جـامـعـة الـشـرق الأوسـط
MIDDLE EAST UNIVERSITY

المشكلات العملية والقانونية للجرائم الإلكترونية
دراسة مقارنة

The Practical and Legal Problems of Cybercrime
A Comparative Study

إعداد الطالب

عبد الله دغش العجمي

إشراف

الدكتور أحمد اللوزي

قدمت هذه الرسالة استكمالاً للحصول على درجة الماجستير في القانون العام

جامعة الشرق الأوسط

2014م

تفويض

أنا الطالب **عبد الله دغش العجمي** أفوض جامعة الشرق الأوسط بتزويد نسخ من رسالتي المعنونة بـــ "المشكلات العملية والقانونية للجرائم الإلكترونية – دراسة مقارنة" للمكتبات الجامعية أو المؤسسات أو الهيئات أو الأشخاص المعنية بالأبحاث والدراسات العلمية عند طلبها.

الاسم: عبد الله دغش العجمي

التوقيع:

التاريخ: 27 / 5 /2014م

قرار لجنة المناقشة

نوقشت هذه الرسالة وعنوانهـــا "المشكلات العملية والقانونية للجرائم الإلكترونية – دراسة مقارنة".

وأجيزت بتاريخ 27 / 5 /2014م

أعضاء لجنة المناقشة		التوقيع
أ- الدكتور محمد الجبور	رئيساً	
الدكتور أحمد اللوزي	مشرفاً	.....
الدكتور صالح حجازي	عضواً خارجياً	.....

شكر وتقدير

أتقدم بوافر الشكر والتقدير إلى أستاذي المشرف الدكتور أحمد اللوزي على ما بذله من جهد مخلص، فقد كان لتوجيهاته ونصائحه الأثر في أن تكون هذه الرسالة بهذه الصورة.

والشكر الموصول إلى عضويْ لجنة المناقشة، وسيكون لملاحظاتهم القيّمة أثراً واضحاً في تصويب هذه الرسالة.

الباحث

الإهداء

إلى والديّ العزيزين
حفظهما الله ورعاهما وأطال في عمرهما

إلى زوجتي وأولادي . . . .
حفظهم الله سنداً وذخراً لي

إلى وطني الغالي ....
دولة الكويت

أهدي هذا الجهد المتواضع

الباحث

قائمة المحتويات

الموضوع **الصفحة**

الموضوع **الصفحة**

الموضوع **الصفحة**

المشكلات العملية والقانونية للجرائم الإلكترونية
دراسة مقارنة

إعداد الطالب
عبد الله دغش العجمي

إشراف الدكتور
أحمد اللوزي

الملخص

إن انتشار وتوسع إطار الجرائم الإلكترونية أصبح أمراً واقعاً في ظل الثورة المعلوماتية والتطور الهائل في وسائل الاتصال الحديثة، إلا أن هناك مشكلات موضوعية وإجرائية تثيرها الجرائم الإلكترونية على الصعيدين التشريعي والعملي.

وقد تصدى المشرّع الأردني لتجريم وعقاب الصور التي ترتكب بها الجرائم الإلكترونية وذلك بموجب قانون جرائم أنظمة المعلومات المؤقت رقم (30) لسنة 2010م، بخلاف المشرّع الكويتي الذي لم يتدخل حتى هذه اللحظة لا بسن قانون خاص بالجرائم الإلكترونية ولا بإجراء تعديل تشريعي على قانون الجزاء بإضافة نصوص تعالج هذا النوع من الجرائم، ونظراً للمشكلات التي تثيرها الجرائم الإلكترونية فقد جاءت هذه الدراسة لبيان طبيعة هذه المشكلات والحلول التشريعية والعملية لمواجهتها.

وقد خرج الباحث بعدد من النتائج، ومن أهمها: أن القواعد التقليدية في التشريع الجزائي الكويتي غير كافية لمواجهة الجرائم الإلكترونية وما تثيره من مشكلات، وأما أهم توصيات هذه الدراسة فهي: دعوة المشرّع الكويتي للإسراع بسن قانون خاص بالجرائم الإلكترونية، أو استحداث فصل خاص بها في قانون الجزاء، وكذلك دعوة المشرّعان الكويتي والأردني لمواجهة تحديات ومشكلات الجريمة الإلكترونية، سواء أكانت الموضوعية منها أم الإجرائية.

The Practical and Legal Problems of Cybercrime

A Comparative Study

By
Abdallah Daghash Al-Ajami

Supervisor
Dr. Ahmad Al-Louzi

Abstract

The proliferation and expansion of the framework of cyber crime has become a reality in the light of the information revolution and the enormous development in the modern means of communication, despite the existence of laws for electronic transactions and other crimes electronic include penalties for each offender, but that there are problems of substantive and procedural posed by cyber crime at both the legislative and practical.

Has confronted the Jordanian legislator to criminalize and punish the pictures that are committed by cyber crime and that under the law of crimes, information systems, temporary number (30) for the year 2010, other than the Kuwaiti legislature, which did not intervene until this moment not to enact a special law offenses electronic and do not make a legislative amendment to the Penal Code by adding texts dealing with this type of crime, and because of the problems posed by cyber crime has made the study of the nature of these problems and the solutions the legislative process and to confront them.

The study has come out with a number of results, and most important: that the traditional rules of criminal legislation in Kuwait is not sufficient to cope with cyber crimes and raises problems, and the most important recommendations: Call Kuwaiti legislature to expedite the enactment of a law on e-crime, or the introduction of a special chapter in the Penal Code, as well as an invitation Kuwaiti and Jordanian lawmakers to address the challenges and problems of cyber crime, whether substantive or procedural ones.

الفصل الأول
مقدمة عامة الدراسة

تمهيد

تشهد الحياة اليومية تطوراً متسارعاً في مجال تقنية المعلومات، وبما أن البيئة الإلكترونية لها رواد عديدون جداً، فقد وجد بعض المجرمين التقنيين في هذه البيئة مجالاً خصباً لارتكاب صور متعددة من الجرائم الإلكترونية عبر وسائل الاتصال الحديثة، ومن أهمها في وقتنا الحاضر "الإنترنت" أو "البريد الإلكتروني" والكمبيوتر، ووسائل التواصل الاجتماعي، ومنها: تويتر، والواتسب، والفيس بوك.

ولا شك أن هذه الجرائم ما ولدت إلا نتيجة إساءة استخدام وسائل الاتصال الإلكترونية التي ظهرت على الساحة الدولية، ولم يكن لها وجود من قبل.

لقد تباينت الصور الإجرامية لظاهرة الجرائم الإلكترونية، وتشعبت أنواعها، فمنها ما يتصل بالاعتداء على ذات النظام الإلكتروني، ومنها ما يتعلق بالاعتداء على المعلومات، ومنها أيضاً الاحتيال الإلكتروني، والتزوير الإلكتروني، وجرائم الاعتداء على الحق في الخصوصية، وجرائم الاعتداء على التحويلات المالية الإلكترونية.

وتضم الجرائم الإلكترونية أشكالاً أخرى يصعب حصرها، ولعلنا نشهد تطوراً ملحوظاً على أساليب هذه الجرائم والشاملة على نشر وصناعة الفايروسات والاختراقات والفرصنة وتعطيل الأجهزة وغيرها.

إن الجرائم الإلكترونية ظاهرة عالمية ونوع مختلف ومغاير تماماً عن أشكال الجرائم الأخرى التي تهدد المجتمع الكويتي والأردني بصفة خاصة، والمجتمع العربي بصفة عامة،

بل وتهدد جميع بلدان العالم، وهذا يتطلب وجود تشريعات رادعة للحد من المشكلات القانونية والعملية التي تثيرها هذه الجرائم.

في الأردن أظهرت أرقام رسمية لمديرية الأمن العام أنه تم تسجيل (3649) جريمة تتعلق بتكنولوجيا المعلومات خلال العام الماضي 2012م، وبلغ عدد المتورطين فيها (186) شخصاً بينهم (168) أردنياً و (18) من جنسيات أجنبية، وبحسب البيانات فإن من بين القضايا المضبوطة قضايا انتحال شخصية "تشهير إلكتروني" وبلغت (43) قضية ألقي القبض على (38) أردنياً تورطوا في تنفيذها، وتهديد إلكتروني وبلغ عددها (25) قضية قبض على (15) أردنياً على خلفيتها، أما جرائم التشهير والابتزاز الإلكتروني فبلغت (74) قضية ألقي القبض على (52) أردنياً على خلفيتها، وبلغت جرائم الاحتيال المالي الإلكتروني (38) قضية ألقي القبض على (32) شخصاً بينهم (2) من جنسية أجنبية والباقي أردنيون، كما بلغت جريمة سرقة البريد الإلكتروني (25) ألقي القبض على (14) من منفذيها وجميعهم أردنيون، كما سجلت قضيتان تتعلق بإنشاء موقع وهمي وألقي القبض على اثنين من الجنسية الأردنية، كما سجلت قضية سرقة بيانات إلكترونية تتعلق بسيرفرات، كما تم تسجيل أربع قضايا في مجال المعاملات المصرفية الإلكترونية، وألقي القبض على أربع أشخاص في هذا المجال[1].

وقد أصدر المشرّع الأردني قانون جرائم أنظمة المعلومات المؤقت رقم (30) لسنة 2010م والذي أسس لتجريم الأفعال التي تستهدف نظم ووسائط وشبكات المعلومات، والآخر على خلاف ذلك لدى المشرّع الكويتي، إذ يوجد فراغ تشريعي في الكويت بخصوص هذه المسألة؛ مما أثار معه مشكلات قانونية وعملية وتحديات في مواجهة الجرائم الإلكترونية،

---

[1] الصمادي، حازم (2013). الجرائم الإلكترونية في التشريع الأردني، مقال منشور في النشرة القضائية التي تصدر عن المجلس القضائي الأردني، كانون الثاني، ص2.

وهذا ما دفع بالباحث إلى دراسة هذه المشكلات في ضوء النقص التشريعي في التشريع الجزائي الكويتي.

مشكلة الدراسة

إن التطور التقني لأساليب ارتكاب الجرائم وخصوصاً تلك التي تتم عبر الإنترنت والحاسوب ووسائل التواصل الاجتماعي، تتطلب من سلطات إنفاذ القانون أن تتعامل مع أشكال مستحدثة من الأدلة في مجال الإثبات الجنائي، لذلك تكمن مشكلة الدراسة في كيفية تقديم دليل رقمي إلكتروني مقبول وذي حجية أمام القاضي الجزائي.

كما تثور إشكالية أخرى تتعلق بمدى كفاية القواعد التقليدية في التشريع الجزائي الكويتي لمواجهة المشكلات الناجمة عن الجرائم الإلكترونية في ظل الفراغ التشريعي بخصوص التنظيم القانوني لهذا النوع من الجرائم في التشريع الكويتي.

كما تثور إشكالية تتعلق بطبيعة المشكلات الموضوعية والإجرائية التي يثيرها هذا النوع من الجرائم، ومدى كفاية معالجة المشرّع الأردني لمواجهة مثل هذه المشكلات.

أهداف الدراسة

تهدف هذه الدراسة إلى التعريف بماهية الجريمة الإلكترونية، وبالمشكلات الموضوعية والإجرائية التي تثيرها، كذلك تهدف إلى المساهمة في إيجاد الحلول للمشكلات العملية والقانونية في الجرائم الإلكترونية، ومحاولة التعمق في كيفية مجابهتها من خلال التشريعات ومنها التشريع الكويتي والأردني.

وأيضاً تهدف إلى وضع ما توصلت إليه من نتائج وتوصيات بين يدي المشرّع الكويتي على أمل أن نجد أذنا صاغية من المشرّع الكويتي في ضرورة التدخل، ووضع تشريع خاص متكامل يهدف إلى مجابهة الجرائم الإلكترونية، والحد منها، للحفاظ على حقوق

الأشخاص في المجتمع الدولي والداخلي على السواء لسد الثغرات في وجه التطـــور الـــسريع للجرائم الإلكترونية.

أهمية الدراسة

يكتسب موضوع هذه الدراسة أهمية متزايدة بسبب استغلال وسائل الاتصال الحديثـــة من قبل مرتكبي الجرائم لتسهيل ارتكابهم لجرائمهم.

إن لموضوع هذه الدراسة أهمية نظرية وعملية لكونه يمـــس كثيـــراً مـــن مـــصالح المجتمع، كما تظهر أهميته في تحديد مصادر المخاطر التي تهدد النظام الإلكترونـــي ونظـــم الشبكات، وتحديد صور الاعتداء على المعلومات، والأنماط المستجدة للجرائم الإلكترونية، كما تظهر أهمية الموضوع من خلال التعرف على الاتجاهات التشريعية الدولية والإقليمية لحماية المعلومات ونظمها الإلكترونية.

كما تكمن أهمية هذه الدراسة في محاولة إيجاد الحلول للمشكلات التي تثيرها الجرائم الإلكترونية في التشريعين الكويتي والأردني وبالأخص في التشريع الكويتي نظراً لعدم وجود تشريع خاص لهذه الجرائم.

فالمشرّع الكويتي قد يستفيد من هذه الدراسة المتواضعة، وكذلك المشرّع الأردني من خلال التعرف على أكثر المشكلات العملية والقانونية بشقيها الموضوعي والإجرائـــي التـــي تثيرها هذه الجرائم المتجددة بشكل مستمر.

كما أن هذه الدراسة تظهر أهميتها من خلال استفادة الباحثين والقضاة مـــن نتائجهـــا وتوصياتها والبناء عليها وتطويرها لإجراء دراسات معمقة في مجال تقنية المعلومات وقانون الكمبيوتر.

أسئلة الدراسة

1. ما طبيعة المشكلات العملية والقانونية التي تثيرها الجرائم الإلكترونية في واقعنا العملي؟
2. ما مدى ملاءمة القواعد القانونية التقليدية في التشريع الجزائي الكويتي في معالجة المشكلات الناجمة عن الجرائم الإلكترونية؟
3. ما التدخل المناسب الذي يجب أن يقوم به المشرّع الكويتي بخصوص مواجهة الجرائم الإلكترونية؟ هل بإصدار قانون مثلما فعل المشرّع الأردني؟ أم بإجراء تعديل على قانون الجزاء؟
4. ما الإطار القانوني للجرائم الإلكترونية؟
5. ما الحلول التشريعية والعملية للحد من المشكلات الناجمة عن الجرائم الإلكترونية؟

حدود الدراسة

<u>الحدود المكانية:</u>

تقتصر بصفة أساسية على التشريع الجزائي الكويتي والأردني، مع التعرض لبعض التشريعات الغربية والعربية بخصوص موقفها من معالجة المشكلات العملية والقانونية التي تثيرها الجرائم الإلكترونية.

<u>الحدود الزمانية:</u>

ستجري الدراسة في العام الدراسي 2014/2013م على قانون الجزاء الكويتي رقم (16) لسنة 1960م، وقانون رقم (31) لسنة 1970م بتعديل بعض أحكام قانون الجزاء الكويتي، وقانون الإجراءات والمحاكمات الجزائية الكويتي رقم (17) لسنة 1960م، وكذلك قانون جرائم أنظمة المعلومات الأردني رقم (30) لسنة 2010م، وقانون العقوبات الأردني

رقم (16) لسنة 1960م وتعديلاته، وقانون أصول المحاكمات الجزائية الأردني رقم (9) لسنة 1961م.

الحدود الموضوعية:

ستبحث هذه الدراسة في مفهوم الجريمة الإلكترونية والمشكلات الموضوعية والإجرائية المتعلقة بها، وكذلك الحلول التشريعية والعملية لمواجهة هذه المشكلات.

محددات الدراسة

تبحث هذه الدراسة في موضوع من موضوعات القانون الجزائي، ومن ثم لا توجد أية محددات من شأنها الحيلولة دون نشر نتائجها وتوصياتها في الكويت والأردن وباقي الدول العربية.

المصطلحات الإجرائية

من المصطلحات ذات العلاقة، هي:

- **نظام المعلومات:** مجموعة البرامج والأدوات المعدّة لإنشاء البيانات أو المعلومات إلكترونياً، أو إرسالها، أو تسلمها، أو معالجتها، أو تخزينها، أو إدارتها.
- **البيانات:** الأرقام والحروف والرموز والأشكال والأصوات والصور التي ليس لها دلالة بذاتها.
- **المعلومات:** البيانات التي تمت معالجتها وأصبح لها دلالة.
- **الشبكة المعلوماتية:** ارتباط بين أكثر من نظام معلومات للحصول على البيانات والمعلومات وتبادلها.
- **الموقع الإلكتروني:** مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد.

