المجلة المغربية للدراسات القانونية والاقتصادية
ISSN(P) : 1142-2489
Numéro 15, AVRIL 2025
REMEJE
العدد 15، أبريل 2025
ISSN(E) : 3085-4555
Revue Marocaine des Eudes Juridiques et Economiques

مخاطر الجريمة الإلكترونية على الأمن القومي الليبي

Risks of Cybercrime on Libyan National Security

د. خالد أحمد مُحَمَّد ابزيم

أستاذ القانون العام المشارك

كلية القانون، جامعة سبها،

kha.ebzim@sebhau.edu.ly

الملخص:

في إطار التقدم الذي يشهده العالم في استخدام شبكة المعلومات والتقنيات الحديثة، أصبح الأمن القومي مُهدداً بأساليب إجرامية جديدة على التشريعات الجنائية، وذلك بما يمثل تهديداً خطيراً للمصالح والأهداف الحيوية، مما قد يؤثر على النظام السياسي والأمني للدولة بشكل يترتب عليه نتائج غير مرغوبة، يُمكن أن تُهدد كيان الدولة وبقاءها.

بناء على ما سبق، سارعت الكثير من بلدان العالم ومن بينها الدول العربية على سن قوانين خاصة بمكافحة الجرائم الإلكترونية. وإسوة بالتشريعات المقارنة تصدى المشرع الليبي للجرائم الإلكترونية بسنه قانون خاص بمكافحة الجرائم الإلكترونية رقم (5) لسنة 2022 والذي حدد فيه جرائم التعدي على عمل النظام المعلوماتي، وبرامج وشبكات المعلومات والمواقع الإلكترونية، وغيرها من الجرائم المعلوماتية الماسة بأمن الدولة القومي والسلامة العامة للمجتمع.

وباستقرائنا للقانون السالف الذكر تبين لنا أنه بالرغم من قيام المشرع الليبي بتشديد في العقوبة عن الأفعال والسلوكيات الإجرامية التي ترتكب باستخدام وسائل تقنية المعلُومات كونها تمس وتهدد المصلحة العامة والأمن القومي للبلاد، إلا أنه لم يُنظم أدلة الإثبات الرقمية، ولم يؤسس لجهة تختص بفحص الأدلة الرقمية لتكون مساعداً للقضاء في الوصول إلى الجريمة ونسبتها إلى فاعلها، الأمر الذي يجعل مواجهة الجريمة الإلكترونية أمراً صعباً على القضاء.

الكلمات المفتاحية: الجريمة الإلكترونية، الأمن القومي، تهديدات، ليبيا.

Abstract:

Within the framework of the progress witnessed by the world in the use of the information network and modern technologies, national security has become threatened by new criminal methods in criminal legislation, which represents a serious threat to vital interests and goals, which may affect the political and security system of the state in a way that results in undesirable results that may threaten the entity and survival of the state. Based on the above, many countries in the world, including Arab countries, have rushed

to enact laws to combat cybercrimes. Similar to comparative legislation, the Libyan legislator has addressed cybercrimes by enacting a special law to combat cybercrimes No. (5) of 2022, which defines crimes of infringement on the work of the information system, information programs and networks, websites, and other cybercrimes that affect the national security of the state and the public safety of society. By examining the aforementioned law, it became clear to us that although the Libyan legislator imposed a harsher penalty for criminal acts and behaviors committed using information technology, as they affect and threaten the public interest and national security of the country, it did not organize digital evidence, nor did it establish a body specialized in examining digital evidence to assist the judiciary in reaching the crime and attributing it to its perpetrator, which makes confronting cybercrime difficult for the judiciary.

Keywords: Cybercrime, National Security, Threats, Libya.

مقدمة:

أفرز التقدم التقني والتكنولوجي ظهور وسائل الكترونية حديثة ومتنوعة، حيث أصبحت مجالاً وفضاءً واسعاً للاستخدام والانتشار اللامحدود. فتلك الوسائل تعتبر من الأمور الحياتية الهامة التي لا يمكن الاستغناء عنها بالنسبة للأفراد أو المؤسسات، فالجميع اليوم بات يعتمد على التقنيات الإلكترونية الحديثة وذلك لتحقيق أغراضٍ عدة كاستقاء المعلومات، والتواصل واكتشاف المعارف، وإجراء البحوث العلمية وما إلى ذلك.

ولكن رغم الإيجابيات التي تمنحها الوسائل الإلكترونية الحديثة للبشرية، إلا أنها في المقابل أفرزت أنواعاً جديدة من الجرائم ألا وهي الجرائم الإلكترونية والهجمات السيبرانية التي تعد خطراً يطال كل المجتمعات الإنسانية ويُصيبها بالأزمات السياسية والاقتصادية والاجتماعية والثقافية والأمنية.

وبناء على ما سبق، فإن الجريمة الإلكترونية أصبحت ظاهرة عالمية يمكن أن تُسبب في ضرر كبير للأفراد والمنظمات والحكومات على حدٍ سواء، حيث خلق استخدام التكنولوجيا والانترنت فرصاً جديدة للمخترقين المجرمين لاستغلال نقاط الضعف وارتكاب الجرائم. وتنقسم هذه الجرائم إلى نوعين، **النوع الأول**: الجرائم الموجهة ضد جهاز الحاسب الآلي أو أنظمة تقنية المعلومات والاتصالات. **والنوع الثاني**: تلك الجرائم التي يكون فيها الحاسب الآلي وسيلة لارتكاب الجرائم الإلكترونية.

ونظراً لكون نشاط مجرمي الانترنت يتم عبر الحدود الوطنية كان من الصعوبة بمكان على وكالات تنفيذ القانون تعقبهم وتقديمهم للعدالة، حيث يستخدمون أساليب متطورة لارتكاب جرائمهم التي تتراح ما بين سرقة البيانات، والاحتيال المالي، والإرهاب الإلكتروني، والتجسس والقرصنة الإلكترونية، وابتزاز الأفراد أو التشهير بهم، إضافة إلى سرقة الحسابات البنكية، والخروقات لتجنيد الشباب والفتيات وحتى الأطفال للقيام بأعمال تخريبية.

وبهذا أصبحت الجرائم الإلكترونية تهدد الأمن القومي لمختلف دول العالم عامة وليبيا خاصةً، مما أدى إلى زعزعة استقرار الدولة وإلحاق الضرر باقتصادها الوطني، وكيانها الإجتماعي، وكذا أضحت أداة لإفساد العلاقات الدولية، لذلك تطلبت الطبيعة العالمية للجرائم الإلكترونية التعاون والتنسيق الدولين لمكافحة هذا التهديد المتزايد بشكل فعال.

وارتباطاً بما سبق؛ فقد بُذلت جهود دولية في مكافحة الجرائم الإلكترونية من خلال الاتفاقيات والمؤتمرات التي حثت الدول على تجريم ومعاقبة مرتكبي الجرائم المعلُوماتية. ونتيجة لذلك سارعت الكثير من بلدان العالم ومن بينها الدول العربية على سن قوانين خاصة بمكافحة الجرائم الإلكترونية. فليبيا كغيرها من الدول تأثرت بموجة التطور التكنولوجي والتقني، فصاحب ذلك ظهور العديد من الممارسات والجرائم ذات الطابع الإلكتروني مست بأمن وسلامة البلاد، هذا الأمر دفع بالمشرع الليبي للتدخل بإصدار القانون رقم (5) لسنة 2022 بشأن الجرائم الإلكترونية. إذ بالرغم من تأخر صدور هذا القانون إلا أنه حتماً سيخفف من حدة الممارسات غير المشروعة التي يقترفها المجرمون عند استخدامهم لجميع الوسائل الإلكترونية.

ناهيك عن أنَّ اتخاذ التدابير التقنية المناسبة لمحاربة تلك الجرائم يُعد أحد أهم الأسلحة الاستراتيجية التي تمتلكها الدول في عصر الثورة الرقمية حالياً، وهو ما يعتبر أعلى تحدي يواجه الأمن القومي الليبي في العصر الحديث، نظراً للمخاطر المصاحبة لتلك الجرائم، لاسيما أن المفهوم الحديث للأمن لا يشمل الأمن العسكري فحسب، بل يشمل أمن الفرد والمؤسسة والأسرة الدولية على جميع المستويات، ومن أهمها أمن المعلومات، الأمر الذي يضع السيادة الوطنية لأي دولة على المحك، خاصة مع زيادة التجسس الإلكتروني على بعض الدول، حيث اسقطت تكنولوجيا المعلومات والاتصالات مفهوم الحدود الجغرافية والسياسية والثقافية فيما بينها.

أهداف البحث:

تهدف هذه الدراسة إلى بيان طبيعة الجرائم الإلكترونية، والتعرف على مدى فاعلية التشريعات الوطنية والمقارنة المقررة لمكافحتها، كما تهدف الدراسة إلى المساهمة في وضع وتوصيف الحلول العملية وذلك من خلال عرض الاستراتيجيات والسبل التي يمكن تبينها والاعتماد عليها لمواجهة هذا النوع من الإجرام.

أهمية البحث:

تكمنُ أهمية هذا البحث في بيان خطورة الجرائم الإلكترونية وما تفضي إليه من تهديدات تمس كيان الدولة وأمنها القومي. كما تزداد أهمية الدراسة وضوحاً في كونها تُلامس أحد المواضيع الحديثة والحساسة بحكم ما تعرفه ليبيا اليوم من ظروف أمنية شائكة وصعبة تتطلب المزيد من الجهد والبحث للوصول إلى حلول تحدُ من تداعيات الجرائم الإلكترونية والسيبرانية، مع الأخذ في الاعتبار إحداث نوع من التوزان بين المتطلبات الأمنية وضرورة توفير أكبر قدر من الحماية للحريات العامة دون الانتقاص منها أو تعطيلها بحجة حفظ النظام العام للدولة.

إشكالية البحث:

تُثار إشكالية أمن واستقرار الدول في ظل انتشار الجرائم الإلكترونية التي أضحت تمثل معضلة أمنية لدى جميع الدول، حيث تزداد خطورتها خاصة على الدول التي تشهد حالة عدم استقرار سياسي وأمني، فتنوع هذه الجرائم وانتشارها يدعو إلى ضرورة البحث في التأثيرات والتداعيات التي تُحدثها هذه الظاهرة. ومن هنا؛ تَدورُ في ذهنِ الباحث عِدة تساؤلات أو استفهامات قانونية وأمنية تتمحور حول إشكالية رئيسية مفادها:

"**إلى أي حدٍ تُشكل الجرائم الإلكترونية خطراً حقيقياً على الأمن القومي الليبي؟**". سنعتمدُ على المنهجين الوصفي التحليلي والمقارن، لنُحاولُ بِواسطتهما الإجابة على هذه الإشكالية وفقاً للمحاور التالية:

أولاً: المحددات العامة للجريمة الإلكترونية (المفهوم والإطار القانوني)

ثانيا: صور الجرائم الإلكترونية الماسَة بالأمن القومي الليبي

ثالثا: آليات مواجهة الجرائم الإلكترونية المُهددة للأمن القومي

المبحث الأول: المحددات العامة للجريمة الإلكترونية (المفهوم والإطار القانوني)

بفعل الثورة التكنولوجية المعاصرة والتي بدأت معالمها تتضح مع القرن الواحد والعشرين، تزامنت معها ظهور العديد من الجرائم المستحدثة، والتي تختلف من حيث محلها وأسلوب ارتكابها عن الجرائم التقليدية، وتُسمى بـ "**الجرائم المعلوماتية**"، حيث تُستخدم فيها تقنيات تكنولوجيا المعلومات والاتصالات، وهذا أدى بالضرورة إلى تطور مفهوم الجريمة بسبب اعتمادها على التقنيات العلمية الحديثة، مما أضفى عليها أبعاداً جديدة لم تكن معروفةً من قبل.

وفي إطار التقدم الذي يشهده العالم في استخدام شبكة المعلومات والتقنيات الحديثة، أصبح الأمن القومي مُهدداً بأساليب إجرامية جديدة على التشريعات الجنائية، وذلك بما يمثل تهديداً خطيراً للمصالح والأهداف الحيوية، مما قد يؤثر على النظام السياسي والأمني للدولة بشكل يترتب عليه نتائج غير مرغوبة، يُمكن أن تُهدد كيان الدولة وبقاءها. ومن أجل ذلك سوف نستعرض في هذا المبحث **مفهوم الجريمة الإلكترونية** وأهم الخصائص التي تميزت بها عن غيرها من الجرائم الأخرى، بعدها سنتناولُ الإطار القانوني الذي يؤطرها وينظمها.

أولا: مفهوم الجريمة الإلكترونية

تعتبر الجرائم الإلكترونية من الجرائم المستحدثة التي ظهرت في عصرنا الحالي، وذلك بسبب ارتباطها بوسائل الإتصال والتقنيات الحديثة كشبكات الإنترنت وأجهزة الكمبيوتر والمواقع الإلكترونية.

وبالنظر إلى خصوصية هذه الجريمة وباختلافها عن الجرائم التقليدية الأخرى، لم يكن من السهل جداً أن تحضى باجماع من الفقهاء والمختصين ولا حتى من المشرع لتحديد وصفها ومعاييرها، حيث أصبح من الصعب أن يكون لها تعريف جامع مانع لها على اعتبار أنها من الجرائم العصرية التي ساهمت في ظهورها التطورات العلمية في مجال الاتصالات وتنقية المعلومات، وما رافق ذلك من تطور شهدته شبكة الانترنت مما ترتب عليه ظهور فئات جديدة من السلوك الإجرامي ومرتكبيه والذي تطور بتطور هذه التقنيات.

