الجمهورية الجزائرية الديمقراطية الشعبية
People's democratic republic of algeria
وزارة التعليم العالي والبحث العلمي
Ministray of higher education and scientific research
جامعة محمد البشير الإبراهيمي- برج بوعريريج-
University of mohammed Al-bachir Al –Ibrahimi-BBA
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق

تخصص: قانون أعمال

الموسومة ب :

الجريمة السيبرانية في القانون الجنائي الجزائري

إعداد الطالبتين :

- بوسام وصال
- بوناب آية

إشراف :

- د. فرشة كمال

لجنة المناقشة

(اللقب والاسم)	(الرتبة)	(الصفة)
• رفاف لخضر	أستاذ محاضر قسم–أ–	رئيسا
• دريسي عبد الله نيابة عن البروفيسور فرشة كمال	أستاذ مساعد قسم–ب–	مشرفا
• حاجي عبد الحليم	أستاذ محاضر قسم–ب–	ممتحنا

السنة الجامعية : 2024/2023

بسم الله الرحمن الرحيم

{الشكر والتقدير}

الحمد لله كثيرا حتى يبلغ الحمد منتهاه والصلاة والسلام على أشرف مخلوق أناره الله بنوره واصطفاه أما بعد.

نتقدم بخالق الشكر والتقدير والإحترام إلى الأستاذ المشرف الدكتور فرشة كمال على توجيهاته طيلة إنجاز هذه المذكرة.

نشكر أيضا الدكتور محمد الصالح بلعقون على ما قدمه لنا، وأفاضنا به من مراجع في دراستنا هذه.

والشكر موصول إلى كل أستاذ أفادنا بعلمه ولم يبخل علينا بالمساعدة في إنجاز ورقتنا البحثية.

كما لا ننسى أن نشكر جميع من قدم لنا يد المساعدة من الزملاء والأقارب سواء من بعيد أو من قريب.

{الإهداء}

الحمد لله وكفى والصلاة على حبيبنا المصطفى وأهله ومن وفى أما بعد

إلى الأمان والحنان وبلسم الزمان، إلى زهرة الحياة وجنة الأرض، أمي ، أختي وصديقتي حفظها الله وأطال في عمرها.

إلى من فنى عمره واستنزف صحته وقوته ليوصلني إلى هذا اليوم، أبي أطال الله في عمره.

إلى من أشُد عضدي به، والجبل الذي أسند عليه، أخي الوحيد سفيان حفظه الله.

إلى أستاذي فرشة كمال وكل أساتذة كلية الحقوق والعلوم السياسية جامعة محمد البشير الإبراهيمي.

كما لا أنسى بالذكر زميلتي في هذا العمل آية بوناب.

وصال

{الإهداء}

الحمد لله و الصلاة والسلام على من أُرسل فينا عبدا ورسولا محمدا بن عبد الله

أهدي ثمرة عملي هذا إلى مفتاح توفيقي في الدنيا والآخرة، جنتي في الأرض والدي حفظهما الله وأطال في عمرهما.

إلى سندي وقوتي وملاذي، إلى من آثروني على أنفسهم: إخوتي حفظهم الله.

إلى أستاذي الفاضل فرشة كمال.

إلى جميع أساتذتي اللذين رافقوني في مشواري الدراسي.

كما لا أنسى بالذكر زميلتي في هذا العمل وصال بوسام.

آية

قائمة المختصرات:

ص = الصفحة

ص ص = من الصفحة إلى الصفحة

د.ط = دون طبعة

د.م = دون مجلد

د.ع = دون عدد

د.ب = دون بلد النشر

د.ت = دون تاريخ النشر

مقدمة

مقدمة:

إن نمط التقدم المتسارع و النمو في العديد من الدول صاحبته آثار سلبية على الجانب الإقتصادي و الإجتماعي والبيئي والأمني مما أدى إلى إبراز أنماط مستحدثة من الجرائم ، حيث تنقسم الجرائم إلى عدة تقسيمات نذكر منها: الجرائم الواقعة على الأموال ومن أمثلتها جريمة السرقة وجريمة النصب والجرائم الواقعة على الأشخاص كجريمة القتل وجريمة الضرب والجرح العمد.

وقد برزت في الأفق جرائم غير تقليدية تقع على نظام الحاسوب وأخرى ترتكب بواسطته وهي ما يُعرف بالجرائم السيبرانية.

لقد مرت الجرائم السيبرانية بتطور تاريخي تبعا لتطور التقنية و استخداماتها، فقبل ظهور الإنترنت كانت توجد الأفعال الإجرامية وكانت هذه الأفعال تشمل القتل والسرقة و النصب والتزوير وغيرها من الجرائم، بيد أن الإنترنت ساعدت على سهولة ارتكاب هذه الجرائم ، ففضاء المعلومات ليسا له مبادئ أخلاقية عامة، فحدود السلوك المقبول أو حتى السلوك الأخلاقي في فضاء المعلومات ليست واضحة، فوجود الإنترنت أدى إلى تطور الجرائم التقليدية واستحداث جرائم جديدة

ومن بين الجرائم المستحدثة والغير تقليدية ما يعرف بالجرائم السيبرانية، فلقد كان المشرع الجزائري يحاسب على الجرائم العادية، ثم ظهرت الجريمة السيبرانية وانتشرت في الآونة الأخيرة وأصبحت ظاهرة جديرة بالنظر والإعتبار تخترق المجتمع وتهدد دعائمه، ولعله الجوهر والسبب الرئيسي لتجريم المشرع لهذه الجريمة، وهو ما دعا به إلى سن تشريعات تتماشى مع المستجدات على الساحة الإجرامية.

إستقرت تسمية الجرائم السيبراينة على هذا الإسم بعد أن عرفت عدة تسميات حيث كانت تسمى بجرائم إساءة إستخدام الحاسب الآلي، ثم إلى تسمية إحتيال الحاسوب والجريمة المعلوماتية، فمصطلح جرائم الكمبيوتر وجرائم التقنية العالية إلى جرائم الهاكزر فجرائم الأنترنت إلى آخر التسميات الجرائم السيبرانية.

أما في التشريع الجزائري فقد أطلق عليها مصطلح الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وقد عرفها بموجب المادة 2 من القانون 09-04 وقد تطرق إليها وإلى كيفية محاربتها في العديد من القوانين التي سنها منها: قانون العقوبات ، وقانون الإجراءات الجزائية ، القانون المدني وقوانين الملكية الفكرية والصناعية ، قانون التأمينات الإجتماعية وغيرها من القوانين.

تظهر أهمية دراستنا لهذا الموضوع في كونه من الموضوعات الأكثر حداثة وإنتشارا في التشريعات الأجنبية والعربية على غرار التشريع الجزائري.

وتعود أسباب اختيارنا لهذا الموضوع لأسباب ذاتية أولها الميول الشخصي لمثل هذه الموضوعات دفعنا لاختيار هذا الموضوع ضمن قائمة المواضيع المقترحة من قبل الأستاذ المشرف، والشغف بكل ماهو جديد في الجرائم الواقعة على المنظومة المعلوماتية والمجال السيبراني، بينما الأسباب الموضوعية فنظرا لأن الجرائم هي عدة أنواع ومن بينها الجرائم السيبراينة جعلنا نُلح في دراسة هذا الموضوع لتمييز الجرائم السيبرانية عن باقي الجرائم وكشف الغموض الذي يكتنف هذا النوع من الإجرام والذي يختلف عن الجرائم التقليدية.

تهدف هذه الدراسة إلى الإحاطة بمضامين الجريمة السيبرانية من خلال الوقوف على دلالتها وكيفيات مكافحتها.

ومن بين الأبحاث والدراسات التي تناولت الموضوع الذي قمنا بدراسته ما يلي:

– عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر، كلية العلوم الإقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرياح–ورقلة– 2019.

– العيد شعثان ومسعود موقفي، الجريمة السيبرانية في القانون الجزائري، مذكرة ماستر كلية الحقوق والعلوم السياسية، جامعة زيان عاشور–الجلفة–2021_2022.

– عيش موسى وخمود محمد، الأمن السيبراني، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة مولود معمري –تيزي وزو– 2023.

– جمال شريف، عبد العزيز زقوار، آليات مواجهة الجريمة السيبراينة في الجزائر، مذكرة ماستر ، كلية الحقوق والعلوم السياسية، جامعة محمد البشر الإبراهيمي–برج بوعريريج– 2022_2023.

بناءا على ما سبق فإن الإشكالية الرئيسية لهذه الدراسة هي: **كيف عالج المشرع الجزائري أحكام الجريمة السيبرانية في مفهومها وكيفية مكافحتها؟**

وبناءً على ما تقدم و للإجابة عن الإشكالية المطروحة وللإحاطة بمضامين الموضوع اعتمدنا على المنهج الوصفي بغرض وصف الجريمة السيبرانية من خلال تعريفها وتبيان خصائصها وصورها وكذا التعرف على مرتكبها، كما اعتمدنا على المنهج التحليلي بغرض تحليل النصوص القانونية ودراسة آليات وأساليب التحري عن الجريمة السيبراينة.

ولمعالجة هذه الدراسة قسمنا موضوع بحثنا إلى فصلين، خصصنا الفصل الأول لدراسة ماهية الجريمة السيبرانية، أما الفصل الثاني فقد خصص إلى دراسة آليات مكافحة التصدي للجريمة السيبرانية في التشريع الجزائري.

الفصل الأول

ماهية الجريمة السيبرانية

الفصل الأول: ماهية الجريمة السيبرانية

تعتبر الجريمة السيبرانية شكل من أشكال الجريمة المتطورة عبر الوطنية والعالمية إذ أنها تعد ظاهرة إجرامية مستحدثة نظرا لإرتباطها بالتكنولوجيا والإتصالات و أهم التطورات التي نعيها اليوم، وذلك بالإستخدام الغير المشروع للحاسب الآلي كأداة لارتكاب الأفعال الغير المشروعة من طرف محترفين بقيامهم بالعديد من الجرائم التي تتمثل في سرقة المعلومات السرية، سرقة الملفات، تدمير البرامج و إتلافها وغيرها من الجرائم التي تتعلق بالتقنية المعتمدة على المعالجة اللآلية للمعطيات،فسار من الضروري إيجاد آليات لمحاربة مثل هذه جريمة.

لكن وقبل التحدث عن آليات محاربة الجريمة السيبرانية ينبغي أولا الإلمام بماهية هذه الأخيرة، لذلك فإن البحث في موضوع الجريمة السيبرانية يستلزم بالضرورة تحديد مختلفا المفاهيم والمصطلحات الدالة عليها.

ستتولى الدراسة في الفصل الأول بالتعرض إلى الإطار المفاهيمي في (المبحث الأول) بينما سنتعرض للإطار القانوني في (المبحث الثاني).

المبحث الأول: الإطار المفاهيمي للجريمة السيبرانية

إن الجرائم السيبرانية هي أخطر الأوجه السلبية التي مست مختلف مجالات الحياة في عصرنا الحالي، هذه الجرائم التي أصبحت كابوس المعاناة لدول العالم لذلك ازداد انتشارها وشكلها وعددها وكذا تنوعت أساليب ارتكابها ولكي نستطيع إيجاد الحلول للسيطرة على هذه الجرائم لابد من التعرف جيدا على هذه الظاهرة الإجرامية.

ولأجل ذلك قد خصصنا هذا المبحث المقسم إلى مطلبين بحيث خصص المطلب الأول إلى مفهوم الجريمة السيبرانية(مفهوم الجريمة السيبرنية)، وخصص المطلب الثاني إلى صور الجريمة السيبرانية(المطلب الثاني)

المطلب الأول: مفهوم الجريمة السيبرانية

مع تطور التكنولوجيا في وقتنا الحالي قد ظهر نوع جديد من الجرائم ألا وهو الجريمة السيبرانية لذا فقد خصصنا هذا المطلب لمعالجة ما يلي : تعريف الجريمة السيبرانية (الفرع الأول)، خصائص الجريمة السيبرانية(الفرع الثاني)،الطبيعة القانونية للجريمة السيبرانية(الفرع الثالث).

الفرع الأول: تعريف الجريمة السيبرانية

لقد تعددت تعريفات الجريمة السيبرانية وتباينت فيما بينها ومن خلال هذا الفرع سنتطرق إلى وضع مختلف هذه التعريفات كالتالي:

أولا: التعريف اللغوي للجريمة السيبرانية

تعرف الجريمة السيبرانية في اللغة على أنها:

السيبرانية كلمة إنجليزية مشتقة من كلمة (cyber) وتعني مرتبط بالحاسوب أو شبكات الحاسوب وقيل تعني فضاء الأنترنت، وقيل كلمة يونانية مشتقة من كلمة (kybernetes) وتعني الشخص الذي يدير دفة السفينة مجازا للمتحكم[1]، وسيبرانية هي كلمة مشتقة من كلمة (cybetneties) أي علم الضبط[2].

ثانيا:التعريف الإصطلاحي

إن مصطلح الجريمة السيبرانية ينقسم في شقيه إلى مصطلح الجريمة أولا فالجريمة فمصطلح الجريمة في اللغة هو الجرم والتعدي أو الذنب وجمعها إجرام أو جروم وهو الجريمة وفي نطاق القانون الجنائي هي فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدابير إحتيازيا.[3]

أما مصطلح الجريمة السيبرانية هو إحدى المصطلحات الحديثة والمستخدمة عن جرائم الأنترنت الذي تعددت مصطلحاته وذلك لنشأة تطور ظاهرة الإجرام المرتبط والمتصل بتقنية المعلومات، وقد صيغ مصطلح الجريمة السيبرانية لأول مرة من قبل ويليام جيبسون* عام 1982 ومنذ ذلك الحين اتسعت الحدود التي تحدد الجريمة السيبرانية، وخلال نشأتها فضل الأجيال الأولى من العلماء والمنظمات مصطلح جرائم الكومبيوتر بالمعنى الضيق للجريمة السيبرانية على مصطلح الجريمة السيبرانية بالمعنى الأوسع للكلمة، ومع تطور المصطلحات المستخدمة جرى بذل جهود أكاديمية لتعريف

[1] خرشف فاطمة ولزار سميرة، **الإطار المفاهيمي والقانوني لمواجهة الجرائم السيبرانية**، مجلة سوسيولوجيا للجريمة مخبر الجريمة والإنحراف بين الثقافة و التمثلات الإجتماعية، جامعة علي لونيسي البليدة2، د.م، د.ع، د.ت.ص60.

[2] منير البعلبكي، **المورد قاموس إنجليزي–عربي**، دار العلم للملايين، د.ط، بيروت،2022،ص241.

[3] أيمن عبد الله فكري، **الجرائم المعلوماتية دراسة مقارنة بين التشريعات العربية والأجنبية**، الطبعة الأولى، مكتبة القانون والإقتصاد،الرياض،2014، ص82.

* ويليام فورد جيبسون ولد في 17 مارس 1948 هو روائي أمريكي كندي له طابع خيالي تأملي ويدعى (بالرسول الأسود) أدخل ويليام جيبسون مصطلح الفضاء الإلكتروني في قصته القصيرة (الكروم المحترق) ثم أشاع هذا المفهوم في روايته الأولى نيورومانسر التي أصدرت عام 1948.

الجريمة السيبرانية، ولابد لأي نهج عصري في هذا الشأن أن يسلم بأن تعبير الجريمة السيبرانية ليس مصطلح قانوني قائم بذاته بل هو تعبير جامع يشمل مجموعة أفعال مرتكبة ضد بيانات أو نظم حاسوبية أو على استخدام موارد المعلومات لأغراض غير مشروعة.[1]

ولقد تعددت التوجهات التي عرفت الجريمة السيبرانية، فقد عُرفت على أنها: نشاط جنائي يمثل إعتداء على برامج وبيانات الحاسب الآلي، وعرفت أيضا بأنها: كل استخدام في صورة فعل أو إمتناع غير مشروع للتقنية المعلوماتية[2].وتعرف أيضا بأنها: cybercrime is a series of organized crimes that attack both cyberspace and cybersecurity. Cybercrime refers to criminal activity commited using computers and the internet.these include unlawful access compuer access to or through a computer système positioning system functionality allowing location based services to discover and publish information about owners. Hijackers have begun to use geographical locations and geographical tags to identify their victims.[3]

[1] ماينو جيلالي و عروس كوثر، **الجريمة السيبرانية في صورها المستحدثة**، مجلة القانون والتنمية، مخبر القانون والتنمية، جامعة طاهري محمد بشار، المجلد4، العدد1، جويلية 2023، ص53.

[2] المقصودي محمد بن أحمد بن علي، **الجرائم المعلوماتية خصائصها وكيفية مواجهتها قانونيا**، ،د.ط، دار المنظومة المملكة العربية السعودية، 2015،ص22.

[3] sunil.c.pawer,dr.s.mente**, cyber crime,cyber space and effects of cyber crime**, international journal of scientifics research in computer science engineering and information technology, Punyashlok Ahilyadevi Holkar Solapur University Solapur, Maharashtra, India volume7, issue1, .2021, p211

ثالثا: التعريف الفقهي:

عرفت الجريمة السيبرانية بتعريفات فقهية كثيرة نذكر منها تعريف الأستاذ (rosenblatt) بأنها: كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزونة داخل الحاسب أو التي تحول عن طريقه، وعرفها الأستاذ (eslie d.ball) بأنها: فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية[1]. ولكن قد عيبت هذه التعاريف في كونها ضيقت مجال الجريمة السيبرانية بحيث حصرتها بالمعرفة الجيدة للإعلام الآلي رغم أنه هناك حالات ترتكب فيها هذه الجريمة بالمعرفة السطحية فقط ولهذا ظهر إتجاه فقهي يوسع من مفهوم الجريمة السيبرانية ومن بين هذه التعريفات الفقهية الموسعة نجد تعريف الفقيه (كلاوس تايدومان) الذي عرفها على أنها: كافة أشكال السلوك الغير مشروع الذي يرتكب باسخدام الحاسب الآلي، وتعريف كل من الأستاذين (clemens martin et bernadatte.h.shell) على أنها: الجريمة التعلقة بتكنولوجيا الحاسب والأنترنت وعددا أيضا الأفعال التي تعد جرائم سيبرانية كل عمليات الدخول أو النسخ غير المشروع وسرقة وسائل الإتصالات وإزعاج وترهيب فئة معينة من الناس أو المؤسسات بالإضافة إلى الإرهاب السيبراني.[2]

رابعا: التعريف القانوني

عرف المشرع الجزائري الجريمة السيبرانية في المادة الثانية من القانون 04/09 والتي سماها ب" الجرائم المتصلة بتكنولوجيات الإعلام والإتصال" بأنها: جرائم المساس

[1] صدام حسين ياسين العابدي،**جرائم الأنترنت وعقوباتها في الشريعة الإسلامية والقوانين الوضعية**، د.ط، المركز العربي للتوزيع،القاهرة،2018،ص43.

