Dirasat: *Shari'a and Law Sciences*, Volume 47, No. 1, 2020

Deanship of Scientific Research

The Role of Jordanian Legislation in Countering Cybercrime and its Impact on Library Information Security

Ashraf Ali Oqlah ALkawakzeh

Legislative Studies and Research Center, Jordanian House of Representatives, Jordan.

Received: 15/5/2019
Revised: 16/7/2019
Accepted: 30/10/2019
Published: 1/3/2020

Citation: ALkawakzeh, A. A. O. . (2020). The Role of Jordanian Legislation in Countering Cybercrime and its Impact on Library Information Security. *Dirasat: Shari'a and Law Sciences*, *47*(1), 428–439. Retrieved from https://dsr.ju.edu.jo/djournals/index.php/Law/article/view/2676

Abstract

The aim of this study was to identify the impact of electronic crimes on the information security in libraries, and to determine the adequacy of national legislation to confront and combat electronic crimes that threaten the information security in libraries and constitute a violation of it.the researcher used the analytical approach by analyzing the legal texts in the legislation and indicating the adequacy of their shortcomings, and the comparative descriptive approach through the legal description of electronic crimes and their impact on the information security of libraries in Jordanian legislation. The study reached a set of conclusions and recommendations, the most important of which was that information and data in libraries are threatened by risks generated by the technological revolution, and they need technical and legal means of protection at the same time to face their risks, and the need remains urgent to develop special texts for the law of electronic crimes that deal with this type of crime in detail and commensurate with the enormous development in the field of technological means, due to the lack of provisions of the law of electronic crimes related to the protection of information security of libraries in particular. The study recommended the need for international cooperation in combating cybercrime by holding conferences, exchanging experiences and concluding agreements.

Keywords Cybercrime, library information security, technical means.

دورالتشريع الأردني في مواجهة الجريمة الإلكترونية و أثرها في أمن معلومات المكتبات

أشرف علي عقلة القواقزة

مركز الدراسات والبحوث التشريعية، مجلس النواب الأردني، الأردن.

ملخّص

هدفت هذه الدراسة إلى الوقوف على أثر الجرائم الإلكترونيّة في أمن المعلومات في المكتبات، وتحديد مدى كفاية التشريعات الوطنية لمواجهة ومكافحة الجرائم الإلكترونيّة التي باتت تهدّد أمن المعلومات في المكتبات وتشكّل خرقًا لها؛ حيث استخدم الباحث المنهج التحليلي من خلال تحليل النصوص القانونية في التشريع وبيان مدى كفايتها من قصورها، والمنهج الوصفي المقارن من خلال الوصف القانوني للجرائم الإلكترونيّة وأثرها في أمن معلومات المكتبات في التشريع الأردني. وتوصّلت الدراسة إلى مجموعة من النتائج والتوصيات، كان من أهمّها أن المعلومات والبيانات في المكتبات مهدّدة بمخاطر أفرزتها الثورة التكنولوجية، وهي بحاجة إلى وسائل حماية تَقَنِيّة وقانونية في آن لمواجهة مخاطرها، كما أنّ الحاجة تبقى ملحّة إلى وضع نصوص خاصّة بقانون الجرائم الإلكترونيّة تعالج هذا النوع من الجرائم على نحوٍ تفصيلي وبما يتناسب مع التطوّر الهائل في مجال الوسائل التكنولوجيّة؛ نظرًا إلى افتقار قانون الجرائم الإلكترونيّة لنصوص تتعلّق بحماية أمن معلومات المكتبات على وجه الخصوص. أوصت الدراسة بضرورة تعاون دولي في مكافحة الجرائم الإلكترونيّة عن طريق عقد المؤتمرات وتبادل الخبرات وعقد الاتفاقيات.

الكلمات الدالّة: الجريمة الإلكترونيّة، أمن معلومات المكتبات، الوسائل التَقَنِيّة.

المقدّمة

أدى التطور الكبير والمتسارع في مجال التكنولوجيا والاتصالات، الذي شهده العالم في السنوات الأخيرة من هذا القرن إلى ظهور العديد من الوسائل الإلكترونيّة التي تُستخدم بِوَصْفِها تَقَنِيّات للتواصل بين الأفراد والجماعات والمؤسسات كمجتمع أطلق عليه "الافتراضي"، والواقع أن هذه الوسائل وإن كانت تُعَدُّ من الإنجازات البشرية المهمّة التي تحقق رفاه المجتمعات فإنها باتت الأكثر استخدامًا لارتكاب الجرائم بصورها وأنماطها المختلفة (العدوان، 2018)، ومنها الاعتداء على أمن المعلومات في المكتبات؛ حيث عملت المكتبات جاهدةً على تطوير آليات عملها أتعتمد على الوسائل الإلكترونيّة الحديثة والنظم المعلوماتية ومصادر المعلومات الإلكترونيّة بهدف توفير خدماتها وتحقيق إمكانية الوصول إليها من الداخل والخارج ودعم وظائفها وأدائها، وفي مقابل ذلك أدّى هذا التطور في عمل المكتبات واعتمادها على الوسائل الإلكترونيّة الحديثة وانفتاحها على العالم بدخولها عالم الإنترنت إلى تعرض أمن المعلومات لديها لخطر الاختراق والتخريب والسرقة وغيرها من الأفعال التي تهدد أمن المعلومات في المكتبات، بحيث يمكن أن يعتدي على هذه المعلومات شخصٌ في أي دولة ومن أي مكان يهدد أمنها ويلحق بها ضررًا بالغًا (خالد، 2017).

وتتعدد الوسائل الإلكترونيّة التي قد يصار إلى استخدامها في هذه الجريمة، والتي تستخدم الإنترنت (الشبكة المعلوماتية) بشكل اساسي لدعم الوسائل الإلكترونيّة في ارتكاب الجرائم الإلكترونيّة، كأجهزة الكمبيوتر، والهواتف الذكية، والفيس بوك، وغيرها الكثير من الوسائل التي يشهدها كل يوم عالم التكنولوجيا والتَقَنِيّات (الشوابكة، 2011).

وبالرغم من الجهود التي بذلتها جميع الدول، ومن بينها المملكة الأردنية الهاشمية، في سبيل الوقاية من هذه الجرائم ومكافحتها، سواء من خلال سَنّ التشريعات أو اتخاذ الإجراءات الأمنية والتَقَنِيّة أو عقد الاتفاقيات والمعاهدات الدولية، فإنّ تلك الجرائم ما زالت تشكّل خطورة كبيرة ومتزايدة تهدّد أمن المكتبات، خاصّة في ظلّ الاعتماد المتزايد على الوسائل الإلكترونيّة وتطوّرها المتسارع، وإزاء هذا كلّه يبرز دور التشريعات الجزائية في مواجهة خطر هذا النوع الجديد من الجرائم الذي بات يهدد المجتمعات بأسرها ويشكّل تحدّيًا كبيرًا لاختلافها النوعي عن الجرائم التقليدية.

وقدر تعلّق الأمر بالتشريع الأردني نجد أن المشرّع الأردني قد سلك هذا النهج أُسوة بغيره من المشرّعين؛ بغية تحقيق أهداف تساعد على حماية مواطنيه ورعاية مجتمعه على حدّ سواء، ابتداء من قانون العقوبات رقم (16) لسنة 1960 وتعديلاته، وقانون المعاملات الإلكترونيّة رقم (15) لسنة 2015 وقانون الاتصالات رقم (13) لسنة 1995، وقانون أصول المحاكمات الجزائية رقم (9) لسنة 1961، وصولًا إلى قانون الجرائم الإلكترونيّة رقم (27) لسنة 2015 الذي يشكّل حجر الأساس لتجريم الأفعال الجرمية الإلكترونيّة ومكافحتها، ومنها جرائم الاعتداء على أمن المعلومات في المكتبات، الأمر الذي سيكون موضوع دراستنا.

وسيتم تناول هذا الموضوع في مطلبين، يهدف أولهما إلى بيان ماهيّة الجرائم الإلكترونيّة، أما ثانيهما فيهدف إلى بيان أنماط الجرائم الإلكترونيّة التي تهدد أمن معلومات المكتبات وطرق الوقاية منها على النحو الآتي:

المطلب الأول: ماهية الجرائم الإلكترونيّة.

المطلب الثاني: أنماط الجرائم الإلكترونيّة التي تهدد أمن المعلومات.

