جـــامـعـــة الـــشـرق الأوسـط
MIDDLE EAST UNIVERSITY
Amman - Jordan

جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية في التشريع الأردني

The Crime of Violating the Confidentiality of Information through Electronic Means in the Jordanian Legislation

إعداد

سلطان فياض محمد السكر

إشراف

الأستاذ الدكتور أحمد محمد اللوزي

قدمت هذه الرسالة استكمالاً لمتطلبات الحصول على درجة الماجستير في القانون العام

قسم القانون العام

كلية الحقوق

جامعة الشرق الأوسط

كانون الثاني، 2022

تفويض

أنا **سلطان فياض محمد السكر**، أفوّض جامعة الشّرق الأوسط بتزويد نسخ من رسالتي الموسومة للمكتبات الجامعيّة أو المؤسسات أو الهيئات أو الأشخاص المعنيين بالأبحاث والدّراسات العلميّة عند طلبها.

الاسم: سلطان فياض محمد السكر.

التاريخ: 11 / 01 / 2022.

التوقيع:

قرار لجنة المناقشة

نوقشت هذه الرّسالة وعنوانها: **جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية في التشريع الأردني.**

للباحث: سلطان فياض محمد السكر.

وأجيزت بتاريخ: 11 / 01 / 2022.

أعضاء لجنة المناقشة:

الاسم	الصفة	جهة العمل	التوقيع
أ. د. أحمد محمد اللوزي	مشرفًا	جامعة الشرق الأوسط	
د. محمد علي الشباطات	عضوًا من داخل الجامعة ورئيسًا	جامعة الشرق الأوسط	
د. أيمن يوسف الرفوع	عضوًا من داخل الجامعة	جامعة الشرق الأوسط	
د. محمد شبلي عبدالمجيد	عضوًا من خارج الجامعة	جامعة جدارا	

شكر وتقدير

قال تعالى: ﴿ ... وَمَن يَشۡكُرۡ فَإِنَّمَا يَشۡكُرُ لِنَفۡسِهِۦۖ وَمَن كَفَرَ فَإِنَّ ٱللَّهَ غَنِيٌّ حَمِيدٞ ١٢﴾ [سورة لقمان,١٢]

الحمد الوفير والشكر الكثير لله وليّ التوفيق

بداية أتقدّم بجزيل الشكر وعظيم العرفان إلى أستاذي المشرف **الأستاذ الدكتور أحمد محمد اللوزي**، لتفضله الكريم بالإشراف على هذه الرسالة، وتكرمه بنصحي وإرشادي طيلة فترة إعداد هذه الرسالة لتخرج بالصورة المثلى.

كما أتقدم بوافر الامتنان العظيم والتقدير العميق إلى السادة **أعضاء لجنة المناقشة**، الذين شرفوني بقبول مناقشة الرسالة، ولإبداء الملاحظات المفيدة.

وأتقدم بالشكر الوفير إلى **جامعة الشرق الأوسط** ممثلة بالكادر التدريسي والإداري لما يقدّموه من جهود في سبيل تيسير العملية التعليمية.

والشكر الجزيل لكل شخصٍ ساعدني أو قدّم لي النصح في سبيل إتمام هذه الرسالة.

الباحث

سلطان فياض محمد السكر

الإهداء

إلى والدتي الحبيبة أطال الله بعمرها، تلك السيدة الحنونة التي قدّمت سعادتي وسعادة إخوتي وراحتنا على سعادتها وراحتها.

إلى من شرفني بحمل اسمه والدي فياض السكر أطال الله بعمره، من بذل الغالي والنفيس في سبيل وصولي لدرجة علمية عالية.

إلى زوجتي من جعلها عزَّ وجلَّ سكناً لي، رفيقة الكفاح والظروف الصعبة، إلى زوجتي الحبيبة، شريكة الحياة ورفيقة الدرب.

إلى أخواتي الخمسة، الغاليات على قلبي.

إلى العضيد أخي يوسف، رعاك الله يا صغيري وألبسك ثوب الصحة والعافية.

الباحث

فهرس المحتويات

الموضوع **الصفحة**

الفصل الأول: خلفية الدراسة وأهميتها

الفصل الثاني: الاطار المفاهيمي لجريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية

الفصل الخامس: الخاتمة، النتائج والتوصيات

جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية في التشريع الأردني

إعداد:

سلطان فياض محمد السكر

إشراف:

الأستاذ الدكتور أحمد محمد اللوزي

الملخّص

إن ظاهرة التطور التكنولوجي الذي يشهده عالمنا اليوم رتبت آثاراً إيجابية يمكن ملاحظتها في عدة قطاعات، كالقطاع الحكومي، والقطاع المصرفي، والصحي، والقطاع الخاص المتمثل بالمؤسسات الكبيرة منها والصغيرة وغيرها، ومن تلك الآثار هو اعتماد تلك القطاعات في تسيير أعمالها على الطرق والوسائل التكنولوجية بدلاً من التقليدية، وتبادل المعلومات السرية عبر أنظمة المعلومات أو عبر شبكة الإنترنت، إلا أن هذا التطور لم يَسلم من فكرة تطويعه ليكون وسيلة لتنفيذ أفعال إجرامية، فقد ظهرت في الآونة الأخيرة صوراً متعددة للجرائم الإلكترونية وبأنماط مختلفة.

كما أن ظهور الجرائم الإلكترونية على الساحة الإجرامية أوجد الضرورة الملحة لوجود تشريع يعالج هذه الجرائم بنصوص قانونية واضحة من خلال بيان أركانها وأنماطها، ومكافحتها من خلال فرض العقاب على مرتكبيها، وبالرجوع للتشريع الأردني نلاحظ أنه لم يقم بمعالجة هذا الموضوع حتى عام 2010 وكان ذلك بقانون جرائم أنظمة المعلومات المؤقت رقم 30 لسنة 2010، ومن ثم تطوّر هذا الموقف ليتجسد بقانون الجرائم الإلكترونية رقم 27 لسنة 2015.

وقد عالجت هذه الدراسة صورة من أبرز صور الجرائم الإلكترونية ألا وهي جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية في التشريع الأردني، وذلك لأنه لطالما سعت التشريعات الجزائية الأردنية نحو توفير الحماية الجزائية للأسرار، وذلك من خلال تجريم إفشاء الأسرار المهنية والتجسس وحماية حرمة الحياة الخاصة، دون التطرق للأسرار بمفهومها الحديث (الالكتروني) بشكل كافٍ.

وقد خلصت الدراسة إلى عدة نتائج، أهمها أن النصوص التي عالجت أفعال الانتهاك الالكتروني لسرية المعلومات هي نصوص عامة، وليست خاصة بتلك الأفعال، فنجد أن ذات النص قد ينطبق على أكثر من جريمة، مما قد يخالف مبدأ الشرعية الجزائية، وأن عملية ضبط وملاحقة واثبات جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية، تتسم بالصعوبة بعض الشيء كونها من الجرائم التي تنطوي على الجانب التقني أكثر من المادي، ولذلك يعتمد في اكتشافها على الدراية العالية بالأمور التقنية من قبل أصحاب الاختصاص في ملاحقتها.

وبذات الوقت أوصت هذه الدراسة بضرورة العمل على تعديل قانون الجرائم الإلكترونية رقم 27 لسنة 2015، وذلك من خلال ايراد نصوص واضحة لمعالجة جريمة انتهاك سرية المعلومات بصورها المتعددة، وتوحيد النصوص التي تجرّم أفعال جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية ضمن تشريع موحد.

الكلمات المفتاحية: انتهاك سرية المعلومات، الوسائل الإلكترونية، التشريع الأردني.

The Crime of Violating the Information Confidentiality through Electronic Means in Jordanian Legislation

Prepared by Sultan Fayyad Mohammad Al -Sukkar

Supervised by Prof. Dr. Ahmad Mohammad Al -Louzi

Abstract

The phenomenon of technological development these days has a positive influence which could be observed in several sectors, such as the governmental sector, Banking sector, health sector, and the private sector represented by small and large institutions and others. Which are using technological means in their business instead of traditional ones, and exchanging the confidential information through information systems or over the Internet. However, this development has been used sometimes to carry out criminal acts. Recently, multiple forms of cyber - crimes have appeared with different patterns.

The emergence of electronic crimes shows the urgent need for necessary legislation for dealing with these crimes with clear legal texts with their pillars and patterns, and combating these crimes by imposing punishment on their perpetrators. When reviewing the Jordan Legislation in this regard we found he did not address this issue until 2010, with information systems a temporary crimes law No.30 of 2010, and then this situation developed to the Cyber-crime Law No. 27 of 2015.

This study dealt with one of the most prominent forms of electronic crimes, which is the crime of violating the confidentiality of information through electronic means in the Jordanian legislation, because the Jordanian penal legislation sought to provide penal protection for confidential matters, by criminalizing the disclosure of these confidential matters ,espionage and protecting the private life. Without adequately addressing the secrets in their modern (electronic) sense

The study concluded the followings, the most important of them is that the texts dealing with acts of electronic breach of confidentiality of information are general texts, not specific to those acts but the same text is used for different types of crimes which may violates the principle of penal legislation .noting that Proving, controlling and follow up of the crime that violating the confidentiality of information through electronic means is somewhat difficult, as the technical side is involved more than the materialistic side , and

therefore its discovery depends on the high knowledge of technical matters by the specialists in prosecuting them.

Therefore, this study recommended the need of amendment of the Cyber-crime Law No. 27 for the year 2015, by including clear texts dealing with the crime of violating the confidentiality of information in all its forms, and unifying the texts of criminalizing the acts of violating the confidentiality of information through electronic means in unified legislation.

Keywords: Violation of Confidentiality of Information, Electronic Means, Jordanian Legislation.

الفصل الأول
خلفية الدراسة وأهميتها

أولاً: المقدمة

شهد القرن العشرين تقدماً واضحاً في وسائل الإتصال، وشكلت الشبكة المعلوماتية الدولية (الإنترنت) أعجوبة القرن التي امتدت عبر كامل أنحاء بقاع العالم وربطت بين شعوبه، وأصبحت وسيلة التعامل اليومي بين الأفراد، حيث أطلق على القرن العشرين بقرن الثورة المعلوماتية، وهذا إشارة إلى الدور البارز التي تلعبه المعلومات في الوقت الراهن، فقد أصبحت قوة لا يستهان بها في أيدي الدولة والأفراد، وكان التطور الهائل الذي شهده قطاعي تكنولوجيا المعلومات والاتصال والاندماج المذهل الذي حدث بينهما فيما بعد المحور الأساسي الذي قامت عليه هذه الثورة. [1]

"إن تبادل البيانات والمعلومات بواسطة الإنترنت، وضعف وسائل الرقابة على هذه العملية، جعل من ارتكاب الجرائم باستخدامها أو عبرها أمراً غاية بالسهولة؛ نظراً لإتساعها وسهولة إخفاء أدلة ارتكابها، وشعور المستخدم بعدم وجود رقابة حقيقية على ما يقوم به من أفعال، كما أن هناك قدرات لدى بعض المجرمين المعلوماتيين على إخفاء جرائمهم أو ما يترتب عليها من آثار، زاد من إحتمالية ارتكاب الجرائم باستخدام تكنولوجيا المعلومات والإنترنت، حيث زادت جرائم الإختراق والإعتداء على البيانات والمعلومات، وجرائم تدمير ونقل البيانات والمعلومات المرفوعة على شبكة الإنترنت أو غيرها من الشبكات، من خلال المواقع الإلكترونية والأنظمة المعلوماتية". [2]

---

(1) ساسي، ريم (2016). الحماية الجنائية لسرية المعلومات الإلكترونية، رسالة ماجستير، جامعة العربي بن مهيدي – أم البواقي، كلية الحقوق والعلوم السياسية، ص5.

(2) النوايسة، عبدالإله، والعدوان، ممدوح (2019). جرائم التجسس الإلكتروني في التشريع الأردني – دراسة تحليلية، دراسات علوم الشريعة والقانون –الجامعة الأردنية، عدد1، ملحق 1 ص467.

ويجد الباحث أننا الآن في صدد اعتمادية مطلقة على الإنترنت في تسيير الأعمال كما هو الحال في المستشفيات والبنوك والمطارات وشبكات البيانات الحكومية وغيرها من القطاعات الحيوية المرتبطة على مستويات محلية ودولية، الأمر الذي تتطلب وجود حماية وضمانة فعالة لأمن المعلومات والبيانات، والجدير بالذكر أيضاً أن الخطورة لا تكمن في الأخطار والتهديدات التي تتعرض لها البيانات والمعلومات المرفوعة على الشبكة المعلوماتية فقط، بل تمدد الخطورة لضعف الجدار الأمني لمعظم الشبكات سواء الحكومية أم الخاصة وبصورة خاصة في الوطن العربي.

الأردن شأنها كشأن باقي الدول تسعى جاهدة لمواكبة التطورات في المجالات كافة منها التحول الرقمي المقترن بالتطور التكنولوجي وذلك لما فيه من منافع تنموية واقتصادية، فقد شهد الأردن بدايات هذا القرن الإنتشار الواسع لإستخدام شبكة الإنترنت بعد ازدياد استعمال الحاسب الآلي بصفة عامة، وبذلك فقد ازدادت الأخطار التي يمكن أن تتعرض لها الشبكات الحكومية أم الخاصة والمعلومات والبيانات المرفوعة عليها.

ولما كانت الجرائم التي ترتكب بواسطة الشبكة المعلوماتية وخاصة تلك التي تنطوي على انتهاك لسرية المعلومات وسلامتها تصل إلى درجة عالية من الخطورة ولضرورة مكافحة مثل هذا النوع من الجرائم فقد جاءت هذه الدراسة من أجل الإحاطة بهذا الموضوع وتسليط الضوء على التشريعات الجزائية الأردنية التي وفّرت الحماية للمحتوى الإلكتروني المتضمّن معلومات سرية تخص الدولة أم الأفراد العاديين والحماية من مخاطر الاستخدام غير المشروع لتقنيات معالجتها، وتحديداً تلك النصوص التي جاءت في قانون الجرائم الإلكترونية وقانون حماية أسرار ووثائق الدولة وأية قانون ساري المفعول متعلق في صلب موضوع الدراسة.

ثانياً: مشكلة الدراسة وأسئلتها

تكمن مشكلة هذه الدراسة بأنها تتناول أحكام المسؤولية الجزائية عن الانتهاكات أو التهديدات التي يتعرض لها أمن المعلومات والبيانات وسلامتها أو ما يعرف بالانتهاك الأمني المتمثل بجريمة انتهاك سرية المعلومات وتغييرها وتعطيل الأنظمة وحجب الخدمة وكسر بعض القواعد النظامية أو الأخلاقية، سواء على الصعيد الحكومي أم على الصعيد المتعلق بالقطاع الخاص، كما تظهر المشكلة في ربط هذه النوع من الجرائم مع جرائم أخرى.

أسئلة الدراسة

تتلخص مشكلة هذه الدراسة من خلال أسئلة الدراسة الآتية:

- ما مفهوم جريمة انتهاك سرية المعلومات وفقاً التشريع الأردني؟
- ما أركان جريمة انتهاك سرية الملعومات وفقاً التشريع الأردني؟
- ما هي السمات التي تميز جريمة انتهاك سرية المعلومات عن دونها من الجرائم؟
- ما هي أبرز صور جريمة انتهاك سرية المعلومات؟
- ما هي وسيلة الحماية التي وفرها المشرّع الأردني لمثل هذه المعلومات السرية وما مدى فاعليتها في مكافحة الانتهاكات الواقعة لها وفيما إذا كانت كافية لذلك أم أنها تحتاج إلى معالجة؟
- ما مدى إمكانية تطبيق أحكام المسؤولية الجزائية على الفاعلين؟

ثالثاً: أهداف الدراسة

هدفت هذه الدراسة إلى ما يأتي:

- بيان مفهوم جريمة انتهاك سرية المعلومات وفقاً للتشريع الأردني.
- تحديد أركان جريمة انتهاك سرية المعلومات وفقاً للتشريع الأردني.

- توضيح خصوصية جريمة انتهاك سرية المعلومات عن غيرها من الجرائم.
- بيان أبرز صور الانتهاكات التي تتعرض لها المعلومات السرية بواسطة الوسائل الإلكترونية.
- بيان وسيلة الحماية التي وفرها المشرّع الأردني لمثل هذه المعلومات السرية ومدى فاعلية الحماية الموفرة.
- تحديد أحكام المسؤولية الجزائية عن الانتهاكات الواقعة للمعلومات السرية.

رابعاً: أهمية الدراسة

تظهر هذه الأهمية من ناحيتين:

- **الناحية النظرية:** ستسهم هذه الدراسة في المساعدة على توضيح جوانب متعددة ومنها سرية المعلومات والجرائم التي تتعرض لها في فضاء الشبكة المعلوماتية والمشكلات الموضوعية والإجرائية لها إن وجدت، كما يستمد الموضوع أهميته لما له من انعكاسات هامة من الناحية العملية على بيئة التعاملات الإلكترونية.
- **الناحية التطبيقية:** إن المرجو من هذه الدراسة أن يتم الإستفادة منها ومن نتائجها من قبل الباحثين والمهتمين وأصحاب القرار وأن تكون إضافة مميزة مخصصة إلى المنظومة القانونية الأردنية وبما يسهم في الوصول إلى أعلى درجات الممارسة الفضلى في تعزيز سيادة القانون، ومعالجة الثغرات كافة التي تنشأ نتيجة لتسارع التطورات التقنية محلياً ودولياً.

خامساً: حدود الدراسة

ستشمل حدود هذه الدراسة فيما يتعلق بأبرز الانتهاكات التي تتعرض لها المعلومات السرية بواسطة الوسائل التقنية وطبيعتها من خلال إستقراء نصوص التشريعات المتمثلة بقانون الجرائم الإلكترونية رقم (27) لسنة (2015) وقانون حماية أسرار ووثائق الدولة رقم (50) لسنة (1971)

وقانون العقوبات رقم (16) لسنة (1960) وتعديلاته و قانون الاتصالات رقم (13) لسنة 1995 وتحليلها والقوانين السارية وقت إجراء هذه الدراسة والمتعلقة بالموضوع.

سابعاً: مصطلحات الدراسة

يقوم الباحث بتعريف مصطلحات الدراسة من خلال العودة إلى المراجع المتخصصة، وذلك للتسهيل على القارئ فهم هذه المصطلحات.

الجريمة: هي كل فعل غير مشروع صادر عن إرادة آثمة. [1]

الجريمة الإلكترونية: سلوك غير مشروع ينصب على معطيات الحاسب الالكتروني (بينات ومعلومات وبرامج) وتطال الحق في المعلومات ،ويستخدم في ارتكابها الوسائل الإلكترونية.[2]

الانتهاك : التعدي على الشيء بدون وجه حق، بغرض الإفشاء أو التخريب وما شابه ذلك. [3]

سرية المعلومات: " منع الكشف عن المعلومات المتواجدة في أنظمة التشغيل و أجهزة الحاسوب و الهواتف الذكية وقواعد البيانات الخاصة بالأفراد او المؤسسات أو المتعلقة بأمن الدولة و الاطلاع عليها ، وذلك من خلال تشفيرها و حمايتها من الاختراقات أو القرصنة أو الهاكرز أو التجسس الإلكتروني" [4].

---

(1) المجالي، نظام توفيق (2020). شرح قانون العقوبات القسم العام. ط7، عمان، دار الثقافة للنشر والتوزيع، ص67.

(2) بشير، عادل حامد (2021). الاثبات الجنائي للجريمة الإلكترونية. القاهرة، دار النهضة العربية، ص12.

(3) الهزاني، محمد ناصر (2018). المسؤولية الجنائية عن انتهاك قواعد الفضاء السيبراني: دراسة تأصيلية مقارنة بالقانون الإماراتي، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، كلية العدالة الجنائية – قسم الشريعة والقانون، الرياض، ص37.

(4) الرحباني، عبير شفيق (2020). الجرائم الإلكترونية ومخاطرها،عمان، دار الثقافة للنشر والتوزيع، ص25.

