

جامعة الشاذلي بن جديد - الطارف
كلية الحقوق والعلوم السياسية
قسم الحقوق



الجمهورية الجزائرية الديمقراطية
الشعبية
وزارة التعليم العالي والبحث العلمي

مذكرة بعنوان:

المسؤولية الجزائية عن الجرائم الالكترونية في التشريع الجزائري

مذكرة مقدمة لإستكمال متطلبات الحصول على شهادة ماستر أكاديمي في
الحقوق تخصص: قانون جنائي وعلوم جنائية

إشراف الأستاذة : غرايبيّة خولة

إعداد الطالب : بوطوطن عبد الرؤوف

الصفة	الهيئة المستخدمة	الرتبة	الإسم واللقب
رئيسا	الشاذلي بن جديد - الطارف	أستاذ محاضر. أ	د بوعزيز عبد الوهاب
مشرفا ومقررا	الشاذلي بن جديد - الطارف	أستاذ محاضر. ب	د غرايبيّة خولة
ممتحنا	الشاذلي بن جديد - الطارف	أستاذ محاضر. ب	د سعدون بلقاسم

السنة الجامعية: 2026/2025

جامعة الشاذلي بن جديد - الطارف
كلية الحقوق والعلوم السياسية
قسم الحقوق



الجمهورية الجزائرية الديمقراطية
الشعبية
وزارة التعليم العالي والبحث العلمي

مذكرة بعنوان:

المسؤولية الجزائية عن الجرائم الالكترونية في التشريع الجزائري

مذكرة مقدمة لإستكمال متطلبات الحصول على شهادة ماستر أكاديمي في
الحقوق تخصص: قانون جنائي وعلوم جنائية

إشراف الأستاذة: غرايبيّة خولة

إعداد الطالب : بوطوطن عبد الرؤوف

الصفة	الهيئة المستخدمة	الرتبة	الإسم واللقب
رئيسا	الشاذلي بن جديد - الطارف	أستاذ محاضر. أ	د بوعزيز عبد الوهاب
مشرفا ومقررا	الشاذلي بن جديد - الطارف	أستاذ محاضر. ب	د غرايبيّة خولة
ممتحنا	الشاذلي بن جديد - الطارف	أستاذ محاضر. ب	د سعدون بلقاسم

السنة الجامعية: 2026/2025

شكر

الحمد لله حمدا كثيرا حتى يبلغ الحمد منتهاه، والصلاة والسلام على أشرف مخلوق أناره الله بنوره واصلحناه

أتقدم بجزيل الشكر إلى

أستاذتي (غرايبيّة خولة) التي أشرفت على هذا العمل ولم تبخل عليّ بأي جهد طيلة إشرافها

وإلى كل أساتذة، عمال و طلبة كلية الحقوق والعلوم السياسية بجامعة الشاذلي بن جديد الطارف

ولكل من ساهم من قريب أو بعيد في إتمام هذا العمل العلمي المتواضع.

الإهداء

أهدي هذا العمل المتواضع إلى

والدي الكريمين الأب الغالي و أمي العزيزة

و جديّ "سي - حمد" و "علاوة" (رحمة الله عليهم) جدتي الحبيبة "يايا"

جدتي الزهرة ، زوجتي الغالية و أولادي وإخوتي وأخواتي الأعزاء و كامل عائلتي فردا
فردا

و إلى كل طلبة كلية الحقوق والعلوم السياسية بجامعة الشاذلي بن جديد - الطارف -

دفعه 2026

و لكل من يطلب العلم من المهد إلى اللحد.

عبد الرؤوف

استمارة تعهد

الجمهورية الجزائرية الديمقراطية الشعبية République Algérienne Démocratique et Populaire		Minister de L'enseignement Supérieur Et de La Recherche Scientifique Université el tarf Faculté de Droit et des Sciences Politiques Département de Droit
وزارة التعليم العالي والبحث العلمي جامعة الشاذلي بن جديد الطارف كلية الحقوق والعلوم السياسية قسم الحقوق		

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

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية

أنا الممضي أدناه،

السيد (ة): بوملو من عبد الرؤوف

الحامل لبطاقة التعريف الوطنية رقم: 117775041

الصادرة بتاريخ: 2020-03-10

عن دائرة: سجى عمار - عنابة

المسجل بقسم: الحقوق والمكلف بإتجاز مذكرة تخرج ماستر

عنوانها: المسؤولية الجنائية عن الجرائم الإلكترونية

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

التاريخ: 2020/06/10

امضاء المعني





ترجع جذور فكرة الجريمة إلى بداية نشأة الإنسان نفسه، إذ ارتبط وجودها بوجوده منذ اللحظات الأولى للتاريخ البشري. وقد اضطلع القضاء بمسؤولية إقامة العدل منذ فجر البشرية، حيث قرر لكل جريمة عقوبة، وجعل من مهمة التجريم والعقاب اختصاصاً حصرياً للمشرع. حيث سعى هذا الأخير إلى مواكبة تطور السياسة الجنائية من خلال تطوير العقوبات، فلم تعد العقوبة موحدة تطبق على جميع الجناة، ولا جامدة تطبق على كل الأفعال، بل أصبحت تتدرج في نوعها ومقدارها بما يتلاءم مع جسامة الجريمة وخطورة مرتكبها.

و لقد شهد العالم تطوراً كبيراً في شتى المجالات والميادين خاصة المجال التكنولوجي، فمن بين هذه التطورات نجد تكنولوجيا وسائل الإعلام والاتصال، فبالرغم من حداثة العهد بهذه التكنولوجيا في مجتمعنا، إلا أنها ودون منازع استطاعت أن تفرض وجودها في حياة كل فرد، فقد ساهم التطور المعاصر في تبادل الأفكار والمعلومات إلى إحداث سلوكيات مقبولة وغير مقبولة، في جميع المجالات التي تتعلق بالفرد والمجتمع، وقد يؤدي الاستخدام المفرط لهذه المواقع، إلى التأثير بالثقافات المفتوحة، وانتشار الجرائم الإلكترونية، أو كما تسمى أيضاً جرائم الانترنت، أو جرائم الكمبيوتر، أو جرائم المعلوماتية. أو الجرائم السيبرانية، التي انتشرت في الآونة الأخيرة وأصبحت ظاهرة جديدة بالنظر والاعتبار، والتي تتم عن طريق التكنولوجيا، وأصبحت ظاهرة تخترق المجتمع وتهدد دعائمه وأمنه.¹

أهمية الدراسة:

تبرز أهمية هذا البحث، في كونه يركز على الجرائم الإلكترونية باعتبارها جرائم جديدة أين لا يمكن أن تطبق عليها نفس الآليات والإجراءات المتبعة في الجرائم التقليدية، مما يفرض على المشرع وضع أساليب وآليات جديدة في البحث والتحري عنها.

¹ الجريمة المعلوماتية في التشريع الجزائري، عمار حشمان، مذكرة ماستر، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرباح وزقلة، سنة 2019.

أسباب اختيار الموضوع:

تعددت أسباب اختيارنا لهذا الموضوع بين أسباب ذاتية ، وموضوعية .

الأسباب الذاتية:

والتي تتمثل في إهتمامنا بمجال الجريمة الإلكترونية التي تندرج ضمن تخصصنا في الماستر القانون الجنائي والعلوم الجنائية، وكونها تدخل ضمن المجال المهني ، إضافة إلى الرغبة الكبيرة في الإثراء المعرفي الخاص بهذا الصنف من الجرائم التي انتشرت في الآونة الأخيرة انتشارا كبيرا داخل مختلف دول العالم عامة، و في الجزائر خاصة.

الأسباب الموضوعية:

أما عن الأسباب الموضوعية فتكمن في طرح موضوع دراستنا للعديد من الإشكالات القانونية نظرا لكثرة استخدام التكنولوجيا والإنترنت في حياتنا اليومية، كما أنها تندرج تحت فئة الجرائم السيبرانية وتشمل عدة جرائم الاحتيال الإلكتروني، السرقة الإلكترونية، التجسس و اختراق النظام الإلكتروني وغيرها من الجرائم الالكترونية، والتي لا بد من الوقوف عليها نظرا لحدثة الموضوع ولتجريم الأفعال والإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات وكذا القواعد الإجرائية الحديثة التي جاء بها قانون الإجراءات الجزائية المعدل والمتمم، والقانون رقم 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. مع ذكر الآليات التي انتهجها المشرع الجزائري لمكافحتها .

الدراسات السابقة:

ان موضوع المسؤولية الجزائية عن الجريمة الالكترونية هو من المواضيع الحديثة ، مما أدى الى قلة الدراسات المتعلقة به ، والتي يمكن أن نذكر منها :

- **صيلع سعد**: آليات مكافحة الجريمة الالكترونية في التشريع الجزائري . وهي أطروحة دكتوراة الطور الثالث (ل.م.د) في تخصص القانون الجنائي، معهد الحقوق والعلوم السياسية ، المركز الجامعي

مرسلي عبد الله، تيازة ، السنة 2024-2025، وطرح الباحث من خلاله اشكالية : ما مدى نجاعة السياسة الجنائية المتخذة من طرف المشرع الجزائري لمكافحة الجريمة الالكترونية .

-**راضية زرقيني**: الحماية الجزائية للمعطيات الشخصية، وهي أطروحة دكتوراة علوم في تخصص القانون العام ، كلية الحقوق والعلوم السياسية ، جامعة الشهيد حمة لخضر ، الوادي، سنة 2021-2022. وطرح الباحث اشكالية : مامدى كفاية الوسائل القانونية التي اعتمدها المشرع الجزائري في مواجهة الجرائم الماسة بالمعطيات ذات الطابع الشخصي.

-**قراوي كلثوم** : جريمة الاحتيال الالكتروني، أطروحة لنيل دكتوراه علوم في القانون العام ، تخصص قانون جنائي والعلوم الجنائية ، كلية الحقوق ، جامعة الجزائر 1، السنة الجامعية 2024-2025. طرحت اشكالية : هل الأحكام الموضوعية والقواعد الاجرائية المنصوص عليها في القانون الجنائي الجزائري كافية لاحتواء جريمة الاحتيال الالكتروني واثباتها أمام القاضي الجنائي.

-**أومدور رجاء** : خصوصية التحقيق في مواجهة الجرائم المعلوماتية ، أطروحة دكتوراه الطور الثالث، ل.م.د ، تخصص القانون الخاص، كلية الحقوق والعلوم السياسية ، جامعة محمد البشير الابراهيمي ، برج بوعريج، سنة 2020-2021 . وطرحت اشكالية : هل كرس المشرع الجزائري أحكاما قانونية تتلاءم مع خصوصية التحقيق لضمان فاعليته في مواجهة الجرائم المعلوماتية والحد من آثارها.

صعوبات الدراسة:

لقد واجهنا خلال دراسة موضوع مذكرتنا بعض الصعوبات، تمثلت أساسا في نقص المراجع المتخصصة في الجريمة الإلكترونية وخاصة تلك التي تدرس الإجراءات المستحدثة للتحقيق في هذا النوع من الجرائم ، بالإضافة إلى ندرة المراجع التي تعنى بالمسؤولية الجنائية عن الجرائم الالكترونية ، ضف إلى ذلك صعوبة البحث في هذا الموضوع لاتصاله بالجانب العلمي التقني الذي يتعلق بالمعطيات الآلية ، خاصة وأن الاجتهاد القضائي محف نوعا ما بخصوص هذا النوع من الجرائم.

إشكالية الدراسة:

تتميز الجريمة الالكترونية بخصائص وصفات تميزها عن الجرائم الأخرى تجعلها صعبة الإثبات ، لعدم وجود آثار مادية تقليدية ، إضافة إلى كونها لا تعترف بالحدود المكانية و الزمنية ، وهذا ما جعل الدول تسعى جاهدة لوضع منظومة قانونية وقضائية فعالة لمحاربة هذا النوع من الجرائم ، والتي سعت الجزائر جاهدة عبر مختلف الإصلاحات مواكبة تطورها السريع وانسيابها داخل المجتمع الجزائري، والتي كان أهمها القانون 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والتي واصلت عبر إصلاحاتها وضع قوانين أخرى كان آخرها مجموعة من المراسيم الرئاسية سنة 2020 .

لذلك ارتأينا من خلال دراستنا هذه طرح الإشكالية الرئيسية التالية :

هل استطاع المشرع الجزائري وضع إطار قانوني متكامل يضمن قيام المسؤولية الجنائية عن الجرائم الالكترونية، أم أن خصوصية هذا النوع من الجرائم تفرض إعادة النظر في بعض القواعد التقليدية للمسؤولية الجنائية ؟

و يتفرع عنها التساؤلات الفرعية التالية:

1- فما هي الآليات المستخدمة لمكافحة الجرائم الالكترونية وما مدى نجاعتها؟

2- وماهي مختلف الصور الجرمية للجريمة الالكترونية وما هي شروط المساءلة الجزائية عنها؟

منهج الدراسة

إن طبيعة موضوع المسؤولية الجنائية عن الجرائم الالكترونية تقتضي استخدام المنهج الوصفي التحليلي ، حيث تطرقنا إلى وصف ظاهرة الجريمة الالكترونية مع ذكر مفاهيمها العامة و خصائصها والتطرق للآليات الموضوعية والإجرائية التي اعتمدها المشرع الجزائري لمكافحة الجريمة الالكترونية .

كما اعتمدنا المنهج التحليلي للتطرق بالتحليل والنقاش من أجل تحليل وتفسير مختلف النصوص القانونية المتعلقة بتعريف و عقوبات الجرائم الالكترونية.

ولمحاولة الإجابة على إشكالية هذه الدراسة ، قسمنا الدراسة إلى فصلين ، الفصل الأول تناول الإطار المفاهيمي للجريمة الالكترونية مع ذكر مختلف خصائصها وآليات مكافحتها في التشريع الجزائري، في حين تناول الفصل الثاني صور المساءلة الجزائية عن الجرائم الالكترونية ، كما قد قسم كل منهما إلى مباحث و مطالب وفروع ، للإلمام بأغلبية المشكلات البحثية المرتبطة بموضوع دراستنا.



الفصل الأول:

الإطار المفاهيمي

للجريمة الإلكترونية

لقد شهد العالم مؤخرا انتشار استخدام التكنولوجيا وتطور عالم الاتصالات مما أدى إلى ظهور الجريمة الإلكترونية، حيث شهدت طرق تنفيذ هاته الجرائم مع ازدياد الاعتماد على الأنظمة الرقمية تطورا وتسارعا رهيبا، مما جعل المجرمين يستغلون الثغرات الأمنية في الشبكات والأنظمة لتحقيق أهداف ربح مالية أو سياسية أو ذات دوافع أخرى.

كما تبرز أهمية مفهوم الجريمة الإلكترونية في توفير إطار لفهم الاختلاف بين الجرائم التي يستخدم فيها الحاسوب والأجهزة الإلكترونية كأداة لتنفيذ الجريمة وتلك التي تُستهدف بشكل مباشر الحاسب نفسه أو الأنظمة الرقمية .

لذلك تناولنا في هذا الفصل ماهية الجريمة الإلكترونية من خلال مبحثين: المبحث الأول تناول مفهوم الجريمة الإلكترونية ، والمبحث الثاني حول آليات البحث والتحري عن الجرائم الإلكترونية في التشريع الجزائري.

المبحث الأول: مفهوم الجريمة الإلكترونية:

لم يتفق الفقه الجنائي على إعطاء تسمية موحدة للجريمة الإلكترونية، فهناك من يطلق عليها تسمية الجريمة الإلكترونية أو المعلوماتية ، أو الجريمة ذات التقنية العالية، في حين يذهب آخرون الى تسميتها جريمة استخدام تكنولوجيا المعلومات والاتصال ، جرائم الانترنت أو الجرائم المستحدثة ، وآخرون جرائم الكمبيوتر ، أو جرائم الهاكر، أو الجرائم السيبرانية. في حين أطلق عليها المشرع الجزائري جرائم المساس بأنظمة المعالجة الآلية للمعطيات في القانون 04-15 لكن حينما أصدر القانون الخاص 09-04 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ، وقد أكد على هذا المسمى لما أصدر الأمر 21-11 والمتعلق بإضافة قطب جزائي وطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال .

