

مذكرة

لنيل شهادة الماستر

تحت عنوان

المسؤولية الجزائية عن الجرائم الإلكترونية في القانون
الجزائري مقارنة بالتشريعات العربية

شعبة: الحقوق

تخصص :

القانون الجنائي والعلوم الجنائية

تحت إشراف الأستاذ (ة) :

بلوط سماح

من إعداد الطالب :

- صديقي سيف الإسلام

لجنة المناقشة

الاسم و اللقب	الرتبة	الصفة	المؤسسة
سهام بوكريريس	أستاذ مساعد	رئيسا	جامعة وهران 1
بلوط سماح	أستاذ مساعد	مشرفا	جامعة وهران 1
حميدي أميمة خديجة	أستاذ مساعد	مناقشا	جامعة وهران 1

السنة الجامعية: 2025 / 2026



الاهداء

من قال " أنا لها نالها، وأنا لها، وإن أبت، رغما عنها أتيت بها "

الحمد لله عند البدء وعند الختام، فما تنأهى درب، ولا ختم جهد، ولا تم سعي إلا بفضلله.

ها أنا اليوم أقف على عتبة تخرجي، وأقطف ثمار تعبى بكل فخر بعد مشقة دامت سنوات

في سبيل الحلم والعلم.

إلى نفسي الطموحة التي بدأت بطموح وانتهت بنجاح.

إلى من أوصاني الله بها خيرا، وجعل الجنة تحت أقدامها، إلى قدوتي ومعلمتي الأولى

وصديقة أيامي، إلى من بفضل دعائها تحقق نجاحي.....

"أمي الغالية"

إلى الذي أحمل اسمه بكل فخر، إلى النور الذي أنار دربي، إلى من كان سندي بعد الله،

إلى من علمني أن الإرادة تصنع المعجزات، ورافقني بكل خطوة.....

"أبي الغالي"

إلى من شددت عضدي بهم فكانوا لي ينابيع أرثوي منها، إلى السند والكتف الثابت الذي

لا يميل....

"أخواتي"

إلى من ساندوني وقت ضعفي، إلى رفقاء الروح الذين شاركوني خطوات هذا الطريق

وشجعوني على المثابرة وإكمال المسيرة.....

"أصدقائي رفقاء السنين"

وفي الأخير أهديكم هذا الإنجاز وثمره نجاحي الذي لطالما تمنيت، وأحمد الله الذي وفقني

لأصل إلى مشارف التخرج بكل فخر.

شكر وتقدير

الحمد لله الذي بنعمته تتم الصالحات، وبفضله وتوفيقه تم إنجاز هذا العمل.

يسعدني أن أوجه أصدق كلمات الشكر والعرفان لأستاذتي الفاضلة "بلوط سماح" مشرفة هذه المذكرة، على ما بذلته من جهد متواصل وصبر جميل، وعلى توجيهاتها القيمة ونصائحها الثمينة طوال فترة إعداد المذكرة، كانت خير مرشد ومعين، فلها مني كل التقدير والامتنان.

كما أتقدم بالشكر الجزيل إلى السادة أعضاء لجنة المناقشة الكرام، الذين تفضلوا بقبول مناقشة هذا العمل، وأن أثنى ملاحظاتهم وآراءهم العلمية التي ستثري البحث وتزيده قيمة.

كما أشكر جميع أساتذتي الأفاضل في مرحلتي الليسانس والماستر، الذين كانوا عوناً لنا ونوراً في طريق العلم.

وبصفة خاصة الأساتذة الذين أشرفوا على تكوين دفعة العلوم الجنائية والقانون الجنائي.

وشكر خاص لإدارة وعماد معهد علم الإجرام، على كل ما قدموه من تسهيلات ودعم طيلة مسيرتنا الأكاديمية.

وفي الأخير أشكر كل من ساهم من قريب أو من بعيد، بدعم معنوي أو علمي، في إتمام هذا العمل، لكل من مد لنا يد العون

جزيل الشكر.

ملخص:

تقوم المسؤولية الجزائية عن الجرائم الإلكترونية على أساس حرية الاختيار و التمييز و الإدراك وقت ارتكاب الجريمة الإلكترونية، التي تعتبر من الجرائم المستحدثة التي تتم في الفضاء الرقمي، على عكس الجريمة التقليدية التي تتم في الواقع المادي، حيث تعتبر من أبرز التهديدات الأمنية في عصرنا الراهن باستغلالها للوسائل الرقمية بالدخول للنظام المعلوماتي و البيانات الشخصية بدون إذن و تعديلها أو اختراقها، فتنوع أنواع هذه الجريمة بين الجرائم الواقعة بواسطة النظام المعلوماتي كجرائم السب و القذف عبر الأنترنت، و بين الجرائم الواقعة على النظام المعلوماتي كالبرامج الإلكترونية، حيث تتفاقم خطورتها بسبب طبيعة الأنترنت العابرة للحدود، لهذا يتطلب التحقيق في هذه الجرائم أساليب متطورة و خبراء متخصصين في الأدلة الجنائية الرقمية، و تعاون دولي و آليات كالأفريبول و اليوروبول و الأوروغيسست لمكافحتها، و ضمان توقيع العقاب على المجرمين.

الكلمات المفتاحية:

المسؤولية الجزائية- الجرائم الإلكترونية- الفضاء الرقمي- النظام المعلوماتي- الإحتيال الإلكتروني- التفتيش الإلكتروني- الحاسب الآلي- التجارة الإلكترونية- التزوير الإلكتروني- الجريمة التقليدية.

Summary:

Criminal liability for cybercrimes is based on the principles of freedom of choice, discernment, and awareness at the time of committing the offense. Cybercrime is considered a modern form of criminality occurring in digital space, contrary to traditional crime that takes place in the physical realm. It represents one of the most prominent security threats in our time by exploiting digital tools to access information systems and personal data without authorization, modifying, or breaching them.

These crimes vary between crimes committed using an information system such as online defamation and libel and crimes committed against an information system such as computer programs and hacking. Their danger is exacerbated by the cross-border nature of the internet. Combatting and addressing this crime requires advanced techniques and experts specialized in digital forensics to strengthen digital legislation and international cooperation through institutional mechanisms, such as Afrapol, Europol, and Eurojust, to combat it effectively and impose maximum penalties on perpetrators.

Keywords:

Criminal Liability - Cybercrime - Digital Space - Information System – Computer - Electronic Fraud - Electronic Search – E-commerce - Electronic Forgery Electronic Blackmail - Traditional Crime.

قائمة المختصرات

ج. ر ج. ج: الجريدة الرسمية للجمهورية الجزائرية

ق ا ج ج: قانون الإجراءات الجزائية الجزائري.

ق ع ج: قانون العقوبات الجزائري.

ص: صفحة.

د. ج: دينار جزائري.

ط: الطبعة

مج: مجلد

مقدمة

مقدمة:

تعد الجريمة ظاهرة مصاحبة للإنسان منذ بداية التاريخ، إذ تطورت أشكالها مع تطور المجتمعات، ومع التسارع العلمي و الثقافي في ظل الثورة التكنولوجية المعاصرة، و انتشار شبكة الأنترنت كأحد أبرز ابتكارات العصر الراهن، عصر الرقمنة أدى اندماج أنظمة الحواسيب مع نظم الاتصالات إلى إحداث تحول جذري في طرق تبادل المعلومات على المستوى العالمي، و قد وصل هذا التأثير إلى حد جعل العالم أشبه بـ " قرية صغيرة " تتجاوز حواجز الزمان و المكان، مما سهل الوصول إلى المعارف، وربط الأفراد عبر القارات، و غيرت بشكل جذري أساليب العمل و التعليم و التواصل.

وعلى الرغم من الإيجابيات الكبيرة التي أتاحتها هذا الانفتاح الرقمي، انتشرت جرائم إلكترونية متطورة تستهدف الأفراد و المؤسسات، تشكل تهديدا حقيقيا يتطلب استجابة قانونية متخصصة، مما استدعى تطوير مفهوم المسؤولية الجزائية لمواكبة طبيعة هذه الجرائم العابرة للحدود، و من هنا يأتي مفهوم المسؤولية الجزائية عن الجريمة الإلكترونية، و الذي يقصد به التزام شخص طبيعي أو اعتباري بالتحمل العواقب القانونية المترتبة على ارتكاب فعل مجرم قانونا باستخدام تقنيات حديثة أو عبر شبكات الإتصال و المعلومات، كما يتميز هذا النوع من المسؤولية بتحديات كبيرة، أبرزها صعوبة إثبات الجريمة في بيئة رقمية متغيرة، و تعقيدات تحديد هوية الجناة الحقيقيين، و مسائل الاختصاص القضائي نظرا للطبيعة المتغيرة التي تتسم بها هذه الجرائم، لذا تسعى التشريعات المعاصرة، و من بينها القانون الجزائي و المقارن إلى تطوير أطر قانونية و إجراءات قادرة على مواجهة هذه المخاطر الإلكترونية المستجدة، و الحفاظ على ضمانات العدالة و حقوق الأفراد في الفضاء الرقمي.

ويكتسب هذا الموضوع أهمية بالغة تتمثل في:

تزايد حالات الجرائم الإلكترونية عالميا، حيث شملت العديد من الضحايا بغض النظر عن الجنس، مما يستدعي ملاحقة المجرمين مرتكبي هذه الجرائم، و تطبيق إجراءات الملاحقة و المحاكمة، مما يعزز اليقين القانوني و يحمي الأفراد و المجتمعات من انتهاكات الخصوصية كالابتزاز و الاحتيال الإلكتروني، و المؤسسات و الشركات من جرائم القرصنة و التجسس الاقتصادي و التلاعب بالبيانات، و هذا ما أدى إلى تفاقم هذه الظاهرة، مما يجعل دراستها و تحليلها أمرا ضروريا للحد من انتشارها، و في هذا الإطار جاء القانون 09-04 المتعلق بالجرائم المعلوماتية، الذي يضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها، بتحديد العقوبات على مرتكبيها و حماية الأفراد، و هذا ما يستدعي دراسة معمقة للحد من هذه الظاهرة بتوقيع العقاب على المجرمين.

فالغاية من دراسة هذا الموضوع تحقيق جملة من الأهداف تتمثل في:

- تحليل الأساليب والتقنيات التكنولوجية المستخدمة في الجرائم الإلكترونية، ودراسة تقنية الجاني ودوافعه.

- تعزيز آليات الحماية القانونية بردع الجناة عبر عقوبات رادعة، ورفع مستوى الوعي المجتمعي لمواجهة هذه الجريمة.

- تعزيز التعاون الدولي والتشجيع على تبادل الخبرات وتسليم القانوني للمجرمين بين الدول لمواجهة الجرائم العابرة للحدود.

- سد الثغرات القانونية وذلك بتطوير تشريعات خاصة بالجرائم الإلكترونية تكمل القوانين الجزائية التقليدية.

- بيان النموذج القانوني للمسؤولية الجزائية عن الجرائم الإلكترونية في التشريع الجزائري مقارنة بالتشريعات العربية.

ويستند أسباب اختيار الموضوع لعدة اعتبارات منها:

أسباب ذاتية: تتمثل في الرغبة الذاتية في دراسة هذا الموضوع بكل جوانبه، نظرا لتأثيره المباشر على حياة الأفراد والمجتمعات وتهديد استقراره.

- وجود ميول واهتمام خاص بمجال التكنولوجيا والفضاء الرقمي.

-الدافع الإنساني وذلك بالشعور بالمسؤولية اتجاه ضحايا الجرائم الإلكترونية، والسعي إلى المساهمة في رفع مستوى الوعي الرقمي والحماية.

أسباب موضوعية: نظرا لكون هذه الجريمة تفتت وتنامت في المجتمع فنحن بحاجة الماسة إلى مكافحة هذه الجرائم بتحسين استخدام الإيجابي لوسائل التواصل الاجتماعي، ونشر حملات توعوية عبر المنصات الاجتماعية الفيسبوك والتيك توك، والأنستغرام حول الأمان الرقمي، ومخاطر مشاركة البيانات الشخصية.

-البحث عن آليات قانونية أفضل لتعويض الضحايا وحمايتهم من التبعات النفسية والمادية.

كما تشمل دراسة الموضوع بعض الصعوبات منها:

- ندرة المراجع القانونية والاجتهادات القضائية، في مجال الجرائم الإلكترونية.

- صعوبة تحديد الإطار القانوني الواجب التطبيق، بحيث قد تتصادف عدة قوانين وطنية ودولية، مع اختلاف التجريم والعقاب باختلاف التشريعات.

- ضعف التأطير القانوني الواضح في التشريع الجزائري لهذه الجريمة.

- اتساع نطاق الموضوع وتشعبه مما يجعل من الصعب الإحاطة بجميع جوانبه في دراسة واحدة.

في عصر أصبحت فيه التكنولوجيا جزءا لا يتجزأ من تفاصيل حياتنا اليومية، لم تعد الجرائم مقتصرة على الفضاء المادي فحسب، بل امتدت لتخترق شاشات أجهزتنا الذكية بصمت

ينطوي على خطورة بالغة، ومنهنا برزت الجرائم الإلكترونية كظاهرة جديدة تطرح تحديات معقدة فيما يخص المسؤولية الجزائية عنها، إذ يصعب تحديدها نظرا للطبيعة الرقمية المعقدة لهذه الأفعال التي تستلزم خبرة فنية متخصصة وآليات تحقيق متطورة لملاحقة مرتكبيها، ومنه نطرح الإشكال التالي: فعلى من تقع المسؤولية الجنائية عن الجرائم الإلكترونية؟ وهل تختلف المسؤولية الجنائية في القانون الجزائري عن التشريعات العربية؟

ومن خلال هذه الإشكالية تفرعت لدينا عدة تساؤلات نلخصها فيما يلي:

- ما المقصود بالجريمة الإلكترونية والمسؤولية الجزائية؟
- ماهي شروط قيام المسؤولية الجزائية عن الجرائم الإلكترونية؟
- ما هي الأركان القانونية لهذه الجريمة؟
- ماهي العقوبات المقررة لها في القانون الجزائري والتشريعات العربية؟
- ماهي أوجه التشابه والاختلاف بين التشريع الجزائري والتشريعات العربية؟

تم الاعتماد في هذه الدراسة على منهجين علميين رئيسيين، وذلك لتغطية مختلف جوانب البحث وهما: المنهج الوصفي، والمنهج التحليلي، وكذلك المنهج المقارن بحيث تم توظيف المنهج الوصفي في وصف وسرد المعلومات والمفاهيم المتعلقة بالمسؤولية الجزائية عن الجرائم الإلكترونية في القانون الجزائري، وعرضها كما وردت في المصادر، مع مقارنتها بالتشريعات العربية ذات الصلة، أما المنهج التحليلي فقد استخدم لتحليل النصوص القانونية والإجراءات المتبعة لمكافحة هذه الجريمة.

تنقسم خطة هذه الدراسة إلى فصلين، يخصص الفصل الأول منها إلى دراسة الإطار الموضوعي للمسؤولية الجزائية عن الجرائم الإلكترونية وفق القانون الجزائري، حيث تطرقت في المبحث الأول إلى ماهية الجريمة الإلكترونية، من خلال مختلف التعاريف وخصائصها، والتميز بينها وبين الجريمة التقليدية وهذا في المطلب الأول، أما المطلب الثاني ارتأيت فيه إلى مفهوم المسؤولية الجزائية و شروطها العامة و خصوصية قيامها في الجرائم الإلكترونية، وفيما يخص المبحث الثاني من الفصل الأول تناولت فيه الإطار التشريعي للجرائم الإلكترونية في الجزائر، و يقسم بدوره إلى مطلبين يتناول الأول أنواع الجرائم الإلكترونية، و يخصص المطلب الثاني إلى دراسة الجريمة الإلكترونية في التشريع الجزائري.

أما الفصل الثاني تعرضت من خلاله إلى الإطار الإجرائي للمسؤولية الجزائية عن الجرائم الإلكترونية وفق القانون الجزائري و بعض التشريعات العربية، و قسمت هذا الفصل إلى مبحثين أيضا، حيث يتناول المبحث الأول منها تنظيم المسؤولية الجنائية وفق القانون الجزائري و بعض التشريعات العربية، تطرقت في المطلب الأول منه إلى تنظيم المسؤولية الجنائية وفق القانون الجزائري ببيان أركان هذه الجريمة، بينما خصصت المطلب الثاني إلى تنظيم المسؤولية الجنائية

وفق بعض التشريعات العربية، أما المبحث الثاني تعرضت فيه إلى المقارنة بين التشريع الجزائري و بعض التشريعات و الآليات العقابية و المؤسساتية لمكافحة الجرائم الإلكترونية، و قسمته إلى مطلبين أيضا، يتناول الأول أوجه التشابه و الاختلاف بين القانون الجزائري و التشريعات العربية، أما الثاني تناولت فيه الآليات العقابية و المؤسساتية لمكافحة الجرائم الإلكترونية.

الفصل الأول:

الإطار الموضوعي للمسؤولية الجزائية عن الجرائم

الإلكترونية

تمهيد:

أدت الاستخدامات الواسعة للوسائل التكنولوجية الحديثة إلى ظهور نوع جديد يسمى الجرائم الإلكترونية التي أصبح ارتكابها سهلاً وأصبحت مخاطرها تهدد أمن المجتمع، حيث تنطبق على الأفعال غير المشروعة التي ترتكب باستخدام الحواسيب والشبكات الرقمية وتستهدفها، بحيث ينشأ هذا الفعل مسؤولية جنائية، مما يستدعي معاقبة كل من يثبت ارتكاب فعل مجرم باستخدام الوسائل التقنية، بالرغم من أن هذا النوع من الجرائم أكثر تعقيداً في معرفة الجناة وتوقيع العقوبات عليهم.

وبهدف دراسة هذا الموضوع بشكل معمق، قمنا بتقسيم الفصل الأول إلى مبحثين، يتناول المبحث الأول ماهية الجريمة الإلكترونية والمسؤولية الجنائية، بينما يركز المبحث الثاني على الإطار التشريعي للجرائم الإلكترونية في الجزائر.

المبحث الأول: ماهية الجريمة الإلكترونية والمسؤولية الجزائية

يعد العصر الحالي مرحلة تشهد تطورا متسارعا في مجال التكنولوجيا الرقمية، وهو ما أتاح فوائد عديدة، إلا أن هذا التقدم أفرز مظاهر تتعارض مع القيم الاجتماعية، فقد أثر هذا التطور بشكل سلبي على العلاقات الإنسانية وشكل تهديدا صريحا لجملة من الحقوق والحريات الفردية، على رأسها الحق في حرمة الحياة الخاصة، مما أدى إلى ظهور جرائم إلكترونية بكثرة وتعدد مرتكبيها، مما نتج قيام المسؤولية الجنائية عن مرتكبي هذه الأفعال غير القانونية وذلك بتحمل نتائج الجريمة المرتكبة.

وهذا الأمر يستدعي دراسة مفهوم الجريمة الإلكترونية و المسؤولية الجزائية، وهذا ما سنتطرق إليه من خلال هذا المبحث.

المطلب الأول: مفهوم الجريمة الإلكترونية وخصائصها وتمييزها عن الجريمة التقليدية

تعتبر الجريمة الإلكترونية من الجرائم التي لا تقل خطورة عن الجريمة التقليدية، بحيث تتميز بالطابع الخاص، ولها أثارها تكون معنوية بالدرجة الأولى وتترتب عليها عواقب مادية محسوسة وذلك باستخدام الحاسوب ووسائل التكنولوجيا الحديثة عبر وسائط تقنية علمية، حيث ينفذ المجرمون هذه الجريمة خلف الشاشات مستغلين الفضاء الرقمي في ارتكاب أفعالهم غير المشروعة.