الوسائل الإلكترونية: وهي تلك الأعمال المادية غير المشروعة أو النشاط المخالف للقوانين والمستخدم بواسطة وسائل معينة من أجهزة الحاسوب والهاتف الذكي. [1]

الشبكة المعلوماتية: ارتباط بين أكثر من نظام معلومات لاتاحة البيانات والمعلومات والحصول عليها. [2]

نظام المعلومات: مجموعة البرامج والادوات المعدة لانشاء البيانات او المعلومات الكترونيا ، او ارسالها او تسلمها او معالجتها او تخزينها او ادارتها او عرضها بالوسائل الالكترونية. . [3]

سادساً: محددات الدراسة

بالرغم من وجود قانون خاص يسمّى بـ (قانون الأمن السيبراني) يسعى لحماية الأمن الوطني والاقتصادي والأمن الإجتماعي من الإختراقات والهجمات التي تتعرض لها أنظمة وشبكات المعلومات من المخترقين إلا أن هذا القانون يندرج تحت قائمة القوانين التنظيمية حيث أنه لم يأتِ بنصوص جزائية خاصة تجرم الانتهاكات المرتكبة خاصة الإنتهاك الأمني للمعلومات.

ثامناً: الإطار النظري والدراسات السابقة

وسيتم تقسيمه إلى:

أولاً: الإطار النظري للدراسة

تتكوّن الدراسة من خمسة فصول، الفصل الأول بعنوان " خلفية الدراسة وأهميتها " ويشمل مقدمة الدراسة ومشكلتها وهدفها وأهمية الدراسة وأسئلتها وحدود الدراسة ومحدداتها ومصطلحات الدراسة والدراسات السابقة ومنهجية الدراسة وأخيراً أدوات الدراسة، ثم يلي ذلك الفصل الثاني بعنوان " الإطار

---

(1) الحوامدة، لورنس سعيد (2017).الجرائم المعلوماتية أركانها وآلية مكافحتها ، جامعة طيبة، كلية الحقوق ، السعودية.

(2) المادة 2 من قانون الجرائم الإلكترونية رقم 27 لسنة 2015.

(3) المادة 2 من قانون الجرائم الإلكترونية رقم 27 لسنة 2015.

المفاهيمي لجريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية "، والفصل الثالث بعنوان " البنيان القانوني لجريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية "، و الفصل الرابع بعنوان " صور جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية " ، يلي ذلك الفصل الخامس بعنوان " الخاتمة ، النتائج و التوصيات "، ويليه قائمة المراجع.

ثانياً: الدراسات السابقة ذات الصلة

1- ريم ساسي (2016). الحماية الجنائية لسرية المعلومات الإلكترونية، رسالة ماجستير، جامعة العربي بن مهيدي – أم البواقي، كلية الحقوق والعلوم السياسية.

هدفت هذه الدراسة إلى تحديد المقصود بالجريمة المعلوماتية وخصاصائها وكما تناولت الدراسة مسألة المجرم المعلوماتي وأهم سماته وفئاته والدوافع التي تصار به لارتكاب الجريمة المعلوماتية، والتعرف على كيفية اصباغ الحماية الجنائية للجرائم الماسة بسرية المعلومات الإلكترونية وفقاً للتشريع الجزائري، وكذلك التعرف على الإطار القانوني للجرائم الماسة بسرية المعلومات الإلكترونية. كما بينت هذه الدراسة أبرز صور الجرائم الماسة بسرية المعلومات والجهود الدولية والوطنية المبذولة في سبيل مكافحتها. ونجد أنه تتفق كلاً من هذه الدراسة والدراسة الحالية من حيث ضرورة تحديد أركان الجريمة المعلوماتية المتعلقة بإنتهاك سرية المعلومات المرفوعة على الشبكة المعلوماتية، ومن حيث ضرورة توفير حماية جنائية فعالة للتصدي لمثل هذه التهديدات والجرائم. لكن الدراسة الحالية اختلفت عن الدراسة السابقة في تقديمها تحليلاً معمقاً بشكل أكبر للنصوص التي تعرضت لجريمة انتهاك سرية المعلومات في التشريع الأردني، وبيان النقص التشريعي وتقديم التوصيات والاقتراحات لسد مثل هذه الثغرات.

2- عمر محمد أبو بكر بن يونس (2004). بعنوان: "الجرائم الناشئة عن استخدام الإنترنت (الأحكام الموضوعية و الجوانب الإجرائية)"، رسالة لنيل درجة الدكتوراه في الحقوق من جامعة عين شمس كلية الحقوق بالقاهرة.

حيث هدفت الدراسة إلى الإلمام بالرقمية لأنها وسيلة الدراسات العلمية بالعالم الافتراضي والأخذ بعين الإعتبار التطور السريع والمستمر في هذا المجال والالمام بالنظام القانوني للإنترنت، واعتباره كفرع جديد من فروع القانون والاعتراف به من منطلق المبادرة لتغطية جوانيه القانونية، وتوصلت الدراسة ضرورة الدعوة إلى تبني فكرة قيام قسم يتناول قانون الإنترنت في كليات الحقوق ويكون متخصصاً، وأهمية تقنين النصوص القانونية في هذا المجال (الفضاء الإلكتروني) وعدم الإستعجال بعدم إصدارها لكي لا توسم بأنها ذات مستوى أقل وذلك من خلال بيان عدد من الجرائم دون الوقوف على مسألة ترتب المسؤولية الجزائية على مرتكبيها الأمر الذي يميز دراستنا الحالية كونها تنصب على بيان أهم صور جريمة انتهاك سرية المعلومات وبيان نطاق المسؤولية المترتبة على فاعليها والحيلولة دون وقوع مثل هذه الانتهاكات.

3- محمد ناصر الهزاني (2018). المسؤولية الجنائية عن انتهاك قواعد الفضاء السيبراني: دراسة تأصيلية مقارنة بالقانون الإماراتي، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية ، كلية العدالة الجنائية – قسم الشريعة والقانون، الرياض.

هدفت الدراسة إلى بيان المسؤولية الجزائية التي رتبها كل من التشريع السعودي و الإمارتي عن انتهاك قواعد الفضاء السيبراني، وتأكيد أن الجرائم السيبرانية أشمل من الجرائم المعلوماتية حيث أن الأخيرة تعتبر جزءًا من الجرائم السيبرانية، كما أنها هدفت إلى بيان القصور التشريعي في كل من النظام السعودي والإمارتي حول مسألة الأمن السيبراني وجرائمه وكيفية مكافحتها، كما ان الباحث عرج على الدور الذي يلعبه القانون الدولي العام متمثل في الاتفاقيات الدولية التي يكون لها الدور في مكافحة الجريمة السيبرانية، أما ما يميز دراستنا الحالية عن هذه الدراسة هو أن الدراسة الحالية

لا تميز بين الجريمة السيبرانية والجريمة المعلوماتية باعتبار أن الوسيلة المرتكبة لكلتهما واحدة وهي الوسيلة الإلكترونية، كما أن الدراسة الحالية تتبنّى فكرة أن مكافحة الجريمة الإلكترونية بصورها مسألة يلقى عاتقها على القانون الداخلي للدولة أكثر من القانون الدولي؛ وذلك من خلال إيجاد نصوص تشريعية فاعلة في مجال حماية أمن المعلومات الإلكتروني.

تاسعاً: منهجية الدراسة

منهج الدراسة

تعتمد الدراسة على المنهج الوصفي والتحليلي وذلك بوصف واقع الإنتهاكات والظواهر من خلال بيان معالم وعناصر النصوص القانونية التي نظمت موضوع انتهاك سرية المعلومات والجرائم التي قد تتعرض لها، وتحليلها بشكل علمي وموضوعي لبيان أحكام المسؤولية الجزائية عن تلك الانتهاكات وللوقوف على أيّ قصور قد شابها.

أدوات الدراسة

تتكون أدوات الدراسة من النصوص القانونية والأنظمة والتعليمات التي تتعلق بموضوع الدراسة وبصورة خاصة في التشريع الأردني.

الفصل الثاني

الاطار المفاهيمي لجريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية

شهد القرن العشرين تطورات مختلفة حصلت في مجال العلوم والتكنولوجيا انبثق عنها ظهور عدد كبير من المواقع الإلكترونية والأنظمة وانتشارها بشكل واسع لتخدم جميع القطاعات وجميع مستخدميها، لكن إلى جانب ذلك فقد تحولت هذه المواقع والأنظمة إلى ساحة لميلاد نوع جديد من الجرائم تعد ذات طبيعة مختلفة ترتكب في بيئة إلكترونية أو افتراضية تختلف عن بيئة الجرائم التقليدية المعروفة، وتعد جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية من أبرز صور الجرائم التي يتم ارتكابها بوساطة شبكة الإنترنت أو ما يعرف بالشبكة المعلوماتية والتي ترتب نتيجة جرمية جسيمة في حال ارتكابها كونها قد تمس بمعلومات ذات طبيعة خاصة أو سرية لا يجوز الكشف عنها إلا من قبل أشخاص مخولين للاطلاع عليها.

ولبيان مفهوم هذه الجريمة يجب أن نبين ماهية الجريمة الإلكترونية أولاً، ومن ثم نتعرض للمجرم المعلوماتي، ومن ثم إلى أبرز الجوانب التقنية لجريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية.

ولذلك سنقسم هذا الفصل إلى ثلاثة مباحث على النحو التالي:

- المبحث الأول: ماهيّة الجريمة الإلكترونية.
- المبحث الثاني: المجرم المعلوماتي.
- المبحث الثالث: الجوانب التقنية لجريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية.

المبحث الأول
ماهية الجريمة الإلكترونية

لقد تطوّرت الظاهرة الاجرامية في الآونة الأخيرة تطوراً مذهلاً سواء في أشخاص مرتكبيها أو في أسلوب ارتكابها والذي يتمثل في استخدام آخر ما توصلت إليه العلوم التقنية والتكنولوجية وتطويعها في خدمة الجريمة، ولما كانت الجريمة الإلكترونية هي ظاهرة إجرامية حديثة النشأة ولتعلقها بتكنولوجيا المعلومات فقد اكتنفها الغموض بالشكل الذي حدا بالكثيرين إلى القول أن الجريمة الإلكترونية لا وجود لها كونها لا تشكل تهديداً، ومن أجل الاحاطة بهذا الموضوع سنتناول الحديث حول الجريمة الإلكترونية في هذا المبحث وذلك بالتعرف على مفهومها و خصائصها .

المطلب الأول
التعريف بالجريمة الإلكترونية

إن الإشكالية التي تكمن في هذا الصدد هي عدم ايجاد تسمية موحدة لهذا النوع من الجرائم فهناك من يطلق عليها تسمية الجرائم الإلكترونية كما هو الحال في التشريع الأردني وهناك من يطلق عليها تسمية جرائم المعلوماتية في حين يذهب آخرون لتسميتها جرائم الحاسوب، وهناك من يسميها جرائم إساءة استخدام تكنولوجيا المعلومات والاتصال، لذلك سوف نحاول في هذا المطلب الوصول إلى تعريف الجريمة الإلكترونية.

ولطالما كانت مسألة وضع تعريف للجريمة الإلكترونية محلاً لاجتهادات الفقهاء فقد تعددت التعريفات وتفاوتت فيما بينها وقد أدت هذه الاجتهادات الفقهية المتشعبة لإيجاد صعوبة في وضع تعريف جامع وشامل للعناصر الأساسية المكونة للجريمة الإلكترونية.

فالاتجاه الأول يعتمد في تعريف الجريمة الإلكترونية على وسيلة ارتكابها ومن بين هذه التعريفات تعريف الفقيه الألماني تيادمان TIEDEMANN لهذا النوع من الجرائم حيث عرفها بأنها: (كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب الآلي)، كما تعرف أيضاً بحسب هذا الاتجاه بأنها:" كل نشاط إجرامي يؤدي فيه نظام الحاسب الآلي دوراً لتمامه على ان يكون هذا الدور على قدر من الأهمية " [1].

ويؤخذ على التعريفات السابقة التي اعتنقها أنصار هذا الاتجاه اعتمادها على وسيلة ارتكاب الجريمة الإلكترونية، ذلك أن تعريف الجريمة الإلكترونية يقوم في الأساس على العمل الرئيسي المكون لها وليس فقط على الوسائل المستخدمة فيها، ذلك أنه لا يمكن أن يطلق على جريمة ما أنها من الجرائم الإلكترونية لمجرد أن الحاسوب أو الوسيلة الإلكترونية مهما كانت قد استخدمت في ارتكابها [2].

أما الاتجاه الثاني فقد اعتمد في تعريفه للجريمة الإلكترونية على موضوع أو محل ارتكاب الجريمة، وهو البيانات أو المعلومات المخزنة في نظام المعلومات أو البرامج، وبحسب هذا الاتجاه فإن المعيار الأساسي المعتمد في تمييز الجريمة الإلكترونية عن دونها من الجرائم ليست الوسيلة المرتكبة من خلالها لا بل من خلال موضوع أو محل الجريمة وما يقع عليها من أفعال كالنسخ، أو التزوير، أو الإتلاف، أو الاعتراض، الإفشاء ... إلخ.

---

(1) عيلي، يامنة، وصابر، قشوش (2017). علم النفس الجنائي. عمان: دار اليازوري للنشر والتوزيع، ص56.

(2) حجازي، عبدالفتاح بيومي، (2006). مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي. الاسكندرية: دار الفكر الجامعي، ص 24-25.

ولعلّ أشهر التعريفات في هذا الاتجاه هو التعريف القائل بأنها " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو الوصول أو التي تحول عن طريقه " [1].

والاتجاه الثالث الذي اعتمده البعض في تعريف الجريمة الإلكترونية فقد بني على أساس المعرفة التقنية كأساس لارتكاب هذه الجريمة، فقد عُرفت بحسب هذا الاتجاه بأنها " أية جريمة يكون متطلباً لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب ".

وفي ذات الاتجاه عُرفت أيضاً بأنها " أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه " [2].

ويؤخذ على هذا الاتجاه أنه يوسع من نطاق هذه الجريمة، ذلك أنه يصعب المساواة بين السلوك غير المشروع قانوناً والسلوك الذي يستحق اللوم أخلاقياً واستهجان الكافة يعارضه أنه ليس بالضرورة أن يكون الانحراف عن الأخلاق والسلوك المؤثم معاقب عليه قانوناً. في الحالات التي تتطلب قدرا كبيرا من المعرفة المعلوماتية التي تتطلبها هذه الجريمة لارتكابها [3].

وقد اتجه بعض الشراح والفقهاء إلى عدم الاعتماد على معيار واحد فقط في تعريف الجريمة الإلكترونية، بل اعتمدوا في تعريفهم لهذه الجريمة على الجمع بين أكثر من معيار، ومن أمثلة التعريفات المختلطة وأبرزها وأشهرها التعريف البلجيكي للجريمة المعلوماتية أو الإلكترونية، والذي أوردته بلجيكا في تقريرها الخاص باستبيان الغش المعلوماتي الذي أجرته منظمة التعاون الاقتصادي

---

(1) المومني، نهلا عبد القادر (2008). الجرائم المعلوماتية. عمان: دار الثقافة للنشر والتوزيع، ص44.

(2) حجازي، عبد الفتاح بيومي، مرجع سابق، ص25.

(3) المرجع السابق نفسه، ص26.

والتنمية (OCDE) عام 1982م بقولها أنها (كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية، يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل تقنية المعلومات) [1].

وبناءً لما تقدم فإن الباحث يرى أنه من المفضل استخدام اصطلاح الجرائم الإلكترونية بدلاً من اصطلاح الجرائم المعلوماتية، على أساس أن لفظ الإلكترونية يعد أكثر شمولية واتساعاً من لفظ المعلوماتية خشية حصرها في مجال ضيق، بالإضافة إلى أنه وبنظر الباحث من الصعب أن يتم اعتماد معيار اساسي واحد لتعريف الجريمة الإلكترونية لأن في ذلك تصعيب من عملية طوي الأفعال التي قد تنطوي تحت ظل الجرائم الإلكترونية، فالأخذ بالمعيار المختلط هو الأنسب حيث أنه يحيط بتلك الأفعال بشكل اشمل من غيره.

وفي تقدير الباحث وعلى ضوء ما سبق يمكن تعريف الجريمة الإلكترونية بأنها: كل فعل أو نشاط غير مشروع يتم بوساطة الوسائل الإلكترونية بمختلف أنواعها موجه لارتكاب جريمة أو عمل مخالف للقانون ضمن الشبكات والأنظمة المعلوماتية وما تحتويه من بيانات أو معلومات مخزنة.

المطلب الثاني
خصائص الجريمة الإلكترونية

تتمتع الجريمة الإلكترونية بعدد من الخصائص هي في الحقيقة من نتائج ذلك التطور الهائل في تقنية المعلومات والاتصالات مما أكسبها طابعاً قانونياً خاصاً يميّزها عن دونها من الجرائم التقليدية أو المستحدثة هذا من ناحية، أما من ناحية أخرى فإن اختلاف الجريمة الإلكترونية عن الجرائم

(1) المنيفي، أحمد محمد، مرجع سابق، ص39.

التقليدية من حيث طبيعة الأفعال الجرمية أكسبها أيضاً خصوصية غير عادية، وهذا ما حدا بنا إلى بيان أهم خصائص الجريمة الإلكترونية ضمن هذا المطلب :

الفرع الأول : محل الجريمة الإلكترونية

الجريمة الإلكترونية كما سبق التعريف بها فإنها فعلٌ أو نشاطٌ غير مشروع، مرتكب بوساطة الوسائل الإلكترونية موجّه لارتكاب جريمة أو عمل مخالف للقانون يقع على بيانات أو معلومات، وعليه؛ يفهم أن محل الجريمة الإلكترونية معنوي لا مادي، ذلك لأنه البيانات والمعلومات ما هي إلا أشياء معنوية غير محسوسة.

الفرع الثاني : صعوبة اكتشاف الجريمة الإلكترونية

توصف الجرائم الإلكترونية بأنها خفية ومستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة، كإرسال فيروسات، وسرقة الأموال والبيانات الخاصة أو اتلافها، والتجسس وسرقة المكالمات وغيرها من الجرائم [1].

وبالتالي فإن هذه الجرائم وفي الغالب لا تترك أثراً لها بعد ارتكابها، كما يصعب الاحتفاظ الفني بآثارها إن وجدت، وهذا كله يصعب من مهمة المحقق العادي في التعامل معها، حيث يستخدم فيها وسائل فنية غير عادية تعتمد التمويه في ارتكابها والتضليل في التعرف على مرتكبيها، وفي كل الأحوال تحتاج مواجهة هذه الجريمة إلى خبرة فنية عالية متخصصة لإثباتها [2].

---

(1) الكعبي، محمد عبيد (2009). الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت. القاهرة: دار النهضة العربية، ص 31.

(2) محمد، رحموني (2018). خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، المجلد 17، العدد 41، ص441.

الفرع الثالث : صعوبة إثبات الجريمة الإلكترونية

يعد إثبات الجريمة الإلكترونية من الأمور التي لا تتم بسهولة فتكمن الصعوبة من حيث تتبعها واكتشافها، فهي كما ذكرنا سابقاً لا تترك أثراً يقتفى في بعض الأحيان، فمعظم الجرائم الإلكترونية تم اكتشافها بمحض الصدفة وبعد وقت طويل من ارتكابها، كما أنها تفتقر إلى الدليل المادي التقليدي كالبصمات مثلاً هذا من جهة، أما من جهة أخرى فإن عملية تعقّبها يتطلب خبرة فنية يصعب توافرها لدى المحقق العادي للتعامل معها، وعلاوة على ذلك أن مرتكب الجريمة الإلكترونية يتعمد إلى ممارسة أساليب التمويه والتضليل والتحايل عند ارتكابه للجريمة لإخفاء هويته الحقيقية [1].

فلا يعد بالأمر الهين استخراج واستنباط الدليل الإلكتروني، وهذا يعود لطبيعة الجريمة الإلكترونية الخاصة بالدرجة الأولى، والدليل الالكتروني نفسه فهو دليل علمي وفني، وتقني، فجميع العوامل السابقة تصعب الأمر على رجل الضابطة العدلية في مجال البحث والتحري في الجرائم الإلكترونية، مما يستدعي ضرورة الالمام بالمهارة التقنية من أجل استخلاص الدليل الالكتروني والتحقق من سلامته ليعد دليلاً مشروعاً لإثبات الجريمة الإلكترونية [2].