[2] طرشي نورة، **مكافحة الجريمة المعلوماتية**، مذكرة الماجيستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر،2011-2012،ص ص3-4.

بأنظمة المعالجة الآلية للمعطيات* المحددة في قانون العقوبات، وأي جريمة ترتكب يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية.[1]

الملاحظ من خلال قراءة المادة السالفة الذكر هو أن المشرع الجزائري اعتمد في تعريف الجريمة السيبرانية على معيارين هما:

أ) التعريف على أساس معيار موضوع الجريمة: وموضوع الجريمة هنا هو المساس بأنظمة المعالجة الآلية للمعطيات وهو الأساس لتحديد الجريمة السيبرانية، وهي الجرائم المحددة في الفصل السابع مكرر من قانون العقوبات تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات" والتي تحكمها المواد 394 مكرر إلى 394 مكرر7 من هذا القانون.[2]

ب) التعريف على أساس معيار وسيلة ارتكاب الجريمة: لقد أضاف المشرع معيارا آخر لتحديد الجريمة السيبرانية وهو وسيلة ارتكاب الجريمة وهي المنظومة المعلوماتية* فوسيلة ارتكاب الجريمة هي محل اعتبار في تكييف الجريمة.

---

* لم يحدد المشرع الجزائري في قانون العقوبات تعريف أنظمة المعالجة الآلية للمعطيات لما استحدث الجرائم الجرائم الماسة بها بموجب القانون 15/04 المؤرخ في 10 نوفمبر 2004 لهذا فيمكن تعريفها استنادا للفقه الفرنسي بتعريف المعطيات من جهة وهي عرض معلومة في شكل إصطلاحي مخصص لتسهيل معالجتها، وتعريف المعالجة الآلية لهذه المعطيات من جهة أخرى على أنها: مجموعة من العمليات المنجزة عن طريق وسائل آلية تتعلق بجمع المعطيات تسجيلها، تحضيرها ، تعديلها، حفضها، إتلافها ، نشرها وبوجه عام إستغلالها.

[1] المادة2، القانون09-04 المؤرخ في 13شعبان 1430 الموافق ل5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية، العدد 47، المؤرخة في 25 شعبان 1430هـ الموافق ل 15 غشت 2009، ص5.

[2] عميمر عبد القادر، **آليات إثبات الجريمة المعلوماتية في التشريع الجزائري**،دراسة مقارنة، أطروحة دكتوراه في القانون العام، كلية الحقوق، جامعة الجزائر2019،1-2020، ص19.

* المنظومة المعلوماتية حسب تعريف القانون الجزائري هي أي نظام منفصل، أو مجموعة من الأنظمة المتصلة ببعضها البعض يقوم واحد منهما أو أكثر بمعالجة آلية المعطيلات تنفيذا لبرنامج معين.

ومن هنا يمكن القول أن الجريمة السيبرانية حسب المشرع الجزائري تنقسم إلى طائفتين، طائفة التي ترتكب ضد نظام المعالجة الآلية للمعطيات وتستهدف المساس الكلي أو الجزئي لهده المنظومة، وهي الجرائم المنصوص عليها في الفصل السابع مكرر من قانون العقوبات، فيما تتضمن الطائفة الثانية كل الجرائم الأخرى المنصوص عليها في قانون العقوبات أو القوانين الخاصة التي يتم ارتكابها أو يسهل ارتكابها باستخدام منظومة معلوماتية أو أي نظام للإتصالات.[1]

الفرع الثاني: خصائص الجريمة السيبرانية

تختص الجريمة السيبرانية بمجموعة من الخصائص والمميزات نذكرها على النحو التالي:

أولا: الجريمة السيبرانية عابرة للحدود

تتميز الجريمة السيبرانية بأنها عابرة للحدود وذلك مع التقدم التكنولوجي واستخدام الحاسب الآلي في شتى مجالات الحياة المختلفة، فلم تعد هذه الجرائم تقتصر على دولة معينة بل تعدت الحدود وأصبح بالإمكان ارتكاب الجرائم عن طريق الحاسب واختراقه لحواسيب في بلد آخر و إتلاف معطياتها فالتعدي في بلد يكون أثره في بلد آخر و هكذا، ومن الأمثلة على هذه الجرائم العابرة للحدود تمكّن أحد الهواة في أوروبا من حل شفرة أحد مراكز المعلومات في البنتاجون ومن ثم اصبح المجال أمامه مفتوحا للعبث ببيانات هذا المركز.[2]

---

[1] عميمر عبد القادر،المرجع السابق، ص20.

[2] غانم مرضي الشمري، **الجرائم المعلوماتية، ماهيتها، خصائصها، كيفية التصدي لها قانونيا**، ، الطبعة الأولى، الدار العلمية والدولية للنشر والتوزيع، عمان، 2016،ص37.

ثانيا: الجريمة السيبرانية صعبة الإثبات

يعد إثبات الجريمة السيبرانية من الأمور الصعبة، حيث يصعب تتبعها واكتشافها، فهي لا تترك أثرا يتقفى، فهي تعتبر مجرد أرقام، فمعظم الجرائم السيبراينة تم اكتشافها بالصدفة وبعد زمن طويل من ارتكابها، كما أنها تفتقر إلى الدليل المادي التقليدي كالبصمات مثلا، ومن جهة أخرى فإن تعقبها يتطلب خبرة فنية يصعب تواجدها عند المحقق العادي للتعامل معها، زيادة على هذا فإن مرتكب هذه الجريمة يتعمد ممارسة التمويه عند ارتكابها والتضليل والتحايل بغاية عدم التعرف عليه.[1]

ثالثا: الجريمة السيبرانية سريعة التنفيذ والإخفاء

لا شك أن سرعة التنفيذ أهم ما يميز الجريمة السيبرانية، الذي يتم مباشرة من قبل الجاني أو من خلال برامج خاصة بذلك، وهو ما يساعد الجاني على تنفيذ جريمته بسرعة فائقة بعيدا عن مسرح الحادث وبطريقة خفية مستترة لا يلحظها المجني عليه ومما يزيد من سرعة تنفيذ الجريمة التقدم التقني الذي أنتج الكثير من الوسائل والبرامج التي تساعد على سرعة تنفيذ الجريمة السيبرانية.[2]

رابعا: قلة الإبلاغ عنها

يعد هذا العنصر من بين الاسباب التي تقف وراء صعوبة اكتشاف الجريمة السيبراينة وإثباتها، ولعل أن المجني عليهم أي ضحايا هذه الجريمة يلعبون دورا رئيسيا في ذلك من خلال الإحجام عن الإبلاغ عنها في حالة اكتشافها، حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية للإنتهاك أو تُمنى بخسائر فادحة من جراء

[1] رحوني محمد، **خصائص الجريمة الإلكترونية ومجالات استخدامها**، مجلة الحقيقة، جامعة أحمدة دراية–أدرار– د.ج العدد41، د.ت،ص ص442_443.

[2] عبد الله بن حسين آل حجراف القحطاني، **تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية**، رسالة الماجيستير في قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، 2014،ص33.

ذلك عن عدم الكشف حتى بين موظيفها عما تعرضت له وتكتفي بإجراءات إدراية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعتها والثقة في كفاءتها، وبالتالي فإن الإبلاغ في هذه الجرائم يكون قليلا بالنسبة للجرائم الأخرى وهذا راجع إلى ما يتعرض له المجني عليه كطرف في الجريمة من تشهير فيما لو أبلغ عن الجريمة.[1]

خامسا: محل وقوع الجريمة السيبرانية

فالجريمة السيبرانية لا تتم في بيئة تقليدية لكن تتم خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب وشبكة الأنترنت مما تجعل الأمور تزداد تعقيدا لدى السلطات، ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية تنساب لدى النظام المعلوماتي مما يجعل أمر طمس الدليل ومحوه كليا أو جزئيا من قبل الفاعل أمرا في غاية الإمكان، حيث تقع الجريمة السيبرانية في العالم الإفتراضي من خلال بيئة المعالجة الآلية للمعطيات التي تحتضن هذه الجرائم أو تزيد من صعوبة التعامل معها، فمحل وقوع الجريمة ومسرحها يصعب تحديده والتعامل معه ويتطلب وجود المعرفة التقنية لاكتشافه، وهذا ما يؤدي بدوره إلى صعوبة جمع الأدلة وتحديدها نظرا للطبيعة الخاصة لمحل وقوع الجريمة السيبرانية.[2]

[1] قاسحي فيروز، **الجريمة الإلكترونية عبر مواقع التواصل الإجتماعي**، مجلة الرسالة للدراسات والبحوث الإنسانية جامعة الجزائر3، المجلد7، العدد8، فيفري2023 ، ص ص206_207.

[2] عبد الله بن حسين آل حجراف القحطاني، المرجع السابق، ص33.

الفرع الثالث: الطبيعة القانونية للجريمة السيبرانية

هناك ما يميز الجريمة السيبرانية عن غيرها من الجرائم التقليدية باعتبارعا جريمة مستحدثة ما جعلها تكتسب طابعا قانونيا خاصا بها وهذا ما سنراه من خلال فرعنا هذا.

أولا: الطبيعة القانونية الخاصة بالجريمة السيبرانية

تتميز الجريمة السيبرانية في أنها تعدو أن تكون بطريقة أوتوماتيكية حديثة على غرار الجرائم التقليدية، فهذه الأخيرة أي الجرائم السيبرانية تعد إفرازا ونتاجا لتقنية المعلومات فهي ترتبط وتقوم عليها، وهذا ما أكسبها لونا وطابعا قانونيا خاصا يميزها عن غيرها من الجرائم التقليدية، فإذا كانت الجريمة بصفة عامة محل تطبيق القانون الجنائي فإنه وبالنظر إلى الطبيعة المتميزة للجريمة السيبرانية فإنها تتعلق غالبا بما يسمى القانون الجنائي السيبراني، وقد أضفت هذه الحقيقة على هذا النوع من الجرائم طبيعة قانونية خاصة سواءا تعلقت بذاتية هذه الجريمة أو تعلقت بخصوصية المحل الذي يقع عليه الإعتداء في ارتكاب هذه الجرائم.[1]

ثانيا: موقف المشرع الجزائري من الجريمة السيبرانية

لم يجد المشرع الجزائري يدا من تعديل قانون العقوبات لسد ما كان من فراغ قانوني في هذا المجال، وكان ذلك بموجب القانون 15/04 المتضمن قانون العقوبات والذي أقر له القسم السابع مكرر منه تحت عنوان" المساس بأنظمة المعالجة الآلية للمعطيات"، ولقد جاء في عرض أسباب هذا التعديل أن التقدم التكنولوجي وانتشار وسائل الإتصال الحديثة أدى إلى بروز أشكال جديدة للإجرام، وقد قدر المشرع الجزائري في تدخله في أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي فتحول إلى معلومات بعد

[1] سعيداني نعيم، **آليات البحث والتحري في الجريمة المعلوماتية في القانون الجزائري**، مذكرة الماجيستير في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر-باتنة-، 2013/2012،ص30.

معالجتها وتخزينها فقام بحماية هذه المعطيات بأوجه عدة، لذلك فقد آثر المشرع الجزائري استخدامه لمصطلح المساس بنظم المعالجة الآلية للمعطيات وينصرف هذا المصطلح وفقا لدلالة الكلمة إلى المعلومات والنظام الذي يحتوي عليها بما في ذلك شبكات المعلومات، ليخرج بذلك في نطاق التجريم تلك الجرائم التي يكون النظام المعلوماتي وسيلة لارتكابها وحصرها فقط في صور الأفعال التي تشكل أعتداء على النظام المعلوماتي.[1]

المطلب الثاني: صور الجريمة السيبرانية

تتعدد أشكال الجريمة السيبرانية وتختلف من حيث الطبيعة والمصادر والأهداف كالتجسس وسرقة المعلومات، وعلى الرغم من تعدد صور الهجمات الإلكترونية، غير أنه من الممكن تقسيمها إلى مجموعات رئيسية كالتالي:

الفرع الأول: التزوير المعلوماتي(السيبراني)

لا شك أن تطور تكنولوجيا الحاسبات الآلية وخاصة مع ظهور طابعات الليزر و الماسحات المتقدمة قد ساهمت على نحو كبير في تزوير المعلومات التي تحتوي على أنظمة الحاسبات الآلية، ومع زيادة الإعتماد على هذه الأخيرة في تخزين ومعالجة الكثير من المعلومات التي لها أهميتها كالبيانات المتعلقة بالميلاد والوفاة وجوازات السفر ورخص القيادة وغير ذلك من البيانات التي يمكن لها التأثير في المعاملات القانونية بوجه عام كان لزاما حماية هذه المعلومات من التلاعب بها. ويتخذ التزوير المعلوماتي صورتين تتمثل الأولى في تلاعب في المعلومات داخل نظام الحاسب الآلي وذلك لتغيير الحقيقة

[1] حشمان عمار، **الجريمة المعلوماتية في التشريع الجزائري**، مذكرة ماستر، كلية العلوم الإقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرباح–ورقلة–2018_2019، ص17.

في هذه المعلومات وقد يتخذ هذا التلاعب صورة تعديل في المعلومات أو محو جزء أو عدة أجزاء منها أو إعاقة أداء وظيفتها.

أما الصورة الثانية فتتمثل في إدخال معلومات غير صحيحة لخلق مستند غير صحيح، ويتم هذا الإدخال بنية إستعمال المعلومات فيما زورت من أجله، وفي الحالتية يتم الإستعانة بتكنولوجيا الحاسب الآلي لإتمام التزوير.[1]

الفرع الثاني: التجسس السيبراني (cyber espionage)

يعد التجسس بصفة عامة من المجالات الخصبة للجريمة السيبرانية، فهو يعد من الجرائم التي يسهل من ارتكابها على الحاسب الآلي، ويتسع التجسس في مجال السيبرانية ليشمل أنماطا متعددة من المعلومات قد تتعلق بأسرار الدولة في العديد من المجالات، أو المعلومات الصناعية.[2] حيث يتم الحصول على معلومات سرية غير مشروعة بهدف الحصول على أفضلية إستراتيجية أو إقتصادية أو عسكرية، فالتجسس السيبراني هو ذلك التجسس الذي يعتمد على استخدام تقنيات التكنولوجيا من أجل الحصول على المعلومات ويختلف التجسس من حيث النوع فهناك التجسس عن طريق الأفراد وهناك التجسس عن طريق الشبكات السلكية أو من خلال الأقمار الصناعية.[3]

---

[1] نائلة عادل محمد فريد قورة، **جرائم الحاسب الآلي الإقتصادية، دراسة نظرية تطبيقية**، ، الطبعة الأولى، منشورات الحلبي الحقوقية، القاهرة، 2015، ص270.

[2] المرجع نفسه، ص 273.

[3] قطاف سليمان و بوقرين عبد الحليم، **مواجهة الجرائم السيبرانية في ضوء الإتفاقيات الدولية**، مجلة البحوث القانونية والإقتصادية، مخبر البحث في الحقوق والعلوم السياسية جامعة عمار ثليجي–الأغواط–،المجلد5، العدد2 2022،ص72.

الفرع الثالث: سرقة المعلومات

إن الحصول الغير المشروع على المعلومات أو بتعبير آخر سرقة المعلومات له خصوصية تميزه عن جريمة السرقة التقليدية، فالمعلومات يجب أن ينظر إليها كقيمة في ذاتها يمكن أن تكون محلا للسرقة آخذين في الإعتبار طبيعتها الخاصة التي تتمثل في عدم قابليتها للإنتقال من حيازة إلى أخرى، إذ يمكن تقدير تجريم الحصول الغير مشروع على المعلومات المبرمجة آليا على أن انتقال حيازة المعلومة ليس بشرط لازم، حيث يمكن أن تتحقق هذه الجريمة حتى لو لم تم الحصول غير المشروع على المعلومات عن طريق نسخها أو عن طريق طباعتها، وقد يكون الحصول الغير المشروع على المعلومات المبرمجة آليا بغرض ارتكاب جريمة أخرى كالإبتزاز أو إفشاء المعلومات إلى منافسين في تجارة أو صناعة، وقد يكون الحصول على المعلومات مقصودا في ذاته، ولا شك أن تجريم سلوك الفاعل في الحالة الأخيرة مبعثه حماية المعلومات المبرمجة آليا وهي حماية تقتضيها أهمية هذه المعلومات ومنه كان لزاما لإقامة نوع من التوازن بين حماية هذه المعلومات و الحق في المعرفة وحرية تدفق المعلومات، كما أن مجرد الإطلاع على المعلومات داخل نظام الحاسب الآلي دون أن يقترن ذلك بنية غير مشروعة لا يتحقق به الحصول الغير المشروع عليها، وهو ما يميز جريمة سرقة المعلومات عن جريمة الدخول الغير مصرح به لنظام الحاسب الآلي، إذ تقوم الأخيرة بمجرد الحصول على المعلومات التي يقوم عليها نظام الحاسب الآلي.[1]

[1] نائلة عادل محمد فريد قورة، المرجع السابق، ص 269.

الفرع الرابع: الإرهاب السيبراني (cyber terrorism)

حيث يمثل الفضاء السيبراني عنصر جذب للتنظيمات الإرهابية على تعدد أنواعها واختلاف إيديولوجيتها، نظرا لما يتيحه من وسيلة إعلام دولية وسلاح في ذات الوقت، إذ يمكن استخدامه من الأطراف المتعددة ويعد تنظيم "داعش" الإرهابي أكثر التنظيمات التي حققت تهديدا على سلامة شبكة الأنترنت العالمية باستخدامها في الدعاية والتمويل والتجنيد وجمع المعلومات وتنسيق الهجمات الإرهابية، ووسيلة لحشد المتعاطفين معه وهم المنتشرون في الكثير من دول العالم، ويستخدم هذا التنظيم وسائل التكنولوجيا بغرض التجنيد ونشر فكره في أوساط الشباب، وكان بإمكان حملاته في بعض الأحيان أن تكون كافية لإثارة أعمال العنف والخوف والرعب لدى الدول المجتمعات.[1]

المبحث الثاني: الإطار القانوني للجريمة السيبرانية

سبق وأن أشرنا في معرض حديثنا عن الإطار المفاهيمي للجريمة السيبرانية بالتعرض إلى مفومها وبالتالي إلى مختلف التعريفات الخاصة بها، وكذا إلى خصائص هذه الجريمة، إضافة إلى الطبيعة القانونية للجريمة السيبرانية، أما في مبحثنا هذا فسنشير إلى الإطار القانوني للجريمة السيبرانية من خلال التحدث عن أركان الجريمة السيبرانية (كمطلب أول) ثم التحدث عن مفتعل هذه الجريمة وهو المجرم السيبراني(المطلب الثاني).