تعد الجريمة الإلكترونية، من أكبر التحديات التي نواجهها في عالمنا المعاصر إن لم تكن أكبرها على الإطلاق، والحديث عن هذه التحديات يتطلب أولاً إعطاء صورة عامة عن تحديد ماهيتها، قبل التعرض إلى بحث المسؤولية الجنائية الناتجة عنها، وهو ما يدعونا إلى التعرض في هذا المبحث إلى مطلبين، الأول خاص بـ : (تعريف الجريمة الإلكترونية من الناحية الفقهية والتشريعية والقانونية استناداً للقوانين الجزائرية)، ثم التعرض في المطلب الثاني إلى : (خصائص الجريمة الإلكترونية) .

المطلب الأول: تعريف الجريمة الإلكترونية:

هي تلك الجرائم المستحدثة التي تطل أموال وحقوق الأشخاص ولا تتم إلا باستخدام الأجهزة الإلكترونية وعن طريق وسائل التواصل والمواقع الإلكترونية.

الفرع الأول: التعريف الفقهي للجريمة الإلكترونية:

لقد أدرج العديد من الفقهاء تعريفات للجريمة الإلكترونية بين مفهومها الضيق والواسع ، حيث عرف الأستاذ MASS الجريمة المعلوماتية بأنها تلك الاعتداءات التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح.

كما عرفها PARKER بأنها كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنها خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل¹.

ولقد عرفها الفقيه "روسبلات ROSENBLATT " استنادا لموضوع الجريمة بأنها "كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومة المخزنة داخل الحاسب الآلي" .

وتعد هذه المفاهيم ضيقة حيث أهملت الكثير من الجرائم الإلكترونية التي بقيت خارج مجال التجريم ، كالتزوير المعلوماتي ، ذلك أن البعض قد استند في تعريفه إلى وسيلة ارتكاب الجريمة والبعض الآخر على موضوع الجريمة.

¹ رمزي حوحو، منيرة بلوغي ، مواجهة الجريمة المعلوماتية في الجزائر، مجلة الحقوق و الحريات ، جامعة محمد خيضر بسكرة ، العدد الثاني ، ص42، 2014.

في حين عرفها أصحاب الاتجاه الموسع أمثال الفقيهان Michel et Credo بأنها جريمة استخدام الحاسب ، بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية على جهاز الحاسب ذاته أو المعدات المتصلة به ، وكذلك الاستخدام غير المشروع لبطاقات الائتمان وانتهاك ماكينات الحاسب الآلية بما تتضمنه من شبكات تحويل الحسابات المالية بطرق الكترونية ، وتزييف المكونات المادية والمعنوية للحاسب...¹.

وعرفها "دافيد تومبسن" بالنظر إلى فاعل في الجريمة بأنها جرائم يكون متطلبا لاقتوافها أن تتوفر لدى فاعلها معرفة تقنية بالحاسب...².

وفي هذا الاتجاه عرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها الجريمة التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورا رئيسيا...³.

وبحسب رأي خبراء المنظمة الأوروبية للتعاقد و التنمية الاقتصادية المنعقد في ماي 1983: "هي كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل تقنية المعلومات...¹.

¹ هلالى عبد الله أحمد ، التزام الشاهد و الاعلام في الجرائم المعلوماتية ، دراسة مقارنة ، القاهرة ، دار النهضة العربية 1997، ص 18.

² أسامة أحمد المناعسة، جلال محمد الزغبى (2001) : جرائم الحاسب الآلى والانترنت، دراسة تحليلية مقارنة دار والنشر والتوزيع، عمان، ص 7.

³ خالد عباد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والانترنت ، الطبعة الأولى، دار الثقافة ، سوريا ، 2001، ص 30.

ففي هذا المقام وجب التطرق إلى تعريف الفقه الجزائري للجريمة الالكترونية، فهناك من الفقهاء من يعرفها بأنها: كل عمل أو امتناع عن عمل يقوم به شخص إضرارا بمكونات الحاسب المادية والمعنوية، وشبكات الاتصال الخاصة به ، باعتبارها من المصالح والقيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها...² .

في حين ذهب آخرون في تعريفهم كما يلي هي : استخدام الأجهزة التقنية الحديثة مثل الحاسب الآلي والهاتف النقال، أو أحد ملحقاتها أو برامجها في تنفيذ أغراض مشبوهة وأمر غير أخلاقية لا يرتضيها المجتمع³.

الفرع الثاني: التعريف القانوني للجريمة الالكترونية:

لقد تناولت العديد من الهيئات الدولية والإقليمية التعريفات التشريعية للجريمة الالكترونية ، والتي من بينها تعريف الجريمة الالكترونية من خلال:

أولا-تعريف مؤتمرات هيئة الأمم المتحدة:

تبنى مؤتمر الأمم المتحدة العاشر لمنع الجريمة و معاقبة المجرمين والذي انعقد سنة 2000 بفيينا تعريف الجريمة الالكترونية بأنها : أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة

¹ أحمد خليفة(2006): الجرائم المعلوماتية، دار الفكر الجامعي، الطبعة الثانية، الإسكندرية، ص87.

² صيلع سعد، آليات مكافحة الجريمة الالكترونية في التشريع الجزائري ، أطروحة دكتوراة، المركز الجامعي مرسلني عبد الله ، تيبازة، 2025/2024، ص20 .

³ ريحانة زيدان ، الجريمة المعلوماتية في التشريع الجزائري و الدولي ، دار الهدى عين مليلة ، الجزائر ، طبعة 2011، ص42.

حاسوبية و داخل نظام الحاسوب وتشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية...¹.

ثانيا- تعريف منظمة التعاون الاقتصادي والتنمية :

عرفت الجريمة الالكترونية بأنها : كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية...².
و كون الجريمة الالكترونية عابرة للحدود فقد اهتمت العديد من الاتفاقيات الاقليمية أيضا بوضع تعريفات لها والتي من أهمها:

ثالثا -تعريف الجريمة الالكترونية في اتفاقية بودابست:

سنة 2001، وهي أول معاهدة دولية لمكافحة الجرائم الالكترونية ، وهو ما شكل نقطة محورية في بلورة التضامن و التعاون الدولي لمواجهة هذه الظاهرة المتنامية، حيث وقعت عليها 30 دولة لتفتح الباب لاحقا أمام دول خارج مجلس أوروبا مثل كندا واليابان و جنوب افريقيا والولايات المتحدة ما يعكس طبيعتها العالمية...³.

¹ ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراة، كلية الحقوق ، جامعة باتنة 1، 2015/2016، ص

² محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الالكترونية (دراسة مقارنة)، دار الفكر والقانون للنشر والتوزيع ، الطبعة الأولى ، سنة 2015، ص15.

³ سعيد مسعود الكثيري الجريمة الالكترونية في ضوء اتفاقية بودابست: الاطار المفاهيمي والتصنيفي، مجلة البحوث القانونية والاقتصادية ، المركز الجامعي بوشوشة، آفلو، المجلد 9، العدد 1، جانفي 2026، ص956.

حيث دعت الدول الأعضاء لاتخاذ الإجراءات الرادعة لمحاربة الجرائم الإلكترونية ، دون أن تتضمن تعريفا لها بل اكتفت بتصنيفها بالجرائم التي تستهدف عناصر أمن المعلومات، والتدخل في المعطيات ، وإساءة استخدام الأجهزة، والتدخل في نظم الحاسوب، والجرائم المرتبطة بالكمبيوتر (التزوير و الاحتيال)، وجرائم المحتوى (وهي جرائم استغلال الأطفال في المواد الإباحية ، وكذلك المتعلقة بانتهاكات حق التأليف والنشر)...¹ ، وتوفير قواعد ملائمة للتحري والتحقيق والضبط والتفتيش والمحكمة، مع التركيز على أهمية التعاون المحلي و الإقليمي.

رابعا-تعريف الجريمة الإلكترونية في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:

والتي أبرمت بالقاهرة 21 ديسمبر 2010، وصادقت عليها الجزائر سنة 2014، حيث اكتفت بتحديد المصطلحات المتعلقة بتقنية المعلومات والتي حددتها بتسعة مصطلحات، تتعلق بوسائل ، وأشخاص ، وموضوع تقنية المعلومات مثل مزود الخدمة والبيانات، البرنامج والنظام المعلوماتي والعديد من المصطلحات الأخرى.

والملاحظ أن معظم الاتفاقيات لم تعرف الجريمة الإلكترونية تعريفا واضحا ، حيث لا يوجد مصطلح موحد للدلالة على هذه الجريمة.

خامسا-تعريف المشرع الجزائري للجريمة الإلكترونية:

أما بالنسبة للمشرع الجزائري، فمن خلال قانون العقوبات أطلق عليها اسم الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وعرفها في المادة 02 من القانون 09_04 المتضمن القواعد

¹ سعد صيلع ، مرجع سبق ذكره ، ص 22، ص 23.

الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ، وبأنها"أي نظام منفصل، أو مجموعة الأنظمة المتصلة مع بعضها البعض أو المرتبطة ، يقوم واحد أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين " ¹.

أنها":جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب ، أو تسهيل ارتكابها عن طريق منظومة معلوماتية، أو نظام الاتصالات الإلكترونية²"، من خلال هذا التعريف، يتضح بأن المشرع الجزائري اعتمد على معيار دور النظام المعلوماتي لتحديد معالم الجريمة، حيث أطلق على الجرائم الموجهة ضد النظام المعلوماتي اسم "جرائم المساس بأنظمة المعالجة الآلية للمعطيات"، كما هو موضح في قانون العقوبات³ ، من نص المادة 394 مكرر إلى نص المادة 394 مكرر 07 ، وقد ترك المجال مفتوحا لأي جريمة أخرى قد ترتكب عبر منظومة معلوماتية ونظام الاتصالات الإلكترونية.

وأما عن خصائص الجريمة الإلكترونية، فمنها ما يتعلق بالجريمة بحد ذاتها ومنها ما يتعلق بالمرجم الإلكتروني وتتمثل في أنها:

- جريمة عابرة للحدود وسريعة التنفيذ.
- جريمة يصعب إثباتها ويسهل إخفاء معالمها.
- يمتنع المجني عليه عن التبليغ فيها ، خاصة عندما يتعلق الم أ ر بالجرائم الخاصة

¹ مادة 02 فقرة -ب- القانون رقم 04 = 09 المؤرخ في 14 شعبان 1430 الموافق ل 5 غشت سنة 2009 و المتضمن القواعد الخاصة بالوقاية المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، الصادر بالجريدة الرسمية العدد 47 بتاريخ 16 أوت 2000.

² القانون 04-09 المؤرخ في 05 أوت 2009 ، يتضمن لقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ، الجريدة الرسمية ، العدد رقم 47 ، ص 5 .

بالتهديد والتشهير .

- صعوبة المطالبة بالتعويض المدني في الجرائم الإلكترونية.
- المجرم الإلكتروني يتميز ببعض السمات كالمهارة والذكاء والمعرفة.
- ولتسليط الضوء على هذه الخصائص قمنا بالتطرق لها في المطلب الثاني .

المطلب الثاني: خصائص الجريمة الإلكترونية وطبيعتها القانونية :

إن طبيعة الجرائم السيبرانية وتمييزها عن الجرائم التقليدية يرجع إلى الوسط الذي ترتكب فيه الجريمة وهي الأداة أو الوسيلة التي استخدمها الجاني في ارتكاب فعله غير المشروع، وتتطلب توفر معرفة أو حد أدنى من أي سلوك إجرامي ينشأ بارتكاب فعل جرمه القانون أو الثقافة التقنية لدى الجاني، وهي لا تخرج عن كون الامتناع عن فعل أمر به القانون، وتتجه إرادة الجاني إليه رغم وجود نص قانوني يجرم السلوك...¹ وتختلف الجريمة المعلوماتية عن الجرائم التقليدية من حيث الأفعال الإجرامية، هذا الاختلاف أكسبها خصوصية غير عادية مما أخذ بنا إلى بيان أهم خصائص الجريمة المعلوماتية ومرتكبيها الملخصة في ما يلي:

الفرع الأول : الخصائص المتعلقة بالجريمة الإلكترونية:

أولاً- خصائص الجريمة الإلكترونية

1- الجريمة المعلوماتية جريمة عابرة للحدود الدولية:

الجريمة المعلوماتية جريمة لا تعترف بالحدود الجغرافية، فهي جريمة عابرة للحدود وبالتالي لا تعترف بعنصر المكان والزمان فهي تتميز بالتباعد الجغرافي واختلاف التوقيتات بين الجاني والمجني

¹مهدي رضا ، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري ،مجلة إيليزا للبحوث والدراسات ،المجلد 06 / العدد : 2 السنة 2021، ص 114 .

عليه، وبذلك أكسبها طبيعة دولية أو كما يطلق عليها جرائم ذات طبيعة متعددة الحدود، فلا يقتصر الضرر المترتب عن الجريمة على المجني عليه -وحده وإنما قد يتعداه إلى متضررين آخرين في دول أخرى نتج عن ذلك العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة وحول تحديد القانون الواجب تطبيقه بالإضافة إلى اختلاف إجراءات الملاحقة القضائية ،متعدية الحدود .

2-سرعة وسهولة تنفيذ الجريمة :

المعلوماتية مع سهولة إخفاء وإتلاف الجناة لأدلة الجريمة وعدم الوقوف على دليل واضح يمكن من التوصل إلى الجناة لا سيما وأن الجاني يعتمد إلى عدم ترك أثر لجريمته ، بالإضافة إلى سهولة محو الدليل من على شبكات الانترنت والحاسب الآلي في زمن قياسي وبللمسة واحدة على لوحة المفاتيح بجهاز الحاسب الآلي على اعتبار أن الجريمة تتم في صورة أوامر تصدر إلى الجهاز مما يؤدي إلى عدم تحديد مرتكبيها ،وإثبات الجريمة وعدم وجود أي أثر كتابي ملموس لما يجري خلال تنفيذها من عمليات وأفعال إجرامية حيث يتم استخدام النبضات الالكترونية في نقل المعلومات¹.

ثانيا-خصائص مرتكب الجرائم الالكترونية "الجاني" :

1-اختلاف طبيعة الجاني في الجرائم المعلوماتية(أنواع الجناة):

لا يمكن تحديد نموذج محدد للمجرم المعلوماتي يوضح شخصيته ومدى جسامة جرمه ، وقد صنف المجرم المعلوماتي الى ثلاثة أنواع :

¹شرويلي فاطمة ، ديدي فضيلة ، آليات مكافحة الجريمة الالكترونية ، مذكرة لنيل شهادة الماستر ، تخصص قانون الأعمال ، معهد الحقوق ، المركز الجامعي صالح أحمد ، النعامة ، سنة 2022-2023، ص19.