وتشمل الصعوبات التي تواجه عملية إثبات الجريمة الإلكترونية ما يلي:

1- غياب الدليل المرئي: حيث سبق وأن تم ذكر أن الدليل الإلكتروني ما هو إلا دليل معنوي لا يمكن رؤيته بالعين المجردة ولا يمكن لمسه، فالدليل المرئي يستوجب القدرة العالية من التقنية لاستخراجه والحصول عليه، وهذا ما نرى أنه غير متوافر لدى رجال الضابطة

---

(1) بدرة، والي (2019). المواجهة الاجرائية لجرائم المعلوماتية، رسالة ماجستير، كلية الحقوق، جامعة محمد بوضياف – المسيلة، ص 12.

(2) هلال، آمنة (2015). الاثبات الجنائي بالدليل الإلكتروني، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر –بسكرة، ص69.

العدلية المختصين بهذا الأمر مما يزيد صعوبة عليهم في عملية اكتشاف تلك الجريمة الإلكترونية المرتكبة.

2- سهولة إخفاء الدليل الالكتروني: إن المجرم المعلوماتي يتميز بأنه مجرم ذكي من الناحية التقنية، فبواسطة هذه الميزة يكون من السهل عليه أن يخفي أي دليل قد يؤدي إلى اكتشاف فعله غير المشروع المرتكب.

3- إعاقة الوصول إلى الدليل: ويتم ذلك من خلال اتخاذ المجرم المعلوماتي أي تدبير تقني يراه مناسباً لمنع الوصول إلى الدليل الالكتروني، لحماية نفسه من العقاب، مثل استخدام تقنية التشفير.

4- صعوبة فهم الدليل المتحصل عليه: وهنا في حالة الوصول إلى ذاك الدليل الذي يثبت الجريمة المقترفة من قبل المجرم المعلوماتي إلا انه لا يمكن تحليله أو تطويعه من خلال رجال الضابطة العدلية ليثبت الجريمة، نظرا لأن طبيعة هذا الدليل تقني ويحتاج إلى دراية تقنية عالية لفهمه.

الفرع الرابع : الجريمة الإلكترونية عابرة للحدود (الزمان والمكان)

إن شبكة الاتصالات التي تربط العالم من خلال الأقمار الصناعية والفضائيات والإنترنت جعلت الانتشار الثقافي وعولمة الثقافة والجريمة أمراً ممكناً وشائعاً، لا يعترف بالحدود الإقليمية للدول، ولا بالمكان ولا بالزمان، وأصبحت ساحتها العالم بأكمله، ففي مجتمع المعلومات تذوب الحدود الجغرافية

بين الدول لارتباط العالم بشبكة واحدة حيث أن أغلب الجرائم المرتكبة عبر شبكة الإنترنت يكون الجاني فيها في دولة ما والمجني عليه من دولة أخرى [1].

الفرع الخامس : الجريمة الإلكترونية من الجرائم الهادئة

ومن الخصائص التي تميز الجريمة الإلكترونية أنها ترتكب بأسلوب هادئ حين ارتكابها، على عكس الجرائم التقليدية التي تحتاج إلى مجهود عضلي في ارتكابها كما الحال في جريمة القتل والخطف التي تحتاج إلى إيذاء وممارسة العنف والسرقة التي تحتاج إلى فعل الخلع والكسر وغيرها من الجرائم، فالجرائم الإلكترونية لا تحتاج أدنى مجهود عضلي بل تعتمد على الدراسة الذهنية، والتفكير العلمي المدروس القائم عن معرفة تقنية الكمبيوتر [2].

(1) الدربي، عبد العالي، واسماعيل، محمد صادق (2012). الجرائم الإلكترونية. ط1، القاهرة: المركز القومي للإصدارات القومية، ص55-56.

(2) مراد، عبد الفتاح، شرح جرائم الكمبيوتر والإنترنت. القاهرة: دار الكتب والوثائق المصرية، ص46.

المبحث الثاني
المجرم المعلوماتي

أصبح الحاسوب على مدى العقود الماضية ركيزة أساسية لأهداف التطور في كل مجالات الحياة، وقد أدى الاستخدام الكبير للمجال المعلوماتي سواء كان في شكل أموال معلوماتية أم أساليب مستحدثة إلى ظهور ما يعرف بالإجرام المعلوماتي والذي يعتبر هذا نتيجة إلزامية لكل تقدّم علمي أو تقني مستحدث، ومع تطور الشبكة المعلوماتية وتوسّع مجالات استخداماته وازدياد أعداد المستخدمين له في العالم أصبح الإنترنت وسطاً ملائماً للتخطيط ولتنفيذ عدد من الجرائم بعيداً عن رقابة وأعين الجهات الأمنية إضافة إلى انه ثبت أن المجرمين المعلوماتيين ليسوا بأشخاص عاديين فهم يتمتعون بقدر كبير من الذكاء والدهاء، ويتحكمون في التقنيات التكنولوجية الحديثة وبالتالي هم قادرون على الذهاب بعيدا في ممارسة الإجرام عن طريق الإنترنت مما يستدعي توفير الأمن المعلوماتي [1].

وبناء على ما تقدم سوف نوضح في هذا المبحث بيان المقصود بالمجرم المعلوماتي ودوافع ارتكابهم للجريمة الإلكترونية ، كما سنتطرق بالحديث في هذا المبحث أيضاً عن طبيعة المجني عليه في الجرائم الإلكترونية .

المطلب الأول
مفهوم المجرم المعلوماتي

يُطلق خبراء أمن المعلومات الإلكترونية مصطلح HACKERS وهي جمع لكلمة هاكر وهو الإنسان الذي يقوم بعمليات الاختراق والتخريب عبر شبكة الإنترنت كما يطلقون مصطلح كراكرز

(1) بشرى، غريبي (2021). خصوصية المجرم المعلوماتي ودوافعه، مجلة نوميروس الأكاديمية، المجلد الثاني، العدد الثاني، ص101-115.

CRACKERS على المتخصصين بفك شفرات البرامج، وليس تخريب الشبكات فهم نوع من الهاكرز المتخصص [1].

والمجرم المعلوماتي هو كل شخص سواء طفل أو رجل أو أنثى يأتي أفعالاً إرادية تشكل سلوكاً إيجابياً أو سلبياً باستخدام تقنية المعلوماتية لإحداث نموذج إجرامي بالاعتداء على حق أو مصلحة، فسمات المجرم المعلوماتي تقترب في كثير من الأحيان من سمات المجرمين ذوي الياقات البيضاء، حيث كل من هؤلاء المجرمين قد يكونوا من ذوي المناصب الرفيعة المستوى ومن التخصصات والكفاءات العالية يتمتعون بالذكاء والقدرة على التكييف الاجتماعي في المحيط الذي يعيشون فيه، بل وان بعضهم يتمتع بالاحترام والثقة العالية من الأشخاص المحيطين بهم في مجال العمل أو المحيط الاجتماعي [2].

المطلب الثاني
دوافع المجرم المعلوماتي لارتكاب الجريمة الإلكترونية

يرتكب المجرم الإلكتروني أو المعلوماتي مختلف أنواع الاعتداءات على نظم الكمبيوتر وتحديداً الاختراقات بدافع التحدي وإثبات المقدرة العملية والتقنية، فالمجرم الإلكتروني ذو مهارات تقنية ودراية بالتكنيك المستخدم في نظام الحاسب الإلكتروني [3] ومن أهم دوافع ارتكاب الجريمة الإلكترونية الشغف بالإلكترونيات، والسعي إلى الربح، والدوافع الشخصية أو المؤثرات الخارجية، والأسباب الخاصة بالمنشأة.

---

(1) موسى، مصطفى محمود (2003). أساليب إجرامية بالتقنية الرقمية. مصر: دار الكتب والوثائق القومية المصرية، ص15.

(2) الكعبي، محمد عبيد، المرجع السابق، ص35.

(3) قشقوش، هدى حامد (1992). جرائم الحاسب الإلكتروني في التشريع المقارن. دار النهضة العربية، ص27.

ومن أهم دوافع ارتكاب الجريمة الإلكترونية ما يلي:

الفرع الأول : السعي إلى تحقيق كسب مالي

إن السعي وراء مكاسب مالية يعد أحد أهداف ارتكاب الجرائم الإلكترونية أو المعلوماتية وهو ما يترتب عليه إدخال تعديل على عناصر الذمة المالية، فطمع الاستيلاء على المال دافعها وبريق المكسب السريع محركها [1].

الفرع الثاني : الانتقام من رب العمل أو أحد الزملاء، وإلحاق الضرر به

يتعرض العاملون في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى لضغوطات نفسية ناجمة عن ضغط العمل والمشكلات المالية، هذه الأمور قد تدفع إلى النزعة نحو تحقيق الربح مما يدفع بعض العاملين لارتكاب جرائم الحاسب الإلكتروني وتحديداً جرائم إتلاف البيانات والبرامج وزرع الفيروسات باعثها الانتقام من المنشأة أو رب العمل أو أحد الزملاء [2].

الفرع الثالث : الرغبة في قهر النظام والتفوق على تعقيد وسائل التقنية

قد يكون الدافع إلى ارتكاب جرائم الحاسب الإلكتروني الرغبة في قهر النظام وتخطي الحواجز حوله، أكثر من رغبة الحصول على الربح، ويتجسد ذلك في نسبة متغيرة من جرائم الحاسب الإلكتروني خاصة ما يعرف بأنشطة الـ (HACKERS) المتطفلين الدخيلين على النظام والمتجسدة في جرائم التواصل مع أنظمة الحاسب –تحديداً عن بعد – الاستخدام غير المصرّح به لنظام الحاسب واختراق

---

(1) العبيد، فهد عبدالله (2016). الإجراءات الجنائية المعلوماتية. الإسكندرية: دار الجامعة الجديدة، ص50.

(2) بشير، عادل حامد ، المرجع السابق ، ص16.

مواقع الإنترنت ومرتكبي هذه الجرائم لديهم (شغف الآلة) دائماً يحاولون إيجاد الوسيلة إلى التفوق عليها [1].

ولا تعتبر الدوافع السابقة الذكر هي الدوافع الوحيدة التي تدفع المجرم المعلوماتي أو الإلكتروني لارتكاب الجرائم الإلكترونية، فيضاف إليها الدوافع السياسية والأيديولوجية كما الحال في جرائم الإرهاب الإلكتروني، ودوافع المنافسة في جرائم الاستيلاء على الأسرار التجارية.

المطلب الثالث
المجني عليه في الجرائم الإلكترونية

إن الحديث عن الجريمة الإلكترونية يجعلنا نسلط الضوء على المجني عليه في الجرائم الإلكترونية وذلك لأنه هو ضحية تلك الأنشطة والأفعال غير المشروعة المرتكبة بواسطة الوسائل الإلكترونية لتحقيق غايات إجرامية، وقد يكون المجني عليه إما شخصاً طبيعياً أو معنوياً كشركة أو مؤسسة اقتصادية أو سياسية.

فيرى الباحث بأن الجرائم الإلكترونية هي جرائم ذات طبيعة خاصة وحتى أن هذا الأمر قد طال المجنى عليه، فالجريمة الإلكترونية عكس الجريمة التقليدية الذي يجب أن يتم تحديد طبيعة المجنى عليه سلفاً في النص القانوني الذي جرمها، كما هو الحال في جريمة القتل فنجد أن قانون العقوبات الأردني قد حدد طبيعة محل جريمة القتل وهو الإنسان الحي، أما في الجرائم الإلكترونية فالحال يختلف بعض الشيء فنرى أنه من المتصور أن جريمة التجسس الالكتروني قد تطال شخصاً طبيعياً ومعنوياً في ذات الوقت، فقطاع البنوك هي أكثر القطاعات المستهدفة وعرضة لمثل هذا النوع من

(1) بشير، عادل حامد، المرجع نفسه، ص16.

الجرائم كونها من القطاعات التي تعتمد على تقنية التكنولوجيا المتمثلة بالحاسوب وملحقاته بشكل رئيسي لتسيير أعماله.

المبحث الثالث
السرية المعلوماتية

ذكرنا سابقاً أن التطورات التي طرأت على مجال تكنولوجيا المعلومات ساهمت في اعتمادها كوسيلة فعالة للتواصل بين الأفراد وأيضاً لتسيير أعمال المؤسسات العامة منها والخاصة هذا من ناحية، أما من ناحية أخرى فقد ساعدت هذه التطورات في تطوير الأسلوب الإجرامي ورفع نسبة وقوع الجريمة كون أن الأمر أصبح ليس من الصعب على المجرم فما هي إلا نقرة زر على لوحة المفاتيح فتتاح أمام المجرم معلومات لا تقدر بأيّ ثمن، لذا ففي هذا المبحث سوف نحاول التعرف على السرية المعلوماتية بشكل أوضح وذلك من خلال بيان ماهيتها و شروطها إن وجدت و تمييزها عن غيرها من المصطلحات التي تتقارب منها.

كما سنتطرق في هذا المبحث حول الحديث عن ماهية تلك المعلومات الإلكترونية المتبادلة عبر وسائل التكنولوجيا وماهي الشروط الواجب توافرها لكي تصلح أن تكون محلاً للحماية الجزائية ، بالإضافة للتعرف على ماهية الوسائل الإلكترونية المستخدمة في ارتكاب الجريمة الإلكترونية.

المطلب الأول
ماهية السرية المعلوماتية وشروطها

ساهم الإنترنت في تسهيل عملية معالجة البيانات لتكوين معلومات ذات فائدة تعود بالنفع على متحصليها وبذات الوقت تبادلها فيما بين مستخدمي هذه الشبكة، والأصل أن تكون هذه المعلومات مباحة للجميع لغاية الاستفادة منها وفقاً للمبدأ المستمد من فقه الشريعة " الأصل في الأشياء الإباحة"،

والاستثناء على هذا المبدأ نجده ونراه عندما تكون هناك بعض القطاعات قد استغلت الفائدة المذكورة أعلاه لتحقيق مقاصدها كالقطاع الأمني والقطاع الحكومي بشكل عام والقطاع التجاري وغيرها، ويلاحظ أن مثل هذه القطاعات تحرص كل الحرص على أن تكون عملية معالجة البيانات و تبادلها عبر أنظمتها بشكل سري لذا سنعمد في هذا المطلب أن نبين ماهية السرية المعلوماتية و شروطها.

الفرع الأول: تعريف السرية المعلوماتية

السرية في اللغة هي المصدر الصناعي المأخوذ من السر Secret والمشتقة من Sacred أي الشيء المقدس حيث أن فكرة السر بدأت من خلال ربطها بالتقديس [1]، وأيضاً السرُّ يعني ما أخفيت، والسر في لغة العرب هو الذي يكتم، وجمعه أسرار وهو ما يكتمه الإنسان في نفسه، أو هو ما تكتمه وتخفيه وما يسره المرء في نفسه من الأمور التي عزم عليها [2]، أو كما في قوله تعالى في كتابه العزيز: ﴿ وَإِن تَجْهَرْ بِٱلْقَوْلِ فَإِنَّهُۥ يَعْلَمُ ٱلسِّرَّ وَأَخْفَى ۝٧ ﴾ [3].

ومصطلح السرية (CONFIDENTIALITY) أو السر فقد اجتهد الفقهاء في تعريفه فقد قيل بأن السر هو " واقعة أو صفة ينحصر نطاق العلم بها في عدد محدد من الأشخاص إذا كانت ثمة مصلحة يعترف بها القانون في أن يظل العلم بها محصوراً في هذا النطاق ". [4]

---

(1) النوري، حسين، (1974). سر المهنة المصرفي في القانون المصري والقانون المقارن، اتحاد المصارف العربية، القاهرة، ص 8.

(2) انظر الموقع الالكتروني، https://www.almaany.com، يوم الاطلاع عليه 28/ 07 /2021.

(3) سورة طه، الآية رقم 7.

(4) حافظ، مجدي محب، (1997). الحماية الجنائية لأسرار الدولة – دراسة تحليلية تأصيلية لجرائم الخيانة والتجسس في القانون المصري والشريعة الاسلامية والقانون المقارن، الهيئة المصرية العامة للكتاب، الاسكندرية، ص 144.

وتعرف السرية اصطلاحاً بأنها: " درجة السرية المتعلقة بمعلومات معينة أو وثائق بالذات، والتي تتطلب الحماية، والتي تكون في صورة تداول محدود" [1].

تم تعريف السرية أيضا على أنها " ضمان أن تكون المعلومات متاحة فقط لأولئك الذين يؤذن لهم بالاطلاع" وهي أحد الأركان الأساسية لأمن المعلومات [2].

كما أن السرية المعلوماتية عُرفت لدى البعض بأنها: التأكد من عدم تعرض المعلومات للأخطار المتمثلة في إمكانية الكشف عنها أو الإطلاع عليها من قبل أشخاص غير مخوّل لهم أو غير مسموح لهم بذلك وفي الحالة التي يكون فيها مالكي هذه المعلومات يرغبون في إبقاء صبغة السرية عليها [3].

أما بالنسبة للمعنى القانوني لمصطلح السرية ومن خلال التطرق إلى نصوص التشريع الأردني وبعد استقراءها سواء قانون العقوبات أو غير من القوانين المتعلقة الشأن بصلب موضوع الدراسة نجد أن المشرّع الأردني لم يضع تعريفاً للسرية أو السر تماشياً مع العرف التشريعي بعدم وضع تعريفات تاركاً ذلك الأمر لاجتهادات الفقه والقضاء.

وتجدر الإشارة هنا، وبحسب رأي الباحث أن السلامة المعلوماتية التي ينادى البعض على أنها مصطلح مرادف للسرية المعلوماتية كونهما ضمانات لحفظ وصيانة أمن المعلومات المخزنة على أجهزة الحاسوب أو تلك المرفوعة على شبكة الإنترنت، ما هي إلا الوسيلة التي تستخدم والتي يتم اتباعها لتحقيق الغاية والتي هي السرية المعلوماتية التي تتمحور حول عدم المساس بتلك المعلومات

---

(1) الشامي، أحمد محمد، وحسب الله، سيد: المعجم الموسوعي لمصطلحات المكتبات والمعلومات الإلكتروني، https://www.elshami.com.

(2) أنظر الموقع الالكتروني، https://ar.wikipedia.org/wiki، يوم الاطلاع عليه: 28/ 07 / 2021.

(3) صورية، بورابة (2016). قواعد الأمن المعلوماتي. (أطروحة دكتوراه غير منشورة). جامعة الجيلالي اليابس. سيدي بلعباس، الجزائر، ص23.

الإلكترونية السرية سواء بانتهاكها أو اعتراضها أو إفشاءها أو بأي صورة من صور التعرض لها لغايات إجرامية.

ويرى الباحث بعد التطرق للتعريفات السابقة أنه يمكن تعريف السرية المعلوماتية بالقول أنها هي عبارة عن ضمانة لصيقة بتلك المعلومات التي تنطوي على جانب من الأهمية العالية والسرية، يوفرها لها صاحب تلك المعلومة، وتتمحور حول عدم السماح للأشخاص غير المخول لهم بالاطلاع على تلك المعلومات أو اعتراضها أو انتهاكها بأي شكل من الأشكال.

بعد التعرف على ماهية السرية المعلوماتية لا بد لنا من أن نتطرق للشروط الواجب توافرها لقيامها وهذا ما سنحاول توضيحه ضمن الفرع التالي.

الفرع الثاني: شروط السرية المعلوماتية

بناءاً على ما تقدّم من تعريف لمفهوم السرية المعلوماتية فإنه من الجدير أن نبيّن ماهية الشروط التي تجعل من الوقائع المعلوماتية كتخزين المعلومات أو تبادلها أمراً سرياً لتمييزها عن دونها من الوقائع المعلوماتية التي تعدّ مباحةً سواء للاطلاع أم للتبادل أو الاستغلال القانوني، ويمكن أن نستخلص هذه الشروط على الوجه الآتي:

أ- أن يكون السر بطبيعته أو بسبب الظروف المحيطة به

تفاوتت اتجاهات الفقه حول موضوع تحديد طبيعة السر فمنهم من ذهب إلى تحديد وصف السرية بالنظر إلى صاحب السر وهذا هو الاتجاه الأول، أما الاتجاه الثاني فأخذ بالمعيار الموضوعي

الذي يستند في تحديد طبيعة السرية إلى الظروف والأحوال الموضوعية التي أحاطت بالواقعة، كالمعلومات التي تتصل بالحياة الخاصة للأفراد [1].

