق، المرجع السابق، ص126.

[2] حليمة علالي، المرجع السابق، ص27.

[3] عرفته المادة 02 من القانون 18-07 المصدر السابق، على أنه: كل شخص طبيعي أو معنوي عمومي أو خاص أو أي كان آخر بمعالج معطيات ذات طابع شخصي إحسان المسؤول عن المعالجة.

[4] خليفة بودواو، السعيد بوزيان، المرجع السابق، ص114.

[5] انظر المادة 39 من القانون 18-07، المصدر السابق.

[6] محمد، العيداني – يوسف زروق، المرجع السابق، ص126.

فيما يخص الأشخاص العاملين تحت سلطة المسؤول عن المعالجة أو المعالج من الباطن فإنهم لا يجوز لهم الولوج إلى المعطيات ذات الطابع الشخصي دون تعليمات المسؤول عن المعالجة إلا في حالة تنفيذ التزام قانوني[1].

2- الالتزام فيما يخص المعالجة المرتبطة بخدمات التصديق الالكتروني والمتعلقة بمجال الاتصالات الالكترونية:

يلتزم مردود وخدمات التصديق الالكتروني بمعالجة المعطيات الشخصية من أجل تسليم وحفظ الشهادات المرتبطة بالتوقيع الالكتروني[2] دون أي أغراض أخرى ماعدا في حالة الموافقة الصريحة لأصحابها، كما يلتزم مقدموا الخدمات في مجال الاتصالات الالكترونية وبعد اتخاذهم جميع الضمانات الضرورية لحماية المعطيات إبلاغ السلطة الوطنية والشخص المعني إذا كان هناك مساس بحياته الخاصة في حالات الإتلاف أو الضياع أو الإفشاء أو الولوج عبر المرخص كما يلزمون بجرد كل انتهاكات تمس المعطيات الشخصية والإجراءات التي اتخذت بشأنها[3].

3- الالتزام عند نقل المعطيات نحو دولة أجنبية:

تعد الانترنت فضاءا عالميا لتبادل المعلومات وتسمح بانتقال كم هائل من النصوص والصور ومعطيات الأنظمة المعلوماتية وهو ما يجعلها تخدع من نطاق القوانين المحلية وصلاحية السلطات الوطنية[4]، ومن جهة أخرى فإن المعطيات الوطنية أصبحت في متناول الشركات الأجنبية العاملة في الجزائر لاسيما شركات الاتصال والبنوك الأجنبية والسفارات وهذا ما يسهل تحويلها إلى دول أخرى في غياب نص يمنع ذلك لهذا تدخل المشرع لإضفاء الحماية اللازمة لهذه المعطيات[5] ومنع على المسؤول عن المعالجة تحويل المعطيات ذات الطابع الشخصي إلى دولة أجنبية إلا بترخيص من السلطة الوطنية متى رأت هذه الأخيرة أن هذه الدولة تضمن مستوى كاف للحياة الخاصة والحريات والحقوق الأساسية للأشخاص والإجراءات الأمنية المناسبة، ومتى رأت أن نقل هذه المعلومات والمعطيات لا يشكل خطرا على الأمن العمومي والمصالح الحيوية للدولة[6].

وأوردت المادة 45 من نفس القانون بعض الحالات التي يجوز فيها نقل البيانات بالرغم من عدم توافر مستوى كاف من الحماية كالموافقة الصريحة للشخص المعني والحالات التي يكون فيها النقل ضروريا للمحافظة على حياة

---

[1] انظر المادة 41 من القانون 18-07، المصدر السابق.

[2] عرفت المادة 02 من القانون 15-04 ، المصدر السابق بأنه: بيانات في شكل الكتروني مرفقة أو مرتبطة منطقيا ببيانات الكترونية أخرى تستعمل كوسيلة توثيق.

[3] امحمد العيداني، يوسف زروق، المرجع السابق، ص126.

[4] يزيد بوحليط، عبد الرحمان فطناسي، المرجع السابق، ص66.

[5] محمد العيداني، يوسف زروق، المرجع السابق، ص127.

[6] انظر المادة 44 من القانون 18-07، المصدر السابق.

شخص أو مصلحة عامة أو لاحترام التزامات قانونية تتعلق بإحقاق العدالة وحقوق الدفاع أمام المحاكم والتعاون القضائي والاتفاقات التي تكون الجزائر طرفا فيها بناء على ترخيص من اللجنة الوطنية.

الفرع الثالث:

الحماية الجزائية للمعطيات ذات ا لطابع الشخصي

إن حماية المعطيات ذات الطابع الشخصي كحق في الحياة الخاصة للأفراد وكذا ضمان تطبيق الالتزامات المنصوص عليها في القانون رقم 18-07 يقتضي فرض قواعد زجرية وذلك بوضع نصوص تجرم كل مساس بهذه المعطيات وكل خرق للالتزامات التي يفرضها القانون وهو ما سنه المشرع في الفصل الثالث من الباب السادس من هذا القانون والذي جاء بعنوان الأحكام الجزائية وهو ما سنتطرق إليه على النحو التالي:

أولا: الجرائم المتعلقة بمعالجة المعطيات الشخصية

في هذا الإطار سنتناول الجرائم المترتبة على عدم احترام حقوق الشخص المعني التي منحه إياها هذا القانون وكذا تلك المترتبة عن عدم احترام الالتزامات المفروضة على المسؤول عن المعالجة بمناسبة معالجة المعطيات الشخصية.

1- الجرائم المتعلقة بعدم احترام حقوق الشخص المعني:

أ- جريمة معالجة المعطيات الشخصية دون موافقة الشخص المعني أو اعتراضه: من أجل تفعيل الالتزام بضرورة الحصول على رضا الشخص المعني، فقد جرم المشرع الجزائري فعل القيام بالمعالجة دون الحصول على موافقته، وكذا في الحالة التي يعبر فيها بشكل صريح عن رفضه عندما يقدم اعتراض في تلك المعالجة، و هذه الحالة ربما قد تثير نوعا من التعقيد، خاصة وإن المشرع قيد حق الاعتراض بأن يكون مبنيا على أسباب مشروعة[1]، حيث أن تقدير مدى مشروعية السبب يخضع للسلطة التقديرية للقاضي وهذا ما يتعارض مع مبدأ الشرعية والذي يستلزم مراعاة الدقة والوضوح في اللفظ والمعنى عند وضع النص الجزائي وكذا وجوب تجنب الغموض والمصطلحات الفضفاضة التي تحمل أكثر من تأويل[2].

أما معالجة المعطيات الحساسة من دون موافقة الشخص المعني فإن المشرع قد شدد في عقوبتها بالنظر للعقوبة المنصوص عليها بالنسبة للمعطيات العادية ذلك أن الأصل في هذه المعطيات عدم جواز معالجتها إلا في الحالات المنصوص عليها في المادة 18 من نفس القانون[3].

---

[1] عز الدين طباش، المرجع السابق، ص36.

[2] إبراهيم بباح إبراهيم، "مبدأ الشرعية الجزائية ضمانة لتكريس سيادة القانون"، مجلة الدراسات القانونية المقارنة، المجلد 07، العدد، 02 2021، ص220.

[3] انظر المادة 57 من القانون 18-07، المصدر السابق.

2- جريمة معالجة المعطيات الشخصية دون تصريح أو دون ترخيص:

وهي الجريمة المنصوص عليها بموجب المادة 56 من القانون 18-07 وهي تقع بمخالفة أحكام المادة 12 من نفس القانون والتي أوجبت أن تخضع كل عملية معالجة للمعطيات ذات الطابع الشخصي لإجرائي التصريح أو الترخيص من طرف السلطة الوطنية لحماية المعطيات الشخصية مالم يوجد نص يستثني عملية معالجة معينة من ذلك[1].

ويعد إعطاء تصريحات كاذبة أو مواصلة نشاط معالجة المعطيات رغم سحب وصل التصريح أو الترخيص الممنوح له جريمة معاقب عليها بنفس عقوبة انعدام التصريح أو الترخيص.

ثانيا: الجرائم المتعلقة بمخالفة التزامات المسؤول عن المعالجة:

1- جريمة عدم الاعتراف بحقوق الشخص المعني بالمعالجة:

وهذه الجريمة نصت عليها المادة 64 من القانون 18-07 وتقوم عند مخالفة مسؤول المعالجة بدون سبب مشروع حقوق الإعلام أو الولوج أو التصحيح أو الاعتراض وهي الحقوق الواردة في الباب الرابع من هذا القانون والتي جاءت تحت عنوان حقوق الشخص المعني وأوجبت على المسؤول عن المعالجة ضمانها لصالح كل شخص تكون معطياته محل معالجة.

إلا أن ما يطرح في هذا الشأن هو ازدواجية التجريم لرفض المسؤول عن المعالجة حق الشخص المعني بالمعالجة المتعلق بالاعتراض المنصوص عليه بموجب هذه المادة، والقيام بالمعالجة رغم اعتراض الشخص المعني المنصوص عليه بالمادة 55 من نفس القانون، لاسيما وأن المشرع لم يبين شكل الرفض المنصوص عليه وعدم الاستجابة لاعتراض الشخص المعني من طرف المسؤول عن المعالجة يعد رفضا بدوره، وفي هذه الحالة من المرجح أن تطرح مسألة تعدد الجرائم ولا بد من وصف الفعل بالوصف الأشد[2] وهو الوصف المنصوص عليه بالمادة 55.

وتجريم الرفض في هذا النص لم يرد بشكل مطلق، إذا اتبعه المشرع بعبارة عندما يصدر دون سبب مشروع وبالتالي هناك حالات يجوز فيها للمسؤول عن المعالجة رفض الاعتراف بتلك الحقوق كما لو كان طلب الشخص المعني يحمل طابعا تعسفيا بالشكل الذي نصت عليه المادة 34[3].

---

[1] أنظر المادة 56 الفقرة 2 من القانون 18-07، المصدر السابق.

[2] أنظر المادة 32 من قانون 66-156 المصدر السابق.

[3] حليمة علالي، المرجع السابق، ص 42.

2- جريمة عدم الالتزام بسرية وسلامة المعالجة للمعطيات الشخصية:

وهو الفعل المنصوص عليه بالمادة 65 من القانون رقم 18-07 ويتحقق السلوك الإجرامي نتيجة خرق المسؤول عن المعالجة الالتزامات الملقاة على عاتقه والمنصوص عليها في المادتين 38 و39 من نفس القانون والمتعلقتان بضمان سلامة[1] وسرية المعالجة للمعطيات الشخصية من الاتلاف العرضي أو غير المشروع أو الضياع العرضي أو التلف أو النشر أو الولوج غير المرخص خاصة إذا كانت المعالجة تتطلب إرسال المعطيات عبر شبكة معينة فإنه يجب حمايتها من أي شكل من أشكال المعالجة غير المشروعة[2]، فهذا النص موجه بشكل مباشر لحماية حرمة الحياة الخاصة في جانب المعطيات الشخصية وأي تقاعس في اتخاذ الترتيبات التقنية والتنظيمية الكافية سيؤدي الى الاضرار بالمعطيات وبأصحابها، بل وأنه أكثر من ذلك فإنه قضي بقيام هذه الجريمة حتى وإن كان الشخص المضرور لم يكن معنيا بالمعالجة ولكن أصيب بضرر جراء استعمال تلك المعالجة، إذا قامت مسؤولية القائم بالمعالجة[3].

وتقوم هذه الجريمة كذلك في حالة اخلال المسؤول عن المعالجة بالالتزامات المفروضة عليه طبقا للمادة 39 في حالة إجراء المعالجة لحسابه والمتمثلة في اختيار معالج من الباطن يقدم الضمانات الكافية المتعلقة بإجراءات السلامة التقنية والتنظيمية والسهر على احترامها وتنظيم عملية المعالجة بموجب عقد أو سند قانوني.

كما ان الاحتفاظ بالمعطيات ذات الطابع الشخصي بعد المدة المنصوص عليها في القانون او تلك الواردة في التصريح او الترخيص يعرض المسؤول عن المعالجة لنفس العقوبة[4].

3- جريمة خرق الالتزام بالتعاون مع السلطة الوطنية:

إن الغرض من إنشاء السلطة الوطنية هو حماية المعطيات ذات الطابع الشخصي وضبط هذا المجال الحساس ومن أجل تفعيل هذا الدور جرم المشرع الجزائري كل عرقلة لعمل السلطة الوطنية والتي منحها القانون في سبيل تحقيق

---

[1] و في نفس الاتجاه جرم المشرع بموجب المادة 93 مكرر 2 من القانون 08-01 المعدل للقانون 83-11 المتعلق بالتامينات الاجتماعية التسليم و الاستلام غير المشروع للبطاقة الالكترونية للمؤمن له اجتماعيا او المفتاح الالكتروني لهيكل العلاج او المفتاح الالكتروني لمهني الصحة و ضاعف العقوبة في نص المادة 93 مكرر 3 في حالة القيام عن طريق الغش بتعديل او حذف المعطيات.

[2] الزهرة جقريف، "المعالجة الخزانية للمعطيات ذات الطابع الشخصي في التشريع الجزائري وفقا لأحكام المادة 18-07"، مجلة العلوم القانونية والاجتماعية، جامعة الجلفة، المجلد السادس، العدد الرابع، ديسمبر 2021، ص 491.

[3] عز الدين طباش، المرجع السابق، ص ص 46، 47.

[4] انظر المادة 65 من القانون 18-07، المصدر السابق.

الهدف من إنشاءها صلاحية القيام بالتحريات ومعاينة المحلات والأماكن التي تتم فيها المعالجة باستثناء المحلات المسكونة وكذا الولوج الى معطيات المعالجة وجميع المعلومات والوثائق أي كانت دعامتها[1].

ويرى أساتذة القانون في هذا الشأن أن الاعتراض هنا هو استعمال كل الطرق التي من شأنها أن تحول دون وصول أعضاء السلطة لكشف المخالفات وأدلتها، سواء كان هذا الاعتراض مادي كمنع الدخول الى المحل أو قطع التيار الكهربائي لمنع تشغيل الأجهزة الإلكترونية أو اعتراض آلي كالامتناع عن إعطاء كلمة المرور للدخول الى النظام المعلوماتي[2].

كما أن العرقلة يمكن أن تكون عن طريق رفض تزويد أعضاء السلطة الوطنية أو أعوانها المعلومات والوثائق الضرورية لتنفيذ المهمة الموكلة لهم من طرف السلطة الوطنية أو اخفاء أو إزالة الوثائق والمعلومات المذكورة[3].

ثالثا: الجرائم المتعلقة بالبيانات المجموعة

1- جريمة استعمال الأساليب غير المشروعة في جمع المعطيات الشخصية

لقد جرم المشرع الجزائري بموجب نص المادة 59 من القانون رقم 18-07فعل القيام بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة، و يعرف الجمع على أنه عملية الإلمام المسبق بالمعطيات وتنظيمها من أجل استعمالها فيما بعد[4].

2- جريمة جمع المعطيات الشخصية المتعلقة بالوضعية الجزائية للشخص المعني

ويقوم السلوك المجرم في هذه الجريمةباتخاذ احد الاشكال التالية: وضع أو حفظ في الذاكرة الآلية المعطيات ذات الطابع الشخصي بخصوص جرائم أو إدانات أو تدابير أمن[5]، اذ خول القانون معالجة هذا النوع من المعطيات ذات الطابع الشخصي للسلطات القضائية و السلطات العمومية و الأشخاص المعنويين الذين يسيرون مصلحة عمومية و مساعدي العدالة في اطار اختصاصتهم القضائية[6]، ويقصد بالوضع إدراج المعطيات ذات الطابع الشخصي والمتعلقة بالماضي الجزائي للشخص المعني في سجلات معلوماتية مهما كانت طبيعتها، بحيث لا يشترط القانون أن تكون معدة خصيصا لذلك، بل قد يكون له غرض آخر وتم إدراج تلك السوابق فيه، كما لو كان

---

[1] أنظر المادة 49 من القانون 18-07، المصدر السابق.

[2] الزهرة جقريف، المرجع السابق، ص 492.

[3] أنظر المادة 61 من القانون 18-07، المصدر السابق.

[4] الزهرة جقريف، المرجع السابق، ص 494.

[5] انظر المادة 68 من القانون 18-07، المصدر السابق.

[6] انظر المادة 10 من القانون 18-07، المصدر نفسه.

السجل متعلقا بتسيير هيئة المستخدمين، أما الحفظ فالمراد به الإبقاء على هذا النوع من المعطيات داخل الذاكرة الآلية عن طريق تسجيلها، بحيث يمكن العودة إليها[1] في أي وقت[2].

3- جرائم الاستعمال غير المشروع للمعطيات الشخصية

تقوم السلوك الاجرامي لهذا الفعل في حالة قيام بالتسبب او تسهيل الاستعمال التعسفي او التدليسي للمعطيات المعالجة او المستلمة او يوصلها الى غير المؤهلين لذلك و يستوي الامر ان يرتكب الفاعل السلوك عن قصد او اهمال منه كما ان الفاعل لا بد ان يكون اما مسؤولا عن المعالجة او معالجا من الباطن و كل شخص مكلف بالنظر الى مهامه بمعالجة معطيات ذات طابع شخصي[3]، كما تقوم هذه الجريمة في حالة انجاز او استعمال معالجة المعطيات لأغراض أخرى غير تلك المصرح بها او المرخص بها[4]، كما تقوم هذه الجريمة في حالة السماح لأشخاص غير مؤهلين بالولوج إلى المعطيات الشخصية[5].

4- جريمة نقل المعطيات ذات الطابع الشخصي نحو دولة اجنبية:

يقوم السلوك الاجرامي في هذه الجريمة في الحالة التي يقوم فيها الجاني بنقل المعطيات ذات الطابع الشخصي الى دولة اجنبية و ذلك في حالة المساس بالامن او المصالح الحيوية للدولة او نقلها في الحالات الأخرى دون احترام الشروط اللازمة و المتمثلة في ترخيص من السلطة الوطنية و ان تضمن هذه الدولة مستوى كاف من للحياة الخاصة و الحريات و الحقوق الأساسية للافراد إزاء المعالجة التي تخضع لها هذه المعطيات أو التي قد تخضع لها[6].

---

[1] الزهرة جقريف، المرجع السابق، ص 495.

[2] في ذات السياق نصت المادة 10 من القانون رقم 15-03 المتعلق بعصرنة العدالة على وجوب ان تضمن الوسائل التقنية المستعملة في ارسال العقود والوثائق والمحررات القضائية سلامة الوثائق المرسلة وامن وسرية المراسلات كما اوجبت المادة 14 من نفس القانون ضمان الوسيلة المستعملة في استجواب وسماع الأطراف عن طريق المحادثة المرئية عن بعد سرية الارسال وامانته.

[3] انظر المادة 69 من القانون 18-07 المصدر السابق.

[4] انظر المادة 58 من القانون 18-07 المصدر نفسه.

[5] انظر المادة 60 من القانون 18-07، المصدر نفسه.

[6] انظر المادة 44 من القانون 18-07، المصدر نفسه.

رابعا: الجزاءات المقررة لجرائم المساس بالمعطيات ذات الطابع الشخصي

1- العقوبات الأصلية

- **بالنسبة للشخص الطبيعي:**

نص المشرع الجزائري في المواد 54 الى 69 من القانون 18-07 عن الاحكام الجزائية المطبقة في حالة ارتكاب احدى الأفعال المجرمة بموجب هذا القانون والجزاءات المقررة لها وباستقراء هذه المواد فان العقوبات للشخص الطبيعي تكون على النحو التالي:

- عقوبة القيام بالمعالجة دون الموافقة الصريحة للشخص المعني او تمكين الغير من الاطلاع عليها او استعمالها في غير الغايات المرتبطة مباشرة بمهام المسؤول عن المعالجة تكون العقوبة بالحبس من سنة الى 03 سنوات والغرامة من 100.000دج الى 300.000دج.

- عقوبة المعالجة بدون تصريح او ترخيص او بعد سحبهما تكون العقوبة بالحبس من سنتين الى 05 سنوات والغرامة من 200.000دج الى 500.000دج.

- عقوبة معالجة المعطيات الحساسة بدون موافقة المعني تكون الحبس من سنتين الى 05 سنوات والغرامة من 200.000دج الى 500.000دج.

- عقوبة استعمال المعطيات المعالجة لأغراض أخرى غير تلك المرخص بها او المصرح بها تكون بالحبس من 06 أشهر الى سنة والغرامة من 60.000دج الى 100.000دج.

- عقوبة السماح لغير المرخص لهم بالولوج الى المعطيات تكون بالحبس من سنتين الى 05 سنوات والغرامة من 200.000دج الى 500.000دج.

- عقوبة عرقلة اعمال السلطة الوطنية تكون بالحبس من 06 أشهر الى سنتين والغرامة من 60.000دج الى 200.000دج.

- عقوبة الولوج الى السجل الوطني لحماية المعطيات ذات الطابع الشخصي تكون العقوبة بالحبس من سنة الى 03 سنوات وبالغرامة من 100.000دج الى 300.000دج.

- عقوبة رفض حقوق الاعلام او الولوج او التصحيح او الاعتراض تكون بالحبس من شهرين الى سنتين والغرامة من 20.000دج الى 200.000دج.

- عقوبة الاخلال بالالتزامات المتعلقة بسرية وسلامة المعالجة والاحتفاظ بالمعطيات بعد المدة القانونية او الواردة في الترخيص او التصريح تكون بالغرامة من 200.000دج الى 500.000دج.

– عقوبة عدم اعلام السلطة الوطنية والشخص المعني عن الانتهاكات للمعطيات الشخصية تكون بالحبس من سنة الى 03 سنوات والغرامة من 100.000دج الى 300.000دج او بإحدى هاتين العقوبتين.

– عقوبة تحويل المعطيات ذات الطابع الشخصي نحو دولة اجنبية تكون بالحبس من سنة الى 05 سنوات وبالغرامة من 500.000دج الى 1.000.000دج.

– عقوبة الجرائم المتعلقة بالمعطيات المتعلقة بالوضعية الجزائية للأشخاص تكون بالحبس من 06 أشهر الى 03 سنوات وبالغرامة من 60.000دج الى 300.000دج.

– عقوبة تسهيل او التسبب في الاستعمال التعسفي او التدليسي للمعطيات تكون بالحبس من سنة الى 05 سنوات وبالغرامة من 100.000دج الى 500.000دج.

– بالنسبة للشخص المعنوي:

يعاقب الشخص المعنوي الذي يرتكب الأفعال المجرمة بموجب هذا القانون وفقا للقواعد المنصوص عليها في قانون العقوبات[1]، وبالرجوع إلى هذا الأخير وبالذات إلى نص المادة 1/18 مكرر منه نجد أن العقوبة هي الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة،الا ان الجدير بالذكر في هذه النقطة ان المسؤولية الجزائية عن الجرائم المنصوص عليها في هذا القانون لا تقوم في حال ارتكاب الفعل من طرف الدولة و الجماعات المحلية و الأشخاص المعنوية الخاضعة للقانون العام[2] على الرغم من التعريفات الواردة في المادة الثانية من القانون 07/18 للاشخاص المسؤولين و المتدخلين في معالجة المعطيات ذات الطابع الشخصي.

2– العقوبات التكميلية

أحال المشرع بالنسبة للعقوبات التكميلية التي يمكن تطبيقها على الأشخاص المخالفون الى قانون العقوبات، وتختلف هذه العقوبات بين الشخص الطبيعي والشخص المعنوي، فالعقوبات التكميلية التي تطبق على الشخص الطبيعي هي: تحديد الإقامة، المنع من الإقامة الحرمان من مباشرة بعض الحقوق، المصادرة الجزئية للأموال، نشر الحكم[3]، أما الشخص المعنوي فإن العقوبات التكميلية التي يمكن أن تطبق عليه فقد حددتها المادة 2/18 مكرر من قانون العقوبات وهي كالتالي: حل الشخص المعنوي، غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 5 سنوات، الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات، المنع من مزاولة نشاط أو عدة أنشطة مهنية أو

[1] انظر ا المادة 70 من القانون رقم 18-07 المصدر السابق.

[2] انظر المادة 51 مكرر من قانون 04-15، المصدر السابق.

[3] انظر المادة 09 من قانون 06-23، المصدر السابق.

اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز خمس سنوات، مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها، نشر وتعليق حكم الإدانة، الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته. هذا بالإضافة الى إمكانية الامر بمسح كل او جزء من المعطيات ذات الطابع الشخصي و مصادرة محل الجريمة بغرض إعادة تخصيصه أو تدميره على نفقة المحكوم عليه[1].

المطلب الثاني:

آليات تحقيق الامن السبيراني في القوانين الموضوعية المتفرقة.

إن الاعتماد على تقنيات المعلومات في جميع الميداين زاد من الحاجة الى اعتماد قواعد موضوعية لحماية الاتصالات والمعلومات وهو ما جعل المشرع الجزائري يسن قواعد في العديد من القوانين الخاصة بغرض المحافظة على سرية البيانات والخصوصية والحقوق وكذا تحقيق نوع من الثقة على مستوى الفضاء السبيراني ونتطرق في هذا المطلب الى اهم هذه القواعد المنصوص عليها بموجب القوانين المتفرقة.

الفرع الأول:

الامن السبيراني في مجال الاتصالات الالكترونية

تحتل مسألة سرية المراسلات والاتصالات مكانة مهمة في مجال حقوق الإنسان باعتبارها تعبيرا عن الحق في حياة الإنسان الخاصة، ولهذا تم تكريس هذا الحق في المواثيق الدولية لاسيما الإعلان العالمي لحقوق الإنسان في مادته الخامسة والاتفاقية الدولية للحقوق المدنية والسياسية في مادتها 17، بالإضافة إلى العديد من الاتفاقيات والمؤتمرات، كما حرصت التشريعات الداخلية على ضمان هذا الحق وبدوره المشرع الجزائري كان سباقا لحماية هذا الحق في أسمى وثيقة للدولة وهي الدستور، إذ نصت عليه مختلف الدساتير التي عرفتها الجزائر منذ تاريخ استقلالها وقد نص المشرع عليه في دستور 2020 بموجب المادة 46 منه والتي أكدت أن سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة تحت طائلة العقوبات الجزائية في حالة المساس بهذه الحقوق دون أمر معلل من السلطة القضائية[2].

---

[1] انظر المادة 72 من القانون 18-07، المصدر السابق.

[2] انظر المادة 46 من المرسوم الرئاسي رقم 20-442 المؤرخ في 15 جمادى الأولى عام 1442 هـ الموافق 30 ديسمبر 2020، المتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر سنة 2020، ج ر ج ج العدد 82 المؤرخة في 15 جمادى الأولى عام 1437 هـ الموافق 30 ديسمبر 2020.

ولاشك أن هذه الحماية تشمل المراسلات والاتصالات الالكترونية وذلك بتعميم الحماية على كافة أشكال المراسلات والاتصالات، وحسنا فعل المشرع ذلك أن الانتشار السريع والمتفاقم لتكنولوجيا المعلومات وزيادة الاعتماد عليها في كافة نواحي الحياة والمعاملات الالكترونية زاد من ضرورة الاهتمام بسرية وخصوصية المعلومات الشخصية المتبادلة في هذه المراسلات والاتصالات في إطار ما يسمى بالخصوصية الالكترونية[1].

أولا: تعريف سرية الاتصالات الالكترونية:

عرف المشرع الجزائري الاتصالات الالكترونية في القانون 18-04 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية على أنها "كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية"[2]في حين عرفها في القانون رقم 09-04 على أنها "أي تراسل أو إرسال أو استقبال علامات أو إشارات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية"[3].

والملاحظ في هذين التعريفين تطابق مفهوم الاتصالات الالكترونية في القانونين ولا يظهر الاختلاف إلا من خلال تحديد الوسيلة المستخدمة في الاتصال في قانون 18-04 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية حاصرا إياها في الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية في حين أنه وسع من مفهوم الوسيلة المستعملة في قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بنصه على عبارة أي وسيلة الكترونية، و يقصد بسرية الاتصالات الالكترونية بأن لكل شخص الحق في كتمان مراسلاته الالكترونية واتصالاته، مع عدم جواز للغير الكشف عنها تحت أي ظرف أو عذر، إلا من خول القانون له ذلك[4]، ولكي تتسم المراسلات الالكترونية بالسرية لابد أن يتوفر فيها شرطين:

- **الشرط الأول**: يتعلق بمضمون الرسالة، بمعنى أن تكون ذات طابع شخصي أو خاص ويعد هذا المعيار معيارا موضوعيا.

---

[1] خالد ممدوح إبراهيم، أمن المراسلات البريد الالكتروني، الدار الجامعية، طبعة 2008، الإسكندرية، مصر، ص70.

[2] انظر المادة 10 من القانون 18-04 المؤرخ في 23 شعبان عام 1939 الموافق لـ 10 مايو سنة2018 المحدد للقواعد العامة المتعلقة بالبريد و الاتصالات اللكترونية، ج ر ج ج العدد 18 الصادرة بتاريخ 13 ماي 2018 ، ص16.

[3] انظر المادة 2 فقرة 09 من قانون 09-04 المصدر السابق.

[4] نور الهدى شافعي، سهام حريزي، تجريم الخصوصية المعلوماتية في ظل القانون الجزائري، مذكرة ماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، 2021/2020، ص 10.

- **الشرط الثاني:** يتعلق برغبة المرسل بأن لا يسمح للغير الإطلاع على محتوى ومضمون الرسالة ويعد هذا المعيار معيارا شخصيا[1].

فقد فرق الفقه فيما يخص المراسلات الالكترونية التي تتم عبر شبكة الانترنت بين تلك المراسلات العامة التي يمكن لأي شخص الإطلاع عليها كما في صفحات (الويب)، فهذا النوع من الخدمات عنصر العلنية فيها متفق عليه ومن ثم تنتفي فيها السرية، أما الرسائل الالكترونية الخاصة التي توجه إلى شخص من أشخاص محددين، كخدمة البريد الالكتروني وخدمة الاتصال المباشر عن بعد فهذه النوعية من الخدمات هي التي تتسم بطابع الخصوصية، إذ ينحصر الاتصال بين طرفين معلومين لبعضهم البعض ولا يجوز للغير الإطلاع على مضمون الرسائل المتبادلة بينهما إلا بإذنهما[2].

تضمن القانون رقم 18-04 المتضمن القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية جملة من التدابير الجديدة مؤكدا على أهمية توفير الخصوصية الرقمية للأفراد من خلال اشتراطه احترام السرية وعدم انتهاك الحرمة و الحياة الخاصة إزاء تلك المراسلات[3].

وقد نص في فحواه على العديد من القواعد التي تضمن أمن وسلامة شبكات الاتصالات الالكترونية وذلك عن طريق إنشاء سلطة الضبط التي أوكل لها مهمة تحقيق الأمن السيبراني وإلزام المتعاملين باحترام التزاماتهم القانونية و قد أخضع إنشاء واستغلال شبكات الاتصالات الالكترونية المفتوحة للجمهور وتقديم خدمات الاتصالات الالكترونية للجمهور إلى احترام شروط خصوصية البيانات والمعلومات التي تم إيصالها بواسطة شبكات الاتصالات الالكترونية واحترام شروط حماية الحياة الخاصة للمشتركين والبيانات ذات الطابع الشخصي[4].

---

[1] سمية بلغيث، الحماية الجنائية للحق في حرمة الحياة الخاصة، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في الحقوق، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، سنة 2021، ص27.

[2] فاطمة الزهراء ربحي تبون، "سرية المراسلات والاتصالات الالكترونية حقا يضمنه القانون"، مجلة الدراسات القانونية، كلية الحقوق جامعة أسيوط، المجلد 07، العدد 02، 2021، ص 622.

[3] نصير يحي الشريف، عبير مزغيش، "الآليات القانونية المكرسة لحماية الحق في الخصوصية الرقمية في التشريع الجزائري،" مجلة البحوث في العقود وقانون الأعمال، كلية الحقوق جامعة قسنطينة 1، المجلد 07، العدد 02، 2022، ص 200.

[4] المادة 97 من القانون 18-04، المصدر السابق.

كما ألزم متعاملي الاتصالات الالكترونية باتخاذ التدابير التي من شأنها أن تضمن سرية المكالمات والمعلومات التي يحوزونها عن مشتركيهم، وأن لا يسمحوا بوضع أي ترتيبات بغرض اعتراض الاتصالات أو مراقبة المكالمات الهاتفية والوصلات والمحادثات والمبادلات الالكترونية دون إذن مسبق من السلطة القضائية[1].

وبالإضافة إلى وجوب اتخاذ التدابير اللازمة ألزم المتعاملين والأشخاص الذين يعملون لديهم باحترام سرية المراسلات الصادرة عن طريق الاتصالات الالكترونية وشروط حماية الحياة الخاصة والمعلومات الاسمية للمشتركين[2] طبقا لاحكام المادة 160من قانون 18-07.

ومن أجل معرفة هوية المستخدمين والتعرف عليهم في حالة وقوع أي عمل غير مشروع ألزم إثبات هوية المشترك لدى المتعامل قبل تشغيل خطه أو تقديم أي خدمة له أما بخصوص الخطوط المجهولة و السابقة لصدور القانون فقد منح المشرع مدة ستة أشهر من تاريخ نشر هذا القانون في الجريدة الرسمية من أجل إثبات هوية كل الخطوط المجهولة و هو ما الزمت به المواد 161 و 162 من قانون 18-07.

ضف إلى ذلك فقد حرص على عدم المساس استعمال شبكات أو خدمات الاتصالات الالكترونية بمايلي:

- النظام العام والدفاع الوطني والأمن العمومي.
- الكرامة وحفظ الحياة الخاصة للآخرين.
- حماية الأطفال، خصوصا فيما يتعلق باستعمال خدمات الانترنت[3].

وفي حال الاستعمال المخالف لذلك فإن المتعامل يجب عليه التدخل الفوري لمنع النفاذ إلى الشبكات أو خدمات الاتصالات الالكترونية بعد اعذاره من طرف سلطة ضبط البريد والاتصالات الالكترونية[4].

ثانيا: صور الجرائم الواقعة على الاتصالات الالكترونية:

نص المشرع الجزائري في القانون رقم 18-04 في المواد 164، 165 و 166 على مجموعة من الأفعال المجرمة بغرض حماية الاتصالات المتعلقة بالاتصالات الالكترونية و قد نص على صور للجرائم المركبة من طرف الأشخاص مهما كانت صفتهم و صور أخرى للجرائم المرتكبة من طرف متعاملي الاتصالات الالكترونية او مستخدميهم.

---

[1] االمادة 119 من القانون 18-04، المصدر السابق.

[2] االمادة 160 من القانون 18-04، المصدر نفسه.

[3] االمادة 117 من القانون 18-04 ، المصدر نفسه.

[4] انظر المادة 118 من القانون 18-04، المصدر نفسه.

1- الجرائم الماسة بسرية الاتصالات الالكترونية:

حدد المشرع الجزائري مجموعة من الصور للافعال التي يعتبر اقترافها جريمة يعاقب عليها القانون وذلك بنص المادة 164 من قانون 18-04 والتي جاءت بصفة العموم وذلك بنص المشرع على عبارة "كل شخص" اذ تطبق على كل الأشخاص بغض النظر عن صفتهم أو علاقتهم بالمراسلات.

- الصورة الاولى: انتهاك سرية المراسلات المرسلة

باعتبار الحق في حرمة المراسلات الالكترونية حقا من حقوق الانسان اللصيقة بالشخصيةفلا يجوز التنازل عنه ولا يمكن التعدي عليها الا في حالات اقرها القانون بموجب اذن قضائي، يصرح فيه بإذاعة او نشر او تسجيل المحادثة ورضا صاحبها او بوجود علاقة إشرافيه بين الجاني وصاحب الحق، وفي غير هذه الحالات يعتبر الفعل انتهاك لسرية المراسلات الالكترونية.[1]

- الصورة الثانية: الافشاء

فيقصد بالإفشاء الإذاعة أي اظهار مضمون الرسالة او لجزء منها وبالتالي تمكن الغير من معرفة والعلم بفحوى الرسالة، ويقصد منه أيضا تغيير توجه الرسالة من علم شخص محدد الى علم عدد غير محدود من الغير وتمكينهم من مشاهدة الرسالة وذلك بالاستعانة بالأجهزة الحديثة سوآءا المستعملة لنقل الصوت او الصورة[2].

- الصورة الثالثة: النشر

يقصد بالنشر نقل مضمون المراسلة الى علم الغير باستخدام وسائل معينة مستخدمة بكثرة في المجتمع والتي تمكن من نشر ومعرفة وتوسيع نطاق العلم بالمراسلة الى عدد غير محدود من الأشخاص الا وهي وسائل النشر المعروفة كالمجلات والصحف والدوريات والمنشورات والمطبوعات الكتابية.

وبالمفهوم الحديث لوسائل النشر أصبحت المراسلة أكثر عرضة للنشر بين عدد لا يمكن حصره من الأشخاص وفي زمن جد قصير فالتقدم التكنولوجي افرز تقنية البلوتوث في الهواتف الذكية، وأيضا صفحات الانترنت التي يتميز النشر فيها بخطورة كبيرة حيث يسمح بطباعتها والاحتفاظ بها.

الصورة الرابعة: الاستعمال غير الشرعي للمراسلات.

لا يجوز اعتراض المراسلات الإلكترونية دون ترخيص أطرافها لان رضا الأطراف يعتبر سببا من أسباب الاباحة فيتحقق الركن المادي في جريمة الاعتداء على المكالمات او المحادثات الالكترونية باستراق السمع للمحادثة واستعمالها

[1] طلعت الشهاوي، "المسؤولية الجنائية عن جرائم الاتصالات"، ط 1، دار النهضة العربية، القاهرة، مصر، 2018، ص 518.

[2] المرجع نفسه، ص 504.