أ- هواة ارتكاب الجرائم الالكترونية:

ويطلق عليهم الهاكرز hackers ، وهم الأشخاص الذين يمتلكون تقنيات عالية مع الالمام بعلوم الحاسوب وبقدرتهم على اختراق شبكات الحاسب الآلي ، وأغلبهم مراهقين وشباب عاطل عن العمل أو طلاب ن حيث يهدف هواة ارتكاب الجرائم المعلوماتية الى الحصول على المعلومات بشتى الوسائل ، ويسخر قدراته في هذا المجال.¹

ب- محترفو ارتكاب الجرائم الالكترونية :

ويطلق عليهم مصطلح Crackers ، ويتميزون بالتخصص العالي في مجال الحاسب الآلي، وتعد هذه الطائفة الأخطر ، حيث تهدف اعتداءاتهم الى تحقيق الكسب المادي لهم أو الجهات التي سخرتهم لارتكاب جرائم الحاسوب ، أو تهدف الى تحقيق أغراض سياسية و التعبير عن موقف فكري، وأفراد هذه الطائفة يتسمون بالتكتم خلافا للهاكرز، فلا يتبادلون المعلومات بشأن أنشطتهم ، بل يحاولون عدم الكشف عن طرقهم التقنية المطورة لارتكاب جرائمهم، وهم أكبر سنا على الأغلب يتراوح أعمارهم بين 25-40 سنة ، وغالبا ما يكونوا عاملين ، او مسؤولين عن أنظمة معلوماتية ، فهم يملكون المعرفة اللازمة والتقنية للتلاعب بالحاسبات الآلية ، ويكمن خطرهم الحقيقي في أنهم كثيرا ما ينظر إليهم بوصفهم مستخدمين مثاليين ، والغالبية العظمى فيهم يشغلون مراكز قيادية هامة، ويتمتعون لذلك بثقة كبيرة في مجال عملهم. ولهم الهيمنة الكاملة على تقنية الالكترونيات ن وعلى قدر كبير من الذكاء² .

ت- المتطرفون من ذوي المثل العليا :

¹شرويلي فاطمة،ديدي فضيلة ، مرجع سابق ذكره ص20.

²شرويلي فاطمة،ديدي فضيلة ، نفس المرجع، ص21

وهي مجموعة تتميز بالدفاع عن غاية أو قضية ليس لها علاقة بمصالحهم الشخصية المباشرة ، وهم على استعداد للانخراط في أنشطة إجرامية من شأنها أن تسبب أضرارا جسيمة للآخرين ، سواء أشخاص أو قطاعات كاملة في المجتمع ، وذلك بدافع سياسي أو اقتصادي ، أوديني أو تتعلق بحقوق الإنسان.

2-صفات الجاني:

ويتوافر لدى معظم مجرمي المعلوماتية مجموعة من الصفات تميزهم عن سواهم من الجناة المتورطين في أنماط الانحراف الأخرى، ومن هذه الصفات:

أ-الذكاء :

يعتبر الذكاء من أهم صفات المجرم المعلوماتي حيث يمتلك المجرم المعلوماتي مهارة الذكاء التي تؤهله إلى القيام بتعدي وتطوير الأنظمة الأمنية والتقنية بالمقارنة بالمجرم التقليدي الذي يميل إلى العنف، فالمجرم المعلوماتي إنسان على مستوى عالي من الذكاء ومتكيف اجتماعياً لا يبين العداء للمجتمع.¹

ب -المهارة والاحتراف :

تعتبر مهارة الاحتراف من أبرز خصائص المجرم المعلوماتي التي تؤهله لأن يولف مهاراته في الاختراق والسرقة والاعتداء على حقوق الملكية الفكرية ومستوى المهارة التي يكون عليها المجرم المعلوماتي هي التي تحدد الأسلوب الذي يرتكب به الجرائم فإذا كان المجرم يتمتع بقدر ضئيل من مستوى المهارة والاحتراف، نجد أن الجرائم التي يرتكبها لا تتعد الإتلاف المعلوماتي أو نسخ

¹ . د رحونيمحمد ، خصائص الجريمة الإلكترونية ومجال استخدامها ، [جامعة أحمد دراية أدرار، مجلة الحقيقة، العدد41، سنة2018، ص 443 .

البيانات والبرامج ، أما إذا كان على درجة عالية من المهارة والاحتراف فإن أسلوبه في ارتكاب الجرائم المعلوماتية يكون مختلف حيث يمكنه استخدام الشبكات في الدخول إلى الحاسب الآلي لسرقة الأموال أو ارتكاب جرائم تجسس وزرع الفيروسات، فالظروف التي تحيط بالجريمة المراد تنفيذها وإمكانات نجاحها واحتمالات فشلها تساعد في تحديد درجة مهارة المجرم التي يتمتع بها .

ت-التخصص :

لا بد أن يتوافر لدى الجناة مرتكبي الجرائم المعلوماتية قدر من المعرفة المعلوماتية بمعنى أنهم متخصصون في هذا الشكل من الانحراف و الإجرام.

و من هنا فيكتسب هذا النمط من الجرائم (السيبرانية) خطورة خاصة ، نظرا لتقنيته العالية من جهة وتعدد أنواع مرتكبيه من جهة أخرى ، وغموض شخصيتهم من جهة أخرى ، حيث أن الهاكرز يتحدون اجراءات نظم المعلومات، دون أن تكون لهم دوافع تخريبية غالبا بل يدفعهم التحدي واثبات تفوقهم وقدراتهم ، على عكس الكراكرز التي تعكس اعتداءاتهم الميول الاجرامية الخطيرة ، والتخريب.¹

- الفرع الثاني :الطبيعة القانونية للجريمة الالكترونية

يثور الجدل بشأن الطبيعة القانونية للجرائم المستحدثة، ولا سيما الجرائم الإلكترونية، حول المركز القانوني للمعلومات والبرامج المعلوماتية، ومدى اعتبارها أموالاً أو قيماً مستقلة تستحق الحماية القانونية. وينقسم الفقه في هذا المجال إلى اتجاهين رئيسيين:

أولاً: استبعاد المعلومات من نطاق الجرائم التقليدية

¹ د رموني محمد ، نفس المرجع السابق، ص 444.

يرى أنصار هذا الاتجاه أن القواعد العامة في القانون الجنائي تقصر الحيازة والاستئثار على الأشياء المادية فقط، وأن محل جريمة السرقة يجب أن يكون شيئاً مادياً ملموساً يمكن نقله وحيازته عن طريق فعل الاختلاس الذي يشكل الركن المادي للجريمة¹.

وبناءً على ذلك، فإن المعلومات والأفكار المجردة لا تعد أموالاً قابلة للحيازة أو الاستيلاء عليها، إلا في حدود الحماية التي توفرها قوانين الملكية الفكرية. ومن ثم، فإن المعلومات لا يمكن أن تكون محلاً للسرقة إلا إذا كانت مثبتة على دعامة مادية كالأقراص أو الأشرطة الممغنطة. ففي هذه الحالة تكون السرقة واقعة على الوسيط المادي ذاته، وليس على المعلومة المجردة. أما إذا تعلق الأمر بالمعلومات في صورتها غير المادية، فإن تطبيق أحكام السرقة التقليدية يثير إشكاليات قانونية تتعلق بتحديد محل الجريمة².

ثانياً: إدراج المعلومات ضمن نطاق الجرائم

يذهب أنصار هذا الاتجاه إلى أن المعلومات والبرامج تمثل قيمة اقتصادية مستقلة عن الوعاء المادي الذي يحتويها، ومن ثم فهي قابلة للحيازة والاستئثار بها بصورة غير مشروعة. ويستند هذا الرأي إلى أن للمعلومات قيمة مالية واقتصادية حقيقية تجعلها جديرة بالحماية القانونية، شأنها شأن الأموال الأخرى.

¹ محمد الصغير مسيكة، مفهوم الجرائم المستحدثة (الإلكترونية)، مجلة الدراسات القانونية والسياسية، جامعة أحمد بن يحيى الومشريسي تيسيمسيلات الجزائر، المجلد 8 العدد 1 جانفي 2022، ص 142 .

² محمد الصغير مسيكة، نفس المرجع، ص 143 .

كما يرى الفقيهان الفرنسيان *Vivant* و *Catala* أن العلاقة التي تربط المعلومة أو البرنامج بمبتكرها تشبه علاقة الملكية التي تربط المالك بماله، مما يبرر منحها حماية قانونية باعتبارها مالا قابلاً للتملك والاستغلال.

ويفرق هذا الاتجاه بين نوعين من المال المعلوماتي:

- 1- **المال المعلوماتي المادي**: ويتمثل في الأجهزة والمعدات الحاسوبية كالشاشات ولوحات المفاتيح ووحدات المعالجة وغيرها¹.
 - 2- **المال المعلوماتي ذو المضمون المعنوي**: ويتمثل في المعلومات والبرامج المخزنة على وسائط مادية كالأقراص الممغنطة والذاكرات الإلكترونية والأسلاك الناقلة للإشارات².
- ومن هذا المنطلق، فإن القيمة الحقيقية للوسائط المادية لا تكمن في مادتها، بل في المعلومات والبرامج التي تحتويها. فحين يتم الاستيلاء على قرص أو شريط ممغنط، فإن الهدف غالباً ليس قيمة الوسيط المادية، وإنما ما يتضمنه من بيانات ومعلومات وبرامج.
- ويؤكد أصحاب هذا الرأي أن البرامج والمعلومات، رغم طبيعتها غير الملموسة، تمتلك وجوداً مادياً يتمثل في الإشارات والنبضات الإلكترونية التي يمكن نقلها واستقبالها ومعالجتها بواسطة الحاسوب، مما يجعلها قابلة للاستحواذ والانتقال. وبالتالي فإنها تصلح لأن تكون محلاً للحماية الجنائية.

¹ محمد الصغير مسيكة نفس المرجع السابق ، ص143

² نفس المرجع ص143

كما يرد هذا الاتجاه على الرأي القائل بأن البرامج والمعلومات لا تعد محلاً للملكية الخاصة لكونها نتاجاً فكرياً مجرداً، مؤكداً أن البرنامج أو المعلومة يعدان ملكاً لصاحبهما أو مبتكرهما، وأن الاستيلاء عليهما دون إذنه يمثل اعتداءً على حقه المشروع.

وقد استند أنصار هذا الاتجاه إلى بعض الأحكام القضائية المقارنة، وعلى رأسها أحكام محكمة النقض المصرية المتعلقة بسرقة التيار الكهربائي، حيث اعتبرت المحكمة أن الكهرباء، رغم عدم تمتعها بكيان مادي ملموس، تعد مالاً قابلاً للسرقة لوجودها المادي من خلال الأسلاك والتوصيلات التي تنقلها. كما أقرت المحكمة إمكانية وقوع السرقة على خدمات الهاتف رغم طبيعتها غير المادية.

وفي السياق ذاته، استند الفقه إلى بعض الاجتهادات القضائية الفرنسية، ومنها قضية **Logabax**، التي أُدين فيها موظف قام بنسخ وثائق سرية دون موافقة صاحب العمل، حيث اعتبرت المحكمة أن الاعتداء وقع على المعلومات ذاتها وليس فقط على الدعامة المادية التي تحتويها.

ويرى أنصار هذا الاتجاه أن مفهوم "الشيء" الوارد في النصوص القانونية لا يقتصر على الأشياء المادية فقط، بل يشمل كذلك القيم المعنوية التي تتمتع بوجود اقتصادي وقانوني، وهو ما يؤيده الفقيه الفرنسي **Vitu...¹**

¹ محمد الصغير مسيكة، نفس المرجع السابق، ص 142 .

ويتضح مما سبق أن الجرائم المستحدثة، وبالأخص الجرائم الإلكترونية، تتميز بطبيعة خاصة جعلت الفقه القانوني يواجه صعوبة في وضع تعريف جامع وموحد لها. ولذلك قيل إن هذه الجرائم "تقاوم التعريف"، نظراً لتعدد الزوايا التي يمكن النظر إليها من خلاله...¹.

فقد ركز بعض الفقهاء على الوسيلة المستخدمة في ارتكاب الجريمة، بينما انصرف آخرون إلى محل الجريمة أو موضوعها، في حين اعتمد فريق ثالث على شخصية الجاني، وجمع فريق رابع بين هذه المعايير المختلفة.

وتتميز الجرائم الإلكترونية بعدة خصائص أهمها طابعها العابر للحدود الوطنية، واعتمادها على الحاسب الآلي أو الشبكات المعلوماتية، وسرعة تنفيذها وتطور أساليب ارتكابها بصورة متواصلة. كما يتميز مرتكبها غالباً بامتلاكه قدراً كبيراً من المعرفة التقنية والمهارة الفنية، بعيداً عن مظاهر العنف التقليدية التي تميز بعض الجرائم التقليدية.

المبحث الثاني : آليات مكافحة الجرائم الإلكترونية في القانون الجزائري :

لقد أفرز التطور في استخدام تكنولوجيا المعلومات في العالم أجمع أنواعاً من الجرائم المستحدثة والتي من أهمها الجرائم الإلكترونية ، التي أدت الى استحداث أجهزة متخصصة لمكافحة الجريمة المعلوماتية ، والتي تتولى مهمة التحري عن هذه الجرائم عبر آليات محددة سواء دولياً أو وطنياً.

¹ محمد الصغير مسيكة ، نفس المرجع السابق ، ص 143 .

وفي إطار التصدي لهاته الجرائم قام المشرع الجزائري بسن قانون 09-04 المتعلق بالوقاية من تكنولوجيات الاعلام و الاتصال ومكافحتها وجلك عبر مجموعة من الآليات و التدابير الاجرائية ، أهمها:

المطلب الأول: الآليات الوقائية

لقد عمد المشرع الجزائري الى استحداث آليات وقائية للتصدي للجرائم الالكترونية واتخذ واستصدر عدة اجراءات وقوانين وكذا هيئات مختصة في مواجهة هته الجرائم ، نتطرق لها في هذا المطلب .

الفرع الأول :المراقبة الالكترونية

وهو إجراء يعرف بأنه تحقيق يباشر خلصة وينتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي لجريمة تحقق وقوعها ، ويتضمن من ناحية استراق السمع ، ومن ناحية أخرى حفاظه على الأشرطة عن طريق أجهزة مخصصة لهذا الغرض.¹

وقد قام المشرع الجزائري بانشاء الأقطاب القضائية المتخصصة في هذا النوع من الجرائم ، وتوسيع دائرة الاختصاص المحلي لضباط الشرطة القضائية عبر كامل التراب الوطني ، في ما يخص جرائم المساس بأنظمة المعالجة الآلية للمعطيات وهذا ما أورده بالذکر المادة 16 مكرر من قانون الإجراءات الجزائية.

¹ -بن موسى خديجة ، الحماية الجنائية للمعطيات في المجال المعلوماتي ، مذكرة ماستر قانون جنائي ،كلية الحقوق و العلوم السياسية ، جامعة غرداية ، 2022،ص54 .

كما سمح المشرع الجزائري باللجوء الى هذا الإجراء في حالات محددة حصرا (المادة 04 من القانون 04-09) وتكون بموجب إذن مكتوب من السلطات القضائية المختصة ، للوقاية من الأفعال الإرهابية أو التخريبية أو الجرائم الماسة بأمن الدولة ، أوفي حال معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني ، أو مؤسسات الدولة أو الاقتصاد الوطني ، وكذلك الأمر في حالة مقتضيات التحريات والتحقيقات القضائية عندما تستدعي الضرورة ، كما يمكن الاستعانة بالمراقبة الالكترونية في اطار تنفيذ المساعدة القضائية الدولية المتبادلة .¹

الفرع الثاني :الاستعانة بمزودي الخدمات للوقاية من الجرائم الالكترونية:

ويكون ذلك من خلال وضع معطيات و محتوى الاتصالات استعانة بمزودي الخدمات تحت تصرف السلطات القضائية المختصة. و حسب (المادة 11من القانون 04-09) تشمل هذه المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال، والمعطيات التي تسمح بالتعرف على مستعملي الخدمة ، والخصائص التقنية وكذلك تاريخ ووقت ومدة الاتصال ، والمعطيات التي تسمح بالتعرف على المرسل إليه ، وكذا عناوين المواقع المطلع عليها. ويطلق عليها المعطيات المتعلقة بحركة السير كما عرفها المشرع في المادة الأولى من هذا القانون .