وبما أن مسألة وضع تعريف للجريمة الإلكترونية محلاً لاجتهادات الفقهاء، لم يتمكن الفقه الجنائي من الاتفاق على تسمية موحدة للجريمة الإلكترونية، إذ أُطلق عليها البعض بالجريمة الإلكترونية، وهناك من يُسميها بجرائم الانترنت، والبعض الأخر يُسميها بالجريمة المعلوماتية، وذهب أخرون إلى تسميتها بجريمة إساءة استخدام تكنولوجيا المعلومات والاتصال، وكذلك سُميت بالجريمة السيبرانية.

وتعددت وتباينت آراء الفقهاء حول مفهوم الجريمة الإلكترونية، حيث نجد من يعرفها من الجانب التقني (الفني) بأنها " نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل

الإجرامي المقصود".[1] وهناك من عرفها من الناحية القانونية، حيث يرى أنصار هذا الاتجاه بأن تعريف الجرائم الإلكترونية يتطلب تحديد المفاهيم والمفردات المرتبطة بارتكاب جرائم الحاسب الآلي وتقنية المعلومات من قبيل (الحاسب الآلي، برنامج الحاسب الآلي، البيانات، الممتلكات، الدخول، الخدمات الحيوية....).

كما أن هناك جانب من الفقه يعرف الجريمة الإلكترونية من زاوية محل الواقعة التي تُكونها فيعرفها بأنها "الجريمة التي تقع على أحد مكونات أو عناصر النظام المعلوماتي".[2] وعرفها أخر من منظُور الأداة أو الوسيلة التي ترتكب عن طريقها الجريمة، فاعتبر أنها " تلك الجريمة التي تُرتكب عن طريق أحد الوسائل الإلكترونية، أي أنها جريمة تكون فيها الأداة أو الوسيلة الإلكترونية التقنية هي وسيلة ارتكابها"، أو هي " عمل إجرامي يستخدم الحاسب الآلي في ارتكابه كوسيلة أساسية".[3] وهناك أتجاه آخر يعرفها من الناحية الموضوعية فيرى أن الجريمة الإلكترونية لا يكفي لإطلاق هذا الوصف عليها بمُجرد استخدام الحاسب الآلي فيها، لكن يشترط أن يقع الفعل داخل نظام الحاسب الآلي لاحتسابها جريمة الكترونية، ولذلك عرَّف الجريمة الإلكترونية بأنها " نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تُرسل عن طريقه".[4]

وعلى سبيل الاجتهاد من جانبنا نُعرف الجريمة الإلكترونية بأنها سلوك إجرامي يُحقق نفع غير مشروع لمرتكبيه ويتم بواسطة استخدام مختلف أجهزة الإتصال وتقنية المعلومات.

وتجدر الإشارة إلى أن التعريفات الفقهية السابقة لمفهوم الجريمة الإلكترونية تباينت وتراوحت بين الضيق التضييق والاتساع، ويرجع ذلك إلى اختلاف الزاويا التي نظر إليها المختصين والفقهاء لهذا النوع من الإجرام.

فالتعريف الضيق للجريمة الإلكترونية هو "كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات، ويهدف إلى الاعتداء على الأموال المادية والمعنوية".[5] أما **التعريف الواسع للجريمة الإلكترونية** فيُقصد به " كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها" أو أنه " كل نشاط إجرامي أو سلوك معاقب عليه قانوناً ارتبط بالحاسب الآلي كوسيلة أو غاية أو كان هو له مساعداً أو محلاً لتحقيق نتيجة

[1] – محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الحقوق والشريعة، جامعة الإمارات، 21 مايو 2005، ص 6.

[2] – اسلام هديب، الأمن السيبراني (الهجمات السيبرانية والجرائم السيبرانية)، الطبعة الأولى، دار مصر للنشر والتوزيع، 2024، ص 277.

[3] – بهاء المري، مكافحة جرائم تقنية المعلومات وحجية الدليل الرقمي في الإثبات، دار مصر للنشر والتوزيع – القاهرة، 2019، ص 29.

[4] – الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجمع البحوث والدراسات، اكاديمية السلطان قابوس لعلوم الشرطة، 2016، ص 21.

[5] – محمد علي سويلم، مكافحة الجرائم الإلكترونية (دراسة مقارنة بالتشريعات العربية والأجنبية)، الطبعة الأولى، دار المطبوعات الجامعية، 2019، ص24.

غير مشروعة تحقق لمرتكبها كسباً وتُلحق بالمجني عليه ضرراً أياً كان نوع النشاط أو السلوك، أو كيفية الارتباط، أو طبيعة أو مقدر الكسب أو الضرر الناشئ عن ذلك السلوك أو النشاط".[1]

ويتضح من ما سبق ذكره، أن بعض الفقهاء يُميزون بين الجريمة الإلكترونية وجرائم الانترنت، رغم الارتباط بين طائفتي هذه الجرائم، حيث يكمُن التمييز بينهما في أن جرائم الانترنت تتطلب اتصالاً بالشبكة الدولية، أما الجرائم الإلكترونية فيُمكن أن ترتكب دون توافر شبكة الانترنت مثل: جرائم تخريب النظم المعلوماتية، وجرائم الاعتداء على حق المؤلف.[2] إلا أننا نرى بأن الجرائم الإلكترونية وجرائم الانترنت وجرائم شبكة المعلومات هي كُلها مصطلحات أو مُسميات مترادفة تفترض الدخول للحاسب الآلي ثم شبكة الانترنت ثم ارتكاب السلوك غير المشروع.

فعلى المستوى التشريعي فنجد أن بعض التشريعات عرَفت الجرائم المعلوماتية بطريقة غير مباشرة، وبعضها لم يتعرض لها واكتفت ببيان عناصر الركن المادي للجريمة، وهذا على اعتبار أن المشرع لا يختص بوضع التعريفات، وإنما هي من مهمة الفقه والقضاء. فمن بين التشريعات التي أعطت تعريفاً للجريمة الإلكترونية هما المشرع الليبي والكويتي والسعودي. فليبيا عرفت في البداية فراغاً تشريعياً بشأن مُكافحة الجرائم الإلكترونية، حيث لم نجد نصاً واضحاً لهذه الجريمة في قانون العقوبات الصادر في سنة 1953، وبعد مُرور نصف قرن من الزمان سن المشرع الليبي قانون الجرائم الإلكترونية رقم (5) لسنة 2022 الذي عرَف الجريمة 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).[3] أما القانون الكويتي فقد عرَفها في المادة الأولى من قانون مكافحة تقنية المعلومات بأنها (كل فعل يتم ارتكابه باستخدام الحاسب الآلي أو شبكة المعلومات أو غيرها من الوسائل التقنية بالمخالفة لأحكام القانون)، كما عرفها المشرع السعودي بموجب نظام مكافحة جرائم المعلوماتية بأنها (كل فعل يتم ارتكابه مُتضمناً استعمال الحاسب الآلي أو شبكة المعلومات بالمخالفة لأحكام النظام).

ويتضح من التعريفات السابقة توافق التشريع الليبي مع المشرعين الكويتي والسعودي في تعريف الجريمة الإلكترونية وهو ما يعكس خطورة وتطور هذا النوع من الجرائم التي تتسم بتنوع وسائل وطرق ارتكابها وتباين خصائصها بمرور الزمن، خاصة مع تطور نظم تقنية المعلومات واستخدام تقنيات الانترنت.

وعلى الصعيد الدولي عرف مكتب تقييم التقنية بالولايات المتحدة الأمريكية الجريمة الإلكترونية بأنها " الجريمة التي تلعب فيها البيانات الحاسوبية والبرامج المعلوماتية دوراً رئيسياً". وعرفها أيضاً بأنها " نشاط جنائي يُمثل اعتداء على برامج

[1] – علي أحمد الفرجاني، جريمة القرصنة المعلوماتية (دراسة مقارنة من الجانبين الموضوعي والإجرائي)، مجلة التشريع، العدد 7 أكتوبر 2005، ص 170.
[2] – عاطف عباس عبد الحميد، جرائم تقنية المعلومات وحقوق الملكية الفكرية، المؤسسة العربية للعلوم والثقافة – القاهرة، 2020، ص 23.
[3] – الفقرة الأولى من المادة (1) من قانون الجرائم الإلكترونية.

وبيانات الحاسب الإلكتروني". وجاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا سنة 2000 تعريف للجريمة الإلكترونية " بأنها أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي، والجريمة تلك شاملة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية".[1]

وبناء على ما سبق، نلاحظ أن التعريف الدولي للجريمة الإلكترونية يعتمد في الغالب على الغرض من استخدام المصطلح: فهناك عدد محدود من الأفعال التي تمس السرية والنزاهة وبيانات الكمبيوتر وأنظمة تمثل جوهر الجريمة الإلكترونية، كما أن هناك أعمال متعلقة بالكمبيوتر لتحقيق مكاسب شخصية أو مالية أو ضرر بما في ذلك الأفعال المتصلة بجرائم محتويات الكمبيوتر.[2]

ثانياً: سمات الجريمة الإلكترونية

نظراً لارتباط الجرائم الإلكترونية بالحاسوب، وبشبكة الانترنت عامة، وبوسائل التواصل الاجتماعي خاصة، وما لها من تأثير كبير على أمن الدولة أضفت عليها مجموعة من السمات والخصائص ميزتها عن غيرها من الجرائم التقليدية الأخرى، نستعرض أهم هذه السمات في الآتي:

1- جريمة عابرة للحدود

تتصف الجريمة الإلكترونية عن بقية الجرائم التقليدية بأنها جريمة عابرة للحدود، أي أنها من الجرائم عبر الوطنية التي تقع بين أكثر من دولة، بمعنى أنها لا تعترف بالحدود الجغرافية للدول، ومع انتشار شبكات الاتصال العالمية أمكن ربط أعداد هائلة من أجهزة الكمبيوتر عبر العالم بهذه الشبكات بحيث أصبح التنقل والاتصال أمراً سهلاً وأمكن معرفة كلمة السر للدخول لأي موقع في شبكة الاتصال سواء تم ذلك بطرق مشروعة – أم غير مشروعة.

وارتباطاً بما سبق، فإن الجرائم الإلكترونية تُوصف بأنها جرائم تعدي عابرة للحدود الواحدة، تشمل عدة دول، وقد يكون المجني عليهم في دول متعددة ومختلفة، ولهذا تُوصف الجريمة بأنها جريمة عابرة للحدود الوطنية. وهذه السمة هي التي ميزت الجريمة الإلكترونية عن غيرها من الجرائم التقليدية، وذلك بسبب أنه يصعب في كثير من الأحيان أن تكون الجريمة التقليدية جريمة عابرة للحدود إلا في أحوال نادرة كجريمة غسل الأموال أو الجرائم الإرهابية.[3]

---

[1] – بوضياف اسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11 سبتمبر 2018، ص 352.

[2] – مختارية بوزيدي، ماهية الجريمة الإلكترونية، الملتقى الوطني حول " آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري، جزائر العاصمة 29 مارس 2017، ص 10.

[3] – محمود أحمد عباينة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع – عمان، 2009، ص 34.

ومن الأمثلة الدّالة على كون الجريمة الإلكترونية جريمة عابرة للحدود، وأنه يُمكن ارتكابها من أي مكان في العالم مع صُعُوبة كشف أدَلتها، حيث تسارع نمو معدلاتها وتضاعفت أضرارها وخسائرها المادية العالمية التي قدرت بـ 450 مليار دولار في عام 2013. وتعرضت منطقة الخليج العربي في عام 2012 إلى هجمات إلكترونية على مُنشآت شركة أرامكو السعودية، وعلى شركة رأس غاز القطرية. وفي مايو عام 2013 أطلقت هجمات إلكترونية على مواقع الكترونية حكومية في المملكة العربية السعودية أدت إلى تعطيل موقع وزارة الداخلية مؤقتاً. وقدرت خسائر النشاطات التجارية في دولة الإمارات العربية المتحدة بسبب الهجمات الإلكترونية بـ422 مليون دولار عام 2012.[1]

2- أسلوب ارتكاب الجريمة

ترتبط جرائم أمن الدولة المرتكبة عن طريق وسائل تقنية المعلومات بأجهزة الحاسب الآلي وشبكة المعلومات (الانترنت)، وهي السمة المميزة لهذه الجريمة عن الجرائم التقليدية، فوسيلة ارتكاب الجريمة في هذه الحالة تقنية تُتيح لمالكها أو مستخدمها أن يتواصل بصورة شرعية أو غير مشروعة مع عدد لا حصر له من أجهزة الحاسب الآلي على مستوى العالم مخترقاً بفعله أي نطاق زمني أو مكاني، وهو الأمر الذي يسهل معه أن ترتكب الجريمة في إقليم بينما تتحقق مخاطرها وأثرها في إقليم آخر.