دون رضا أطراف المحادثة، فان كان مسبوقا برضا الأطراف او مصرح بها في الأحوال التي ينص عليها القانون فهنا لا يكتمل الركن المادي وبالتالي انعدام الجريمة، ويتحقق الركن المادي حتى وان كانت الأفكار والآراء المنتهكة لا تتسم بالسرية المهم ان يكون الانتهاك بغير رضا الأطراف· فبالنسبة للمحادثات الالكترونية فيتحقق الاعتداء فيها في حالة عدم قبول او موافقة أطراف الحوار وذلك عكس الحوار المفتوح الذي يعتبر قرينة على رضا أطرافها على سماع المحادثة، الا انه في بعض الحالات يتم الحصول على محل النشر بطريقة مشروعة أي برضا صاحبه ولكن نشره يعتبر جريمة وذلك في حالة إذا كان المجني عليه غير مميز او ارادته معيبة، كما يشترط في هذا الرضا ان يكون معاصرا للمراسلة الالكترونية[1].

– الصورة الخامسة: الاخبار عن وجود المراسلة الالكترونية.

وفي هذه الصور يظهر حرص المشرع على حماية سرية الاتصالات الاكترونية اذ اعتبر حتى الاخبار بوجود هذه المراسلة جريمة يعاقب عليها القانون حتى بدون التطرق الى فحواها.

2– الجرائم المتعلقة بالاعتداء على المراسلات الالكترونية:

وهي المنصوص عليها بموجب المواد 165 و166 من قانون 18-04 وهي الصور تتمثل فيمايلي:

– الصورة الأولى: فتح المراسلات الالكترونية

يقوم الجاني في هذه الصورة بالولوج غير المشروع الى المعلومات و البيانات المرسلة عن طريق المراسلات الالكترونية و ذلك عن طريق إزالة العائق المادي الذي يضعه المرسل للمحافظة على سرية بريده[2]، و يتم الفتح عادة بدواعي التطفل على البريد الالكتروني او ما يعرف بالتصنت، و يكون ذلك باستخدام تقنيات حديثة لانتهاك السرية مثل: الاختراق والفيروسات المعلوماتية واقتحام البريد الصوتي للمتعامل الإلكتروني وتثبيت برامج التجسس على الهاتف المحمول والقرصنة بواسطة هوائيات المحمول.[3]

[1] محمود احمد طه، المرجع السابق، ص90.

[2] نبيل محمدة عثمان عرعارة، الحماية الجنائية للحق في حرمة المراسلات عبر البريد الالكتروني، ط 01، المصرية للنشر و التوزيع، القاهرة، مصر، 2008، ص 71.

[3] رشيدة بوبكر، الحماية الجزائية للتعاملات الالكترونية، ط 1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2020، ص 579.

– الصورة الثانية: تحويل المراسلات الالكترونية:

يعتبر فعل تحويل المراسلات الصادرة او المرسلة او المستقبلة عن طريق الاتصالات الالكترونية جريمة يقوم بها متعامل الاتصالات الالكترونية او عون مستخدم لديه، ويكون ذلك بتحويل المراسلات الى بريد الجاني او أي بريد آخر.

– الصورة الثالثة: تخريب المراسلات الالكترونية:

و يكون ذلك باتلافها سواء بصفة كلية او بصفة جزئية و ذلك بالتقليل من قيمته و جعله غير قابل للاستعمال او تعطيله و يتم التخريب عادة عن طريق ادخال بعض الأنظمة المخربة للنظام المعلوماتي كالفيروسات التي تعيق عملية الدخول الى البريد الالكتروني و تحول دون الاستفادة منه[1].

ويستوي في ذلك ان يقوم المتعامل او العون المستخدم بالفعل المادي او امر او يساعد في تحقيق السلوك المادي للجريمة[2] كما يشترط في العون المستخدم ان يرتكب هذه الأفعال في اطار ممارسة مهامه و ليس خارجها.[3]

تعتبر جريمة الاعتداء على المراسلات والمحادثات الالكترونية من الجرائم العمدية التي تتطلب توافر القصد الجنائي بعنصريه العلم و ذلك ثبوت علم الفاعل بعدم مشروعية هذا الفعل و الإرادة ذلك باتجاه ارادة الجاني لارتكاب الفعل المكون للجريمة، ويشترط أيضا ان يكون التنصت قد حصل في غير الاحوال المصرح بها قانونا أو بغير رضا المجني عليه، وبالمفهوم المخالف في حالة القيام بالتنصت في الأحوال التي نص عليها القانون فان القصد الجنائي ينتفي ومن ثم ينتفي الركن المعنوي.[4]

ثالثا: الجزاء المقرر للجرائم الواقعة على الاتصالات الالكترونية.

ان جريمة انتهاك سرية المراسلات الالكترونية يمكن ان ترتكب من طرف أي شخص مهما كانت طبيعته وصفته هذا ما دفع بالمشرع الجزائري لوضع عقوبات تختلف حسب طبيعة الجاني وهذا ما سنتناوله في هذا الفرع ضمن نقطتين أساسيتين نتناول فيهما: عقوبة الشخص الطبيعي(أولا)،

عقوبة الشخص المعنوي (ثانيا) وظروف التشديد (ثالثا).

---

[1] مسعود حشايشي، مروان مشري، حماية الحق في الخصوصية المعاوماتية في التشريع الجزائري، مذكرة ماستر، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة،2022، ص 40.

[2] انظر المادة 165 من القانون 18-04 المصدر السابق.

[3] انظر المادة 166 من القانون 18-04، المصدر نفسه.

[4] طلعت الشهاوي، المرجع السابق، ص 506.

- **عقوبة الشخص الطبيعي**

- عقوبة المساس بسرية الاتصالات الالكترونية تكون بالحبس من (1) سنة إلى (5) سنوات وبغرامة مالية من 500.000 دج الي 1.000.000دج. [1]
- عقوبة الاعتداء على الاتصالات الالكترونية وقد فرق المشرع الجزائري في العقوبة وتختلف على حسب صفة الجاني على النحو التالي:

– اذا كان مرتكب الجريمة متعامل للاتصالات الالكترونية[2] فان العقوبة تكون بالحبس من (1) سنة الى (3) سنوات وبغرامة مالية من 1.000.000 دج الى5.000.000 دج او بإحدى هاتين العقوبتين[3].

– اذا كان مرتكب الجريمة عون مستخدم من طرف متعامل الاتصالات الالكترونية فان العقوبة تكون بالحبس من (6) أشهر الي سنتين(2) وغرامة مالية تتراوح بين 500.000 دج الى 1.000.000دج او بإحدى هاتين العقوبتين.[4]

– اذا كان مرتكب الجريمة شخص غير متعاملي الاتصالات الالكترونية و الاعوان المستخدمين من طرفهم فان العقوبة تكون الحبس من شهرين (2) الى سنة واحدة(1) وغرامة مالية تقدر بـ

200.000 دج الى 500.000 دج[5]

– وتسري نفس العقوبات على الشريك تطبيقا لما ورد في المواد 165 و 166 من القانون 04/18 اذا كان الفاعل احد متعاملي الاتصالات الالكترونية او احد مستخدميه.

- **عقوبة الشخص المعنوي**

نصت المادة 187 من القانون 04/18 على المسؤولية الجزائية للشخص المعنوي في ايطار الجرائم الواردة في هذا القانون وتقدير العقوبة في هذه الحالة يعود لنصوص قانون العقوبات في ما يخص تحديد المسؤولية الجزائية للشخص المعنوي في المادة 18 مكرر.

---

[1] انظر المادة 164 من القانون 18-04 المصدر السابق.

[2] عرفته المادة 10 في الفقرة 30 من القانون 18-04 ، المصدر نفسه على انه: كل شخص طبيعي او معنوي يستغل شبكة الاتصالات الالكترونية المفتوحة للجمهور و/ او يقدم للجمهور خدمة الاتصالات الالكترونية.

[3] انظر المادة 165 من القانون 18-04، المصدر نفسه.

[4] انظر المادة 166 من القانون 18-04، المصدر نفسه.

[5] انظر المادة 167 من القانون 18- 04، المصدر نفسه.

- **ظروف التشديد**

تطبيقا لما ورد في المادة 188 من القانون 04/18 تشدد العقوبة على مرتكبي الجرائم السالفة الذكر في حالة واحدة فقط وهي حالة العود.

الفرع الثاني:

الامن السيبراني في مجال قوانين الملكية الفكرية

يلعب الإنتاج الفكري دورا فعالا في إرساء أسس التقدم الحضاري والثقافي والاقتصادي، ولهذا لقى هذا الموضوع اهتماما كبيرا على المستوى الدولي والوطني، فقد سارعت التشريعات الى إيجاد وسائل حماية لهذ الإنتاج بمختلف صوره وهذا ما أدى الى ظهور القوانين المتعلقة بالملكية الفكرية، وقد أصبحت هذه القوانين من اهم فروع القانون خاصة امام التطور التكنولوحي الهائل بفعل ثورة التقنيات والمعلومات والذي زاد من ضرورة حماية الحقوق المترتبة عن الملكية الفكرية، فهذا القانون يعد من الأركان الأساسية لحماية شبكة الاتصالات و المعلومات باعتباره يحمي الابداع الفكري من الاستعمال غير المشروع.

ولهذا فقد حمت اغلب تشريعات دول العالم المصنفات المتعلقة بالحاسوب بما فيها برامج الحاسب الالي وقواعد البيانات ضمن حقوق المؤلف وما يترتب عليها من حماية للحقوق الأدبية و المالية لاصحاب هذه المصنفات مثل المصنفات التقليدية[1]، وقد حاول المشرع الجزائري تحقيق نوع من الانسجام مع التطور العلمي المتسارع والمتعاقب وما اقتضاه ذلك من وجوب بسط الحماية على برامج الكومبيوتر لما يتطلبه تكوينه من عمل ذهني[2]، حيث وسع الامر رقم 03-05 [3]المتعلق بحقوق المؤلف والحقوق المجاورة من قائمة المؤلفات المحمية وذلك بادماج برامج المعلوماتية ضمن المصنفات الاصلية وكما شدد عقوبة المساس بحقوق المؤلفين.[4]

أولا: نطاق الحماية بموجب قوانين الملكية الفكرية.

لقد عددت الاتفاقيات الدولية والقوانين الداخلية لا سيما الامر 03-05 المتعلق بحقوق المؤلف والحقوق لمجاورة بعض المصنفات التي ترد عليها الحماية القانونية، وقد جاء هذا التعداد على سبيل المثال لا الحصر تاركا الباب

---

[1] كوثر مازوني، "الشبكة الرقمية وعلاقتها بالملكية الفكرية"، دار الجامعة الجديدة، طبعة 2008، ص ص 19، 21.

[2] عثماني رضوان، مكافحة جرائم المعلوماتية في القانون الجزائري والدولي، أطروحة دكتوراه في العلوم، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة وهران2، محمد بن احمد، 2024/2023، ص 141.

[3] الامر 03-05 المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة، ج ر ج ج عدد44، الصادرة بتاريخ 2003/07/23.

[4] سليمان قطاف، عبد الحليم بوقرين، المرجع السابق، ص 350.

مفتوحا امام المصنفات الجديدة كالمصنفات الرقمية التي تعتبر نمطا جديدا من المصنفات والتي تشملها الحماية بمجرد توافر الشروط والقواعد القانونية[1] المطلوبة قانونا والمتمثلة في شرط الاصالة التي تشكل عموما الجهد الفكري المبذول من طرف المبدع مهما كان نوع المصنف ونمط تعبيره ودرجة استحقاقه ووجهته، وسواء كان هذا المصنف مثبتا ام لا باي دعامة تسمح بابلاغه الى الجمهور[2] طبقا للمادة 03 من امر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة، كما منح للمؤلف دون سواه طبقا للمادة 27 من نفس القانون العديد من الحقوق الحصري من بينها: استنساخ المصنف باي وسيلة كانت، ووضع اصل المصنف او نسخ منه رهن التداول بين الجمهور، وابلاغ المصنف الى الجمهور عن طريق البث الإذاعي السمعي او السمعي البصري او بالوسائل السلكية او الالياف البصرية او التوزيع السلكي او اية وسيلة أخرى لنقل الإشارات الحاملة للاصوات او للصور و الأصوات معا، بالإضافة الى إبلاغه للجمهور باي منظومة معالجة معلوماتية.

وقد اختلف الفقه حول تقسيم هذا المصنفات الا ان اغلبهم قسمها حسب طبيعتها القانونية الى مصنفات مرتبطة بالحاسب الالي وتشمل برامج الحاسب الالي وقواعد البايانات وطبوغرافيا الدوائر المتكاملة ومصنفات مرتبطة بشبكة الانترنيت وتتمثل في أسماء المواقع، محتوى الوقائع من صور ورسومات وأصوات ومؤثرات حركية والتي يطلق عليها المصنفات المتعددة الوسائط.

1- المصنفات المتعلقة بالحاسب الآلي

- **برامج الحاسب الآلي**: هي مجموعة من التعليمات الموجهة من الإنسان إلى الآلة التي تسمح لها بتنفيذ مهمة معينة، كما تطرقت اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية في إطار المنظمة العالمية للتجارة (تربس) الى البرامج في المادة 10-1 على أنه: «تتمتع برامج الحاسوب الآلي سواء كتبت بلغة المصدر أم بلغة الآلة بالحماية باعتبارها أعمال أدبية بموجب معاهدة برن لسنة 1971».

وتنقسم هذه البرامج إلى فئتين رئيسيتين:

- **الفئة الأولى**: هي برامج التشغيل التي تقوم بتشغيل الجهاز والتحكم في العمليات الداخلية[3]، اذ تعد هذه البرامج خصيصا لتنظيم عمل أجهزة الحاسب منذ بدأ تشغيلها وحتى اغلاقها، اين تخزن هذه البرامج في الذاكرة الداخلية

---

[1] باقدي دوجة، حماية حقوق الملكية الفكرية على الانترنيت، مذكرة دكتوراه تخصص قانون عام، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2020، ص 19.

[2] كوثر مازوني المرجع السابق، ص32.

[3] نور الدين بن عيشة، خليل بن بتيش، حماية الملكية الفكرية في الفضاء الالكتروني، مذكرة ماستر تخصص قانون الاعلام الالي والانترنت، جامعة محمد البشير الابراهيمي، برج بوعريريج، 2023/2022، ص17.

للحاسب باعتبارها تؤدي وظائف أساسية للمتعاملين وكمثال عن ذلك برامج التشغيل، برامج الكتابة او الرسم برامج الجداول والاحصائيات والبرامج الخاصة بحفظ الملفات واسترجاعها ومسحها ومن اشهر هذه البرامج برامج WINDOWS الصادر عن شركة MICROSOFT.[1]

- **الفئة الثانية:** فهي برامج التطبيق يكون الغرض منها تنفيذ مهام إدارية او وظيفية معينة وهي المخصصة لمعالجة مشاكل المستخدمين، مثل العمليات الحسابية وتنظيم أعمال الشركات.

وللإشارة فان هذه الحماية المقررة قانونا لا تشمل الا برنامج الحاسوب وليس سنده المادي الذي يستفيد هو الاخر من الحماية المقررة لبراءة الاختراع متى توفرت شروطها، اما شكل البرنامج الذي يظهر على الشاشة فحمايته كقاعدة عامة تخضع لنظام الرسوم والنماذج الصناعية[2]

-**قواعد البيانات:** هي طريقة ذكية لتجميع البيانات وتخزينها في نظام حاسوبي متقدم لمعالجتها وقد تطرقت اليها اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية في إطار المنظمة العالمية للتجارة (تربس) في المادة 10-2: «تتمتع بالحماية البيانات المجمعة او المواد الأخرى سواء كانت في شكل مقروء آليا او أي شيء اخر إذا كانت تشكل خرقا فكريا نتيجة انتفاء وترتيب محتواها». ويمكن تعريف قواعد البيانات بأنها مجموعة من المعلومات المنظمة والمنسقة التي تتعلق بموضوع معين وتم جمعها وترتيبها بطريقة مبتكرة مع إمكانية تدخل الحاسوب في إدارتها ،وفي هذا الصدد من المهم التمييز بين المحتوى الالكتروني وبين قاعدة البيانات فالاول هو الصيغة (format) التي يتم بها نقل المصنفات اما الاخر فهو شكل (form) المصنف نفسه، فهناك العديد من المصنفات تعتبر الكترونية ولكنها ليست قواعد بيانات وبالمقابل فان العديد من قواعد البيانات ليست الكترونية[3]، وتتالف قاعدة البيانات الالكترونية من الأرقام والصور والمفاهيم التي يتم معالجتها عادةً على الحاسوب وتحويلها إلى معلومات.[4]

تعتبر قواعد البيانات المرتبطة بالحاسوب من أحدث الأساليب المستخدمة لتخزين واسترجاع المعلومات في تطبيقات المعالجة الإلكترونية للمعلومات، وتلعب دورًا متزايد الأهمية في المجالات التجارية والصناعية ومن المتوقع أن

[1] كوثر مازوني، المرجع السابق، ص 106.

[2] عثماني رضوان، المرجع السابق، ص 142.

[3] رامي إبراهيم حسن الزواهرة، "النشر الرقمي للمصنفات وأثره على الحقوق الأدبية والمالية للمؤلف (دراسة مقارنة)"، ط 1، دار وائل للنشر عمان، 2013، ص 191.

[4] نور الدين بن عيشة، خليل بن بتيش، المرجع السابق، ص 18.

يزداد استخدامها في المستقبل لمواجهة تحديات التنظيم وكمية البيانات الكبيرة المتعلقة بالمشاريع الكبرى[1]، ونظرا للقيمة الاقتصادية الكبيرة لقواعد البيانات فقد ذهبت بعض التشريعات الى تعزيز الحماية لها وذلك بفرض قوانين خاصة للحماية الى جانب قانون حماية المؤلف.[2]

– طبوغرافيا الدوائر المتكاملة :لقد اعتبر المشرع الجزائري طبوغرافيا الدوائر المتكاملة حق من حقوق الملكية الصناعية ونظمها بموجب الامر 03-08 [3] وهي تقنية متقدمة في مجال الإلكترونيات، وتمثل تقدمًا مذهلاً [4] و تمنح صاحبها الحماية اذا كان هذا التصميم اصليا و ذلك اذا كان ثمرة مجهود فكري لمبتكره ولم يكن متداولا لدى مبتكري التصاميم الشكلية وصانعي الدوائر المتكاملة[5]، وهذا ما جعل جانب من الفقة يرى عدم تلائم قواعد الملكية الصناعية للتطبيق على هذه التصاميم ذلك انه وعلى الرغم من انها تعتبر نموذجا بوصفها تصاميم ثلاثية الابعاد الا انها تتميز بوظيفة متميزة من حيث الابتكار على نحو مختلف عن الرسوم والنماذج الصناعية.[6]

2– المصنفات المتعلقة بشبكة الإنترنت.

– إسم الموقع أو نطاق الإنترنت:هو عنوان على شبكة الانترنت يسمح بتحديد ذلك الموقع وتمييزه عن غيره من المواقع الأخرى ولا يمكن للمستخدم الدخول الى الموقع الا عن طريقه[7]، يتكون من مجموعة من الصفحات المرتبطة عبر شبكة الإنترنت وتحتوي على صور وملفات صوتية ومقاطع فيديو، و يعتبر اسم الموقع من أهم وأول مصنفات الملكية الفكرية في بيئة الإنترنت.[8]

---

[1] سومية بومعزة، حقوق المؤلف في النطاقين التقليدي والرقمي في ظل التشريع الجزائري، مذكرة لنيل شهادة الماجستير في الحقوق، تخصص ملكية فكرية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2016، ص 120.

[2] رامي إبراهيم حسن الزواهرة، المرجع السابق، ص200.

[3] الامر 03-08 المؤرخ في 19 جمادى الأولى عام 1424 الموافق لـ 19 يوليو سنة 2003 يتعلق بحماية التصاميم الشكلية للدوائر المتكاملة، ج ر العدد 44 الصادر بتاريخ 23 يوليو سنة 2003، ص 35.

[4] سومية بن قويدر، المرجع السابق، ص 08.

[5] انظر المادة 03 من الامر 03-08، المصدر السابق.

[6] صبري حمد خاطر،" مدى تطويع القواعد القانونية التقليدية في مواجهة المعلومات (دراسة مقارنة)"، د.ط، دار الكتب القانونية، مصر، 2014، ص110.

[7] كوثر مازوني، المرجع السابق، ص 214.

[8] عبد الكريم محمد ظلام، مروة احمد بادنجكي، " حماية المصنفات الإلكترونية في الفضاء الرقمي"، مجلة المستقبل للدراسات القانونية والسياسية، المركز الجامعي آفلو، العدد 02، المجلد 06، 2022، ص 06.

ان نظام التسمية الخاصة بالمواقع ينقسم الى مستويين:

أ- أسماء النطاق من المستوى الأول (TLD): هي الجزء المتواجد في يمين اسم النطاق وهي نوعين:

- **أسماء النطاق الدولية:** و هذه متاحة للاستخدام العام ومجانية بمعنى آخر، لا يحتاج المستخدم إلى ترخيص خاص للدخول إلى هذه المواقع.[1] وتختار هذه المواقع اما لطبيعة المنظمة او نشاطها بصفة مستقلة دون الاخذ بعين الاعتبار بلدها الأصلي وهي بدورها تنقسم الى قسمين:

- أسماء النطاق المفتوحة للتسجيل: والتي نجد من ضمنها: "COM" بالنسبة للمؤسسات التجارية، "ORG" بالنسبة للمنظمات غير الربحية، "NET" بالنسبة لمسير الانترنت.[2]

- أسماء النطاق المقيدة التسجيل: وهي مخصصة حصرا لجهات معينة وهناك إجراءات لحجز هذه الأسماء ومن مؤسسات محددة والتي من ضمنها:"INT"خاص بالمنظمات الدولية، "EDU" خاص بالمعاهد التربوية و "MIL" و "GOV" خاصان بالجيش الامريكي والحكومة .

- **أسماء النطاق المحلية:** وهي مواقع تشير الى بلد التسجيل فهي أسماء مواقع محلية حسب إشارة دولية معبر عنها بواسطة حرفين يشيران الى بلد معين مثال: "DZ" الجزائر، "IT" إيطاليا، "FR" فرنسا.

ب- أسماء النطاق من المستوى الثاني (SLDST) :وتسمى أيضا اسماء النطاق المحلية الدنيا وهي تتكون من الجزء الدي يقع على يسار اخر نقطة في اسم النطاق و مثالها"ASSO.FR" للجمعيات الفرنسية.

وقد اختلفت الآراء الفقهية في اعتباره عنصر من عناصر الملكية الفكرية الجديرة بالحماية وبالرجوع إلى التشريع الجزائري نجده لا يخص اسم النطاق بحماية خاصة، على غرار بعض الدول الأجنبية، لذلك فإنه يمكن إدراجه ضمن المصنفات المحمية بموجب قانون حق المؤلف والحقوق المجاورة، على أساس وجود عنصر الأصالة فيه، فالقانون يحمي كل المصنفات التي يتوفر فيها هذا الشرط كما أشرنا سابقا، أيا كان الشكل الذي اتخذته وأيا كانت وسيلة توصيلها للغير.[3]

- الوسائط المتعددة: عرف المصنف المتعدد الوسائط على انه مجموعة من الخدمات التفاعلية التي تستعمل دعامة رقمية واحدة من أجل معالجة ونقل المعلومات بمختلف أشكالها: نصوص، معطيات صور ثابتة، صور متحركة

---

[1] نايت اعمر علي، الملكية الفكرية في إطار التجارة الإلكترونية، مذكرة لنيل شهادة الماجستير في القانون، فرع القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، بجامعة مولود معمري، تيزي وزو ،2014، ص22.

[2] كوثر مازوني، المرجع نفسه، ص 217.

[3] باقدي دوجة، المرجع السابق، ص 86، 98.

خيالية أو حقيقية، فهي صيغ مركبة تجمع بين الصوت والصورة والفيديو بشكل رقمي ،ويمكن استخدامها بطريقة تفاعلية من خلال أقراص مدمجة مثل الـ CD-ROM و DVD-ROM، وهي شائعة الاستخدام في الوقت الحالي[1].

– **النشر الإلكتروني:** قد اختل الفقهاء وتعددت الآارء بخصوص وضع تعريف للنشر الإلكتروني، الا ان معناها لا يخرج عن اعتباره العملية التي يتم من خلالها إعادة الوسائط المطبوعة كالكتب والأبحاث العلمية بصيغة يتم استقبالها ونقلها وتوزيعها باستخدام الوسائط الإلكترونية الرقمية مثل شبكات الاتصالات والأقراص المضغوطة.وعلى الرغم من ما يوفره هذا النشر عن طريق تقنيات النشر الرقمي والتي تعتمد أساسا على استخدام الكمبيوتر وبرمجيات، من مزايا لا سيما امام توفير الجهد والمال واتاحته لاكبر قدر من المستخدمين، إلا أن هناك بعض المآخذ والسلبيات على النشر الرقمي خاصة باعتباره يشكل النسبة الاكبر للانتهاكات التي تقع على حقوق المؤلفين عبر شبكة الإنترنت بصور مختلفة كالنسخ أو التداول غير المشروع للمصنفات أو تشويه المصنفات والتعديل فيها جراء الدخول غير المشروع لمواقع الإنترنت والعبث بمحتويات المصنفات الرقمية والحذف والتعديل عليها وغيرها من أعمال القرصنة.[2]

ثانيا: الحماية الجزائية والجزاءات المقررة لها

تناولت مختلف التشريعات و الاتفاقيات المتعلقة بحق الملكية حماية المصنفات المتعلقة بالحاسوب والمصنفات المنشورة رقميا، وقد تناول المشرع الجزائري ذلك طبقا لأمر 05-03 الخاص بحقوق المؤلف والحقوق المجاورة، بحيث نص صراحة على حماية كل المصنفات المتعلقة بالحاسوب سواء كانت برامج إعلام آلي أو قواعد بيانات ، باعتبارها مصنفات ذهنية محمية بموجب هذا القانون، مع اعتبار برامج الحاسب الآلي مصنف أدبي وبالتالي فإن هذه المصنفات محمية بقانون التأليف، ويعطي لمالكها حقا حصريا في استنساخ المصنف بغض النظر عن الوسيلة المستعملة، او وضع المصنف السمعي البصري رهن التداول بين الجمهور بواسطة التأجير او التاجير التجاري لبرامج الحاسوب وإبلاغه عن طريق استعمال الوسائل السلكية او اللاسلكية واية منظومة معالجة معلوماتية[3] ، ولحماية هذه المصنفات فقد اقر المشرع الجزائري العقوبات التالية:

---

[1] نور الدين بن عيشة، خليل بن بتيش، المرجع السابق، ص 20.

[2] رامي إبراهيم حسن الزواهرة، المرجع السابق، ص67.

[3] انظر المادة 27 من الامر 03-05 المصدر السابق.

- **العقوبات الأصلية :**

– **العقوبة البسيطة:** تتمثل العقوبة لمرتكب جنحة التقليد لمصنف أو أداء، بالحبس من ستة (06) أشهر إلى ثلاث (03) سنوات، و بغرامة من خمسمائة ألف دينار 500.000دج إلى مليون دينار 1.000.000دج سواء كان النشر في الجزائر او الخارج[1].

– **العقوبة المشددة:** تكون في حالة العود ففي هذه الحالة تكون العقوبة بضعف العقوبة المنصوص عليها في الحالة المنصوص عليها في المادة 153 من الامر 03-05

- **العقوبات التكميلية:** تتمثل العقوبات التكميلية فيمايلي:

– **الغلق المؤقت:** وذلك لمدة لا تتعدى ستة أشهر للمؤسسة التي يستغلها المقلد أو شريكه، وأن يكون الغلق النهائي عند الاقتضاء.[2]

– **المصادرة:** سواء مصادرة المبالغ التي تمثل الإيرادات الناتجة عن الاستغلال غير الشرعي لمصنف أو أداء محمي، وإتلاف العتاد الذي أنشئ لمباشرة النشاط غير المشروع، وكل النسخ المقلدة .[3]

–نشر ملخص الحكم: هو عقوبة جوازية يقصد بها التشهير بالمحكوم عليه، والتأشير على شخصيته الأدبية والمالية، فهي ماسة بالشرف والاعتبار، تكون هذه العقوبة بطلب من الطرف المدني بنشر الإدانة في الصحف وتعليق هذه الاحكام في الأماكن التي تحددها ومن ضمن ذلك باب مسكن المحكوم عليه وكل مؤسسة او قاعة حفلات يملكها على نفقة المحكوم عليه شريطة ان لا تتعدى هذه المصاريف الغرامة المحكوم بها.[4]

و الملاحظ ان المشرع الجزائري لم ينص على عقوبة الشخص المعنوي في هذا المجال، وهو شيء طبيعي على اعتبار ان إقرار المسؤولية الجزائية في القانون الجزائري لم يكن الا سنة 2004 وذلك بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتضمن تعديل قانون العقوبات وهو التاريخ اللاحق لصدور قانون حقوق المؤلف والحقوق المجاورة وهو ما يستدعي ضرورة تعديله بادراج المسؤولية الجزائية للشخص المعنوي من اجل مواكبة هذا القانون للنصوص الحديثة وضمان الردع العام لهذه الجرائم لا سيما امام التطور السريع الجرائم واتساع رقعة المستفيدين و المرتكبين لهذه الجرائم للأشخاص المعنوية الفاعلة في هذا المجال وتحقيقها لارباح طائلة نتيحة الأفعال الماسة بالحقوق الواردة في هذا القانون.

---

[1] انظر المادة 153 من الامر 03-05، المصدر السابق.

[2] انظر المادة 156 من الامر 03-05، المصدر نفسه.

[3] انظر المادة 157 من الامر 03-05، المصدر نفسه.

[4] انظر المادة 159 من الامر 03-05، المصدر نفسه.

من جهة اخرى يمكن أن تطبق أحكام الملكية الصناعية لحماية أصحاب حقوق البراءات أو الرسوم أو النماذج الصناعية، أو أصحاب العلامات، إذا كانت متاحة عبر شبكة الأنترنت كما يكن حماية البرامج على أسس نظام البراءة بصفة عامة، إذا توفرت في البرنامج شروط البراءة ، ومنحت له على أساس ذلك البراءة على البرنامج، كما يمكن تطبيق أحكام العلامات في حالة تقليد العلامة المسجلة والمنشورة على الشبكة وحمايتها في حالة النزاع بينها وبين اسم النطاق يحمل نفس العلامة مملوك لشخص آخر غير صاحب الحق على العلامة، كما يمكن حماية المواقع كذلك عن طريق الرسوم والنماذج بالنظر إلى شكل الموقع.[1]

الفرع الثالث:

الامن السبيراني في مجال التوقيع والتصديق الالكترونيين

لم يعد أمام أي دولة خيار الا أن تواكب العصر ولا تتخلف عن الركب و ذلك بالاتجاه نحو المجتمع الالكتروني والتكنولوجيا الرقمية، فلا يمكن إنكار الدور الجوهري الذي تلعبه الرقمنة لإحراز منافع في شتى المجالات، إلا أن اللجوء إلى هذه التقنيات والتي يصاحبها التطور الهائل لتكنولوجيا الاتصال واستخداماتها في مجال المعلومات أدى إلى التزايد الهائل في المعلومات وتراكمها من جهة وتزايد المتعاملين في هذا المجال، مما تطلب ضرورة إيجاد آلية لتعزيز الثقة من أجل بناء مجتمع الكتروني يقوم على الثقة، وقد واكب المشرع الجزائري هذه التطورات ومتطلباته وأصدر القانون 15-04[2] المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين والذي يلعب دورا كبيرا في تحقيق الأمن السبراني.

أولا: التوقيع الالكتروني

1- تعريف التوقيع الالكتروني:

عرف المشرع الجزائري التوقيع الالكتروني على أنه "بيانات في شكل الكتروني مرفقة أو مرتبطة منطقيا ببيانات الكترونية أخرى، تستعمل كوسيلة توثيق"[3].

---

[1] كوثر مازوني، المرجع السابق، ص94.

[2] القانون رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436 الموافق للأول فبراير سنة 2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونين، الصادر بتاريخ 20 ربيع الثاني عام 1436 الموافق فبراير سنة 2015. ج ر ج ج العدد 06، ص 6.

[3] انظر المادة 02 الفقرة 01 من القانون 15-04، مصدر نفسه.

فالتوقيع الالكتروني في منظور المشرع الجزائري هو عبارة عن بيانات إلكترونية مرتبطة ببيانات الكترونية أخرى كالرموز ومفاتيح التشفير الخاصة، يحوزها الموقع ويتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله.[1]

ويتضمن التوقيع الالكتروني سمات منفردة تتمثل في رموز أو إشارات كما تتخذ شكل أرقام تكون خاصة بالموقع[2] وتؤدي إلى معرفة شخصية الموقع بدقة ويتم ذلك بوسائل التحقق من هوية المستخدم ويعبر عن رضا الموقع بمضمون السند وقبوله به وهو ما عبر عنه المشرع صراحة بنص المادة 06 من القانون 15/04 بنصها على "يستعمل التوقيع الالكتروني لتوثيق هوية الموقع وإثبات قبوله مضمون الكتابة في الشكل الالكتروني".

وما يلاحظ في التعريف الذي جاء به المشرع الجزائري أن هذا التعريف لم يحدد صور التوقيع الالكتروني، بل اكتفى بالإشارة إلى أن التوقيع يكون في الشكل الالكتروني، أيا كان هذا الشكل وهذا ما يفتح المجال أمام الاعتراف بجميع صور التوقيع الالكتروني[3].

وللتنويه فقد حرص المشرع الجزائري على تأمين آلية إنشاء التوقيع الالكتروني[4] الموصوف[5] وذلك بوجوب توفيرها المتطلبات التالية:

1* أن تتضمن بواسطة الوسائل التقنية والإجراءات المناسبة على الأقل ما يأتي:

أ- ألا يمكن عمليا مصادفة البيانات المستخدمة لإنشاء المواقع الإلكترونية إلا مرة واحدة، وأن يتم ضمان سريتها بكل الوسائل التقنية المتوفرة وقت الاعتماد.

ب- ألا يمكن إيجاد البيانات المستعملة لإنشاء التوقيع الإلكتروني عن طريق الاستنتاج وأن يكون هذا التوقيع محميا من أي تزوير عن طريق الوسائل التقنية المتوفرة وقت الاعتماد.

---

[1] عبد القادر سمام، الحماية القانونية للتجارة الالكترونية في التشريع الجزائري مذكرة ماستر، تخصص قانون القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، 2020/2019، ص72.

[2] صياد حبيب، التوقيع والتصديق الالكترونيين في التشريع الجزائري، مذكرة ماستر قانون إداري، قسم الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، 2021 ص12.

[3] حسين جفالي، المرجع السابق، ص194.

[4] عرف المشرع الجزائري آلية إنشاء التوقيع الالكتروني على أنها: جهاز أو برنامج معلوماتي معد لتطبيق بيانات إنشاء التوقيع الالكتروني طبقا للمادة 4/02 من قانون 15-04، المصدر السابق.

[5] انظر المادة 10 من القانون 15-04، المصدر نفسه.

ج- أن تكون البيانات المستعملة لإنشاء التوقيع الإلكتروني محمية بصفة موثوقة من طرف الموقع الشرعي من أي استعمال من قبل الآخرين.

2* يجب أن لا تعدل البيانات محل التوقيع وأن لا تمنع أن تعرض هذه البيانات على الموقع قبل عملية التوقيع[1].

2- صور التوقيع الإلكتروني:

يتخذ التوقيع الإلكتروني أشكالا عدة بحسب الوسيلة أو التقنية التي تستخدم في إنشائه، أهمها:

- التوقيع باستخدام البطاقات الممغنطة المقترنة بالرقم السري:

تعد هذه الصورة من التوقيعات الإلكترونية الأكثر شيوعا لدى الجمهور ولا تتطلب عناء أو خبرة معينة[2] وهذه الطريقة للتوقيع أفرزتها التقنيات التي استخدمت من أجل الإسراع في إنجاز المعاملات البنكية، فقد درجت البنوك على إصدار بطاقات إلكترونية مصحوبة برقم سري تمنحها لعملائها لاستخدامها في سحب وإيداع النقود أو لسداد ثمن السلع والخدمات، بحيث تسحب النقود أو تدفع من خلال جهاز آلي تؤمنه البنوك للعملاء كجهاز الصراف الآلي أو أجهزة الدفع الإلكتروني الموجودة في المحلات التجارية[3].

وهذه الصورة من أكثر الصور أمانا وثقة ذلك أن المعاملة تتم باقتران إدخال البطاقة في الجهاز مع إدخال الرقم السري للعميل والذي تحيطه اعتبارات سرية وفي حالة نسيان الرقم السري أو فقد البطاقة يتم تجميد كل العمليات[4].

- التوقيع بالقلم الإلكتروني:

وهذه الطريقة يمكن أن تتم بواسطة قلم إلكتروني يمكنه الكتابة على شاشة الكمبيوتر عن طريق برنامج هو المسيطر والمحرك لهذه العملية، ويقوم هذا البرنامج بوظيفتين أساسيتين الأولى وهي خدمة التقاط التوقيع والثانية هي خدمة التحقق من صحة التوقيع[5]، إذ يتم بهذه الطريقة نقل التوقيع التقليدي اليدوي باستخدام الماسح الضوئي، ثم

---

[1] انظر المادة 11 من القانون 15-04، المصدر السابق.

[2] حسام محمد نبيل الشنراقي، "جراءم الاعتداء على التوقيع الإلكتروني"، ط 1، دار الكتب القانونية، مصر، 2013، ص 73.

[3] حسين جفالي، المرجع السابق، ص 195.

[4] حسام محمد نبيل الشنراقي، المرجع السابق، ص 75.

[5] عادل هيليس، موسى كاسحي، مداخلة بعنوان دور وأهمية التوقيع الإلكتروني في تسهيل المعاملات التجارية والمالية، ملتقى وطني حول: الإصلاحات المالية والمصرفية في الجزائر الواقع والمأمول، كلية العلوم الاقتصادية والتجارية وعلوم التسيير جامعة وهران2، محمد بن أحمد بالتعاون مع مخبر التوجهات والتحديات الجديدة للسياسات التنموية في الجزائر، يوم 30 ماي 2022، ص 5.