¹مهدي رضا ، الجرائم السبرانية وآليات مكافحتها في التشريع الجزائري ، مجلة اليزا للبحوث والدراسات ، المجلد 06، العدد 02،2021،ص118.

كما نصت (المادة 12 من القانون 04-09) على مجموعة التزامات خاصة بمقدمي خدمات الانترنت وتشمل :

- التدخل الفوري لسحب المحتويات المخالفة للقوانين أو حضر الدخول إليها.
- الالتزام بموضع ترتيبات تقنية تحصر إمكانية الدخول إلى الموزعات التي تحتوي المعطيات المتعلقة بالخدمات التكميلية المستعملة والمطلوبة ، والمعطيات التي تسمح بالتعرف على المرسل إليه والمواقع المطع عليها. حيث يشترط قيام مقدمي الخدمات بحفظ معطيات حركة السير.

المطلب الثاني: الآليات الردعية الإجرائية

كان لابد للمشروع الجزائري للتصدي ومحاربة الجرائم المستحدثة الالكترونية من استحداث آليات ردعية سواءا في مكافحة الجريمة عن طريق الاجراءات الجديدة وكذا الهيئات والهيكل المختصة بمحاربة هته الجرائم ، التي نتطرق لها في هذا المطلب .

الفرع الأول: آليات مكافحة الجريمة الالكترونية

أولا -تفتيش وحجز المنظومة المعلوماتية:

لقد تم وضع مجموعة من الترتيبات التقنية لمراقبة الاتصالات الالكترونية ، وتجميع وتسجيل محتواها في حينها ،القيام باجراءات التفتيش والحجز داخل المنظومة المعلوماتية (المادة 03 من القانون 09-04).

تعد اجراءات التفتيش والضبط من اجراءات التحقيق التي تختص بها سلطة التحقيق ويناط لضابط الشرطة القضائية القيام بهما في حالات استثنائية ، ويعتبر التفتيش وسيلة يمكن من خلاله الحصول على أدلة في بيان وظهور الحقيقة ، ولا يكفي في التفتيش مجرد توافر شروطه سواء الموضوعية أو الشكلية ، بل يلزم أيضا ضرورة مراعاة حدوده الداخلية والتي يتمثل أهمها في ضرورة التقيد بالغرض من التفتيش اثناء تنفيذه ، وفقا لما نص عليه قانون الاجراءات الجزائية.¹

ثانيا- تمديد الاختصاص بنظر هذه الجرائم :

لقد أجاز المشرع الجزائري بموجب الفقرة الثانية من المادة 37 من قانون الاجراءات الجزائية تمديد اختصاص وكيل الجمهورية في جرائم محددة على سبيل الحصر ، ومن بينها جرائم المعالجة الآلية للمعطيات الى دائرة محاكم أخرى محددة عن طريق التنظيم ، وهو نفسه بالنسبة لتمديد اختصاص قاضي التحقيق بموجب لفقرة الثانية من المادة 40 من قانون الاجراءات الجزائية. كما نصت الفقرة الأخيرة من المادة 329 من قانون الاجراءات الجزائية الجزائري على تمديد الاختصاص المحلي للمحكمة في تالجرائم المحددة على سبيل الحصر ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

¹ عزالدين عثمانى ، اجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال و المعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، العدد الرابع، جانفي 2018، ص 60.

وقد حدد المشرع سنة 2006 تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق بموجب المرسوم التنفيذي رقم 06-348.

وتجدر الإشارة أن المادة 16 من قانون الاجراءات الجزائية عاجلت تمديد الاختصاص لضباط الشرطة القضائية الى كامل التراب الوطني ، فيما يتعلق بالبحث ومعاينة جرائم محددة بنص المادة ، ومن بينها الجرائم الماسة بالمعالجة الآلية للمعطيات ، حيث أجازت المادة 47 التفتيش والمعاينة والحجز في هذه الجرائم في أي ساعة من النهار أو الليل باذن من وكيل الجمهورية.¹

وما يفسر خروج المشرع عن معايير الاختصاص الأصلي في الجرائم المعلوماتية هو :

-اتساع مكان ارتكاب الجرائم المعلوماتية خارج حدود الاختصاص الاقليمي التقليدي، وانتشار الأعمال المكونة لهذه الجرائم داخل وخارج حدود الدولة .

-التمسك بالمعايير الأصلية للاختصاص يشكل عائقا أمام مواجهة الجرائم المعلوماتية .

- الطبيعة الخاصة لهذه الجرائم.

ثالثا - تبادل المساعدة القضائية الدولية:

¹أومدوررجاء، خصوصية التحقيق في مواجهة الجرائم المعلوماتية ، اطروحة دكتوراة لل.م.د، جامعة محمد البشير الابراهيمي ، برج بوعرييج، سنة 2021/2020 ، ص88-89 .

لقد تطرق القانون الجزائري الى المساعدة القضائية المتبادلة كعنصر مهم في مواجهة الاجرام الالكترونية ، ومن بين النقاط التي تبرز ذلك نجد:¹

-القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ، القانون 04/09 المؤرخ في 2009، حيث تظهر مجالات التعاون القضائي الدولي في :

-في مجال مراقبة الاتصالات الالكترونية نص المشرع على الحالات التي تسمح باللجوء الى المراقبة الالكترونية ، ومن بينها في اطار تنفيذ طلبات المساعدة القضائية المتبادلة.

- كذلك في اطار تفتيش المنظومة المعلوماتية فقد أشار المشرع للمساعدة القضائية المتبادلة وهذا في حالة ما اذا كانت المعطيات المبحوث عنها يمكن الدخول اليها انطلاقا من منظومة معلوماتية تقع خارج الاقليم الوطني يكون الحصول عليها بمساعدة السلطات الأجنبية المختصة ، طبقا للاتفاقيات الدولية ، أو لمبدأ المعاملة بالمثل .

- كما كرس القانون مبدأ التعاون والمساعدة القضائية في حالة ما اذا كان مرتكبها أجنبيا ، وتستهدف مؤسسات الدولة ، وأسند مهام الرقابة على هذه الجرائم للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بمقتضى المادة 13 التي حددت مسؤولياتها ، من بينها تبادل المعلومات مع نظيرتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد مكان تواجدهم.

¹برقوق يوسف ، المساعدة القضائية المتبادلة لمواجهة الجرائم الالكترونية ، مجلة البصائر للدراسات القانونية ، المجلد 01 العدد 01 ، سنة 2021، ص 1.99

رابعا - القوانين اللاحقة المدعمة للقانون 04-09 للحد من الإجرام السيبراني:

لقد أدخل المشرع الجزائري مجموعة من التعديلات على كل من قانون العقوبات وقانون الاجراءات الجزائية ، كما استحدث القانون 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال ومكافحتها ، اضافة الى القانون 04-18 المتعلق بالقواعد العامة للبريد والاتصالات الالكترونية ، والقانون 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي .¹

وصدرت في سنة 2020 مجموعة من المراسيم الرئاسية ،منها المرسوم الرئاسي الذي أعاد سير وتنظيم الهيئة الوطنية للوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال ،والمرسوم الرئاسي المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

الفرع الثاني :الهيكل الخاصة للتصدي للجرائم الالكترونية :

أولا -الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها:

وهي هيئة تم انشاؤها في اطار الإصلاحات التي انتهجتها الجزائر لإصلاح العدالة لمكافحة الجريمة الالكترونية ، والتي أنشئت بموجب المادة 13 من القانون (04/09) ومن مهامها تفعيل التعاون القضائي والدولي و الأمني ، وإدارة وتنسيق عمليات الوقاية ، والمساعدة التقنية

¹ د .بوضياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهةها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف - المسيلة، العدد 11 ، سبتمبر 2018 ، ص 369.

للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية في حالة الاعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني ، ولذلك أنشئت هذه الهيئة التي تعد بمقتضى المادة الأولى من المرسوم الرئاسي رقم 183/20 ، فان هذا المرسوم جاء لبيان كيفية تشكيل هذه الهيئة وكذا طريقة وكيفية سيرها . حيث تعد "سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلالية المالية ، توضع تحت سلطة رئيس الجمهورية" ¹... ، ويحدد مقر الهيئة في الجزائر العاصمة ، ويمكن نقله الى أي مكان آخر من التراب الوطني بموجب مرسوم رئاسي. وتتكون هذه الهيئة من : مجلس التوجيه، والمديرية العامة التي تضم كل من (مديرية المراقبة الوقائية واليقظة الالكترونية ، مديرية الادارة والوسائل ، مصلحة الدراسات والتلخيص، مصلحة التعاون واليقظة الالكترونية).

وحددت مهامها :

- اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها .

- ضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالاعمال الارهابية والتخريبية والمساس بأمن الدولة.

¹ أعمارحشمان ، الجريمة المعلوماتية في التشريع الجزائري ، مذكرة ماستر العلوم الاقتصادية والتجارية والتسيير ، امعة ورقلة ، جويلية 2019 ، ص 33 .

- تجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصدرها ومسارها من أجل استعمالها في الاجراءات القضائية .
- المساهمة في تكوين محققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الاعلام والاتصال .

- المساهمة في تحيين المعايير القانونية في مجال اختصاص الهيئة.¹
- وكذلك تبادل المعلومات مع نظيراتها في الخارج قصد جمع وتحديد مكان المعلومات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الاعلام والاتصال وتواجههم.

ثانيا- السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي :

استحدث المشرع الجزائري بموجب القانون 07-18 سلطة وطنية تسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي ، وهي عبارة عن سلطة ادارية مستقلة ، تضمن عدم انطواء استعمال تكنولوجيات الاعلام والاتصال على أي أخطار اتجاه حقوق الأشخاص والحريات العامة والحياة الخاصة، توضع لدى رئيس الجمهورية وذلك بهدف حماية المعطيات، وهذا ما جاء

حسب ما نصت عليه المادة 47 من الدستور سنة 2020 حيث نصت عل : حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسيتكريسا لمبدأ الحفاظ على كرامة الإنسان وحقوقه في عدم انتهاك مراسلاته واتصالاته بالإضافة إلى الحقوق الواردة على

¹أومدور رجاء، مرجع سبق ذكره، ص 93.

المعطيات ذات الطابع الشخصي ، سواء منها المدنية أو البيولوجية أو غيرها من المعطيات¹...، وتتمثل مهامها في :

-تلقي التصريحات المسبقة المتعلقة بمعالجة المعطيات ذات الطابع الشخصي، حيث يجب أن يودع التصريح مسبقاً بأي شكل من الأشكال ، حيث يمكن تقديمه الكترونياً ، ويسلم وصل ايداع أو يرسل فوراً بالطريق الإلكتروني في مدة محددة 48 ساعة.(المادة من 13 الى 16)

-اخضاع المعالجة لنظام الترخيص: حسب المواد من 17 الى 21، حيث لابد للسلطة الوطنية من احترام وحماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص، كما تمنح التراخيص

بنقل المعطيات ذات الطابع الشخصي نحو الخارج، وفقاً لشروط محددة قانوناً ، ونشر التراخيص الممنوحة في السجل الوطني .

-الاعلام وتقدير الاستشارات والاقتراحات اللازمة: حيث تسهر السلطة على اعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم ، وتقديم الاستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي.

-اصدار أوامر: حيث تأمر باغلاق معطيات أو سحبها أو اتلافها .

-تطوير علاقات التعاون مع السلطات الأجنبية المماثلة: وفقاً لمبدأ المعاملة بالمثل .

¹سعدصيلع، مرجع سابق ، ص231

- اعداد تقرير سنوي: حيث تقوم باعداده ورفع له لرئيس الجمهورية.

ولقد اشترط القانون 07-18 الموافقة المسبقة من الشخص الطبيعي الذي تكون المعطيات ذات الطابع الشخصي المتعلقة به محل معالجة ، كما لا يمكن معالجة المعطيات المتعلقة بالطفل الا بعد حصول موافقة من ممثله الشرعي، أو بترخيص من القاضي المختص.¹

ثالثا- المنظومة الوطنية لأمن الأنظمة المعلوماتية:

ليست الهيئة الوطنية للوقاية ومكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ، ولا السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي لوحدها هيئات ادارية ذات طابع غير أمني مكلفة بمكافحة الجرائم الالكترونية ، بل استصدر المشرع منظومة وطنية لأمن الأنظمة المعلوماتية بموجب المرسوم الرئاسي 20-05 التي تتكون من :

-المجلس الوطني لأمن الأنظمة المعلوماتية

-وكالة أمن الأنظمة المعلوماتية

تدير الوكالة لجنة توجيه وتزود بلجنة علمية ، وتتوفر على مركز وطني عملياتي لأمن الأنظمة المعلوماتية ومديريات ومصالح تقنية وادارية موضوعة تحت سلطة المدير العام الذي يسير بدوره الوكالة ويسهر على تنسيق و تنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية ، وتنفيذ المخططات والبرامج المسطرة من قبل لجنة التوجيه.

¹أومدوررجاء، مرجع سبق ذكره ، ص 96

رابعاً-المؤسسات الأمنية ودورها في مكافحة الجريمة الالكترونية :

1-مساهمة الدرك الوطني:

يحارب الدرك الوطني الجرائم المنظمة ومنها الجرائم الالكترونية، وذلك باستعمال وسائل تحريات الشرطة العلمية والتقنية وخبرة الأدلة الجنائية ، ويمارس هذه المهمة طبقاً لأحكام قانون الاجراءات الجزائية ، وتتمثل المهام الموكلة لأجهزة الدرك الوطني في مكافحة الجريمة الالكترونية التي تقسم الى ثلاث مستويات : على المستوى المركزي، الجهوي، المحلي.¹ على المستوى المركزي حيث تعمل على دعم أعمال البحث والتحقيق من خلال عدة أجهزة وهي: مديرية الأمن العمومي والاستغلال والتي تعمل على التنسيق بين مختلف الوحدات الاقليمية والمركز التقني العلمي، في مجال أعمال البحث والتحري في الجرائم الالكترونية ، بالاضافة الى المصلحة المركزية للتحريات الجنائية وهي هيئة ذات اختصاص وطني من بين مهامها مكافحة الجريمة المرتبطة بتكنولوجيا الاعلام والاتصال.²

¹عمار حشمان ، الجريمة المعلوماتية في التشريع الجزائري ، مذكرة ماستر العلوم الاقتصادية والتجارية والتسيير ، امعة ورقلة ، جويلية 2019 ، ص 41 .

² نفس المرجع السابق ، ص 41 .

-المعهد الوطني للأدلة الجنائية وعلم الاجرام *INCC/GN*: وهو جهاز تابع للدرك الوطني أنشئ بموجب المرسوم الرئاسي رقم 183/04 يتكون من 11 دائرة متخصصة في عدة مجالات تتضمن الخبرة والتكوين والتعليم والبحوث والدراسات والتحليل في علم الجريمة.¹

يسهر أفراد الدائرة على تأمين اليقظة التكنولوجية ، من أجل تحيين المعارف ، التقنيات والطرق المستعملة في مختلف الخبرات العلمية. وتنقسم الى مخبر الاعلام الآلي ، مخبر الفيديو ، ومخبر الصوت.