مشكلة الدراسة

لا شكّفي أنّ الثورة التكنولوجية التي شهدها العالم خلال العقود الأخيرة من هذا القرن قد ساهمت في ظهور أنماط جديدة من الجرائم التي لم تكن مألوفة من قبل، ومن أهمها الجرائم الإلكترونيّة، وباعتماد المكتبات على الوسائل الإلكترونيّة وإدخالها للتكنولوجيا في صميم عملها وانفتاحها على العالم ووجودها على شبكة الويب والشبكات المحلية سعيًا منها إلى التسهيل على المستفيدين بالوصول إلى المعلومات واستخدام مرافقها ودعمًا لوظائفها الإداريّة أصبح الاعتداء على أمن المعلومات في المكتبات أمر محتمل، وبالرغم من بذل المشرّع الأردني جهدًا كبيرًا في التصدي لمواجهة الجرائم الإلكترونيّة على نحوٍ عام فإنّ زيادة فاعلية مواجهة هذا النوع الجديد من الجرائم المستحدثة يتطلّب مراجعة للسياسات التشريعية الأردنية وبذل مزيد من الجهود في هذا المجال؛ لذا تتمثل مشكلة هذه الدراسة في تعرُّف **مدى كفاية التشريعات الجزائية الأردنية في مكافحة جرائم الاعتداء الإلكتروني على أمن المعلومات في المكتبات**، خاصّة قانون الجرائم الإلكترونيّة.

ثالثًا: عناصر مشكلة الدراسة

نبني إشكالية الدراسة على عدد من تساؤلات، مفادها.

- هل يمكن تحديد أنماط الوسائل الإلكترونيّة التي ترتكب عن طريقها جريمة الاعتداء الإلكترونيّة على أمن المعلومات في المكتبات؟
- ما موقف المشرّع الجزائي الأردني وسياسته في التعامل مع هذا النوع من الجرائم؟

فرضيات الدراسة

يرى الباحث أن فرضيات الدراسة تستند إلى ما يلي:

- يمكن تحديد أنماط الوسائل الإلكترونيّة التي ترتكب عن طريقها جريمة الاعتداء الإلكترونيّة على أمن المعلومات في المكتبات.
- هناك نقص واضح في التشريعات الأردنية بشأن جرائم الاعتداء الإلكتروني على أمن المعلومات في المكتبات ووضع الحلول للمشكلات التي تواجه هذا الموضوع.
- إمكانية تحديد المخاطر التي افرزتها التَقَنِيّات الحديثة التي تهدد أمن المكتبات.

أهمية الدراسة

تتمثل الأهمية البحثية لهذه الدراسة في أنها تعالج موضوعًا قانونيًّا مهمًّا وتساهم من ثَمَّ -ولو على نحو متواضع- في سدّ النقص في المكتبة القانونية الخاصة بالجرائم الإلكترونيّة في التشريع الأردني التي تخلو إلى حدّ ما من أبحاث قانونية متخصّصة بهذا المجال، ودراسة موقف الفقه والقضاء من موضوع الجرائم الإلكترونيّة، خاصّة جريمة الاعتداء على أمن المعلومات في المكتبات في القانون الأردني، ومن هنا جاء هذا البحث ليضيف جهدا متواضعا ولتغطية ما اعترى الموضوع من نقص.

أهداف الدراسة

تسعى هذه الدراسة إلى تحقيق هدف أساسي منها، هو الإحاطة بموضوع الجرائم الإلكترونيّة وأثرها في أمن المعلومات في المكتبات وضبط حدودها ومجالها والإلمام بإحكامها، خاصّة بسبب ما نراه اليوم من تطور هائل في الوسائل الإلكترونيّة التي شملت جميع الميادين وانفتاح العالم على بعضه بحيث أصبح قرية صغيرة، وانتشار الجريمة وتطورها وعدم وقوفها عند حدود معيّنة، بحيث أصبحت تهدد جميع الدول دون استثناء، كما تسعى إلى تحقيق الأهداف الآتية:

- تقديم رؤية قانونية واضحة حول الجرائم الإلكترونيّة وأثرها في أمن المعلومات في المكتبات، ووسائلها، وخصائصها.
- تحديد مدى كفاية التشريعات الوطنية لمواجهة ومكافحة الجرائم الإلكترونيّة، خاصّة الاعتداء على أمن المعلومات في المكتبات.
- تحديد ماهية الوسائل الإلكترونيّة وأنواعها التي ترتكب عن طريقها جرائم الاعتداء الإلكتروني على أمن المعلومات في المكتبات.
- الإحاطة بموقف المشرّع الجزائي الأردني وسياسته في التعامل مع هذا النوع من الجرائم.

منهجية الدراسة

المنهج المتبع في هذه الدراسة هو المنهج التحليلي من خلال تحليل النصوص القانونية في التشريع وبيان مدى كفايتها من قصورها، والمنهج الوصفي المقارن من خلال الوصف القانوني للجرائم الإلكترونيّة وأثرها في أمن معلومات المكتبات في التشريع الأردني.

المطلب الأول

ماهية الجرائم الإلكترونيّة

تعتبر الجريمة الإلكترونيّة من الآثار السلبية التي خلفتها التَقَنِيّات العالمية، وفي ضوء ذلك سارعت الدول إلى وضع التشريعات الخاصة بمكافحة الجرائم الإلكترونيّة، ومن أمثلة ذلك سَنُّ المشرّع الأردني قانون جرائم أنظمة المعلومات رقم (30) لسنة 2010 المعدل بموجب قانون الجرائم الإلكترونيّة رقم (27) لسنة 2015، إضافة إلى قانون المعاملات الإلكترونيّة رقم (15) لسنة 2015.

ولا شكّ في أنّ هذا النوع من الجرائم المستحدثة قد أخذ حيزًا كبيرًا من الدراسات من أجل تحديد المقصود بها، وكذلك خصائصها التي تمتاز بها وأهم أنواعها، وهو ما سنتناوله في هذا المبحث على النحو الآتي:

الفرع الأول: المقصود بالجرائم الإلكترونيّة.

إن تعريف الجرائم الإلكترونيّة يقتضي منا في البداية التمهيد له بتعريف الجريمة بصورة عامة، لتمييزها عن الجرائم المستحدثة، والتي بات يطلق عليها الجرائم الإلكترونيّة، هذا ولم تتناول التشريعات الجزائية ومنها التشريع الأردني، خشية حصرها في مجال معين بحيث تصبح قيدًا على هذه التشريعات، تاركًا المشرّع مهمة تعريفها إلى الفقه والقضاء.

كما تعددت التعريفات الفقهية في تحديد المقصود بالجريمة بصفة عامة، إلّا أنه لا يوجد بينها اختلاف كبير؛ حيث عرفها جانب من الفقه بأنها "سلوك غير مشروع صادر عن إرادة جنائية يقرر لها القانون عقوبة أو تدبيرا احترازيا" (حسني، 1989)، كما عرفها البعض بأنها "كل فعل أو امتناع عن فعل صادر عن شخص مميز، يحدث خرقًا أو اضطرابًا اجتماعيًّا عامًّا أو خاصًّا، ويعاقب عليه القانون بعقوبة جزائية أو تدبير احترازي" (نجم، 2000).

من ذلك يتضح لنا أن جميع الجرائم لها سمات مشتركة، في كون أن السلوك الإجرامي يجب أن يكون مخالفًا للقانون، كما أن الإخلال بأحكام هذا القانون يوقع على مرتكبيه الجزاء الجنائي المناسب.

أما الجريمة الإلكترونيّة فهي إحدى الجرائم المستحدثة، التي عادة ما تتخذ أنماطًا لم يألفها المجتمع، فهي تختلف باختلاف أساليب ارتكابها

وموضوعها واتساع دائرة تأثيرها، وفي نوع الجناة الذين يقومون بارتكابها، مستعينين بالتطورات العلمية الكبيرة في هذا المجال (سقف الحيط، 2015)، الأمر الذي ترتب عليه وضع عدة مصطلحات للدلالة عليها، من أهمها: جرائم الحاسوب أو الإنترنت[1]، وجرائم إساءة استخدام تَقَنِيّة المعلومات، والجرائم المستحدثة جرائم التَقَنِيّة العالمية، والجرائم المعلوماتية، والجرائم الافتراضية، وغيرها الكثير من التسميات.

وحسنًا فعلَ المشرّع الأردني عندما أطلق على هذا النوع من الجرائم تسمية الجرائم الإلكترونيّة، وذلك عندما أطلق على القانون الذي يعتبر الحجر الأساسي في معالجة ومواجهة هذه الجرائم اسم قانون الجرائم الإلكترونيّة[2]، في حين نجد أن هناك بعض التشريعات أطلقت على هذه الجرائم، جرائم تَقَنِيّة المعلومات[3].