ويؤيد الباحث الاتجاه الأول الذي استند في تحديد طبيعة السر بالنظر إلى صاحبه لا للظروف التي أحاط به، وعلة ذلك أن طبيعة المعلومات التي تكون سرية باعتقاد شخص وجديرة بالحماية قد لا تكون كذلك باعتقاد شخص آخر، وبالتالي فإن تقدير السر وأهميته يعود لصاحبه لا للظروف المحيطة كما أنه من الصعب أحياناً حصر تلك الظروف المحددة أو الأحوال المعينة التي ساهمت في جعل المعلومات سرية.

ب-ألا يكون معلوماً للكافة

يفتقد الشيء صفة السرية متى كان معلوماً للناس كافة، على انه تجدر الاشارة هنا أن هذه الصفة لا تزول عن الشيء حتى لو كان معروفاً للكافة، دام أنه غير مؤكد، فالسر يمكن أن يكون معروفاً لدى عدد كبير من الناس ما دام أنهم محددين ضمن فئة معينة كالأفراد ضمن محيط عمل واحد، أو كأفراد العائلة الواحدة، بالرغم من ذلك فتبقى صفة السرية لصيقة بالشيء، لكنه تنتفي هذه الصفة عنه متى علم به أشخاص لا تربطهم بصاحب السر علاقة خاصة، كالعلم بوقائع قضية ما عن طريق جلسة محاكمة علنية [2].

---

(1) عزيزة، رابحي (2018). الأسرار المعلوماتية وحمايتها الجزائية. (رسالة دكتوراه منشوره). جامعة أبو بكر بلقايد –تلسمان، الجزائر، ص38–39.

(2) عزيزة، رابحي، مرجع سابق، ص39.

المطلب الثاني
تمييز السرية عن الخصوصية

وبعد التعرف على السرية المعلوماتية بشكل واضح في المطلب السابق، وجدنا أنه ايضاً من الضرورة أن نفرقها عما يقاربها من مصطلحات قابلتنا ونحن في صدد دراستها، وهذا ما سنبينه ضمن هذا المطلب.

أظهرت لنا عملية البحث حول السرية المعلوماتية بعض المفاهيم القريبة منها كمصطلح الخصوصية، فما كان علينا سوى أن نبين سبب ذلك وماهية العلاقة بين كلا المصطلحين.

فالخصوصية من الناحية اللغوية يقصد بها حالة الخصوص، فيقال خصّه الشيء فيقال خصّه خصاً، واختصه أي أفرده دون غيره، ويقال اختص فلان بالأمر وتخصص له إذا انفرد [1].

يلاحظ أن الخصوصية من الناحية اللغوية تقترب من مفهوم السرية لكنها ليست مرادفة لها، ويعود ذلك لأن السرية تفترض الكتم والخفي، أما من ناحية الخصوصية وأن كانت قد تفترض قدر لا بأس فيه من الكتم والخفي لكنها قد تتوفر رغم انعدام السرية، كما ان الخصوصية كحق لا يقتصر مداه على عدم الكشف عن الأسرار بل يعني كذلك الامتناع أو الحول دون الاعتداء على خصوصيات الآخرين، ومن هنا نلاحظ أن السرية تعدّ جوهراً أساسياً للحق في الخصوصية هذا إن لم تكن وجهاً ملازماً للأخير.

(1) انظر الموقع الإلكتروني، https://www.almaany.com، يوم الاطلاع عليه: 30 / 07 / 2021.

ومصطلح " الخصوصية " يعرف بأنه: " حرص الفرد على الاحتفاظ بجانب من حياته وأفكاره وميوله وانشطته في مجال الحرمات الشخصية لنفسه أو لمن يختارهم من أعضاء عائلته واصدقائه وعدم الإفشاء غير المصرّح به" [1].

وبحسب هذا التعريف يتوضح لنا أن الخصوصية وكما قال الجانب الأكبر من الفقه انها هي حق ملازم ولصيق للإنسان، ترتبط بالفرد نفسه أكثر من ارتباطها بصلب محل الخصوصية كالمعلومة الإلكترونية المتبادلة عبر الوسائل الإلكترونية، فالخصوصية تعني أي أمر يتعلق بالحياة الخاصة للفرد كالمكالمات أو الصور أو مراسلات البريد الإلكتروني.

وبناءاً على ما تقدّم، فقد اختلفت وجهات النظر حول هذا الشأن فهناك من يقول أن السرية والخصوصية هما عبارة عن شيء واحد لا يمكن الفصل والتمييز بينهما، والجانب الآخر من ذهب بالقول أنه هناك ضرورة ماسة للتمييز بين كلا المصطلحين على اعتبار أنهما مختلفان وإن تقاربا في المعنى والغاية المرادة من توافرهما، وهذا ما سنتعرض له في الفروع التالية:

الفرع الأول: الإتجاه الأول: السرية والخصوصية هما شيئان مختلفان يجدر الفصل بينهما

يتجه جانب من الفقه إلى أنه لا يجوز الخلط بين السرية والخصوصية، على اعتبار أن الخصوصية تأتي متوسطة بين حالتي السرية والعلنية فإذا كان المشرّع يحمي الحق في الخصوصية فهو يحمي الحق في السرية من باب أولى ولكن يمكن أن يكون ما هو خصوصي ولكن لا يكون سرياً في ذات الوقت، فالسر هو ملكية لصاحبه فقط أما الخصوصي فهو ما لا يظهر للعلن حتى ولو لم يكن كتمانه قد وصل إلى حد السر.

---

(1) الشامي، أحمد محمد، وحسب الله، سيد، مرجع سابق.

متبنّوا هذا الاتجاه خلصوا بالقول بأن السرية تفترض حالة الكتم والخفي، أما الخصوصية فلا يلزم لتوافرها هذا القدر العالي من الكتم والخفي، "وفي هذا النطاق يقول إدوارد شليز: أن الفارق بين الخصوصية والسرية يكمن في أن السرية يحظر القانون الإعلان عنها أو الكشف عنها، أما الخصوصية فالكشف عن المعلومات أو الإعلان عنها مسألة ترجع إلى تصرف من يملك المعلومات" [1].

الفرع الثاني: الإتجاه الثاني: القائل بالربط بين السرية والخصوصية

يذهب أنصار هذا الاتجاه إلى الربط الوثيق بين الحق في الخصوصية والسرية، ويجعلهما وجهان لعملة واحدة، فالبعض يطلق على حقة في المحافظة على خصوصيات حياته الشخصية مصطلح حقه في السرية وعدم جعلها عرضة للناس كافة أو أن تكون موضوعاً متداولاً بينهم، فالإنسان له الحق في أن يعيش حياة هادئة بمنأىً عن العلانية والنشر.

فيظهر لنا مما تقدّم أن حماية مجال الحق في الخصوصية يتطلب لتحقيقه حماية السرية للمعلومات والوقائع المكونة والمتعلقة بالحق ذاته.

وبعد استعراض الاتجاهين السابقين الذكر، يرى الباحث أن كلاً من مصطلحي السرية والخصوصية مستقلان بحد ذاتهما وإن تداخلا في بعض المواضع كالأمور الشخصية التي ينطوي عليها الحق في الخصوصية، إلا أن السرية يعد نطاقها أكثر شمولاً واتساعاً، فالسرية بالأصل تشتمل على الحق في الخصوصية جنباً إلى جنب مع بعض الأسرار الأخرى كالأسرار الحكومية والسياسية والاقتصادية والمصرفية والمهنية والأسرار التجارية للتجار، أما الخصوصية فهي محددة بنطاق

---

(1) بن سعيد، صبرينة (2015). حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا " الاعلام والاتصال ". (اطروحة دكتوراه غير منشورة)، جامعة الحاج لخضر – باتنه، الجزائر، ص72.

خصوصيات الشخص وحياته أي أنها تدور بالوجه الأعم حول حياة الفرد الخاصة، وبذلك يؤيد الباحث الاتجاه الأول القائل بضرورة الفصل بين السرية والخصوصية.

المطلب الثالث
ماهية المعلومات الإلكترونية

أصبحت تكنولوجيا المعلومات والاتصالات من أهم المتغيرات التي تجتاح العالم حالياً، فقد أتاح الإنترنت المجال أمام تبادل كل المعلومات الخطرة والمحظورة والمهمة كمعلومات استخباراتية أو حكومية أو مالية أو تجارية عبر ضغطة خفيفة على زر لوحة المفاتيح لجهاز الكمبيوتر، إلا أنه يصاحب هذا المجال مجال آخر وهو ارتكاب أفعال إجرامية إلكترونية بحق هذه المعلومات المتبادلة عبر الشبكة المعلوماتية سواء بتخريبها أم الإفشاء عنها أو حتى باستغلالها بطرق غير مشروعة، وعليه سنحاول في هذا المطلب توضيح ماهية تلك المعلومات الإلكترونية التي تكون محلاً للجريمة الإلكترونية وطبيعتها.

الفرع الأول: تعريف المعلومة

المعلومات من حيث مدلولها اللغوي مشتقة من المادة اللغوية " علم "، وهي مادة غنية بالكثير من المعاني كالعلم والإحاطة بباطن الأمور والوعي والإدراك واليقين والإرشاد والإعلام والشهرة، والتميز والتيسير، وتحديد المعالم، والمعرفة، والتعليم والتعلم، والدراية ... إلى آخر ذلك من المعاني المتصلة بوظائف العقل [1].

ومصطلح المعلومات (INFORMATION) هو مصطلح شائع منذ القدم وتم استعماله في مجالات متنوعة مما جعل له استخدامات مختلفة في الاستعمال الدارج، فتعرف المعلومة اصطلاحا وفقاً للمعجم الموسوعي لمصطلحات المكتبات والمعلومات بأنها: " البيانات التي تمت معالجتها لتحقيق هدف معين أو لاستعمال محدد، لأغراض اتخاذ القرارات، أي البيانات التي أصبح لها قيمة بعد تحليلها، أو تفسيرها، أو تجميعها في شكل ذي معنى والتي يمكن تداولها وتسجيلها ونشرها وتوزيعها في صورة رسمية أو غير رسمية وفي أي شكل " [2].

كما تعرف أيضا أنها: " المادة الأولية التي من خلالها أو بواسطتها يمكن إعداد الأفكار" [3].

أما بالنسبة لموقف المشرّع الأردني من إيراد تعريف لمصطلح المعلومات فبالرجوع لقانون الجرائم الإلكترونية رقم 27 لسنة 2015 في المادة الثانية منه على أنها " البيانات التي تمت معالجتها وأصبح لها دلالة " [4].

---

(1) فتيحة، رصاع (2012). الحماية الجنائية للمعلومات على شبكة الإنترنت. جامعة أبي بكر بلقايد – تلسمان – كلية الحقوق والعلوم السياسية. الجزائر، ص25.

(2) الشامي، أحمد محمد، وحسب الله، سيد، مرجع سابق.

(3) العريان، محمد علي (2004). الجرائم المعلوماتية. دار الجامعة الجديدة للنشر، الاسكندرية، ص36.

(4) قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015، نشر هذا القانون في العدد (5343) في الجريدة الرسمية بتاريخ 4 أيار 2015.

الفرع الثاني: الشروط الواجب توافرها في المعلومة محل الحماية الجزائية وطبيعتها القانونية

بعد البحث واستعراض آراء الفقه وجد الباحث بأنه هنالك العديد من الباحثين ذهبوا نحو سرد مجموعة من الشروط لكي تكون المعلومات محلاً للحماية الجزائية يمكن بيانها كما يلي:

الشرط الأول: أن تكون المعلومة محدد ومبتكرة

تعرف المعلومة بأنها: " تعبير وصياغة محددة، تجعل رسالة ما قابلة للتبليغ والتبادل عن طريق علامات أو إشارات مختارة "، فوفقاً لهذا التعريف فإنه يجب أن تكون المعلومة محددة، فإذا انعدم تحديدها تكون المعلومة منعدمة. فالمعلومة المحددة هي التي تكون محصورة في إطار معين أما عن المعلومة المبتكرة فيجب أن تكون المعلومة مبتكرة، أي أن تتسم بالأصالة ولا يستطيع أي أحد الوصول إليها بيسر وسهولة، وبمفهوم المخالفة فإن المعلومة غير المبتكرة، متى كانت شائعة يسهل الوصول إليها من قبل أي شخص ولا يمكن نسبها لأي شخص محدد[1].

الشرط الثاني: أن يتوافر في المعلومة السرية والاستئثار

أن تكون المعلومة سرية: يقصد بها أن تكون محيطة بجدار من السرية أي ضرورة الاحتفاظ بهذه المعلومة في نطاق محدد من الأشخاص، أي أن تكون الرسالة التي تحملها محددة بمجموعة معينة من الأشخاص، وبدون هذه السرية فالمعلومة تكون عامة شائعة بين الناس، وبالتالي لا تتمتع بأي حماية جنائية، فصفة السرية لازمة للمعلومة. وتكتسب المعلومة هذه الصفة أي السرية إما بإرادة الشخص باكتشاف مجال حديث، أو بحسب طبيعتها كاكتشاف شيء لم يكن معروفا من قبل، أو باجتماع الأمرين معاً كالرقم السري للبطاقة الائتمانية هذا عن صحة السرية [2].

---

(1) فتيحة، رصاع، مرجع سابق، ص30.

(2) فتيحة، رصاع، المرجع نفسه، ص 31.

أما عن خاصية الاستئثار، فالمقصود بالاستئثار:" اختصاص شخص على سبيل الانفراد إما بشيء أو قيمة ما " [1]، فتعد أمرا ضروريا في المعلومة، لأنه في جميع الجرائم التي تنطوي على اعتداء قانوني على القيم يستأثر الفاعل بسلطة تخص الغير وعلى نحو مطلق، وتتوافر للمعلومة صفة الاستئثار إذا كان الوصول إليها غير مصرح به إلا لأشخاص محددين ويمكن أن ينبع الاستئثار من سلطة شخص أو جهة ما على المعلومة أو على التصرف فيها [2].

إلى جانب شرط التحديد والابتكار وشرط السرية والاستئثار السابق بيانهم، وبعد الدراسة والبحث وجد الباحث أنه هناك مجموعة من الشروط غير المتفق عليها ما بين الفقه يشترط البعض توافرها في المعلومات لكي تتمتع بالحماية الجزائية وتسمى هذه الشروط بالشروط الفنية، كونها تنطوي على جانب تقني أكثر من الجانب القانوني، ويمكن بيان هذه الشروط على النحو التالي:

1- المعالجة الآلية

هناك من يشترط أن تكون المعطيات معالجة آلياً لكي تخضع للتجريم، ويقصد بها العمليات المتعددة والتي تتم بصفة آلية عن طريق معالجتها داخل النظام. ونحن من جهتنا نؤيد ذلك لأنه لولا وجودها داخل النظام المعلوماتي لما أثرنا إشكالية هذه الدراسة أساساً [3].

2- اتخاذ تدابير جدية للمحافظة على سرية المعلومة:

يرى البعض أنه حتى يمكن حماية المعلومات السرية جزائياً، لابد من اتخاذ صاحبها إجراءات وتدابير جدية لحمايتها والمحافظة على سريتها خاصة إذا كانت تلك المعلومات على قدر من الأهمية

---

(1) الفار، عبد القادر (2016). المدخل لدراسة العلوم القانونية –مبادئ القانون –النظرية العامة للحق. ط16. دار الثقافة للنشر والتوزيع – عمان، ص130.

(2) عزيزة، رابحي، مرجع سابق، ص32–33.

(3) عزيزة، رابحي، المرجع السابق، ص34.

كالمعلومات السياسية والاقتصادية والتجارية. ومن تلك التدابير استخدام كلمات السر أو عمليات التشفير وغيرها من تدابير الحماية الفنية [1].

الفرع الثالث: أنواع المعلومات

تقسم المعلومات إلى خمسة طوائف، الأولى منها هي المعلومات الاسمية، والتي تتضمن المعلومات الشخصية والموضوعية، والطائفة الثانية من المعلومات هي المعلومات المباحة أو الشاغرة، أما الثالثة منها فهي المعلومات الخاصة بالمصنفات الفكرية ،والطائفة الرابعة التي تتمثل بالمعلومات السرية ، أما عن الطائفة الأخير وهي المعلومات العسكرية، وفيما يلي سنتناول تفصيل كل طائفة على حدى :

الطائفة الأولى: المعلومات الاسمية

وتنقسم هذه المعلومات بدورها إلى مجموعتين وهما المعلومات الشخصية والمعلومات الموضوعية:

النوع الأول: المعلومات الشخصية

وتعرف المعلومات الشخصية بأنها تلك المعلومات التي ترتبط بأحد الأشخاص ارتباطاً وثيقاً كاسمه، لقبه، موطنه، جنسيته، وضعه الاجتماعي [2] صحيفة السوابق العدلية .... كل شيء يتعلق بحياته الخاصة.

وإن التقدّم والتطور الهائل والسريع في شبكة الإنترنت الذي نشهده اليوم جعل منه وسيلة فعالة للربط والاتصال بين مختلف شعوب العالم ولتخزين المعلومات وعرضها، وهذا الأمر أوجد معلومات شخصية إلكترونية كالبريد الإلكتروني، الصور الشخصية، الأرقام السرية لبطاقات الائتمان والحسابات

---

(1) المرجع السابق نفسه.

(2) فتيحة، رصاع، مرجع سابق، ص28.

البنكية وكل المعلومات التي يستخدمها الشخص أثناء تفاعله على الإنترنت كالمعلومات المتواجدة على الصفحة الشخصية في الفيسبوك، فتلك المعلومات هي ذات طبيعة خاصة لا يجوز للغير الاطلاع عليها دون إذن مسبق من صاحبها وإلا اعتبر متعدياً [1].

النوع الثاني: المعلومات الموضوعية

وهي تعبر عن طائفة المعلومات الموجهة للغير، فهذه المعلومات على عكس المعلومات الشخصية لا تتعلق ولا ترتبط بأحد الأشخاص، بل هي موجهة للتعبير عن الرأي اتجاه الغير ومثال ذلك المقالات الصحفية والملفات الإدارية للعاملين لدى جهة معينة.

الطائفة الثانية: المعلومات المباحة أو الشاغرة

وهي تلك المعلومات التي يكون الهدف من وجودها عرضها على الكافة دون حاجة إلى إذن من شخص معين لأنها بدون مالك، مثل تقارير البورصة اليومية والنشرات الجوية، لكن يجدر الذكر أنه تنعقد ملكية هذا النوع من المعلومات متى ما قام أحد الأشخاص بجمعها وتخزينها، بقصد تكوين معلومات جديدة فإنها لا تصبح متاحة بل ستتصف بالسرية الأمر الذي يرتب لها الحماية التشريعية والجزائية في حالة قيام أحد الأشخاص بالاعتداء عليها [2].

الطائفة الثالثة: المعلومات الخاصة بالمصنفات الفكرية

وتمثل هذه الطائفة المعلومات المحمية بموجب تشريعات الملكية الفكرية أو الصناعية، منها المصنفات الأدبية والفنية كالمؤلفات أو البرامج المعلوماتية أو الأغاني أو الأفلام، والأسرار التجارية والذي يميز هذه الطائفة من المعلومات عن دونها من المعلومات أنها تتميز بالحماية الثنائية، فالأولى

---

(1) عزيزة، رابحي، مرجع سابق، ص40.

(2) عزيزة، رابحي، مرجع سابق، ص41.

بموجب التشريعات الناظمة لهذه المعلومات والاخرى جزائية مستوحية من القانون لكونها معطيات داخل نظام المعالجة الآلية للبيانات، إلا أن هذه الحماية ليست دائما متوافرة فالمعيار المعتمد في توافرها هو متى وجدت شروط المعلومة محل الحماية الجزائية كشرط التحديد والابتكار والاستئثار والسرية السالفة الذكر مسبقاً قامت الحماية الثنائية المعنية أعلاه [1].

الطائفة الرابعة: المعلومات السرية

هي المعلومات التي يكون الاطلاع عليها وحيازتها مقتصراً على الأشخاص المصرح أو المخول لهم وبالتناوب يكون محظوراً على غيرهم، وفي حالة الحصول عليها من غير المصرح لهم بها فذاك يمثل نشاطاً إجرامياً [2].

