الإطارُ القانوني لتجريم القرصنة الإلكترونية في مملكة البحرين

بقلم
المستشار الدكتور/ محمد فؤاد الحريري
نائب رئيس مجلس الدولة المصري

الملخص

يستعرض البحث مفهوم ظاهرة القرصنة وأنواعها المختلفة، ويُوضح المقصود بجرائم القرصنة الإلكترونية وما يترتب عليها من آثار خطيرة، وأنواع المخترقين الإلكترونيين، وكذلك يتناول أهم طرق مكافحة هذه الجرائم، مع الإشارة إلى مفهوم القرصنة المشروعة أو ما يُعرف بالقرصنة الأخلاقية، ودورها في هذا الشأن.

كما يُلقي الضوء على الإطار القانوني الذي وضعه المشرع البحريني لتجريم ظاهرة القرصنة الإلكترونية بهدف مكافحتها والتصدي لها والحد من آثارها السلبية، وذلك من خلال عرض وتحليل أهم أحكام القوانين السارية ذات العلاقة، وهي القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات، وقانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨، وكذلك يُشير البحث إلى الدور الحيوي الذي تؤديه وزارة الداخلية البحرينية في مجال إنفاذ القوانين والتشريعات المتعلقة بمكافحة جرائم القرصنة الإلكترونية، وكذلك دورها البارز في الوقاية من هذه الجرائم.

الكلمات المفتاحية: القرصنة الإلكترونية، القرصنة المشروعة، الجرائم الإلكترونية، جرائم تقنية المعلومات، حماية البيانات الشخصية.

Abstract

The research reviews the concept of the phenomenon of hacking and its various types and clarifies the meaning of electronic hacking crimes and their serious effects, and the types of electronic hackers, as well as dealing with the most important ways to combat these crimes, with reference to the concept of legal hacking or what is known as ethical hacking, and its role in this regard.

Then it sheds light on the legal framework established by the Bahraini legislator to criminalize the phenomenon of electronic hacking with the aim of combating it, addressing it and limiting its negative effects, by presenting and analyzing the most important provisions of the relevant applicable laws, namely law No. (60) of 2014 regarding information technology crimes and law of protection of personal data promulgated by law No. (30) of 2018. The research also refers to the vital role played by the Bahraini Ministry of Interior in the field of enforcement of laws and legislation related to combating electronic hacking crimes, as well as its prominent role in preventing these crimes.

المقدمة

يُوصف العصر الحالي بأنه عصر التكنولوجيا؛ لأنها طالت شتى مجالات الحياة، والإنسان في سباق مستمر مع الزمن بقصد الوصول إلى أحدث الوسائل التكنولوجية لاستخدامها في حياته لما توفره من وقت وجهد ومال. ونجم عن الحرص على مواكبة ركب التطور ثورة في مجال الاتصالات وتكنولوجيا الحاسوب ونُظم المعلومات، وقد أحدث ظهور شبكة الإنترنت تغيراً كبيراً في أنماط الحياة على اختلاف درجاتها، وأسهمت هذه الشبكة في إلغاء الكثير من الحواجز التي تفصل بين الدول، فأصبح العالم قرية صغيرة يسهل فيها التواصل، ولم يَعُد البشر أسرى لمكانهم فوق كوكب الأرض[١].

وقد ذاع الحديث عن ثورة الاتصالات وتقنية المعلومات، ومجتمع المعلوماتية، وما رافقه من مصطلحات جديدة منها الأرشيف الإلكتروني، والمعالجة عن بُعد، والحوكمة الإلكترونية، والتحكيم الإلكتروني، والتجارة الإلكترونية[٢].

وفي ظل هذه الثورة ظهرت القرصنة الإلكترونية التي تُعد من أهم وأخطر الظواهر التي تمس حياتنا جميعاً في الوقت الراهن؛ حيث إننا معرضون – في أي وقت وفي أي مكان – لحدوث اختراق لحساباتنا البنكية، أو سطو على بياناتنا الشخصية، أو أجهزتنا الإلكترونية عن طريق أشخاص مجهولين، وغالباً ما يترتب على هذا الاختراق أو السطو أضرار مادية وأدبية جسيمة قد يصعب تداركها.

وقد أصبحت جرائم القرصنة الإلكترونية خطراً حقيقياً يؤثر سلباً على الأفراد والمجتمعات؛ إذ تُعد هذه الجرائم من الجرائم العابرة للحدود؛ حيث أعطى انتشار شبكة الإنترنت إمكانية ربط أعداد هائلة من أجهزة الحاسوب المرتبطة بالشبكة العنكبوتية من غير أن تخضع لحدود الزمان والمكان، ولذلك فإن من السهولة بمكان أن يكون المجرم في بلد ما والمجني عليه مقيماً في بلد آخر، وهنا تظهر الحاجة إلى وجود تنظيم قانوني دولي وداخلي متلائم معه لمكافحة مثل هذا النوع من الجرائم وضبط فاعليها، وتتشابه الجرائم الإلكترونية في ذلك مع بعض الجرائم، مثل: جريمة غسل الأموال[٣].

١. د. علاء محمد الفواعير، العقود الإلكترونية دراسة مقارنة، دار الثقافة للنشر والتوزيع، ٢٠١٤، ص ١٥.

٢. د. إلياس ناصيف، العقود الدولية، العقود الإلكترونية في القانون المقارن، منشورات الحلبي الحقوقية، لبنان، ٢٠٠٩، ص ٥.
ويمكن تعريف مصطلح "الأرشيف الإلكتروني" بأنه مكان حفظ الوثائق والمستندات الإلكترونية التي يتم تحويلها من مستندات ورقية عن طريق المسح الضوئي، ويتم استخدام هذا الأرشيف من قبل الجهات الحكومية كجزء من متطلبات الحكومة الإلكترونية. كما يمكن تعريف مصطلح "المعالجة عن بُعد" بأنه نقل البيانات الطبية الإلكترونية مثل الصور وأفلام الفيديو وسجلات المرضى من مكان إلى آخر من أجل تقييم حالة المريض الصحية أو تقديم الرعاية الطبية اللازمة، أو بهدف تحسين رعاية المرضى. ويُعرف مصطلح «الحوكمة الإلكترونية» بأنه استخدام القطاع العام تكنولوجيا المعلومات والاتصالات لتقديم الخدمات الحكومية وتبادل معلومات معاملات الاتصالات من خلال تكامل مختلف الأنظمة والخدمات القائمة بذاتها بين الحكومة والأفراد، وبين الحكومة والشركات، وبين الحكومات وبعضها البعض. ويُقصد بمصطلح «التحكيم الإلكتروني» قضاء اتفاقي من نوع خاص ينشأ من اتفاق أطراف المنازعة على إحالة المنازعة التي تتعلق في الغالب بالتجارة الإلكترونية إلى محكم خارجي يتولى تسويتها عبر وسائط الاتصالات الإلكترونية ووسائل الاتصال الحديثة، ويصدر حكماً ملزماً لأطراف المنازعة، ومن أمثلة المنازعات التي يمكن تسويتها عن طريق التحكيم الإلكتروني المنازعات الناجمة عن الاخلال بالعقود الإلكترونية، ومسئولية مزودي خدمة الإنترنت، ومنازعات أسماء النطاق، والسداد الإلكتروني.

٣. عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية دراسة مقارنة، رسالة ماجستير في القانون، جامعة الشرق الأوسط، ٢٠١٤، ص ٢٠.

أهمية البحث

تكمن أهمية البحث في انتشار ظاهرة جرائم القرصنة الإلكترونية في عالمنا المعاصر بشكل غير مسبوق، وضرورة نشر الوعي اللازم بين مستخدمي شبكة الإنترنت ومواقع وتطبيقات التواصل الاجتماعي بخطورة هذه الجرائم وآثارها التي تهدد أمن واقتصاد المجتمع، وكيفية مواجهتها، وبيان أهمية وجود تنظيم تشريعي حاسم ومتطور للحد من هذه الجرائم والتصدي لها بكل حزم، وملاحقة مرتكبيها، وذلك في ضوء كونها ظاهرة عالمية تعاني منها جميع الدول، وتُشكل انتهاكاً صريحاً للخصوصية وحرية الفضاء الإلكتروني.

أهداف البحث

تتمثل أهداف البحث في بيان مفهوم ظاهرة القرصنة الإلكترونية، وتحديد أبرز صور الجرائم التي تُرتكب في ظلها، وتوضيح ما يترتب عليها من آثار خطيرة تهدد الأفراد والمجتمعات اقتصادياً واجتماعياً، وتحديد أنواع المخترقين الإلكترونيين، وكذلك بيان أهم طرق مكافحة جرائم القرصنة الإلكترونية، مع الإشارة إلى مفهوم القرصنة المشروعة أو القرصنة القانونية legal hacking أو ما يُعرف بالقرصنة الأخلاقية ethical hacking باعتبارها من أهم طرق المكافحة المُتبعة في الآونة الأخيرة. كما يستعرض البحث التنظيم القانوني لتجريم ظاهرة القرصنة الإلكترونية غير المشروعة في مملكة البحرين بهدف الحد منها وحماية الأفراد والمجتمع من مخاطرها وأضرارها.

إشكالية البحث

يحاول البحث الإجابة على التساؤلات الآتية: ما المقصود بظاهرة جرائم القرصنة الإلكترونية؟ وما هي أسباب انتشارها؟ ومن هم قراصنة المعلومات؟ وما هي أهم الطرق والأساليب التي يمكن اتباعها لمكافحة جرائم القرصنة الإلكترونية؟ وما هو الإطار القانوني الذي وضعه المشرع البحريني لتجريم ظاهرة القرصنة الإلكترونية غير المشروعة؟ وما مدى فعالية هذا الإطار ونجاحه في تحقيق أهدافه المنشودة؟ وما هي أبرز الجهود التي تبذلها السلطة التنفيذية في مملكة البحرين لمواجهة ومكافحة هذا النوع من الجرائم المتزايدة؟

منهج البحث

سوف يتبع الباحث المنهج الوصفي التحليلي، وذلك من خلال عرض وتحليل أهم أحكام القوانين والتشريعات التي تمثل الإطار القانوني المعمول به في مملكة البحرين لتجريم ظاهرة القرصنة الإلكترونية غير المشروعة بغرض مكافحتها والوقاية من آثارها الضارة.

خطة البحث

في ضوء ما تقدم، سيتم دراسة الموضوع من خلال تقسيم هذا البحث إلى مبحثين، وذلك على النحو الآتي:

المبحث الأول: مفهوم القرصنة الإلكترونية وجرائمها وآثارها وأهم طرق مكافحتها.

المبحث الثاني: التنظيم القانوني لتجريم ظاهرة القرصنة الإلكترونية في ضوء التشريع البحريني.

المبحث الأول

مفهوم القرصنة الإلكترونية وجرائمها وآثارها وأهم طرق مكافحتها

تم تقسيم المبحث الأول إلى ثلاثة مطالب؛ حيث يستعرض المطلب الأول مفهوم ظاهرة القرصنة الإلكترونية وأشهر صور جرائمها، ويوضح المطلب الثاني الآثار المترتبة على ظاهرة القرصنة الإلكترونية، ثم يلقي المطلب الثالث الضوء على أهم طرق مكافحة جرائم القرصنة الإلكترونية.

المطلب الأول
مفهوم ظاهرة القرصنة الإلكترونية وصور جرائمها

"القَرْصَنَةُ" مصدر الفعل "قرصنَ"، وعُرفت في اللغة العربية بأنها السَّطو على سفن البحار، فيقال: "نَشِطَتِ القَرْصَنَةُ عَلَى الشَّوَاطِئِ قَدِيماً"[1]، ومن يمتهنها يُسمى قرصان، والجمع قراصنة. وهذا المصطلح مشتق من كلمة "pirate" اللاتينية، ويعني "سارق البحر".

ويُقصد بالقرصنة البرية نصب الكمائن من قبل قطاع الطرق واللصوص للمسافرين في المناطق الجبلية والطرق السريعة.

كما عُرفت القرصنة الجوية بأنها الاستيلاء على طائرة أثناء طيرانها، فيقال: "تَعَرَّضَتِ الطَّائِرَةُ لِلْقَرْصَنَةِ أي: تم تَحْوِيلُ اتِّجَاهِهَا عَلَى يَدِ قَرَاصِنَةٍ مُخْتَطِفِينَ"[2].

ويُعتبر قرصنة، وفقاً لاتفاقية الأمم المتحدة لقانون البحار (UNCLOS) لعام ١٩٨٢[3]، أي عمل غير قانوني من أعمال العنف أو الاحتجاز أو أي عمل سلب يُرتكب لأغراض خاصة بواسطة طاقم أو ركاب سفينة خاصة أو طائرة خاصة، ويكون موجهاً في أعالي البحار ضد سفينة أو طائرة أخرى، أو ضد أشخاص أو ممتلكات على ظهر تلك السفينة أو على متن تلك الطائرة، أو يكون موجهاً ضد سفينة أو طائرة أو أشخاص أو ممتلكات في مكان يقع خارج ولاية أية دولة، وكذلك أي عمل من أعمال الاشتراك الطوعي في تشغيل سفينة أو طائرة مع العلم بوقائع تضفي على تلك السفينة أو الطائرة

---

١. راجع في ذلك معجم المعاني الجامع – معجم عربي عربي، منشور على الرابط:
https://www.almaany.com/ar/dict/ar-ar/%D982%%D8%B1%D8%B5%D986%%D8%A9/
تاريخ الدخول: ٢٠٢٢/٩/٧

٢. المرجع السابق.

٣. (UNCLOS) هي اختصار لعبارة "United Nations Convention on the Law Of the Sea" اتفاقية الأمم المتحدة لقانون البحار.

صفة القرصنة[1].

ومن جهة أخرى، تم تعريف القرصنة الأدبية في مجال حقوق الملكية الفكرية بأنها عبارة عن التوزيع غير المصرح به، أو السرقة، أو الاستنساخ، أو النسخ، أو الأداء، أو التخزين، أو البيع، أو أي استخدام آخر لحق من حقوق الملكية الفكرية محمي بموجب قانون حقوق النشر أو قانون حق المؤلف، فهي شكل من أشكال انتهاك حقوق النشر. كما تم تعريف القرصنة أيضاً بأنها سَطْو على حقوق المِلْكية الفِكرية أو الأدبية، أو عملية النسخ غير القانوني للكتب، والقطع الموسيقية، وبرامج الحاسوب.

ولذلك قيل بأن عبارة "قرصن فُلانٌ" تعني قام بأعمال سَلْب بَحْريّ، أو حَوّل اتِّجاه سفينة أو طائرة لغَرَض اقْتصادي أو سياسي، أو سطا على حاسوب أو خادوم عن طريق الشبكة وتحكم به عن بعد، أو سطا على حقوق الملكية الفكرية أو الأدبية أو الفنية.

ويتضح مما تقدم، أن هناك عدة أنواع للقرصنة، أبرزها القرصنة البحرية، والقرصنة البرية، والقرصنة الجوية، والقرصنة الأدبية، والقرصنة الإلكترونية.

ويشير مفهوم القرصنة الإلكترونية إلى ممارسات غير مشروعة تستهدف التحايل على نظام المعالجة الآلية للبيانات وتقنية المعلومات بهدف الوصول غير المرخص للحسابات وأنظمة التشغيل، أو إتلاف المستندات المعالجة إلكترونياً، وذلك من خلال أساليب متنوعة قد تعتمد على الهندسة الاجتماعية، أو البرمجيات الخاصة بذلك. وتختلف الطبيعة الإجرامية للقرصنة من قضية إلى أخرى باختلاف الدافع الإجرامي لمرتكبيها، إذ قد يكون الدافع شخصياً، وقد يكون الدافع مادياً لتحقيق مكاسب مالية غير مشروعة، مثل سرقة بيانات البطاقات الائتمانية، وتحويل الأموال من الحسابات المصرفية بدون وجه حق، بالإضافة إلى التصيد الإلكتروني، والتهديد والابتزاز بنشر المعلومات الخاصة والسرية في حال عدم قيام الضحية بدفع أو تحويل المبلغ المالي المطلوب.

كما يُقصد بالقرصنة الإلكترونية عملية اختراق لأجهزة الحاسوب عبر شبكة الإنترنت، ويقوم بهذه العملية شخص أو مجموعة من الأشخاص لديهم خبرة واسعة في برامج الحاسوب، إذ يمكنهم بواسطة برامج مساعدة الدخول إلى حاسوب يخص شخصاً آخر، والتعرف على محتوياته.

وتُعتبر القرصنة الإلكترونية من أبرز أشكال الجرائم الإلكترونية، والمقصود بالجريمة الإلكترونية كل فعل أو امتناع يتم إعداده أو التخطيط له، ويتم بموجبه استخدام أي نوع من الحواسيب الآلية سواء حاسب شخصي، أو شبكات الحاسب الآلي، أو الإنترنت، أو وسائل التواصل الاجتماعي؛ لتسهيل ارتكاب جريمة أو عمل مخالف للقانون، أو تلك التي تقع على الشبكات نفسها عن طريق اختراقها بقصد تخزينها، أو تعطيلها، أو تحريف أو محو البيانات أو البرامج التي تحويها[2].

---

١. راجع المادة (١٠١) من اتفاقية الأمم المتحدة لقانون البحار (UNCLOS) لعام ١٩٨٢.

٢. عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية دراسة مقارنة، مرجع سابق، ص ١٤.

وقد انتشرت الجرائم الإلكترونية في السنوات الأخيرة بشكل كبير للغاية، ويعزو ذلك إلى عدة أسباب منها توفر الشبكة العنكبوتية، والرغبة في الشهرة، والسعي نحو الربح المادي مقابل التجسس والابتزاز، والرغبة في الانتقام، وتوفر الأجهزة الإلكترونية بأسعار معقولة وسهولة اقتنائها.

وتتعدد صور جرائم القرصنة الإلكترونية، مثل المطاردة الإلكترونية، وهي أحد أنماط جرائم المحتوى المتعلقة بإساءة استخدام تكنولوجيا المعلومات والاتصالات الحديثة ولاسيما مواقع التواصل الاجتماعي؛ حيث تشمل أنشطة سرقة وجمع المعلومات والبيانات الشخصية، ثم التهديد والإرهاب الممنهج للضحايا المستهدفين بأساليب ووسائل إلكترونية مختلفة، وتمتد إلى المراقبة والسب والقذف والتحرش والتنمر الإلكتروني وما إلى ذلك عبر مواقع التواصل الاجتماعي، والمدونات، وغرف المحادثة، وغيرها من المواقع.

وكذلك تُعتبر الفيروسات والبرمجيات الخبيثة من صور جرائم القرصنة الإلكترونية؛ وهي برمجيات تصيب الأجهزة والحواسيب والشبكات ولديها القدرة على التكاثر والانتشار السريع، ويمكن الإصابة بالفيروسات والبرمجيات الخبيثة عن طريق الروابط والصفحات والإعلانات الترويجية الإلكترونية المشبوهة على الإنترنت، أو المستلمة عبر البريد الإلكتروني، أو حتى الرسائل النصية، كما يمكن الإصابة بها عن طريق تصفح وتنزيل الملفات الرقمية المقرصنة من على الإنترنت، أو نقلها من جهاز إلى جهاز آخر.

وقد تم تعريف الفيروسات بأنها عبارة عن برنامج حاسب آلي أو جزء من برنامج يعدل المعلومات ويدمرها، ويتم زرعه على الأقراص والاسطوانات الخاصة بالحاسب الآلي، ويظل خاملاً لفترة محددة ثم ينشط فجأة في توقيت معين ليدمر البرامج والبيانات المسجلة، ويمتد أثره التخريبي ليشمل الإتلاف والحذف والتعديل. وقد يمس الفيروس برنامجاً معيناً أو يمس كافة البرامج الموجودة على ذاكرة الجهاز المعلوماتي ويدمر الجهاز بأكمله، وينتقل عبر جميع البرامج والشبكات المتصلة بالجهاز المعلوماتي[1].

كما يُعد الاحتيال باستخدام بطاقات الائتمان عبر الإنترنت من أكثر عمليات القرصنة الإلكترونية شيوعاً في الوقت الراهن، ويتخذ الاحتيال الإلكتروني أشكالاً عديدة، إلا أنها تهدف جميعها إلى حصول الجناة على مبالغ مالية بطريقة غير مشروعة من الضحايا، والتي قد تكون عن طريق سرقة أرقام البطاقات الائتمانية، أو دفع الضحية لإرسال حوالات مالية أو شيكات رقمية لإجراء عمليات شراء لمنتجات وهمية على الإنترنت، أو دفعهم إلى الكشف عن معلومات شخصية متعلقة بحساباتهم البنكية والبطاقات المرتبطة بها عن طريق الاتصال الهاتفي أو الرسائل النصية أو البريد الإلكتروني أو المتاجر الإلكترونية المشبوهة، والتي تؤدي في النهاية إلى تمكن الجناة من خداع الضحايا عن

١. حنان ريحان مبارك المضحكي، الجرائم المعلوماتية دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، ٢٠١٤، ص ١٢٨ – ١٢٩.

طريق الاستخدام غير المصرح وغير المشروع لبيانات البطاقات الائتمانية.

وقد يتعرض البعض لقرصنة البريد الإلكتروني، أو الصفحة الشخصية على مواقع التواصل الاجتماعي، وأحياناً يرتبط الأمر بخسائر مادية عند اختراق البيانات البنكية عن طريق شبكة الإنترنت.

ويُعتبر التعرض لمثل هذه القرصنة الإلكترونية بمثابة جرس إنذار للتأكد من سلامة برنامج الحماية من الفيروسات المستخدم. وجدير بالذكر أن الاعتماد على برامج مجانية يتم تحميلها من شبكة الإنترنت قد يُسهل عمل القراصنة؛ لأنه لا يوفر الحماية المطلوبة للبيانات[1].