3- المصلحة التي تهددها الجريمة (المصلحة المحمية)

إذا كانت هذه الجريمة لا تقع إلا باستخدام وسائل تقنية المعلومات، فإنها في الوقت ذاته لا تستهدف إلا الإضرار بأمن الدولة، حيث تقع على الرموز والمؤسسات التابعة للدولة، عن طريق اختراق المواقع الإلكترونية الرسمية وسرقة المعلومات السرية أو تغييرها، ونشر تلك المعلومات أو منحها لجهات أجنبية. كما قد تقوم هذه الجريمة في حالة تم شحن وتحريض الرأي العام داخل الدولة أو خارجها للقيام ببعض الأفعال الإجرامية المناهضة لسياسة الدولة تمهيداً للإطاحة بالنظام السياسي، أو زعزعةاستقراره، أو تأليب الرأي العام المحلي والعالمي ضده.[2]

وتكمن خصوصية الجريمة الإلكترونية في أنها قد تؤدي إلى إحداث خلل في التركيبة الاجتماعية في الدولة كخطوة أولية لإشاعة الاضطرابات والفوضى، وذلك عن طريق إثارة الفتن والقلاقل بين أطياف الشعب الواحد، وخاصة في المجتمعات التي تتضمن وجود تعدد مجتمعي أو أقليات سكانية سواء كان التصنيف المجتمعي ديني أو عرقي، حيث يسهل في هذا النوع من المجتمعات إثارة النزاعات العنصرية والطائفية.[3]

[1] – الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجمع البحوث والدراسات، أكاديمية السلطان قابوس، سلطنة عمان، 2016، ص 113.
[2] – علي حامد الخولي، الحماية الجنائية لأمن الدولة (دراسة مقارنة)، دار المعرفة الجامعية – القاهرة، 2014، ص 81.
[3] – رأفت عبد الفتاح حلاوة، الجرائم الماسة بأمن الدولة (جريمة قلب نظام الحكم)، دار النهضة العربية – القاهرة، 2010، ص 16.

وقد تستهدف هذه الجريمة اصطناع الأزمات عن طريق نشر الشائعات عبر وسائل تقنية المعلومات، وهو ما قد يلقى صدى مجتمعي حيث يوجد للأزمة مؤيدين ومعارضون على المستوى الداخلي والخارجي، إذ منهم من يرغب في إنهاء الأزمة، ويوجد من يسعى إلى تفاقمها إذا كانت موجودة في الواقع، فهي جريمة تهدف في العموم إلى تهديد حالة الأمن العام للمجتمع، أو الإخلال به، في أي من مجالاته المختلفة بشكل يؤدي إلى المساس في النهاية بالنظام العام.[1]

4- صعوبة اكتشاف الجريمة واثباتها

تتسم الجرائم الإلكترونية بأنها من الجرائم المخفية، إذ أن هناك صعوبة في اكتشاف والاستدلال على مرتكبيها، حيث أن الجناة لا يتركون أثراً مادياً يمكن من خلاله التعرف عليهم بخلاف الجرائم التقليدية، كما أن مباشرة التحقيق والاستدلال يحتاج إلى دراية كبيرة بتقنية المعلومات مما يتعذر على الأجهزة الضبطية التعامل معها. فعادة ما يتم اكتشاف الجريمة الإلكترونية بمحض الصدفة، ويُرجع السبب في ذلك إلى عدم ترك الجناة أثراً خارجياً مرئياً؛ لأنها من الجرائم التي تتسم باللاعنف فتنصب على البيانات والمعلومات المخزنة في نظم الحواسيب ووسائط التخزين عبر تغييرها أو حذفها أو نسخها، فيؤدي إلى محو أي أثر كتابي. فالجريمة الإلكترونية لا عنف فيها ولا آثار للاقتحام المادي، وإنما هي أرقام وبيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحاسبات.[2]

كما أنَّ الصعوبة في إثبات الجريمة الإلكترونية عادةً ما تُمكن الجُناة مرتكبي تلك الجرائم الذين يتسمون بالذكاء والدهاء والخبرة أثناء ارتكابها من الإفلات من العقاب، إضافة إلى عدم ملائمة الأدلة والتقنية الواردة في القانون الجنائي التقليدي لأكتشافها أو إثباتها.[3] فصعوبة إثبات هذه الجريمة يرجع إلى عدة أسباب من بينها وسيلة تنفيذها والتي تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد. بالإضافة إلى الإحجام عن الإبلاغ عنها في حالة اكتشافها لخشية المجني عليه من فقد ثقة عملائه، فضلاً عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الواحدة.[4]

5- خصوصية الجاني المعلوماتي

تختلف الجرائم الإلكترونية عن الجرائم التقليدية بأنه لا يرتكبها مجرم عادي، بل يرتكبها أشخاص يمتلكون مهارة تقنية وخبرة في مجال الحاسب الآلي والشبكات، وهو الأمر الذي يُضفي الطابع الاحترافي على كل من يرتكب هذه الجريمة،

[1] – محمد علي سويلم، مكافحة الجرائم الإلكترونية (دراسة مقارنة بالتشريعات العربية والأجنبية)، مرجع سابق، ص 116.
[2] – معاشي سميرة، الجريمة الإلكترونية (دراسة تحليلية لمفهوم الجريمة المعلوماتية)، مجلة الفكر، العدد 17 يونيو 2018، ص 412-413.
[3] – محمد عبد الله أبوبكر سلامة، جرائم الكمبيوتر والانترنت، منشأة المعارف، 2006، ص 99.
[4] – هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، 1992، ص 55.

مما يزيد مهمة ضبطه صعوبةً وتعقيداً، خاصة في ظل التطور المطرد في الوسائل التقنية، والذي يجعل من طرق ارتكاب تلك الجرائم أمراً ميسور الحصول عليه عن طريق المواقع الإلكترونية ووسائل التواصل الاجتماعي.[1]

ويُصنف مجرمي الجرائم الإلكترونية إلى مجرمين مخترقين ومحترفين وحاقدين، فالمخترق مثل الهاكرز يعد شخصاً بارعاً في استخدام الحاسب الآلي، وغالباً ما يكون لدى المجرم المخترق فضول في استخدام حسابات الآخرين بطرق غير مشروعة. أما المحترفون فهم الأكثر خطورة بين مجرمي الانترنت، حيث أنهم يمتلكون مهارات تُمكنهم من عدم ترك أي دليل خلفهم يُمكن من خلاله ملاحقتهم أو تتبع أعمالهم الإجرامية، ويهدف البعض منهم إلى الاعتداء لتحقيق الكسب غير المشروع، وذلك عبر الدخول إلى حسابات البنوك، والبعض الآخر يدخل من أجل تحقيق أغراض سياسية، والتعبير عن وجهة نظر أو فكرة، وبالنسبة لفئة الحاقدين فهم ليس لديهم أهداف للجريمة ولا يسعون لتحقيق مكاسب سياسية أو مادية، لكن يتحركون لرغبة الانتقام والثأر كالأمور الطائفية.[2]

6- سُرعة تنفيذ الجرائم الإلكترونية

تتصف الجريمة الإلكترونية بأنها من الجرائم سريعة التنفيذ، ما يزيد من خطورتها على الأمن القومي للدولة، حيث أنه لا يستغرق تنفيذها عبر الكمبيوتر وقت طويل، ولكن هذا لا يعني أنها لا تتطلب الإعداد لها قبل التنفيذ أو استخدام معدات وبرامج معينة.

وغالباً ما يتمثل الركن المادي فيها بالضغط على مفتاح معين في جهاز الحاسب الآلي، مع إمكان تنفيذ ذلك عن بُعد دون اشتراط التواجد في مسرح الجريمة، ولهذا فإن الجريمة الإلكترونية ولسهولة ارتكابها شكلت عنصر إغراء للمجرمين؛ إذ أن ارتكابها لا يتعدى سوى توفر إمكانية استغلال التكنولوجيا والتقنية الحديثة، خُصوصاً عندما يكون الجاني موظفاً عاماً، أو في إحدى الشركات التي تعتمد على الحاسب الآلي في طبيعة عملها المتعلق بالمعلومات أو الأموال بحيث يكون لديها كافة المعلومات اللازمة لتحقيق اختراقات متعددة ومتتالية لأنظمة الحاسب الآلي في الشركة وتحقيق أرباح طائلة.[3]

ثالثاً: البنيان القانوني للجرائم الإلكترونية

يتكون البنيان القانوني لأي جريمة من مجموعة أركان لا تقوم الجريمة إلاَّ بتوافرها، وتبعاً لذلك اشترط المشرع الجنائي الليبي لقيام الجريمة الإلكترونية جُملة من الأركان يُبنى عليها الكيان القانوني لها، وينتفي هذا الكيان بانتفائها أو تخلفها، وتتمثل هذه الأركان في الآتي:

---

[1] – مُحَمَّد عبد الله طالب، التحريض على جرائم أمن الدولة من جهة الداخل، دار الفكر والقانون – القاهرة، 2010، ص 40.

[2] – إبراهيم خالد ممدوح، الجرائم المعلوماتية، دار الفكر الجامعي – الإسكندرية، 2009، ص 78.

[3] – مُحَمَّد علي سويلم، مكافحة الجرائم الإلكترونية (دراسة مقارنة بالتشريعات العربية والأجنبية)، مرجع سابق، ص 32.

1–الركن الشرعي

يغلب على التشريعات الجنائية المعاصرة مبدأ أساسي وهو مبدأ " لا جريمة ولا عقوبة إلا بنص "،[1] وهو ما يُسمى بمبدأ " شرعية الجريمة والعقوبة ". ومفاد هذا المبدأ أن يكون السلوك وقت اقترافه مُجرَم بنص قانوني بالإضافة للعقوبة إزاء الفعل المرتكب سواء ورد النص على تجريم الفعل في قانون العقوبات أو في أي قانون آخر. ويتمثل جوهر الركن الشرعي في تجريم الاعتداء على المصلحة محل الحماية الجنائية؛ فالجريمة في نظر الفقه لا تقوم بمجرد المخالفة الشكلية لنص التجريم، وإنما يجب أن يتعارض الفعل مع المصلحة المحمية بذات النص التجريمي، فإذا لم يكن هناك تعارض انتفت صفة عدم المشروعية عن الفعل، أي انتفى الركن الشرعي وبالتالي تنتفي الجريمة.

ونظراً لحداثة وخطورة الجرائم ذات الطابع المعلوماتي (الإلكتروني) فإن هناك من النظم القانونية التي اتجهت إلى سن قانون خاص لمكافحة الجريمة الإلكترونية، كمل فعل المشرع الإماراتي، حيث عالج الجريمة المعلوماتية في المرسوم (5) لسنة 2012، في حين اتجهت نُظم قانونية أخرى إلى مكافحة الجريمة الإلكترونية عبر تعديل قانون العقوبات، كما فعل المشرع الجزائري، حيث أضاف القسم (السابع مكرر) نُصوص عقابية عن صور الجريمة الإلكترونية وعقوباتها وحالات تشديد العقوبة.[2]

أما بالنسبة للمشرع الليبي – كما قلنا سابقاً – فإنه عالج الجريمة الإلكترونية في قانون خاص، والمتمثل في القانون رقم (5) لسنة 2022 بشأن الجرائم الإلكترونية والذي حدد فيه جرائم التعدي على عمل النظام المعلوماتي، وبرامج وشبكات المعلومات والمواقع الإلكترونية، وغيرها من الجرائم المعلوماتية الماسة بأمن الدولة القومي والسلامة العامة للمجتمع المتمثلة في مساعدة الجماعات الإرهابية، والتنصت غير المشروع، وتعطيل الأعمال الحكومية، وغسل الأموال، والتزوير والاحتيال الإلكتروني، وجرائم بطاقة التعامل الإلكتروني، وجرائم التعدي على الحقوق الفكرية.

2– الركن المادي

يقوم الركن المادي لأي جريمة على ثلاث عناصر وهي السلوك الإجرامي والنتيجة التي يُعاقب عليها المشرع، ووجود علاقة سببية تربط بين كل من السلوك الإجرامي والنتيجة. لكن في جرائم المعلوماتية يبقى التساؤل المطروح في هذا الصدد؛ هل عنصر السلوك الجُرمي المتطلب في كافة الجرائم التقليدية ينطبق أيضاً على الجريمة الالكترونية محل البحث؟ لا سيما أن الجاني في هذه الأخيرة يختلف عن الجاني في غيرها من الجرائم من حيث كونه ذو خبرة كافية في مجال استخدام

[1] – المادة (1) من قانون العقوبات الليبي لسنة 1953م.

[2] – تم إضافة القسم السابع لقانون العقوبات الجزائري الصادر عام 1966 وذلك في عام 2004، وقد تضمن القسم المذكور ثماني مواد، تضمنت حالات التجريم والعقاب، وحالات تشديد العقوبة.

التقنيات الحديثة.[1] ناهيك عن أن السلوك الجرمي الذي سيصدر منه في مجال ارتكاب الجريمة الالكترونية حتماً سيختلف عن الجاني التقليدي. إلا أنه لا مناص من التسليم بضرورة توافر هذا العنصر لقيام الركن المادي للجريمة الالكترونية، إذ يكادُ يكونُ هذا العنصر هو ما يميزها عمَّا سواها من الجرائم التقليدية الأخرى، فمثلاً نجد السلوك الإجرامي في جريمة الإرهاب الإلكتروني تتمثل في إطلاق صفحات أو مواقع تدعو وتُحرض على الإنضمام لمثل هذه الجماعات، أو مثلاً تبين كيفية صنع قنابل.

وباستقرائنا لقانون الجرائم الإلكترونية نجد أن المشرع الليبي قد اكتفى بالسلوك الإجرامي المجرد لقيام الركن المادي بصرف النظر عن العلاقة السببية والنتيجة، حيث اعتبر أن مجرد الدخول غير المصرح به جريمة كاملة، وهذا ما نصت عليه المادة (5) من قانون الجرائم الإلكترونية بأن (المواقع الإلكترونية وأنظمة المعلومات الرقمية ملك لأصحابها لا يجوز الدخول إليها أو إلغائها أو حذفها أو اتلافها أو تعطيلها أو تعديلها أو نقل أو نسخ بياناتها دون موافقة مكتوبة أو إلكترونية صريحة من مالكها). وأيضا المادة (11) التي قضت بأنه (يعد الدخول لأجهزة وأنظمة الحاسب الآلي أو إلى نظام معلوماتي أو شبكة معلوماتية أو موقع الكتروني غير مشروع، إذا تم الاختراق بشكل مُتعمد لوسائل وإجراءات الحماية لها بشكل كُلي أو جزئي دون تصريح أو بما يُخالف التصريح).

