



الجرائم الإلكترونية وسبل مكافحتها في ظل التشريع الليبي

أفراح سالم عمر الدغري

الأكاديمية الليبية للدراسات العليا . جنزور - ليبيا

abrahymalharthaltweel@gmail.com

Cybercrimes and ways to combat them under Libyan legislation

Afrah Salem Omar Al-Daghri

Libyan Academy for Graduate Studies, Janzour, Libya

تاريخ الاستلام: 2026/6/29 تاريخ المراجعة: 2026/7/20 تاريخ القبول: 2026/7/28- تاريخ النشر: 2026/8/25

الملخص

شهد العالم خلال العقود الأخيرة تطوراً متسارعاً في مجال تكنولوجيا المعلومات والاتصالات ، وأصبح استخدام الحاسب الآلي وشبكة المعلومات الدولية جزءاً أساسياً من مختلف مجالات الحياة ، رغم الإيجابيات التي يوفرها النظام المعلوماتي في كل الميادين إلا أنه لا يخلو من بعض المخاطر ؛ لأن المعلومة باعتبارها علماً لمعالجة المعطيات آلياً أصبحت تثير عدة مشكلات من الناحية القانونية ، وأصبحت تمس العديد من المصالح والحقوق من بينها البيانات والمعلومات الخصوصية والأموال والأنظمة المعلوماتية ، الأمر الذي فرض على المشرع ضرورة وضع قواعد قانونية تتلائم مع طبيعة الجرائم توفر الحماية الجنائية اللازمة للمجتمع .

الكلمات المفتاحية : الجرائم الإلكترونية ، الحماية الجنائية ، التشريع الليبي

Abstract

Over recent decades ,the world has witnessed rapid developments in the field of information and communications technology (ICT) .the use of computers and the international information network (the internet) has become an essential part of various aspects of life .

Despite the advantages provided by information systems in all fields, they are not without certain risks.

Information, regarded as a science for the automated processing of data, has raised several legal problems and affected numerous interests and rights, including private data, confidential information, financial assets, and cyber systems.

Consequently, this has necessitated the legislator to establish legal rules tailored to the nature of cybercrimes, providing the required criminal protection for society.

Keywords: Cybercrimes, criminal protection, Libyan Legislation.

المقدمة :

تعاني المجتمعات الإلكترونية في الآونة الأخيرة من انتهاك للحقوق والخصوصيات الإلكترونية ، وهو ما يعرف بالجرائم الإلكترونية ، وتتميز هذه الأخيرة عن الجرائم التقليدية بخصوصية وسائل ارتكابها ، وسرعة انتشارها واتساع نطاق آثارها ، وقد أصبحت هذه الجرائم اليوم تهدد العديد من المصالح والحقوق ، كالأموال والبيانات والمعلومات الخاصة ، وأمام تزايد هذه الجرائم أصبح من الضروري وجود حماية قانونية فعالة تتلاءم مع طبيعتها وتطور وسائل ارتكابها¹.

ويهدف هذا البحث إلى التعرف على ماهية الجرائم الإلكترونية وأبرز صورها ، ثم الوقوف على سبل الحماية منها في التشريع الليبي ولا سيما في ضوء القانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية ، وبيان مدى كفاية الحماية في مواجهة التطورات المتسارعة في هذا المجال ، وفي نطاق المقدمة لابد أن نمر على بعض مفرداتها الضرورية ، وكما يلي :

¹ آمال قارة ، الحماية الجزائية للمعلومات في التشريع الجزائري ، دار هومة للنشر والتوزيع ، الجزائر ، ط2 ، 2007 ، ص 6 .

أولاً / أهمية البحث : للبحث أهمية علمية وعملية ، فالأولى تتمثل في إثراء الدراسات القانونية المتعلقة بالجرائم الإلكترونية وبيان خصوصية هذه الجرائم ، وما تثيره من إشكالات قانونية .

أما الثانية فتتمثل في بيان مدى فاعلية الحماية التي يوفرها التشريع الليبي لمواجهة الجرائم الإلكترونية ، والمساهمة في تحديد أوجه القصور واقتراح سبل يمكن أن تسهم في تعزيز الحماية الجنائية .

ثانياً / إشكالية البحث : تتمثل إشكالية البحث في التساؤل الرئيسي الآتي :

إلى مدى نجاح التشريع الليبي في توفير الحماية الجنائية اللازمة لمواجهة الجرائم الإلكترونية والحد من مخاطرها ؟
ويتفرع عن هذه التساؤل الرئيسي مجموعة من الأسئلة :

- ماهي الجريمة الإلكترونية ؟ وما هي أهم خصائصها ؟

- ما أبرز صور الجرائم الإلكترونية ؟

- ماهي الطبيعة القانونية للجرائم الإلكترونية ؟

- ما أوجه الحماية الجنائية التي قررها المشرع الليبي لمواجهة الجرائم الإلكترونية ؟

- هل جاءت نصوص هذا القانون ملائمة للواقع ؟ أو هل أحاط المشرع الليبي بكل أنماط الجرائم الإلكترونية ؟

- هل بالإمكان تطبيق جمع أدلة الإثبات التقليدية على الجرائم الإلكترونية ومدى كفايتها ؟

ثالثاً / أهداف البحث : يسعى البحث إلى تحقيق الأهداف الآتية :

1- بيان مفهوم الجرائم الإلكترونية وخصائصها .

2- التعرف على أبرز صور الجرائم الإلكترونية .

3- بيان موقف التشريع الليبي من الجرائم الإلكترونية .

4- توضيح صور الحماية الجنائية التي قررها التشريع الليبي .

رابعاً / نطاق البحث : يقتصر نطاق البحث على دراسة ماهية الجرائم الإلكترونية من حيث معرفة مفهومها وخصائصها وأهمية وصور الجرائم الإلكترونية ، وأيضاً سبل الحماية من الجرائم الإلكترونية في ظل التشريع الليبي

خامساً / منهجية البحث : اعتمد هذا البحث على المنهج الوصفي التحليلي ؛ وذلك من خلال وصف ظاهرة الجرائم الإلكترونية وبيان مفهومها وخصائصها وصورها ، ثم تحليل النصوص القانونية الواردة في التشريع الليبي وبصفه خاصة القانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية .

سادساً / خطة البحث : تم الاعتماد على الخطة الثنائية ، وسيكون من مطلبين رئيسيين وكل مطلب ينقسم إلى فرعين وهما كالآتي :

المطلب الأول / ماهية الجرائم الإلكترونية.

الفرع الأول / مفهوم وخصائص الجرائم الإلكترونية.

الفرع الثاني/ صور الجرائم الإلكترونية وطبيعتها القانونية .

المطلب الثاني/ سبل الحماية الجنائية من الجرائم الإلكترونية في ظل التشريع الليبي.

الفرع الأول / سياسة التجريم والعقاب في مواجهة الجرائم الإلكترونية.

الفرع الثاني / سياسة الحماية الإجرائية للجرائم الإلكترونية

المطلب الأول / ماهية الجرائم الإلكترونية

تعد الجرائم الإلكترونية من جرائم المستحدثة التي بدأت في الانتشار بشكل واسع في الآونة الأخيرة ، فلا يوجد مصطلح قانوني موحد للدلالة على هذه الجرائم ، وعليه سنتناول مفهوم الجرائم الإلكترونية في **الفرع الأول** ، وخصائصها في **الفرع الثاني** .

الفرع الأول / مفهوم الجرائم الإلكترونية وخصائصها .

أولاً / مفهوم الجرائم الإلكترونية

لا يوجد اجماع موحد على تعريف الجريمة الإلكترونية ، فهي تختلف باختلاف العلماء وتخصصاتهم فتظهر بمسميات عدة ، فالبعض يطلق عليها الغش المعلوماتي ، والبعض الآخر يطلق عليها جريمة الاختلاس المعلوماتي أو الإحتيال المعلوماتي ، وآخرون يفضلون تسميتها الجرائم الإلكترونية أو المعلوماتية¹ .

فالتطور التكنولوجي المتسارع ترافقه تكيفات للجريمة وبروز أشكال أخرى جديدة ومعقدة في المجتمع الرقمي حسب الوسيلة المستخدمة والهدف من ارتكابها ، وهناك عدة تعريفات يمكن تقديمها كالآتي :

¹ أسامه أحمد المناعسة ، جلال محمد الزعبي ، جرائم تقنية نظم المعلومات الإلكترونية ، دراسة مقارنة ، ط2 ، دار الثقافة للنشر والتوزيع ، عمان ، الأردن ، 2014 ، ص 86،87 .