- **التصريح:** الإذن الممنوح من صاحب العلاقة إلى شخص أو أكثر أو للجمهور للدخول إلى أو استخدام نظام المعلومات أو موقع إلكتروني أو الشبكة المعلوماتية بقصد الاطـــلاع أو إلغاء أو حذف أو إضافة أو تغيير أو إعادة نشر بيانات أو معلومات أو حجب الوصـــول إلأيها أو إيقاف عمل الأجهزة أو تغيير موقع إلكتروني أو إلغائه أو تعديل محتوياته.
- **البرامج:** مجموعة من الأوامر والتعليمات الفنية المعدّة لإنجاز مهمة قابلة للتنفيذ باستخدام أنظمة المعلومات.
- **الفيروسات:** هي برامج يتم إنتاجها خصيصاً لكي تلحق نفسها ببعض البرامج المـــشهورة وذلك عن طريق تزييف أو تعديل بسيط للتوقيع الخاص بالبرنامج الأصـــلي (مجموعـــة الأرقام الثنائية)، وتتمكن هذه البرامج من تدمير البرامج والمعلومات أو إصابة الأجهـــزة بالخلل بعدة طرق، فمنها ما يبدأ بالعمل مباشرة عند الإصابة، وبعضها عند تنفيذ بعـــض الأوامر، وتتميز هذه الفيروسات بقدرتها على التكاثر والانتقال من جهاز إلى آخـــر عـــن طريق الملفات المتبادلة بين المستخدمين[1].
- **المستند الإلكتروني:** هو عبارة عن سجل أو مستند يتم إنشاؤه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة إلكترونية على وسيط مملوس أو علـــى أي وسيط إلكتروني آخر ويكون قابلاً للاسترجاع بشكل يمكن فهمه[2].
- **الجريمة الإلكترونية:** هي فعل غير مشروع ناتج عن إرادة آثمـــة يقـــرر لهـــا القـــانون عقوبة[1]،

---

[1] عبد الله، عبد الله عبد الكريم (2011). جرائم المعلوماتية والإنترنت – الجرائم الإلكترونية، منشورات الحلبي الحقوقية، بيروت، ص53.

[2] الصمادي، حازم، مرجع سابق، ص2.

وهي أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية[2].

الدراسات السابقة

من الدراسات ذات الصلة بموضوع هذا البحث:

- دراسة العنزي، سليمان بن مهجع (2003) دراسة بعنوان: "**وسائل التحقيق في جرائم نظم المعلومات**"، أكاديمية نايف العربية للعلوم الأهلية، رسالة ماجستير.

هدفت هذه الدراسة إلى تحديد وسائل التحقيق في الجرائم المعلوماتية وذلك بالكشف عن الجوانب المختلفة المحيطة بجريمة نظم المعلومات بتجديد أنماطها ودوافعها وإبراز أضرارها، وحصر الأساليب والأدوات المستخدمة من قبل مجرمين نظم المعلومات، وبذلك تختلف عن دراستي كون الدراسة الحالية تبحث في المشكلات الناجمة عن الجرائم الإلكترونية دون البحث في وسائل التحقيق فيها.

- الدسوقي، محمد (2003) دراسة بعنوان: "**الحماية الجنائية لسرية المعلومات**"، دار الكتب القانونية، مصر.

تناولت هذه الدراسة مسألة ضخامة التدفق والمخزون المعلوماتي الإلكتروني وتنوعه وانطوائه على أسرار البشر وخصوصياتهم مشيراً إلى أن هذا المخزون بات ميداناً خصباً للمتطفلين والمجرمين.

وقامت الدراسة بتقديم اقتراح على البحرين وجميع الدول العربية الانضمام لاتفاقية بودابست المتعلقة بالجرائم الإلكترونية لعام 2001م وذلك بغية توسيع نطاق التعاون الدولي

---

[1] المومني، نهلا عبد القادر (2012). الجرائم المعلوماتية، دار الثـقافة، عمان، ط1، الإصدار السادس، ص50.

[2] الصماوي، حازم، مرجع سابق، ص2.

فيما يتعلق بالجرائم الاقتصادية، وهي تختلف عن دراستي لأن الدراسة الحالية لن تبحث بشكل تفصيلي في موضوع الدراسة السابقة المذكورة، وإنما تقتصر على بحث المشكلات الناجمة عن الجرائم الإلكترونية في التشريع الكويتي والأردني.

- حميد، عبد الله قاسم (2010) دراسة بعنوان: "**الحماية الجنائية للمعلومات الإلكترونية**"، رسالة ماجستير، جامعة عين شمس.

تناول الباحث التحول إلى التطبيقات الإلكترونية، والوقوف على النصوص التي تنظم هذه المسؤولية، ومقارنتها بالتطورات التي طرأت على أساليب ارتكاب مثل هذه الجرائم المستحدثة، وبحث مدى تناسب تطبيقها على هذه الجرائم، إضافة إلى اقتراح الحلول التشريعية لمكافحة جرائم المعلومات التي ارتبطت بالتطور التقني وما صحبه من ثورة تقنية في مجال المعلومات أو المعرفة على مستوى العالم.

وتوصل الباحث إلى نتائج، منها: أن دولة الإمارات العربية المتحدة كانت من أوائل الدول التي تصدت للجرائم المعلوماتية أو الإلكترونية، وذلك من خلال إصدار القانون الاتحادي رقم (2) لسنة 2006م في شأن مكافحة جرائم تقنية المعلومات، كما تم إنشاء دوائر قضائية متخصصة للنظر في الجرائم الإلكترونية، وتختلف عن الدراسة الحالية لأن دراستي تبحث في مشكلات الجرائم الإلكترونية في التشريع الكويتي والأردني.

- الخوالدة، محمد سليمان (2012) دراسة بعنوان: "**جريمة الدخول غير المشروع إلى موقع إلكتروني أو نظم معلومات وفق التشريع الأردني – دراسة مقارنة**"، دار الثـــقافة، عمان.

تناول الباحث الطبيعة القانونية لجريدة الدخول غير المشروع لموقع إلكتروني أو نظام معلومات وذلك بتطبيقها على واقع النص القانوني من خلال وصف أركان هذه الجريمة وصور النشاط الجرمي المكون لها، ومسؤولية مرتكب هذا النوع من الجرائم المستحدثة،

والجزاء المقرر لها وفق نصوص قانون جرائم أنظمة المعلومات الأردني لعام 2010م مقارنة مع بعض التشريعات الجنائية المقارنة، وخلصت الدراسة إلى عدد من النتائج والتوصيات، كان من أهمها: أنه من الضروري إدخال نصوص قانونية تعاقب على جريمة إتلاف المعلومات والبيانات بحد ذاتها وتقرر مسؤولية الشخص المعنوي في حال ارتكاب الجرائم المعلوماتية، والمعاقبة على الشروع في مثل هذه الجرائم، وهذه الدراسة تتشابه في بعض مفرداتها مع دراستي الحالية، إلا أنها تختلف عنها كون أن دراستي تبحث حصراً في المشكلات الناجمة عن الجرائم الإلكترونية في ضوء التشريع الكويتي وكذلك الأردني.

الإطار النظري للدراسة

قمت بتقسيم هذه الدراسة إلى خمسة فصول تناولت في الفصل الأول المقدمة، وفي الفصل الثاني مفهوم الجريمة الإلكترونية من خلال التعريف بها وبيان إطارها القانوني.

وفي الفصل الثالث سنتكلم عن المشكلات الموضوعية والإجرائية التي تتولد عن الجرائم الإلكترونية، وفي الفصل الرابع سوف نقوم بتسليط الضوء على الحلول التشريعية والعملية من أجل مكافحة تحديات ومشكلات الجرائم الإلكترونية، وفي الفصل الخامس سوف نتعرض للخاتمة والنتائج والتوصيات التي خلصت إليها الدراسة.

منهجية الدراسة

سأتبع المنهج التحليلي الوصفي المقارن من خلال إيراد النصوص ذات الصلة بموضوع الدراسة في التشريع الأردني، وكذلك التشريع الكويتي، وتحليلها، ومقارنتها للوصول إلى نتائج وتوصيات تجيب على أوجه النقص التشريعي لدى المشرّع الكويتي بخصوص مواجهة تحديات ومشكلات الجرائم الإلكترونية، وسوف أتعرض لموقف بعض التشريعات الغربية والعربية بهذا الشأن، وإيراد أحكام قضائية أجنبية.

الفصل الثاني

مفهوم الجريمة الإلكترونية

يتطلب دراسة مفهوم الجريمة الإلكترونية أن يتناول الباحث التعريف بهذه الجريمة، وكذلك بيان إطارها القانوني، وسأقوم ببحث هذا الفصل في مبحثين:

المبحث الأول: التعريف بالجريمة الإلكترونية.

المبحث الثاني: الإطار القانوني للجريمة الإلكترونية.

المبحث الأول

التعريف بالجريمة الإلكترونية

إن بيان المشكلات القانونية والعملية التي تثيرها الجريمة الإلكترونية تتطلب من الباحث أن يقوم ببحث مسألة أولية تتعلق بالتعريف بهذه الجريمة من خلال بيان معناها، وطبيعتها القانونية، وكذلك خصائصها، وسأقسم هذا المبحث إلى ثلاثة مطالب.

المطلب الأول

معنى الجريمة الإلكترونية

لم يتناول المشرّع الأردني تعريفاً للجريمة الإلكترونية في قانون جرائم أنظمة المعلومات المؤقت رقم (30) لسنة 2010م، كما أنه لا يوجد في التشريع الكويتي قانوناً يتناول التنظيم القانوني للجريمة الإلكترونية.

وقد تناول الفقه القانوني تعريفات مختلفة للجريمة الإلكترونية، ويمكن ردّها إلى خمسة اتجاهات، وعلى النحو الآتي:

الاتجاه الأول: يعرّف الجريمة الإلكترونية بأنها: كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب[1].

يلاحظ الباحث أن هذا التعريف يستند إلى وسيلة ارتكاب الجريمة الإلكترونية باستخدام الحاسب الآلي كي تعدّ جريمة إلكترونية.

الاتجاه الثاني: يعرّف الجريمة الإلكترونية بأنها: نشاط غير مشروع موجّه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه[2].

يلاحظ أن هذا التعريف يستند إلى وجوب أن يكون الحاسب الآلي هو محل الجريمة الإلكترونية، وقد فسّر جانب من الفقه أن هذه الجريمة هي جريمة اعتداء على الأموال المعلوماتية، وهي عبارة عن الأدوات المكوّنة للحاسب الآلي، وبرامجه، ومعداته[3].

الاتجاه الثالث: يعرّف الجريمة الإلكترونية بأنها: أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه والتحقيق فيه وملاحقته قضائياً[4].

ويلاحظ أن هذا التعريف يأخذ بوجوب إلمام الفاعل بتقنية المعلومات الإلكترونية من حيث استخدام الحاسب الآلي كي تعدّ جريمته من الجرائم الإلكترونية.

---

(1) انظر: الجنيهي، منير محمد، والجنيهي، ممدوح محمد (2006). جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، ط1، ص14؛ وكذلك: رستم، هشام محمد (1999). جرائم الحاسب المستحدثة، دار الكتب القانونية، مصر، ط1، ص110.

(2) قشقوش، هدى حامد (1992). جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، ص5.

(3) العريان، محمد علي (2009). الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، ط2، ص170.

(4) الشوا، سامي (1993). الغش المعلوماتي كظاهرة إجرامية مستحدثة، بحث في مؤتمر الجمعية المصرية للقانون الجنائي، القاهرة، 25-28 أكتوبر، ص516.

الاتجاه الرابع: يعرّف هذا الاتجاه الجريمة الإلكترونية بأنها: الاعتداءات القانونية التي يمكن أن ترتكب بواسطة الوسائل الإلكترونية بغرض تحقيق الربح[1].

وقد عرّفت منظمة التعاون الاقتصادي والتنمية التابعة للأمم المتحدة الجريمة الإلكترونية بأنها: كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية الإلكترونية[2].

ما يلاحظ على هذين التعريفين أن التعريف الأول اشترط أن يحقق الفاعل ربحاً، وهذا الأمر برأي غير متحصل دائماً من الجرائم الإلكترونية، كما أن الفعل المرتكب قد لا يكون عمدياً فقد يحصل بطريقة غير مباشرة، كما أن تعريف منظمة التعاون الاقتصادي والتنمية أدرج الأموال المادية، وهذه الأموال – كما يرى البعض[3] – يمكن حمايتها بموجب نصوص قانون العقوبات التقليدية ولا حاجة لقانون خاص لحمايتها.

الاتجاه الخامس: يعرّف الجريمة الإلكترونية بأنها: كل فعل أو امتناع عبر فعل من مسألة الاعتداء على الأموال المعنوية (معطيات الحاسب) يكون ناتجاً بطريقة مباشرة وغير مباشرة لتدخل التقنية الإلكترونية[4].

وبرأي الباحث فإن الاتجاه الأخير يعدّ التعريف الذي جاء به متوافقاً مع التطوّر المستمر للجرائم الإلكترونية ولوسائلها التقنية، وبخاصة أنه شمل الأموال المعنوية دون

---

(1) عبد الله، عبد الله عبد الكريم (2011). جرائم المعلوماتية والإنترنت – الجرائم الإلكترونية، منشورات الحلبي الحقوقية، بيروت، ط1، ص15.

(2) أورد هذا التعريف د. عبابنة، محمد أحمد (2005). جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، ط1، ص17.

(3) عبابنة، محمود أحمد، مرجع سابق، ص19.

(4) عبابنة، محمود أحمد، مرجع سابق، ص19.

الأموال المادية، وبذلك يكون هذا التعريف إلى حد ما قد جمع المعايير التي جاءت بها الاتجاهات الأربع سالفة الذكر.

وفي ضوء ما سبق، فإن الباحث يقترح تعريفاً للجريمة الإلكترونية بأنها: كل فعل أو امتناع يتم إعداده أو التخطيط له، ويتم بموجبه استخدام أي نوع من الحواسيب الآلية سواء حاسب شخصي أو شبكات الحاسب الآلي أو الإنترنت أو وسائل التواصل الاجتماعي لتسهيل ارتكاب جريمة أو عمل مخالف للقانون، أو تلك التي تقع على الشبكات نفسها عن طريق اختراقها بقصد تخزينها أو تعطيلها أو تحريف أو محو البيانات أو البرامج التي تحويها.

المطلب الثاني

الطبيعة القانونية للجريمة الإلكترونية

يتمحور الحديث عن الطبيعة القانونية للجريمة الإلكترونية حول الوضع القانوني للبرامج والمعلومات، وهل لها قيمة في ذاتها أم أن قيمتها تتمثل في أنها مجموعة مستحدثة من القيم القابلة للاستثناء يمكن الاعتداء عليها بأية طريقة كانت؟

انقسم الفقه إلى اتجاهين: الأول يرى أنه وفقاً للقواعد العامة فإن الأشياء المادية وحدها هي التي تقبل الحيازة والاستحواذ، وأن الشيء موضوع السرقة يجب أن يكون مادياً أي له كيان مادي ملموس حتى يمكن انتقاله وحيازته عن طريق الاختلاس المكوّن للركن المادي في جريمة السرقة، ولما كانت المعلومة لها طبيعة معنوية ولا يمكن اعتبارها من قبيل القيم القابلة للحيازة والاستحواذ، إلا في ضوء حقوق الملكية الفكرية، لذلك تستبعد المعلومات ومجرد الأفكار من مجال السرقة، ما لم تكن مسجلة على اسطوانة أو شريط، فإذا ما تمّ سرقة إحدى هاتين الدعامتين الخارجية، فلا تثور مشكلة قانونية في تكييف الواقعة علىأنها سرقة مال معلوماتي ذو طبيعة مادية، وإنما المشكلة تثور عندما نكون أمام سرقة مال معلوماتي غير

مادي[1]؛ والاتجاه الثاني يرى المعلومات ما هي إلا مجموعة مستحدثة من القيم قابلة للاستحواذ مستقلة عن دعامتها المادية، ذلك أن المعلومات لها قيمة اقتصادية قابلة لأن تحاز حيازة غير مشروعة، وأنها ترتبط كما يقول الأستاذان (Vivant & Catala) بمؤلفها عن طريق علاقة التبني التي تقوم بينهما كالعلاقة القانونية التي تتمثل في علاقة المالك بالشيء الذي يملكه، بمعنى أن المعلومات مال قابل للتملك أو الاستغلال على أساس قيمته الاقتصادية وليس على أساس كيانه المادي، ولذلك فهو يستحق الحماية القانونية ومعاملته معاملة المال[2].