وهذا ما سلكه المشرع الأردني لقيام الركن المادي للجريمة، إلا إذا كان الجريمة تتطلب تحقيق نتيجة معينة، وذلك بمُوجب المادة (65) من قانون العقوبات رقم (16) لسنة 1960 بأن (لا عبرة بالنتيجة إذا كان القصد أن يؤدي إليها ارتكاب الفعل إلا إذا ورد نص صريح على أن نية الوصول إلى تلك النتيجة تُولف عنصراً من عناصر الجُرم الذي يتكون كله أو بعضه من ذلك الفعل).

نعتقد بحق إنه يتطلب في النشاط أو السلوك المادي في جرائم الانترنت وجود بيئة رقمية واتصال بالانترنت، ويستلزم أيضاً معرفة بداية هذا النشاط والشروع فيه ونتيجته. وفي هذا الصدد نرى بأن العلاقة السببية للجريمة الإلكترونية تتحقق حينما يقوم الجاني بربط جهاز الحاسوب بالانترنت ومن ثم القيام باختراق الأجهزة الأخرى أو اختراق المواقع الإلكترونية واستيلاءه على البيانات حينما يتم نسخها أو نشرها.

ولا تستلزم كل جريمة أعمال تحضيرية؛ إذ في حقيقة الأمر يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في جرائم الكمبيوتر والانترنت حتى ولو كان القانون لا يُعاقب على الأعمال التحضيرية، إلا أنه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشيء فشراء برامج اختراق ومعدات لفك الشفرات وكلمات المرور، وحيازة صور دعارة للأطفال تُمثل جريمة في حد ذاتها.[2]

3- الركن المعنوي

[1] – هروال، نبيلة هبة، الجوانب الاجرائية لجرائم الانترنت، دار الفكر الجامعي، الطبعة الأولى، 2007، ص45.

[2] – مُحَمَّد علي سويلم، مكافحة الجرائم الإلكترونية (دراسة مقارنة بالتشريعات العربية والأجنبية)، مرجع سابق، ص 54.

لتوقيع العقوبة لا يكفي أن يقوم الفاعل بارتكاب الفعل المكون للجريمة أي الركن المادي فيها، وإنما يُلزم فوق ذلك أن يتوافر الركن المعنوي اللازم لقيام المسؤولية الجنائية. وعليه فإن الجريمة المعلوماتية (الإلكترونية) كغيرها من الجرائم تتطلب بالأساس وجود القصد الجنائي العام بعنصريه (العلم، والإرادة) لتحديد وقيام المسؤولية الجنائية، فعلم الجاني يجب أن ينصرف إلى إدراك إرتكابه للنشاط الالكتروني غير المشروع المكون للجريمة الالكترونية كما تطلبها النص التجريمي، علاوةً على اتجاه إرادته المعتبرة قانوناً إلى تحقيق ماديات الجريمة كما تطلبها القانون.

وتأسيساً على ما سبق، يرى الباحث بأن الجريمة الإلكترونية هي تُعد أحد صور الجرائم العمدية، حيث لا يتصور إتيان هذا النوع من الإجرام على سبيل الخطأ. فالمجرم الإلكتروني عندنا يتوجه إلى ارتكاب فعل غير مشروع فهو يعلم بأركانها. وبالرغم من أن بعض المخترقين يُبررون أفعالهم بأنهم مُجرد فضولين، وأنهم قد تسللوا صُدفة، فلا انتفاء للعلم كعنصر للقصد الجنائي، وأنه كان يجب عليهم أن يتراجعوا بمجرد دخولهم ولا يستمرون في الاطلاع على أسرار الأفراد والمؤسسات؛ لأن جميع المجرمين والأشخاص الذين يرتكبون هذه الأفعال يتمتعون بمهارات عقلية ومعرفية كبيرة؛ وعليه فإن القصد الجنائي العام متوافر في جميع الجرائم الإلكترونية دون استثناء. ولكن هذا لا يحُول دون ضرورة قيام القصد الجنائي الخاص في بعض الجرائم الإلكترونية التي يتطلب المشرع توافره لدى الجاني لقيامها، مثل جرائم التشهير وتشوية السمعة على الانترنت، وجرائم نشر الفيروسات عبر الشبكة، وفي كل الأحوال يرجع الأمر في تحديد وجود هذا العنصر للسلطة التقديرية لقاضي الموضوع.[1]

وبما أن الركن المعنوي للجريمة الإلكترونية يتطلب توافر العنصرين (العلم والإرادة)، نتساءل حول مدى كفاية هاذين العنصرين لقيام هذه الجريمة، أم يستلزم الأمر توافر الركن المفترض، وهو إجادة الفاعل لأنظمة الحاسوب لكي يتم محاسبته ؟.

بالنظر إلى نصوص قانون رقم (5) لسنة 2022 بشأن الجرائم الإلكترونية نجد أن المشرع الليبي لم يشترط لقيام هذه الجريمة توافر الركن المفترض، وهو بذلك قد سار على نفس اتجاه المشرع الإماراتي وذلك في المرسوم بقانون رقم (5) لسنة 2021 حيث نص على أن مجرد الدخول غير المصرح به إلى أنظمة المعلومات جريمة، وبالتالي لم يشترط توافر الركن المفترض.

وعلى اعتبار أن الجرائم الإلكترونية لم تعرفها المجتمعات إلا منذ أمدٍ قريب، وأنها تختلف في طبيعتها عن الجرائم التقليدية؛ لأنها تكون في بعض الأحيان عابرة للحدود ويستطيع المجرم التخفي خلف أسوار شبكات الانترنت وأجهزة الحاسوب، علاوة على إمكانية المجرم محُو آثار الدخول غير المصرح به مما يعكس الصعوبة في إثباتها، لذا تقتضي المصلحة

[1] – مهداوي حنان، التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري، مجلة الفكر القانوني والسياسي، المجلد السادس، العدد 22 نوفمبر 2022، ص 1067.

العامة بعدم اشتراط ركن مفترض؛ لأن الأخير يُضيق من نطاق التجريم إلى حين البحث عن آليات ناجعة لمواجهة تلك الجريمة الخطيرة متعددة الأبعاد.[1]

المبحث الثاني: صور الجرائم الإلكترونية الماسة بأمن الدولة القومي

تطرح مسألة الأمن نفسها وبقوة من بين المسائل الحيوية في المجتمعات المعاصرة، والتي تعرف تحولات وتواجه تهديدات أمنية متنامية في مجال الجرائم الالكترونية والجرائم الإرهابية العابرتين للحدود، خاصة وأن وسائل الاتصال الجديدة في عصر المعلومات ولا سيما الشبكات الاجتماعية أصبحت تُسهل من عملية نشر المعلومات الصحيحة منها أو الزائفة، والتي قد تُنمي الشعور بانعدام الأمن.[2] حيث لم تعُد الجرائم الإلكترونية متعلقة بالذمة المالية أو الحياة الخاصة للأفراد، بل أصبح لها تأثير واسع على الأمن القومي للدولة.

ولا شك في أن الجريمة الإلكترونية بصوُرها المختلفة تُمثل أحد أهم العناصر المهددة لكيان الدولة، وزعزعة أمنها واستقرارها عبر مختلف الأنشطة والأعمال التخريبية المعادية، والتي تستهدف أجهزة ومؤسسات الدولة وأنظمة معلوُماتها الحسّاسة من خلال محاولة التأثير على تلك البرامج وتخريبها وتعطيلها، مما يخلق حالة من الفوضى والاضطراب الذي غالباً ما يضر بأجهزتها الدولة القومية[3] ويعمل على شللها واضعافها.

كما تتزايد خطورة الجرائم الإلكترونية أكثر في البُلدان التي تعرف اضطرابات أمنية مستمرة، كليبيا مثلاً التي شهدت ما يزيد عن عقد من الزمن حالة من الفوضى وعدم الاستقرار السياسي، نتيجة الصراع على السلطة الذي أفضى إلى انقساماً سياسياً حاداً وفراغاً أمنياً مما انعكس على الحياة العامة في البلاد، فاستشرت جميع أنواع الجرائم ومن بينها الجرائم الإلكترونية التي ساهمت وبشكل كبير في نشر الإشاعات وبث الفرقة واشتعال فتيل الحروب الداخلية بين الفرقاء الليبيين.

وتأسيساً على ما سبق، هناك العديد من التهديدات والمخاطر المحتملة الواقعة على أنظمة المعلومات وبصفةٍ خاصة أمن المعلومات، سواءً تعلق الأمر بتلك التهديدات والمخاطر المرتبطة بالداخل أو حتى احتمالية الاختراقات التي يكون مصدرها خارجي، مما يؤدي في نهاية المطاف إلى اختراق حسابات وبيانات الأشخاص والكيانات إلكترونياً بطريقة غير مشروعة نتيجة التغرات الأمنية المصاحبة لتلك القواعد البيانية والقُصور في إجراءات الحماية.[4]

---

[1] – علي حمزة عسل الخفاجي، السياسة الجنائية للمشرع الجزائي في حماية الأمن السيبراني، الطبعة الأولى، دار مصر للنشر والتوزيع، 2024، ص 56.

[2] – خالد أحمد مُحَّد ابزيم، الضبط الإداري وإشكالية التوازن بين حفظ الأمن العام وضمان حقوق الأفراد وحرياتهم في التشريع الليبي، ورقة بحثية مقدمة للمؤتمر العلمي الدولي حول السياسات الأمنية في ليبيا بين الواقع والمأمول، أغسطس 2023، ص 401.

[3] – يُعرف الأمن القومي بأنه " تأمين كيان الدولة ضد الأخطار التي تُهددها داخلياً وخارجياً، وتهيئة مصالحها، وتهيئة الظروف المناسبة لتحقيق أهدافها وغاياتها القومية"، للتوضيح أكثر أنظر: علي الدين هلال، الأمن القومي العربي (دراسة في الأصول)، مجلة شؤون عربية، العدد 35، يناير 1984، ص 6.

[4] – رياض بن عربية، الأبعاد الإستراتيجية للجرائم الإلكترونية وتهديداتها للأمن الوطني، مجلة دفاتر البحوث العلمية، المجلد 9، العدد 1 لسنة 2021، ص 273.

ولعله من الأهمية بمكان الأشارة إلى أنَّ صور حدوث الجريمة الالكترونية تتعدد وتختلف بحسب اختلاف الوسائل المستخدمة والجهات المسؤولة في ارتكابها، وعليه؛ فقد حدد المشرع الليبي بعض صور الجرائم الإلكترونية الماسة بأمن الدولة القومي في قانون الجرائم الإلكترونية رقم (5) لسنة 2022، وسنبين بشيءٍ من الإيجاز –غير المخل– كل تلك الصور وفقاً لما يلي:

أولا: جريمة الإرهاب الإلكتروني

يُعتبر الإرهاب الإلكتروني من أخطر الجرائم العصرية التي تُعاني منها جميع المجتمعات، والتي يستخدم فيها المهاجمون وسائل التكنولوجيا الحديثة للوُصول إلى أهدافهم الخبيثة، ويُعرف الإرهاب الإلكتروني بأنه " العُدوان أو التخويف أو التهديد المادي والمعنوي باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد عبر الفضاء الإلكتروني". وتكمُن خطُورة هذا النوع من الإرهاب الإلكتروني في سهُولة استخدام هذا السلاح مع شدة أثره وضرره، حيث يقوم مستخدمه بعمله الإرهابي وهو في منزله أو مكتبه، أو في أي مكان آخر يستطيع من خلاله تنفيذ فعله الإجرامي، ومما يسهل من ذلك أن هذا النوع من الإرهاب يعتمد على البرمجيات والانترنت كسلاح له.[1]

وبناء على ما سبق، يُمكن القول أن المشرع الليبي قد تفطن لمخاطر وتهديدات جرائم الإرهاب الإلكتروني على كيان المجتمع والدولة، فعمد على تجريمها في قانون خاص يهدف إلى مُكافحة الجرائم الإلكترونية،[2] حيث أشارت المادة (45) منه بأنه (يُعاقب بالسجن كُل من أنشأ موقع أو نشر معلومات على شبكة المعلومات الدولية أو إحدى الوسائل الإلكترونية لجماعة إرهابية تحت مُسميات تمويهية لتسهيل الاتصالات بقيادتها، أو أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة، أو أية أدوات تستخدم في أعمال محظورة).