فعرها البعض بأن الجرائم الإلكترونية " كل فعل مؤذ باستخدام الحاسب الآلي أو الشبكة المعلوماتية"¹ . كما عرفها آخرون بأنها " كل فعل غير مشروع ناجم عن سوء استغلال المعرفة بتقنية المعلومات بصفة أساسية لدى مرتكبه ، أو الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الهاتف الجوال "² . أيضاً هي " كل سلوك إجرامي يتم بمساعدة الكمبيوتر "³ .

نلاحظ من التعريفات السابقة أنها تركز على مرتكب الجريمة من خلال صفاته التي تمكنه من ممارسة هذا النوع من الجريمة ، كالكفاءة التقنية والقدرة على التحكم فيها واستخدامها في هذا الاتجاه.

والجريمة في البيئة الافتراضية هي كل المخالفات المرتكبة ضد الأفراد أو الجماعات بقصد إيذاء السمعة أو إلحاق الأذى المادي أو المعنوي باستخدام شبكة الإنترنت ، وتندرج تحت هذا المسمى كل الأعمال ذات الصلة بالحاسوب لأغراض شخصية أو لتحقيق مكاسب مالية أو إلحاق الضرر ، كالجرائم المتصلة بالهوية ، وانتهاك حقوق الملكية الفكرية للمعلومات أو الإضرار بمحتويات الأجهزة أو إتلافها⁴ .

وعلى ذلك فقد عرفها المشرع الليبي في المادة الأولى من قانون رقم 5 لسنة 2022م بشأن مكافحة الجرائم الإلكترونية بأنها " كل فعل يرتكب من خلال استخدام أنظمة الحاسب الآلي أو شبكة المعلومات الدولية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون "⁵ .

وعلى الرغم من غياب تعريف موحد في أغلب القوانين الوطنية، إلا أن بعض الاتفاقيات الدولية والإقليمية سعت إلى تقديم تعريفات محددة لهذا النوع من الجرائم، وذلك لأغراض التنسيق القانوني والتعاون القضائي بين الدول. ومن أبرز هذه المبادرات :

اتفاقية مجلس أوروبا حول الجريمة الإلكترونية (بودابست) ، التي تُعد أول صك دولي ملزم يسعى إلى توحيد المفاهيم والإجراءات في هذا المجال. وقد عرفت الجرائم الإلكترونية على أنها " الأفعال التي تستهدف أو تُرتكب بواسطة أنظمة الحاسوب، أو التي يُستخدم فيها الحاسوب كأداة لارتكاب الجريمة"⁶ .

وقد جاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين بأنها " أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية ، أو داخل نظام حاسوبي ، التي يمكن ارتكابها في بيئة الكترونية "⁷ .

وقد عرفت أيضاً منظمة التعاون الاقتصادي والتنمية التابعة للأمم المتحدة ، الجريمة الإلكترونية " بأنها كل فعل أو إمتناع من شأنه الإعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية الإلكترونية "⁸ .

وفي مشروع اتفاقية الاتحاد الإفريقي للأمن السيبراني وحماية البيانات ذات الطابع الشخصي ، لم تتضمن تعريفا للجرائم الإلكترونية لعدم وجود تعريفا جامعاً مانعاً لهذه الجرائم ولكنها اكتفت بتحديد الجرائم ضد تكنولوجيا المعلومات والاتصالات.⁽⁹⁾

ويلاحظ أن هذه الاتفاقيات وإن اختلفت في الصياغة فإنها تشترك في جوهر المفهوم وهو اعتبار الجريمة الإلكترونية بأنها كل فعل غير مشروع يُرتكب باستخدام نظام معلوماتي أو شبكة إلكترونية، ويهدف إلى المساس بسرية أو سلامة أو توافر البيانات أو الأنظمة أو الخدمات الرقمية".

ثانياً / خصائص الجرائم الإلكترونية

¹ لورنس سعيد أحمد الحوامدة ، الجرائم المعلوماتية " أركانها وآلية مكافحتها " ، دراسة تحليلية مقارنة ، مجلة الميزان للدراسات الإسلامية والقانونية ، المجلد الرابع ، العدد الأول ، جامعة العلوم الإسلامية العالمية ، الأردن ، 2017 ، ص 107 .

² مختارية بوزيدي ، ماهية الجرائم الإلكترونية ، بحث مقدم ضمن أعمال الملتقى الوطني ، آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري ، مركز جيل البحث العلمي ، الجزائر ، 29_مارس_2017 ، ص 9 .

³ محمود إبراهيم غازي ، الحماية الجنائية للخصوصية والتجارة الإلكترونية ، مكتبة الوفاء القانونية ، الإسكندرية ، ط1 ، 2014 ، ص118 .

⁴ ذياب موسى البداينة ، الجرائم الإلكترونية ، المفهوم والأسباب - ورقة علمية مقدمة إلى الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحوليات الإقليمية والدولية ، عمان ، الأردن ، من 2 إلى 4 سبتمبر ، 2014 ، ص 3،4 .

⁵ انظر الجريدة الرسمية، قانون رقم 5 لسنة 2022م بشأن مكافحة الجرائم الإلكترونية، العدد 1 السنة الأولى 2023.

⁶ انظر مجلس أوروبا، مجموعة المعاهدات الأوروبية، الاتفاقية المتعلقة بالجرائم الإلكترونية، رقم 185، 2001م.

⁷ الأمم المتحدة ، الجرائم المتعلقة بشبكات الحاسوب ، المؤتمر 10 للأمم المتحدة لمنع الجريمة ومعاقبة المجرمين ، فيينا ، 10-17-أبريل ، 2000 ، الوثيقة رقم (A/CONF.187/01) .

⁸ منظمة التعاون الاقتصادي والتنمية (OECD) ، الجريمة المرتبطة بالحاسوب ، تحليل السياسة القانونية ، باريس ، 1986 ، ص 4 .

⁹ انظر اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية (2024م). منشور على الموقع الإلكتروني:

<https://ccdcoe.org/uploads/2018/11/AU-270614-CSConvention.pdf>

نظراً لإرتباط الجريمة الإلكترونية بجهاز الحاسوب وشبكة الإنترنت بصفة عامة ، ووسائل التواصل بصفة خاصة ، فإن هناك مجموعة من الخصائص المميزة لهذه الجرائم تميزها عن خصائص الجرائم التقليدية ، ومن هذه الخصائص ما يلي :

1-جريمة عابرة للحدود : أن الجرائم الإلكترونية ربما ترتكب عن طريق حاسب آلي في دولة في حين تتحقق النتيجة الإجرامية في دولة أخرى ¹ ، وهنا تميزت بالتباعد الجغرافي بين الفاعل والمجني عليه ، وبين الوجهة التقنية الحاسب كأداة الجريمة ، وبين المعطيات أو البيانات محل الجريمة في نظام الحاسب المستهدف بالإعتداء ² .

وهنا تظهر الحاجة لوجود تنظيم قانوني دولي وداخلي متلائم معه لمكافحة مثل هذا النوع من الجرائم وضبط فاعليها ، وحيث أن التشريعات الداخلية متفاوتة فيما بين كل دولة من دول العالم ، تظهر العديد من المشاكل حول صاحب الاختصاص القضائي لهذه الجريمة وإشكالات أخرى متعلقة بإجراءات الملاحقة القضائية ، وتتشابه الجرائم الإلكترونية في هذه الخاصية مع بعض الجرائم مثل جرائم غسيل الأموال ، وجرائم المخدرات ³ .

2-جريمة صعبة الإثبات والاكتشاف : تكمن صعوبة إثبات مثل هذه الجريمة أنها لا تترك في الغالب أثراً مادياً ظاهرياً يمكن ضبطه فيصعب اكتشافها ، فكل ما يحدث فيها هو مجرد تحرك وانتقال لذنبات ونبضات إلكترونية من خلال استخدام النظم المعلوماتية وشبكة الإتصال ⁴ .

والوسيلة المستخدمة لإرتكاب الجريمة هي نبضة إلكترونية ينتهي دورها خلال أقل من ثانية واحدة ، وكأن الجاني يقوم بتدمير الدليل بمجرد استعماله ويقوم بذلك بكل هدوء ودون إحداث أية ضجة ، وذلك على خلاف الكثير من الجرائم التي نعرف .