وهناك من يقول: "إنه يجب أن نفرق بأن هناك مالاً معلوماتياً مادياً فقط ولا يمكن أن يخرج عن هذه الطبيعة وهي آلات وأدوات الحاسب الآلي مثل وحدة العرض البصري، ووحدة الإدخال، وأن هناك من المال المعلوماتي المادي ما يحتوي على مضمون معنوي هو الذي يعطيه القيمة الحقيقية وهي المال المادي الشريط الممغنط أو الاسطوانة الممغنطة أو الذاكرة أو الأسلاك التي تنتقل منها الإشارات من على بعد، كما هو الحال في جرائم التجسس عن بُعد، إذن من المنطق القول إذا حدثت سرقة فإنه لا يسرق المال المسجل عليه المعلومة والبرامج لقيمته المادية وهي ثمن الشريط أو ثمن الاسطوانة، وإنما يسرق ما هو مسجل عليهما من معلومات وبرامج"[3].

"إن التحليل المنطقي يفرض الاعتداد بفكرة الكيان المادي للشيء الناتج عنه اختلاس المال المعنوي للبرامج والمعلومات، وأنها لا يمكن أن تكون شيئاً ملموساً محسوساً، ولكن لهما

---

(1) المطردي، مفتاح بو بكر (2012). الجريمة الإلكترونية، ورقة مقدّمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، السودان، 23-25 أيلول، ص17.

(2) نقلاً عن: سلامة، محمد عبد الله (2007). موسوعة جرائم المعلوماتية – جرائم الكمبيوتر والإنترنت، المكتب العربي الحديث، الإسكندرية، ص43-44.

(3) الزعبي، جلال محمد والمناعسة، أسامة محمد (2013). جرائم تقنية نظم المعلومات الإلكترونية، دار الثــقافة، عمان، ط1، الإصدار الرابع، ص36-37.

كيان مادي قابل للانتقال والاستحواذ عليه بتشغيل الجهاز ورؤيتهما على الشاشة مترجماً إلى أفكار تنتقل من الجهاز إلى ذهن المتلقي، وانتقال المعلومات يتم عن طريق انتقال نبضات ورموز تمثل شفرات يمكن حلها إلى معلومات معينة لها أصل صادرة عنه يمكن سرقته، وبالتالي لها كيان مادي يمكن الاستحواذ عليه (البرامج والمعلومات)، وطالما أن موضوع الحيازة (أي المعلومات) غير مادي، فإن واقعة الحيازة تكون من نفس الطبيعة أي غير مادية (ذهنية)، وبالتالي يمكن حيازة المعلومات بواسطة الالتقاط الذهني عن طريق البصر"[1].

وعند حديثنا عن طبيعة الجرائم الإلكترونية يجب علينا أن نتحدث أيضاً عن ذلك من خلال الحديث عن أكثر الصور شيوعاً لاختلاف كل منها في تكييفها عن الأخرى.

أولاً: الجرائم الإلكترونية جرائم أموال:

إن الجرائم الإلكترونية وفقاً للمفهوم الذي بيناه آنفاً، تظهر بصورتين[2]:

الأولى: جرائم واقعة باستخدام الحاسب الآلي، ومنها استخدام الحاسب الآلي لتزييف العملة، أو التزوير في محررات رسمية، أو الاختلاس[3]، أو استخدام الحاسب الآلي لأغراض الدخول

---

(1) قشقوش، هدى حامد، مرجع سابق، ص51-52.

(2) المومني، نهلا، مرجع سابق، ص64.

(3) من الأمثلة الواقعية على الاختلاس بواسطة الحاسب الآلي قيام أحد الموظفين في مكتب محاسبة في أمريكا/ كاليفورنيا باختلاس أكثر من مليون دولار عن طريق التلاعب الحسابات التي يريها بالمكتب لشركة شحن خضار وفواكه إذ لاحظ بحكم كونه محاسباً أن عملية التدقيق والمراجعة على حسابات شركة الشحن غير دقيقة، وغير كاملة، فقام باختلاق سبع عشرة شركة وهمية جعل لها في حسابا شركة الشحن مستحقات مالية عن خدمات تؤديها، بحيث يقوم هو بالاستيلاء على تلك المبالغ، مع حرصه على ألا يتجاوز نسبة ما يختلسه النسب المعقولة حتى لا تثار حوله المشاكل، فقام بإعداد برنامج خاص يتولى وفقاً لمعايير حسابية – تراعي مختلف الظروف الواقعية لإيرادات الشركة ومصروفاتها – تحديد مقدار الاختلاس دون أن يكشف أمره في عمليات التدقيق والمراجعة، ومن العجيب أن أمر هذا المجرم لم يكتشف إلا بمحض الصدفة نتيجة لضخامة قيمة الشيكات، فصدر على المختلس حكم بالسجن عشر سنوات. انظر: الهيتي، محمد حماد مرهج (2004). التكنولوجيا الحديثة والقانون الجنائي، دار الثـقافة، عمان، ط1، ص46.

غير المشروع للبيانات والمعلومات المخزنة على حاسب آلي آخر، وذلك عبر شبكات الاتصال الدولية، أو بصورة مباشرة بغية الحصول على منافع نقدية أو غيرها، أو أخذ المعلومات والبيانات.

الثانية: جرائم واقعة على الحاسب الآلي بمشتملاته المتعلقة بالجانب المادي، أو بالجانب المعنوي كجرائم تعديل أو تحوير أو تقليد برامج الحاسب الآلي، وجرائم تدمير المعلومات والبيانات الخاصة بالحاسب الآلي نفسه، بالإضافة إلى الجرائم التقليدية العادية التي تطال الجانب المادي للحاسب الآلي كالسرقة والإتلاف.

وفي كلتا الحالتين يمكن أن توصف الجرائم الإلكترونية بأنها جرائم أموال، إذ موضوعها دائماً هو المال، هذا مع التسليم بأن الجانب المعنوي للحاسب الآلي وما يشتمل عليه المال بالمعنى الفني والقانوني.

ولعل ما يدعم وجهة النظر هذه من أن الجرائم الإلكترونية هي جرائم أموال هو ضخامة السلوكيات غير المشروعة والناتجة عن استخدام الحاسب الآلي لتحقيق مكاسب مالية سواء تمّ ذلك بالغش أو الاحتيال أو أعمال التخريب والهدم أو المضاربات غير المشروعة، وكلها جرائم تقع على الأموال من منظور قانون العقوبات[1].

وفي هذه الحالة من الممكن أن تكون الكثير من جرائم الأموال التقليدية جرائم أموال إلكترونية أيضاً، فقد تكون الجريمة الإلكترونية جريمة سرقة، وقد تكون جريمة احتيال، وقد تكون أيضاً جريمة إساءة ائتمان (خيانة الأمانة)، وقد تكون جريمة إتلاف لمال الغير[2].

---

[1] انظر مثلاً: المواد (399-458) عقوبات أردني.

[2] الزعبي، جلال محمد والمناعسة، أسامة محمد مرجع سابق، ص38.

ثانياً: الجرائم الإلكترونية جرائم أشخاص:

من الممكن وقوع جرائم أشخاص من خلال النظام الإلكتروني، ولكن هذا الشكل لا يجد الكثير من التطبيقات العملية على أرض الواقع، إذ ينحصر أثرها في مجموعة ضيقة من جرائم الأشخاص وذلك في جرائم الذم، والقدح، والتحقير، وجريمة إفشاء الأسرار سواء التجارية أو الشخصية، وكذلك جرائم التهديد، والتحريض، وجرائم الاعتداء على الحياة الخاصة عبر الإنترنت.

ثالثاً: الجرائم الإلكترونية جرائم أمن دولة وجرائم مخلة بالثـــقة العامة والآداب العامة:

نظراً للطبيعة الخاصة التي تتمتع بها جرائم أمن الدولة وإمكانية وقوع الكثير منها عن طريق الوسائل المحكية أو المقروءة، فهي بذلك تعدّ جريمة ملائمة لتقع عبر الوسائل الإلكترونية سواء فيما يخص أمن الدولة الداخلي أو الخارجي، مثل جرائم التجسس، وجرائم الاتصال بالعدو، وجرائم إثارة الفتن، والحض عليها، والجرائم الماسة بالوحدة الوطنية، وتعكير صفو الأمة[1].

أما الجرائم المخلة بالثـــقة العامة والآداب العامة فهي أيضاً قابلة للوقوع عبر الوسائل الإلكترونية وذلك مثل جرائم التزوير، وتقليد الأختام، وتزوير الأوراق البنكية، والمسكوكات، وانتحال الشخصية[2].

وبالرجوع إلى قانون جرائم أنظمة المعلومات الأردني، يجد الباحث أن المشرّع الأردني أحسن حينما تدخل وحسم الجدل الفقهي في طبيعة الجرائم الإلكترونية، إذ إنه عالج صوراً متعددة من هذه الجرائم وحدد لها عقوبات، وهي: الجرائم المرتبطة بالذمة المالية والتي

---

[1] منصور، محمد حسين (2010). المسؤولية الإلأكترونية، دار المعارف، الإسكندرية، ط2، ص148.

[2] حجازي، عبد الفتاح بيومي (2008). التزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، ط1، ص58-59.

تتعلق ببطاقات الائتمان، أو بالبيانات، أو المعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية بموجب المادة (6) منه، وكذلك جرائم غش الحاسب الآلي (التحال المعلوماتي)، بموجب المادتين (3، 4) من القانون المذكور، وأيضاً عالج الجرائم المتصلة بالحياة الخاصة لجريمة التقاط أو اعتراض أو التنصت على المرسل من خلال النظام الإلكتروني في المادة (5) من القانون المذكور، وكذلك جريمة نشر أعمال إباحية تتعلق بالاستغلال الجنسي لمن لم يكمل الثامنة عشرة من العمر، أو ترويج هذه الأعمال بمقتضى المادة (8) من نفس القانون، وكذلك جريمة ترويج الدعارة بموجب المادة (9) من ذات القانون، وكذلك القيام بأعمال إرهابية أو دعم لجماعة، أو تنظيم، أو جمعية تقوم بأعمال إرهابية، أو تمويلها بموجب المادة (10) من نفس القانون، وكذلك أي اطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني، أو العلاقات الخارجية للمملكة الأردنية، أو السلامة العامة، أو الاقتصاد الوطني، وذلك بموجب المادة (11) من القانون المذكور.

أما بالنسبة للمشرّع الكويتي، فحتى وقتنا الحالي لم يتدخل ليسن قانوناً خاصاً بالجرائم الإلكترونية؛ رغم أهميته القانونية والعملية لمكافحة هذا النوع من الجرائم، وفي هذا الصدد، يرى جانباً من الفقه القانوني الكويتي أن: عقوبة الجرائم الإلكترونية والاختراقات غير المشروعة بالكويت تصل إلى التكييف القانوني للجريمة الإلكترونية باختلاف الوقائع التي تم ارتكابها، وعلى سبيل المثال: إذا كان الدخول على حسابات الأشخاص لدى البنوك، والاستيلاء على أموال منها، فإن الوقائع قد تشكل جنحة السرقة وفقاً للمادة (221) من قانون الجزاء الكويتي، أو جناية السرقة المنصوص عليها بالمواد (222، 223، 224، 225، 226، 227) من قانون الجزاء، حيث تصل العقوبة إلى 3 سنوات، أما إذا كان الدخول إلى الحسابات والمواقع الشخصية على شبكة الإنترنت، فإن كان ذلك بنشر عبارات أو ألفاظ تشكل قذفاً أو

سباً يكون ذلك معاقباً بالجنحة المؤثمة بالمادتين (209، 210) من قانون الجزاء الكويتي رقم (16) لسنة 1960م.

وقد تشكل الأفعال إحدى الجنايات المتعلقة بأمن الدولة الخارجي أو أمن الدولة الداخلي المنصوص عليها في القانون رقم (31) لسنة 1970م بتعديل بعض أحكام قانون الجزاء، فضلاً عن الجنح المؤثمة بالقانونن رقم (9) لسنة 2011 بشأن إساءة استعمال أجهزة الاتصالات الهاتفية وأجهزة التنصت[1].

المطلب الثالث

خصائص الجريمة الإلكترونية

نظراً لارتباط الجريمة الإلكترونية بجهاز الحاسوب، وشبكة الإنترنت بصفة عامة، ووسائل التواصل الاجتماعي بصفة خاصة، فقد أضفى عليها ذلك مجموعة من الخصائص المميزة لها عن خصائص الجريمة التقليدية، ومن هذه الخصائص ما يلي:

أولاً: جريمة عابرة للحدود:

أعطى انتشار شبكة الإنترنت إمكانية لربط أعداد هائلة من أجهزة الحاسوب المرتبطة بالشبكة العنكبوتية من غير أن تخضع لحدود الزمان والمكان، لذلك فإن من السهولة بمكان أن يكون المجرم في بلد ما والمجني عليه مقيم في بلد آخر، وهنا تظهر الحاجة لوجود تنظيم قانوني دولي وداخلي متلائم معه لمكافحة مثل هذا النوع من الجرائم وضبط فاعليها، وحيث إن التشريعات الداخلية متفاوتة فيما بين كل دولة من دول العالم، تظهر العديد من المشاكل حول صاحب الاختصاص القضائي لهذه الجريمة وإشكالات أخرى متعلقة بإجراءات الملاحقة

---

[1] الكندري، عبد الله (2013). مقال قانوني بعنوان: "الجرائم الإلكترونية في التشريع الكويتي"، جريدة الأنباء، جريدة كويتية يومية شاملة، العدد الصادر يوم الإثنين 22 يوليو 2013م، ص7. موقع الجريدة: www.alanba.com.kw.

القضائية، وتتشابه الجرائم الإلكترونية في هذه الخاصية مع بعض الجرائم مثل جرائم غسيل الأموال، وجرائم المخدرات[1].

ثانياً: جريمة صعبة الإثبات والاكتشاف:

تكمن صعوبة إثبات مثل هذه الجريمة أنها لا تترك في الغالب أثراً مادياً ظاهراً يمكن ضبطه، فضلاً عن التباعد الجغرافي الذي يثير الإشكال بدايةً، حيث تشير الدراسات أن ما يتم اكتشافه من جرائم المعلومات يصل إلى نسبة 1% والذي يتم الإبلاغ عنه من هذه النسبة لا يكاد يصل إلى 5% فقط[2].

والوسيلة المستخدمة لارتكاب الجريمة هي نبضة إلكترونية ينتهي دورها خلال أقل من ثانية واحدة، وكأن الجاني يقوم بتدمير الدليل بمجرد استعماله ويقوم بذلك بكل هدوء ودون إحداث أية ضجة، وذلك على خلاف الكثير من الجرائم التي نعرف[3].

ثالثاً: خصوصية مجرم المعلومات:

قد لا تتأثر الجرائم التقليدية بالمستوى العلمي للمجرم كقاعدة عامة، ولكن الأمر مختلف تماماً بالنسبة للمجرم المعلوماتي والذي يكون عادة من ذوي الاختصاص والمعرفة في مجال تقنية المعلومات.

وقد تمّ تصنيف مجرمي الجرائم الإلكترونية إلى المخترقين والمحترفين والحاقدين.

أ. **المخترقون:** مثل الهاكرز الذي يعدّ شخصاً بارعاً في استخدام الحاسب الآلي ولديه فضول في استخدام حسابات الآخرين بطرق غير مشروعة، الأمر الذي يدل على أنهم أشخاص

---

(1) القطاونة، مصعب (2010). الإجراءات الجنائية الخاصة في الجرائم المعلوماتية، بحث مقدّم لشبكة قانوني الأردن، ص5.

(2) القطاونة، مصعب، مرجع سابق، ص6.

(3) المطردي، مفتاح بو بكر، مرجع سابق، ص8.

متطفلون وغير مرحب بهم لدى الغير، وأغلبهم ما يكون جانبهم تحدي الشباب للدخول إلى المواقع الرسمية، وبعض الأحيان الدخول إلى مواقع الحسابات من أجل إثبات الذات، وغالباً تكون أعمارهم في سن المراهقة[1].

ب. **المحترفون:** وهم الأكثر خطورة بين مجرمي الإنترنت، حيث يهدف البعض منهم إلى الاعتداء لتحقيق الكسب غير المشورع المتمثل في الناحية المادية وذلك عبر الدخول في حسابات البنوك، والبعض الآخر يدخل من أجل تحقيق أغراض سياسية والتعبير عن وجهة نظره أو فكرة، وغالباً أعمال هؤلاء تكون بين 25 و 40 سنة[2].