وفي إطار مُكافحة الأعمال الإرهابية تصدى أيضاً المشرع الليبي لظاهرة الإرهاب الإلكتروني وذلك بمُوجب المادة (15) من القانون رقم (3) لسنة 2014 بشأن مكافحة الإرهاب التي نصت بأنه (يُعاقب بالسجن مدة لا تقل عن خمس سنوات ولا تزيد عن عشر سنوات، كل من قام بالدعاية أو الترويج أو التضليل للقيام بواسطة الرسائل أو المواقع الإلكترونية، أو بأي وسيلة من وسائل البث أو النشر أو بواسطة الرسائل أو المواقع الإلكترونية التي يُمكن للغير الإطلاع عليها، وتُشدد العقوبة لتكون السجن مدة لا تزيد عن خمسة عشر سنة، إذا كان الترويج داخل دور العبادة أو بين القوات المسلحة أو الشرطة، أو في الأماكن الخاصة بهذه القُوات).[3]

وفي ذات السياق نجد أن التشريعات المقارنة هي أيضاً عمدت على تجريم الأعمال الإرهابية التي تُستخدم فيها الوسائل الإلكترونية، ومنها المشرع الكويتي الذي يُعاقب "كُل من أنشأ موقعاً لمنظمة إرهابية أو لشخص إرهابي أو نشر

[1] – أسامة صلاح محمود الماحي، الجرائم المعلوماتية المُهددة للأمن القومي المصري، مجلة البحوث القانونية والاقتصادية – المنوفية، العدد 1/ 57، 2023، ص 79.

[2] – القانون رقم (5) لسنة 2022 بشأن الجرائم الإلكترونية، نشر في الجريدة الرسمية، العدد 1، 27 سبتمبر 2022.

[3] – القانون رقم (3) لسنة 2014 بشأن مكافحة الإرهاب، نشر بتاريخ 9 سبتمبر 2014.

عن أيهما معلومات على الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات ولو تحت مسميات تمويهية".[1] وسار على نفس الاتجاه المشرع الإماراتي الذي جرم كل من يقوم بإنشاء موقعاً إلكترونياً أو من يقوم بنشر معلومات أو أخبار او رسوم باستخدام شبكة المعلومات ووسائل تنقية المعلومات بقصد إحداث ضرر بأمن الدولة وتعريض مصالحها للخطر.[2]

وبناء على ما تقدم من النصوص السابقة نلاحظ مدى التطابق بين قانون الجرائم الإلكترونية الليبي و القانونين الإماراتي والكويتي من حيث تجريم أغلب –إن لم نقل كل– صور السلوك الإجرامي التي تؤدي إلى قيام جريمة الإرهاب الإلكتروني، ما يدل على حجم التهديدات الأمنية التي تحدثها هذه الصورة من الجرائم الإلكترونية، حيث باتت الجماعات الإرهابية الإجرامية تستغلُ وسائل تقنية المعلومات في نشر الشائعات والأخبار الزائفة والمغلوطة عن الدول والحكومات، وذلك في محاولة منها لتأليب الرأي العام، وبث الفتن في المجتمع، ويعد هذا الأمر هو البيئة المناسبة لنمو وانتشار هذه الجماعات.[3] وهو بالفعل ما حصل في ليبيا بعد احداث عام 2011 عندما توغلت الجماعات الإرهابية داخل المدن والقُرى مُستغلة الوضع الأمني الهش آنذاك في البلاد، فقامت بعميات إرهابية متعددة في بعض المناطق الليبية مستخدمة وسائل الاتصال وتقنية المعلومات المختلفة بغية تحقيق أهدافها بالسيطرة على أجزاء كبيرة من الدولة.

ثانياً: الدخول غير المشروع للنظام المعلوماتي (الاختراق الإلكتروني)

يعد فعل الاختراق هو المحور الرئيسي للركن المادي في هذا النوع من الجرائم فهو – أي الاختراق الالكتروني– يُعد من أكثر صور الجرائم الإلكترونية شيوعاً، لذلك جرَم المشرع فعل الاختراق لذاته وبصورة مجردة، دون أن يترتب عليه نتيجة مادية، ودون أن يستهدف الجاني من ارتكابه غرضاً معيناً.

وتُعد من أبرز صور جرائم الإختراق الإلكترونية Hacking/trespassing تلك الأفعال التي تعمد إلى الدخول بدون وجه حق أو سبب مشروع إلى نظام ما أو جهاز كمبيوتر، وذلك لأسباب متعددة منها: التجسس ومعرفة معلومات سرية مُعينة، أو تشويه موقع إلكتروني أو شخص سواء كان طبيعي أو اعتباري، أو بغرض تغيير بعض البيانات والمعلُومات أو حذفها وغيرها من الأسباب، ويتم الإختراق عن طريق القراصنة (الهاكرز) الذين يستغلون ضعف الأنظمة التقنية لبعض مواقع التواصل الاجتماعي والمواقع الإلكترونية، فيقُومُون باستغلال الثغرات الأمنية في مزودات الويب وأنظمة التشغيل.[4]

[1] – المادة (10) من قانون رقم (63) لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات.

[2] – المواد (21 و23) من المرسوم بقانون الاتحادي رقم (34) لسنة 2021 الخاص بمكافحة الشائعات والجرائم الإلكترونية.

[3] – إسلام هديب، الأمن السيبراني (الهجمات السيبرانية والجرائم السيبرانية)، الطبعة الأولى، دار مصر للنشر والتوزيع، 2024، ص 304-305.

[4] – نرمين نبيل الأزرق، مُحددات المسؤولية الجنائية لجرائم الاختراق والاعتراض والانتحال وآليات الردع في التشريعات العربية في العصر الرقمي (دراسة تحليلية مقارنة)، مجلة البحوث الإعلامية، العدد 56 يناير لسنة 2021، ص 1059.

وقد عرف المشرع الليبي الاختراق بأنه " القدرة على الوصول إلى أي وسيلة لتقنية المعلومات بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاصة".[1] وعرّف أيضاً المشرع المصري فعل الاختراق بأنه "الدخول غير المرخص به أو المخالف لأحكام الترخيص أو الدخول بأي طريقة غير مشروعة إلى نظام معلوماتي أو حاسب آلي أو شبكة معلوماتية وما في حكمها".[2]

ويُفهم من التعريفات السابقة أن فعل الاختراق يعد مُرادفاً لفعل الدخول غير المشروع الذي قد يكون موجه للمعلومات والبيانات المخزنة على جهاز الحاسوب، مما يجعلها هدفاً للمُجرم المعلُوماتي عندما يقوم بتوجيه هجمات إليها مباشرة، حيث يسعى المخترق إلى زراعة الفيروسات لتدمير المعطيات والملفات المخزنة أو العبث فيها أو تعديلها، أو المساس بالمحتوى، أو قد تكون بهدف تعطيل القدرة والكفاءة للأنظمة الرقمية والمعلوماتية لمؤسسات الدولة، وهنا تقع الجريمة إما على المكونات المادية لنظام المعلومات أو البرامج المخزن عليها النظام المعلُوماتي. وقد يكون الإختراق بهدف الاستيلاء على البيانات والمعلُومات المخزنة أو المنقُولة عبر النظام، وينصب الاعتداء في الحالة الأخيرة على المعلومات باعتبارها هي المحور الأساس الذي تدور حوله عمل النظام المعلُوماتي، ومن صور هذه الجرائم التلاعب في المعلُومات أو سرقتها أو إتلافها.[3]

وبناء على ما سبق، فقد تولى المشرع الليبي بيان مفهوم عدم المشروعية في جريمة الاختراق الإلكتروني بموجب نص المادة (11) من قانون الجرائم الإلكترونية التي نصَّت على أنه (يعد الدخول لأجهزة وأنظمة الحاسب الآلي أو إلى نظام معلوماتي أو شبكة معلوماتية أو موقع الكتروني غير مشروع، إذا تم الاختراق بشكل مُتعمد لوسائل وإجراءات الحماية لها بشكل كُلي أو جزئي دون تصريح أو بما يُخالف التصريح).

ونلحظ من المادة السابقة بأن المشرع لم يشترط حدوث نتيجة مُعينة على هذا الاختراق، وغاية ما هنالك أنه اعتبرها من جرائم الخطر المجرد، ما يدُل على أن هذه الظاهرة تُشكل تهديداً على البيانات والمعلومات المخزنة في الحاسب الآلي والمواقع والأنظمة المعلوماتية، ومن ثم فإنها تمس الحياة الشخصية والأمن الداخلي والخارجي للدولة واقتصادها الوطني على حدٍ سواء. وهذا ما استدعى تجريم الاختراق المجرد لمواجهة هذه المخاطر والحد من آثارها وتحجيمها إلى حين القضاء عليها وعلى مُسبباتها.

والجدير بالذكر، نُلحظ أن المشرع غفل عن مسألة مهمة جداً في هذا الصدد، وهي عدم تحديده إن كان الاختراق واقعاً على موقع الكتروني حكومي أو موقع خاص. وهذا ما لم تُشرْ إليه المادة (11) من قانون الجرائم الإلكترونية، على خلاف التشريعين المصري والإماراتي اللذانِ جرّما اختراق المواقع الإلكترونية المملُوكة لأشخاص القانون الخاص والعام.

[1] – الفقرة الثانية من نص المادة (1) من قانون الجرائم الإلكترونية.

[2] – المادة (1) من القانون رقم (175) لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات.

[3] – أحمد جابر الجزار، الأمن السيبراني في ضوء قانون مكافحة جرائم تقنية المعلومات رقم (175) لسنة 2018، الطبعة الأولى، المجموعة العالمية للطباعة والنشر والتوزيع، 2024، ص 30.

ولعله من الأهمية بمكان الإشارة إلى أن جريمة الدخول غير المشروع طبقاً لنص المادة (11) سالف الذكر قد تضمن هذه الجريمة في صورتها التي تُرتكبُ بقصدٍ عمدي دون القصد الخطأ؛ ومن هنا نرى أن المشرع في هذا النص قد ضيق من النطاق التجريم باشتراط التعمد في الدخول غير المشروع، وهذا مسلك غير محمُود منه؛ لأنه قد يؤدي إلى افلات بعض المجرمين من العقاب. كما أن هذا الاتجاه الذي تبناه ذات المشرع يجعلنا نتساؤل هل تقوم هذه الجريمة في حق الشخص الذي يدخل بطريق الخطأ على المواقع والأنظمة المعلوماتية؟، وبعبارة أخرى ما هو مناط العقوبة بالنسبة للأشخاص الذين يدخلون بالخطأ إلى المواقع والأنظمة الإلكترونية من دون ترخيص؟ ولعلنا نُجيب على هذا التساؤل، بقولنا إن فعل الدخول غير العمدي (خطأً) للمواقع اللاإكترونية يُمكن اسناده إلى تطبيق القواعد العامة في هذا الشأن الواردة في قانون العقوبات الليبي.

وبالرجوع إلى نص المادة (12) نجد أن المشرع الليبي قد اعتمد على مبدأ التفريد في العقاب عندما ميَز في العقوبة المترتبة على فعل الإختراق على المواقع والأنظمة المعلوماتية، حيث نجد أنه نص على الظروف المُشددة للعقاب عن أفعال الدخول غير المشروع، فعمد إلى تخفيف العقوبة إذا نتج عن الدخول إلغاء أو حذف أو إضافة أو تدمير أو إفساد أو إتلاف أو حجب أو تعديل أو نقل أو نسخ بيانات أو تعطيل عمل نظام المعلومات أو تغيير موقع إلكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو انتحال شخصية مالكه، بينما شدَد العقاب في حالة نجم عن عملية الإختراق إعاقة عمل النظام المعلوماتي أو تعطيل الشبكة المعلوماتية أو عمل الموقع الإلكتروني أو إفساد محتوياتهم.[1] تبعاً لذلك أن التكييف القانوني للجريمة يُشدد، وتتحول من قيد ووصف الجنحة إلى قيد ووصف الجناية، بل وتُضاعف العقوبة بحسب الأحوال. ولكن في الحقيقة نستغرب من موقف المشرع الليبي حول هذه المسألة، حيث نرى أن هذه التفرقة لا مقتضى لها؛ لأن الأفعال الواردة في الفقرة الثانية من المادة (12) ليس أقل خطورة من الأفعال الأخرى الواردة في الفقرة الثالثة من نفس المادة، لذلك من الأجدر أن يكون التشديد شاملاً لهذه الصور ودون استثناء.

ثالثاً: جريمة التجسس المعلوماتي

عرفت ليبيا في السنوات الماضية تطوراً كبيراً في شكل وهيكلية بعض مرافقها العامة بتحولها من الطابع التقليدي إلى الطابع الإلكتروني المستحدث، مما جعلها عُرضة لظاهرة غير معهودة سابقاً تتمثل في التجسس الإلكتروني، أو نشر الوثائق الرسمية عبر المواقع الإلكترونية بشكل عام، أو مواقع التواصل الاجتماعي على وجه الخُصُوص، وطرحها للإطلاع ومُشاركتها والتعليق عليها، على الرغم من أنه يفترض في الكثير من هذه الوثائق أنها سرية وغير قابلة للإطلاع عليها من قبل العامة، وبعضها قد تكون وثائق رسمية ومهمة ذات طابع قضائي أو أمني أو سياسي أو اقتصادي ولأسباب تتعلق بالمصلحة العامة أو الحفاظ على الأمن القومي.

[1] – المادة (12) من قانون الجرائم الإلكترونية.