الطائفة الخامسة: المعلومات العسكرية

تعد المعلومات إحدى الوسائل المستخدمة لبناء الاستراتيجية العسكرية لدولة ما، فهذه المعلومات التي تتصل بالنشاط العسكري للدولة تلعب دوراً هاماً في تحقيق الأمن ودراسة حالة العدو على سبيل المثال، والمعلومات العسكرية تتسم بطابع سري خاص كون أن كشفها أو إفشائها قد يؤدي إلى زعزعة الامن واندلاع الحروب ومن الامثلة على هذا النوع من المعلومات الخطط العسكرية والأسرار العسكرية والمشروعات النووية [3].

---

(1) ساسي، ريم، مرجع سابق، ص36 –37.

(2) الحسيني، عمار عباس (2017). جرائم الحاسوب والإنترنت المعلوماتية (الجرائم المعلوماتية)، بيروت: منشورات زين الحقوقية، ص83.

(3) الحسيني، عمار عباس، المرجع نفسه، ص 83.

المطلب الرابع
ماهية الوسائل الإلكترونية المستخدمة في ارتكاب الجرائم الإلكترونية

إن النشاط الإجرامي الذي يسعى المجرم المعلوماتي لتحقيقه لا يمكن أن يتحقق من غير وسيلة والوسيلة المعنية في هذا الصدد هي الوسيلة الإلكترونية التي لا يمكن حصرها كما لا يمكن التنبؤ بما ستكون عليه هذه الوسائل مستقبلاً لما تشهده من تطور سريع وتنوع واضح لا سيما وأن الاكتشافات في مجال علوم التكنولوجيا أضحت لا يمكن إيقافها أو السيطرة عليها، لذلك سنتعرف في هذا المطلب على ماهية هذه الوسائل وخصائصها وأنواعها.

الفرع الأول: التعريف بالوسائل الإلكترونية

إن الوسائل الإلكترونية هي ما يرتبط باستخدام التقنيات الحديثة والتي تعتبر كتطبيق للحاسب الآلي بشكل عام وترتبط بتقنيات الاتصالات الحديثة وتكنولوجيا المعلومات [1]، " والتي بالتالي ترتبط بشكل أو بآخر بنظام الحاسب الآلي أو الالكتروني (الكمبيوتر) بحيث يعتبر الكمبيوتر كنظام معلوماتي هو محور التعامل الالكتروني بغض النظر عن الصورة التي يظهر من خلالها ، وأيضا هنالك ما وراء ذلك والذي يربط بين عوالم الاتصال الحاسوبي والذي يعرف بشبكة الإنترنت وعليه فلا بد من الوقوف على معنى الحاسب الآلي أو الالكتروني لبيان الوسيلة الأساسية في الجرائم الإلكترونية ، وكذلك توضيح المقصود بشبكة الإنترنت" [2].

التعريف بالحاسب الآلي (الكمبيوتر): يعرف الحاسب الآلي لدى البعض على أنه " جهاز الكتروني يستطيع أن يقوم بأداء العمليات الحسابية والمنطقية للتعليمات المعطاة له بسرعات كبيرة

---

(1) حجازي، عبد الفتاح بيومي (2009). الجرائم المستحدثة، ط1 (منشأة المعارف، الاسكندرية، ص1.

(2) ربايعة، عبد اللطيف محمود (2016). " الجرائم الإلكترونية" (التجريم والملاحقة والإثبات)، بحث مقدم إلى المؤتمر الاول للجرائم الالكترونية في فلسطين، جامعة النجاح الوطنية، نابلس، ص7.

تصل إلى عشرات الملايين من العمليات الحسابية في الثانية الواحدة وبدرجة عالية الدقة ولدية القدرة على التعامل مع كم هائل من البيانات وتخزينها واسترجاعها عند الحاجة إليها " [1] أو هو " مجموعة من الأجهزة المتكاملة تعمل مع بعضها البعض بهدف تشغيل مجموعة من البيانات الداخلة وفقا لبرنامج موضوع مسبقا للحصول على نتائج معينة " [2]. وبمعنى بسيط يمكن القول بأنه جهاز يهتم بمعالجة البيانات بطريقة آلية مسبقة الضبط بحيث يتم الحصول على نتاج هذه العملية عند الطلب.

وبالتالي فإن الحاسوب كنظام متكامل إنما يعمل في إطار معادلة ثلاثية الأطراف، بحيث يتكون من مجموعة من الأجهزة التي تشكل الكيان المادي الملموس لنظام الحاسوب والتي يطلق عيها لفظ (Hard ware) أي المعدات كطرف أول، وكذلك من مجموعة من المعلومات والأوامر أو التعليمات والتي يطلق عليها لفظ (Soft ware) أي البرمجيات، أما الطرف الثالث بالمعادلة والذي يحقق القيمة الفعلية للمعدات والبرمجيات هو وجود الأشخاص الذين يتعاملون مع البرمجيات ويستخدمونها كل حسب هدفه. [3]

التعريف بالإنترنت: يمكن تعريف الإنترنت بأنها عبارة عن شبكة مشاركة معلوماتية إلكترونية لوكالات حكومية وهيئات خاصة ومعاهد علمية وأفراد في كل دول العالم عن طريق أجهزة الحاسب " الكمبيوتر" بمختلف أحجامها وأنواعها أو أجهزة الهاتف النقال، كما تعني بالمعنى التقني الدقيق الترابط بين شبكات الحواسيب أو ما يقوم مقامها والمنتشرة في كل أنحاء العالم عن طريق الاتصال السلكي أو اللاسلكي [4].

---

(1) ابراهيم، خالد ممدوح (2008). أمن الجريمة المعلوماتية، ط1، الاسكندرية: الدار الجامعية، ص14.

(2) ابراهيم، خالد ممدوح، المرجع نفسه، ص14.

(3) المومني، نهلا عبد القادر، مرجع سابق، ص21.

(4) الحسيني، عمار عباس، مرجع سابق، ص20.

الفرع الثاني: خصائص الوسائل الإلكترونية

يرى الباحث بأن الوسائل الإلكترونية المستخدمة في ارتكاب الجرائم الإلكترونية تتمتع بالعديد من الصفات أو الخصائص والتي تميزها عن الوسائل التقليدية في ارتكاب الجريمة، ومن أهم الخصائص التي تتمتع بها الوسائل الإلكترونية ما يلي:

أولاً: خاصية الانسيابية من الرقابة

إذ أن الوسائل الإلكترونية المستخدمة في ارتكاب الجرائم قد أعطت العديد من الأشخاص الميزات كتخطي الحدود الجغرافية والزمانية والعمرية والمحلية والدولية، بالإضافة إلى حدود الرقابة والقيود القانونية التي تتركز على حماية الأنظمة والشبكات المعلوماتية من النشاطات الإجرامية التي من الممكن ان تطالها.

ثانياً: خاصية المرونة

تتجلى خاصية المرونة في الوسائل الإلكترونية المستخدمة في ارتكاب الجرائم بشكل واضح في النتيجة الإجرامية المتحققة، حيث أنه كلما زادت قدرات جهاز الحاسوب المستخدم أو الهاتف النقال كلما زاد لدى المجرم القدرة على تحقيق نتيجة إجرامية أكثر جسامة، وبالتالي زيادة قدرة ومرونة جهاز الحاسوب المستخدم لارتكاب الجريمة تؤدي إلى ارتكاب افعال إجرامية أكثر جسامة مقارنة عندما يكون الجهاز غير مرن وغير مساعد أو مؤهل لارتكاب الجرائم الإلكترونية.

ويجدر الإشارة هنا أن المجرم المعلوماتي الذي يريد أن يرتكب جريمة إلكترونية ما، لابد عليه أن يهيئ الأداة المستخدمة في ذلك، فالمجرم المعلوماتي كما سبق البيان هو مجرم ذكي تقنياً، حيث من الممكن أن يعمل على تطوير برنامج ما أو جهاز ما بشكل فائق من الناحية التقنية مما يساعده في ارتكاب في جريمته.

الفرع الثالث: أنواع الوسائل الإلكترونية

لا يمكن حصر الوسائل الإلكترونية التي تستخدم لارتكاب الجريمة الإلكترونية كما لا يمكن التنبؤ بما ستكون عليه هذه الوسائل مستقبلاً لما تشهده من تطور متسارع وتنوع واضح لا سيما وان الاكتشافات في هذا المجال باتت مما لا يمكن إيقافه أو السيطرة عليها، وعلى العموم فإن أبرز الوسائل المستخدمة في ارتكاب الجريمة الإلكترونية هي:

أولاً: الإختراق عن طريق استخدام الأنظمة المعلوماتية

إن الكثير من الأنظمة المعلوماتية التي تعتمدها القطاعات المختلفة في تسيير أعمالها وارسال المعلومات وتسليمها واستلامها أو معالجتها أو تخزينها أو ادارتها من خلالها قد تكون مليئة بالثغرات التقنية، التي تسمح للمجرم المعلوماتي باستغلال هذه الثغرات والتسلل للنظام المعلوماتي بأكمله بواسطة ثغرة قد تكون ضئيلة نوعاً ما، وصولاً إلى تحقيق هدفه ألا وهو النتيجة الجرمية المرجوة من وراء هذا الإختراق أو التسلل.

ثانياً: التقاط كلمات السر وجمعها

إن أنشطة الاعتداء التي تتم باستعمال كلمة السر تتم غالباً فيما سبق عن طريق تخمين كلمات السر مستفيدة من ضعف الكلمات عموما وشيوع اختيار الافراد لكلمات سهلة تتصل بمحيطهم الاسري أو محيط العمل أو حياتهم الشخصية، فإن الجديد استخدام برمجيات يمكنها التقاط كلمات السر خلال تجوالها في جزء من الشبكة أو أحد عناصرها ومراقبتها ومتابعتها لحركة الاتصال على الشبكة، بحيث يقوم هذا البرنامج من حيث الأصل بجمع أول 128 بايت أو أكثر مثلا من كل اتصال بالشبكة التي تجري مراقبتها تتبع حركة الاتصال عليها. وعندما يطبع المستخدم كلمة السر أو اسمه، فإن البرنامج يجمع هذه المعلومات وينسخه إضافة إلى أن أنواعاً من هذه البرامج تجمع المعلومات الجزئية وتعيد

تحليلها وربطها معاً، كما تقوم بعضها بإخفاء أنشطة الالتقاط بعد قيامها بمهمتها [1].

ثالثاً: استخدام البرامج

تعد هذه الوسيلة التقليدية من الوسائل الأكثر شيوعاً في ارتكاب الجريمة الإلكترونية، حيث لا تتطلب جهد كبير ولا معرفة تقنية عالية، حيث أن كل العملية تعتمد على وجود برنامجين أحدهما في جهاز الجاني والآخر يزرع أو يرسل لجهاز الضحية عن طريق عدة طرائق أشهرها البريد الإلكتروني ليكون البرنامج المؤتمر بأوامر الجاني، إذ يقوم الجاني بإرسال رسائل للضحية يرفق بها ملفا يحتوي على ذاك البرنامج الخبيث ليقوم بعدها الضحية بفتح هذا الملف وتحميل الملف على أنه برنامج مفيد وجيد ليكتشف أنه لا يعمل أو أنه يعمل على غير المتوقع وفي هذه الاثناء يقوم البرنامج باحتلال جهاز الضحية ويبدأ بالمهام المطلوبة منه كالتجسس والاختراق والسرقة، ولعل أشهر هذه البرامج الخبيثة هو برنامج حصان طروادة.

وفي خلاصة هذا الفصل يرى الباحث أن الجرائم الإلكترونية تعد من الجرائم الحديثة التي تتسم بطابع التطور المستمر فهي تزاد تطوراً بتطور التكنولوجيا ووسائلها، وهي جرائم تحدث نتائج جرمية جسيمة وفتاكة، فمرتكب هذا النوع من الجرائم هو مجرم يمتاز بسمات الذكاء العالي والمهارة التقنية المميزة التي باستطاعته تطويعها لإحداث جريمة لدافع ما، كجريمة انتهاك سرية المعلومات مثلاً فانتهاك سرية معلومات لمؤسسة أو منشأة ما قد يحدث نتائج جرمية خطرة تعود عليها بالضرر الكبير، وبذات الوقت تعود بالنفع على مرتكبها كونه قد اكتسب معلومات لا تقدر بثمن حول تلك المؤسسة أو المنشأة باستطاعته استغلالها لصالحه أو لصالح المستفيدين من تلك المعلومات وذلك من خلال بيعها أو تداولها بقصد زعزعة المؤسسة أو المنشأة.

---

(1) عزيزة، رابحي، مرجع سابق، ص115.

الفصل الثالث

البنيان القانوني لجريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية

تقع جريمة انتهاك سرية المعلومات في المجال الإلكتروني بالاطلاع على معلومات من قبل أشخاص غير مصرح أو مخول لهم ذلك، وكما أنه يتخذ انتهاك سرية المعلومات عبر الوسائل الإلكترونية عدة صور فإما صورة الدخول والبقاء غير المصرح به أو الاعتراض غير القانوني لانتقال المعلومات الإلكترونية.

و الجدير بالذكر أنه تكمن خطورة هذه الجريمة حينما تتحقق النتيجة الجرمية ، فالمعلومات السرية إذا وقعت بيد شخص غير مصرح أو مخول له الحصول عليها أو الاطلاع عليها أو الافشاء عنه ، قد يؤدي الى تحقق مخاطر عديدة نذكر منها على سبيل المثال و ليس الحصر عدم استقرار الأمن اذا كانت المعلومات تتعلق بأمن الدولة ، والخسارة فيما اذا كانت تلك المعلومات تنطوي على أسرار تجارية .

وللحديث عن هذه الجريمة بشكل أكثر تفصيلاً سوف نعمد إلى تقسيم هذا الفصل إلى المباحث التالية:

- المبحث الأول: الركن الشرعي لجريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية.
- المبحث الثاني: الركن المادي لجريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية.
- المبحث الثالث: الركن المعنوي لجريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية.

المبحث الأول

الركن الشرعي لجريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية

يتشكل البنيان القانوني لأية جريمة من ثلاثة أركان وهي الركن الشرعي ومن ثم الركن المادي وبالإضافة إلى الركن المعنوي، ويساعد هذا التقسيم على تحديد البناء والوصف القانوني لأي فعل وعليه سوف نتناول الحديث بداية عن الركن الشرعي في هذا المبحث وذلك من خلال استعراض النصوص القانونية التي شرعها المشرع الأردني حول الجريمة موضوع الدراسة كقانون الجرائم الإلكترونية رقم 27 لسنة 2015 و قانون الاتصالات رقم 13 لسنة 1995 و قانون حماية أسرار ووثائق الدولة رقم 50 لسنة 1971 ومن ثم نستعرض الركن المادي والمعنوي ضمن مباحث مستقلة.

يعرف الركن الشرعي بأنه الصفة غير المشروعة للفعل، ويكتسبها الفعل إذا توافر شرطان: الأول خضوع الفعل لنص التجريم والذي يقرر فيه القانون عقاباً لمن يرتكبه، والشرط الثاني عدم خضوع الفعل في ظروف ارتكابه لسبب من أسباب التبرير لأن انتفاء سبب التبرير شرط لاكتساب الفعل صفة عدم المشروعية التي أكسبها له نص التجريم [1].

(1) حسني، محمود نجيب (1985). شرح قانون العقوبات، القسم العام. ط 5، رقم 27، دار النهضة العربية، ص55.

المطلب الأول
قانون الجرائم الإلكترونية رقم 27 لسنة 2015

المشرّع الأردني لم يتدخل لمواجهة الجرائم الإلكترونية حتى وقت متأخر من ظهورها، حيث ظل هناك فراغاً تشريعياً حتى عام 2010، وفي عام 2011 فقد صدر القانون المؤقت (جرائم أنظمة المعلومات رقم 30 لسنة 2010) ومن ثم فقد صدر قانون الجرائم الإلكترونية رقم 27 لسنة 2015 الذي جاء ببعض الفروقات البسيطة عن القانون المؤقت كتجريم أفعال جديدة كالذم والقدح الإلكتروني والفروقات من الناحية اللغوية والصياغة.

أما فيما يخص الجريمة موضوع هذه الدراسة فالمشرّع الأردني لم يأتِ بنص قانوني واضح ليجرم هذا النوع من الجريمة ، حيث أنه بعد استقراء مواد القانون رقم 27 لسنة 2015 نلاحظ أن المشرّع الأردني قد قام بشمل العديد من الأفعال ضمن مظلة التجريم إلا أنه يؤخذ عليه أنه لم يكن هذا التجريم تفصيلياً بل كان عموماً وهذا من وجهة نظر الباحث، وفيما يلي سنستعرض المواد التي شملت فعل الانتهاك لكن بصورة أو بصياغة لغوية مختلفة بعض الشيء:

الفرع الأول: المادة (3) " جريمة الدخول غير المصرح به "

أ. يعاقب كل من دخل قصدا إلى الشبكة المعلوماتية أو نظام معلومات باي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح، بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن (100) مائة دينار ولا تزيد على (200) مائتي دينار أو بكلتا هاتين العقوبتين.

ب. إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة لإلغاء أو حذف أو إضافة أو تدمير أو افشاء أو اتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل الشبكة المعلوماتية أو نظام معلومات الشبكة المعلوماتية فيعاقب الفاعل بالحبس مدة

لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار.

ج. يعاقب كل من دخل قصدا إلى موقع الكتروني لتغييره أو الغائه أو اتلافه أو تعديل محتوياته أو اشغاله أو انتحال صفته أو انتحال شخصية مالكه بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار.

وعليه؛ يفهم من نص المادة السابق أن المشرّع الأردني وخاصة في الفقرة (أ) منها أنه حدى نحو تجريم الدخول المجرد من التصريح بشكل عام، وقد عرف المشرّع الأردني مصطلح التصريح في المادة 2 من ذات القانون بقوله أنه " الإذن الممنوح من صاحب العلاقة إلى شخص أو أكثر أو للجمهور للدخول إلى أو استخدام نظام المعلومات أو الشبكة المعلوماتية بقصد الاطلاع أو الغاء أو حذف أو اضافة أو تغيير أو اعادة نشر بيانات أو معلومات أو حجب الوصول إليها أو إيقاف عمل الأجهزة أو تغيير موقع الكتروني أو الغائه أو تعديل محتوياته "، هذا من جهة أما من جهة أخرى نلاحظ أن المشرّع الأردني في كلا الفقرتين (ب) و (ج) قد شدد التجريم بزيادة العقوبة بحدّيها الأدنى والأعلى واشترط تواجد القصد الخاص لتطبيقهما كالإلغاء أو الحذف أو الإفشاء أو انتحال الشخصية إلخ، إذ يفهم من وراء هذا التشديد أن الدخول غير المصرح به لغايات جرمية معينة هو أشد خطورة من ذاك المنصوص عليه في الفقرة (أ).

الفرع الثاني: المادة (4) " جريمة إدخال أو نشر برنامج الغاء "

يعاقب كل من أدخل أو نشر أو استخدم قصداً برنامجاً عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ أو التقاط أو تمكين الآخرين من الاطلاع على بيانات أو معلومات أو إعاقة أو

تشويش أو إيقاف أو تعطيل عمل نظام معلومات أو الوصول إليه أو تغيير موقع إلكتروني أو إلغائه أو اتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه دون تصريح أو بما يجاوز أو يخالف التصريح يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار.

من خلال قراءة هذا النص نجد أن المشرّع الأردني قد أوجب العقاب لكل من استخدم وسيلة إلكترونية كالبرامج أو غيرها لغايات إجرامية كالتدمير أو الافشاء، والتشويش على حركة المعلومات والبيانات، أي أن المشرّع ارتكز في التجريم والتشديد في العقاب في هذه المادة على أساس الوسيلة المستخدمة والقصد الجرمي الخاص المتمثل في إلغاء المعلومات أو حذفها أو تدميرها أو إفشائها ... إلخ من الغايات المذكورة في نص المادة سابقاً.

الفرع الثالث: المادة (5) " جريمة الاعتراض غير القانوني "

وتنص المادة على ما يلي:

يعاقب كل من قام قصداً بالتقاط أو باعتراض أو بالتنصت أو أعاق أو حوّر أو شطب محتويات على ما هو مُرسل 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.

ونجد أنّ المشرّع الأردني ذهب في هذه المادة إلى تجريم افعال الاعتراض غير القانونية للمعلومات أو البيانات المتبادلة عبر الشبكة المعلوماتية أو نظام المعلومات، وسنتحدث عن هذه الأفعال بشكل أكثر تفصيلاً لاحقاً.