وفيما يتصل بأنواع قراصنة المعلومات أو المخترقين الذين يقومون بتنفيذ عمليات القرصنة الإلكترونية، فإنه يمكن تصنيفهم إلى قسمين، وهما: الهاكرز Hackers وهؤلاء يمكن أن ننعتهم بالمبتدئين أو الهواة الذين يكون الهدف من وراء اختراقهم للأنظمة الإلكترونية التعلم والتسلية على الأغلب. والكراكرز Crackers وهم المخترقون المحترفون الذين يكون دخولهم إلى الحواسيب من أجل غاية معينة تحقق لهم ما يهدفون إليه[2].

وقد تم إطلاق مصطلح «الكراكر» للتمييز بين الهاكر الآمن والهاكر الخبيث؛ حيث يُقصد بالهاكر الآمن من يستخدم الحاسوب وشبكة الإنترنت لاختراق نظم الأمن والشبكات، بغرض الدخول غير المصرح به. ورغم قدرة الهاكر الفائقة على الاختراق، إلا أنه غير مؤذ، فهو لا يقوم بالاختراق بغرض التخريب أو الإيذاء، وإنما نتيجة حبه للحرية وشعوره بأن الإنترنت أو العالم الافتراضي يؤمن له هذه الحرية؛ إذ إنه لا يقيم أهمية لحواجز الشفرات وكلمات المرور، بل يخترق أعتى الأماكن سرية وحصانة بغرض الاطلاع على التقنية، دون أن يتلف أو يخرب أي شيء.

ويُقصد بالهاكر الخبيث أو الكراكر المخترق ذو النوايا الإجرامية، بحيث يقوم بما هو شرير وما يُشكل جريمة كالإتلاف، أو التخريب، أو الإرهاب، أو الابتزاز، أو العدوان على الأموال بالاحتيال والسرقة وغيرها[3]. وبالرغم من تميز الاثنين بالذكاء وروح التحدي وعدم خوفهم من مواجهة المجهول، إلا

---

١. راجع في ذلك مقال بعنوان: القرصنة الإلكترونية، منشور على الرابط:
https://www.dw.com/ar/%D8%A7%D984%%D982%%D8%B1%D8%B5%D986%%D8%A9-%D8%A7%D984%%D8%A5%D984%%D983%%D8%AA%D8%B1%D988%%D986%D98%A%D8%A9/t-19111848

تاريخ الدخول: ٢٠٢٢/٩/٧

٢. راجع في ذلك بحث بعنوان: جريمة القرصنة الإلكترونية، منشور على الرابط:
https://www.mohamah.net/law/%D8%A8%D8%AD%D8%AB-%D982%%D8%A7%D986%%D988%%D986%%D98%A-%D985%%D981%%D98%A%D8%AF-%D8%AD%D988%%D984-%%D8%AC%D8%B1%D98%A%D985%%D8%A9-%D8%A7%D984%%D982%%D8%B1%D8%B5%D986%%D8%A9-%D8%A7%D984%%D8%A5%D984%/

تاريخ الدخول: ٢٠٢٢/٩/٢٨

٣. د. محمد طارق عبدالرؤوف الخن، جريمة الاحتيال عبر الإنترنت (الأحكام الموضوعية والأحكام الإجرائية)، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، ٢٠١١، ص ١٨٤ وما بعدها.

أن الكراكر يقوم دائماً بأعمال التخريب والاقتحام لأسباب غير إيجابية، وهذا الشخص هو الذي يستحق تسمية قرصان الحاسوب، بينما الهاكر يبتكر الحلول للمشاكل ويحاول أن يبدع في عمله.

وذهب أحد الخبراء في مجال القرصنة الإلكترونية وأمن المعلومات إلى أن أحد التعريفات التي تُصحح مفهوم القرصنة عند الكثيرين هو أن القرصان مصطلح يُطلق على أولئك الذين يكتبون التعليمات البرمجية، وعلى أولئك الذين يستغلونها. (Hacker is a term for both those who write code, and those who exploit it.) وعلى الرغم من اختلاف أهداف كل منهم، إلا أنهم في النهاية لديهم نفس التكنيك في التغلب على المشاكل؛ لأنه – ببساطة – فهم البرمجة مهم لمن يريد التحايل على الأنظمة، يساعده على اكتشاف الأخطاء البرمجية والثغرات الأمنية، وعلى الجانب الآخر فهم سبب حدوث الاختراق (الثغرة نفسها أو الخطأ البرمجي) سينفع المبرمج أو مصمم النظام الأمني، وسيعلمه أكثر حتى يتفحص أكواده وإعدادات الأجهزة لديه[1].

وسواء كان المخترق وكالة حكومية أو أية منظمة إجرامية، فإن لديه مستويات من التسلسل الهرمي، وتقسيم المهام، والتعاون اللازم لشنّ الهجمات الإلكترونية، وليس غريباً تجنيد عدد كبير من المخترقين، أو فرق كاملة لتنفيذ مهام محددة، مثل التسلل بشكل سري، أو تشفير الاتصالات والعمليات الأخرى، أو توفير البنى التحتية للحماية الذاتية والاختباء، والتعامل مع الأموال والعملات المشفرة مثل بيتكوين[2].

كما أن هناك قراصنة أقل تنظيماً غير أن أهدافهم محدودة للغاية. ومن أبرز الأمثلة (Script kids) أو القراصنة المبتدئون، الذين يستغلون نقاط الضعف في الأنظمة الحاسوبية لتحقيق أرباح ضئيلة، لكنهم سرعان ما تقبض عليهم السلطات لأنهم غالباً ما يكتشفون الثغرة عن طريق الخطأ، ويقومون بإساءة استخدامها دون إخفاء آثارهم بصورة كافية. ويبدو لهؤلاء أنهم قد فازوا بجائزة كبرى، ويعتريهم شعور وهمي بأنهم لا يقهرون، لكنهم في نهاية الأمر ليسوا سوى لصوص عاديين.

وعلى هذا النحو، هناك أنواع من المخترقين حسب الدوافع، وهم: المنتقمون (avengers)، المرتزقة (mercenaries)، النشطاء (activists)، الدول (states)، المنظمات الإجرامية (criminal organizations)، الإرهابيون (terrorists)[3].

---

١. أحمد المشد، القرصنة الإلكترونية وأمن المعلومات، مؤسسة الأمة العربية للنشر والتوزيع، القاهرة، ٢٠١٧، ص ١٣.

٢. من الجدير بالذكر أن العملات المشفرة تُعد من الأصول الافتراضية، ويعتبر هذا المصطلح من المصطلحات الحديثة التي ظهرت مؤخراً في إطار الاقتصاد الرقمي الذي يتجه العالم نحوه بسرعة كبيرة، وتُعرف الأصول الافتراضية بأنها أي منتج رقمي يتم إصداره، وإدراجه، وحفظه، وتداوله، من خلال المنصات الرقمية المختلفة، كما تُعرف بأنها نوع من أنواع تداول العملات الإلكترونية؛ لأنها إحدى العملات الرقمية التي يتم تداولها رقمياً بين الأفراد، وقد تم استخدام الأصول الافتراضية على نطاق واسع في السنوات الأخيرة في ضوء تطور التقنيات الرقمية في الدول التي بدأت في تبني هذا النوع من التجارة المالية في مشاريعها واستثماراتها المختلفة. وهناك العديد من أنواع العملات المشفرة المنتشرة حالياً، من أشهرها بيتكوين، وبيتكوين كاش، وإيوس. ومن أهم التحديات التي تواجه هذا النوع المستحدث من المعاملات في ظل الاقتصاد الرقمي: القدرة على الرقابة، ووضع ضوابط تحكم حركة الأسواق، وتمنع عمليات الاحتيال، وتحفظ وتحمي حقوق المستثمرين والمتعاملين.

٣. راجع في ذلك مقال بعنوان: هل ما نعرفه عن قراصنة الإنترنت صحيح؟ منشور على الرابط:

المطلب الثاني
الآثار المترتبة على ظاهرة القرصنة الإلكترونية

تطورت عمليات القرصنة الإلكترونية غير المشروعة، وعُرفت كظاهرة عالمية تتضمن في معظم الأحيان أكثر أشكال الجريمة المنّظمة تقدماً. وقد نمت جرائم القرصنة الإلكترونية – باعتبارها من الجرائم الإلكترونية – في العقد الماضي بشكل لم يسبق له مثيل على شبكة الإنترنت ووسائل التواصل الاجتماعي.

والحقيقة أن الجرائم الإلكترونية أو ما يُسمى بـ cyber crimes هي ظواهر إجرامية تقرع أجراس الخطر لتنبه مجتمعنا عن حجم المخاطر والخسائر التي يمكن أن تنجم عنها، خاصة أنها جرائم ذكية تنشأ وتحدث في بيئة إلكترونية أو بمعنى أدق رقمية، يقترفها أشخاص مرتفعو الذكاء ويمتلكون أدوات المعرفة التقنية، مما يسبب خسائر للمجتمع ككل على المستويات الاقتصادية والاجتماعية والثقافية والأمنية[1].

وتنتمي اليوم أعمال القرصنة إلى شبكة عالمية لها قيادتها ومنظماتها، وتعمل وفق مخططات معينة، وتمتلك وسائل اتصال ونقل حديثة وأسلحة، وتستخدم أحدث التقنيات في الاتصال عبر الأقمار الاصطناعية مما يثير الكثير من التساؤلات حول عملها وخلفيات نشاطها وتداعياته، مما يضع منظمات عالمية، ودولاً، وسياساتها في دائرة الشك والاتهام[2].

وقد أثبت الواقع العملي أن الهجمات الإلكترونية المنظمة تمثل خطراً حقيقياً؛ لأنه غالباً ما يتم تنفيذ الهجوم بعد استعداد طويل متضمناً إستراتيجيات الهروب، والاستعداد للاختراق المضاد، وعمليات التمويه، مما يُصعب مهمة المدافعين في صد هذا الهجوم.

ويترتب على جرائم القرصنة الإلكترونية العديد من الآثار السلبية؛ حيث بات هذا النوع من القرصنة خطراً يهدد اقتصاديات العالم، والتي تتنوع أشكالها بدءاً من اختراق البريد الشخصي، والقرصنة المصرفية على حسابات مالية، وصولاً إلى التجسس الاقتصادي للحصول على

---

https://1-a1072.azureedge.net/news/scienceandtechnology/202129/7//%D982%%D8%B1%D8%A7%D8%B5%D986%%D8%A9-%D8%A7%D984%%D8%A5%D986%%D8%AA%D8%B1%D986%%D8%AA-%D985%%D986-%%D987%%D985-%%D-988%%D983%%D98%A%D981-%%D98%A%D8%B9%D985%%D984%%D988%%D9%86%D89%F

تاريخ الدخول: ٢٠٢٢/٩/١١

١. د. علي عدنان الفيل، الإجرام الإلكتروني دراسة مقارنة، منشورات زين الحقوقية، ٢٠١١، ص ٨.

٢. د. أحمد عَلّو، القرصنة بين العصور القديمة وعصر التكنولوجيا، بحث منشور على الرابط:
https://www.lebarmy.gov.lb/ar/content/%D8%A7%D984%%D982%%D8%B1%D8%B5%D986%%D8%A9-%D8%A8%D98%A%D986-%%D8%A7%D984%%D8%B9%D8%B5%D988%%D8%B1-%D8%A7%D984%%D982%%D8%AF%D98%A%D985%%D8%A9-%D988%%D8%B9%D8%B5%D8%B1-%D8%A7%D984%%D8%AA%D983%%D986%%D988%%D984%%D988%%D8%AC%D98%A%D8%A7

تاريخ الدخول: ٢٠٢٢/٩/٧

أسرار علمية، أو خطط شركات وأنظمة لتطوير منتجاتها[1].

وفي ظل أزمة جائحة فيروس كورونا التي ضربت العالم خلال عام ٢٠٢٠، زادت الاتهامات لبعض الدول بالتجسس على الشركات العالمية الكبرى التي تطور لقاحات للوقاية من الفيروس، خاصة في الولايات المتحدة الأمريكية وأوروبا. وتحولت اللقاحات في عام ٢٠٢٠ إلى مسألة تجسس ملموس مع كشف وكالة تجسس كورية جنوبية في فبراير من عام ٢٠٢١ عن أن قراصنة كوريين شماليين سعوا لاختراق أنظمة كمبيوتر مجموعة «فايزر» العملاقة بحثاً عن معلومات حول اللقاح المضاد لوباء كوفيد-١٩ وعلاجاته[2].

وللقرصنة الإلكترونية تأثيرات سلبية على الإبداع والقطاع الثقافي عموماً؛ حيث تمثل الصناعات الثقافية والمعلوماتية الآن مكونات مهمة وفعالة ومعترف بها بشكل جيد في التطور الاقتصادي والثقافي لأية دولة، وبالتالي فإن أعمال السرقة التي تقوض هذه الصناعات لها تأثير سلبي واضح على الثروة الوطنية، والتنمية المستدامة[3].

وتُعد قرصنة برامج الحاسوب مشكلة عالمية، وقد بلغت الخسائر في اقتصاديات الدول المتقدمة والنامية قيمة هائلة بسبب هذا النوع من القرصنة الإلكترونية؛ لأن تطوير البرمجيات يتطلب استثمارات مالية كبيرة. كما أن الفيروسات والبرمجيات الخبيثة تُلحق أضراراً بالغة بالأجهزة والحواسيب المستهدفة تتراوح بين التعطيل الجزئي، وبين التشفير الكامل لكل ما تحتويه ذاكرة التخزين من ملفات، وفي بعض الحالات الأكثر خطورة تكون الإصابة بالبرمجيات الخبيثة مرتبطة بعمل منظم، حيث يطلب الجناة من الضحايا دفع مبالغ مالية مقابل إزالة التشفير واستعادة الملفات الرقمية المتضررة، وهو ما يُطلق عليه «جرائم الفدية» في مجال الجرائم الإلكترونية.

وبالرغم من أن التكنولوجيا الرقمية ساعدت على الانتشار الواسع للمصنفات الرقمية، وسهلت من تبادل البيانات والمعلومات بسرعة عالية وبتكلفة زهيدة، إلا أنها في نفس الوقت ساهمت وبشكل واسع في تعدد أشكال الاعتداء على الحقوق الواردة على هذه المصنفات، خاصةً القرصنة الإلكترونية التي تسببت في إشكاليات كبيرة ليس على الصعيد القانوني فقط، بل على الصعيدين الاقتصادي

---

١. راجع في ذلك مقال بعنوان: القرصنة الإلكترونية.. هل تعلم قيمة الخسائر التي تكبّدها للعالم؟ منشور على الرابط:
https://www.alaraby.co.uk/economy/%D8%A7%D984%%D982%%D8%B1%D8%B5%D9%86%D8%A9-%D8%A7%D984%%D8%A5%D984%%D983%%D8%AA%D8%B1%D98%8%D986%%D98%A%D8%A9-%D987%%D984-%%D8%AA%D8%B9%D984%%D985-%%D982%%D98%A%D985%%D8%A9-%D8%A7%D984%%D8%AE%D8%B3%D8%A7%D8%A6%D8%B1-%D8%A7%D984%%D8%AA%D98%A-%D8%AA%D983%%D8%A8%D991%%D8%AF%D987%%D8%A7-%D984%%D984%%D8%B9%D8%A7%D984%%D985%%D89%F

تاريخ الدخول: ٢٠٢٢/٩/١١

٢. المرجع السابق.

٣. داريل بانيثي، استمرار القرصنة وآثارها على الإبداع والثقافة والتنمية المستدامة، دراسة معدة بناء على طلب أمانة منظمة الأمم المتحدة للتربية والعلوم والثقافة في الجلسة الثالثة عشرة للجنة الدولية لحقوق المؤلف، باريس، ٢٠٠٥.

والفكري[1].

وبالإضافة إلى ما تقدم، فإن انتشار جرائم القرصنة الإلكترونية يمثل خطراً كبيراً على الفرد والمجتمع؛ حيث تؤدي هذه الجرائم إلى مشاكل تهدد الأمن والاقتصاد. ولا شك أن عدم القدرة على مكافحة الجرائم الإلكترونية داخل أي مجتمع يضر بالموثوقية الرقمية لبيئة الأعمال مما يؤثر سلباً على خطط التنمية الاقتصادية، وعملية التحول الرقمي، كما تؤثر الجرائم الإلكترونية المتعلقة بالمحتوى ونشر الشائعات والأخبار الكاذبة، والإرهاب الفكري، والسب، والقذف، والتشهير، وغيرها من الجرائم المرتكبة باستخدام تكنولوجيا المعلومات والاتصالات الحديثة بشكل مباشر على الاستقرار الاجتماعي، والأمن والسلم الأهلي.

ومن ناحية أخرى، فإن السلطات المختصة في كل دولة تواجه تحديات في مجال الإثبات الجنائي لجرائم القرصنة الإلكترونية، وما يترتب على ذلك من صعوبة ملاحقة مرتكبي هذه الجرائم والقبض عليهم وتقديمهم للعدالة، وتعويض المتضررين. فالإثبات الجنائي هو إقامة الدليل على وقوع الجريمة ونسبتها إلى فاعل معين، والهدف من ذلك هو بيان مدى التطابق بين النموذج القانوني للجريمة وبين الواقعة المعروضة. وتثير مسألة الإثبات في جرائم الإنترنت صعوبات كبيرة أمام القائمين على التحقيق؛ وذلك لعدة أمور منها التخزين الإلكتروني للمعطيات الذي يجعلها غير مرئية وغير مفهومة بالعين المجردة، ويُشكل انعدام الدليل المرئي المفهوم عقبة كبيرة أمام كشف الجرائم، وقد يشكل تشفير البيانات المخزنة إلكترونياً أو المنقولة عبر شبكات الاتصال عن بُعد عقبة أمام إثبات الجريمة المعلوماتية والبحث عن الأدلة، كما أن سهولة محو الدليل في زمن قصير تُعد من أهم الصعوبات التي تعترض العملية الإثباتية في مجال جرائم الإنترنت. وتتعقد المشكلة عندما يتعلق الأمر بمعلومات أو بيانات تم تخزينها في الخارج بواسطة شبكة الاتصال عن بُعد؛ حيث لا تكفي القواعد التقليدية في الإثبات لضبط مثل هذه المعلومات بحثاً عن الأدلة وتحقيقها[2].

المطلب الثالث
طرق مكافحة جرائم القرصنة الإلكترونية

لم يعد استخدام شبكة الإنترنت قاصراً على باحثي الجامعات والموظفين بالمؤسسات والهيئات العامة، بل اتجه إليها أيضاً الأفراد والمؤسسات الخاصة والمشروعات الخاصة لما في الإبحار عبر الشبكة من فوائد كثيرة، فقد تزايدت المعاملات الإلكترونية، والبحث عن المعلومات، وتبادل الخبرات في نواحٍ

---

١. طه عيساني، القرصنة الإلكترونية؛ الضرر الاقتصادي والفكري، بحث مقدم في جامعة الجزائر، منشور على منصة المنهل الإلكترونية على الرابط:

https://platform.almanhal.com/Files/292628/

تاريخ الدخول: ٢٠٢٢/٩/٢٧

فنية وصناعية متعددة[1].

ونظراً لانتشار جرائم القرصنة الإلكترونية ضد الأفراد والشركات والمؤسسات الخاصة والدول، فقد بذلت الشركات والمؤسسات الكبرى والحكومات جهوداً كبيرة بغرض توفير الطرق المناسبة لمكافحة جرائم القرصنة الإلكترونية، كما عملت على تطوير منظومات إلكترونية متكاملة للحماية والحد من مخاطر هذه الجرائم.

وفي هذا المجال، تنشط شركات تقنية المعلومات جاهدة في إنتاج ما هو جديد لحماية البيانات والمعلومات المتداولة عبر شبكات الحاسب الآلي وكذلك برامج هذا الحاسب؛ لأن هواة اختراق هذه الشبكات أو المخترقين من هؤلاء لا يكفون عن التجول عبر الشبكة الدولية للإنترنت، ومحاولة اقتحام مواقع هذه الشبكة أياً كانت الجهة التابعة لها أو التي تتولى حمايتها، فهم يخترقون مواقع المصارف والمؤسسات المالية والشركات الصغرى والكبرى والمؤسسات العسكرية متى كان ذلك ممكناً. ومن مظاهر تلك الحماية استخدام برامج الجدران النارية، وهي عبارة عن فلاتر معلوماتية يكون مكانها مدخل ومخارج الشبكات في الإدارة الإلكترونية بحيث تتحكم في عملية دخول وخروج المعلومات أو البيانات، وكذلك يمكن تشفير البيانات والمعلومات المتداولة عبر الشبكة، وهذا التشفير يعني تحويل الكلمات المكتوبة إلى أرقام أو إلى صورة رقمية لا يمكن معرفة مضمونها إلا عن طريق فك الشفرة ذاتها، كما يمكن حفظ نسخ إضافية من البيانات والمعلومات المتداولة في مكان آمن بحيث يسهل استرجاعها في حال حصول تلف أو تدمير لمعلومات الحكومة الإلكترونية[2].

وتحرص الشركات والمؤسسات الخاصة على التأكد من أن موظفيها جاهزون ومستعدون بشكل جيد لمواجهة جرائم القرصنة الإلكترونية؛ حيث إن هناك عاملاً واحداً مشتركاً يجمع بين العديد من الشركات التي وقعت فريسة لمجرمي الإنترنت، وهو عدم الاستعداد وعدم تلقي الموظفين التدريب اللازم. ولذلك تعمل الشركات على نشر الوعي بين موظفيها ليدرك كل منهم أن أمن الإنترنت جزء من وظائفهم، وأن التحدي الرئيسي يتمثل في جعلهم يفهمون أن أمن المعلومات هو مسئولية الجميع، وليس فقط مسئولية فريق تكنولوجيا المعلومات.