المطلب الأول: أركان الجريمة السيبرانية

إن الجريمة السيبرانية كغيرها من الجرائم تتطلب لقيامها تحقق أركان الجريمة ومن خلال هذا المطلب سنرى كيف تحقق أركان الجريمة الثلاث في مثل هذه الجرائم كالتالي:

[1] غريب حكيم، **الإرهاب السيبراني والأمن الدولي: التهديدات العالمية الجديد وأساليب المواجهة**، المجلة الجزائرية للدراسات السياسية، المدرسة الوطنية العليا للعلوم السياسية، المجلد5، العدد2،ص ص103-104.

الفرع الأول: الركن الشرعي

أدرك المشرع الجزائري خطورة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فجرَم الشروع في ارتكاب هذه الجرائم مع أنها جنح، حيث أن الأصل في التجريم بالنسبة للشروع في الجنح لا يكون إلا بنص قانوني، وقد نصت المادة 30 من قانون العقوبات الجزائري على أن جريمة الشروع بشكل عام تحت عنوان المحاولة حيث نصت على " كل المحاولات لارتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال ليس فيها تؤدي مباشرة إلى ارتكابها تعتبر كالجناية نفسها إذا لم توقف أو لم تخب آثارها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها حتى ولو لم يكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها".[1] كما نصت المادة 394 مكرر7 على جريمة الشروع في مجال المعلوماتية وذلك بأن " يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها"، وتجريمة الشروع وفقا لهذا النص يهدف إلى توسيع نطاق العقوبة للجرائم السيبرانية، لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية، حتى أنه قد ساوى بين الشروع والجريمة التامة من حيث العقوبة.[2]

الفرع الثاني: الركن المادي

إن النشاط أو السلوك المادي في الجريمة السيبرانية يتطلب وجود بيئة رقمية وجهاز كمبيوتر واتصال بشبكة الأنترنت، ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته، فمثلا يقوم مفتعل الجريمة بتجهيز الكمبيوتر لكي يتحقق له حدوث الجريمة فيقوم بتحميل الحاسب ببرامج اختراق، أو أن يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج

[1] المادة 30، الأمر رقم 66-156 المؤرخ في 18 صفر 1386 الموافق ل8 يونيو 1966 المتضمن قانون العقوبات المعدل والمتمم، الجريدة الرسمية، العدد49، المؤرخة في 11 يونيو 1966، ص702.

[2] غلاب فايز محمد راجح ، **الجرائم المعلوماتية في القانون الجزائري والقانون اليمني**، أطروحة الدكتوراه في الحقوق كلية الحقوق، جامعة الجزائر1، 2011-2012 ، ص150.

إلى تهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة وتحميلها على الجهاز المضيف hosting server، كما يستطيع أن يقوم بجريمة اعداد برامج فيروسات تمهيدا لبثها، إن ارتكاب الجريمة عبر الأنترنت يحتاج بالضرورة إلى منطق تقني وبدونه لا يمكن للشخص حتى الإتصال بالأنترنت سواء كان الشخص يقصد ارتكاب جريمة أم لمجرد التصفح، وهذا السلوك المادي أي المنطق التقني يجعل هذه الجريمة ذات طابع موحد بالضرورة فهي تبَاشر من حيث النشاط المادي فيها والنشاط التقني هو أمرا لازما وإلا فقدت الجريمة مقوماتها.[1]

الفرع الثالث: الركن المعنوي

يتحقق الركن المعنوي في الشروع بتوافر القصد الجنائي الذي يتطلب توافر عنصري العلم والإرادة ويشترط لتحقق عنصر العلم أن يكون الجاني عالما بكل واقعة ذات أهمية قانونية في تكوين الجريمة، وفي مجال الجرائم السيبرانية ينبغي أن يكون الجاني عالما بكل واقعة ذات أهمية قانونية تدخل في تكوين الجريمة سواءا تمثلت تلك الجريمة بجريمة الدخول والبقاء الغير المشروع إلى نظام المعالجة الآلية للمعطيات أو جريمة التلاعب بمعطيات الحاسوب أو جريمة التعامل بالمعطيات غير الشرعية الناتجة التي يمكن أن ترتكب بها إحدى الجرائم السيبرانية المنصوص عليها في قانون العقوبات الجزائري، ففي جريمة الدخول الغير مشروع على سبيل المثال يجب أن يعلم الجاني أنه يقوم بمحاولة الدخول الغير المشروع إلى الحاسب الآلي غير المصرح له بالدخول إلى نظامه وهكذا بالنسبة إلى بقية الجرائم. وإذا ما توفر عنصر العلم على النحو السابق فيتعين توافر العنصر الثاني من عناصر القصد الجنائي وهو الإرادة التي بموجبها يتطلب أن تتجه تلك

[1] خالد محمود إبراهيم، **الجرائم المعلوماتية**، ، الطبعة الثانية، دار الفكر الجامعي،الإسكندرية،2019، ص93.

الإرادة لتحقيق نتيجة وهي الدخول، إلا أن النتيجة لا تتحق لعوامل خارجة عن إرادة الفاعل.[1]

المطلب الثاني: المجرم السيبراني

يسمى القائم بالجريمة السيبرانية بالمجرم السيبراني وفي هذه الجريمة لا نكون بصدد التحدث عن مجرم عادي بل أمام مجرم ذي مهارات تقنية وذي علم بالتكتيك في نظام الحسابات اللآلية، وشخصية هذا الأخير تجعل منه شخصا يتسم بسمات خاصة تضاف إلى سمات المجرم العادي، وكذلك بالنسبة لدوافع ارتكاب هذه الجريمة فإنها أيضا تختلف عن دوافع ارتكاب الجرائم الأخرى وهذا ما سنكتشفه من خلال مطلبنا هذا بحيث سيكون تعريف المجرم السيبراني(الفرع الأول)، سمات المجرم السيبراني(الفرع الثاني)،فئات المجرم السيبراني(الفرع الثالث)، ودوافع ارتكاب الجريمة السيبرانية(الفرع الثالث).

الفرع الأول: تعريف المجرم السيبراني

هو كل شخص سواءا كان طفل، رجل، أنثى، يأتي أفعالا إرادية تشكل سلوكا إيجابيا أو سلبيا باستخدام تقنية المعلوماتية لإحداث نموذج إجرامي بالإعتداء على حق أو مصلحة، حيث أن سماته تشبه في كثير من الأحيان سمات مجرمي الياقات البيضاء، إذ أن كل من هؤلاء المجرمين قد يكونوا من ذوي المناصب الرفيعة والمستوى العالي ومن ذوي التخصصات الكفاءات العالية.[2]

[1] غلاب فايز محمد راجح ، المرجع السابق، ص153.

[2] بن عقون حمزة، **السلوك الإجرمي للمجرم المعلوماتي**، شهادة الماجيستير في العلوم القانونية، علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر – باتنة–2011–2012، ص28.

الفرع الثاني: سمات المجرم السيبراني

لعل ما يميز المجرم السيبراني أنه يعود دائما للجريمة فهو قد لا يحقق الجريمة بهدف الإيذاء وإنما نتيجة شعوره بقدرته ومهارته، وهذا ما يجعله ينفرد بسمات تميزه عن باقي الجرمين وهي:

أولا: المهارة

إن المهارة هي أبرز سمة للمجرم السيبراني، إذ يتطلب لتنفيذ الجريمة السيبرانية قدرا من المهارة يتمتع بها الجاني، وقد يكتسبها من الدراسة المتخصصة في المجال السيبراني أو في مجال التكنولوجيا، أو عن طريق التفاعل الإجتماعي مع الآخرين، وذلك لا يعني بالضرورة أن يكون المجرم السيبراني على قدر كبير من العلم في هذا المجال وأن تكون له خبرة كبيرة فيه، لثبوت بعض مجرمي السيبرانية رغم عدم تلقيهم المهارة الكافية لارتكاب الجريمة السيبرانية عن طريق التعليم أو الخبرة المكتسبة في هذا المجال.[1]

ثانيا: المعرفة

و تعني التعرف على كل الظروف والملابسات التي تحيط بالجريمة المزعم ارتكابها وامكانيات نجاحها، واحتمال فشلها، والفاعل عادة ما يُمهد لارتكاب الجريمة بالتعرف على كل الظروف المحيطة بها، حتى يتجنب الأمور الغير المتوقعة التي من شأنها ضبط فعله واكتشاف أمره، والمجرم السيبراني يتميز بالمعرفة بمفهومها السابق ليجمع تصورا كاملا لجريمته، ويحاول الإفلات من عواقبها، وذلك يرجع إلى أن المسرح الذي ترتكب فيه

[1] محمد علي سكيكر، **الجريمة المعلوماتية وكيفية التصدي لها**، ، د.ط، دار الجمهورية للصحافة، مصر، 2010 ص51.

الجريمة هو نظام الحاسب الآلي فيحاول قبل تنفيذها تطبيقها على أنظمة مشابهة، حتى يتعرف على كيفية الخروج منها.[1]

ثالثا: السلطة

والسلطة هنا يقصد بها الحقوق التي يتمتع بها المجرم السيبراني والتي تمكنه من ارتكاب جريمته، وهذه السلطة إما تكون مباشرة كالشفرة الخاصة بالدخول إلى النظام المعلوماتي التي تعطي للفاعل مزايا متعددة مثل فتح الملفات أو محو أو تعديل محتوياتها أو بجرد قرائتها أو كتابتها، وقد تتمثل هذه السلطة في حق استعمال الحاسب الآلي نفسه أو الدخول إلى مكان تواجده كما هو الحال في الشبكات الداخلية لبعض الإدارات وقد تكون هذه السلطة غير مباشرة كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر.[2]

رابعا: الوسيلة

إن وسيلة تنفيذ الجريمة السيبراينة تتميز في أغلب الحالات بطابعها التقني، مما يجعل أدلة الإدانة فيها غير كافية، ويرجع ذلك إلى عدم وجود أي أثر كتابي ملموس، إذ يتم نقل المعلومات إلكترونيا، بالإضافة إلى إمكانية الجاني من إخفاء دليل الإدانة في أقل من ثانية.[3]

الفرع الثالث: فئات المجرم السيبراني

وهي بدورها تُسفر إلى عدة تقسيمات أي طوائف مختلفة وهي كالتالي:

---

[1] محمد علي سكيكر، نفس المرجع.

[2] سوير سفيان، **جرائم المعلوماتية**، شهادة الماجيستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعولم السياسية جامعة بوبكر بلقايد –تلمسان– 2010–2011، ص24.

[3] غريبي بشرى، **خصوصية المجرم المعلوماتي ودوافعه**، مجلة نوميروس الأكاديمية، جامعة أبو بكر بلقايد–تلمسان– المجلد2، العدد2، 2021، ص106.

أولا: فئة القراصنة hakers

وهم فئة المجرمين الأقل خطورة والذين تتوافر لديهم خبرة معتبرة في مجال الحاسب الآلي ووظائفه ومكوناته، ونظم المعلوماتية، ومعرفة البرامج التي يجري العمل بها كالبرامج المحاسبية، وبما أن هؤلاء يمارسون مواهبهم لغرض الولوج الى نظم المعلومات بدافع الفضول أو اللهو، فهم لا يدركون ولا يقدرون النتائج المحتملة التي يمكن أن تؤدي إليها أفعالهم غير المشروعة، لذلك فإن هذه الفئة تعد أقل خطورة، ولكن مع ذلك يلاحظ أن ازدياد الأعداد المستخدمة لتكنولوجيا الاعلام والاتصال، وما يتبعه من ازدياد نسبة الجرائم في هذا المجال، فلا يستبعد معه احتمال إنزلاق هذه الفئة من مجرد هواة للأفعال غير المشروعة إلى المحترفين.[1]

ثانيا: فئة القراصنة الخبيثون crakers

تعد هذه الطائفة أخطر شكل من أشكال الهاكرز، حيث تمتاز بضررها الكبير والواسع، وينقسمون إلى قسمين منهم المحترفون ذوي الإنجازات العالية في الرقمنة والحاسوب، أو يعملون محللي نظم أو مبرمجين وعلى دراية ببرامج التشغيل والثغرات الموجودة به، ومنهم الهواة اللذين يحملون درجة علمية تساعدهم في تعلم البرمجة ونظم التشغيل و استخدامها وتطويرها حسب حاجاتهم الخاصة، وغالبا ما يتمثل موضوع عمل هذه الفئة في استهداف الكيانات الأكبر، كالهجوم على البنوك العالمية والمؤسسات الإقتصادية إما بدوافع ربحية أو دوافع قومية، وعلى سبيل المثال نذكر الهاكر الجزائري

[1] يعيش تمام شوقي، **الجريمة المعلوماتية، دراسة تأصيلية مقارنة**، ، الطبعة الأولى، مطبعة الرمال، الجزائر، 2014 ص22.

حمزة بن دلاج الذي يعد من أخطر الهاكر في العالم، حيث قام بعدة أعمال استهدفت بنوكا عالمية وتسبب في خسائر كبيرة لها.[1]

ثالثا: أصحاب المشاكل الشخصية Petsomal probleme solvers

وهم أصحاب حل المشاكل الشخصية، وهم الأكثر شيوعا بين مجرمي السيبرانية ويترتب على ارتكابها للجرائم السيبرانية خسائر قد تكون كبيرة وتلحق بالمجنى عليهم وارتكابهم لهذه الجرائم غرضه ليس ربحا ماديا بقدر ماهو الرغبة لإيجاد حلول لمشكلاتهم الشخصية التي تواجههم، وهؤلاء المجرمون يتمتعون بخبرة عالية في مجال الحاسبات اللآلية بحكم عملهم في هذا المجال، وغالبا ما تكون جرائمهم ضد المؤسسة المالية التي ينتمون إليها.[2]

رابعا: جماعات إرهابية متطوعة exterm adrocates

وهم يمثلون الجماعات الإرهابية أو المتطرفة، ويعملون في شكل جماعة تعمل تحت معتقدات، وأفكار سياسية أو اجتماعية أو دينية بغرض فرض معتقاداتهم باللجوء إلى النشاط الإجرامي، واستخدامهم في ذلك العنف ضد الأشخاص و الممتلكات، وهذه الجماعات تتمتع بدرجة عالية من التنظيم، ومن أهدافها اختراق أنظمة الحاسبات اللآلية التي أخذت المؤسسات المختلفة داخل الدول في الإعتماد عليها في تسيير نشاطها.[3]

خامسا: الأطفال والمراهقين البالغين من العمر بين مجموعة 6 ألى 18 children and adolescents between the age group of 6-18 years

---

[1] سلامي لخضر، **الجريمة الإلكترونية عبر مواقع التواصل الإجتماعي**، أطروحة دكتوراه، كلية العلوم الإجتماعية جامعة وهران 2، 2002-2023،ص66.

[2] محمد علي سكيكر، المرجع السابق، ص54.

[3] المرجع نفسه، ص55.

تمارس الجريمة السيبرانية بواسطة هذه الفئة نتيجة الإرتباط الوتيري بوسائل المعلوماتية والتواصل الإجتماعي وقد فُسرت أسباب الممارسة لهذه الفئة في the simple reason for this type of dilinquent behaivour pattern in children is seen mostly due the inquisitivenss to know and explor their thing, other cognate reason may be to prove thir selves to be outstanding omongst other children in their group,and the reasons may be psychological even.[1]

الفرع الرابع: دوافع ارتكاب الجريمة السيبرانية

تقوم الجريمة بقيام عناصرها وتحقق أركانها أيا كان الباعث أو الدافع* لارتكابها والبواعث التي تؤدي بالمجرم السيبراني لارتكاب الجريمة السيبرانية قد تعددت وهي:

أولا:الرغبة في التعلم

وهي الرغبة الشديدة في كل ما يتعلق بأنظمة الحاسوب والشبكات الإلكترونية ولهذا يشير الأستاذ (ليفي) في كتابه قراصنة الأنظمة إلى أخلاقيات هؤلاء القراصنة والتي ترتكز على مبدأين أساسين:

1) إن الدخول إلى أنظمة الحاسوب يمكن أن يعلمك كيف يسير العالم

2) إن عملية جمع المعلوكات يجب أن تكون غير خاضعة للقيود

فهناك من يرتكب هذه الجرائم بغية الحصول على المزيد من المعلومات وسبر أغوار هذه التقنية المتسارعة النمو والتطور، وهذه الجماعات يقومون بالبحث واكتشاف الأنظمة والعمل من خلال تعليم بعضهم، ويفضل هؤلاء القراصنة البقاء مجهولين أكبر وقت ممكن حتى يتمكنوا من الإستمرار في التواجد داخل الأنظمة، ويكرس البعض منهم كل وقته في

[1] mohamed chawki, achraf darwish, ,**cybercrime digital forensics and jurisdiction**,internatinal association of cybercrime,france, 593, 2015, p17

* الدافع هوالمحرك للإرادة الذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والإنتقام

كيفية اختراق المواقع الممنوعة والتقنيات الأمنية لأنظمة الحاسوب، بشكل عام يرى هؤلاء المجرمون أن جميع المعلومات مفيدة يجب أن تتاح حرية نسخها والأطلاع عليها إلا أنهم يقررون بضرورة إغلاق بعض نظم المعلومات وعدم السماح بالوصول إلى بعضها خاصة بعض المعلومات السرية التي تخص الأفراد.[1]

ثانيا: الرغبة في تحقيق الربح وكسب المال

إن الرغبة في تحقيق مكاسب مادية قد تكون البواعث التي تؤدي بمرتكبي الجريمة السيبرانية القيام بها، ومن أجل تحقيق مكاسبهم المالية يلجؤون إلى إقتراف الجريمة السيبرانية إما عن طريق المساومة أو البرامج أو المعلومات المتحصل عليها بطريق الإختلاس من جهاز الحاسوب أو عن طريق استعمال بطاقة سحب آلي مزورة أو منتهية الصلاحية وغير ذلك الكثير، ولقد اشارت مجلة (securite informatique)* ألى أن 43 % من حالات الغش المعلن عنها قد تمت من خلال اختلاس الأموال و 23% من أجل سرقة المعلومات و19% أفعال إتلاف و 15% الإستعمال الغير المشروع للحاسوب من أجل تحقيق أغراض شخصية.ويمكن أن نوضح مدى تحقيق الأرباح المادية نتيجة هذا الإجرام من خلال ما يرويه أحد هؤلاء المجرمين في سجن كاليفورنيا بقوله: لقد سرقت أكثر من نصف مليون دولار بفضل أجهزة الحاسوب جهاز الضرائب في الولايات المتحدة الأمريكية وبإمكاني أن أكرر ذلك في إي وقت لقد كان شيئا سهلا أنا أعرف أسلوب جهاز الحاسوب للضرائب وقد وجدت ثغرات كثيرة في نظامه يمكن أن تمدني بمبالغ طائلة لو لم يكن سوء الحظ قد صادفني.[2]

---

[1] نهلا عبد القادر مومني، **الجرائم المعلوماتية**، ، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، 2010، ص89.