ويُعرف جانب من الفقه التجسس الإلكتروني بأنه " دخول الجاني إلى الشبكة المعلوماتية، أو نظام المعلُومات، أو موقع إلكتروني للحصول على محتوى إلكتروني غير مُتاح للجمهور، يمُس الأمن الوطني أو العلاقات الخارجية للدولة أو السلامة العامة أو الاقتصاد الوطني".[1]

وترتيباً على ما سبق، يعد التجسس من المجالات الخصبة للجريمة المعلوماتية، فهو يعتبر أحد الجرائم التي يُستخدم في ارتكابها الحاسب الآلي، ويتسع التجسس في مجال المعلُوماتية ليشمل أنماطاً مُتعددة من المعلُومات قد تتعلق بأسرار الدولة في العديد من المجالات، ولا سيما الدفاع أو المعلومات الصناعية؛ ولا شك أن التقدم الكبير الذي لحق بالاتصالات والحاسبات الآلية نجم عنه إيجاد وسائل أكثر فاعلية للتجسس، وهو ما اسفر بدوره عن ظهور ما يُسمى بالتجسس المعلوماتي.[2]

وعلى أية حال؛ فإن شيوع أساليب وتقنيات ظاهرة التجسس على شبكات الاتصال المعلوماتية؛ يستلزم بالضرورة وضع نصوص قانونية تحد من هذه الجريمة، لا سيما أن النصوص التقليدية في هذا المجال لا تنطبق إلا على التقاط المراسلات الشفوية والمحادثات التي تتم بين الأشخاص. وعلى هذا الأساس جرَم المشرع الليبي فعل التصنت غير المشروع، بموجب قانون الجرائم الإلكترونية، بنصه على إنه (يُعاقب بالحبس مدة لا تقل عن سنة كُل من تصنت لصالح نفسه أو لصالح غيره على الاتصالات التي تُجرى عبر شبكة المعلومات الدولية أو أي وسيلة إلكترونية أخرى، وتكُون العقوبة السجن إذا كان التصنت بقصد الحصول على أسرار حكومية أو أمنية أو عسكرية أو مصرفية، فإذا نشر الأسرار المذكورة بالفقرة السابقة عبر شبكة المعلومات الدولية أو أي وسيلة إلكترونية أخرى أو مكّن شخص أو جهة أخرى من الحصول عليها تكون العقوبة السجن المؤبد).[3]

وهنا نُلاحظ أن المشرع شدَد العقوبة في حالة كان الغرض من التصنت الحصول على أسرار تمس الأمن القومي، وبوصفها جريمة مُشددة ضاعف المشرع الجنائي العقوبة أكثر في حالة تم نشر هذه الأسرار السرية عبر الشبكات المعلُوماتية أو بأي وسيلة إلكترونية أو في تمكين وتسهيل الغير من الوصول إليها. وهذا المسلك إن دلَّ على شيء، فإنما يدلُ على إدراكه لخطورة هذه الأفعال التي تُشكل خطراً على الأمن والسلامة العامة للدولة.

ولا ريب في أن فعل الأعتراض أثناء نقل المعلُومات والبيانات عبر الشبكات يعد تجسس معلوماتي، وخير ما قام به المشرع الليبي في هذا الصدد عندما عاقب على سلوك الاعتراض الذي يرتكبه الجُناة، حيث نص على أنه (يُعاقب

[1] – علي عوض الجيرة وآخرون، أثر الجريمة الإلكترونية على سير المرافق العامة الإلكترونية في التشريع الأردني، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد 21، العدد 2 لسنة 2021.

[2] – علي حمزه عسل الخفاجي، السياسة الجنائية للمشرع الجزائي في حماية الأمن السيبراني، دار مصر للنشر والتوزيع، الطبعة الأولى، 2024، ص 102.

[3] – المادة (47) من قانون الجرائم الإلكترونية.

بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن 1000 ألف دينار ولا تزيد على 5000 خمسة آلاف دينار كُل من اعترض نظاماً معلوماتياً بقصد الحصول على بيانات رقمية أو للربط مع أنظمة إلكترونية أخرى).[1]

وبما أن الجريمة الإلكترونية من جرائم الخطر فأن المشرع لم يكتفي بتجريم فعل الاعتراض غير المصرح به للبيانات والمعلُومات، إنما جرَم أيضاً بيع أو تداول الوسائل التي تستخدم في فعل التعرض بأي صورة كانت، حيث قضى بمُعاقبة (كُل من قدم أو أنتج أو زرع أو استورد أو أصدر أو روج أو حاز بقصد الاستخدام غير المشروع جهازاً أو برنامجاً معلوماتياً أو أي بيانات معلُوماتية مُعدة لإظهار كلمات السر أو رموز الدخول أو لكسر الحجب، يُعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن 1000 ألف دينار ولا تزيد على 10000 عشرة آلاف دينار).[2]

رابعاً: جريمة الاعتداء وإتلاف المعلومات المملوكة لأجهزة ومرافق الدولة

إزاء التطورات السريعة لتكنولوجيا المعلومات والاتصالات التي جاءت لخدمة الإنسان، إلا إنه لم يُحسن البعض استخدامها، فقد أبانت ممارسات التعامل مع هذه الوسائل التكنولوجية الحديثة عن مخاطر استخدامها، حيث يقُوم الجُناة بارتكاب صور متخلفة ومُتعددة للإجرام تمُس سير المرافق العامة بانتظام، تتمثل هذه الصور في الإتلاف والتعدي الإلكتروني الممارس على أنظمة الحاسوب والمعلومات الخاصة بأجهزة الدولة ومؤسساتها.

ويُقصد بالإتلاف المعلومتي في مجال المرفق العام الإلكتروني بأنه "كل فعل من شأنه حذف أو إلغاء أو إزالة أو تدمير نظام معلوماتي مهمته تقديم الخدمات العامة بُغية إشباع رغبات الجمهور، حفاظاً على المصلحة العامة". بمعنى آخر كل ما يدخُل تحت مُسمى اعتداء تقني هدفه التغيير من سمات المرفق العام الإلكتروني وملامحه، إما بإزالة أو حذف أو تعديل برمجيات معينة بنحوٍ يُعطل أو يُوقف معه تقديم الخدمات العمومية.

وتتعد صور الإتلاف المعلوماتي: فمنها ما يؤثر على ماديات النظام المعلوماتي بتعطيلها أو ايقافها عن العمل، ومن هذه الصور الاعتداء على المعلومات بما يؤدي إلى إعاقة واعتراض النظام وتعطيله عن العمل، أو الاعتداء على المعلُومات المخزنة على المواقع الإلكترونية لمرافق الدولة بإضافة برمجيات معينة " فيروسات"؛ بُغية جعل تلك المعلومات والبيانات لا نفع لها ولا فائدة فيها.

وباستقرائنا لنصوص قانون الجرائم الإلكترونية، نجد أن المشرع الليبي حدد الركن المادي في جريمة إتلاف المعلومات والبيانات الإلكترونية الحكومية في أكثر من نص، منها ما جاء في المادة (5) التي منحت خصوصية للمواقع الإلكترونية بعدم الدخول إليها أو أو إلغائها أو حذفها أو إتلافها أو تعطيلها أو تعديلها أو نقل أو نسخ بياناتها دون موافقة مكتوبة وصريحة من مالكها. كما تناولت أيضاً الفقرة الثالثة من المادة (12) فعل الإتلاف المعلوماتي بنصها على تشديد العقوبة —كما قلنا سابقاً – في حال تسبب الاختراق غير المشروع للنظام المعلوماتي في إتلاف أي بيانات أو معلومات يتضمنها

[1] – المادة (13) من قانون الجرائم الإلكترونية.
[2] – المادة (14) من قانون الجرائم الإلكترونية.

النظام، وذلك برفع العقوبة السالبة للحرية والعقوبة المالية. ونظراً لأهمية الخدمات التي تقدمها المرافق القضائية للمواطنين عمد المشرع على حماية كل الأدلة القضائية الرقمية من الإتلاف والعبث وذلك بموجب المادة (36) التي نصت على معاقبة (.....كل من قام بإتلاف أدلة قضائية معلوماتية أو بإخفائها أو التعديل فيها أو محوها أو العبث بها بأي شكل من الإشكال).

ولعل من الأهمية بمكان الإشارة إلى جميع أشكال التعدي الأخرى على النظام المعلوماتي التي جرمها المشرع الليبي منها ما جاء في نص المادة (15) بمعاقبة (... كل من يقوم بصورة غير مشروعة بإلحاق ضرر مادي بغيره، عن طريق إدخال أو تبديل أو محو أو تدمير أو بيانات معلوماتية بأي شكل من أشكال التعدي على عمل النظام المعلوماتي، للحصول دون وجه حق على منفعة مادية لنفسه أو لغيره). وأيضا ما ورد في المادة (16) بمعاقبة (... كل من قام بصورة غير مشروعة بإدخال أو تبديل أو محو أو تدمير بيانات معلوماتية نتج عنها بيانات غير صحيحة، بقصد استخدامها أو التعويل عليها في أغراض قانونية، كما لو كانت هذه البيانات صحيحة سواء كانت هذه البيانات مقروءة ومفهومة بشكل مباشر أو غير مباشر،... وكل من قام باستعمال تلك البيانات المعلوماتية المنصوص عليها في الفقرة السابقة مع علمه بأنها صحيحة).

وتأسيساً على ما سبق، نلاحظ وبجلاء أن المشرع الليبي قد انتهج سياسة تجريمية تُوسع من نطاق التجريم لأفعال التعدي والإتلاف للأنظمة المعلوماتية، وهذا ما كان واضحاً عندما قام بإدخال بعض السلوكيات في دائرة جرائم التعدي والإتلاف المعلوماتي منها صورة التأثير في النظام الإلكتروني،[1] وأيضا الاعتراض أو التعرض المعلوماتي،[2] وأي فعل أخر يهدف منه الجاني إلى تعطيل أو عرقلة الأعمال الحكومية أو السلطة العامة عن طريق استخدامه لوسائل تقنية المعلومات.[3]

خامساً: جرائم التحريض والترويج للفِتن والشائعات

أصبحت مواقع التواصل الاجتماعي من أهم الوسائل التي ارتكزت عليها المخططات الإجرامية لنشر العنف والفوضى والأعمال الإرهابية، ونشر الشائعات والأخبار المغلوطة، وزعزعت القناعات الفكرية والثوابت العقائدية والمقومات الأخلاقية والاجتماعية التي من شأنها إحداث بلبلة وفوضى داخل المجتمع، مما جعلها تُشكل خطراً على الأمن القومي لكل الدول وبصفة خاصة الدول النامية.

ونظراً لنُقص الإمكانيات والتدابير لمكافحة هذه الظاهرة الخطرة على الأمن المجتمعي، لا سيما في الفترة ما بعد الربيع العربي، وظفت الجماعات الإرهابية المتطرفة، وبعض الأفراد من ذوي الأفكار الهدَامة وسائل التواصل الاجتماعي والتقينات الحديثة لإثارة الفتن وزعزعة أمن الدولة، بهدف بث الرعب في نفوس المواطنين.

[1] – المادة (10) من قانون الجرائم الإلكترونية.
[2] – المادة (13) من قانون الجرائم الإلكترونية.
[3] – المادة (34) من قانون الجرائم الإلكترونية.

ولا يُخفى على أحد أن حالة عدم الاستقرار السياسي والأمني داخل أي دولة غالباً ما تخلق بيئة خصبة لارتكاب مثل هذا النوع من الجرائم، لا سيما أن هذه الجرائم لم يجد الجُناة فيها صعوبة كبيرة لاقترافها. فليبيا بعد أحداث فبراير عام 2011 طغى على مشهدها الصراعات والحروب الأهلية، ولعل ما زاد في تأزم الوضع فيها هو استغلال ضعاف النفوس غياب حكم القانون وضعف الأجهزة الأمنية، فقاموا بارتكات جرائم مُستخدمين وسائل الاتصال الحديثة، ومن بين هذه الجرائم نشر معلومات أو أخبار غير صحيحة وكاذبة ساهمت وبشكل كبير في اشتعال فتيل الحروب ما بين الجماعات المسلحة بل حتى ما بين المناطق والقبائل، ومن ثم فإن هذه الأفعال بالضرورة ستُهدد أمن المجتمع واستقراره السياسي، وتُدمر كل مُرتكزات التنمية في البلاد.

وتأسيساً على ما سبق، حاول المشرع الليبي التصدي لكل الأفعال التي تُدخل في نطاق جريمة التحريض والترويج للفتن والشائعات والتي تتم باستخدام وسائل تقينة المعلومات، فهناك العديد من النصوص التي تتصل بمثل هذا النوع من العمل الإجرامي، أوردها ذات المشرع في قانونه الخاص بمكافحة الجرائم الإلكترونية، منها ما نصت عليه المادة (29) بأنه (يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن 1000 ألف دينار ولا تزيد عن 10.000 عشرة آلاف دينار كل من قام بنشر أو توزيع معلومات تُثير النعرات العنصرية أو الجهوية أو المذهبية التي تهدف إلى التمييز بين أشخاص معينين عبر شبكة المعلومات الدولية أو غيرها من الوسائل الإلكترونية). وفي إطار تعزيز حماية أمن الدولة وصيانة النظام العام من أي تهديد قد يقع نتيجة إثارة الفتن وترويج للشائعات المغرضة، نصت المادة (37) من ذات القانون على أنه (يُعاقب بالسجن مدة لا تقل عن خمس سنوات وبغرامة لا تقل عن 10.000 عشرة آلاف دينار ولا تزيد عن 100.00 مائة ألف دينار كل من بثّ إشاعة أو نشر بيانات أو معلُومات تُهدد الأمن والسلامة العامة في الدولة أو أي دولة أخرى من خلال شبكة المعلومات الدولية، أو استعمال أي وسيلة الكترونية أخرى). وخير ما فعل المشرع عندما شدد في العقوبة بالنسبة لأفعال الترويج في نشر الشائعات عبر وسائل التواصل الاجتماعي وتقنية المعلومات، حيث اعتبرها من الجرائم الجنائية، أي أنها من جرائم الخطر التي تُشكل تهديداً مباشراً على الأمن القومي الليبي.