3- صعوبة الكشف والتتبع : تُعدّ الجرائم الإلكترونية من الجرائم التي تنسم في الغالب بالخفاء والاستتار ، إذ إنّ الضحية قد لا يدرك وقوعها رغم حدوثها أثناء وجوده على الشبكة ، نظراً لما يتمتع به مرتكبوها من قدرات تقنية عالية تمكّنهم من تنفيذ أفعالهم الإجرامية بدقة ومهارة . وتشمل هذه الأفعال ، على سبيل المثال ، إرسال الفيروسات الخبيثة ، وسرقة الأموال أو البيانات الشخصية ، أو إتلافها ، والتجسس الإلكتروني ، والتنصّت على المكالمات ، وغيرها من الجرائم ذات الطبيعة الرقمية .

وبناءً على ذلك ، فإن هذه الجرائم نادراً ما تخلف أثراً مادية واضحة يمكن الاستدلال بها بعد ارتكابها ، كما أنّ الاحتفاظ الفني بالأدلة الرقمية – إن وجدت – يُعدّ أمراً بالغ الصعوبة نظراً لطبيعتها الزائلة وسرعة محوها أو تعديلها . وهذا ما يجعل مهمة المحقق التقليدي في التعامل مع هذا النوع من الجرائم معقدة ومحدودة الجدوى ، إذ تتطلب هذه الوقائع وسائل فنية متقدمة وتقنيات تحقيق رقمية متخصصة تعتمد على التحليل الإلكتروني وتنسم بقدر عالٍ من الترميز والتضليل في تتبّع الجناة وتحديد هويتهم .

وعليه ، فإن مواجهة الجرائم الإلكترونية وإثباتها تستلزم خبرة تقنية عالية المستوى ، وفتحاً فنية متخصصة قادرة على تحليل الأدلة الرقمية وجمعها وفقاً للمعايير القانونية والفنية المعترف بها .

4- خصوصية مجرم المعلومات : قد لا تتأثر الجرائم التقليدية بالمستوى العلمي للمجرم كقاعدة عامة ، ولكن الأمر مختلف تماماً بالنسبة للمجرم المعلوماتي والذي يكون عادة من ذوي الاختصاص والمعرفة في مجال تقنية المعلومات ، وقد تم تصنيف مجرمي الجرائم الإلكترونية إلى المخترقين ، والمحترفين ، والهاكرز .

المخترقون : مثل الهاكرز الذي يعد شخصاً بارعاً في استخدام الحاسب الآلي ولديه فضول في استخدام حسابات الآخرين بطرق غير مشروعة ، الأمر الذي يدل على أنهم أشخاص متطفلون وغير مرحب بهم لدى الغير ، وغالباً تكون أعمارهم في سن المراهقة ⁵ .

أما المحترفون : وهم الأكثر خطورة بين مجرمي الإنترنت ، حيث يهدف البعض منهم إلى الإعتداء لتحقيق الكسب غير المشروع المتمثل في الناحية المادية وذلك عبر الدخول في حسابات البنوك ، والبعض الآخر يدخل من أجل تحقيق أغراض سياسية والتعبير عن وجهة نظره أو فكرة ، وغالباً أعمار هؤلاء تكون بين 25 و40 سنة ⁶ .

¹ محمد محمود الشركسي ، الجريمة الإلكترونية وسبل مكافحتها في ضوء أحكام الفقه الإسلامي ، دراسة مقارنة ، مجلة المنارة العلمية ، العدد الثاني ، مايو ، 2021 ، ص 184 .

² محمد علي سويلم ، جرائم الكمبيوتر والإنترنت - دراسة مقارنة ، دار المطبوعات الجامعية ، الإسكندرية ، ط1 ، 2019 ، ص 69 .

³ مصعب القطاونه ، الإجراءات الجنائية الخاصة في الجرائم المعلوماتية ، بحث مقدم لشبكة قانوني ، الأردن ، 2010 ، ص 5 .

⁴ أيمن عبدالله فكري ، الجرائم المعلوماتية ، دراسة مقارنة في التشريعات العربية والأجنبية ، مكتبة القانون والإقتصاد ، الرياض ، ط1 ، 2014 ، ص 106 .

⁵ نانلة عادل ، جرائم الحاسب الآلي الاقتصادية ، منشورات العلى الحقوقية ، بيروت ، ط1 ، 2012 ، ص 178 .

⁶ خالد ممنوح إبراهيم ، الجرائم المعلوماتية ، دار الفكر الجامعي ، الإسكندرية ، ط1 ، 2009 ، ص 78 .

الحاقدون : وهم الذين ليس لديهم أي أهداف للجريمة ولا يسعون لمكاسب سياسية أو مادية ، ولكن يتحركون لرغبة في الانتقام والتأثر كالأمر الطائفية .

5- الطابع غير المادي (اللامادي) للجريمة : تتميز الجرائم الإلكترونية عن الجرائم التقليدية من حيث طبيعة الوسائل والجهد المبذول في ارتكابها؛ فإذا كانت الجريمة التقليدية تتطلب جهداً مادياً أو عضلياً مباشراً كما هو الحال في جرائم القتل أو السرقة أو الاعتداء، فإن الجريمة الإلكترونية لا تحتاج إلى مثل هذا الجهد، إذ تقوم أساساً على النشاط الذهني والفكري المعتمد على المعرفة التقنية والدراسة العلمية المتخصصة في مجال الحاسوب وتقنيات المعلومات. ويعود ذلك إلى أن هذا النوع من الجرائم يتمثل في التلاعب بالمعطيات والبيانات الإلكترونية من خلال تغييرها أو تعديلها أو محوها من السجلات المخزنة في ذاكرة أنظمة الحاسبات أو شبكات المعلومات. ومع ذلك، فقد ذهب بعض الباحثين والجهات الأمنية – ومن أبرزها مكتب التحقيقات الفيدرالي الأمريكي – (FBI) إلى تشبيه الجرائم الإلكترونية بجرائم العنف، وذلك لتشابه الدوافع النفسية والسلوكية لدى مرتكبيها مع دوافع الجناة في جرائم الاعتداء المادي، من حيث الرغبة في السيطرة، وإثبات الذات، وإلحاق الضرر بالآخرين، وإن اختلفت الوسائل والنتائج بينهما.

الفرع الثاني / صور الجرائم الإلكترونية وطبيعتها القانونية

سنتناول في هذا الفرع صور الجرائم الإلكترونية أولاً ، والطبيعة القانونية للجرائم الإلكترونية ثانياً .

أولاً / صور الجرائم الإلكترونية : للجرائم الإلكترونية صور عديدة ولهذا سنتطرق لبعض من الصور وهي كالاتي :

1- جريمة الابتزاز الإلكتروني : غالبية التشريعات لم تضع مصطلح للابتزاز الإلكتروني حيث انقسم الفقه حول تعريفه إلى اتجاهين ضيق وواسع، **الاتجاه الضيق عرفه** على أنه " توصل الجاني إلى الاستحواذ على بيانات ومعلومات شخصية تخص المجني عليه ثم تهديده بكشفها أو نشرها إذا لم يقيم الأخير بالقيام بعمل ما أو الامتناع عنه أو أداء مبالغ مالية للجاني " ، كما يعرف وفقاً للأنصار ذات الاتجاه الضيق على أنه أحد الطرق التي يمارسها الجاني على المجني عليه وذلك من خلال تهديده بفضح أو نشر معلومات أو بيانات أو صور شخصية تخصه إن امتنع عن تنفيذ أغراضه المادية أو المعنوية¹.

ويتضح مما سبق أن الاتجاه الضيق في تعريف جريمة الابتزاز الإلكتروني يركز على مضمون الابتزاز الإلكتروني والغرض منه والذي يتخذ غالب صورة التهديد بنشر المعلومات أو الصور أو الفيديوهات أو بيانات تم الحصول عليها من خلال وسائل الاتصال الإلكترونية وتهديد المجني عليه بنشرها، إذا لم يقوم بدفع مبالغ مالية أو القيام بعمل معين أو الامتناع عن عمل يحدده الجاني².

أما **الاتجاه الموسع فعرفه** على نحو أكثر اتساعاً عن التعريف السابق ووفقاً لهذا الاتجاه فإن " الابتزاز الإلكتروني يتحقق من خلال قيام الجاني باستخدام الوسائط الإلكترونية والتوصل من خلالها لمعلومات وبيانات وصور سرية تخص المجني عليه ثم تهديده بنشرها لاستيلاء على مبالغ مالية أو دفع المجني عليه لأداء عمل غير مشروع " ³، كما عرّف على أنه كل تهديد يرتكبه الجاني بنفسه أو من خلال وسيط عبر إحدى الوسائل الإلكترونية ضد المجني عليه على نحو يؤثر في نفسيته أو شخص عزيز لديه مما يحمله على القيام بما يكلفه به الجاني من أفعال مشروعة أو غير مشروعة .