* مجلة securite informatique أي بالعربية مجلة أمن المعلومات هي مجلة متخصصة في الأمن المعلوماتي أصدرت من طرف شهاب نجار يناير 2018.

[2] نهلا عبد القادر مومني، المرجع السابق، ص90.

ثالثا: المتعة والتحدي وقهر النظام المعلوماتي والرغبة في تحقيق الذات

إن اختراق الأنظمة الإلكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة كبيرة بالنسبة لمرتكبها وتسلية تغطي أوقات فراغه، على صعيد آخر قد يكون الدافع وراء ارتكاب الجرائم السيبرانية هو قهر الأنظمة الإلكترونية والتغلب عليها، إذ يميل مرتكبو هذه الجرائم إلى أظهار تفوقهم على وسائل التكنولوجيا الحديثة، فمجرمو السيبرانية يمتلكهم الشعور بالبحث عن القوة ويؤدي ارتكابهم للجرائم السيبرانية إلى تعويضهم عن شعور الدونية ففي بعض الأحيان وُجد أنه بمجرد إظهار إحساس جنون العظمة هو الدافع لارتكاب فعل الغش السيبراني.[1]

رابعا: دافع العقيدة

يتعبر من أهم دوافع ارتكاب الجرائم السيبراينة، وهي ذات منطلق إيديولوجي عقائدي غالبا ما أحدث ضررا كبيرا عبر المنظومة المعلوماتية، سببه الرئيسي العداوة التي تكنها طائفة ما لطائفة أخرى أو جماعة ما لجماعة أخرى، وقد يتعدى ذلك ليشمل كيانات أكبر كالدول والأقاليم، حيث أن كثيرا من الأشخاص يبررون محاولات اختراقهم لأجهزة الغير بتأويلات غريبة وأفكار سيئة، فهناك من يبرر اختراق جهاز ما أو موقع بحجة أنه على غير المذهب أو الطائفة، أو بحجة تكفيره والإطلاع على أسراره لفضحه وتشهيره، وعادة ما يهدف أصحاب هذه الدوافع للإنتقام أكثر من أي هدف آخر.[2]

[1] المرجع نفسه، ص92.

[2] سلامي لخضر، المرجع السابق، ص73.

خلاصة الفصل الأول:

إن ما يمكن الوصول إليه من خلال دراستنا للفصل الأول أن الجريمة السيبرانية قد تعددت واختلفت مفاهيمها وتعاريفها، وقد عرفها شارعنا الجزائري في المادة 2 من القانون 04/09 معتمدا في تعريفها على أساس معيارين

– المعيار الأول هو موضوع ارتكاب الجريمة وهو المساس بأنظمة المعالجة الآلية للمعطيات.

– المعيار الثاني فهو وسيلة ارتكاب الجريمة وهي المنظومة المعلوماتية وهذه الأخيرة هي محل اعتبار في تكييف الجريمة السيبرانية أما مصطلح الجريمة السيبرانية فهو مصطلح مستحدث فقد كان يطلق عليها تقليديا بمصطلح جرائم الكمبيوتر مثلا وبالنسبة للمشرع الجزائري فقد أطلق عليها مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، ولعل أن أهم ما يميز هذه الجريمة عن باقي الجرائم التقليدية الأخرى أنها تتم خارج الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب، كذلك فإن لتحقق هذه الجريمة ينبغي توفر أركانها (الركن الشرعي، الركن المادي، الركن المعنوي)، أما فيما يخص القائم بهذه الجريمة فيسمى بالمجرم السيبراني ولا يكون مجرما عاديا فهو مجرم ذي مهارات تقنية في نظام الحسابات الآلية وشخصيته تجعله متميزا عن الجرم العادي فهو يتميز بالمهارة والسلطة والمعرفة، وتختلف فئاته من فئة لأخرى، ولعل أن أكبر ما يدفعه للقيام بجريمته هذه كسب المال وحب التحدي وإظهار الذات.

الفصل الثاني:

آليات التصدي للجريمة السيبرانية في التشريع الجزائري

الفصل الثاني: آليات التصدي للجريمة السيبرانية في التشريع الجزائري

إن التطور السريع في التكنولوجيات و تقنيات المعلومات أدى إلى وجود ثغرات في النصوص القانونية المنظمة للجرائم السيبرانية الأمر الذي قد يجعل من القواعد القانونية والإجراءات التقليدية مقتصرة في مكافحة هذا النوع من الإجرام، وهذا ما دفع بالمشرع الجزائري بضرورة استحداث قوانين وآليات جديدة لمكافحة الجريمة السيبرانية.

إستنادا إلى ما سبق وبعد الإلمام بماهية الجريمة السيبرانية من خلال استعراض مختلف تعاريفها وخصائصها وصورها وكذا الطبيعة القانونية الخاصة التي تنفرد بها فضلا عن تحديد أركانها وصفة القائم بها، سنستعرض في هذا الفصل كيفيات التصدي لها، وذلك في مبحثين، المبحث الأول بعنوان الآليات القانونية لمكافحة الجريمة السيبرانية في التشريع الجزائري، والمبحث الثاني بعنوان الآليات الإجرائية لمكافحة الجريمة السيبرانية في التشريع الجزائري.

المبحث الأول: الآليات القانونية لمكافحة الجريمة السيبرانية في التشريع الجزائري

من أجل مواجهة الجريمة السيبرانية قام المشرع الجزائري بسن العديد من القوانين التي سنتعرف عليها من خلال هذا المبحث، بحيث سنتطرق إلى مكافحة الجريمة السيبراينة في القوانين العامة(المطلب الأول)، ثم إلى مكافحة الجريمة السيبراينة في القوانين الخاصة(المطلب الثاني).

المطلب الأول: مكافحة الجريمة السيبرانية في القوانين العامة

لقد وضع المشرع الجزائري قوانين عامة من أجل محاربة الجرائم السيبرانية سنتعرف عليها من خلال هذا المطلب كالتالي:

الفرع الأول: مكافحة الجريمة السيبرانية بموجب الدستور

لقد كفل دستور الجزائر لسنة 1996 وكذا التعديل الطارئ عليه بموجب القانون المعدل له سنة 2016 حماية الحقوق الأساسية والحريات الفردية، وعلى أن تضمن الدولة عدم انتهاك حرمة الإنسان، وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات وقانون الإجراءات الجزائية وقوانين أخرى والتي تحضر كل مساس بهذه الحقوق، ومن أهم المبادئ الدستورية العامة المادة 38.[1]

[1] بوضياف أسمهان، **الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر**، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، د.م، العدد11، سبتمبر 2018، ص361.

"الحريات الأساسية وحقوق الإنسان والمواطن مضمونة"[1].

كما جاء التعديل 2020 بنصوص قانونية اعتبرها ضمانات للمتقاضي لحماية حقوقه الدستورية ولتجريم أي فعل أو سلوك من شأنه المساس بها نذكر منها على سبيل المثال المادة 55 تنص على أنه: "يتمتع كل مواطن بالحق في الوصول إلى المعلومات والوثائق والإحصائيات، والحصول عليها وتداولها، لا يمكن أن تمس ممارسة هذا الحق بالحياق الخاصة للغير وبحقوقهم، وبالمصالح المشروعة للمؤسسات، وبمقتضيات الأمن الوطني".[2] كما تنص المادة 178 على أنه:" كل أجهزة الدولة المختصة مطالبة في كل وقت وفي كل مكان، وفي جميع الظروف، بالسهر على تنفيذ أحكام القضاء يعاقب القانون كل من يمس باستقلالية القاضي، أو يعرقل حسن سير العدالة وتنفيذ قرارتها.[3]"

الفرع الثاني: القانون الدولي العام

لقد ظهر اهتمام الدولة الجزائرية وانشغالها بالجريمة السيبرانية من خلال المصادقة على الاتفاقيات الدولية الجماعية بما فيهم الاتفاقيات الدولية التي تتجلى في نص المادة 171 التي ألزمت القاضي في ممارسة وظيفته بتطبيق المعاهدات المصادق عليها وقوانين الجمهورية وكذا قرارت المحكمة الدستورية، وحسب نشاط وازرة العدل فيما يخص التعاون متعدد الأطراف: صادقت الجازئر على المستوى الجهوي:على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بموجب المرسوم الرئاسي رقم 252 المؤرخ في 13 ذي القعدة 1435 الموافق ل 8سبتمبر2014يتضمن التصديق على الاتفاقية العربية لمكافحة

[1] المادة 38، القانون رقم 16-01 المؤرخ في 26 جمادى الأولى 1437 الموافق ل6 مارس 2016 يتضمن التعديل الدستوري، الجريدة الرسمية، العدد14،المؤرخة في 27 جمادى الأولى 1437 الموافق ل7 مارس 2016، ص10.

[2] المادة 55، التعديل الدستوري 2020، المؤرخ في 15 جمادى الأولى 1442 الموافق ل30 ديسمبر 2020 يتعلق بإصدار التعديل الدستوري، الجريدة الرسمية، العدد 82، المؤرخة في 15 جمادى الأولى 1442 الموافق ل 30 ديسمبر 2020، ص15.

[3] المادة 178، دستور الجزائر 2020، المصدر نفسه.

جرائم تقنية المعلومات المحررة بالقاهرة 2010 وتحتوي على 43 مادة جاء في مضمونها: تهدف هذه الإتفاقية إلى تعزيز التعاون وتدعيمه في مجال مكافحة جرائم تقنية المعلومات لدرء اخطار هذه الجرائم، ونجد في الفصل الثاني تفصيلا للأفعال التي تعد مجرمة، وفي الفصل الثالث تعرضت لنطاق تطبيق الأحكام الإجرائية وفي الفصل الرابع تعرضت للتعاون القانوني والقضائي وفي الفصل الخامس الى الأحكام الجزائية.[1]

الفرع الثالث: قانون العقوبات وقانون الإجراءات الجزائية

أولا: قانون العقوبات

تدارك المشرع الجزائري خلال السنوات الأخيرة ولو نسبيا الفراغ القانوني في مجال الإجرام السيبراني بموجب القانون 04-15 المتضمن تعديل قانون العقوبات الذي بموجبه جرم المشرع بعض الأفعال المتصلة بالمعالجة الآلية للمعطيات وهي: -جريمة التوصل أو الدخول غير المصرح به: حيث تقوم بمجرد الدخول الغير المرخص به وعن طريق الغش إلى المنظومة المعلوماتية وهذا ما أشارت إلية المادة 394 مكرر من قانون العقوبات على أنه: " يعاقب بالحبس والغرامة كل من يحاول أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك وتضاعف العقوبة إذا ترتب على ذلك حدف أو تغيير لمعطيات المنظومة أو ترتب عن الأفعال المذكورة تخريب نظام أشغال المنظومة".[2]

- جريمة التزوير المعلوماتي جريمة الإستيلاء على المعطيات : تعد هذه الجريمة من بين أكثر الجرائم وقوعا في العالم الإفتراضي وهذا ما أقرته المادة 394 مكرر 2 بنصها على:

[1] عقياش بريزة ومبارك حنان، **آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري**، مذكرة ماستر، تخصص إعلام آلي وأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي-برج بوعريريج-2022، ص57.

[2] المادة 394 مكرر، القانون 04-15، المؤرخ في 27 رمضان 1425 الموافق ل 8 نوفمبر 2004، المتضمن تعديل قانون العقوبات،الجريدة الرسمية، العدد71، المؤرخة في 11 نوفمبر 2004،ص ص11-12.

"1-كل من يقوم عمدا أو عن طريق الغش تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية2- حيازة أو إفشاءأو إستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم."[1]

- جريمة إتلاف وتدمير المعطيات: تطرق إليها المشرع الجزائري بموجب المادة 394 مكرر1 والتي تنص على:" يعاقب بالحبس أو الغرامة كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدَل بطريق الغش المعطيات التي تتضمنها."[2] وجريمة الإتلاف هنا تتمثل في إزالة معطيات نظام المعالجة الآلية عن طريق الفيروسات مثلا: أنشطة الأنترنت المجسدة لجرائم المحتوى الضار_والتصرف الغير قانوني نصت مواد القسم السابع مكرر من قانون العقوبات وخاصة المادة 394 مكرر 2\2 تجريم أفعال الحيازة الإفشاء والنشر التي ترد على المعطيات الآلية بأهداف المنافسة غير المشروعة الجوسسة، الإرهاب، التحريض على الفسق، وجمع الأفعال غير المشروعة وذلك بعقوبتي الحبس والغرامة إضافية إلى ما نصت عليه المادة394 مكرر6 بتوقيع عقوبة تكميلية في غلق المواقع التي تكون محلا لجريمة من الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات، تتمثل الجزاءات المقررة بموجب الفصل السابع مكرر في العقوبات الأصلية وهي عقوبة الحبس والغرامة وعقوبات تكميلية بموجب نص المادة 394 مكرر 6 المتمثلة في مصادرة الأجهزة والبرامج والوسائل المستخدمة وإغلاق المواقع والمحل وأماكن الإستغلال ومثال ذلك إغلاق مقهى الإنترنت الذي ترتكب فيه هذه الجرائم بشرط علم مالكه وقد أورد المشرع الجزائري ظروفا تشديدية لعقوبة الجريمة ففي حالة الدخول والبقاء الغير مشروع إذا ترتب على ذلك تغيير لمعطيات

[1] أنظر إلى المادة 394 مكرر2، القانون04-15 ، المصدر نفسه.

[2] أنظر إلى المادة 394 مكرر1، القانون 04-15 ، المصدر السابق.

المنظومة أو تخريب النظام أو في حالة إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام.

وقد استثنى المشرع من العقاب الأعمال التحضيرية للجرائم السيبرانية المرتكبة من طرف شخص منفرد وذلك حسب المادة 394 مكرر5 ، كما نصت المادة 394 مكرر4 على توقيع العقوبة على الشخص المعنوي الذي يرتكب إحدى الجرائم الواردة في الفصل السابع مكرر بغرامة تعادل 5 مرات الحد الأقصى للغرامة المحددة للشخص الطبيعي والشروع في الجريمة السيبرانية يعاقب عليه بالعقوبة المقررة للجريمة ذاتها، غير أن المسؤولية للشخص المعنوي لا تستبعد المسؤولية الجزائية للشخص الطبيعي بصفتهم فاعلين أو شركاء في نفس الجريمة.[1]

ثانيا: قانون الإجراءات الجزائية

فيما يتعلق بمتابعة الجريمة السيبرانية فهي تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية كالتفتيش والمعاينة، واستجواب المتهم والضبط والتسرب و الشهادة والخبرة، غير أن المشرع الجزائري نص على تمديد الإختصاص المحلي لوكيل الجمهورية في الجرائم السيبرانية، وقد نص على التفتيش في المادة 45 الفقرة 7 من القانون 07/17 المعدل والمتمم لقانون الإجراءات الجزائية حيث اعتبر أن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه في القواعد العامة من حيث الشروط الشكلية والموضوعية، ونص كذلك على التوقيف للنظر في جريمة المساس

[1] صغير يوسف، **الجريمة المرتكبة عبر الأنترنت**، مذكرة ماجيستير في القانون، كلية الحقوق والعلوم السياسية جامعة ملود معمري–تيزي وزو– 2013،ص ص110–111.

بأنظمة المعالجة الآلية للمعطيات في المادة 51 الفقرة 6 وكذلك على اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.[1]

الفرع الرابع: القانون الإداري

وباعتباره قسما من أقسام القانون العام فقد سن المشرع الجزائري حزمة من القوانين كآلية من آليات مكافحة الجريمة السيبرانية وأولها هو القانون المتعلق بالتوقيع الإلكتروني: فقد أصدر شارعنا القانون 15-03.[2] حيث تطرق في الفصل الثاني إلى المنظومة المعموماتية المركزية لوازرة العدل والإشهاد على صحة الوثائق الإلكترونية وضمان حمايتها أما الفصل الثالث تعرض إلى إرسال الوثائق و الإجراءات القضائية بالطريق الإلكتروني، والفصل الخامس تعرض إلى الأحكام الجزائية منه تعاقب على كل من حماية التوقيع والتصديق الإلكترونين حيث أن المادة 17 منه تعاقب على كل من يستعمل بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع الكتروني يتعلق بتوقيع شخص آخر، أما المادة 18 فتعاقب كل شخص حائز على شهادة إلكترونية يستعملها بعد انتهاء صلاحيتها أو إلغاؤها.

أما ثاني قانون فهو القانون 18-07 :المؤرخ في 25 رمضان 1439 الموافق ل 10 يونيو 2018 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، فقد وضع المشرع الجزائري مجموعة من الآليات المتعلقة بالعالم الإفتراضي والتي يمكن إنجازها في عدة نقاط:

- إستحداث سلطة وطنية لحماية المعطيات ذات الطابع الشخصي.

---

[1] عمور راضية، **الجريمة الإلكترونية وآلبات مكافحتها في التشريع الجزائري**، المجلة الأكاديمية للبحوث القانونية والسياسية، مخبر الحقوق والعلوم السياسية، جامعة الأغواط، المجلد6، العدد1، 2022، ص97.