الجدير بالذكر، أنه وبالرغم من الضغط الكبير الذي تمارسه المنظمات الحقوقية الدولية والوطنية على صانع القرار الليبي بإلغاء القانون رقم (5) لسنة 2022 بشأن الجرائم الإلكترونية، إلا أن المشرع استطاع إلى حدٍ ما تجريم الكثير من الأفعال التي تمس الحياة الشخصية والمصلحة العامة والأمن القومي للبلاد.

وفي ذات السياق، وصفت تلك المنظمات الحقوقية القانون قانون الجرائم الإلكترونية بأن" قانون قمعي"،[1] يعمل على تقييد وتجيم حقوق وحريات الأفراد. وأنه جاء بعبارات فضفاضة من قبيل (تهديد الأمن والسلامة العامة) مما يفتح المجال أمام السلطات ذات العلاقة تفسيرها بالشكل الذي يؤدي بالنتيجة إلى استهداف الصحافيين والمدافعين عن الحقوق

[1] – محمود قنديل، قانون رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية في ليبيا الحماية المفقودة والعقوبات المشددة، مجموعة بحوث، مركز مُدافع لحقوق الإنسان، سبتمبر 2023، ص 5.

والحريات المدنية والسياسية. أي وبعبارة أخرى يمنح القانون للسلطات الضبطية صلاحيات تقديرية واسعة لتقييد حرية التعبير والرأي والمعتقد عبر الانترنت وتجريمها على أساس النظام العام والآداب العامة. كما يُعطي القانون ايضاً حسب رأيها السلطات الليبية سُلطة الملاحقة القضائية على الأفعال المرتكبة في الخارج طالما امتدت تداعياتها داخل ليبيا، يشمل ذلك الأشخاص في البُلدان التي لا تعتبر هذه الأفعال غير قانونية.

وأخيراً نرى بأن نصوص التجريم الواردة في قانون رقم (5) لسنة 2022 المشار إليه والماسة بأمن الدولة باستخدام وسائل تقنية المعلومات شاملة لكثير من الأفعال، يكاد يكون مسلكاً طبيعياً من المشرع الذي حاول تضمين أكبر قدر ممكن من الأفعال حفاظاً على هيبة الدولة ومكانتها، حيث أن الحفاظ على مصلحة الدولة العُليا يستلزم اتساع الركن المادي ليشمل كل ما يحتمل أن يضر بهذه المصلحة.

المبحث الثالث: آليات مواجهة الجرائم الإلكترونية المُهددة للأمن القومي

على اعتبار أن جرائم الأمن القومي التي تُرتكب عبر وسائل تقنية المعلُومات من الجرائم الاستثنائية التي يسهل ارتكابها، وتُحقق أثراً يتعدى عادة الجرائم التقليدية، كان لزاماً التخطيط والاستعداد لمواجتها من خلال تبني طرق وآليات تواكبها في الحداثة، وتُناسب طُرق ارتكاب هذا النوع من الجرائم. وهو ما سنتاوله في هذا المبحث على النحو التالي:

أولا: إنشاء هيئات مُتخصصة في مجال حماية الأمن المعلوماتي

الكثير من التشريعات العربية التي جرَمت الأفعال التي تدخل في نطاق الجرائم الإلكترونية، رأت بأنه من الضروري تأسيس هيئات أو مجالس متخصصة في حماية الأمن المعلوماتي، وهذا نظراً للطبيعة التقنية لوسائل ارتكاب الجريمة الإلكترونية، وآثارها التي تكون مُدمرة في بعض حالات الاختراق سواء على أمن الدولة أو على اقتصادها.

وتأسيساً على ما سبق، وإسوة بالتشريعات المقارنة استحدث المشرع الليبي بموجب القرار رقم (28) لسنة 2013 الهيئة الوطنية لأمن وسلامة المعلُومات، حيث تهدف الهيئة إلى (توفير السياسات والمعايير الاستراتيجية اللازمة من أجل تأمين سلامة البيانات الرقمية ووسائل الاتصال، وكذلك توفير خدمات المصادقة الإلكترونية والتشفير، إلى جانب وضع وتنفيذ آليات الاستجابة الفورية للحوادث المتعلقة بشؤون تكنُولوجيا المعلُومات والاتصالات، وكذلك الاهتمام بشؤون حوكمة الانترنت ومجالاتها بالإضافة لدورها كمنسق لجميع شؤون أمن وسلامة المعلُومات والاتصالات على المستوى المحلي والدولي).[1]

وتتولى الهيئة الوطنية لأمن وسلامة المعلُومات العديد من المهام[2] والاختصاصات أبرزها في الآتي:

1- إعداد السياسات والاستراتيجات لرفع كفاءة مستوى أمن وسلامة الاتصالات والمعلُومات بشكل مستمر.

2- مراقبة الشبكات الوطنية وتطويرها لرفع من أدائها وللتأكد من سلامتها ومطابقتها للمعايير المعتمدة.

[1] – المادة (3) من قانون الهيئة الوطنية لأمن وسلامة المعلُومات.

[2] – المادة (4) من قانون الهيئة الوطنية لأمن وسلامة المعلُومات.

3- رفع مستوى الوعي والإدراك بمفاهيم أمن المعلُومات والمخاطر المحدقة بها.

4- وضع برامج تدريبية للرفع من قُدرات الكوادر الوطنية المتخصصة في مجال الأمن المعلُوماتي.

5- التصدي للهجمات التي قد تتعرض لها الشبكة المعلُوماتية وتحديد مصدرها.

6- التواصل والتعاون مع المنظمات الإقليمية والدولية المتخصصة في مجال أمن المعلومات.

7- ضمان سلامة المعاملات والمبادلات التجارية للخدمات المقدمة من الحكومة الإلكترونية.

وبناء على هذه المهام تلتزم كل الجهات الحكومية برفع مستوى أمنها المعلوماتي لحماية شبكاتها وأنظمتها وبياناتها الإلكترونية، والالتزام بما تصدرها الهيئة الوطنية لأمن وسلامة المعلُومات من سياسات وقرارات[1] وضوابط وإرشادات بهذا الشأن؛ كما تلتزم كافة الوزارات والقطاعات والدوائر الحكومية بتمكين الهيئة من مباشرة اختصاصاتها وتنفيذ مهامها بشكل كامل.[2] ونظراً للدور الذي تلعبه الهيئة في مواجهة الجرائم الإلكترونية يرى الباحث أنه من الضروري أن يلزم المشرع القطاعات الحكومية بإبلاغ الهيئة بأي خطر أو تهديد لأمنها المعلوماتي سواء كان واقع أو مُحتمل.

ثانياً: تعميم نظام شبكي إلكتروني كأحد آليات المُراقبة المعلُوماتية

هو نظام للمُراقبة بالكاميرات الذكية ومُزود ببرامج تغذية وتحليل للبيانات يختص ببرامج الاختراق، ذلك بوضع سيناريوهات مُحتملة لتعامل الحراسة مع الهجمات الإلكترونية، وذللك للمساهمة في الضبط الإداري لتلك الجريمة، ففي ظل التطور الهائل للكتنولوجيا أصبحت الكاميرات الذكية ذات ضرورة حتمية لرصد كافة مناحي الحياة، ترصد كُل حركة وساكنة لحفظ النظام والأمن، من خلال نظام تقني مُعقد يعتمد على سيناريوهات مُسبقة وتحليل للمعلُومات من خلال الذكاء الاصطناعي، فتقوم بمُراقبة كافة النظم المعلُوماتية من داخل النظام، لرصد أي نشاط غير طبيعي، فلتلك الكاميرات أهداف وقائية وتوجيهية، فمعرفة المهاجم بوجود الكاميرات يُساهم في تردده عن ارتكاب الجريمة، لذا بات من الضروري الاعتماد على تلك التقنية التي أصبحت عاملاً أساسياً في ضبط المنظومة الأمنية الإلكترونية.[3]

ثالثاً: استخدام خوارزمية الوساطة

تفترض هذه الخوازمية أن الشخص يُصبح مؤثراً وفعالاً أكبر كُلما كان الوسيط الذي يستخدمه أكثر فعالية في التواصل، حيث تُعتبر هذه الخوازمية أن الشخص إذا كان يتواصل بنفسه دون وسطاء فإنه يعدُو مؤثراً بصورة أكبر في المحيطين، وهي الخوازمية التي يُمكن استخدامها لمتابعة الحسابات الشخصية أو الصفحات التي يُديرها أصحابها بأنفسهم، وقياس تأثير هذه الصفحات في متابعيها.

[1] – المادة (5) من قانون الهيئة الوطنية لأمن وسلامة المعلُومات.

[2] – علي حمزه عسل الخفاجي، السياسة الجنائية للمشرع الجزائي في حماية الأمن السيبراني، مرجع سابق، ص 123.

[3] – أشرف السعيد أحمد، تكنولوجيا المعلّومات في المجال الأمني، دار الكتاب الحديث – القاهرة، 2020، ص 36.

وباستخدام الخوازميات يُمكن لتحليل المعلومات التي ترد عن طريق مواقع التواصل ورسم خريطة تصوريَة لمدى امتداد أثر الحسابات المشبُوهة مع رصد الظواهر التي تستجد عقب النشر وذلك للوقوف على العلاقة بين النشر والاستجابة، حيث تتحدد بموجب هذه العلاقة القدرة على التأثير، وقوة سُرعة الاستجابة، ومدى ردت فعل المتلقين لرسائل هذا الحساب التي يبثها عن طريق النشر، ويُمكن أيضاً تطوير خوارزميات لرصد الكلمات والعبارات المرتبطة بجرائم أمن الدولة، وهي السياسة الأمنية التي انتهجها موقع انستغرام بالنسبة لظاهرة التنمر حيث يستخدم خوارزميات الكشف عن الصور والمحتويات المكتُوبة التي تتضمن عبارات تدل على التنمر ليتناولها بالحذف.[1]

رابعاً: تدريب الموظفين

غالباً ما يكون الموظفون هم الحلقة الأضعف في الأمن المعلُوماتي، وعليه تحتاج الحكومات والمنظمات إلى برامج تدريبية واضحة ودقيقة لموظفيها على كيفية التعامل مع ممارسات الأمن المعلُوماتي، على أن يتضمن البرنامج التدريبي على طرق التعرف على رسائل البريد الإلكتروني المخادعة، وكيفية إنشاء كلمات مرور قوية، وكيفية الإبلاغ عن الأنشطة المشبوهة.

خامساً: الإطار الأمني / الحماية

تحتاج الحكومات والمنظمات إلى تطوير أمني شامل يتضمن سياسات وإجراءات ومبادئ توجيهية لحماية أنظتها ومعلُوماتها. ويجب أن يُغطي إطار العمل الأمني جميع جوانب الأمن المعلوماتي، بما في ذلك ضوابط الوصول وأمن الشبكة وتشفير البيانات والاستجابة للحوادث. وفي إطار تعزيز الأمن المعلُوماتي يتوجب على الحكومات التأكد من أن أنظمتها وبرامجها وتطبيقاتها مُحدثة بأحدث تصحيحات الأمان والتحديثات، وهو ما سيساعد في التخفيف من مخاطر الثغرات الأمنية المعروفة التي يُمكن لمجرمي الانترنت استغلالها.[2]

سادساً: التعاون الدولي

كما – قلنا سالفاً – أن الجرائم الإلكترونية لا تعتد بالحدود الإقليمية، حيث تُشكل مسألة متابعة وحفظ الأدلة المتعلقة بها تحدياً كبيراً، وذلك لارتباطها باختصاصات قضائية مُتعددة ذات نُظُم مُختلفة في حفظ الأدلة، لذلك تبرز الحاجة إلى ضرورة التعاون الدولي فيما بين سُلُطات الدولة التي ارتكبت فيها الجريمة الدولية والدولة التي عبر من خلالها النشاط الإجرامي، وسُلُطات الدولة التي نفذت فيها الجريمة.[3]

ولتحقيق أهداف التعاون الدولي يجب اتخاذ التدابير التالية:

[1] – سارة جريفيت، هل يُمكن للتكنولوجيا أن تضع حداً للتحرش والتنمر، ترجمة مُحَمَّد أحمد أمين، دار المكتب الحديث – القاهرة، 2021، ص 43.

[2] – دراجي شهرزاد وجديدي ضياء الدين رمضان، تهديد الجرائم الإلكترونية عبر الحدود: التحديات والاستراتيجات الدولية لمواجهتها، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد السابع، العدد 2 لسنة 2023، ص 1413.

[3] – فاتن علي بشينة، الجرائم المعلُوماتية وسبل مكافحتها على الصعيد الدولي، مجلة الاصالة، المجلد 2، العدد 9 يونيو 2024، ص 509.