وبمطالعة التشريع الليبي المتعلق بقانون رقم 5 لسنة 2022م يتبين أن المشرع الليبي لم يتناول جريمة الابتزاز من ضمن الجرائم المعاقب عليها في إطار هذا القانون .

2- الاحتيال عبر الوسائط الإلكترونية : يقصد بالاحتيال الإلكتروني استخدام الوسائل التقنية أو الشبكات المعلوماتية في ارتكاب سلوك احتيالي بقصد الإستلاء على مال الغير ، وذلك من خلال إيهام المجني عليه أو تضليله بوسائل إلكترونية ، كاستخدام مواقع أو حسابات وهمية أو رسائل إلكترونية أو انتحال هوية رقمية ، بما يؤدي إلى تسليمه ماله أو تمكين الجاني من الحصول عليه دون وجه حق ، وتظل الجريمة في جوهرها قائمة على فكرة الاحتيال التقليدي إلا أن الوسيلة المستخدمة في تنفيذها تكون إلكترونية⁴.

¹ عبدالرحمن بن عبدالله المسند ، جريمة الابتزاز ، مطبوعات الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر ، ط1 ، الرياض ، 2018 ، ص 15 .

² سامي مرزوق نجاء المطيري ، المسؤولية الجنائية عن الابتزاز الإلكتروني في النظام السعودي ، رسالة ماجستير ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، 2015 ، ص 27 .

³ ممدوح رشيد مشرف الرشيد العنزي ، الحماية الجنائية للمجني عليه من الابتزاز ، المجلة العربية للدراسات الأمنية ، المجلد 33 ، العدد 70 ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، 2017 ، ص 199 .

⁴ خليل سعيد خليل عبيه ، القالب التشريعي لجرائم انتحال الصفة والشخصية الإلكتروني ، دراسة مقارنة ، مجلة العلوم الإنسانية والإدارية ، العدد 22 ، مارس ، 2021 ، ص 87 .

ويقع هذا النوع من الجرائم عند إدخال بيانات أو تعديلها أو حذفها في نظام معلوماتي بقصد الخداع ، بهدف الحصول على مكاسب مالية غير مشروعة أو الإضرار بحقوق الآخرين .

وتتضمن المادة 8 من اتفاقية بودابست حكماً خاصاً يُجرّم هذا الفعل¹ ، مُشيرةً إلى تزايد مخاطره مع توسّع المعاملات الإلكترونية وبطاقات الدفع.. ولا ارتكاب هذه الجريمة، يجب توافر القصد الجنائي في شكلين : القصد العام وهو التلاعب بجهاز الكمبيوتر بطريقة تُلحق الضرر بالآخرين، والقصد الخاص وهو نية الجاني تحقيق منفعة اقتصادية لنفسه أو للآخرين ويغطي النص جميع أشكال الأفعال التي قد تؤثر على وظائف الحاسوب ، سواءً أكانت تتعلق بإدخال أو إتلاف أو حذف أو طمس ، إذ إنها تمثل اعتداءً مباشراً على سلامة نظام المعلومات وأدائه لوظائفه المختلفة.

ويشير الإتلاف هنا إلى حذف أو إفساد البيانات أو البرامج بطريقة تجعلها غير صالحة للاستخدام ، مما يؤدي إلى تعطيل نظام المعلومات وإضعاف وظائفه ، سواءً من خلال مكونات مادية أو غير مادية.

وتُجرّم المادة 9 من الاتفاقية الأفعال المتعلقة بالمحتوى الإباحي ، وخاصةً **استغلال الأطفال** ، من خلال تجريم إنتاج أو توزيع أو حيازة أو عرض هذه المواد عبر أنظمة الحاسوب. تُعرّف الاتفاقية "القاصر" بأنه أي شخص دون سن الثامنة عشرة ، مع منح الدول الأطراف سلطة تخفيض هذا الحد العمري إلى السادسة عشرة ، وتهدف هذه المادة إلى تعزيز حماية الأطفال من الاستغلال الجنسي عبر وسائل الإعلام ، استجابة للقلق الدولي المتزايد الذي أعرب عنه في القمم الأوروبية وفي بروتوكولات حقوق الطفل .

على الرغم من أهمية هذه المادة ، تُنقّد الاتفاقية لاقتصار الحماية الجنائية على القاصرين فقط ، على عكس بعض التشريعات العربية التي تُوسّع نطاق الحماية لتشمل جميع الأفراد بغض النظر عن سنهم ، مما يوفر حماية أوسع ضد إساءة استخدام أنظمة المعلومات لنشر محتوى غير أخلاقي .

3- سرقة المعلومات والبيانات إلكترونياً : تتمثل هذه الصورة في الاستيلاء على المعلومات أو البيانات المخزنة أو المتداولة في الأنظمة المعلوماتية دون حق ، سواءً كان ذلك عن طريق الدخول غير المشروع إلى النظام أو نسخ البيانات أو نقلها أو الحصول عليها بوسائل تقنية غير مشروعة .

وهذه الصورة مهمة جداً أنها تمثل اعتداءً مباشراً على المعلومات والبيانات ، وهي أبرز المصالح التي أصبحت محل حماية جنائية في البيئة الرقمية² .

تتعدد صور وأشكال تخزين البيانات والمعلومات المعالجة إلكترونياً، فقد تكون تلك البيانات والمعلومات مخزنة على هيئة نبضات كهربائية في دوائر إلكترونية مُجمّعة، أو في وسائط وأوعية معينة - كالبطاقات الورقية المثقبة ، والأشرطة والأقراص المغناطيسية - كما أنها قد تكون في حالة بث وانتقال من نهاية طرفية إلى أخرى ، والتوصل غير المشروع إلى تلك البيانات والمعلومات له في كلّ حالة من حالتها تخزين ، إذا كانت البيانات والمعلومات في حالة انتقال فيما بين النهايات الطرفية ، فإن أساليب التجسس عليها ، والتقاطها تختلف باختلاف الوسيلة الناقلة ، إذا كان نقلها عبر الأسلاك المعدنية ، أو خطوط الهاتف المخصصة لتنظيم الاتصالات الإلكترونية لا يحتاج معترضها لأكثر من مجرد جهاز التقاط بسيط يمكن تركيبه من وحدات إلكترونية تتوافر في الأسواق ، وتنشيطه بطريقة خفية داخل صناديق التوزيع التي تنتهي إليها معظم وسائل الاتصال السلكية واللاسلكية ، وقد يضاف جهاز بث إلى جهاز الالتقاط كي يعمل حسب حال وجود بيانات أو إشارات في السلك أو الخط الذي تجري مراقبته³ .

ومن جرائم التجسس الإلكتروني ذات الصلة في القانون الليبي : التصنّت او اعتراض الاتصالات : يعاقب عليه القانون بالحبس لمدة لا تقل عن 6 أشهر كل موظف عمومي أبلغ عن محادثة هاتفية أو بريدية أو رسالة أخرى، بينما تصل العقوبة إلى السجن إذا ارتكبت من قبل شخص آخر.

التجسس الاقتصادي : يُعاقب عليه بالسجن لمدة لا تقل عن سنة وغرامة مالية تصل إلى 25 ألف دينار، وفقاً للمادة 24 من القانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية.

4- التشهير الإلكتروني : يقصد به استخدام الوسائل الإلكترونية ولا سيما مواقع التواصل الاجتماعي والمواقع الإلكترونية ، لنشر أو تداول عبارات أو صور أو معلومات من شأنه الإساءة إلى سمعة شخص أو الحط من اعتباره أو النيل من شرفه أمام الغير.

¹ انظر اتفاقية بودابست بشأن الجريمة الإلكترونية لسنة 2001 ، المادة 8 ، 9 ، الخاصة بالإحتيال المرتبط بالحاسب ، وانظر كذلك رحاب علي عميش ، الجريمة المعلوماتية ، دراسة مقارنة بين القانون الليبي والإماراتي ، مجلة معهد دبي القضائي ، المجلد الثاني ، العدد الرابع ، يوليو 2-14 ، ص 67،103 .

² أحلام محمود النهوي ، جرائم الحاسب الآلي وسبل مكافحتها ، المجلة الليبية العالمية ، العدد 20 ، 2017 ، ص 10، 17 .