ويميل الباحث إلى إطلاق مصطلح "الجريمة الإلكترونيّة" على هذه الجرائم؛ حيث إن هذا المصطلح أكثر شمولًا ويمكن أن يشمل جميعَ التسميات السابقة؛ وذلك للمبرّرات الآتية:

1- أن هذا المصطلح أكثر مرونة، وبالتالي فإنه يمكن أن يستوعب التطورات السريعة في عالم التكنولوجيا وعدم وقوفه عند وسيلة معينة يمكن أن تتطور إلى أشكال ووسائل جديدة في المستقبل مثل الهواتف الذكية[4] وغيرها من التَقَنِيّات المستحدثة.

2- أن مصطلح "الجرائم الإلكترونيّة" نابع من طبيعة هذه الجريمة ومن وسيلة ارتكابها، فهذا النوع من الجرائم يقع باستخدام وسيلة إلكترونيّة، وينصب على معطيات يتم الاعتداء عليها بطريقة إلكترونيّة.

3- أن التسليم بأحد التسميات السابقة مثل جرائم الحاسوب أو جرائم الإنترنت قد يجعل هذا النوع من الجرائم قاصر ومحصور فقط بالجرائم التي يمكن أن ترتكب بواسطة أجهزة الحاسوب دون غيرها، أو بواسطة الإنترنت دون غيره، بالرغم من أن جميع هذه الجرائم يتم ارتكابها من خلال الوسائل الإلكترونيّة.

ولم يتناول المشرّع الأردني تعريفًا للجريمة الإلكترونيّة في قانون الجرائم الإلكترونيّة رقم (27) لسنة 2015، لارتباط هذا النوع من الجرائم بنواتج الاستخدام الخاطئ للوسائل الإلكترونيّة، ذلك أنها ترتبط بالطبيعة الخاصة لتلك الوسائل والعالم الافتراضي التي تتصل به وتحاكيه، تاركًا أمر تحديد التعريف المناسب للفقه والقضاء.

ومن التشريعات التي أخذت على عاتقها تعريف الجرائم الإلكترونيّة التشريع الأمريكي الذي عرّف الجريمة الإلكترونيّة بأنها "الاستخدام غير المصرح به الأنظمة الكمبيوتر المحمية أو ملفات البيانات أو الاستخدام الضار المتعمد لأجهزة الكمبيوتر، أو الملفات وتتراوح خطورة تلك الجريمة بين جنحة من الدرجة الثانية إلى جناية من الدرجة الثالثة"[5]، كما عرّفها المشرّع السعودي بأنها "أي فعل يرتكب متضمنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لإحكام هذا النظام"[6].

وبناء على ما سبق، فقد اختلفت أيضًا التعريفات الفقهية للجريمة الإلكترونيّة؛ فمنهم من أخذ في الاعتبار عند تعريفه لهذا النوع من الجرائم بطبيعة الوسيلة الإلكترونيّة، ومنهم من أخذ بالارتباط بين الجريمة وبين الوسائل الإلكترونيّة، ومنهم من تناول في تعريفه الخاصية التي تربط التجريم بالعالم الافتراضي أو الرقمي.

وفي هذا السياق ذهب البعض إلى تعريف الجريمة الإلكترونيّة بأنها "جريمة تتعلق بالكيانات المعنوية ذات القيمة المادية أو القيمة المعنوية البحتة أو كلاهما معًا، كما أنها تتكون من عناصر أساسية هي عناصر الجريمة والسلوك والوصف الإجرامي والنص القانوني على تجريم السلوك وإيقاع العقوبة، وهي تهدف إلى الحصول على معلومات الأجهزة أو بالأشخاص أو الاعتداء على الأشخاص بواسطة هذه الأجهزة" (حسن، 2015).

كما عرّفها البعض بأنها "سلوك غير مشروع جنائيًا موجه نحو إساءة استعمال النظام الآلي لمعالجة المعلومات باستخدام الحاسب الآلي أو أية وسيلة تَقَنِيّة أخرى" (الصفو، 2014).

وفي الفقه الإنجليزي عرّفها البعض بأنها "الجريمة التي تشمل جميع الأنشطة غير القانونية التي يكون فيها الحاسوب، أو أنظمته، أو شبكة المعلومات، أو البيانات، هي الهدف الأساسي من هذه الجريمة؛ وأيضًا، تلك الأنشطة غير المشروعة أو الجرائم التي ترتكب باستخدام الحاسوب أو بمساعدته، أو باستخدام نظم الحاسوب، أو شبكات المعلومات أو البيانات" (سقف الحيط، 2015).

وممّا سبق يتضح الاختلاف الكبير بين الباحثين والفقهاء في تعريف الجريمة الإلكترونيّة، ومن ثَمَّ يمكن بدورنا أن نعرّف الجريمة الإلكترونيّة بأنها "كل فعل أو امتناع عن فعل باستخدام أدوات التَقَنِيّات ووسائلها الإلكترونيّة، أو تلك التي تقع على هذه الأدوات والوسائل، يشكل اعتداء على مصلحة يحميها القانون أو يهددها بالخطر، ويستلزم توقيع عقوبة جزائية عليه.

الفرع الثاني: خصائص الجرائم الإلكترونيّة.

هناك عدد من السِّمات التي تتصف بها الجرائم الإلكترونيّة وتميّزها عن الجرائم التقليدية؛ وذلك نظرًا إلى ارتباطها على نحوٍ أساسي بوسائل التكنولوجيا المتطورة، وسوف نحاول أن نبرز أهم هذه الخصائص على النحو الآتي:

أولًا: الجريمة الإلكترونيّة جريمة مستحدثة.

تعتبر الجرائم الإلكترونيّة من الجرائم المستحدثة التي لم تظهر إلى حيز الوجود إلا منذ أربعة عقود تقريبًا متزامنة في ذلك مع شيوع استخدام أجهزة الحاسوب وظهور الإنترنت، وذلك على خلاف الجرائم التقليدية التي عرفها الإنسان منذ بدء الخليقة (حسن، 2015) وكانت محلًّا للتطور السريع الذي لم يتوقف عند حد معين، وتزامن معه تطور هائل في وسائط الاتصالات الإلكترونيّة وتكنولوجيا المعلومات (Kipper, 2007)، الأمر الذي أدى إلى ظهور أنماط جديدة للجرائم الإلكترونيّة، وتوالي الظهور المتسارع لأنماط أخرى يشهده العالم في كل يوم، مما يصعب معه في كثير من الأحيان مواجهتها والتعرف على مرتكبيها ومكافحتها بصورة كاملة وبشكل سريع (المعيني، 2011).

ثانيًا: الجريمة الإلكترونيّة جريمة عابرة للحدود.

أدى ظهور شبكات المعلومات (الإنترنت)، والتطور غير المسبوق في الوسائل الإلكترونيّة إلى تلاشي كل الحدود بين الدول، الأمر الذي جعل من العالم قرية صغيرة، يسهل التواصل بين الأفراد والجماعات ليس داخل الدولة الواحدة فقط بل بين الدول والقارات في جميع أنحاء العالم، وهذا ما جعل من الجريمة الإلكترونيّة جريمة عابرة للحدود (عبد الباقي، 2018).

ومما تقدم يرى الباحث ضرورة بذل مزيد من الجهود للتعاون الدولي في مواجهة الجرائم الإلكترونيّة وملاحقة المجرمين الإلكترونيين، وعقد مزيد من الاتفاقيات الثنائية والجماعية في مجال التعاون القانوني والقضائي بين الدول وتسهيل مهان مأموري الضبط القضائي بشأن إجراء الكشف والمعاينة والتفتيش وكذلك تسهيل الإجراءات القضائية وعدم التذرّع بالحدود السياسية في الحد من مواجهة مثل هذه الجرائم، وعقد المؤتمرات الدولية لتبادل الخبرات الدولية في مجال التَقَنِيّات الإلكترونيّة للقضاء على الجرائم الإلكترونيّة[7].

ثالثًا: الجريمة الإلكترونيّة تتيح للجناة محو الأدلة وإعاقة الوصول إليه.

فالبيانات والمعلومات المتداولة على شبكة الإنترنت والوسائل الإلكترونيّة الحديثة تكون مخزنة على وسائط تخزين ممغنطة لا تقرأ إلّا بواسطة أجهزة تَقَنِيّة مخصصة لذلك الغرض، وتوفر برمجيات الحاسوب والاتصالات أيضًا إمكانية تشفير هذه البيانات والمعلومات؛ أي ترجمة البيانات إلى شيفرة سرية، وإخفائها بحيث تبدو وكأنها بيانات بريئة، بعيدا عن الرقابة أو بعيدًا عن سلطة الضبط والتفتيش (العلماء، 2004)، وتسهل هذه البرمجيات على الجناة محو الدليل في زمن قياسي باعتبار أن الجريمة تتم في صورة أوامر تصدر للجهاز الالكتروني، وما يحس الجاني أنه مراقب وأنّ جريمته ستنكشف حتى يبادر بإلغاء هذه الأوامر ومحوها، الأمر الذي يجعل كشف الجريمة وتحديد مرتكبها أمرًا في غاية الصعوبة (ارحومة، 2009).