ولا ريب أن نشر الثقافة الأمنية بين موظفي الشركات والمؤسسات الخاصة يعني أن الموظفين سوف يكونون أكثر يقظة وأقل عرضة للانخداع بالحيل الإلكترونية، وبدون هذه الثقافة يمكن أن تصبح أية شركة أو مؤسسة معرضة للهجوم الإلكتروني.

ويُعد التدريب العملي وسيلة مهمة لجعل واقع الجريمة الإلكترونية أكثر واقعية للموظفين، في الوقت الذي يُختبر فيه كيفية الاستجابة للتهديدات. وينبغي أن يتم هذا التدريب بالاقتران مع تدابير وقائية

---

١. د. شحاته غريب شلقامي، التعاقد الإلكتروني في التشريعات العربية دراسة مقارنة، دار الجامعة الجديدة، ص ٨ وما بعدها.

٢. مستشار د. عبدالفتاح بيومي حجازي، النظام القانوني للحكومة الإلكترونية، الكتاب الثاني الحماية الجنائية والمعلوماتية للحكومة الإلكترونية، دار الكتب القانونية، ٢٠٠٧، ص ٨ وما بعدها.

مثل تطبيق ضوابط ومرشحات مكافحة الانتحال، وحماية الحسابات بما يعرف بالتوثيق الثنائي[1].

ومن المعلوم أن القانون المحلي في جميع دول العالم يُجرم عمليات القرصنة الإلكترونية، ومع ذلك نجد دولاً وشركات كبرى لجأت إلى ما يمكن تسميته بالقرصنة المشروعة أو القرصنة الحميدة أو القرصنة الأخلاقية عبر التعاقد مع قراصنة معلومات ودّيين يهاجمون أنظمتها لرصد نقاط ضعفها، ومن ثم تعمل على مواجهة هذه المشكلات، ووضع الحلول المناسبة لها في إطار الاستعداد لمنع الاختراقات الإلكترونية المُحتملة في ظل زيادة تهديدات القرصنة الإلكترونية.

وتُعد القرصنة المشروعة أو القرصنة الأخلاقية من أهم الطرق التي شاع استخدامها في الفترة الأخيرة من جانب العديد من الدول والمؤسسات والشركات في إطار حرصها على التصدي لجرائم القرصنة الإلكترونية بصورة فعّالة.

وتؤدي القرصنة الأخلاقية مهمة معاكسة لما تقوم به القرصنة الضارة؛ حيث تتضمن القرصنة الأخلاقية محاولة مصرح بها للوصول غير المصرح به إلى نظام كمبيوتر، أو تطبيق، أو بيانات. ويعتمد تنفيذ الاختراق الأخلاقي على تكرار إستراتيجيات وأفعال المهاجمين الضارين المفسدين. وتساعد هذه الممارسة في تحديد الثغرات الأمنية التي يمكن حلها بعد ذلك قبل أن تُتاح الفرصة للمهاجمين الضارين لاستغلالها.

ويُعرف المتسللون أو القراصنة الأخلاقيون، المعروفون أيضاً باسم «القبعات البيضاء»، بأنهم خبراء أمنيون يقومون بإجراء هذه التقييمات الأمنية. ويساعد العمل الاستباقي الذي يقومون به على تحسين الوضع الأمني للمؤسسة أو الشركة بموافقة مسبقة من المؤسسة أو الشركة أو مالك أصول تكنولوجيا المعلومات[2].

وباتت اليوم هيئات عدّة كبيرة مثل البنتاجون، والبنوك، وشركات الطيران، وعمالقة التكنولوجيا، وأخرى أصغر حجماً تُحصى بالآلاف، تعرض برامج مكافآت تُعرف بـ (غنيمة رصد أوجه الخلل). وتضم أكبر منصة للقراصنة الودّيين "هاكر وان" أكثر من ٨٠٠ ألف عضو تقريباً. وفي عام ٢٠٢٠، قدّم العملاء مكافآت مالية بلغت مستوى قياسي عند ٤٤ مليون دولار. وقد تكون العائدات التي يجنيها قراصنة المعلومات كبيرة جداً، فقد تخطّى مئتان من مصطادي نقاط الخلل عتبة الـ ١٠٠ ألف

---

١. راجع في ذلك مقال للكاتب روب وو بعنوان: ما المهارات المطلوبة لمكافحة القرصنة الإلكترونية؟، منشور على الرابط:
https://1-a1072.azureedge.net/news/presstour/201818/7//%D985%%D8%A7-%D8%A7%D984%%D985%%D987%%D8%A7%D8%B1%D8%A7%D8%AA-%D8%A7%D984%%D985%%D8%B7%D984%%D988%%D8%A8%D8%A9-%D984%%D985%%D-983%%D8%A7%D981%%D8%AD%D8%A9-%D8%A7%D984%%D982%%D8%B1%D8%B5%D986%%D8%A9

تاريخ الدخول: ٢٠٢٢/٩/٨

٢. راجع في ذلك بحث بعنوان: ethical hacking منشور على الرابط:
https://www.synopsys.com/glossary/what-is-ethical-hacking.html

تاريخ الدخول: ٢٠٢٢/١٠/٥

دولار من المكافآت منذ بدء تعاونهم مع المنصة المشار إليها، وتجاوز تسعة منهم عتبة المليون دولار[1].

وفي إطار مكافحة ومواجهة جرائم القرصنة الإلكترونية، ينبغي على جميع مستخدمي شبكة الإنترنت المشاركة في هذه العملية، وحماية معلوماتهم الشخصية، وتفادى الهجمات الإلكترونية من خلال اتباع قواعد وسلوكيات الحماية الإلكترونية بأنفسهم كخط دفاع أول، وذلك عن طريق عدم الوثوق في أي شخص غريب، وعدم مناقشة الأمور الشخصية على شبكة الإنترنت، وعدم إرسال أي صور أو فيديوهات شخصية لأي شخص، أو نشر بيانات شخصية عبر الإنترنت، مثل العناوين وأرقام الهواتف وعناوين البريد الإلكتروني، وعدم الإفصاح عن كلمات المرور الخاصة لأي شخص، كما يجب استخدام كلمات عبور معقدة، والعمل على تغييرها باستمرار، ويجب المحافظة على إعدادات الخصوصية القوية على الحسابات في تطبيقات التواصل الاجتماعي، واستخدام خاصية التحقق الثنائي إن وجدت، ويتعين عدم التعامل مع رسائل البريد الإلكتروني المرسلة من الغرباء لأنها قد تحتوي على برمجيات خبيثة، وعدم تداول التطبيقات والبرمجيات مجهولة المصدر، فضلاً عن سرعة الإبلاغ في حال التعرض لنشاط إلكتروني مشبوه، وعدم التردد في التواصل مع الجهات المختصة في الدولة بشأن ذلك.

ولا يفوتنا أن ننوه إلى أن مواجهة جرائم القرصنة الإلكترونية لا تقتصر على الجانب التقني فقط، وما قد يعتبره البعض هجمات غير ذات صلة في فترات مختلفة قد يكون جزءاً من إستراتيجية هجومية شاملة؛ لأنه من المألوف أن تقوم المنظمات الإلكترونية الإجرامية بعمليات هجومية صغيرة لمعرفة الأصول والمواقع الإستراتيجية المطلوبة لعمليات لاحقة أكثر شمولاً. ولذلك يجب أخذ الحيطة والحذر عند تلقي أي تهديد إلكتروني مهما كان حجمه، كما يجب الوقوف على نقاط القوة والضعف في النظام المطلوب حمايته.

المبحث الثاني
التنظيمُ القانوني لتجريم ظاهرة القرصنة الإلكترونية في ضوء التشريع البحريني

جذبت مشكلة جرائم القرصنة الإلكترونية الانتباه الدائم من قبل صُنّاع السياسة الحكوميين، والمسئولين عن إنفاذ القانون من أجل مكافحة هذه الجرائم، كما ركزت المعاهدات والاتفاقيات الدولية والإقليمية على مواجهة هذه المشكلة والحد منها؛ وذلك باعتبار أن القرصنة الإلكترونية تُعد من أخطر أشكال الجرائم الإلكترونية ذات الطبيعة المتطورة.

وفي مملكة البحرين، اهتمت السلطة التشريعية بوضع تنظيم قانوني متطور لتجريم ظاهرة القرصنة الإلكترونية وتحديد صور جرائمها بهدف مكافحتها والحد من انتشارها؛ كما تحرص على تحديث القوانين ذات العلاقة بهذه الجرائم، والتي أصبحت خطراً وتحدياً من التحديات الكبيرة التي تواجه الأفراد والشركات، بل والوزارات والجهات الحكومية ذاتها.

---

١. راجع في ذلك مقال بعنوان: هل ما نعرفه عن قراصنة الإنترنت صحيح؟ مرجع سابق.

وقد تبلور هذا الاهتمام في إصدار عدة قوانين حديثة بشأن جرائم تقنية المعلومات، وحماية البيانات الشخصية، وتنظيم المعاملات الإلكترونية، من أبرزها القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات، وقانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.

كما انضمت المملكة لعدة اتفاقيات دولية وإقليمية تستهدف مكافحة جرائم القرصنة الإلكترونية، والجريمة المنظمة عبر الحدود الوطنية، والفساد بصفة عامة. وفي هذا السياق صدرت عدة قوانين منها القانون رقم (٤) لسنة ٢٠٠٤ بالموافقة على انضمام مملكة البحرين إلى اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والبروتوكولين المكملين لها، والقانون رقم (٢) لسنة ٢٠١٧ بالتصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والقانون رقم (٤) لسنة ٢٠١٧ بالتصديق على الاتفاقية العربية لمكافحة الجريمة المنظَّمة عبر الحدود الوطنية، والقانون رقم (٦) لسنة ٢٠١٧ بالتصديق على الاتفاقية العربية لمكافحة الفساد.

وكذلك أبرمت المملكة عدة اتفاقيات ثنائية مع بعض الدول الأخرى بغية العمل على مكافحة هذا النوع من الجرائم الضارة، ومن ذلك صدور القانون رقم (٥) لسنة ٢٠١٧ بالتصديق على الاتفاقية بين حكومة مملكة البحرين وحكومة جمهورية الهند بشأن التعاون لمكافحة الإرهاب الدولي والجريمة المنظَّمة عبر الوطنية والإتجار غير المشروع بالعقاقير والمخدرات والمؤثرات العقلية والسلائف الكيميائية، والقانون رقم (٤١) لسنة ٢٠١٨ بالتصديق على الاتفاقية بين حكومة مملكة البحرين وحكومة جمهورية قبرص بشأن التعاون في مكافحة الإرهاب والجريمة المنظَّمة والإتجار بالمخدرات والمؤثرات العقلية والهجرة غير المشروعة والجرائم الجنائية الأخرى المنصوص عليها في الاتفاقية.

وقد حرص المشرع البحريني على النص صراحة على حظر غسل الأموال المُتحصَّلة من جرائم القرصنة بسبب انتشارها الواسع في وقتنا الحالي؛ حيث تنص المادة (٢) من المرسوم بقانون رقم (٤) لسنة ٢٠٠١ بشأن حظر ومكافحة غسل الأموال وتمويل الإرهاب، المعدلة بالقانون رقم (٢٥) لسنة ٢٠١٣[١]، على أن «يحظر غسل الأموال المتحصَّلة من الجرائم التالية، وسواء وقعت هذه الجرائم في داخل المملكة أو خارجها:

أ) جرائم المخدرات والمؤثرات العقلية.

ب) جرائم الخطف والقرصنة.

ج) جرائم الإرهاب وتمويله...»

وبالإضافة إلى ما تقدم، تولي الحكومة في مملكة البحرين اهتماماً كبيراً بالأمن السيبراني كإحدى الركائز الرئيسية في المنظومة التقنية بالمملكة؛ حيث يعتمد ازدهار الاقتصاد ونموه على أمن البنية التحتية لقطاع الاتصالات وتقنية المعلومات. وتعتبر الحكومة أن ضمان تأمين البنية التحتية

١. أضيفت عبارة "وتمويل الإرهاب" بعد عبارة "غسل الأموال" أينما وردت في المرسوم بقانون رقم (٤) لسنة ٢٠٠١ بشأن حظر ومكافحة غسل الأموال عدا ما وردت في الفقرات (٢-١) و(٢-٣) و(٢-٤) و(٢-٥) بالمادة (٢)، والفقرة (٣-٢) بالمادة (٣)، والفقرتين (٤-٤) و(٤-٥) بالمادة (٤) بموجب القانون رقم (٥٤) لسنة ٢٠٠٦.

في المملكة ضد التهديدات السيبرانية والمادية هدفاً مستمراً، ويثبت ذلك تميزها بوجود منظومة واضحة لحوكمة الأمن السيبراني أو الأمن الإلكتروني متمثلة في الإدارة العامة لمكافحة الفساد والأمن الاقتصادي والإلكتروني، والمركز الوطني للأمن السيبراني التابعين لوزارة الداخلية.

وفي هذا الإطار انتهت محكمة التمييز البحرينية في حكم حديث إلى أنه ولئن كان البنك هو المسئول عن سحب أي مبالغ بطرق احتيالية غير مشروعة كأعمال القرصنة الإلكترونية وغيرها باعتبار أن مسئوليته تجاه هذه الأموال مسئولية مفترضة أساسها تحمل البنك تبعية مخاطر نشاطه، والتي تفرض عليه واجب اتخاذ ما يحول دون هذه المخاطر، غير أن تلك المسئولية ترتفع إذا ارتكب العميل خطأ فاحشاً حال دون اتخاذ البنك ما تقتضيه ظروف الحال بإيقاف الضرر الحاصل به وبالعميل[1].

وفي ضوء ما تقدم، وفي حدود أغراض البحث الماثل، تم تقسيم هذا المبحث إلى ثلاثة مطالب؛ حيث يوضح المطلب الأول أهم أحكام القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات، ويستعرض المطلب الثاني أبرز أحكام قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨، ويلقي المطلب الثالث الضوء على دور وزارة الداخلية في مكافحة جرائم القرصنة الإلكترونية.

المطلب الأول

١. راجع حكم محكمة التمييز البحرينية الصادر في الطعن رقم ٢١٠ لسنة ٢٠١٩ قضائية بجلسة ٢٠١٩/١٠/١، وقد ورد به ما يلي: أقيم الطعن على سبب واحد ينعى به الطاعن على الحكم المطعون فيه مخالفة القانون والخطأ في تطبيقه والقصور في التسبيب والفساد في الاستدلال والإخلال بحق الدفاع ، ذلك أنه تمسك في دفاعه أمام محكمة الموضوع أن عمليات سحب تمت من حسابه المصرفي لدى البنك المطعون ضده دون أن يجريها أو يعلم بها وقد أكد الخبير أن هذه السحوبات تمت بواسطة الصرف الآلي بمدينة تايوان بطريق القرصنة الإلكترونية رغم وجوده داخل مملكة البحرين أثناء إجراء هذه السحوبات مما تنعقد مسئولية البنك في رد المبالغ المخصومة من حسابه باعتبار أنها كانت وديعة لديه أثناء عملية القرصنة ولاسيما أن البنك – بخلاف ما تمسك به في دفاعه – لم يقم بإرسال أي رسالة نصية على هاتفه المحمول المدون بسجلات البنك – المطعون ضده – وطلب مخاطبة شركة الاتصالات لإثبات دفاعه في هذا الشأن، غير أن الحكم المطعون فيه رفض طلبه رغم جوهريته وقضى برفض الدعوى مما يعيبه ويستوجب نقضه. وحيث إن هذا النعي مردود، ذلك أنه ولئن كان البنك هو المسئول عن سحب أي مبالغ بطرق احتيالية غير مشروعة كأعمال القرصنة الإلكترونية وغيرها باعتبار أن مسئوليته تجاه هذه الأموال مسئولية مفترضة أساسها تحمل البنك تبعية مخاطر نشاطه والتي تفرض عليه واجب اتخاذ ما يحول دون هذه المخاطر، غير أن تلك المسئولية ترتفع إذا ارتكب العميل خطأ فاحشا حال دون اتخاذ البنك ما تقتضيه ظروف الحال بإيقاف الضرر الحاصل به وبالعميل، وكان الواقع الثابت بالأوراق أن حساب الطاعن لدى البنك قد أجريت عليه عمليات سحب خارج مملكة البحرين بواسطة بطاقته الائتمانية عن طريق جهاز الصرف الآلي في التواريخ ٢٠١٣/١٢/٨، ٢٠١٣/١٢/٩، ٢٠١٣/١٢/١٠، ٢٠١٣/١٢/١١، ٢٠١٣/١٢/١٢ بقيمة المبلغ المطالب به، وكان الطاعن قد قام بتغيير رقم هاتفه الذي أبلغ البنك المطعون ضده به وقت فتح الحساب ولم يقم بتجديد هذه البيانات لدى البنك كما تقضي التعليمات، وقد وافاه البنك بكشوف حسابه لديه ولم يحرك ساكنا ويسارع إلى البنك للإبلاغ عن عمليات السحب التي تمت ويدعي بعدم علمه أوصلته بها، وهو سلوك لا يتفق وسلوك الرجل الطبيعي في مثل هذه الظروف، وهو ما حال دون اتخاذ الإجراءات اللازمة، فإن مسئولية المطعون ضده ترتفع عنه بسبب هذا الخطأ الفاحش ولا يلومن الطاعن إلا نفسه، وإذ التزم الحكم الابتدائي المؤيد بالحكم المطعون فيه هذا النظر، فإنه لا يكون قد خالف القانون، ويضحى النعي عليه غير سديد. ولما تقدم يتعين القضاء برفض الطعن وإلزام الطاعن بمصاريف الطعن.

أهم أحكام قانون جرائم تقنية المعلومات[1]

مع التطور التقني السريع والمستمر وانتشار استخدام شبكة الإنترنت وما ترتب على ذلك من ظهور نوع جديد من المجرمين يرتكبون جرائم إلكترونية عديدة قد يصعب التعامل معها، فقد بات من الأهمية بمكان وضع قانون رادع لكل شخص يستغل التكنولوجيا وشبكة الإنترنت لتنفيذ جرائمه وقرصنته الإلكترونية، ولذلك أصدر المشرع البحريني القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات.

ويُمثل هذا القانون حماية جنائية لكل من يستخدم التكنولوجيا وتقنية المعلومات؛ حيث يحدد جرائم تقنية المعلومات، والعقوبات المقررة لها، والإجراءات الخاصة بها، وذلك من أجل مكافحة هذه الجرائم والحد منها بشكل فعّال.

وباستقراء أحكام قانون جرائم تقنية المعلومات المشار إليه، نجد أن المشرع يحدد معاني معينة للعبارات والمصطلحات المستخدمة في هذا القانون باعتبار أنه قانون ينظم موضوعاً ذا طبيعة فنية خاصة، ويتناول الفصل الأول من القانون المذكور العقوبات الخاصة بجرائم تقنية المعلومات، والتي تم تقسيمها إلى ثلاثة أنواع، وهي: (١) الجرائم الواقعة على أنظمة وبيانات وسيلة تقنية المعلومات. (٢) الجرائم ذات الصلة بوسائل تقنية المعلومات. (٣) الجرائم ذات الصلة بالمحتوى. ويستعرض الفصل الثاني من القانون سالف الذكر الصلاحيات والسلطات الممنوحة للنيابة العامة والمحكمة المختصة بشأن جرائم تقنية المعلومات.

ونظراً لما يتمتع به قانون جرائم تقنية المعلومات المشار إليه من أهمية بالغة في إطار حرص المشرع البحريني على مواجهة جرائم القرصنة الإلكترونية، نستعرض أهم أحكامه التي تنظم الموضوعات سالفة الذكر، وذلك على النحو الآتي:

أولاً: تعريف المصطلحات المستخدمة في قانون جرائم تقنية المعلومات.

وضع المشرع في المادة (١) من قانون جرائم تقنية المعلومات المشار إليه تعريفات محددة لبعض الكلمات والعبارات والمصطلحات المستخدمة فيه باعتبار أنها عبارات ومصطلحات فنية دقيقة، ومن أبرزها عبارة «تقنية المعلومات» التي تشمل كل أشكال التقنية المستخدمة لإنشاء، ومعالجة، وتخزين، وتبادل، واستخدام، وعرض المعلومات بمختلف صيغها.

ويُقصد بكلمة «المعلومات» كل ما يمكن تخزينه، ومعالجته، وتوليده، ونقله باستخدام وسائل تقنية المعلومات، وبوجه خاص الكتابة، والصور الثابتة والمتحركة، والصوت، والأرقام، والحروف، والرموز، والإشارات، وغيرها.

وتم تعريف عبارة «وسيلة تقنية المعلومات» بأنها أية أداة، أو وسيلة إلكترونية، أو مغناطيسية، أو بصرية، أو كهروكيميائية، أو أية أداة تدمج بين تقنيات الاتصال والحوسبة، أو أية أداة أخرى لديها

١. القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات، منشور في الجريدة الرسمية العدد رقم (٣١٧٨) بتاريخ ٢٠١٤/١٠/٩.