³ د. محمد أمين الشوابكة ، جرائم الحاسوب والإنترنت (الجريمة المعلوماتية) ، دار الثقافة للنشر والتوزيع ، عمان ، 2004 ، ص 112 ، 115 .

وتكمن خصوصية التشهير الإلكتروني في سرعة انتشار المحتوى وإمكانية وصوله إلى عدد كبير من الأشخاص ، فضلاً عن إمكانية نشره وتداوله ، مما قد يؤدي إلى اتساع نطاق الضرر الواقع على المجنى عليه .¹

ثانياً / الطبيعة الجرائم الإلكترونية :

إن دراسة الجرائم بشكل عام والجرائم الإلكترونية بشكل خاص تدخل في دراسة القسم الخاص لقانون العقوبات ، إلا أن الجرائم الإلكترونية تمثل ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي الإلكتروني² ، على اعتبار أن معظم هذا النوع من الجرائم يرتكب ضمن نطاق المعالجة الإلكترونية الجنائية المعلوماتية للبيانات سواء أكان في تجميعها أو في تجهيزها أو في إدخالها إلى الحاسب المرتبط بشبكة المعلومات الدولية ، وكل هذا بغاية الحصول على معلومات معينة .

وأحياناً قد ترتكب الجريمة الإلكترونية في مجال معالجة الكلمات أو معالجة النصوص ، وهذا النوع الأخير من الجرائم لا يعدو أن يكون طريقة أتمتية يمكن المستخدم من تحرير الوثائق والنصوص على الحاسوب مع توفير إمكانية التصحيح والتعديل والمسح والتخزين والاسترجاع والطباعة .

فجميع تلك العمليات هي وثيقة الصلة بالجرائم محل بحثنا ، وعليه لا بد للجاني من استيعابها فضلاً عن أن الجاني قد يتعامل مع مفردات جديدة كالبرامج والمعطيات التي تشكل محل الإعتداء أو تستخدم وسيلة له³.

أن التحري عن النظام القانوني الملائم لطبيعة الجرائم الإلكترونية عبر الشبكة المعلوماتية الدولية ، يهدف بشكل أساسي إلى معرفة ماهية النصوص القانونية الوضعية التي يجب تطبيقها على خدمات نشر المواقع والمعلومات فيها ، فضلاً عن معرفة النظام القانوني للمسؤولية الذي يفترض تطبيقه على الأشخاص المسؤولين عن هذا النشر وخصوصاً لنرجح موقف الدول بهذا الشأن ، من هنا يتضح أن الطبيعة القانونية الخاصة لهذه الجرائم من خلال المجال الذي يمكن أن ترتكب فيه ، ومن جانب آخر المحل الذي يقع عليه الإعتداء المذكور ، فالتطور السريع في مجال المعلوماتية قد يفسح المجال لإقتناء وسائل إلكترونية تمكن المتجاوزين لإستخدامها في ارتكاب جرائم مختلفة ؛ لأن الإجراء الإلكتروني يتعلق بكل سلوك غير مشروع فيما يتعلق بالمعالجة الآلية لبيانات وإدخال المعلومات ونقلها ، ومن ثم يتحتم ضمه إلى نطاق القانون الجنائي على الرغم من أن معظم نصوصه المقارنة عاجزة عن مواكبة التطور المعلوماتي أو لما يحويه من فراغ تشريعي في هذا المجال⁴.

ولهذا يمكن القول أن الجرائم الإلكترونية تتمتع بطبيعة قانونية خاصة ومركبة ، إذ ترتبط من ناحية بالقواعد العامة في قانون العقوبات ، ومن ناحية أخرى تفرض البيئة الرقمية خصائص جديدة على السلوك الإجرامي ووسيلة ارتكابه ومحل الإعتداء ، ولذلك لم يعد من الدقيق النظر إلى الجريمة الإلكترونية باعتبارها مجرد جريمة تقليدية ارتكبت باستخدام الحاسوب أو شبكة الإنترنت ، وإنما أصبحت بعض صورها تمثل أنماطاً إجرامية تستلزم أحكاماً قانونية خاصة تتلائم مع طبيعة البيئة الرقمية ، وتتضح الطبيعة الخاصة للجرائم الإلكترونية في أن الوسيلة الإلكترونية قد تكون مجرد وسيلة لإرتكاب جريمة تقليدية ، كما في حالات النصب أو التهديد أو القذف التي تتم عبر شبكة الإنترنت⁵.

المطلب الثاني/ سبل الحماية الجنائية من الجرائم الإلكترونية في ظل التشريع الليبي

الجرائم الإلكترونية الذي شهدها العالم في النظام المعلوماتي والفضاءات الافتراضية أوجبت على المشرع الليبي إصدار قانون الجرائم الإلكترونية أسوة بغيره ، بقصد مخاطبة الأفراد بالقاعدة القانونية وهنا نقف لنتساءل هل نجح التشريع الليبي في توفير الحماية الجنائية اللازمة لمواجهة الجرائم الإلكترونية والحد من مخاطرها ؟ للإجابة عن هذا التساؤل يتحتم علينا الإشارة إلى سياسة التجريم والعقاب في مواجهة الجرائم الإلكترونية في الفرع الأول ، وسياسة الحماية الإجرائية للجرائم الإلكترونية في الفرع الثاني .

الفرع الأول / سياسة التجريم والعقاب في مواجهة الجرائم الإلكترونية

يعد القانون رقم(5) لسنة 2022م بشأن مكافحة الجرائم الإلكترونية أول قانون ليبي خاص ينظم مكافحة هذا النوع من الجرائم ، وقد عرف المشرع الليبي الجريمة الإلكترونية في المادة الأولى " بأنها كل فعل يرتكب من خلال استخدام

1 أحلام محمود النهوي ، مرجع سبق ذكره ، ص19،18

2 علي محمد سويلم ، مرجع سبق ذكره ، ص 9 .

3 محمد محمود الشركسي ، مرجع سبق ذكره ، ص 185 .

4 محمد محمود الشركسي ، نفس المرجع ، ص 185 .

5 عبدالفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت ، دار الفكر الجامعي ، الإسكندرية ، ط1 ، 2006 ، ص 435 .

أنظمة الحاسب الآلي أو شبكة المعلومات بالمخالفة لأحكام القانون " ¹، ويكشف هذا الاتجاه عن تبني المشرع الليبي سياسة تجريبية خاصة تهدف إلى إخضاع الأفعال التي تمثل اعتداء على الأنظمة المعلوماتية والبيانات والحقوق والمصالح المرتبطة بالبيئة الرقمية لنطاق التجريم والعقاب .

ومن أبرز صور ذلك تجريم الدخول غير المشروع إلى أجهزة الحاسب الآلي أو النظام المعلوماتي أو الشبكة المعلوماتية أو الموقع الإلكتروني ، حيث يتحقق الدخول غير المشروع بالوصول إلى بيانات ومعلومات مخزنة داخل الحاسب الآلي دون رضا المسؤول عنها ²، فأغلب هذه الجرائم تقتضي اقتران فعل الدخول غير المشروع أولاً متى تم ذلك عمداً دون تصريح أو بالمخالفة لحدود التصريح الممنوح ، فضلاً عن تشديد الحماية عندما يقترب الدخول غير المشروع بأفعال من شأنها حذف البيانات أو إضافتها أو إتلافها أو إفشائها أو حجبها أو تعديلها أو نسخها أو تعطيل النظام المعلوماتي ، أو إذا ترتب على الفعل إعاقة عمل النظام أو الشبكة أو الموقع الإلكتروني أو إفسادها ³.

وباستقراء نصوص قانون الجرائم الإلكترونية الليبي نجد أن المشرع قد جرم الدخول غير المشروع في مادته (11) بأنه " يُعد الدخول لأجهزة وأنظمة الحاسب الآلي أو إلى نظام معلوماتي أو شبكة معلوماتية أو موقع إلكتروني غير مشروع إذا تم الاختراق بشكل متعمد لوسائل وإجراءات الحماية لها بشكل كلي أو جزئي دون تصريح..... "ونلاحظ من هذا النص أن المشرع الليبي قد توسع في محل الجريمة الذي من الممكن أن يكون موقع إلكتروني أو نظاماً معلوماتياً أو شبكة معلوماتية وفي نفس الوقت لم يضع تعريفات لهذه المصطلحات في مادته الأولى ، وقد قرر المشرع الليبي لجريمة الدخول للأنظمة المعلوماتية أو شبكة المعلومات في حال اختراق وسائل وإجراءات الحماية بشكل كلي أو جزئي سواء بدون تصريح أو مخالفة لأحكام التصريح " عقوبة الحبس مدة لا تزيد عن سنة أو الغرامة التي لا تقل عن 100 ولا تزيد عن 500 دينار ، أو العقوبتين معاً .