نقل صورة التوقيع الى الملف المراد إضافة التوقيع إليه لإعطائه الحجية اللازمة، بهذه الصورة يتم نقل توقيع الشخص متضمنا المحدد عبر شبكة الاتصال الإلكتروني[1] بالرغم من مميزات هذه الصورة وسهولة استعمالها إلا أنه لا يتمتع بدرجة عالية من الأمان لإمكانية احتفاظ المرسل بنسخة من التوقيع وإعادة لصقها في أي مستند إلكتروني أخر و الادعاء على أن صاحب التوقيع الفعلي هو واضعها[2].

– التوقيع البيومتري:

يعتمد هذا النظام على الصفات المميزة للإنسان وخصائصه الطبيعية والسلوكية التي تختلف من شخص لآخر كبصمة الأصابع وبصمة شبكة العين ونبرة الصوت ودرجة ضغط الدم، وغيرها من الصفات الجسدية والسلوكية التي يمكن تعتمد باعتبارها توقيعا إلكترونيا[3]، إذ يتم التوقيع في هذه الصورة بأخذ صورة دقيقة من هذه الخواص ثم يقوم بتخزينها بصورة مشفرة بذاكرة الحاسوب، حيث يستطيع صاحب الشأن وعند رغبته استعمال هذه الصورة لابرام تصرف قانوني معين بالرجوع إليها وتوثيق تصرفه[4]، إلا أن ما يؤخذ على هذا النوع من التوقيع أنه يحتاج تكاليف عالية، كما أنه وبالرغم من دقته والثقة المتوفرة فيه إلا أنه ليس بعيدا عن التزوير، فيمكن تسجيل بصمة الصوت ثم إعادة بثها، أو تزوير بصمة العين بتقليدها عن طريق بعض أنواع العدسات اللاصقة وإمكانية خضوع الذبذبات الحاملة للصوت أو الصورة للنسخ وإعادة الاستعمال مما يؤدي لافتقادها للأمن والسرية[5].

– التوقيع الرقمي:

تعتمد هذه الصورة من صور التوقيع الالكتروني على استخدام تقنيات علم التشفير واختصارها إلى مجموعة من الأرقام ذو الخانات الرقمية "اللوغاريتميات" التي تشكل في نهاية المطاف ما يمكن تسميته بالبصمة الرقمية أو التوقيع الرقمي[6]. ويعد هذا النوع من التوقيع الأكثر استخداما نظرا لطابع الأمان والثقة الذي يوفرها وكذا بسهولة

---

[1] عبد الوهاب مخلوفي، التجارة الإلكترونية عبر الانترنت، أطروحة دكتوراه في الحقوق لتخصيص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، الجزائر، 2012، ص186.

[2] عبد القادر سمام، المرجع السابق، ص 76.

[3] سامية بولافة، الطاهر غيلاني، "التوقيع الالكتروني في ظل القانون 15-04"، المجلة الجزائرية للامن الانساني، جامعة باتنة 1، المجلد 05، العدد 01، جانفي 2020، ص 116.

[4] ضياء أمين مشيمش، ا"لتوقيع الالكتروني"، د.ط، المنشورات الحقوقية، بيروت، لبنان، 2003، ص129.

[5] حسين جفالي، المرجع السابق، ص 198.

[6] عادل دهيليس – موسى كاسحي، المرجع السابق، ص8.

تحديد هوية الموقع وتميزه بدقة[1] إلا أنه عيب عليه وجود إمكانية سرقة هذه الأرقام، نظرا للتطور التكنولوجي، وازدياد عمليات الاحتيال والقرصنة ومحاولة فك الشيفرة واستعمالها في أغراض غير مشروعة[2].

3- الحماية الجزائية للتوقيع الالكتروني:

تعد منظومة إنشاء التوقيع الالكتروني جهازا أو برنامج معلوماتي معد لتطبيق بيانات إنشاء التوقيع الالكتروني[3]، إذ يتم فيها تبادل البيانات بين طرفي (صاحب التوقيع ومؤدي خدمات التصديق أو المورد الالكتروني) من خلال الحاسب الآلي وباستخدام أنظمة وبرامج معينة مما يجعلها منظومة معلوماتية تخضع للحماية وفقا للنصوص المتعلقة بالمساس بأنظمة المعالجة للبيانات[4]، وبالتالي فإن جرائم الاعتداء على النظام المعلوماتي للتوقيع الالكتروني أو جريمة إتلاف التوقيع الالكتروني تقعان تحت طائلة هذه النصوص، أما بالنسبة لجريمة التزوير التوقيع الالكتروني فإنه بالرغم من استحداث المشرع الجزائري لنصوص المساس بالمعالجة الآلية للمعطيات والتي تضمنت بعض طرق التزوير كالتعديل والمحو والإدخال إلا أن المشرع لم يتطرق إلى التزوير الحاصل في المجال المعلوماتي ولم يتطرق لها بشكل خاص[5] وقد أورد المشرع نوعا من الحماية الجزائية الخاصة بموجب القانون رقم 15-04 بالنسبة للتوقيع الالكتروني الموصوف في نص المادة 68 من القانون 15-04.

- جريمة حيازة أو إفشاء أو استعمال بيانات توقيع موصوفة خاصة بالغير:

ويتمثل السلوك الإجرامي في هذه الجريمة إحدى الصور:

- الحيازة.
- الإفشاء.
- الاستعمال.

ويكفي القيام بإحدى هذه الأفعال عند التعامل مع بيانات التوقيع الالكتروني بقيام المسؤولية الجزائية في جانب الفاعل.

---

[1] حسين جفالي، المرجع السابق، ص 198.

[2] سامية بولافة-الطاهر غيلاني، المرجع السابق، ص115.

[3] انظر المادة 4/2 من القانون 15-04، المصدر السابق.

[4] حسين جفالي، المرجع السابق، ص 213.

[5] حبيب صياد، المرجع السابق، ص49.

– **العقوبة المقررة قانونا:** فيما يخص العقوبة فقد حددها المشرع بالحبس من ثلاثة (03) أشهر إلى ثلاث (03) سنوات وبغرامة من مليون دينار 1.000.000 دج إلى 5.000.000 دج أو بإحدى هاتين العقوبتين فقط[1].

ثانيا: التصديق الالكتروني

1– تعريف التصديق الالكتروني:

لم يعرف المشرع الجزائري التصديق الالكتروني في حد ذاته وإنما عرف شهادة التصديق الالكتروني على أنها وثيقة في شكل الكتروني تثبت الصلة بين بيانات التحقق من التوقيع الالكتروني والموقع[2]، إلا أنه يقصد به على العموم تلك الوسيلة الفنية الآمنة للتحقق من صحة التوقيع أو المحرر، حيث يتم تأكيد نسبه إلى شخص أو كيان معين عبر جهة موثوق بها أو طرف محايد[3] وتقوم هذه الجهة بإصدار شهادات الكترونية للمصادقة على صحة التوقيع وتعيين صاحب التوقيع ومنع التلاعب به أو بمحتوى البيانات[4] وقد منح المشرع هذه الصلاحية لمؤدي خدمات التصديق الالكتروني[5] تحت إشراف وبترخيص[6] من السلطة الاقتصادية للتصديق الالكتروني والمتمثلة في السلطة الاقتصادية للتصديق الالكتروني والمتمثلة في السلطة المكلفة بضبط البريد والمواصلات السلكية واللاسلكية[7].

وفي هذا الإطار ألزم المشرع الجزائري المورد الالكتروني أن يكون وصل موقع الانترنت الخاص به بمنصة الدفع الالكتروني مؤمنا بواسطة نظام تصديق الكتروني وذلك تعزيزا منه لحماية التجارة الالكترونية بصفة عامة وحماية المستهلك الالكتروني بصفة خاصة[8].

2– أنواع شهادات التصديق الالكتروني:

تنقسم شهادات التصديق الالكتروني إلى شهادات بسيطة وشهادات موصوفة.

---

[1] انظر المادة 68 من القانون 15–04، المصدر السابق.

[2] انظر المادة 7/02 من القانون 15–04، المصدر نفسه.

[3] آمال بوبكر، "التصديق الالكتروني"، مجلة المفكر للدراسات القانونية والسياسية، جامعة خميس مليانة، العدد 3، سبتمبر 2018، ص 212.

[4] حسين جفالي، المرجع السابق، ص203.

[5] عرف المشرع مؤدي خدمات التصديق الالكتروني في المادة 12/20 من القانون 04/15 على انه: شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق الكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الالكتروني.

[6] انظر المادة 33 من القانون 15–04، المصدر السابق.

[7] انظر المادة 29 من القانون 15–04، المصدر نفسه.

[8] انظر المادة 28 من قانون 18–05 المؤرخ في 10 مايو 2018 المتعلق بالتجارة الالكترونية، ج ر ج ج العدد 28.

– **شهادة التصديق البسيطة:** هي عبارة عن وثيقة تصدرها الجهة المختصة بالتصديق الالكتروني دون أن تحدد بيانات مسبقة.

– **شهادة تصديق موصوفة:** هي شهادة تصدرها جهات مؤهلة لإصدار شهادات التصديق الالكتروني تحتوي على بيانات محددة قانونا والتي من شأنها دعم عنصر الائتمان في التعاملات الالكترونية[1] وقد ألزم المشرع أن تحتوي هذه الشهادة على المتطلبات التالية:

– أن تمنح من قبل طرف ثالث موثوق أو من قبل مؤدي خدمات تصديق الكتروني طبقا لسياسة التصديق الالكتروني الموافق عليها.

– أن تمنح للموقع دون سواه.

– أن تتضمن: إشارة على منح هذه الشهادة كشهادة تصديق الكتروني موصوفة.

– تحديد هوية الطرف الثالث أو مؤدي خدمات التصديق الالكتروني والبلد الذي يقيم فيه.

– اسم الموقع أو الاسم المستعار الذي يسمح بتحديد هويته.

– إمكانية إدراج صفة خاصة للموقع حسب العرض من استعمال الشهادة.

– بيانات تتعلق بالتحقق من التوقيع الالكتروني.

– الإشارة إلى بداية ونهاية صلاحية الشهادة، رمز تعريف الشهادة التوقيع الالكتروني الموصوف لمؤدي الخدمات أو الشخص الثالث الموثوق.

– حدود استعمال الشهادة – حدود قيمة المعاملات التي يستعمل فيها الشهادة عند الاقتضاء، الإشارة إلى الوثيقة التي تثبت تمثيل الشخص الطبيعي أو المعنوي عند الاقتضاء[2] (هناك بيانات إلزامية وأخرى ليست إلزامية)

ثالثا: التزامات مؤدي خدمات التصديق الالكتروني:

لكي يتمكن مؤدي خدمات التصديق الالكتروني من تحقيق أهداف التصديق الالكتروني من جهة وحماية البيانات من جهة أخرى فرض القانون على عاتق مؤدي خدمات التصديق الالكتروني جملة من الالتزامات:

---

[1] سعاد يحياوي، "التصديق الالكتروني آلية تقنية لضمان وحماية المعاملات التجارية الالكترونية في القانون الجزائري"، مجلة الدراسات القانونية المقارنة، جامعة الشلف، المجلد 08، العدد 01، بسنة 2022، ص698.

[2] انظر المادة 15 من القانون 15-04 المصدر السابق.

1- الالتزام بالتحقق من صحة البيانات المقدمة:

يلتزم مؤدي خدمات التصديق الالكتروني قبل منح شهادة التصديق الالكتروني أن يتحقق من تكامل بيانات الإنشاء مع بيانات التحقق من التوقيع، أو فيما يخص الأشخاص المعنوية فإنه ملزم بالاحتفاظ بسجل خاص فيه هوية الممثل القانوني للشخص المعنوي، حتى يمكن تحديد هوية الشخص الطبيعي عند كل استعمال للتوقيع الالكتروني[1].

- إذ يقوم مقدم خدمة التصديق الالكتروني بفحص هذه المعلومات وتقدير توافقها مع المستندات المقدمة ويتفرع عن هذا الالتزام التزامات أخرى نذكر منها:

✓ عدم إمكانية مؤدي خدمات التصديق الالكتروني جمع البيانات الشخصية للمعني إلا بعد موافقته الصريحة.

✓ عدم جواز جمع البيانات الشخصية غير تلك الضرورية فقط بمنع وحفظ شهادة التصديق.

✓ عدم جواز استعمال هذه البيانات خارج نطاق نشاط التصديق الالكتروني[2].

✓ عدم إمكانية حفظ أو نسخ بيانات إنشاء توقيع الشخص الذي منحت له شهادة التصديق الالكتروني الموصوفة[3].

2- الالتزام بإصدار وإلغاء شهادات التصديق:

بعد تحقق مؤدي خدمات التصديق الالكتروني من صحة البيانات المقدمة يقوم بإصدار شهادة التوقيع الالكتروني والتي يطلق عليها اصطلاحا "بطاقة إثبات الهوية الالكترونية" ذلك أنها تعتبر المرجع الأساسي للتأكد من صحة المحرر الالكتروني، أو التوقيع الالكتروني ونسبه لصاحبه وكذا هوية الموقع ومدى استجابته للشروط القانونية[4].

كما يقوم مؤدي خدمات التصديق بإلغاء شهادة التصديق الالكتروني في الآجال المحددة في سياسة التصديق بناء على طلب صاحب هذه الشهادة أو في الحالات التي يتبين أنه تم منح هذه الشهادة بناء على معلومات خاطئة أو مزورة أو إذا أصبحت المعلومات الواردة في شهادة التصديق الالكتروني غير مطابقة للواقع أو إذا تم انتهاك سرية بيانات إنشاء التوقيع، وأنها لم تصبح مطابقة لسياسة التصديق، وفي حالة وفاة الشخص الطبيعي أو حل شخص المعنوي صاحب شهادة التصديق الالكتروني[5].

---

[1] انظر المادة 44 من القانون 15-04، المصدر السابق.

[2] انظر المادة 43 من القانون 15-04، المصدر نفسه.

[3] انظر المادة 48 من القانون 15-04، المصدر نفسه.

[4] منصور محمد حسين، "الإثبات التقليدي والالكتروني"، د.ط، دار الفكر الجامعي، مصر، 2006، ص66.

[5] المادة 45 من القانون 15-04، المصدر السابق.

بالإضافة إلى التزام مؤدي خدمات التصديق بإصدار وإلغاء شهادة التصديق الالكتروني فإنه مكلف بتسجيل هذه الشهادة ونشرها وحفظها[1].

3- الالتزام بالسرية:

يجب على مؤدي خدمات التصديق الالكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادة التصديق الالكتروني المفتوحة[2]، ويعد هذا الالتزام من أخطر الالتزامات الملقاة على عاتق مؤدي خدمات التصديق الالكتروني، وذلك نظرا لأهمية وحساسية البيانات والمعلومات المتعلقة بشهادة التصديق الالكترونية، وذلك دعما للثقة بين المتعاملين بالوسائل الالكترونية.

رابعا: الحماية الجزائية:

سعى المشرع الجزائري في قانون 04/15، المتعلق بالتوقيع والتصديق الالكترونيين إضفاء المصداقية للتوقيع الالكتروني عن طريق شهادة التصديق الالكتروني بنوع من الحماية وذلك عن طريق اقراره لوسيلة التشفير في هذا القانون، ويكون التشفير بالتغيير في شكل البيانات عن طريق تحويلها إلى رموز وإشارات لحماية هذه البيانات من إطلاع الغير عليها أو تعديلها أو تغييرها[3]، إذ تستخدم في هذه التقنية مفتاحين مرتبطين الاول مفتاح التشفير الخاص[4] والثاني مفتاح التشفير العمومي[5].

إلا أنه على الرغم ذلك فإنه لا غنى عن اللجوء إلى الآليات الردعية لمخالفة الأحكام التي جاء بها هذا القانون لاسيما لحماية التوقيع الالكتروني والبيانات المتعلقة به.

وتعتبر آليات خاصة تضاف إلى الآليات العامة في مجال النصوص التي نص عليها المشرع الجزائري لحماية المعلومات والبيانات والتي سبق التطرق إليها والمنصوص عليها في قانون العقوبات أو المنصوص عليها في القانون رقم 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي.

---

[1] انظر المادة 41 من القانون 15-04، المصدر السابق.

[2] انظر المادة 42 من القانون 15-04، المصدر نفسه.

[3] مصطفى صحراوي، "الحماية الفنية والجزائية للتوقيع الالكتروني على ضوء القانون 04/15 المتعلق بالتوقيع والتصديق الالكترونيين"، مجلة البحوث في الحقوق والعلوم السياسية، جامعة تيارت، المجلد 4، العدد 2، 2018، ص95.

[4] عرفته المادة الثانية الفقرة 08 من القانون 04/15 المتعلق بالتوقيع والتصديق الالكتروني على أنه: عبارة عن سلسلة من الإعداد يحوزها حصريا الموقع فقط، وتستخدم لإنشاء التوقيع الالكتروني، ويرتبط هذا المفتاح بمفتاح تشفير عمومي.

[5] عرفته المادة الثانية الفقرة 09من القانون 04/15 المتعلق بالتوقيع والتصديق الالكتروني على انه: عبارة عن سلسلة من الاعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقيق من الامضاء الالكتروني وتدرج في شهادة التصديق الالكتروني.

إذ أنه وفي حالات المتعلقة بجرائم الاعتداء على النظام المعلوماتي للتوقيع الالكتروني وجرائم تزويد التوقيع الالكتروني وإتلافه وذلك بالتعديل أو المحو أو الإدخال وهي الحالات التي لم ينص عليها المشرع الجزائري في القانون 04/15 فإنه يمكن تطبيق النصوص الواردة في القسم السابع مكرر من قانون العقوبات المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات.

ونذكر من بين الجرائم المنصوص عليها في القانون 15-04 والتي تهم بحثنا:

1- الجرائم المرتكبة من الغير:

جريمة حيازة أو إفشاء أو استعمال بيانات توقيع موصوفة خاصة بالغير: ويتخذ السلوك الإجرامي في هذه الجريمة إحدى هذه الأفعال ويقوم بمجرد الحيازة أو الإفشاء أو الاستعمال لبيانات إنشاء توقيع الالكتروني[1]،وتشترط في صفة مرتكب الجريمة أن يكون من الغير كما أنه ومن الملاحظ أن المشرع الجزائري خص في هذا النص التوقيع الالكتروني الموصوف[2] دون غيره.

- العقوبة المقررة قانونا: لقد رصد لها المشرع عقوبة الحبس من 03 أشهر إلى 03 سنوات وبالغرامة من مليون إلى خمس ملايين دينار جزائري[3].

2- الجرائم المرتكبة من طرف مؤدي خدمات التصديق الالكتروني:

جريمة جمع البيانات الشخصية للموقع واستخدامها في غير محلها:في هذه الجريمة ربط المشرع الجزائري قيامها بصفة الجاني وهو مؤدي خدمات التصديق الالكتروني دون غيره أما فيما يخص السلوك الإجرامي فهو مخالفة ما جاءت به المادة 43 من قانون 04/15 والتي ألزمت مؤدي خدمات التصديق الالكتروني بعدم جمع المعلومات الشخصية للمعني إلا بعد أخذ موافقته الصريحة وبالتالي فإن الإخلال بهذا الالتزام وعدم حصول مؤدي خدمات التصديق الالكتروني على الموافقة الصريحة يجعلها تحت طائلة العقوبات المنصوص عليها بهذه المادة.

---

[1] ويقصد بها طبقا للمادة الثانية الفقرة الثانية من القانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين: بيانات فريدة مثل الرموز أو مفاتيح التشفير الخاصة التي يستعملها الموقع لإنشاء التوقيع الالكتروني.

[2] وهو التوقيع الذي اعتبره المشرع مماثلا للتوقيع المكتوب سواء كان لشخص طبيعي أو معنوي طبقا للمادة 8 من القانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين، كما اشترط بموجب المادة 07 من نفس القانون توفير متطلبات خاصة لإعطائه هذه التسمية وهي أن تنشأ على أساس شهادة تصديق الكتروني موصوفة – ارتباطه بالموقع دون سواه – أن يمكن من تحديد هوية الموقع – مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الالكتروني – أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع – ارتباطه بالبيانات الخاصة به بحيث يمكن الكشف عن التغيرات الملاحقة بهذه البيانات.

[3] المادة 68 من القانون 15-04، المصدر السابق.

أما الإلزام الثاني والذي نصت عليه هذه المادة فهو تقيد مؤدي خدمات التصديق الالكتروني بجمع البيانات الشخصية الضرورية لمنح وحفظ شهادة التصديق الالكتروني دون غيرها من البيانات الشخصية وذلك بغرض الحفاظ على الخصوصية التي تتمتع بها هذه البيانات، كما أنه يتقيد من جهة أخرى باستعمالها في الإطار المتعلق بشهادة التصديق الالكتروني وحظر عليه استعمالها في أعراض أخرى.

– العقوبة المقررة قانونا:

رصد المشرع الجزائري لهذه الجريمة عقوبة الحبس من ستة (06) أشهر إلى ثلاث (03) سنوات، وبالغرامة من مائتي ألف دينار جزائري إلى مليون دينار جزائري أو بإحدى هاتين العقوبتين.

3– الجرائم المرتكبة من الأشخاص المكلفة بالتدقيق:

جريمة الكشف عن معلومات سرية: يتمثل السلوك الإجرامي في قيام الشخص المكلف بالتدقيق بكشف المعلومات السرية والتي اطلع عليها أثناء قيامه بواجبه المتمثل في التدقيق والإشارة فإن الأشخاص الذين أوكل لهم القانون هذه المهمة الأعوان التابعين للسلطة الاقتصادية للتصديق الالكتروني[1] ومكتب التدقيق المعتمد وفقا لما نصت عليه المادة 51 من القانون 15-04.

– العقوبة المقررة قانونا: حدد المشرع الجزائري لهذه الجريمة عقوبة الحبس من ثلاثة (03) أشهر إلى سنتين (02) وبالغرامة من عشرين (20.000 دج) إلى مائتي ألف (200.000 دج) أو بإحدى هاتين العقوبتين[2].

– العقوبات المقررة للشخص المعنوي: نص على قيام المسؤولية الجزائية في جانب الأشخاص المعنوية التي ترتكب إحدى الجرائم المنصوص عليها في هذا القانون بغرامة تعادل (05) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي.

[1] انظر المادة 73 من القانون 15-04، المصدر السابق.

[2] انظر المادة 75 من القانون 15-04، المصدر نفسه.

خلاصة الفصل:

حاول المشرع الجزائري ضمان بيئة رقمية امنة و منظمة و حماية البنية التحتية الرقمية من التهديدات السبيرانية، و ذلك من خلال وضع قواعد عامة في قانون العقوبات يهدف من خلالها إلى وضع قواعد ردعية لحماية أنظمة المعالجة الالية للمعطيات و حماية الدولة و مؤسساتها و خصوصية الافراد و كرامتهم في الفضاء السبيراني، و من اجل تعزيز هذه الحماية سن العديد من الاحكام في القوانين الخاصة في مجالات كثيرة، و التي تطرقنا الى أهمها في هذا الفصل اذ وضع اليات لحماية البيانات ذات الطابع الشخصي و فرض قواعد خاصة عند معالجتها يجب التقيد بها سواء من المسؤول عن المعالجة او من باقي الأشخاص، كما وضع آليات أخرى لحماية خصوصية الاتصالات و المراسلات الالكترونية من جميع الانتهاكات حماية منه للحياة الخاصة، كما أنه يمكن اسناد حماية الفضاء الرقمي الى قوانين حماية الملكية الفكرية و ذلك بادراجه للمصنفات الرقمية كجزء من المصنفات التي تشملها الحماية بموجب هذه القوانين، ضف الى ذلك حماية التعامل في المجال الالكتروني بسنه لقواعد خاصة بالتوقيع و التصديق الالكترونيين، و يبدو من خلال هذه النصوص و التعديلات تاثر المشرع الجزائري بالمبادرات الدولية و الاتفاقيات و على وجه الخصوص اتفاقية بودابست المبرمة سنة 2001 و التابعة لمجلس اوربا واضحا، و لا سيما من خلال المصطلحات التي جاء بها المشرع الجزائري و بعض الاحكام التي جاءت متوافقة مع هذه الاتفاقية.

الفصل الثاني: الآليات الإجرائية والهيكلية لتحقيق الامن السبيراني في التشريع الجزائري

ان الوصول الى فضاء سبيراني امن لا يتحقق بسن قواعد موضوعية وحدها اذ لابد أن ترافقه آليات إجرائية تحدد المسار المشروع للتصدي لهذا النوع المستحدث من التهديدات لا سيما وان الاليات الاجرائية التقليدية لا يمكن لها ان تفي بالغرض المنشود نظرا لاعتماد الفاعلين في الميدان السبيراني على تقنيات و أساليب جد متطورة، وقيام الأفعال فيها في واقع مفترض يتعامل مع كيانات منطقية غير ملموسة، وهذا ما جعل المشرع الجزائري يتماشى مع هذا التطور ويحدد آليات جديدة تتلائم مع طبيعة هذا النوع من الأفعال تضاف الى تلك الإجراءات للكشف و التحري عن الجريمة في المسرح التقليدي، وذلك من خلال سن إجراءات جديدة في قانون الإجراءات الجزائية يتشترك فيها مع بعض أنواع الأخرى من الجرائم الخطيرة بالإضافة الى سن اجراءات خاصة لمكافحة هذا النوع من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال، من جهة أخرى فان طبيعة الجريمة السبيرانية العابرة للحدود جعل التعاون الدولي في هذا المجال وسيلة مهمة وناجعة لتحقيق الامن السبيراني لا سيما في مجال تبادل المعلومات والخبرات، ولاضفاء نوعا من النجاعة والحماية المقربة استحدث مؤسسات اوكل لها مهمة الرقابة المباشرة والسهر على حسن تطبيق القواعد المقررة قانونا حسب مجال تخصصها ومؤسسات أخرى تكون مختصة للتحري عن هذا النوع من الجرائم بالإضافة الى مؤسسات قضائية متخصصة. لذلك نحاول في هذا الفصل دراسة الآليات الاجرائية لتحقيق الامن السبيراني (المبحث الأول)، ثم نتطرق الى الهيئات الفاعلة لتحقيق الأمن السيبراني (المبحث الثاني).

المبحث الأول: الآليات القانونية الإجرائية لتحقيق الأمن السيبراني

لم تتاثر القواعد الموضوعية وحدها بالمباردات الدولية لتحقيق السبيراني فالقواعد الإجرائية بدورها تاثرت بهذه الأخيرة، ذلك لأن الإشكالات التي أصبحت تعيق طريق الوصول الى الكشف عن الأفعال التي تتم في الفضاء الرقمي و عدم نجاعة القواعد التقليدية فرضت على المشرع ان يجد آليات مفيدة للتصدي لهذا النوع من الأخطار، والذي اصبح يشكل تهديدا حقيقيا على الامن والسكينة العامة، اذ حين المشرع بعض القواعد التقليدية وذلك بتمديده للاختصاص المحلي للشرطة القضائية الى كامل التراب الوطني في الجرائم الماسة بانظمة المعالجة الالية، و جواز إمكانية التفتيش و المعاينة و الحجز في المحلات السكنية و غير السكنية في كل ساعات النهار او الليل في هذه الجرائم، بالاضافة الى جواز تمديد الوقف للنظر لمرة واحدة، الا انه وبالرغم من ذلك فانه اصبح لازما إضفاء آليات إجرائية جديدة وهو ما فعله المشرع سنة 2006 بموجب القانون رقم 06-22 المتضمن تعديل القانون الإجراءات الجزائية والذي تم فيه تبني أساليب جديدة للتحري، وبعد ذلك تم سن إجراءات خاصة بهذا النوع من الجرائم دون سواه نظرا للطابع التقني الذي تتمتع به هذه السلوكات، وذلك بموجب القانون رقم 09-04المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

المطلب الأول:

الآليات الاجرائية المستحدثة في قانون الإجراءات الجزائية

إن عدم قدرة أساليب التحري التقليدية على تحقيق الغاية المنشودة منها نظرا لما تتمتع به الجرائم السيبرانية من خصوصية وصعوبة في اثباتها من جهة، وخطورتها على الفرد والمجتمع والدولة من جهة اخرى، وخاصة أن مرتكبيها في غالب الأحيان هم أشخاص لهم دراية عالية بمجال التقنية والمعلومات ويعتمدون على وسائل متطورة، دفع المشرع لاستحداث أساليب جديدة للتحري تتخذها الضبطية القضائية تحت مراقبة واشراف السلطة القضائية نظرا لمساسها بالخصوصية المكفولة دستوريا.

وقد استحدث المشرع هذه الإجراءات بموجب القانون رقم 06-22[1] بإضافة الفصل الرابع والخامس إلى الباب الثاني تحت عنوان وسائل التحري الخاصة وهي المتمثلة في: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، والتسرب.

[1] القانون 06-22 المؤرخ في 20-12-2006 يعدل ويتمم الامر 66-155 المتضمن قانون الإجراءات الجزائية، ج ر ج ج العدد 84.

الفرع الأول:

اعتراض المراسلات والتسجيل والتقاط الصور

وهو ما يطلق عليه اسم الترصد الالكتروني[1] نص عليه المشرع في المادة 65 مكرر 05 من قانون الإجراءات الجزائية دون تعريفه مكتفيا بتحديد مجال تطبيق هذا النظام، والذي حصره في بعض الجرائم المحددة من بينها الجرائم الماسة في المعالجة الآلية للمعطيات[2] ويقصد بها تلك العملية التي تسمح بمراقبة سرية المراسلات السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة أو المعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو في مشاركتهم ارتكاب الجريمة وتتم عن طريق الاعتراض والتسجيل والنسخ للمراسلات والتي هي عبارة عن بيانات قابلة للإنتاج أو التوزيع أو التخزين أو الاستقبال أو العرض، والملاحظ أن المشرع استبعد الخطابات الخطية التي تتم عن طريق البريد[3].

وبالنسبة لتسجيل الأصوات فهو تلك العملية التقنية التي تتم بواسطتها مراقبة وتسجيل المحادثات الشفوية التي يتفوه بها شخص أو عدة أشخاص بصفة سرية في مكان خاص أو عام[4].

أما بالنسبة لالتقاط الصور فهو تلك العملية التقنية التي يتم بواسطتها التقاط صور لشخص أو عدة أشخاص بغض النظر عن طبيعة مكان تواجدهم سواء كان خاصا أو عاما، ويطلق على هذه التقنية التصوير الفوتوغرافي ويتم بواسطة أجهزة دقيقة ومتطورة[5].

واللجوء إلى هذه الإجراءات يجب أن يكون مصحوبا بجمله من الشروط القانونية والمتمثلة في:

– توافر إذن مكتوب من الجهات القضائية المختصة، أي من طرف وكيل الجمهورية في مرحلة التحقيق الابتدائي، أو من طرف قاضي التحقيق في مرحلة التحقيق القضائي تحت طائلة بطلان الإجراء القضائي.

– التسبيب وذلك بتبيان دواعي اللجوء إلى الاعتراض ومراقبة المراسلات ومدى جدية تلك الدواعي ودورها في إظهار الجريمة والجناة.

---

[1] عبد الحليم بن بادة، محمد سعد بوحادة، المرجع السابق، ص25.

[2] أسامة مصعل، الإجرام السيبراني، مذكرة ماستر، تخصص قانون جنائي، قسم الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة سنة2018، ص46.

[3] محمد شنه، "إجراءات البحث والتحري عن الجرائم في التشريع الجزائري"، ط 1، ألفا للتوثيق والنشر والتوزيع، 2024، ص109.

[4] انظر المادة 65 مكرر 5 من قانون 06-22، المصدر السابق.

[5] نادية تياب، آليات مواجهة الفساد في الصفقات العمومية رسالة مقدمة لنيل شهادة الدكتوراه كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2014/2013، ص337.

– تحديد الجرائم محل الاعتراض والمراقبة التي لا يتوجب أن لا تخرج عن ما هو مقرر قانونا مع مراعاة سرية الإجراءات وكتمان السر المهني[1].

– يجب تحرير عن الانتهاء محضر عن كل عملية اعتراض أو تسجيل للمراسلات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتركيب والتسجيل الصوتي أو السمعي البصري والذي يجب أن يتضمن تاريخ وساعة بداية هذه العمليات والانتهاء منها[2].

– نسخ المراسلات أو الصور والمحادثات المسجلة في إظهار الحقيقة في محضر يودع بالملف، كما تنسخ وتترجم المكالمات التي تتم باللغات الأجنبية عند الضرورة بمساعدة مترجم يسخر لهذا الغرض.

الفرع الثاني:

التسرب

نظم المشرع الجزائري هذا الإجراء في المواد 65 مكرر 11 إلى غاية المادة 65 مكرر 18 من ق.إ.ج وقد عرفه في المادة 65 مكرر 12 بأنه قيام ضابط أو عون الشرطة القضائية بهوية مستعارة تحت مسؤولية ضابط مكلف بتنسيق العملية لمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بايهامهم أنه فاعل معهم أو شريك لهم.

وعليه فالتسرب عملية منظمة يحضر لها بدقة تامة، تستهدف أوساطا معينة قائمة على دراسة مسبقة لها بحيث يتم الوقوف على أدق خصوصياتها وتفاصيلها[3] وتهدف هذه العملية إلى التوغل داخل خلية إجرامية ومعرفة نشاطاتها والكشف عن الأشخاص المتورطين سواء كانوا فاعلين أصليين أم شركاء، وذلك بتوفير جميع الوسائل البشرية والتقنية اللازمة[4].

– **أولا : شروط التسرب**

ونظرا لما تتطلبه عملية التسرب من سرية وحيطة وحذر حرص المشرع على إحاطته بجعله من الشروط من أجل حسن سير هذه العملية.

---

[1] نوال مجدوب، "الآليات الإجرائية للكشف عن الجريمة المعلوماتية"، مجلة البحوث القانونية والاقتصادية، المركز الجامعي مغنية، المجلد 06، العدد 3، 2023، ص203.

[2] انظر المادة 65 مكرر 9 من 06-22، المصدر السابق.

[3] محمد شنه، المرجع السابق، ص117.

[4] زيدان زبيحة، المرجع السابق، ص169.

– الشروط المتعلقة بطبيعة الجريمة:

أتاح المشرع الجزائري إمكانية اللجوء إلى إجراء التسرب في الجرائم المنصوص عليها بالمادة 65 مكرر 3 من ق.إ.ج على سبيل الحصر ومن بين هذه الجرائم نجد بعض أنواع الجرائم السيبرانية والمتعلقة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

– الشروط المتعلقة في المتسرب:

اشترط المشرع الجزائري أن يكون المتسرب إما ضابط من ضباط الشرطة القضائية أو عونا للشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية[1] ويشترط فيه اطلاعه على كيفية استعمال الوسائل الإعلامية والتقنية الحديثة كالإعلام الآلي وتقنياته، أجهزة الاتصال والوسائل الأخرى[2]، لاسيما وأن عملية التسرب في نطاق الجريمة السيبرانية تتمثل في دخول العون المتسرب إلى العالم الرقمي وذلك باختراقه لمواقع معينة وفتح ثغرات الكترونية فيها أو اشتراكه في محادثات غرف الدردشة، أو الظهور بمظهر كما لو كان فاعلا مثلهم مستخدما أسماء أو صفات وهمية[3].

ومن أجل تمكين المتسرب من انجاز العملية على أحسن وجه أباح القانون القيام ببعض التصرفات المجرمة قانونا لاسيما استخدام هوية مستعارة[4] وله في هذا الشأن تغيير اسمه أو لقبه وبيانات الحالة المدنية بصفة عامة، وكذا بطاقات الهوية الشخصية إلى غير ذلك[5].

كما أقر القانون عدم قيام مسؤولية الجزائية في بعض الأفعال المحددة على سبيل الحصر وهي:

– اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.

– استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال[6].

---

[1] المادة 65 مكرر 12 من القانون 06-22، المصدر السابق.

[2] محمد شنه، المرجع السابق، ص119.

[3] أسامة مصمل، المرجع السابق، ص49.

[4] انظر المادة 65 مكرر 12 من قانون 06-22، المصدر السابق.

[5] محمد شنه، المرجع السابق، ص120.

[6] انظر المادة 65 مكرر 14، من قانون 06-22 ، المصدر السابق.

ومن أجل ضمان أمن العنصر المتسرب فقد جرم القانون كشف هوية المتسرب وشد العقوبة في حال تسبب هذا الكشف المساس بالسلامة الجسدية لهم ولأفراد عائلتهم (أزواج وأبناء وأصول مباشرين)[1] وتزيد العقوبة في حال تسبب الكشف في وفاة أحد هؤلاء الأشخاص.

– الشروط المتعلقة بالإجراءات عملية التسرب:

إن عملية التسرب التي يقوم بها ضابط الشرطة القضائية أو العون الذي يعمل تحت مسؤوليته يجب أن تكون بموجب إذن صادر من وكيل الجمهورية أو قاضي التحقيق حسب الحالة، كما يجب أن يكون هذا الإذن مكتوبا ومسببا وذلك تحت طائلة البطلان، ضف إلى ذلك ذكر الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤولية[2].

تحديد ضابط الشرطة المكلف بتنسيق عملية التسرب تقديرا يتضمن العناصر الضرورية لمعاينة الجرائم بشرط أن لا تعرض هذه الجرائم من الضابط أو العون المتسرب للخطر وكذا الأشخاص المسخرين طبقا للمادة 65 مكرر 14[3].