كم أنه من بين المهام الموكلة الى المعهد الوطني للأدلة الجنائية وعلم الاجرام ومكافحة الجريمة الالكترونية ، من خلال البحث والتحقيق في الدليل الرقمي، اذا ماتلقى طلبات من من الجهات القضائية لاجراء الخبرة ، و تقوم بها مصلحة الاعلام الآلي والتي تقوم برصد ومراقبة ، وتتبع عمليات الاختراق والقرصنة المعلوماتية ، وكذا اكتشاف المعلومات المسروقة ،وتفكيك البرامج المعلوماتية الخبيثة . و المعهد هو مؤسسة عمومية تتمتع بالشخصية المعنوية والاستقلال المالي، توضع تحت وصاية وزير الدفاع الوطني ، ويمارس قائد الدرك الوطني سلطات الوصاية بتفويض منه. وفي المعهد الوطني لعلم الأدلة الجنائية و علم الاجرام بصفته الهيئة المكلفة بالتحليل والخبرات في ميدان علم الاجرام ووضع سياسة لمكافحة الاجرام ، حيث توجد هيئة مركزية أخرى تابعة للدرك الوطني تضطلع بمكافحة الجريمة الالكترونية وهي :

-مركز الوقاية من جرائم المعلوماتية *CPLCIC/GN*:¹

¹ نفس المرجع السابق، ص 42

وهو تابع بيدرك الوطني ويكلف بمهمتين : المهمة الأولى : وهي قبلية تتعلق بالتدقيق والوقاية .
والمهمة الثانية تتعلق بردع الجرائم الماسة بالطفولة. ولهذا أنشيء مكتب خاص بحماية الأحداث عبر
الانترنت بغرض تقديم الدعم التقني للوحدات الاقليمية في التحري وجمع الأدلة الجنائية.

ان مركز الوقاية من جرائم الاعلام الآليوالجرائم الالكترونية أنشئت سنة 2008، وهو هيئة تقنية
تعمل تحت وصاية مديرية الأمن العمومي والاستعمال لقيادة الدرك الوطني ، للبحث عن الأدلة في
شبكة الانترنت والشاركة في عملية التحري .²

هذا بالنسبة للهيئات المركزية ، وهناك هيئات أخرى جهوية ومحلية ، أما الجهوية تهتم بتنسيق
مختلف النشاطات بين وحدات الشرطة القضائية ، ودعمها بمختلف الوسائل الخاصة بالتحريات ،
نظرا للوسائل المادية لديه وعدد الأفراد الهائل للدرك الوطني ، والصلاحيات التي خولها لهم القانون
.

أما على المستوى المحلي فللدرك الوطني فصائل للبحث ينتمي اليها أفراد ذو خبرة في ميدان الشرطة
القضائية ، هذه الفصائل مكلفة بمكافحة الأشكال الخطيرة للجرائم ومنها الجرائم الالكترونية ،
وهذه الوحدات الخاصة تساهم في تدعيم نشاطات البحث والتحري التي تقوم بها الفرق الاقليمية
للدرك الوطني.

¹أدرور نجاة ، مرجع سبق ذكره ، ص101.

²سعد صيلع ، مرجع سبق ذكره، ص 232

وقد استحدثت وحدات الدرك الوطني عدة تطبيقات وبرامج تقنية لحماية البنى التحتية المعلوماتية ، ومنع تسريب مختلف الامتحانات والمسابقات عبر وسائل التواصل الاجتماعي ، كما أنه تم وضع تطبيق الكتروني خاص بمستخدمي الطرق الوطنية (تطبيق طريقي) ، كما أنه تجدر الإشارة الى موضوع القانون الذي تم الانتهاء منه بين الدرك الوطني ووزارة التربية الوطنية المتضمن تصريح تصفح الانترنت للقاصرين ، وهو بمثابة ميثاق يتضمن المبادئ التوجيهية الأمنية للأطفال و المراهقين هذا لتعليمهم وتثقيفهم حول مختلف مخاطر الشبكات الاجتماعية و الانترنت خاصة منها الناقلة لرسائل منافية للقيم الأخلاقية ، والديمقراطية وحقوق الانسان ، وتوزيع هذا الميثاق على المدارس.¹

- في 2017 عالج المركز 100 جريمة تتعلق بالأطفال والمراهقين ، و 20 جريمة مالية ، حيث أن الجرائم المالية مازالت محدودة لأن التجارة الالكترونية والدفع الالكتروني كان في بدايته ، وهي اليوم أكثر حدة وتطورا.

- المصلحة المركزية للتحريات الجنائية SCIC/GN

وهي تابعة للدرك الوطني تقوم بالتحقيق العلمي والتقني والعملي ، ويبقى اجراء التحقيق في الجرائم المعلوماتية ليس سهلا لعدم اعترافه بالحدود المكانية والزمانية. والجدير بالذكر أن المحققين

¹ نفس المرجع السابق ، ص 43

علم المستوى المحلي من فصائل الأبحاث التي تشمل محققي جرائم الاعلام الآلي ، يختصون بالتحقيق ومقاربة تقنية أولية. وهو كذلك بالنسبة لخلايا الشرطة العلمية والتقنية على المستوى المحلي.

2- مساهمة الأمن الوطني في مكافحة الجريمة الالكترونية:

- المخابر:

لقد أنشأت الجزائر أول مخبر للشرطة العلمية والتقنية غداة الاستقلال وواكب التطورات الحاصلة في العالم وأصبح علمها محكم وتخصصها التكنولوجي والعلمي أعطى نتائج ملموسة للجهاز القضائي .

ان المؤسسة الأمن الوطني دورها في التصدي للجرائم الالكترونية ، حيث تم انشاء المعهد الوطني للبحث في علم التحقيق الجنائي الذي يعتبر مؤسسة ادارية لها الاستقلال المالي والاداري تحت وصاية وزير الداخلية وتتبع الى المديرية العامة للأمن الوطني ، ويضم قسم علمي وتقني ، بالاضافة الى مصلحة قاعدة المعطيات ، ومن بين المهام الموكلة لهذا المعهد ما جاءت به المادة 05 من المرسوم الرئاسي أنها تتولى: اعادة تقارير الخبرة ، وتحليل المؤشرات المادية والتقنية بناء على طلب السلطة القضائية المختصة.¹

¹لسعد صيلع، مذكرة دكتوراة ، ص234

كما أن المعهد يقوم بالاشتراك مع المعاهد والمخابر الوطنية والأجنبية في ميدان البحث في علوم التحقيق. حيث يتلقى المعهد الطلبات من الجهات القضائية لاجراء الخبرة من أجل الكشف عن الأدلة الرقمية ، وهذا من خلال عدة مصالح التي تنقسم الى مخابر والتي من بينها مصلحة الخبرات الخاصة بالدلائل التكنولوجية وتكلف بما يأتي : تحليل بطلب من السلطات القضائية المختصة الدلائل المادية التي جمعها اثر معاينة المخالفات والتحريات في ميادين الدلائل المعلوماتية وجرائم الكمبيوتر والبصمات الصوتية ومعالجة الصورة والاشارة واستعمال الهواتف المحمولة واعداد تقارير الخبرة. في مجال البحث عن الدلائل الالكترونية. وقد استحدثت مخابر الشرطة العلمية سنة 2007 الكائن مقرها بكل من الجزائر العاصمة ووهران وقسنطينة تحتوي على أقسام مختصة في الأدلة الرقمية من خلال استغلال الأجهزة كأدوات التخزين الرقمية ، كما تم تدعيم المصالح الولائية للشرطة القضائية بما يقارب 23 خلية لمكافحة الجرائم الالكترونية (08 خلايات لولايات الشرق، 08 لولايات الوسط، 06 خلايا لولايات الغرب و 01 لولايات الجنوب).

- المصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال:¹

واستحدثت الأمن الوطني مصلحة مركزية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية ، مشكلة النواة الأولى على مستوى المديرية العامة للأمن الوطني سنة 2011، وفي 2015 تم استحداث المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال أضيفت للهيكل التنظيمي لمديرية الشرطة القضائية ، وتم انشاء معهد وطني للدراسات العليا للأمن الوطني سنة 2017.

¹ نفس المرجع السابق ، ص44

ومنه فان للمديرية العامة للأمن الوطني دورا أساسيا في مواجهة الجرائم المعلوماتية من خلال دورها الوقائي والردعي والتحسيصي. من خلال عقد دورات افتراضية على مستوى شبكات المعلومات عموما ومواقع التواصل الاجتماعي خصوصا ، أو لمواجهة الاحلال بالنظام العام ، في حالة المنشورات الهدامة ، تمس النظام العام كعرض أجهزة حساسة أو منوعات للبيع عبر مواقع التواصل الاجتماعي ، حيث يتم التدخل لتحديد هوية صاحب الحساب واتخاذ الاجراءات القانونية اللازمة. كما تعمل المديرية على تلقي الشكاوي التي قد تكون مباشرة أو غير مباشرة عن طريق ارسال النيابة العامة للقضية للتحقيق فيها.وعلى المستوى الجوي ومن خلال الهيكل التنظيمي للمكتب المركزي الوطني انتربول الجزائر.

اذ يوجد المكتب الرابط للانتربول ل48 ولاية، واستخدام قاعدة المعطيات 24/7، حيث يعمل الجهاز 24/7 على تحديد المعلومات اللازمة حول الأشخاص، والمركبات موضوع التحقيق.



الفصل الثاني:

صور المساءلة الجزائية عن
الجرائم الإلكترونية

يطلق على المعلومات في العصر الحديث اسم البترول الرمادي petrole gris أو بالانجليزية petrolgrayish نسبة الى المادة الرمادية في المخ ، حيث أصبحت أنظمة المعلومات محل استهداف من قبل نوع جديد من المجرمين يستهدف مختلف البرامج المخزنة داخل النظام المعلوماتي سواء بالسرقة أو التخريب و الإتلاف . وسنتناول في هذا الفصل صور هذه الجرائم الالكترونية وصور المساءلة الجزائية من خلال مبحثين، تناول المبحث الأول الاطار الموضوعي للجريمة الالكترونية (الصور الجرمية)، من خلال مطلبين : المطلب الأول الجرائم الواقعة بواسطة النظام المعلوماتي والواقعة عليه ، والمطلب الثاني الصور الجرمية للجريمة الالكترونية . وأما المبحث الثاني فتناول المسؤولية الجزائية عن الجرائم الالكترونية من خلال مطلبين : المطلب الأول شروط مساءلة الشخص الطبيعي عن الجريمة الالكترونية، والمطلب الثاني المسؤولية الجزائية للشخص المعنوي عن الجرائم الالكترونية . حيث سيتم في كل مطلب التطرق للعقوبات التي فرضها المشرع الجزائي على الجريمة الالكترونية من خلال مختلف القوانين.

المبحث الأول : الإطار الموضوعي للجريمة الإلكترونية محل المساءلة الجزائية (الصور الجرمية)

المطلب الأول : الجرائم الواقعة بواسطة النظام المعلوماتي والواقعة عليه :

لقد قسم المشرع الجزائري الجريمة الإلكترونية إلى نوعين : الجرائم التي تقع بواسطة النظام المعلوماتي والجرائم التي تقع على النظام المعلوماتي .

الفرع الأول: الجرائم التي تقع بواسطة النظام المعلوماتي :

يحدد هذا التصنيف أهم الجرائم المتعلقة أو المتصلة بالنظام المعلوماتي ، ويستعمل الحاسوب للولوج إلى الأنظمة المعلوماتية واستعمالها في تنفيذ الجريمة وتسهيل الوصول للنتيجة الإجرامية ومضاعفة جسامتها وتنقسم الى ثلاثة أقسام ، الواقعة على الأشخاص ، والجرائم الواقعة على الأموال ، والجرائم الواقعة على الأسرار.¹

أولاً- الجرائم الواقعة على الأشخاص بواسطة النظام المعلوماتي :

حيث عرفها أحد الفقهاء باسم الاعتداء على جرمية الحياة الخاصة للأفراد باعتباره من أهم الحقوق الخاصة بالفرد وحياته ، وكذلك هي الجرائم التي تنال بالاعتداء أو تهدد بالحقوق اللصيقة بالشخص والتي تعتبر من بين مقومات الشخصية ، ولا تمس بالجانب الاقتصادي ، ومن أهم الحقوق الخاصة بالأفراد الحق في الحياة ، الحق في السلامة الجسدية ، الحق في صيانة الشرف ، والحق في الحرية ومن بين الجرائم ، الأكثر شيوعاً : جريمة المضايقة والملاحقة ، جريمة انتحال الشخصية ، وكذا جرائم التشهير وتشويه السمعة .²

¹ د. بوضياف إسمهان ، مجلة الأستاذ الباحث للدراسات القانونية والسياسية مرجع سابق ، ص 357.

² نفس المرجع ص 357 .

ثانيا- الجرائم الواقعة على الأموال بواسطة النظام المعلوماتي :

وتستهدف هذه الجرائم الذمة المالية للأشخاص ويكون الدافع من ارتكابها هو الطمع في الحصول أو الاستيلاء على الأموال ، وتحقيق الكسب السهل والسريع ، وقد يكون الدافع أحيانا من ارتكابها هو قهر نظام منشأة أو شركة ما أو تخطي حواجز الحماية ، أو بدافع الانتقام من صاحب تلك الشركة أو أحد عناصرها ، كالسطو ، والسرقة ، والتحويل الإلكتروني الغير مشروع للأموال ، وغسيل الأموال ، وقرصنة الحسابات الشبكية الغير مشروعة .

ثالثا - الجرائم الإلكترونية الواقعة على الأسرار :

وتقع هذه الجرائم بواسطة النظام المعلوماتي لإفشاء الأسرار سواءا كانت عامة أو خاصة، سواءا تعلقت هذه الأسرار بالمؤسسات أو بالأشخاص مثل أسرار الدولة العسكرية والاقتصادية، وأسرار المهنة والهدف سرقة المعلومات الخاصة بالعامل أو الموظف والتشهير به ، أو بيع هذه المعلومات ، والضغط عليهم من أجل فعل شيء أو الإمتناع عن فعله .¹

الفرع الثاني: الجرائم الواقعة على النظام المعلوماتي:

تتمثل أشكال الاعتداء على أنظمة المعالجة الآلية للمعلومات في ما يلي :

أولا-الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات :

¹ نفس المرجع السابق ص 357

يقصد به الدخول الإلكتروني عن طريق الأساليب و الوسائل التقنية كالدخول لمركز النظام المعلوماتي والذي لم يحدد المشرع الجزائي الطريقة التي يتم لدخول بها ، فالجريمة تتحقق بأي وسيلة، ومن أكثر التقنيات استعمالا لتحقيق الدخول الى النظام...¹ نذكر منها :

- استخدام البرامج المصممة لاختراق أنظمة الحماية:

وهي برامج مصممة خصيصا من طرف أشخاص مختصين يسمون القراصنة أو الهاكرز تستخدم لفك التشفير واختراق أنظمة الحماية للمواقع الحكومية أو الخاصة التي تحتوي معطيات الأشخاص وهي التقنيات والبرامج التي تعرف بما يلي:

-**الفخ :** وهو عبارة عن منفذ يجهز به النظام مسبقا من قبل مصمم النظام ليسمح له لاحقا بانزال برامج تعيق سير عمله.

-**التخفي:** ويعني انتحال صفة من له الحق في الدخول الى النظام ثم الحصول على كل امتيازاته في الاطلاع على المعلومات .

- **القناة المخفية:** وهو من أخطر الاعتداءات ،يتطلب ذكاءا فائقا من المعتدي لاختراق سياسة الأمن والحماية المعتمدة في الأنظمة المعلوماتية لتهرب المعلومات .

التسلل: ومعناه التسلل وراء مستعمل مرخص له بالدخول الى النظام المعلوماتي، وتخطي حاجز الدخول.

ثانيا- جرائم الاعتداء على المعطيات في أنظمة المعالجة الآلية:

¹راضية عيمور ، الجريمة الإلكترونية وآليات مكافحتها في التشريعات الجزائرية، جامعة الاغواط ،المجلة الاكاديمية للبحوث القانونية والسياسية ، العدد الأول، المجلد السادس ، السنة 2022، ص 99 .