ومن خلال هذا المطلب، سيتم التطرق إلى مفهوم الجريمة الإلكترونية، عبر تقسيمه إلى فرعين يتناول الفرع الأول تعريفها وخصائصها، بينما يخصص الفرع الثاني للتمييز بينها وبين الجريمة التقليدية.

الفرع الأول: تعريف الجريمة الإلكترونية وخصائصها

سنتطرق في هذا الفرع لتعريف الجريمة الإلكترونية انطلاقا من التعريف الفقهي، مروراً بالتعريف القانوني، وذكر خصائصها وذلك على النحو التالي:

أولاً: مفهوم الجريمة الإلكترونية

أ - التعريف الفقهي:

اختلف الفقه الجنائي ولم يتفق على تعريف تشريعي شامل لهذا النوع من الجرائم، وبالتالي تعددت التعريفات بشأن الجريمة الإلكترونية نظرا للتطور المستمر لتكنولوجيا المعلومات

والاتصالات، إذ تباينت في هذا السياق اتجاهات فقهية بين موسع لمفهوم هذه الجريمة وبين مضيق، وذلك وفقا لما يلي:

1 - الاتجاه الضيق لمفهوم الجريمة الإلكترونية:

سعى هذا الاتجاه إلى تحديد مفهوم الجريمة الإلكترونية ضمن إطار معايير محددة، سواء كانت معايير شخصية تتعلق بدراية الجاني التقنية، أو شخصية ترتبط بطبيعة الفعل الإجرامي، و في هذا الإطار قدم فقهاء القانون الجنائي تعريفات عدة، فهناك من عرفها بأنها كل فعل غير مشروع أو عمل متعمد، يستخدم بالحاسوب أو شبكات الإتصال كأداة رئيسية يستهدفها كهدف للجريمة، كما عرفها الأستاذ Rosen Blat بأنها: " كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف، أو الوصول إلى المعلومات المخزنة داخل الحاسب، أو التي تحول عن طريقه " ¹، و عرفت الدكتور هدى قشقوش بأنها: " كل سلوك غير مشروع أو غير مسموح به، فيما يتعلق بالمعالجة الآلية للبيانات أو نقل البيانات " ².

إلا أن هذه التعريفات تستبعد مجموعة واسعة من الأفعال غير المشروعة التي يستخدم فيها الحاسوب كأداة لارتكاب الجريمة كالاختيال المعلوماتي، وقد تبنت وزارة العدل الأمريكية تعريفا آخر للجريمة الإلكترونية في تقريرها المتعلق بجرائم المعلوماتية الصادر عام 1989 بكونها: " كل فعل غير مشروع يكون العلم بتكنولوجيات الحاسبات الآلية بقدر كبير لازم لارتكابه من ناحية، ولملاحقته وتحقيقه من ناحية أخرى " ³.

يظهر من هذا التعريف أن المعرفة العميقة بتكنولوجيات الحواسيب ليست ضرورية فقط لتنفيذ الجريمة الإلكترونية، بل أيضا لكشفها وملاحقة مرتكبيها والتحقيق معهم، مما يعني أن هذه المعرفة المتخصصة يجب أن تتوافر لدى الجهات المكلفة بكشف الجرائم وملاحقتها وليس فقط لدى الجناة.

2 - الاتجاه الموسع لمفهوم الجريمة الإلكترونية:

¹ محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الأمني، وزارة الداخلية، الأكاديمية الملكية للشرطة، مملكة البحرين، 2010، ص 09.

² مشري راضية، الجريمة الإلكترونية دلالة المفهوم وفعالية المعالجة، مجلة أبحاث قانونية وسياسية، جامعة 8 ماي 1945، قالمة، المجلد 6، العدد 1، سنة 2021، ص 3.

³ سفيان سوير، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلوم الإجرام، كلية الحقوق، جامعة أبو بكر بلقايد تلمسان، الجزائر، 2011، ص 12.

يرى فريق آخر من الفقهاء ضرورة تبني مفهوم موسع للجريمة الإلكترونية، لا يحصرها في الحاسوب أو في موضوع الجريمة، بل يمتد ليشمل فعل إجرامي يرتبط باستخدام التقنية في الأجهزة المعلوماتية والإلكترونية على اختلافها، لذا عرفوها بأنها " كل فعل إجرامي متعمد له صلة بالمعلوماتية، ينتج عنه خسارة للمجني عليه أو كسبا يحققه الفاعل " .

كما عرفت منظمة التعاون الاقتصادي والتنمية بأنها: " كل فعل أو امتناع من شأنه الإعتداء على الأموال المادية أو المعنوية، وينجم بطريقة مباشرة أو غير مباشرة عن استخدام التقنية المعلوماتية " ⁴.

كما تبنى مؤتمر الأمم المتحدة العاشر لمنع الجريمة و معاقبة المجرمين تعريفاً أوسع، حيث اعتبر أن الجريمة الإلكترونية هي " أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، و الجريمة تشمل مبدئياً جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية " ⁵.

وبالتالي هذا التعريف استطاع أن يحيط بمختلف الصور الإجرامية للجريمة الإلكترونية، سواء التي ترتكب بواسطة النظام المعلوماتي أو داخل هذا النظام على المعطيات والبرامج والمعلومات، كما يشمل الجرائم الواقعة في البيئة الإلكترونية عموماً، ولم يركز هذا التعريف على صفات الجاني التقنية أو على وسيلة ارتكاب الجريمة أو غايتها، بل تجنب التضييق الذي قد يتيح إفلات العديد من صور هذه الجرائم من العقاب.

من خلال استعراض التعريفات الفقهية السابقة لمفهوم الجريمة الإلكترونية، نجد أنها تركزت على مفاهيم عامة مرتبطة بالحاسوب والبيانات، وقد كان الفقهاء الذين تبنا الاتجاه الموسع أكثر حكمة، نظراً للتطور السريع في العالم الافتراضي، فبشكل عام يقوم تعريف الجريمة الإلكترونية على ثلاثة عناصر: السلوك ووصفه التجريمي، والنص القانوني الذي يجرم هذا السلوك ويحدد عقوبته، ومحل الإعتداء المتمثل في معطيات الحاسوب ونظمه.

ب - التعريف القانوني:

عرف المشرع الجزائري الجريمة الإلكترونية في القانون رقم 24-06 المتضمن تعديل قانون العقوبات، الذي نصت أحكامه في القسم السابع مكرر على المساس بأنظمة المعالجة الآلية

⁴يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، في ضوء الاتفاقيات العربية لمكافحة جرائم تقنية المعلومات، قانون العقوبات، ق إ ج، قوانين خاصة، دار الجامعة الجديدة، الإسكندرية، 2019، ص 50.

⁵مشري راضية، مرجع سابق، ص 4.

للمعطيات⁶، ثم تلاه بالقانون 04-09 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها⁷.

بالرجوع إلى قواعد القانون 06-24 من المادة 394 مكرر إلى المادة 394 مكرر 2، نجد أنه حدد مفهوم المساس بأنظمة المعالجة الآلية للمعطيات، حيث حددها في المادة 394 مكرر كالآتي:

يعاقب بالحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 60.000 دج إلى 200.000 دج، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف ذلك إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة، تكون العقوبة الحبس من سنة (1) إلى ثلاث (3) سنوات والغرامة من 100.000 دج إلى 300.000 دج⁸.

أما المادة 394 مكرر 1 فقد أشارت إلى ما يلي:

يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها⁹.

وبالنسبة للمادة 394 مكرر 2 فقد بينت المساس بأنظمة المعالجة الآلية للمعطيات من الآتي:

يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 1000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش بما يأتي:

⁶ القانون رقم 06-24 المؤرخ في 19 شوال عام 1445 هـ الموافق ل 28 أبريل سنة 2024، المعدل والمتمم، المتضمن قانون العقوبات الجزائري، الجريدة الرسمية، العدد 30.

⁷ القانون رقم 04-09 المؤرخ في 14 شعبان عام 1430 هـ الموافق ل 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 25 شعبان عام 1430 هـ، الموافق ل 16 غشت سنة 2009.

⁸ المادة 394 مكرر من قانون العقوبات الجزائري، المعدل من قانون 06-24.

⁹ المادة 394 مكرر 1 من قانون العقوبات الجزائري، المعدل من قانون 06-24.

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

2- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم¹⁰.

كما عرف القانون 04-09 الجريمة الإلكترونية في المادة 02 منه بقولها: " يقصد في مفهوم هذا القانون بما يأتي:

- الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

- منظومة معلوماتية:

أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.

- معطيات معلوماتية:

أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها¹¹.

مما سبق نستنتج أن المشرع الجزائري وسع المفهوم ليشمل كل جريمة ترتكب بواسطة منظومة معلوماتية، مما يعكس إرادة المشرع في مكافحة هذه الجرائم.

ثانيا: خصائص الجريمة الإلكترونية

تتسم الجريمة الإلكترونية بمجموعة من الخواص أو السمات التي تجعلها مختلفة عن الجرائم التقليدية وذلك بسبب حدوثها وتطور الأساليب والأدوات المستخدمة في ارتكابها، سنبين ذلك فيما يلي:

¹⁰المادة 394 مكرر 2 من قانون العقوبات الجزائري، المعدل من قانون 06-24.

¹¹المادة 02، من القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

أ- جريمة عابرة للحدود

و يقصد بذلك أن الحدود السياسية أو الجغرافية ليست عائقا أمام هذا النوع من الجرائم، و ذلك بفضل التطور الهائل في وسائل الاتصالات و الترابط الكبير بين الأجهزة عبر الشبكة الإلكترونية العالمية، حيث يمكن للجاني أن يكون في بلد و المجني عليه في بلد آخر، و هكذا فالجرائم الإلكترونية تقع في أغلب الأحيان عبر حدود دولية كثيرة¹²، ففي هذا الفضاء الرقمي بات العالم كله كقرية صغيرة، و أصبحت الحدود مجرد خطوط وهمية على الخرائط، و هذا ما يعني أن مسرح الجريمة المعلوماتية لم يعد محليا بل أصبح عالميا، إذ أن الفاعل يرتكب جريمته عن بعد بتباعد المسافات بين الفعل الذي يتم من خلال كمبيوتر الفاعل و بين المعلومات محل الاعتداء¹³، مما يصعب تتبعها أو كشفها بحيث يتطلب ذلك تعاون دوليا فعالا لمواجهتها.

ب- جريمة صعبة الإثبات

تتسم هذه الجرائم بصعوبة في مرحلة التحقيق وإثبات الوقائع، وذلك لأنها ترتكب بأسلوب خفي ودون ترك أي دليل مادي ملموس يمكن الاستناد إليه، فالأدوات المستخدمة في ارتكابها غير ظاهرة للغير ولا تخلف أثرا ماديا في الواقع المادي المحسوس، لأنها تقتصر إلى الدليل المادي التقليدي كال بصمات مثلا¹⁴، مما يجعل أمر إثباتها وتقديم الأدلة القاطعة عليها مهمة معقدة وأمر صعبا يحتاج إلى خبرة فنية عالية و متخصصة.

ج- جريمة تتسم بالنعومة والسهولة

تتميز الجريمة الإلكترونية بكونها جريمة سهلة التنفيذ، إذ لا تتطلب مجهودا عضليا، بل تعتمد على الدراسة الذهنية و التفكير العلمي المدروس القائم عن معرفة تقنية الكمبيوتر¹⁵، و غالبا ما تحدث هذه الجرائم دون مواجهة مباشرة بين الجاني والضحية، حيث يتم ارتكابها عن بعد، نظر للطبيعتها الافتراضية التي لا تحتاج إلى وقت طويل أو مكان محدد لارتكابها، و ذلك لكون

¹² عبد الفتاح مراد، شرح جرائم الكمبيوتر والانترنت، دار الكتب والوثائق المصرية، القاهرة، مصر، ص 42.

¹³ نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، لبنان، الطبعة الأولى، 2005، ص 52.

¹⁴ رستم هشام، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، مجلة الامن والقانون، دبي، الإمارات العربية المتحدة، العدد 02، 1999، ص 11.

¹⁵ عبد الفتاح مراد، مرجع سابق، ص 46.

هذا النوع من الجرائم تقوم على معطيات و بيانات يمكن تعديلها أو تغييرها أو حذفها من السجلات المخزنة في ذاكرة الحواسيب¹⁶.

د - جرائم لا يتم التبليغ عنها غالبا

توصف الجرائم الإلكترونية بطابعها الخفي والمستتر في معظم الحالات، إذ نادرا ما ينتبه الضحية إلى وقوعها، حتى وإن حدثت أثناء وجوده على الشبكة، ويعود ذلك إلى امتلاك الجاني مهارات تقنية تمكنه من تنفيذ جريمته بدقة متناهية كإرسال الفيروسات، أو سرقة الأموال والبيانات الخاصة أو إتلافها و غيرها من الجرائم¹⁷، ونتيجة لذلك فإن هذه الجرائم غالبا لا تترك أثرا ملموسا بعد ارتكابها، وحتى في حال وجود أثر يصعب تقنيا تحليله، وبهذا يتطلب ذلك التعامل مع وسائل تقنية متطورة للوصول إلى مرتكبيها.

الفرع الثاني: التمييز بين الجريمة الإلكترونية والجريمة التقليدية

سنشير في هذا الفرع إلى التمييز بين الجريمة الإلكترونية التي تقع في بيئة رقمية، وبين الجريمة التقليدية التي ترتكب في الواقع المادي، وذلك على النحو التالي:

أ- من حيث نطاق اقترافها

تخضع الجريمة التقليدية لنطاق مكاني محدد بإقليم الدولة التي وقعت فيها الجريمة، أي في واقع مادي ملموس، في المقابل تتجاوز الجريمة الإلكترونية الحدود الجغرافي لأنها ترتكب في واقع افتراضي وفضاء رقمي عبر شبكة الأنترنت، بحيث يرتكب الجاني جريمته في بلد والمجني عليه يكون في بلد آخر.

ب- من حيث أداء الأفعال الإجرامية

تقوم الجرائم التقليدية على دوافع فردية كالانتقام أو الإضرار بالضحايا أو تحقيق الربح، أما الجرائم الإلكترونية تنشأ عن تخطيط دقيق ومنظم يتجاوز الحدود الإقليمية، بهدف تحقيق الربح واكتساب الثروة والسلطة والنفوذ باستخدام الحاسب الآلي وشبكات الأنترنت.

ج- الفرق بين المجرم التقليدي والمجرم الإلكتروني

المجرم التقليدي هو شخص عادي اعتاد على ارتكاب نوع محدد من الجرائم العادية، نظرا لظروف أحاطت به كونه يعتمد في تنفيذ جرائمه على أدوات تقليدية للوصول إلى هدفه، حتى لو اضطر على استخدام العنف، و بالتالي يمكن تحديده عبر شهود أو أدلة مادية، عكس المجرم

¹⁶د. رحمني محمد، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، جامعة احمد دراية، أدرار، العدد 41، سنة 2018، ص 442.

¹⁷محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت، دار النهضة العربية، القاهرة، مصر، 2009، ص 31.

الإلكتروني الذي سخر التطور الهائل للتكنولوجيا المعلومات والاتصالات وصولاً إلى غاياته¹⁸، مما يمنحه قدرة على تنفيذ جرائم معقدة دون الحاجة إلى مواجهة مباشرة مع الضحايا، حيث يتسم بالذكاء و الاحتراف في استخدام وسائل التقنية الحديثة لتنفيذ الجريمة، و لا يميل للعنف لأنه لا يواجه المجني عليه، بل يتعامل مع وسائل متطورة كالحاسب الآلي و البرمجيات، شبكات الإتصال لتنفيذ جريمته، و بالتالي غالباً ما يكون الجاني مجهول الهوية و يصعب تعقبه.

المطلب الثاني: مفهوم المسؤولية الجنائية وشروط قيامها

عرف مفهوم المسؤولية الجنائية تطوراً تاريخياً مواكباً لتطور القوانين، حيث يعتبر ركيزة أساسية في النظام القانوني، يبدأ بمرحلة تحديد الشخص المسؤول جزائياً بعد إثبات الجريمة ونسبتها إلى المتهم، بهدف تحديد العقوبة المناسبة له، وعليه تقوم هذه المسؤولية على ركن أساسي يتمثل في اكتمال عناصر الجريمة من علم وإرادة وحرية اختيار، يحددها المشرع لتحصيل الجاني تبعات أفعاله.

وفي هذا السياق سيتم التطرق في الفرع الأول إلى مفهوم المسؤولية الجنائية بمختلف التعاريف، بينما سيتناول الفرع الثاني شروطها العامة، وخصوصية قيام للمسؤولية الجنائية في الجرائم الإلكترونية.

الفرع الأول: تعريف المسؤولية الجنائية

سنخصص هذا الفرع لتعريف المسؤولية الجنائية بدءاً من التعريف اللغوي، مروراً بالتعريف الفقهي إلى القانوني، وذلك على النحو التالي:

مفهوم المسؤولية الجنائية

أولاً: التعريف اللغوي

مصدر: سأل يسأل، فهو سائل، و سألته و سألته، أي طرح عليه السؤال، فهو المسؤول: المطلوب منه، فالمسؤولية الجزائية هي الحالة أو الصفة التي تجعل الشخص مطالبا بأمر ما، وتقع عليه تبعاته، يقال: أنا بريء من مسؤولية هذا العمل، وتطلق أخلاقياً على التزام الشخص بما يصدر عنه قولاً أو عملاً، وتطلق قانوناً على الالتزام بإصلاح الخطأ الواقع على الغير طبقاً للقانون¹⁹.

ثانياً: التعريف الفقهي

تعددت التعريفات الفقهية للمسؤولية الجزائية، حيث عرفها البعض بأنها: استحقاق مرتكب الجريمة العقوبة المقررة لها، وترتبط هذه المسؤولية بفاعل أهل للتكليف الجزائي، فتستحق عليه

¹⁸ عبد الكريم خالد الردايدة، الجرائم المستحدثة واستراتيجية مواجهتها، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، 2013، ص 34.

¹⁹ المعجم الوجيز، مجمع اللغة العربية، طبعة خاصة بوزارة التربية والتعليم، 1993، ص 299.

العقوبة حماية لهذا التكليف، بينما يرى آخرون أنها: "صلاحية الإنسان لصدور الأفعال والاقوال منه على وجه يعتد به شرعا"²⁰.

وتعرف أيضا بأنها: " تحمل الإنسان نتائج الأفعال المحرمة التي يأتيها مختارا، وهو مدركا لمعانيها ونتائجها "، وسواء أكان ما اقترفه من معصية ماساً بحق من حقوق الله تعالى، أو ماساً بحق من حقوق العباد²¹، و هناك من يعرفها بأنها: "صلاحية الشخص لتحمل الجزاء الجنائي المقرر للجريمة التي ارتكبها"²².

فمن هذه التعريفات نستنتج أنه يستوجب توافر شرط المسؤولية أي أن يكون المسؤول جنائيا مدركا لطبيعة أفعاله ومختارا حال ارتكابه للجريمة الإلكترونية، وإلا انتفت عنه المسؤولية الجنائية.

فالجريمة ليست كيانا ماديا ملموسا فحسب بل تمتد إلى الكيان النفسي، فبمجرد قيام المسؤولية الجنائية في حق مرتكب الواقعة الإجرامية لا يكفي إسناد هذه الواقعة إليه إسنادا ماديا بحتا، وإنما يلزم أن تتوافر رابطة نفسية تربطه بها، تشكل الأساس الحقيقي للحكم بتوافر العنصر المتمثل في الخطأ الجنائي²³.