الفرع الرابع: المادة (12) " جريمة الدخول على بيانات أو معلومات غير متاحة للجمهور "

وتنص المادة على ما يلي:

أ. يعاقب كل من دخل قصداً دون تصريح أو بما يخالف أو يجاوز التصريح إلى الشبكة المعلوماتية أو نظام معلومات بأي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمسّ الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (5000) خمسة آلاف دينار.

ب. إذا كان الدخول المشار اليه في الفقرة (أ) من هذه المادة بقصد إلغاء تلك البيانات أو المعلومات أو اتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها أو افشائها، فيعاقب الفاعل بالأشغال المؤقتة وبغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة آلاف دينار.

ج. يعاقب كل من دخل قصدا إلى موقع الكتروني للاطلاع على بيانات معلومات غير متاحة للجمهور تمس بالأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن (500) خمسمائة دينار.

د. إذا كان الدخول المشار إليه في الفقرة (ج) من هذه المادة لإلغاء تلك البيانات أو المعلومات أو اتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها، فيعاقب الفاعل بالأشغال المؤقتة وبغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة آلاف دينار.

ويفهم من نص المادة السابقة أن المشرّع الأردني قد وفر الحماية الجزائية الخاصة لتلك المعلومات أو البيانات التي تتصل بالأمن الوطني أو بالعلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني وذلك من خلال تشديد العقوبة المفروضة على مرتكب تلك الأفعال، وعلة ذلك بحسب رأي

الباحث أن المعلومات والبيانات المحمية بموجب هذه المادة هي ذات طبيعة خاصة وحساسة وتؤثر على أمن واستقرار المجتمع الأردني ودرءاً للمساس بها فقد رفع المشرّع العقوبة لحمايتها من أي انتهاك قد يطالها.

وبهذا نكون قد استعرضنا النصوص التي جاء بها قانون الجرائم الإلكترونية رقم (27) لسنة 2015 والتي تتعلق بجريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية، ولكن الأمر لا يقف إلى حد النصوص السابقة ذكرها فقط فالقانون ذاته في نص المادة (15) قد جرم أي فعل مجرم في تشريع أو قانون آخر نافذ فيما لو تم بوسيلة إلكترونية والتي جاء نصها بأنه: كل من ارتكب أي جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية أو أي نظام معلومات أو موقع إلكتروني أو اشترك أو تدخل أو حرض على ارتكابها يعاقب بالعقوبة المنصوص عليها في ذلك التشريع. وبرأي الباحث أن الهدف من وراء النص على المادة السابقة هو أن المشرّع أراد ان يوسع من مظلة التجريم خوفاً من أن يشابه عيب القصور في التجريم، وبهذا فقد فتح المجال أمامنا نحو البحث في القوانين الاخرى لاستعراض النصوص التي نصت على أفعال تتعلق بالانتهاك الواقع على المعلومات السرية.

المطلب الثاني
قانون الاتصالات رقم 13 لسنة 1995

نجد المشرّع الأردني وبالرجوع إلى نصوص قانون الاتصالات رقم 13 لسنة 1995 قد جرم الأفعال التي تشكل جريمة الإعتراض غير القانوني والتي تتم من خلال شبكات الاتصالات أو من خلال اعتراض الموجات الراديوية وهذا ما يمثل إحدى صور أفعال أو انشطة جريمة انتهاك سرية

المعلومات عبر الوسائل الإلكترونية ، لذا سنستعرض في هذا المطلب هذه النصوص والوقوف عليها ضمن الفروع التالية.

الفرع الأول: المادة 76 " جريمة شطب محتويات رسالة "

وتنص المادة على ما يلي:

(كل من اعترض أو أعاق أو حور أو شطب محتويات رسالة بواسطة شبكات الاتصالات أو شجع غيره على القيام بهذا العمل يعاقب بالحبس مدة لا تقل على شهر ولا تزيد على ستة أشهر أو بغرامة لا تزيد على (200) دينار أو بكلتا العقوبتين). نلاحظ أن المشرّع الأردني في نص هذه المادة قد وفر الحماية الجزائية لتلك الرسالة التي تحتوي على بيانات أو معلومات والتي يتم تبادلها عبر شبكات الاتصالات سواء أكانت هذه الشبكات عامة أم خاصة، وعرف القانون ذاته ما المقصود بشبكات الاتصالات بصورتيها العامة والخاصة وذلك بقوله أن شبكات الاتصالات العامة هي منظومة اتصالات أو مجموعة منظومات لتقديم خدمة الاتصالات العامة للمستفيدين وفقا لأحكام هذا القانون، أما عن شبكات الاتصالات الخاصة فهي منظومة اتصالات تشغل لمصلحة شخص واحد أو مجموعة واحدة من الأشخاص تجمعهم ملكية مشتركة لخدمة حاجاتهم الخاصة.

الفرع الثاني: المادة 80/أ " جريمة اعتراض الموجات "

وتنص المادة على ما يلي:

أ . كل من قام متعمدا باي اجراء لاعتراض موجات راديوية مخصصة للغير أو بالتشويش عليها أو بقطعها يعاقب بالحبس مدة لا تقل عن ستة أشهر أو بغرامة لا تقل عن (5000) دينار ولا تزيد على (25000) دينار أو بكلتا هاتين العقوبتين.

وهذه المادة تجرم فعل الاعتراض فيما إذا وقع على موجات راديوية يستخدمها الغير، ويقصد بالموجات الراديوية كما عرفها المشرّع الأردني بالقانون ذاته بأنها هي عبارة عن موجات كهرومغناطيسية ذات ترددات تقل عن ثلاثة آلاف (جيجا هيرتز) تبث في الفضاء دون موجه اصطناعي، وتستخدم هذه الموجات لغايات نقل أو بث أو استقبال أو ارسال الرموز أو الإشارات أو الاصوات أو الصور أو البيانات أو المعلومات، وعلة توفير هذه الحماية هي أنه بعض القطاعات الحيوية تعتمد اعتماداً كلياً على تلك الموجات في عملية تبادل بيانتها أو معلوماتها السرية، لذا لا بد من حماية تلك العملية.

المطلب الثالث

قانون حماية أسرار ووثائق الدولة رقم 50 لسنة 1971

يعد هذا القانون من القوانين التقليدية التي سنّها المشرّع الأردني في سبيل ضمان حماية وثائق الدولة السرية كالوثائق العسكرية أو الاقتصادية أو السياسية من أي فعل قد ينال منها أو يطالها، وذلك لما قد يترتب على الاطلاع عليها أو إفشائها من مساس لمصلحة الدولة، ونجد أن هذا القانون قد عرف الأسرار المراد حمايتها على عكس قانون الجرائم الإلكترونية رقم 27 لسنة 2015 بقوله أنها هي " اية معلومات شفوية أو وثيقة مكتوبة أو مطبوعة أو مختزلة أو مطبوعة على ورق مشمع أو ناسخ أو اشرطة تسجيل أو الصور الشمسية والافلام أو المخططات أو الرسوم أو الخرائط أو ما يشابهها والمصنفة وفق احكام هذا القانون " [1] . وسنستعرض ضمن هذا المطلب النصوص التي جاء بها هذا القانون والتي تتعلق بالجريمة موضوع هذه الدراسة وذلك ضمن الفروع التالية.

---

(1) المادة 2 من قانون حماية أسرار ووثائق الدولة رقم 50 لسنة 1971.

الفرع الأول: المادة 14 " جريمة الدخول إلى مكان محظور "

وتنص المادة على ما يلي:

(من دخل أو حاول الدخول إلى مكان محظور قصد الحصول على أسرار أو أشياء أو وثائق محمية أو معلومات يجب أن تبقى سرية حرصاً على سلامة الدولة عوقب بالأشغال الشاقة المؤقتة وإذا حصلت هذه المحاولة لمنفعة دولة أجنبية عوقب بالأشغال المؤبدة وإذا كانت الدولة الأجنبية عدوة فتكون العقوبة الإعدام). جاء المشرّع الأردني بنص هذه المادة لردع كل من حاول الدخول أو قد دخل إلى أي مكان يحفظ به أسرار أو وثائق الدولة والتي تحرص على أن تبقيها سرية، والجدير بالذكر أنه يفهم من مضمون النص السابق أن الدخول المشار إليه فيها هو الدخول المادي وليس الإلكتروني. ومن هنا يثار التساؤل هل يتصور أن يكون هذا الدخول إلكترونياً وما هو الأساس القانوني في التجريم والعقاب فيما إذا تم.

بالرجوع إلى نص المادة 15 من قانون الجرائم الإلكترونية نجد أنها تفرض العقاب على أية جريمة مجرمة وفق أي تشريع فيما إذا تمّت باستخدام الشبكة المعلوماتية أو النظام المعلوماتي وبذات العقوبة، وبالتالي فإنه من المتصور أن يتم الدخول المشار إليه أعلاه بشكل إلكتروني، كالدخول إلى موقع إلكتروني عائد للدولة يحتوي على معلومات سرية.

الفرع الثاني: المادة 15 " جريمة سرقة وثائق أو معلومات سرية "

وتنص المادة على ما يلي:

أ. من سرق أسرار أو أشياء أو وثائق أو معلومات كالتي ذكرت في المادة السابقة أو استحصل عليها عوقب بالأشغال المؤقتة لمدة لا تقل عن عشر سنوات.

ب. إذا اقترفت الجناية لمنفعة دولة أجنبية كانت العقوبة بالأشغال المؤبدة وإذا كانت الدولة الأجنبية عدوة فتكون العقوبة الاعدام.

والهدف من وراء التجريم في هذه المادة هو حماية المعلومات السرية من السرقة التي تكون لغايات شخصية، أو استخباراتية، أو تجسسية، دون النظر إلى الوسيلة المستخدمة في ارتكاب فعل السرقة أو الاستحصال، أي أن المشرّع الأردني ارتكز في التجريم على معرفة الجاني ان محل الجريمة هو معلومات سرية لا يجوز الاطلاع عليها أو افشائها، وكما ان هذا النص جاء على اطلاقه كونه لم يحدد وسيلة بعينها لتطبيق النص على الواقعة، ويرى الباحث أنه لا يوجد ما يمنع من تفعيل النص فيما إذا تم بوسيلة الكترونية وحقق ذات النتيجة الجرمية.

الفرع الثالث: المادة 16 " جريمة إفشاء الأسرار بحكم الوظيفة "

وتنص المادة على ما يلي:

أ. من وصل إلى حيازته أو علمه اي سر من الأسرار أو المعلومات أو اية وثيقة محمية بحكم وظيفته أو كمسؤول أو بعد تخليته عن وظيفته أو مسؤوليته لأي سبب من الأسباب فأبلغها أو أفشاها دون سبب مشروع عوقب بالأشغال المؤقتة مدة لا تقل عن عشر سنوات.

ب. ويعاقب بالأشغال المؤبدة إذا ابلغ ذلك لمنفعة دولة اجنبية وإذا كانت الدولة الاجنبية عدوة فتكون العقوبة الاعدام.

يطلع الموظف بحكم وظيفته على الكثير من الأمور والأسرار التي تتضمنها الوثائق الرسمية التي بين يديه وقد تحتوي هذه الوثائق على معلومات عسكرية أم اقتصادية أم سياسية، كما قد يطلع على أمور سرية تتعلق بخصوصيات المواطنين، وبناءً على ذلك يحظر على هذا الموظف أن يقوم بإفشاء الأسرار وإلا سوف يتعرض للمسؤولية الجزائية والمدنية مجتمعات أم منفردات، وهذا هو الهدف

من ايجاد نص المادة السابق ألا وهو تجريم أي إفشاء يتم بواسطة الوظيفة سواء بالطريقة التقليدية أم بالطريقة الحديثة (الإلكترونية) [1].

(1) أنظر الموقع الإلكتروني https://www.almadenahnews.com/article/899065، يوم الاطلاع عليه: 2021/11/18

المبحث الثاني

الركن المادي لجريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية

ذكرنا في المبحث السابق النصوص القانونية التي تشكل الركن الشرعي لجريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية، ومن الواضح أن هذه الجريمة كأي جريمة أخرى تتطلب لقيامها تحقق الركنين المادي والمعنوي، ناهيك عن الركن الشرعي، وفي هذا المبحث سنتناول الحديث عن الركن الثاني من أركان هذه الجريمة وهو الركن المادي.

الركن المادي للجريمة هو الفعل الذي يراه العالم الخارجي إبان ارتكابه ويتم إدراك هذا الفعل بواسطة الحواس كون أن الفعل يعد من قبيل الأفعال المادية الملموسة، في حين أنه لا توجد جريمة ترتكب دون وجود هذا الركن سنداً للقاعدة التي تقول بأنه " لا جريمة دون ركن مادي "، ويقوم الركن المادي للجريمة عادة على ثلاثة عناصر: الفعل (النشاط الإجرامي الإيجابي أو السلبي)، النتيجة، والعلاقة السببية بين الفعل والنتيجة [1].

إلا أن الركن المادي للجريمة الإلكترونية يختلف نوعاً ما عن الجرائم التقليدية كونه يقوم على صور فعل الاعتداء والمتمثلة في النصوص القانونية التجريمية ويتحقق السلوك أو النشاط الإجرامي المكون للجريمة موضوع الدراسة والتي تعد نوعاً من الجرائم الإلكترونية بجميع الأفعال التي تؤدي إلى انتهاك سرية المعلومات المخزنة على الشبكة المعلوماتية أو نظام المعلومات، وقد جاءت التشريعات بتعبيرات مختلفة للدلالة على هذا السلوك ومنها تعبير " الاطلاع " و" الإفشاء" و" الدخول غير المصرح به " أو اي سلوك يتيح انتهاك سرية المعلومات، والجدير بالذكر أن غالبية التشريعات

---

(1) المجالي، نظام توفيق، مرجع سابق، ص251.

ومنها التشريع الأردني الذي لم يحدد طريقة بعينها لوقوع جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية وكما لم يحدد لها نتيجة محددة.

ويرى الباحث أنه من الجدير أن تعتبر هذه الجريمة من جرائم الضرر " الجرائم المادية "، أي تلك الجرائم التي تتطلب حصول نتيجة إجرامية تترتب على سلوك الجاني وليس على مجرد قيام سلوك أو النشاط الإجرامي وفي هذه الحالة تعتبر من الجرائم الشكلية، وهو أمر بديهي يترتب على جريمة انتهاك سرية المعلومات التي تتطلب حدوث إطلاع أو إفشاء على تلك المعلومات بحيث تصبح متاحة لأشخاص غير مخول لهم الاطلاع عليها أو ان تصبح متاحة لعامة الناس، ومن ثم لابد أن تقوم علاقة السببية بين الفعل أو السلوك الاجرامي وبين النتيجة الاجرامية التي حصلت، بمعنى ان تكون نتائج الانتهاك بمختلف صوره، ناتجة عن ذلك الفعل أو السلوك الإجرامي.

المبحث الثالث

الركن المعنوي لجريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية

يقصد بالركن المعنوي أو بالقصد الجرمي الإرادة التي يقترن بها الفعل أو السلوك الإجرامي أو ما يعرف بنية ارتكاب الجريمة، المشرّع الأردني في المادة 63 من العقوبات نص على أنه: " النية: هي إرادة ارتكاب الجريمة على ما عرفها القانون ".

ويعرف الركن المعنوي بحسب الفقه أنه: " العلاقة التي تربط بين ماديات الجريمة وشخصية الجاني مرتكبها "، فهو العلاقة بين محل الإذناب التي يستحق الجاني العقاب المفروض قانوناً [1].

ويتخذ هذا الركن إما صورة القصد وعندها توصف الجريمة بأنها جريمة قصدية أو عمدية بمعنى أن يكون الفاعل أراد أن يرتكب الفعل المكون للجريمة وبذات الوقت قاصداً تحقيق النتيجة الجرمية وراء ذاك الفعل كما هو الحال فيما لو دخل شخص ما لموقع إلكتروني قاصداً الاطلاع على ما يحتويه من معلومات سرية أو لإفشائها، أو ان يتخذ الركن المعنوي صورة الخطأ وعندها توصف الجريمة بأنها غير مقصودة ومثال ذلك أن يقوم شخص ما بالدخول إلى موقع إلكتروني محظور الدخول إليه عن طريق الخطأ، فتتم الجريمة وتتحقق نتيجتها، ولكن لم يتعدى الدخول لتحقيق مقاصد اخرى كالاطلاع على معلومات محظورة أو إفشائها.

وتعد جريمة انتهاك سرية المعلومات الإلكترونية من الجرائم العمدية التي يتطلب قيام الركن المعنوي فيها وجود القصد الجرمي القائم على عنصري العلم والارادة، فنعصر " العلم " يعبر عن علم الجاني أن ينتهك سرية معلومات إلكترونية يحرص على الحفاظ على سريتها، وبخلاف ذلك أي أن يظن الجاني مثلا انه يطلع على معلومات تعود له فهنا ينتفي عنصر العلم، ومن النادر حدوث هذه

---

(1) إبراهيم، خالد ممدوح (2007). الجرائم المعلوماتية، دار الفكر الجامعي، الاسكندرية، ص243.

الفرضية، أما بشأن عنصر " الإرادة " والذي يلقب بأنه جوهر الركن المعنوي فهو يعبر عن اتجاه إرادة الجاني نحو تحقيق التنجية الإجرامية والتي تتمثل بالاطلاع على المعلومات السرية لغاية استغلالها أو افشائها أو جعلها متاحة للجميع وغيرها من المقاصد الجرمية التي يمكن أن ترتكب من قبل الجاني.

كما يجدر الإشارة هنا أنه تواجه عملية استخلاص الركن المعنوي في الجرائم الإلكترونية العديد من الإشكالات والصعوبات، كصعوبة استخلاص الجوانب الموضوعية للركن المعنوي في ظل بيئة الإنترنت أو البيئة الرقمية، حيث يكون على قاضي الموضوع دور البحث عن إرادة الفاعل المنصرفة إلى إرادة الفعل وإرادة النتيجة، وإلى علمه بالوقائع دون الحاجة لإثبات العلم بالقوانين باعتباره أمراً مفترضاً واستناداً إلى قاعدة " لا يعتد بالجهل بالقانون"، بالنسبة لإرادة الفعل فإن طبيعة الجرائم الإلكترونية لا تزيد من صعوبة استخلاصها ولا تخفف فالأمر يعتبر ذات الصعوبة كما هو الحال في الجرائم التقليدية، لكن تثار الصعوبة بالنسبة لإرادة النتيجة والعلم بالوقائع المكونة للجريمة فعلى القاضي أن يكون ملماً إلماماً تاماً بالنتائج المترتبة على الجريمة الإلكترونية، خاصة في حالة تعدد وتفاقم النتائج فهنا يزداد الأمر صعوبة، كما تكمن الصعوبة أمام القاضي حين استخلاص الركن المعنوي وهو في صدد جريمة إلكترونية حين يكون عليه أن يثبت أن الجاني يعلم بالتفاصيل المكونة للركن المادي بما في ذلك علمه بالأركان الخاصة والظروف المشددة، فعلى القاضي أن يكون ملماً بكافة أركان الجريمة الإلكترونية وظروفها [1].

(1) العتوم، محمد شبلي (2021). جرائم تكنولوجيا المعلومات " النظرية العامة للجرائم الالكترونية". عمان: دار الثقافة للنشر والتوزيع، ص122-128.

الفصل الرابع

صور جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية وصعوبات إكتشافها وإثباتها

إن من خصائص الجريمة الإلكترونية كما سبق الذكر أنه من السهولة ارتكابها وتعد هذه الخاصية السبب الرئيسي في تنوع أساليب ارتكاب هذا النوع من الجرائم، والجريمة موضوع هذه الدراسة هي جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية والتي تعد من قبيل الجرائم الإلكترونية قد تتخذ صور متعددة لكن النتيجة الجرمية هي واحدة وهي الاطلاع على معلومات إلكترونية سرية أو الافشاء عنها من قبل أشخاص غير مخوّل لهم ذلك أو اعتراض تلك المعلومات.

كما يجدر الإشارة إلى أن التنوع في أساليب إرتكاب جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية أدى إلى خلق معوقات أو صعوبات تقف أمام عملية اكتشافها وإثباتها الأمر الذي قد يطيل من أمر إلقاء القبض على المجرم المعلوماتي مقترف الجريمة و مجازاته.