– الشروط المتعلقة بالمدة:

لا يمكن أن تتجاوز مدة عملية التسرب المحددة في الإذن 4 أشهر كحد أقصى مع إمكانية تجديد المدة حسب مقتضيات التحري والتحقيق وضمن نفس الشروط الشكلية والزمنية، كما يجوز للقاضي الذي أذن بإجرائها أن يأمر بتوقيفها قبل القضاء المدة المرخص بها[4]. غير أنه وفي حالة اللجوء إلى ذلك فإن العون المتسرب يمكن له أن يواصل في نشاطاته للوقت الكافي لتوقيف عملية المراقبة وهو نفس الأسلوب الذي أجازه القانون في حال انتهاء المدة المحددة برخصة التسرب وعدم تجديدها وذلك ولتهيئة الظروف الملائمة لتوقف العنصر المتسرب عن هذا النشاط وذلك حفاظا على سلامته على أن لا يتجاوز هذه المدة 04 أشهر على أكثر تقدير[5].

وما تجدر الإشارة إليه أن المشرع الجزائري ونظرا لخطورة هذه الجرائم والتي يسمح فيها اللجوء إلى أساليب التحري الخاصة وخصوصيتها واتساع نطاق ارتكابها ولزوم السرعة لمجابهتها مدد اختصاص ضباط الشرطة القضائية

---

[1] المادة 65 مكرر 16، من قانون 06-22، المصدر السابق

[2] انظر المادة 65 مكرر 15 من قانون 06-22، المصدر نفسه.

[3] انظر المادة 65 مكرر 13 من قانون 06-22، المصدر نفسه.

[4] المادة 65 مكرر 15 من قانون 06-22، المصدر نفسه.

[5] انظر المادة 65 مكرر 17 من قانون 06-22، المصدر نفسه.

إلى كامل الإقليم الوطني وهذا من ضمن التدابير غير المألوفة والتي استحدثها المشرع الجزائري من أجل مواجهة هذه الجرائم بطريقة أكثر فعالية.

المطلب الثاني:

الآليات المستحدثة وفقا لقانون الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها

نظرا للطبيعة التقنية التي يتميز بها الجرائم السيبرانية ومتطلبات تحقيق الأمن السيبراني استحدث المشرع الجزائري بموجب القانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بعض الإجراءات والآليات للوقاية والتصدي للجرائم السيبرانية والتي تقع في عالم فضاء افتراضي، إذ جاء بأحكام تتلائم مع خصوصية هذه الجرائم خاصة ما تعلق بإجراءات التحقيق والتفتيش وحجز المعطيات والاستعانة بكل شخص له دراية وخبرة لمساعدة جهات التحقيق في الكشف عن الجريمة المعلوماتية.

الفرع الأول:

مراقبة الاتصالات الالكترونية:

نص المشرع على هذا الإجراء بموجب المادة 03 من القانون 04/09 ويقصد به مراقبة شبكة الاتصالات أو استخدام التقنية الالكترونية لجمع المعطيات والمعلومات عن المشتبه فيه سواء كان شخصا أو مكانا أو شيئا مرتبط بالزمن لتحقيق غرض أمني أو لأي غرض آخر[1]، فالمراقبة الالكترونية هي إجراء تستعمل فيه تقنية المعلومات لمراقبة وتتبع كل ما يقوم به المشتبه فيه من إرسال واستقبال لمكالمات صوتية أو كتابات أو صور أو معلومات باستعمال وسائل تكنولوجيات الإعلام والاتصال[2].

-أولا: حالات اللجوء إلى المراقبة الالكترونية:

حدد المشرع الجزائري الحالات التي يتم فيها اللجوء إلى مراقبة الاتصالات على سبيل الحصر وهي:

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

---

[1] عبد الحليم بن بادة، محمد سعد بوحادة، المرجع السابق، ص28.

[2] ليندة بومحراث، مداخلة بعنوان: إجراءات التحقيق الخاصة بالجرائم السيبرانية يوم دراسي حول: الجريمة السيبرانية، مجلس قضاء قسنطينة وجامعة الأمير عبد القادر للعلوم الإسلامية، يوم 20 أفريل 2022، ص19.

– لمقتضيات التحديات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث دون اللجوء إلى المراقبة الالكترونية.

– في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[1].

وباستقراء هذه المادة نجد أن المشرع الجزائري لم يعتبر هذا الإجراء طريقة من طرق الحصول على الأدلة الجنائية الرقمية فقط، بل أدرجه أيضا ضمن التدابير الوقائية من الجريمة السيبرانية حماية للنظام العام من التهديد[2].

–ثانيا: الضوابط المتعلقة بالمراقبة الالكترونية:

نص المشرع الجزائري على مجموعة من الضوابط والشروط التي يتم احترامها عند اللجوء إلى إجراء المراقبة الالكترونية وذلك نظرا لخطورة هذا الإجراء على حقوق وحريات الفرد، وهذه الضوابط تتمثل في:

– الإذن: يعد الإذن من بين الضمانات التي وضعها المشرع الجزائري للحفاظ على خصوصية الأفراد، إذ لا يجوز إجراء عمليات المراقبة الالكترونية إلا بإذن من السلطات القضائية المختصة، وذلك حتى لا يتم تقييد حرية الأفراد وخصوصيتهم في سرية الاتصالات في حالة ما إذا تركت الحرية للرجال الضبطية القضائية في مراقبة الاتصالات الالكترونية، وجاعلا إياه في يد السلطات القضائية المختصة وفي حالة الجرائم الموصوفة بجرائم الإرهاب والتخريب والماسة بأمن الدولة يتم منح الإذن لضباط الشرطة القضائية من قبل النائب العام لدى مجلس قضاء الجزائر، ويكون صالحا لمدة 06 أشهر قابلة للتجديد.

كما شدد المشرع على أن المعطيات المجمعة من عملية المراقبة تكون موجهة حصريا للوقاية من الاعتداءات الإرهابية، والماسة بأمن الدولة وذلك تحت طائلة العقوبات في حالة المساس بالحياة الخاصة للغير.

عند الانتهاء من المراقبة السرية للاتصالات يتم تسجيل تلك الاتصالات وتخزينها على وسائط مادية قابلة للنقل، بغية استخدامها فيما بعد لإثبات الجريمة الواقعة.

وما ينبغي الإشارة إليه أن المراقبة السرية للاتصالات الالكترونية لا يمكن اعتبارها نوعا من أنواع التفتيش وذلك لورودها على البيانات الالكترونية المتحركة والتي تتجسد هنا بالاتصالات الالكترونية حال اجرائها دون تلك التي انتهت وخزنت في حيث أن التفتيش يرد على البيانات الالكترونية الساكنة أو المخزنة[3].

---

[1] انظر المادة 4 من قانون رقم 09-04 ، المصدر السابق

[2] سليمان النحوي، آليات مكافحة الجريمة السيبرانية في التشريع الجزائري، مداخلة مقدمة ضمن فعاليات الملتقى الدولي، المنظم من طرف كلية الحقوق والعلوم السياسية، قسم الحقوق جامعة برج بوعريريج الموسوم بعنوان: الإجرام السيبراني المفاهيم والتحديات، يومي 11 و12 أفريل 2017، ص14.

[3] ليندة بومحراث، المرجع السابق ص21.

الفرع الثاني:

تفتيش المنظومة المعلوماتية

أورد المشرع الجزائري هذا الإجراء في المادة الخامسة من قانون 04/09، والتفتيش بوجه عام هو إجراء قضائي يهدف إلى الحصول على أدلة تساعد في كشف الحقيقة ويتميز بخاصتي الجبر والإكراه، أي أن الإنسان يخضع له مجبرا، إذا لم يوافق على إجرائه برضاه، ويتضمن هذا الإجراء مساسا بمستودع سر الإنسان، سواء كان مسكنا أو جسمه، وهو إجراء يهدف إلى جمع الأدلة التي تساهم في كشف الحقيقة[1].

ويقصد بالتفتيش في الجريمة السيبرانية تفتيش النظم المعلوماتية ولو عن بعد من خلال جمع الأدلة المخزنة أو المسجلة بشكل الكتروني كالملفات والبرامج المخزنة في الحواسيب والمعطيات والاتصالات الالكترونية سواء كانت معطيات ذات طابع مادي أو معنوي تفيد كدليل الكتروني في الكشف عن الحقيقة أو هو البحث الدقيق أو الإطلاع على محل منحه القانون حماية خاصة[2].

وقد أجاز المشرع اللجوء إلى هذا الإجراء في نفس الحالات التي يتم اللجوء فيها إلى إجراء مراقبة الاتصالات الالكترونية[3].

أولا: ضوابط إجراء تفتيش المنظومة المعلوماتية

يتكون محل التفتيش من مكونات مادية لكل منها وظيفة محددة وتصل مع بعضها بشكل يجعلها تعمل كنظام متكامل مثل الشاشة ولوحة المفاتيح ووحدة الذاكرة، ووحدة التحكم ووحدة الإخراج[4]، كما يتكون من مكونات معنوية والتي تسمى أيضا بالكيانات المنطقية وهي مجموعة البرامج والوثائق المتعلقة بتشغيل وحدة معالجة البيانات[5]، كما يتكون إضافة إلى ذلك من شبكات الاتصال البعدية السلكية واللاسلكية والتي تشمل في مكوناتها مقدم الخدمة والمزود الآلي المضيف والملحقات التقنية[6].

---

[1] سامي جلال ففي حسين، ا"لتفتيش في الجرائم المعلوماتية (دراسة مقارنة)"، ط01، دار الكتب القانونية، القاهرة، مصر، 2011، ص55.

[2] يوسف مناصرة، "الدليل الالكتروني في القانون الجزائري دراسة مقارنة"، ط01، دار الخلدونية، الجزائر، 2021، ص348.

[3] انظر المادة 05 من القانون 09-04، المصدر السابق.

[4] خالد عياد الحلبي، "إجراءات التحدي والتحقيق في جرائم الحاسوب والانترنت"، ط 1، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011، ص158

[5] زيدان زيبحة ز، المرجع السابق، ص132.

[6] عائشة بوخبزة ، الحماية الجزائرية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماجيستير في القانون الجنائي، كلية الحقوق، جامعة وهران، 2013، ص179.

ويخضع الدخول إلى المكونات المادية للحاسوب بحثا عن الشيء المتعلق بالجريمة المعلوماتية من أجل كشف الحقيقة عنها وعن مرتكبها للإجراءات القانونية الخاصة بالتفتيش، وإن جواز تفتيش تلك المكونات يتوقف على طبيعة المكان الموجودة فيه هل هو مكان عام أم مكان خاص، فإذا كانت موجودة في مكان خاص فلا يجوز تفتيشها إلا بنفس الضمانات المقررة قانونا في التفتيش التقليدي[1]. والتفتيش في الكيانات المادية للحاسوب لا يشكل أي عائق نظرا لسهولة ضبط المجهزة وحجزها واتلافها إلا أن الأشكال يثور عندما ينصب التفتيش على مكونات الكمبيوتر المعنوية كالبرامج وقواعد البيانات، ذلك أن تفتيش هذه البيانات يتطلب الكشف عن الرقم السري للمرور إلى الملفات وكذا كلمات السر أو الشفرات[2]، هذا من جهة ومن جهة أخرى فإن مدى صلاحية معطيات الحاسوب للتفتيش هو في حد ذاته محل جدل فقهي[3]، إذ يرى جانب من الفقه أن المكونات المعنوية لا تصلح بطبيعتها لأن تكون محلا للتفتيش باعتبار أن التفتيش يهدف إلى ضبط أدلة مادية، كما يرى بعضهم أن النبضات والإشارات الالكترونية الممغنطة لا تعد من قبيل الأشياء المحسوسة وبالتالي لا تأخذ حكم الأشياء المادية عند التفتيش، وهذا يقتضي أحكاما خاصة، في حين يرى جانب آخر من الفقه أن المكونات المعنوية تخضع للتفتيش مثلها مثل المكونات المادية[4] ومرد ذلك إلى عمومية نصوص التفتيش للتوسع في تفسيرها من أجل مد حكمها إلى البيانات المخزنة آليا في الأنظمة المعلوماتية[5]. وقد حسم المشرع الجزائري هذا الجدل في نص المادة 05 من القانون 04/09 وأجاز الدخول بغرض التفتيش إلى المكونات المعنوية للحاسب الآلي.

أما في مجال التفتيش في شبكات الحاسوب فإن المشرع الجزائري قد تفطن إلى تقنية ذات أهمية بالغة في عالم المعلوماتية ويتعلق الأمر بارتباط شبكة الحواسيب ببعضها البعض، وبالتالي وجود ترابط بين الأنظمة المعلوماتية، فشبكة الانترنت هي نفسها شبكة ممتدة من خلال اتصال أجهزة الحواسيب الآلية اتصالات سلكيا أو لا سلكيا فتكون مرتبطة ببعضها البعض في مكان واحد وهو ما يطلق عليه الشبكة المحلية أو موزعة ومرتبطة بواسطة خطوط

---

[1] خالد عباد الحلبي، المرجع السابق، ص159.

[2] زيدان زيبحة، المرجع السابق، ص132.

[3] نبيلة هبة هروال، "الجوانب الإحداثية لجرائم الانترنت في مرحلة الاستدلالات"، د.ط، دار الفكر الجامعي، الإسكندرية، مصر، 2013، ص225.

[4] كوثر عز الدين، بشرى آية عبد المومن، إجراءات البحث والتحدي في الجريمة الالكترونية، مذكرة ماستر تخصص قانون أعمال، قسم الحقوق جامعة الشادلي بن جديد، الطارف، 2022، ص57.

[5] نبيلة هبة هروال، المرجع السابق، ص227.

الهاتف أو بواسطة الأقمار الصناعية[1] وهو ما عبر عليه المشرع بعبارة "لو عن بعد" في نص المادة 05 من القانون 05-04 وهذا الامتداد لشبكات الحاسوب يمكن أن يكون في دولة واحدة أو عدة دول.

ثانيا: حالات تمديد التفتيش

1- الحالة الأولى: تمديد التفتيش إلى منظومة معلوماتية داخل الإقليم الوطني

إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها[2]، والملاحظ أن تمديد التفتيش إلى منظومة أخرى بناء على هذا النص يكتسي طابعا خاصا فهو يجرى عن بعد، ويقوم على مجرد الشك ويتم بشكل سريع تماشيا مع طابع السرعة الفائقة التي يجرى فيها نقل المعلومة أو المعلومات[3] وخوفا من طمس وإتلاف الأدلة الرقمية، وقد أوجد هذا النص حلا لمشكلة تجاوز الاختصاص المحلي كجهة التحقيق وحماية خصوصية الغير من الاعتداءات[4]، وذلك بالزامه إعلام السلطة القضائية المختصة مسبقا.

2- الحالة الثانية: تمديد التفتيش إلى منظومة معلوماتية خارج الإقليم الوطني

من المشاكل التي تواجه سلطات الادعاء في جمع الأدلة قيام مرتكبي الجرائم بتخزين بياناتهم في أنظمة تقنية المعلومات خارج الدولة عن طريق شبكة الاتصالات البعدية بهدف عرقلة التحقيقات، ولمواجهة هذه الإشكالية بدأت التشريعات القانونية في التصدي لها عن طريق إمكانية التفتيش في حاسوب متواجد في إقليم أجنبي ومن بين هذه التشريعات التشريع الجزائري، إلا أنه وتفاديا لتحفظ الفقه على القيام بهذا الإجراء لانتهاكه سيادة الدولة الأجنبية[5]، فإن المشرع جعل الحصول على المعطيات المبحوث عنها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل[6].

---

[1] زيدان زيبحة، المرجع السابق، ص139.

[2] انظر المادة 05 من قانون 09-04، المصدر السابق.

[3] زيدان زيبحة، المرجع السابق، ص140.

[4] عاشور عياشي، عبد الحق يعيش، آليات مكافحة جريمة التجسس الالكتروني في التشريع الجزائري، مذكرة ماستر تخصص قانون الإعلام الآلي والانترنت، قسم الحقوق، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2024، ص ص 69، 70.

[5] نبيلة هبة هروال، المرجع السابق، ص240.

[6] انظر المادة 05 من القانون 09-04، المصدر السابق.

ونظرا لما تطلبه التفتيش والجانب التقني لهذه الأفعال فإن المشرع أجاز الاستعانة بذوي الاختصاص سواء عن طريق تسخير من لديهم خبرة في مجال عمل المنظومة المعلوماتية بغية مساعدة الجهة القائمة بتفتيش المنظومة المعلوماتية، وتزويدها بكل ما من شأنه تسهيل مهمتها.

الفرع الثالث:

حجز المعطيات المعلوماتية

نص المشرع الجزائري على هذا الإجراء في المادة 06 من القانون 09-04، ويعرف الحجز بأنه العثور على أدلة خاصة بالجريمة التي يباشر التحقيق بشأنها وحفظ هذه الأدلة، والضبط هو الغاية من التفتيش والنتيجة المستهدفة من خلاله[1]، إلا أنه وإن كان حجز الأشياء المادية كالمعدات والأوراق والمستندات بعد شيئا سهلا وغير مثيرا لأي إشكالات في نظر القانون فإنه ليس من السهل أبدا توقيع الحجز على منظومة معلوماتية ذلك أن المعلومات هي في الأصل شيء معنوي[2].

وقد أثار محل الحجز في الجرائم المعلوماتية جدلا كبيرا بدوره وانقسم فقهاء القانون إلى قسمين: يرى أنصار القسم الأول أن المعلومات المعالجة الكترونيا في عالم افتراضي غير مادي وغير ملموس لا يمكن حجزها الا عن طريق التصوير أو نقلها بواسطة مختلف دعائم التخزين الالكترونية.

فيما يرى أنصار الاتجاه الثاني أن المعلومات المعالجة الكترونيا ماهي إلا ذبذبات الكترونية أو موجات كهرومغناطيسية قابلة للتسجيل والحفظ والتخزين، يمكن نقلها وبثها واستقبالها وإعادة انتاجها وبذلك لا يمكن إنكار وجودها المادي[3].

وقد انحاز المشرع الجزائري إلى الاتجاه القائل بإمكانية حجز المعلومات وهو ما يظهر من خلال استقراء نص المادة 06 من قانون 09-04 وذلك بتأكيده على إمكانية حجز المنظومة المعلوماتية برمتها إذا كان ذلك ضروريا لمصلحة التحقيق أو القيام بحجز المعطيات المعنية بالذات.

---

[1] إيمان ثابت، آسية ميهوب، إجراءات التحري الخاصة في الجريمة الالكترونية، مذكرة ماستر تخصص قانون الإعلام الآلي والانترنت، كلية الحقوق والعلوم السياسية، جامعة البشير الإبراهيمي، برج بوعريريج، 2024، ص 71.

[2] زيدان زيبحة، المرجع السابق، ص148.

[3] ايمان ثابت –آسية ميهوب ، المرجع السابق، ص71-72.

أولا: التدابير المتعلقة بعملية حجز المعطيات المعلوماتية

وذلك بعد نسخها على دعامة مادية أو أي وعاء للبيانات كطبعها على الورق أو ضبطها على الشاشة وذلك لتسهيل قراءتها والتعامل معها ذلك لعدم إمكانية التعامل مع تلك المعطيات في شكلها الأولي المعنوي وهي عبارة عن نبضات أو ذبذبات الكترونية أو إشارات ممغنطة[1].

1- الحفاظ على سلامة المعطيات:

إضافة إلى إلزام المشرع نسخ المعطيات محل البحث وحتى المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في احراز وفقا لقانون الإجراءات الجزائية، ألزم السلطة القائمة بالتفتيش والحجز الحفاظ على سلامة هذه المعطيات، كما أجاز استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات[2].

2- منع الإطلاع على المعطيات المحجوزة ذات المحتوى المجرم

أجاز المشرع الجزائري للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الإطلاع على هذه المعطيات التي يشكل محتواها جريمة وكمثال عن هذه الإجراءات نص على تكليف أي شخص مؤهل للقيام بذلك باستعمال الوسائل التقنية اللازمة والمناسبة لذلك[3].

3- الحجز عن طريق منع الوصول إلى المعطيات

خشية محو أو إتلاف أو نقل أو ضياع الأدلة أعطى المشرع الجزائري وفقا للمادة 07 من القانون 09-04 للجهات القضائية سلطة الأمر بالتحفظ عليها، وقد حصر حالات اللجوء إلى هذا الإجراء في حالة وحيدة وهي استحالة إجراء الحجز لأسباب تقنية وفي هذه الحالة يتعين على سلطة التحقيق استعمال التقنيات اللازمة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة أو إلى نسخها.

---

[1] زيبدان زيبحة، المرجع السابق، ص150.

[2] انظر المادة 02 من القانون 09-04، المصدر السابق.

[3] انظر المادة 08 من القانون 09- 04، المصدر نفسه.

4- استعمال المعطيات المحجوزة في الحدود الضرورية للتحريات والتحقيقات القضائية

منع المشرع استعمال المعلومات المتحصل عليها من أي استعمال غير مشروع تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به وجعل استعمال هذه المعلومات إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية[1]، إذ تبقى هذه المحجوزات تحت تصرفها إلى غاية انتهاء إجراءات المحاكمة.

ثانيا: الصعوبات المتعلقة بحجز المعطيات المعلوماتية

نظرا للطابع الخاص الذي تتميز به الجرائم السيبرانية فإن حجز المعطيات والأدلة الرقمية يعتريه الكثير من الصعوبات من أبرزها:

- ضخامة حجم وكم البيانات والملفات المعلوماتية التي تتواجد في البيئة المعلوماتية تصعب من إمكانية تحديد الملفات والبيانات المعلوماتية المجرمة من بين هذا الكم الهائل[2].

- صعوبة ضبط الوسائل الفنية المستخدمة في إتلاف البرامج مثل الفيروس، وضبط بيانات الكمبيوتر Data لعدم وجود أي دليل مرئي في هذه الحالات.

- سهولة تدمير الدليل في ثوان معدودات[3] وصعوبة استعادة الأدلة وإعادة تركيبها نظرا لاستعمال بعض البرامج المتخصصة في إخفاء المعلومات والبيانات وذلك لخلق ما يعرف بنظام ملفات أمن عبر استخدام الشبكة العالمية (الانترنت)[4].

- صعوبة اكتشاف هذه الجرائم لعدم تركها لأي أثر خارجي[5] لأن هذا النوع من الجرائم لا تخلف في الغالب آثار مادية كتلك التي تخلفها الجرائم التقليدية إذ لا يمكن رؤيتها إلا من خلال الاستعانة بأجهزة ووسائل تقنية[6] باعتبارها تكون في شكل أرقام من قطع صلبة ورموز وشيفرات.

---

[1] انظر المادة 09 من القانون 09-04، المصدر السابق.

[2] أسماء عاصف، الجرائم الرقمية وطرق إثباتها، مذكرة ماستر، تخصص قانون قضائي، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، 2024، ص 66.

[3] أمير فرج يوسف، "الجرائم المعلوماتية على شبكة الانترنت"، دار المطبوعات الجامعية، الإسكندرية، طبعة 2009، ص237.

[4] أمير فرج يوسف، ا"لأدلة الالكترونية ودورها في مكافحة الجريمة الالكترونية والمعلوماتية"، ط 1، مؤسسة المعرفة لنشر وتوزيع الكتب، مصر، 2024، ص44.

[5] أشرف عبد القادر قنديل، "الإثبات الجنائي في الجريمة الالكترونية"، دار الجامعة الجديدة للنشر، مصر، طبعة 2015، ص97.

[6] أسماء عاصف، المرجع السابق، ص65.

– صعوبة تحديد مكان تواجد جهاز الحاسب الآلي مصدر النشاط الإجرامي لذلك تستعين سلطات التحقيق بنظام الفحص الالكتروني يسمى بعلم البصمات المعاصر الذي يتم من خلال تتبع الحركة العكسية لمسار الانترنت إلى غاية الوصول إلى عنوان الرقمي للجهاز[1].

– الأحجام عن الإبلاغ والذي يكون مرده إما عدم دراية المجني عليه بإصابة نظامه بفيروس معلوماتي واعتداء على منظومته المعلوماتية مما ينتج عنه عدم إمكانية حجز الدليل الرقمي لفوات مدة طويلة عن الفعل، أو يكون مرده رغبة المجني عليه في عدم التبليغ حفاظا على الثقة بينه وبين الذين يستخدمون هذا النظام[2].

– صعوبة الحصول على الأدلة من أجهزة الكمبيوتر الموجودة في دولة أخرى، وحتى في حالة وجود إجراءات دولية والتي من شأنها تسهيل تبادل الأدلة الرقمية، فإن معظم هذه الإجراءات معقدة وهي ليست عملية مناسبة لهذا النوع من الجرائم والتي تتميز بالسرعة والخطورة[3].

– نقص الخبرة لدى رجال الضبط القضائي وأجهزة الأمن بصفة عامة وكذلك لدى أجهزة العدالة الجنائية ممثلة في سلطات الاتهام والتحقيق الجنائي وذلك فيما يتعلق بثقافة الحاسب الآلي والالمام بعناصر الجرائم المعلوماتية وكيفية التعامل معها[4].

الفرع الرابع:

فرض التزامات على مقدمي الخدمات

إن صعوبة الحصول على الدليل في مجال الجرائم السيبرانية والتعرف على هوية الجاني يقتضي الاستعانة بمقدمي الخدمات[5] ولهذا فإن المشرع فرض جملة من الالتزامات بغرض تسهيل عمل سلطات التحقيق ولتحقيق النجاعة اللازمة لتحقيق الأمن السيبراني ومن هذه الالتزامات:

---

[1] عبد القادر فلاح، "حجز وحفظ المعطيات في الجريمة الالكترونية"، مجلة صوت القانون، جامعة خميس مليانة، المجلد 8، العدد 01، 2021، ص182.

[2] خيرت على محرز، "التحقيق في جرائم الحاسب الآلي"، د.ط، دار الكتاب الحديث، الجزائر، 2012، ص 50.

[3] أمير فرج يوسف، الأدلة الالكترونية ودورها في مكافحة الجريمة الالكترونية والمعلوماتية، المرجع السابق، ص42.

[4] خيرت على محرز، المرجع السابق، ص81.

[5] مقدمي الخدمات عرفها المشرع في المادة 2 فقرة د على أنهم: كل كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام الاتصالات، وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها.

أولا: مساعدة سلطات التحقيق

يجب على مؤدي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية والتفتيش و ذلك بجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وهي المعطيات المحددة في المادة 11 من القانون 09-04 ووضعها تحت تصرف هذه السلطات.

كما يتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين والمعلومات المتصلة بها تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق[1].

ثانيا: حفظ المعطيات المتعلقة بحركة السير

لقد رتب القانون 09-04 على عاتق مقدم خدمة الانترنت كذلك التزاما آخر طبقا للمادة 11 وهو:

- حفظ المعلومات التي من شأنها تمكين جهات التحقيق من التعرف على مستعملي الخدمة والمعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.
- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.
- المعطيات التي تسمح بالتعرف على المرسل إليه والمرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

وقد حدد مدة الاحتفاظ بهذه المعطيات لمدة سنة واحدة من تاريخ التسجيل، كما جعل الاخلال بهذه الالتزامات يؤدي إلى قيام المسؤولية الجزائية في حالة ما إذا أدى هذا الاخلال إلى عرقلة حسن سير التحريات القضائية[2].

ثالثا: التدخل الفوري لسحب المحتويات

يتعين علي مقدمي خدمات الانترنت التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن، كما يجب عليهم وضع ترتيبات تقنية تسمح بحضر إمكانيات الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام والآداب العامة وأخبار المشتركين لديهم بوجودها[3].

---

[1] انظر المادة 10 من القانون 09-04، المصدر السابق.

[2] انظر المادة 11 من القانون 09- 04، المصدر نفسه.

[3] رضوان عثماني، مكافحة جرائم المعلوماتية في القانون الجزائري والدولي، أطروحة دكتوراه تخصص قانون جنائي، جامعة وهران 2، محمد بن أحمد، 2024، ص 108.

المطلب الثاني:

التعاون الدولي لتحقيق الأمن السيبراني

ان من السمات المميزة للجرائم السبيرانية هي انها جريمة عابرة للحدود و لا يقتصر نطاقها على المستوى الوطني و انما يتعداه ليشمل النطاق الاقليمي و حتى الدولي هذا ما يتبعه قصور التشريعات الداخلية عن تحقيق الامن السبيراني و هو ما جعل من التعاون الدولي آلية ناجعة تكمل ما جاءت به التشريعات الداخلية في مجال البحث عن الأدلة وتبادل المعلومات والخبرات وحتى تنفيذ الاحكام وفي هذا الاطار سنتطرق الى التعاون الدولي على المستوى الأمني ثم التعاون الدولي على المستوى القضائي و من ثم نعرج للحديث عن التعاون الدولي بخصوص تسليم المجرمين .

الفرع الأول:

التعاون الدولي على المستوى الأمني

يقصد بالتعاون الأمني الدولي هو تبادل العون والمساعدة وتضافر الجهود المشتركة بين طرفين دوليين أو أكثر لتحقيق نفع أو خدمة أو مصلحة مشاركة في مجال التصدي لمخاطر الإجرام، وما يرتبط به من مجالات أخرى.[1] و قد سعت الجزائر الى توطيد علاقات التعاون الدولي مع العديد من المنظمات الدولية و الإقليمية في اطار مكافحة الجريمة السبيرانية[2] نذكر منها:

أولا– المنظمة الدولية للشرطة الجنائية (الأنتربول).

تعد هذه المنظمة أقدم صور التعاون الامني في مكافحة الجريمة، أنشئت سنة 1923 بفينا و يقع مقرها الرسمي بمدينة ليون الفرنسية، انضمت الجزائر إلى هذه المنظمة أثناء انعقاد الجمعية العامة للأنتربول في هلسنكي بفنلندا، خلال شهر أوت 1963 بمشاركة 53 دولة ممثلة بالمكتب المركزي الوطني، حيث يعمل هذا الأخير تحت الوصاية المباشرة لمديرية الشرطة القضائية – المديرية العامة للأمن الوطني ويباشر مهامه وفقا لنصوص التشريعات الوطنية ملتزما بالأطر القانونية المسيرة للمنظمة الدولية للشرطة الجنائية[3].

---

[1] رضوان عثماني المرجع السابق ص 190.

[2] اسيا لعمراني، "التعاون الدولي في مجال الجريمة السيبرانية:الجزائر نموذجا "، المجلة الجزائرية للعلوم السياسية و العلاقات الدولية، المجلد 03، العدد 02 ، ديسمبر 2010، ص 84.

[3] رضوان عثماني، المرجع السابق، ص 192.

وتقوم هذه المنظمة بالعمل على التنسيق بين أجهزة الشرطة للدول الأعضاء من أجل التعاون في مكافحة الجريمة الالكترونية[1]، ومن بين مهامها في هذا المجال هو تعقب مجرمي المعلوماتية عامة وشبكة الأنترنت خاصة، أيضا تعقب الأدلة الرقمية وضبطها والقيام بعملية التفتيش العابر للحدود لمكونات الحاسب الآلي المنطقية والأنظمة المعلوماتية وشبكات الاتصال بحثا عن ما قد تحويه من أدلة وبراهين على ارتكاب الجريمة الالكترونية[2]، حيث يتم تبادل المعلومات من خلال منصة الاتصالات الآمنة التي تعمل على مدار الساعة وطوال أيام الأسبوع من أجل تسهيل التحقيقات المتعلقة بالجرائم الالكترونية وذلك من أجل تحقيق الأمن السيبراني[3]، إضافة إلى قيامها بتنظيم دورات تكوينية لتبادل الخبرات وتقديم الدعم الفني لأجهزة الشرطة، والمصالح الأمنية الدولية حتى يتسنى إعطاء بعد دولي لعملها[4].

ثانيا– منظمة الشرطة الجنائية الافريقية (الأفريبول):

هي أكبر منظمة شرطة في القارة الإفريقية أنشئت في 13 ديسمبر 2015 بالجزائر مكونة من قوات الشرطة لـ41 دولة، و يقع مقرها في الجزائر العاصمة ترتكز مهام الأفريبول في مضاعفة رصيد التعاون الشرطي الإقليمي والدولي، تحديد السياسة العامة للشرطة الجنائية وتوفير التكوين وإعادة تأهيل مختلف أجهزة الشرطة الإفريقية التي تشهد تأخرا أو ضعفا على مستوى الأداء، تعزيز قيم السلم والأمن والاستقرار في القارة الإفريقية، رفع التحديات وإيجاد الحلول الجادة والفعالة للجرائم العديدة التي تواجهها بعض الدول الإفريقية و التي من بينها الجرائم المعلوماتية[5].

و قد أولت الجزائر أهمية بالغة لآلية التعاون الشرطي الأفريقي كونها أداة تعاون إقليمية في غاية الأهمية لمجابهة المخاطر الجديدة التي باتت أداة تهدد الأمن والسلم الدوليين في إطار مواصلة السعي مع جميع الأطراف والشركاء للرقي بها وبأدائها[6] و يتمثل الدور الأساسي لهذه المنظمة الأفريبول في مكافحة الجرائم وتعقب المجرمين، حيث تعتبر

---

[1] يوسف حسن يوسف، "الجرائم الدولية للأنترنت"، ط1، المركز القومي للإصدارات القانونية، القاهرة، مصر،2001، ص146.

[2] حسين بن سعيد بن سيف الغافري، "السياسة الجنائية في موجهة جرائم الأنترنت (دراسة مقارنة)"، دار النهضة العربية، القاهرة، مصر، سنة 2009، ص507.

[3] شعبان أبو عجيلة عصارة، أبو المعالي محمد عيسى أبو المعالي، "الرصد المبكر لخطر الجريمة،" مجلة العلوم القانونية والشرعية، كلية القانون، جامعة الزاوية، ليبيا، العدد السادس (06)، يونيو2015، ص321.

[4] الحاج عيسى بن عمر ، "الأنتربول كآلية دولية شرطية لمكافحة الجريمة المنظمة العابرة للحدود"، مجلة الدراسات القانونية والسياسية، جامعة عمار تيجي بالأغواط، الجزائر، العدد الثالث، جانفي2016، ص262.

[5] براهيم جمال، التحقيق الجنائي في الجرائم الالكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص القانون، قسم الحقوق، كلية الحقوق والعلوم الإنسانية، جامعة مولود معمري، تيزي وزو، الجزائر، 2018، ص308.

[6] أسيا لعمراني، المرجع السابق، ص87.

الجرائم التي تقع في الفضاء الإلكتروني أخطر الجرائم التي تهدد الأمن العالمي، فالأنظمة الدفاعية وكذا البيانات الحساسة المتعلقة بالدول، بل وحتى الإستراتيجيات الاقتصادية للشركات العالمية الكبرى أصبحت متداولة في هذا الفضاء السبيراني مما جعله يصبح مجالا مستهدفا من خلال اختراق شيفرات أنظمة الدول والحصول على معلومات لذلك فإن محور اهتمام الأفريبول أضحى يتماشى مع التطورات الحاصلة على الصعيد العالمي والإقليمي من خلال التنسيق وتبادل الأدلة الالكترونية لمكافحة الإجرام الإلكتروني[1].

ثالثا– الوكالة الأوروبية لمكافحة الجريمة (اليوروبول):

إقترح انشاء جهاز اليوربول في قمة لكسمبورج عام 1991، بوصفه مكتبا مركزيا للشرطة الجنائية في دول الإتحاد الأوروبي، تم تأسيسه بموجب إتفاقية ماستريخت، ووقعت إتفاقية اليوروبول في بروكسل بتاريخ 26 يونيو 1995 من قبل سفراء 15 دولة عضو في الإتحاد الأوروبي و دخلت اتفاقية يوروبول حيز التنفيذ في أكتوبر 1998 و لم يبدأ هذا الجهاز نشاطه الا سنة 1999[2] و قد تم العمل على تطوير التعاون الدولي للشرطة بين الدول الأعضاء في الاتحاد الأوروبي ودول جنوب البحر الأبيض المتوسط، وكذلك بين دول جنوب البحر الأبيض المتوسط فيمابينها، في مجال مكافحة الجوانب الرئيسية للجريمة المنظمة بدءا بالإرهاب، ثم تهريب المخدرات، الاتجار بالبشر، الجريمة المالية، جرائم الأنترنت، الإتجار بالأسلحة، التهريب والتزوير والمخاطر الناجمة عن الأحداث الكبرى، كما أنشأ جهاز الشرطة الأوروبية (أوروبول) في 2015 وحدة لمحاربة جرائم المعلوماتية تغطي القارة الأوروبية بأكملها كما تم إقرار التعاون الأمني في جوان 2018 بين وكالة الشرطة الأوروبية "أوروبول" ودول عربية وإسلامية مثل الجزائر ومصر والأردن ولبنان والمغرب وتونس وتركيا لتعزيز سبل التعاون في مجال تبادل المعلومات والبيانات الشخصية للأفراد.[3] و يعتبر هذا الجهاز من بين اهم اليات مكافحة الجرائم السبيرانية نظرا لتمتعه بامكانيات كبيرة في مجال تكنولوجيا المعلومات و الاتصالات مما يتيح له تتبع الأنشطة الاجرامية بكفاءة وسرعة[4].

---

[1] عبد العزيز لزعر، رشيد زياني، آلية الإتحاد الإفريقي للتعاون الشرطي (الأفريبول) ودورها في مكافحة الجريمة الإلكترونية the african union police cooperation mechanism (afripd) and its role infighting cyber-crime، مجلة متون ((Moutouneاج د، مولاي الطاهر سعيدة، المجلد 14، العدد 3، جامعة معسكر مخبر الأدوات القانونية للسياسة العقارية مخبر تشريعات القانون الإقتصادي، معسكر، ص255،258.

[2] محمد نذير بن عرفة – يوسف حوري، "اليوروبول كالية لمكافحة الجريمة الالكترونية"، مجلة الدراسات القانونية والسياسية، المجلد 11، العدد 01، جانفي 2025، ص ص 38-39.

[3] اسيا لعمراني، المرجع السابق، ص 86.