إن الاهتمام بضرورة توفير حماية قانونية للبرامج والمعلومات بصفة عامة و الحماية الجنائية بصفة خاصة يعود إلى ضخامة الاستثمارات المادية والبشرية في قطاع المعلوماتية وقد حدد المشرع الجزائري جرائم الاعتداء على المعطيات في نظام المعالجة الآلية في المادة "394 مكرر"، مثل القرصنة وسرقة المعلومات ، أو الخاصة بإتلاف برامج الحاسوب و معلوماته، وأقر بعقوبات مختلفة في قانون العقوبات تتنوع بين غرامات مالية و الحبس، و سيتم التطرق إليها في المطلب الموالي...¹

المطلب الثاني: الصور الجرمية للجريمة الالكترونية

الفرع الأول: الجرائم التي تقع على الأشخاص :

هي الجرائم التي تنال بالاعتداء أو تهدد بالخطر الحقوق ذات الطابع الشخصي البحث، أي الحقوق اللصيقة بالشخص والتي تعتبر من بين المقومات الشخصية وتخرج عن دائرة التعامل الاقتصادي، ومن أهم هذه الحقوق الحق في الحياة والحق في سلامة الجسم وفي الحرية والحق في صيانة الشرف ومن هذه الجرائم نتطرق إلى كل من الجرائم التالية :

أولا- جريمة انتحال الشخصية :

هي جريمة قديمة جدا تتمثل صورها في الكثير من الجرائم التي ترتكب بالطرق التقليدية، إلا أنه ومع انتشار شبكة الانترنت فقد أخذ هذا النوع شكلا جديدا وهي انتحال شخصية الفرد على الشبكة الالكترونية واستغلالها أسوء استغلال وذلك بأخذ البيانات الشخصية كالعنوان وتاريخ الميلاد ورقم الضمان الاجتماعي وما شابهها من أجل الحصول على بطاقات ائتمانية وغيره،

¹راضية عيمور ، نفس المرجع السابق ص ص99

ومن خلال هذه المعلومات يستطيع المحرم إخفاء شخصيته الحقيقية والتصرف بحرية تحت اسم مستعار، وغالبا ما يتحصل المنتحل على تلك المعلومات عن طريق الكم الهائل من الإعلانات التي تزدحم بها شبكة الانترنت...¹.

ثانيا - جريمة المضايقة والملاحقة :

وهو نوع حديث من الجرائم المتزايدة باستمرار مع كل إضفاء وتحديث يطال برامج الحوارات المتبادلة والردشة، وهي عبارة عن مساحات معروفة في الفضاء الإلكتروني تتيح لمستخدميها الاشتراك في محادثات بين بعضهم البعض.

وجرائم الملاحقة تشمل رسائل تهديد وتخويف ومضايقة وقد شبه القضاة هذه الجريمة خارج الشبكات بجرائم التهديد العلني، ولا تتطلب الجريمة المرتكبة عبر الإنترنت أي اتصال مادي بين المجرم والضحية مما يدل أن لها تأثيرات سلبية نفسية فهي لا تؤدي إلى أي تصرفات عنف مادية...².

ثالثا - جرائم التغيرير والاستدراج :

هيمن أشهر جرائم الانترنت ومن أكثرها انتشارا خاصة بين أوساط صغار السن من مستخدمي الشبكة، وهي تقوم على عنصر الإيهام حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين علاقة صداقة أو زواج على الانترنت والجريمة المعلوماتية التي قد تتطور إلى لقاء مادي بين الطرفين، وهذه الجرائم لا تعرف الحدود ولا يمكن حصرها، وهي دون حدود سياسية أو اجتماعية

¹. منير محمد الجنبيهي، جرائم الانترنت والحاسب الآلي وسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005، ص 12 .

² محمد أمين احمد الشوابكة، جرائم الحاسوب الأولى والانترنت، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، 2004، ص 45 .

اذ يستطيع كل مراسل عبر الشبكة ارتكابها بكل سهولة وكذلك يقع ضحيتها أي مستخدم حسن النية...¹.

رابعاً- جرائم التشهير وتشويه السمعة :

مع انتشار الشائعات والأخبار الكاذبة التي تطول وتمس رموز الشعوب سواء كانت تلك الرموز فكرية أو سياسية أو حتى دينية، وقد ظهرت على شبكة الانترنت بعض المواقع والتي جندت نفسها لهدف واحد هو خدمة تلك الشائعات والأخبار الكاذبة وذلك بهدف تشهير وتشويه سمعة تلك الرموز، وكذلك لتسميم أفكار الناس أو محاولة ابتزاز بعض الأشخاص بنشر الشائعات عنهم.

وأبرز وسائل ارتكاب هذه الجريمة إنشاء مواقع على الشبكة تحتوي المعلومات المطلوب ادراجها ونشرها أو إرسالها عبر المواقع الإلكترونية، ومن أمثلتها إرسال الصور الغير اللائقة أو معلومات غير صحيحة...²

خامساً- الجرائم المخلة بالأخلاق والآداب العامة :

إذا كانت شبكة الانترنت تتسم بالعالمية ولا تقتصر علمستخدم دون الآخر، فإن ما يتم عرضه من مواد تعد مخلة بالآداب والأخلاق العامة في بلد معين قد تشكل جريمة يعاقب عليها القانون في حين أنها لا تكون كذلك في أي بلد آخر، وتشمل هذه الجرائم تحريض القاصرين على أنشطة جنسية غير مشروعة وإفسادهم عبر الوسائل الإلكترونية أو محاولة إغوائهم لارتكاب هذه الأنشطة، أو نشر معلومات عنهم عبر الحاسب الآلي ودعوتهم إلى القيام بالأعمال الفاحشة، وتصوير قاصرين ضمن أنشطة للجنس.

¹ عبد الكريم شيباني، الحماية الإجرائية والموضوعية للجريمة المعلوماتية، مذكرة لنيل شهادة ماستر، كلية الحقوق والعلوم السياسية، جامعة د. الطاهر مولاوي، سعيدة ، سنة 2016 / 2015 ، ص 19 .

² منير محمد الحنبيهي، ممدوح محمد الجنيبيهي ، المرجع السابق، ص 13

والأعمال الإباحية هي من أشهر الأعمال الحالية وأكثرها رواجاً خاصة في الدول العربية وأوروبا والدول الآسيوية، وتشمل الجرائم المخلة بالأخلاق والآداب العامة على الانترنت كافة الإشكال سواء كانت صور أو فيديو أو حوارات أو أرقام هاتفية مما خول هذه الشبكة أن تكون في متناول أيدي الجميع ودون أي حواجز...¹.

الفرع الثاني: الجرائم التي تقع على الأموال :

هي جرائم الاعتداء على الأموال والتي تهدد الحقوق ذات القيمة المالية ويدخل في نطاق هذه الحقوق الحق ذو قيمة اقتصادية.

فإذا كان موضوع الاعتداء على الأموال في نطاق ما ينصب على الحاسب الآلي ذاته وما يرتبط به من أسلاك وما يتصل به من ملحقات فإنه هنا لا يثير أي صعوبة في تطبيق النصوص الجزائية التقليدية كون الأمر يتعلق بمال عادي منقول، أما إذا وقع الاعتداء على ما يتعلق بفن الحاسب الآلي من برمجيات النظام فإن النصوص التشريعية التقليدية قاصرة عن حمايتها لما لهذا المجال من طابع خاص غير تقليدي....².

أولاً- جرائم صناعة ونشر الفيروسات :

الفيروس هو برنامج مثل أي برنامج آخر موجود على جهاز الحاسب الآلي، ولكنها مصممة بحيث يمكنها التأثير على كافة البرامج الأخرى الموجودة على الجهاز بأن تجعل تلك البرامج نسخة منها أو أن تعمل على مسح كافة البرامج الأخرى وبالتالي تعطلها عن العمل.

وأما عن مبدأ عملها فيتحدد طبقاً لأسلوب تصميمها، فقد تبدأ بالعمل بمجرد فتح الرسالة الموجودة بها، وقد تبدأ بمجرد تشغيل البرنامج الموجودة عليه، وتعتبر هذه الصناعة من أهم جرائم الانترنت أو أكثرها اتساعاً وانتشاراً، ويعود تاريخ الفيروسات لأول مرة في أربعينيات القرن

¹انظر محمد امين احمد الشوابكة، المرجع أعلاه، ص. 114 .

²انظر محمد امين احمد الشوابكة، المرجع السابق، ص. 136

الماضي حين تحدث عنها العالم الرياضي "فون نيو مان" على صعيد الحاسب الآلي دون الانترنت، ومن أشهرها "فيروس رسائل الحب"، "فيروس الدودة الحمراء"، وقد أحدث هذا الأخير أعطالا في أكثر من ربع مليون جهاز كمبيوتر في اقل من 9 ساعات عام 2001...¹

ثانيا- جرائم الاختراقات :

الاختراق هو عبارة عن عملية دخول غير مصرح به إلى أجهزة الغير أو للشبكات الالكترونية، ويتم هذا الاختراق بواسطة برامج متطورة يستخدمها كل من يملك الخبرة وله القدرة على تخطي أي إجراءات أو أنظمة حماية اتخذت لحماية تلك الحاسبات أو الشبكات. وتختلف أسباب الاختراق باختلاف أهداف المخترق، فمنهم من يخترق أجهزة البعض أو مواقعهم لمجرد الفضول والبعض الآخر لسرقتها، وهذا هو السبب الأبرز الذي يدفع المخترقين إلى الدخول إلى مواقع الحواسيب الأخرى لسرقة معلوماتهم التي قد يكونون قد عرضوها مقابل مبلغ مالي للاطلاع عليها. وقد يكون السبب تبديل أو تحريف أو تعطيل المعلومات في أجهزة الغير، وهو أخطر أنواع الاختراق، ومن أبرز ضحايا الاختراق فهي مواقع الانترنت التي يقوم المخترقون بتحريف تصاميمها ومعلوماتها وهذه العملية تسمى تغيير وجه الموقع.....²

ثالثا - جريمة تعطيل الأجهزة والشبكات :

يطال التعطيل أجهزة الحاسب الآلي عبر برامجها، كما قد يؤدي تعطيل البرامج إلى أعطال فنية تقع على القطع الالكترونية للجهاز والهدف من التعطيل منع الحواسيب والشبكات من تأدية عملها دون أن تتم عملية اختراق فعلية لتلك الأجهزة وتتم عملية تعطيل الأجهزة عن طريق

¹ منير محمد الحنيهي ممدوح محمد الحنيهي، المرجع السابق ، ص. 36

² نفس المرجع ، ص . 37

إرسال عدد هائل من الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المأرود تعطيلها وهو الأمر الذي يعيقها عن تأدية عملها(13)....¹

رابعاً - جريمة النصب والاحتيال :

أصبح التعاقد عبر الانترنت حاجة وضرورة نظراً لسرعة وسهولة التعامل عبرها، لكن هذه الميزة ما لبثت أن شابتها سلبيات عديدة هي عبارة عن أفعال إجرامية تعرف بالنصب والاحتيال² ومن بينها:

- خرق التعاملات عبر طرق احتيال جديدة تم ابتكارها، وكذلك ازدت من وقوع جرائم النصب التيليزال يقع فيها عدد كبير من مستخدمي الانترنت.

- أما المظهر الأبرز للاحتيال فهو سرقة معلومات البطاقات الائتمانية واستخدام هذه المعلومات لسرقة المبالغ الموجودة داخل حسابات الضحايا، ومرتكبوا الجرائم عبر تلك الوسائل يسهل هروبهم وتواريتهم لذلك من الصعب جداً ملاحقتهم والقبض عليهم.

المبحث الثاني: المسؤولية الجزائية عن الجرائم الإلكترونية .

تعرف المسؤولية الجزائية بشكل عام بأنها عبارة عن التزام بتحمل الجزاء الذي ترتبه القواعد القانونية كأثر للفعل الذي يرتكب خروجاً على أحكامها....³

المطلب الأول: شروط مساءلة الشخص الطبيعي البالغ والحدث عن الجرائم الإلكترونية.

¹ - منير محمد الحنيهي ممدوح محمد الحنيهي، مرجع سابق، ص. 38

² - عبدالكريم شيباني، مرجع سابق، ص 23

³ كمال الدين محمد ، أحكام المسؤولية الجنائية ، أساسها و تطورها ، ط2، دار النهضة العربية ، 1991

الفرع الأول : المسؤولية الجزائية للشخص البالغ عن الجرائم الإلكترونية:

والمسؤولية الجزائية للشخص الطبيعي البالغ عن الجرائم الإلكترونية هي التزام الفرد بتحمل النتائج العقابية الناتجة عن أفعال غير مشروعة يرتكبها باستخدام التقنيات الحديثة. فهناك ارتباط وثيق بين المسؤولية الجزائية وبين الجريمة كواقعة أو حقيقة قانونية ، فلا قيام لتلك المسؤولية دون مرتكب الجريمة أو المسؤول عنها، وأن المجرم لا يتخذ هذه الصفة إلا بعد ثبوت ارتكابه الجريمة المنصوص عليها في قانون العقوبات.....¹.

وتعتمد المسؤولية الجزائية للشخص الطبيعي البالغ على عدة أسس أو أركان أهمها :

أولا- أركان وأسس قيام المسؤولية الجنائية عن الجرائم الإلكترونية للشخص البالغ.

1-الركن الشرعي : المتمثل في وجود نص قانوني في قانون العقوبات يجرم الجرائم الإلكترونية والتي نص عليها المشرع الجزائري في المادة 2 من قانون رقم 09-04 حيث جرم الأعمال الماسة بأنظمة المعالجة الآلية للمعطيات في مواد من 394 مكرر إلى 394 مكرر 7 من قانون العقوبات.....².

2- الركن المادي: أي قيام الشخص بسلوك إجرامي إلكتروني كالدخول أو البقاء غير المشروع في أنظمة المعالجة الآلية للمعطيات غير المصرح به والتسلل لنظم المعلومات والتلاعب بالمعطيات، سواء بالإدخال أو التعديل أو الإزالة...³، أو الاحتيال المعلوماتي باستخدام التكنولوجيا للحصول على أموال بطرق غير مشروعة.

¹ خلفي عبد الرحمان ، الإجراءات الجزائية في التشريع الجزائري ، دار بلقيس ، 2015، ص 91

² عائشة فاضل : المسؤولية الجزائية في الجرائم الإلكترونية (الجزائر نموذجاً) مجلة الحقوق و الحريات ، مجلد 11 ، ص 615:

³ محمد خليفة ، خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مواجهتها، كلية الحقوق والآداب والعلوم الاجتماعية، جامعة 08 ماي 45 قالمة.

3- الركن المعنوي: توفر القصد الجنائي أي انصراف إرادة الفاعل إلى تحقيق النتيجة الإجرامية بوعي و إدراك.

4- الإدراك والتمييز: يجب أن يكون الشخص عاقلا وبالغا ليتحمل مسؤولية أفعاله.

ثانيا-العقوبات المقررة للشخص الطبيعي البالغ عن الجرائم الإلكترونية .

طبقا لقانون العقوبات بناء على المواد 11-12-13 من الاتفاقية الدولية للإجرام المعلوماتي يجب أن تكون العقوبات رادعة وتتضمن عقوبات أصلية و عقوبات تكميلية تطبق على الشخص الطبيعي والمعنوي، وتنقسم العقوبات المطبقة على الشخص الطبيعي إلى :

1_ العقوبات الأصلية :

ينص المشرع الجزائري في المادة 394مكرر من قانون العقوبات على عقوبة الحبس تتراوح من ثلاثة أشهر إلى سنة حسب الفعل المرتكب، وبغرامات مالية تتراوح بين (50000 دج) إلى (200000 دج) لكل من يدخل أو يبقى عن طريق الغش في كل جزء من منظومة المعالجة الآلية للمعطيات...¹.

وتضاعف العقوبة إذا درست هذه الأفعال حذف أو تقييم المعطيات، الاعتداء العمدي على منظومة المعطيات...التي تكون عقوبته بالحبس من 6 أشهر الى سنتين وغرامة مالية من 50000 الى 150000 .