ثالثا: التعريف القانوني

لم يضع المشرع الجزائري تعريفا محددا للمسؤولية الجزائية على غرار باقي التشريعات سواء في قانون العقوبات أو في قانون الإجراءات الجزائية، بل ترك مهمة تعريفها للفقهاء والاجتهاد القضائي، فمن الناحية القانونية تعرف المسؤولية بأنها أهلية الإنسان العاقل الواعي لأن يتحمل جزاء، أو عقاب نتيجة أفعاله، فهي في جوهرها التزام يفرض على الشخص بالخضوع لشيء، أو التزامه به ضد إرادته²⁴، فالمقصود من المسؤولية الجنائية أن يكون مرتكب الجريمة أهلا لتحمل نتائج فعله غير المشروع، وذلك من خلال تطبيق الجزاء الجنائي المقرر سواء، كان عقوبة سالبة للحرية أو غرامة مالية أو تدبيرا أمنيا.

كما قد اكتفى المشرع الجزائري باستبعاد المسائلة الجنائية حينما تنتفي حرية الاختيار، حيث نصت المادة 47 من قانون العقوبات على أنه: " لا عقوبة لمن كان في حالة جنون وقت

²⁰ ط.د. برمضان الطيب، المسؤولية الجنائية في الفقه الإسلامي والقانون الجزائري، مجلة المعيار، جامعة الجزائر 1، المجلد 12، العدد 01، 2021، ص 89.

²¹ ط.د. برمضان الطيب، مرجع سابق، ص 90.

²² عبد العزيز زعبار، أساس المسؤولية الجنائية وفق التشريع الجزائري، مذكرة مقدمة لاستكمال نيل شهادة الماستر، كلية الحقوق، تخصص القانون الجنائي والعلوم الجنائية، جامعة غرداية، سنة 2024، ص 8.

²³ سلامة مأمون، شرح قانون العقوبات، القسم العام، دار الفكر العرب، الأردن، 2009، ص 199.

²⁴ ط.د. برمضان الطيب، مرجع سابق، ص 90.

ارتكاب الجريمة..."، ونصت المادة 48 أيضا على أنه: " لا عقوبة على من اضطرت به إلى ارتكاب الجريمة قوة لا قبل له بدفعها ".

ونصت المادة 49 على أنه: " لا يكون محلا للمتابعة الجزائية القاصر الذي لم يكمل (10) سنوات.

لا توقع على القاصر الذي يتراوح سنه من 10 إلى أقل من 13 سنة إلا تدابير الحماية أو التهذيب.

ويخضع القاصر الذي يبلغ سنه من 13 إلى 18 سنة إما لتدابير الحماية أو التهذيب أو لعقوبات مخففة²⁵.

فمن خلال هذه المواد، يتبين أن المشرع الجزائري جعل الأهلية الجنائية شرطا أساسيا لقيام المسؤولية الجنائية، إذ لا يمكن مسائلة الشخص جنائيا إلا إذا كان أهلا لذلك أي بتوافر عنصري الإرادة أو الاختيار والإدراك لديه.

الفرع الثاني: الشروط العامة للمسؤولية الجزائية وخصوصية قيامها في الجرائم الإلكترونية
سننظر في هذا الفرع إلى الشروط العامة للمسؤولية الجنائية، وخصوصية قيامها في الجرائم الإلكترونية، سنبين ذلك فيما يلي:

أولاً: شروطها العامة

1- الأهلية الجزائية

يقصد بها مجموعة من الصفات الشخصية من عوامل ذهنية عقلية، ونفسية يلزم توفرها في الشخص مرتكب الجريمة، بحيث تكون لديه القدرة على تحمل تبعه أفعاله، حيث لا تتحقق هذه الأهلية إلا بتوافر النضج العقلي الكافي الذي يتكون منذ الولادة حيث لا يعتبر الصغير أهلا لعدم اكتمال أهليته، و الصحة العقلية بحيث يحدد القانون سنا معينة لكي يعتبر عندها الشخص عاقلا مميزا، لكن مع ذلك قد يبلغ الشخص سن التمييز دون أن يكون سليم العقل، إما لعدم نمو ملكاته الذهنية نموا طبيعيا رغم بلوغه السن القانوني، أو لإصابته بمرض عقلي أو نفسي يفقد أهليته الجنائية²⁶، و عليه تنقسم الأهلية الجنائية إلى:

أ - أهلية الوجوب

²⁵ القانون 01-14 المؤرخ في 04 فبراير 2014، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 08 يونيو 1966، المتضمن تعديل قانون العقوبات، (ج، ر، ج، ج، الصادر في 16 فبراير 2014، العدد 07).

²⁶ فرج رضا، شرح قانون العقوبات الجزائري القسم العام، الطبعة الثانية، الشركة الوطنية للنشر والتوزيع، الجزائر، 1976، ص 106.

يقصد بها صلاحية الشخص للإلزام والالتزام، وهي شخصية قانونية تثبت لكل شخص طبيعي منذ ولادته، وتشمل جميع الحقوق والالتزامات أيًا كان نوعها وتستمر حتى وفاته، أي تثبت هذه الأهلية للإنسان بناءً على ثبوت الذمة له²⁷، وتنقسم بدورها إلى نوعين:

- أهلية الوجوب ناقصة

تثبت للجنين في بطن أمه، وتتمثل في صلاحية الإنسان لثبوت بعض الحقوق له فقط، مثل انتقال الميراث أو الوصية، أما بالنسبة للالتزامات والواجبات فلا تثبت في حقه ولا تجب في ماله نفقة أقاربه، ولا تصح منه هبة أو صدقة حتى لو تمت بواسطة وليه.

- أهلية الوجوب كاملة

تثبت للشخص بمجرد ولادته حياً، فيحق له التمتع بالحقوق وتحمل في ذمته الالتزامات، فيملك ما يشتري له أو يوهب، ويتحمل الواجبات كتعويض قيمة ما يتلفه، حتى لو كان صبياً، فهو ملزم بكل ما يتعلق بحق الغير حماية لأنفسهم وأموالهم، وإذا جنى الصبي على الغير، فإن جزاءه يكون مالياً لا بدنياً²⁸

ب - أهلية الأداء

تعرف أهلية الأداء بأنها صلاحية المكلف لاعتبار أقواله وأفعاله شرعاً، أي صلاحية الشخص لممارسة الأعمال التي يتوقف اعتبارها الشرعي على العقل، كما يمكن تعريفها بأنها صلاحية الشخص لممارسة الأعمال القانونية باسمه ولحسابه، وأساس هذه الأهلية هو "التمييز" لا الحياة²⁹، وتنقسم بدورها إلى ثلاثة أنواع رئيسية:

- أهلية الأداء الكاملة

هي أهلية الشخص لأن يعتد بجميع تصرفاته، سواء كانت قولية أو عملية أو اعتقادية، فالتكاليف الشرعية تصبح لازمة له ببلوغه سن الرشد مع كونه عاقلاً، أما التصرفات المالية فتصبح نافذة منه ببلوغه سن الرشد مع كونه عاقلاً وراشداً، وتكون هذه الأهلية للبالغ العاقل الذي اكتمل لديه الإدراك والتمييز³⁰.

- أهلية الأداء القاصرة

²⁷ زيدان عبد الكريم، الوجيز في أصول الفقه، مؤسسة الرسالة، بيروت، طبعة 7، 1997، ص 92.

²⁸ حسني محمود نجيب، شرح قانون العقوبات، القسم العام، دار النهضة العربية، 1998، ص 578.

²⁹ ط.د. برمضان الطيب، مرجع سابق، ص 91.

³⁰ عوض محمد، قانون العقوبات القسم العام، دار المطبوعات الجامعية، طبعة 1، مصر، 1969، ص 142.

تكون للصبي المميز الذي لم يبلغ سن الحلم، وكذلك للسفيه ومعناه ضعيف الإدراك، وتعني صلاحية الشخص لاعتبار بعض تصرفاته شرعا، دون أن يلزم بالتكاليف الشرعية كالصلاة والصوم، وإن صحت منه إذا قام بها، وتسمى لدى البعض بأهلية التعبد³¹.

– أهلية الأداء منعدمة

تكون للصبي غير المميز والمجنون، فلا يصح منه أي تصرف قانوني فهو غير أهل للتبرع ولا للتصرف ولا للاعتناء بشؤونه، ولا يؤخذ على أفعاله مؤاخذه بدنية، لكنه يضمن في ماله ما يتلفه من أموال الغير.

2 – حرية الاختيار

حرية الاختيار هي تعني مقدرة المرء على توجيه إرادته إلى الوجهة التي يريد، أي قدرته على دفع إرادته في جهة يعينها من الوجهات المختلفة التي يمكن أن تتخذها، فلا يكفي أن يكون قادرا على فهم وتمييز أعماله وإدراك نتائجها، بل يجب أن يكون بوسعه توجيه هذه الإرادة بحرية، فإذا كان المرء عاقلا مميزا، فإن عليه أن يواجه إرادته توجيهها سليما يتفق وأهداف القانون، ولا يتحقق له ذلك إلا إذا كان حر الاختيار³².

3 – الخطورة الإجرامية

تعددت التعريفات الفقهية لمفهوم الخطورة الإجرامية، فهناك من عرفها بأنها: "حالة نفسية يحتمل معها أن يكون صاحبها مصدرا لجريمة في المستقبل"، وهناك من يعرفها بأنها: "استعداد يتوافر لدى الشخص يجعل من المحتمل إقدامه إلى ارتكاب جرائم في المستقبل"، وهناك من يعرفها بأنها: "حالة من عدم التوازن في شخصية الفرد، مصدرها تكوينه المادي أو النفسي أو ظروفه البيئية، وتدفعه إلى احتمال ارتكاب الجرائم"³³.

ثانيا: خصوصية قيام المسؤولية الجنائية في الجرائم الإلكترونية

أ – عنصر التمييز والإرادة

يعتبر هذا العنصر شرط أساسي لقيام المسؤولية الجنائية، حيث يجب أن تتوافر في الجاني القدرة على فهم أفعاله ونتائجها، أي أن يكون واعيا بسلوكه الغير مشروع وقت ارتكابه الجريمة، وأن تتوفر فيه نية الإضرار كإحداث ضرر بنظم المعالجة الآلية للمعلومات، ما يسمى بالدخول الغير المشروع إلى أنظمة الحاسوب³⁴ باستخدام وسائل فنية وتقنية وهو بكامل إرادته.

³¹ عوض محمد، مرجع سابق، ص 143.

³² عبد العزيز زعبار، مرجع سابق، ص 12.

³³ بوحية وسيلة، المسؤولية الجنائية الدولية عن الجرائم ضد الإنسانية، مذكرة ماجيستر تخصص القانون الجنائي الدولي، جامعة سعد دحلب، البليلة، 2016، ص 39.

³⁴ نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة 2، دار الثقافة للنشر والتوزيع، الأردن، 2010.

ب- خصوصية الفاعل والدافع

غالبا ما يكون مرتكب الجريمة ذكيا ويمتلك مهارات عالية كإمكانية إخفاء هويته إلكترونيا واستخدام برامج تشفير وانتحال شخصيات، كما تتنوع دوافعه بين الربح المادي الاحتيال، طلب فدية (برامج فدية)، الاختراق لسرقة بيانات بنكية، ونفسية كالانتقام والتحدي التقني.

ج- صعوبة الإثبات

تعتبر الأدلة الرقمية غير ملموسة وقابلة للتلف، بحيث يمكن تعديلها بسهولة والتلاعب بالأوقات والتواريخ وحذفها بشكل شبه نهائي، مما يصعب تتبع مصدر الجريمة، ويتطلب تقنيات تحقيق متطورة.

المبحث الثاني: الإطار التشريعي للجرائم الإلكترونية في الجزائر

في ظل تطور التكنولوجيا والمعلومات تبرزت الجريمة الإلكترونية، التي تعد من الظواهر الاجتماعية الأكثر شيوعا وخطورة في وقتنا الحالي، فهي من الجرائم التي تتسم بالذكاء وتقع في الفضاء الرقمي حيث يرتكبها أشخاص ذوي قدرات تقنية وفنية عالية، مما يصعب التحقيق فيها والكشف عن مرتكبيها وهذا الأمر يتطلب تدخل القانون لوضع حد لهذه الظاهرة الاجتماعية التي أصبحت تهدد قيم وأركان المجتمع.

ولهذا في سبيل مواكبة تطورات التكنولوجيا والجرائم المرتبطة بها، قام المشرع الجزائري بسن قواعد قانونية في إطار القانون رقم 04-15 المتضمن قانون العقوبات المتعلق بالمساحات بأنظمة المعالجة الآلية للمعطيات، ثم يليه القانون 06-24 المعدل والمتمم من نفس القانون، والقانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام و الإتصال ومكافحتها.

وهذا ما يستدعي إلى دراسة أنواع الجريمة الإلكترونية، والتعرض إلى الطبيعة القانونية لهذه الجريمة، وهذا ما سنتطرق إليه من خلال هذا المبحث.

المطلب الأول: أنواع الجرائم الإلكترونية

تعد الجرائم الإلكترونية من الجرائم المستحدثة التي تقع في العالم الافتراضي، حيث يكون الجاني مستغلا الفضاء الرقمي لارتكاب أفعاله الغير مشروعة، والتي ترتكب بواسطة الأجهزة الإلكترونية، بحيث تستهدف الكيانات المعنوية للحاسب الآلي عكس الجريمة التقليدية التي تقع في العالم المادي وتستهدف الكيانات المادية للحاسب الآلي.

فقد اختلف الفقهاء في تقسيم الجرائم الإلكترونية نتيجة لتشعبها وتطورها، فكلما ظهرت وسيلة جديدة لاستخدام الحاسب الآلي والإنترنت ظهرت معها جريمة جديدة، وبهذا لم يستقر الفقه على معيار واحد لتصنيفها، فمنهم من يصنفها حسب وسيلة ارتكاب الجريمة، ومنهم من يعتمد على محل الجريمة، وعلى هذا الأساس سنتطرق في الفرع الأول إلى الجرائم الواقعة بواسطة النظام المعلوماتي، أما الفرع الثاني إلى الجرائم الواقعة على النظام المعلوماتي.

الفرع الأول: الجرائم الواقعة بواسطة النظام المعلوماتي

يعد الحاسب الآلي في هذا النوع من الجرائم وسيلة لتسهيل النتيجة الإجرامية ومضاعفتها، حيث يهدف الجاني من وراءها إلى تحقيق ربح مادي بطرق غير مشروعة، مستخدماً النظام المعلوماتي أو برامجه كوسيلة لتنفيذ الجريمة، وتنقسم هذه الجرائم بدورها إلى:

أولاً: الجرائم الواقعة على الأشخاص

تتمتع الحياة الشخصية بخصوصية وحرمة لا يجوز انتهاكها، حيث ترتكب هذه الجريمة من خلال الاطلاع على البيانات والمعلومات الشخصية أو تسجيل مكالمات ومقاطع الفيديو أو مراقبتها، ويتمثل الركن المادي في جريمة نشر المواد الإباحية بالسلوك الذي يتخذه الفاعل بإنشاء صفحات تحتوي على أفعال مخلة بالأداب العامة ونشرها عبر الأنترنت، أما الركن المعنوي فيتمثل في الحالة النفسية للجاني، أي قصده بنشر الصور مع علمه وإرادته بذلك³⁵، وعلى هذا الأساس يمكن الإشارة إلى جملة من الجرائم في هذا السياق، وذلك على النحو التالي:

أ - جرائم التعدي الإلكتروني على الحياة الخاصة

تتسم الشبكة العنكبوتية بأنها فضاء تنتقل عبره المعلومات بشكل واضح، مما يجعل أي بيانات تثبت عبرها عرضة للاعتراض أو الاطلاع غير المشروع، لا سيما في غياب تأمين الحسابات الشخصية و غياب آليات حماية فعالة للبيانات الحساسة، لذلك يشكل تأمين الخصوصية و الهوية الرقمية و المعلومات الشخصية و المعاملات المالية الشاغل الأكبر لمستخدمي هذه الشبكة ، نظراً لما قد يترتب على الاختراق أو الإهمال من تداعيات خطيرة، تبدأ من إطلاع الغير على خصوصيات الشخص رغم سعيه لإبقائها محصورة، وصولاً إلى الخسائر

³⁵ يوسف خليل يوسف العفيفي، الجرائم الإلكترونية في التشريع الفلسطيني " دراسة تحليلية مقارنة "، رسالة لنيل شهادة الماجستير في القانون العام، كلية الشريعة والقانون " الجامعة الإسلامية "، غزة، 2013، ص 26.

المادية و تراجع الثقة في المؤسسات، لا سيما إذا كان الطرف المتضرر مؤسسة مالية وخدمة يفترض بها الالتزام بأعلى درجات الدقة و الأمان في حماية بيانات العملاء³⁶.

تعدد صور الإعتداء على الخصوصية عبر الوسائط الإلكترونية، ومن أبرزها: جمع البيانات وتخزينها بطرق غير مشروعة، وإساءة استخدام المعلومات الشخصية، والتقصير في دقتها، والإفشاء غير المصرح به لها، كما تشمل هذه الجرائم انتهاك سرية الاتصالات والمراسلات، وإتلاف البيانات أو البرامج باستخدام الفيروسات، ويمكن حصر انتهاك الخصوصية على الأنترنت في أربعة أشكال رئيسية، وهي: اقتحام العزلة الشخصية، وكشف الأسرار، ونشر الادعاءات الكاذبة، والاستخدام غير المأذون به لا سيم الشخص أو صورته³⁷.

ب - الجرائم المخلة بالآداب العامة عبر الأنترنت

تعد الجرائم المخلة بالآداب العامة عبر الأنترنت أحد أنماط إدارة المعلومات في إطار الرقابة و التوجيه الإعلامي، حيث تقوم على عمليات جمع البيانات و تحليلها و فحصها بهدف رصد المخالفات أو الحد من الخطابات غير الأخلاقية أو المضللة، غير أن هذه الممارسات تتطلب استثمارا كبيرا للوقت و الجهد من قبل الجهات المعنية، مما يزيد من أهميتها و تأثيرها على مختلف الفئات، و قد تمتد تأثيراتها لتشمل حقوق الإنسان، سواء على مستوى الأفراد أو المجتمعات المحلية أو حتى العلاقات الدولية، و لهذا يجب معالجة هذه الجرائم بدقة، لضمان تحقيق التوازن بين الرقابة و احترام الحقوق، و المساهمة في تعزيز العدالة و المساواة بين أفراد المجتمع و مختلف الفئات.

ج - جرائم السب والقذف عبر الأنترنت

تعد جرائم السب والقذف من أكثر الجرائم شيوعا في الفضاء الإلكتروني، حيث عرفها المشرع الجزائري في المادتين 296 و 297 من قانون العقوبات على النحو التالي:

القذف: " يعد قذفا كل ادعاء بواقعة من شأنها المساس بشرف واعتبار الأشخاص أو الهيئة المدعى عليها به أو إسنادها إليهم أو إلى تلك الهيئة ويعاقب على نشر هذا الادعاء أو ذلك الإسناد مباشرة أو بطريق إعادة النشر حتى ولو تم ذلك على وجه التشكيك أو إذا قصد به

³⁶ سليم حميداني وعباسي سهام، اختراق الخصوصية في العالم الرقمي، حدود الظاهرة ومطالب الحماية القانونية، مجلة البحوث في الحقوق والعلوم السياسية، جامعة ابن خلدون تيارت، المجلد 04، العدد 02، 2019، ص 33-46.

³⁷ راضية مشري، مرجع سابق، ص 15.

شخص أو هيئة دون ذكر الاسم ولكن كان من الممكن تحديدهما من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الإعلانات موضوع الجريمة³⁸.

السب: "يعد سبا كل تعبير مشين أو عبارة تتضمن تحقيرا أو قدحا لا ينطوي على إسناد أية واقعة"³⁹.