القدرة على استقبال أو إرسال البيانات ومعالجتها وتخزينها واسترجاعها بسرعة فائقة.
ويُقصد بعبارة «نظام تقنية المعلومات» أداة أو مجموعة أدوات متصلة أو ذات صلة ببعضها، ويقوم واحد منها أو أكثر بمعالجة آلية لبيانات وسيلة تقنية المعلومات وفقاً لبرنامج.
ويُقصد بعبارة «بيانات وسيلة تقنية المعلومات» تمثيل لحقائق، أو لوقائع، أو لمعلومات، أو لمفاهيم في صورة مناسبة تسمح لنظام تقنية المعلومات بمعالجتها.
كما تم تعريف كلمة «برنامج» بأنها مجموعة تعليمات معبراً عنها بكلمات، أو رموز، أو طرق، أو بصورة أخرى، إذا تضمنتها أي من الوسائط التي يمكن قراءتها آلياً، تكون قادرة على جعل وسيلة تقنية المعلومات تؤدي عملاً معيناً أو تحدث نتيجة محددة.
ويُقصد بعبارة «مزود خدمة» أي مما يأتي: (أ) أية جهة عامة أو خاصة توفر لمستخدمي خدمتها إمكانية الاتصال بواسطة نظام تقنية المعلومات. (ب) أية جهة أخرى تقوم بمعالجة أو تخزين بيانات وسيلة تقنية المعلومات نيابة عن الجهة المشار إليها في البند (أ) سالف الذكر، أو عن مستخدمي خدماتها.
ويُقصد بعبارة «بيانات خط السير» بيانات وسيلة تقنية المعلومات ينتجها نظام تقنية المعلومات خاصة بالاتصال بواسطة نظام تقنية المعلومات تشكل جزءاً من سلسلة هذا الاتصال.
وكذلك يُقصد بعبارة «بيانات المحتوى» بيانات وسيلة تقنية المعلومات، خلافاً لبيانات خط السير، يتم إرسالها كجزء من اتصال. وتم تعريف كلمة «تلف» بأنها تعييب، أو تعطيل، أو إلغاء، أو حذف، أو تدمير، أو تغيير، أو تعديل، أو تحريف، أو حجب بيانات وسيلة تقنية المعلومات، أو تعييب أو إعاقة نظام تقنية المعلومات.
ويُقصد بمصطلح «التشفير» عملية تحويل المعلومات، أو نظم، أو وسائل تقنية المعلومات، أو الاتصالات إلى رموز غير مفهومة أو مبعثرة بحيث يصعب قراءتها أو معرفتها دون إعادتها إلى هيئتها الأصلية باستخدام كلمة سرية معينة أو أداة التشفير المستخدمة.

ثانياً: الجرائم الواقعة على أنظمة وبيانات وسيلة تقنية المعلومات.

من المستقر عليه أن الجريمة تقوم على ثلاثة أركان، وهي الركن القانوني (الشرعي)، والركن المادي، والركن المعنوي. والمقصود بالركن القانوني الصفة غير المشروعة للفعل، ويعني مبدأ شرعية الجرائم والعقوبات أنه لا عقوبة ولا جريمة إلا بنص في القانون، وهذا معناه أن القاضي لا يملك خلق جريمة جديدة أو عقوبة جديدة لجريمة قائمة، وإنما يلزم لخلق شيء من ذلك تدخل التشريع ذاته[1].
ولذلك يقضي الدستور البحريني في المادة (٢٠/أ) منه بأنه لا جريمة ولا عقوبة إلا بناء على قانون.
ويتمثل مبدأ شرعية الجرائم والعقوبات بالنسبة إلى الجرائم الإلكترونية فيما ورد النص عليه في قانون جرائم تقنية المعلومات المشار إليه.

---

١. د. محمد زكي أبوعامر، قانون العقوبات القسم العام، الدار الجامعية، بيروت، ١٩٩٣، ص ٢٤.

ويُقصد بالركن المادي ماديات الجريمة؛ أي المظهر الذي تبرز به إلى العالم الخارجي، ويقوم هذا الركن على ثلاثة عناصر، وهي الفعل (السلوك الإجرامي)، والنتيجة، وعلاقة السببية.

أما الركن المعنوي فيُقصد به الإرادة التي يقترن بها الفعل سواء في صورة القصد أو الخطأ. والركن المعنوي في الجريمة هو الحالة النفسية للجاني، والعلاقة التي تربط ماديات الجريمة وشخصية الجاني، فهذا الركن هو المسلك الذهني أو النفسي للجاني باعتباره محور القانون الجنائي؛ ذلك أنه في إطار هذا الركن تتوافر كافة مقومات المسئولية الجنائية من علم، وإرادة آثمة، وقصد إجرامي، مع إقرار حق الدولة في العقاب الذي يُبنى على هذه المقومات. ويتوافر القصد الجنائي في حق الجاني في ثلاث حالات، وهي الأولى: إذا كان الجاني يتوقع ويريد أن يترتب على فعله أو امتناعه حدوث الضرر أو وقوع الخطر الذي حدث والذي يعلق عليه القانون وجود الجريمة. الثانية: إذا نجم عن الفعل أو الامتناع ضرر أو خطر أكثر جسامة مما كان يقصده الفاعل، وهي حالة جواز القصد التي ينص القانون صراحة على إمكان ارتكابها بهذا الوصف. الثالثة: الحالات التي يعزى فيها القانون الفعل إلى الفاعل نتيجة لفعله أو امتناعه، أي حالات يفترض فيها القانون توافر القصد الجنائي لدى الجاني، وهو ما يُطلق عليه «العمد المفترض»، وهو مستمد من أنه طالما أن النتيجة الجسيمة التي تحققت نشأت عن فعل الجاني، فمقتضى ذلك أن هذا الفعل كان صحيحاً لإحداثها، ولكونه كذلك، فإن الجاني يجب أن يتحمل نتائجه، سواء توقعها أم لم يتوقعها.

ويُعد توافر الركن المعنوي في الجرائم الإلكترونية من الأمور الأساسية في تحديد طبيعة السلوك المرتكب وتكييفه لتحديد النصوص التي يلزم تطبيقها؛ إذ بدون الركن المعنوي لن يكون هناك سوى جريمة واحدة هي جريمة الدخول غير المشروع على نظام المعالجة الآلية للبيانات. أما جريمة تجاوز الصلاحيات في الدخول على هذا النظام يلزم لتوافرها أن يكون هناك صلاحية للدخول على نظام ما، وأن تتوافر في هذا النظام أنظمة معينة ليس من حق هذا الشخص الدخول عليها، فيقوم المذكور بالدخول على أي من هذه الأنظمة، وفي هذه الحالة لا تتوافر سوى جريمة واحدة حيث إن المذكور يملك صلاحية الدخول على النظام الأساسي ولا يملك الدخول على أنظمة خاصة فيها. ويلزم لتكوين النشاط المادي هنا أن يكون السلوك الإجرامي مرتكباً في إطار نشاط ثان وليس النشاط الأول، ومثل هذا الأمر يجعل جريمة تجاوز صلاحيات الدخول من الجرائم التي لا تتطلب ركناً معنوياً، وهذا الأمر غير صحيح في القانون[1].

وقد قرر المشرع البحريني في قانون العقوبات الصادر بالمرسوم بقانون رقم (١٥) لسنة ١٩٧٦ أنه لا يجوز مساءلة الشخص عن جريمة إلا إذا قام بها عمداً أو خطأ؛ حيث تنص المادة (٢٤) من هذا القانون على أن «لا يسأل شخص عن جريمة إلا إذا ارتكبها عمداً أو خطأ.»

١. راجع في ذلك عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية دراسة مقارنة، مرجع سابق، ص ٢٩ وما بعدها.

وقد بينت المادة (٢٥) من قانون العقوبات المشار إليه الجريمة العمدية؛ إذ تنص على أن «تكون الجريمة عمدية إذا اقترفها الفاعل عالماً بحقيقتها الواقعية وبعناصرها القانونية. وتعتبر الجريمة عمدية كذلك إذا توقع الفاعل نتيجة إجرامية لفعله فأقدم عليه قابلاً المخاطرة بحدوثها.»

كما بينت المادة (٢٦) من قانون العقوبات ذاته الجريمة غير العمدية؛ إذ تنص على أن «تكون الجريمة غير عمدية إذا وقعت النتيجة الإجرامية بسبب خطأ الفاعل. ويعتبر الخطأ متوافراً سواء توقع الفاعل نتيجة فعله أو امتناعه وحسب أن في الإمكان اجتنابها أو لم يتوقعها وكان ذلك في استطاعته، أو من واجبه.»

وقد حددت المادة (٢٧) من قانون العقوبات ذاته متى ينتفي العمد؛ إذ تنص على أن "ينتفي العمد إذا وقع الفعل المكون للجريمة بناء على غلط في واقعة تعد عنصراً من عناصرها القانونية أو في ظرف لو تحقق لكان الفعل مباحاً. على أن ذلك لا يمنع من عقاب الفاعل على ما قد يتخلف عن فعله من جريمة غير عمدية أو أية جريمة أخرى."

وانطلاقاً مما تقدم، فقد وضع المشرع في قانون جرائم تقنية المعلومات المشار إليه عقوبات جنائية لكل من يرتكب جريمة من الجرائم الواقعة على أنظمة وبيانات وسيلة تقنية المعلومات؛ حيث تقضي المادة (٢) من هذا القانون بأن يُعاقب بالحبس مدة لا تزيد على سنة وبالغرامة التي لا تجاوز ثلاثين ألف دينار أو بإحدى هاتين العقوبتين، كل من قام دون مسوغ قانوني بالدخول إلى نظام تقنية المعلومات أو جزء منه. وإذا نتج عن الدخول إفشاء للبيانات المخزنة في وسيلة أو نظام تقنية المعلومات أو جزء منه عُدّ ذلك ظرفاً مشدداً[١].

ويتضح من ذلك أن المشرع يجرم الدخول إلى نظام تقنية المعلومات أو جزء منه إذا كان دخولاً غير مشروع؛ أي لا يستند إلى مسوغ قانوني، ويقرر المعاقبة على ذلك بالحبس مدة لا تزيد على سنة وبالغرامة التي لا تجاوز ثلاثين ألف دينار أو بإحدى هاتين العقوبتين، وإذا نتج عن هذا الولوج غير المشروع إفشاء للبيانات المخزنة في وسيلة أو نظام تقنية المعلومات أو جزء منه، يعتبر ذلك ظرفاً مشدداً[٢].

وتتحقق جريمة الاعتداء أو اختراق جهاز الحاسب الآلي أو المواقع في الشبكة المعلوماتية بطريقة غير مشروعة بأن يدخل الجاني لصفحات المواقع الإلكترونية ويقوم بالاطلاع على البيانات والمعلومات الموجودة بها دون أن يكون مصرحاً له بذلك. وقد يكون الدخول مباشراً أو غير مباشر، فيكون مباشراً باستخدام أجهزة الإخراج مثل الشاشة أو الطابعة أو السماعات الملحقة بالجهاز، وقد

---

١. راجع المادة (٢) من القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات.

٢. تجدر الإشارة إلى أن المادة (٧٦) من قانون العقوبات الصادر بالمرسوم بقانون رقم (١٥) لسنة ١٩٧٦ تنص على أن "عند توافر ظرف من الظروف المشددة في الجريمة يجوز توقيع العقوبة على الوجه الآتي:

إذا كانت العقوبة المقررة أصلاً للجريمة هي الغرامة ضوعف حدها الأقصى أو قضي بالحبس بدلاً منها. فإذا كانت الحبس ضوعف الحد الأقصى. وإذا كانت السجن الذي يقل حده الأقصى عن خمس عشرة سنة وصل إلى هذا الحد فإن كانت السجن المؤقت وصل إلى السجن المؤبد.»

يكون الدخول غير مباشر كالدخول غير المصرح به لشبكات الاتصال والمعالجة عن بُعد ويكون عادة بالتقاط المعلومات المتواجدة بين النظام المعلوماتي والنهاية الطرفية، أو التقاط الإشعاعات الصادرة عن النظام المعلوماتي وتتم هذه الطريقة بوسيلة إلكترونية عن طريق اعتراض بيانات إلكترونية وتسجيلها والتلاعب بها ثم إعادة ارسالها، أو الدخول غير المشروع من خلال النظام المعلوماتي أو معرفة كلمة السر أو مفتاح الشفرة المخول للدخول.

وقد أقر القضاء الفرنسي مجموعة من المبادئ التي يجب إعمالها في حالة دخول أحد الأشخاص للمواقع الإلكترونية والاطلاع على بياناتها تتلخص في: (١) استئذان أو إخطار صاحب الموقع المراد استغلال البيانات أو المعلومات الموجودة في موقعه. (٢) احترام القوانين واللوائح التي تحكم حق الملكية الذهنية. وقد قضت إحدى المحاكم الفرنسية بأن التعدي على المواقع الإلكترونية دون احترام المبادئ السابقة يشكل سلوكاً متطفلاً ويعتدي على عمل وجهود الآخرين المالية[١].

ويتحقق الركن المعنوي لجريمة اختراق المواقع الإلكترونية بتحقق القصد الجنائي المتمثل في علم الجاني بأن الفعل الذي يقوم به، وهو الاتصال بهذا الموقع، فعل غير مشروع ويمس مصلحة الغير، واتجاه إرادته لإتمام وقيام هذا الاتصال، أما إذا ما بقي في الموقع الإلكتروني الذي دخله بطريق غير مشروع مع علمه بذلك فتتحقق جريمة البقاء في الموقع الإلكتروني التي تتطلب قصداً خاصاً. ونظراً للصعوبات التي تعتري التحقق من توافر القصد الجنائي في عملية الدخول والبقاء غير المشروع في المواقع الإلكترونية، فإنها تبقى مسألة موضوعية ينفرد لتحديدها قاضي الموضوع؛ حيث يبحث في الموضوع من عدة جوانب من حيث توافر القصد من عدمه، والغاية من الدخول، ووجود برامج حماية لهذا الموقع من الاختراق، أو طلب كلمة سر، أو توقيع إلكتروني، وما في حكمها[٢].

وتقضي المادة (٣) من قانون جرائم تقنية المعلومات المشار إليه بمعاقبة كل من أحدث تلفاً في بيانات وسيلة تقنية المعلومات أو نظام تقنية المعلومات بالحبس وبالغرامة التي لا تجاوز خمسين ألف دينار أو بإحدى هاتين العقوبتين، وتُضاعف العقوبة إذا ترتب على ارتكاب الجريمة إعاقة لسير أي من المرافق العامة أو لأعمال ذات منفعة عامة، أو تهديد لحياة الناس، أو أمنهم، أو صحتهم، أو مساس بسلامة بدن إنسان، أو تغيير، أو تعييب، أو شطب، فحوص طبية، أو تشخيص طبي أو علاج إنسان. وتكون العقوبة السجن المؤبد أو المؤقت إذا ترتب على ارتكاب الجريمة موت إنسان عمداً[٣].

كما تقرر المادة (٤) من القانون ذاته بأن يُعاقب بالحبس وبالغرامة التي لا تجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين كل من تنصت أو التقط أو اعترض دون مسوغ قانوني مستخدماً وسائل فنية، إرسالاً غير موجه للعموم لبيانات وسيلة تقنية المعلومات، سواء كانت البيانات مرسلة من نظام تقنية المعلومات أو إليه أو ضمنه، ويشمل هذا الإرسال أي انبعاثات لموجات كهرومغناطيسية من نظام

١. حنان ريحان مبارك المضحكي، الجرائم المعلوماتية دراسة مقارنة، مرجع سابق، ص ١٠١ وما بعدها.

٢. المرجع السابق، ص ١٠٧.

٣. راجع المادة (٣) من القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات.

تقنية المعلومات تحمل معها هذه البيانات. وإذا نتج عن التنصت، أو الالتقاط، أو الاعتراض، إفشاء للإرسال أو جزء منه دون مسوغ قانوني، عُدّ ذلك ظرفاً مشدداً[١].

وتقضي المادة (٥) من القانون ذاته بمعاقبة كل من قام بإرسال بيانات وسيلة تقنية المعلومات تتضمن تهديداً بإحداث تلف لحمل غيره على أن يقدم له أو لغيره عطية أو مزية من أي نوع أو أداء عمل أو الامتناع عنه، بالحبس وبالغرامة التي لا تجاوز ثلاثين ألف دينار أو بإحدى هاتين العقوبتين، وتكون العقوبة السجن مدة لا تزيد على خمس سنين والغرامة التي لا تجاوز ستين ألف دينار إذا بلغ الجاني مقصده[٢].

ثالثاً: الجرائم ذات الصلة بوسائل تقنية المعلومات.

أورد المشرع في قانون جرائم تقنية المعلومات عدة أحكام للجرائم ذات الصلة بوسائل تقنية المعلومات، وذلك في المواد (٧) و(٨) و(٩) من القانون المذكور؛ حيث تقرر المادة (٧) معاقبة كل من قام بإدخال، أو تعييب، أو تعطيل، أو إلغاء، أو حذف، أو تدمير، أو تغيير، أو تعديل، أو تحريف، أو حجب بيانات وسيلة تقنية المعلومات تخص إحدى المصالح الحكومية أو الجهات التي ورد ذكرها في المادة (١٠٧) من قانون العقوبات، على نحو من شأنه إظهار بيانات غير صحيحة على أنها صحيحة، بنية استعمالها كبيانات صحيحة، سواء كانت هذه البيانات مفهومة بشكل مباشر أو غير مباشر، بالسجن مدة لا تزيد على عشر سنوات. وتكون العقوبة الحبس إذا ارتكبت الجريمة بشأن بيانات وسيلة تقنية المعلومات لا تخص إحدى المصالح أو الجهات المشار إليها إذا كان من شأن ذلك إحداث ضرر[٣].

ويلزم لتحقيق القصد الجنائي لدى الجاني في الجريمة سالفة الذكر أن يكون سلوكه اتجه إلى إدخال، أو تعييب، أو تعطيل، أو إلغاء، أو حذف، أو تدمير، أو تغيير، أو تعديل، أو تحريف، أو حجب بيانات وسيلة تقنية المعلومات تخص إحدى المصالح الحكومية أو الجهات المذكورة في المادة (١٠٧) من قانون العقوبات، وأن يكون عالماً بأن سلوكه يترتب عليه إظهار بيانات غير صحيحة على أنها صحيحة بنية استعمالها كبيانات صحيحة، وأن تتجه إرادته إلى ذلك[٤].

---

١. راجع المادة (٤) من القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات.

٢. راجع المادة (٥) من القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات.

٣. راجع المادة (٧) من القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات.

٤. جدير بالذكر أن المادة (١٠٧) من قانون العقوبات الصادر بالمرسوم بقانون رقم (١٥) لسنة ١٩٧٦ تقضي بأن المقصود بالموظف العام في حكم قانون العقوبات هم القائمون بأعباء السلطة العامة والعاملون في وزارات الحكومة ومصالحها ووحدات الإدارة المحلية، وأفراد القوات المسلحة، وأعضاء المجالس والوحدات التي لها صفة نيابية عامة سواء كانوا منتخبين أو معينين، وكل من فوضته إحدى السلطات العامة في القيام بعمل معين وذلك في حدود العمل المندوب له، ورؤساء وأعضاء مجالس الإدارة والمديرون وسائر العاملين في الهيئات والمؤسسات العامة والوحدات التابعة لها، ورؤساء وأعضاء مجالس الإدارة والمديرون وسائر العاملين في الشركات وفي أية كيانات أخرى مهما كانت طبيعتها، شريطة أنْ تكون تلك الجهات مملوكة بالكامل للدولة أو لإحدى الهيئات أو المؤسسات العامة أو الوحدات التابعة لها.

وتقضي المادة (٨) من قانون جرائم تقنية المعلومات المشار إليه بأن يُعاقب بالحبس من توصل دون مسوغ قانوني إلى الاستيلاء على مال مملوك للغير، أو حصل على أية مزية لنفسه أو لغيره، أو إلى توقيع سند أو إلغائه أو إتلافه أو تعديله باتخاذ اسم كاذب أو صفة غير صحيحة أو بالاستعانة بطريقة احتيالية، وذلك من خلال إدخال، أو تعييب، أو تعطيل، أو إلغاء، أو حذف، أو تدمير، أو تغيير، أو تعديل، أو تحريف، أو حجب بيانات وسيلة تقنية المعلومات، أو عن طريق القيام بأي تدخل في عمل نظام تقنية المعلومات[١].

وتُعد هذه الجريمة من الجرائم العمدية، ويتحقق الركن المعنوي لها بتحقق القصد الجنائي العام القائم على العلم والإرادة؛ أي العلم بعناصر الجريمة والإرادة التي تتجه إلى إحداث الضرر المترتب على هذه الجريمة فالجاني في هذه الجريمة يعلم أن المال الذي يقع عليه فعله مملوك للغير، وأن الفعل الذي سيؤتيه من شأنه أن يضر بهذا الغير، وتتجه إرادته إلى ذلك.

وتقرر المادة (٩) من قانون جرائم تقنية المعلومات المشار إليه معاقبة كل من قام باستخدام التشفير في سبيل ارتكاب، أو إخفاء أي من الجرائم المنصوص عليها في هذا القانون، أو أي قانون آخر، بالحبس وبالغرامة التي لا تجاوز مائة ألف دينار، أو بإحدى هاتين العقوبتين[٢].

ويتضح من ذلك أن المشرع يعاقب بالحبس وبالغرامة التي لا تجاوز مائة ألف دينار، أو بإحدى هاتين العقوبتين، كل من قام بعملية تحويل المعلومات، أو نظم، أو وسائل تقنية المعلومات، أو الاتصالات إلى رموز غير مفهومة أو مبعثرة بحيث يصعب قراءتها أو معرفتها دون إعادتها إلى هيئتها الأصلية باستخدام كلمة سرية معينة أو أداة التشفير المستخدمة، وذلك في سبيل ارتكاب أو إخفاء أي من الجرائم المنصوص عليها في قانون جرائم تقنية المعلومات المشار إليه، أو أي قانون آخر.

رابعاً: الجرائم ذات الصلة بالمحتوى.