¹نادية لاکلي ، الجريمة السيبرانية في الجزائر والعقوبات المقررة لها، مجلة الاجتهاد القضائي، المجلد 15 العدد 01 مارس 2023، مدونة الثقافة القانونية، ص 269.

2- العقوبات التكميلية :

إضافة إلى العقوبات الأصلية، ينص المشرع على عقوبات تكميلية للتشديد من ردع هذه الجرائم، وتتمثل هذه العقوبات في مصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجريمة الماسة بالأنظمة المعلوماتية، مع مراعاة حقوق الغير وإغلاق المواقع التي تكون محلا لممارسة الجرائم الماسة بالأنظمة المعلوماتية، و إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالکها حسب (المادة 394 مكرر).

كما أصبح الشروع في الجريمة معاقب عليه بنفس العقوبة المقررة على الجنحة ذاتها حسب ما جاءت به المادة 11. فتشترك جرائم المعطيات في ثلاثة أحكام تتعلق بالعقوبة، أولاها تتعلق بالعقوبات التكميلية، فكل جرائم المعطيات لها نفس العقوبات التكميلية وهي المصادرة والغلق حسب (المادة 394 مكرر 06)...¹.

والثانية تتعلق بتشديد العقوبة على الشخص المعنوي، فقد نصت المادة 394 مكرر 04 على مضاعفة عقوبة الشخص المعنوي الذي يرتكب جرائم المعطيات إلى خمسة أضعاف ما هو مقرر للشخص الطبيعي.

والثالثة هي تشديد عقوبة تلك الجرائم إلى الضعف إذا ارتكبت ضد مؤسسات الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام "المادة 394 مكرر 04".

الفرع الثاني : مسؤولية الشخص الحدث عن الجرائم الإلكترونية.

¹ د. محمد خليفة ، خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مواجهتها، ص 386 ، كلية الحقوق والأداب والعلوم الاجتماعية جامعة 08 ماي 45 قلالة.

إن الصغير يولد فاقد الإدراك ، إلا أن عقله يبدأ بالنمو تدريجيا حتى يصل مرحلة الإدراك التام، أي مرحلة النضوج والخبرة اللازمين لإدراك ماهية أفعاله ، والإحاطة بالنتائج المادية والمعنوية التي تترتب عن مخالفته القوانين والأنظمة، والإدراك التام يبدأ بإكمال سن 18، ومع ذلك فإن المشرع الجزائري قد نص على اعتبار القصر الذين لم يكملوا 13 مسؤولون جزائيا ، عن الجريمة التي يرتكبونها ، ولا يعد قصرهم مانعا من موانع المسؤولية الجزائية ، لكن لاتفرض في حقهم أي عقوبة جزائية ، وإنما مجرد تدابير حماية ، حيث ينص في المادة 49/1 من قانون العقوبات على أن لاتوقع على القاصر الذي لم يكمل الثالثة عشر الا لتدابير الحماية أو التربية¹.

كما تحكم المسؤولية الجنائية للطفل القاصر " دون سن 18 سنة" عند ارتكابه جرائم الكترونية إلى قواعد عامة تحدد أهليته ونصوص خاصة بالتجريم الرقمي

القواعد العامة التي تحدد مسؤولية وأهلية القاصر والنصوص الخاصة

- تحدد المسؤولية الجنائية للقاصر عن الجرائم الالكترونية كم يلي :

حسب المادة 62 يمارس وكيل الجمهورية الدعوى العمومية لمتابعة الجرائم التي يرتكبها الأطفال ، فاذا كان الأطفال :

دون 10 سنوات فهو منعدم المسؤولية الجزائية تماما ولا يتابع قضائيا .

من 10 سنوات إلى 13 سنة : فحسب المادة 72 من قانون حماية الطفل 15- 12 فلا يمكن وضع الطفل الذي يقل سنه عن 13 سنة ، رهن الحبس المؤقت الا استثناء ، كما لا يمكن في مواد الجناح اذا كان الحد الأقصى للعقوبة المقررة أقل من 3 سنوات أو يساويها ، وضع الطفل رهن الحبس المؤقت ، فهو ذو مسؤولية ناقصة لا يخضع لعقوبات سالبة للحرية ، بل يطبق عليه قاض الأحداث تدابير الحماية والتهديب (كالتوبيخ أو التسليم للوالدين).

من 13 سنة إلى 18 سنة : ²ولا يجوز حسب المادة 73 من القانون 15- 12 ايداع الطفل الذي يبلغ سن 16 عشر الى أقل من 18 سنة رهن الحبس المؤقت الا لمدة شهرين قابلة للتجديد مرة

قراوي كلثوم ، جريمة الاحتيال الالكتروني ، أطروحة دكتوراة علوم في القانون العام ، كلية الحقوق ، جامعة الجزائر 1، سنة 2024-

¹2025، ص105.

²القانون 15- 12 ، المادة 73، والمادة 72.

واحدة، كما أنه يستفيد من مسؤولية مخففة حيث يجوز لقاضي الأحداث تطبيق تدابير الحماية أو إيقاع عقوبات جزائية مخففة "تخفف العقوبة المقررة للجريمة إلى النصف ، وتستبدل عقوبة الإعدام أو السجن المؤبد" ، بالحبس من " 10 إلى 20 سنة " ¹.

ثانيا- نصوص تجريم الأفعال الإلكترونية .

تكشف أفعال القاصر الرقمية بناء على المواد التالية من (ق ع) والقوانين مكملة له :

- المادتان (298 و 299 ، ق ع) : التي تجرم القذف والسب عبر الانترنت ومنصات التواصل .
- المادة (303 مكرر من ق ع) : تجريم مساس الحياة الخاصة للأفراد " كنشر الصور والفيديوهات دون إذن .
- قانون 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها (مثل القرصنة، اختراق الأنظمة، والابتزاز الإلكتروني).
- تتم محاكمة القاصر حصرا أمام محكمة الأحداث في جلسات سرية مراعاة لمصلحته الفضلى .
- المطلب الثاني: المسؤولية الجزائية للشخص المعنوي عن الجرائم الإلكترونية .

الفرع الأول : شروط مساءلة الشخص المعنوي عن الجريمة الإلكترونية.

تتم مساءلة الشخص المعنوي مثل الشركات والجمعيات عن الجرائم الإلكترونية بناء على قواعد قانونية محددة تهدف إلى منع استغلال الهياكل المؤسسية في تنفيذ الهجمات السيبرانية أو عمليات الاحتيال الرقمي، و هذا وفقا لقانون العقوبات :

¹ الأمر رقم 66-156 المتضمن قانون العقوبات ، المعدل والمتمم، المادتان 49، 50 ، المؤرخ 08 جوان 1966 والمواد: 04، 91 ، 94، 113 ، قانون حماية الطفل 15-12 ، المؤرخ في 15 جوان 2015 .

أولاً- أن يكون الشخص المعنوي خاضعا للقانون الخاص : حيث يطبق على الشركات التجارية والجمعيات والشركات المدنية وعادة ما تعفى الدولة و الجماعات المحلية البلديات والولايات و الأشخاص المعنوية التابعة للقانون العام من المسؤولية الجزائية، لكنها قد تسأل مدنيا...¹

صدور الفعل من أجهزة أو ممثلين شرعيين : حيث يجب أن يكون الشخص المعنوي ممثلا قانونيا يملك سلطة اتخاذ القرار والتوقيع أو الأشخاص المفوضين رسميا للعمل باسم الكيان.

ثانيا- وقوع الجريمة لحساب الشخص المعنوي : وهو شرط جوهري، حيث يجب أن يثبت أن الجريمة الإلكترونية ارتكبت من أجل تحقيق ربح مادي للشركة مثل سرقة بيانات المنافسين، أو لخدمة أهداف المؤسسة مثل التهرب الضريبي عبر التلاعب بأنظمة المعالجة الآلية .

وجود نص قانوني صريح يقرر المسؤولية : فوفقا لمبدأ " لا جريمة و لا عقوبة إلا بنص " يجب أن ينص قانون مكافحة الجرائم المعلوماتية أو قانون العقوبات صراحة على إمكانية معاقبة الشخص المعنوي في تلك الجريمة المحددة مثل: (المادة 394 مكرر 4 من قانون العقوبات) المدرجة بموجب القانون رقم :15/04 الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات التي نصت " يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل(5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي".²...

الفرع الثاني : العقوبات المقررة للشخص المعنوي عن الجرائم الإلكترونية .

¹ هباش عمران ، المسؤولية الجزائية للشخص المعنوي عن جرائم الصرف ،مذكرة دكتوراه،جامعة محمد بوضياف المسيلة ،سنة 2018،ص 10 .

² القانون 15/04 المعدل والمتمم لقانون العقوبات , مادة 394 مكرر 4 ص 4 .

يسأل الشخص المعنوي عن هذه الجرائم، سواء بصفته فاعلا أصليا أو شريكا أو مت دخلا كما يسأل عن الجريمة التامة أو الشروع فيها بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة أحد أعضائه وممثليه، وبالتالي فإن عقوبة الشخص المعنوي تتمثل في الغرامة التي تعادل (05) خمس مرات الحد الأقصى المقرر للشخص الطبيعي علما أن نص المادة 18 مكرر، فلقد تضمنت نصوص المواد 51 مكرر و 18 مكرر المستحدثة بموجب القانون رقم 15/04 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات قرار المسؤولية الجزائية متى قامت شروطها.

أولا - العقوبات الأصلية (الغرامة) :

والتي تتضاعف من مرة إلى (05) خمس مرات للحد الأقصى للغرامة المقررة للشخص الطبيعي.

ثانيا - العقوبات التكميلية : تتمثل في :

- حل الشخص المعنوي.
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز (05) خمس سنوات.
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز (05) خمس سنوات.
- المنع من مزاوله نشاط أو عدة أنشطة مهنية بشكل مباشر أو غير مباشر نهائيا لمدة لا تتجاوز (05) خمس سنوات.
- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.
- نشر و تعليق حكم الإدانة.

-الوضع تحت الحراسة القضائية لمدة لا تتجاوز (05) خمس سنوات، وتنص الحراسة على ممارسة النشاط الذي أدى إلى ممارسة الجريمة .

حيث سن المشرع الجزائري عدة قوانين تخص الجريمة الالكترونية وتتمثل قي :

ثالثا- القوانين المتعلقة بالجريمة الإلكترونية في الجزائر:

1- قانون العقوبات الجزائري:

التعديل رقم 04-08 الذي دخل حيز التنفيذ في عام 2004، يعالج الجرائم المتعلقة باستخدام تكنولوجيا المعلومات والاتصالات، ويوضح مختلف الجرائم الإلكترونية مثل الاحتيال عبر الإنترنت، التسلل إلى أنظمة الكمبيوتر، وتعطيل الأنظمة.

2- قانون مكافحة جرائم المعلوماتية :

- قانون رقم 18-06:(صدر في عام 2018): ويعد القانون الجزائري الأكثر شمولاً لمواجهة الجرائم المرتبطة بالتكنولوجيا الحديثة. يهدف هذا القانون إلى مواجهة جريمة القرصنة الإلكترونية، الاحتيال الإلكتروني، التجسس، التحرش الإلكتروني، و التهديدات عبر الإنترنت.

- المادة 32 من قانون الإعلام:

- تنص على أنه في حال استخدام الإنترنت لنشر معلومات كاذبة أو تهديدات، فإن الشخص المرتكب لهذه الأفعال يعرض نفسه لعقوبات تصل إلى السجن .

الخاتمة

مما سبق ذكره نجد أن الجرائم الالكترونية تعتبر إحدى أخطر الأوجه السلبية للتطور السريع الذي مس جميع المجالات العلمية والتكنولوجية في عصرنا الحالي ، والتي عانت منها الدول المتقدمة قبلنا بسبب تنوع أساليب ارتكاب الجرائم الالكترونية كما وكيفا، مما أوجد صعوبة في مكافحتها. ولقد استعصى تعريف الجريمة الالكترونية في مختلف التشريعات حتى وصفت بالجريمة المستعصية التعريف ، في حين عرفها المشرع الجزائري من خلال قانون 04-15 في القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات ، فتتحقق الجريمة الالكترونية بمجرد أن ترتكب الجريمة ، او يسهل ارتكابها عن طريق منظومة معلوماتية ، أو نظام للاتصالات الالكترونية.

إن المشرع الجزائري قد تبنى سياسة مزدوجة للتصدي للجريمة الالكترونية ، بحيث وضع من جهة العديد من القوانين والمراسيم والأجهزة لمكافحة الجريمة الالكترونية ، من خلال تعديل الجوانب والآليات الموضوعية والإجرائية للتشريعات العقابية (قانون العقوبات وقانون الإجراءات الجزائية) ، والتي تجرم العديد من الأفعال كالمساس بأنظمة المعالجة الآلية للمعطيات ، كما قام بتكييف آليات إجرائية تتعلق بتمديد الاختصاص للأقطاب الوطنية في مرحلة أولى ، كما استحدث سنة 2021 قطب وطني يعالج القضايا المعقدة للجريمة الالكترونية عبر الوطن ، للبحث والتحري عن مرتكبيها ، بموجب مختلف القوانين التي سنها بدءا بقانون العقوبات 01-09 المتعلق بتجريم السب والقذف عبر وسائل الاتصال لمختلف هيئات و مؤسسات الدولة، وبعدها دائما ما سعى لوضع قوانين تتلاءم مع هذه الظاهرة المستجدة ، فوضع مفهوما موسعا للجريمة الالكترونية من خلال قانون 09-04، كما عدد مختلف الجرائم والأفعال في التعديل الذي جاء به قانون العقوبات في القانون 04-15، الأمر 20-06 .

الخاتمة

- إن المشرع الجزائري لم يستصدر قانونا جامعاً لمختلف صور الجريمة الالكترونية، وإنما حددها من خلال قانون العقوبات ومختلف التعديلات التي جاءت فيه من خلال عدة قوانين مثل القانون 07-18، والأمر 11-21، والمرسوم الرئاسي 21-439.

هذا التنوع التشريعي من شأنه أن يساهم بشكل فعال في الوقت الراهن للحد من تفاقم ظاهرة الإجرام الالكتروني في الجزائر.

- تعتبر الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها (المرسوم الرئاسي 21-493)، من أبرز هيئات المشرع الجزائري لمكافحة الجريمة الالكترونية.

- ان الجريمة الالكترونية تقترب في بيئة المعالجة الآلية للبيانات، وتنتقل بسهولة عبر العالم الافتراضي غير معرفة بالحدود الاقليمية و السياسية للدول، لذلك جاءت العديد من الاتفاقيات الدولية لمحاربتها أهمها اتفاقية الأمم المتحدة.

- ان الصعوبات المتعلقة بالجرائم المعلوماتية وخصوصيتها تستدعي لمواجهتها اتخاذ تدابير عدة منها:

- التكوين المستمر للأجهزة المكلفة بالتحقيق في الجرائم الالكترونية وكيفية التعامل مع الأدلة الالكترونية.

- الاستعانة بالخبرة الفنية العمالية في المجال المعلوماتي لتحديد نوعية الأدلة الالكترونية، واستخدام أساليب الفحص والتدقيق لاستخراجها.

- اتخاذ السلطات المختصة في الجانب المعلوماتي تدابير لرصد حركة هواة الحاسب الآلي ، وحركة المشبوهين في الجرائم المالية والمخدرات ، وجرائم الاستغلال الجنسي للأطفال ورصد مختلف المواقع المشبوهة ، اضافة الى متابعة المسجلين في جرائم التزوير و الاحتيال.

- تحسيس المواطن بدوره في وجوب التبليغ عن الجرائم المعلوماتية بمختلف أنواعها.