وللحديث عن الصور التي تتخذها جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية والصعوبات التي تواجه عملية اكتشاف الجريمة وإثباتها سوف يتم تقسيم هذا الفصل إلى أربعة مباحث على النحو المبيّن:

- المبحث الأول: جريمة الدخول غير المصرّح به.
- المبحث الثاني: جريمة الاعتراض غير القانوني لانتقال المعلومات و البيانات.
- المبحث الثالث: صعوبات اكتشاف جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية.
- المبحث الرابع: صعوبات الإثبات الجنائي لجريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية.

المبحث الأول
جريمة الدخول غير المصرح به

اختلف الفقه في التسميات التي أطلقها على الجريمة التي نحن بصددها فمنهم من سماها بـ (الدخول غير المشروع) [1] أو (الولوج غير المسموح به في نظم المعلومات) ومنهم من ذهب إلى تسمية الدخول غير المصرّح به إلى النظام المعلوماتي [2]، وللتعرف على ماهية هذه الجريمة والأركان العامة لهذه الجريمة سنقسم هذا المبحث إلى المطالب التالية .

المطلب الأول
ماهية الجريمة

يعرف الدخول غير المصرح به (UNAUTHORIZED ACCESS) بأنه عبارة عن عملية توجيه هجمات إلى معلومات الكمبيوتر أو خدماته بقصد المساس بالسرية أو المساس بالسلامة والمحتوى والتكاملية أو تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالها [3].

ويكون الدخول إلى النظام المعلوماتي، مشروعاً متى ما كان قد تمّ عن طريق من هم مخولين بذلك الدخول، أما فيما إذا تم الدخول بصورة عكس ذلك أي بدون أي تخويل أو تصريح فنحن بصدد جريمة إلكترونية.

وتتنوع الوسائل التي يمكن اللجوء إليها لإتمام الدخول غير المصرح به إلى النظام المعلوماتي أو الشبكة المعلوماتية، ففي الاغلب أن مثل هذا الدخول لا يتطلب أكثر من تشغيل جهاز الكمبيوتر

---

(1) حجازي، عبد الفتاح بيومي، مكافحة جرائم الكمبيوتر، مرجع سابق ص 353 وما بعدها.

(2) الحسيني، عمار عباس، مرجع سابق، ص253.

(3) ابراهيم، خالد ممدوح، مرجع سابق، ص 84.

أو فتح برنامج خاص لمثل هذا الدخول، وقد يتطلب الأمر الحصول على شفرات خاصة بالدخول باستخدام جهاز لفك هذه الشيفرة، كما يمكن الدخول عن طريق وسائل أخرى للدخول لأنظمة الحاسبات الآلية تعتمد على ضعف الانظمة ذاتها وضعف وسائل الحماية فيها أو عن طريق الثغرات الموجودة في تلك الأنظمة [1].

المطلب الثاني
أركان الجريمة

هذه الجريمة كأي جريمة أخرى لا بد لقيامها من توافر أركان الجريمة وهي الركن الشرعي الذي يتمثل في النص القانوني على تجريم أفعال الدخول غير المصرح به إلى نظام المعلومات، بالإضافة إلى الركن المادي والمعنوي، لذا سنعمد إلى تناول هذه الأركان في الفرع على النحو التالي:

الفرع الأول: الركن الشرعي

من خلال مراجعة النصوص التشريعية الأردنية وجدنا أن المشرع قد عاقب على أفعال الدخول غير المصرح به إلى النظام المعلوماتي بشكل واضح وصريح، فبالرجوع إلى نص المادة (3) من قانون الجرائم الإلكترونية رقم 27 لسنة 2015 نلاحظ تجريمه للدخول غير المصرّح به [2].

الفرع الثاني: الركن المادي

يتمثل الركن المادي لهذه الجريمة في فعل الدخول غير المشروع إلى أنظمة المعلومات أو الشبكات الإلكترونية أو المواقع الإلكترونية، وتجدر الإشارة هنا إلى أنه لا يعد جريمة الدخول المجرد

---

(1) قورة، نائلة محمد فريد (2005). جرائم الحاسب الاقتصادية " دراسة نظرية وتطبيقية "، بيروت، منشورات الحلبي الحقوقية، ص316.

(2) انظر: المادة (3) من قانون الجرائم الإلكترونية رقم 27 لسنة 2015.

إلى النظام المعلوماتي، إنما يكتسب صفة التجريم متى ما تم بدون تصريح أو إذن من مالك النظام أو الحائز له والذي يعد الأساس المعتمد للتفريق بين الإباحة والتجريم [1].

ومن الجدير بالذكر أن جريمة الدخول غير المصرّح به تعد في عددٍ من التشريعات كالمشرّع الأردني من قبيل الجرائم الشكلية التي تتحقق بمجرد قيام السلوك المكون لها دون النظر إلى نتائج تترتب على هذا الدخول بخلاف بعض التشريعات التي جعلت هذه الجريمة من جرائم النتيجة التي تتطلب لقيام الركن المادي فيها، حصول نتيجة إجرامي كالحصول على معلومة سرية نتيجة لذلك الدخول.

ويتجسد السلوك الجرمي لجريمة الدخول غير المصرح به بشقّين هما الدخول وعدم التصريح ، فالنسبة لعنصر الدخول فقد عرفت المذكرة الإيضاحية لقانون جرائم أنظمة المعلومات الدخول غير المصرح به بأنه: (التطفل أو القرصنة على موقع إلكتروني أو نظام معلومات غير متاح للعموم الدخول إلى أي منهما دون تصريح) ، أما بالنسبة لعدم التصريح فإنه لا تتم جريمة الدخول غير المصرح به إلى أنظمة المعلومات إلا إذا تمت بصورة غير مشروعة أي بدون وجود تصريح أو تخويل للدخول وقد عرف المشرّع الأردني التصريح في المادة (2) من قانون الجرائم الإلكترونية رقم 27 لسنة 2015 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 الغائه أو تعديل محتوياته " [2].

---

(1) الحسيني، عمار عباس، مرجع سابق، ص261-262.

(2) العتوم، محمد شبلي، مرجع سابق، ص37.

الفرع الثالث: الركن المعنوي

جريمة الدخول غير المصرح به هي جريمة عمدية فلا بد من أن يتوافر القصد الجرمي و القصد فيها إما أن يكون قصد عام يتطلب عنصري العلم والإرادة ، وذلك باتجاه إرادة الجاني لارتكاب الفعل وتحقيق النتيجة المرجوة والمتوقعة من ذاك الفعل، أي أن يكون لدى الجاني الالمام الكافي بماهية وأركان فعله غير المشروع وأن يتوافر لديه العلم بأنه يقوم بالدخول إلى موقع إلكتروني ونظام المعلومات من غير تصريح أي أن القصد العام يقف إلى حد الدخول إلى ذاك الموقع الالكتروني أو نظام المعلومات دون تخويل أو تصريح ، وقد يكون القصد الجرمي بصورة خاصة أي أن فعل الدخول غير المصرح به هو لغايات إجرامية محددة سابقاً لدى الجاني كالاطلاع على معلومات سرية أو إفشائها مخزنة على موقع إلكتروني أو نظام معلومات فنلاحظ هنا أن نطاق الدخول دون تصريح قد تعدى ليصل إلى تحقيق غايات جرمية معينة الأمر الذي يستوجب معه تشديد العقوبة على الجاني.

المبحث الثاني
جريمة الاعتراض غير القانوني لانتقال المعلومات والبيانات

نصت المادة الثالثة من اتفاقية بودابست لعام 2001 على أنه: " يجب على كل طرف أن يتبنّى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية وفقاً لقانونه الداخلي واقعة القانون العمدي وبدون حق من خلال وسائل فنية للإرسال غير العلني لبيانات الحاسب بما في ذلك الانبعاثات الكهرومغناطيسية من جهاز حاسب يحمل هذه البيانات، كما يمكن لأي طرف أن يستوجب أن ترتكب الجريمة بنية إجرامية أو ترتكب الجريمة في حاسب يكون متصلاً عن بُعد بحاسب آخر " [1]. وكان الغرض من النص على هذا الشكل من الجريمة هو لحماية الحق في حرية الاتصالات وبذات الوقت حماية المحتوى السري المتبادل بين جهتي الاتصال من التدخل أو الاعتراض الخارجي، لذا سنتطرق في هذا المبحث إلى مفهوم جريمة الاعتراض غير القانوني في المطلب الأول، وأركانها في المطلب الثاني.

المطلب الأول
ماهية الجريمة

فعل الاعتراض غير القانوني يعني التدخل غير المشروع بالاتصالات التي تجري عبر شبكات الاتصال، سواء أكان هذا التدخل على صورة اعتراض للرسائل الإلكترونية والمعلومات المتبادلة عبر الشبكة المعلوماتية، أو إعاقتها أو تحويرها أو شطب محتوياتها، وقد يأتي أيضاً على صورة التشويش

(1) المادة (3) من اتفاقية بودابست لعام 2001:
https://rm.coe.int/budapest-convention-in-arabic/1680739173

على الموجات المعتمدة لإتمام عملية الاتصال مع الغير وذلك من خلال استخدام الانبعاثات الكهرومغناطيسية بصورة مسيئة، الأمر الذي يؤدي إلى تعطيل الحاسب الآلي عن أداء وظائفه [1].

وبصيغة بسيطة يرى الباحث بأنه من الممكن أن نشبه أفعال الإعتراض غير القانوني بالتنصت على مكالمة هاتفية، بحيث أن المعترض بمجرد قيامه بفعل الإعتراض يمكن له أن يطلع على محتوى الإتصال القائم داخل نظام حاسب آلي واحد أو بين نظامين مختلفين عبر الشبكة، أو بين عدة أنظمة مرتبطة بشبكة اتصالات، ولعل الوسيلة الأبرز لمعرفة المعترض لمحتوى الاتصال هو من خلال استخدام الموجات الكهربائية الصادرة عن جهاز الحاسوب بصورة غير مشروعة مما يساعده على جمع المعلومات عن بُعد.

ويؤدي اعتراض المعلومات إلى منع وصولها إلى المنوي إرسالها إليها، سواء أكان المعترض قد تمكن من معرفة ماهيتها ومحتواها أم لم يتمكن، وسواء أدى ذلك إلى محو أو إتلاف أو تحوير الرسالة أم لو يؤدِ [2].

المطلب الثاني
أركان الجريمة

تقوم هذه الجريمة على الأركان العامة للجريمة شأنها كشأن باقي الجرائم، لذا سنتناول في هذا المطلب الحديث عن أركان جريمة الاعتراض غير القانوني:

---

(1) العمايرة، منذر عبدالرزاق (2012). مدى الحماية الجنائية للمعلومات عبر الحاسوب والإنترنت. (أطروحة دكتوراه غير منشورة)، جامعة عمان العربية، عمان، الأردن، ص 190.

(2) العمايرة، منذر عبدالرزاق، المرجع نفسه، ص 191.

الفرع الأول: الركن الشرعي

موقف المشرّع الأردني إزاء أفعال الاعتراض غير القانوني للمعلومات والبيانات يتمثل بتجرميها بعدة مواضع من القانون، فبالرجوع لقانون الاتصالات رقم 13 لسنة 1995 جاءت المادة (76) الخاصة بالرسائل المنقولة عبر شبكات الاتصال ونصت على ما يلي: " كل من اعترض أو اعاق أو حور أو شطب محتويات رسالة بواسطة شبكات الاتصالات أو شجع غيره على القيام بهذا العمل يعاقب بالحبس مدة لا تقل على شهر ولا تزيد على ستة أشهر أو بغرامة لا تزيد على (200) دينار أو بكلتا العقوبتين" [1].

كما جاءت المادة (80/أ) من القانون ذاته لتجريم فعل اعتراض الموجات والتي تنص على ما يلي: أ . كل من قام متعمدا باي اجراء لاعتراض موجات راديوية مخصصة للغير أو بالتشويش عليها أو بقطعها يعاقب بالحبس مدة لا تقل عن ستة أشهر أو بغرامة لا تقل عن (5000) دينار ولا تزيد على (25000) دينار أو بكلتا هاتين العقوبتين. [2]

وبالنظر للمادة (5) من قانون الجرائم الإلكترونية رقم 27 لسنة 2015 والتي جاء نصها كما يلي: يعاقب كل من قام قصدا بالتقاط أو باعتراض أو بالتنصت أو اعاق 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 [3].

---

(1) المادة (76) من قانون الاتصالات رقم 13 لسنة 1995.

(2) المادة (80) من قانون الاتصالات رقم 13 لسنة 1995.

(3) المادة (5) من قانون الجرائم الإلكترونية رقم 27 لسنة 2015.

ويلاحظ أن المشرّع الأردني عقد الاختصاص في تجريم أفعال الاعتراض غير القانوني في أكثر من في أكثر من قانون، ولعل ذلك يرجع إلى حرص المشرّع على تجريم هذا الفعل كونه يرتب آثاراً إجرامية خطيرة تعود بالضرر الكبير على المجني عليهم كون أن معلوماتهم التي يحرصون على الحفاظ على سريتها وخصوصيتها قد أصبحت في متناول شخص يمكن له ان يستغلها لغايات إجرامية أو أن يبتزّهم بها.

الفرع الثاني: الركن المادي

يتحقق النشاط المادي لهذا الشكل من الجريمة بتوافر فعل الإعتراض للرسائل المنقولة عبر شبكات الاتصال أو اعتراض الموجات الراديوية أو اعتراض كل ما هو مرسل عبر الشبكة المعلوماتية أو عن طريق أي نظام معلومات، و يستوي أن يكون الاعتراض من خلال الالتقاط والذي يعرف بأنه مشاهدة البيانات أو المعلومات أو الحصول عليها، أو عبر التنصت والذي يعني الاستماع أو قراءة رسالة ممن لا يملك الحق في ذلك، والاعاقة وهي تأخير وصول الرسالة إلى الجهة المرسلة إليها أو منع وصولها كلياً، والتحوير أي الذي يعني تغيير أو تعديل محتوى الرسالة بشكل كلي أو جزئي ، وآخرا الشطب و هو الاتلاف الكامل لمحتوى الرسالة سواء بالمحو أو التدمير ، أو تشويهها على نحو لا يجعلها غير صالحة للاستعمال[1].

الفرع الثالث: الركن المعنوي

تعتبر جريمة الاعتراض غير القانوني من الجرائم القصدية التي تتطلب توافر القصد الجنائي بشقيه العلم والإرادة، فلا بد أن الجاني يعلم وهو في صدد فعل الاعتراض أنه بقوم بالتنصت على المكالمات مثلاً والكشف على عملية نقل المعلومات السرية وذلك بغير وجود أي رضا من جهات

(1) العتوم، محمد شبلي، مرجع سابق، ص42.

الاتصال، ومن جهة أخرى يجدر الإشارة أنه فيما لو كان هذا المعترض كان مكره على إتيان أفعال الاعتراض من قبل أشخاص آخرين مثلا لما لديه من مهارة تقنية وفنية أو كان دخوله لشبكة الاتصال غير إرادي فهنا انتفى القصد الجنائي وبذلك لا نكون أمام جريمة يعاقب عليها القانون. [1]

(1) ساسي، ريم، مرجع سابق، ص65.

المبحث الثالث

صعوبات اكتشاف جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية

إن الخصائص الفريدة التي تتسم بها الجرائم الإلكترونية جعلها تتميز عن الجرائم التقليدية وبما أن الجريمة موضوع هذه الدراسة كما ذكرنا سلفاً هي تمثل صورة من صور الجرائم الإلكترونية العديدة فتنطبق عليها ذات الخصائص هذا من جهة ، أما من جهة أخرى فإن هذه الخصائص ذاتها تلعب دور العائق الصعب أو الحائل الذي يواجه أصحاب الاختصاص في عملية اكتشاف جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية ويرجع ذلك لعدة أسباب لا يمكن حصرها لذا سنحاول في هذا المبحث توضيح أو بيان تلك الصعوبات على النحو التالي:

المطلب الأول

فقدان الآثار التقليدية للجريمة

إن شأن جريمة انتهاك سرية المعلومات المرتكبة بالوسائل الإلكترونية كشأن باقي الجرائم الإلكترونية حيث أنها تبقى مجهولة ما لم يتم الإبلاغ عنها لوحدة مكافحة الجرائم الإلكترونية أو للجهات المختص أمرها بهذا النوع من الجرائم من قبل المجني عليه، والجدير بالذكر أيضا أن الجرائم الإلكترونية ليست كالجرائم العادية فهي لا تصل للجهات المعنية بطريقة اعتيادية كونها لا تخلّف آثاراً مادية ملموسة كتلك التي تخلّفها الجرائم العادية مثل الكسر في جريمة السرقة والتي تعتبر من الجرائم التقليدية [1].والمقصود بالآثار المادية في هذا الصدد هو الأثر المادي الملموس و الذي يتم إدراكه بواسطة الحواس كرؤية جثة المجنى عليه كما هو الحال في جريمة القتل أو رؤية السلاح الذي تم بواسطته ارتكاب الجريمة .

---

(1) حجازي، عبد الفتاح بيومي (1995). الدليل الجنائي والتزوير في جرائم الكمبيوتر –دراسة متعمقة في جرائم الحاسب الآلي والإنترنت. مصر، بهجات للطباعة والنشر، ص41.

ويرى الباحث أن الصعوبة أو الإشكالية التي تثار هنا هو أن جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية لا تتم إلا بإتيان أفعال أو أنشطة تتمثل في الاختراق و الدخول غير المصرح به أو استخدام البرامج المقرصنة أو إدخالها لجهاز المجني عليه و القيام بالكشف على تلك المعلومات السرية الذي يحتويها الجهاز أو النظام المعلوماتي أو الموقع الإلكتروني ، وأن مثل تلك الأفعال أو الأنشطة ترتكب في ظل فضاء إلكتروني لا يمكن إدراكه من قبل الحواس عكس الجرائم التقليدية الأمر الذي يزيد صعوبة في اكتشافها من قبل المختصين .

المطلب الثاني
عدم الإبلاغ عن الجريمة للجهات المختصة

ويظهر ذلك غالباً بالنسبة للجهات المالية كالمصارف والبنوك والمؤسسات الاقتصادية الكبيرة، إذ أن هذه الجهات المجني عليها تفضل في الغالب الأعم أن تحرص على كتمان الجرائم الإلكترونية والتي منها جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية وعلة ذلك كي تتفادى هذه الجهات الآثار السلبية التي ترتبها عملية الإفصاح عن هذه الجرائم، كتضاؤل الثقة بها من قبل العملاء المتعاملين معها، وبيان عجز الشركة أو المؤسسة عن تحقيق الأمان الكافي لمعلومات العملاء لديها [1].

فالابلاغ عن جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية من قبل الجهات المذكورة أعلاه و غيرها من المعتدى عليهم بهذه الجريمة ليس بالأمر الهين وهذا من وجهة نظر الباحث ، إذ انها تفضل الاحجام عن الابلاغ عن الجريمة عن الابلاغ عنها و انتشار ذلك بين افراد المجتمع لأن

(1) الشمري، غانم مرضي (2016). الجرائم الإلكترونية –ماهيتها – خصائصها – كيفية التصدي لها قانوناً. عمان، دار الثقافة للنشر والتوزيع، ص175

ذلك قد يؤدي إلى ضعف الثقة بالجدار الامني لتلك المؤسسة أو المنشأة و خسارتها لعملاءها و قد يصل الامر إلى إنهيارها كلياً .

المطلب الثالث
صعوبة الوصول إلى الجاني

تعرفنا في هذه الدراسة سابقاً أن المجرم المعلوماتي هو مجرم ذكي من الناحية التقنية وباستغلال هذه الميزة فإنه يتعمد إخفاء جريمته، ويتم ذلك من خلال إزالة آثار تلك الجريمة عن طريق التلاعب بقواعد البيانات والقوائم في جهاز الكمبيوتر والبرامج، بالإضافة إلى انتحال شخصية أخرى حتى لا يتمكن أحد من التعرف عليه في حال اكتشاف الجريمة [1] أو من خلال تغيير المعرف الرقمي (IP ADDRESS) الخاص بالجهاز المستخدم لإتمام جريمة انتهاك سرية المعلومات [2].