[4] محمد نذير بن عرفة- يوسف حوري، المرجع السابق، ص 38

رابعا– وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية (الأوروجيست)

بدأت مناقشة إنشاء وحدة تعاون قضائي لأول مرة في إجتماع المجلس الأوروبي في تامبيري بفلندا يومي 15و 16 من شهر أكتوبر سنة 1999، بحضور رؤساء الدول والحكومات وفي 14 من شهر ديسمبر سنة 2000 وبمبادرة من البرتغال وفرنسا والسويد وبلجيكا، تم تشكيل وحدة تعاون قضائي مؤقتة تحت إسم (pro Eurojust) بدأت عملها رسميا في الفاتح من شهر مارس سنة 2001، وبعد هجمات 11من شهر سبتمبر 2001 التي شهدتها الولايات المتحدة الأمريكية، إزداد التركيز على مكافحة الإرهاب. ولم يعد الأمر ينصب على المجال الوطني والإقليمي فقط بل تعداه ليشمل البعد الدولي مما دفع المجلس الأوروبي إلى إصدار قرار في 28 من شهر فبراير سنة 2002 تم من خلاله إنشاء الأوروجيست كوحدة تنسيق قضائي[1]. وهي وكالة تابعة للاتحاد الأوربي تتعاون قضائيا في المسائل الجنائية يقع مقرها في مدينة لاهاي الهولندية، مهمتها الأساسية هي التنسيق بين السلطات القضائية المكلفة بالتحقيقات ولها من الصلاحيات ما يؤهلها لفتح تحقيق ومباشرة متابعة جزائية[2]. وتعتبر هذة الوكالة دعامة فعالة في مجال التحقيقات والملاحقات التي تقوم بها السلطات القضائية الوطنية خاصة فيما يتعلق بالإجرام الإلكتروني.[3]

الفرع الثاني:

التعاون الدولى على المستوى القضائي

إن التعاون القضائي يعد الآلية الرئيسية للكفاح ضد الجريمة العابرة للحدود بأبعادها المختلفة وفيما يتعلق بالجريمة الالكترونية فان فعالية التحقيق والملاحقة القضائية غالبا ما تقتضي الحاجة إلى مساعدة السلطات في البلد الذي كان منشأ للجريمة، أو من السلطات في البلد الذي عبر من خلاله النشاط المجرم وهو في طريقه إلى الهدف أو المكان الذي قد توجد أدلة الجريمة [4]، و هي عبارة عن إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بخصوص جريمة من الجرائم [5]. و لقد نص المشرع على التعاون و المساعدة القضائية الدولية في الفصل السادس من القانون 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال

---

[1] خضرة شنتير ، المرجع السابق، ص250.

[2] عبد العزيز أحمد، خصوصية التحقيق في الجريمة المعلوماتية، مذكرة مقدمة لنيل شهادة الماستر في الحقوق، تخصص القانون الجنائي والعلوم الجنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الدكتور الطاهر مولاي سعيدة، 2021-2022، ص52.

[3] اسيا لعمراني، المرجع السابق ص86.

[4] فاطمة اخلاص بن عزوز – وهيبة سالمي، المرجع السابق، ص 56.

[5] رضوان عثماني المرجع السابق، ص197.

و مكافحتها و اكد على إمكانية تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكتروني[1].

أولا: صور التعاون القضائي الدولي: وتتمثل فيمايلي:

1- تبادل المعلومات:

ويشمل مبدأ تبادل المعلومات تقديم البيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة أجنبية وهي بصدد النظر في جريمة الكترونية، و فد نصت على هذه الصورة الكثير من الاتفاقيات الدولية كاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية [2]، و كذا اتفاقية الرياض للتعاون القضائي العربي[3] بشأن ضرورة تبادل المعلومات بين الدول الأطراف والتنسيق بين الأنظمة القضائية، والاتفاقية المتعلقة بالتعاون القضائي بين الجزائر وفرنسا الموقعة بتاريخ 05 أكتوبر سنة 2016.[4]

وقد نص المشرع الجزائري على هذه الصورة في المادة 17 من القانون 04/09 مؤكدا على ان استجابة الدولة الجزائرية لطلبات تبادل المعلومات لا يكون الا في إطار الاتفاقيات الدولية ذات الصلة ومبدأ المعاملة بالمثل.

2 – نقل الإجراءات:

ويقصد به قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية، وهي بصدد جريمة ارتكبت في إقليم دولة أخرى و لمصلحة هذه الدولة ، متى توافرت شروط معينة من أهمها التجريم المزدوج الذي يقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات، بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها[5].

ولقد أقرت العديد من الاتفاقيات الدولية منها والإقليمية هذه الصورة كإحدى صور المساعدة القضائية الدولية على غرار اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية.

---

[1] انظر المادة 16 من القانون 09-04، المصدر السابق.

[2] صادقت عليها الجزائر بتحفظ بتاريخ 05-02-2002 بموجب المرسوم الرئاسي رقم 02-55 الصادر بتاريخ 10-02-2002، ج ر العدد 09

[3] صادقت عليها الجزائر بتاريخ 11-02-2001 بموجب المرسوم الرئاسي رقم 01-47 الصادر بتاريخ 12-02-2001، ج ر ج ج العدد 11.

[4] صادقت عليها الجزائر بتاريخ 25-02-2018 بموجب المرسوم الرئاسي رقم 18-73 الصادر بتاريخ 28-02-2018، ج ر ج ج العدد 13.

[5] اسيا لعمراني، المرجع السابق، ص83.

3- الانابة القضائية

تجد الانابة القضائية أساسها القانوني في القانون الجزائري في المواد 721 و ما بعدها من قانون الإجراءات الجزائية و يقصد بهذه الصورة طلب اتخاذ إجراء قضائي من إجراءات الدعوى العمومية تتقدم به الدولة الطالبة إلى دولة اخرى لتعذر القيام بهذا الإجراء بنفسها وهدف هذه الصورة تسهيل الإجراءات الجزائية بين الدول بما يكفل إجراء التحقيقات اللازمة[1] لكشف الحقيقة لاسيما سماع الشهود وإجراء المعاينات وكافة إجراءات التحقيق، وترسل للدولة المنابة ملف بالدعوى الجنائية مرفق بمحاضر الاستدلالات والتحقيقات والمستندات، ويبين في طلب الإنابة الإجراء المراد اتخاذه تحديدا، و يرسل من الجهات القضائية وبالطريق الدبلوماسي[2]، وفي هذا الصدد فان الإنابة القضائية على هذا النحو تستلزم وقتا أكثر مما يحتمل الأمر في العالم الافتراضي، وهو ما يستلزم ضرورة التعاون القضائي بصور أكثر فعالية بما يحقق عنصر الزمن لما له من أهمية في مجال مواجهة الجريمة الإلكترونية[3].

وتجدر الإشارة ان الانابة القضائية في مجال التعاون الدولي بشكل عام والجريمة السيبرانية بشكل خاص تواجهها عده عقبات لاسيما ما يتعلق ببطء تنفيذ الانابة و إجراءاتها بسبب فوارق اللغة والاختلاف في الإجراءات وغيرها من الأسباب، كما انها تصطدم بعقبة أخرى وهي مبدأ السيادة و ذلك ان ارتكاب هذا النوع من الجرائم في احدى الدول ومحاكمته في دولة أخرى باعتبارها الدولة التي وقت فيها النتيجة الجرمية تستوجب البحث عن الأدلة في البلد الذي وقعت فيه باعتباره مسرحا للجريمة ما يجعل الدول تتمسك باختصاصها على أساس مبدا الاقليمية والذي يعد مظهرا من مظاهر السيادة[4].

وفي هذا السياق فان المشرع الجزائري تمسك باختصاصه في حالة ارتكاب الجرائم المتصلة بتكنولوجيا الاعلام والاتصال خارج الإقليم الوطني من طرف اجنبي و تستهدف مؤسسات الدولة الجزائرية او الدفاع الوطني او المصالح الاستراتيجية للاقتصاد الوطني[5]

---

[1] فاطمة اخلاص بن عزوز – وهيبة سالمي، المرجع السابق، ص 59.

[2] انظر المادة 721 من الامر 66-155، المصدر السابق.

[3] رضوان عثماني المرجع السابق، ص201.

[4] اسيا صوان ، التعاون الدولي في مكافحة الجرائم المعلوماتية، مذكرة ماستر تخصص الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، 2022، ص 77.

[5] المادة 15 من القانون 09-04، المصدر السابق.

ثانيا– القيود الواردة على المساعدة القضائية الدولية

لم يجعل المشرع الجزائري تنفيذ طلبات المساعدة القضائية على اطلاقه فقد الزم رفض تنفيذها اذا كان من شأنها المساس بالسيادة الوطنية او النظام العام و من جهة أخرى فقد ألزم ان تكون الاستجابة لطلبات المساعدة مقيدة بشرط الحفاظ على سرية المعلومات المبلغة او بشرط عدم استعمالها في غير ما هو موضح في الطلب [1].

الفرع الثالث:

التعاون الدولي على مستوى تسليم المجرمين

يعتبر اعتبار تسليم المجرمين شكل من أشكال التعاون الدولي في كافحة الجريمة والمجرمين وحماية المجتمعات من المخلين بأمنها واستقرارها وعدم افلات المجرمين من العقاب فهو عمل بمقتضاه تقوم الدولة التي لجأ إلى أرضها شخص متهم أو محكوم عليه في جريمة تسلمه إلى الدولة المختصة لمحاكمته أو تنفيذ العقوبة عليه[2]. وقد نصت عليه العديد من الاتفاقيات الدولية لا سيما اتفاقية بودابست المبرمة بسنة 2001 والاتفاقية العربية لمكافحة جرائم تقنية المعلومات[3] ويجد تسليم المجرمين أساسه القانوني في التشريع الداخلي في الباب الأول من الكتاب السابع المتضمن العلاقات بين السلطات القضائية الأجنبية.

أولا– شروط تسليم المجرمين:

يتم تسليم المجرمين بناء على شروط محددة نوجزها في مايلي:

– لا يمكن تسليم أحد الا بمقتضى اتفاقية دولية مصادق عليها او بموجب قانون.

– ان لا يكون المطلوب لاجئا سياسيا استفاد قانونا من حق اللجوء.[4]

– ازدواجية التجريم : بان يكون المطلوب تسليمه قد اقترف فعلا مجرما في كلا تشريع الدولتين باعتباره جناية أو جنحة في القانون الجزائري و يعاقب عليه بعقوبة جناية او عقوبة جنحة اذا كان الحد الأقصى للعقوبة المطبقة سنتين او اقل في الدولة الطالبة او اذا تعلق بمتهم قضي عليه بعقوبة تساوي او تجاوز الحبس لمدة شهرين، اما بخصوص الشروع والاشتراك فانه تطبق عليه نفس القواعد بشرط ان يكون معاقبا عليه في الدولتين، ويتم التسليم بدون إعطاء

---

[1] المادة 18 من قانون 09-04، المصدر السابق.

[2] فاطمة اخلاص بن عزوز – وهيبة سالمي، المرجع السابق، ص60.

[3] صادقت عليها الجزائر بتاريخ 08 سبتمبر 2014 بموجب المرسوم الرئاسي رقم 14-252 الصادر بتاريخ 28 سبتمبر 2014، ج ر ج ج العدد 57.

[4] المادة 50 من دستور الجمهورية الجزائري الديمقراطية الشعبية الصادر بموجب المرسوم الرئاسي 20-442 بتاريخ 30-12-2020، ج ر ج ج، العدد 82.

اعتبار لمدة العقوبة اذا كان الشخص المطلوب تسليمه قد سبق الحكم عليه في أي بلد كان بحكم نهائي بالحبس لمدة شهرين او اكثر في جنحة من جنح القانون العام.[1]

- أن لا يكون المطلوب تسليمه جزائريا الجنسية بوقت وقوع الجريمة المطلوب التسليم من اجلها.
- أن لا يكون للجناية او الجنحة صبغة سياسية او لا يكون التسليم مطلوب لغرض سياسي.
- أن الا تكون الجناية او الجنحة ارتكبت في الأراضي الجزائرية.
- أن لا تكون الوقائع قد تمت المتابعة فيها والحكم نهائيا في الأرضي الجزائرية ولو كانت ارتكبت خارجها.
- ان لا تكون الدعوى العمومية قد سقطت بالتقادم طبقا لقوانين الدولة الطالبة او المطلوب اليها التسليم.
- ان لا يكون صدر عفو في الدولة الطالبة او الدولة المطلوب اليها التسليم في حال ارتكاب الجريمة من الجرائم التي يجوز ان تكون موضوع متابعة في هذه الدولة اذا ارتكبت خارج اقليمها من شخص اجنبي عليها.[2]

ويثار في هذا الصدد بعض العوائق التي تواجه إجراءات تسليم المجرمين لاسيما تلك المتعلقة بازواجية التجريم وعدم تماشي التشريعات الوطنية مع بعضها في هذا المجال وقصور بعض التشريعات في التجريم في المجال السبيراني لاسيما امام حداثة هذا النوع الاجرام، وتزاحم طلبات التسليم لنفس الشخص سواء عن نفس الجريمة او لجرائم أخرى.[3]

ثانيا- إجراءات تسليم المجرمين:

- يوجه طلب التسليم إلى الحكومة الجزائرية بالطريق الدبلوماسي ويرفق به إما الحكم الصادر بالعقوبة وإما أوراق الإجراءات الجزائية التي صدر بها الأمر رسميا بإحالة المتهم إلى جهة القضاء الجزائي، أو التي تؤدي إلى ذلك بقوة القانون وإما أمر القبض أو أية ورقة صادرة من السلطة القضائية ولها ذات القوة على أن تتضمن هذه الأوراق الأخيرة بيانا دقيقا للفعل الذي صدرت من أجله وتاريخ هذا الفعل[4].

- يتولى وزير الخارجية تحويل طلب التسليم بعد فحص المستندات ومعه الملف إلى وزير العدل لذي يتحقق من سلامة الطلب ويعطيه خط السير الذي يتطلبه القانون.[5]

---

[1] المادة 697 من الامر 66- 155، المصدر السابق.

[2] المادة 698 من الامر 66-155، المصدر نفسه.

[3] صوان اسيا، المرجع السابق، ص 78.

[4] انظر المادة 702 من الامر 66-155، المصدر السابق.

[5] انظر المادة 703 من الامر 66-155، المصدر نفسه.

-يقوم النائب العام باستجواب الأجنبي للتحقق من شخصيته ويبلغه المستند الذي قبض عليه بموجبه وذلك خلال الـ 24 ساعة التالية للقبض عليه.[1]

- ينقل الأجنبي في أقصر أجل ويحبس في سجن العاصمة، وتحول في الوقت ذاته المستندات المقدمة تأييدا لطلب التسليم إلى النائب العام لدى المحكمة العليا الذي يقوم باستجواب الأجنبي، ويحرر بذلك محضرا خلال 24 ساعة طبقا لاحكام المواد 705 و 706 من قانون الإجراءات الجزائية.

- ترفع المحاضر وكافة المستندات إلى الغرفة الجنائية بالمحكمة العليا، ويمثل الأجنبي أمامها في ميعاد أقصاه ثمانية أيام تبدأ من تاريخ تبليغ المستندات ، اين يتم استجوابه.[2]

- إذا قرر صاحب الشأن عند مثوله أنه يتنازل عن التمسك بالنصوص السابقة وأن يقبل رسميا تسليمه إلى سلطات الدولة الطالبة فتثبت المحكمة هذا الإقرار، وتحول نسخة من هذا الإقرار بغير تأخير بواسطة النائب العام إلى وزير العدل لاتخاذ ما يلزم بشأنها[3] وفي الحالة العكسية تقوم المحكمة العليا بإبداء رأيها المعلل في طلب التسليم ويكون هذا الرأي في غير صالح الطلب إذا تبين للمحكمة وجود خطأ او ان الشروط القانونية غير مستوفاة، وهذا الرأي يكون نهائيا لما جاء في المواد 709 و 710 من قانون الإجراءات الجزائية.

[1] المادة 704 من الامر 66-155، المرجع السابق.
[2] المادة 707 من الامر 66-155، المرجع نفسه.
[3] المادة 708 من الامر 66-155، المرجع نفسه.

المبحث الثاني: الآليات الهيكلية لتحقيق الأمن السيبراني

أولى المشرع الجزائري عناية لتحقيق الامن السيبراني وذلك بزيادة اعتماد أنظمة أمن معلومات متطورة تندرج ضمن إستراتيجية وطنية شاملة لحماية البنى التحتية المعلوماتية، التي أضحت في صميم الاستخدامات اليومية لتكنولوجيات الإعلام والاتصال وشبكات الإنترنت ضف الى ذلك قام باستحداث هيئات ومؤسسات متخصصة لمكافحة الجريمة السيبرانية بالنظر إلى تعقيداتها وتنامي مخاطرها وتختلف هذه الهياكل حسب طبيعتها الى هياكل قضائية وهياكل غير قضائية، وهو ما سنتطرق اليه في هذا المبحث.

المطلب الأول:

الهيئات القضائية

في إطار محاربة الجرائم المعقدة والتي تندرج ضمنها الجرائم الماسة بانظمة المعالجة الالية للمعطيات تم استحداث مؤسسات قضائية جديدة تتمثل في الأقطاب الجزائية المتخصصة، ومن جهة أخرى ونظرا للطابع التقني للجرائم المتصلة بتكنولوجيا الاعلام والاتصال تم استحداث مؤسسة قضائية خاصة بهذا النوع من الجرائم دون غيرها وهي القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.

الفرع الأول:

الأقطاب الجزائية المتخصصة

نظرا لتزايد الجرائم المعقدة كان من الضروري على الدولة الجزائرية تطوير آليات خاصة لمواجهتها ولهذا السبب تم إستحداث الأقطاب الجزائية المتخصصة التي سنتطرق إليها في هذا الفرع.

أولا: تعريف الأقطاب الجزائية المتخصصة:

سعى المشرع الجزائري من وراء إنشائه للأقطاب الجزائية المتخصصة إلى سد العجز القائم على فكرة غياب هيئات قضائية متخصصة ومؤهلة لمكافحة الإجرام المستحدث على الصعيدين المحلي والدولي وخاصة بعد اثبات عجز القضاء العادي وعدم قدرته على التكفل بهذا النوع من الإجرام.

المشرع الجزائري لم يعط تعريفا قانونيا للأقطاب الجزائية المتخصصة، بل أكثر من ذلك فانه لا يوجد أي نص قانوني أو تنظيمي يؤسس لهذا المصطلح باستثناء نص المادة 24 من القانون العضوي 05-11[1]، الذي تضمن

[1] المادة 24 من القانون العضوي رقم 05-11 مؤرخ في 10 جمادى الثانية 1426 الموافق ل17 يوليو 2005 يتعلق بالتنظيم القضائي، ج رج ح عدد 51 الصادر في 13 جمادى الثانية 1426 الموافق ل20 يوليو 2005.

إقرارا صريحا من المشرع على إمكانية إنشاء أقطاب قضائية متخصصة ذات اختصاص إقليمي موسع لدى المحاكم، يتحدد اختصاصها النوعي في قانون الإجراءات الجزائية حسب الحالة[1].

غير أن هذا النص لقد فقد أثره بعد ما أصدر المجلس الدستوري رأيا بعدم دستوريته، غير أن المشرع الجزائري لما أدرج في المادة 24 من القانون العضوي 05-11 إمكانية إنشاء أقطاب يكون قد أدرج حكما تشريعيا في نص قانوني عضوي، وأخل بالتبعية لذلك بالمبدأ الدستوري القاضي بتوزيع مجالات الاختصاص المستمد من المادتين 122 و123 من الدستور، والذي يخول هذه الصلاحية للقوانين العادية وليس العضوية[2].

الا انه يمكن تعريفها من خلال مهامها بأنها جهات قضائية ذات اختصاص إقليمي موسع أنشئت لغرض النظر في بعض الجرائم التي حددها القانون حصرا والمتمثلة في جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.[3] بالإضافة إلى اختصاصها بالنظر في جرائم الفساد التي أدرجها المشرع ضمن مجال اختصاصها النوعي بموجب تتميم قانون الوقاية من الفساد ومكافحته.[4]

كما يمكن تعريفها أيضا بأنها عبارة عن جهات قضائية متخصصة للنظر في بعض الجرائم حددها القانون حصرا، بجانب الاختصاص الموسع الذي منحها إياها المشرع الجزائري فهي تمارس اختصاصها العادي.[5]

---

[1] إيمان رتيبة شويطر، "الأقطاب الجزائية المتخصصة كتوجه لمكافحة جرائم الأعمال"، مجلة البحوث في العقود وقانون الأعمال، المجلد 07، العدد 01، جامعة الإخوة منتوري، قسنطينة1، الجزائر،2022، ص51.

[2] رأي المجلس الدستوري رقم 01-ر.ق ع- م د- 05 مؤرخ في 10 جمادى الأولى 1426 الموافق ل 17 يونيو 2005، يتعلق بمراقبة مطابقة القانون العضوي المتعلق بالتنظيم القضائي للدستور، ج رج ج عدد 51 الصادر في 13 جمادى الثانية 1426 الموافق ل 20 يوليو 2005.

[3] المادة 37، 40-2، 329 فقرة أخيرة، من القانون رقم 14-04 مؤرخ في 27 رمضان 1425 الموافق ل10 نوفمبر 2004 يعدل ويتمم الأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، ج رج ج عدد 71 الصادرة في 27 رمضان 1425 الموافق ل10 نوفمبر 2004.

[4] المادة 24 مكرر 1 من الأمر 10-05 المؤرخ في 16 رمضان 1431 الموافق ل 26 أوت 2010 المعدل والمتمم للقانون رقم 06-01 المتعلق بالوقاية من الفساد ومكافحته، ج رج ج عدد 50 الصادرة في 01 سبتمبر 2010.

[5] عمیور خدیجة، "قواعد اختصاص الأقطاب الجزائية للنظر في جرائم الفساد"، مجلة دراسات في الوظيفة العامة، المركز الجامعي، البيض، الجزائر، العدد 02، ديسمبر 2014، ص 134.

ثانيا: نطاق اختصاص الأقطاب الجزائية المتخصصة:

حيث يتحدد اختصاص الأقطاب الجزائية المتخصصة كما يلي:

1- الاختصاص الإقليمي الموسع:

تختص الأقطاب الجزائية المتخصصة بالفصل حصريا في الجرائم التي جعلها القانون من اختصاصها، ويعقد اختصاصها الإقليمي ليشمل كافة مراحل الإجراءات من تحريات أولية إلى غاية صدور الحكم وتتميز هذه الأقطاب بأنها جهات قضائية أو محاكم ذات اختصاص محلي موسع، وهذا ما نصت عليه المواد 37 فقرة 02، 40 فقرة 02 و 329 فقرة أخيرة من قانون الإجراءات الجزائية المعدل والمتمم بالقانون 14-04، حيث تم بموجب هذه المواد توسيع الاختصاص المحلي لكل من وكيل الجمهورية وقضاة التحقيق والحكم في بعض المحاكم إلى دائرة الاختصاص المحلي للأقطاب الجزائية المتخصصة.[1]

واتبعت هذه النصوص بصدور المرسوم التنفيذي رقم 06-348 [2]المعدل والمعمم والمتمم بالمرسوم التنفيذي رقم 16- 264.[3] اين تم تحديد بموجب هذا المرسوم المحاكم ذات الاختصاص الإقليمي إليها كما يلي:

- القطب الجزائي المتخصص بمحكمة سيدي أحمد (الجزائر): ويمتد اختصاصه المحلي ليغطي منطقة الوسط، ويشمل المحاكم التابعة للمجالس القضائية التالية: الجزائر، الشلف، الأغواط، البليدة، البويرة، تيزي وزو، الجلفة، المدية، المسيلة، بومرداس، تيبازة وعين الدفلى.[4]

- القطب الجزائي المتخصص بمحكمة قسنطينة: ويمتد اختصاصها المحلي ليغطي مناطق الشرق ويشمل المحاكم التابعة للمجالس القضائية التالية:قسنطينة، أم البواقي، باتنة، بجاية، تبسة، جيجل، سكيكدة، سطيف، عنابة، قالمة، برج بوعريريج، الطارف، خنشلة، سوق أهراس، ميلة.[5]

---

[1] إيمان رتيبة شويطر، المرجع السابق، ص53.

[2] المرسوم التنفيذي 06-348 المؤرخ في 05 أكتوبر 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم و وكلاء الجمهورية و قضاة التحقيق، الصادر بتاريخ 08 أكتوبر 2006، ج ر العدد 63

[3] مرسوم تنفيذي رقم 16-267 مؤرخ في محرم 1438 الموافق ل17 أكتوبر 2016، يعدل المرسوم التنفيذي رقم 06-348 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج رج ج عدد 62 الصادرة في 21 محرم 1438 الموافق ل 23 أكتوبر 2016.

[4] المادة 2 من المرسوم التنفيذي رقم 06-348، مؤرخ في 12 رمضان 1427 الموافق ل 05 أكتوبر 2006، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج رج ج عدد 63 الصادرة في 15 رمضان 1427 الموافق ل08 أكتوبر 2006.

[5] المادة 2 فقرة 02 من المرسوم التنفيذي رقم 267-16، المرجع السابق.

– **القطب الجزائي المتخصص بمحكمة ورقلة:** ويمتد اختصاصه المحلي ليغطي مناطق الجنوب ويشمل المحاكم التابعة للمجالس القضائية التالية: ورقلة، أدرار، تامنغست، إيليزي، بسكرة، الوادي وغرداية.[1]

– **القطب الجزائي المتخصص بمحكمة وهران:** ويمتد اختصاصه المحلي ليغطي مناطق الغرب، ويشمل المحاكم التابعة للمجالس القضائية التالية: وهران، بشار، تلمسان، تيارت، تندوف، سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض، تيسمسيلت، النعامة، عين تيموشنت وغيليزان.[2]

2– الاختصاص النوعي:

إن قواعد الاختصاص النوعي من النظام العام، بحيث لا يجوز الإتفاق على مخالفتها من قبل الأطراف، ويقصد بالاختصاص النوعي سلطة مخولة لجهة قضائية بالفصل في دعاوى معينة دون سواها وتنعقد لها هذه السلطة بالنظر إلى طبيعة النزاع ونوعه بحيث تختص الأقطاب الجزائية المتخصصة وعلى سبيل الحصر بالنظر في الجرائم منها ما هو ذو طابع جنحي ومنها ما هو ذو طابع جنائي حددها لها القانون.

تتمثل هذه الجرائم المنصوص عليها في المواد 37 فقرة 02، 40 فقرة 02 و329 فقرة أخيرة من قانون الإجراءات الجزائية المعدل بالقانون رقم 04-14 تتمثل فيما يلي:

1- جرائم المخدرات.

2- الجريمة المنظمة العابرة للحدود الوطنية.

3- الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

4- جرائم تبييض الأموال.

5- جرائم الإرهاب.

6- الجرائم المتعلقة بالتشريع الخاص بالصرف.

7- جرائم الفساد.[3]

نستنتج من خلال هذه النصوص أن الاختصاص النوعي للأقطاب الجزائية المتخصصة منحصر في الجرائم التي تتسم بالخطورة والتعقيد والتي يجب تسخير جملة من الآليات المتطورة التي تساعد الأقطاب عند قيامها بالتحريات.

---

[1] المادة 2 فقرة 03 من المرسوم التنفيذي رقم 06-348، المصدر السابق.

[2] المادة 2 فقرة 04، المصدر نفسه.

[3] إيمان رتيبة شويطر، المرجع السابق، ص 54،55.

الاختصاص النوعي للأقطاب الجزائية المتخصصة هو اختصاص من نوع خاص، حيث تختص الأقطاب بالنظر في القضايا التي خولها إياها القانون صراحة على سبيل الحصر إلا أن اختصاصها هذا ليس اختصاص مانعا على غيرها من جهات القضاء، بل أنه معلق على شرط المطالبة بالإجراءات من قبل النيابة اذ يجوز لها بعد تبليغها بنسخة من ملف القضية أن تتركها تسير وفق الإجراءات القانونية العادية وأمام جهات القضاء العادي، بالرغم من أن الأمر يتعلق بإحدى الجرائم التي ينعقد الاختصاص بشأنها للقطب.[1]

ثالثا: المتابعة أمام الأقطاب الجزائية المتخصصة:

وضع المشرع الجزائري قواعد لتحديد كيفية انعقاد الاختصاص لهذه الجهات القضائية المتخصصة وذلك في المواد 40 مكررة إلى 40 مكرر 5 من قانون الإجراءات الجزائية وعليه سوف نقوم بتوضيح كيفية انعقاد الاختصاص للأقطاب الجزائية المتخصصة ثم سير المحاكمة أمامها.

1- إجراءات المطالبة وانعقاد لاختصاص للأقطاب الجزائية المتخصصة:

- اذا تعلق الامر بإحدى الجرائم التي يشملها الاختصاص النوعي للاقطاب الجزائية المتحصصة يحيل وكيل الجمهورية لدى المحكمة المختصة إقليميا نسخة من إجراءات التحقيق المحررة عن الشرطة القضائية الى وكيل الجمهورية لدى الجهة القضائية دات الاختصاص الإقليمي الموسع.[2]

- اذا اعتبرها وكيل الجمهورية لدى الجهة القضائية ذات الاختصاص الموسع تدخل ضمن اختصاص المحكمة يطالب بعد اخذ راي النائب العام بالاجراءات فورا، وفي هذه الحالة يتلقى ضباط الشرطة القضائية العاملين بدائرة اختصاص هذه المحكمة التعليمات منه مباشرة.[3]

- يمكن لوكيل الجمهورية لدى المحكمة ذات الاختصاص الإقليمي الموسع بعد اخذ راي النائب العام ان يطالب بملف الإجراءات خلال جميع مراحل الدعوى و في هذه الحالة اذا كان قد تم فتح تحقيق قضائي فان قاضي التحقيق يصدر امر بالتخلي عن الإجراءات لفائدة قاضي التحقيق لدى المحكمة ذات الاختصاص الإقليمي الموسع.[4]

---

[1] إيمان رتيبة شويطر، المرجع السابق، ص55.

[2] انظر المادة 40 مكرر 01 من قانون 20-04 المؤرخ في 30-08-2020 يعدل ويتمم الامر 66-155 المتضمن قانون الإجراءات الجزائية، ج ر ج ج العدد 51.

[3] انظر المادة 40 مكرر2، من قانون 20-04، المصدر السابق.

[4] انظر المادة 40 مكرر 03، من قانون 20- 04، المصدر نفسه.

2- سير المحاكمة أمام الأقطاب الجزائية المتخصصة:

يخضع نظام المحاكمة أمام المحاكم ذات الاختصاص الموسع للقواعد المقدرة في قانون الإجراءات الجزائية، سواء تعلق الأمر بالمبادئ التي تحكم المحاكمة أو بالإجراءات المتبعة إلى غاية صدور حكم في موضوع الجريمة وتتمثل اهم هذه المبادئ فيما يلي:[1]

– علنية الجلسات: الأصل هو علنية الجلسات فهي من أهم ضمانات التقاضي وبالتالي يتحقق بها حياد القاضي فيكون أكثر حرص على تحقيق العدالة. والاستثناء يجوز أن تجرى المحاكمة في جلسة سرية إذا كانت ما في العلنية ما هو خطر على النظام العام، غير أنه النطق بالحكم يجب أن يكون في جلسة علنية، وذلك استنادا إلى نص المادة 285 من قانون الإجراءات الجزائية اذا تعلق الامر بجناية و المادة 355 من نفس القانون اذا تعلق الامر بجنحة.

– شفهية المرافعات: يقصد بها أن تتم مناقشة الدفوع التي قدمها الخصوم وطلبات النيابة العامة شفاهة.

– الوجاهية: تجري إجراءات المحاكمة بحضور الخصوم او بعد تكليفهم طبقا للطرق القانونية ويعد ذلك من أهم ضمانات المحاكمة العادلة.[2]

الفرع الثاني:

القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

إستحدث المشرع الجزائري القطب الجزائي كجهة متخصصة لمعالجة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها بموجب الامر 21-11 المتضمن تعديل قانون الإجراءات الجزائية.

أولا: اختصاص القطب المستحدث:

نظرا لتفاقم الجرائم الإلكترونية قام المشرع الجزائري باستحداث هذا القطب كجهة متخصصة لمعالجة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والجرائم المرتبطة بها، ومنحه اختصاصا وطنيا من أجل تجاوز العوائق التي تواجهها الجهات القضائية.

[1] عميور خديجة، المرجع السابق، ص138.

[2] المواد 345- 346، من الامر 66-155، المصدر السابق.

1- الاختصاص النوعي:

يتحدد الاختصاص النوعي للمحاكم انطلاقا من تصنيف الجريمة الذي يبنى على العقوبة المقررة لها في القانون وذلك بعد تكييف الواقعة وربطها بالنص القانوني المناسب.[1]وينعقد اختصاص هذا القطب بالحكم في الجرائم المرتكبة او يسهل ارتكابها استعمال منظومة معلوماتية او نظام للاتصالات الالكترونية او أي وسيلة أخرى او الية ذات صلة بتكنولوجيات الاعلام و الاتصال و الجرائم المنصوص عليها في الباب السادس من قانون الإجراءات الجزائية اذا كانت تشكل جنحا[2].

بالنظر في أحكام المادة: 211 مكرر 22 من الأمر 21-11، فإن القطب المستحدث يختص بمعالجة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والجرائم المرتبطة بها، غير أنه ينبغي التمييز بين المراحل التالية:

- خلال مرحلة المتابعة الجزائية:

يتولى وكيل الجمهورية على مستوى القطب المستحدث استنادا إلى أحكام الفقرة الأولى من المادة 211 مكرر 22 من الأمر 21-11 بمتابعة كافة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها، سواء كانت القضية في طور البحث والتحري أو تم إيداع المحاضر الخاصة بها على مستوى نيابة الجمهورية، ويتصرف فيها طبقا للقانون.

- خلال مرحلة التحقيق القضائي:

بموجب أحكام الفقرة الأولى من المادة 211 مكرر22 من الأمر 21-11 يتولى قاضي التحقيق على مستوى القطب المستحدث بالتحقيق في كافة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها، ويتصرف فيها طبقا للقانون.

- خلال مرحلة المحاكمة:

حسب ما جاء في نص المادة 211 مكرر 22 في الفقرة الثانية منها من الأمر 21-11، يفوض لقاضي الحكم لدى القطب المستحدث بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها الموصوفة بالجنح، فلا يمكن لقضاة الحكم تناول الجرائم الموصوفة بالجنايات على مستوى القطب المستحدث، كونها من

---

[1] علي عبد القادر القهوجي،" شرح أصول المحاكمات الجزائية"، الكتاب الثاني، منشورات حلب الحقوقية، لبنان، 2007، ص410.

[2] انظر المادة 211 مكرر 22 من الامر 21-11 المؤرخ في 05 غشت 2021 يعدل ويتمم الامر 66-155 المتضمن قانون الإجراءات الجزائية، ج ر ج ج العدد 65.

اختصاص محكمة الجنايات الابتدائية، وتبقى الجنايات التي تم التحقيق فيها من طرف القطب المستحدث، فهي تخضع لاختصاص محكمة الجنايات لمجلس قضاء الجزائر.[1]

2- الاختصاص الإقليمي:

أعطى المشرع الجزائري القطب المستحدث اختصاص وطنيا استنادا لنص المادة 211 مكرر 23 من الأمر 21-11، ليمارس بذلك كل من وكيل الجمهورية وقاضي التحقيق ورئيس القطب اختصاصهم عبر كافة الإقليم الوطني، وذلك وفقا لنمطين:

أ-الاختصاص الحصري: بمعنى أنه اختصاص القطب المستحدث حصريا ودون سواه بمعالجة الجرائم بتكنولوجيات الإعلام والاتصال عبر كافة الإقليم الوطني ويكون ذلك في حالتين:

الحالة الأولى: بالنسبة للجرائم المحددة قانونا والجرائم المرتبطة بها: لقد حصرت المادة 211 مكرر 24 من الأمر 21-11 المتمم لقانون الإجراءات الجزائية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال التي يختص بها القطب المستحدث عبر الإقليم الوطني ودون سواه:[2]

- الجرائم التي تمس بأمن الدولة أو بالدفاع الوطني.
- جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن والسكينة العامة أو استقرار المجتمع.
- جرائم نشر وترويج أنباء مغرضة تمس بالنظام والأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية.
- جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية.
- جرائم الاتجار بالأشخاص أو الأعضاء البشرية أو تهريب المهاجرين.
- جرائم التمييز أو خطاب الكراهية.[3]

بالرجوع إلى المادة 188 من قانون الإجراءات الجزائية والتي حددت على سبيل الحصر الحالات التي يعتبر فيها إن هناك ارتباطا بين الجرائم، وعليه فإن حالات الارتباط بين الجرائم وفق المادة السالفة الذكر تنحصر فيما يلي:

---

[1] جمال الدين بوقرة، جمال الدين عنان، "القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال"، the national penal polefor combating offenses related to information and communication technologies، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 07، العدد 01، جامعة محمد بوضياف، المسيلة، جوان 2022، ص 1684،1685.

[2] جمال الدين بوقرة، جمال الدين عنان، المرجع نفسه، ص1685.

[3] المادة 211 مكرر 22 من الأمر رقم 21-11 المصدر السابق.