[2] القانون 15-03 المؤرخ في 11 ربيع الثاني عام 1436 الموافق ل 1 فبراير 2015 المتعلق بعصرنة العدالة الجريدة الرسمية، العدد6، المؤرخة في 3 فبراير 2015،ص4.

– وضع مجموعة إلتزامات ملقاة على عاتق المسؤول عن المعالجة الالية للمعطيات ذات الطابع الشخصي كما يمكن للسلطة الوطنية القيام بالتحريات ومعاينة المحلات والأماكن التي تتم فيها المعالجة باستثناء محلات السكن كما يمكنها الولوج إلى معطيات المعالجة اتخاذ السلطة الوطنية لمجموعة إجراءات إدارية في حالة خرق أحكام القانون من طرف المسؤول عن المعالجة، كما قام هذا القانون بتجريم الإعتداء على المعطيات ذات الطابع الشخصي بعقوبات مالية وأخرى سالبة للحرية، إضافة إلى هذا القانون المتعلق بحماية المعلومات والوثائق الإدارية: حيث جاء الأمر 21-09 [1]في المادة 16 منه يمنع الموظف العمومي من الإدلاء لوسائل الإعلام أو في وسائل التواصل الاجتماعي بأي معلومة أو تعليق أو تصريح أو مداخلة حول المعلومات أو حول الوثائق التي اطلع عليها بحكم مهامه أو حول مسائل مازالت قيد الدارسة لدى الجهة التي يعمل بها ما لم يكن مرخصا بذلك.[2]

المطلب الثاني: مكافحة الجريمة السيبرانية في القوانين الخاصة

بعد التعرض لمحاربة الجريمة السيبرانية من خلال القوانين العامة التي وضعها المشرع الجزائري، سنعرض من خلال هذا المطلب القوانين الخاصة المكافحة للجريمة السيبرانية في التشريع الجزائري.

الفرع الأول: القانون المدني

ترتيبا على الأهمية الدستورية لحرمة الحياة الخاصة فقد سارع المشرع ونص على أن لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن

[1] الأمر 21-09 المؤرخ في 27 شوال 1442 الموافق ل8 يوليو 2021 المتعلق بحماية المعلومات والوثائق الإدارية الجريدة الرسمية، العدد91،المؤرخة في 5 ديسمبر 2021، ص9.

[2] عقباش بريزة ومبارك حنان، المرجع السابق،ص ص58-59.

يطلب وقف هذا الإعتداء مع التعويض عما لحقه من ضرر وهذا ما جاء به نص المادة 124 من التقنين المدني:" كل عمل أيا كان يرتكبه المرء يسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض"، وقد جاء هذا النص عاما وشاملا لأي اعتداء يقع على أي حق من الحقوق الملازمة لشخصيته بما فيها الحق في الحياة الخاصة، وقد أورد النص مبدأ مهما هو حق من وقع إعتداء على حياته الخاصة في التعويض عما لحقه من ضرر، فالمسؤولية المدنية ترتب الحق في الحكم بالتعويض فالفعل الضار هو أساس المسؤولية وهو الركن الأساسي الذي يؤسس عليه الحق في رفع الدعوى القضائية عن الإعتداءات السيبرانية التي تمس الحياة الخاصة على شبكة الأنترنت، وهو عنصر متحول وصعب التحديد في الجرائم التي تمس الخصوصية على المواقع الإلكترونية لما تشكله من صعوبات في الإثبات وفي تحديد هوية المتعدي، وفي هذه المسألة قد حذى المشرع الجزائري في إقامة المسؤولية عن الفعل السيبراني الشخصي على أساس الخطأ الواجب الإثبات، فلا يكفي أن يحدث الضرر الذي يمس عناصر الحياة الخاصة بل يجب أن يكون ذلك الفعل السيبراني قد وصل إلى درجة الخطأ الذي يشكل اعتداء قابل للإثبات وإن وقع على الشبكة.[1]

الفرع الثاني: القانون الدولي الخاص

تعتبر مسألة التعاون القضائي بين الدول محط اهتمام وضرورة تفرضها طبيعة العلاقات الدولية الخاصة عبر الحدود، بل هي كما يراها جانب من الفقه مفروضة بمقتضى هدف القانون الدولي الخاص وغايته المتمثلة في التعاون المشترك بين النظم القانونية، وقد حرصت الدول المختلفة منذ زمن طويل تحقيقا لمصلحتها المشتركة على عدم إفلات المجرمين من العقاب وذلك بإبرام إتفاقيات ثنائية بشأن التعاون القانوني

[1] بوضياف أسمهان، المرجع السابق، ص362.

والقضائي فيما بينها في المجال الجنائي بصفة عامة واتخذت وسائل هذا التعاون صورا متنوعة كالإنابة القضائية وتسليم المجرمين، ونجد مساعي وحرص الدولة الجزائرية من خلال مصادقتها على الإتفاقيات الدولية الثنائية، وقد أبرمت الجزائر 71 إتفاقية دولية ثنائية مع 42 دولة متعلقة بمجملها بالتعاون القضائي والقضائي في المجال الجزائي و إتفاقيات تتعلق بتسليم المجرمين حسب الموقع الإلكتروني لوازرة العدل، فالبسبة للإنابة القضائية الدولية فتقسم إلى نوعين:

– الإنابة القضائية الدولية الواردة من الخارج في حالة متابعة غير سياسية في بلد أجنبي تسلم الإنابة القضائية الواردة من السلطة الأجنبية بالطريق الدبلوماسي وترسل الى وازرة العدل بالأوضاع المنصوص عليها في المادة 703 من قانون الإجراءات الجزائية وتنفذ الإنابات القضائية إذا كان لها محل وفقا للقانون الجزائري.

كما أنه من الجائز حضور ممثل عن الدولة طالبة الإنابة عند القيام بالإجراء المطلوب لذلك يتعين إحاطة الجهة الطالبة علما بمكان وزمان تنفيذه لكي يرتاح الطرف ذي الشأن أن يحضر إذا شاء أو أن يوكل من ينوب عنه، وإذا تم القيام بالإجراء على قاضي التحقيق أن يقدم الأوارق المتعلقة به إلى وازرة العدل وفي حالة ما تعذر تنفيذ الإجراء المطلوب لأي سبب ان فلابد من إشعار الدولة طالبة الإنابة بالطرق الدبلوماسية بتعذر تنفيذ الإجراء وسببه.

–الإنابة القضائية الدولية الدولية المرسلة إلى الخارج فترسل من قاضي التحقيق عن طريق السلم الإداري إلى السيد وزير العدل الذي يرسلها بدوره إلى وزارة الخارجية الجزائية التي تبلغها بالطريق الدبلوماسي للسطات القضائية الأجنبية وإذا كان هناك إتفاق بين الجزائر والدولة الأجنبية فإنه يستغنى عن الطريق الدبلوماسي سواء بالنسبة للإنابة الصادرة أو الواردة. وأما بالنسبة لتسليم المجرمين فلقد تنامت في الآونة الأخيرة ظاهرة

فرار المجرمين الإلكترونيين صحبة الأموال التي جنوها من الجرائم التي اقترفوها من الدولة صاحبة الاختصاص بمحاكمتهم إلى دولة أخرى ولمواجهة هذه الظاهرة عمدت مختلف دول العالم إلى إقامة نظام فعال لتسليم المجرمين والمتهمين والذي يحول دون حصول المجرمين على مأوى آمن لهم ولأموالهم كما يحرمهم من الإستفادة من الإختلاف في الأنظمة القانونية والقضائية للدول، ولقد تم تنظيم نصوص في قانون الإجراءات الجزائية في الكتاب السابع تحت عنوان في العلاقات بين السلطات القضائية الأجنبية الباب الأول : في تسليم المجرمين الفصل الأول: في شروط تسليم المجرمين من المواد 694 إلى 701، الفصل الثاني: في إجراءات التسليم الواد من 702 إلى 713، في الفصل الثالث: آثار التسليم المواد من 714 إلى 718، الفصل الرابع: في العبور الترانزيت المادة 719، الفصل الخامس: في الأشياء المضبوطة المادة 720.[1]

الفرع الثالث: قانون الملكية الفكرية

إن اهتمام المشرع الجزائري بوضع قوانين الملكية الفكرية كان بهدف حماية حق الإنسان في الإبداع والإبتكار كعاملين جوهريين في تقدم المجتمع، ولما كانت المكونات المنطقية للحاسب الآلي من برامجه وبياناته ثمرة من مجهود فكري إنساني، كان لزاما على المشرع إحاطة هذه المكونات بالحماية المقررة في قانون الملكية الفنية الأدبية وذلك بتجريم الأفعال التي تشكل اعتداءً عليها، التي تكمن في الإعتراف بوصف المصنف الفكري لمعطيات الحاسب الآلي، حيث تم الإعتراف به صراحة من خلال الأمر 03-05[2] بوصف المصنف* المحمي لمصنفات الإعلام الآلي، وأن أي اعتداء على الحق

[1] عقباش بريزة ومبارك حنان، المرجع السابق، ص64.

[2] الأمر 03-05 المؤرخ في 19 جويلية 2003 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية العدد44،المؤرخة في 23 يوليو 2003 ، ص3.

* المصنف هو: الوعاء المعرفي الذي يحمل إنتاجا أدبيا أو علميا أو فنيا مبتكرا ، مهما كان نوعه أو أهميته أو طريقة التعبير فيه أو الغرض من تصنيفه.

المالي أو الأدبي لمؤلف البرامج والبيانات يشكل فعلا من أفعال التقليد المنصوص عليها في المادة 151 من الأمر 03-05 السابق الذكر وتأخذ جنح التقليد الماسة بمصنف برامج وبيانات الحاسب الآلي ثلاث صور الصورة هي:

- الجنح المرتبطة بالحق المعنوي للمؤلف والتي تحددها الفقرة 1 من المادة 151 من الأمر السالف الذكر (الكشف غير المشروع على المصنف الأدبي والفني كأن يتم الكشف عن برامج في الوقت أو بطريقة يرى المؤلف أنها غير مناسبة، المساس بسلامة المصنف الأدبي أو الفني كأن يقوم شخص بتعديل أو تغيير أو حذف أو إضافة أو تحويل على البرامج أو بيانات الحاسب دون إذن المؤلف).

- الجنح المرتبطة بالحق الأدبي للمؤلف(الإستنساخ غير الشرعي للمصنف المادة 151 فقرة 1 ويقوم فيها الشخص بنسخ بيانات أو برامج الحاسب في شكل نسج مقلدة دون إذن المؤلف، الإبلاغ الغير شرعي للمصنف وهو إبلاغ الجمهور بهذا المصنف دون علم وترخيص من المؤلف)، أما بالنسبة للصورة الثالثة فتتمثل في الجنح المرتبطة بالمصنف المقلد وتتعلق هذه الجنح بالتصرفات والتعاملات التي ترد على المصنف المقلد الذي يمكن أن يكون برامج أو بيانات الحاسب الآلي وهي : إستيراد أو تصدير نسخ مقلدة من المصنف، بيع نسخ مزورة من المصنف، تأجير مصنف مقلد أو عرضه للتداول، الرفض عمدا في دفع المكافأة المستحقة بمقتضى الحقوق المقررة للمؤلف، ولقد نصت المواد من 153إلى 185 على العقوبات المقررة لهذه الأفعال، فتكون العقوبات الأصلية المقررة لجنح تقليد معطيات الحاسب الآلي عقوبة الحبس وعقوبة الغرامة، أما العقوبات التكميلية فتتمثل في: مصادرة المبالغ المساوية لأقساط الإيرادات المحصلة من الإستغلال الغير المشروع للمصنف مصادرة وإتلاف كل عتاد أنشأ خصيصا لمباشرة النشاط الغير مشروع

وكل النسخ المقلدة، الأمر بتسليم العتاد والنسخ المقلدة أو قيمة ذلك، الأمر بطلب من المتضرر بتعليق ونشر أحكام الإدانة على نفقة المحكوم عليه.[1]

الفرع الرابع: قانون الملكية الصناعية

لقد واجه المشرع الجزائري الجريمة السيبرانية من خلال قانون الملكية الصناعية وذلك من خلال أحكام العلامات التجارية أولا والتي ينظمها الأمر 03-06[2] والمعدل للأمر 67-223 المؤرخ في 19 أكتوبر 1967 المتضمن أحكام العلامات التجارية والعلامات التجارية أو الصناعية وسيلة من وسائل المنافسة المشروعة بين المنتجين أو التجار شأنها شأن بقية حقوق الملكية الصناعية بحيث إذا اتخذ أحد التجار أو المنتجتين علامة تجارية أو صناعية معينة تمييزا لبضائعه أو منتجاته فإنه يمنع على غيره من التجار أو منتجين إستخدام نفس هذه العلامة لتمييز سلع متماثلة؛ أي أنها تتمع بالحماية المقررة لحقوق الملكية الصناعية،[3] شريطة أن تكون جديدة ومميزة وغير مخالفة للنظام العام والآداب العامة.

وبالنسبة لبرامج الحاسب الآلي فإنها تستفيد من نفس الحماية الجنائية للعلامات التجارية، فكل برنامج يحمل إسما خاصا به لذلك فقد عمد أصحاب البرامج إلى تسجيل هذا الإسم كعلامة تجارية لهذه البرامج ولما كانت هذه الحماية قاصرة على الإسم دون المحتوى فقد لجأ أصحاب البرامج إلى وضع الإسم مقترنا به بالإضافة إلى مواجهة المشرع الجزائري للجريمة السيبراينة من خلال العلامات التجارية في قانون الملكية الفكرية

---

[1] ناجية شيخ، **حول مكافحة الجريمة الإلكترونية في التشريع الجزائري**، مجلة العلوم القانونية السياسية، جامعة مولود معمري تيزي وزو، المجلد 9، العدد2، جوان 2018، ص ص 695،696.

[2] الأمر 06-03 المؤرخ في 19 جويلية 2003 المتعلق بالعلامات، الجريدة الرسمية، العدد 44، المؤرخة في 23 يوليو 2003، ص22.

[3] قارة آمال، **الجرائم المعلوماتية**، رسالة ماجيستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 2001-2002، ص 109.

فقد تمت مواجهته لها أيضا من خلال أحكام براءة الإختراع * والتي يجب أن يتوافر فيها شرط الإبتكار والجدة والمشروعية بالإضافة إلى القابلية للتطبيق الصناعي وفي هذه الحالة يتحصل المخترع على براءة الإختراع لكن السؤال المطروح هنا هل يمكن لبرامج الحاسب الآلي أن تستفيد من الحماية بواسطة براءات الإختراع؟ فتجدر الإشارة هنا من خلال طرح هذا التساؤل إلى أن المشرع الجزائري قد استبعد البرامج المعلوماتية صراحة من مجال الحماية بواسطة براءة الإختراع وذلك طبقا للمادة 7 من الأمر 03-07[1] المتضمن براءة الإختراع.[2]

بالإضافة إلى القوانين المذكورة أعلاه التي واجه بها المشرع الجزائري الجريمة السيبرانية فإن هناك قوانين أخرى نذكرها على النحو التالي:

- القانون 09-04: المتعلق بالقواعد الخاضة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها السابق ذكره، يخول هذا القانون لبعض السلطات المختصة بالقيام بعمليات المراقبة لكل الإتصالات الإلكترونية بهدف الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة إذا تلقوا معلومات عن احتمال اعتداء على منظومة معلوماتية لكن في حدود ما يسمح به القانون، تحت طائلة العقوبات المقررة في قانون العقوبات عن جنحة المساس بالحق في الحياة الخاصة.[3]

* براءة الإختراع هو إبتكار أي إنتاج صناعي جديد أو اكتشاف طريقة جديدة للحصول على إنتاج صناعي قائم أو نتيجة صناعية موجودة أو الوصول إلى تطبيق جديد لطريقة صناعية معروفة.

[1] الأمر 03-07 المتلعق ببراءة الإختراع، المؤرخ في 19 جمادى الأولى 1424 الموافق ل 19 يوليو 2003، الجريدة الرسمية، العدد44، المؤرخة في 23 يوليو 2003، ، ص27.

[2] فشار عطا الله، **مواجهة الجريمة المعلوماتية في التشريع الجزائري**، مداخلة مقدمة إلى الملتقى المغاربي حول القانون والمعلوماتية المزمع ، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور بالجلفة، 2009، د.ص.

[3] زناتي محمد السعيد و جواج يمينة، **أثر الجرائم السيبرانية على الحريات الفردية**، المجلة الإفريقية للدراسات القانونية والسياسية، جامعة عبد الحميد بن باديس، المجلد6، العدد 1، 2022، ص54.

– قانون الإعلام: فكل القوانين المتعلقة بالصحافة تُلزم الصحفي باحترام الحريات العامة للآخرين وحفظ حقوقهم وعدم المساس بحرمة حياتهم الخاصة، وكذا الإلتزام بالحيدة والموضوعية في عرض المادة الصحفية والإمتناع عن نشر ما يتعارض مع مبادئ الحرية والمسؤولية الوطنية وحقوق الإنسان وقيم الأمة العربية والإسلامية.[1] لذلك فقد نص المشرع الجزائري على نفس المبادئ في المادة 2 من القانون 12-05 المتعلق بالإعلام على أنه: "يمارس نشاط الإعلام بحرية في إطار أحكام هذا القانون العضوي والتشريع والتنظيم المعمول بهما وفي ظل احترام: الدستور وقوانين الجمهورية الدين الإسلامي وباقي الأديان .... حق المواطن في إعلام كامل وموضوعي _ سرية التحقيق القضائي _ كرامة الإنسان والحريات الفردية والجماعية.[2]

– القانون 18-04 المتعلق بالقواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية[3]: حيث استحدث هذا القانون مجموعة آليات للتصدي للجرائم السيبرانية منها إستحداث سلطة ضبط من بين مهامها السهر على احترام متعاملي البريد والإتصالات الإلكترونية تجريم انتهاك سرية المراسلات عن طريق البريد والإتصالات الإلكترونية أو إفشاء مضمونها أو نشرها أو استعمالها دون ترخيص من المرسل إلى المرسل إليه وتجريم

[1] المرجع نفسه، ص55.

[2] المادة 2، القانون العضوي رقم 12-05 المؤرخ 1433 الموافق ل 12 يناير 2012 ، المتعلق بالإعلام الجريدة الرسمية، العدد2، المؤرخة في 15 يناير 2012 ، ص21.