1. إستحداث مكاتب مُتخصصة لجمع المعلومات عن مُرتكبي الجرائم المعلُوماتية، ويتمثل الدور المحوري لهذه المكاتب في العمل على تعزيز التعاون بين سُلطات الدول من الناحية القضائية في مجال مكافحة الجريمة، وكذا مُلاحقة المجرمين وذلك بتتبع المعلُومات وتعميمها بالإضافة إلى تقديم المعُونة وتبادل الخبرات عند الاقتصاء.[1]
2. إنشاء شبكة واسعة من الشركاء الخارجين من أجل تبادل البيانات الأساسية، مثال ذلك نقاط الضعف أو عيوب المنتجاب والخدمات.
3. تقديم الدعم للدول التي تنطلق منها الهجمات الإلكترونية لتطوير قُدُرات كوادرها من الفنيين المتخصصين من أجل التعامل مع هجمات الجريمة الإلكترونية.
4. ضرورة اتخاذ تدابير تشريعية لمكافحة الجريمة المعلُوماتية ومخاطرها المدمرة على جميع الدول، خاصة في ظل شيوع شبكات المعلُومات والتوسع الكبير في أنظمة الحوسبة ونقل المعلُومات، ومُكافحة كافة الأنشطة التي تستهدف أمن المعلُومات.[2]
5. حث جميع الدول على القيام ببعض العمليات الشرطية والأمنية المشتركة فيما بينها بُغية ملاحقة وتعقب المجرم المعلُوماتي، وجمع الأدلة الرقمية وضبطها. والقيام بعملية التفتيش العابر للحدود لمكونات الحاسب الآلي والأنظمة المعلُوماتية بحثاً على الأدلة.
6. التوقيع والتصديق على الاتفاقيات الإلكترونية والأمن المعلوماتي التي تخدم المصلحة العامة لكافة الدول.
7. عقد الندوات والمؤتمرات المحلية والإقليمية والدولية في مجالات الجريمة الإلكترونية.
8. الانضمام للتحالفات المحلية والإقليمية والدولية في مواجهة الجريمة الإلكترونية بما يُحقق المصلحة العليا للدول في هذا المجال.

[1] – قزران مصطفي وزرقين عبد القادر، الآليات الدولية لمكافحة الجريمة الإلكترونية، مجلة صوت القانون، المجلد 8، العدد 2 لسنة 2022، ص 1226.
[2] – علي حمزه عسل الخفاجي، السياسة الجنائية للمشرع الجزائي في حماية الأمن السيبراني، مرجع سابق، ص 166.

الخاتمة:

خَلُصَ الباحثُ إلى جُملةٌ من **النتائج** ولعل أبرزها ما يلي:

1- لم يتفق الفقه الجنائي والإداري على تسمية موحدة للجريمة الإلكترونية، إذ أُطلق عليها البعض بالجريمة الإلكترونية، والبعض الأخر يُسميها بالجريمة المعلوماتية، وذهب أخرون إلى تسميتها بجريمة إساءة استخدام تكنولوجيا المعلومات والاتصال، وكذلك سُميت بالجريمة السيبرانية.

2- من أبرز السمات التي تميزت بها الجريمة الإلكترونية عن غيرها من الجرائم التقليدية أنها جريمة لا تقع إلا باستخدام وسائل تقنية المعلُومات، وأنها عابرة للحدود، ومن الصعب اكتشافها والتعرف على مُرتكبيها.

3- إسوة بالتشريعات المقارنة تصدى المشرع الليبي للجرائم الإلكترونية بسنه قانون خاص بمكافحة الجرائم الإلكترونية رقم (5) لسنة 2022 والذي حدد فيه جرائم التعدي على عمل النظام المعلوماتي، وبرامج وشبكات المعلومات والمواقع الإلكترونية، وغيرها من الجرائم المعلوماتية الماسة بأمن الدولة القومي والسلامة العامة للمجتمع.

4- لقيام الركن المادي للجرمية فقد اكتفى المشرع بالسلوك الإجرامي، بصرف النظر عن العلاقة السببية والنتيجة، حيث اعتبر أن مجرد الدخول للمواقع والأنظمة المعلُوماتية غير المصرح بها جريمة.

5- شكلت الجريمة الإلكترونية بصوُرها المختلفة أحد أهم العناصر المهددة لكيان الدولة، وزعزعة أمنها واستقرارها عبر مختلف الأنشطة والأعمال التخريبية المعادية التي تستهدف أجهزة ومؤسسات الدولة وأنظمة معلوُماتها الحسَاسة من خلال محاولة التأثير على تلك البرامج وتخريبها وتعطيلها، مما خلق حالة من الفوضى والاضطراب التي قد أضر بأجهزة الدولة القومية وعملت على شللها واضعافها.

6- شدد المشرع الليبي في العقوبة عن الأفعال والسلوكيات الإجرامية التي ترتكب باستخدام وسائل تقنية المعلُومات كونها تمس وتهدد المصلحة العامة والأمن القومي للبلاد.

7- استحدث المشرع الهيئة الوطنية لأمن وسلامة المعلُومات وذلك بموجب القرار رقم (28) لسنة 2013 مهمتها وضع السياسات والاستراتيجيات الوقائية لحماية الأمن المعلُوماتي.

8- لم يُنظم المشرع أدلة الإثبات الرقمية، ولم يؤسس لجهة تختص بفحص الأدلة الرقمية لتكون مساعداً للقضاء في الوصول إلى الجريمة ونسبتها إلى فاعلها، الأمر الذي يجعل مواجهة الجريمة الإلكترونية أمراً صعباً على القضاء.

2. وقد خَلُصَ إلى عددٍ من **التوصيات** ولعل أهمُها ما يلي: -

1- يوصي الباحث بضرورة إجراء تعديلات على قانون الجرائم الإلكترونية بما يتماشى مع متطلبات الإدارة العامة الإلكترونية وخصوصية الجرائم المعلُوماتية.

2- نوصي المشرع وبشدة تضمين إدلة الاثبات الإلكترونية في قانون الجرائم الإلكترونية، وأن يعهد للهيئة الوطنية لأمن وسلامة المعلومات مهمة فحص الأدلة ليكون الجهة المساعدة للقضاء في التثبت من وقوع الجريمة الإلكترونية ونسبتها إلى فاعلها.

3- نوصي وبشدة بضرورة تفعيل قانون رقم (5) لسنة 2022 على الصعيد الوطني، والعمل على تجريم بعض الأفعال التي غفل عنها القانون لتجاوز حالة الفراغ التشريعي وضمان سد الثغرات ومواكبة التطور التكنولوجي وأداواته.

4- تفعيل نظام المكافحة الوقائية للحماية من الإرهاب الإلكتروني من خلال تفعيل دور المؤسسات التوعوية بالجتمع الليبي.

5- إلزام الهيئات القائمة على إدارة المرافق العامة بالدولة على إجراء فحوصات دورية ومُستمرة لأمنها المعلُوماتي تحت مراقبة " الهيئة الوطنية لأمن وسلامة المعلُومات، بواسطة أفراد وجهات مُرخص لها لذلك من مجلس الهيئة، وإلزام شركات الاتصالات بعدم تجاوز حدود التصريح في جمع المعلُومات.

6- نوصي بتفعيل التعاون الدولي ومبدأ المساعدة القانونية والقضائية المتبادلة وتسليم المجرمين.

7- نوصي بزيادة الوعي الرقمي لأفراد المجتمع من خلال عقد الندوات والمؤتمرات والجلسات الحوارية وعبر وسائل الإعلام المختلفة، وحث المجتمع المدني للقيام بدوره في توعية الشباب من الوقوع في الجرائم المعلُوماتية اللأخلاقية عبر شبكة الانترنت.

قائمة المصادر والمراجع

أولاً: الكتب

- أشرف السعيد أحمد، تكنولوجيا المعلُومات في المجال الأمني، دار الكتاب الحديث – القاهرة، 2020.
- اسلام هديب، الأمن السيبراني (الهجمات السيبرانية والجرائم السيبرانية)، الطبعة الأولى، دار مصر للنشر والتوزيع، 2024.
- أحمد جابر الجزار، الأمن السيبراني في ضوء قانون مكافحة جرائم تقنية المعلومات رقم (175) لسنة 2018، الطبعة الأولى، المجموعة العالمية للطباعة والنشر والتوزيع، 2024.
- إبراهيم خالد ممدوح، الجرائم المعلوماتية، دار الفكر الجامعي – الإسكندرية، 2009.
- بهاء المري، مكافحة جرائم تقنية المعلومات وحجية الدليل الرقمي في الإثبات، دار مصر للنشر والتوزيع – القاهرة، 2019.
- رأفت عبد الفتاح حلاوة، الجرائم الماسة بأمن الدولة (جريمة قلب نظام الحكم)، دار النهضة العربية – القاهرة، 2010.
- سارة جريفيت، هل يُمكن للتكنولوجيا أن تضع حداً للتحرش والتنمر، ترجمة مُحَمَّد أحمد أمين، دار المكتب الحديث – القاهرة، 2021.
- علي حمزه عسل الخفاجي، السياسة الجنائية للمشرع الجزائي في حماية الأمن السيبراني، الطبعة الأولى، دار مصر للنشر والتوزيع، 2024.
- علي حامد الخولي، الحماية الجنائية لأمن الدولة (دراسة مقارنة)، دار المعرفة الجامعية – القاهرة، 2014.
- عاطف عباس عبد الحميد، جرائم تقنية المعلومات وحقوق الملكية الفكرية، المؤسسة العربية للعلوم والثقافة – القاهرة، 2020.
- مُحَمَّد علي سويلم، مكافحة الجرائم الإلكترونية (دراسة مقارنة بالتشريعات العربية والأجنبية)، الطبعة الأولى، دار المطبوعات الجامعية، 2019.
- مُحَمَّد عبد الله طالب، التحريض على جرائم أمن الدولة من جهة الداخل، دار الفكر والقانون – القاهرة، 2010.
- مُحَمَّد عبد الله أبوبكر سلامة، جرائم الكمبيوتر والانترنت، منشأة المعارف، 2006.
- محمود أحمد عباينة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع – عمان، 2009.
- هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، 1992.
- هروال، نبيلة هبة، الجوانب الاجرائية لجرائم الانترنت، دار الفكر الجامعي، الطبعة الأولى، 2007.

ثانياً: المجلات والأبحاث والمقالات العلمية

- الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجمع البحوث والدراسات، اكاديمية السلطان قابوس لعلوم الشرطة، 2016.
- أسامة صلاح محمود الماحي، الجرائم المعلوماتية الُمهددة للأمن القومي المصري، مجلة البحوث القانونية والاقتصادية – المنوفية، العدد 1/ 57، 2023.
- بوضياف اسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11 سبتمبر 2018.
- خالد أحمد مُحَّد ابزيم، الضبط الإداري وإشكالية التوازن بين حفظ الأمن العام وضمان حقوق الأفراد وحرياتهم في التشريع الليبي، ورقة بحثية مقدمة للمؤتمر العلمي الدولي حول السياسات الأمنية في ليبيا بين الواقع والمأمول – بنغازي، أغسطس 2023.
- رياض بن عربية، الأبعاد الإستراتيجية للجرائم الإلكترونية وتهديداتها للأمن الوطني، مجلة دفاتر البحوث العلمية، المجلد 9، العدد 1 لسنة 2021.
- دراجي شهرزاد وجديدي ضياء الدين رمضان، تهديد الجرائم الإلكترونية عبر الحدود: التحديات والاستراتيجات الدولية لمواجهتها، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد السابع، العدد 2 لسنة 2023.
- علي عوض الجيرة وآخرون، أثر الجريمة الإلكترونية على سير المرافق العامة الإلكترونية في التشريع الأردني، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد 21، العدد 2 لسنة 2021.
- علي أحمد الفرجاني، جريمة القرصنة المعلوماتية (دراسة مقارنة من الجانبين الموضوعي والإجرائي)، مجلة التشريع، العدد 7 أكتوبر 2005.
- علي الدين هلال، الأمن القومي العربي (دراسة في الأصول)، مجلة شؤون عربية، العدد 35، يناير 1984.
- فاتن علي بشينة، الجرائم المعلُوماتية وسبل مكافحتها على الصعيد الدولي، مجلة الاصالة، المجلد 2، العدد 9 يونيو 2024.
- قزران مصطفي وزرقين عبد القادر، الآليات الدولية لمكافحة الجريمة الإلكترونية، مجلة صوت القانون، المجلد 8، العدد 2 لسنة 2022.

- نرمين نبيل الأزرق، مُحددات المسؤولية الجنائية لجرائم الاختراق والاعتراض والانتحال وآليات الردع في التشريعات العربية في العصر الرقمي (دراسة تحليلية مقارنة)، مجلة البحوث الإعلامية، العدد 56 يناير لسنة 2021.
- مهداوي حنان، التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري، مجلة الفكر القانوني والسياسي، المجلد السادس، العدد 22 نوفمبر 2022.
- معاشي سميرة، الجريمة الإلكترونية (دراسة تحليلية لمفهوم الجريمة المعلوماتية)، مجلة الفكر، العدد 17 يونيو 2018.
- مختارية بوزيدي، ماهية الجريمة الإلكترونية، الملتقى الوطني حول " آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري، جزائر العاصمة 29 مارس 2017.
- محمود قنديل، قانون رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية في ليبيا الحماية المفقودة والعقوبات المشددة، مجموعة بحوث، مركز مُدافع لحقوق الإنسان، سبتمبر 2023.
- مُحَمَّد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الحقوق والشريعة، جامعة الإمارات، 21 مايو 2005.

ثالثاً: القوانين والقرارات

- قانون العقوبات، صدر في: 28 نوفمبر 1953.
- قانون رقم 04-15 لسنة 2004 والمعدل لقانون العقوبات الجزائري الصادر عام 1966.
- القانون رقم (5) لسنة 2022 بشأن الجرائم الإلكترونية، نشر في الجريدة الرسمية، العدد 1، 27 سبتمبر 2022.
- القانون رقم (3) لسنة 2014 بشأن مكافحة الإرهاب، نشر بتاريخ 9 سبتمبر 2014.
- القانون رقم (63) لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات – الكويت.
- المرسوم بقانون الاتحادي رقم (34) لسنة 2021 الخاص بمكافحة الشائعات والجرائم الإلكترونية – الإمارات العربية المتحدة.
- القانون رقم (175) لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات – مصر.
- القرار رقم (28) لسنة 2013 بشأن إنشاء الهيئة الوطنية لأمن وسلامة المعلُومات.