وبرأي الباحث أن أغلب الجرائم التي ارتكبت ضد سلامة و سرية المعلومات هي جرائم مجهولة من حيث مرتكبها ، حيث أنه إذا أردنا أن نعد الاحصائيات حول هذا الموضوع فسنجد الرقم كبيراً ، فالجهل بمرتكب الجريمة قد يشكل عائقاً أمام تلك الجهات المختصة في ملاحقة وضبط الجريمة فلا يمكن أن يتم ملاحقة جريمة أو ممارسة أي إجراء قانوني لمجازاة مرتكب الجريمة دون معرفة هويته.

المطلب الرابع
نقص ميزة وخبرة الشرطة وجهات الادعاء والقضاء

إن من أشد الصعوبات التي تواجه عملية اكتشاف جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية باعتبارها جريمة إلكترونية هو وجود نقص واضح في الخبرة التقنية لدى أجهزة الضبط

---

(1) بشير، عادل حامد، مرجع سابق، ص35-36.

(2) انظر الموقع الإلكتروني، https://ar.wikipedia.org/wiki/، يوم الاطلاع عليه: 2021/11/15.

القضائي وجهات الإدعاء والقضاء في مجال الجرائم الإلكترونية خاصة في الدول النامية وحديثة العهد بوسائل التكنولوجيا [1] ، ويرى الباحث أنه من الممكن القول بأن الأردن هي دولة حديثة العهد في المجال التكنولوجي حيث يلاحظ أن هناك نقصاً في الخبرة لدى أفراد وحدة مكافحة الجرائم الإلكترونية خاصة ان الجريمة الإلكترونية هي جريمة تتنوع بأنماط و أساليب مختلفة في ارتكابها وكما أنه هي عبارة عن جريمة تعتمد على المهارة التقنية في عملية كشفها.

كما يرى الباحث أن هذه الخبرة التقنية لا تأتي دون تدريب متخصص في مجال تكنولوجيا المعلومات وشبكات الاتصال يقام من قبل جهة مختصة تتوافر لديها الخبرة الكافية في مجال التدريب ، على أن يكون التدريب بشكل مستمر ومواكب لتطور التكنولوجيا ، لأن الجرائم الإلكترونية والتي منها جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية في تطور سريع و متزايد .

المبحث الرابع

صعوبات الإثبات الجنائي لجريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية

إلى جانب الصعوبات التي تواجه عملية إكتشاف جريمة إنتهاك سرية المعلومات عبر الوسائل الإلكترونية ، يتضح لنا ومن خلال دراستنا هذه أنه أيضاً تظهر بعض الصعوبات التي تواجه عملية إثبات تلك الجريمة من قبل المختصين بذلك بعد اكتشافها ، فالاثبات الجزائي لا يمكن أن يتحقق دون وجود دليل وحيث أن هذه الصعوبات تختلف عن صعوبات الاكتشاف المذكورة في المبحث السابق فسنوضحها في هذا المبحث ضمن المطالب التالية :

---

(1) الشمري، غانم مرضي، مرجع سابق، ص173.

المطلب الأول
عدم ظهور الدليل المادي

في حال إكتشاف جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية فإنه لابد من وجود أدلة إثبات تثبت قيام كافة أركان هذه الجريمة ، والجدير بالذكر هنا أن جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية تتم في بيئة أو إطار لا يتصل بالعالم المادي الملموس ألا وهو العالم الافتراضي المتمثل بالشبكة المعلوماتية وما تحتويه من مواقع إلكترونية وأنظمة معلوماتية، ففي الجرائم التقليدية نلاحظ أن دليل الإثبات يكون مرئياً كالسلاح الناري أو الأداة الحادة التي ستعمل في القتل أو الضرب، أما في جريمة انتهاك سرية المعلومات فالدليل غير مرئي يتمثل بالمعالجة الآلية للبيانات أو من خلال تشفير تلك البيانات و المعلومات التي بحوزة الجاني أو من خلال استخدام النبضات الإلكترونية [1]، وهي عبارة عن عمليات تقنية لا يمكن إدراكها بسهولة و يسر .

المطلب الثاني
سهولة إخفاء الدليل

يمكن للجاني في جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية الدخول لأي موقع إلكتروني أو نظام معلوماتي والاطلاع على ما يحتويه من معلومات سرية غير مخول له الاطلاع عليها ومن ثم الخروج من ذاك الموقع أو النظام ومحو جميع الأدلة التي مكّنته من إتمام جريمته والتي يمكن من خلالها الاستدلال على هويته الحقيقية، مثل تغيير الرقم التعريفي للجهاز المستخدم في ارتكاب الجريمة وغير من تلك الأساليب التي يستطيع فعلها جراء خبرته الفنية والعقلية.

---

(1) الحمداني، ميسون خلف (2016). مشروعية الأدلة الإلكترونية في الاثبات الجنائي، مجلة البحوث والدراسات العربية، العدد 65، ص214.

وبرأي الباحث أنه حتى وفي حالة كشف الجريمة طالما أنه لا يوجد ما يثبت وقوع الجريمة أو ارتكابها بأدلة قانونية مشروعة فلا يمكن محاكمة الجاني عم اقترفه ، فالمجرم المعلوماتي دائما يحرص كل الحرص على أنه لو تم اكتشاف الجريمة لأي سبب كان فلا يوجد ما يثبتها لأنه أستخدم ذكاءه و دهاءه في إخفاء هذا الدليل ليفلت من العقوبة و الجزاء .

المطلب الثالث
صعوبة الوصول إلى الدليل

يحرص الجاني بشكل شديد على ضرورة عدم ضبط أي دليل يدينه لذلك يلجأ إلى زيادة الصعوبة أمام قدرة جهات التحري والتحقيق في ضبط تلك الأدلة وذلك من خلال استخدامه كلمات مرور أو استخدام تقنيات التشفير [1]. فالمجرم المعلوماتي وهو في صدد ارتكابه للجريمة يحيط نفسه بتدابير أمنية وقائية تزيد من صعوبة إثبات جريمته حال اكتشافها من قبل المختصين.

ويقصد الباحث في هذا المطلب أنه حتى وإن وصل العلم للجهات المختصة في ضبط وملاحقة جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية أن هنالك دليل يثبت قيام أو وقوع الجريمة فلا يمكن لهم الوصول له إذا كان المجرم المعلوماتي قد أحاطه بتقنيات أو وسائل حماية هدفها إبقاءها بعيداً عن أيدي الجهات أعلاه لكي لا تثبت الجريمة و يتم مجازاته وفق القانون .

وفي الخلاصة يرى الباحث بأنه لا يمكن حصر الصعوبات التي تواجه سواء عملية إكتشاف أو إثبات جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية كونها تمتاز بسمة التطور المتسارع والتنوع لذا فلا يمكن التنبوء بما ستكون عليه حال هذه الصعوبات في المستقبل .

---

(1) بشير، عادل حامد، مرجع سابق، ص44.

الفصل الخامس
الخاتمة، النتائج والتوصيات

وبعد الإنتهاء من دراسة جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية كصورة من صور الجرائم الالكترونية من حيث بيان ماهية الجرائم الإلكترونية وخصائصها ومن ثم البحث في البنيان القانوني لجريمة إنتهاك سرية المعلومات عبر الوسائل الإلكترونية و التعرف على طبيعة كل صورة لهذه الجريمة توصل الباحث من خلال هذه الدراسة إلى النتائج والتوصيات التالية:

أولاً: النتائج

1- تعد جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية واحدة من أهم أشكال الجريمة الإلكترونية في الوقت الحاضر التي تتعرض لها العديد من القطاعات التي اعتمدت على ظاهرة تطور تكنولوجيا المعلومات في سبيل تسيير أعمالها.

2- يتضح من خلال هذه الدراسة أيضاً أن المجرم المعلوماتي هو مجرم يختلف عن ذاك المجرم التقليدي، كونه يتميز عنه بالمعرفة التقنية العالية لتوظيفها في المجال الإجرامي، أو ما يعرف الذكاء المعلوماتي.

3- خلصت هذه الدراسة إلى ضرورة الفصل بين كل من السرية والخصوصية، على اعتبار إن السرية هي أكثر شمولية من الخصوصية التي تتصل بالمعلومات الشخصية، وبالتالي لا يمكن القول بأن الحق في الخصوصية حق يصل نطاقه إلى سقف المعلومات البنكية أو العسكرية مثلاً.

4- وضحت هذه الدراسة المقصود بالمعلومة من الجانب القانوني والجانب التقني وطبيعتها وأنواعها، وماهية الشروط التي يجدر توافرها لتكون محلاً يصلح توفير الحماية الجزائية له.

5- بينت هذه الدراسة ماهية الوسائل الإلكترونية وخصائصها، كون هي الوسيلة المستخدمة في ارتكاب الجرائم الإلكترونية ومنها جريمة انتهاك سرية المعلومات.

6- تتخذ جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية العديد من الصور، فكل صورة تتطلب قيام ركن مادي مختلف عن الاخرى، لكن النتيجة الجرمية هي واحدة.

7- إن الأساس القانوني لجريمة انتهاك سرية المعلومات بصورها المتعددة هي نصوص المواد 3 و4 و5 و12 من قانون الجرائم الإلكترونية رقم 27 لسنة 2015، كما أتاح نص المادة 15 من ذات القانون تجريم أي فعل من شأنه أن ينال من سرية المعلومات وهو مجرم وفق قانون آخر في حال تم بالصورة الإلكترونية وبذات العقاب.

8- إن النصوص التي عالجت أفعال الانتهاك الالكتروني لسرية المعلومات هي نصوص عامة، وليست خاصة بتلك الأفعال، فنجد انه ذات النص قد ينطبق على أكثر من فعل مشكل لأكثر من جريمة مما قد يخالف مبدأ الشرعية الجزائية.

9- إن عملية ضبط وملاحقة واثبات جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية، تتسم بالصعوبة بعض الشيء كونها من الجرائم التي تنطوي على الجانب التقني أكثر من المادي، ولذلك يعتمد في اكتشافها على الدراية العالية بالأمور التقنية من قبل أصحاب الاختصاص في ملاحقتها.

ثانياً: التوصيات

1- ضرورة تعديل قانون الجرائم الإلكترونية رقم 27 لسنة 2015، وذلك من خلال ايراد نصوص واضحة لمعالجة جريمة انتهاك سرية المعلومات بصورها المتعددة.

2- ضرورة توحيد النصوص التي تجرم افعال جريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية ضمن تشريع موحد.

3- ضرورة تعديل المادة الثانية من قانون الجرائم الإلكترونية رقم 27 لسنة 2015 لإضافة تعريف محدد لمصطلح المعلومات السرية.

4- العمل على تعديل قانون الأمن السيبراني رقم (16) لسنة 2019 كون أن طابعه هو طابع تنظيمي لا تجريمي، ولا يحقق الغاية المرجوة من سنة، وهذا التعديل يكون إما بإضافة نصوص تجريمية له أو من خلال دمجه بقانون الجرائم الإلكترونية للتخلص من ازدواجية التشريع باعتبارهما قانونين يسعيان لذات الهدف.

5- يجب العمل على إعداد وعقد دورات تدريبية من قبل مديرية الأمن العام لأفراد وحدة مكافحة الجرائم الإلكترونية، تهدف إلى السمو بالمستوى التقني لديهم ليساعدهم في سرعة اكتشاف الجريمة الإلكترونية وضبطها دون أية صعوبة تقنية قد تواجههم أثناء ذلك.

6- يرى الباحث بأنه من الضرورة تشديد العقوبات المفروضة على الأفعال المكونة لجريمة انتهاك سرية المعلومات عبر الوسائل الإلكترونية وذلك لردع هذا النوع من الجرائم.

قائمة المراجع

أولاً: القرآن الكريم.

ثانياً: الكتب

إبراهيم، خالد ممدوح (2007). **الجرائم المعلوماتية**، دار الفكر الجامعي، الإسكندرية.

إبراهيم، خالد ممدوح (2008). **أمن الجريمة المعلوماتية**، ط1، الدار الجامعية، الإسكندرية.

اسماعيلي، يامنة، وصابر، قشوش (2017). علم **النفس الجنائي**، دار اليازوري للنشر والتوزيع، عمان.

بشير، عادل حامد (2021). **الاثبات الجنائي للجريمة الإلكترونية**، دار النهضة العربية، القاهرة.

الحوامدة، لورنس سعيد (2017).**الجرائم المعلوماتية أركانها وآلية مكافحتها** ، جامعة طيبة، كلية الحقوق ، السعودية.

حافظ، مجدي محب (1997). **الحماية الجنائية لأسرار الدولة – دراسة تحليلية تأصيلية لجرائم الخيانة والتجسس في القانون المصري والشريعة الاسلامية والقانون المقارن**، الهيئة المصرية العامة للكتاب، الإسكندرية.

حجازي، عبد الفتاح بيومي (1995). **الدليل الجنائي والتزوير في جرائم الكمبيوتر –دراسة متعمقة في جرائم الحاسب الآلي والإنترنت**، بهجات للطباعة والنشر، مصر.

حجازي، عبد الفتاح بيومي (2006). **مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي**، دار الفكر الجامعي، الإسكندرية.

حجازي، عبد الفتاح بيومي (2009). **الجرائم المستحدثة**، منشأة المعارف، الإسكندرية.

حسني، محمود نجيب (1985). **شرح قانون العقوبات، القسم العام**، دار النهضة العربية، القاهرة.

الحسيني، عمار عباس (2017). **جرائم الحاسوب والإنترنت المعلوماتية (الجرائم المعلوماتية)**، منشورات زين الحقوقية، بيروت.

الدربين، عبد العالي، واسماعيل، محمد صادق (2012). **الجرائم الإلكترونية**، ط1، المركز القومي للإصدارات القومية، القاهرة.

الرحباني، عبير شفيق (2020). **الجرائم الإلكترونية ومخاطرها**، دار الثقافة للنشر والتوزيع، عمان.

الشمري، غانم مرضي (2016). **الجرائم الإلكترونية –ماهيتها – خصائصها – كيفية التصدي لها قانوناً**، دار الثقافة للنشر والتوزيع، عمان.

العبيد، فهد عبدالله (2016). **الإجراءات الجنائية المعلوماتية**، دار الجامعة الجديدة، الإسكندرية.

العتوم، محمد شبلي (2021). **جرائم تكنولوجيا المعلومات " النظرية العامة للجرائم الإلكترونية"**، دار الثقافة للنشر والتوزيع، عمان.

العريان، محمد علي (2004). **الجرائم المعلوماتية**، دار الجامعة الجديدة للنشر، الإسكندرية.

الفار، عبد القادر (2016). **المدخل لدراسة العلوم القانونية –مبادئ القانون –النظرية العامة للحق**، دار الثقافة للنشر والتوزيع، عمان، ط16.

قشقوش، هدى حامد (1992). **جرائم الحاسب الإلكتروني في التشريع المقارن**، دار النهضة العربية، القاهرة.

قورة، نائلة محمد فريد (2005). **جرائم الحاسب الاقتصادية " دراسة نظرية وتطبيقية "**، منشورات الحلبي الحقوقية، بيروت.

الكعبي، محمد عبيد (2009). **الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت**، دار النهضة العربية، القاهرة.

المجالي، نظام توفيق (2020). **شرح قانون العقوبات القسم العام**، ط7، دار الثقافة للنشر والتوزيع، عمان.

مراد، عبدالفتاح (2007). **شرح جرائم الكمبيوتر والإنترنت**، دار الكتب والوثائق المصرية، الإسكندرية.

موسى، مصطفى محمود (2003). **أساليب إجرامية بالتقنية الرقمية**، دار الكتب والوثائق القومية المصرية، مصر.

المومني، نهلا عبد القادر (2008). **الجرائم المعلوماتية**، ط1، دار الثقافة للنشر والتوزيع، عمان.

نمور، محمد سعيد (2019). **أصول الإجراءات الجزائية – شرح لقانون أصول المحاكمات الجزائية**، دار الثقافة للنشر التوزيع، عمان.

النوري، حسين (1974). **سر المهنة المصرفي في القانون المصري والقانون المقارن**، اتحاد المصارف العربية، القاهرة.

ثالثاً: الرسائل والأطاريح الجامعية

بدرة، والي (2019). **المواجهة الاجرائية لجرائم المعلوماتية**، رسالة ماجستير، جامعة محمد بوضياف – المسيلة، كلية الحقوق والعلوم السياسية.

بن سعيد، صبرينة (2015). **حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا " الاعلام والاتصال "**، (اطروحة دكتوراه غير منشورة)، جامعة الحاج لخضر – باتنه، الجزائر.

بن يونس، عمر محمد أبو بكر (2004). الجرائم **الناشئة عن استخدام الإنترنت (الأحكام الموضوعية والجوانب الإجرائية)**، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس.

ساسي، ريم (2016). الحماية **الجنائية لسرية المعلومات الإلكترونية**، رسالة ماجستير، جامعة العربي بن مهيدي – أم البواقي، كلية الحقوق والعلوم السياسية

صورية، بوربابة (2016). **قواعد الأمن المعلوماتي**. (أطروحة دكتوراه غير منشورة). جامعة الجيلالي اليابس. سيدي بلعباس، الجزائر.

عزيزة، رابحي (2018). **الأسرار المعلوماتية وحمايتها الجزائية**. (رسالة دكتوراه منشوره). جامعة ابو بكر بلقايد –تلسمان، الجزائر.

العمايرة، منذر عبد الرزاق (2012). **مدى الحماية الجنائية للمعلومات عبر الحاسوب والإنترنت**. (أطروحة دكتوراه غير منشورة)، جامعة عمان العربية، عمان، الأردن.

فتيحة، رصاع (2012). **الحماية الجنائية للمعلومات على شبكة الأنترنت**. جامعة أبي بكر بلقايد – تلسمان – كلية الحقوق والعلوم السياسية. الجزائر.

الهزاني، محمد ناصر (2018). **المسؤولية الجنائية عن انتهاك قواعد الفضاء السيبراني: دراسة تأصيلية مقارنة بالقانون الإماراتي**، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، كلية العدالة الجنائية – قسم الشريعة والقانون، الرياض.

هلال، آمنة (2015). **الاثبات الجنائي بالدليل الإلكتروني**، رسالة ماجستير، جامعة محمد خيضر –بسكرة، كلية الحقوق والعلوم السياسية.

رابعاً: البحوث

بشرى، غريبي (2021). خصوصية المجرم المعلوماتي ودوافعه، **مجلة نوميروس الأكاديمية**، المجلد الثاني، العدد الثاني.

الحمداني، ميسون خلف (2016). مشروعية الأدلة الإلكترونية في الاثبات الجنائي، **مجلة البحوث والدراسات العربية**، العدد 65.

ربايعة، عبد اللطيف محمود (2016). **الجرائم الإلكترونية (التجريم والملاحقة والإثبات)**، بحث مقدم إلى المؤتمر الأول للجرائم الإلكترونية في فلسطين، جامعة النجاح الوطنية، نابلس.

محمد، رحموني (2018). خصائص الجريمة الإلكترونية ومجالات استخدامها، **مجلة الحقيقة**، المجلد 17، العدد 41.

النوايسة، عبدالإله، والعدوان، ممدوح (2019). جرائم التجسس الإلكتروني في التشريع الأردني – دراسة تحليلية، **دراسات علوم الشريعة والقانون –الجامعة الأردنية**، عدد1، ملحق 1.

خامساً: التشريعات الأردنية:

قانون الاتصالات رقم 13 لسنة 1995.

قانون الجرائم الإلكترونية رقم 27 لسنة 2015.

قانون العقوبات رقم 16 لسنة 1960.

قانون حماية أسرار ووثائق الدولة رقم 50 لسنة 1971.

المذكرة الايضاحية لقانون جرائم أنظمة المعلومات لسنة 2010.

سادساً: المواقع الإلكترونية

- https://www.almaany.com
- https://ar.wikipedia.org/wiki
- https://www.elshami.com
- https://rm.coe.int/budapest-convention-in-arabic/1680739173
- https://www.psd.gov.jo
- https://www.almadenahnews.com/article/899065

﴿ دَعۡوَىٰهُمۡ فِيهَا سُبۡحَٰنَكَ ٱللَّهُمَّ وَتَحِيَّتُهُمۡ فِيهَا سَلَٰمٞۚ وَءَاخِرُ دَعۡوَىٰهُمۡ أَنِ ٱلۡحَمۡدُ لِلَّهِ رَبِّ ٱلۡعَٰلَمِينَ ١٠ ﴾

[سورة يونس, ١٠]