ج. **الحاقدون:** وهم الذين ليس لديهم أي أهداف للجريمة ولا يسعون لمكاسب سياسية أو مادية ولكن يتحركون لرغبة في الانتقام والتأثر كالأمور الطائفية[3].

رابعاً: جريمة مغرية للمجرمين[4]:

نظراً للصفات التي تتمتع بها مثل هذه الجريمة، والصعوبات التي تثور عند محاولة اكتشافها أو ملاحقتها، فإن ذلك يشكل إغراءً كبيراً للمجرمين وخصوصاً أنه يمكن تحقيق مكاسب طائلة من وراء مثل هذا النوع من الجرائم، ونتيجة لكل ما سبق تعد مثل هذه الجرائم جريمة تستهوي الكثيرين لسهولتها، وكثرة مكاسبها.

خامساً: عدم وجود مفهوم مشترك للجريمة الإلكترونية:

لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها، فالبعض يطلق عليها جريمة الغش المعلوماتي، والبعض الآخر يطلق

---

(1) قورة، نائلة عادل (2012). جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، ط1، ص178.

(2) إبراهيم، خالد ممدوح (2009). الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط1، ص78.

(3) إبراهيم، خالد ممدوح، مرجع سابق، ص79.

(4) عبابنة، محمود أحمد، مرجع سابق، ص30.

عليها جريمة الاختلاس المعلوماتي، أو الاحتيال المعلوماتي، وآخرون يفضلون تسميتها بالجريمة المعلوماتية[1].

ومن وجهة نظر الباحث فإنه يفضل اصطلاح الجريمة الإلكترونية للدلالة على الجرائم المرتكبة بواسطة الحاسوب والإنترنت، فاصطلاح الجريمة الإلكترونية عام ويشتمل وسائل الاتصال الإلكترونية الحالية والمستقبلية المستخدمة في التعامل مع البيانات وتبادلها.

كما أن التطور التكنولوجيا نتج عنه تطور في طرق إثبات الجريمة والتعامل معها، فالجرائم العادية يسهل – غالباً – تحديد مكان ارتكابها، في حين أنه من الصعوبة بمكان تحديد مكان وقوع الحادثة عند التعامل مع الجرائم الإلكترونية، لكون الرسائل وملفات الكمبيوتر تنتقل من نظام معلوماتي إلى آخر في ثوان معدودة، كما أنه لا يقف أمام انتقال الملفات والمستندات والرسائل عبر شبكة الإنترنت أية حدود دولية أو جغرافية، ونتيجة لذلك فإن تحديد أي محكمة تحدد أي قانون يطبق سوف يكون مشكلة بين الدول مما يستدعي التعاون بين دول العالم[2].

كما أن مشروعية الجريمة أمر نسبي من دولة إلى أخرى، فمثلاً تجارة المخدرات في الأردن والكويت محرمة نهائياً، بينما في الدول الإسكندنافية مصرّح بها في حدود الاستعمال الشخصي فقط، بل إن مشروعية الجريمة قد تختلف داخل البلد الواحد، فمثلاً نجد داخل الولايات المتحدة الأمريكية أن ألعاب القمار عبر الإنترنت مسموح بها في ولاية لاس فيجاس بينما هي محرمة قانوناً في ولاية نيويورك[3].

---

[1] تفصيلاً انظر: الزعبي، جلال والمناعسة، أسامة، مرجع سابق، ص86-87.

[2] حجازي، عبد الفتاح بيومي (2004). جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، ص148.

[3] عفيفي، كامل عفيفي (2010). جرائم الكمبيوتر، دار النهضة العربية، القاهرة، ص76.

سادساً: وقوع الجريمة الإلكترونية أثناء المعالجة الآلية للبيانات:

من خصائص الجريمة الإلكترونية أنها تقع أثناء عملية المعالجة الآلية للبيانات والمعطيات الخاصة بالكمبيوتر، ويمثل هذا النظام الشرط الأساسي الذي يتعين توافره حتى يمكن البحث في قيام أو عدم قيام أركان الجريمة الإلكترونية الخاصة بالتعدي على نظام معالجة البيانات، ذلك أنه في حالة تخلف هذا الشرط تنتفي الجريمة الإلكترونية[1].

"وقد كان هناك اقتراح من قبل مجلس الشيوخ الفرنسي حال تعديل قانون العقوبات الحالي، بوضع تعريف محدد لعملية المعالجة الآلية للبيانات أو المعطيات، ولكن حذف هذا التعريف باعتبار أنها عملية فنية تخضع للتطور السريع، وبالتالي سيكون أي تعريف لها قاصراً، وكان هذا التعريف ينص على أنها: "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، والتي تتكون كل منها من الذاكرة، والبرامج، والمعطيات، وأجهزة الإدخال، والإخراج، وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات والتي عن طريقها يتم تحقيق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضعاً لنظام الحماية الفنية"[2].

والجريمة الإلكترونية قد تقع أثناء عملية المعالجة الآلية للبيانات في أي مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلي للبيانات سواء عند مرحلة إدخال البيانات، أو أثناء مرحلة المعالجة، أو أثناء مرحلة إخراج المعلومات.

---

[1] قورة، نائلة، مرجع سابق، ص55.

[2] نقلاً عن: القهوجي، علي عبد القادر (2000). الحماية الجنائية للبيانات المعالجة إلكترونياً، بحث مقدّم إلى مؤتمر القانون والكمبيوتر والإنترنت والذي عُقد خلال الفترة من 1-3 مايو، كلية الشريعة والقانون، جامعة الإمارات العربية، ص43.

سابعاً: الجريمة الإلكترونية جريمة مستحدثة:

تعدّ الجرائم الإلكترونية من أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل أخطاراً جسيمة في ظل العولمة، فلا غرابة أن تعدّ الجرائم الإلكترونية – سواء التي تتعرض لها أجهزة الكمبيوتر أو التي تسخر تلك الأجهزة في ارتكابها – من الجرائم المستحدثة، حيث إن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة، بحيث يتجاوز هذا التقدم بقدراته وإمكاناته أجهزة الدولة الرقابية، بل إنه أضعف من قدراتها في تطبيق قوانينها، بالشكل الذي أصبح يهدد أمها وأمن مواطنيها[1].

ثامناً: احتمال تعدد الأوصاف القانونية لمحل الجريمة الإلكترونية:

إن محل الجريمة الإلكترونية قد يظهر بمظهرين أحدهما مادي والثاني معنوي، كما هو الحال بالنسبة للمعلومات فقد تكون في حالة انتقال أو موجودة في ذاكرة النظام الإلكتروني أي أنها في حالة غير مادية، والشكل الآخر أن تكون المعلومات متجسدة في صورة مادية بتخزينها على دعامة إلكترونية، حتى أن المعلومات غير المادية بطبيعتها يمكن أن تخضع لأكثر من نص قانوني، وفقاً لما إذا كانت في شكل مادي أو غير مادي، وفي الشكل الأخير يوجد لها أكثر من نص قانوني يمكن أن تخضع له، مثال ذلك اعتبارها مصنف أدبي مما يثير مشكلة تعدد الأوصاف القانونية على ذات المحل[2].

---

[1] إبراهيم، خالد ممدوح، مرجع سابق، ص86.

[2] إبراهيم، خالد ممدوح، مرجع سابق، ص87-88.

المبحث الثاني

الإطار القانوني للجريمة الإلكترونية

سنبحث من خلال هذا المبحث ببيان الملامح التي توضح لنا الإطار القانوني للجرائم الإلكترونية، وهذا يتطلب بيان أركانها، وتحديد أطرافها، ومحلها، وآليات تنفيذها، ولذلك سنقسم هذا المبحث إلى ثلاثة مطالب.

المطلب الأول

أركان الجريمة الإلكترونية

تقوم الجريمة بشكل عام على أركان ثلاثة، هي[1]:

- **الركن الشرعي:** وهو الصفة غير المشروعة للفعل، وتتمثل قاعدة التجريم والعقاب للجرائم الإلكترونية في ما ورد النص عليه في قانون جرائم أنظمة المعلومات الأردني.
- **الركن المادي:** وهو ماديات الجريمة التي تبرز به إلى العالم الخارجي.
- **الركن المعنوي:** وهو الإرادة التي يقترن بها الفعل سواء في صورة القصد أو الخطأ.

وسأبحث الركنين المادي والمعنوي في الجرائم الإلكترونية وذلك في فرعين.

الفرع الأول: الركن المادي في الجرائم الإلكترونية:

من المشكلات العملية التي تثيرها الجريمة الإلكترونية طبيعة الركن المادي في الجريمة الإلكترونية، ذلك أن مفهوم أو مناط التجريم ينصب على نظام إلكتروني يساء استعماله أو يتم اقتحامه على نحو غير مشروع، بما يكون لذلك الاستعمال أو الاقتحام من أثر مادي ملموس يظهر إما في صورة تدمير للمعلومات، وهو ما يثير إمكانية الإتلاف العمدي

---

[1] الجبور، محمد (2012). الوسيط في قانون العقوبات – القسم العام، دار وائل، عمان، ط1، ص59.

للمنقولات، أو السرقة وذلك عن طريق إساءة استعمال بطاقات الائتمان، أو يثير شبهة التزوير عن طريق التلاعب في بيانات الحاسب الآلي، كما سنرى من خلال هذه الجراسة.

إن السلوك الإجرامي في الجريمة الإلكترونية يرتبط دائماً بالمعلومة المخزنة على الحاسب الآلي، أو تلك التي يتم إدخالها للحاسب الآلي، وصعوبة المشكلة أن السلوك الإجرامي قد يتحقق بمجرد ضغط زر في الحاسب فيتم تدمير النظام المعلوماتي أو حصول التزوير أو السرقة عن طريق التسلل إلى نظام أرصدة العملاء في البنوك أو إساءة استعمال بطاقات الائتمان[1].

إن السلوك الإجرامي بوصفه عنصراً في الركن المادي في الجريمة التقليدية يتم رؤيته رؤى العين والتأكد منه كفعل القتل أو السرقة أو التزوير، ولكن صعوبة الجريمة الإلكترونية، والركن المادي فيها خاصة أن الجريمة ترتكب عن طريق معلومات تتدفق عبر نظم الحاسب الآلي لا يمكن الإمساك مادياً بها، تماماً مثل التيار الكهربائي الذي يسري في توصيلة دون أن نراه[2]، لذلك يتعين تحليل السلوك الإجرامي في الجريمة الإلكترونية خاصة ما يتعلق فيها بفكرة المال في جرائم الاعتداء على المال العام أو الخاص، كما لا بدّ من العرض لصور السلوك الإجرامي في الجريمة الإلكترونية.

إن النشاط أو السلوك المادي في الجريمة الإلكترونية يتطلب وجود بيئة رقمية وجهاز كمبيوتر واتصال بشبكة الإنترنت، ويتطلب أيضاً معرفة بداية هذا النشاط والشروع فيه ونتيجته، فعلى سبيل المثال يقوم مرتكب الجريمة بتجهيز الكمبيوتر لكي يحقق له حدوث الجريمة، فيقوم بتحميل الحاسب ببرامج اختراق، أو أن يقوم بإعداد هذه البرامج بنفسه، وكذلك

---

[1] معاشي، سميرة (2011). ماهية الجريمة المعلوماتية، بحث منشور في مجلة المنتدى القانوني، العدد السابع، جامعة محمد خيضر بسكرة، الجزائر، ص280.

[2] حجازي، عبد الفتاح، مرجع سابق، ص114.

قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة وتحميلها على الجهاز المضيف، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيداً لبثها، وليس كل جريمة تستلزم وجود أعمال تحضيرية، وفي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في جرائم الكمبيوتر والإنترنت – حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية – إلا أنه في مجال تكنولوجيا المعلومات، الأمر يختلف بعض الشيء، فشراء برامج اختراق، ومعدات لفك الشفرات وكلمات المرور، وحيازة صور دعارة للأطفال، فمثل هذه الأشياء تمثل جريمة في حد ذاتها[1].

إن النشاط أو السلوك المادي في الجريمة الإلكترونية يعدّ محلاً لتساؤلات عديدة فيما يتعلق ببدايته أو الشروع في ارتكاب الجريمة، ومثل هذا النشاط يختلف عما هو الحال عليه في العالم المادي، فارتكاب الجريمة عبر الإنترنت يحتاج بالضرورة إلى منطق تقني، وبدونه لا يمكن للشخص حتى الاتصال بالإنترنت، سواء كان بقصد ارتكاب جريمة أم لمجرد التصفح أو الدخول في الاتصال المباشر كالمحادثة وغيرها.

وهذا السلوك المادي الإيجابي الممثل في المنطق التقني يجعل الجريمة عبر الإنترنت ذات طابع موحد بالضرورة، فهي تباشر من حيث السلوك أو النشاط المادي فيها، كأحد عناصر الركن المادي يضاف إلى فلسفة الركن المادي في الجريمة، مثل هذا الأمر تداركه المشرّع الأردني حين نص على جرائم يمكن أن ترتكب عبر الكمبيوتر، ففي مثل هذه النصوص نجد المشرّع الأردني يقرر صراحةً عبارة ... "إذا ارتكبت الجريمة باستخدام نظام معلومات أو الشبكة المعلوماتية ..." أو عبارة "... باستخدام المعالجة الآلية للبيانات" ففي مثل

---

[1] حجازي، عبد الفتاح، مرجع سابق، ص113.

هذه الحالات يكون المشرّع الأردني مدركاً لمسألة الشروع في ارتكاب جريمة عبر الشبكة المعلوماتية المرتبطة بالإنترنت[1].

لذلك يعدّ الدفع بعدم وجود قدرات تقنية حال الاتهام بارتكاب جريمة عبر الإنترنت من الدفوع الموضوعية الجوهرية التي تلتزم محكمة الموضوع بالرد عليه تفصيلاً، وإلا عاب حكمها عيباً في التسبيب بما يسمح بقبول نقضه، ولقد جعلت الطبيعة الموحدة للجريمة عبر الإنترنت، من حيث اتحاد جميع أشكالها المادية في ضرورة استخدام الآلة كوسيط إلى ارتكابها أن اتصفت هذه الجريمة بالضرورة بالطابع التقني[2].

ولكي يتوافر الركن المادي في الجريمة الإلكترونية، فلا بدّ من حصول النتيجة الإجرامية على أن ترتبط بالسلوك الإجرامي بعلاقة سببية.

الفرع الثاني: الركن المعنوي للجريمة الإلكترونية:

الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، فالركن المعنوي هو المسلك الذهني أو النفسي للجاني باعتباره محور القانون الجنائي، ذلك أنه في إطار هذا الركن تتوافر كافة مقومات المسؤولية الجنائية، من علم وإرادة آثمة وقصد جرمي مع إقرار حق الدولة في العقاب الذي يبنى على هذه المقومات، لذلك يمكن تعريف الركن المعنوي بأنه: العلاقة التي تربط بين ماديات الجريمة وشخصية الجاني مرتكبها، وهذه العلاقة هي محل الأذناب في معنى استحقاق العقاب، ومن ثم يوجه إليها لوم القانون وعقابه[3].

---

[1] راجع: نصوص المواد (4، 5، 6، 8، 9، 10) من قانون جرائم أنظمة المعلومات الأردني رقم (30) لسنة 2010م.

[2] إبراهيم، خالد ممدوح، مرجع سابق، ص100.

[3] حسني، محمود نجيب (1971). النظرية العامة للقصد الجنائي، دار النهضة العربية، ط2، ص90.

ويتوفر القصد الجنائي في حق الجاني في حالات ثلاثة، هي[1]:

الأولى: إذا كان الجاني يتوقع ويريد أن يترتب على فعله أو امتناعه حدوث الضرر أو وقوع الخطر الذي حدث والذي يعلق عليه القانون وجود الجريمة.

الثانية: إذا نجم عن الفعل أو الامتناع ضرر أو خطر أكثر جسامة مما كان يقصده الفاعل، وهي حالة جواز القصد التي ينص عليها القانون صراحةً على إمكان ارتكابها بهذا الوصف.

الثالثة: الحالات التي يعزى فيها القانون الفعل إلى الفاعل نتيجة لفعله أو امتناعه، أي حالات يفترض فيها القانون توافر القصد الجنائي لدى الجاني افتراضاً، وهو مستمد من أنه طالما أن النتيجة الجسيمة التي تحققه نشأت عن فعل الجاني، فمقتضى ذلك أن هذا الفعل كان صحيحاً لإحداثها، ولكونه كذلك فإن الجاني يجب أن يتحمل نتائجه، توقعها أم لم يتوقعها.