ثانيا: الجرائم الواقعة على الأموال

إن الانفتاح المالي الرقمي خلق بيئة خصبة للأنشطة الإجرامية، إذ استغل بعض المجرمين هذه الفرصة لتنفيذ عمليات غير مشروعة، مستحدثين أساليب متعددة للسطو والاحتيال نعرض أبرزها فيما يلي:

أ - جرائم التجارة الإلكترونية

ساهم الاستخدام الواسع للإنترنت و الاستفادة من مكتسبات العصر الرقمي في ازدهار التجارة الإلكترونية، التي أتاحت مزايا عديدة لكنها في المقابل شهدت تصاعدا في حجم الجرائم المرتبطة بها، فالتجارة الإلكترونية تقوم على تسلم المنتجات و أداء الخدمات بصيغة رقمية، مع غياب المستندات الورقية، مما يصعب التمييز بين الرسالة الأصلية و المستنسخة، و يفتح المجال لجرائم التزوير و الاحتيال و قرصنة البيانات الشخصية، كما يتعرض المستهلك لممارسات خادعة، كاللجوء إلى أساليب دعائية مضللة⁴⁰ تهدف إلى دفعه للتعاقد دون الالتزام بشروط المطابقة و السلامة المتعلقة بالسلعة أو الخدمة المعلن عنها.

ب - جرائم غسيل الأموال إلكترونيا

يعد غسيل الأموال أحد أبرز الجرائم شيوعا، كونه يرتبط ارتباطا وثيقا بالجريمة المنظمة العابرة للحدود، كتهريب المخدرات و الأسلحة، و تمويل الإرهاب و التزوير، حيث تشير تقديرات صندوق النقد الدولي إلى أن حجم الأموال التي تغسل سنويا يتراوح بين 620 إلى 1600 مليار دولار، و يعد الجهاز المصرفي الأداة الأكثر فعالية في منح الشرعية لهذه الأموال، إذ توجه أنشطة غاسلي الأموال إلى المصارف عبر تنفيذ عمليات مصرفية معقدة تتضمن وسطاء و شركات وهمية، و البحث عن ملاذات مالية آمنة يصعب فيها تتبع الأصول و الودائع⁴¹، و لا

³⁸المادة 296 من قانون العقوبات الجزائري، المعدل من قانون رقم 23-06.

³⁹المادة 297 من قانون العقوبات الجزائري، المعدل من قانون رقم 23-06.

⁴⁰راضية مشري، مرجع سابق، ص 13.

⁴¹راضية مشري، مرجع سابق، ص 13.

يمكن إنجاز هذه العمليات بسرعة و احترافية دون الاستعانة بالأنظمة المعلوماتية، التي تزيد من فرص نجاحها و تعقد مهمة الأجهزة الرقابية.

ثالثاً: الجرائم الواقعة على أمن الدولة

من أهم الجرائم الإلكترونية التي تهدد أمن الدولة ومجتمعاتها، يمكن الإشارة إلى:

أ - الإرهاب الإلكتروني

الإرهاب الإلكتروني هو استخدام الوسائط الإلكترونية لارتكاب أعمال عدوانية أو ترويعية أو تهديدية، سواء كانت مادية أو معنوية، موجهة ضد الإنسان في دينه أو عرضه أو ماله بغير حق، و يعتمد الإرهابيون على شبكة الأنترنت لنشر أفكارهم المتطرفة و الترويج لمبادئهم، بل و تجاوز ذلك إلى تعليم أساليب ووسائل تنفيذ العمليات الإرهابية، إذ تحتوي الشبكة على مواد ومعلومات تدعم الأنشطة الإرهابية، بما في ذلك مواقع متخصصة في تعليم صناعة المتفجرات، وكيفية استهداف المواقع الإلكترونية و تعطيلها، إضافة إلى طرق اختراق البريد الإلكتروني و آليات تنفيذ الهجمات السيبرانية⁴².

ب - جرائم التجسس الإلكتروني

تتعرض الدول باستمرار لخطر الوقوع ضحية أنشطة التجسس الإلكتروني، الذي يعد نمطا حديثا من أنماط الحصول على المعلومات السرية، حيث يتم استهداف المعلومات الحساسة في المجال العسكري و القطاعات الحيوية للدولة بوسائل تتجاوز الأساليب التقليدية، و يتم في إطار هذه الجرائم اختراق الأجهزة الإلكترونية للمؤسسات العسكرية و الأمنية، و كذا القطاعات الاقتصادية المهمة، بهدف سرقة البيانات أو إتلافها، كما تشمل عمليات التجسس الإلكتروني استهداف الأطراف البشرية القائمة على إدارة تلك القطاعات، و سرقة معلوماتهم الشخصية أو المهنية لاستغلالها في الدخول غير المشروع إلى قواعد البيانات السرية.

وقد يتخذ التجسس الإلكتروني بعدا اقتصاديا، حيث يهدف إلى الحصول على معلومات ذات طابع مالي، أو ممارسة أنشطة الإبتزاز والضغط، أو بيع المعلومات الحساسة في الأسواق غير المشروعة.

الفرع الثاني: الجرائم الواقعة على النظام المعلوماتي

⁴²راضية مشري، مرجع سابق، ص 16.

هناك نوع آخر من الجرائم الإلكترونية يتعلق بالنظام المعلوماتي، ويستهدف إما مكوناته المادية أو مكوناته المنطقية، أو المعلومات المتضمنة فيه، حيث تنقسم هذه الجرائم إلى:

أولاً: الجرائم الواقعة على المكونات المادية للنظام المعلوماتي

تقوم هذه الجرائم على الأجهزة والمعدات الملحقة بالنظام المعلوماتي كالأقراص المدمجة (الأسطوانات) والأشرطة والكابلات، ونظراً للطبيعة المادية لهذه المعدات فإن الجرائم الواقعة عليها تعتبر جرائم تقليدية، كأن تكون محلاً للسرقة أو خيانة الأمانة أو الإلتلاف العمدي أو الإحراج أو العبث بمفاتيح التشغيل، مما يترتب عليها خسائر كبيرة، حيث وقع هذا النوع من الجرائم في فرنسا أدى إلى إلتلاف معدات مؤسسة كبيرة متخصصة في بيع الأنظمة وتوثيقها، بلغت قيمة الخسائر الناتجة عن ذلك 5 ملايين فرنك فرنسي⁴³.

ثانياً: الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي

تعد هذه الصورة من أكثر الجرائم الإلكترونية انتشاراً أو خطورة، حيث تتم عن طريق الاحتيال على معطيات نظم المعالجة الآلية للمعطيات، وذلك بإتلافها أو حذفها أو تغييرها.

فقد عالج المشرع الجزائري هذا النمط من الجرائم من خلال نص المادة 394 مكرر 1 المعدلة من قانون العقوبات، والتي تنص على أنه " يعاقب بالحبس من سنة (1) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000 إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"⁴⁴.

ومن أجل معالجه عناصر هذه الجريمة يتوجب تحديد مفهوم الإلتلاف ثم الوسائل التي يتحقق بها، حيث يقصد بالإلتلاف إفناء مادة الشيء أو هلاكه كلياً، وبالتالي توقف الشيء تماماً عن أداء منفعته ولو لم تفنى مادته سواء كان هذا التوقف كلياً أو جزئياً، ويكون الشيء غير صالح للاستعمال بجعله لا يقوم بوظيفته المصمم من أجلها على النحو الكامل، كما يقصد بإتلاف برامج الحاسوب الآلي ومعلوماته إلتلاف أو محو تعليمات البرامج والبيانات ذاتها، ويطلق على هذه الجريمة مصطلح " تدمير نظم المعلومات " وعادة لا يستهدف مرتكب هذا الإلتلاف تحقيق فائدة مالية لنفسه، بل مجرد إعاقة نظام المعلومات⁴⁵.

⁴³د. بوضياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، جامعة محمد بوضياف، المسيلة، 2018، ص 12.

⁴⁴المادة 394 مكرر 1، من قانون العقوبات الجزائري، المعدل من قانون رقم 24-06.

⁴⁵د. بوضياف إسمهان، مرجع سابق، ص 12.

وعلى ضوء هذه التعريفات يمكن القول بأن الإلتلاف لا يتحقق فقط بالتأثير على مادة الشيء بل يتحقق كذلك حتى في حال الإنقاص من قيمة الشيء الاقتصادية، مما يعني ان العبرة في الإلتلاف ليست مجرد التعرض لمادة الشيء و إنما بمدى مساس الفعل بقيمته، حيث يتحقق الإعتداء الذي يعاقب عليه القانون على اعتبار أن الفعل قد أذهب بأهمية الشيء بالنسبة للملكية، و من أجل الإشارة إلى مدلول الإلتلاف استخدم المشرع الجزائري عدة تعابير حيث وردت عبارات (أدخل، أزال، عدل)، ورغم أن لهذه التعابير مدلولات خاصة بها إلا أنها تندرج جميعها تحت مدلول الإلتلاف وهذا ما ذهبت إليه بعض التشريعات المقارنة خاصة التشريع الفرنسي.

ثالثا: الجرائم الواقعة على البرامج الإلكترونية

وتنقسم هذه الجرائم بدورها الى نوعين رئيسيين:

أ - الجرائم الواقعة على البرامج التطبيقية

تتم هذه الجرائم عن طريق تحديد البرنامج أولا ثم التلاعب به أو تعديله، ومن أمثلتها قيام أحد المبرمجين في البنوك الأمريكية بتعديل برنامج، حيث أضاف دولارا واحدا على كل حساب يزيد عن 10 دولارات وقام بتقييد المصاريف الزائدة في حساب خاص به أطلق عليه اسم (zzwick)⁴⁶.

ب - الجرائم الواقعة على برامج التشغيل

برامج التشغيل هي البرامج المسؤولة عن عمل النظام المعلوماتي حيث تقوم بضبط ترتيب العمليات الخاصة بالنظام، وتقوم هذه الجرائم على طريقة تزويد البرنامج بمجموعة تعليمات إضافية للوصول إليها بشفرة تسمى " باب خلفي (backdoor) "، مما يمكن من الدخول الى جميع المعطيات التي يتضمنها النظام المعلوماتي، ومثال الجريمة تصميم برنامج يتم من خلاله تنفيذ الفعل الإجرامي وقد ورد مثال على ذلك ما قامت به إحدى الشركات التأمينية الأمريكية في مدينة لوس أنجلوس بواسطة مبرمجها، إذ قامت بتصميم برنامج يقوم بتصنيع وثائق تأمين أشخاص وهميين بلغ عددهم 46.000 شخص، بهدف تقاضي الشركة لعملات من اتحاد شركات التأمين⁴⁷.

⁴⁶د. بوضياف إسمهان، مرجع سابق، ص 13.

⁴⁷تمديلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، المؤتمر الدولي الرابع عشر، طرابلس، 2017، ص 104.

المطلب الثاني: الجريمة الإلكترونية في التشريع الجزائري

تعد الجرائم الإلكترونية من الجرائم المستحدثة التي ظهرت بفعل التطور التقني ومع انتشار وسائل الإتصال الرقمية كالأنترنت والمواقع الإلكترونية التي تتيح للعالم تبادل المعلومات عن بعد.

ومن خلال هذا المطلب، سيتم التطرق إلى الطبيعة القانونية للجريمة الإلكترونية وهذا في الفرع الأول، أما الفرع الثاني التطرق إلى موقف المشرع الجزائري من هذه الجريمة.

الفرع الأول: الطبيعة القانونية للجريمة الإلكترونية

سنبين من خلال هذا الفرع الطبيعة القانونية التي تتميز بها الجريمة الإلكترونية كونها تقع في عالم افتراضي، وذلك فيما يلي:

تتميز الجريمة الإلكترونية بطبيعة قانونية خاصة وفريدة تنبثق من خصوصية البيئة الرقمية التي ترتكب فيها، كونها جرائم مستحدثة غير مادية عابرة للحدود، تستهدف أمن المعلومات وأنظمة المعالجة الآلية، شبكات المعلومات تمتلك قدرة استثنائية على نقل وتبادل البيانات ذات الطابعين الشخصي والعام في آن واحد، مما يخلق فضاء إجراميا معقدا، ويرجع ذلك أساسا إلى التوسع الهائل في بنوك المعلومات المتنوعة، إضافة إلى رغبة الأفراد المتزايدة في الارتباط الدائم بهذه الشبكات.

ترتكب هذه الجرائم في سياق المعالجة الإلكترونية للبيانات، سواء تعلق الأمر بمرحلة جمع المعلومات، أو تجهيزها أو إدخالها إلى الحواسيب المرتبطة بالشبكة بهدف الحصول على بيانات محددة، كما قد تحدث هذه الأفعال غير المشروعة في مجال معالجة النصوص أيضا.

تتجلى صعوبة التكييف القانوني لهذه الجرائم في طبيعتها الخاصة التي تختلف جوهريا عن الجرائم التقليدية، فالقواعد القانونية التقليدية لم توضع أصلا لمواجهة هذه الظواهر الإجرامية المستحدثة، وبالتالي فإن محاولة تطبيقها على هذا النوع من الجرائم يثير إشكاليات عديدة، على رأسها مسائل الإثبات القانوني وتعقبات مرتكبي هذه الجرائم⁴⁸.

في ضوء هذه الاعتبارات، يمكن القول إن الجرائم الإلكترونية تتمتع بطبيعة قانونية خاصة⁴⁹ تستدعي معالجة تشريعية وقضائية متميزة تتلاءم مع خصائصها الفريدة.

⁴⁸د. بوضياف إسمهان، مرجع سابق، ص 11.

⁴⁹محمد زكي أبو عامر وعلي عبد القادر القهوجي، قانون العقوبات " القسم الخاص "، دار النهضة العربية، القاهرة، 1993، ص 09.

الفرع الثاني: موقف المشرع الجزائري من الجريمة الإلكترونية

سنتطرق في هذا الفرع إلى موقف المشرع الجزائري من الجريمة الإلكترونية وذلك فيما يلي:

نظرا لحدثة الجريمة الإلكترونية وتباين النظم القانونية والثقافية بين الدول، لم يتم الاتفاق على مفهوم موحد لها، مما أدى إلى غياب تعريف دقيق لهذه الظاهرة الإجرامية، وقد اختار المشرع الجزائري تسميتها بـ " الجرائم المتصلة بتكنولوجيا الإعلام والاتصال "⁵⁰، وكخطوة أولى لمواجهة هذا النوع من الجرائم، أدخلت الحكومة الجزائرية تعديلات على قانون العقوبات بالإضافة إلى القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 و المتمم للأمر رقم 66-156 المؤرخ في 08 يونيو 1966⁵¹، أضيف القانون رقم 24-06 المؤرخ في 28 أبريل 2024 المعدل و المتمم، والمتضمن قانون العقوبات، حيث قد استحدثت هذه التعديلات عقوبات خاصة بالمساس بأنظمة المعالجة الآلية للمعطيات، وذلك في المواد من 394 مكرر إلى مكرر 7 ضمن القسم السابع مكرر، و تتراوح هذه العقوبات من ستة (6) أشهر إلى عشر (10) سنوات، مع غرامات مالية تتراوح بين 60.000 إلى 5.000.000 دينار جزائري، حسب حجم كل جريمة ودرجة خطورتها، كما جرم المشرع الجزائري الأفعال التي تمس أنظمة الحاسب الآلي، استجابة للأشكال المستجدة للإجرام الناتجة عن الثورة المعلوماتية، و هو ما دفعه إلى تعديل قانون العقوبات بموجب القانون 06/24 تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات "⁵².

يعد القانون 09/04 أول قانون في الجزائر يهتم بتنظيم تبادل المعلومات الرقمية، و يؤطر مختلف أنواع المعاملات و الخدمات الإلكترونية، و قد عرفت المادة 02 منه الجريمة الإلكترونية بأنها: " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، و أية جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات الإلكترونية "⁵³، تظهر هذه المادة حرص المشرع على تحقيق الشرعية التشريعية مع استيعاب الأنشطة الاجتماعية الإلكترونية التي يصعب حصرها نظرا لتطور أساليبها و سرعة تغيرها تبعا للتطور التقني، مما يتيح للقاضي هامشا واسعا من التقدير، و بناءا على هذه المادة ، يقسم المشرع الجزائري هذه الجرائم إلى ثلاثة أنواع:

⁵⁰أمنية بوشعرة، سهام موساوي، الإطار القانوني للجريمة الإلكترونية، مذكرة تخرج لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة بجاية، 2018، ص 12.

⁵¹

⁵²المواد 394 مكرر، ومكرر 7، 6، 5، 4، 3، 2، 1 من قانون العقوبات الجزائري، من قانون رقم 04-15 و 06-24 المعدل من قانون 24-06.

⁵³المادة 02 من القانون 09-04، مرجع سابق.

- جرائم المساس بأنظمة المعالجة الآلية للمعطيات.
 - جرائم ترتكب أو يسهل ارتكابها عن طريق المنظومة المعلوماتية.
 - جرائم ترتكب أو يسهل ارتكابها عن طريق نظام الاتصالات الإلكترونية⁵⁴.
- يتضح من موقف المشرع الجزائري إزاء تعريف هذه الجريمة أنه منحها مفهوما واسعا عاما، ورغم تحديده لمجالها عبر ارتباطها بتكنولوجيا الإعلام والاتصال، إلا أن الصيغة المفتوحة للتعريف تجعل المجال واسعا ليشمل أي نوع من الجرائم التي قد يفرزها التطور التكنولوجي، خاصة في ظل التسارع الكبير الذي يشهده هذا المجال، وقد ورد في المادة السابقة النص على: ".... أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات الإلكترونية"⁵⁵.
- باستخدام المشرع الجزائري لمصطلح " الجرائم المتصلة بتكنولوجيات الإعلام والاتصال "، للإشارة إلى الجرائم الإلكترونية، فإنه يجمع بين تقنية الحوسبة وتقنية الاتصالات الحديثة، فالأولى تقوم على استخدام الوسائل التقنية لإدارة وتنظيم ومعالجة البيانات، بينما تعتمد الثانية على وسائل تقنية لنقل المعلومات بشتى أنواعها، ولذلك نرى أن المشرع الجزائري وفق في اختيار هذا المصطلح، الذي يتسق مع المفهوم الواسع للجرائم الإلكترونية، وذلك للأسباب الآتية:
- الجرائم الناشئة في البيئة الرقمية هي جرائم حديثة، يرتبط مفهومها بظهور التكنولوجيا الحديثة وما يرافقها من تطور مستمر في تشغيل المعلومات وتخزينها ونقلها بشكل إلكتروني.
 - يتمتع هذا المصطلح بمفهوم واسع، يشمل جميع الأفعال التي ترتكب في بيئة افتراضية، بما فيها الجرائم التي تقع على نظم المعالجة الآلية للبيانات أو تستخدمها كوسيلة لارتكابها.
 - يعبر هذا المصطلح عن الطابع التقني المميز للجرائم الإلكترونية.
 - غير أن المشرع لم يحدد صور السلوك المجرم الذي يرتكب أو يسهل ارتكابه ضمن منظومة معلوماتية أو نظام اتصالات إلكترونية.
 - كما أن هذا التعريف يتضمن تكرارا، ذلك أن مفهوم نظام الاتصالات الإلكترونية يندرج ضمن مصطلح المنظومة المعلوماتية، خاصة وأن المشرع الجزائري عرف هذه الأخيرة في المادة 02 بأنها: " نظام منفصل، ومجموعة من الأنظمة المتصلة أو المرتبطة ببعضها، يقوم واحد منها أو

⁵⁴يزيد بوحليط، مرجع سابق، ص 55.

⁵⁵راضية مشري، مرجع سابق، ص 6.

أكثر بمعالجة آلية للمعلومات، لتنفيذ برنامج معين"، ومن جهة نظرنا فإن التعريف الأقرب للدقة للجريمة الإلكترونية هو أنها كل فعل يتم باستخدام النظام المعلوماتي، ويكون لهذا الضام دور رئيسي في ارتكاب السلوك المجرم⁵⁶.

⁵⁶يزيد بوحليط، مرجع سابق، ص 59-60.