رابعًا: امتناع المجني عليهم عن التبليغ.

من الملاحظ أن الجرائم الإلكترونيّة لا يتم في الغالب الإبلاغ عنها، أما بسبب الخوف من التشهير أو لعدم اكتشاف الضحية لها أو لعدم ثقته بإمكانية وقدرة الأجهزة الأمنية والقضائية المختصة بالكشف عن هذا النوع من الجرائم ومعاقبة مرتكبيه، خاصة إذا ما كان الاعتداء من مجرم خارج حدود الدولة التي يوجد بها المجني عليه، كما أن معظم الجرائم الإلكترونيّة يتم اكتشافها بالمصادفة وبعد مرور وقت كبير على ارتكابها، إضافة إلى أن الجرائم التي لم تكتشف هي أكبر بكثير من الجرائم الإلكترونيّة التي تم الكشف عنها، وتبدو هذه الظاهرة بشكل أكبر بالنسبة إلى المؤسسات المالية كالبنوك والمؤسسات الادخارية، التي تخشى من التبليغ عن هذه الجرائم حفاظا عل سمعتها التجارية وألا يؤثر ذلك في ثقة المتعاملين معها وانصرافهم بالتالي عنها (المومني، 2008).

خامسًا: الجريمة الإلكترونيّة جريمة الأذكياء.

تتميز الجرائم الإلكترونيّة بأنها لا تتطلب عنفًا أو مجهودًا لتنفيذها، فهي تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية التي تتطلب مجهودًا بدنيًا أكبر لتنفيذها، مثل القتل والسرقة والاغتصاب، أو الكسر والخلع والسطو وغيرها من الجرائم، فالجرائم الإلكترونيّة لا تتطلب سوى علم كافي بالجوانب التَقَنِيّة والفنية للأجهزة الإلكترونيّة، فهي جرائم هادئة بطبيعتها لا تحتاج للعنف (الحمود، 2007)، ولا أثار فيها للعنف أو الدماء وإنما مجرد أرقام وبيانات.

كما أنها تنفذ عن بُعد دون الحاجة إلى التواجد في مسرح الجريمة أو في المكان والزمان الذي يتواجد به المجني عليه، ومن مغرياتها المكاسب المادية الضخمة التي يمكن تحقيقها في وقت قصير، وفي الواقع إن الكثير من المجرمين الإلكترونيين هم من صغار السن والمراهقين، نظرًا إلى أنّ هاتين الفئتين من أكثر الفئات متابعتًا وهوسًا بالوسائل الإلكترونيّة الحديثة، وأكثر الفئات التي تقضي وقتًا طويلًا في استخدامها، الأمر الذي يؤكد عدم حاجة هذا النوع من الجرائم للقوة البدنية في ارتكابها وتحقيق نتائجها (العفيفي، 2013).

المطلب الثاني

أنماط الجرائم الإلكترونيّة التي تهدد أمن المعلومات وطرق الوقاية منها

لا شك في أنّ هناك أنماطًا متعددة للجرائم الإلكترونيّة، وبتتبع الأدبيات التي تطرقت إلى تحديد أنماط وأنواع الجرائم الإلكترونيّة، نجد أن هناك

صعوبة في تحديد معيار معين للتمييز بين أنماط الجرائم الإلكترونيّة، للتغير المستمر في أنماطها، وتطور التَقَنِيّة الحديثة الذي يواكبه تطور في أساليب ارتكابها[8]، وبناء على ذلك نجد بأن التقسيم المناسب لأنماط الجرائم الإلكترونيّة هو التقسيم الذي يقوم على تقسيم الجرائم الإلكترونيّة إلى نمطين رئيسيين يتمثلا في ما يلي: الجرائم الإلكترونيّة التي تستهدف المعلومات والبيانات الإلكترونيّة نفسها، الجرائم الإلكترونيّة التي تقع باستخدام الوسائل الإلكترونيّة.

ولا شك أيضًا في أن أمن المكتبات ومراكز المعلومات تتعرض عادة للتهديدات والهجمات الإلكترونيّة ومشاكل تمس بأمنها وسلامه محتوياتها مثل السرقة والتخريب والعبث كمخاطر الناتجة عن التطورات التَقَنِيّة الحديثة ونظم المعلومات الإلكترونيّة والشبكات، وتزداد الأهمية المعطاة لأنظمة حماية وأمن المعلومات كلما ازداد الاعتماد على أجهزة الحاسوب وشبكاتها في مجال التخزين والاسترجاع.

فأمن المعلومات يعني الطرق والوسائل المعتمدة للسيطرة على جميع أنواع ومصادر المعلومات وحمايتها من السرقة والتشويه والتلف والضياع والتزوير والاستخدام غير المرخص وغير القانوني، أو هي مجموعة الإجراءات والتدابير الوقائية التي تستخدم للمحافظة على المعلومات وسريتها من السرقة أو التلاعب أو الاختراق غير المشروع (العكيلي و زبون، 2017).

كما أن أمن المعلومات مفهوم يشير إلى النظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها، ومن زاوية تَقَنِيّة، يشير إلى الوسائل والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية، ومن زاوية قانونية، فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة، وهذا هو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها (جرائم الكمبيوتر والانترنيت) (خالد، 2017).

الفرع الأول: الجرائم الإلكترونيّة التي تستهدف المعلومات والبيانات الإلكترونيّة.

ويقوم هذا النمط من أنماط الجرائم الإلكترونيّة على فكرة أن تكون الوسائل الإلكترونيّة والإنترنت والبيانات محلًا للجريمة، أي أن يكون هدف المجرم فيها هو البيانات والمعلومات المخزنة والمنقولة عبر قنوات الإنترنت المفتوحة (العامة) أو المغلقة (الخاصة) (الشوابكة، 2011)، ومنها الاعتداء على معلومات المكتبات التي باتت مفتوحة ومتاحة على شبكة الإنترنت، ويخرج الاعتداء على الكيانات المادية للحاسوب وأجهزة الاتصال والوسائل الإلكترونيّة الأخرى من نطاق البحث حسب هذا التصنيف؛ لأن هذه الكيانات محل صالح لتطبيق نصوص التجريم التقليدية المنظمة لجرائم الأموال والتدمير والإتلاف وغير ذلك، أما محل الجريمة الإلكترونيّة هو دائمًا المعطيات، إما بذاتها، أو بما تمثله من قيمة معرفية، وموضوع الجريمة الإلكترونيّة هنا يكون بالاعتداء على هذه المعطيات بسرقتها أو إتلافها أو تغييرها أو الدخول الغير مصرح به أو استغلالها لتنفيذ جريمة (سقف الحيط، 2015).

وهناك العديد من أشكال الجرائم الإلكترونيّة التي تنطوي تحت هذا النوع أو النمط وتتعلق بالأنظمة والمعلومات، من أهمها:

أولا: جريمة الدخول غير المصرح به

ويقصد بها الولوج إلى البيانات والمعلومات والبرامج المخزنة على الأجهزة المتصلة بالشبكة المعلوماتية دون إذن[9]، ويمكن هنا ان تنطبق حالة الدخول إلى البيانات والمعلومات التابعة للمكتبات بشكل غير مصرح به، وتشدد العقوبة إذا كان القصد من ذلك المساس بسرية المحتوى، أو تعطيل قدرة وكفاءة الأنظمة للقيام بإعمالها، أو بهدف إلغاء أو حذف أو إضافة أو تدمير نظام المعلومات، أو تغيير موقع الكتروني أو إلغائه أو إتلافه، وتتطلب هذه الجريمة وجود ركن مادي وركن معنوي، بحيث يتمثل الركن المادي بفعل الدخول إلى مكونات الكمبيوتر بمكوناته المنطقية، أما الركن المعنوي فيتمثل بالقصد الجرمي كون هذه الجريمة من الجرائم العمدية التي تتطلب العلم والإرادة لقيامها (إبراهيم، 2009).