[3] القانون 18-04، المؤرخ في 24 شعبان 1439 الموافق ل 10 مايو 2018 المحدد القواعد العامة المتعلة بالبريد و الإتصلات الإلكترونية، الجريدة الرسمية، المؤرخة في 13 مايو 2013، العدد27، ص3.

محاولة فتح أو تخريب أو تحويل البريد أو المساعدة في هذه الجريمة.[1] وسنت مجموعة العقوبات المقررة لهذه الجرائم ضمن المواد من 164 إلى 188 من هذا القانون.[2]

– القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الآلي: فلقد أقر هذا القانون المبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي فنجد المادة 7 من هذا القانون تنص على ضرورة إبداء الموافقة الصريحة للشخص المعنيٍ من أجل السماح بمعالجة معطياته الشخصية، وله التَّراجع عن موافقته في أي وقت، غير أن موافقته لا تكون ضرورية متى تعلق الأمر باحترام قانوني يخضع له المعني، ولم يغفل أيضا في حماية المعطيات الخاصة بالأطفال فقد جاءت المادة 8 من نفس القانون متوقفة على موافقة ممثله الشرعي أو بترخيص من القاضي المختص عند الإقتضاء.

كما أن السلطة الوطنية تخضع أي معالجة تتمضن أخطار ظاهرة على احترام وحماية الحياة الخاصة لترخيص مسبق بواسطة قرار مسبق يبلغ إلى المسؤول عن المعالجة في تاريخ 10 أيام من تاريخ إيداع التصريح، كما يمنح الترخيص بمعالجة المعطيات الحساسة في حالة ما إذا كانت كانت المعالجة ضرورية لحماية المصالح الحيوية للشخص المعني أو لشخص آخر كما منح هذا القانون ممارسة حق التصحيح أو التحيين أو مسح أو إغلاق المعطيات الشخصية عندما يتبين له أن هذه المعطيات غير مكتملة أو غير صحيحة أو لكون معالجتها ممنوعة قانون، وأضافت المادة 36 من القانون نفسه حق الشخص في الاعتَّرض على معالجة معطياته الشخصية، خاصة إذا

[1] مهدي رضا ، **الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري**، مجلة إيليزا للبحوث والدراسات، جامعة محمد بوضياف المسيلة، المجلد6، العدد2، 2021، ص121.

[2] أنظر إلى المواد من 164 إلى 188 من القانون 18-04 المؤرخ في 10 ماي 2018، المتعلق بالقواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية.

تعلق الأمر بأغراض دعائية أو تجارية، وألزم المسؤول عن المعالجة باتخاذ كل التدابير التقنية والاحتِّزازات اللازمة من أجل حماية وتأمين المعطيات ذات الطابع الشخصي من القرصنة والتلف وكل استخدام غير مشروع، كما ألزمته بالسر المهني وعدم إفشاء المعطيات التي وصلت إلى عمله.[1]

– قانون التأمينات الإجتماعية: بمقتضى أحكام قانون التأمينات الإجتماعية 08-01[2]، ثم بمقتضى هذا القانون تشديد العقوبة في ما يتعلق بالمساس الغير مشروع للبطاقة الإلكترونية للمُؤَمن له اجتماعيا، وقد عاقب المشرع الجزائري كل من يسلك أو يستلم بهدف الإستعمال الغير المشروق للبطاقة الإلكترونية للمُؤمن له اجتماعيا كما يشمل العقاب التعديل أو الحذف الكلي أو الجزئي للمعطيات التقنية والإدارية المدرجة في البطاقة الإلكترونية أو نسخ البرمجيات المتعلقة باستعمال البطاقة الإلكترونية، كما أقر أيضا عقوبة للشخص المعنوي في الغرامة ضعف الغرامة المقررة للشخص الطبيعي ومصادرة الاجهزة المستعملة وكدا غلق المحلات وأماكن الإستغلال التي تكون محل الجنح.[3]

[1] شويرب جيلالي ومراد فائزة، **الآليات الدولية والوطنية لمكافحة الجريمة السيبرانية**، مجلة الدراسات القانونية والسياسية، مخبر السيادة والعولمة، جامعة الدكتور يحي فارس المدية، المجلد9، العدد2 ، جوان 2023 ص163.

[2] القانون 08-01، المؤرخ في الموافق ل 23 جانفي 2008 المتعلق بالتأمينات الإجتماعية، الجريدة الرسمية، العدد4،المؤرخة في 27 يناير 2008، ص4.

[3] خلف فاروق، **الآليات القانونية لمكافحة الجريمة المعولماتية**، الملتقى الوطني "الجريمة المعلوماتية بين الوقاية والمكافحة"، جامعة محمد خيضر بسكرة،د.ت، ص ص11-12.

المبحث الثاني : الآليات الإجرائية لمكافحة الجريمة السيبراينة في التشريع الجزائري

بالإضافة إلى الآليات القانونية التي جاء بها المشرع الجزائري لمواجهة الجريمة السيبراينة، فقد أتى أيضا بمجموعة من الآليات الإجرائية لمجابهتها والتي تنقسم بدورها إلى الآليات الإجرائية الوقائية(المطلب الأول)، والآليات الإجرائية المؤسساتية(المطلب الثاني).

المطلب الأول: الآليات الإجرائية الوقائية

إتخذ المشرع الجزائري عدة آليات وقائية للرصد المبكر لمخاطر الجرائم السيبراينة سنتعرف عليها من خلال مطلبنا هذا بالتعرض للآليات الإجرائية الوقائية التقليدية (الفرع الأول)، ثم إلى الآليات الإجرائية الوقائية المستحثة (الفرع الثاني).

الفرع الأول: الآليات الإجرائية الوقائية التقليدية

وتتمثل في ما يلي :

أولا: مراقبة الإتصالات الإلكترونية

بين المشرع الجزائري من خلال القانون 09-04 السالف الذكر الحالات التي يسمح فيها باللجوء إلى المراقبة الإلكترونية حيث يتضمن هذا القانون حماية الحريات الفردية لا سيما منها الخصوصية، وقد أورد بوضوح من خلال هذه المادة الأحكام الخاصة بالمراقبة الإلكترونية التي لا يجوز إجراءها إلا بإذن السلطات القضائية المختصة، كما تتمثل الحالات المحددة للجوء إلى المراقبة الإلكترونبة في 4 حالات وهي:

– للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

– في حالة توفر معلومات عن احتمال اعتداء على منظومة المعلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني.

– لمقتضيات التحريات والتحقيقات القضائية، عندمل يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون الجوء إلى المراقبة الإلكترونية.

– في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطات القضائية المختصة. فالمشرع من خلال حصره لهذه الحالات أراد أن يوازن إلى حد ما بين حرية الافراد في سرية الاتصالات و احترام خصوصيتهم وبين مكافحة الجرائم الماسة بالنظام والأمن العموميين، حتى لا يتم تقييد حرية الأفراد ولايتم الإخلال بالأحكام القانونية التي تضمن سرية الإتصالات في حالة ما إذا تركت الحرية لرجال الضبطية القضائية في مراقبة الإتصالات الإلكترونية وجعل اجراء المراقبة في يد السلطات القضائية، وفي حالة الجرائم الموصوفة بجرائم الإرهاب والتخريب والماسة بأمن الدولة يتم منح الإذن لضابط الشرطة القضائية إجراء عملية المراقبة من قبل النائب العام لدى مجلس قضاء الجزائر، يكون صالحا لمدة 6 أشهر قابلة للتجديد، كما شدَد المشرع أن المعطيات المجمعةجراء عملية المراقبة تكون موجهة حصريا للوقاية من الإعتداءات الإرهابية والماسة بأمن الدولة، وذلك تحت طائلة العقوبات في حالة المساس بالحياة الخاصة للغير.[1]

[1] معتوق عبد اللطيف، **الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن**، مذكرة ماجيستير في العلوم القانونية، تخصص قانون جنائي وعلوم جنائية،كلية الحقوق والعلوم السياسية، جامعة العقيد الحاج لخضر –باتنة– 2011–2012، ص 131.

ثانيا: تفتيش المنظومة المعلوماتية

يتم التفتيش في الجريمة العادية من قبل رجال الشرطة القضائية وبموجب إذن كتابي صادر عن وكيل الجمهورية أو قاضي التحقيق ولا بد من استظهار هذا الإذن عند التفتيش الذي يمس الأماكن أو الأشخاص كما يجب حضور المتهم أو من ينوبه أو شهود، ولا يمكن التفتيش إلا في ساعات محددة قانونا من الساعة الخامسة صباحا إلى الساعة الثامنة مساءا أما التفتيش في الجريمة السيبرانية أو ما يعرف بتفتيش المنظومة المعلوماتية* فيقوم به ضباط الشرطة القضائية إلى جانب الجهات القضائية التي يؤول إليها الإختصاص للتحقيق في هذه الجريمة، كما يمكن اللجوء إلى أشخاص مؤهلين كالخبارء والتقنيين في الإعلام الآلي لإجراء هذه العملية.[1] إذ يكون محل التفتيش في المنظومة المعلوماتية هو جهاز الكمبيوتر والأجهزة المتصلة به والشبكة التي تشمل في مكوناتها مقدم الخدمة والمزود الآلي والمضيف والملحقات التقنية وعليه فهو ينكب على المكنات التالية: المكونات المادية hardware والمكونات المعنوية والمنطقية لجهاز الكمبيوتر software بالإضافة إلى شبكات الإتصال البعدية السلكية واللاسلكية هذه المكونات التي يمكن أو توجد في حوزة شخص أو أن تكون موضوعة في مكان له في حرمه كالمسكن.[2] لذلك فعند البحث عن الدليل (الدليل الرقمي) فإنه يتطلب البحث في

* تفتيش المنظومة المعلوماتية يقصد به : الإطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه يستوي في ذلك أن يكزن هذا المحل جهاز الحاسوب أو نُظمه أو النترنت

[1] بوراس نادية، **الإستراتيجيات الوطنية لمواجهة جرائم المساس بأنظمة المعالجة الآلية للمعطيات**، مجلة الحقوق والحريات، جامعة لمين دباغين، المجلد10، العدد3، 2023، ص588.

[2] بوخبزة عائشة، **الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري**، مذكرة ماجيستير في القانون الجنائي، كلية الحقوق، جامعة وهران،2012-2013، ص179-180.

البيئة الإفتراضية التي تقع داخل الحاسب وشبكة الإنترنت أي التعامل مع مختلف المعلومات والبيانات الرقمية المتواجدة بالشبكة، كما يشمل أيضا مختلف الوسائل المادية للحاسوب كالأقراص المضغوطة، حيث يجري التفتيش على يد فريق يتكون من: المحقق الرئيسي ويكون ممن لهم الخبرة في التحقيق الجنائي، خبراء الحاسوب شبكات الأنترنت الذين يعرفون كيفية التعامل مع مثل هذه الجرائم، خبراء ضبط وتحرير الأدلة الرقمية العارفين بأمور تفتيش الحاسوب، خبراء الحاسوب اللذين يتعاملون مه الأنظمة البرمجية، خبراء التصوير والبصمات والرسم التخطيطي.[1]

ثالثا: حجز المعطيات المعلوماتية

يتم الحجز هنا يكون عن المعطيات المتحصلة من التفتيش، والتي تكون مفيدة في الكشف عن الجرائم ومرتكبيها، فالقانون رخص بنسخ المعطيات محل البحث وليس حجز كل المنطومة، كما يمكن نسخ المعطيات اللازمة لفهمها، ويتم تخزين هذه المعطيات على دعامة تخزين إلكترونية وتحجز وتوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية، فإذا استحال إجراء الحجز لأسباب تقنية يتعين على السلطات المكلفة بالتفتيش إستعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، وإذ اقتضى الحفاظ عليها لمقتضيات التحقيق لا سيما إذا كانت المعطيات المحجوزة ذات محتوى مُجرَم فإن للسلطات التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الإطلاع على هذه المعطيات، كما يمنع استعمال المعلومات المتحصل

[1] العوفي دليلة، **آليات محاربة الجريمة المعلوماتية**، أطروحة دكتوراه في علوم الإعلام والإتصال، كلية العلوم والإعلام والإتصال، جامعة الجزائر3، 2019-2020، ص ص331-334.

عليها عن طريق عمليات المراقبة إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية، وهذا تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به.[1]

الفرع الثاني: الآليات الإجرائية الوقائية المستحدثة

وهي بدورها تتقسم إلى ثلاث إجراءات وقائية وتتمثل في :

أولا : التسرب

التسرب كما تعرفه المادة 65 مكرر 12 من قانون الإجراءات الجزائية: "قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الاشخاص المشتبه في ارتكابها جناية أو جنحة بإيهامهم بأنه فاعل معهم أو شريك لهم أو خاف".ويسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة، أو أن يرتكب عند الضرورة فعلا مخالفا دون أن يكون مسؤولا جنائيا، وبشرط أن لا يشكل ذلك تحريضا على ارتكاب جرائم الافعال التالية:

– إقتناء 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.

– إستعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الإتصال.

وإذا اقتضت ضرورات التحري أو التحقيق الإبتدائي في الجرائم المتلبس بها التالية: جرائم المخدرات، الجرائم المنظمة عبر الحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال، جرائم الإرهاب، الجرائم المتعلقة بالتشريع الخاص

[1] عمراني أحمد، **الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها في التشريع الجزائري والتشريع المقارن** مجلة الحضارة الإسلامية، جامعة وهران، د.م، العدد16، ماي 2012، ص611.

بالصرف وكذا جرائم الفساد، فإنه يجوز لوكيل الجمهورية المختص أو قاضي التحقيق بعد إخطار وكيل الجمهورية وتحت مراقبتهما الإذن كتابيا لظابط الشرطة القضائية بمباشرة عملية التسرب بالشروط التالية:

– يحرر ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب تقريرا يتضمن العناصر الضرورية لمعاينة الجرائم غير تلك التي قد تعرض للخطر أمن الضابط أو العون المتسرب وكذلك الاشخاص المسخرين للقيام بالعميات التقنية.

– يجب أن يكون الإذن المسلم تحت طائلة البطلان مكتوبا ومسببا، وتذكر فيه الجريمة التي تبرر اللجوء إلى هذا الإجراء، وهوية ضابط الشرطة التي تتم العملية تحت مسؤوليته، ومدة عملية التسرب التي لا يمكن أن تتجاوز 4 أشهر قابلة للتجديد ضمن نفس الشروط الشكلية والزمنية، وتودع هذه الرخصة بالملف بعد الإنتهاء من عملية التسرب.

– يجوز للقاضي الذي منح الرخصة أن يأمر بوقفها في أي وقت قبل انقضاء المدة المحددة، غير أنه يمكن للعون أو الضابط المتسرب طلب تمديدها للوقت الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسؤول جنائيا على ألا تتجاوز مدة 4 أشهر

– يعاقب كل من يكشف الهوية الحقيقية للضباط وأعوان الشرطة القضائية الذين باشروا العملية تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات بالعقوبات المنصوص عليها في المادة 65 مكرر16 من قانون الإجراءات الجزائية.[1]

ثانيا: اعتراض المراسلات والمراقبة الإلكترونية

[1] بن مالك أحمد، **خصوصية الجريمة المعلوماتية وسبل مكافحتها في التشريع الجزائري**، المجلة الجزائرية للحقوق والعلوم السياسية، جامعة تمنغست، المجلد8، العدد1، 2023، ص ص13–14.

يقصد باعتراض المراسلات، تلك العملية التي تسمح بمراقبة سرية المراسلات السلكية واللاسلكية في إطار البحث والتحري عن الجريمة، وجمع الأدلة والمعلومات حول الاشخاص المشتبه في ارتكابهم أو مشاركتهم في ارتكاب الجرم، وعليه فإن عملية إعتراض أو مراقبة المراسلات* تتم عن طريق ترتيبات تقنية سرية، يتم وضعها دون موافقة الأشخاص المعنيين المشتبه بهم، بغرض التصنت والتقاط وتثبيت وتسجيل البيانات المرسلة أو المحادثات التي أجراها المشتبه في أماكن عامة أو خاصة من أجل استعمالها كدليل لمواجهته، كما تعد المراسلات عبر البريد الإلكتروني مجالا خصبا للربط والإتصال الإلكتروني(18-04) بين الاشخاص في مختلف أنحاء العالم وبوقت قياسي ومن ثم إخضاعها لعملية الإعتراض والمراقبة للكشف عن الجرائم السيبرانية

: ولكي تكون المراسلات محلا لإجراء الإعتراض أو المراقبة يجب أن تتسم بالسرية ولا يتحقق ذلك إلا بتوفر عنصرين هما: فحوى الرسالة والتي تنصب على معلومات أو أفكار سرية أو شخصية، تحديد المرسل إليه ورغبته في عدم السماح للغير بالإطلاع على مضمون المراسلة، مع الإشارة أن المشرع الجزائري لم يتبن إجراء مراقبة الإتصالات الإلكترونية كإجراء للتحقيق القضائي وكذا التحري بموجب القانون 09-04 بل أعطى التصريح للجهات القضائية باستعمال الإعتراض بهدف الوقاية من بعض الجرائم التي تشكل خطرا على أمن الدولة وإتماما لهذا الهدف قد استحدث الهيئة الوطنية الخاصة بالوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والإتصال، ولاعتراض المراسلات يجب أن تكون هذه العملية مرهونة بشروط قانونية تتمثل في:

* تعرف عملية مراقبة المراسلات على أنها : إعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الإتصال السلكية أو اللاسلكية.

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

– التسبيب: أي تبيان دواعي اللجوء إلى الإعتراض ومراقبة المراسلات وتبيان مدى جدية تلك الدواعي ودورها في إظهار الجريمة و الجناة.

– تحديد الجرائم محل الإعتراض والمراقبة والتي يتوجب أن لا تخرج عن ماهو مقرر قانونا مع مراعاة سرية الإجراءات وكتمان السر المهني.[1]

ثالثا: جمع وتسجيل المعطيات

تنص المادة العاشرة من القانون 09-04 السابق ذكره على: "في إطار تطبيق أحكام هذا القانون يتعين على مقدمي الخدمة تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها... ويتعين على مقدمي الخدمات كتمان سرية المعلومات التي ينجزونها بطلب من المحققين، وكذلك المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق."[2] وطبقا لنص المادة 12 من القانون نفسه يتعين على مقدمي خدمة الإنترنت ما يلي:

– التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن.