حدد المشرع في قانون جرائم تقنية المعلومات المشار إليه صور الجرائم ذات الصلة بالمحتوى، ووضع لكل منها العقوبة المناسبة؛ حيث تقضي المادة (١٠) من هذا القانون بأن يُعاقب بالحبس مدة لا تقل عن سنة وبالغرامة التي لا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين، كل من أنتج مادة إباحية بقصد توزيعها بواسطة نظام تقنية المعلومات، أو استورد، أو باع، أو عرض للبيع أو الاستخدام، أو تداول، أو نقل، أو وزع، أو أرسل، أو نشر، أو أتاح مادة إباحية بواسطة نظام تقنية المعلومات. وتكون العقوبة هي الحبس مدة لا تقل عن سنتين وبالغرامة التي لا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين إذا كانت المادة الإباحية موجهة إلى الأطفال، أو وضعت في متناولهم.

كما تقضي المادة ذاتها بأن يُعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبالغرامة التي لا تجاوز ثلاثة آلاف دينار أو بإحدى هاتين العقوبتين كل من حصل لنفسه أو لغيره على مادة إباحية بواسطة نظام

---

١. راجع المادة (٨) من القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات.

٢. راجع المادة (٩) من القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات.

تقنية المعلومات، أو حاز مادة إباحية داخل نظام تقنية المعلومات، أو في أية وسيلة تقنية المعلومات. وتكون العقوبة الحبس مدة لا تقل عن ستة أشهر وبالغرامة التي لا تقل عن ثلاثة آلاف دينار أو بإحدى هاتين العقوبتين إذا كانت المادة الإباحية موجهة إلى الأطفال، أو وضعت في متناولهم[1].

خامساً: السلطات الممنوحة للنيابة العامة والمحكمة المختصة بشأن جرائم تقنية المعلومات.

وضع المشرع في الفصل الثاني من قانون جرائم تقنية المعلومات المشار إليه الإجراءات الخاصة بجرائم تقنية المعلومات التي تباشرها النيابة العامة وقاضي المحكمة الصغرى، وذلك في المواد من (١١) حتى (١٩) من القانون المذكور.

وبالاطلاع على أحكام هذه المواد، تبين أن المادة (١١) من القانون سالف الذكر تحدد الجرائم التي تسري عليها أحكام الفصل الثاني من هذا القانون، وهي: الجرائم المنصوص عليها في الفصل الأول من هذا القانون، والجرائم المنصوص عليها في أي قانون آخر إذا ارتكبت باستخدام نظام تقنية المعلومات، وجمع الأدلة التي تكون في صورة إلكترونية والمتعلقة بأية جريمة[2].

وفيما يتعلق بالسلطات والصلاحيات الممنوحة للنيابة العامة بخصوص جرائم تقنية المعلومات، نجد أن المشرع منح النيابة العامة صلاحية أن تأمر أي شخص بالقيام على وجه السرعة بالحفاظ على سلامة بيانات معينة لوسيلة تقنية المعلومات، بما في ذلك بيانات خط السير المخزنة داخل نظام تقنية المعلومات، تكون في حيازته أو تحت سيطرته، وبالإبقاء على سلامة هذه البيانات متى رأت الحاجة لذلك لإظهار الحقيقة في أية جريمة وتوافرت لديها دلائل تحملها على الاعتقاد بأن هذه البيانات عرضة للفقد أو التغيير.

ويجوز للنيابة العامة أن تأمر هذا الشخص بالحفاظ على البيانات والإبقاء على سلامتها لمدة لا تزيد على تسعين يوماً، وللمحكمة الكبرى الجنائية منعقدة في غرفة المشورة أن تأذن للنيابة العامة، بناء على طلب مشفوع بالمبررات يقدم قبل انقضاء المدة المشار إليها بثلاثة أيام، مد هذه الفترة لمدة أو لمدد متعاقبة لا يزيد مجموعها على تسعين يوماً أخرى.

ويحق للنيابة العامة أن تأمر هذا الشخص بالمحافظة على سرية الأمر الصادر له وفقاً لأحكام القانون لمدة لا تزيد على تسعين يوماً، قابلة للتجديد لمدة أو لمدد متعاقبة لا يزيد مجموعها على تسعين يوماً أخرى[3].

---

١. في تطبيق أحكام المادة (١٠) من القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات، يُقصد بعبارة "مادة إباحية عن الأطفال" التعريف الوارد للمواد الإباحية عن الأطفال في البروتوكول الاختياري الملحق باتفاقية حقوق الطفل بشأن بيع الأطفال وبغاء الأطفال والمواد الإباحية عن الأطفال.

٢. راجع المادة (١١) من القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات.

٣. راجع المادة (١٢) من القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات.

ويحق أيضاً للنيابة العامة أن تأمر أي شخص يكون حائزاً أو تحت سيطرته بيانات معينة لوسيلة تقنية المعلومات بتقديمها على وجه السرعة بما في ذلك البيانات المخزنة داخل نظام تقنية معلومات أو أية وسيلة تقنية المعلومات. وللنيابة العامة أن تأمر أي مزود خدمة بتقديم أية معلومات تكون في حيازته أو تحت سيطرته عن أي مشترك في خدماته أو مستخدم لها، سواء كانت هذه المعلومات في صورة بيانات وسيلة تقنية المعلومات أو في أية صورة أخرى، ولا يدخل في ذلك بيانات خط السير والمحتوى، وذلك كله متى رأت النيابة العامة الحاجة لذلك لإظهار الحقيقة في الجريمة[١].

ويجوز للنيابة العامة أن تصدر أمراً مسبباً بالدخول إلى وتفتيش نظام تقنية المعلومات المتصل بالجريمة، أو أي جزء منه، وأية بيانات لوسيلة تقنية المعلومات مخزنة فيه، وأي من وسائط تخزين بيانات وسيلة تقنية المعلومات التي من المحتمل أن يكون مخزناً عليها بيانات متصلة بالجريمة[٢].

كما منح المشرع للنيابة العامة سلطة الضبط والتحفظ على بيانات وسيلة تقنية المعلومات التي يتم الدخول إليها، ويشمل ذلك الضبط والتحفظ على نظام تقنية المعلومات، أو أي جزء منه، أو أي من وسائط تخزين بيانات وسيلة تقنية المعلومات، واستنساخ بيانات وسيلة تقنية المعلومات والاحتفاظ بالنسخة، والمحافظة على سلامة بيانات وسيلة تقنية المعلومات، ورفع بيانات وسيلة تقنية المعلومات من نظام تقنية المعلومات الذي تم الدخول إليه، أو جعل الدخول إليها غير متاح[٣].

ويجوز للنيابة العامة – بعد الحصول على إذن من قاضي المحكمة الصغرى لمدة لا تزيد على ثلاثين يوماً قابلة للتجديد لمدة أو مدد أخرى مماثلة – تكليف أي شخص مختص بالقيام بجمع وتسجيل بيانات خط السير وبيانات المحتوى، أو أي منهما، المتعلقة باتصالات محددة يتم إرسالها بواسطة نظام تقنية المعلومات، وذلك حين حدوث هذه الاتصالات، أو تكليف أي مزود خدمة بالقيام بالأعمال سالفة الذكر، أو تقديم المساعدة اللازمة لمن كلفته النيابة العامة بالقيام بهذه الأعمال. كما يجوز لها تكليف أي شخص مختص للقيام بحجب بيانات محتوى أية وسيلة تقنية المعلومات أو أي جزء منها ارتكبت بواسطتها أي من جرائم تقنية المعلومات[٤].

وقد خول المشرع لقاضي المحكمة الصغرى سلطة الأمر بالقيام على وجه السرعة بالحفاظ على بيانات خط السير المتصلة بالجريمة سواء كان الإرسال قد تم بثه من خلال مزود خدمة واحد أو أكثر، وكذلك الأمر بالكشف عن قدر كاف من بيانات خط السير لتمكين النيابة العامة من تحديد مزود الخدمة والمسار الذي تم إرسال هذه البيانات من خلاله، وذلك كله على النحو المبين في المادة (١٤) من قانون جرائم تقنية المعلومات[٥].

---

١. راجع المادة (١٣) من القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات.
٢. راجع المادة (١٥) من القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات.
٣. راجع المادة (١٦) من القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات.
٤. راجع المادة (١٨) من القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات.
٥. راجع المادة (١٤) من القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات.

كما يحق لقاضي المحكمة الصغرى، بناءً على طلب النيابة العامة، وبعد اطلاعه على الأوراق أن يأمر أي شخص مختص أو على دراية بكيفية عمل نظام تقنية المعلومات وبالتدابير المطبقة لحماية البيانات المخزنة في هذا النظام، بأن يوفر لها، وبالقدر المعقول، المعلومات اللازمة لتمكينها من تنفيذ الإجراءات المنصوص عليها في المادتين (١٥) و(١٦) من قانون جرائم تقنية المعلومات المشار إليه[١].

سادساً: العقوبات.

حرص المشرع على وضع عقوبات لكل من تسول له نفسه عدم الامتثال لأمر أو تكليف أصدره قاضي المحكمة الصغرى أو أصدرته النيابة العامة، بحسب الأحوال، في إطار الإجراءات القانونية الخاصة بجرائم تقنية المعلومات؛ حيث تقضي المادة (١٩) من قانون جرائم تقنية المعلومات بأن يُعاقب بالحبس مدة لا تزيد على سنتين وبالغرامة التي لا تجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين كل من لم يمتثل، قبل انقضاء المهلة التي حددها قاضي المحكمة الصغرى أو النيابة العامة بحسب الأحوال، لأمر أو تكليف صدر له وفقاً لحكم أي من الفقرتين (١) أو (٢) من المادة (١٢)، أو أي من المادتين (١٣) أو (١٤)، أو الفقرة (١) من المادة (١٨) من قانون جرائم تقنية المعلومات.

كما يُعاقب بالحبس مدة لا تزيد على سنة وبالغرامة التي لا تجاوز ثلاثة آلاف دينار أو بإحدى هاتين العقوبتين كل من خالف الأمر المشار إليه في الفقرة (٣) من المادة (١٢) من قانون جرائم تقنية المعلومات، أو حكم الفقرة (٢) من المادة (١٨) من هذا القانون. وتكون العقوبة السجن مدة لا تزيد على خمس سنين إذا كان الجاني موظفاً عاماً أو مكلفاً بخدمة عامة.

وقد تضمن الفصل الثالث من قانون جرائم تقنية المعلومات المشار إليه أحكاماً متفرقة ذات أهمية بالغة تتصل بهذه الجرائم؛ حيث يقرر المشرع في المادة (٢٠) من هذا القانون المعاقبة على الشروع في الجرائم المنصوص عليها في هذا القانون بنصف العقوبة المقررة للجريمة التامة[٢].

ويقرر في المادة (٢١) من القانون ذاته معاقبة الشخص الاعتباري بالغرامة المقررة للجريمة إذا ارتكبت باسمه أو لحسابه أو لمنفعته أية جريمة من الجرائم المنصوص عليها في هذا القانون، وكان ذلك نتيجة موافقة أو تستر أو إهمال جسيم من أي عضو مجلس إدارة، أو رئيس، أو مدير، أو أي مسئول آخر مفوض من قبل ذلك الشخص الاعتباري. وفي حال العود يجوز أن تحكم المحكمة بحل الشخص الاعتباري أو غلق المقر الذي تمت فيه الجريمة أو المقار التي يمارس فيها نشاطاً يتعلق بالجريمة غلقاً نهائياً أو للمدة التي تقدرها المحكمة، وذلك كله مع عدم الإخلال بالمسئولية الجنائية للشخص الطبيعي[٣].

---

١. راجع المادة (١٧) من القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات.

٢. راجع المادة (٢٠) من القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات.

٣. راجع المادة (٢١) من القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات.

كما يقرر في المادة (٢٣) من قانون جرائم تقنية المعلومات المشار إليه معاقبة كل من قام بارتكاب جريمة منصوص عليها في أي قانون آخر بواسطة نظام أو أية وسيلة تقنية معلومات، بالعقوبة المقررة لتلك الجريمة[١].

المطلب الثاني
أهم أحكام قانون حماية البيانات الشخصية[٢]

يُقصد بحماية البيانات الشخصية حماية خصوصية المعلومات المتعلقة بشخص الفرد وحياته الخاصة من التعرض للاعتداء، خاصة في ظل التحديات الرقمية، وانتشار جرائم القرصنة الإلكترونية.

وقد انتشرت في العصر الحديث ظاهرة تجميع البيانات والمعلومات الخاصة بالأشخاص وتخزينها ومعالجتها على الحاسب الآلي. وتتفاوت وتتعدد الأغراض من وراء ذلك؛ حيث يتم إنشاء بطاقات بيانات معلوماتية عن الأشخاص على الإنترنت، فقد تتعلق بالعملاء ليجري تحليلها للوقوف على نواحي الاستهلاك القائمة في المجتمع، وقد تتعلق باعتبارات الأمن لدى أجهزة الشرطة، وقد تكون لأغراض التأمين، أو الدراسات السياسية والسكانية والاجتماعية[٣].

ولقد اهتم المشرع البحريني بوضع تنظيم قانوني حديث يحمي البيانات الشخصية، فأصدر قانون حماية البيانات الشخصية بموجب القانون رقم (٣٠) لسنة ٢٠١٨، والذي يهدف إلى منع الاعتداء على حق المواطنين والمقيمين في حماية بياناتهم الشخصية وخصوصيتهم المقررة بموجب أحكام الدستور والقوانين ذات العلاقة، وتعزيز الحقوق والحريات الدستورية، وإيجاد إطار قانوني يوازن ما بين آليات حقوق الأفراد في حماية بياناتهم الشخصية، وبين السماح بمعالجة البيانات والمعلومات والاحتفاظ بها في ظل الفضاء الإلكتروني، وانتشار مفاهيم البيانات الضخمة والذكاء الاصطناعي.

والبين من الاطلاع على قانون حماية البيانات الشخصية المشار إليه أنه يضع أحكام معالجة البيانات الشخصية باستخدام الوسائل الآلية استخداماً كلياً أو جزئياً، ويتضمن القواعد العامة لمشروعية معالجة هذه البيانات، وأحكام نقل هذه البيانات إلى خارج المملكة، كما أنشأ هيئة عامة تُسمى «هيئة حماية البيانات الشخصية» تكون لها الشخصية الاعتبارية، وتتمتع بالاستقلال المالي والإداري، وتخضع لرقابة الوزير المختص بشئون العدل أو أيٌّ وزير آخر يصدر بتسميته مرسوم، وتتولى هذه الهيئة مباشرة كافة المهام والصلاحيات اللازمة لحماية البيانات الشخصية، ويُصدر مجلس إدارتها القرارات اللازمة لتنفيذ أحكام القانون المذكور.

---

١. راجع المادة (٢٣) من القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات.

٢. قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨، منشور في الجريدة الرسمية العدد رقم (٣٣٧٥) بتاريخ ٢٠١٨/٧/١٩.

٣. د. محمد حسين منصور، المسئولية الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٣، ص ٣٧٢.

ومن الجدير بالذكر أنه في عام ٢٠١٩ صدر مرسوم بتحديد الجهة الإدارية التي تتولى المهام والصلاحيات المقرَّرة لهيئة حماية البيانات الشخصية المشار إليها، وهو المرسوم رقم (٧٨) لسنة ٢٠١٩؛ حيث قضى بأن تتولى وزارة العدل والشئون الإسلامية والأوقاف المهام والصلاحيات المقرَّرة لهيئة حماية البيانات الشخصية بموجب أحكام قانون حماية البيانات الشخصية سالف الذكر[١].

وطبقاً للمادة الأولى من المرسوم رقم (٧٨) لسنة ٢٠١٩ المشار إليه، تتولى وزارة العدل والشئون الإسلامية والأوقاف المهام والصلاحيات المقرَّرة لهيئة حماية البيانات الشخصية بموجب أحكام قانون حماية البيانات الشخصية، وذلك إلى حين رصْد الاعتماد المالي للهيئة في الميزانية العامة للدولة، وصدور مرسوم بتشكيل مجلس الإدارة. ويتولى وزير العدل والشئون الإسلامية والأوقاف المهام والصلاحيات المقرَّرة بموجب القانون المشار إليه لكل من مجلس إدارة الهيئة ورئيس مجلس الإدارة. ويتولى وكيل الوزارة للعدل والشئون الإسلامية بذات الوزارة المهام والصلاحيات المقرَّرة للرئيس التنفيذي.

وينص المشرع في قانون حماية البيانات الشخصية المشار إليه على تعريفات معينة لبعض المصطلحات الفنية المستخدمة فيه، ويحدد نطاق تطبيق أحكامه، ويضع القواعد العامة لمشروعية معالجة البيانات الشخصية، وضوابط نقْل البيانات الشخصية إلى خارج المملكة، كما يبين الإخطارات والتصاريح اللازمة لعملية المعالجة، ويوضح حقوق صاحب البيانات، ويحدد العقوبات التي يُحكم بها على من يخالف أحكامه.

ونظراً لأهمية هذا القانون، نستعرض أهم أحكامه التي تنظم الموضوعات سالفة البيان، وذلك على النحو الآتي:

أولاً: تعريف المصطلحات المستخدمة في قانون حماية البيانات الشخصية.

حدد المشرع في المادة (١) من قانون حماية البيانات الشخصية آنف الذكر تعريفات معينة للمصطلحات الفنية المستخدمة فيه نظراً لطبيعتها الخاصة، ومن أهم هذه المصطلحات مصطلح «بيانات أو بيانات شخصية» الذي يُقصد به أية معلومات في أية صورة تخصُّ فرداً مُعَّرفاً، أو قابلاً بطريق مباشر أو غير مباشر لأن يُعَرَّف، وذلك بوجه خاص من خلال رقم هويته الشخصية، أو صفة أو أكثر من صفاته الشكلية أو الفسيولوجية أو الذهنية أو الثقافية أو الاقتصادية أو هويته الاجتماعية، ولتقرير ما إذا كان الفرد قابلاً لأن يُعَرَّف، تراعى كافة الوسائل التي يستخدمها مدير البيانات أو أيُّ شخص آخر، أو التي قد تكون متاحة له.

وبذلك فإن أي بيان يكون من شأنه التعرف على هوية شخص ما، كاسم الشخص، أو رقم هويته، أو رقم جواز السفر، أو الهاتف، أو رقم العضوية في أية مؤسسة، أو صورته الشخصية، أو صور المستندات المتعلقة بشخصه، أو وظيفته، أو معلوماته المصرفية، أو بريده الإلكتروني، يدخل في نطاق

---

١. المرسوم رقم (٧٨) لسنة ٢٠١٩ بتحديد الجهة الإدارية التي تتولى المهام والصلاحيات المقرَّرة لهيئة حماية البيانات الشخصية، منشور في الجريدة الرسمية العدد رقم (٣٤٣٩) بتاريخ ٢٠١٩/١٠/٣.

البيانات الشخصية المحمية بموجب القانون.

ويرى بعض الفقه أن المعلومة الشخصية عبارة عن بيان متعلق بشخص طبيعي معين أو قابل للتعيين، وتتم معالجة البيانات الشخصية بأساليب آلية عبر عمليات الجمع والتسجيل والتنظيم والتخزين والنقل والتعديل والاستنباط والتقريب والنشر، توصلاً إلى نتائج وأغراض معينة. ولذلك أجمعت التشريعات على خضوع إنشاء واستخدام نظم المعالجة المعلوماتية للبيانات الشخصية لرقابة الدولة، سواء من حيث إنشائها، أو نشاطها، أو تحديد أهدافها، بالإضافة إلى الإشراف المتوالي عليها[1].

ويُقصد بعبارة «بيانات شخصية حسَّاسة» أية معلومات شخصية تكشف على نحو مباشر أو غير مباشر عن أصل الفرد العِرْقي، أو الإثْني، أو آرائه السياسية، أو الفلسفية، أو معتقداته الدينية، أو انتمائه النقابي، أو سِجِل السوابق الجنائية الخاص به، أو أية بيانات تتعلق بصحته أو حالته الجنسية.

كما يُقصد بكلمة «المعالجة» أية عملية أو مجموعة عمليات يتم إجراؤها على بيانات شخصية بوسيلة آلية أو غير آلية، ومن ذلك جمْع تلك البيانات، أو تسجيلها، أو تنظيمها، أو تصنيفها في مجموعات، أو تخزينها، أو تحويرها، أو تعديلها، أو استعادتها، أو استخدامها، أو الإفصاح عنها، من خلال بثِّها، أو نشرها، أو نقلها، أو إتاحتها للغير، أو دمجها، أو حجْبها، أو مسْحها، أو تدميرها.

وتم تعريف عبارة «منظومة ملفات» بأنها أية مجموعة بيانات شخصية لا تعالَج بواسطة جهاز يعمل آلياً بناءً على تعليمات تُعطَى له، ولكنها مرتَّبة على نحو يتيح الحصول منها على معلومات عن الأفراد الذين تخُصُّهم هذه البيانات.

ويُقصد بكلمة «الشخص» أيُّ شخص طبيعي أو اعتباري، بما في ذلك أية جهة عامة، بينما يُقصد بكلمة «الفرد» أيُّ شخص طبيعي، كما يُقصد بعبارة «مدير البيانات» الشخص الذي يقرر، بمفرده أو بالاشتراك مع الآخرين، أغراض ووسائل معالجة بيانات شخصية معينة. وفي الحالات التي تكون فيها هذه الأغراض والوسائل مقرَّرة بموجب القانون، يُعَد مديراً للبيانات الشخص المنوط به الالتزام بالقيام بالمعالجة.