إن توافر الركن المعنوي في الجرائم الإلكترونية يعدّ من الأمور الهامة في تحديد طبيعة السلوك المرتكب وتكييفه لتحديد النصوص التي يلزم تطبيقها، إذ بدون الركن المعنوي لن يكون هناك سوى جريمة واحدة هي جريمة الدخول أو الولوج غير المشروع. فمثلاً إن التمييز بين جريمة الدخول غير المشروع على نظام المعالجة الآلية للبيانات وبين جريمة تجاوز الصلاحيات في الدخول على مثل هذا النظام، يعدّ تمييزاً دقيقاَ.

ففي جريمة تجاوز صلاحية الدخول، فإنه يلزم لتوافرها أن يكون هناك صلاحية للدخول على نظام ما، على أن تتوافر في داخل هذا النظام أنظمة معينة ليس من حق هذا الشخص الدخول عليها، فيقوم المذكور بالدخول عليه، ففي هذه الحالة لا تتوافر سوى جريمة واحدة، حيث إن المذكور يملك صالحة الدخول على النظام الأساسي ولا يملك الدخول على أنظمة خالة فيها، إلا أن تكوين النشاط المادي هنا يلزم أن يكون السلوك الإجرامي مرتكباً في

---

[1] للتفصيل راجع: الجبور، محمد، مرجع سابق، ص238 وما بعدها.

إطار نشاط ثان وليس النشاط الأول، مثل هذا الأمر يجعل جريمة تجاوز صلاحيات الدخول معتبراً من الجرائم التي لا يتطلب فيها ركناً معنوياً، وهذا الأمر محرم قانوناً.

ونتيجة لذلك فإن القضاء الأمريكي لم يستقر على حال بالنسبة لبعض الجرائم التي ترتكب باستخدام الإنترنت من حيث مدى تحديد ما إذا كانت تتطلب قصداً عاماً أم خاصاً، فذلك لا يمانع في تطلب قصد جنائي خاص في جريمة التهديد، إلا أنه يقر من جديد أنه يكفي بالقصد العام عن ذات الجريمة، كما هو الشأن في جريمة التهديد بالبريد الإلكتروني وعبر المجموعات الإخبارية وفق ما هو مقرر في القسم والقصد العام فيها، بينما يتم استدلاء معالمه من النظرة الموضوعية إلى السلوك الشخصي من مجموعة الظروف المحيطة بالجريمة بما في ذلك فحص الحالة العقلية لمرتكب الجريمة[1].

"أما في القضاء الفرنسي فإن منطق سوء النية يكتسح النصوص التي تطبق بشأن الإنترنت، حتى أن هذه الجرائم لا يمكن أن تدخل حيز التطبيق ما لم يتوافر سوء النية في منطق القصد الخاص وإرادة الإضرار، ومن ذلك ما هو مقرر في المادة (15-226 عقوبات فرنسي جديد) التي تشترط سوء النية حين وجود عدوان على البريد الإلكتروني، وبما يجعل ذلك بالضرور متطابقاً مع ما هو مقرر في المادة (L 32-1 II.5) من تقنين البريد والاتصالات الصادر بالقانون المؤرخ 1996/7/26م التي تلزم وزير الاتصالات الفرنسي بالسهر على مبدأ احترام سرية الاتصالات"[2].

"كذلك الحال لدى المشرّع البريطاني، فالركن المعنوي في الجريمة الإلكترونية يتطلب أن تنصرف إرادة الجاني نحو الدخول إلى البيانات أو المعطيات المخزنة في أي حاسوب، إذ

---

[1] إبراهيم، خالد ممدوح، مرجع سابق، ص109.

[2] موسى، مصطفى محمد (2010). دليل التحري عبر شبكة الإنترنت، دار الكتب القانونية، مصر، ص143.

جرم المشرّع البريطاني الدخول غير المصرّح به للنظام الإلكتروني بموجب المادة الأولى من قانون إساءة استخدام الحاسوب البريطاني لعام 1990م، وكذلك جرم الدخول غير المصرّح به إلى النظام الإلكتروني بهدف ارتكاب جريمة أخرى بموجب المادة الثانية من نفس القانون"[1].

المطلب الثاني

تحديد المقصود بأطراف ومحل الجريمة الإلكترونية

سنبحث أولاً في المقصود بأطراف الجريمة الإلكترونية، وثانياً سنبحث في محل هذه الجريمة، من خلال فرعين:

الفرع الأول: أطراف الجريمة الإلكترونية:

لا بدّ للجريمة الإلكترونية كغيرها من الجرائم أن يكون لها فاعل ومجني عليه.

أولاً: الفاعل في الجريمة الإلكترونية:

بالإضافة إلى الشروط العامة الواجب توافرها في مرتكب الجريمة الإلكترونية من سلوك منحرف وعلم وإرادة في نتائج هذا السلوك، ينبغي أن يكون هذا الشخص على درجة معينة من العلم والخبرة العملية في شؤون عالم الحاسوب وتقنية المعلومات، وقد سماه البعض بالمجرم الإلكتروني أو المجرم المعلوماتي[2].

وبهذا المعنى لا يتصور أن يكون الجاني في الجريمة الإلكترونية إلا شخصاً طبيعياً ذا أهلية وقدرة على أن يكون محلاً لتوقيع العقوبة وهو الأمر الذي لا يتصور حدوثه إلا بالنسبة

---

[1] تفصيلاً راجع: الرواشدة، سامي والهياجنة، أحمد (2009). مكافحة الجريمة المعلوماتية بالتجريم والعقاب، المجلة الأردنية في القانون والعلوم السياسية، جامعة مؤتة – الأردن، المجلد (1)، العدد (3)، ص128 وما بعدها.

[2] الشوا، سامي، مرجع سابق، ص517.

للشخص الطبيعي دون الشخص المعنوي[1]، كما لا يتصور أن يكون الجاني هنا إلا شخصاً ذا خبرة ودراية في علم الحاسوب سواء أكان مستخدماً أو مبرمجاً أو مجرد هاو أو محترف لجرائم الحاسوب وتقنية المعلومات[2].

هذا ويتميز الفاعل في الجريمة الإلكترونية بعدد من السمات والخصائص، هي: أنه يتمتع بالمهارة والمعرفة والذكاء، كما أنه إنسان اجتماعي، كذلك يعمل على تبرير ارتكاب جريمته وفي الوقت ذاته يتولد لديه شعور بالخوف من كشف جريمته، كما أن الفاعل في هذه الجريمة يتمتع بالسلطة تجاه النظام الإلكتروني.

ثانياً: المجني عليه في الجرائم الإلكترونية:

إذا كان الغالب الأعم بأن مرتكب الجريمة الإلكترونية يكون شخصاً طبيعياً، فإن المجني عليه هنا هو بالغالب الأعم شخص معنوي كالبنوك والشركات الكبرى والمؤسسات الحكومية والوزارات والمنظمات والهيئات المالية، وغيرها من الأشخاص الاعتبارية التي تعتمد في إنجاز أعمالها على الحواسيب[3].

حيث يصعب تصور وقوع الجريمة الإلكترونية بالنسبة للأفراد العاديين وإن كان ذلك غير مستبعد، إذ قد يتعرض الفرد العادي لشكل من أشكال الجريمة الإلكترونية فيما إذا كان من بين الأشخاص الذين يحفظون أسرارهم التجارية وأعمالهم وشؤونهم داخل الحاسوب الخاص به، ونبغي لقيام الجريمة الإلكترونية في هذا الفرض أن يكون الشخص العادي (المجني عليه) هنا من بين الأشخاص الذين قد ينجذب إليهم الجناة كأن يكون ذا منصب

---

[1] سلامة، محمد عبد الله، مرجع سابق، ص63.

[2] الزيدي، وليد (2009). القرصنة على الإنترنت والحاسوب، دار أسامة للنشر، عمان، ط3، ص54.

[3] قاسم، محمد عبد الله (2010). الحماية الجنائية للمعلومات الإلكترونية، دار الكتب القانونية، مصر، ط1، ص148.

سياسي رفيع أو رجل أعمال مرموق أو صاحب شهرة عالمية في قطاع من القطاعات الاقتصادية أو الاجتماعية العسكرية[1].

وعلى الرغم من إمكانية تعرض الجميع للجريمة الإلكترونية سواء أكانوا أشخاصاً معنوية أو طبيعية إلا أن معظم الجرائم الإلكترونية ترتكب من أجل أمرين وهما: المال والمعلومات، وبالتالي يمكن القول بأن الغالبية العظمى من المجني عليهم في الجرائم الإلكترونية هم إما مؤسسات مالية كالبنوك والمصارف وشركات الصرافة، وإما شركات المعلومات بصرف النظر عن نوع هذه المعلومات أو قيمتها إذ قد تكون بالغة الأهمية كالمعلومات العسكرية والمخابراتية، وقد تكون معلومات رياضية أو فنية أو اجتماعية بسيطة[2].

إن تحديد نطاق خاص يضم كافة فئات المجني عليهم في الجرائم الإلكترونية يعد أمراً صعباً بسبب حقيقة أن المجني عليهم في هذه الجرائم غالباً من يكتشفونها بعد حصولها، الأمر الذي دفعهم في غالب الأحيان إلى السكوت والإذعان لها وتفضيل هذا الموقف السلبي عن القيام بالتصريح عن تعرض أجهزتهم ومعلوماتهم التي يفترض فيها الأمان والسرية إلى الدخول غير المشروع والانتهاك[3]، وهو الأمر الذي يشكل بحد ذاته سبباً في ازدياد معدل الجرائم الإلكترونية وصعوبة اكتشافها أو الحد منها، ومن ثم كثرة مشكلاتها ثم الصعيد القانوني والعملي.

---

(1) الدسوقي، محمد (2003). الحماية الجنائية لسرية المعلومات، دار الفكر العربي، القاهرة، ط1، ص56.

(2) الشوا، سامي، مرجع سابق، ص158.

(3) الخوالدة، محمد، مرجع سابق، ص50.

الفرع الثاني: محل الجريمة الإلكترونية:

لعل الجرائم الإلكترونية تستهدف أحد أو كل العناصر التالية[1]:

أولاً: المعلومات:

تشمل الجرائم الإلكترونية في هذه الحالة سرقة أو تغيير أو حذف المعلومات، فمثلاً في حالة النشاط الجرمي الذي يستهدف اختراق بريد إلكتروني والعبث بمحتوياته، أو سرقة المعلومات المخزنة في موقع ما والاستفادة منها بما يحمل في طياته بعضاً من انتهاك الخصوصية وحقوق الملكية الفكرية وأنماطاً جرمية أخرى.

ثانياً: الأجهزة:

تشمل الجرائم الإلكترونية في هذه الحالة تعطيل أجهزة الكمبيوتر أو تخريبها عبر إرسال الفيروسان أو البرامج التي تحوي أنظمة هجومية مما يسبب تلفاً في أنظمة الكمبيوتر يؤدي لشلل كل الأنشطة المرتبطة بهذا الجهاز أو الأنظمة المرتبطة به.

ولنتصور مدى الدمار والخسائر التي ستلحق بشبكة مصارف مرتبطة بأنظمة عبر كمبيوتر مركزي يحوي حسابات علماء، فما الذي سيحصل لو تم تعطيل الكمبيوتر المركزي أو إتلاف أنظمته؟

"فمثلاً في الولايات المتحدة الأمريكية أصدر مكتب التحقيقات الفيدرالي الأمريكي إنذاراً عاماً يحذر مستخدمي الإنترنت من مخاطر رسائل إلكترونية جديدة، تنطوي على فخ،

---

[1] الملط، أحمد خليفة (2006). الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط2، ص167 وما بعدها.

يدفع المستخدمين إلى الكشف عن بيانات حساباتهم المالية الشخصية، ليصار لاحقاً إلى السطو عليها"[1].

"وحذرت دائرة شكاوى جرائم الإنترنت التابعة للمكتب الفيدرالي، من ظهور مجموعة من الرسائل الإلكترونية التي تزعم أن المتلقي قد قام بعمليات شراء لبضائع عبر الشبكة، وتستدرجه للكشف عن بيانات حساباته، وقالت الدائرة إن نموذجين من تلك الرسائل تم رصدهما، تدعي الأولى أن المتلقي قد عقد طلبية لشراء جهاز كمبيوتر عبر الشبكة، وتطلب منه في حال عدم رغبته بإتمام الطلبية الدخول إلى وصلة البيانات الشخصية لإلغائها، وسيجد متصفح البريد الإلكتروني الذي يدخل تلك الوصلة معلومات شخصية حول حساباته المالية، يتوجب عليه الكشف عنه لإلغاء عملية الشراء المزعومة، وبذلك يحقق أصحاب تلك الرسائل هدفهم، أما النموذج الثاني فيتضمن بيان كشف مشتريات مرسلة كملف PDF، تحتوي على فيروس يتسلل إلى جهاز الكمبيوتر الشخصي للمتلقي، ما أن يقوم بالدخول وتشغيل الرسالة لقراءتها"[2].

ثالثاً: الأشخاص أو الجهات:

تهدف فئة كبيرة من الجرائم الإلكترونية أشخاص أو جهات بشكل مباشر كالتهديد أو الابتزاز أو السرقة أو ممارسة الفاحشة. فمثلاً سرقة المال عبر الإنترنت باستخدام أرقام لبطاقات مصرفية تعود للغير، أو الحض على الفجور وممارسة الفاحشة مع قاصر عبر

---

[1] تمام، أحمد (2009). الحماية الجنائية للحاسب الآلي، دار النهضة العربية، القاهرة، ص270.

[2] تمام، أحمد، مرجع سابق، ص271.

الإنترنت، أو الإرشادات التي تحمل في طياتها تعليمات إرهابية كلها موجهة ضد أشخاص أو جهات بعينها[1].

المطلب الثالث

الآليات التي تنفذ بها الجريمة الإلكترونية

الواقع أن هناك دوراً تلعبه وسائل الاتصال الإلكترونية في مجال ارتكاب الجرائم الإلكترونية وفي مجال اكتشافها، وذلك على النحو الآتي:

أولاً: قد تكون شبكة الإنترنت هدفاً للجريمة، وذلك كما في حالة الدخول غير المصرّح به إلى أنظمة البيانات في مواقع إلكترونية معينة لتدمير المعطيات أو الاستيلاء على البيانات المخزنة أو المنقولة عبر النظم، أو أن يتم إخفاء هذا النشاط الجرمي بإعادة إنتاج وطرح هذه البيانات عبر نفس الشبكة ولمشتركين يستخدمون الدفع عبر الإنترنت وهكذا، وهذا ما أكده المشرّع الأردني في المادتين (3، 4) من قانون جرائم أنظمة المعلومات.

ثانياً: قد تكون شبكة الإنترنت أداة الجريمة لارتكاب جرائم إلكترونية عبرها فقط، كما في حالة استغلال الإنترنت للاستيلاء على الأموال بإجراء تحويلات غير مشروعة أو استخدام التقنية في عمليات التزييف والتزوير، أو استخدام التقنية في الاستيلاء على أرقام بطاقات ائتمان وإعادة استخدامها والاستيلاء على الأموال بواسطة ذلك، ومن ثم الدخول في عمليات دفع إلكترونية وشراء عبر الإنترنت لإخفاء المصدر الحقيقي غير المشروع للأموال القذرة، وقد نص المشرّع الأردني على تجريم مثل هكذا حالات بموجب المادة (6) من قانون جرائم أنظمة المعلومات. ولعل أبرز ما يمكن أن نشاهده

---

[1] الجنيهي، منير محمد، والجنيهي، ممدوح محمد (2005). بروتوكولات وقوانين الإنترنت، دار الفكر الجامعي، الإسكندرية، ط1، ص76-77.

في هذا الإطار أنشطة غسل الأموال التي تتم عبر الإنترنت وما يرتبط بها من عمليات معقدة ظاهرها التجارة الإلكترونية والتعاقد عبر الإنترنت وباطنها إخفاء المصادر الحقيقية غير الشرعية للأموال.

ثالثاً: وقد تكون شبكة الإنترنت هي البيئة التي ينمو في رحمها الإجرام المعلوماتي وذلك كما في إبرام اتفاقيات لترويج المخدرات وأنشطة الشبكات الإباحية والإرهابية وغسل الأموال[1].