جاء المشرّع الأردني من خلال قانون الجرائم الإلكترونيّة بنصوص تكفل تجريم فعلي الدخول والبقاء غير المصرح به لنظام المعلومات بموجب نص المادة (3) من قانون الجرائم الإلكترونيّة[10]، وهو ما تناوله المشرّع الإماراتي بالتجريم وفق ما جاءت المواد (2، 3) من قانون مكافحة جرائم تَقَنِيّة المعلومات رقم (5) لسنة 2012، ويرى الباحث هنا أنه يمكن الاعتماد على هذه النصوص بشكل قانوني لمواجهة كل فعل يشكل دخول غير مصرح به للبيانات والمعلومات الخاصة بالمكتبات، سواء اقتصر الامر على مجرد الدخول أو بهدف الحاق الضرر بتلك المعلومات.

ثانيًا: جريمة إدخال أو نشر برامج بهدف الإضرار بالغير

وتقوم هذه الصورة من صور الجرائم الإلكترونيّة على قيام المجرم بإدخال أو نشر أو استخدام برامج عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات، بهدف إلحاق الضرر بالغير، إي مهاجمة أو تخريب المعلومات والشبكة المعلوماتية والمواقع الإلكترونيّة، ولا يشترط هنا الدخول إلى نظام الغير فقد يتحقق هذا الجرم باستخدام برامج عن بعد مثل برامج الفيروسات[11] وبرامج الدودة (الشوابكة، 2011)، والقنبلة المعلوماتية (الكبجي، 2013)، لهذه الغاية، ويمثل هذا النوع من الجرائم أكثر الجرائم خطورة على أمن معلومات المكتبات وقد تناول المشرّع الأردني هذه الصورة بالتجريم من خلال النص عليه في المادة (4) من قانون الجرائم الإلكترونيّة[12].

ويرى الباحث أن هذا النص كفيل بحماية أمن معلومات المكتبات من إي مهاجمة أو تخريب للمعلومات والشبكة المعلوماتية والمواقع الإلكترونيّة الخاصة بالمكتبات ومعاقبة المجرم اذا ما توافرت جميع العناصر المطلوبة هنا لقيام هذه الصورة من صور الجرائم الإلكترونيّة التي تشكل اعتداء على أمن معلومات المكتبات.

الفرع الثاني: الجرائم الإلكترونيّة التي تقع باستخدام الوسائل الإلكترونيّة

ويتم تصنيف الجرائم حسب هذا المعيار إلى جرائم واقعة على الأموال، وجرائم واقعة على الأشخاص، والتي سنتناولها بإيجاز على النحو الآتي:

أولًا: جرائم واقعة على الأشخاص عبر الوسائل الإلكترونيّة

لا شك بأن الهدف الأسمى لوضع القوانين وسن التشريعات، حماية سلامة الأشخاص من مختلف الانتهاكات التي يتعرضون لها سواء في أبدانهم أو في حياتهم الخاصة أو في سمعتهم واعتبارهم، وقد أتاحت الثورة الإلكترونيّة للمجرمين تسخير الفضاء الكوني لتحقيق أغلب صور الاعتداء على الأشخاص من جنح بسيطة إلى جنايات كبرى-أما كفاعل اصلي أو كفاعل معنوي- وبأبسط الأساليب والوسائل، من خلال التلاعب ببرمجة البيانات عن بعد وبكبسة زر واحده (الشوابكة، 2011)، ومن أبرز صور الجرائم الإلكترونيّة الواقعة على الأشخاص:

1- جرائم الاعتداء على حرمة الحياة الخاصة عبر الوسائل الإلكترونيّة:

حظيت الحياة الخاصة للإفراد بحماية دستورية وقانونية في مختلف تشريعات الدول المتقدمة[13]، وتتمثل الحياة الخاصة للإفراد بصورتها المستحدثة ببنوك المعلومات والتي يقصد بها مجموعة المعلومات التي يتم معالجتها الكترونيًا، وذلك من أجل بثها عبر شبكة الإنترنت، بحيث يمكن للمشترك الوصول إليها من خلال ربط الوسيلة الإلكترونيّة الخاصة به (حاسوب، هاتف،...الخ) بشبكة الإنترنت، بحيث باتت بنوك المعلومات هذه مهددة بالعديد من الانتهاكات والاعتداءات مثل التلاعب بالمعلومات والبيانات الشخصية، وإفشاء هذه البيانات، أو حذفها أو مسحها أو سرقتها (الشوابكة، 2011)، وكذلك مراقبة الأشخاص أو تسجيل مكالمات صوتية أو فيديو بشكل غير مشروع، وهو ما نص عليه المشرّع الأردني في المادة(5)[14] من قانون الجرائم الإلكترونيّة.

2- جرائم الابتزاز الإلكتروني:

وتتمثل هذه الصورة في استخدام الوسائل الإلكترونيّة في تهديد وابتزاز الغير لحمله على القيام بأفعال أو الامتناع عنه، وجاء القانون الإماراتي رقم (5) لسنة 2012 ليعطي 3حماية اشمل لمستخدمي الإنترنت وذلك بالنص في المادة (16)على الحماية صراحة ضد كل من استعمل الشبكة العنكبوتية أو إحدى وسائل تَقَنِيّة المعلومات في ابتزاز أو تهديد أي شخص، ولم ينص المشرّع الأردني على هذه الصورة من صور الجرائم الإلكترونيّة في قانون الجرائم الإلكترونيّة، بالرغم من خطورتها حيث تعتبر من أكثر الجرائم حدوثًا عبر الوسائل الإلكترونيّة، ويتناول المشرّع الأردني هذه الصورة بالتجريم في المادة (75) من قانون الاتصالات الأردني رقم (13) لسنة 1995[15].

3- الجرائم الجنسية والإخلال بالآداب العامة:

لا شك في أن عالمية نطاق التكنولوجيا وانفتاحها أدى إلى تحولها إلى ساحة مفتوحه لممارسة جميع أنواع الجرائم الممكنة والمحتملة، ومن ضمنها الأعمال المخلة بالآداب العامة والأخلاق، والتي تختلف وتتباين من دولة إلى أخرى، ومن أبرز أشكالها: جرائم نشر المواد الإباحية، وجرائم الاستغلال الجنسي للأطفال، وجريمة إفساد الطفل، وغيرها من الجرائم التي تشكل إخلالًا بالآداب العامة (سقف الحيط، 2015)، وعالج المشرّع الأردني هذا النوع من الجرائم الإلكترونيّة بالعقاب على أي فعل ينطوي على إرسال أو نشر عن طريق نظام المعلومات أو الشبكة المعلوماتية قصدا كل ما هو مسموع أو مقروء أو مرئي يتضمن أعمالًا إباحية وتتعلق بالاستغلال الجنسي والترويج للدعارة بأي وسيلة من الوسائل الإلكترونيّة، وذلك بموجب المادة (9، 10) من قانون الجرائم الإلكترونيّة[16].

ثانيًا: جرائم واقعة على الأموال عبر الوسائل الإلكترونيّة

لم تعد الوسائل الإلكترونيّة مجرد وسيلة لإلحاق الضرر بالغير، ولم تقتصر أساليب إساءة استخدام الثورة التَقَنِيّة على الاعتداء على الأشخاص، بل تجاوزت ذلك لتطال الذمة المالية للغير، الأمر الذي يشكل اعتداء على أموال الغير والتي إحاطتها النصوص القانونية بالحماية، وفي خضم التطورات التَقَنِيّة ابتكر البعض العديد من طرق الاعتداء على أموال الغير، على غرار السطو والسرقة، والتحويل الالكتروني غير المشروع، وقرصنة البطاقات الائتمانية وغيرها الكثير من الصور:

1- الاحتيال الإلكتروني:

والاحتيال[17] هو فعل خداع من المحتال يهدف إلى حمل المجني عليه، على تسليم ماله إلى الجاني، والمجني ما كان ليقبل بهذا التصرف لو عرف بالحقيقة، ويقع الاحتيال الإلكتروني على المنتفعين بخدمات الشبكات المعلوماتية والوسائل الإلكترونيّة الحديثة، للاستيلاء على أموالهم وتبديدها، وهو ما نص عليه المشرّع الإماراتي في المادة (10) من قانون الجرائم الإلكترونيّة بأن " كل من توصل عن طريق الشبكة المعلوماتية، أو إحدى وسائل تَقَنِيّة المعلومات، إلى الاستيلاء لنفسه أو لغيره على مال منقول، أو على سند، أو توقيع هذا السند، وذلك بالاستعانة بطرق احتيالية، أو باتخاذ اسم

كاذب، أو انتحال صفة غير صحيحة، متى كان ذلك من شأنه خداع المجني عليه...إلخ".