[1] مجدوب نوال، **الآليات الإجرائية للكشف عن الجريمة المعلوماتية**، مجلة البحوث القانونية و الإقتصادية المركز الجامعي مغنية، المجلد6، العدد3، 2023، ص ص203-204.

[2] المادة 10، القانون 09-04، المصدر السابق.

– وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.[1]

المطلب الثاني: الآليات الإجرائية المؤسساتية

نظرا لتفاقم الظاهرة السيبرانية من يوم لآخر في معظم دول العالم والتي من بينها الجزائر وبعد مواجهتها بآليات إجرائية قانونية ، فقد سخرت الجزائر أيضا آليات إجرائية مؤسساتية تتمثل في هيئات ووحدات متخصصة مهمتها الوقاية من الجرائم السيبرانة سنتعرف عليها على النحو الآتي:

الفرع الأول: الهيئة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال

أنشئت هذه الهيئة بموجب القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، والذي حددت المادة 14 منه مهام الهيئة والمتمثلة:

– تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال.

– مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات المتعلقة بهذه الجرائم.

– تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.[1]

[1] بن مالك أحمد، المرجع السابق، ص 16.

أما فيما يخص تشكيلة الهيئة فقد نصت عليها المادة الثالثة من المرسوم 19-127 :" تظم الهيئة من مجلس توجيه ومديرية عامة". حيث يترأس مجلس التوجيه وزير الدفاع الوطني أو ممثله ويتشكل من ممثلي الوزارات التالية: وزارة الدفاع الوطني الوزارة المكلفة بالداخلية، وزارة العدل، الوزارة المكلفة بالمواصلات السلكية واللاسلكية، بعدما كانت هذه الهيئة تضم حسب المادة 6 من المرسوم 15-261 [2]الذي يحدد تشكيلة وتنظيم كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها لجنة مديرة ومديرية عامة ومديرية للمراقبة الوقائية واليقظة الإلكترونية ومديرية التنسيق الإلكتروني ومركز للعمليات التقنية وملحقات جهوية حيث يترأس اللجنة المديرة الوزير المكلف بالعدل.[3]

الفرع الثاني: السلطة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال

بمقتضى القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، تم إنشاء سلطة وطنية لحمايـة المعطيات ذات الطابع الشخصي لدى رئيس الجمهورية، مقرها بالجزائر العاصمة، تتمتع بالشخصية المعنوية والاستقلال المالي والإداري، وحسب المادة 23 من القانون ذاته فإن السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي تتشكل من ثلاث شخصيات يتم اختيارهم من

---

[1] بوهرين فتيحة، **الجريمة المعلوماتية في التشريع الجزائري**، مجلة الحقوق والعلوم الإنسانية، جامعة قسنطينة2 المجلد14، العدد4، 2021، ص10.

[2] المرسوم الرئاسي 15-261، المؤرخ في 24 ذي الحجة 1436 الموافق ل 8 أكتوبر 2015 ،يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنزلوجيات الإعلام والإتصال، الجريدة االرسمية، العدد53 الموؤرخة في 8 أكتوبر 2015، ص16.

[3] حوالف حليمة ومهاجي فاطمة الزهراء، **معالم الجريمة المعلوماتية في القانون الجزائري**، مجلة البحوث القانونية والسياسية، جامعة تلمسان، المجلد3، العدد6، 2021، ص152.

قبل رئيس الجمهورية من ذوي الإختصاص في عمل السلطة الوطنية، تضم ثلاثة قضاة يتم اقتراحهم من قبل المجلس الأعلى للقضاء من بين قضاة المحكمة العليا ومجلس الدولة، وعضو من كل غرفة من غرفتي البرلمان يتم اختيار كل منهما من قبل رئيس كل غرفة بعد التشاور مع رؤساءالمجموعات البرلمانية، وكذا ممثل واحد عن المجلس الوطني لحقوق الإنسان، وممثل عن وزير الدفاع الوطني، وممثل عن وزير الشؤون الخارجية، وممثل عن الوزير المكلف بالداخلية، وممثل عن وزير العدل حافظ الاختام، وممثل عن الوزير المكلف بالبريد والمواصلات السلكية وللاسلكية والتكنولوجيات والرقمنة وعضوين آخرين عن كل من الوزير المكلف بالصحة، ووزير العمل والتشغيل والضمان الاجتماعي، يتم اختيارهم بناءً على كفاءتهم في الميادين القانونية والتقنية في مجال المعطيات ذات الطابع الشخصي، وقد أوكل المشرع الجزائري للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي عدة مهام مهمة خاصة وأنها تلعب دورا كبيرا في حماية المعطيات ذات الطابع الشخصيً وتكمن هذه المهام في:

– تلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي، وتمنح التراخيص عند الاقتضاء، إذا تبين لها أن المعالجة المعتزم القيام بها تتضمن أخطارا ظاهرة على احترام وحماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص.

– تقوم السلطة الوطنية بإعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم، كما تقدم الاستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي أو التي تقوم بتجارب أو خبرات من طبيعتها أن تؤدي إلى مثل هذه المعالجة.

– تلقي الاحتجاجات والطعون والشكاوي بخصوص تنفيذ معالجة المعطيات ذات الطابع الشخصي وإعلام أصحابها بمآلها.

– الترخيص بنقل المعطيات ذات الطابع الشخصي وفقا للشروط المنصوص عليها في هذا القانون خاصة المادتين 44 و45 منه.

– الأمر بإجراء التغييرات اللازمة من أجل حماية المعطيات ذات الطابع الشخصي المعالجة، والأمر بإغلاق معطيات أو سحبها أو إتلافها، خاصة إذا كانت معالجة تلك المعطيات غير مطابقة للقانون 18-07 .

– تقديم أي اقتراح من شأنه تبسيط وتحسين الإطار التشريعي والتنظيمي لمعالجة المعطيات ذات الطابع الشخصي.[1]

الفرع الثالث: الوحدات التابعة لأسلاك الأمن الوطني

توجد على مستوى جهاز الأمن الوطني ثلاث وحدات مكلفة بالبحث و التحري والتحقيق في الجريمة السيبرانية وهي:

– المخبر المركزي للشرطة العلمية بالجزائر العاصمة.

– المخبر الجهوي للشرطة العلمية بقسنطينة.

– المخبر الجهوي للشرطة العلمية بوهران.

في سبيل تدعيم المصالح الولائية للشرطة القضائية قامت المديرية العامة للأمن الوطني سنة 2010 بخلق ما يقارب 23 خلية لمكاقحة الجريمة السيبرانية على مستوى ولايات الوطن، لتقوم فيما بعد بتعميم الخلايا على جميع مصالح أمن ولايات الوطن.[2]

---

[1] شنيتر خضرة، **الآليات القانونية لمكافحة الجريمة الإلكترونية**، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية،جامعة أحمد دراية أدرار، 2021، ص ص173-174 .

[2] بوزنون سعيدة، **مكافحة الجريمة الإلكترونية في التشريع الجزائري**، مجلة العلوم الإنسانية، جامعة الإخوة منتوري قسنطينة، المجلد ب، العدد52، ديسمبر2019، ص53.

الفرع الرابع: المعهد الوطني للأدلة الجنائية وعلم الإجرام

يتكون من إحدى عشر دائرة متخصصة في مجالات مختلفة، تضمن إنجاز الخبرة التعليم والتكوين وتقديم المساعدات التقنية، بحيث تتكفل دائرة الإعلام الآلي والإلكتروني بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة، كما تقدم المساعدة التقنية للمحققين في المعاينات.[1]

ويحتوي المعهد الوطني للأدلة الجنائية وعلم الإجرام على العديد من الأقسام والمصالح المختصة والتي من شأنها ضمان تأدية المهام الموكلة له بكل إحترافية ودقة نذكر منها:

– مصلحة البصمات ويتم عبر هذه المصلحة مقارنة البصمات للتعرف على الجثث – مصلة الوثائق وفي هذه المصلحة يتم التأكد من صحة الوثائق والإمضاءات والتحقق من النقود وكذا التأكد من صحة الوثائق السرية

– مصلحة الإعلام الآلي ويتم على مستوى هذه المصلحة رصد ومراقبة وتتبع عمليات الإختراق والقرصنة السيبراينة، قسم التحليل الدقيق والذي يتم من خلاله إجراء عمليات المسح الإلكتروني، قسم السيارات أين يتم التعرف على السيارات المسروقة وتتبع عملية تغيير وتحريف الأرقام الخاصة، إضافة إلى هذه الاقسام والمصالح هناك قسم الحرائق والإنفجارات، قسم الطب الشرعي، قسم علم الإنسان والأسنان الشرعيين، قسم الإدارة مصلحة البيولوجيا الشرعية، مصلحة علم الإدمان...[2]

---

[1] خلدون عائشة، **الجريمة المعلوماتية في القانون الدولي والجزائري**، مجلة القانون والعلوم السايسية، جامعة زيان عاشور بالجلفة، المجلد9، العدد1، 2023، ص142.

[2] بلقاسم سميحة وحميد بوشوشة، **الجرائم الإلكترونية بعد جديد للإجرام في الجزائر وواقعها وآليات مجابهتها** مجلة العلوم الإنسانية لجامعة أم البواقي، المجلد10، العدد1، جوان 2023، ص551.

خلاصة الفصل الثاني:

يتضح لنا من خلال دراسة الفصل الثاني المعنون ب: " آليات التصدي للجريمة السيبرانية في التشريع الجزائري، هو أن المشرع الجزائري وكغيره من المشرعين قد سعى إلى التخلص من الإجرام المعلوماتي وذلك بوضعه لآليات قانونية وأخرى إجرائية لمجابهته، إذ تتمثل الآليات القانونية في حزمة من القوانين المواجهة للجريمة السيبرانية.

تنقسم القوانين المشار إليها إلى قوانين عامة على رأسها الدستور الجزائري الذي كفل حماية الحقوق الأساسية والحريات الفردية وضمن عدم انتهاك حرمة الإنسان الخاصة، والقانون الدولي العام الذي من خلاله أبرمت الجزائر الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، بالإضافة إلى قانون العقوبات الذي جرَم بعض الافعال المتصلة بالمعالجة الآلية للمعطيات نذكر منها جريمة التزوير المعلوماتي وتكون العقوبة على هذه الجرائم بالحبس والغرامة كعقوبة أصلية وبمصادرة الأجهزة وإغلاق المواقع والمحلات كعقوبة تكميلية، وكذلك قانون الإجراءات الجزائية والقانون الإداري، هذا الاخير الذي كان دوره في مجابهة الجريمة السيبرانية بإصدار جملة من القوانين أهمها القانون المتعلق بالتوقيع الإلكتروني، أما بالنسبة للقوانين الخاصة فنجد القانون المدني الذي ساهم من خلاله المشرع الجزائري في حماية حرمة الحياة الخاصة ونص على أن كل من تعرض لإعتداء في حرمته الخاصة جاز له المطالبة بالتعويض عن الضرر، وقد إبرمت الجزائر عدة اتفاقيات دولية ثنائية في هذا المجال من بينها 71 إتفاقية في التعاون القضائي في المجال الجزائي وتسليم المجرمين، إضافة إلى قانون الملكية الفكرية وقانون الملكية الصناعية وقوانين أخرى كقانون التأمينات والقانون 18-07 المتعلق بحماية الاشخاص الطبيعية في مجال المعطيات ذات الطابع الآلي.

وتتمثل الآليات الإجرائية في: آليات إجرائية وقائية والتي تنقسم بدورها إلى آليات إجرائية وقائية تقليدية وهي: مراقبة الإتصالات الإلكترونية، تفتيش المنظومة المعلوماتية و حجز المعطيات المعلوماتية، وآليات إجرائية وقائية مستحدثة وهي: التسرب، إعتراض المراسلات والمراقبة الإلكترونية، جمع وتسجيل المعطيات.

أما فيما يخص الهيئات التي وضعتها الدولة الجزائرية لمكافحة الجريمة السيبرانية فتتمثل في:الهيئة الوطنية، السلطة الوطنية، الوحدات التابعة لأسلاك الأمن الوطني و المعهد الوطني للأدلة الجنائية.

الخاتمة:

الخاتمة:

تعرضنا من خلال هذه الدراسة المستحدثة في مختلف الدول ألا وهي الجريمة السيبرانية، والتي تختلف عن الجرائم المعروفة.

حيث سماها المشرع الجزائري بالجرائم المتصلة بتكنولوجيا الإعلام والإتصال وقد تميزت هذه الجريمة بطبيعتها الخاصة التي تجسدت في خصائصها على أنها جريمة عابرة للحدود باستخدام الحاسوب وكذلك سرعة التنفيذ ، وصعوبة الإكتشاف والإثبات.

لتحقيق هذه الجريمة وكغيرها من الجرائم ينبغي توافر أركانها الركن الشرعي والركن المادي، بالإضافة إلى الركن المعنوي.

وقد تأخذ الجريمة السيبرانية عدة أشكال وصور كالتجسس السيبراني وسرقة المعلومات وتزويرها والإرهاب السيبراني.

وللقيام بهذه الأفعال غير المشروعة التي تمس الحاسب الآلي، لابد من أن يكون شخص يتسم بسمات خاصة عن سمات المجرم العادي، والمعرفة الكافية في المجال التكنولوجي والسيبراني و الذي يسمى بالمجرم السيبراني الذي يتميز بالذكاء والمهارة والسلطة، والذي تصنف فئاته من الأكبر خطرا وهي فئة القراصنة الخبيثون والجماعات الإرهابية إلى الفئات الأقل خطورة وهي فئة القراصنة وأصحاب المشاكل الشخصية وفئة الأطفال والمراهقين.

ولكل من هذه الفئات أو المجرمين باعث دفعه إلى ارتكاب جرمه، فهناك من يتجه نحو ارتكاب هذا الإجرام من أجل رغبته الشديدة في التعلم، وهناك من تكون أسبابه مادية كالرغبة في كسب المال، وكذا من أجل المتعة والتحدي وحتى يمكن أن يكون الدافع هو العقيدة.

ولمكافحة الجريمة السيبرانية كرس المشرع الجزائري مجموعة من الإستراتيجيات والآليات القانونية (الموضوعية) والإجرائية لمواجهتها، إذ تتمثل الآليات القانونية في حزمة من القوانين تنقسم بدروها إلى قوانين عامة وأخرى خاصة، أما بالنسبة للآليات الإجرائية فهي الأخرى تنقسم إلى قسمين: الآليات الإجرائية التقليدية والآليات الإجرائية المستحدثة.

أما فيما يخص الهيئات التي وضعها مشرعنا الجزائري تتمثل في: الهيئة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، السلطة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، الوحدات التابعة لأسلاك الأمن الوطني وأخيرا المعهد الوطني للأدلة الجنائية.

من خلال ما سبق توصلنا إلى مجموعة من النتائج التالية:

– لم يضع المشرع الجزائري قانون خاصا بالجريمة السيبرانية للتحكم فيها بصرامة.

– لم يستقر المشرع الجزائري على استخدام مصطلح واحد للدلالة على الجرائم السيبرانية حيث سماها بموجب القانون 04-15 المتضمن قانون العقوبات بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، ثم بموجب القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال استخدم مصطلح الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

– تتميز الجريمة السيبرانية عن غيرها من الجرائم بالطبيعة الخاصة التي تعدو عليها سواءا تعلقت بذاتية هذه الجريمة أو تعلقت بخصوصية المحل الذي يقع عليه الإعتداء في ارتكاب هاته الجرائم.

– تتم الجريمة السيبرانية خارج الواقع المادي الملموس على غرار الجرائم الأخرى التي تقوم في بيئة تقليدية، كما أنها تختلف عنها في صعوبة الكشف عنها واثباتها نظرا لخفيتها وسرعة تنفيذها.

– إستحدث المشرع الجزائري قسما خاصا بالمساس بأنظمة المعالجة الآلية للمعطيات، غير أنه اكتفى بالنص على جرائم محددة وترك المجال للنصوص العقابية التقليدية في بعض الجرائم الأخرى كجرائم الغش السيبراني والسب والقذف الإلكترونيين.

– استحداث المشرع الجزائري لتدابير وقائية خاصة بالجريمة السيبرانية أهمها: المراقبة الإلكترونية و تفتيش المنظومة المعلوماتية وحجزها، بالإضافة إلى استحداثه لآليات وقائية مستحدثة بموجب قانون الإجراءات الجزائية، خاصة اعتراض المراسلات و جمع وتسجيل المعطيات.

– كما استحدث قوانين تدعم مكافحة الجريمة السيبرانية أهمها: القانون 18–04 المحدد للقواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية والقانون 18–07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

إنطلاقا من النتائج السابقة نتوصل إلى هذه التوصيات:

– وضع قانون خاص بالجريمة السيبرانية، مع ضرورة وضع تقنين يُعنى بتوحيد مفهوم المصطلحات ذات الصلة بالجريمة السيبرانية.

– ضرورة توحيد تسمية الجريمة وجعلها تواكب التسميات العالمية بالإشارة لها باسم الجريمة السيبرانية بدلا من التسمية الحالية(الجرائم المتصلة بتكنولوجيات الإعلام والإتصال).

– إن التقدم التكنولوجي وانتشار وسائل الإتصال الحديثة يحتم على المشرع الجزائري تعديل النصوص القانونية.

– عدم إهمال حماية البيانات والخصوصيات ويتم ذلك بنشر الوعي الرقمي بين المستخدمين وكيفية تفادي التعدي على بياناتهم الشخصية وتعريفهم بحجم الخطورة التي ترصدهم في حالة عذم اتخاذ الإحتياطات الوقائية اللازمة.

– تشجيع الجامعات والمراكز البحثية على تنظيم العديد من الندوات التي تهتم بالتعرف على هذه الجرائم ومعالجتها وكيفية مكافحتها.

– الدعوة إلى إدراج تخصص جديد في تخصصات الدراسة ألا وهو تخصص القانون الجنائي، واستحداث مقاييس جديدة كمقياس القانون الجنائي السيبراني.

– تدعيم الباحثين بالدعم المادي والمعنوي لإجراء المزيد من البحوث و الدراسات حول الإجرام السيبراني وكيفية مجابهتها.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولا: قائمة المصادر

النصوص القانونية

- الأمر 66-156، المؤرخ في 13 صفر 1486 الموافق ل8 يونيو 1966 يتضمن قانون العقوبات، الجريدة الرسمية، العدد11، المؤرخة في 11 يونيو1966.