كما اتجه المشرع الليبي إلى تجريم صور متعددة من السلوك الإجرامي الإلكتروني لتشمل مختلف صور الإعتداء التي تقع على البيئة الرقمية ، حيث جاءت في المادة (13) تحت عنوان **الاعتراض أو التعرض** بأنه " يعاقب ...كل من اعترض نظاماً معلوماتياً بقصد الحصول على بيانات رقمية أو للربط مع أنظمة إلكترونية أخرى "، ووضع لها عقوبة الحبس مدة لا تقل عن سنة ، وبغرامة لا تقل عن 1000 دينار ، ولا تزيد عن 5000 دينار .

وأيضاً أن المشرع الليبي لم يكتفِ بنص الاعتراض ، وإنما أفرد نصاً آخر في المادة (47) لجريمة **التنصت** وجاء فيها " يعاقب بالحبس مدة لا تقل عن سنة كل من تنصت لصالح نفسه أو لصالح غيره على الاتصالات التي تجري عبر شبكة المعلومات الدولية أو وسيلة إلكترونية أخرى ، وتكون العقوبة السجن إذا كان التنصت بقصد على أسرار حكومية أو أمنية أو عسكرية أو مصرفية"وشدد العقوبة أكثر إذا كان وراء هذا التنصت نشر الأسرار التي تحصل عليها الجاني بعقوبة السجن المؤبد .

ولم يقتصر المشرع الليبي الحماية على الأنظمة والأجهزة ، وإنما امتدت إلى البيانات والمعلومات والحقوق المرتبطة بها ، كما أحاط بعض الأفعال الإلكترونية الأخرى بالتجريم والعقاب ، بما يحقق حماية لمصالح متعددة في البيئة الرقمية ، كذلك لم يعزل المشرع الجرائم الإلكترونية عن النظام العام للتجريم ، إذ قررت المادة (49) تطبيق أحكام قانون العقوبات والقوانين المكملة له عندما ترتكب الجرائم التقليدية باستخدام الشبكة المعلوماتية أو أي نظام معلوماتي ، وهو ما يؤكد التكامل بين الحماية الخاصة التي قررها قانون مكافحة الجرائم الإلكترونية والحماية العامة المقررة في قانون العقوبات .

الفرع الثاني / سياسة الحماية الإجرائية للجرائم الإلكترونية

إن ظهور جرائم حديثة لم يكن منصوص عليها في قانون العقوبات وعدم إمكانية إخضاعها لها الأمر الذي جعل أغلب المشرعين يتجه للتدخل التشريعي لمعالجة هذه الصورة الحديثة سواء بتعديل نصوص قانون العقوبات أو بإصدار نصوص خاصة تنظم الإجراءات المتبعة في جمع أدلى الجرائم الإلكترونية بما يتوافق وطبيعة هذه الجرائم ، فالجرائم التي ترتب بطرق فنية متطورة قد يكون من الصعب إثباتها بالأدلة التقليدية فهي بحاجة إلى أدلى تتناسب مع طبيعة هذه الجرائم لتتمكن من فحص الأدلة وفك رموزها وتتبعها بطرق فنية ، ورغم أن المشرع لم يحدد الأدلة على سبيل الحصر وإنما أجاز القاضي القيام بأي دليل يراه لازماً لإظهار الحقيقة ، ونظراً لطبيعة الجرائم الإلكترونية والأساليب التي تقوم عليها فإن الأمر يتطلب الاستعانة بإجراءات تتماشى مع طبيعة هذه الجرائم للوصول إلى الدليل بطريق

¹ القانون رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية ، الصادر عن مجلس النواب الليبي ، الجريدة الرسمية ، السنة الأولى ، العدد 1 ، 16 يناير 2023 .

² أسامة بن غانم العبيدي ، جريمة الدخول غير المشروع إلى النظام المعلوماتي " دراسة قانونية في ضوء القوانين المقارنة " ، مجلة دراسات المعلومات العدد 14 ، 2012 ، ص 19 .

³ د. هيفاء عبد العالي فرج ، الحماية الجنائية للمواقع الإلكترونية والأنظمة المعلوماتية للدولة ، دراسة مقارنة ، مجلة العلوم القانونية ، كلية القانون ، جامعة المرقب ، الخمس ، ليبيا ، المجلد 11 ، العدد 2 ، ديسمبر 2023 ، ص 55 .

مشروع ، ولذلك لجأ العديد من المشرعين استحداث طرق إجرائية متطورة للتمكن من تتبع الجناة وعدم إفلاتهم من العقاب وأهم هذه الإجراءات هي : التسرب الإلكتروني ، اعتراض المراسلات ، المراقبة الإلكترونية¹ .

أولاً / التسرب الإلكتروني : اتجه المشرع إلى توفير حماية إجرائية وفنية لمواجهة خصوصية هذه الجرائم ، من خلال الاعتداد بالدليل الجنائي الرقمي وتنظيم بعض المسائل المرتبطة بضبط الجرائم الإلكترونية ، حيث أعطى لبعض الموظفين المختصين صفة مأموري الضبط القضائي لدخول إلى الفضاء الإلكتروني بطريقة خفية منتحلاً اسماً مستعاراً وانضمامه إلى أحد المجموعات المشتبه في ارتكابهم لجناية أو جنحة في الجرائم التي تقع بالمخالفة لأحكام القانون ، وإيهامهم أنه معهم ليكسب ثقتهم ومن ثم التعامل معه بارتياح تمكنه من الوصول إلى المعلومات المتعلقة بالجريمة² ، وهو إجراء اقتضته الضرورة لمنع ارتكاب الجرائم الخطرة التي يحددها القانون والقبض على مرتكبيها في حالة الوصول إليه ومعرفته ، الأمر الذي قد يعرضه للخطر في حالة الوصول إليه ومعرفته ، كما أن فعله هذا قد يترتب عليه قيامه بأفعال مجرمة كحيازته لمادة ممنوعة أو تخزينه لمحصلات الجريمة أو غيرها من التصرفات ، إلا أنه هنا لا يتحمل المسؤولية الجنائية عما قام به من أفعال وتصرفات لغرض القبض على المجرمين لأنه قام بهذه الأفعال تنفيذ لواجب فرضه عليه القانون³ ، ونظراً لخطورة هذا الإجراء وتعرضه للمساس بسرية المراسلات بين الأفراد فإن القانون قد حصره في جرائم معينة وعلى درجة من الخطورة وبإذن مسبق ؛ وذلك كضمانة لخطورة هذا الإجراء وما يشكله من تعدي على حرمة المراسلات وخصوصيتها، ولهذا يمكن الإعتماد على نص الفقرة الثانية من المادة السابعة من قانون الجرائم الإلكترونية التي نصت على أن تكون مراقبة الرسائل الإلكترونية والمحادثات بإذن من القاضي الجزئي ، وهو يتفق مع نصوص قانون الإجراءات الجنائية الليبي في المادتين (79 و180).

ثانياً / اعتراض المراسلات : هي عملية مراقبة سرية للمراسلات السلكية أو اللاسلكية للوصول إلى أدلة متعلقة بالجريمة حول المشتبه في ارتكابها ، وهو إجراء يمس بحرية الأفراد والتعرض لخصوصياتهم ومكمن سرهم ، إلا أنه ولطبيعة هذه الجرائم الإلكترونية فإن الإطلاع على المراسلات أمر توجبه مقتضيات التحقيق ذلك أن هذه الجرائم يتم أغلبها عن طريق المراسلات الإلكترونية والاتصالات فهو إجراء له الدور البالغ في تتبع المشتبه بهم والوصول إلى الأدلة المتعلقة بالجريمة⁴.

وإذا كان قانون الإجراءات الجنائية قد جعل ذلك من اختصاص قاضي التحقيق والقاضي الجزئي وأوجب على النيابة العامة الحصول على إذن من القاضي الجزئي عند قيامها بضبط المراسلات ومراقبة المكالمات الهاتفية بموجب نص المادة (18) فإن هذا النص قد جاء عاماً بحيث ينطبق على كل المراسلات والاتصالات بحيث تشمل المراسلات والمكالمات الهاتفية أو الإلكترونية فتخضع المراسلات والمكالمات الإلكترونية لنصوص قانون الإجراءات الجنائية ويتطلب بها توافر الشروط المتطلبية لذلك وألا يتم اللجوء إليها إلا في حدود ضيقة ولغرض اظهار الحقيقة⁵.