2- التحويل غير المشروع للأموال والسطو على بطاقات الائتمان:

فرضت التَقَنِيّات الحديثة على التعامل بالأموال في عصرنا الحالي صفة البيانات الإلكترونيّة المخزنة على الوسائل الإلكترونيّة الحديثة، وأدت الثورة الرقمية إلى إمكانية إجراء تحويلات ومبادلات لهذه الأموال من أي مكان في العالم، وقد تمكن المجرمون الإلكترونيون من التلاعب في هذه البيانات المخزنة في ذاكرة الوسائل الإلكترونيّة وإجراء تحويلات غير مشروعة لأموال الغير وإدخالها في حساباتهم (سقف الحيط، 2015)، والحصول على البيانات والمعلومات المتعلقة بالمستخدمين قد يتم من قبل العاملين على إدخال البيانات أو من قبل المجرمين الإلكترونيين المختصين في مثل هذه العمليات (الشوابكة، 2011).

وتتعدد الوسائل والأساليب المتبعة من قبل العصابات الإلكترونيّة في مجال السطو على بطاقات الائتمان، وقد جرم المشرّع الأردني الجرائم المالية الإلكترونيّة التي تقع على بطاقات الائتمان في المادة (6) من قانون الجرائم الإلكترونيّة رقم (27) لسنة 2015[18].

3- جرائم غسيل الأموال الإلكترونيّة:

من أخطر الجرائم الإلكترونيّة المالية جرائم غسيل الأموال الإلكترونيّة، حيث بدأت عملية غسيل الأموال من تجارة المخدرات والمقامرة والجنس وغيرها من الجرائم الأخرى، ومن المجالات التي يتم من خلالها غسيل الأموال عبر الإنترنت المضاربة على الأسهم في البورصة، والمجالات في هذا الشأن لا حصر لها (يوسف، 2011).

الفرع الثاني: طرق الوقاية من المخاطر التي تتعرض لها أمن المعلومات الإلكترونيّة

تتعرض المعلومات والبيانات في المكتبات اليوم للعديد من المخاطر التي تهدد أمنها، سواء كانت مخاطر أمنية مادية كالحريق والسرقة او مخاطر إلكترونيّة يفرضها التطور التكنولوجي والالكتروني غير المسبوق في مجال الاتصالات، والتي باتت المكتبات جزء لا يتجزأ منه، ولقد تناولنا سابقًا النصوص القانونية الواردة في قانون الجرائم الإلكترونيّة والتي يمكن الاعتماد عليها في حماية أمن معلومات المكتبات، لكن نعرض هنا اهم طرق الوقاية الفنية التي يمكن اتباعها في سبيل تجنب المخاطر التي قد تصيب المكتبات وبنيتها المعلوماتية وتعرضها للخراب والتدمير او السرقة او السيطرة عليها بالوسائل الإلكترونيّة الحديثة.

أولًا: الوقاية من الاختراق

يعتبر الهجوم على المواقع واختراقها على شبكة الانترنيت من الجرائم الشائعة في العالم (الجنبيهى و الجنبيهى، 2006)، ولكي تتم عملية الاختراق لا بد من برنامج يتم تصميمه للمخترق الذي يريد اختراق الحاسب الآلي لشخص آخر أو اختراق الكتروني على شبكة الانترنيت أو اختراق البريد الالكتروني الخاص بشخص ما ان يتم ذلك الاختراق. وقد صُمّم العديد من تلك البرامج التي تتيح عملية الاختراق وتجعلها سهله، وتصنف الاختراق إلى ثلاث أنواع اختراق الأجهزة اما النوع الثاني اختراق المواقع اما النوع الثالث اختراق البريد، ومصدر التهديد الاختراق هو الهاكرز عبر شبكة الانترنيت وضرره التحكم التام بجهاز الضحية مع احتمالية سرقة المعلومات وجمع كلمات العبور أو تدمير الملفات المهمّة، ومن طرق الوقاية لهذا التهديد استخدام جدران اللهيب مع تعطيل خاصية المشاركة في الملفات والطباعة واستخدام كلمات عبور ذكية.

ثانيًا: الوقاية من الفيروسات: أي برنامج، أو مجموعة من التعليمات، التي تلحق ضررا بنظام المعلومات أو البيانات، على أن تكون لدية القدرة على التضاعف والانتشار (داود، 2004).

إن الفيروس -كما سبقت الإشارة إليه- هو أجزاء من برامج ذات أهداف شريرة يتم إلحاقها ببرامج أخرى وتنتشر عند تنفيذ البرنامج الملوث والبرامج ذات أهداف الشريرة يعني بها وأي برامج تضاف او تحذف او تعدل في احد نظم المعلومات بهدف إلحاق الأذى بالنظام أو تعديل مهمّه (McGraw and Morriset, 2000)نستنتج أن الفيروس برنامج له خواص التضاعف، التخفي، إلحاق الأذى، وان مصدره البريد الالكتروني والبرامج المجانية فان الضرر تدمير أو تحريف الملفات والمعلومات في الجهاز مع إمكانية نقل العدوى إلى كل من تراسلهم أو تتعامل معهم الكترونيا وان سبيل الحماية وطرق الوقاية منها هو استخدام البرامج المضادة للفيروسات بشكل متواصل وعدم فتح الملحقات المشبوهة ذات الطبيعة التنفيذية في الرسائل الإلكترونيّة وتجنب تنزيل البرامج المجانية مجهولة المصدر (السريحي، 2001).

ثالثًا: الوقاية من حصان طروادة: هو أحد أساليب الهجوم الخطيرة التي تشبه الفيروسات والتي تختفي مفاجأة شريرة تظهر في وقت معين، وهو يختلف عن الفيروس في انه لا يتكأثر ولا يلتصق بالملفات وإنما هو برنامج مستقل بذاته ويحمل بين طياته توقيت وأسلوب استيقاظه وبدئه النشاط. مصدره من البريد الالكتروني والمواقع المشبوهة التي تستخدم جافا سكريبت وجافا ابليتس واكتف إكس وضرره هو التجسس على كلمات العبور وتدمير الملفات وان سبل الحماية وطرق الوقاية هو تعطيل خاصية قبول وتشغيل البرامج في المتصفح مثل الجافا والأكتف إكس والجافا أبليتس واستخدام برامج الحماية من الفيروسات وجدران اللهب وتجنب تنزيل البرامج المجانية مجهولة المصدر.

رابعًا: الوقاية من الهجوم على المواقع وتعطيلها: مصدرها الهاكرز (المخترقون) وضررها سرقة خدمة وتعديل المعلومات وتعطيل المواقع

باستخدام جهازك دون علمك وان سبل الحماية وطرق الوقاية وضع كلمات العبور واستخدام جدران اللهب وحماية الخادم ببرامج الكشف عن الحركة من وإلى الأجهزة الخادمة (السريحي، 2001).

خامسًا: الوقاية من التجسس على البريد الالكتروني[19]:

ومصدره الهاكرز ومن يشاركونك الجهاز فعليًّا وأن ضرره هو الاطلاع على الرسائل فعليا من جهازك او اعتراض الرسالة أثناء الإرسال او الكتابة وإرسال الرسائل باسمك وان سبل الحماية وطرق الوقاية استخدام كلمات عبور ذكية مع تجنّب استخدام خاصية إكمال وحفظ اسم المستخدم وكلمات العبور وتشفير الرسائل مع الخروج الصحيح من البرنامج أثناء ابتعادك عن الجهاز.

وكذلك التجسس على البريد الالكتروني، ومصدره من مرسلي أحصنة طروادة ومن يستطيعون الوصول إلى جهازك في المكتب او المنزل فان ضرره يقع على تسجيل كل حرف ورقم تدخله عن طريق لوحة المفاتيح والاطلاع عليه لاحقا وان سبيل الحماية وطرق الوقاية هو استخدام برنامج مضاد للفيروسات ووضع كلمات العبور في جهازك لتقييد استخدام اي شخص اخر لجهازك

الخاتمة

بعد الانتهاء من البحث في مسألة على قدر كبير من الأهمية في مجال القانون الجنائي، دور التشريع الأردني في مواجهة الجرائم الإلكترونيّة وأثرها في أمن المعلومات المكتبات، والتي تناولت إبراز الأسس والركائز التي تقوم عليها هذا النوع من الجرائم، فانصبت هذه الدراسة بالتركيز على الوسائل الإلكترونيّة التي أفرزتها الثورة التكنولوجية والتي باتت تستخدم في ارتكاب هذا النوع من الجرائم، حيث تناولت الدراسة بيان لأهم هذه الوسائل واهم المخاطر التي خلتها الثورة التكنولوجية والتي باتت تهدد أمن المعلومات في المكتبات، ومن ثم البحث في مدى كفاية التشريعات الأردنية في مواجهة الجرائم الإلكترونيّة التي تهدد أمن المعلومات في المكتبات، وأهم طرق الوقاية منها.