الخاتمة

-تحسيس المجتمع وخاصة الأولياء بالجانب السلبي للتكنولوجيات الحديثة ، وبوجوب حماية القصر عبر الانترنت ، مع وجوب التبليغ عن التهديدات التي يتعرض لها القصر بأي شكل من الأشكال.

-تفعيل دور وسائل الاعلام المختلفة عن أماكن تلقي البلاغات في الجرائم المعلوماتية .

ومن هنا فقد أصبح لزاما على الدول من أجل مواكبة عصر المعلوماتية ومواجهة الجرائم الالكترونية بتعدد أشكالها تعزيز التعاون الدولي ووضع تشريعات من خلال اتفاقيات ومعاهدات لتسهيل الوصول للمجرمين ، في ظل تحول المجتمعات الى مجتمعات معلوماتية تعتمد على التقنية الرقمية في أداء أعمالها .

المقترحات

وفي ضوء التطور المتسارع لهذه الجرائم، يمكن اقتراح جملة من التوصيات، من أهمها:

1. إنشاء هيئة وطنية جديدة متخصصة لمراقبة جرائم الإنترنت ورصد تطوراتها، وتقديم الاستشارات القانونية والإجرائية للجهات المختصة.
2. مراجعة وتعديل قانون العقوبات وقانون الإجراءات الجزائية بما يتلاءم مع طبيعة الجرائم الإلكترونية وأساليب ارتكابها الحديثة.
3. العمل على وضع تعريف قانوني موحد للجريمة المستحدثة (الالكترونية) يشمل مختلف صور السلوك الإجرامي المعلوماتي.
4. تعزيز الوعي المجتمعي بمخاطر الجرائم الإلكترونية وبيان آثارها القانونية والعقوبات المترتبة عليها.
5. إدراج مواد دراسية تتعلق بالأنظمة المعلوماتية والجرائم الإلكترونية في المناهج التعليمية، وخاصة في كليات الحقوق والمعاهد القضائية، بما يساهم في إعداد كوادر مؤهلة للتعامل مع هذا النوع من الجرائم.

ملخص الدراسة

أدى التطور المتسارع لتكنولوجيا الإعلام والاتصال إلى ظهور فضاء رقمي جديد يُعرف بالفضاء لسيراني، والذي أحدث تغيرات كبيرة في حياة الأفراد والمؤسسات. ورغم ما وفره هذا الفضاء من مزايا عديدة، فقد صاحبه انتشار أنماط جديدة من الجرائم عُرفت بالجرائم الإلكترونية أو المعلوماتية، والتي تتطور باستمرار مع تطور التقنيات الحديثة.

وتشمل هذه الجرائم العديد من الأفعال غير المشروعة، مثل الاختراق وسرقة البيانات والابتزاز الإلكتروني والاحتيال عبر الشبكات، كما قد تمتد آثارها إلى المؤسسات والدول من خلال استهداف الأنظمة والشبكات الحيوية وتعطيل الخدمات الأساسية. ويستغل مرتكبو هذه الجرائم التقنيات الرقمية لتنفيذ أفعالهم الإجرامية بسهولة وسرعة، مما يسبب أضراراً مادية ومعنوية جسيمة.

وانطلاقاً من خطورة هذه الظاهرة، يهدف هذا البحث إلى بيان مفهوم الجريمة الإلكترونية وخصائصها، وبيان أهم الآليات القانونية التي اعتمدها المشرع الجزائري لمكافحتها، مع دراسة المسؤولية الجنائية المترتبة عنها، سواء تعلق الأمر بالشخص الطبيعي أو الشخص المعنوي، وذلك في إطار تعزيز الحماية القانونية للأفراد والمؤسسات في البيئة الرقمية.

الكلمات المفتاحية: الجريمة الإلكترونية، الجرائم المستحدثة، المجرم الإلكتروني، المسؤولية الجنائية، المساءلة الجزائية.

Abstract :

The rapid development of information and communication technologies has led to the emergence of a new digital environment known as cyberspace. While this environment has provided numerous benefits for individuals and institutions, it has also facilitated the spread of new forms of crime,

commonly referred to as cybercrime or computer-related crime, which continue to evolve alongside technological advancements.

Cybercrime encompasses a wide range of illegal activities, including hacking, data theft, electronic blackmail, and online fraud. The impact of these crimes extends beyond individuals to affect institutions and even states, particularly through attacks targeting critical networks and infrastructure or disrupting essential services. Cybercriminals exploit modern technologies and information networks to carry out their unlawful activities with greater speed and efficiency, causing significant material and moral harm.

Given the seriousness of this phenomenon, this research aims to examine the concept and characteristics of cybercrime, as well as the legal mechanisms adopted by the Algerian legislator to combat it. The study also addresses the criminal liability arising from such offenses, whether committed by natural persons or legal entities, with the objective of strengthening legal protection for individuals and institutions within the digital environment.

Keywords: Cybercrime; Cybercriminal; CriminalLiability; CriminalAccountability.

قائمة المصادر

و

المراجع

المصادر :

* المصادر الخارجية:

- 1- الاتفاقية بودابست بشأن الجرائم الإلكترونية، الموقعة في بوداست في تاريخ 23 نوفمبر 2001 .
- 3- .الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة في القاهرة في 31 ديسمبر 2010.

* النصوص القانونية :

- القانون رقم 09-04، المؤرخ في فيفري 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ، الجريدة الرسمية عدد47، الصادرة بتاريخ 16 فيفري 2009.

-القانون رقم 18-04 المؤرخ في 10 مايو 2018، المتضمن تحديد القواعد المتعلقة بالبريد والاتصالات الالكترونية ، الجريدة الرسمية ، عدد27، الصادرة في 13 مايو 2018.

-القانون رقم 18-07 مؤرخ في 10 جوان 2018، متعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ، الجريدة الرسمية عدد 34، الصادر بتاريخ 10 جوان 2018.

-قانون حماية الطفل 15-12 ، المؤرخ في 15 جوان 2015 .

-القانون 15/04 المعدل والمتمم لقانون العقوبات, المادة 394.

-الأمر رقم 66-156 المتضمن قانون العقوبات ، المعدل والمتمم، المادتان ، المؤرخ 08 جوان 1966 .

* المراجع :

• الكتب

- خالدعباد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والانترنت ، الطبعة الأولى، دار الثقافة ، سوريا ، 2001.
- أحمد خليفة،الجرائم المعلوماتية، دار الفكر الجامعي،الطبعة الثانية،الإسكندرية، ط2006.
- ربيحة زيدان ، الجريمة المعلوماتية في التشريع الجزائري و الدولي ، دار الهدى عين مليلة ، الجزائر ، ط2011.
- رمزي حوحو، منيرة بلوغي ، مواجهة الجريمة المعلوماتية في الجزائر، مجلة الحقوق و الحريات ، جامعة محمد خيضر بسكرة ، العدد الثاني ، 2014.
- هالالي عبد الله أحمد ، التزام الشاهد و الاعلام في الجرائم المعلوماتية ، دراسة مقارنة ، القاهرة ، دار النهضة العربية 1997.
- محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الالكترونية (دراسة مقارنة)، دار الفكر والقانون للنشر والتوزيع ، الطبعة الأولى ، سنة2015.
- أسامة أحمد المناعسة، جلال محمد الزغبى، جرائم الحاسب الآلي والانترنت، دراسة تحليلية مقارنة دار وائل للنشر والتوزيع، عمان ، سنة 2001.
- بن مكي نجاة، الساسة الجنائية لمكافحة الجرائم المعلوماتية ، منشورات دار الخلدونية ، 2017.
- محمد أمين احمد الشوابكة، جرائم الحاسوب الأولى والإنترنت، دار الثقافة للنشر والتوزيع، ط2004 .

- منير محمد الجنبهي ممدوح محمد الجنبهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، ط 2005.
- سعيد مسعود الكثيري الجريمة الالكترونية في ضوء اتفاقية بودابست: الاطار المفاهيمي والتصنيفي، مجلة البحوث القانونية والاقتصادية ، المركز الجامعي بوشوشة ، آفلو، المجلد 9، العدد 1، جانفي 2026.
- د بوضياف إسمهان ، الجريمة الإلكترونية و الإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية و السياسية، جامعة محمد بوضياف، المسيلة، العدد 11 ، سبتمبر 2018.
- الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري ،مجلة إيليزا للبحوث والدراسات ، المجلد 06 / العدد : 2 السنة : 2021 .
- مهدي رضا ، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري ، مجلة اليزا للبحوث والدراسات ، المجلد 06، العدد 02، 2021.
- محمد الصغير مسيكة ، مفهوم الجرائم المستحدثة (الالكترونية)،مجلة الدراسات القانونية والسياسية ،جامعة أحمد بن يحيى الونشريسي تيسيمسيلات الجزائر، المجلد 8 العدد 1 جانفي 2022 .

● الأطروحات والمذكرات

- صيلع سعد،آليات مكافحة الجريمة الالكترونية في التشريع الجزائري ، أطروحة دكتوراة، المركز الجامعي مرسلبي عبد الله ،تيزازة، 2025/2024 .
- ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراة، كلية الحقوق ، جامعة باتنة 1، 2016/2015 .
- هباش عمران ، المسؤولية الجزائية للشخص المعنوي عن جرائم الصرف ،مذكرة دكتوراه،جامعة محمد بوضياف المسيلة ،سنة 2018 .

- بن موسى خديجة ، الحماية الجنائية للمعطيات في المجال المعلوماتي ، مذكرة ماستر قانون جنائي ، كلية الحقوق و العلوم السياسية ، جامعة غرداية ، 2022.
- عبد الكريم شيباني، الحماية الإجرائية والموضوعية للجريمة المعلوماتية، مذكرة لنيل شهادة ماستر، كلية الحقوق والعلوم السياسية، جامعة د. الطاهر مولاي، سعيدة ، سنة 2016 / 2015 .

فهرس المحتويات

فهرس المحتويات :

الصفحة	العنوان
	الشكر
	الإهداء
8	المقدمة
8	أهمية الدراسة
8	أسباب إختيار الموضوع
9	الدراسات السابقة
10	صعوبات الدراسة
10	إشكالية الدراسة
11	منهج الدراسة
12	الفصل الأول :الإطار المفاهيمي للجرائم الالكترونية
14	المبحث الأول: مفهوم الجريمة الالكترونية
16	المطلب الأول: تعريف الجريمة الالكترونية
16	الفرع الأول: التعريف الفقهي للجريمة الالكترونية
18	الفرع الثاني: التعريف القانوني للجريمة الالكترونية
18	أولا- تعريف مؤتمرات هيئة الأمم المتحدة
19	ثانيا- تعريف منظمة التعاون الاقتصادي والتنمية

فهرس المحتويات :

19	ثالثا- تعريف الجريمة الالكترونية في اتفاقية بودابست
20	رابعا- تعريف الجريمة الالكترونية في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
20	خامسا- تعريف المشرع الجزائري للجريمة الالكترونية
22	المطلب الثاني: خصائص الجريمة الالكترونية وطبيعتها
22	الفرع الأول : الخصائص المتعلقة بالجريمة الالكترونية
22	أولا- خصائص الجريمة الإلكترونية
23	ثانيا- خصائص مرتكب الجرائم الإلكترونية
26	الفرع الثاني: الطبيعة القانونية للجرائم الالكترونية
26	أولا- استبعاد المعلومات من نطاق الجرائم التقليدية
27	ثانيا- إدراج المعلومات ضمن نطاق الجرائم
30	المبحث الثاني: آليات مكافحة الجرائم الإلكترونية في القانون الجزائري
31	المطلب الأول: الآليات الوقائية
31	الفرع الأول : المراقبة الإلكترونية
32	الفرع الثاني : الاستعانة بمزودي الخدمات للوقاية من الجرائم الإلكترونية
33	المطلب الثاني : الآليات الإجرائية و الردعية
33	الفرع الأول : آليات مكافحة الجريمة الإلكترونية
33	أولا- تفتيش و حجز المنظومة المعلوماتية

فهرس المحتويات :

34	ثانيا- تمديد الاختصاص بنظر هذه الجرائم
35	ثالثا- تبدل المساعدة القضائية الدولية
36	رابعا- القوانين اللاحقة المدعمة للقانون 09-04 للحد من الاجرام السيبراني
37	الفرع الثاني: الهياكل الخاصة للتصدي للجرائم الإلكترونية
37	أولا- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها
39	ثانيا- السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي
41	ثالثا- المنظومة الوطنية لأمن الأنظمة المعلوماتية
42	رابعا- المؤسسات الأمنية و دورها في مكافحة الجريمة الإلكترونية
49	الفصل الثاني: صور المساءلة الجزائية عن الجرائم الالكترونية
51	المبحث الأول : الإطار الموضوعي للجريمة الإلكترونية محل المساءلة الجزائية (الصور الجرمية)
51	المطلب الأول : الجرائم الواقعة بواسطة النظام المعلومات والواقعة عليه
51	الفرع الأول: الجرائم التي تقع على الأموال بواسطة النظام المعلوماتي
51	أولا- الجرائم الواقعة على الأشخاص بواسطة النظام المعلوماتي
52	ثانيا- الجرائم الواقعة على الأموال بواسطة النظام المعلوماتي
52	ثالثا- الجرائم الإلكترونية الواقعة على الأسرار

فهرس المحتويات :

52	الفرع الثاني : الجرائم الواقعة على النظام المعلوماتي
52	أولاً- الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات
53	ثانياً- جرائم الاعتداء على المعطيات في أنظمة المعالجة الآلية
54	المطلب الثاني : الصور الجرمية للجريمة الإلكترونية
54	الفرع الأول : الجرائم التي تقع على الأشخاص
54	أولاً- جريمة انتحال الشخصية
54	ثانياً- جريمة المضايقة و الملاحقة
55	ثالثاً- جرائم التغيرير والاستدراج
55	رابعاً- جرائم التشهير وتشويه السمعة
56	خامساً- الجرائم المخلة بالأخلاق والأداب العامة
56	الفرع الثاني: الجرائم التي تقع على الأموال
57	1- جرائم صناعة الفيروسات
57	2- جرائم الاختراقات
58	3- جرائم تعطيل الأجهزة والشبكات
58	4- جريمة النصب والاحتيال
59	المبحث الثاني: المسؤولية الجزائية عن الجرائم الإلكترونية
59	المطلب الأول : شروط مساءلة الشخص الطبيعي البالغ والحدث عن الجرائم

فهرس المحتويات :

	الالكترونية
59	الفرع الأول : المسؤولية الجزائية للشخص البالغ عن الجرائم الالكترونية
59	أولا- أركان وأسس قيام المسؤولية الجنائية عن الجرائم الإلكترونية للشخص البالغ
60	ثانيا- العقوبات المقررة للشخص الطبيعي البالغ عن الجرائم الالكترونية
62	الفرع الثاني: مسؤولية الشخص الحدث عن الجرائم الإلكترونية
62	أولا- القواعد العامة التي تحدد مسؤولية أهلية القصر والنصوص الخاصة
62	ثانيا- نصوص تجريم الأفعال الإلكترونية
63	المطلب الثاني: المسؤولية الجزائية للشخص المعنوي عن الجرائم الالكترونية
63	الفرع الأول: شروط مساءلة الشخص المعنوي عن الجريمة الإلكترونية
63	أولا- أن يكون الشخص المعنوي خاضعا للقانون الخاص
63	ثانيا- وقوع الجريمة لحساب الشخص المعنوي
64	الفرع الثاني: العقوبات المقررة للشخص المعنوي عن الجرائم الإلكترونية
64	أولا- العقوبات الأصلية (الغرامة)
66	ثانيا- العقوبات التكميلية
67	ثالثا- القوانين المتعلقة بالجريمة الإلكترونية في الجزائر
68	الخاتمة

فهرس المحتويات :

71	ملخص الدراسة
73	قائمة المصادر والمراجع
78	فهرس المحتويات