وفي هذا السياق ترى الدراسات القانونية الحديثة أن غياب تنظيم إجرائي خاص بالجرائم الإلكترونية في قانون الجرائم الإلكترونية رقم (5) لسنة 2022 لا يمنع من الإستناد إلى القواعد العامة الواردة في قانون الإجراءات الجنائية ، مع ضرورة مراعاة طبيعة الدليل الإلكتروني والحفاظ على مشروعيته واحترام حرمة المراسلات والبريد الإلكتروني والمحادثات الخاصة ، وأن تكون المراقبة في أضيق نطاق ولمدة محددة وتحت رقابة القضاء⁶.

وعليه فإن اعتراض المراسلات الإلكترونية يمثل إجراءً إجرائياً ذا أهمية خاصة في مكافحة الجرائم الإلكترونية ، إلا أن مشروعيته تظل مرتبطة باحترام الضمانات القانونية والقضائية المقررة لحماية سرية الاتصالات والحياة الخاصة ، بحيث لا يتحول البحث عن الدليل الإلكتروني إلى وسيلة للتوسع غير المشروع لخطورة هذه الجرائم وما لها من تأثير على

ثالثاً / المراقبة الإلكترونية : بداية يجب أن نفرق بين المراقبة التي تقع بناءً على اتهام موجه إلى شخص معين بناءً على تحقيق مفتوح لغرض ضبط الأدلة المتعلقة بالجريمة الجاري التحقيق بشأنها ، وبين المراقبة الوقائية التي تسعى إلى كشف أي خطر أو تهديد يضر المجتمع من خلال ما ينشر على المواقع الإلكترونية فيتم التصدي لها ومنعها وحجب هذه المنشورات ومنعها من النشر وهو إجراء وقائي لجأ إليه المشرع لخطورة هذه الجرائم وما لها من تأثير على

1. د. بشير الشعاب بحيج ، إجراءات جمع أدلة الإثبات في الجرائم الإلكترونية في القانون الليبي ، مجلة كلية الشريعة والقانون ، المجلد 6 ، العدد 1 ، 2025 ، ص 14 .

2. محمد علي سويلم ، مرجع سبق ذكره ، ص 793 .

3. د. بشير الشعاب بحيج ، مرجع سبق ذكره ، ص 14 .

4. د. بشير الشعاب بحيج ، المرجع نفسه ، ص 16 .

5. محمد علي سويلم ، مرجع سبق ذكره ، ص 810 .

6. جميلة سعيد مصباح شوران ، التفتيش في الأوساط الإلكترونية ، مجلة أبحاث ، جامعة سرت ، كلية الآداب ، المجلد 15 ، العدد 1 ، مارس ، 2023 ، ص 113 ، 129 .

المجتمع وقد حصرها في جرائم معينة ، وتكتسب هذه الوسيلة الإجرائية أهمية خاصة في مجال الجرائم الإلكترونية بالنظر إلى سرعة تداول البيانات وإمكانية محوها أو تغييرها ، الأمر الذي يجعل الوسائل التقليدية في جمع الاستدلالات غير كافية لمواجهة هذا النمط الإجرامي¹ .

وقد أخذ المشرع الليبي بالمراقبة في قانون مكافحة الجرائم الإلكترونية رقم (5) لسنة 2022 م ، حيث أجاز للهيئة الوطنية لأمن وسلامة المعلومات مراقبة ما ينشر ويعرض عبر شبكة المعلومات الدولية أو أي نظام تقني آخر ، كما اشترط بالنسبة إلى مراقبة الرسائل الإلكترونية أو المحادثات صدور أمر قضائي من القاضي الجزئي المختص ، ويعد هذا الشرط ضماناً إجرائية وحرمة المراسلات بحيث لا تتحول المراقبة الإلكترونية إلى وسيلة للتدخل غير المشروع في الحياة الخاصة للأفراد .

ومن ثم فإن مشروعية المراقبة الإلكترونية لا تتوقف على وجود نص يجيزها فحسب ، وإنما تستلزم كذلك احترام الضمانات المقررة قانوناً وفي مقدمتها صدور الإذن من السلطة القضائية المختصة ، وتحديد نطاق المراقبة وموضوعها ومدتها ، وقصر استخدامها على الحالات التي تقتضيها ضرورة الكشف عن الجريمة ، بما يحقق التوازن بين مقتضيات مكافحة الجرائم الإلكترونية من جهة وحماية الحق في الخصوصية وسرية المراسلات والاتصالات من جهة أخرى ، وتبرز أهمية هذا الضابط بصورة أكبر في الجرائم الإلكترونية باعتبار أن المراقبة قد تنصب على الرسائل والمحادثات والبيانات الشخصية وغيرها من المعلومات ذات الطبيعة الخاصة ، ولذلك فإن إخضاعها للرقابة القضائية يمثل ضماناً أساسية لمشروعية الدليل الإلكتروني المستمد منها ، ويحول دون التوسع في استعمال هذه الوسيلة بما يمس الحقوق والحريات الفردية² .

على الرغم من أهمية تنظيم المراقبة الإلكترونية في قانون مكافحة الجرائم الإلكترونية الليبي ، إلا أن النص التشريعي يظل بحاجة إلى مزيد من التفصيل فيما يتعلق بالضوابط الإجرائية لمباشرة هذا الإجراء ولا سيما تحديد مدة المراقبة ، وشروط تجديدها والبيانات التي يجوز إخضاعها للمراقبة والإجراءات الواجب اتباعها في حفظ ما يتم الحصول عليه من بيانات فضلاً عن بيان مصير البيانات التي لا صلة لها بالجريمة ، ويعد تنظيم هذه المسائل بصورة أكثر تفصيلاً أمراً مهماً لتحقيق التوازن بين فعالية مكافحة الجرائم الإلكترونية وحماية الحقوق والحريات الفردية³ .

الخاتمة

بهذا نكون قد وصلنا إلى نهاية بحثنا – الجرائم الإلكترونية وسبل مكافحتها في ظل التشريع الليبي – وأن لنا أن نشير إلى النتائج والتوصيات التي توصلنا إليها من خلال دراسة هذا البحث والتي تتمثل في الآتي :
أولاً / النتائج :-

- 1-أظهرت الدراسة أن الجرائم الإلكترونية تمثل نمطاً إجرامياً مستحدثاً يختلف عن الجرائم التقليدية من حيث وسيلة ارتكابها وطبيعة محل الإعتداء ، الأمر الذي يفرض أساليب قانونية وفنية تتلائم مع خصوصيتها .
- 2-تبين أن الجريمة الإلكترونية تتميز بمجموعة من الخصائص من أهمها سرعة ارتكابها ، وصعوبة اكتشاف مرتكبيها ، وإمكانية ارتكابها عن بُعد ، فضلاً عن قدرتها على تجاوز الحدود الإقليمية للدولة.
- 3- كشف الدراسة عن تعدد صور الجرائم الإلكترونية وتنوعها تبعاً للمصلحة القانونية محل الحماية ، فلم تعد الاعتداءات الإلكترونية مقتصرة على البيانات والأنظمة لمعلوماتية ، وإنما امتدت إلى الأموال والأشخاص والخصوصية وغيرها من المصالح .
- 4-أثبتت الدراسة أن خطورة الجرائم الإلكترونية لا تقتصر على الأفراد وإنما تمتد إلى المؤسسات والقطاعات الاقتصادية والمالية والأمنية ، الأمر الذي جعل مكافحتها ضرورة تتجاوز حماية المصلحة الفردية إلى حماية المجتمع والدولة .
- 5-تبين أن المشرع الليبي اتجه إلى توفير حماية جنائية خاصة للجرائم الإلكترونية من خلال إصدار القانون رقم (5) لسنة 2022م بشأن مكافحة الجرائم الإلكترونية ، وهو ما يمثل خطوة تشريعية مهمة في مواجهة التطور المتزايد للجرائم المرتكبة باستخدام الوسائل التقنية .

6-خلصت الدراسة إلى أن التشريع الليبي رغم أهميته في تنظيم مكافحة الجرائم الإلكترونية ، يحتاج إلى مزيد من التطوير والتفصيل بما يواكب التطورات التقنية المتسارعة ؛ لأنه لم ينص المشرع على القواعد الإجرائية التي تنظم كيفية مواجهة هذه الجرائم والوصول إلى الدليل على ارتكابها ، الأمر الذي يترتب عليه الرجوع إلى نصوص قانون الإجراءات الجنائية كونها نصوص عامة تسري على كل الجرائم بغض النظر عن وسيلة التي ارتكبت بها الجريمة .