ملخص الفصل الأول:

تعتبر الجريمة الإلكترونية، من الجرائم المستحدثة، فهي كسلوك غير مشروع يستخدم بالحاسوب أو عن طريق شبكات التواصل كوسيلة أو محل، فالقانون 04-09 جرم الأفعال كالدخول الغير مشروع و الاحتيال الإلكتروني، كما تتميز هذه الجريمة بخصائص و سمات تميزها عن باقي الجرائم، فهي جريمة عابرة للحدود، و صعبة الإثبات، و تتسم بالنعومة و السهولة، و لا يتم التبليغ عنها غالبا، كما قد تتميز الجريمة الإلكترونية الحديثة عن الجريمة التقليدية في كون هذه الجريمة تقع في الفضاء الرقمي حيث يرتكب الجاني جريمته في بلد و المجني عليه يكون في بلد آخر، أما الجريمة التقليدية تقع في واقع مادي ملموس يكون فيه مسرح للجريمة، و حتى تقوم المسؤولية الجنائية لهذه الجريمة يجب توافر شروط منها الأهلية الجنائية الإرادة و حرية الاختيار حتى يتعاقب المجرم على أفعاله، حيث أن هذه الجريمة واسعة و متشعبة قد ترتكب بواسطة النظام المعلوماتي كالتعدي على حرمة الحياة الخاصة و التجارة الإلكترونية و الإرهاب الإلكتروني، و لهذا قام المشرع الجزائري بتجريم هذه الجريمة وصنفها ضمن الجرائم السيبرانية التي تهدد الأمن المعلوماتي للأفراد والمؤسسات بكونها فعل غير قانوني.

الفصل الثاني:

الإطار الإجرائي للمسؤولية الجزائية عن الجرائم الإلكترونية

وفق القانون الجزائري وبعض التشريعات العربية

تمهيد:

تطرح الجرائم الإلكترونية، بحكم طبيعتها التقنية والمعقدة إشكالات قانونية وإجرائية بالغة الصعوبة، تتعلق في جوهرها بكيفية إسناد الفعل الإجرامي إلى فاعله، وجمع الأدلة الرقمية والتحقق من صحتها وحجبتها وصولاً إلى إقامة المسؤولية الجزائية، فإذا كانت قواعد المسؤولية الجزائية التقليدية قد وضعت في الأصل لمواجهة أفعال مادية ملموسة، فإن البيئة الرقمية تقتضي تطوير آليات إجرائية استثنائية تراعي خصوصية الوسائل الإلكترونية والأدلة المعلوماتية، مع الحفاظ على ضمانات المحاكمة العادلة وحقوق الدفاع.

حيث بذلت الدول العربية جهوداً تشريعية متفاوتة لمواكبة التطورات التقنية المتسارعة، فسعت إلى تكييف قواعد الإجراءات الجزائية التقليدية تتلاءم مع طبيعة الجريمة الإلكترونية، كما استحدثت إجراءات جديدة كالسرب الإلكتروني واعتراض المراسلات والمراقبة الإلكترونية، إذ أن التشريع الجزائري يمكن وضعه في موازنة مع التشريعات العربية من خلال التعديلات التي أدخلت على قانون العقوبات وقانون الإجراءات الجزائية، بوضع عقوبات رادعة على مرتكبين هذه الجرائم.

وفي هذا السياق، يمكن اعتبار أن نقطة البداية في هذا الفصل، الذي يحمل عنوان " الإطار الإجرائي للمسؤولية الجنائية عن الجرائم الإلكترونية وفق القانون الجزائري وبعض التشريعات العربية"، تتمثل في تقسيمه إلى مبحثين رئيسيين: يتناول المبحث الأول تنظيم المسؤولية الجنائية وفق القانون الجزائري وبعض التشريعات العربية، مع التركيز على أركان الجريمة الإلكترونية وإجراءات التحقيق العامة و الخاصة لهذه الجريمة، بينما يناقش المبحث الثاني المقارنة بين التشريع الجزائري وبعض التشريعات العربية، وآليات مكافحة هذه الجرائم بما في ذلك التحديات والحلول الممكنة.

المبحث الأول: تنظيم المسؤولية الجزائية وفق القانون الجزائري للجرائم الإلكترونية

تعد المسؤولية الجزائية ركيزة أساسية في أي نظام قانوني جزائي، حيث أرسى المشرع الجزائري قواعد هذه المسؤولية من خلال مزيج تشريعي متكامل، يستمد مادته من قانون العقوبات الذي يحدد الأفعال المجرمة والعقوبات المقررة لها، ومن قانون الإجراءات الجزائية الذي ينظم آليات إثباتها ومحاكمة مرتكبيها، بالإضافة إلى قوانين خاصة استحدثت لتغطية جرائم مستحدثة.

وعليه تم تقسيم هذا المبحث إلى مطلبين الأول يتناول الأركان القانونية للجريمة الإلكترونية، والثاني تطرقنا فيها إلى إجراءات التحقيق العامة والخاصة لهذه الجريمة.

المطلب الأول: أركان الجريمة الإلكترونية

تستند الجريمة الإلكترونية في قيامها على ثلاثة أركان أساسية، الركن الشرعي بنص يجرم الفعل، والركن المادي حيث يكون هناك سلوك إجرامي ملموس أو معنوي، والركن المعنوي من خلال القصد الجنائي، وذلك بحكم وقوعها في الفضاء الرقمي.

وهذا ما يستدعي إلى دراسة الأركان القانونية للجريمة الإلكترونية، وذلك بالنظر في الفرع الأول إلى الركن الشرعي وفي الفرع الثاني إلى الركن المادي والركن المعنوي.

الفرع الأول: الركن الشرعي

يعتبر الركن الشرعي الأساس الذي تبنى عليه أي جريمة، حيث يقوم هذا الركن في الجرائم الإلكترونية على وجود نص تشريعي يجرم السلوك و يحدد العقوبة المناسبة له، و أن يكون هذا النص ساريا من حيث الزمان و المكان و الأشخاص على مرتكبي الفعل الإجرامي، و ذلك وفقا لمبدأ شرعية الجرائم و العقوبات، طبقا للمادة الأولى من قانون العقوبات الجزائري التي تقضي بأنه " لا جريمة و لا عقوبة أو تدابير أمن بغير قانون"⁵⁷، تعتبر هذه المادة ضمانا أساسية للمجرم إذ لا يجوز تطبيق أي عقوبة غير تلك المنصوص عليها صراحة في القانون، حيث مع الانتشار المتزايد و المستمر للجرائم الإلكترونية أصبح من الضروري على الدول سن تشريعات و نصوص قانونية خاصة لمواجهة هذه الجرائم و مكافحتها.

فالركن الشرعي في الجرائم المعلوماتية هو نص التجريم الواجب بالتطبيق على الفعل و العقوبة المقررة له، إذ أن بالرجوع إلى القانون رقم 04-09 الذي يحدد القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها، و قانون العقوبات الجزائري و

⁵⁷المادة 1 من قانون العقوبات الجزائري المعدل والمتمم.

حسب آخر تعديل بموجب القانون رقم 06-24 التي نصت صراحة على المساس بأنظمة المعالجة الآلية للمعطيات في المواد من 394 مكرر إلى 394 مكرر 8 من قانون العقوبات المعدل و المتمم و التي عاقبت على هذه الجريمة، فالمادة 394 مكرر 1 نصت على أنه " يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات و بغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"⁵⁸.

الفرع الثاني: الركن المادي والركن المعنوي

أولاً: الركن المادي

يشترط في الركن المادي وجود فعل أو امتناع يمكن إثباته، إذ أن لا عبرة فيما يجول في ذهن الإنسان من أفكار ما لم تترجم إلى سلوك مادي لأن النوايا وحدها لا تدخل نطاق التجريم، وهذا ما يجعل هذا الركن يتفاوت حسب طبيعة الفعل وتصنيفه، حيث يتألف هذا الركن من السلوك المادي والنتيجة الإجرامية والعلاقة السببية بينهما، والمتمثلة في:

أ - السلوك الإجرامي

يتمثل السلوك الإجرامي في الجريمة الإلكترونية في:

- الدخول أو البقاء عن طريق الغش في نظام المعالجة الآلية للمعطيات

يقصد بفعل الدخول هنا، الدخول المادي باستخدام الوسائل التقنية والرقمية التي تظهر من خلالها المعطيات المعلوماتية، ولا يعد فعل الدخول في حد ذاته سلوكاً غير مشروع، بل يكتسب الصفة الإجرامية عندما يتم دون ترخيص⁵⁹، وهذا ما أشار إليه المشرع الجزائري في المادة 394 مكرر من قانون العقوبات المعدل والمتمم، حيث نص على ما يلي: " يعاقب بالحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 60.000 دج إلى 200.000 دج، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات، أو يحاول ذلك..."⁶⁰.

ويقصد بفعل البقاء غير المشروع، استمرار شخص في التواجد داخل نظام المعالجة الآلية للمعطيات دون إذن من صاحب النظام أو من له سلطة التحكم فيه، كأن يدخل شخص إلى النظام عن طريق الخطأ أو بحسن نية ثم يظل فيه رغم علمه بعدم جواز بقائه لعدم حصوله على ترخيص بذلك⁶⁰، حيث نصت الفقرة الثانية من المادة 394 مكرر على ذلك بقولها:

⁵⁸المادة 394 مكرر 1 من القانون رقم 06-24 المعدل والمتمم من قانون العقوبات الجزائري.

⁵⁹مهداوي حنان، التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري، مجلة الفكر القانوني والسياسي، كلية الحقوق والعلوم السياسية جامعة محمد لمين دباغين سطيف 2، المجلد 6، العدد 2، 2022، ص 7.

⁶⁰قارة آمال، الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق، جامعة الجزائر، 2001، ص 44.

"تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة. وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة، تكون العقوبة الحبس من سنة (1) إلى ثلاث (3) سنوات والغرامة من 100.000 دج إلى 300.000 دج". فالحالة الأولى تكون إذا نتج عن الدخول أو البقاء محو أو تعديل في البيانات التي يحتويها النظام، أما الحالة الثانية تكون إذا ترتب على الدخول أو البقاء تخريب نظام اشتغال المنظومة أو إعاقته عن أداء وظيفته.

ب - النتيجة الإجرامية

تتحقق النتيجة الإجرامية من خلال:

- جرائم الإعتداء على المعطيات الموجودة داخل نظام المعلوماتية

نص المشرع الجزائي على هذا النوع من الجرائم في المادتين 394 مكرر 1 و 394 مكرر 2 من قانون العقوبات المعدل والمتمم، حيث جاء فيهما:

المادة 394 مكرر 1: "يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

المادة 394 مكرر 2: "يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش بما يأتي:

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

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

يتضح من هذين النصين أن جرائم الإعتداء على المعطيات الموجودة داخل نظام المعلوماتية تتخذ صورتين رئيسيتين:

1- جريمة التلاعب بالمعطيات

تتحقق هذه الجريمة وفقا للمادة 394 مكرر 1، بارتكاب إحدى الصور الثلاث التالية:

- الإدخال بطريق الغش لمعطيات في نظام المعلوماتية.
- المحو بطريق الغش لمعطيات في نظام المعلوماتية.
- التعديل بطريق الغش لمعطيات في نظام المعلوماتية.

2- جريمة التعامل في معطيات غير مشروعة

تتحقق هذه الجريمة وفقا للمادة 394 مكرر 2، بارتكاب إحدى الصورتين التاليتين:

- التعامل في معطيات صالحة لارتكاب جريمة:

يقصد بالتعامل هنا أي سلوك يكشف عن وجود علاقة بين شخص ومعطيات غير مشروعة، حيث تتجلى هذه العلاقة في قيام الشخص بأحد الأنشطة الآتية: تصميم هذه المعطيات، البحث في مضمونها، تجميعها، توفيرها، نشرها، أو الإتجار فيها، أي أن المعطيات تصل إلى يد الجاني وتكون تحت تصرفه ليرتكب بواسطتها جريمة⁶¹.

- التعامل في معطيات متحصلة من جريمة:

يتحقق هذا السلوك المجرم بالقيام بأحد الأفعال التي نصت عليها المادة 394 مكرر 2، والمتمثلة في: حيازة، إنشاء، نشر، أو استعمال المعطيات التي تم الحصول عليها نتيجة جريمة الدخول أو البقاء بطريق الغش، أو نتيجة جريمة التلاعب بالمعطيات.

ج - العلاقة السببية ما بين السلوك الإجرامي والنتيجة

تعتبر العلاقة السببية أحد عناصر الركن المادي فهي الصلة بين السلوك الذي يعترف به القانون كسبب والأثر الذي يعترف به القانون كنتيجة، حيث تعتبر الرابطة بين السلوك الإجرامي والنتيجة الإجرامية، بمعنى أن الشخص لا يتحمل التبعة القانونية عما اقترفه من فعل إلا إذا كان فعله وحده هو سبب حصول النتيجة، ففي الجرائم الإلكترونية يجب أن يتضمن السلوك الدخول الحاسوب، ثم التعدي على خصوصية النظام المعلوماتي، وهنا تقوم العلاقة السببية بمجرد وقوع ضرر، سواء كانت الجريمة تامة أو في مرحلة الشروع في ارتكابها⁶².

ثانيا: الركن المعنوي

تتطلب الجريمة الإلكترونية لقيامها للركن المعنوي إلى جانب الركن الشرعي والمادي لها، فهي تعد من الجرائم العمدية القائمة على أساس وجود القصد الجنائي الذي يقوم بتوافر عنصري العلم والإرادة.

1- القصد العام

أ - العلم

يقصد به إدراك الفاعل لطبيعة أفعاله، أي على الجاني أن يكون على علم بأن الولوج إلى داخل النظام بشكل غير مصرح به يعتبر جريمة لما يتضمنه من برامج و معلومات⁶³، كما يجب

⁶¹ مهداوي حنان، مرجع سابق، ص 9.

⁶² عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2004، ص 267.

⁶³ عشا حزمة، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، العدد 02، المجلد 06، جامعة محمد بوضياف، المسيلة، 2020، ص 175.

أن يكون الجاني مدركاً لطبيعة الفعل أو الامتناع الذي يقوم به وأنه سبب ضرراً للمجني عليه⁶⁴، فالأصل أن الفاعل في الجريمة الإلكترونية يوجه سلوكه الإجرامي نحو ارتكاب فعل غير مشروع أو غير مسموح به مع علمه و قاصداً ذلك.

ب - الإرادة

وتتمثل في رغبة الجاني نحو تحقيق نتيجة غير مشروعة، كالمساس بحق أو مصلحة يحميها القانون، إذ يجب أن تتجه إرادة الجاني إلى تحقيق نتيجة إجرامية محددة والمتمثلة في المساس بأنظمة المعالجة الآلية للمعطيات بالدخول إليها بطريقة غير قانونية. تنقسم الإرادة إلى إرادة الفعل وإرادة النتيجة لإثبات المسؤولية ويحب أن تكون إرادة الفعل متجهة نحو ارتكاب الفعل دون وجود عيوب في الإرادة مثل الإكراه، وتوافر إرادة النتيجة الناشئة عن ذلك السلوك بالتهديد المقترن بطلب اتجاهها نحو تحقيق النتيجة الجرمية من ذلك التهديد، وهي الحصول على منفعة من المجني عليه أيا كان شكلها.

2- القصد الخاص

هو ما يشترط توافره في بعض الجرائم دون غيرها، حيث لا يكفي لارتكاب الفاعل الفعل بل يجب التأكد من تحقق النتيجة الإجرامية، فالجريمة الإلكترونية تتطلب معرفة خاصة بتكنولوجيا المعلومات لتنفيذها، مما يجعلها جريمة عمدية يكتفي فيها بالقصد العام ولكن هذا لا يمنع من توافر القصد الجنائي الخاص في بعضها، كجرائم تشويه السمعة عبر الأنترنت وجرائم نشر الفيروسات عبر الشبكة.

المطلب الثاني: إجراءات التحقيق العامة والخاصة للجريمة الإلكترونية

تتميز الجريمة الإلكترونية بإجراءات تختلف عن الجريمة التقليدية، سواء تعلق الأمر بمرحلة جمع الاستدلالات، أو التحقيق، أو المحاكمة، وهذا راجع لطبيعتها المرتبطة بالفضاء الرقمي، مما يستدعي اعتماد أساليب مبتكرة في معالجتها ومتخصصة تجمع بين مراقبة الاتصالات الإلكترونية، والخبرة الفنية في التعامل مع البيئة الرقمية، والتفتيش المنظم للأجهزة والبيانات، ومعاينة الأدلة من خلال فحص الأجهزة وهذا لضمان صحتها وقبولها أمام المحكمة.

حيث سنتطرق في هذا الفرع الأول إلى إجراءات التحقيق العامة للجريمة الإلكترونية، وفي الفرع الثاني إلى إجراءات التحقيق الخاصة.

الفرع الأول: إجراءات التحقيق العامة للجريمة الإلكترونية

⁶⁴ باقر غازي حنون، حسان حماد، حميد، جريمة الابتزاز الإلكتروني، دراسة مقارنة، مجلة، دراسات البصرة، العدد 42، سنة 2016، ص 69.

سنتطرق في هذا الفرع لإجراءات التحقيق العامة منها الخبرة الفنية، التفتيش، المعاينة، وذلك على النحو التالي:

أولاً: الخبرة الفنية وتدريب الكوادر

أ - الخبرة

تعتبر الخبرة أحد الإجراءات التي يعتمد عليها القضاء لإثبات الجريمة الإلكترونية و تحليل الأدلة الرقمية وكشف أنماطها، وهذا ما يتطلب الاستعانة بأصحاب الخبرة والاختصاص في المجال الفني والتقني، حيث تمثل الخبرة وسيلة للتفسير الفني للأدلة والاستعانة بالمعلومات العلمية، فهيلست دليلاً مستقلاً بذاته، بل تقييم للدليل القولي أو المادي⁶⁵.

يلعب الخبير التقني أو المختص بالجرائم الإلكترونية دوراً محورياً في التحقيق و المحاكمة و ذلك من خلال خبراته و مؤهلاته العالية و مقدرته الفنية و معرفته الشاملة لشبكة الأنترنت و التعامل مع هذه الجريمة التي خلقتها التقنية الحديثة، و ذلك للحفاظ على الأدلة الرقمية دون تلف⁶⁶، فقد تكون الجريمة المرتكبة تزوير مستندات أو تلاعباً في البيانات أو إطلاق فيروسات أو تجسس⁶⁷.

قد تكتسب الخبرة أهمية بالغة في مجال الجرائم الإلكترونية و ذلك من خلال تحديد مصدر الجريمة بتحليل عناوين (IP) و تتبع مصدر الرسائل، و تحديد مصدر الحسابات المزيفة و استرجاع الرسائل المشفرة بما فيها الملفات، لهذا يكلف الخبير بتحليل الأجهزة الإلكترونية و ذلك لفحص الحواسيب و الهواتف و الخوادم المستخدمة في الجريمة، و التأكد من وجود برامج خبيثة اختراق، كما يتم كشف هوية الجاني عبر طريق تقنيات تتبع المستخدمين، حتى و إن كانوا يستخدمون وسائل إخفاء الهوية (VPN، أو المتصفحات المجهولة...)، و في الأخير إعداد تقرير فني حيث يقدم الخبير تقريراً تقنياً للقاضي يتضمن نتائج الفحص و الدلائل التقنية ، مع إبداء رأيه الفني حول كيفية وقوع الجريمة.

أجاز المشرع الجزائري للمحقق الاستعانة بالخبرة وندب خبير في أي وقت أثناء التحقيق، بهدف كشف الحقيقة بالدقة اللازمة، ويعد ندب الخبير في المسائل الفنية الدقيقة واجبة في مجال الجرائم الإلكترونية نظراً لتعقيدها، ولتطور أساليب ارتكابها.

⁶⁵ حمد فتحي سرور، الوسيط في شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، الطبعة السابعة، 1996، ص 588.