- الأمر 03-05 المؤرخ في 19 جويلية 2003 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية ، العدد 44،المؤرخة في 23 يوليو 2003.

- الأمر 06-03 المؤرخ في 19 جويلية 2003 المتعلق بالعلامات، الجريدة الرسمية العدد 44، المؤرخة في 23 يوليو 2003.

- الأمر 03-07 المتلعق ببراءة الإختراع، المؤرخ في 19 جمادى الأولى 1424 الموافق ل 19 يوليو 2003، الجريدة الرسمية، العدد44، المؤرخة في 23 يوليو 2003 .

- القانون 04-15، المؤرخ في 27 رمضان 1425 الموافق ل 8 نوفمبر 2004 المتضمن تعديل قانون العقوبات،الجريدة الرسمية، العدد71 ، المؤرخة في 11 نوفمبر 2004.

- القانون 08-01، المؤرخ في الموافق ل 23 جانفي 2008 المتعلق بالتأمينات الإجتماعية، الجريدة الرسمية، العدد4، المؤرخة في 27 يناير 2008.

- القانون 09-04، المؤرخ في 14 شعبان 1430 الموافق ل 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها الجريدة الرسمية، العدد 47، المؤرخة في 16 غشت 2009.

- القانون العضوي رقم 12-05 المؤرخ 1433 الموافق ل 12 يناير 2012 المتعلق بالإعلام الجريدة الرسمية، العدد2،المؤرخة في 15 يناير 2012.

- القانون 15-03 المؤرخ في 11 ربيع الثاني عام 1436 الموافق ل 1 فبراير 2015 المتعلق بعصرنة العدالة الجريدة الرسمية، العدد6، المؤررخة في 3 فبراير 2015.

- المرسوم الرئاسي 15-261، المؤرخ في 24 ذي الحجة 1436 الموافق ل 8 أكتوبر 2015 ،يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنزلوجيات الإعلام والإتصال، الجريدة االرسمية، العدد53، الموؤرخة في 8 أكتوبر 2015.

- القانون 16-01، المؤرخ في 16 جمادى الأولى 1437 الموافق ل 6 مارس 2016 ستضمن التعديل الدستوري، الجريمة الرسمية، العدد 14، المؤرخة في 7 مارس 2016.

- القانون 18-04، المؤرخ في 24 شعبان 1439 الموافق ل 10 مايو 2018 المحدد القواعد العامة المتعلة بالبريد و الإتصلات الإلكترونية، الجريدة الرسمية، العدد27، المؤرخة في 13 مايو 2013.

- التعديل الدستوري 2020، المؤرخ في 15 جمادى الأولى 1442 الموافق ل30 ديسمبر 2020، يتعلق بإصدار التعديل الدستوري، الجريدة الرسمية، العدد82 المؤرخة في 30 ديسمبر 2020.

- الأمر 21-09 المؤرخ في 27 شوال 1442 الموافق ل8 يوليو 2021 المتعلق بحماية المعلومات والوثائق الإدارية، الجريدة الرسمية، العدد91،المؤرخة في 5 ديسمبر 2021.

ثانيا: قائمة المراجع

1/ الكتب:

- المصمودي محمد بن أحمد بن علي، **الجرائم المعلوماتية خصائصها وكيفية التصدي لها ومواجهتها قانونيا**، د.ط، دار المنظومة، المممكة العربية السعودية 2015.

- أيمن عبد الله فكري، **الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية و الأجنبية**، الرياض، الطبعة الأولى، مكتبة القانون والإقتصاد، 2014.

- خالد محمد إبراهيم، **الجرائم المعلوماتية**، الطبعة الثانية، دار الفكر الجامعي الإسكندرية 2010.

- صدام حسين ياسين العابدي، **جرائم الأنترنت وعقوباتها في الشريعة الإسلامية والقوانين الوضعية**، د.ط المركز العربي للتوزيع، القاهرة،2011.

- غانم مرضى الشمري، **الجرائم المعلوماتية**، ماهيتها، خصائصها، وكيفية التصدي لها قانونيا، الطبعة الأولى، الدار العلمية الدولية للنشر والتوزيع،عمان،2016.

- محمد علي سكيكر، **الجريمة المعموماتية وكيفية التصدي لها**، د.ط، دار الجمهورية لمصحافة، د.م، 2010.

- نائلة عادل محمد فريد قورة، **جرائم الحاسب الآلي الإقتصادية**، دارسة نظرية تطبيقية الطبعة الأولى، منشوارت الحلبي الحقوقية،القاهرة،2005.

- نهلا عبد القادر مومني، **الجرائم المعلوماتية**، الطبعة الأولى، دار الثقافة للنشر والتوزيع،عمان، 2010.

- يعيش تمام شوقي، **الجريمة المعلوماتية**، دارسة تأصيلية مقارنة، الطبعة الأولى،مطبعة الرمال، الجزائر، 2019.

2/ الرسائل الجامعية :

أ) أطروحات الدكتوراه :

- العوفي دليلة، **آليات محاربة الجريمة المعلوماتية**، أطروحة دكتوره، كلية العلوم و الإعلام والإتصال، جامعة الجزائر3، 2019-2020.

- سلامي لخضر، الجريمة الإلكترونية عبر مواقع التواصل الإجتماعي، أطروحة دكتوره، كلية الحقوق، جامعة وهران2، 2022-2023.

- شنيتر خضرة، الآليات القانونية لمكاقحة الجريمة الإلكترونية، أطروحة دكتوره ،كلية الحقوق والعلوم السياسية، جامعة أحمد درارية-أدرار-2021.

- عميمر عبد القادر، آليات إثبات الجريمة المعلوماتية في التشريع الجزائري،دراسة مقارنة، أطروحة دكتوره في القانون العام، كلية الحقوق، جامعة الجزائر1،2019-2020.

- غلاب فايز محمد راجح، الجرائم المعلوماتية في القانون الجزائري واليمني أطروحة دكتوره، كلية الحقوق، جامعة الجزائر1، 2009-2010.

ب) رسائل (شهادات)الماجيستير :

- بن عقون حمزة، **السلوك الإجرامي للمجرم المعلوماتي**، شهادة ماجيستير في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2011-2012.

- بوخبزة عائشة، **الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري** شهادة ماجيستر، كلية الحقوق، جامعة وهران، 2012-2013.

- سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في التشريع الجزائري** شهادة ماجيستر في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر-باتنة-2012-2013.

- سوير سفيان، **الجرائم المعلوماتية**، شهادة ماجيستر في العلوم الجنائية وعلم الإجرام كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد-تلمسان-2010-2011.

- صغير يوسف، **الجريمة المرتكبة عبر الأنترنت**، شهادة ماجيستر، كلية الحقوق والعلوم السياسية، جامعة مولود معمري-تيزي وزو-2013.

- طرشي نورة، **مكافحة الجريمة المعلوماتية**، شهادة الماجيستر في القانون الجنائي كلية الحقوق ، جامعة الجزائر1، 2011-2012.

- عبد الله بن حسين آل حجراف القحطاني، **مهارات التحقيق الجنائي في الجرائم المعلوماتية**، رسالة الماجيستر في قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، 2014.

- قارة أمال، **الجريمة المعلوماتية**، شهادة ماجيستر، كلية الحقوق ، جامعة الجزائر1 2001-2002.

ج) مذكرات الماستر:

- حشمان عمار، **الجريمة المعلوماتية في التشريع الجزائري**، مذكرة ماستر، كلية العلوم الإقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرياح-ورقلة- 2018_2019.

- عقباش بريزة ومبارك حنان، **آليات مواجهة الجريمة المعلوماتية في التشريع الجزائري** مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي-برج بوعريريج-2021-2022.

3/ المقالات:

- بوراس نادية، **الإستراتيجيات الوطنية لمواجهة جرائم المساس بأنظمة المعالجة الآلية للمعطيات**، مجلة الحقوق والحريات، جامعة محمد لمين دباغين، المجلد10 العدد3، 2023.

- بوزنون سعيدة، **مكافحة الجريمة المعلوماتية في التشريع الجزائري**، مجلة العلوم الإنسانية، جامعة الإخوة منتوري-قسنطينة- المجلد ب، العدد 52، ديسمبر 2019.

- بوضياف أسمهان، **الجريمة المعلوماتية والإجراءات التشريعية لمواجهتها في الجزائر** مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، د.م سبتمبر2018.

- بلقاسم سميحة وحميد بوشوشة، **الجريمة المعلوماتية بعد جديد للإجرام في الجزائر واقعها وآليات مكافحتها**، مجلة العلوم الإنسانية لجامعة أم البواقي، المجلد10، العدد1 جوان 2023.

- بن مالك أحمد، **خصوصية الجريمة المعلوماتية وسبل مكافحتها في التشريع الجزائري**، المجلة الجزائرية للحقوق والعلوم السياسية، جامعة تمنغست، المجلد8 ،العدد1 2023.

- بوهرين فتيحة، **الجريمة المعلوماتية في التشريع الجزائري**، مجلة الحقوق والعلوم الإنسانية، جامعة قسنطينة2، المجلد14، العدد4، 2021.

- حوالف حليمة و مهاجي فاطمة الزهراء، **معالم الجريمة المعلوماتية في القانون الجزائري**، مجلة البحوث القانونية والسياسية، جامعة تلمسان، المجلد3، العدد6 2021.

- خرشف فاطمة ولزار سميرة، **الإطار القانوني والمفاهيمي لمواجهة الجرائم السيبرانية** مجلة سيسيولوجيا الجريمة، مخبر الجريمة والإنحارف بين الثقافة والتمثلات الإجتماعية د.م، د.ع، د.ت.

- خلدون عائشة، **الجريمة المعلوماتية في القانون الدولي والقانون الجزائري**، مجلة القانون والعلوم السايسية، جامعة زيان عاشور-الجلفة- المجلد9 ، العدد1، 2023.

- رحموني محمد، **خصائص الجريمة الإلكترونية ومجالات استخدامها**، مجلة الحقيقة جامعة أحمد دراية-أدرار- د.م، العدد41، د.ت.

- زناتي محمد السعيد ويمينة جواج، **أثر الجرائم السيبرانية على الحريات الفردية** المجلة الإفريقية للدراسات القانونية والسياسية، جامعة عبد الحميد بن باديس الملجد6، العدد1 2016.

- شويرب جيلالي ومراد فائزة، **الآليات الدولية الوطنية لمكافحة الجريمة السيبرانية** مجلة الدراسات القانونية والسياسية، مخبر السيادة والعولمة، جامعة يحي فارس -المدية- المجلد 9، العدد2، جوان2023.

- عمراني أحمد، **الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها في التشريع الجزائري والتشريع المقارن**، مجلة الحضارة الإسلامية، جامعة وهران المجلد525، العدد15، ماي 2012.

- عميمور راضية، **الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري**، المجلة الأكاديمية للبحوث القانونية والسايسية، مخبر الحقوق والعلوم السياسية المجلد 6، العدد1 2022.

- غربي بشرى، **خصوصية المجرم المعلوماتي ودوافعه**، مجلة نوميروس الأكاديمية جامعة أبو بكر بلقايد–تلمسان– المجلد2، العدد2، 2021.

- غريب حكيم، **الإرهاب السيبراني والأمن الدولي: التهديدات العالمية الجديدة وأساليب المواجهة**، المجلة الجزائرية للدراسات السياسية، المدرسة الوطنية العليا للدراسات السياسية، المجلد5، العدد2.

- فيروز قاسحي، **الجريمة الإلكترونية عبر مواقع التواصل الإجتماعي**، مجلة الرسالة للدراسات والبحوث الإنسانية، جامعة الجزائر3، المجلد7،العدد8 فيفري2023.

- قطاف سليمان وبوقرين عبد الحليم، **مواجهة الجرائم السيبرانية في ضوء الإتفاقيات الدولية**، مجلة البحوث القانونية والإقتصادية، مخبر البحث في الحقوق والعلوم السياسية المجلد 5، العدد2، 2022.

- ماينو الجيلالي وعروس كوثر، **الجريمة السيبرانية في صورها المستحدثة**، مجلة القانون والتنمية، مخبر القانون والتنمية، المجلد 4، العدد1، جويلية2023.

- مجدوب نوال، **الآليات الإجرائية للكشف عن الجريمة المعلوماتية**، مجلة البحوث القانونية والإقتصادية، المركز الجامعي مغنية، المجلد 6، العدد3، 2023.

- مهدي رضا، **الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري**، مجلة إيليزا للبحوث والدراسات، جامعة محمد بوضياف–المسيلة– المجلد6، العدد2، 2021.

- ناجية شبخ، **حول مكافحة الجريمة الإلكترونية في التشريع الجزائري**، مجلة العلوم القانونية والسايسية، جامعة مولود معمري –تيزي وزو– المجلد9، العدد2 جوان 2018.

4/ المداخلات العلمية:

- خلف فاروق، **الآليات القانونية لمكافحة الجريمة المعلوماتية**، الملتقى الوطني" الجريمة المعلوماتية بين والوقاية والمكافحة"، جامعة محمد خيضر –بسكرة–د.ت.

- فشار عطا الله، **مواجهة الجريمة العلوماتية في التشريع الجزائري**، مداخلة مقدمة إلى الملتقى المغاربي حول القانون والمعلوماتية ، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور بالجلفة، 2009.

5/ القواميس:

- منير البعلبكي، المورد قاموس إنجليزي–عربي، دار العلم للملايين، د.ط، بيروت 2022.

6/ المراجع الأجنبية:

- sunil.c.pawer,dr.s.mente, cyber crime,cyber space and effects of cyber crime, international journal of scientifics research in computer science engineering and information technology, Punyashlok Ahilyadevi Holkar Solapur University Solapur, Maharashtra, India volume7, issue1, 2021, p211.

-mohamed chawki, achraf darwish, ,cybercrime digitalforensics and jurisdiction,internatinal association of cybercrime,france, 593, 2015, p17.

فهرس المحتويات

فهرس المحتويات

العنوان	الصفحة
شكر وتقدير	/
إهداء	/
مقدمة	1
الفصل الأول: ماهية الجريمة السيبرانية	6
المبحث الأول: الإطار المفاهيمي للجريمة السيبرانية	7
المطلب الأول: مفهوم الجريمة السيبرانية	7
الفرع الأول: تعريف الجريمة السيبرانية	7
الفرع الثاني: خصائص الجريمة السيبراينة	12
الفرع الثالث: الطبيعة القانونية للجريمة السيبرانية	14
المطلب الثاني: صور الجريمة السيبرانية	16
الفرع الأول: التزوير المعلوماتي (السيبراني)	16
الفرع الثاني: التجسس السيبراني	17
الفرع الثالث: سرقة المعلومات	17
الفرع الرابع: الإرهاب السيبراني	18
المبحث الثاني: الإطار القانوني للجريمة السيبرانية	18
المطلب الأول: أركان الجريمة السيبرانية	19
الفرع الأول: الركن الشرعي	19
الفرع الثاني: الركن المادي	20
الفرع الثالث: الركن المعنوي	20
المطلب الثاني: المجرم السيبراني	21
الفرع الأول: تعريف المجرم السيبراني	21
الفرع الثاني: سمات المجرم السيبراني	22

الفرع الثالث: فئات المجرم السيبراني	24
الفرع الرابع: دوافع ارتكاب الجريمة السيبرانية	26
الفصل الثاني: آليات التصدي للجريمة السيبراينة في التشريغ الجزائري	32
المبحث الأول: الآليات القانونية لمكافحة الجريمة السيبراني في التشريع الجزائري	33
المطلب الأول: مكافحة الجريمة السيبرانية في القوانين العامة	33
الفرع الأول: مكافحة الجريمة السيبرانية بموجب الدستور	33
الفرع الثاني: القانون الدولي العام	34
الفرع الثالث: قانون العقوبات وقانون الإجراءات الجزائية	35
الفرع الرابع: القانون الإداري	37
المطلب الثاني: مكافحة الجريمة السيبرانية في القوانين الخاصة	39
الفرع الأول: القانون المدني	39
الفرع الثاني: القانون الدولي الخاص	40
الفرع الثالث: قانون الملكية الفكرية	42
الفرع الرابع: قانون الملكية الصناعية	43
المبحث الثاني: الآليات الإجرائية لمكافحة الجريمة السيبراينة في التشريع الجزائري	48
المطلب الأول: الآليات الإجرائية الوقائية لمكافحة الجريمة السيبرانية في التشريع الجزائري	48
الفرع الأول: الآليات الإجرائية الوقائية التقليدية	48
الفرع الثاني: الآليات الإجرائية الوقائية الحديثة	52
المطلب الثاني: الآليات المؤسساتية لمكافحة الجريمة السيبرانية في التشريع الجزائري	56
الفرع الأول: الهيئة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال	56

الفرع الثاني: السلطة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال	57
الفرع الثالث: الوحدات التابعة لأسلاك الأمن الوطني	59
الفرع الرابع: المعهد الوطني للأدلة الجنائية وعلم الإجرام	60
الخاتمة	65
قائمة المصادر والمراجع	70
فهرس المحتويات	80

ملخص:

تعد الجرائم السيبرانية من الأنماط الإجرامية المستحدثة التي أفرزتها تكنولوجيات الإعلام والإتصال الحديثة، وذلك للتزايد المطرد في القدرات التكنولوجية، فهي تختلف تماما عن الجرائم التقليدية من حيث طبيعتها، خصائصها، أنواعها ووسائل تنفيذها.

هذا ما استدعى تدخل المشرع الجزائري لوضع حد لهذا التنامي الخطير في ميدان الإجرام السيبراني، عن طريق سن نصوص قانونية تجرم وتعاقب الأفعال التي تشكل اعتداءا أو تهديدا للأمن السيبراني، مع استحداث هيئات تعمل من أجل مكافحة هذا النوع من الإجرام.

كيف عالج المشرع الجزائري أحكام الجريمة السيبرانية في مفهومها وكيفية مكافحتها؟

Summary :

Cybercrime is one of the new criminal patterns craeted by information and communication technologies because of the excessive increase in technological capabilities, it differs from traditional crimes in nature, characteristics and means of inmplementation.

This is why Algeria's legislature has intervened to put an end to this dangerous growth in cybercrime by enacting legal texts that hounour and punish acts that constitute an attack on threat to cybersecurity, while establishing bodies to combat this type of crime.

How did Algerian legislators adress the provisions of cybercrime in their concepts and haw to combat them?