وتبعًا لذلك تم تقسيم هذه الدراسة إلى مطلبين تطرق الباحث في كل منها إلى أحد تلك المجالات بالدراسة والتحليل، ونستطيع القول إننا قد توصلنا إلى النتائج والتوصيات الآتية:

أولًا: النتائج:

1- تعتبر جرائم الاعتداء الإلكتروني على أمن المعلومات في المكتبات من بين أكثر الجرائم الإلكترونيّة شيوعًا، والتي أخذت طابعًا خاصًا وارتبطت ارتباطًا وثيقًا بالتطور الهائل في مجال الوسائل الإلكترونيّة الذي يشهده العالم في وقتنا الحاضر.

2- حسنًا فعل المشرّع الأردني عندما أطلق على هذا النوع من الجرائم تسمية الجرائم الإلكترونيّة، وذلك عندما أطلق على القانون الذي يعتبر الحجر الأساسي في معالجة ومواجهة هذه الجرائم اسم قانون الجرائم الإلكترونيّة.

3- تتعرض المعلومات والبيانات في المكتبات إلى مخاطر حقيقية أفرزتها الثورة التكنولوجية وهي بحاجة إلى وسائل حماية تَقَنِيّة وقانونية في آنٍ لمواجهة مخاطرها.

ثانيًا: التوصيات.

1- نتمنى على المشرّع الأردني إضافة إلى الحماية المقررة في نصوص قانون الجرائم الإلكترونيّة والتي يمكن الاستفادة منها في تحقيق الحماية المطلوبة لأمن المكتبات، خاصّةً المواد (3، 4) من قانون الجرائم الإلكترونيّة، أن يستحدث نصوص خاصة بحماية المكتبات ومعلوماتها.

2- يوصي الباحث المشرّع بتشديد العقوبة المقررة للاعتداء على البيانات والمعلومات الخاصة بالمكتبات ومعاملتها معاملة البيانات والمعلومات التي تتعلق بالمعاملات المالية او المصرفية واالتي شدد المشرّع العقاب بالاعتداء عليها نظرا لأهميتها بإضافة عبارة «أو التي تشكل اعتداءً على أمن المكتبات» بعد عبارة «او بالمعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونيّة المادة (6) من قانون الجرائم الإلكترونيّة.

3- يوصي الباحث بضرورة وجود تعاون دولي في مكافحة الجرائم الإلكترونيّة عن طريق عقد المؤتمرات وتبادل الخبرات وعقد الاتفاقيات التي من شأنها إتاحة تعاون دولي فاعل لمواجهة هذا النوع من الجرائم المستحدثة التي لم تعد تقف عند حدود معينة.

الهوامش

1() هناك من يفرق بين جرائم الحاسوب والإنترنت، على أساس أن جريمة الحاسوب تقع بواسطة الحاسب الآلي أو على مكوناته المادية والمعنوية، أما جرائم الإنترنت فهي تلك الجرائم العابرة للحدود والتي ترتكب بواسطة الإنترنت أو عليها من شخص ذا دراية فائقة، بالرغم من أن بعض جرائم الإنترنت لم تعد بحاجة إلى دراية فائقة لارتكابها، بل صارت في بعضها لا تحتاج إلى معرفة أساسيات استخدام الحاسوب، كقيام شخص بسرقة كلمة المرور والدخول

لحساب بنكي، وتحويل الأموال إلى حسابه، أو ارتكاب جرائم الذم والقدح والتحقير من خلال المواقع الإلكترونيّة، وهو موضوع دراستنا هنا. انظر: هروال، نبيلة هبه (2006)، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، ص 54.

2() انظر: قانون الجرائم الإلكترونيّة الأردني رقم (27) لسنة 2015، المنشور في الجريدة الرسمية رقم (5343)، الصادر بتاريخ 2015/6/1، منشورات مركز قسطاس.

3() انظر: قانون جرائم تَقَنِيّة المعلومات الاتحادي رقم (5) لسنة 2012، منشور على موقع وزارة العدل لدولة الإمارات العربية المتحدة على الرابط:/http://www.elaws.gov.ae

4() الهواتف الذكية (Smart Phones)، وهي إحدى الوسائل التكنولوجية الحديثة التي تقوم بعدة وظائف منها مشغل ملفات وسائط متعددة من خلال تطبيق أي بود، وهاتف خلوي من خلال تطبيق الهاتف، وكاميرا الرقمية من خلال تطبيق الكاميرا، والإنترنت اللوحي من خلال تطبيق متصفح الإنترنت، للمزيد من المعلومات انظر: موقع ويكيبيديا الموسوعة الحرة.

5() انظر: القانون الأمريكي رقم 1213 لسنة 1996 الخاص بمواجهة جرائم الكمبيوتر، مشار إليه في كتاب رامي متولي القاضي (2011)، مكافحة الجرائم المعلوماتية، ط1، دار النهضة العربية: القاهرة، ص23.

(6) انظر: الماد (1/8) من نظام مكافحة الجرائم المعلوماتية السعودي رقم (17) لسنة 1428هـ، مشار إليه في الموقع الرسمي لمجلس الوزراء السعودي على الرابط التالي: http://www.boe.gov.sa/

(7) لا بد من الإشارة هنا إلى قانون الإمارات العربي الإسترشادي لمكافحة جرائم تَقَنِيّة المعلومات، حيث تم اعتماد مجلس وزراء العدل العرب في دورته التاسعة عشرة بالقرار 495-د بتاريخ 2003/10/8، ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم 417-د، تاريخ 21/2004،

8() عبابنة، محمود أحمد (2005)، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان: الأردن، ص 47.

(9) عرف قانون الجرائم الإلكترونيّة الأردني التصريح بأنه: الإذن الممنوح من صاحب العلاقة إلى شخص أو أكثر أو للجمهور للدخول إلى أو استخدام نظام المعلومات أو الشبكة المعلوماتية بقصد الاطلاع أو إلغاء أو حذف أو إضافة أو تغيير أو إعادة نشر بيانات أو معلومات أو حجب الوصول إليها أو إيقاف عمل الأجهزة أو تغيير موقع الكتروني أو إلغائه أو تعديل محتوياته.

10() انظر: المادة (3) من قانون الجرائم الإلكترونيّة الأردني رقم (27) لسنة 2015.

11() والفيروس برنامج يصممه الجاني، يتمثل في مجموعة من التعليمات التي تتكاثر بشكل سريع، يهدف إلى الوصول البرامج والنظام ألمعلوماتي للغير، وتعمل على إتلافها أو تدميرها، ومن الأمثلة عليها فايروس طروادة، فايروس ميليسيا، فايروس الحب، انظر: زين الدين، بلال أمين (2008)، جرائم نظم المعالجة الآلية للبيانات، دار الفكر الجامعي، الإسكندرية، ص 372.

(12) انظر: المادة (4) من قانون الجرائم الإلكترونيّة الأردني رقم (27) لسنة 2015.

(13) كفل الدستور الأردني الحقوق والحريات الفردية في الفصل الثاني من الدستور والتي تشمل الحقوق الطبيعية اللصيقة بشخص الإنسان أو تلك المتعلقة بالحقوق والحريات الفكرية، وكذلك ما يتعلق بالحقوق والحريات الاقتصادية، وجاءت المادة (18) منه لتكفل حرمة المراسلات البريدية والبرقية إذ اعتبرت جميع هذه المراسلات سرية

14() تنص المادة (5) من قانون الجرائم الإلكترونيّة الأردني رقم (27) لسنة 2015 على انه" يعاقب كل من قام قصدًا بالتقاط أو باعتراض أو بالتنصت أو أعاق أو حور أو شطب محتويات على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار".

(15) وضع المشرّع الأردني بموجب قانون الجرائم الإلكترونيّة رقم (27) لسنة 2015 نصًا عامًا يمكن اعتباره المرجعية القانونية لتجريم كل فعل يعد جريمة بموجب التشريعات الأخرى والذي يتم ارتكابه باستخدام الشبكة المعلوماتية او أي نظام معلومات، انظر: نص المادة (15) من هذا القانون.

16()انظر: نص المادة (9) من قانون الجرائم الإلكترونيّة، نص المادة (10) من ذات.

(17) نصت المادة (417) من قانون العقوبات الأردني على معاقبة من يستولي على مال غيره، المنقول أو غير المنقول أو على إسناد لغيره تتضمن تعهدًا أو إبراءً، باستعمال طرق احتيالية من شأنها إيهمّ المجني عليه بوجود أمر لا حقيقة له، بادعاء صفة كاذبة والتصرف بالمال.

(18) انظر نص المادة (6) من قانون الجرائم الإلكترونيّة رقم (27) لسنة 2015.