وبذلك فإن كل من يقرر طريقة الحصول على البيانات الشخصية وطريقة التصرف فيها – وهو ما يُعرف قانوناً بمعالجة البيانات – يُعتبر مديراً للبيانات، وتقع على عاتقه مسئولية الالتزام بتطبيق الشروط القانونية للحصول على البيانات والتصرف فيها. وبناء عليه، يجب على كل مؤسسة أو شركة أو جهة تحصل من خلال تعاملها على معلومات شخصية لعملائها وتقرر طريقة معالجتها، الالتزام بالمعايير المقررة قانوناً لحماية البيانات الشخصية.

ويعني مصطلح «معالِج البيانات» الشخص الذي يتولى معالجة البيانات لحساب مدير البيانات ونيابة عنه، ولا يشمل ذلك كل مَن يعمل لدى مدير البيانات أو معالِج البيانات. وتم تعريف مصطلح

---

١. د. محمد حسين منصور، المسئولية الإلكترونية، مرجع سابق، ص ٣٧٢ وما بعدها.

«مراقب حماية البيانات» بأنه الشخص الذي يتم اعتماده من قِبَل الهيئة وِفْقاً لحكم المادة (١٠) من قانون حماية البيانات الشخصية.

ويعني مصطلح «صاحب البيانات» الفرد أو الشخص موضوع البيانات. ويُقصد بمصطلح «متسَلِّم البيانات» أيُّ شخص يُفصَح له عن بيانات شخصية، سواء كان طرفاً ثالثاً أو غيره، ولا يشمل ذلك الشخص الذي يُفصَح له عن بيانات لمباشرة اختصاص قانوني محدَّد أو للقيام بواجب عام محدد.

وتم تعريف مصطلح «الحَجْب» بأنه التأشير بأية وسيلة على البيانات المخزَّنة تمنَع أية معالجة لاحقة لها، فيما عدا تخزينها، كما تم تعريف مصطلح «التسويق المباشر» بأنه أيُّ اتصال، بأية وسيلة، يتم من خلاله توجيه مادة تسويق أو دعاية إلى شخص محدَّد.

ثانياً: نطاق تطبيق قانون حماية البيانات الشخصية.

حدد المشرع في المادة (٢) من قانون حماية البيانات الشخصية المشار إليه نطاق تطبيقه؛ حيث قرر سريان أحكام هذا القانون على المعالجات الآتية: (أ) معالجة البيانات باستخدام الوسائل الآلية استخداماً كلياً أو جزئياً. (ب) معالجة البيانات التي تُشكّل جزءاً من منظومة ملفات أو يُقصَد بها أنْ تُشكّل جزءاً من هذه المنظومة، بوسيلة غير آلية.

كما قرر سريان أحكام هذا القانون على الأشخاص الآتيين: (أ) كل شخص طبيعي يقيم عادة في مملكة البحرين أو له مقر عمل فيها. (ب) كل شخص اعتباري له مقر عمل في المملكة. (ج) كل شخص طبيعي أو اعتباري، لا يقيم عادة في المملكة، وليس له مقر عمل فيها، يعالِج بيانات باستخدام وسائل موجودة في المملكة، ما لم يكن الغرض من استخدام هذه الوسائل مجرد مرور البيانات من خلال المملكة فحسب.

وقد أوجب المشرع على كل شخص اعتباري من المشار إليهم في البند (٢/ج) من المادة (٢) من قانون حماية البيانات الشخصية أنْ يعيِّن ممثلاً مفوَّضاً عنه في المملكة لمباشرة التزاماته المقرَّرة بموجب أحكام هذا القانون، وأنْ يُخطِر هيئة حماية البيانات الشخصية فور قيامه بهذا التعيين وبأيِّ تغيير يطرأ عليه.

كما قرر المشرع عدم سريان أحكام قانون حماية البيانات الشخصية على المعالجات الآتية: (أ) معالجة البيانات التي تتم من قبل أيِّ فرد لأغراض لا تتجاوز الشئون الشخصية أو العائلية. (ب) عمليات المعالجة المتعلقة بالأمن الوطني التي تتولاها وزارة الدفاع، أو وزارة الداخلية، أو الحرس الوطني، أو جهاز الأمن الوطني، أو غيرها من الأجهزة الأمنية للمملكة. ولا تُخِل أحكام هذا القانون بمتطلبات مراعاة السرية اللازمة في شئون قوة دفاع البحرين[١].

١. راجع المادة (٢) من قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.

ثالثاً: القواعد العامة لمشروعية معالجة البيانات الشخصية.

حرص المشرع على وضع قواعد عامة لمشروعية معالجة البيانات الشخصية في الفصل الثاني من الباب الأول من قانون حماية البيانات الشخصية المشار إليه.

وقد حدد المشرع في المادة (٣) من القانون سالف الذكر الضوابط الخاصة بجودة البيانات؛ حيث أوجب مراعاة عدة أمور بشأن البيانات الشخصية التي تتم معالجتها، وتتمثل هذه الأمور فيما يلي:

(١) أن تكون معالجتها منصفة ومشروعة.

(٢) أن تكون قد جُمِعت لغرض مشروع ومحدَّد وواضح، وألا تتم معالجتها لاحقاً، وألا يتم إجراء معالجة لاحقة لها على نحو لا يتوافق مع الغرض الذي جُمِعت من أجله، ولا تُعَدُّ معالجة غير متوافقة مع الغرض الذي جُمِعت من أجله البيانات المعالَجة اللاحقة لها التي تتم حصراً لأغراض تاريخية، أو إحصائية، أو للبحث العلمي، وبشرط ألا تتم لدعم اتخاذ أيِّ قرار أو إجراء بشأن فرد محدد.

(٣) أن تكون كافية وذات صلة وغير مفرطة بالنظر للغرض من جمْعِها أو الذي تمت المعالَجة اللاحقة لأجله.

(٤) أن تكون صحيحة ودقيقة، وتخضع لعمليات التحديث عندما يكون لذلك مقتضىً.

(٥) ألا تبقى في صورة تسمح بمعرفة صاحب البيانات بعد استنفاد الغرض من جمْعِها أو الذي تتم المعالَجة اللاحقة لأجله. وتُحفَظ البيانات التي يتم تخزينها لفترات أطول لأغراض تاريخية أو إحصائية أو للبحث العلمي في صورة مجهولة بتحويرها، وذلك بوضْعها في صورة لا تُمكِّن مِنْ نسبة هذه البيانات إلى صاحبها. ويتعين إنْ تعذَّر ذلك تشفير هوية أصحابها.

وتضع المادة (٤) من قانون حماية البيانات الشخصية الاشتراطات العامة للمعالجة المشروعة؛ حيث تحظر معالجة البيانات الشخصية دون موافقة صاحبها، وذلك ما لم تكن هذه المعالجة ضرورية لتنفيذ عقد يكون صاحب البيانات طرفاً فيه، أو لاتخاذ خطوات بناءً على طلب صاحب البيانات بهدف إبرام عقد، أو لتنفيذ التزام يرتِّبه القانون، خلافاً لالتزام عقدي، أو صدور أمر من محكمة مختصة أو النيابة العامة، أو لحماية المصالح الحيوية لصاحب البيانات، أو لمباشرة المصالح المشروعة لمدير البيانات أو أيِّ طرف ثالث يُفصَح له عن البيانات، ما لم يتعارض ذلك مع الحقوق والحريات الأساسية لصاحب البيانات.

وقد حدد المشرع في المادة (٥) من قانون حماية البيانات الشخصية الاشتراطات الخاصة بمعالجة البيانات الشخصية الحساسة؛ حيث حظر معالجة البيانات الشخصية الحساسة دون موافقة صاحبها، باستثناء المعالجة التي يقتضيها قيام مدير البيانات بالتزاماته ومباشرة حقوقه المقرَّرة قانوناً في مجال علاقة العمل التي تربطه بالعاملين لديه، والمعالجة الضرورية لحماية أيِّ إنسان إذا كان صاحب البيانات – أو الوصي أو الولي أو القَيِّم عليه – غير قادر قانوناً على إعطاء موافقته على ذلك، وبشرط الحصول على تصريح مسبق من هيئة حماية البيانات الشخصية، ومعالجة البيانات

التي أتاحها صاحبها للجمهور، والمعالجة الضرورية لمباشرة أيٍّ من إجراءات المطالبة بالحقوق القانونية أو الدفاع عنها، بما في ذلك ما يقتضيه التجهيز لهذا الأمر والاستعداد له، والمعالجة الضرورية لأغراض الطب الوقائي أو التشخيص الطبي أو تقديم الرعاية الصحية أو العلاج أو إدارة خدمات الرعاية الصحية من قِبَل مرخَّص له بمزاولة أيٍّ من المهن الطبية، أو أيِّ شخص ملزَم بحكم القانون بالمحافظة على السرِّية، والمعالجة التي تتم في سياق أنشطة الجمعيات بأنواعها والنقابات وغيرها من الجهات التي لا تهدف إلى تحقيق ربح، وذلك بشرط أن تتم المعالجة في حدود ما هو ضروري للغرض الذي أنشئت الجمعية أو النقابة أو الجهة من أجله، وأن ترد المعالجة على بيانات تخص أعضاء تلك الجمعية أو النقابة أو الجهة أو لأفراد لهم اتصال منتظم معها بحكم طبيعة نشاطها، وألا يتم الإفصاح عن البيانات لأيِّ شخص آخر ما لم يوافق صاحب البيانات على ذلك[1].

كما حرص المشرع على تنظيم معالجة البيانات لأغراض الصحافة أو الآداب أو الفنون؛ حيث قرر عدم سريان أحكام المواد (٣) و(٤) و(٥) من قانون حماية البيانات الشخصية على معالجة البيانات الشخصية التي تتم حصراً للأغراض الصحفية أو الفنية أو الأدبية، وذلك بشرط أن تكون البيانات صحيحة ودقيقة وتخضع لعمليات التحديث والتصحيح، وأن تتوافر تدابير تكفل عدم استخدام البيانات لأية أغراض أخرى خلافاً للأغراض الصحفية أو الفنية أو الأدبية، وألا يتم الإخلال بالتشريعات المعمول بها بشأن تنظيم الصحافة والطباعة والنشر[2].

ويحظر المشرع معالجة البيانات الشخصية المتعلقة برفع الدعاوى الجنائية ومباشرتها وبالأحكام الصادرة فيها، ويُستثنَى من هذا الحظر ما يلي: (أ) المعالجة التي تتم من قِبَل أية جهة عامة مختصة بالقدر الذي يقتضيه تنفيذ المهام المنوطة بها قانوناً. (ب) المعالجة التي تتم من قبل أيِّ شخص اعتباري بالقَدر الذي يقتضيه تحقيق أهدافه المقرَّرة قانوناً. (ج) المعالجة التي تتم من قبل أي شخص بالقَدر الذي تقتضيه مباشرة إجراءات التقاضي في الدعاوى المرفوعة منه أو عليه. (د) المعالجة التي تتم من قِبَل المحامين بالقَدر الذي تقتضيه مباشرة مصالح موكليهم. (هـ) المعالجة التي تتم لأغراض مباشرة مهنة الصحافة أو البحث العلمي.

ومع ذلك، لا تُخِل الاستثناءات المشار إليها بالالتزام المقرَّر قانوناً بشأن المحافظة على سرية البيانات. ويجوز للنيابة العامة، والقضاء العسكري، والنيابة العسكرية، والوزارة المعنية بشئون العدل، ووزارة الداخلية دون سواهم إنشاء سجلات كاملة لقيد جميع الدعاوى الجنائية والأحكام الصادرة فيها، وإمساكها[3].

وقد حرص المشرع على إلزام مدير البيانات باتخاذ التدابير الفنية والتنظيمية الكفيلة بالحفاظ على أمان عملية معالجة البيانات الشخصية؛ حيث أوجب عليه تطبيق التدابير الفنية والتنظيمية التي

---

١. راجع المادة (٥) من قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.

٢. راجع المادة (٦) من قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.

٣. راجع المادة (٧) من قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.

تكفل حماية البيانات من الإتلاف غير المقصود أو غير المصرَّح به، أو من الفقْد العَرَضي، أو مما هو غير مصرَّح به من التغيير أو الإفصاح أو النفاذ أو أيٍّ من الصور الأخرى للمعالَجة. كما أوجب عليه أن تكفل هذه التدابير توفير مستوى مناسب من الأمان بمراعاة ما وصلت إليه أحدث أساليب الحماية التقنية، والتكلفة المترتبة على ذلك، وطبيعة البيانات موضوع المعالجة، والمخاطر التي قد تنشأ من هذه المعالجة. ويجب أن تكون التدابير الفنية والتنظيمية مدوَّنة ومتاحاً الاطلاع عليها من ذوي الشأن، ومن هيئة حماية البيانات الشخصية، ومدير البيانات، ومعالِج البيانات.

وفي الحالات التي يُكلَّف فيها معالِج البيانات بمعالَجة البيانات، أوجب المشرع على مدير البيانات بمراعاة اختيار معالِج بيانات يوفِّر ضمانات كافية بشأن تطبيق التدابير الفنية والتنظيمية الواجب مراعاتها في معالجة البيانات. وعلى مدير البيانات اتخاذ الخطوات المعقولة للتَّحَقُّق من الالتزام بهذه التدابير، كما يجب أن تتم المعالَجة وِفْقاً لعقد مكتوب يُبرم بين مدير البيانات ومعالِج البيانات يتضمن ألا يباشر معالِج البيانات أية معالجة إلا وِفْقاً لتعليمات من مدير البيانات، وأن يلتزم معالِج البيانات فيما يخص الأمان والسرية بذات الالتزامات المقرَّرة في شأن مدير البيانات[1].

وقد ناط المشرع بمجلس إدارة هيئة حماية البيانات الشخصية إصدار قرار بتحديد الاشتراطات التي يتعيَّن توفرها في التدابير الفنية والتنظيمية المشار إليها، ونفاذاً لذلك أصدر وزير العدل والشئون الإسلامية والأوقاف القرار رقم (٤٣) لسنة ٢٠٢٢ بتحديد الاشتراطات التي يتعين توافرها في التدابير الفنية والتنظيمية الكفيلة بحماية البيانات الشخصية[2]، ووضع تعريفاً لمصطلح تصميم لحماية الخصوصية (Privacy by Design)، بأنه طريقة نظام مُعالجة البيانات والتي تسعى إلى توفير أقصى درجات الخصوصية بشكل استباقي من خلال ضمان حماية البيانات تلقائياً في النظام التكنولوجي أو المُمارسة التجارية، وتطبيق تدابير الأمان في جميع مراحل المعالجة بشكل يتوقع مشاكل الخصوصية ويمنعها قبل حدوثها.

ونظراً لأهمية عملية معالجة البيانات الشخصية وآثارها، فقد أوجب المشرع الحفاظ على سرية المعالجة؛ حيث حظر على مدير البيانات الإفصاح عن أية بيانات شخصية إلا بموافقة صاحب هذه البيانات، أو تنفيذاً لأمر قضائي صادر من محكمة مختصة، أو النيابة العامة، أو قاضي التحقيق، أو النيابة العسكرية. كما حظر على مدير البيانات معالجة أية بيانات شخصية بالمخالفة لأحكام قانون حماية البيانات الشخصية.

وبصفة عامة حظر المشرع على أيٍّ فرد من المتاح لهم النفاذ إلى بيانات شخصية القيام بأية معالَجة لها إلا بموافقة مدير هذه البيانات، أو تنفيذاً لأمر قضائي صادر من محكمة مختصة، أو قاضي التحقيق، أو النيابة العامة، أو النيابة العسكرية، كما حظر عليهم استخدامها لمنفعتهم الخاصة أو

---

١. راجع المادة (٨) من قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.

٢. قرار وزير العدل والشئون الإسلامية والأوقاف رقم (٤٣) لسنة ٢٠٢٢ بتحديد الاشتراطات التي يتعين توافرها في التدابير الفنية والتنظيمية الكفيلة بحماية البيانات الشخصية، منشور في الجريدة الرسمية العدد رقم (٣٥٩٣) بتاريخ ٢٠٢٢/٣/١٧.

لمنفعة الغير، ويستمر هذا الحظر بعد انتهاء علاقة العمل، أو مدة العقد[1].

رابعاً: ضوابط نقل البيانات الشخصية إلى خارج مملكة البحرين.

يتناول الفصل الثالث من الباب الأول من قانون حماية البيانات الشخصية مسألة نقل البيانات الشخصية إلى خارج مملكة البحرين في مادتين، وهما المادتان (١٢) و(١٣).

وتتعلق المادة (١٢) من القانون المذكور بنقل البيانات الشخصية إلى بلدان وأقاليم توفِّر مستوى كافياً من الحماية؛ حيث تحظر على مدير البيانات نقل البيانات الشخصية إلى خارج مملكة البحرين في غير الحالات الآتية:

١- أنْ يكون النقل إلى بلد أو إقليم مدرج في كشف تتولى هيئة حماية البيانات الشخصية إعداده وتحديثه يتضمن أسماء البلدان والأقاليم التي تقدِّر الهيئة أنَّ لديها تشريعات أو أنظمة معمولاً بها تكفل مستوى كافياً من الحماية للبيانات الشخصية، ويُنشَر هذا الكشف في الجريدة الرسمية.

٢- أنْ يكون النقل بتصريح يصدر من الهيئة في كل حالة على حدة، وذلك إذا قدَّرت أنَّ البيانات سوف يتوافر لها مستوى كافٍ من الحماية، ويكون تقدير الهيئة بمراعاة كافة الظروف المحيطة بعملية نقل البيانات، وبوجه خاص ما يأتي:

أ- طبيعة البيانات المطلوب نقْلُها، والغرض من معالجتها ومدة المعالجة.

ب- البلد أو الإقليم مصدر هذه البيانات والوجهة النهائية لها، وما يتوافر في تلك البلدان أو الأقاليم من تدابير لحماية البيانات الشخصية.

ج- الاتفاقيات الدولية والتشريعات ذات العلاقة المعمول بها لدى البلد أو الإقليم الذي سوف تُنقَل إليه البيانات.

ويجوز أن يكون التصريح المشار إليه مشروطاً أو لفترة زمنية محددة[2].

واستثناءً من أحكام المادة (١٢) من قانون حماية البيانات الشخصية، أجاز المشرع لمدير البيانات أن ينقل بيانات شخصية خارج المملكة إلى بلد أو إقليم لا يوفر مستوى كافياً من الحماية للبيانات إذا وافق صاحب البيانات على هذا النقل، أو إذا كان هذا النقل لبيانات مستخرجة من سجل تم إنشاؤه وفقاً للقانون بغرض توفير معلومات للجمهور، سواءً كان الاطلاع على هذا السجل متاحاً للكافة أو مقصوراً على ذوي المصلحة وِفْقاً لشروط معينة، وفي هذه الحالة يتعيَّن للاطلاع على هذه المعلومات استيفاء الشروط المقرَّرة للاطلاع على السجل، أو إذا كان هذا النقل ضرورياً لأي مما يأتي:

(١) تنفيذ عقد بين صاحب البيانات ومدير البيانات، أو لاتخاذ خطوات سابقة بناءً على طلب صاحب البيانات بهدف إبرام عقد.

(٢) تنفيذ أو إبرام عقد بين مدير البيانات وطرف ثالث لمصلحة صاحب البيانات.

(٣) حماية مصالح حيوية لصاحب البيانات.

---

١. راجع المادة (٩) من قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.

٢. راجع المادة (١٢) من قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.

(٤) تنفيذ التزام يرتِّبه القانون، خلافاً لالتزام عقدي، أو صدور أمر من محكمة مختصة، أو النيابة العامة، أو قاضي التحقيق، أو النيابة العسكرية.

(٥) إعداد أو مباشرة مطالَبة قانونية أو الدفاع عنها.

كما أجاز المشرع لهيئة حماية البيانات الشخصية التصريح بنقْل بيانات شخصية، أو مجموعة منها، إلى بلد أو إقليم لا يكفل مستوى كافياً من الحماية وِفْقاً لمتطلبات المادة (١٢) المشار إليها، إذا قدم مدير البيانات ضمانات كافية بشأن حماية الخصوصية والحقوق والحريات الأساسية للأفراد[١].

وبذلك يتضح أن قانون حماية البيانات الشخصية أرسى قاعدة أساسية تتمثل في عدم جواز الحصول على البيانات الشخصية أو معالجتها دون الحصول على موافقة كتابية صريحة من صاحب البيانات، وذلك ما لم ينص القانون على خلاف ذلك. واشترط القانون موافقات خاصة لبعض حالات المعالجة كنقل البيانات الشخصية خارج مملكة البحرين، فنصت المادة (١٢) من هذا القانون على حظر نقل البيانات خارج المملكة بدون موافقة خاصة من صاحبها إلا إذا كان ذلك بتصريح خاص من وزارة العدل والشئون الإسلامية والأوقاف؛ وذلك باعتبارها الجهة التي تتولى القيام بمهام وصلاحيات هيئة حماية البيانات الشخصية عملاً بأحكام المرسوم رقم (٧٨) لسنة ٢٠١٩ سالف الذكر.

خامساً: الإخطارات والتصاريح اللازمة لعملية معالجة البيانات الشخصية.

يتضمن الفصل الرابع من الباب الأول من قانون حماية البيانات الشخصية المشار إليه أحكام الإخطارات والتصاريح اللازمة لعملية معالجة البيانات الشخصية، وذلك في المادتين (١٤) و(١٥) من القانون المذكور.

والمستفاد من المادة (١٤) من قانون حماية البيانات الشخصية الواردة تحت عنوان «إخطار الهيئة» أن المشرع يُلزم مدير البيانات بإخطار هيئة حماية البيانات الشخصية قبل بدء عملية المعالَجة التي تتم آلياً كلياً أو جزئياً، أو لمجموعة عمليات من ذلك بقصْد تحقيق غرض واحد أو عدة أغراض ذات صلة ببعضها.