⁶⁶ أسامة أبو الحاج، دليلك الشخصي إلى الأنترنت، دار النهضة العربية، القاهرة، 1998، ص 20.

⁶⁷ أرشد بشير إبراهيم، التحقيق الجنائي في جرائم تقنية المعلومات، بحث منشور في مجلة دراسات استراتيجية، مركز الإمارات للدراسات والبحوث الاستراتيجية، العدد 131، 2008، ص 69.

ب - تدريب الكوادر

تتطلب طبيعة هذه الجرائم معرفة متخصصة بالأنظمة المعلوماتية و كيفية استخدامها، و لا تتحقق هذه المعرفة إلا من خلال تدريب القائمين على أعمال التحري و التحقيق، حيث يجب أن يشتمل التدريب في الجرائم الإلكترونية على كيفية تشغيل الحاسبات و الوسائل الإلكترونية لاكتساب مهارات في البرمجيات و المعالجة الإلكترونية للبيانات، و هذا عن طريق تدريب عملي عبر المحاكاة لسيناريوهات واقعية كالتهديد عبر الفيسبوك أو الواتساب بنشر صورهم ، كما أن الاشتراك في منصات مثل (CERT،INTERPOL) يساعدهم للاطلاع على أحدث أساليب مكافحة هذه الجريمة.

علاوة على ذلك، ينبغي للأجهزة الأمنية استقطاب متخصصين ذوي كفاءات في المجال الإلكتروني و ضمهم و الاستفادة منهم، و من أجل ذلك ينبغي على كليات الشرطة من جهة أن تعمل جاهدة لقبول دفعات الجامعيين من خريجي كليات الإعلام الآلي لتخرجهم ضباطا مؤهلين قانونيا و تقنيا، و في الوقت نفسه يتعين على كليات القانون جعل مادة الإعلام الآلي و تقنية المعلومات من المواد الأساسية، لتكوين ثقافة قانونية و حاسوبية لدى الخريجين⁶⁸.

كما يمكن أن يتم التعاون الدولي في مجال مكافحة تدريب الكوادر من خلال عقد ندوات ومؤتمرات متخصصة في مواجهة تلك الجرائم، وعلى هامش هذه المؤتمرات والندوات، ورش العمل الجماعي التي تعقد اللقاءات وتبادل الآراء والخبراء⁶⁹.

ثانيا: معاينة مسرح الجريمة الإلكترونية

تختلف معاينة الجريمة الإلكترونية اختلافا جوهريا عن الجريمة التقليدية، لأنها لا تقع في مكان مادي بل داخل بيئة الحاسوب و البيانات الرقمية المنتشرة في شبكاته، و ذاكرته، و أقراصه الصلب⁷⁰.

حيث يقصد بمعاينة الجريمة الإلكترونية معاينة الآثار و البصمات الإلكترونية التي يتركها مستخدم الشبكة المعلوماتية و التي تشمل الدخول إلى نظام المعالجة الآلية للمعطيات مثلا الرسائل المرسلة للضحية، و كافة الاتصالات الإلكترونية التي تمت من خلال الحاسب الآلي في حالة تهديد المجني عليه بصوره أو مقابل الحصول على منفعة ما، فالمعاينة تتم داخل تلك

⁶⁸ حسين بن سعيد بن سيف الغافري، الجهود الدولية في مكافحة جرائم الأنترنت، القاهرة، دار النهضة العربية، 2009، ص 44.

⁶⁹ حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنت، مرجع سابق، ص 685-686.

⁷⁰ حسين طاهري، الجرائم الإلكترونية، دار الخلدونية، الطبعة الأولى، الجزائر، 2022، ص 71.

الأجهزة أو داخل شبكة الأنترنت من خلال الاطلاع على بيانات المتهم كالولوج إلى بريده الإلكتروني أو حسابه على مواقع التواصل الاجتماعي، كما يمكن فحص الحاسوب الخاص بالمتهم لتعرف على المواقع التي زارها أو الملفات التي حملها أو اخترقها، وبهذا يمكن لسلطة التحقيق الانتقال إلى العالم الافتراضي للمعينة من مكتبها الخاص بها في المحكمة من خلال حاسبها الآلي، كما يمكن اللجوء إلى مقهى الأنترنت (Internet Café)، و التوجه إلى عمل مزود بخدمة الأنترنت (Server Provider) الذي يعتبر أفضل مكان يمكن إجراء المعينة فيه في الجرائم الإلكترونية.

فمصرح الجريمة في الجرائم الإلكترونية هو مسرح سبيرانتي افتراضي يقع في بيئة الحاسوب، بحيث لا يتم التعامل مع هذه الأدلة الموجودة إلا على يد خبير متخصص في هذا النوع من الأدلة الرقمية.

ثالثا: التفتيش في مجال الجرائم الإلكترونية

يعد التفتيش إجراء من إجراءات التحقيق الابتدائي إذا صدر الأمر من قاضي التحقيق بعد توليه القضية، أما إذا صدر الأمر من وكيل الجمهورية إلى ضابط الشرطة القضائية أثناء مرحلة جمع الاستدلالات، يعتبر إجراءات استدلاليا⁷¹، حيث أن الجريمة الإلكترونية من الجرائم التي يصعب إثباتها، كون الجاني لا يترك آثار مادية باعتباره مجرما محترفا يتقن استخدام النظام المعلوماتي وأساليب البيئة الرقمية، إذ يتطلب في هذا النوع من الجرائم تدريباً خاصاً و تكنولوجيا متطور لجمع الأدلة و إجراءات التفتيش، حيث يتم التفتيش من خلال الولوج إلى الأنظمة المعلوماتية و البرامج المستخدمة، و البحث في البيانات الرقمية المخزنة، و ذلك وفقاً لمقتضيات البحث و التحري.

فالتفتيش في الجرائم الإلكترونية إما يكون عن المكونات المادية للحاسوب، أو عن المكونات المعنوية كالبيانات والمعلومات وهي كالاتي:

أ -تفتيش المكونات المادية للحاسب الآلي

يعد تفتيش المكونات المادية للحاسب الآلي في إطار الجرائم الإلكترونية إجراء يمكن تطبيق القواعد التقليدية للتفتيش عليه بسهولة، فمن المنطق عليه أن الولوج إلى هذه المكونات المتعلقة بهذه الجريمة يخضع لإجراءات قانونية خاصة بالتفتيش، كطبيعة المكان الذي توجد فيه

⁷¹على شلال، المستحدث في قانون الإجراءات الجزائية الجزائري، ط 2، دار هومه للطباعة والنشر والتوزيع، الجزائر، 2020، ص 48.

أو صفته فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حرمة خاصة، فلا يجوز هنا تفتيشها إلا في حالات التي يجوز فيها التفتيش و بنفس الإجراءات المقررة قانوناً في التشريعات المختلفة، مع مراعاة ما إذا كانت المكونات منعزلة عن غيرها، أو متصلة بحاسوب آخر في مكان آخر كمنزل غير المتهم، أو إذا كان الشخص يحمل المكونات أو يسيطر عليها في مكان عام، و بالتالي يجب مراعاة القيود القانونية لتفتيش تلك الأماكن⁷².

ب- التفتيش عن المكونات المعنوية للحاسب الآلي

اختلف الفقهاء حول جواز التفتيش أو عدم جوازه في المكونات المعنوية للحاسب الآلي، حيث يرى أصحاب الاتجاه الأول جواز التفتيش وضبط البيانات الإلكترونية بمختلف أشكالها، مستندين إلى أن القوانين الإجرائية عندما تنص على الإذن بضبط أي شيء، فإن ذلك يجب أن يفسر على نحو يشمل بيانات الكمبيوتر المحسوسة وغير المحسوسة، أما الاتجاه الثاني يرى أن المفهوم المادي لا ينطبق على بيانات الحاسب غير المرئية أو غير الملموسة.

فقد تعرضت التشريعات العربية له، منها المشرع الأردني تعرض لموضوع التفتيش عن الكيانات المعنوية للحاسب الآلي، حيث نص على أنه: " يجوز لموظفي الضابطة العدلية بعد الحصول على إذن من المدعي العام المختص أو من المحكمة المختصة، الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم"⁷³، و المشرع القطري الذي أجاز في نص المادة 14 على أنه " للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص و الأماكن و أنظمة المعلومات ذات الصلة بالجريمة... و يجب أن يكون أمر التفتيش مسبباً و محدداً، و يجوز تجديده أكثر من مرة ما دامت مبررات هذا الإجراء قائمة... فإذا أسفر التفتيش عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة، يتعين على مأموري الضبط القضائي عرضها على النيابة العامة لاتخاذ ما يلزم بشأنها"⁷⁴، إضافة إلى ذلك نصت في المادة 15 على: " لا يجوز استبعاد أي دليل ناتج عن وسيلة من وسائل تقنية المعلومات أو أنظمة المعلومات أو شبكات

⁷² د. مخلص إبراهيم الزعبي، فاعلية القوانين والتشريعات العربية في مكافحة الجرائم الإلكترونية، المجلة العربية للنشر العلمي، العدد 37، 2021، ص 287.

⁷³ المادة رقم 12، الفقرة (أ)، من قانون جرائم أنظمة المعلومات الأردني رقم 9 لسنة 2010.

⁷⁴ المادة رقم 14، من قانون مكافحة الجرائم الإلكترونية القطري، لسنة 2014.

المعلومات أو المواقع الإلكترونية أو البيانات و المعلومات الإلكترونية بسبب طبيعة ذلك الدليل⁷⁵.

فنستنتج من هذه النصوص أن المشرع الأردني والقطري أحسنا التوجه إلى جواز التفتيش على الكيانات المعنوية للحاسب الآلي.

الفرع الثاني: إجراءات التحقيق الخاصة للجريمة الإلكترونية

استحدث التشريع الجزائي تماشياً مع التشريعات الحديثة إجراءات خاصة لمواجهة الجرائم الإلكترونية، نظراً لخطورتها وسرعة ارتكابها، وبهذا نقسم هذه الإجراءات إلى نوعين رئيسيين:

أولاً: مراقبة الاتصالات الإلكترونية

نظراً للخطورة البالغة التي تمثلها الجريمة الإلكترونية، لجأ المشرعون إلى سن قوانين تمنح السلطات المختصة صلاحية مراقبة جوانب معينة من الأنشطة الخاصة للأفراد، وذلك بهدف جمع الأدلة اللازمة للكشف عن الحقيقة، كما استحدث المشرع الجزائي إجراء المراقبة الإلكترونية بموجب المادة (3) من القانون 04-09 المتعلق بالوقاية من الجرائم المتصلة بالتكنولوجيا الاعلام والاتصال ومكافحتها، حيث أجاز هذا النص تبعاً لمتطلبات التحريات والتحقيقات القضائية الجارية في إطار هذا النوع من الجرائم، اللجوء إلى وضع أساليب بحث وتدابير تقنية خاصة لمواجهةها، فقد جاء في نص المادة (4) من نفس القانون حالات تستدعي اللجوء إلى المراقبة الإلكترونية للاتصالات يمكن حصرها كالآتي:

- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة⁷⁶.

⁷⁵ المادة رقم 15، من قانون مكافحة الجرائم الإلكترونية القطري، لسنة 2014.

⁷⁶ المادة 3 و 4 من القانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بالتكنولوجيا الاعلام والاتصال ومكافحتها.

كما قد نجد أن قانون الإجراءات الجزائية نص على المراقبة الإلكترونية في اعتراض المراسلات والتقاط الصور وتسجيل الأصوات، وتتمثل هذه الأساليب في:

أ - اعتراض المراسلات

يعتبر اعتراض المراسلات نوعاً من أنواع المراقبة الإلكترونية، حيث أجاز المشرع الجزائري في المادة 65 و المعدلة بموجب القانون 14-25 التي تنص على أنه "يعد محضر اتفاق الوساطة سنداً تنفيذياً طبقاً للتشريع الساري المفعول"⁷⁷، حيث حصر المشرع مفهوم المراسلات في تلك التي تتم بواسطة وسائل الإتصال السلكية واللاسلكية، وهو ما يعرف اصطلاحاً "بالتتصت التليفوني"، رغم أن المشرع الجزائري لم يتطرق إلى تعريف صريح لهذه التقنية بل اكتفى بتعريف الاتصالات الإلكترونية فقط باعتبار أن المراقبة الإلكترونية تتمثل في مراقبة شبكة الاتصالات، غير أن القضاء الفرنسي عرفها على أنها تقنية يتم من خلالها الاعتراض عن طريق ربط خط هاتفية للمشتبه فيه للجوء إلى تسجيل المكالمات في أنشطة مغناطيسية⁷⁸.

كما تنص المادة 22 من المرسوم التنفيذي رقم 20-62 المؤرخ في 20 رجب 1441 الموافق ل 15 مارس سنة 2020، "على أنه يلتزم صاحب الرخصة باتخاذ التدابير التي من شأنها أن تضمن سرية المعلومات التي يحوزها على المشتركين وكذا سرية مكالماتهم وألا يسمح بوضع أي ترتيبات بغرض اعتراض الاتصالات أو مراقبة المكالمات الهاتفية والمحادثات والمبادلات الإلكترونية دون إذن مسبق من السلطة القضائية وفقاً للتشريع المعمول به".

وبهذا نستخلص أن مراقبة المراسلات السلكية واللاسلكية بشكل سري تعتبر جزءاً من إجراءات البحث والتحري عن الجرائم، ووسيلة لجمع الأدلة والمعلومات المتعلقة بالأشخاص المشتبه بتورطهم فيها. غير أن المراقبة الإلكترونية للاتصالات الشخصية تعتبر انتهاكاً لخصوصية الأفراد إذا لم تتم وفقاً للضوابط والشروط التي يحددها القانون.

ب - التقاط الصور

يقصد بها تثبيت صورة شخص على مادة خاصة مما يسهل الاطلاع عليها و نسخها و ذلك باستخدام الوسائل المعدة لذلك⁷⁹.

⁷⁷ المادة 65 المعدلة بموجب القانون 14-25

⁷⁸ شنتير خضرة، الآليات القانونية لمكافحة الجريمة الإلكترونية، دراسة مقارنة، 2022، ص 133.

⁷⁹ شنتير خضرة، مرجع سابق، ص 140.

بمعنى أي النقاط أو تسجيل أو نشر صور أو فيديوهات خاصة دون إذن من صاحبها، يعتبر انتهاكا لخصوصية الإنسان ويعاقب عليه القانون، كجريمة الإبتزاز الإلكتروني التي تتم من خلال تهديد الضحايا للحصول على مبالغ مالية، وبالتالي تعد جريمة النقاط الصور جريمة في حد ذاتها تتطلب إجراءات خاصة للتحقيق وكشف الجناة.

ج - تسجيل الأصوات

يقصد بتسجيل الأصوات مراقبة الأحاديث وكل الاتصالات سواءا السلكية أو اللاسلكية وتسجيلها باستخدام أجهزة إلكترونية.

حيث يتم تسجيل الأصوات بوضع أجهزة تنصت في أماكن خاصة أو عمومية و إخفاؤها لتلقي الأحاديث و تسجيلها، و ذلك لإعادة سماعها عندما تستدعي الحاجة، فتسجيل الأصوات يكون عبر مسافات بعيدة دون الحاجة إلى البقاء قريبا من المكان المراد تسجيله⁸⁰، و من أمثلة عن ذلك التجسس عبر الهواتف المحمولة باستخدام تقنية البلوتوث التي يطلق عليها تسمية السن الأزرق (Bluetooth) و التي تسمح بالنقاط التسجيلات و المحادثات الواردة من هاتف شخص آخر ضمن نطاق مسافة محددة.

كما توجد منظومة تدعى (Schwarz identity) طورتها شركة ألمانية، تعمل على تحويل الإشارات الصادرة عن الهواتف إلى كلمات مسموعة، ولم تقتصر أنشطة الشركة على ذلك، بل مكنت التقنية أيضا من تحديد مواقع المستخدمين، وطورت جهازا إلكترونيا يستخدم الميكروفون المدمج في الهاتف المحمول لتسجيل جميع الأصوات، ويشترط لهذا الإجراء الحصول على إذن مسبق من السلطة المختصة.

ثانيا - حفظ المعطيات المتعلقة بحركة السير

هي تلك البيانات الناتجة عن الاتصالات الإلكترونية و التي تشكل عنصرا أساسيا في سلسلة الإتصال، يعني قيام مزودي خدمات الإتصال بجمع معلومات رقمية التي تتيح التعرف على مستخدمي الخدمة، ثم حفظها و تخزينها في أرشيف منظم و الاحتفاظ بها لاستخدامها لاحقا، قصد تمكين جهات التحقيق للاستفادة منها و استعمالها في التحقيق⁸¹، حيث تتضمن هذه

⁸⁰ وعلى جمال، حقوق المشتبه فيه عند إجراء البحث والتحري الخاصة، مجلة الدراسات الحقوقية، جامعة الدكتور طاهر مولاي، سعيدة، الجزائر، العدد 3، 2015، ص 77.

⁸¹ رشيدة بوكري، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري، الطبعة الأولى منشورات الحلبي الحقوقية، بيروت لبنان، 2012، ص 448.

البيانات مصدر الإتصال، و الوجهة المرسل إليها، المسار المتخذ أثناء الإتصال، ووقت الإتصال و مدة استمراره، حجم البيانات المتداولة و نوع الخدمة المستخدمة، عنوان (IP) المستخدم في الإتصال، رقم الهاتف أو البريد الإلكتروني المستخدم⁸².

يساعد هذا الإجراء أجهزة الأمن والقضاء من جمع الأدلة وذلك بتحديد هوية الجاني بحيث يمكن للسلطات تتبع عنوان (IP) من خلال تحليل الرسائل والاتصالات، وبهذا يعتبر دليل رقمي قضائي يستخدم كحجة أمام القضاء ولكن بشرط يكون بإذن من القانون.

المبحث الثاني: تنظيم المسؤولية الجنائية وفق بعض التشريعات العربية وآليات مكافحة هذه الجرائم

مع التوسع الكبير في استخدام تكنولوجيا المعلومات والاتصالات، ظهرت جرائم سيبرانية تسمى بالجرائم الإلكترونية، والتي باتت تشكل تهديدا حقيقيا للأفراد والمجتمع بسبب الأضرار النفسية والمادية التي تسببها، لذا برزت الحاجة إلى وضع أطر قانونية تحدد المسؤولية الجنائية عن الأفعال غير المشروعة التي ترتكب عبر الفضاء الرقمي بحكم طبيعتها العابرة للحدود.

وفي هذا السياق تتفاوت التشريعات العربية في معالجتها، حيث سعى كل من المشرع الجزائري، والمشرع المصري، والأردني، والسعودي، والإماراتي، إلى مواكبة التطورات التقنية عبر إصدار قوانين خاصة لمكافحة جرائم تقنية المعلومات أو تعديل قوانين العقوبات، وإدراكا لخطورة هذه الظاهرة، سعى المشرع الجزائري إلى ضبطها قانونيا، من خلال تضمينها في قانون العقوبات وقانون الوقاية من جرائم تكنولوجيا المعلومات والإتصال، وذلك لمكافحتها ومواجهة هذا النوع من الجرائم الخطيرة، لذا تم تفعيل آليات عقابية مقررة للمجرمين بهدف ردع الجناة وحماية الضحايا، كما هناك آليات مؤسسية متخصصة تعمل على ملاحقة الجناة ونشر الوعي المجتمعي.

وعليه سيتم تقسيم هذا المبحث إلى مطلبين، الأول يتناول المقارنة بين التشريع الجزائري والتشريعات العربية بما فيه التشريع المصري، الأردنني السعودي، أما الثاني يتناول الآليات العقابية والمؤسسية لمكافحة هذه الجريمة.

⁸²المادة 12 فقرة ه القانون 09-04: " يتعين على مقدمي خدمات الأنترنت ما يلي:

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

ب- وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.