¹ د. بشير الشعاب بحيج ، مرجع سبق ذكره ، ص 17 .

² نبيلة قيشاح ، ضمانات المراقبة الإلكترونية في التشريع الجزائري ، مجلة الحقوق والعلوم السياسية ، المجلد 10 ، العدد 2 ، 2023 ، ص 1104 .

³ د. بشير الشعاب بحيج ، مرجع سبق ذكره ، ص 17 .

ثانياً / التوصيات :

- 1-نوصي بمراجعة وتطوير أحكام القانون رقم (5) لسنة 2022م بشأن مكافحة الجرائم الإلكترونية بصورة دورية ، بما يضمن مواكبته للتطور المستمر في وسائل ارتكاب الجرائم الإلكترونية وصورها المستحدثة .
- 2-نوصي بوضع تنظيم إجرائي أكثر تفصيلاً للأدلة الإلكترونية ، يتضمن قواعد واضحة بشأن ضبطها وجمعها وحفظها واستخراجها وتقديمها أمام القضاء ، مع ضمان المحافظة على سلامتها وعدم العبث بمحتواها .
- 3-نوصي بإجراء المزيد من الدراسات القانونية المتخصصة في الجرائم الإلكترونية ، وبصفة خاصة الدراسات المتعلقة بالإثبات الرقمي ، والمسؤولية الجنائية ، وحماية الأطفال من الجرائم الإلكترونية .

قائمة المراجع

أولاً / الكتب :

- 1-إبراهيم ، خالد ممنوح . (2009) . الجرائم المعلوماتية . الإسكندرية . مصر : دار الفكر العربي.
- 2- المناعسة، أسامة أحمد ، والزعبي ، جلال محمد . (2014) . جرائم تقنية نظم المعلومات الإلكترونية .دراسة مقارنة .(2007) . الحماية الجزائية للمعلومات في التشريع الجزائري . ط2 ، الجزائر : دار هومة للنشر والتوزيع .
- 3- فكري ، أيمن عبدالله.الجرائم المعلوماتية. (2014) . دراسة مقارنة في التشريعات العربية والأجنبية . الرياض : مكتبة القانون والاقتصاد .
- 4- سويلم ، محمد علي .جرائم الكمبيوتر والإنترنت — دراسة مقارنة .(2019) . الإسكندرية : دار المطبوعات الجامعية .
- 5- المسند ، عبدالرحمن بن عبدالله . جريمة الابتزاز . (2018) . الرياض : مطبوعات الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر .
- 6- البيومي ، عبدالفتاح حجازي . مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت . (2006) . الإسكندرية : دار الفكر الجامعي .
- 7- الشوابكة ، محمد أمين . جرائم الحاسوب والإنترنت (الجريمة المعلوماتية) . (2004) . عمان : دار الثقافة للنشر والتوزيع .
- 8 - غازي ، محمود إبراهيم . الحماية الجنائية للخصوصية والتجارة الإلكترونية . (2014) . الإسكندرية : مكتبة الوفاء القانونية .
- 9- عادل ، نائلة . جرائم الحاسب الآلي الاقتصادية . (2012) . بيروت : منشورات العلى الحقوقية

ثانياً / رسائل الماجستير :

- 1-المطيري ، سامي مرزوق نجاء . المسؤولية الجنائية عن الابتزاز الإلكتروني في النظام السعودي . رسالة ماجستير . (2018) . جامعة نايف العربية للعلوم الأمنية . الرياض : المملكة العربية السعودية .

ثالثاً / البحوث والمجلات :

- 1- النهوي ، أحلام محمود . جرائم الحاسب الآلي وسبل مكافحتها . (2017) . المجلة الليبية العالمية ، العدد 20 .
- 2 العبيدي ، أسامة بن غانم . جريمة الدخول غير المشروع إلى النظام المعلوماتي " دراسة قانونية في ضوء القوانين المقارنة " . (2012) . مجلة دراسات المعلومات . العدد 12 .
- 3- الشعاب ، بشير بحيج . إجراءات جمع أدلة الإثبات في الجرائم الإلكترونية في القانون الليبي . (2025) . مجلة كلية الشريعة والقانون . المجلد 6 . العدد 1.
- 4- شوران ، جميلة سعيد مصباح . التفتيش في الأوساط الإلكترونية . (2013) . مجلة أبحاث .. كلية الآداب . جامعة سرت المجلد 15 . العدد 1.
- 5- البداينة ، ذياب موسى . الجرائم الإلكترونية . (2014) . المفهوم والأسباب — ورقة علمية مقدمة إلى الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية . عمان . الأردن . من 2 إلى 4 سبتمبر .
- 6- رحاب علي عميش ، الجريمة المعلوماتية ، دراسة مقارنة بين القانون الليبي والإماراتي ، مجلة معهد دبي القضائي ، المجلد الثاني ، العدد الرابع ، يوليو 2-14 .
- 7-لورنس سعيد أحمد الحوامدة، الجرائم المعلوماتية " أركانها وآلية مكافحتها " ، دراسة تحليلية مقارنة ، مجلة الميزان للدراسات الإسلامية والقانونية ، المجلد الرابع ، العدد الأول ، جامعة العلوم الإسلامية العالمية ، الأردن ، 2017 .
- 8- بوزيدي ، مختارية . ماهية الجرائم الإلكترونية . بحث مقدم ضمن أعمال الملتقى الوطني . آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري . (2017) . ، الجزائر : 29- مارس . مركز جيل البحث العلمي .

- 9- القطاونه ، مصعب الإجراءات الجنائية الخاصة في الجرائم المعلوماتية . (2010) . بحث مقدم لشبكة قانوني الأردن.
- 10- الشركسي ، محمد محمود . الجريمة الإلكترونية وسبل مكافحتها في ضوء أحكام الفقه الإسلامي . دراسة مقارنة . (2021) . مجلة المنارة العلمية . مايو . العدد الثاني .
- 11- إعبية ، خليل سعيد خليل . القالب التشريعي لجرائم انتحال الصفة والشخصية الإلكترونية . دراسة مقارنة (2021) . مجلة العلوم الإنسانية والإدارية . مارس . العدد 22.
- 12- مشرف ، ممدوح ، و العنزي ، رشيد الرشيد . الحماية الجنائية للمجني عليه من الإبتزاز . (2017) . المجلة العربية للدراسات الأمنية . الرياض : المجلد 33 . جامعة نايف العربية للعلوم الأمنية . العدد 70 .
- 13- قيشاح ، نبيلة . ضمانات المراقبة الإلكترونية في التشريع الجزائري . (2023) . مجلة الحقوق والعلوم السياسية . المجلد 10 . العدد 2 .
- 14- فرج ، هيفاء عبد العالي . الحماية الجنائية للمواقع الإلكترونية والأنظمة المعلوماتية للدولة . دراسة مقارنة . (2023) . مجلة العلوم القانونية . كلية القانون . جامعة المرقب . الخمس . ليبيا : ديسمبر . المجلد 11 . العدد 2.

رابعاً / القوانين واللوائح :

- 1-أنظر الجريدة الرسمية. قانون رقم 5 لسنة 2022م . بشأن مكافحة الجرائم الالكترونية . (2023) . السنة الأولى . العدد 1.
- 2- منظمة التعاون الاقتصادي والتنمية (OECD) . الجريمة المرتبطة بالحاسوب . (1986) . باريس : تحليل السياسة القانونية.
- 3- الأمم المتحدة، الجرائم المتعلقة بشبكات الحاسوب، المؤتمر 10 للأمم المتحدة لمنع الجريمة ومعاينة المجرمين . (2000) . فيينا : 10-17-أبريل . الوثيقة رقم (A/CONF,187/01) .
- 4-اتفاقية بودابست بشأن الجريمة الإلكترونية لسنة 2001 . الخاصة بالإحتيال المرتبط بالحاسب .
- 5- أنظر مجلس أوروبا. مجموعة المعاهدات الأوروبية. الاتفاقية المتعلقة بالجرائم الالكترونية. (2001) . رقم 185.
- 6- انظر اتفاقية الاتحاد الافريقي بشأن الأمن السيبراني وحماية البيانات الشخصية (2024م). منشور على الموقع الالكتروني:

<https://ccdcoe.org/uploads/2018/11/AU-270614-CSConvention.pdf>