- "إذا ارتكب في وقت واحد من عدة أشخاص مجتمعين.
- إذا ارتكبت من أشخاص مختلفين حتى ولو في أوقات متفرقة وفي أماكن مختلفة ولكن على اثر تدبير إجرامي سابق بينهم.
- إذا كان الجناة قد ارتكبوا بعض هذه الجرائم للحصول على وسائل ارتكاب الجرائم الأخرى أو تسهيل ارتكابها أو إتمام تنفيذها أو جعلهم في مأمن من العقاب.
- أو عندما تكون الأشياء المنتزعة أو المختلفة أو المتحصلة عن جناية أو جنحة قد أخفيت كلها أو بعضها."[1]

الحالة الثانية: بالنسبة للجرائم الأكثر تعقيدا:

القطب المستحدث يختص حصريا بالنظر في الجرائم المعقدة المرتبطة بتكنولوجيا الإعلام والاتصال وكذا الجرائم المرتبطة التي تمتد عبر كامل التراب الوطني.[2]

حيث عرفت المادة 211 مكرر25 الجريمة الأكثر تعقيدا بأنها: "الجريمة التي بالنظر إلى تعدد الفاعلين أو الشركاء أو المتضررين، أو بسبب اتساع الرقعة الجغرافية لمكان ارتكاب الجريمة، أو جسامة أثارها، أو الأضرار المترتبة عليها، أو لطباعها المنظم، أو العابر للحدود الوطني، أو لمساسها بالنظام والأمن العموميين، تتطلب استعمال وسائل تحري خاصة، أو خبرة فنية متخصصة، أو اللجوء إلى تعاون قضائي دولي."[3]

نظرا لخصوصية هذه الجرائم المتطورة تجعل من أجهزة التحقيق التقليدية عاجزة عن البحث والتحري عنها وضبط الدليل والتوصل إلى مرتكبيها، لذلك أعطى المشرع الجزائري الاختصاص الحصري إلى القطب المستحدث، نظرا لما يتمتع به من آليات مستحدثة تساعده في مكافحة هذه الجرائم.[4]

ب- الاختصاص التفضيلي:

يتمتع القطب المستحدث عند معالجته للجرائم المتصلة بتكنولوجيا الإعلام والاتصال والجرائم المرتبطة بها المحددة في نصوص المواد 211 مكرر24، 211 مكرر25، باختصاص مشترك مع باقي الجهات القضائية المختصة إقليميا، مع تمتعه بأفضلية معالجتها، فيمارس وكيل الجمهورية لدى القطب المستحدث وكذا قاضي التحقيق ورئيس

---

[1] المادة 188 من الأمر 14-04، المصدر السابق.

[2] المادة 211 مكرر25 فقرة1 من الأمر 11-21، المصدر السابق.

[3] المصدر نفسه.

[4] جمال الدين بوقرة، جمال الدين عنان، مرجع سابق، ص1686.

القطب اختصاصا مشتركا مع الجهة القضائية المختصة محليا وذلك بموجب المواد 37، 40، 329 من قانون الإجراءات الجزائية، والتي تضبط معيار الاختصاص المحلي بمكان ارتكاب الجريمة أو محل إقامة أحد المتهمين، أو محل القبض على أحدهم، مع جواز تمديده لدائرة اختصاص محاكم أخرى عندما يتعلق الأمر: بجرائم المخدرات، الجريمة المنظمة عبر الحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال والإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف.[1]

ثانيا: القواعد الإجرائية الخاصة بالقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

بناءا لما ورد في 21-11 المتمم لقانون الإجراءات الجزائية سنتطرق تفصيلا لأهم القواعد الإجرائية الخاصة بالقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

1- الاختصاص الإقليمي الوطني:

يتمتع القطب الجزائي الوطني المتخصص في الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال باختصاص وطني شامل، يغطي كافة الجرائم التي تندرج ضمن اختصاصه النوعي استنادا لنص المادة 211 مكرر 23 من قانون الإجراءات الجزائية: "يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وكذا قاضي التحقيق، ورئيس ذات القطب صلاحياتهم في كامل الإقليم الوطني."[2] يستفاد من هذه المادة أن جميع قضاة هذا القطب، بمن فيهم وكيل الجمهورية، قاضي التحقيق، وقاضي الحكم الذي يشغل منصب رئيس القطب، يمارسون اختصاصا وطنيا يشمل كامل التراب الجزائري، دون أن يعد ذلك خرقا لقواعد الاختصاص، أو تجاوز له، ويعد هذا استثناءا من القواعد العامة للإجراءات الجزائية، التي تقضي بتحديد الاختصاص المحلي استنادا إلى مكان ارتكاب الجريمة، أو محل إقامة المشتبه فيهم، أو مكان توقيفهم.[3]

يجوز أن يمتد اختصاص القطب الجزائي الوطني المتخصص في مكافحة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال إلى خارج التراب الوطني، وذلك وفقا لما نصت عليه المادة 15 من القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والتي خولت المحاكم الجزائرية صلاحية تطبيق القانون

---

[1] جمال الدين بوقرة، جمال الدين عنان ، المرجع السابق ، ص1686.

[2] المادة 211 مكرر23 من الأمر 21-11، المصدر السابق.

[3] محمد هامل محمد، مباركة مباركة، ا" لقطب الجزائي الإقتصادي والمالي كآلية لمكافحة جريمة التهريب"، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد الخامس، العدد2، جامعة عمار ثليجي، الأغواط، سنة2020، ص876.

الجزائري على الجرائم المرتكبة خارج الوطن، حتى وإن كان مرتكبيها أجنبيا، طالما كانت تستهدف مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية المرتبطة به.

كما يمكن توسيع الاختصاص الإقليمي للقطب الجزائي الوطني على جرائم التمييز وخطاب الكراهية المرتكبة خارج التراب الوطني، متى كانت الضحية جزائريا، وهو ما يعد تكريسا لمبدأ الشخصية في جانبه الإيجابي، حيث يمنح المشرع للدولة الحق في بسط ولايتها القضائية على الأفعال الإجرامية المرتكبة في الخارج ضد أحد رعاياها. يشكل هذا التمديد تجسيدا لمقتضيات المادة 588 من قانون الإجراءات الجزائية، والتي تم تعديلها بموجب الأمر رقم 15-02 المؤرخ في 23 يوليو 2015، والتي تقضي بإمكانية متابعة ومحاكمة أي أجنبي وفقا لأحكام القانون الجزائري.[1]

2- قواعد اتصال القطب بملف القضية:

لم يخصص المشرع الجزائري قواعد إجرائية حصرية بالقطب وحده، وإنما جعله يتقاسم هذه القواعد مع الإجراءات المعمول بها على مستوى الجهات القضائية ذات الاختصاص الموسع، وكذلك مع تلك المطبقة بمحكمة مقر مجلس قضاء الجزائر، وبناءا على ذلك، فإن اتصال القطب بملف القضية يتم عبر نوعين من الإجراءات تبعا لطبيعة الاختصاص المنعقد يتعلق النوع الأول بالإجراءات المعتمدة عند إنعقاد الاختصاص الحصري للقطب كما هو منصوص عليه في المادتين 211 مكرر24 و 211 مكرر25 من قانون الإجراءات الجزائية، حيث أحال المشرع إلى تطبيق القواعد الإجرائية المتعلقة بالاختصاص المشترك لمحكمة مقر المجلس القضائي الواردة في المواد من 211 مكرر15 إلى 211 مكرر19 من نفس القانون.[2]

تبعا لذلك، توجه التقارير الإخبارية وإجراءات التحقيق في الجرائم المنصوص عليها في المادة 211 مكرر24، وكذا الجرائم الأكثر تعقيدا الواردة في المادة 211 مكرر25 من قانون الإجراءات الجزائية، مباشرة من قبل مصالح الضبطية القضائية إلى وكيل الجمهورية لدى القطب الجزائي المتخصص في مكافحة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال. ويتلقى ضباط الشرطة القضائية في هذه الحالة تعليماتهم مباشرة من وكيل الجمهورية، وإذا تبين لهذا الأخير أن الوقائع المبلغ عنها لا تندرج ضمن اختصاص القطب وفقا لأحكام المادتين 211 مكرر24 و211

---

[1] شريفة سوماتي، "القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال كآلية جديدة ضمن الجهاز القضائي المتخصص "

National penal pole for combating crimes related to information and communication technologies as a new machamism within the specialzed judiciary body، مجلة الدراسات القانونية (صنف ج)، المجلد 08، العدد 02، جامعة يحي فارس بالمدية، الجزائر، جوان 2022 ، ص500.

[2] شريفة سوماتي، المرجع السابق، ص501.

مكرر25 من نفس القانون فإنه يصدر مقررا بالتخلي عن الملف لصالح وكيل الجمهورية المختص إقليميا. وينطبق نفس الإجراءات على قاضي التحقيق، فإذا تبين له أن الوقائع المعروضة عليه لا تدخل ضمن اختصاصه يصدر أمرا بعدم الاختصاص تلقائيا، وذلك بعد أخد رأي وكيل الجمهورية وبناءا على إلتماسات هذا الأخير.

وفي هذه الحالة لا تعاد إجراءات المتابعة او التحقيق كما تعتبر الإجراءات الشكلية المتخدة قبل صدور أمر عدم الاختصاص صحيحة ومعتمدة قانونا.

يحال ملف الإجراءات بمبادرة من وكيل الجمهورية إلى النيابة العامة المختصة إقليميا متى أصبح أمر قاضي التحقيق بعدم الاختصاص نهائيا وتضل الأوامر الصادرة عن قاضي التحقيق سارية المفعول سواء بالقبض أو بالإيداع، أما النوع الثاني من القواعد الإجرائية فيتعلق بالإجراءات المطبقة في حال إنعقاد الاختصاص المشترك بين القطب الجزائي والجهات القضائية ذات الاختصاص الموسع، والتي أحال بشأنها المشرع إلى الأحكام الواردة في المواد من 211 مكرر 4 إلى 211 مكرر15 من قانون الإجراءات الجزائية غير أن هذه الأحكام لا تزال تفتقر إلى بعض التفصيل إذ لم توضح آلية الإشتراك بين الهيئات القضائية المعنية ولا كيفية ممارسته، بل إكتفت فقط بتحديد طرق اتصال القطب الجزائي المتخصص بملف القضية.[1]

وبناءا على ذلك يتولى وكيل الجمهورية على مستوى القطب الجزائي المتخصص في الجرائم الإلكترونية متابعة ملف القضية سواء بشكل تلقائي أو بناءا على طلب من وكلاء الجمهورية في الجهات القضائية المختصة حيث يقوم هؤلاء الوكلاء فورا وبجميع الوسائل المتاحة بإرسال نسخ من التقارير الإخبارية والإجراءات التحقيقية التي أتممتها الشرطة القضائية في إطار الجرائم المتعلقة بالمخدرات والجرائم التي تمس أنظمة المعالجة الآلية للبيانات بالإضافة إلى الجرائم المنظمة ذات الطابع الجنحي إلى وكيل الجمهورية المختص في القطب.أيضا يمكن لوكيل الجمهورية لدى القطب أن يطالب بملف الإجراءات إذا اعتبر أن الجريمة تدخل ضمن اختصاصه، ويمكن له أن يطالب بملف الإجراءات خلال التحريات الأولية أو المتابعة والتحقيق القضائي وفي هذه الحالة يصدر وكيل الجمهورية لدى الجهات القضائية ذات الاختصاص الموسع أمر بالتخلي لصالح هذا الأخير.

وفي حال فتح تحقيق قضائي تحال إلتماسات وكيل الجمهورية لدى القطب الجزائي المتخصص في الجرائم الإلكترونية المتضمنة المطالبة بملف الإجراءات من قبل وكيل الجمهورية على قاضي التحقيق المخطر بالملف، ويصدر قاضي التحقيق في هذه الحالة أمرا بالتخلي لصالح قاضي التحقيق بالقطب الجزائي.[2]

---

[1] شريفة سوماتي، المرجع السابق، ص 503-504.

[2] شريفة سوماتي، المرجع السابق، ص504.

المطلب الثاني:

الهيئات غير القضائية

في إطار الإصلاحات ذات الأبعاد القانونية والأمنية والسياسية، التي أنتهجتها الجزائر مؤخرا وسعيا لتعزيز دولة القانون والعدالة في مواجهة الجريمة الإلكترونية، وتعزيز الثقة في التعامل وكذا دعم الهيئات القضائية أصدرت الدولة عدة نصوص قانونية تهدف إلى إنشاء مصالح وهيئات تضم موارد بشرية وإمكانات مادية وتقنية، في مجالات مختلفة لكل منها مهام مختلفة الا تسعى جميعا الى تأمين البنية التحتية للفضاء السيبراني.

الفرع الأول:

الهيئات المستقلة

سنتطرق من خلال هذا الفرع الى بعض الهيئات المتخصصة والتي تتمتع بالاستقلال المالي والإداري وتتمتع بالشخصية المعنوية.

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

لقد نصت المادة 13 من القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المرتبطة بتكنولوجيا لإعلام والاتصال ومكافحتها، على استحداث هده الهيئة، محددة دورها في الوقاية والمكافحة.[1]

و قد تضمن المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015، تشكيلة الهيئة الوطنية للوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال ومكافحتها، وتنظيم مهامها وكيفيات سيرها وفقا لما نص عليه القانون.[2]

وفي سياق تطوير الإطار التنظيمي لهذه الهيئة، أصدر المشرّع الجزائري لاحقا المرسوم الرئاسي رقم 19-172 [3]الذي جاء ليعيد ضبط تشكيل الهيئة الوطنية للوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال ومكافحتها، وتنظيمها وكيفية عملها، حيث تضمن هذا المرسوم مواد تحدد أحكامها بوضوح.

---

[1] المادة 13 من القانون رقم 09-04 ، المصدر السابق.

[2] المرسوم الرئاسي رقم 15-261، المؤرخ في 24 ذي الحجة عام 1436، الموافق 8 أكتوبر 2015، الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنشور بالج.ر العدد 53 بتاريخ 08أكتوبر 2015.

[3] المرسوم الرئاسي رقم 19-172 المؤرخ في 03 شوال عام 1440 الموافق 6 يونيو سنة 2019 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، الصادر بتاريخ 9يونيو سنة 2019، ج ر ج ج العدد 37.

وفي مرحلة لاحقة، أصدر المشرّع مرسوما رئاسيا جديدا تحت رقم 20-183 [1]، هدف إلى إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها محددا تشكيلها وتنظيمها وصلاحياتها، وقد انهى العمل ببعض المواد السابقة، مع الحفاظ على مهام الهيئة ودورها في إطار مكافحة هذا النوع من الجرائم.[2]

1- تشكيلية الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:

حسب ما جاء في المادة الأولى من المرسوم 20-183 تعد الهيئة:" سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلالية المالية، توضع تحت سلطة رئيس الجمهورية""يحدد مقر الهيئة بمدينة الجزائر، ويمكن نقله إلى أي مكان آخر من التراب الوطني بموجب مرسوم رئاسي."

و حسب هذا المرسوم فان تشكيلة الهيئة تتكون من مجلس توجيه ومديرية عامة، يديرها مدير عام يتم تعينه بموجب مرسوم رئاسي، وتنتهي مهامه بحسب الأشكال نفسها[3].

تضم المديرية العامة مديرتين ومصلحتين وهما:

- مديرية للمراقبة الوقائية واليقظة الإلكترونية.
- مديرية للإدارة والوسائل.
- مصلحة للدراسات والتلخيص.
- مصلحة للتعاون واليقظة التكنولوجية[4].

كما أن مجلس التوجيه يضم مجموعة من الأعضاء، هم:

- الوزير المكلف بالعدل.
- الوزير المكلف بالداخلية.

---

[1] المرسوم الرئاسي 20-183 المؤرخ في 21 ذي القعدة عام 1441 الموافق 13 يوليو سنة 2020 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الصادر بتاريخ 18 يوليو سنة 2020، ج، ر ج ج العدد 40.

[2] سمير بارة، الدفاع الوطني والسياسات الوطنية للأمن السيبراني(CyperSecurity) في الجزائر الدور والتحديات، ورقة بحثية مقدمة في إطار أشغال الطبعة الثانية من الملتقى الدولي حول: سياسات الدفاع الوطني بين الالتزامات السيادية والتحديات الإقليمية، كلية الحقوق والعلوم السياسية ومخبر التحولات السياسية والاقتصادية والاجتماعية والقانونية في التجربة الجزائرية، جامعة قاصدي مرباح، ورقلة، يومي الإثنين وثلاثاء 30،31 جانفي 2017، ص437.

[3] المادة 09 من المرسوم الرئاسي رقم 20-183، المصدر السابق.

[4] المادة 11 من المرسوم الرئاسي رقم 20-183 المصدر السابق.

- الوزير المكلف بالمواصلات السلكية واللاسلكية.
- المدير العام للأمن الداخلي.
- قائد الدرك الوطني.
- المدير العام للأمن الوطني.
- ممثل عن رئاسة الجمهورية.
- ممثل عن وزارة الدفاع الوطني[1].

2- مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

تضمن المرسوم الرئاسي رقم 20-183 إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فقد نص المشرع الجزائري في المادة الرابعة من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تتلخص هده المهام فيما يلي:

- اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.
- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيا الإعلام، لاسيما من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية.

-ضمان المراقبة والوقاية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة.

- تجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.
- السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.
- تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا الإعلام والاتصال.
- المساهمة في تحسين المعايير القانونية في مجال اختصاصها[2]".

وأضافت المادة السابعة من المرسوم 20-183 المهام الموكلة لمجلس التوجيه وتتلخص في الآتي:

---

[1] المادة 06 من المرسوم الرئاسي رقم 20- 183، المصدر السابق.

[2] المادة 04 من المرسوم الرئاسي رقم 20- 183، المصدر نفسه.

- الإشراف والمراقبة لعمل الهيئة.
- دراسة كل المسألة تخضع لمجال اختصاص الهيئة.
- التداول حول الإستراتيجية الوطنية للوقاية من الجرائم الالكترونية ومكافحتها.
- العمل على دراسة فرص تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم الالكترونية.
- القيام بتقييم دوري لحالة التهديد التي تسببها الجرائم الالكترونية من أجل تحقيق الأهداف المنشودة من عمليات المراقبة.
- اقتراح كل من شأنه تسهيل البحث والتقييم المباشر في مجال الوقاية من الجرائم الالكترونية.
- بالإضافة إلى مهام إدارية كالموافقة على برنامج عمل الهيئة ودراسة التقرير السنوي لنشاطاتها والمصادقة عليها.
-إبداء الرأي وتقديم اقتراحات في كل ماله علاقة بمهام الهيئة.
- تولي دراسة مشروع والموافقة عليه.
- ضبط المعايير القانونية في مجال اختصاصه.

بناء على استدعاء من رئيسه فإن مجلس التوجيه يجتمع مرتين في السنة في دورة عادية، كما لديه الإمكانية في الاجتماع في دورة غير عادية بناء على استدعاء من رئيسه أو بطلب من أحد أعضائه، أو من المدير العام للهيئة.[1]

وحسب ما جاء في المادة 15 وما بعدها، فإن المديرية العامة تتولى مهام أخرى من خلال ما تضمه من مديريات ومصالح. مديرية للمراقبة واليقظة الالكترونية، مديرية للإدارة والوسائل، مصلحة للدراسات والتلخيص، مصلحة التعاون واليقظة التكنولوجيا.[2]

تكلف مديرية المراقبة الوقائية واليقظة الإلكترونية مهمة المراقبة الوقائية للاتصالات الالكترونية من أجل الوقاية من جرائم معينة مثل: الجرائم الموصوفة بالأفعال الإرهابية والتخريبية والاعتداء على أمن الدولة.

كما أسندت إليها مهام أخرى من بينها:

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في حالة ما إذا طلب منها ذلك.
- تقديم المساعدات في مجال الخبرات القضائية التي تتطلب أساليب تحر خاصة لأجل مكافحة الجرائم الإلكترونية.[3]

---

[1] المادة 08، من المرسوم الرئاسي رقم 20- 183، المصدر السابق.

[2] المادة 11، من المرسوم الرئاسي رقم 20-183، المصدر نفسه.

[3] المادة 15 من المرسوم الرئاسي رقم 20-183، المصدر النفسه.

ولذلك تضع مديرية المراقبة الوقائية واليقظة الالكترونية كل التجهيزات والوسائل والأجهزة التقنية ضرورية من أجل تنفيذ مهامها على المنشآت القاعدية للمتعاملين ومقدمي الخدمات والذين هم ملزمون بحكم القانون على تقديم المساعدات الضرورية لها للقيام بتنفيذ مهامها على أكمل وجه[1]، كما تملك الهيئة صلاحية الطلب أي وثيقة أو معلومة من أي جهاز أو مؤسسة أو مصلحة تراها ضرورية للقيام بمهامها[2].

كما تقوم كل من مديرية الإدارة والوسائل، ومصلحة الدراسات والتلخيص، ومصلحة التعاون واليقظة التكنولوجية، بأداء مجموعة من المهام نصت عليها المواد 18، 19، والمادة 20 على التوالي ومن بينها، أهم المهام الموكلة لمديرية الإدارة والوسائل:

- الاهتمام بالجانب الإداري وتقديمها للمساعدات المادية.
- التكلف بتسيير المواد البشرية والوسائل والمنشئات القاعدية، صيانتها وصياغة العتاد.
- إعداد احتياجات الهيئة حين دراستها للتقديرات الميزانية[3].

ومن بين المهام الموكلة لباقي المصالح:

- جمع ومراقبة الإجراءات المتعلقة بالطلبات القضائية، إعداد محاضر للمراقبة الوقائية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية.
- التعاون مع الشركاء لتنفيذ العمليات الوقائية من الجرائم الإلكترونية ومكافحتها.

من خلال استعراض المهام الموكلة للهيئة، يتضح الدور البارز الذي ينتظر منها القيام به في مجال الوقاية من الجرائم الالكترونية، إضافة إلى تحديد وتقييم حالة التحديد التي تطرحها هذه الجرائم بشكل دوري، فضلا عن وضع الخطط والبرامج الكفيلة بتحقيق الأهداف المرجوة.

وفي مقدمة مهامها، تضطلع الهيئة بتنشيط وتنسيق جهود الوقاية من الجرائم الإلكترونية ومكافحتها.[4]

كما تعد أداة فعالة في مراقبة الاتصالات الالكترونية بهدف الكشف عن الجرائم المرتبطة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة.

---

[1] المادة 17، من المرسوم الرئاسي رقم 20-183، المصدر السابق.

[2] المادة 21، من المرسوم الرئاسي رقم 20-183، المصدر نفسه.

[3] المادة 18، من المرسوم الرئاسي رقم 20-183، المصدر نفسه.

[4] آمال بن صويلح، ا لهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الإلكتروني بالجزائر، ورقة بحثية مقدمة في إطار الملتقى الدولي حول: الإجرام السيبراني المفاهيم والتحديات، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، يومي11-12 أفريل 2017، ص04.

وتبرز أهمية الهيئة في عمليات جمع المعلومات، وتوفيرها، وتسجيل المعطيات الرقمية وحفظها مع تحديد مصدرها ومسارها، باعتبار هذه العمليات من أبرز وسائل الوقاية من الجرائم الالكترونية ومكافحتها والقبض على مرتكبيها.

ثانيا: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

1- نشأة وتشكيلة السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:

بموجب القانون 19-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، تم استحداث سلطة وطنية لحماية هذه المعطيات، تتسم بالشخصية المعنوية والاستقلال المالي والإداري، ويقع مقرها بالجزائر العاصمة، وتخضع لوصاية رئيس الجمهورية[1].

تنص المادة 23 من القانون سالف الذكر على أن السلطة تتكون من ثلاثة أعضاء يتم تعيينهم من قبل رئيس الجمهورية، ممن تتوفر فيهم الكفاءة والخبرة في مجال حماية المعطيات الشخصية، ويشترط أن يكون أحدهم قاضيا من المحكمة العليا أو مجلس الدولة، ويقترحون من قبل المجلس الأعلى للقضاء بعد التشاور مع غرفتي البرلمان.

كما تضم السلطة أعضاء ممثلين عن عدة هيئات ومؤسسات، وهم: ممثل عن المجلس الوطني لحقوق الإنسان، ممثل عن وزارة الشؤون الخارجية، ممثل عن وزارة العدل، ممثل عن وزارة الداخلية، ممثل عن وزارة البريد والاتصالات السلكية واللاسلكية والتكنولوجيات والرقمنة، بالإضافة إلى ممثلين عن وزارة الصحة، ووزارة العمل والتشغيل والضمان الاجتماعي[2]. وتختار هذه التشكيلة بناءا على الكفاءة في الجوانب القانونية والتقنية المرتبطة بمجال حماية المعطيات، ويعين رئيس وأعضاء السلطة الوطنية من قبل رئيس الجمهورية بموجب مرسوم رئاسي، لعهدة قابلة للتجديد، كما أن المشرع لم يحدد عدد المرات التي يسمح فيها التجديد إن كانت مرة واحدة أو عدة مرات، كما أن تلك الخبرة التي يكتسبها العضو من خلال مارسته لمهامه داخل السلطة الوطنية تعد عاملا مهما في التسيير الجيد لهذه السلطة، خاصة بالنسبة للقضاة.

خاصة وأن رئيس السلطة الوطنية وأعضائها ملزمون بالحفاظ على الطابع السري للمعطيات ذات الطابع الشخصي والمعلومات التي اطلعوا عليها بهذه الصفة ولو بعد إنتهاء مهامهم[3].

2- مهام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:

اسند المشرع الجزائري للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي جملة من المهام الحيوية، التي تؤهلها للعب دور محوري في حماية هذه المعطيات ذات الطابع الشخصي، بوصفها امتدادا لجزء لا يتجزأ من الحياة

---

[1] القانون رقم 18-07، المصدر السابق.

[2] فتيحة حزام، المرجع السابق، ص293.

[3] محمد العيداني، يوسف زروق، المرجع السابق، ص123.

الخاصة للأفراد، والتي لا يجوز المساس بها أو انتهاكها. وتعد هذه السلطة، وفقا لأحكام القانون 18-07 الجهة المخولة بمراقبة مدى مطابقة معالجة المعطيات ذات الطابع الشخصي للإطار القانوني والتنظيمي، بما يضمن عدم انحراف استخدام تكنولوجيا الإعلام والاتصال، لاسيما الوسائط الرقمية، بما يشكله ذلك من تهديد محتمل لحقوق الأفراد وحرياتهم الخاصة[1].

وفي هذا السياق، تضطلع السلطة الوطنية بعدد من المهام الأساسية، نذكرها في التالي:

- تلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي طبقا للمادة 7 من القانون 18-07 ، ومنح التراخيص عند الاقتضاء طبقا للمادة 13 من نفس القانون، وإذا تبين لها أن المعالجة المعتزم القيام بها تتضمن أخطارا ظاهرة على احترام وحماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص.

- إعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم، كما تقدم الاستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي أو التي تقوم بخبرات وتجارب من طبيعتها أن تؤدي إلى مثل هذه المعالجة[2].

- تلقي الطعون والشكاوي بخصوص تنفيذ معالجة المعطيات ذات الطابع الشخصي وإعلام أصحابها بمآلها.

- التصريح بنقل المعطيات ذات الطابع الشخصي إلى الخارج وذلك وفقا للشروط المنصوص عليها في هذا القانون بما في ذلك المادتين 44 و45 منه[3].

- الأمر بإجراء التغييرات اللازمة من أجل حماية المعطيات ذات الطابع الشخصي المعالجة، والأمر بإغلاق أو إتلاف المعطيات، خاصة إذا كانت تلك المعطيات غير المطابقة لقانون 18-07[4].

- تقديم إقتراحات التي من شأنها تحسين الإطار التشريعي والتنظيمي لمعالجة المعطيات ذات الطابع الشخصي.

- إدراج التراخيص الممنوحة والآراء المقدمة في السجل الوطني المنصوص عليه في المادة الثامنة والعشرين من القانون 18-07.

- تعزيز علاقات التعاون مع السلطات الأجنبية النظيرة، مع مراعاة مبدأ المعاملة بالمثل[5].

---

[1] المادة 25 من القانون رقم 18-07، المصدر السابق.

[2] الفقرة 02 و 03 من المادة 25، من القانون 18-07، المصدر نفسه.

[3] المادة 44، من القانون 18-07، المصدر نفسه.

[4] المادة 35، من القانون 18-07، المصدر نفسه.

[5] الفقرة العاشرة من المادة 25، من القانون 18-07، المصدر نفسه.

– إصدار عقوبات إدارية وفقا للمادة 46 من القانون 18-07 والتي جاء فيها: " تتخذ السلطة الوطنية في حق المسؤول عن المعالجة في حال خرقه لأحكام هذا القانون، الإجراءات الإدارية التالية: الإنذار، الإعذار، السحب المؤقت لمدة لا تتجاوز سنة، أو السحب النهائي لوصل التصريح أو الترخيص، الغرامة. تكون قرارات السلطة الوطنية قابلة للطعن أمام مجلس الدولة وفقا للتشريع الساري المفعول."

– وضع معايير في مجال حماية المعطيات ذات الطابع الشخصي، ووضع قواعد السلوك والأخلاقيات التي تخضع لها معالجة هذه المعطيات، وتعد تقريرا سنويا حول نشاطاتها ترفعه إلى رئيس الجمهورية. كما تقوم السلطة الوطنية لحماية المعطيات ذات الشخصي بإعلام النائب العام المختص فورا، في حالة معاينة وقائع تحتمل الوصف الجزائي[1].

ولحسن سيرة السلطة الوطنية تم تزويدها بأمانة تنفيذية، يقوم بتسييرها أمين تنفيذي كما يتم مساعدته في مهامه مستخدمون، كما أنهم ملزمون بالحفاظ على سرية المعلومات التي يطلعون عليها أثناء أو ممارسة مهامهم[2].

ثالثا: وكالة أمن الأنظمة المعلوماتية:

تم استحداث وكالة امن الأنظمة المعلوماتية بموجب المادة 17 من المرسوم الرئاسي 20-05 [3] هي مؤسسة عمومية ذات طابع إداري، تتمتع بالإستقلال المالي و الشخصية المعنوية، مقرها في مدينة الجزائر.

1– تشكيل وكالة امن الأنظمة المعلوماتية

تتشكل الوكالة من مركز وطني عملياتي لأمن الأنظمة المعلوماتية ومديريات ومصالح تقنية وإدارية موضوعة تحت سلطة المدير العام الذي يسيرها، كما أنها تدير لجنة توجيه مزودة بلجنة علمية، وتتكون هذه الأخيرة من ممثلي عدة وزارات ومصالح، سلطات، هيئات، كما يمكنها الاستعانة بأي شخص أو مؤسسة من شانها أن تساعدها في أعمالها.[4]

2– مهام وكالة امن الأنظمة المعلوماتية

– تحضير عناصر الاستراتيجية الوطنية لامن الأنظمة المعلوماتية وعرضها على المجلس وتنسيق تنفيدها.

---

[1] المادة 25 من قانون 18-07، المصدر السابق.

[2] المادة 25 من قانون 18-07، المصدر نفسه.

[3] المرسوم الرئاسي 20-05 المؤرخ في 24 جمادى الأولى عام 1441 الموافق 20 جانفي سنة 2020 يتعلق بوضع منظومة وطنية لامن الأنظمة المعلوماتية الصادر بتاريخ 26 جانفي 2020، ج ر ج ج العدد 04.

[4] المادة 22 من المرسوم الرئاسي 20-05، المصدر نفسه.

– اقتراح كيفيات اعتماد مزودي خدمات التدقيق في مجال امن الأنظمة المعلوماتية ومتابعة عمليات التدقيق لامن الأنظمة المعلوماتية وضمان اليقظة التكنولوجية في هذا المجال.

– اجراء تحقيقات رقمية في حالة الهجمات او الحوادث السبيرانية التي تستهدف المؤسسات الوطنية

– اجراء المشورة والمساعدة الإدارية للمؤسسات العمومية والخاصة من اجل وضع استراتيجية امن الأنظمة المعلوماتية ومرافقة الإدارات والمؤسسات في معالجة الحوادث المتصلة بهذا المجال.

– جرد الأنظمة المعلوماتية وعرضها على المجلس للموافقة على تصنيفها، واعداد وتحيين خارطة للأنظمة المعلوماتية المصنفة.

– اقتراح مشاريع نصوص تشريعية او تنظيمية في مجال امن الأنظمة المعلوماتية وتقديم توصيات واعداد وتحديث المرجعيات والإجراءات والأدلة العلمية، واقتراح مشاريع اتفاقات دولية والاعتراف المتبادل مع الهيئات الدولية.

– اعتماد منتجات امن الأنظمة المعلوماتية والتصديق عليها واعتماد منظومات انشاء وفحص التوقيع الالكتروني.

– تحديد معايير وإجراءات منح علامة الجودة والتصديق واعتماد منتجات ومقدمي الخدمات.

– القيام بنشاطات التكوين والتوعية ذات الصلة بامن أنظمة المعلومات وتقديم توجيهات في مجال تكوين أعوان المؤسسات العمومية، واقتراح تدابير الترقية والبحث والتطوير الوطنية في المجال، وتنشيط وتوجيه أنشطة البحث والتطوير، وتعزيز ثقافة تأمين الأنظمة المعلوماتية.

– ابرام مشاريع شراكة في المجال واعداد تقارير دورية وحصيلة سنوية عن نشاطها، واعداد وتحيين خارطة حالات هشاشة الأنظمة المعلوماتية على المستوى الوطني وضمان تبادل المعلومات مع الأمانة التقنية للجنة الوطنية لتصنيف النقط الحساسة.

– تنظيم والمشاركة في الاحداث و التظاهرات العلمية والتقنية المتعلقة بامن الأنظمة المعلوماتية.[1]

يتفانى المدير العام على تنفيذ البرامج المسطرة من طرف لجنة التوجيه، كما يمكنه أيضا أن يستشير اللجنة العلمية في المسائل التي تخص أو ذات الطابع العلمي، لأن هذه الأخيرة متكونة من عشرة أعضاء وخبراء في مجال أمن الأنظمة المعلوماتية، لذلك فالاستعانة بأهل الاختصاص أمر لا بد منه وضروري لرسم إستراتيجية فعالة في وضع منظومة وطنية لحماية وأمن الأنظمة المعلوماتية[2]، كما يمكن لهذه اللجنة إبداء الرأي وتقديم الوصايا في عدة مسائل

[1] انظر المادة 18 من المرسوم الرئاسي رقم 20-05، المصدر السابق.

[2] المادة 31، من المرسوم الرئاسي رقم 20-05، المصدر نفسه.

مثل طريقة تنفيذ برامج ومشاريع البحث والتطوير، مع ضمان تجانسها مع المقترحات المقدمة من المدير العام للوكالة، كما أنها تقوم بإختيار المراجع العلمية وتنظم وتشارك في كل ما يخص أمن الأنظمة المعلوماتية وكل المسائل ذات الطابع العلمي التي يعرضها عليها المدير العام للوكالة، إعادة التأهيل وتنشيط عمليات التكوين العلمي لفائدة مستخدمي الوكالة، وأيضا مستخدمين في الإدارات والمؤسسات والهيئات العمومية المكلفة بأمن الأنظمة المعلوماتية، كما يمكنها الاستعانة بأي شخص خبير علمي أو له كفاءة في مجال أمن الأنظمة المعلوماتية.[1]

كما أن للوكالة الحق في طلب أي وثيقة أو معلومات التي تراها مفيدة للقيام بالمهام الموكلة لها بموجب هذا المرسوم، من الهيئات والمؤسسات والمتعاملين المزودين بنظام إعلام.[2]

رابعا: سلطة ضبط البريد والاتصالات الإلكترونية

في إطار تزايد التهديدات السيبرانية في هذا السياق، جاء القانون رقم 18-04 المؤرخ في 10ماي 2018 المتعلق بالقواعد العامة للبريد والاتصالات الإلكترونية ليؤسس إطارا قانونيا حديثا ينظم هذا القطاع ويمنح دورا مهما لسلطة ضبط البريد والاتصالات الإلكترونية خاصة فيما يتعلق بحماية الشبكات وتحقيق الأمن السيبراني.

1- نشأة سلطة ضبط البريد والاتصالات الإلكترونية:

تعد سلطة ضبط البريد والاتصالات الإلكترونية هيئة إدارية مستقلة، أنشئت بموجب القانون رقم 18-04 المؤرخ في 10 ماي 2018، وهي تتمتع بالشخصية المعنوية والاستقلال المالي، وتسند إليها مهمة تنظيم ومراقبة نشاطات البريد والاتصالات الإلكترونية، في إطار الأحكام التشريعية والتنظيمية السارية وتخضع هذه الهيئة للوصاية الإدارية للوزير المكلف بالبريد والاتصالات الإلكترونية، مع احتفاظها باستقلالية ممارسة مهامها.[3]

تعد سلطة ضبط البريد والاتصالات الإلكترونية هيئة تنظيمة مستقلة تتولى مهام رقابية وتنظيمية تتهدف إلى تأطير قطاع الاتصالات وضمان حسن سيره، وتكتسي هذه المهام أهمية خاصة في ظل التحديات المتزايدة المرتبطة بالأمن السيبراني، حيث تمكن الصلاحيات الممنوحة لها بموجب القانون 18-04 من التدخل لحماية الشبكات، مراقبة التجهيزات، وضمان احترام المتعاملين للمعايير الأمنية، مما يجعلها فاعلا أساسيا في تعزيز الأمن السيبراني على المستوى الوطني و قد أولى لها القانون صراحة مهمة تحقيق الامن السبيراني[4].

---

[1] المادة 32 و33، من المرسوم الرئاسي رقم 20-05، المصدر السابق.

[2] المادة 19، من المرسوم الرئاسي رقم 20-05، المصدر نفسه.

[3] المادة 12 من القانون رقم 18-04 المصدر السابق.

[4] انظر المادة 13 الفقرة 15 من القانون رقم 18-04، المصدر نفسه.

2- اختصاصات سلطة ضبط البريد والاتصالات الالكترونية

تختلف اختصاصات سلطة الضبط البريد والاتصالات الالكترونية بحسب الأدوار التي منحها لها المشرع في القانون 18-04.