ويُعفى مدير البيانات من تقديم هذا الإخطار إلى الهيئة بشأن المعالَجة التي يكون الغرض الوحيد منها إمساك سجل وِفْقاً للقانون بهدف توفير معلومات للجمهور، سواء كان الاطلاع على هذا السجل متاحاً للكافة أو مقصوراً على ذوي المصلحة، ومعالجة البيانات التي تتم في سياق أنشطة الجمعيات بأنواعها والنقابات وغيرها من الجهات التي لا تهدف إلى تحقيق الربح، ومعالجة صاحب العمل لبيانات العاملين لديه في الحدود الضرورية لمباشرة مهامه والتزاماته وتنظيم شئونه ومباشرة حقوقه وحماية حقوق العاملين لديه، والحالات التي يتم فيها تعيين مراقب حماية بيانات.

ويجب أن يتضمَّن الإخطار المشار إليه عدة بيانات منها اسم مدير البيانات وعنوانه، وكذا معالِج البيانات إن وُجِد، والغرض من المعالجة، ووصْف البيانات وبيان فئات أصحاب البيانات ومتسلِّمي

١. راجع المادة (١٢) من قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.

هذه البيانات أو فئاتهم، وأي نقْل للبيانات إلى بلد أو إقليم خارج مملكة البحرين يُعتَزَم القيام به[١].

والمستفاد من المادة (١٥) من قانون حماية البيانات الشخصية الواردة تحت عنوان «التصريح المسبق» أن المشرع يحظر إجراء عمليات معينة من عمليات المعالَجة دون تصريح كتابي مسبق من هيئة حماية البيانات الشخصية، وتتمثل هذه العمليات فيما يلي:

أ- المعالَجة الآلية للبيانات الشخصية الحسَّاسة، وذلك في الحالة المشار إليها في البند (٢) من المادة (٥) من قانون حماية البيانات الشخصية، وهي المعالجة الضرورية لحماية أيِّ إنسان إذا كان صاحب البيانات – أو الوصي أو الولي أو القَيِّم عليه – غير قادر قانوناً على إعطاء موافقته على ذلك.

ب- المعالَجة الآلية للبيانات القياسات الحيوية (Biometrics) التي تُستخدَم للتَّعَرُّف على الشخصية.

ج- المعالَجة الآلية للبيانات الوراثية، باستثناء المعالَجة التي تتم من قِبَل الأطباء والمتخصصين في مُنشأة طبية مرخَّصة وتكون ضرورية لأغراض الطب الوقائي أو التشخيص الطبي أو تقديم العلاج أو الرعاية الصحية.

د- المعالَجة الآلية التي تنطوي على ربْط ملفات بيانات شخصية لدى اثنين أو أكثر من مديري البيانات تعالَج من قِبَلهم لأغراض مختلفة.

هـ- المعالَجة التي تكون عبارة عن تسجيل بصري مما يُستخدَم لأغراض المراقبة.

ويتضح مما تقدم أن المشرع يحظر استخدام المعالجة الآلية لربط البيانات الشخصية بين أكثر من جهة، كأن يتم ربط البيانات الشخصية للعملاء في شركتين مختلفتين، أو استخدام المعالَجة الآلية للبيانات القياسات الحيوية (Biometrics) والتي تُستخدَم للتّعَرُّف على الشخصية، كتلك التي تستخدم من خلال التطبيقات الإلكترونية على الأجهزة الذكية، أو استخدام المعالَجة التي تكون عبارة عن تسجيل بصري مما يُستخدَم لأغراض المراقبة، كوضع كاميرات للمراقبة عن بُعد، وذلك كله بدون الحصول على تصريح كتابي مسبق من وزارة العدل والشئون الإسلامية والأوقاف باعتبارها الجهة التي تتولى القيام بمهام وصلاحيات هيئة حماية البيانات الشخصية عملاً بأحكام المرسوم رقم (٧٨) لسنة ٢٠١٩ المشار إليه.

ويتم تقديم طلب التصريح المسبق ويُبَت فيه وفقاً للقواعد والإجراءات التي يصدر بتحديدها قرار من وزير العدل والشئون الإسلامية والأوقاف باعتباره يتولى مهام وصلاحيات مجلس إدارة هيئة حماية البيانات الشخصية عملاً بأحكام المرسوم رقم (٧٨) لسنة ٢٠١٩ المشار إليه.

ويجب أن يتضمَّن طلب التصريح ذات البيانات التي يجب أنْ يتضمَّنها الإخطار الذي يتعيَّن تقديمه وفقاً للمادة (١٤) من قانون حماية البيانات الشخصية. ويجوز لوزارة العدل والشئون الإسلامية والأوقاف خلال خمسة أيام عمل من تاريخ تسَلُّم الطلب أنْ تطلب من مدير البيانات استيفاء أيِّ نقص في بيانات الطلب، وعلى مقدّم الطلب استيفاء النقص خلال أيام العمل الخمسة التالية، وإلا

١. راجع المادة (١٤) من قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.

تعيَّن على هذه الوزارة البت في الطلب بناءً على ما تضمَّنه من معلومات.

وتمنح وزارة العدل والشئون الإسلامية والأوقاف التصريح في حالة استيفاء الطلب الاشتراطات التي يصدر بتحديدها قرار من وزير العدل والشئون الإسلامية والأوقاف. ويجب على هذه الوزارة أن تبت في طلب التصريح وإخطار صاحب الشأن بالنتيجة خلال ثلاثين يوماً من تاريخ تقديمه، وإذا لم يتسلَّم مدير البيانات رداً من الوزارة خلال الفترة المشار إليها عُدَّ ذلك رفضاً ضمنياً للطلب[1].

سادساً: حقوق صاحب البيانات.

اهتم المشرع بالنص صراحة على حقوق صاحب البيانات في قانون حماية البيانات الشخصية؛ حيث أفرد لهذه الحقوق فصلاً خاصاً، وهو الفصل الخامس من الباب الأول من هذا القانون. ويتألف هذا الفصل من عشر مواد، وهي المواد من (١٧) حتى (٢٦).

والمستفاد من المادة (١٧) من قانون حماية البيانات الشخصية أن المشرع حدد المعلومات التي يجب إحاطة صاحب البيانات بها؛ حيث قرر أنه في الحالات التي يتم فيها الحصول على البيانات من صاحبها مباشرة، يجب على مدير البيانات إحاطته عند تسجيل هذه البيانات بما يلي:

(١) اسم مدير البيانات كاملاً ومجال نشاطه أو مهنته، بحسب الأحوال، وعنوانه.

(٢) الأغراض التي من أجلها يُعتزَم معالجة البيانات.

(٣) أية معلومات ضرورية أخرى، بحسب ظروف كل حالة، يكون من شأنها أنْ تكفل جعْل المعالَجة منصفة بالنسبة لصاحب البيانات، ومن ذلك أسماء متسَلِّمي البيانات أو فئاتهم، وبيان ما إذا كانت الإجابة على أية أسئلة توجَّه إلى صاحب البيانات إجبارية أو اختيارية، وعند الاقتضاء توضيح العواقب التي تترتب على الامتناع عن الإجابة، وبيان ما إذا كان سيتم استخدام البيانات لأغراض التسويق المباشر.

وفي حالة الحصول على البيانات من غير صاحبها، أوجب المشرع على مدير البيانات إحاطة صاحب البيانات خلال خمسة أيام من البدء في تسجيل هذه البيانات بالمعلومات سالفة الذكر، والأغراض التي تم من أجلها جمْع البيانات، وأية معلومات ضرورية أخرى، بحسب ظروف كل حالة، يكون من شأنها جعْل المعالَجة منصفة بالنسبة لصاحب البيانات، ومن ذلك فئات البيانات، ومصدر البيانات، وذلك باستثناء الحالات التي يقتضي واجب المحافظة على أسرار المهنة المقرَّر قانوناً عدم الإفصاح عن المصدر[2].

ومفاد المادة (١٨) من قانون حماية البيانات الشخصية أنه يجب على مدير البيانات، بناءً على طلب من صاحب البيانات مشفوع بما يثبت هويته، أن يخطر مقدِّم الطلب دون مقابل خلال ميعاد أقصاه خمسة عشر يوم عمل من تاريخ الطلب، عما إذا كان مدير البيانات يعالِج بيانات شخصية خاصة بصاحب الطلب.

---

١. راجع المادة (١٥) من قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.

٢. راجع المادة (١٧) من قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.

وفي حالة وجود معالَجة من أيِّ نوع لهذه البيانات، يلتزم مدير البيانات بإخطار صاحب البيانات في صورة مفهومة بالبيانات موضوع المعالَجة كاملة، وأية معلومات تتوافر لدى مدير البيانات أو متاحة له عن مصدر البيانات، وذلك باستثناء الحالات التي يفرِض فيها القانون واجب المحافظة على سرية المصدر، والغرض من معالَجة البيانات، وأسماء متسَلِّمي البيانات أو فئاتهم[١].

وقد أوضحت المادة (١٩) من قانون حماية البيانات الشخصية الحالات التي يجب فيها إخطار صاحب البيانات بأن له الحق في الاعتراض على التسويق المباشر؛ حيث تقضي بأنه يجب على مدير البيانات في الحالات التي يتوقع فيها الاستخدام لأغراض التسويق المباشر لبيانات شخصية يحتفظ بها إخطار صاحب البيانات بأن له الحق في الاعتراض لديه، ودون مقابل، على هذه المعالجة[٢].

وبينت المادة (٢٠) من القانون ذاته حق صاحب البيانات في الاعتراض على المعالجة لأغراض التسويق المباشر؛ حيث أوجبت على مدير البيانات، بعد مُضِي فترة لا تجاوِز عشرة أيام عمل من تاريخ تسَلُّمه طلباً من صاحب البيانات مشفوعاً بما يثبت هويته، عدم البدء في المعالَجة التي تتم لأغراض التسويق المباشر لأية بيانات شخصية خاصة بمقدِّم الطلب، أو التوقف عن هذه المعالجة٣.

كما تقرر المادة (٢١) من القانون ذاته حق صاحب البيانات في الاعتراض على المعالَجة التي تُلحِق به أو بغيره ضرراً مادياً أو معنوياً؛ حيث تُلزم مدير البيانات، بعد مُضِي فترة لا تجاوِز عشرة أيام عمل من تاريخ تسَلُّمه طلباً من صاحب البيانات مشفوعاً بأسباب الطلب وأدلته وبما يثبت هويته، بعدم البدء في معالَجة أية بيانات شخصية خاصة بمقدِّم الطلب أو التوقف عن معالجتها كلياً أو لغرض أو على نحو معيَّن، وذلك إذا ما كانت المعالجة لذلك الغرض أو على ذلك النحو تُلحِق بصاحب البيانات أو غيره ضرراً مادياً أو معنوياً غير يسير وغير مبرَّر، أو إذا ما قامت أسباب معقولة تترجَّح نتيجة لها أنْ تُلحِق المعالَجة لذلك الغرض أو على ذلك النحو بصاحب البيانات أو غيره ضرراً مادياً أو معنوياً غير يسير وغير مبرر[٤].

وتمنح المادة (٢٢) من القانون ذاته الحق لصاحب البيانات في الاعتراض على القرارات التي تتم بناءً على المعالَجة الآلية في الحالات التي يتم فيها اتخاذ قرار استناداً فقط لمعالَجة آلية لبيانات شخصية لتقييم صاحب بيانات من ناحية أدائه في العمل، أو مركزه المالي، أو مدى كفاءته للاقتراض، أو سلوكه، أو مدى جدارته بالثقة. ويحق لصاحب البيانات أن يطلب اتِّباع أسلوب آخر لا يعتمد فقط على المعالَجة الآلية، ويجب على متخذ القرار إجابته إلى طلبه دون مقابل[٥].

كما تمنح المادة (٢٣) من القانون ذاته الحق لصاحب البيانات في المطالبة بالتصحيح والحَجْب

---

١. راجع المادة (١٨) من قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.
٢. راجع المادة (١٩) من قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.
٣. راجع المادة (٢٠) من قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.
٤. راجع المادة (٢١) من قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.
٥. راجع المادة (٢٢) من قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.

والمسح؛ حيث تقضي بأنه يجوز لكل صاحب بيانات أنْ يتقدم إلى مدير البيانات بطلب، مشفوع بما يثبت هويته، لتصحيح أو حَجْب أو مسح البيانات الشخصية الخاصة به بحسب الأحوال، إذا كانت معالجتها تتم بالمخالفة لأحكام القانون، وعلى الأخص إذا كانت البيانات غير صحيحة أو ناقصة أو غير محدَّثة، أو إذا كانت معالجتها غير مشروعة. ويجب على مدير البيانات، ما لم يكن لديه مسوِّغ مقبول قانوناً، الاستجابة للطلب دون مقابل، على أنْ يكون ذلك خلال عشرة أيام عمل من تاريخ تسَلُّم الطلب[1].

وقد حددت المادة (٢٤) من قانون حماية البيانات الشخصية شروط الاعتداد بموافقة صاحب البيانات في الحالات المشار إليها في هذا القانون، وتتمثل هذه الشروط في أنْ تكون الموافقة صادرة عن شخص كامل الأهلية، وأن تكونْ مكتوبة وصريحة وواضحة ومحدَّدة بمعالجة بيانات معينة، وأن تكون صادرة بناءً على إرادته الحرة بعد إحاطته تماماً بغرض أو أغراض معالَجة البيانات، وإحاطته، عند الاقتضاء، بالعواقب التي تترتب على عدم موافقته.

وإذا كان صاحب البيانات ناقص الأهلية أو عديمها، فيُعتد في هذه الحالة بموافقة الولي أو الوصي أو القيِّم في الحدود التي رسمها القانون. ويحق لصاحب البيانات، بموجب إخطار يُصدِره لمدير البيانات، أن يسحب في أيِّ وقت موافقته على معالجة بياناته الشخصية[2].

وقد أجازت المادة (٢٥) من قانون حماية البيانات الشخصية لكل صاحب مصلحة أو صفة أنْ يتقدم إلى هيئة حماية البيانات الشخصية بشكوى، إذا كان لديه ما يحمله على الاعتقاد بوقوع أية مخالفة لأحكام القانون سالف الذكر، أو بأن شخصاً ما يقوم بمعالجة بيانات شخصية بالمخالَفة لأحكامه[3].

وبذلك يكون المشرع قد أتاح لكل ذي مصلحة أو صفة أن يتقدّم بشكوى إلى وزارة العدل والشئون الإسلامية والأوقاف باعتبارها الجهة المختصة بالقيام بمهام هيئة حماية البيانات الشخصية، إذا كان لديه ما يحمله على الاعتقاد بوقوع أية مخالفة لأحكام قانون حماية البيانات الشخصية، أو بأن شخصاً ما يقوم بمعالجة بياناته الشخصية خلافاً لأحكام القانون. وبالتالي ضمن المشرع لكل الأفراد أن بياناتهم الشخصية تُعالج بطريقة مشروعة ومنصفة، وكفل لهم سبل المحافظة على حقوقهم في هذا الشأن.

سابعاً: العقوبات المقررة في قانون حماية البيانات الشخصية.

من المعلوم أن هناك نوعين من المسئولية القانونية، وهما المسئولية المدنية والمسئولية الجنائية، ويترتب على الأولى عقوبات مدنية تتمثل في التعويض الجابر للضرر، ويترتب على الأخيرة عقوبات جنائية تتمثل في الغرامة أو العقوبات السالبة للحرية. وحرصاً من المشرع البحريني على حماية البيانات الشخصية فقد نص في قانون حماية البيانات الشخصية المشار إليه على هذين النوعين من المسئولية القانونية.

١. راجع المادة (٢٣) من قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.
٢. راجع المادة (٢٤) من قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.
٣. راجع المادة (٢٥) من قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.

وفيما يتصل بالمسئولية المدنية، فقد أجاز المشرع لكل من لحقه ضرر نشأ عن معالجة بياناته الشخصية من قِبَل مدير البيانات، أو عن إخلال مراقب حماية البيانات بأحكام قانون حماية البيانات الشخصية، أن يطالب مدير البيانات أو مراقب حماية البيانات، بحسب الأحوال، بالتعويض الجابر لما لحقه من ضرر[1].

أما فيما يتعلق بالمسئولية الجنائية، فقد حدد المشرع في المادة (٥٨) من قانون حماية البيانات الشخصية العقوبات الجنائية التي يجوز الحكم بها على كل من يخالف أحكام هذا القانون، والتي تتراوح ما بين الحبس والغرامة[2]، وذلك التزاماً بالمبدأ الدستوري الذي يقضي بأنه لا جريمة ولا عقوبة إلا بناء على قانون[3].

وقد حرص المشرع على وضع نص خاص حدد فيه العقوبة الجنائية التي يتم الحكم بها على الشخص الاعتباري إذا ارتُكِبت باسمه، أو لحسابه، أو لمنفعته أية جريمة من الجرائم المنصوص عليها في المادة (٥٨) من قانون حماية البيانات الشخصية، وكان ذلك نتيجة تصرُّف، أو امتناع، أو موافقة، أو تستُّر، أو إهمال جسيم من أيٍّ من أعضاء مجلس إدارة الشخص الاعتباري، أو أيِّ مسئول مفوَّض آخر في ذلك الشخص الاعتباري، أو ممن يتصرف بهذه الصفة؛ حيث قرر معاقبة الشخص الاعتباري

---

١. راجع المادة (٥٧) من قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.

٢. تنص المادة (٥٨) من قانون حماية البيانات الشخصية المشار إليه على أن "يُعاقَب بالحبس مدة لا تزيد على سنة وبالغرامة التي لا تقل عن ألف دينار ولا تتجاوز عشرين ألف دينار، أو بإحدى هاتين العقوبتين، كلُّ مَن:

أ- عالج بيانات شخصية حساسة بالمخالفة لحكم المادة (٥) من هذا القانون.

ب- نقل بيانات شخصية خارج المملكة إلى بلد أو إقليم بالمخالفة لحكم أيٍّ من المادتين (١٢) و(١٣) من هذا القانون.

ج- عالج بيانات شخصية دون إخطار الهيئة بذلك بالمخالفة لحكم البند (١) من المادة (١٤) من هذا القانون.

د- تخلَّف عن إخطار الهيئة بأيِّ تغيير يطرأ على البيانات التي قام بإخطار الهيئة بها إعمالاً لحكم البند (١) من المادة (١٤) من هذا القانون، وذلك بالمخالفة لحكم البند (٦) من ذات المادة.

هـ- عالج بيانات شخصية دون تصريح مسبق من الهيئة بالمخالفة لحكم المادة (١٥) من هذا القانون.

و- قدَّم إلى الهيئة أو إلى صاحب البيانات بيانات كاذبة أو مضلِّلة أو على خلاف الثابت في السجلات أو البيانات أو المستندات التي تكون تحت تصَرُّفه.

ز- حجَب عن الهيئة أية بيانات أو معلومات أو سجلات أو مستندات من تلك التي يتعيَّن عليه تزويد الهيئة بها أو تمكينها من الاطلاع عليها؛ للقيام بمهامها المقرَّرة بموجب هذا القانون.

ح- تسبَّب في إعاقة أو تعطيل عمل مفتشي الهيئة أو أيِّ تحقيق تكون الهيئة بصدد إجرائه.

ط- أفصح عن أية بيانات أو معلومات من المتاح له النفاذ إليها بحكم عمله أو استخدمها لمنفعته أو لمنفعة الغير، وذلك دون وجه حق وبالمخالفة لأحكام هذا القانون.

٢- يعاقَب بالغرامة التي لا تقل عن ثلاثة آلاف دينار ولا تتجاوز عشرين ألف دينار مَن خالف حكم أيٍّ من البندين (١) أو (٢) من المادة (٣٢) من هذا القانون، وفي حالة الحكم بالإدانة للمحكمة أنْ تقضي بمصادرة المبالغ المتحصَّلة من الجريمة.

٣- يعاقَب بالحبس مدة لا تزيد على شهر وبالغرامة التي لا تقل عن مائة دينار ولا تتجاوز خمسمائة دينار، أو بإحدى هاتين العقوبتين، كل مَن استعمل دون وجه حق شعار الهيئة أو رمزاً أو شارة مماثلة أو مشابهة له.»

٣. تنص المادة (٢٠/أ) من الدستور البحريني على أن "لا جريمة ولا عقوبة إلا بناء على قانون، ولا عقاب إلا على الأفعال اللاحقة للعمل بالقانون الذي ينص عليها.»

بما لا يجاوز مِثْلَي الغرامة المقرَّرة للجريمة مع عدم الإخلال بالمسئولية الجنائية للشخص الطبيعي[١].
وأخيراً، فقد أجاز المشرع التصالح في بعض الجرائم المنصوص عليها في المادة (٥٨) من قانون حماية البيانات الشخصية المشار إليها بشرط الحصول على موافقة مجلس إدارة هيئة حماية البيانات الشخصية؛ حيث سمح لمجلس إدارة الهيئة أو مَن يفوِّضه الموافقة على التصالح، في غير حالة العوْد، في أيٍّ من الجرائم المنصوص عليها في البنود (١/ج) و(١/د) و(١/هـ) من المادة (٥٨) من قانون حماية البيانات الشخصية، وذلك في أية حالة تكون عليها الدعوى قبل صدور حكم باتٍّ فيها، مقابل سداد الحد الأدنى للغرامة المقرَّرة خلال سبعة أيام من الموافقة على التصالح. ويترتب على تمام التصالح انقضاء الدعوى الجنائية بالنسبة للجريمة محل التصالح، وذلك مع عدم الإخلال بحق المضرور في التعويض إنْ كان له مقتضى[٢].