المطلب الأول: أوجه التشابه والاختلاف بين القانون الجزائري والتشريعات العربية

تعد الجريمة الإلكترونية من أبر التحديات المعاصرة التي تواجه المشرع في ظل الثورة الرقمية، مما يستوجب تضافر الجهود الدولية والعربية لمواجهتها، وفي هذا السياق يندرج القانون الجزائري ضمن النموذج القانوني العربي في التصدي لهذه الظاهرة، حيث يشترك ويختلف مع التشريعات العربية في مجموعة من المبادئ العامة والأهداف المتعلقة بتقنية المعلومات.

حيث سنتناول في هذا المطلب أوجه التشابه والاختلاف بين القانون الجزائري والتشريعات العربية في الجريمة الإلكترونية، سنخصص الفرع الأول إلى تحديد أوجه التشابه بينهما، أما الفرع الثاني إلى تحديد أوجه الاختلاف بينهما.

الفرع الأول: أوجه التشابه بين القانون الجزائري والتشريعات العربية للجريمة الإلكترونية

سنتطرق في هذا الفرع إلى أوجه التشابه بين القانون الجزائري والتشريعات العربية للجريمة الإلكترونية، وذلك حسب ما يلي:

أولاً: اعتماد تعريف موضوعي للجريمة

اتفقت مع القوانين العربية والجزائرية على تعريف الجريمة الإلكترونية بأنها " فعل غير مشروع يتم باستخدام وسائل تقنية المعلومات أو يستهدف أنظمة المعالجة الآلية للمعطيات، حيث ركزت الجزائر على " المساس بأنظمة المعالجة الآلية للمعطيات "، وتبنت التشريعات العربية منها مصر والإمارات تعريفات مشابهة تشمل الجرائم الموجهة ضد الأنظمة أو التي تسهل ارتكابها.

ثانياً: استحداث قواعد إجرائية خاصة

اتفقت التشريعات العربية والتشريع الجزائري على ضرورة منح الضبطية القضائية صلاحيات خاصة وأساليب تحقيق جديدة، نظراً لصعوبة إثبات الجرائم الإلكترونية كالتفتيش الإلكتروني للنظام المعلوماتي وحجز البيانات والدعائم الإلكترونية الكمبيوتر الهاتف، وإنشاء أجهزة متخصصة مثل شرطة الجرائم الإلكترونية.

ثالثاً: التعاون الدولي والإقليمي

التزمت التشريعات العربية ككل مثل باقي الدول العربية على المصادقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، مما يوحد المفاهيم الإجرائية للتعاون وتسليم المجرمين،

حيث تستخدم معظم القوانين بما فيها الجزائر مصطلحات مثل " جرائم تقنية المعلومات "، أو " المساس بأنظمة المعالجة الآلية ".

الفرع الثاني: أوجه الاختلاف بين القانون الجزائري والتشريعات العربية للجريمة الإلكترونية

سنتطرق في هذا الفرع إلى أوجه الاختلاف بين القانون الجزائري والتشريعات العربية للجريمة الإلكترونية، وذلك حسب ما يلي:

أولاً: من ناحية المصطلحات المستعملة

هنالك اختلاف في الكلمات المفتاحية للنصوص القانونية الجزائرية التي تجرم هذه الجريمة، خاصة فيما يتعلق بمعالجة الأنظمة الآلية للمعطيات، إذ تخلو النصوص من شرح المصطلحات التي تدل على تحقق الركن المادي للجريمة الإلكترونية، مما يؤدي أي وجود إشكالات ونقص في بيان أساليب ارتكابها، حيث جاءت في المادة 394 مكرر 2 عبارات عامة وغامضة كالبحث، التصميم، توفير، تجميع، مما يصعب تصور وقوع الجريمة بناء على هذه الألفاظ.

على غرار باقي التشريعات العربية الأخرى من بجها التشريع الإماراتي الذي خصص مادة كاملة لتعريف المصطلحات المستعملة بشأن مكافحة جرائم تقنية المعلومات، كالبرنامج المعلوماتي، نظام المعلومات الإلكتروني، المستند الإلكتروني، العنوان البروتوكولي، كما أن المشرع المغربي لجأ في صياغة نصوصه المتعلقة بالأنظمة الآلية للمعطيات إلى استخدام عبارات تقنية صعبة الفهم، وغلب على أسلوبه التعقيد في معظم المواد⁸³.

ثانياً: من ناحية التجريم

تتباين النصوص القانونية بين التشريعات المقارنة من حيث إدراج بعض صور الجرائم أو إغفالها، فالمشرع المغربي على سبيل المثال لم يستثن أفعال البقاء داخل نظام المعالجة الآلية للمعطيات، حتى ولو كان الدخول إليه بطريق الخطأ كما أضاف جريمة عرقلة سير نظام المعالجة الآلية للمعطيات، وهي جريمة لا وجود لها في قانون العقوبات الجزائري، كما استعمل المشرع المغربي لفظ "الاحتتيال" بدلا من الغش⁸⁴، عكس المشرع الجزائري الذي استعمل لفظ "غش" في المادة 394 مكرر 1 من قانون العقوبات.

⁸³ياسين بن عمر، المعالجة القانونية للجرائم الإلكترونية في القانون الجزائري والتشريعات المقارنة (التشريع المغربي والإماراتي نموذجا)، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 03، 2019، ص 716-717.

⁸⁴ياسين بن عمر، مرجع سابق، ص 715.

كما نلاحظ أن المشرع الجزائري لم يوسع نطاق تجريم الصور التقليدية للجرائم التي ترتكب بواسطة النظام المعلوماتي، بل اقتصر على الجرائم التي تمس الأنظمة المعلوماتية في ذاتها، أي أن محل الجريمة هو النظام المعلوماتي نفسه، وهذا يؤدي إلى عدم انطباق بعض النصوص التقليدية على الجرائم الإلكترونية الحديثة كجريمة التزوير الإلكتروني⁸⁵.

ثالثا: من ناحية توقيع العقاب

يختلف القانون الجزائري مع التشريعات العربية في توقيع العقاب و تشديده على المجرمين، حيث تميز التشريع الجزائري بتشديد العقوبات المالية مقارنة بالحبس، إذ تصل الغرامة إلى 2.000.000 دج، في جرائم إدخال أو تعديل أو إزالة معطيات عن طريق الغش طبقا للمادة 394 مكرر 1 من قانون العقوبات، و تصل الغرامة حداها الأقصى إلى 5.000.000 دج في الجرائم التي تناولتها المادة 394 مكرر 2، و رفع المشرع الجزائري من عقوبة الحبس في حالة واحدة، و هي الجرائم المتعلقة بتقديم المساعدة لارتكاب أفعال إرهابية طبقا للمادة 87 مكرر 11 و 12 من قانون العقوبات⁸⁶، بينما المشرع الإماراتي كان أكثر تشديدا للعقوبة في حالة تعلق الأمر بالمساس بأمن الدولة و النظام العام، حيث قد تصل العقوبة إلى السجن المؤبد و ذلك في حالة محاولة تغيير نظام الحكم بأي وسيلة إلكترونية مستعملة، كما اعتبر المشرع الإماراتي استخدام وسيلة تقنية معلوماتية، أو شبكة معلومات أو نظام معلوماتي إلكتروني في حد ذاته ظرف تشديد، إذا كان بغرض استخدام جرائم أخرى غير منصوص عليها في قانون مكافحة جرائم تقنية المعلومات كما نص على تدابير احترازية ضد المحكوم عليه بوضعه تحت المراقبة أو الحرمان من استخدام أي شبكة معلوماتية⁸⁷، في حين أن المشرع الجزائري حصر حالة اللجوء إلى نصوص عقابية أشد، إذا تعلق الأمر باستهداف جريمة الدفاع الوطني، أو الهيئات و المؤسسات.

وبالتالي يمكن القول إن المشرع الجزائري اعتمد على مضاعفة الغرامات المالية على الجسدية، بينما المشرع الإماراتي قد شدد العقوبات في الجرائم الإلكترونية لتشمل الجانب المالي والجسدي.

المطلب الثاني: الآليات العقابية والمؤسسية لمكافحة الجرائم الإلكترونية

⁸⁵آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، ط 2، 2007، ص 137.

⁸⁶المادتين 87 مكرر 11 و 12 من القانون رقم 16-02 المؤرخ في 19 يونيو 2016 المتمم للأمر 66-156 المتضمن قانون العقوبات

الجزائري، العدد 37، بتاريخ 22 يونيو 2016.

⁸⁷ياسين بن عمر، مرجع سابق، ص 716-717.

أصبحت الجرائم الإلكترونية من أخطر الجرائم المستحدثة في العصر الرقمي نظرا للتطور المتسارع في الإتصال و التكنولوجيا، مما يسهل الوصول إلى البيانات الشخصية من خلال الدخول إلى النظام المعلوماتي و تهديد الضحية بنشر معلوماته أو صور خاصة به، و لمكافحة هذا النوع من الجرائم تتم تفعيل آليات عقابية و مؤسساتية، حيث تتمثل الآليات العقابية في المنظومة القانونية التي تحدد الأفعال المجرمة و العقوبات المقررة لها، بهدف ردع الجناة و حماية الضحايا، في حين تتجلى الآليات المؤسساتية في دور الهيئات الأمنية، القضائية و المؤسسات المتخصصة مثل الأفريل و اليوروبول و الأوروجيست كوحدات إقليمية لمكافحة هذه الجريمة.

وعليه قسمنا هذا المطلب إلى فرعين، الأول يتناول الآليات العقابية لمكافحة الجرائم الإلكترونية، أما الثاني تناولنا فيها الآليات المؤسساتية لمكافحة الجرائم الإلكترونية.

الفرع الأول: الآليات العقابية لمكافحة الجرائم الإلكترونية

سنتطرق في هذا الفرع إلى العقوبات الأصلية والتكميلية للجريمة الإلكترونية، وذلك حسب ما يلي:

أولاً: العقوبات الأصلية

هي العقوبات الأساسية المقررة للجريمة التي تفرض مباشرة على الجاني، حيث أقرها المشرع الجزائري في إطار قانون العقوبات، والمتمثلة فيما يلي:

حيث نصت المادة 394 مكرر من قانون العقوبات الجزائري المعدل والمتمم بموجب القانون رقم 06-24 على أنه: " يعاقب بالحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 60.000 دج إلى 200.000 دج، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة، تكون العقوبة الحبس من سنة (1) إلى ثلاث (3) سنوات والغرامة من 100.000 دج إلى 300.000 دج⁸⁸.

⁸⁸المادة 394 مكرر من القانون رقم 06-24 المعدل والمتمم من قانون العقوبات الجزائري.

كما تنص المادة 394 مكرر 1 على أنه: " يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها "89.

وبالتالي تشمل هذه المواد العقوبات المقررة للجرائم الإلكترونية في صورتها البسيطة وفي صورتها المشددة، والمتمثلة في الحبس والغرامات المالية، حيث أن جريمة الدخول أو البقاء غير المشروع إلى المنظومة المعلوماتية في صورتها البسيطة لا تؤدي إلى حدوث أضرار تلحق بالمعطيات، أما في صورتها المشددة تكون عمدية وذلك من خلال حذف أو تغيير في المعطيات أو تخريب.

ثانيا: العقوبات التكميلية

يقصد بالعقوبات التكميلية تلك العقوبة التي تضاف إلى العقوبة الأصلية بناء على تقدير القاضي، والهادفة إلى تعزيز الردع.

حيث نصت المادة 394 مكرر 6 من قانون العقوبات على الجرائم الإلكترونية بأنه: " مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكيها "90.

وعليه تتمثل العقوبات التكميلية لهذه الجريمة في:

أ - المصادرة

عرفتها المادة 15 من قانون العقوبات الجزائري بأنها: " الأيلولة النهائية إلى الدولة لمال أو مجموعة أموال معينة أو ما يعادل قيمتها عند الاقتضاء "91.

حيث نصت المادة 13 من نظام مكافحة جرائم المعلوماتية على أنه:

" يجوز الحكم بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في أي من الجرائم المنصوص عليها في هذا النظام، أو الأموال المحصلة منها كما يكون الحكم بإغلاق الموقع الإلكتروني أو مكان تقديم الخدمة إغلاقا نهائيا أو مؤقتا، متى كان مصدرا لارتكاب هذه الجرائم وكانت الجريمة

⁸⁹المادة 394 مكرر 1، مرجع سابق.

⁹⁰المادة 394 مكرر 6 من القانون رقم 04-15 من قانون العقوبات الجزائري.

⁹¹المادة 15 من القانون رقم 24-06 المعدل والمتمم من قانون العقوبات الجزائري.

قد ارتكبت بعلم مالكة⁹²، واستنادا للمادة 394 مكرر 6 يجب لتطبيق إجراء المصادرة في الجرائم الإلكترونية توافر الشروط التالية:

- أن يحكم على المتهم بعقوبة أصلية عن إحدى الجرائم الإلكترونية الواردة في القسم الخاص بالاعتداء على أنظمة المعالجة الآلية للمعطيات.
- أن تكون الأموال أو الأشياء المراد مصادرتها قد استخدمت في ارتكاب الجريمة الإلكترونية.
- ألا تخل المصادرة بحقوق الغير حسن النية، إذا كانت الوسيلة المستخدمة في الجريمة لشخص آخر غير المتهم، لكن بشرط عدم علم هذا الغير حسن النية بأن هذه الوسائل استخدمت في ارتكاب جريمة.

و مما سبق نستنتج أن المصادرة هي نقل ملكية المال إلى الدولة بصورة نهائية، و نلاحظ أن الفرق بين المصادرة والغرامة المالية يكمن في أن هذه الأخيرة هي عقوبة مالية نقدية أصلية، بينما المصادرة عقوبة عينية تكميلية، ولا تطبق إلا على الأشياء التي تكون حيازتها مشروعة وذات صلة بالجريمة، حيث حددت المادة 13 من نظام مكافحة الجرائم المعلوماتية السعودي هذه الصلة بقولها: " الأجهزة والبرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام "، وإذا لم تكن الأشياء التي تم استخدامها في الجريمة ليست ملكا للجاني فلا يحكم القاضي بمصادرتها وذلك كما نصت عليه المادة 13 بقولها " مع عدم الإخلال بحقوق الغير حسن النية".

ب - الغلق

يعتبر الغلق من العقوبات التكميلية إلى جانب المصادرة، حيث نصت عليه المادة 394 مكرر من قانون العقوبات الجزائري، تشمل عقوبة الغلق في مجال الجرائم الإلكترونية:

- غلق المواقع الإلكترونية التي كانت محلا للجريمة.
- غلق المحل أو مكان الاستغلال إذا ارتكبت الجريمة بعلم من مالك المحل.
- كما نصت المادة 16 مكرر 1 من قانون العقوبات الجزائري على أنه: " يترتب على عقوبة غلق المؤسسة منع المحكوم عليه من أن يمارس فيها النشاط الذي ارتكبت الجريمة بمناسبته، ويحكم بهذه العقوبة إما بصفة نهائية أو لمدة لا تزيد عن عشر (10) سنوات في حالة الإدانة لارتكاب جنائية، وخمس (5) سنوات في حالة الإدانة لارتكاب جنحة

⁹²المادة 13 من نظام مكافحة الجرائم المعلوماتية.

ويجوز أن يأمر بالنفاذ المعجل بالنسبة لهذا الإجراء⁹³.

فالمقصود بالمواقع التي تكون محل الغلق هي التي نفذت فيها الجريمة، بالدخول الغير المشروع إلى الأنظمة والتلاعب بالمعطيات، أما المواقع التي تعرضت للاعتداء عبر هذه الجرائم تعتبر ضحية ولا يصح غلقها، حيث لم يحدد المشرع المدة الزمنية للغلق سواء للمحلات أو المواقع الإلكترونية، مما يعني أن الغلق قد يكون مؤقتا أو دائما حسب تقدير القاضي.

الفرع الثاني: الآليات المؤسسية لمكافحة الجرائم الإلكترونية

سنتطرق في هذا الفرع إلى المؤسسات والآليات الإقليمية لمكافحة الجريمة الإلكترونية، الأفربول واليوروبول والأوروجيست، وذلك حسب ما يلي:

أولا: الأفربول وكالة إقليمية لمكافحة الجرائم الإلكترونية

أنشأت منظمة الأفربول (Afrapol) كآلية إقليمية تهدف إلى تعزيز التعاون الشرطي بين الدول الإفريقية على المستويات الاستراتيجية والعمليات والتقنية، لمكافحة الجرائم العابرة للحدود خاصة الجرائم الإلكترونية، وذلك من خلال التنسيق مع المؤسسات الشرطية الوطنية والإقليمية والدولية⁹⁴.

و قد جاءت فكرة إنشاء هذه المنظمة إثر الندوة الإفريقية الثانية و العشرون للأنتربول بمشاركة ممثلي الدول الإفريقية لإنشاء بهدف وضع آلية للتعاون المشترك، و تمت الموافقة على فكرة إنشاء الأفربول خلال اجتماع مدراء ووكلاء الشرطة العاملين في الجزائر، كما تم بعد ذلك إقرار القوانين المنظمة للأفربول من قبل الدول و الحكومات الإفريقية خلال القمة العادية الثانية و العشرون (22) للإتحاد الإفريقي التي انعقدت بالعاصمة الإثيوبية أديس أبابا خلال شهر جانفي سنة 2017، و بموجب المادة 2 من النظام الأساسي لآلية الإتحاد الإفريقي للتعاون الشرطي، يعتبر الأفربول مؤسسة تقنية،و آلية للتعاون الشرطي بين دول الإتحاد الإفريقي حيث يقوم على جملة من المبادئ الأساسية منها، احترام مبادئ الديمقراطية و حقوق الإنسان، و تعزيز أخلاقيات المهنة الشرطية⁹⁵.

⁹³المادة 16 مكرر 1 من القانون رقم 06-23 من قانون العقوبات الجزائري.

⁹⁴براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص قانون عام، قسم الحقوق، كلية الحقوق والعلوم الإنسانية، جامعة مولود معمري، تيزي وزو، الجزائر، 2018، ص 308.

⁹⁵جوزي صليحة، الجزائر تحتضن الجمعية العامة الأولى لآلية الإتحاد الإفريقي للتعاون في مجال الشرطة "الأفربول"، مجلة الشرطة، وحدة الطباعة الروبية، الجزائر، العدد 136، 2017، ص 9.

تقوم منظمة الأفرربول بدور مهم في مكافحة الجريمة الإلكترونية، من خلال عدة آليات أبرزها:

- دعم التحقيقات المشتركة بين الدول، خاصة في هذه الجرائم الأكثر خطورة وتعقيدا في كشف الجناة وذلك لتفكيك الشبكة الإجرامية واعتقال أعضائها.
- تبادل المعلومات والأدلة الرقمية بين أجهزة الشرطة حول شبكات الجرائم الإلكترونية العابرة للحدود.
- تنظيم دورات تدريبية لضبط الشرطة وتطوير قدراتها في إكتشاف المجرمين الإلكترونيين وملاحقتهم.

ومما سبق نستنتج أن الأفرربول لها أهمية كبيرة في مكافحة الجرائم الإلكترونية من خلال قدرتها على التنسيق الإقليمي وتقديم الدعم الفني وتبادل المعلومات، ومع تزايد هذه الجرائم أصبح تعزيز دور الأفرربول أكثر ضرورة في وقت الحالي نظرا لانتشارها وخطورتها.