رابعاً: أما من حيث دور شبكة الإنترنت في اكتشاف الجريمة الإلكترونية التي تتم عبر الشبكة، فإن الإنترنت يستخدم الآن على نطاق واسع في تتبع الجرائم، عوضاً عن أن جهات إنفاذ القانون تعتمد على النظم التقنية في إدارة المهام من خلال بناء قواعد البيانات المشتركة وأطر التعاون الدولي، ومع تزايد نطاق الجرائم الإلكترونية، واعتماد مرتكبيها على وسائل التقنية المتجددة والمتطورة، فإنه أصبح لزاماً استخدام نفس وسائل الجريمة المتطورة للكشف عنها، من هنا تلعب شبكة الإنترنت ذاتها دوراً رئيساً في كشف الجرائم الإلكترونية والإنترنت وتتبع فاعليها، بل وإبطال أثرها[2].

خامساً: إن كثرة وسائل التواصل الاجتماعي في وقتنا الحاضر وتنوعها وجدت احتمالاً قل نظيره في ارتكاب الجرائم الإلكترونية، ولعل "تويتر" يعدّ من أبرز هذه الوسائل الذي

---

(1) عبد الله، عبد الله عبد الكريم، مرجع سابق، ص21، وراجع أيضاً: نصوص المواد (8، 9، 10) من قانون جرائم أنظمة المعلومات الأردني.

(2) الرومي، محمد أمين (2003). جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، ص64.

اكتسح مجال العالم الافتراضي بعد أن اقتنع مرتكبو الجرائم الإلكترونية بأنه وسيلة فعّالة لارتكاب هذه الجرائم وذلك من خلال تفريداتهم وسهولة كتابتها وإرسالها[1].

هذا ويجب عدم الخلط بين دور الوسائل الإلكترونية في الجريمة الذي يكون إما الهدف المباشر للاعتداء، أو وسيلة الاعتداء، أو تكون بيئة ومخزن للجريمة، وبين محل الجريمة السابق بيانه الذي يكون دائماً المعلومات والأجهزة والأشخاص والهيئات إما بذاتها أو بما تمثله.

---

[1] انظر في هذا المعنى: الحسيني، محمد (2013). مقال بعنوان: "مختصون يطالبون بتشريع خاص للجرائم الإلكترونية في الكويت، منشور في محليات جريدة "هنا الكويت" الصادرة في 12 فبراير، ص3.

الفصل الثالث

المشكلات الموضوعية والإجرائية المتعلقة بالجريمة الإلكترونية

تعدّ الجرائم الإلكترونية من أكبر التحديات التي نواجهها في وقتنا الحاضر، والحديث عن المشكلات القانونية والعملية التي تثيرها هذه الجرائم، لا بدّ لنا من بيان المشكلات الموضوعية والإجرائية المتعلقة في هذه الجرائم، لذلك سأقسم هذا الفصل إلى مبحثين:

المبحث الأول: المشكلات الموضوعية التي تثيرها الجريمة الإلكترونية.

المبحث الثاني: المشكلات الإجرائية التي تثيرها الجريمة الإلكترونية.

المبحث الأول

المشكلات الموضوعية التي تثيرها الجريمة الإلكترونية

تعدّ الجرائم الإلكترونية نوعاً مستحدثاً من الجرائم التي تتحدى القواعد التقليدية للتجريم والعقاب التي تتطلب ضرورة تحقق أركان الجريمة، لذلك فإن هذا النوع من الجرائم يثير مشكلات قانونية وعملية من الناحية الموضوعية، وهذه المشكلات ترتبط بدورها في صور الجرائم الإلكترونية.

لذلك سأبحث المشكلات الموضوعية التي تثيرها الجرائم الإلكترونية في إطار صور هذه الجرائم، وهنا لن أتعرض لجميع الجرائم التي يتناولها قانون العقوبات سواء في الأردن أو في الكويت، بل سأعرض للحالات التي تثير مشكلة في تطبيق النصوص القانونية، وبخاصة في القانون الكويتي، وذلك عائد إلى الفراغ التشريعي لمواجهة هذه الجرائم في دولة الكويت بخلاف الوضع لدى المشرّع الأردني، إذ يوجد قانوناً خاصاً يعالج هذا النوع من الجرائم، هو قانون جرائم أنظمة المعلومات المؤقت رقم (30) لسنة 2010م.

ولأن المجال لا يتسع للحديث عن كل أنواع الجرائم الإلكترونية، فقد اخترت أكثرها إثارة للمشكلات القانونية وهي: جرائم الاعتداء على الحياة الخاصة، وجرائم الاعتداء على الأموال، وجريمة التزوير، وجريمة سرقة المال المعلوماتي، وسأبحث المشكلات التي تثيرها هذه الصور في أربعة مطالب.

المطلب الأول

المشكلات المتعلقة بجرائم الاعتداء على الحياة الخاصة للأفراد

المقصود من التطرق لموضوع جرائم الاعتداء على الحياة الخاصة للأشخاص التعرض لتلك الجرائم التي يتعذر علينا مواجهتها بالنصوص التقليدية، فالاعتداء عليها يتم بواسطة هذه التقنية التي أدت إلى سلب مادية السلوك ومناقشة الحالات التي تثيرها مشكلة في تطبيق النصوص التقليدية في قانون الجزاء الكويتي رقم (16) لسنة 1960م، وتكشف مدى الحاجة إلى التصدي التشريعي لهذا النوع من الجرائم وهي جرائم الاعتداء على الحياة الخاصة.

إن عناصر الحق في الحياة الخاصة تتكون من عناصر ليست محل اتفاق بين الفقهاء، فيمكن القول بأنها تشمل حرمة جسم الإنسان، والمسكن، والصورة، والمحادثات، والمراسلات، والحياة المهنية[1].

أما علاقة الحياة الخاصة بالتقنية الإلكترونية فقد ظهرت أهميتها بانتشار بنوك المعلومات في الآونة الأخيرة لخدمة أغراض متعددة وتحقيق أهداف المستخدمين في المجالات العلمية والثـــقافية والعسكرية[1].

---

[1] كايد، أسامة عبد الله (1999). الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، ص48.

هكذا أصبحت الشبكات الإلكترونية مستودعاً خطيراً للكثير من أسرار الإنسان التي يمكن الوصول إليها بسهولة وسرعة لم تكن متاحة في ظل سائر وسائل الحفظ التقليدية، فأصبحت بنوك المعلومات أهم وأخطر عناصر الحياة الخاصة للإنسان في العصر الحديث.

وعليه، فإن القوانين المقارنة اهتمت بهذه المسألة، ففي فرنسا أصدر المشرّع القانون رقم (17) لسنة 1978م الخاص بالمعالجة الآلية للبيانات والحريات، وتضمن الباب الأول من ذلك القانون مجموعة من المبادئ القانونية التي أشارت إلى أن المعالجة الإلكترونية للبيانات يجب أن تكون لخدمة المواطن فقط، ولا يجوز أن تتضمن اعتداءات على شخصيته أو حياته الخاصة وحرياته، وفي الباب الثاني من ذاك القانون أنشئ ما أطلقت عليه اللجنة القومية الخاصة بمراقبة تنفيذ أحكام هذا القانون ووجوب استشارة اللجنة قبل معالجة البيانات، وتطبيقاً لذلك قضت محكمة (Nantes) بتاريخ 1985/12/16م بإدانة شخص قام بإجراء معالجة إلكترونية للبيانات الشخصية دون الأخطار السابق لهذه اللجنة[2]، وورد في القانون استثناءان: الأول يتعلق بحالة جمع البيانات الضرورية في إثبات الجرائم، وبشرط أن يكون هذا التخزين لدى جهات قضائية أو لدى السلطات العامة، فلا يجوز لجهات القطاع الخاص وغير الجهات المشار إليها بصفة عامة إدخال مثل هذه البيانات إلى الحاسب الآلي الخاص بها، والثاني يتعلق بحرية الصحافة بنشر البيانات الشخصية المعالجة في موضوع معين في إطار حرية التعبير[3].

أما في أمريكا، فهناك أكثر من قانون لحماية البيانات أو الحياة الخاصة، فكان أول قانون صادر بهذا الخصوص سنة 1970م لحماية البيانات وحق الوصول إليها لتصحيح

---

(1) سلامة، محمد عبد الله، مرجع سابق، ص69.

(2) نقلاً عن: قايد، أسامة، مرجع سابق، ص65.

(3) العبابنة، محمود أحمد، مرجع سابق، ص76.

البيانات غير الصحيحة، ثم صدر القانون الخاص بالخصوصية سنة 1974م ثم استمرت التعديلات المتلاحقة بهذين القانونين، وجاء في هذا القانون الأخير أن الهدف منه هو حماية الحياة الخاصة للمواطن الأمريكي في مواجهة الحاسب الآلي الذي بات يهدد الحياة الخاصة وبشكل متزايد، وجاء في المادة 552/أ على أنه لا يجوز لأية جهة (وكالة) أن تنشئ أي معلومات يتضمنها نظام للمعلومات بأي وسيلة من وسائل الاتصال لأي شخص أو لأية جهة أخرى ما لم يكن ذلك بناءً على طلب كتابي وبموافقة صاحب الشأن الذي تتعلق به المعلومات، وتم إيراد استثناءات على هذا النص في حالة ما إذا كان ذلك تحقيقاً للمصلحة العامة أو إجابة لأمر المحكمة، كذلك صدر في الولايات المتحدة قانون خصوصية الاتصالات الإلكترونية سنة 1986م[1].

أما في بريطانيا، فالحال لديها مختلف عن فرنسا وأمريكا، إذ إن إنجلترا ترفض أن تعترض باستقلالية الحق في الحياة الخاصة، وفي قضية كوريللي ضد وول الشهيرة التي قام المدعي عليهم فيها بنشر وبيع صور المدعية دون إذنها الأمر الذي دفعها للقضاء وطلب التعويض وإيقاف النشر والبيع، رفضت المحكمة الحكم لها على أساس أن ادعاءها لا يرتكز إلى أي أساس من القانون، وليس هناك نص يجرم هذا، إضافة إلى أن نشر الصورة لا ينطوي على تشهير بالمدعية، وتبعاً لذلك فلقد سار القضاء الإنجليزي على هذا المنوال في العديد من الأحكام مستندة في ذلك إلى أن فكرة الخصوصية في حد ذاتها فكرة هلامية غير محددة المضمون، وتمس مسائل حساسة دستورية وسياسية، ولا أساس قانوني لإمكانية الإضرار به،

---

[1] قشقوش، هدى (2007). جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة، ص160.

ومن الصعوبة بمكان وضع حدود فاصلة بين ما يعد من العموم، ما يعد من الخصوص ولا توجد سوابق قضائية في هذا الخصوص[1].

غير أن هذا الاتجاه لا يمكن أن نأخذ به على إطلاقه في إنجلترا، فهناك العديد من النصوص التي تحمي الحياة الخاصة متناثرة بين القانونين المدني والجنائي، كنصوص التشهير والقذف الواردة في قانون العقوبات الإنجليزي، ونصوص التعدي على ملكية الغير، والمضايقات، والإخلال بالثـــقة، وقانون التلغراف السلكي عام 1949م، وقانون البريد العام 1967م[2].

أما على مستوى التشريعات العربية، ففي الأردن لا يوجد هناك قوانين خاصة لحماية الحياة الخاصة، وإنما هناك مجموعة من النصوص القانونية المتناثرة التي تنتشر في قانون العقوبات وقانون أصول المحاكمات الجزائية، ففي قانون العقوبات رقم (16) لسنة 1960م وتعديلاته، ورد بنص المادة (355) عقوبة من يقوم بإفشاء أسرار تحصل عليها بحكم وظيفته أو إبقاءها في حيازته بعد انتهاء عمله، ثم قام بإفشائها، وكذلك ورد بنص المادة (356) من ذات القانون عقوبة من كان يعمل بمصلحة البرق والبريد ويقوم بالاطلاع على الرسائل والاستماع إلى المحادثات الهاتفية.

وفي قانون أصول المحاكمات الجزائية الأردني رقم (9) لسنة 1961م وتعديلاته وردت عدة مواد قانونية تنظم عملية القبض على المتهم وتفتيش بيته أو تفتيشه شخصياً واستجوابه بهدف عدم المساس بحريته الشخصية وحياته الخاصة المادة 348 مكررة.

---

(1) الرواشدة، سامي والهياجنة، أحمد، مرجع سابق، ص143.

(2) العبابنة، محمود أحمد، مرجع سابق، ص78.

إلا أنه وبعد أن أصدر المشرّع الأردني قانون جرائم أنظمة المعلومات المؤقت رقم (30) لسنة 2010م، فقد أورد جرائم إلكترونية تتعلق بالخصوصية وبشكل خاص بالنسبة للشخصيات العامة أو البيانات المتصلة بالحياة الخاصة وتشمل جرائم الاعتداء على المعطيات السرية أو الخاصة، وجرائم الاعتداء على البيانات الشخصية المتعلقة بالحياة الخاصة[1].

وكذلك جرم المشرّع الأردني فعل التنصت أو التقاط أو اعتراض الرسائل، فكل من يتنصت لأي رسائل عن طريق شبكة المعلومات أو أجهزة الحاسوب أو يلتقطها أو يعترضها دون تصريح يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على سنة أو بغرامة لا تقل عن 200 دينار ولا تزيد على 1000 دينار أو بكلتا العقوبتين[2].

أما في مصر، فلقد أضاف المشرّع المادة (309 مكرر) إلى قانون العقوبات المصري بموجب القانون رقم (37) لسنة 1972م والتي تعاقب بالحبس مدة لا تزيد على سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن، كذلك أضاف المشرّع المصري جريمة جديدة ضمنها المادتين (21، 22) من القانون رقم (96)، فبشأن تنظيم سلطة الصحافة حيث جاء فيهما عقاب الصحفي الذي يتعرض للحياة الخاصة للمواطنين وفرض عقوبة الحبس سنة والغرامة التي لا تقل عن 5000 جنيه ولا تزيد على 10.000 جنيه أو بأحدهما[3].

أما في دولة الكويت فلا يوجد قانون خاص يجرم على أساسه الأفعال التي تستهدف الحياة الخاصة من خلال نظم ووسائط وشبكات إلكترونية، وهذا يعني أن المشرّع الكويتي ما

---

[1] راجع: المادتين (3، 5) من قانون جرائم أنظمة المعلومات الأردني، وانظر أيضاً المادة (76) من قانون الاتصالات الأردني رقم (13) لسنة 1995م.

[2] بموجب المادة (5) من قانون جرائم أنظمة المعلومات الأردني.

[3] نقلاً عن: رمضان، مدحت (2007). جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، ص11-12.

زال متأخراً كثيراً في اللحاق بالمشرّع الأردني بهذا الخصوص، خاصة بعد أن صدر القانون العربي النموذجي لجرائم الكمبيوتر عام 2009م.

وعليه، فما حدود الحماية الجنائية للحياة الخاصة في التشريع الكويتي؟

تتمثل النصوص الجنائية في التشريع الكويتي التي صيغت لحماية الحياة الخاصة في تجريم الأفعال التالية:

أولاً: أول هذه الجرائم هي جريمة انتهاك حرمة المسكن التي نصت عليها المادة (255) من قانون الجزاء، وذلك لما للمسكن من أهمية كبرى في نظر المشرّع الكويتي، لا لأن للمسكن حرمة كبرى فقط، لكن لأن المسكن في ثــقافة المشرّع الذي وضع هذا النص يمثل قلعة حصينة لا يمكن اختراقها إلا بالدخول المادي غير المشروع و/أو دون رغبة صاحبه.