المطلب الثالث
دور وزارة الداخلية في مكافحة جرائم القرصنة الإلكترونية

من المعلوم أنه في ظل جرائم القرصنة الإلكترونية قد يساهم أكثر من شخص في دول مختلفة في ارتكاب جريمة واحدة يقع ضحيتها عدد من الأفراد يقيمون في بلدان متعددة، فتظهر مشكلة التعارض والاختلاف بين التشريعات الإجرائية في دول العالم، ومنها اختلاف الجهات المختصة بالتفتيش، والشروط والإجراءات والندب لأعضاء الضابطة العدلية فيها. وتقتضي مكافحة جرائم المعلومات والقرصنة الإلكترونية توحيد التشريعات الإجرائية، وأن يكون نظام الإثبات بالدليل الإلكتروني واحداً بين الدول التي تقع فيها هذه الجرائم، وهذا أمر مستحيل تحقيقه[٣]. ولذلك لابد أن يكون هناك تعاون دولي يتفق مع طبيعة هذه الجرائم التي تتميز بطابع خاص يقتضي أن تكون هناك إجراءات تحقيقية سريعة، ويسمح هذا التعاون الدولي بسهولة الاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وذلك عن طريق انشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالإنترنت والحاسوب وتعميمها[٤].

وتؤدي وزارة الداخلية في مملكة البحرين دوراً بارزاً وحيوياً في إطار مواجهة ومكافحة جرائم القرصنة الإلكترونية منذ سنوات طويلة؛ حيث تم إنشاء إدارة مكافحة الجرائم الاقتصادية بوزارة الداخلية في عام ٢٠٠٤ بموجب المرسوم رقم (٦٩) لسنة ٢٠٠٤ بإعادة تنظيم وزارة الداخلية[٥]؛ وذلك

---

١. راجع المادة (٥٩) من قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.

٢. راجع المادة (٦٠) من قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.

٣. راجع في ذلك د. جميل عبد الباقي الصغير، الجوانب الإجرائية المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ٢٠٠١، ص ٧٢ وما بعدها.

٤. راجع في ذلك مستشار د. عبدالفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، ٢٠٠٢، ص ١٠٢ وما بعدها.

٥. المرسوم رقم (٦٩) لسنة ٢٠٠٤ بإعادة تنظيم وزارة الداخلية، منشور في الجريدة الرسمية العدد رقم (٢٦٥٩) بتاريخ ٢٠٠٤/١١/٣.

من أجل حماية الحقوق والمصالح المشروعة للمواطنين والمقيمين والشركات في ظل سيادة القانون.
وحرصاً على مواكبة التطورات التي تشهدها الساحة على جميع الأصعدة المحلية والإقليمية والدولية في مجال الأمن الاقتصادي والإلكتروني، وفي ظل تزايد الجرائم الاقتصادية والجرائم الإلكترونية، وغسيل الأموال، والجريمة المنظمة بكافة أشكالها، وجرائم الفساد، فقد تم تطوير إدارة مكافحة الجرائم الاقتصادية بوزارة الداخلية لتصبح الإدارة العامة لمكافحة الفساد والأمن الاقتصادي والإلكتروني، وذلك بموجب المرسوم رقم (١٠٩) لسنة ٢٠١١ بتعديل بعض أحكام المرسوم رقم (٦٩) لسنة ٢٠٠٤ بإعادة تنظيم وزارة الداخلية[١].

وتُعنى الإدارة العامة لمكافحة الفساد والأمن الاقتصادي والإلكتروني بالأمن الاقتصادي والإلكتروني في مختلف القطاعات بالمملكة، ويشمل ذلك قطاع الطاقة، والقطاع المالي والمصرفي، والقطاع الصحي، والقطاع التعليمي، وغيرها من القطاعات.

وتتألف هذه الإدارة العامة من عدد من الإدارات الأمنية التي تهدف إلى حفظ دعائم الاقتصاد الوطني، وتعزيز البيئة الاقتصادية الآمنة لدفع عجلة التنمية، وهي: إدارة مكافحة جرائم الفساد، وإدارة مكافحة الجرائم الإلكترونية، وإدارة مكافحة الجرائم الاقتصادية، وإدارة التحريات المالية، وإدارة البحث والتحري، وإدارة الشئون الدولية والإنتربول.

وتعتمد هذه الإدارة العامة في إستراتيجيتها في مكافحة الجريمة الإلكترونية على أحدث العلوم الأمنية، وتستهدف خفض بيئة المخاطر الرقمية للحد من الجرائم المرتكبة باستخدام تكنولوجيا المعلومات والاتصالات الحديثة من خلال إنفاذ القانون، والوقاية من الجريمة الإلكترونية بكافة أنماطها المستحدثة، وتلقي ومباشرة البلاغات الأمنية وإحالتها للنيابة العامة، وتنفيذ الاستراتيجيات المتعلقة بمكافحة جرائم تقنية المعلومات في المملكة، بالإضافة إلى متابعة ومراجعة التشريعات مع الجهات المختصة، والتعاون والمشاركة في الجهود الدولية لمكافحة الجريمة الإلكترونية العابرة للحدود الوطنية، وذلك كله بغية حماية المجتمع من الآثار السلبية لهذه الآفة المعاصرة.

كما تضطلع الإدارة العامة سالفة الذكر بدور مهم للغاية في توعية الجمهور بالجرائم الإلكترونية؛ حيث تقوم بعقد العديد من الندوات التثقيفية وورش العمل والمحاضرات التوعوية في المدارس والجامعات والمؤسسات الحكومية والخاصة بهدف تعزيز دور الأفراد في المحافظة على أمنهم الإلكتروني، والتبليغ عن الجريمة قبل وقوعها، بالإضافة إلى نشر العديد من الموضوعات التوعوية عبر وسائل الإعلام المختلفة المسموعة والمقروءة والمرئية، ومن خلال المواقع الإلكترونية الخاصة بوزارة الداخلية على منصات التواصل الاجتماعي.

---

١. المرسوم رقم (١٠٩) لسنة ٢٠١١ بتعديل بعض أحكام المرسوم رقم (٦٩) لسنة ٢٠٠٤ بإعادة تنظيم وزارة الداخلية، منشور في الجريدة الرسمية العدد رقم (٣٠٢٨) بتاريخ ٢٠١١/١٢/١.

ومن ناحية أخرى، تعمل الإدارة العامة المشار إليها على رصد الممارسات واتجاهات الأنشطة المشبوهة من خلال فريق تقني يعمل على مدار الساعة لتأخذ دوراً استباقياً قبل وقوع الجريمة، خصوصاً تلك التي تهدف إلى الاحتيال، أو نشر الشائعات والأخبار الكاذبة، أو الإضرار ببيئة الأعمال والأنشطة التجارية، كما يقوم الفريق التقني بالتعاون مع الجهات الحكومية ذات الصلة بحجب تلك المواقع بعد اتخاذ الإجراءات القانونية حيال ذلك.

وتأكيداً لاهتمام المملكة بالأمن السيبراني، فقد تم إنشاء المركز الوطني للأمن السيبراني بموجب المرسوم رقم (٦٥) لسنة ٢٠٢٠ بتعديل بعض أحكام المرسوم رقم (٦٩) لسنة ٢٠٠٤ بإعادة تنظيم وزارة الداخلية[١]، ويشتمل هذا المركز على رئيس تنفيذي بدرجة وكيل وزارة، ويتبعه نائب الرئيس للعمليات السيبرانية بدرجة وكيل مساعد، وتتبعه عدة إدارات هي: إدارة الحماية السيبرانية، وإدارة الاستجابة الوطنية، وإدارة التنسيق والتحليل، وإدارة الدعم وعمليات الحاسب الآلي، وإدارة تطوير النُّظُم الأمنية، وإدارة المتابعة والتثقيف، وإدارة السياسات السيبرانية.

وتحرص وزارة الداخلية دائماً على الاستعداد لمواجهة التهديدات الجديدة الناشئة عن التطور المستمر في التكنولوجيا، وذلك من خلال إعداد إستراتيجيات مستقبلية تواكب التحديات، ومن ذلك تبني مفهوم الشرطة الذكية، والتوسع في استخدام تطبيقات الذكاء الاصطناعي.

خاتمة البحث

بعد الانتهاء من دراسة موضوع البحث الماثل، نخلص إلى عدة نتائج وتوصيات نوضحها على النحو الآتي:

أولاً: النتائج

١- يقُصد بجرائم القرصنة الإلكترونية ممارسات غير مشروعة تهدف إلى التحايل على نظام المعالجة الآلية للبيانات وتقنية المعلومات بغية الوصول غير المرخص إلى الحسابات وأنظمة التشغيل، أو إتلاف المستندات المعالجة إلكترونياً، أو تعديل البيانات، أو سرقتها، أو إتلافها، أو أي إجراءات ضارة أخرى، وذلك من خلال أساليب متنوعة تعتمد على وسائل التقنية المتطورة.

٢- تُعد جرائم القرصنة الإلكترونية من أخطر التحديات التي تواجهنا في الوقت الراهن، فهي ظاهرة عالمية منتشرة انتشاراً واسعاً بسبب الثورة التكنولوجية الكبيرة التي نعيشها اليوم، وشيوع استخدام شبكة الإنترنت ومواقع التواصل الاجتماعي المتنوعة، وقد تتصل الأرباح المُتحصلة من تلك الجرائم بأنشطة إجرامية أخرى، مثل: غسل الأموال، وتمويل الإرهاب، والاتجار بالبشر.

---

١. المرسوم رقم (٦٥) لسنة ٢٠٢٠ بتعديل بعض أحكام المرسوم رقم (٦٩) لسنة ٢٠٠٤ بإعادة تنظيم وزارة الداخلية، منشور في الجريدة الرسمية العدد رقم (٣٤٩٣) بتاريخ ٢٠٢٠/١٠/١٥.

٣- يتميز قرصان المعلومات الذي يرتكب جرائم القرصنة الإلكترونية بأنه يكون عادة من ذوي المعرفة في مجال تقنية المعلومات. وتم تصنيف قراصنة المعلومات إلى نوعين، وهما: الهاكرز Hackers وهؤلاء يعملون على ابتكار الحلول للمشاكل بصفة عامة، والكراكرز Crackers وهم المخترقون المحترفون الذين يقومون دائماً بأعمال التخريب والاقتحام والاعتداء على الأموال.

٤- تولي مملكة البحرين اهتماماً بالغاً بتجريم ظاهرة القرصنة الإلكترونية بهدف مكافحة جرائمها، والوقاية منها، وحماية الأفراد والمجتمع من شرورها. وقد حققت نجاحاً ملحوظاً في هذا الشأن؛ حيث أصدرت عدة قوانين حديثة بشأن جرائم تقنية المعلومات، وحماية البيانات الشخصية، وتحرص على التطوير والتحديث المستمر لهذه القوانين، وانفاذها بكل شفافية وحسم، وكذلك تعمل على توفير خدمات تقنية المعلومات والاتصالات بشكل مستدام وآمن يدعم تحقيق اقتصاد رقمي قوي، كما أن لديها منظومة لحوكمة الأمن الإلكتروني تتجسد في الإدارة العامة لمكافحة الفساد والأمن الاقتصادي والإلكتروني، والمركز الوطني للأمن السيبراني التابعين لوزارة الداخلية.

ثانياً: التوصيات

١- نوصِي الجهات الرسمية المعنية في مملكة البحرين بإنشاء دوائر قضائية متخصصة للنظر في جرائم القرصنة الإلكترونية في ظل تزايد أعداد القضايا الخاصة بها وتطورها بصورة مستمرة؛ إذ تتميز هذه الجرائم عن الجرائم التقليدية بكونها جرائم عابرة للحدود، ومن الصعب إثباتها، وترتبط ارتباطاً وثيقاً بشبكة الإنترنت.

٢- نوصِي المشرع البحريني بتحديث وتطوير طرق التحري والملاحقة والتحقيق واستخدام أشكال مستحدثة من الأدلة في مجال الإثبات الجنائي فيما يتعلق بهذه الجرائم، مع ضرورة توفير التدريب والتأهيل اللازمين للمختصين على كيفية التعامل مع هذا النوع من الجرائم لمواجهة تهديدات الأمن السيبراني المتزايدة.

٣- نوصِي الجهات الرسمية المعنية في مملكة البحرين بزيادة الاهتمام بنشر الوعي بين مستخدمي شبكة الإنترنت ومواقع التواصل الاجتماعي بمخاطر جرائم القرصنة الإلكترونية وكيفية تجنبها قدر الإمكان؛ إذ يمثل وعي المستخدمين خط الدفاع الأول للوقاية الاستباقية من هذه المخاطر. ونقترح عقد المزيد من ورش العمل التدريبية والجلسات النقاشية مع أبرز الخبراء والشركات العاملة في مجال حماية الأمن السيبراني.

٤- ينبغي على جميع الدول التعاون فيما بينها، وتطوير التشريعات الخاصة بمكافحة جرائم القرصنة الإلكترونية مع النص على عقوبات جنائية شديدة مما يُمكنها من مواجهة تحديات التطورات التكنولوجية المتسارعة، وتحسين حماية البيانات؛ لأن كل شيء في حياتنا المعاصرة بات متصلاً بالفضاء الإلكتروني.

قائمة المصادر والمراجع

أولاً: المصادر الأساسية

١- قانون حماية البيانات الشخصية الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨.

٢- القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات.

٣- المرسوم بقانون رقم (٤) لسنة ٢٠٠١ بشأن حظر ومكافحة غسل الأموال وتمويل الإرهاب، وتعديلاته.

٤- قانون العقوبات الصادر بالمرسوم بقانون رقم (١٥) لسنة ١٩٧٦، وتعديلاته.

٥- اتفاقية الأمم المتحدة لقانون البحار (UNCLOS) لعام ١٩٨٢.

٦- المرسوم رقم (٦٥) لسنة ٢٠٢٠ بتعديل بعض أحكام المرسوم رقم (٦٩) لسنة ٢٠٠٤ بإعادة تنظيم وزارة الداخلية.

٧- المرسوم رقم (٧٨) لسنة ٢٠١٩ بتحديد الجهة الإدارية التي تتولى المهام والصلاحيات المقرَّرة لهيئة حماية البيانات الشخصية.

٨- المرسوم رقم (١٠٩) لسنة ٢٠١١ بتعديل بعض أحكام المرسوم رقم (٦٩) لسنة ٢٠٠٤ بإعادة تنظيم وزارة الداخلية.

٩- المرسوم رقم (٦٩) لسنة ٢٠٠٤ بإعادة تنظيم وزارة الداخلية.

١٠- قرار وزير العدل والشئون الإسلامية والأوقاف رقم (٤٣) لسنة ٢٠٢٢ بتحديد الاشتراطات التي يتعين توافرها في التدابير الفنية والتنظيمية الكفيلة بحماية البيانات الشخصية.

ثانياً: الكتب والرسائل

١- أحمد المشد، القرصنة الإلكترونية وأمن المعلومات، مؤسسة الأمة العربية للنشر والتوزيع، القاهرة، ٢٠١٧.

٢- د. إلياس ناصيف، العقود الدولية، العقود الإلكترونية في القانون المقارن، منشورات الحلبي الحقوقية، لبنان، ٢٠٠٩.

٣- د. جميل عبد الباقي الصغير، الجوانب الإجرائية المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ٢٠٠١.

٤- حنان ريحان مبارك المضحكي، الجرائم المعلوماتية دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، ٢٠١٤.

٥- داريل بانيثي، استمرار القرصنة وآثارها على الإبداع والثقافة والتنمية المستدامة، دراسة مُعدة بناء على طلب أمانة منظمة الأمم المتحدة للتربية والعلوم والثقافة في الجلسة الثالثة عشرة للجنة الدولية لحقوق المؤلف، باريس، ٢٠٠٥.

٦- د. شحاته غريب شلقامي، التعاقد الإلكتروني في التشريعات العربية دراسة مقارنة، دار الجامعة الجديدة.

٧- عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية دراسة مقارنة، رسالة ماجستير في القانون، جامعة الشرق الأوسط، ٢٠١٤.
٨- مستشار د. عبدالفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، ٢٠٠٢.
٩- مستشار د. عبدالفتاح بيومي- حجازي، النظام القانوني للحكومة الإلكترونية، الكتاب الثاني الحماية الجنائية والمعلوماتية للحكومة الإلكترونية، دار الكتب القانونية، ٢٠٠٧.
١٠- د. علاء محمد الفواعير، العقود الإلكترونية دراسة مقارنة، دار الثقافة للنشر والتوزيع، ٢٠١٤.
١١- د. علي حسن الطوالبه، أبحاث في جرائم تقنية المعلومات، دار الكتب والدراسات العربية، الإسكندرية، ٢٠١٨.
١٢- د. علي عدنان الفيل، الإجرام الإلكتروني دراسة مقارنة، منشورات زين الحقوقية، ٢٠١١.
١٣- د. محمد حسين منصور، المسئولية الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٣.
١٤- د. محمد زكي أبوعامر، قانون العقوبات القسم العام، الدار الجامعية، بيروت، ١٩٩٣.
١٥- د. محمد طارق عبدالرؤوف الخن، جريمة الاحتيال عبر الإنترنت (الأحكام الموضوعية والأحكام الإجرائية)، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، ٢٠١١.

ثالثاً: الأبحاث والمقالات المنشورة على شبكة الإنترنت

١- د. أحمد عَلّو، القرصنة بين العصور القديمة وعصر التكنولوجيا، بحث منشور على الرابط:
https://www.lebarmy.gov.lb/ar/content/%D8%A7%D984%%D982%%D8%B1%D8%B5%D986%%D8%A9-%D8%A8%D98%A%D986-%%D8%A7%D984% %D8%B9%D8%B5%D988% %D8%B1-%D8%A7%D984% %D982% %D8%AF%D98 %A%D985% %D8%A9-%D988%%D8%B9%D8%B5%D8%B1-%D8%A7%D984%%D8%AA%D983%%D986%%D988%%D984%%D988%%D8%AC%D98%A%D8%A7 (Accessed on: 7 September 2022)
٢- روب وو، مقال بعنوان: ما المهارات المطلوبة لمكافحة القرصنة الإلكترونية؟ منشور على الرابط:
https://1-a1072.azureedge.net/news/presstour/201818/7//%D985%%D8%A7-%D8%A7%D984%%D985%%D987%%D8%A7%D8%B1%D8%A7%D8%AA-%D8%A7%D984%%D98%5%D8%B7%D984%%D988%%D8%A8%D8%A9-%D984%%D985%%D-983%%D8%A7%D981%%D8%AD%D8%A9-%D8%A7%D984%%D982%%D8%B1%D8%B5%D986%%D8%A9 (Accessed on: 8 September 2022)
٣- طه عيساني، القرصنة الإلكترونية؛ الضرر الاقتصادي والفكري، بحث في جامعة الجزائر، منشور على منصة المنهل الإلكترونية على الرابط:
https://platform.almanhal.com/Files/292628/ (Accessed on: 27 September 2022)

٤- بحث بعنوان: ethical hacking منشور على الرابط:
https://www.synopsys.com/glossary/what-is-ethical-hacking.html (Accessed on: 5 October 2022)

٥- بحث بعنوان: جريمة القرصنة الإلكترونية، منشور على الرابط:
https://www.mohamah.net/law/%D8%A8%D8%AD%D8%AB-%D982% %D8%A7%D986% %D988% %D986% %D98 %A-%D985%%D981%%D98%A%D8%AF-%D8%AD%D988%%D984-%%D8%AC%D8%B1%D98%A%D985%%D8%A9-%D8%A7%D9--84%D982% %D8%B1%D8%B5%D986% %D8%A9-%D8%A7%D984%%D8%A5%D984%/ (Accessed on: 28 September 2022)

٦- مقال بعنوان: القرصنة الإلكترونية، منشور على الرابط:
https://www.dw.com/ar/%D8%A7%D984%%D982%%D8%B1%D8%B5%D986%%D8%A9-%D8%A7%D984%%D8%A5%D984%%D983%%D8%AA%D8%B1%D988%%D986%%D98%A%D8%A9/t-19111848 (Accessed on: 7 September 2022)

٧- مقال بعنوان: القرصنة الإلكترونية.. هل تعلم قيمة الخسائر التي تكبّدها للعالم؟، منشور على الرابط:
https://www.alaraby.co.uk/economy/%D8%A7%D984%%D982%%D8%B1%D8%B5%D986%%D8%A9-%D8%A7%D984%%D8%A5%D984%%D983%%D8%AA%D8%B1%D988%%D986%%D98%A%D8%A9-%D987%%D984-%%D8%AA%D8%B9%D984%%D985-%%D982%%D98%A%D985%%D8%A9-%D8%A7%D984%%D8%AE%D8%B3%D8%A7%D8%A6%D8%B1-%D8%A7%D984%%D8%AA%D98%A-%D8%AA%D983%%D8%A8%D991%%D8%AF%D987%%D8%A7-%D9-84%%D984%%D8%B9%D8%A7%D984%%D985%%D89%F (Accessed on: 11 September 2022)

٨- مقال بعنوان: هل ما نعرفه عن قراصنة الإنترنت صحيح؟، منشور على الرابط:
https://1-a1072.azureedge.net/news/scienceandtechnology/202129 /7 //%D982% %D8%B1%D8%A7%D8%B5%D986% %D8%A9-%D8%A7%D984% %D8%A5%D986% %D8%AA%D8%B1%D986% %D8%AA-%D985% %D986-% %D987% %D985-% %D-988%%D983%%D98%A%D981-%%D98%A%D8%B9%D985%%D984%%D988%%D986%%D89%F (Accessed on: 11 September 2022)

٩- معجم المعاني الجامع - معجم عربي عربي، منشور على الرابط:
https://www.almaany.com/ar/dict/ar-ar/%D982%%D8%B1%D8%B5%D986%%D8%A9/ (Accessed on: 7 September 2022)