(19) راجع الموقع الإلكتروني Safola.com/summary.chtml//http.

المصادروالمراجع

العدوان، م.، و السلامات، ن. (2018). مشروعية وحجية الدليل المستخلص من التفتيش الالكتروني في التشريع الجزائي الأردني، *دراسات: علوم الشريعة والقانون*، 45(2).

ارحومة، م. (2009). الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، *المؤتمر ألمغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس*.

الصفو، ن. (2014). *دراسات في القانون الجنائي المقارن- جريمة الإخلال بالآداب العامة بواسطة وسائل تَقَنِيّة المعلومات*. الإسكندرية: دار الجامعة الجديدة.

المعيني، س. (2011). التحقيق في جرائم تَقَنِيّة المعلومات، *دورية الفكر الشرطي، الشارقة*، 4.

العلماء، م. (2004). جرائم الإنترنت والاحتساب عليها، *مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة - كلية الشريعة والقانون*.
الحمود، ع. (2007). عولمة الجريمة الاقتصادية، *جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية*.
الشوابكة، م. (2011). *جرائم الحاسوب والإنترنت- الجريمة المعلوماتية*. عمان، الأردن: دار الثقافة للنشر والتوزيع.
الكبجي، ب. (2013). مدى توافق أحكام جرائم أنظمة المعلومات في القانون الأردني مع الأحكام العامة للجريمة، *رسالة ماجستير، جامعة الشرق الأوسط، عمان*.
العكيلي، ه.، و زبون، ب. (2017). أمن المعلومات وتطبيقاته في اقسام علم المعلومات والمكتبات، *المجلة الأردنية للمكتبات والمعلومات*، 52(1).
المومني، ن. (2008). *الجرائم المعلوماتية*. (ط1). الأردن: دار الثقافة للنشر والتوزيع.
العفيفي، ي. (2013)، الجرائم الإلكترونيّة في التشريع الفلسطيني "دراسة تحليلية مقارنة"، *رسالة ماجستير، الجامعة الإسلامية، غزة، فلسطين*.
حسني، م. (1989). *شرح قانون العقوبات-القسم العام*. القاهرة، مصر: دار النهضة العربية.
داود، ح. (2004). *أمن الشبكات المعلومات*. (ط1). الرياض: الادارة العامة للطباعة والنشر.
السريحي، ح. (2001). النشر الالكتروني: دراسة لأهم القضايا ذات العلاقة بعلم المكتبات والمعلومات، *الاتجاهات الحديثة في المكتبات والمعلومات*، 17.
حسن، ع. (2015). سياسة المشرّع الإماراتي لمواجهة الجرائم الإلكترونيّة، *الفكر الشرطي، الشارقة، الإمارات*، 24(95).
إبراهيم، خ. (2009). *الجرائم المعلوماتية*. (ط1). الإسكندرية: دار الفكر الجامعي.
سقف الحيط، ع. (2015). *جرائم الذم والقدح والتحقير المرتبة عبر الوسائط الإلكترونيّة "دراسة مقارنة"*. (ط2). عمان: دار الثقافة للنشر والتوزيع.
عبد الباقي، م. (2018). التحقيق في الجريمة الإلكترونيّة واثباتها في فلسطين" دراسة مقارنة"، *دراسات: علوم الشريعة والقانون*، 45(4).
خالد، ف. (2017). سياسة أمن المعلومات في المكتبات ومراكز المعلومات، *مجلة الأردنية للمكتبات والمعلومات*، 52(4).
الجنبيهى، م.، و الجنبيهى، م. (2006). *أمن المعلومات الالكتروني*. مصر: دار الفكر الجامعي.
نجم، ص. (2000). *شرح قانون العقوبات(القسم العام-النظرية العامة للجريمة)*. (ط4). عمان، الأردن: دار الثقافة للنشر والتوزيع.
يوسف، ح. (2011). *جريمة غسل الأموال عبر شبكات الإنترنت وبنوك الويب*. (ط1). القاهرة: المركز القومي للإصدارات القانونية.
قانون العقوبات الأردني رقم(16) لسنة 1961.
قانون أصول المحاكمات الجزائية الأردني رقم(9) لسنة 1961.
قانون الاتصالات الأردني رقم(13) لسنة 1995 وتعديلاته.
قانون المطبوعات والنشر وتعديلاته رقم(8) لسنة 1998.
قانون العقوبات المصري رقم(58) لسنة 1937.
قانون الجرائم الإلكترونيّة الأردني رقم(27) لسنة 2015.
قانون الإمارات العربي الاسترشادي لمكافحة جرائم تَقَنِيّة المعلومات.
موقع وزارة العدل لدولة الإمارات العربية المتحدة على الرابط http://www.elaws.gov.ae .

References:

Al Adwan, M., & Alsalamat, N. (2016). The legality and authenticity of the evidence extracted from the electronic inspection in the Jordanian penal legislation. *Dirasat: Shari'a and Law Sciences*, *45*(4). Retrieved from https://archives.ju.edu.jo/index.php/law/article/view/13887

Abdelbaqi, M. (2016). Investigating and proving cybercrime in Palestine: a comparative study. *Dirasat: Shari'a and Law Sciences*, *45*(4). Retrieved from https://archives.ju.edu.jo/index.php/law/article/view/14120

McGraw, G., and Morriset, G. (2000). Attacking malicious code, *a report to the infosec research council submitted IEEE software and presen-ted to the IRC, USA.*

Arhumah, M. (2009). Procedural problems raised by transnational cybercrime, *first Maghreb conference on informatics and Law, Academy of higher studies, Tripoli*.

Al-Safo, N. (2014). *Studies in comparative criminal law - the crime of disturbing public morals by means of Information Technology*. Alexandria: new university House.

Almaini, S. (2011). Investigation of Information Technology crimes, *police thought journal, Sharjah*, 4.

Alolama', M. (2004). Cybercrime and accounting, law, *computer and Internet Conference, United Arab Emirates University-Faculty of Sharia and law*.

Al-Hamoud, P. (2007). Globalization of economic crime, *Naif Arab University for Security Sciences, Riyadh, Saudi Arabia*.

Al-shawabkeh, M. (2011). *Computer and Internet Crime-Information crime*. Amman, Jordan: House of culture for publishing and distribution.

Al-kabji, B. (2013). Compliance of the provisions of Information Systems crimes in Jordanian law with the general provisions of the crime, *master thesis, Middle East University, Amman*.

Al-Akili, H., and Zubon, B. (2017). Information security and its applications in the Departments of Information Science and libraries, *Jordanian Journal of libraries and information*, 52(1).

Momani, N. (2008). *Information crimes*. (1st ed.). Jordan: House of culture for publishing and distribution.

Al-Afifi, J. (2013). Cybercrime in Palestinian legislation "comparative analytical study", *master thesis, Islamic University, Gaza, Palestine*.

Hosni, M. (1989). *Explanation of the Penal Code-General section*. Cairo, Egypt: Arab renaissance House.

David, H. (2004). *Information network security*. (1st ed.). Riyadh: General Directorate of printing and publishing.

Serihi, H. (2001). Electronic publishing: a study of the most important issues related to library and information science, *recent trends in libraries and Information*, 17.

Hassan, A. (2015). UAE legislator's policy to counter cybercrime, *police thought, Sharjah, UAE*, 24(95).

Ibrahim, K. (2009). *Information crimes*. (1st ed.). Alexandria: University think tank.

Saqf Alhaet, P. (2015). *Crimes of slander, slander and contempt arranged through electronic media "comparative study"*. (2nd ed.). Amman: House of culture for publishing and distribution.

Khalid, F. (2017). Information security policy in libraries and information centers, *Jordanian Journal of libraries and information*, 52(4).

Elginbehy, M. and Elginbehy, M. (2006). *Electronic information security*. Egypt: Dar Alfikr.

Najam, P. (2000). *Explanation of the Penal Code (General section-general theory of crime).* (4th ed.). Amman, Jordan: House of culture for publishing and distribution.

Yousuf, H. (2011). *The crime of honey money over internet networks and web banks*. (1st ed.). Cairo: National Center for legal publications.

The Jordanian Penal Code No. 16 of 1961.

Jordanian code of Criminal Procedure No. 9 of 1961.

Jordanian Telecommunications Law No. 13 of 1995, as amended.

The publications and Publications Law, as amended No. 8 of 1998.

Egyptian Penal Code No. 58 of 1937.

Jordanian Cybercrime Law No. 27 of 2015.

UAE guiding law to Combat Information Technology Crimes.

Website of the Ministry of Justice of the United Arab Emirates, http://www.elaws.gov.ae .