أما جريمة الاطلاع على الرسائل فقد نصت عليها المادة (37) من نفس القانون أن "يعاقب بالحبس مدة لا تقل عن 6 أشهر كل موظف عمومي تابع لمصلحة البريد أو التلفون أخفى أو أوقف رسالة أو اطلع عليها وأفشى للغير ما حوته، ويراد من الرسالة المكاتبات والمحادثات التلفونية والبرقيات وما إلى ذلك من وسائل الإرسال"، أما إذا ارتكب الأفعال المذكورة أشخاص آخرون فتكون العقوبة الحبس مدة لا تزيد على ستة أشهر أو الغرامة التي لا تتجاوز عشرين جنيهاً على أن يكون ذلك بناءً على شكوى الطرف المتضرر، فإذا كان المشرّع الكويتي قد توسع في مفهوم الرسالة حيث يمكننا تطبيق مفهومها في هذا النص على رسائل البريد الإلكتروني، إلا أن هذه الحماية لا يمكن أن تمتد إلى البيانات المخزنة في أي نظام من نظم المعلومات لأي جهة أخرى سواء كانت عامة أو خاصة، فالحاسب الآلي اليوم لم يعد جهازاً للاتصال ومعالجة المعلومات فقط، بل أصبح مستودعاً ضخماً للمعلومات والبيانات

في آن واحد، كذلك ما نصت عليه المادة (78) من قانون الإجراءات الجنائية الكويتي رقم (17) لسنة 1960م بأنه: "للأشخاص ومساكنهم ورسائلهم حرمة وحرمة الشخص تحمي جسمه وملابسه وما يوحد معه من أي متعة، وحرمة المسكن تشمل كل مكان مسور أو محاط بأي حاجز مستعمل أو معد للاستعمال كمأوى، وحرمة الرسالة تمنع الاطلاع على الرسائل البريدية أو البرقية أو الهاتفية أثناء نقلها أو انتقالها من شخص إلى آخر".

ثانياً: نص المشرّع الكويتي كذلك على جريمة إذاعة معلومات تتعلق بإجراء جنائي في المادة (143) من قانون الإجراءات الجنائية، وهنا الحماية مقتصرة على الإجراءات الجنائية.

أما جريمة إفشاء أسرار الوظيفة المنصوص عليها في المادة (355) من قانون الجزاء الكويتي، فتتمثل في "كل موظف عمومي يخل بواجبات وظيفته أو يسيء استعمالها بأن يفشي معلومات سرية أو يسهل بأي طريقة كانت الوصول إلى الإفشاء بها"، ويتضح من هذا النص أنه يتضمن شرطاً مفترضاً يتمثل في أن الجاني في هذه الجريمة موظفاً عمومياً بالإضافة إلى أن هذه الحماية تقتصر على المعلومات الرسمية، ومن ثم تكون هذه الحماية قاصرة على حماية البيانات الاسمية أو الشخصية غير الرسمية والمخزنة في نظم المعلوماتية معينة وهو ما نصل معه إلى عدم وجود أي نص يتعلق بحماية المعلومة أو البيانات الخاصة بصفة عامة بغض النظر عن مصدرها وعن النظام الإلكتروني المخزنة فيه، سواء تم جمعها من قبل الموظف العام أم غيره.

وفي الكويت، نجد أن مرسوم تنظيم سوق الكويت للأوراق المالية رقم (7) لسنة 2010م أنشأ في المادة الخامسة منه لجنة برئاسة وزير التجارة والصناعة وهي مسؤولة بصفة خاصة عن اتخاذ ما يلزم من إجراءات نحو العمليات المشكوك في سلامتها، والتي تتم بعد استغلال المعلومات غير المعلنة، كذلك قانون الشركات التجارية الكويتي الجديد رقم (25)

لسنة 12، الذي نص في المادة (2/140) على عدم جواز قيام ممثل الشخص الاعتباري باستغلال المعلومات التي وصلت إليه بحكم موقعه.

خلاصة القول: إن المشرّع الكويتي يفرد قانوناً خاصاً لحماية خصوصية الإنسان، كما فعل المشرّع الأردني وبعض التشريعات الغربية التي تتعلق بالخصوصية في قوانين العقوبات والإجراءات والشركات التجارية والأوراق المالية، وبمجمل هذه النصوص لم نجد نصاً تشريعياً واحداً يتعلق بحماية الحياة الخاصة من مخاطر الحاسب الآلي وبنوك المعلومات.

تجدر الإشارة هنا إلى معاهدة بودابست لسنة 2001م التي تهدف إلى توحيد الجهود الدولية لمكافحة جرائم الكمبيوتر التي تضمنت العديد من التعريفات للأفعال المجرمة تاركة لكل دولة تحديد العقوبة التي تراها مناسبة للفعل.فنصت المادة (2) منها على تجريم الدخول غير المشروع إلى أي نظام معلوماتي، ونصت المادة (3) منها على أن تجرم الدول الأعضاء كل اعتراض لهذه البيانات بأي وسيلة إلكترونية دون وجه حق، أما المواد (4) وما بعدها فنصت على تجريم أي تعديل في البيانات أو تحريفها أو تدميرها أو تعديلها أو تغيير مسارها، كما نصت المادة (5) على تجريم التدخل في النظام المعلوماتي والعمليات المنطقية، ونصت المادة (6) على إساءة استخدام النظام المعلوماتي بشكل يؤدي إلى إفشاء نظم الحماية الخاصة به دون وجه حق.هكذا نجد أنه على المشرّع الكويتي التدخل بالحماية الجنائية اللازمة لأن عناصر الحياة الخاصة لم تعد تقتصر على المسكن، والصورة، والمحادثات الهاتفية أو الرسائل البريدية، فتقنية المعلومات في عصر العولمة قد أفرزت عناصر مستحدثة للخصوصية يجب أن تشكل مراكز قانونية جديدة في حاجة ماسة للحماية.

هكذا نجد أن الحق في الحياة الخاصة بعناصره المستحدثة غير مشمول بالحماية الجنائية اللازمة في التشريع الكويتي، فهل تحظى الأموال بهذا القدر من الحماية الجنائية؟

المطلب الثاني

المشكلات المتعلقة بجرائم الاعتداء على الأموال

إذا كان قانون الجزاء الكويتي شأنه شأن كل قوانين العقوبات الأخرى قد جرم الاعتداء على الأموال في صورها التقليدية كالسرقة، والنصب، وخيانة الأمانة، واختلاس الأموال العامة، فقد كان ذلك في ظل عصر لا يعرف سوى النقود الورقية أو المعدنية وما يحل محلها من صكوك أو أوراق مالية كالكمبيالات، والسند الأذني في عصر المصارف التقليدية ذات المقر المحدد مكانياً، وقد كان أقصى ما وصلت إليه من تقدم متمثلاً في إجراء التحويلات المصرفية بإجراءات ورقية معقدة ومقابل رسوم مالية معينة[1]، فإذا كان الركن المادي للسرقة المتمثل في الاختلاس يمكن أن يطبق على التحويلات المالية غير المشروعة التي تتم عبر المصارف التقليدية، فذلك لأن جريمة السرقة من الجرائم ذات القالب الحر لم يحدد المشرّع شكل السلوك الإجرامي لها، يمكن أن يتم بأي فعل يؤدي إلى حرمان المجني عليه من المال المنقول وإدخاله في حيازة الجاني، كذلك الحال بالنسبة لجريمة النصب، حيث يتحقق السلوك الإجرامي لها بالاستيلاء على أموال الآخر بالطرق الاحتيالية[2]، فهل ينطبق ذلك على جرائم السرقة والاحتيال التي ترتكب عن طريق التقنية الإلكترونية؟

وسأقوم بعرض الوسائل الفنية التي يتم عن طريقها الاختلاس قبل أن نعرض تكييفها القانوني في ظل الفراغ التشريعي في الكويت؛ وذلك في فرعين:

---

(1) العنزي، سليمان بن مهجع (2003). وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، ص113.

(2) نجم، محمد صبحي (2010). قانون العقوبات، القسم الخاص، دار الثـقافة، ط1، الإصدار الثامن، ص254.

الفرع الأول: الوسائل الفنية للتحويل الإلكتروني للأموال:

يتم التحويل غير المشروع للأموال بعدة وسائل يصعب حصرها لسرعة وتيرة التطور في هذا المجال، لكن يمكن الإشارة إلى أكثرها انتشاراً[1].

أولاً: استخدام برامج معدّة خصيصاً لتنفيذ الاختلاس: أشهر هذه الوسائل هو تصميم برامج معينة تهدف إلى إجراء عمليات التحويل الآلي من حساب إلى آخر سواء كان ذلك من المصرف نفسه أو من حساب آخر في مصرف آخر على أن يتم ذلك في وقت معين يحدده مصمم هذا البرنامج، وأشهر هذه الوقائع قيام أحد العاملين بمركز الحاسبات المتعاقد مع مصرف الكويت التجاري لتطوير أنظمة المعلومات بالاستيلاء على مبالغ طائلة من المصرف بعد أن تمكن من اختيار خمسة حسابات راكدة في خمس فروع محلية للمصرف وأعدّ لها برنامجاً تمثلت مهمته في تحويل مبالغ معينة من هذه الحسابات إلى حسابات أخرى فتحت باسمه في الفروع نفسها على أن تتم عملية التحويل أثناء وجوده بالطائرة في طريقه إلى المملكة المتحدة عائداً إلى بلاده بعد انتهاء عقد عمله، ثم فتح حسابات أخرى فور وصوله وطلب من المصرف تحويل هذه المبالغ إلى حساباته الجديدة في بريطانيا[2]، كما توجد برامج أخرى تقوم بخصم مبالغ ضئيلة من حسابات الفوائد على الودائع المصرفية بإغفال الكسور العشرية بحيث يتحول الفارق مباشرة إلى حساب الجاني، لأنها برامج تعتمد على التكرار الآلي لمعالجة معينة مما يؤدي إلى صعوبة اكتشاف هذه الطريقة رغم ضخامة المبلغ، وهو أن هذه الاستقطاعات

---

(1) انظر تفصيلاً في هذه الصور: الفيل، علي عدنان (2012). جريمة الاحتيال عبر البريد الإلكتروني، مجلة الحقوق، الكويت، العدد 2، السنة 36، ص148-154.

(2) العنزي، سليمان، مرجع سابق، ص103.

تتم على مستوى آلاف الأرصدة في وقت واحد مع ضآلة المبلغ المخصوم من كل حساب على حدة، بحيث يصعب أن ينتبه إليه العميل[1].

ثانياً: التحويل المباشر للأرصدة: يتم ذلك عن طريق اختراق أنظمة الحاسب وشفرات المرور، وأشهرها قيام أحد خبراء الحاسب الآلي في الولايات المتحدة باختراق النظام المعلوماتي لأحد المصارف وقيامه بتحويل 12 مليون دولار إلى حسابه الخاص في ثلاث دقائق فقط، وعادة ما يتم ذلك أيضاً عن طريق إدخال معلومات مزيفة وخلق حسابات ومرتبات وهمية وتحويلها إلى حساب الجاني، ويمكن أن يتم التحويل المباشر أيضاً عن طريق التقاط الإشعاعات الصادرة عن الجهاز إذا كان النظام المعلوماتي متصلاً بشبكة تعمل عن طريق الأقمار الصناعية، فهناك بعض الأنظمة التي تستخدم طابعات سريعة تصدر أثناء تشغيلها إشعاعات إلكترومغناطيسية ثبت أنه من الممكن اعتراضها والتقاطها أثناء نقل الموجات وحل شفراتها بواسطة جهاز خاص لفك الرموز وإعادة بثها مرة أخرى بعد تحويرها[2]، وهو ما نصت عليه اتفاقية بودابست في المادة (5) كما سبق أن ذكرنا.

ثالثاً: التلاعب بالبطاقات المالية: لقد ظهرت أولى هذا النوع من الاحتيال بالتقاط الأرقام السرية لبطاقات الائتمان وبطاقات الوفاء المختلفة من أجهزة الصرف الآلي للنقود إلى أن ظهرت الصرافة الآلية، أما جرائم الاعتداء على هذه البطاقات فتتمثل في استخدامها من قبل غير صاحب الحق بعد سرقتها أو بعد سرقة الأرقام السرية الخاصة بها وهو ما

---

(1) الحسيني، عمر الفاروق (1995). المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي، دار النهضة العربية، القاهرة، ص43-44.

(2) الشوا، محمد سامي (1994). ثورة المعلومات وانعكاسها على قانون العقوبات، دار النهضة العربية، القاهرة، ص70-72.

يتم عن طريق اختراق بعض المواقع التجارية التي يمكن أن تسجل عليها أرقام هذه البطاقات، وفي هذا النوع من الاعتداءات لا نجد صعوبة في تطبيق نصوص جرائم السرقة والنصب عليها سواء تم ذلك عن طريق سرقة البطاقة نفسها، أو عن طريق سرقة الرقم السري واستخدامه استخداماً غير مشروع للتحايل على المؤسسات المالية وصرف هذه المبالغ خاصة أن النموذج التجريمي لجريمة النصب لم يشترط في الوسائل الاحتيالية أن تكون مرتكبة ضد الإنسان، فيكفي أن ترتكب هذه الوسائل الاحتيالية ضد الآلة ما دامت تؤدي إلى الحصول على نفع غير مشروع إضراراً بالآخر، وهو ما نصت عليه المادة (217) والمادة (249) من قانون الجزاء الكويتي تحت عنوان: السرقة والنصب والإتلاف والقرصنة.

رابعاً: جرائم الاعتداء على أجهزة الصرف الآلي للنقود: تثور هذه المشكلة في حالة استخدام الجهاز لصرف ما يتجاوز الرصيد الفعلي إذا تمّ ذلك بواسطة العميل صاحب البطاقة، فالمسألة هنا لا تعدو أن تكون مسألة مديونية بين المؤسسة المالية العميل، ولا يمكن تكييفها بأنها سرقة طبقاً للمادة (217) من قانون الجزاء الكويتي، لأن الاستيلاء على المبلغ لم يتم دون رضاء المؤسسة المالية طالما أن هذه المؤسسة المالية تعلم بأن الجهاز غير مرتبط بسقف حساب العميل حتى لا يتجاوزه.

خامساً: جرائم الاستيلاء على النقود الإلكترونية: يمكن تعريف النقود الإلكترونية بأنها: "قيمة نقدية مخزنة على وسيلة إلكترونية مدفوعة مقدماً، وغير مرتبطة بحساب مصرفي، تحظى بقبول غير من قام بإصدارها، وتستعمل كأداة دفع"[1]، وتتمثل أهم عناصرها في أن قيمتها النقدية تشحن على بطاقة بلاستيكية، أو على القرص الصلب للحاسب

---

[1] الجنبيهي، منير (2006). البنوك الإلكترونية، دار الفكر الجامعي، الإسكندرية، ط1، ص47.

الشخصي للمستهلك، فهي تختلف عن البطاقات الائتمانية، لأن النقود الإلأكترونية يتم دفعها مسبقاً، بالإضافة إلى أنها ليست مرتبطة بحساب العميل، فهي أقرب إلى الصكوك السياحية منها إلى بطاقة الائتمان، أي أنها استحقاق عائم على مؤسسة مالية، يتم بين طرفين، هما: العميل والتاجر، دون الحاجة إلى تدخل طرف ثالث، كمصدر هذه النقود مثلاً، فهي مجموعة من البروتوكولات والتوقيعات الرقمية التي تتيح للرسالة الإلكترونية أن تحل فعلياً محل تبادل العملات النقدية، ومن هذه البطاقات ما يعمل عن طريق إدخالهاإلى المركز الخاص بالمعاملة المصرفية لدى البائع أو الدائن حيث تم انتقال البيانات الاسمية من البطاقة إلى الجهاز الطرفي للبائع تحول عليه نتائج عمليات البيع والشراء إلى البنك الخاص بالبائع[1].

الفرع الثاني: التكييف القانوني للوسائل الفنية للتحويل الإلكتروني للأموال:

لقد جرم المشرّع الأردني الاطلاع غير المشروع بوسائل إلكترونية على محتويات بطاقات الائتمان والبيانات المالية والمصرفية، وذلك بموجب المادة (6) من قانون جرائم أنظمة المعلومات، والتي جاء نصها: "أ. كل من حصل قصداً دون تصريح عن طريق الشبكة المعلوماتية أو أي نظام معلومات على بيانات أو معلومات تتعلق ببطاقات الائتمان أو بالبيانات أو المعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين أو بغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (2000) ألفي دينار أو بكلتا هاتين العقوبتين، ب. كل من استخدم عن طريق الشبكة المعلوماتية أو أي نظام معلومات قصداً دون سبب مشروع بيانات أو معلومات تتعلق ببطاقات الائتمان أو بالبيانات أو المعلومات التي تستخدم في تنفيذ المعاملات المالية أو

---

[1] حجازي، عبد الفتاح (2007). صراع الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، ص609.

المصرفية الإلكترونية للحصول لنفسه أو لغيره على بيانات أو معلومات أو أموال أو خدمات تخص الآخرين يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة آلاف دينار".