أ- الاختصاص الرقابي لسلطة ضبط البريد والاتصالات الإلكترونية:

استنادا على نص المادة 15 من القانون رقم 18-04 السالف الذكر والتي تنص على أنه "يحق لسلطة الضبط أن تطلب من المتعاملين وكل شخص طبيعي أو معنوي متحصل على شهادة المطابقة في مفهوم المادة 143 من هذا القانون، تقديم كل وثيقة أو معلومة ضرورية للقيام بالمهام أوكلها إليها هذا القانون أو بمقتضاه، بدون أن يحتج في مقابلها بإنشاء السر المهني أو سرية الوثائق أو المعلومات المطلوبة.[1]

نصت المادة 15 من القانون 18-04 على تمكين سلطة ضبط البريد والاتصالات الإلكترونية من الولوج إلى المعلومات والوثائق بما فيها السرية، دون إمكانية الاحتجاج بالسر المهني وتعد هذه الصلاحيات ذات أهمية بالغة في مجال الأمن السيبراني، إذا تخول للسلطة جمع البيانات التقنية.

ب- الاختصاص العقابي لسلطة ضبط البريد والاتصالات الالكترونية:

بالرجوع إلى أحكام المواد من القانون رقم 18-04 المتعلق بالبريد والاتصالات الإلكترونية نجد أن سلطة ضبط البريد والاتصالات الإلكترونية تعمل على تنظيم ومراقبة قطاع الاتصالات والبريد في البلاد، حيث تتمتع هذه السلطة بعدة اختصاصات عقابية تهدف إلى تطبيق القوانين وضمان وسلامة البيانات والاتصالات، حيث تتمثل مهمة سلطة ضبط البريد والاتصالات الإلكترونية في تطبيق القوانين واللوائح وفرض العقوبات عند الضرورة بهدف تحقيق الأمن السيبراني.[2]

ج- الاختصاص التحكيمي لسلطة ضبط البريد والاتصالات الإلكترونية:

يعرف التحكيم بأنه تولية وتقليد وتفويض من طرفي الخصومة لطرف ثالث ليفصل في النزاع، بمعنى أن طرفي النزاع يتفقان على تعيين شخص محايد ومختص يسمى المحكم لتولي مهمة حل النزاع بشكل نهائي وملزم، ويعتبر التحكيم آلية بديلة لتسوية النزاعات حيث يتيح للأطراف تجنب اللجوء إلى القضاء لحل نزاعاتهم. لم يتم تعميم وظيفة التحكيم على جميع الهيئات الإدارية المستقلة بل اقتصرت على بعضها فقط ومن بينها سلطة ضبط البريد والاتصالات

[1] المادة 15 من القانون 18-04، المصدر السابق.

[2] محمد الأمين رحالي، عبد الحكيم روبة، "النظام القانوني لسلطة ضبط البريد والاتصالات الإلكترونية"، مذكرة مكملة لنيل شهادة الماستر في الحقوق، تخصص قانون عام، كلية الحقوق، جامعة عين تيموشنت، -بلجاج بوشعيب-، الجزائر، 2024، ص ص48، 49.

الإلكترونية، حيث تتميز وظيفة التحكيم المخولة لسلطة ضبط البريد والاتصالات الإلكترونية ببعض الخصوصيات مما يميزها عن وظائف التحكيم الأخرى.[1] ولآلية التحكيم التي تمارسها سلطة ضبط البريد والاتصالات الالكترونية دور مهم وفعال في تحقيق الأمن السيبراني وذلك من خلال تسوية النزاعات الفنية المتعلقة بأمن الشبكات فعند لجوء المتعاملين إلى سلطة الضبط لحل مثل هذه النزاعات فإن قرارات التحكيم التي تصدرها تضمن الحفاظ على استقرار وأمن البنى التحتية الرقمية، وكذلك التسريع في حل النزاعات، فالتحكيم كآلية بديلة وسريعة لتسوية النزاعات يسمح بتفادي الإنقطاعات والخلافات المطولة التي تضعف الأمن المعلوماتي أو تستغل في هجمات سيبرانية.

خامسا: السلطة الوطنية للتصديق الإلكتروني:

تم استحداث هذه الهيئة بموجب المادة 16 من القانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الالكترونيين والتي نصت على ان تؤسس لدى الوزير الأول هيئة إدارية مستقلة ذات شخصية معنوية وإستقلال مالي تسعى السلطة الوطنية للتصديق الإلكتروني تسجل الإعتمادات المالية للازمة لسير هذه السلطة ضمن ميزانية الدولة[2].

كما تم انشاء بموجب هذا القانون السلطة الحكومية للتصديق الالكتروني لدى الوزير الكلف بالبريد وتكنولوجيات الاعلام والاتصال تتمتع بالاستعلال المالي والشخصية المعنوية[3]، بالإضافة الى تعيين السلطة المكلفة بضبط البريد والمواصلات السلكية واللاسلكية سلطة اقتصادية للتصديق[4].

1- تشكيل السلطة الوطنية للتصديق الالكتروني:

تتشكل السلطة من مجلس يتشكل بدوره من خمسة أعضاء من بينهم الرئيس يعينهم رئيس الجمهورية على أساس الكفاءة لاسيما في مجال العلوم التقنية المتعلقة بتكنولوجيات الاعلام والاتصال وفي مجال قانون تكنولوجيات الاعلام والاتصال وفي اقتصاد تكنولوجيات الاعلام والاتصال تحدد عهدة الأعضاء بأربع سنوات قابلة للتجديد مرة واحدة [5]، كما تشكل من مصالح تقنية وإدارية يسيرها مدير عام يعينه رئيس الجمهورية بناء على اقتراح من الوزير

[1] محمد الأمين رحالي، عبد الحكيم روبة، المرجع السابق، ص 56.
[2] المادة 16 من القانون 15-04، المصدر السابق.
[3] المادة 26 من القانون 15-04، المصدر نفسه.
[4] المادة 29 من القانون 15-04، المصدر نفسه.
[5] المادة 19 من القانون 15-04، المصدر نفسه.

الأول.[1] وتكلف السلطة الوطنية للتصديق الإلكتروني بتحديد السياسة الوطنية للتصديق والتوقيع الإلكترونيين، كما تضطلع بمهمة ترقية استعمالها وتطوير آلياتها وضمان دقة وموثوقية استخدامه[2].

2- اختصاصات السلطة الوطنية للتصديق الإلكتروني:

تمارس السلطة الوطنية للتصديق الإلكتروني جملة من الصلاحيات والاختصاصات ذات الطابع الرقابي وقائية قمعية.

أ- اختصاص تنظيمي:

تعد السلطة الوطنية للتصديق الإلكتروني هيئة ضبط عليا غير أنها لا تتمتع باختصاص إصدار النصوص التنظيمية في مجال التوقيع والتصديق الإلكترونيين إذ يعود هذا الإختصاص إلى الوزير الأول[3]. غير أنها تتمتع بسلطة إصدار قرارات نافذة، تتعلق بمنح الرخص والإعتمادات والتأهيلات التي تمكن المتعاملين من الولوج إلى مجالي التجارة الإلكترونية حيث تنص المادة 30-02 من القانون رقم 04/15 في تحديدها للمهام الموكلة للسلطة الإقتصادية للتصديق الإلكتروني على أنها تختص بمنح التراخيص لمؤدي خدمات التصديق الإلكتروني بعد موافقة السلطة، كما تختص السلطة بإبرام إتفاقيات الإعتراف المتبادل مع الدول الأجنبية في مجال التصديق الإلكتروني[4].

ب- اختصاص إستشاري:

تعتبر السلطة الوطنية للتصديق الإلكتروني الهيئة الخبيرة المختصة في مجال التوقيع والتصديق الإلكترونيين، إذ تضطلع بإتخاذ عدة تدابير ذات طابع إستشاري في هذا المجال.

- تقوم السلطة الوطنية للتصديق الإلكتروني بإقتراح مشاريع تمهيدية لنصوص تشريعية متعلقة بالتوقيع والتصديق الإلكترونيين تعرض على الوزير الأول للنظر فيها.

- إقتراح سياسة شاملة تتمثل في مجموعة قواعد وإجراءات تنظيمية وتقنية تتعلق بالتصديق الإلكتروني.

---

[1] المادة 20 من القانون 15-04، المصدر نفسه.

[2] صبرينة جبايلي، "النظام القانوني للسلطة الوطنية للتصديق الإلكتروني"، مجلة العلوم الإنسانية، جامعة عباس لغرور خنشلة، عدد48، المجلد أ، ديسمبر 2017، ص422.

[3] أمينة قهواجي، ليلى مطالي، "الإطار المفاهيمي والقانوني للتوقيع والتصديق الإلكترونيين في الجزائر"، مجلة المشكلة في الإقتصاد التنمية والقانون، العدد 08، المجلد 04، كلية العلوم الإقتصادية التجارية وعلوم التسيير، جامعة بومرداس، الجزائر، 23-05-2019، ص ص30،29.

[4] المرجع نفسه، ص30.

– تتولى السلطة الوطنية للتصديق الإلكتروني مهمة تعزيز التنسيق بين السلطتين الحكومية والإقتصادية للتصديق الإلكتروني وذلك من خلال القيام بعمليات التدقيق على مستوى كل من هاتين السلطتين[1].

ج– اختصاص قمعي:

بإعتبار السلطة الوطنية للتصديق الإلكتروني هيئة تنسيقية بين السلطتين الحكومية والإقتصادية للتصديق الإلكتروني فإن جميع الاختصاصات التنظيمية والقمعية لاسيما مايتعلق بفرض العقوبات المالية والإدارية من قبل السلطة الإقتصادية تضل خاضعة لموافقة مسبقة من السلطة الوطنية للتصديق الإلكتروني.

فهي بذلك كغيرها من السلطات الإدارية المستقلة تملك سلطة توقيع العقوبات بصورة غير مباشرة وذلك في حالة عدم إحترام مؤدي خدمات التصديق الإلكتروني لأحكام دفتر الأعباء أو سياسة الإقتصادية، أو في حالة إنتهاكه للمقتضيات التي يتطلبها الدفاع الوطني والأمن العمومي[2].

الفرع الثاني:

الهيئات التابعة لأجهزة أخرى

سعيا من المشرع على تدعيم البنية للفضاء السيبراني وبناء منظومة معلوماتية آمنة ومتكاملة وضمان النجاعة اللازمة في الكشف عن الجريمة في هذا المجال والتحري عنها دعم الجهات الفاعلة في هذا المجال بهيئات تابعة لها متخصصة وأوكل لها بعض المهام بغرض مساعدة هذه الجهات في أداء عملها.

اولا: المجلس الوطني لأمن الأنظمة المعلوماتية

يعد المجلس الوطني لأمن الأنظمة المعلوماتية من بين العناصر المكونة للمنظومة الوطنية لأمن الأنظمة المعلوماتية وقد تم انشائه بموجب المادة 04 من المرسوم الرئاسي 20–05 المتعلق بوضع منظومة وطنية لامن الأنظمة المعلوماتية.

1– تشكيلة المجلس الوطني لامن الأنظمة المعلوماتية

يتراسه وزير الدفاع الوطني او ممثله، ويتكون المجلس من: ممثل عن رئاسة الجمهورية، ممثل عن الوزير الأول، الوزير المكلف بالشؤون الخارجية، الوزير المكلف بالداخلية، الوزير المكلف بالعدل، الوزير المكلف بالمالية، الوزير المكلف بالطاقة، الوزير المكلف بالاتصالات، الوزير المكلف بالتعليم العالي. يمكن أن يستعين المجلس بأي شخص أو مؤسسة من شأنه تنويره في أعماله.[3]

---

[1] صبرينة جبايلي، المرجع السابق، ص493.

[2] أمينة قهواجي، ليلى مطالي، المرجع السابق، ص30.

[3] المادة 05 من المرسوم الرئاسي رقم 20–05، المصدر السابق.

يتوفر على أمانة تقنية يسيرها أمين عام توضع تحت سلطة رئيس المجلس، وذلك لضمان قيام المجلس بأداء مهامه على أكمل وجه.

تقوم الأمانة التقنية بعدة مهام منها: إعداد مشروع القواعد الداخلية المنظمة للمجلس، جمع الوثائق والمعلومات اللازمة لتحضير أعماله من أي إدارة أو مؤسسة أو هيئة، وهي خاصية خطيرة ومهمة في الوقت نفسه، لأنها بإمكانها الإطلاع على معلومات قد تمس خصوصية الحياة الخاصة، لذلك تكون هناك آليات مرفقة مع هذه المهام تضمن حماية تلك الخصوصية، كما تتولى تسيير الموارد البشرية والمادية وحفظ الوثائق والأرشيف، والعمل كمنسق بين المجلس والوكالة.[1]

2- مهام المجلس الوطني لأمن الأنظمة المعلوماتية

وضحت المادة الرابعة من المرسوم الرئاسي رقم 20-05 والمتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية مهام المجلس الوطني لأمن الأنظمة المعلوماتية، ونذكر منها:

- القيام بتحديد عناصر الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من قبل الوكالة وتحديدها.

-دراسة التقارير المتعلقة بتنفيذ تلك الإستراتيجية والموافقة عليها ودراسة تقرير نشاط الوكالة ومخطط عملها والموافقة عليه.

-كما أن للمجلس الوطني لأمن الأنظمة المعلوماتية دور مهم في الموافقة على اتفاقيات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في مجال أمن الأنظمة المعلوماتية، صلاحية الموافقة على سياسة التصديق الإلكتروني التي تنجزها السلطة الوطنية للتصديق الإلكتروني.[2] تصنيف الأنظمة المعلوماتية والموافقة عليها و التي يوجد منها أنواع كثيرة، نخص بالذكر:

- نظم المعلومات الإدارية (الأنظمة المسؤولة عن تقديم المعلومات الضرورية للإدارة).
- أنظمة دعم القرار(اتخاذ القرار المناسب لحل المشكل، خلق فرص للإبتكار والتطوير).[3]

---

[1] المواد 7، 8 و9 من قانون 18-07، المصدر السابق.

[2] المادة الرابعة من المرسوم الرئاسي رقم 20-05، المصدر السابق.

[3] عومار بوطبيبة، دراسة واقع نظم المعلومات بمديرية الشباب والرياضة لولاية قسنطينة، مذكرة مقدمة لنيل شهادة الماجستير في الإدارة والتسيير الرياضي، المركز الجامعي محمد الشريف مساعدية سوق أهراس، الجزائر، 2012/2011، ص63.

ثانيا: الهياكل التابعة للامن الوطني:

لطالما لعبت الشرطة الجزائرية دورا كبيرا في مكافحة الجريمة، ومع تطور التقنيات الحديثة واكبت هذه التطورات وساهمت في تحقيق الأمن السيبيراني، اذ تهدف استراتيجيتها إلى كشف الجريمة والقبض على مفتعلها، كما تهدف أيضا للحد منها وحماية الحريات والحفاظ على الحقوق، كما أنها تكون على استعداد لمواجهة الكوارث والأزمات بفاعلية من أجل الضبط الجيد للأمن والحفاظ على النظام العام[1]، والقيام بجميع المهام المسندة للأمن الوطني كما حددها التشريع المعمول به، وقد خصص الأمن الوطني لضمان المكافحة الفعالة للجريمة الإلكترونية موارد بشرية متخصصة[2]، وذلك من خلال تعزيز صفوفه بضباط ذوي خلفيات جامعية ذات مستوى عالي خاصة في ميادين العلوم الإنسانية والعلوم الاجتماعية، وضمان الاستفادة من التدريبات عالية المستوى في العلاقات العامة وإدارة عمل الفرق الشرطية والتعامل مع الحالات الخاصة في صفوف المنحرفين والمجرمين[3]، كما خصص الأمن الوطني موارد هيكلية وتنظيمية لمحاربة الجريمة الإلكترونية كمديرية الشرطة القضائية والمصلحة المركزية لمكافحة الجريمة السيبيرانية. ولأن الجريمة الإلكترونية في توسع وتطور مستمر تم إتخاذ خطوة أخرى، حيث تم توسيع التشكيل الأمني وذلك عن طريق تكوين فصائل على مستوى جميع الولايات تابعة للمصالح الولائية للشرطة القضائية بأمن الولايات.[4]

ومن أجل مواكبة التطور التكنولوجي وكذا الرفع من المستوى المعرفي والمهاري والأدائي للمحققين، تم ادراج صنفين من التكوين المتخصص، الصنف الأول: محقق في الجريمة المعلوماتية"ICC"، خص بإطارات ومفتشي المصالح المحققة في مجال الجريمة المعلوماتية.

الصنف الثاني: متدخل أول في الجريمة المعلوماتية"PICC"، خاص بأعوان الشرطة العاملين في مجال مكافحة الجريمة المعلوماتية.[5]

---

[1] نعيمة براري، الاتصال بين الشرطة والمواطن ودوره في مكافحة الجريمة في الجزائر دراسة تحليلية استطلاعية بالجزائر العاصمة، رسالة نيل شهادة الدكتوراه في علوم الإعلام والاتصال، كلية العلوم السياسية والإعلام، جامعة الجزائر 3، 2013/2012، ص117.

[2] المادة 109 من المرسوم التنفيذي رقم 10-322، المتضمن القانون الأساسي الخاص بالموظفين المنتمين للأسلاك الخاصة بالأمن الوطني، ج ر ج ج العدد 78، الصادرة بتاريخ 26 ديسمبر 2010.

[3] عبد العزيز ديلمي، دور الشرطة المجتكعية في الوقاية من الجريمة والانحراف دراسة نظرية لبناء نموذج للشرطة الجوارية في الجزائر، أطروحة مقدمة لنيل شهادة الدكتوراه في علوم اجتماع الجريمة والانحراف، قسم علم الاجتماع، كلية العلاوم الإنسانية والاجتماعية، جامعة الجزائر 2، 2013/2012، ص ص562،563.

[4] تقرير المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والنشر والإشهار وحدة الطبع رويبة، الجزائر، العدد 144، سبتمبر2019، ص69.

[5] تقرير المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، المرجع نفسه، ص70.

ولأن التدريب والتعليم أساس العملية التطورية، عمل جهاز الأمن الوطني على تطوير قدرات ومهارات واستثمار طاقة العاملين في التعليم العالي، وذلك من أجل مواكبة وإعطاء أنسب الحلول وأفضلها والحصول على قوة بشرية متخصصة، ومن أجل هذا تم إنشاء عدة مرافق خصصت لهذا الغرض ونذكر منها المعهد الوطني للبحث في علم التحقيق الجنائي،[1] والذي يضم خمسة مخابر جهوية، موجودة في: وهران، قسنطينة، ورقلة، بشار و تمنراست، وتعتبر بمثابة امتداد لنشاطات المعهد في مجال الخبرة والتكوين والبحث العلمي، فهي تقوم بإجراء التحاليل والخبرة العلمية اللازمة لسير التحقيقات القضائية المقدمة لها من قبل المحققين والقضاة والسلطات المؤهلة، كما توفر أيضا الدعم التقني الضروري المجهز بكل الوسائل الملائمة لتسيير مواقع حدوث الجريمة، كما تساهم في أشغال المجلس العلمي للمعهد.[2]ولأجل المواجهة الفعالة للجريمة السبيرانية، فإن الشرطة تقوم بوضع قائمة اسمية لضباط مختصين يمكن الاستعانة بهم في مجال البحث والتحري في قضايا الجرائم الإلكترونية.

ثالثا: الهياكل التابعة للدرك الوطني:

لمصالح الدرك الوطني دور فعال في مكافحة الجريمة بصفة عامة والجريمة السيبيرانية في الآونة الأخيرة بصفة خاصة، يعد الدرك الوطني من بين قوات الأمن الفعالة في مكافحة الإجرام عموما والجريمة الإلكترونية خصوصا، ويعود ذلك للإمكانيات البشرية والمادية التي يمتلكها والمخصصة لهذا الغرض، فأصبحت مكافحة الجريمة والحفاظ على الأمن العمومي في الفضاء السيبراني الوطني من أولويات الدولة الجزائرية.

ولأن عملية مواكبة التطورات التي تحدث في مجال التكنولوجيات الحديثة، أمر لابد من تحقيقه وذلك للوصول إلى تحقيق الخدمات الأمنية لحماية المواطنين، يعمل جهاز الدرك الوطني على تكوين الإطارات وأعوان الدرك الوطني بشكل مستمر، من خلال إنشاء مدارس ومعاهد تدعم هذا الغرض، كمدرسة الشرطة القضائية التابعة للدرك الوطني[3]، والمعهد الوطني للشرطة القضائية، الذي يقوم بتكوين متخصصين في الشرطة القضائية، وإجراء بحوث متعلقة بالظواهر الاجتماعية ذات صلة بالجريمة[4].

---

[1] المادة 03 من المرسوم رئاسي رقم 04-432، المؤرخ في 17 ذي القعدة عام 1425 الموافق ل29 ديسمبر2004، المتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي، ج ر ج ج العدد 84، الصادرة بتاريخ29 ديسمبر2004.

[2] المادة 09 من القرار الوزاري المشترك، المؤرخ في 26 ربيع الأول 1428 الموافق 14 أبريل سنة2007، المتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، ج ر ج ج العدد 36 بتاريخ 03 يونيو 2007.

[3] المادة الرابعة من المرسوم الرئاسي رقم 08-151، المؤرخ في 20 جمادى الأولى 1429 الموافق 226 مايو 2008، المتضمن إحداث مدرسة للشرطة القضائية تابعة للدرك الوطني، ج ر ج ج العدد 27، الصادرة بتاريخ 28 مايو 2008.

[4] عبد العزيز ديلمي، المرجع السابق، ص479.

يضم الدرك الوطني هياكل المعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي لضمان التحكم الجيد في الجرائم التي تحدث، ويعد المعهد مؤسسة فاعلة في تحديد السياسة الجنائية المثلى لمكافحة الإجرام بشتى أنواعه، ثبتت فعاليتها في ميادين علمي الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي من خلال البحوث المتعلقة بالجرائم والعمل على ترقية البحث التطبيقي وأساليب التحريات، تستعان فيها بالتكنولوجيات الدقيقة، والاستفادة من النتائج المتوصل إليها في كل الملتقيات والمحاضرات أو الندوات التي يشارك فيها على الصعيدين الوطني والدولي، وتهدف من خلالها إلى تطوير مستويات الذين يخضعون لدورات تحسين المستوى والتكوين ما بعد التدرج في تخصصات العلوم الجنائية التي تنظم من طرف المعهد، بالإظافة إلى مهام أخرى قد يظطلع بها[1]. و يضم المعهد الوطني للادلة الجنائية العديد من الأقسام و المصالح المختصة و التي من بينها مصلحة الاعلام الالي و التي يتم على مستواها رصد و مراقبة و تتبع عمليات الاختراق و القرصنة المعلوماتية و كذا اكتشاف المعلومات المسروقة و تفكيك البرامج المعلوماتية.

و بالإضافة الى المعهد الوطني للأدلة الجنائية وعلم الإجرام الذي يعد من بين المؤسسات التي لها دور في مكافحة الجريمة الإلكترونية والذي يسعى جاهدا لتطوير الهياكل المتخصصة في مكافحة الجريمة الإلكترونية والتصدي للجرائم السبيرانية نذكر كذلك من بين الأجهزة العملياتية التابعة لقيادة الدفاع الوطني مركز الوقاية من جرائم الاعلام الالي و الجرائم المعلوماتية التي تم إنشاؤه سنة 2008 و الذي يعمل على تامين منظومة المعلومات لخدمة الامن العمومي و اعتبر بمثابة مركز توثيق و يعكف هذا المركز على تحليل المعطيات و بيانات الجرائم المعلوماتية المرتكبة و تحديد هوية مرتكبيها.[2]

[1] المادة الرابعة من المرسوم الرئاسي رقم 04-183، المصدر السابق.

[2] سمير بارة، الامن السبيراني في الجزائر: السياسات و المؤسسات، المجلة الجزائرية للامن الإنساني، العدد الرابع، جويلية 2017، ص ص 270-272.

خلاصة الفصل

ان تبني منظومة قانونية إجرائية و مؤسسات مختصة في مجال الأنظمة المعلوماتية و تكنولوجيات الاعلام و الاتصال يلعب دورا مهم في الحفاظ على الامن السبيراني، وهو ما سعى اليه المشرع الجزائري من خلال تحيين قانون الإجراءات الجزائية باستحداث إجراءات جديدة و هي الإجراءات المتعلقة باساليب التحري الخاصة و التي تعد من بين الإجراءات التي تتعارض مع الحقوق و الحريات الأساسية المحمية قانونيا الا ان المشرع لجأ اليها في بعض الجرائم الخطيرة و التي تعد الجريمة المعلوماتية احداها، و قد احاطتها بجملة من الشروط حتى يحافظ على ما جاءت به النصوص القانونية لحماية الافراد و حياتهم الخاصة و يوازن بين المصالحة العامة و المصلحة الفردية، كما تم استحداث أجهزة قضائية متخصصة في هذا النوع من القضايا و ذلك باستحداث الأقطاب الجزائية المتخصصة بالإضافة الى قطب جزائي وطني لمكافحة الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال، ساعيا الى تحقيق النجاعة والفعالية على مستوى التحقيق والمحاكمة، بالإضافة الى تبني اجراءات خاصة في مجال الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال، كما تم استحداث جهات أخرى غير قضائية تتكامل فيما بينها لحماية مصالح الدولة و الافراد في هذا المجال، و هو ما يظهر المكانة المهمة التي اصبح يحضى بها موضوع الامن السبيراني و الذي اصبح هاجسا على المستوى الوطني و الدولي لا سيما ان التهديدات المتعلقة به تستهدف البنى التحتية الحيوية وا لمؤسسات الحكومية، والأنظمة المصرفية، وحتى الأفراد، دون أي اعتبارات جغرافية او الشخصية.

خـــاتـمة

لقد أضحى الأمن السيبراني في العصر الراهن أحد أبرز التحديات التي تواجه الدول والمجتمعات، نتيجة التطور الهائل في تكنولوجيا المعلومات والاتصال، وما صاحبه من توسع في استخدام الفضاء السيبراني في مختلف مناحي الحياة، سواء المستوى الفردي أو المؤسساتي أو حتى السيادي، فقد بات الفضاء الرقمي مجالا حيويا لممارسة الأنشطة الإقتصادية، والإدارية والخدماتية، والتعليمية وحتى الأمنية، وهو ما جعل منه مجالا مفتوحا للفرص، لكنه أيضا ساحة خصبة لمخاطر متعددة أبرزها الهجمات السيبرانية والجرائم المعلوماتية والتعدي على الخصوصية والمعطيات الشخصية.

وفي هذا السياق جاءت هذه المذكرة لتسليط الضوء على الجهود التي بدلها المشرع الجزائري من أجل مواجهة هذه التحديات، وتأطير الفضاء السيبراني بقواعد قانونية تكفل تحقيق التوازن بين الحرية الرقمية ومتطلبات الأمن العام. وقد ظهر لنا أن المشرع الجزائري كان واعيا بحجم الرهانات التي يفرضها التحول الرقمي، مما دفعه إلى إدراج منظومة تشريعية تتناول الأمن السيبراني من زوايا متعددة سواء عبر النصوص العامة أو القوانين الخاصة.

وقد بدأ الاهتمام الرسمي بالأمن السيبراني في الجزائر بشكل تدريجي، حيث كانت البداية من خلال التصدي لظاهرة الجرائم الإلكترونية بموجب أحكام قانون العقوبات المعدل، ثم جاء قانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. ومع تطور الظواهر المرتبطة بالفضاء السيبراني، اعتمدت الجزائر قانون 18-07 المتعلق بحماية الأشخاص الطبيعية في مجال المعطيات ذات الطابع الشخصي، يشكل محطة مهمة في تكريس حق الأفراد في الخصوصية الرقمية.

إضافةً الآليات المؤسساتية القضائية التي تسهم في تحقيق الأمن السيبراني والتي تتجلى في استحداث هيئات مؤسساتية وقضائية متخصصة لمكافحة الجريمة السيبرانية، ولأن التهديدات السيبرانية ذات طابع عابر للحدود لم تكن الأبيات المخصصة لها على المستوى الداخلي لوحدها قادرة على مجابهتها بل استلزم الأمر لإيجاد آليات مكافحة بتنسيق وتعاون إقليمي ودولي تتكاثف فيه كل الجهود وتتوحد من أجله كل القوى لإيجاد آليات فعالة لتحقيق الأمن السيبراني.

وعليه يمكن القول أن المشرع الجزائري قد أبان عن إرادة حقيقية في بناء إطار قانوني يواكب متطلبات الأمن السيبراني، إلا أن النصوص القانونية على أهميتها لا تكفي وحدها لضمان أمن شامل في القضاء الرقمي، بل لابد من تبني مقاربة شاملة ومتكاملة قوامها التكوين والتوعية والتعاون الوطني والدولي، والإستثمار في التكنولوجيا وتعزيز البحث العلمي في هذا المجال، وذلك من أجل بناء بيئة رقمية آمنة تضمن حماية الأفراد والمؤسسات والدولة على حد سواء.

فالأمن السيبراني لم يعد شأنا تقنيا أو قانونيا محضاً، بل أضحى أحد مقومات السيادة الوطنية، وجزء لا يتجزأ من الأمن القومي، مما يستدعي إرادة سياسية قوية، وتخطيا إستراتيجيا طريلا، لضمان أن تكون الجزائر في مصاف الدول القادرة على حماية فضائها الرقمي بكل فعالية وإقتدار.

لقد توصلت الدراسة إلى عدة نتائج نوردها كالأتي:

– الأمن السيبراني أصبح ضرورة قانونية و سيادية فقد تبين لنا انه لم يعد شأنا تقنيا فحسب، بل أصبح يشكل أحد أعمدة السيادة الوطنية، وركيزة أساسية من ركائز الأمن القومي في ظل التهديدات المتزايدة المرتبطة بالفضاء الرقمي.

– على الرغم من وقوع التهديدات السبيرانية في فضاء افتراضي واستهدافها للأنظمة المعلوماتية والمعلومات الالكترونية في بيئة رقمية على هيئة إشارات ونبضات غير مرئية تتم على مستوى شبكة الاتصالات الالكترونية الا ان انعكاساتها تعد أشد وطأة من الجريمة التقليدية وعواقبها وخيمة سواء على المستوى العسكري أو الاقتصادي او الاجتماعي.

– وجود تطور ملحوظ في الإطار التشريعي الجزائري، فقد أظهر البحث أن المشرع الجزائري قد خطى خطوات هامة في تنظيم الأمن السيبراني من خلال تعديل القوانين الموضوعية والإجرائية وسن قواعد تتماشى مع الجريمة السيبرانية إضافة الى إصدار قوانين متخصصة مما يعكس وعيا تشريعيا متزايدا بخطورة التهديدات السبيرانية الا و بالرغم من ذلك الا ان القانون الجزائري مزال يشهد ثغرات قانونية كبيرة في هذا المجال، مما ينتج عنه افلات الفاعلين كانعكاس عن مبدأ الشرعية فان كان القانون شمل جانبا من هذه الأفعال غير المشروعة الا انه لم يشمل جانبا كبيرا منها مثل السرقة الو التزوير المعلوماتيين و الذي تعرضت له أولى الخطوات التشريعية الدولية في مكافحة الجريمة السبيراني بالإضافة الى بعض انواع النصب الجديدة التي باتت تعرف انتشارا واسعا في هذا الفضاء.

– الإعتماد على مقاربة قانونية ومؤسساتية متكاملة حيث بينت الدراسة أن المشرع الجزائري لم يقتصر على إصدار النصوص القانونية بل دعمها بإنشاء مؤسسات وهيئات مختصة، منها القضائية كالقطب الجزائي المتخصص في الجرائم المتصلة بتكنولوجيات الاعلام والإتصال وأخرى غير قضائية كالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والإتصال وسلطة الضبط التي اوكل لها مهمة تحقيق الامن السبيراني والوكالة الخاصة بامن الأنظمة المعلوماتية.

– الدور الكبير الذي يلعبه ضباط الشرطة الضبطية القضائية في تحقيق الامن السبيراني وأهمية تكوين المختصين في هذا المجال لاسيما وان هذا النوع من الجرائم يغلب عليه الطابع التقني والعلمي وتعدي اختصاصاتهم من أجهزة

تكافح الجرائم الى جهاز وقائي طبقا للصلاحيات المخولة لهم بموجب القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.

– الأهمية الكبيرة للتعاون الدولي في تحقيق الامن السيبراني، نظرا للطبيعة العابرة للحدود لهذا النوع من الجرائم، اذ اتضح من خلال الدراسة وجود اليات قانونية لتنفيذ هذا النوع من التبادل الا انه عمليا تعترضها العديد من العقبات لا سيما بطء الإجراءات والذي يتعارض مع طبيعة الجريمة السبيرانية التي تتميز بالسرعة في التنفيذ والسرعة في التخلص من الأدلة، وعدم وجود أدوات قانونية تضمن تنفيذه.

– أظهرت الدراسة انه من الصعوبات التي تواجه التعاون الدولي في التصدي للجرائم السبيرانية هو عدم تماثل المنظومات التشريعية بين الدول سواء من الناحية الموضوعية او من الناحية الإجرائية مما يحول دون تحقيق الهدف المنشود لاسيما في مجال تسليم المجرمين.

– خلصنا من خلال هده الدراسة الى التشتت الكبير في القوانين المتعلقة بالامن السبيراني بوجود القوانين كثيرة مما يتحقق معه صعوبة الالمام والإحاطة بهذه القواعد القانونية وظهور فرضية تعارض احكام القوانين فيما بينها.

– ضعف الثقافة المجتمعية في مجال الأمن السيبراني حيث أظهر البحث وجود ضعف واضح في وعي الأفراد والمؤسسات الصغيرة بمخاطر الفضاء السيبراني وطرق الوقاية منها، وهو ما يشكل ثغرة يمكن استغلالها في تنفيذ هجمات إلكترونية وإختراقات.

ومما سبق يمكن أن نخرج بمجموعة من التوصيات ندكرها فيما يلي:

– وجوب تدعيم البنية التحتية لحماية الفضاء السبيراني واتخاذ جميع الاحترازات التقنية لحماية الأنظمة المعلوماتية وشبكة الاتصالات التكنولوجية من جميع التهديدات المحتملة.

– وجوب إعداد استراتيجية وطنية شاملة للأمن السيبراني، يوصى بوضع إستراتيجية وطنية واضحة ومحدّدة الأهداف، تُشرك فيها مختلف الفاعلين، وتُبنى على مبادئ الوقاية، الاستجابة، والتعافي، مع تحديد مؤشرات الأداء وسبل التقييم الدوري.

– وجوب مراجعة وتحيين الإطار القانوني بصفة دورية، اذ ينبغي على المشرع الجزائري تحديث النصوص القانونية المتعلقة بالأمن السيبراني بشكل مستمر، لمواكبة التطورات التكنولوجية والتهديدات المستجدة في الفضاء الرقمي، مع سد الثغرات القانونية التي قد يستغلها مرتكبوا الجرائم السيبرانية.

– تفعيل التنسيق بين الهيئات والمؤسسات ذات الصلة ويُوصى بوضع آلية تنسيق فعالة بين مختلف الهيئات االتي تهدف الى تحقيق فضاء سبيراني امن، كالوكالة الوطنية لأمن نظم المعلومات، السلطة الوطنية لحماية المعطيات الشخصية، والقطب الجزائي، لتفادي التداخل أو التعارض في الصلاحيات وضمان استجابة موحدة.

-تعزيز صلاحيات الهيئات الوطنية للأمن السيبراني، اذ يستحسن توسيع الصلاحيات الممنوحة لتشمل الرقابة التقنية الفعلية، وإصدار تعليمات ملزمة للهيئات العمومية والخاصة، إضافة إلى تعزيز استقلاليتها المالية والإدارية.

- تدعيم الأجهزة الفاعلة في هذا المجال بالوسائل المادية اللازمة وتجهيزها باحدث الوسائل المستعملة في مجال تكنولوجيا المعلومات والاتصال وذلك حتى تكون هناك نجاعة في مواجهة التهديدات المحتملة باعتبار ان العالم الافتراضي مفتوح امام العالم باسره وهذا الأخير يشهد ثورة تكنولوجية تعدت كل التوقعات والذكاء الاصطناعي مثال على ذلك.

- تكوين العامل البشري في المجال التقني والقانوني في مجال الامن السيبراني لتحقيق الفاعلية في هدا المجال بغرض الالمام بالمعارف المتخصصة في المجال لضمان التطبيق الأمثل للقواعد الازمة لتفادي التهديدات المحتملة في الدرجة الاولى ومكافحتها في الدرجة الثانية لا سيما في القطاعات الحساسة.

- تشجيع البحث العلمي والتطوير في مجال الأمن السيبراني من خلال دعم مراكز البحث الجامعية والمؤسسات العلمية لتطوير حلول وطنية في مجال الحماية السيبرانية، وتطوير برامج وأنظمة معلوماتية قادرة على تأمين البنى التحتية الحيوية.

-دعم القطب الجهات القضائية المتخصصة في الجرائم السيبرانية، و ذلك بتمكين هذا القطب من الموارد البشرية والتقنية اللازمة، مع ضمان تكوين متخصص للقضاة، وكل الضبط القضائي العاملين فيه، نظراً للطبيعة التقنية المعقدة لهذه الجرائم.

- تعزيز التعاون الدولي والإقليمي بالنظر إلى الطبيعة العابرة للحدود للتهديدات السيبرانية، فمن الضروري الانخراط الفعّال في الاتفاقيات الدولية، وتبادل المعلومات والخبرات مع الدول الأخرى، والمنظمات المختصة، بما يعزز قدرة الجزائر على مواجهة التهديدات الرقمية المشتركة.

- ابرام تشاور بين الدول والاتفاقيات من اجل موائمة التشريعات الداخلية لبعضها بغرض إزالة العقبات القانونية في مجال التعاون الدولي خاصة تلك المتعلقة بتعارض مبدأ السيادة والاختصاص القضائي وازدواجية التشريع التي تحول دون تنفيذ إجراءات التعاول فيما يخص تنفيذ الانابات القضائية وتسليم المجرمين.

- ابرام اتفاقيات دولية لتفادي المرور بالطرق الدبلوماسية في هذا النوع من المجال نظرا لعدم توافقه مع هذا النوع من الاخطار الذي يتصف بالسرعة.