ثانيا: اليوروبول وكالة إقليمية لمكافحة الجرائم الإلكترونية

يعد اليوروبول (Europol) وكالة إقليمية تركز على تعزيز التعاون بين دول الإتحاد الأوروبي و ذلك لتصدي الجرائم الخطيرة العابرة للحدود، و بخصوص الجرائم الإلكترونية يقوم اليوروبول بدور محوري لمواجهة من خلال المركز الأوروبي لمكافحة الجرائم الإلكترونية (EC3)، حيث ساهم هذا المركز إسهاما كبيرا في الجهود التي تبذلها الدول الأعضاء لحماية المواطنين و الشركات و الحكومات الأوروبية من هذه الجريمة، مما يسهل اعتقال الجناة إضافة إلى قيامه بتحليل مئات الآلاف من الملفات التي تكون في معظمها خبيثة أو محملة بفيروسات إلكترونية⁹⁶.

ومن بين أبرز الاختصاصات التي يضطلع بها اليوروبول في مجال مكافحة الجرائم الإلكترونية ما يلي:

- مساندة التحقيقات التي تجريها السلطات المختصة في الدول الأعضاء.
- تجميع وتحليل المعلومات الاستخباراتية المتعلقة بالجرائم السيبرانية.

⁹⁶ شنتير خضرة، مرجع سابق، ص 263.

- تنسيق الجهود بين الدول الأوروبية لتفكيك الشبكات المسؤولة عن هذه الجرائم، ومثال عن ذلك في حالات برامج الفدية (Ransomware) تلعب اليوروبول دورا حاسما في تتبع المجرمين، وتفكيك البنية التحتية الرقمية التي يستخدمونها، وتنسيق عمليات الاعتقال عبر الحدود.

ثالثا: الأوروبيست وكالة إقليمية لمكافحة الجرائم الإلكترونية

تمثل وكالة الأوروبيست (Eurojust) أحد الأعمدة الرئيسية في نظام العدالة الجنائية التابعة للإتحاد الأوروبي، إذ تهدف إلى تعزيز التنسيق القضائي والتعاون بين الدول الأعضاء في التصدي للجرائم الجنائية المعقدة، وعلى رأسها الجرائم الإلكترونية التي تعد من أخطر صور الجريمة السيبرانية، حيث تتمثل أهمية الأوروبيست كون هذه الجرائم عابرة للحدود، تتوزع عناصرها بين دول متعددة سواء من حيث الجناة أو البنية الرقمية أو الضحايا، وتقوم الأوروبيست بمهمة محورية تشمل:

- تسهيل التعاون القضائي العابر للحدود.

- التنسيق بين النيابة العامة وأجهزة التحقيق الأوروبية.

- إنشاء ودعم فرق التحقيق المشتركة.

و إلى جانب ذلك تقدم الأوروبيست في حدود صلاحياتها، آراء فنية لليوروبول بعد دراسة التحليلات التي ينجزها، سواء بمبادرة منها أو بطلب من مكتب المدعي العام الأوروبي، فالأوروبيست منذ تأسيسها أدت دورا بارزا في التصدي لهذه الجرائم، و باستعراض هذه المهام الذي تلعبه هذه الوكالة في مكافحتها للجريمة الإلكترونية على الصعيد الأوروبي⁹⁷.

⁹⁷ شنتير خضرة، مرجع سابق، ص 267.

ملخص الفصل الثاني:

تعتبر الجرائم الإلكترونية من أخطر الجرائم السيبرانية التي تهدد أمن وسلامة الأفراد والمجتمع، حيث يجب توفر ثلاثة أركان لقيام هذه الجريمة، الركن الشرعي، المادي والمعنوي، وذلك لتوقيع العقاب على المجرمين وعدم إفلاتهم، وللكشف عن هذه الجريمة لا بد من اللجوء إلى إجراءات تحقيقية عامة وخاصة، من بينها الخبرة والتفتيش والمعاينة، كذلك المراقبة الإلكترونية واعتراض المراسلات والنقاط الصور وذلك بهدف الحصول على دليل جنائي رقمي، ولمكافحة هذه الجريمة الإلكترونية وتجريمها وضع المشرع الجزائري وبعض التشريعات العربية آليات عقابية جزائية أصلية وتكميلية للحد منها، وأخرى مؤسساتية تعاونية لمكافحتها والقضاء عليها.

الخاتمة

تعد الجريمة الإلكترونية من أبرز التهديدات الرقمية التي تواجه المجتمعات في عصرنا الحالي، حيث يتضح من خلال تحليل هذه الجريمة انها لا تقتصر على الاختراق الأمني، بل تمثل اعتداء على كرامة الضحايا واستقرارهم المالي والاجتماعي، و أن المسؤولية الجنائية لهذه الجرائم تقوم على أساس حرية الاختيار و التمييز و العلم و الإرادة وقت دخوله للنظام المعلوماتي و اختراقه أو تغيير معلومات، مما يستوجب مواجهة شاملة و متكاملة للحد من هذه الظاهرة، وعلى الرغم من التقدم الكبير في مجال الأمن السيبراني و التشريعات الرقمية، لازالت الجرائم الإلكترونية متفشية بسبب التقنيات التي يستخدمها المجرمون، وعدم وجود تعاون دولي فعال في جميع الحالات، ومع ذلك فإن الأمل قائم في الحد من هذه الجريمة من خلال تعزيز التعاون الدولي بين الحكومات والمنظمات الأمنية لمطاردة المجرمين عبر الحدود، وتطوير أنظمة الذكاء الاصطناعي للكشف المبكر عن هذه الجرائم قبل تفاقمها، و لضمان حماية عالمية فعالة للبرامج و أنظمة المعالجة الآلية للمعطيات و الشبكات ككل، و ذلك لزيادة الوعي في المجتمع، بتحديث القوانين باستمرار لمواكبة الأساليب الإجرامية الجديدة، وبهذا فإن مكافحة الجرائم السيبرانية الرقمية ليست مسؤولية الأجهزة الأمنية وحدها، بل هي مسؤولية مشتركة بين الحكومات والمؤسسات التقنية، من خلال العمل الجماعي بنشر الوعي المستمر لبناء فضاء رقمي آمن يحترم فيه خصوصية الأفراد وتضمن حقوقهم.

النتائج:

من خلال الدراسة المتعمقة للمسؤولية الجنائية عن الجرائم الإلكترونية، يمكن واستخلاص النتائج التالية:

- تعتمد الجريمة الإلكترونية على استخدام التكنولوجيا الحديثة وشبكات الأنترنت، كفضاء رقمي للجريمة.

- تقوم المسؤولية الجنائية في هذه الجرائم على أساس حرية الاختيار، ومناطقها التمييز والعلم والإرادة وقت ارتكاب الفعل المجرم، بالدخول بدون إذن إلى النظام المعلوماتي وتخريبه أو حذف المعلومات أو تغييرها.

- اختلاف الجريمة الإلكترونية عن الجريمة التقليدية بكون الأولى تتم في بيئة رقمية كاستعمال الحاسوب والأنترنت، في الإعتداء على حرمة الحياة الخاصة للأفراد، وذلك بالدخول إلى البرامج أو الأنظمة المعلوماتية واختراقها، أما الثانية تقع في العالم المادي يكون فيه مسرح للجريمة باستخدام وسائل تقليدية.

- صعوبة إثبات الجرائم الإلكترونية بسبب طبيعة الأدلة الرقمية الهشة، والحاجة إلى خبراء متخصصين.

- تعد هذه الجريمة من الجرائم العابرة للحدود حيث يمكن للمجرم أن يعمل في دولة والضحية في أخرى مما يعقد عملية الملاحقة القضائية.

- وجود اختلاف بين القانون الجزائري وبعض التشريعات العربية في مجال تشديد العقوبة في هذه الجريمة.

- إنشاء آليات مؤسسية لمكافحة الجرائم الإلكترونية، مثل الأفريبول واليوروبول والأوروجيست، وذلك للحد من هذه الجريمة.

المقترحات:

- تحديث التشريعات باستمرار عبر سن قوانين خاصة بالجرائم الإلكترونية تتضمن عقوبات رادعة.

- ضرورة إبرام اتفاقيات عربية ودولية لتعزيز التعاون الدولي في مجال مكافحة الجرائم المعلوماتية، وذلك لتسليم المجرمين وعدم إفلاتهم من العقاب.

- إلزام الشركات بتطبيق معايير أمنية عالية لحماية البيانات والأجهزة والبرامج.
- ضرورة تعديل بعض التشريعات الجزائية الحالية بما يتلائم مع طبيعة جرائم الأنترنت.
- ضرورة نشر الوعي الرقمي بين المستخدمين لتفادي التعدي على بياناتهم الشخصية.
- إنشاء مرصد وطني لرصد ومتابعة جرائم الإلكترونيّة، وذلك بتطوير برامج تدريبية متخصصة للكوادر الأمنية والقضائية.

قائمة المصادر والمراجع

Les références

قائمة المصادر والمراجع:

المصادر:

أولاً: النصوص القانونية

• الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق ل 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية الجزائي، المعدل والمتمم، المنشور في الجريدة، العدد 48.

• القانون رقم 14-01 المؤرخ في 04 فبراير 2014، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 08 يونيو 1966، المتضمن تعديل قانون العقوبات، ج، ر، ج، ج، الصادر في 16 فبراير 2014، العدد 07.

• قانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 هـ الموافق ل 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47، الصادر بتاريخ 25 شعبان عام 1430 هـ، الموافق ل 16 غشت سنة 2009.

• قانون رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436 هـ الموافق ل 01 فبراير سنة 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

• قانون رقم 06-23 المؤرخ في 29 ذي القعدة عام 1427 هـ الموافق ل 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 156-66 المؤرخ في 18 صفر عام 1386 الموافق ل 8 يونيو 1966 المتضمن قانون العقوبات الجزائي، الجريدة الرسمية، العدد 87، الصادرة بتاريخ 04 ذي الحجة عام 1427 هـ الموافق ل 24 ديسمبر سنة 2006.

• قانون رقم 06-24 المؤرخ في 19 شوال عام 1445 هـ الموافق ل 28 أبريل سنة 2024 المعدل والمتمم المتضمن قانون العقوبات الجزائي، الجريدة الرسمية، العدد 30.

المراجع:

أولاً: الكتب

• أسامة أبو الحجاج، دليلك الشخصي إلى الأنترنت، دار النهضة العربية، القاهرة، 1998.

• المعجم الوجيز، مجمع اللغة العربية، طبعة خاصة بوزارة التربية والتعليم، 1993.

• حسني محمود نجيب، شرح قانون العقوبات، القسم العام، دار النهضة العربية، 1998.

- حسين بن سعيد بن سيف الغافري، الجهود الدولية في مكافحة جرائم الأنترنت، القاهرة، دار النهضة العربية، 2009.
- حسين طاهري، الجرائم الإلكترونية، دار الخلدونية، الطبعة الأولى، الجزائر، 2022.
- حمد فتحي سرور، الوسيط في شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، الطبعة السابعة، 1996.
- زيدان عبد الكريم، الوجيز في أصول الفقه، مؤسسة الرسالة، بيروت، طبعة 7، 1997.
- سلامة مأمون، شرح قانون العقوبات، القسم العام، دار الفكر العرب، الأردن، 2009.
- شنتير خضرة، الآليات القانونية لمكافحة الجريمة الإلكترونية، دراسة مقارنة، 2022.
- عبد الفتاح مراد، شرح جرائم الكمبيوتر والانترنت، دار الكتب والوثائق المصرية، القاهرة، مصر.
- عبد الكريم خالد الردايدة، الجرائم المستحدثة واستراتيجية مواجهتها، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، 2013.
- على شملال، المستحدث في قانون الإجراءات الجزائية الجزائري، ط 2، دار هومه للطباعة والنشر والتوزيع، الجزائر، 2020.
- عوض محمد، قانون العقوبات القسم العام، دار المطبوعات الجامعية، طبعة 1، مصر، 1969.
- فرج رضا، شرح قانون العقوبات الجزائري القسم العام، الطبعة الثانية، الشركة الوطنية للنشر والتوزيع، الجزائر، 1976.
- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت، دار النهضة العربية، القاهرة، مصر، 2009.
- محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الأمني، وزارة داخلية، الأكاديمية الملكية للشرطة، مملكة البحرين، 2010.
- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، لبنان، الطبعة الأولى، 2005.
- نمديلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، المؤتمر الدولي الرابع عشر، طرابلس، 2017.

• نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة 2، دار الثقافة للنشر والتوزيع، الأردن، 2010.

• يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، في ضوء الاتفاقيات العربية لمكافحة جرائم تقنية المعلومات، قانون العقوبات، ق إ ج، قوانين خاصة، دار الجامعة الجديدة، الإسكندرية، 2019.

ثانيا: المقالات العلمية

• أرشد بشير إبراهيم، التحقيق الجنائي في جرائم تقنية المعلومات، بحث منشور في مجلة دراسات استراتيجية، مركز الإمارات للدراسات والبحوث الاستراتيجية، العدد 131، 2008.

• باقر غازي حنون، حسان حماد حميد، جريمة الابتزاز الإلكتروني، دراسة مقارنة، مجلة دراسات البصرة، العدد 42، سنة 2016.

• د. بوضياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، جامعة محمد بوضياف، المسيلة، 2018.

• د. مخلد إبراهيم الزعبي، فاعلية القوانين والتشريعات العربية في مكافحة الجرائم الإلكترونية، المجلة العربية للنشر العلمي، العدد 37، 2021.

• رحموني محمد، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، جامعة أحمد دراية، أدرار، العدد 41، سنة 2018.

• رستم هشام، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، مجلة الأمن والقانون، دبي، الإمارات العربية المتحدة، العدد 02، 1999.

• سليم حميداني وعباسي سهام، اختراق الخصوصية في العالم الرقمي، حدود الظاهرة ومطالب الحماية القانونية، مجلة البحوث في الحقوق والعلوم السياسية، جامعة ابن خلدون تيارت، المجلد 04، العدد 02، 2019.

• ط.د. برمضان الطيب، المسؤولية الجنائية في الفقه الإسلامي والقانون الجزائري، مجلة المعيار، جامعة ال جزائر 1، المجلد 12، العدد 01، 2021.

• عشاش حمزة، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، العدد 02، المجلد 06، جامعة محمد بوضياف، المسيلة، 2020.

• مشري راضية، الجريمة الإلكترونية دلالة المفهوم وفعالية المعالجة، مجلة أبحاث قانونية وسياسية، جامعة 8 ماي 1945، قالمة، المجلد 6، العدد 1، سنة 2021.

• مهداوي حنان، التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري، مجلة الفكر القانوني والسياسي، كلية الحقوق والعلوم السياسية، جامعة محمد أمين دباغين سطيف 2، المجلد 6، العدد 2، 2022.

• وعلي جمال، حقوق المشتبه فيه عند إجراء البحث والتحري الخاصة، مجلة الدراسات الحقوقية، جامعة الدكتور طاهر مولاي، سعيدة، الجزائر، العدد 3، 2015.

• جوزي صليحة، الجزائر تحتضن الجمعية العامة الأولى لآلية الاتحاد الإفريقي للتعاون في مجال الشرطة " الأفيبول"، مجلة الشرطة، وحدة الطباعة الروبية، الجزائر، العدد 136، 2017.

• ياسين بن عمر، المعالجة القانونية للجرائم الإلكترونية في القانون الجزائري والتشريعات المقارنة (التشريع المغربي والإماراتي نموذجا)، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 03، 2019.

ثالثا: الأطروحات والمذكرات الجامعية:

أطروحات دكتوراه:

• براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص قانون عام، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزوو، الجزائر، 2018.

• عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2004.

رسائل الماجستير والماستر:

• أمينة بوشعرة، سهام موساوي، الإطار القانوني للجريمة الإلكترونية، مذكرة تخرج لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة بجاية، 2018.

• بوحيه وسيلة، المسؤولية الجنائية الدولية عن الجرائم ضد الإنسانية، مذكرة ماجستير تخصص القانون الجنائي الدولي، جامعة سعد دحلب، البليدة، 2016.

- سفيان سوير، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلوم الإجرام، كلية الحقوق، جامعة أوبكر بلقايد تلمسان، الجزائر، 2011.
- عبد العزيز زعبار، أساس المسؤولية الجنائية وفق التشريع الجزائري، كذكره مقدمة لاستكمال نيل شهادة الماستر، كلية الحقوق، تخصص القانون الجنائي والعلوم الجنائية، جامعة غرداية، سنة 2024.
- قارة آمال، الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق، جامعة الجزائر، 2001.
- يوسف خليل يوسف العفيفي، الجرائم الإلكترونية في التشريع الفلسطيني " دراسة تحليلية مقارنة"، رسالة لنيل شهادة الماجستير في القانون العام، كلية الشريعة والقانون " الجامعة الإسلامية"، غزة، 2013.

فهرس المحتويات

الفهرس

i.....	شكر واهداء
1.....	المقدمة
5.....	الفصل الأول: الاطار الموضوعي للمسؤولية الجنائية عن الجرائم الالكترونية
6.....	تمهيد:
7.....	المبحث الأول :ماهية الجريمة الالكترونية و المسؤولية الجنائية
7.....	المطلب الاول: مفهوم الجريمة الالكترونية و خصائصها و تمييزها عن الجرائم التقليدية
7.....	الفرع الأول : تعريف الجريمة الالكترونية
13.....	الفرع الثاني :التمييز بين الجريمة الالكترونية و الجريمة التقليدية
14.....	المطلب الثاني: مفهوم المسؤولية الجنائية و شروط قيامها
14.....	الفرع الأول : تعريف المسؤولية الجنائية
16.....	الفرع الثاني: الشروط العامة للمسؤولية الجنائية وخصوصية قيامها
19.....	المبحث الثاني: الاطار التشريعي للجرائم الالكترونية في الجزائر
19.....	المطلب الأول: الجريمة الالكترونية في التشريع الجزائري
20.....	الفرع الأول : الطبيعة القانونية للجريمة الالكترونية
23.....	الفرع الثاني:موقف المشرع الجزائري من الجريمة الالكترونية
26.....	المطلب الثاني :أنواع الجرائم الالكترونية
26.....	الفرع الاول:الجرائم الواقعة بواسطة النظام المعلوماتي
27.....	الفرع الثاني: الجرائم الواقعة على النظام المعلوماتي
30.....	ملخص الفصل الاول:

الفصل الثاني: الاطار الاجرائي للمسؤولية الجنائية عن الجرائم الالكترونية وفق القانون الجزائري	
وبعض التشريعات العربية.....	31
تمهيد:.....	32
المبحث الاول: تنظيم المسؤولية الجنائية وفق القانون الجزائري وبعض التشريعات العربية.....	33
المطلب الاول: تنظيم المسؤولية الجنائية وفق القانون الجزائري اركان الجريمة الالكترونية	33
الفرع الاول: الركن الشرعي.....	33
الفرع الثاني: الركن المادي و الركن المعنوي.....	34
المطلب الثاني: تنظيم المسؤولية الجنائية وفق بعض التشريعات العربية.....	37
الفرع الاول: تنظيم المسؤولية الجنائية إجراءات التحقيق العامة للجريمة الالكترونية	37
الفرع الثاني: إجراءات التحقيق الخاصة للجريمة الالكترونية	42
المبحث الثاني: المقارنة بين التشريع الجزائري وبعض التشريعات العربية واليات مكافحة هذه الجرائم.....	45
المطلب الاول: أوجه التشابه و الاختلاف بين القانون الجزائري وبعض التشريعات العربية للجريمة الالكترونية.....	46
الفرع الاول: أوجه التشابه بين القانون الجزائري وبعض التشريعات العربية.....	46
الفرع الثاني: أوجه الاختلاف بين القانون الجزائري وبعض التشريعات العربية.....	47
المطلب الثاني: الاليات العقابية و المؤسساتية لمكافحة الجرائم الالكترونية	49
الفرع الاول:الاليات العقابية لمكافحة الجرائم الالكترونية	49
الفرع الثاني: الاليات المؤسساتية لمكافحة الجرائم الالكترونية	52

55.....	ملخص الفصل الثاني:
56.....	الخاتمة.
60.....	المصادر والمراجع.
66.....	الفهرس.