- سن قانون موحد خاص بالامن السيبراني يتضمن قواعد موضوعية وإجرائية موحدة لا سيما وان الكثير من الدول سارعت لاصدار قوانين خاصة به ومن بينهما دول جوار وذلك لتفادي تشتت القوانين وتعارضها.

– نشر الوعي بين افراد المجتمع حول المخاطر الناجمة عن التعامل في الفضاء الرقمي بعد زيادة التعامل في مجال التجارة الدولية وزيادة استعمال تكنولوجيات الاعلام والاتصال من طرف شرائح المجتمع المختلقة والمخاطر الناجمة عن استغلال البيانات الشخصية في أغراض غير مشروعة ونشر ثقافة الأمن السبيراني في المجتمع وذلك عن طريق إعداد برامج وطنية للتوعية موجهة لمختلف فئات المجتمع، بهدف تعزيز الثقافة الرقمية، والتحذير من المخاطر السبيرانية، والتشجيع على تبني السلوكيات الآمنة في الفضاء الرقمي.

قائمة المصادر

والمراجع

1- المصادر:

- الدساتير:

- المرسوم الرئاسي رقم 20-442 المؤرخ في 15 جمادى الأولى عام 1442 الموافق 30 ديسمبر 2020 المتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء اول نوفمبر سنة2020، الصادر 15 جمادى الأولى عام 1442 الموافق ل30 ديسمبر 2020، ج ر ج ج العدد 82، بتاريخ.

- الاتفاقيات الدولية:

- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية ل المصادق عليها من الجزائر بتحفظ بموجب المرسوم الرئاسي رقم 02-55 المؤرخ في 22 ذي القعدة عام 1422 الموافق ل05 فبراير 2002 الصادر بتاريخ 27 ذي القعدة عام 1422 الموافق 10 فبراير 2002 ج ر ج ج العدد 09.

- اتفاقية الرياض للتعاون القضائي المصادق عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم 01-47 المؤرخ 17 ذي القعدة عام 1421 الموافق 11فبراير 2001 الصادر بتاريخ 18 ذو القعدة عام 1421 الموافق 12 فبراير 2001 ج ر ج ج العدد 11.

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المثادق عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 13 ذي القعد عام 1435 الموافق 08 سبتمبر 2014 الصادر بتاريخ 04 ذو الحجة عام 1435 28 سبتمبر 2014، ج ر ج ج العدد 57.

- الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الفرنسية الموقعة بباريس بتاريخ 05 أكتوبر سنة 2016 المصادق عليها من الجزائر بموجب المرسوم الرئاسي 18-73 المؤرخ في 09 جمادى الثانية عام 1439 الموافق 25 فبراير 2018 الصادرة 12 جمادى الثانية عام 1439 الموافق 28-02-2018، ج ر ج ج العدد 13.

- القوانين:

- القانون العضوي رقم 05-11 المؤرخ في 10 جمادى الثانية 1426 الموافق ل 17 يوليو 2005 يتعلق بالتنظيم القضائي الصادر بتاريخ 13 جمادى الثانية عام 1426 الموافق 20 يوليو 2005، ج ر ج ج العدد 51.

- القانون رقم 04-14 المؤرخ في 27 رمضان 1425 الموافق 10 نوفمبر 2004 يعدل ويتمم قانون الإجراءات الجزائية، الصادر بتاريخ في 27 رمضان 1425 الموافق 10 نوفمبر 2004، ج ر ج ج العدد 71.

- القانون رقم 04-15 المؤرخ في 27 رمضان 1425 الموافق 10 نوفمبر المعدل والمتمم لامر رقم 66-156 والمتضمن قانون العقوبات، الصادر بتاريخ في 27 رمضان 1425 الموافق 10 نوفمبر 2004 ج ر ج ج العدد 71.

- القانون رقم 06-22 المؤرخ في 29 ذي القعدة 1427 الموافق 20 ديسمبر 2006 يعدل ويتمم الامر 66-155 المتضمن قانون الإجراءات الجزائية، الصادر بتاريخ 04 دو الحجة 1427 الموافق 24 ديسمبر 2006، ج ر ج ج العدد 84.

- القانون رقم 06-23 المؤرخ في 29 ذي القعدة 1427 الموافق 20 ديسمبر 2006، المعدل والمتمم للامر رقم 66-156 المتضمن قانون العقوبات، الصادر بتاريخ 4 دي الحجة 1427 الموافق 24 ديسمبر 2006، ج ر ج ج العدد 84.

-القانون رقم 08-01 المؤرخ في 15 محرم عام 1429 الموافق 23 يناير سنة 2008 المتمم للقانون رقم 83-11 المتعلق بالتامينات الاجتماعية، الصادر بتاريخ 19 محرم عام 1429 الموافق 27 يناير 2008، ج ر ج ج العدد 04.

- القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق 05 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الصادر بتاريخ 25 شعبان 1430 الموافق 16 غشت 2009، ج ر ج ج العدد 47.

- القانون رقم 15-03 المؤرخ في 11 ربيع الثاني 1436 الموافق اول فبراير 2015 المتعلق بعصرنة العدالة، الصادر بتاريخ 20 ربيع الثاني 1436 الموافق ل 10 فبراير 2015، ج ر ج ج العدد 06.

- القانون رقم 15-04 المؤرخ في المؤرخ في 11 ربيع الثاني 1436 الموافق اول فبراير 2015، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الصادر بتاريخ 20 ربيع الثاني 1436 الموافق ل 10 فبراير 2015، ج ر ج ج العدد 06.

- القانون رقم16-02 المؤرخ في 14 رمضان 1437 الموافق 19 يونيو 2016 المتمم للأمر رقم 66-156 والمتضمن قانون العقوبات، الصادر بتاريخ 17 رمضان 1437 الموافق 22 يونيو 20116، ج ر ج ج العدد 37.

- القانون رقم 18-04 المؤرخ في24 شعبان عام 1439 الموافق 10 مايو سنة 2018 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الصادر بتاريخ 27 شعبان 1439 الموافق 13 مايو 2004،ج ر ج ج العدد 27.

- القانون رقم 18-05 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو 2018 ، المتعلق بالتجارة الإلكترونية، الصادر بتاريخ 30 شعبان 1439 الموافق 16 مايو 2018، ج ر ج ج العدد 28.

- القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، الصادر بتاريخ 25 رمضان عام 1439 الموافق 10 يونيو 2018، ج ر ج ج العدد 34

- القانون 20-01 المؤرخ في 9 ذي الحجة عام 1441 الموافق 30 يوليو 2020 المعدل والمتمم للامر رقم 66-156 المتضمن قانون العقوبات، الصادر بتاريخ 9 دو الحجة عام 1441 الموافق 30 يوليو 2020، ج ر ج ج العدد 44.

- القانون 24-06 المؤرخ في 19 شوال عام 1445 الموافق 28 ابريل 2024 المعدل والمتمم للامر رقم 66-156 المتضمن قانون العقوبات، الصادر بتاريخ 21 شوال عام 1445، الموافق ل 30 ابريل 2024، ج ر ج ج العدد 30.

– الأوامر:

- الأمر رقم 66-155 الصادر بتاريخ 18 صفر 1386 الموافق 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية.

- الامر 66- 155 الصادر بتاريخ 18 صفر 1386 الموافق 08 يونيو 1966، المضمن قانون العقوبات.

- الأمر 03_05 المؤرخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو 2003 المتعلق بحقوق المؤلف والحقوق المجاورة، الصادر بتاريخ 23 جمادى الأولى عام 1424 الموافق 23 يوليو 2003،ج ر ج ج العدد 44.

- الأمر 03-08 المؤرخ المؤرخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو 2003 يتعلق بحماية التصاميم الشكلية للدوائر المتكاملة، الصادر بتاريخ 23 جمادى الأولى عام 1424 الموافق 23 يوليو 2003، ج ر ج ج العدد 44

- الأمر 10-05 المؤرخ في 16 رمضان 1431 الموافق ل 26 غشت 2010 المعدل والمتمم للقانون رقم 06-01 المتعلق بالوقاية من الفساد ومكافحة، الصادر بتاريخ 22 رمضان عام 1431 الموافق اول سبتمبر 2010، ج ر ج ج عدد 50.

- الأمر 21-11 مؤرخ في 16 محرم عام 1443 الموافق 25 غشت 2021، يتمم قانون الإجراءات الجزائية، الصادر بتاريخ 17 محرم عام 1443 الموافق 26 غشت 2021، ج ر ج ج العدد 65،

- **المراسيم:**

– المراسيم الرئاسية:

- المرسوم الرئاسي رقم 04- 432، المؤرخ في 17 ذي القعدة عام 1425 الموافق ل 29 ديسمبر 2004، المتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي، الصادر بتاريخ 17 ذو القعدة عام 1425 الموافق 29 ديسمبر 2004، ج رج ج العدد 84.

- المرسوم الرئاسي رقم 08-151، المؤرخ في 20 جمادى الأولى عام 1429 الموافق 26 مايو 2008، المتضمن إحداث مدرسة للشرطة القضائية تابعة للدرك الوطني، الصادر بتاريخ 22 جمادى الأولى عام 1429 الموافق 28 مايو 2008، ج ر ج ج العدد 27.

- المرسوم الرئاسي رقم 15- 261 المؤرخ في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر 2015 ، الذي يحدد تشكيلة تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها الصادر بتاريخ 24 ذي الحجة 1436 الموافق 08 أكتوبر 2015، ج ر. ج ج العدد 53.

- المرسوم الرئاسي 19-172 المؤرخ في 603 شوال عام 1440 الموافق 6 يونيو سنة 2019 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، الصادر بتاريخ 6 شوال 1440 الموافق 09 يونيو 2019، ج ر ج ج العدد 37.

- المرسوم الرئاسي 20-05 المؤرخ في 24 جمادى الأولى عام 1441 الموافق 20 جانفي سنة 2020 يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية الصادر بتاريخ اول جمادى الثانية عام 1441 الموافق 26 جانفي 2020، ج ر ج ج العدد 04.

- المرسوم الرئاسي 20- 183 المؤرخ في 21ذي القعدة عام 1441 الموافق 13 يوليو سنة 2020 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الصادر بتاريخ 26 ذو القعدة 1441 الموافق 18 يوليو 2020، ج ر ج ج العدد 40

المراسيم التنفيذية:

- المرسوم التنفيذي رقم 06-348 المؤرخ في 12 رمضان عام 1427 الموافق 05 أكتوبر 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، الصادر بتاريخ 15 رمضان عام 1427 الموافق 08 أكتوبر 2006، ج ر ج ج العدد 63.

- المرسوم التنفيذي رقم 10-322، المؤرخ في 16 محرم عام 1432 الموافق 22 ديسمبر سنة 2010 المتضمن القانون الأساسي الخاص بالموظفين المنتمين للأسلاك الخاصة بالأمن الوطني، الصادر بتاريخ 20 محرم عام 1432 الموافق 26 ديسمبر 2010، ج ر ج ج العدد78،

- المرسوم التنفيذي رقم 16-267 المؤرخ في 15 محرم عام 1438 الموالفق 17 أكتوبر 2016، يعدل المرسوم التنفيذي رقم 06-348 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، الصادر بتاريخ 21 محرم 1438 الموافق 23 اكتوبر 2016، ج ر ج ج العدد 62.

القرارات:

- القرار الوزاري المشترك، المؤرخ في 26 ربيع الأول عام 1428 الموافق 14 أبريل سنة2007، المتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، الصادر بتاريخ 17 جمادى الأولى عام 1428 الموافق 03 يونيو 2007، ج ر ج ج العدد 36.

2- المراجع:

- الكتب:

- بوبكر رشيدة، الحماية الجزائية للتعاملات الالكترونية، ط1، منشورات الحلبي الحقوقية، بيروت لبنان،2020.

- بوسقيعة أحسن ، الوجيز في القانون الجزائري الخاص، ط10، دار هومة للنشر والتوزيع، الجزائر، د ت ن

- حسن الزواهرة رامي إبراهيم، النشر الرقمي للمصنفات وأثره على الحقوق الأدبية والمالية للمؤلف (دراسة مقارنة)، ط1، دار وائل للنشر، عمان، 2013.

- خاطر صبري حمد، مدى تطويع القواعد التقليدية في مواجهة المعلومات(دراسة مقارنة)، د ط، دار الكتب القانونية، مصر، 2014.

- خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر (أساليب وثغرات)، دار الهدى، طبعة 2010، الجزائر.

- خليفة محمد، الحماية الجنائية لمعطيات الحاسب الآلي في قانون الجزائري المقارن، ط3، دار الجامعة الجديدة، الإسكندرية، مصر، د ت ن.

- زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، ط2011، الجزائر.

- سامي منصور، الأعمال الاجرامية التي تستهدف الأنظمة المعلوماتية، دط، دار المنشورات الحقوقية، بيروت، لبنان، د ت ن.

- طعباش أمين ، الحماية الجنائية للمعاملات الإلكترونية، مكتبة الوفاء القانونية، ط1، مصر، 2015.

- طلعت الشهاوي، المسؤولية الجنائية عن جرائم الاتصالات، ط1، دار النهضة العربية، القاهرة، مصر2018.

- علي عبد القادر قهوجي، الحماية الجنائية لبرامج الكمبيوتر، دط، المكتبة القانونية، القاهرة، 1999.

- علي عدنان الفيل، الاجرام الالكتروني، منشورات زين الحقوقية، الموصل، ط1، 2011

- عمر ابو الفتوح عبد العظيم الحطامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا، دراسة مقارنة، د ط، النهضة العربية، القاهرة، 2010.

- عياد الحلبي خالد، إجراءات التحدي والتحقيق في جرائم الحاسوب والانترنت، ط1، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011.

- فرج يوسف أمير، الأدلة الالكترونية ودورها في مكافحة الجريمة الالكترونية والمعلوماتية، ط1، مؤسسة المعرفة لنشر وتوزيع الكتب، مصر، 2025.

- فرج يوسف أمير، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية، طبعة 2009.

- ففي حسين سامي جلال، التفتيش في الجرائم المعلوماتية (دراسة مقارنة)، ط1، دار الخلدونية، الجزائر، 2021.

- قارة امال، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط2، دار هومة،

- قنديل أشرف عبد القادر، الإثبات الجنائي في الجريمة الالكترونية، دار الجانعة الجديدة للنشر، مصر، طبعة 2015.

- محرز خيرت علي، التحقيق في جرائم الحاسب الآلي، د ط، دار الكتاب الحديث، الجزائر، 2012.

- محمد أمين الشوابكة، جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، دار الثقافة للنشر والتوزيع، ط1، مصر، 2015.

- نبيل محمد عثمان عرعارة، الحماية الجنائية للحق في حرمة المراسلات عبر البريد الالكتروني، ط01، المصرية للنشر والتوزيع، القاهرة، مصر، 2008.

- هروال نبيلة هروال، الجوانب الإحداثية لجرائم الانترنت في مرحلة الاستدلالات، د ط، دار الفكر الجامعي، الإسكندرية، مصر،2013.

- المقالات العلمية:

- العيداني رزق، زروق يوسف، حماية المعطيات الشخصية في الجزائر على ضوء القانون رقم 18-07، مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي تندوف، العدد5، ديسمبر 2018.

- بارة سمير، الامن السبيراني في الجزائر: السياسات و المؤسسات، المجلة الجزائرية للامن الإنساني، العدد الرابع، جويلية 2017.

- بن خليفة الهام ، غريسي جمال ، التجسس الالكتروني كجريمة ماسة بأمن الدولة في التشريع الجزائري، مجلة دفاتر السياسة والقانون، جامعة ورقلة، المجلد 14، العدد 01، 2022.

- بوداود خليفة، بوزيان السعيد ، معالجة المعطيات ذات الطابع الشخصي بين الضمانات القانونية الدولية والداخلية، مجلة البحوث والدراسات، جامعة الوادي، المجلد 20، العدد 02، سنة 2023.

- شميشم رشيد، الحق في الصورة، مجلة البحوث والدراسات العلمية، جامعة المنيعة، العدد الثالث، ديسمبر 2009.

- شويطر ايمان رتيبة ، الأقطاب الجزائية المتخصصة كتوجه لمكافحة جرائم الأعمال، مجلة البحوث في العقود وقانون الأعمال، مجلة البحوث في العقود وقانون الأعمال، المجلد 07، العدد 01، جامعة الاخوة منتوري، قسنطينة1، الجزائر، 2022.

- مجدوب نوال، الآليات الإجرائية للكشف عن الجريمة المعلوماتية، مجلة البحوث القانونية والاقتصادية، المركز الجامعي مغنية، المجلد 06، العدد 3، 2023.

- بن علال نزيهة، الإطار القانوني لحماية المعطيات ذات الطابع الشخصي في الفضاء الالكتروني في ظل القانون رقم 18-07، مجلة دائرة البحوث والدراسات القانونية والسياسية، المركز الجامعي تيبازة، المجلد 4، العدد 2، سنة2020.

- بوبكر آمال، التصديق الالكتروني، مجلة المفكر للدراسات القانونية والسياسية، جامعة خميس مليانة، العدد 3، سبتمبر2018.

- بوحليط يزيد، فطناسي عبد الرحمان، الحماية الإدارية والجزائية في مجال المعطيات ذات الطابع الشخصي على ضوء القانون 18-07، مجلة أبحاث قانونية وسياسية، جامعة جيجل، المجلد06، العدد 02، ديسمبر2021.

- بوزيان كريم، الحماية الجزائية لمستخدمي الصحة في ظل قانون العقوبات لسنة 2020، مجلة الدراسات القانونية والمقارنة، جامعة المدية، المجلد07، العدد 01، سنة 2020.

- بوقرة جمال الدين، عنان جمال الدين، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، the national penal polefor combating offenses related to information and communication technologies، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 07، العدد 01، جامعة محمد بوضياف، المسيلة، جوان2022.

- تقرير المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والنشر والإشهار وحدة الطبع رويبة، الجزائر، العدد 144، سبتمبر2019.

- جبايلي صبرينة، النظام القانوني للسلطة الوطنية للتصديق الالكتروني، مجلة العلوم الإنسانية، جامعة عباس لغرور خنشلة، عدد 48، المجلد أ، ديسمبر2017.

- جغريف الزهرة، المعالجة الخزانية للمعطيات ذات الطابع الشخصي في التشريع الجزائري وفقا لأحكام المادة 18-07، مجلة العلوم القانونية والاجتماعية، جامعة الجلفة، المجلد السادس، العدد الرابع، ديسمبر 2021.

- حزام فتيحة ، الحق في الحياة الخاصة بالبيئة الرقمية دراسة مقارنة، مجلة الدراسات القانونية المقارنة، جامعة الشلف، المجلد 08، العدد 01، 2022.

- خالدي فتيحة، تأثير التجسس الالكتروني على الحق في الخصوصية المعلوماتية، مجلة البحوث والحقوق والعلوم السياسية، جامعة تيارت، المجلد 07، العدد 01، 2021.

- رامي حليم، جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات، مجلة دراسات وأبحاث، جامعة الجلفة، المجلد 01، العدد 01، 2009.

- زروقي عباسية، جرائم الاعتداء على الحياة الخاصة عبر شبكات التواصل الاجتماعي وآليات الحماية، مجلة القانون والعلوم السياسية، المركز الجامعي النعامة، المجلد08، العدد 02، 2022.

- سوماتي شريفة، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال كآلية جديدة ضمن الجهاز القضائي المتخصص National penal pole for combating crimes related to information and communication technologies ad a new machamism within the specialzed judiciary body، مجلة الدراسات القانونية (صنف ج)، المجلد 08، العدد 02، جامعة يحي فارس بالمدية، الجزائر، جوان 2022، ذو الحجة 1443.

- طباش عز الدين، الحماية الجزافية للمعطيات الشخصية في السريع الجزائري، المجلة الأكاديمية للبحث القانوني، جامعة بجاية، العدد 2، 2018.

- طوبال عبد السلام، منى غبولي، الضمانات القانونية لحماية المعطيات ذات الطابع الشخصي في التدرج الجزائري، مجلة العلوم القانونية والاجتماعية، جامعة ريان عاشور بالجلفة، المجلد 05، العدد 02، جوان 2020.

- عصارة أبو عجيلة شعبان، أبو المعالي محمد عيسى أبو المعالي، الرصد المبكر لخطر الجريمة، مجلة العلوم القانونية والشرعية، كلية القانون، جامعة الزاوية، ليبيا، العدد السادس، يونيو2015.

- عميور خديجة، قواعد اختصاص الأقطاب الجزائية للنظر في جرائم الفساد، مجلة دراسات في الوظيفة العامة، المركز الجامعي، البيض، الجزائر، العدد 02، ديسمبر2014.

– قهواجي أمينة، مطالي ليلى، الإطار المفاهيمي والقانوني للتوقيع والتصديق الإلكترونيين في الجزائر، مجلة المشكلة في الاقتصاد التنمية والقانون، العدد 08، المجلد 04، كلية العلوم الاقتصادية التجارية وعلوم التسيير، جامعة بومرداس، الجزائر،2023.

– لعمراني آسيا، التعاون الدولي في مجال الجريمة السيبرانية، الجزائر نموذجا، المجلة الجزائرية للعلوم السياسية والعلاقات الدولية، المجلد03، العدد 02، ديسمبر2010.

– مامن بسمة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، المجلد 09، العدد 01، 2022.

– مجدوب نوال، الآليات الإجرائية للكشف عن الجريمة المعلوماتية، مجلة البحوث القانونية والاقتصادية، المركز الجامعي مغنية، المجلد 06، العدد3، 2023.

– مهدي رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة إليزا للبحوث والدراسات، المركز الجامعي اليزي، المجلد 06، العدد 02، سنة 2021.

– هامل محمد، يوسفي مباركة ، القطب الجزائي الاقتصادي والمالي كآلية لمكافحة جريمة التهريب، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد الخامس، العدد2، جامعة عمار ثليجي، الأغواط، سنة2020.

– يحياوي سعاد، التصديق الالكتروني آليك تقنية لضمان وحمايك المعاملات التحارية الالكترونية في القانون الجزائري، مجلة الدراسات القانونية المقارنة، جامعة الشلف، المجلد 08، العدد 01، 2022.

– الرسائل العلمية:

– اطروحات الدكتوراة:

– باقدي دوجة، حماية حقوق الملكية الفكرية على الانترنيت، مذكرة دكتوراه تخصص قانون عام، كلية الحقوق و العلوم السياسية، جامعة مولود معمري، تيزي وزو، 2020 .

– براري نعيمة، الاتصال بين الشرطة والمواطن ودوره في مكافحة الجريمة في الجزائر دراسة تحليلية استطلاعية بالجزائر العاصمة، رسالة نيل شهادة الدكتوراه في علوم الإعلام والاتصال، كلية العلوم السياسية والإعلام، جامعة الجزائر3، 2013/2012.

– تياب نادية، آليات مواجهة الفساد في الصفقات العمومية، رسالة مقدمة لنيل شهادة الدكتوراه كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013/2014.

– رابحي عزيزة، الاسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، سنة 2017.

- عثماني رضوان، مكافحة جرائم المعلوماتية في القانون الجزائري والدولي، أطروحة دكتوراه تخصص قانون جنائي، جامعة وهران2. محمد بن أحمد، الجزائر، 2024/2023.

- مخلوفي عبد الوهاب، التجارة الإلكترونية عبر الانترنت، أطروحة دكتوراه في الحقوق لتخصيص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، الجزائر، 2012.

- رسائل الماجستير:

- بوخبزة عائشة، الحماية الجزائرية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماجيستير في القانون الجنائي، كلية الحقوق، جامعة وهران، الجزائر، 2012/2013.

- بوطبيبة عومار، دراسة واقع نظم المعلومات بمديرية الشباب والرياضة لولاية قسنطينة، مذكرة لنيل شهادة الماجستير في الإدارة والتسيير الرياضي، المركز الجامعي محمد الشريف مساعدية سوق أهراس، الجزائر، 2012/2011.

- بودراع عبد العزيز خصوصية الجرائم الماسة بانظمة المعالجة الالية للمعطيات، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر، سنة 2011.

- مذكرات الماستر:

- ثابت ايمان، ميهوب اسية، إجراءات التحري الخاصة في الجريمة الالكترونية، مذكرة ماستر تخصص قانون الإعلام الآلي والانترنت، كلية الحقوق والعلوم السياسية، جامعة البشير الإبراهيمي، برج بوعريريج، الجزائر،2023/2024.

- حشايشي مسعود، مشري مروان ، حماية الحق في الخصوصية المعلوماتية في التشريع الجزائري، مذكرة ماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف،المسيلة، الجزائر،2021/2022.

- زروال العيد، نغزة عثمان ، جريمة انتهاك الحياة الخاصة عبر الانترنت، مذكرة ماستر، تخصص قانون الإعلام الآلي والانترنت، كلية العلوم السياسية والحقوق، جامعة محمد البشير الإبراهيمي، 2022/2021.

- عياشي عاشور، يعيش عبد الحق ، آليات مكافحة جريمة التجسس الإلكتروني في التشريع الجزائري، مذكرة ماستر تخصص قانون الإعلام الآلي والانترنت، قسم الحقوق، جامعة البشير الإبراهيمي، برج بوعريريج، الجزائر، 2023/2024.

- بن عزوز فاطة الزهراء، سالمي وهيبة، الاليات القانونية لمكافحة الجرائم الماسة بالامن الالكتروني، مذكرة ماستر في الحقوق تخصص القانون الجنائي، كلية الحقوق و العلوم السياسية، جامعة زيان عاشور، الجلفة، 2020/2019،

- بودواب سمير– لديوي فؤاد ، جرائم المساس بانظمة المعالجة الالية للمعطيات، مذكرة شهادة ماستر، تخصص قانون جنائي وعلوم جنائية، جامعة 20 اوت 1955، سكيكدة، جوان 2024، ص25.

- بوقرة مبركة، طالبي آسيا، الحماية الجزائرية للمعطيات الشخصية في ظل القانون 07/18، مذكرة ماستر، جامعة قاصدي مرباح، ورقلة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2021/2022.

- رحالي محمد الأمين، روبة عبد الحكيم، النظام القانوني لسلطة ضبط البريد والاتصالات الإلكترونية، مذكرة مكملة لنيل شهادة الماستر في الحقوق، تخصص قانون عام، كلية الحقوق، جامعة عين تيموشنت -بلجاح بوشعيب، الجزائر،2024.

- عاصف أسماء، الجرائم الرقمية وطرق إثباتها، مذكرة ماستر، تخصص قانون قضائي، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، الجزائر، 2023/2024.

- عائشة نايري، الجريمة الالكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الإداري، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة احمد دراية- ادرار، سنة 2017.

- عرفة سارة – طابون سليمة، تكليف الجريمة الالكترونية في التشريع الجزائري مذكرة ماستر، تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، سنة 2020، 2021.

- عز الدين كوثر، عبد المومن بشرى آية ، إجراءات البحث والتحدي في الجريمة الالكترونية، مذكرة ماستر تخصص قانون أعمال، قسم الحقوق، جامعة الشادلي بن جديد الطارف، الجزائر، 2021/2022.

- علاني حليمة، الحماية الجنائية للمعطيات الشخصية في التشريع الجزائري، مذكرة تخرج لاستكمال متطلبات نيل شهادة ماستر، جامعة قاصدي مرياح، كلية الحقوق والعلوم السياسية، تخصص قانون جنائي، 2018/2019.

- عيساني لامية، كعال فطيمة، جريمتي الخيانة والتجسس في أصل القضاء العسكري الجزائري، مذكرة ماستر، تخصص جنائي وعلوم جنائية ، كلية الحقوق والعلوم السياسية، قسم الحقوق جامعة العربي بن مهيدي، أم البواقي، 2021/2020.

- مختاري كوثر، الاعتداء على الحياة الخاصة على شبكات التواصل الاجتماعي، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2017/2018.

- التظاهرات العلمية:

- الملتقيات الدولية:

- النحوي سليمان، آليات مكافحة الجريمة السيبرانية في التشريع الجزائري، مداخلة مقدمة ضمن فعاليات الملتقى الدولي، المنظم من طرف كلية الحقوق والعلوم السياسية، قسم الحقوق جامعة برج بوعريريج الموسوم بعنوان: الإجرام السيبراني المفاهيم والتحديات، يومي 11 و 12 أفريل 2017.

- بارة سميرة، الدفاع الوطني والسياسات الوطنية للأمن السيبراني (CyperSecurity)في الجزائر الدور والتحديات، ورقة بحثية مقدمة في إطار أشغال الطبعة الثانية من الملتقى الدولي: سياسات الدفاع الوطني بين

الالتزامات السيادية والتحديات الإقليمية، كلية الحقوق والعلوم السياسية ومخبر التحولات السياسية والإقتصادية والاجتماعية والقانونية في التحربة الجزائية، جامعة قاصدي مرباح، ورقلة، الجزائر، يومي الإثنين والثلاثاء 30،31 جانفي 2017.

– بن بادة عبد الحليم، بوحدة محمد سعد، مداخلة بعنوان: جريمة التجسس الإلكتروني نمط جديد من التهديدات السيبرانية الماسة بأمن دول المنطقة– دراسة سياسية قانونية، الملتقى الدولي الأول الموسوم بامن المعلومات في الفضاء الالكتروني الرهانات و التحديات في شمال افريقيا، المنعقد يومي 17 و 18 فيفري 2022، كلية الحقوق و العلوم السياسية، جامعة غرداية.

– بن صويلح امال، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الإلكتروني بالجزائر، ورقة بحثية مقدمة في إطار الملتقى الدولي حول: الإجرام السيبراني المفاهيم والتحديات، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، يومي 11-12 أفريل 2017.

– الملتقيات الوطنية:

– دهيليس عادل، كاسحي موسى، مداخلة بعنوان دور وأهمية التوقيع الإلكتروني في تسهيل المعاملات التجارية والمالية، ملتقى وطني حول: الإصلاحات المالية والمصرفية في الجزائر الواقع والمأمول، كلية العلوم الاقتصادية والتحارية وعلوم التسيير ، جامعة وهران 2، محمد بن أحمد بالتعاون مع مخبر التوجهات والتحديات الجديدة للسياسات التنموية في الجزائر، يوم 30 ماي 2022.

– الأيام الدراسية:

– بومحراث ليندة، مداخلة بعنوان: إجراءات التحقيق الخاصة السيبرانية يوم دراسي حول: الجريمة السيبرانية، مجلس قضاء قسنطينة وجامعة الأمير عبد القادر للعلوم الإسلامية، يوم 20 أفريل 2022.

– المواقع:

– الموقع الرسمي لوزارة البريد والمواصلات السلكية واللاسلكية mpt. gov. dz تاريخ الاطلاع 01-06-2025 الساعة 05:03.

الفهرس

الموضوع	الصفحة
مقدمة	2
الفصل الأول: الآليات القانونية الموضوعية لتحقيق الامن السبيراني	7
المبحث الأول: الاليات القانونية الموضوعية لتحقيق الامن السبيراني في قانون العقوبات	9
المطلب الأول: حماية أنظمة المعالجة الالية للمعطيات كآلية لتحقيق الامن السبيراني	9
الفرع الأول: مفهوم أنظمة المعالجة الالية للمعطيات	9
الفرع الثاني: صور جريمة المساس بانظمة المعالجة الالية للمعطيات	11
الفرع الثالث: الجزاءات المقررة لجرائم المساس بانظمة المعالجة الالية للمعطيات	17
المطلب الثاني: النصوص التقليدية كآلية لتحقيق الامن السبيراني	19
الفرع الأول: الجرائم الواقعة على أمن الدولة في الفضاء السبيراني	19
الفرع الثاني: الجرائم الواقعة على الافراد في الفضاء السبيراني	23
الفرع الثالث: الجرائم الواقعة على الاموال في الفضاء السبيراني	27
المبحث الثاني: الآليات القانونية الموضوعية لتحقيق الامن السبيراني في القوانين الخاصة	33
المطلب الاول: حماية المعطيات ذات الطابع الشخصي كآلية لتحقيق الأمن السبيراني	33
الفرع الأول: المبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي	33
الفرع الثاني: ضوابط عمليات المعالجة الآلية للمعطيات الشخصية	38
الفرع الثالث: الحماية الجزائية للمعطيات ذات ا لطابع الشخصي	44
المطلب الثاني: آليات تحقيق الامن السبيراني في القوانين الموضوعية المتفرقة	51
الفرع الأول: الامن السبيراني في مجال الاتصالات الالكترونية	51
الفرع الثاني: الامن السبيراني في مجال قوانين الملكية الفكرية	59
الفرع الثالث: الامن السبيراني في مجال التوقيع والتصديق الالكترونيين	66
خلاصة الفصل	77
الفصل الثاني: الآليات الإجرائية والهيكلية لتحقيق الامن السبيراني في التشريع الجزائري	78
المبحث الأول: الآليات القانونية الإجرائية لتحقيق الأمن السبيراني	80

المطلب الأول: الآليات الاجرائية المستحدثة في قانون الإجراءات الجزائية	80
الفرع الأول: اعتراض المراسلات والتسجيل والتقاط الصور	81
الفرع الثاني: التسرب	82
المطلب الثاني: الآليات المستحدثة وفقا لقانون الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها	85
الفرع الأول: مراقبة الاتصالات الالكترونية	85
الفرع الثاني: تفتيش المنظومة المعلوماتية	87
الفرع الثالث: حجز المعطيات المعلوماتية	90
الفرع الرابع: فرض التزامات على مقدمي الخدمات	93
المطلب الثاني: التعاون الدولي كآلية لتحقيق الأمن السيبراني	95
الفرع الأول: التعاون الدولي على المستوى الأمني	95
الفرع الثاني: التعاون الدولى على المستوى القضائي	98
الفرع الثالث: التعاون الدولى على مستوى تسليم المجرمين	101
المبحث الثاني: الآليات الهيكلية لتحقيق الأمن السيبراني	104
المطلب الأول: الهيئات القضائية	104
الفرع الأول: الأقطاب الجزائية المتخصصة	104
الفرع الثاني: القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال	109
المطلب الثاني: الهيئات غير القضائية	116
الفرع الأول: الهيئات المستقلة	116
الفرع الثاني: الهيئات التابعة لأجهزة أخرى	129
خلاصة الفصل	134
خاتمة	136
المصادر والمراجع	142
الفهرس	154
الملخص	157

ملخص البحث:

شهد العالم في العقود الأخيرة تحولاً رقمياً شاملاً، تزامن مع توسع كبير في استخدام تكنولوجيات الإعلام والاتصال في شتى مناحي الحياة، مما أدى إلى نشوء فضاء جديد يُعرف بـ"الفضاء السيبراني"، الذي لم يعد مجرد بيئة معلوماتية، بل تحول إلى ساحة للصراع والتحديات الأمنية العابرة للحدود. وفي ظل هذا الواقع، أصبحت التهديدات السيبرانية تشكل خطرًا حقيقيًا على الدول، الأفراد، المؤسسات، والمنشآت الحيوية، سواء من حيث الاختراقات، سرقة البيانات، التجسس الإلكتروني، أو تدمير الأنظمة الحساسة.

إن مواجهة هذه التهديدات لم تعد ممكنة بالوسائل التقنية فقط، بل أصبحت تستوجب تدخلًا قانونيًا وتشريعيًا واضحًا، إضافة إلى بناء هياكل مؤسساتية وقضائية وطنية فعّالة ومتخصصة في رصد ومجابهة مختلف المخاطر السيبرانية. وقد سعت الجزائر، على غرار بقية دول العالم، إلى تبنّي سياسات وتشريعات خاصة بالأمن السيبراني، وهو ما حاولنا دراسته في هذه المذكرة من خلال تسليط الضوء على الأليات القانونية لتحقيق الأمن السيبراني في التشريع الجزائري.

الكلمات المفتاحية:

الامن السيبراني– الجريمة السيبرانية– أنظمة معلومات– اتصالات الكترونية– تكنولوجيا الاتصال.

اللغة الفرنسية:

Au cours des dernières décennies, le monde a connu une transformation numérique profonde, accompagnée d'une expansion massive de l'utilisation des technologies de l'information et de la communication dans tous les domaines de la vie. Cela a conduit à l'émergence d'un nouvel espace appelé « cyberspace », qui n'est plus un simple environnement informationnel, mais est devenu un champ de conflits et de défis sécuritaires transfrontaliers

Face à cette réalité, les menaces cybernétiques représentent un danger réel pour les États, les individus, les institutions et les infrastructures vitales, que ce soit en termes de piratage, de vol de

données, d'espionnage électronique ou de destruction de systèmes sensibles.

La lutte contre ces menaces ne peut plus se limiter aux moyens techniques, mais exige également une intervention juridique et législative claire, ainsi que la mise en place de structures institutionnelles et judiciaires nationales efficaces et spécialisées dans la détection et la lutte contre les risques cybernétiques. L'Algérie, à l'instar des autres pays, a œuvré à l'adoption de politiques et de législations spécifiques en matière de cybersécurité, ce que nous avons tenté d'analyser dans ce mémoire à travers l'étude des mécanismes juridiques mis en place pour garantir la sécurité cybernétique dans la législation algérienne

اللغة الإنجليزية:

In recent decades, the world has undergone a profound digital transformation, accompanied by a significant expansion in the use of information and communication technologies in all areas of life. This has led to the emergence of a new domain known as "cyberspace," which is no longer just an informational environment, but has become a battlefield for cross-border security challenges and conflicts.

In this context, cyber threats now pose a real danger to states, individuals, institutions, and critical infrastructures, whether through hacking, data theft, cyber espionage, or the destruction of sensitive systems.

Confronting these threats is no longer achievable through technical means alone; it also requires clear legal and legislative intervention, along with the establishment of effective and specialized national institutional

and judicial structures to monitor and combat various cyber risks. Like other countries, Algeria has sought to adopt specific policies and legislation on cybersecurity, which we aimed to explore in this dissertation by highlighting the legal mechanisms put in place to ensure cybersecurity within Algerian legislation.