كذلك تدخل القانون العربي النموذجي لجرائم الكمبيوتر بالنص على تجريم الصور السابقة والاستيلاء على الأموال، فنص في المادة (6) على أنه: "كل من استخدم بطاقة ائتمانية للسحب الإلكتروني من الرصيد خارج حدود رصيده الفعلي أو باستخدام بطاقة مسروقة أو تحصل عليها بأية وسيلة بغير حق أو استخدام أرقامها في السحب أو الشراء وغيرها من العملات المالية مع العلم بذلك، يعاقب بالحبس الذي لا تقل مدته عن ( )، وبالغرامة ( )، وهو ما يعني أن هذا النص يعدّ قاصراً على توفير الحماية لغيرها من البطاقات لتقدير الدولة.

أما في الكويت، ففي ظل الفراغ التشريعي بشأن مكافحة الجرائم الإلكترونية، فأرى بأن الدخول على حسابات الأشخاص لدى البنوك والاستيلاء على أموال منها، فإن ذلك قد يشكل جنحة السرقة المنصوص عليها في المادة (221) من قانون الجزاء، أو جناية السرقة المنصوص عليها في المواد (222، 223، 224، 225، 226، 227) من نفس القانون، حيث تصل العقوبة إلى 3 سنوات، ولهذا نكرر الدعوة للمشرّع الكويتي للتصدي لمثل هذا النوع من الجرائم من خلال سن قانون خاص يتناسب وطبيعتها الخاصة.

المطلب الثالث

المشكلات المتعلقة بجرائم التزوير

تنص المادة (257) من قانون الجزاء الكويتي بأنه: "يعدّ تزويراً كل تغيير للحقيقة في محرر بقصد استعماله على نحو يوهم بأنه مطابق للحقيقة ...".

وتنص المادة (258) من نفس القانون على أنه: "كل من ارتكب تزويراً يعاقب بالحبس مدة لا تتجاوز ثلاث سنوات وبغرامة لا تتجاوز ثلاثة آلاف روبية أو بإحدى هاتين العقوبتين".

ما يهمنا في هذا الصدد محل جريمة التزوير، لأنها من الجرائم ذات القالب الحر التي لم يحدد المشرّع فيها شكلاً معيناً للسلوك الإجرامي، لأنها لكنه حدد محل هذا السلوك بالمحرر دون أن يعرفه أو يحدد مضمونه تاركاً للفقه والقضاء هذه المهمة.

فالمحرر هو مجموعة من المعاملات والرموز التي تعبر تعبيراً اصطلاحياً عن مجموعة مترابطة من الأفكار والمعاني الصادرة عن شخص أو أشخاص معينين، وتكمن القيمة الحقيقية له ليس في مادته أو ما يحتويه بل يكمن فيما لهذا التعبير من دلالة اجتماعية[1].

فجوهر جريمة التزوير هو الإخلال بالثــقة العامة التي أراد المشرّع حمايتها في هذا المحرر لما له من آثار قانونية باعتباره وسيلة للإثبات[2].

ولما كان ذلك، فإن قوة المحرر في الإثبات هي جوهر الحماية الجنائية له ومن هنا ذهبت بعض الآراء الفقهية إلى أن كل مادة تصلح للإثبات يجوز أن تكون محلاً للتزوير مهما كان شكلها أو مساحتها ولا أهمية للمادة المستعملة في الكتابة يستوي أن تكون مصنوعة من خشب أو جلد[3]، فإذا كانت فكرة التوسع في مفهوم المحرر مطروحة في الفقه الجنائي قبل ظهور الجرائم الإلكترونية فإن هذا التوسع يبدو أكثر إلحاحاً في ظل الفراغ التشريعي لمواجهة جرائم التزوير المرتكبة بواسطة الحاسب الآلي في التشريع الكويتي، إلا أن هذا الاتجاه واجه نقداً شديداً حيث ذهب جانب من الفقه الفرنسي قبل صدور القانون رقم (19) لسنة 1988م

---

(1) حسني، محمود نجيب (1972). شرح قانون العقوبات – القسم الخاص، دار النهضة العربية، القاهرة، ص322.

(2) الشوا، محمد سامي، مرجع سابق، ص155.

(3) المرصفاوي، حسن صادق (1991). قانون العقوبات الخاص، منشأة المعارف، الإسكندرية، ص116.

الخاص بالغش المعلوماتي إلى رفض اعتبار التعبير الواقع على الاسطوانات الممغنطة تزويراً، استناداً إلى اعتبارين أولهما: انتفاء الكتابة، لأن التغيير انصب على نبضات إلكترومغناطيسية، والثاني هو عدم التيقن من صلاحيتها في الإثبات[1]، ويؤيد هذا الرأي قياس ذلك على انتفاء التزوير في التغيير الي يطرأ على الصوت المسجل، والعلة هي انعدام عنصر الكتابة، بالإضافة إلى أن النبضات الإلكترومغناطيسية تمثل جزءاً من ذاكرة الآلة أو برنامج تشغيلها وهو ما يمكن أن يتحقق معه الإتلاف أو التقليد إذا توافرت شروطهما، وقد بدأ الفكر القانوني الحديث يقبل فكرة الوثيقة الإلكترونية استناداً إلى أن المادة التي تصنع منها الوثيقة ليست عنصراً فيها[2].

ولقد اعترفت بعض الدول بحجية المستندات الإلكترونية في الإثبات ومن ثم إلى اعتبارها محلاً لجريمة التزوير، وقد كانت المملكة الأردنية سباقة في ذلك حيث أصدرت قانون الأوراق المالية المؤقت رقم (23) لسنة 1997م الذي نص في المادة (2/24) على أن: "تعتبر القيود المدونة في سجلات البورصة وحساباتها سواء كانت مدونة يدوياً أو إلكترونياً أو أي وثائق صادرة عنها دليلاً على تداول الأوراق".

أما بالنسبة لتجريم تزوير الوثائق الإلكترونية، فقد كان القانون الفرنسي رقم (19) الصادر في يناير 1988م أول التشريعات التي جرمت تزوير المستندات المعلوماتي، فنص في المادة (5/462) على أن: "كل من ارتكب أفعالاً تؤدي إلى تزوير المستندات المعلوماتية أياً كان شكلها بأي طريقة تؤدي إلى حدوث ضرر للغير، فإنه يعاقب بالسجن من سنة إلى خمس سنوات وغرامة لا تقل عن 20.000 فرنك"، ونصت الفقرة السادسة من ذات المادة

---

[1] الشوا، محمد سامي، مرجع سابق، ص155.

[2] عبد اللاه، أحمد هلالي (2003). الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، دار النهضة العربية، القاهرة، ط1، ص253.

علىمعاقبة كل من استخدم بتبصير المستندات المعلوماتية المزورة طبقاً للفقرة السابقة، ولم يكتف المشرّع الفرنسي بذلك بل إنه نص على إمكانية ارتكاب جريمة التزوير خطأ لأن التغيير والتحريف للمعلومات المخزنة خطاً وإن كان غير متصور في المستندات والوثائق التقليدية، إلا أنه كثيراً ما يحدث في المجالات المعلوماتية لأن الدخول إلى الأنظمة المعلوماتية لا يحدث دائماً بشكل متعمد، فمن الممكن أن يحدث بشكل غير معتمد نتيجة الدخول الخاطئ إليه وهو ما يجب النص عليه في تجريم التزوير في المستندات المعلوماتية[1].

أما القانون العربي النموذجي لجرائم الكمبيوتر فقد نص في المادة (7) على أن: "كل من غير في البيانات المخزنة في المستندات المعالجة آلياً أو البيانات المخزنة في ذاكرة الحاسب الآلي أو على شريط أو اسطوانة ممغنطة أو غيرها من الوسائط يعاقب بـــ ( ) وهو متروك لكل دولة على حدة"، كما نصت المادة (8) منه على تجريم استخدام المستندات المعالجة آلياً مع العلم بتزويرها.

تجدر الإشارة إلى أن كل حالات السرقة والاحتيال التي تتم عن طريق تزوير البيانات إلكترونياً، لنجد أننا أمام حالة من حالات تعدد الجرائم، ويتحقق فيها التعدد المعنوي للجرائم خاصة مثل التلاعب الذي يتم في الأرصدة المصرفية، لأن عمليات التحويل غير المشروعة تتم عن طريق تعديل في البيانات والأسماء أو تعديل في البرامج المعلوماتية المعالجة لهذه البيانات[2].

فإذا كان السلوك الإجرامي في هذه الحالة متمثلاً في تعديل البرامج والبيانات، يترتب عليه تحويلات مالية غير مشروعة، فإن السلوك أو الفعل يظل واحداً يتحقق به أكثر من

---

(1) نقلاً عن: قشقوش، هدى، مرجع سابق، ص148-149.

(2) القهوجي، علي (1999). الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية، الإسكندرية، ط1، ص93.

نموذج تجريمي في هذه الحالة، وهو ما يوجب تطبيق أحكام التعدد المعنوي والارتباط بين الجرائم[1].

ومن وجهة نظر الباحث أن هذا التوسع في تفسير مفهوم "المحرر" لا يغني عن ضرورة تدخل المشرّع الكويتي لمواجهة التزوير المرتكب بالحاسب الآلي على المستندات والوثائق الإلكترونية لأن المسألة تحتاج أولاً إلى الاعتراف بحجية هذه المستندات الإلكترونية في الإثبات قبل تجريم تحريفها، بالإضافة إلى أن تجريم التعديل في هذه البيانات يجب أن يخضع لعقوبات أشد من عقوبة التزوير التقليدية نظراً لاختلاف حجم الضرر والخسائر الناتجة عن تحريف هذه البيانات وتزويرها، والذي زاد المشكلة تعقيداً أن المشرّع الكويتي لم يصدر حتى هذه اللحظة قانوناً خاصاً بالمعاملات الإلكترونية كي يعترف بحجية المستندات الإلكترونية في الإثبات.

وقد نصت اتفاقية بودابست في المادة (7) على تجريم أي تبديل أو محو أو إخماد لأي بيانات مخزنة في أي نظام معلوماتي يؤدي إلى إنتاج بيانات غير حقيقية لغرض استعمالها لأغراض قانونية على أنها صحيحة وذلك سواء كانت فورية القراءة من عدمها.

وهو ما يقطع الجدل حول قابلية المستند للقراءة بالعين المجردة، واعتبار المستند الإلكتروني وثيقة قابلة للقراءة، مشمولة بالحماية الجنائية.

يتضح لنا مما سبق أن الجريمة الإلكترونية تثير مشكلات عديدة في تطبيق النصوص القانونية الحالية في التشريع الكويتي، فإن وجد النص القانوني وأمكن إعمال المطابقة بينه وبين السلوك المرتكب، لا نجد العقوبة تتناسب وحجم الخسائر الناتجة عن ارتكاب مثل هذه الجريمة، وإذا أمكن إعمال المطابقة وكانت العقوبة رادعة، فإننا نواجه عقبة كبيرة في عمليات

---

[1] الفيل، علي عدنان، مرجع سابق، ص154.

ضبط هذه الجرائم وإثباتها لأن القواعد التقليدية للإثبات وضعت لتواجه سلوكاً مادياً يحدث في العالم الافتراضي ولا تتناسب لإثبات جريمة مرتكبة في عالم إلكتروني أو فضاء افتراضي غير ملموس يتكون من ذبذبات وموجات غير مرئية، وهو ما يحتم ضرورة التدخل التشريعي من مجلس الأمة الكويتي لتنظيم هذه المسألة عن طريق الاعتراف لقوة المستندات الإلكتروني في الإثبات، واعتبارها من قبيل الوثائق قبل النص على تجريم تزويرها أو التعديل فيها وتحريفها حسب الأحوال.

وبالرجوع إلى قانون جرائم أنظمة المعلومات الأردني، نجد أن المشرّع الأردني قد عالج التزوير الإلكتروني وذلك من خلال تجريمه للجرائم الإلكترونية المتعلقة بالحاسوب ومحتوياته كإتلاف وتشويه وتغيير البيانات والمعلومات، وبرامج الحاسوب، والتحوير، والتلاعب في المعلومات المخزنة داخل النظام المعلوماتي، واستخدامها لتزوير المستندات المعالجة آلياً واستخدامها، وهذا ما نصت عليه المادتان (3، 4) من قانون جرائم أنظمة المعلومات.

تجدر الإشارة هنا إلى أن البعض يرى[1] بوجوب إخضاع التزوير الإلكتروني إلى نص المادة (76) من قانون الاتصالات الأردني رقم (13) لسنة 1995م والتي تنص: "كل من اعترض أو أعاق أو حوّر أو شطب محتويات رسالة بواسطة شبكات الاتصالات أو شجع غيره على القيام بهذا العمل يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد عن ستة أشهر أو بغرامة لا تزيد عن مائتي دينار أو بكلتا العقوبتين".

إلا أن البعض يرى أن هذا الرأي لا يستقيم وذلك لأن هذه المادة لا تغطي إلا صورة واحدة من صور التزوير المعلوماتي المتعلقة بالرسائل المنقولة بواسطة شبكات الاتصال، وهذا

---

[1] الرواشدة، سامي، والهياجنة، أحمد، مرجع سابق، ص135.

من شأنه إفلات مرتكبي تزوير معطيات الحاسب المخزنة للبرامج والبيانات، إضافة إلى أن العقوبات غير متناسبة وغير رادعة أيضاً[1].وبخصوص موقف بعض التشريعات الأجنبية من موضوع التزوير الإلكتروني، ففي ألمانيا استحدث المشرّع المادة (269) عقوبات[2] والتي تنص على: "كل من باشر بغرض التحايل على الروابط القانونية:

1. التخزين الإلكتروني أو المغناطيسي غير المشروع أو بأي وسيلة أخرى غير مرئية أو غير مقروءة مباشرة، لبيانات متخصصة لكي تستعمل كوسائل إثبات.
2. أو التعديل غير المشروع لهذه البيانات المختزنة سواء بوسيلة قانونية أو غير قانونية.
3. أو استعمل هذه البيانات المختزنة أو عدلها يعاقب ...".

هذه المادة حسبت الخلاف الناشئ حول صلاحية نصوص القانون الألماني لمواجهة التزوير الإلكتروني، حيث أكدت هذه المادة المستحدثة على معاقبة المزور الإلكتروني.

أما في فرنسا، فجاء القانون الفرنسي الجديد المتضمن فصلاً للمعالجة الآلية للمعلومات، وجاء في المادة (3/2/1/323) عقوبات مختلفة للتعديل أو التغيير في المعطيات، فالفقرة الأولى أشارت إلى أنه: "إذا نتج عن ذلك حذف أو تعديل للمعطيات الموجودة في النظام أو تحريف لمجريات النظام، فإن العقوبة هي سنتان سجن وغرامة قيمتها مائتي ألف فرنك"، والفقرة الثانية من المادة جاء فيها: "كل من يقوم بإعاقة أو تزوير مجريات نظام عالجة آلية للمعطيات، فإنه يعاقب بالسجن لمدة ثلاث سنوات وغرامة نقدية قيمتها ثلاثمائة ألف فرنك"، والفقرة الثالثة جاء فيها: "كل من يدخل بطريقة مخادعة معطيات داخل نظام المعالجة الآلية أو من يحذف أو يعدل بطريقة مخادعة معطيات موجودة في النظام، فإنه يعاقب بالسجن

---

[1] عبابنة، محمود أحمد، مرجع سابق، ص110.

[2] الشوا، محمد سامي، مرجع سابق، ص164.

لمدة ثلاث سنوات وغرامة قيمتها ثلاثمائة ألف فرنك فرنسي[1].أما في المملكة المتحدة، فصدر فيها قانون التزوير والتزييف الخاص بالمحررات عام 1981م والذي تمّ تعريف السند القابل للتزوير بأنه: "كل اسطوانة أو شريط ممغنط أو شريط صوتي، أو أي جهاز آخر سجل فيه أو عليه معلومات، أو حفظت بوسائل ميكانيكية أو إلكترونية أو بوسائل أخرى"، ثم صدر قانون إساءة استخدام الكمبيوتر عام 1990م الي صدر استجابة لفشل النيابة في الاتهام أو الحصول على الإدانة[2].أما في الولايات المتحدة الأمريكية، فتناول القانون الفيدرالي رقم (18) في مادته (1029) المتعلقة بالاحتيال والنشاط المتعلق بالاتصال مع أدوات الوصول إلى الحاسب الآلي، تجريم أفعال التزوير المرتبطة بمعطيات الحاسب الآلي وذلك في الفقرة (A) البند الثالث، والعقاب عليها بالحبس لمدة لا تزيد عن عشر سنوات أو بالغرامة أو بالعقوبتين معاً[3].

ومن التطبيقات القضائية الإنجليزية بهذا الخصوص، قضية R.V. Levin أنه: أيدت محكمة الاستئناف البريطانية قرار الحكم القاضي بإدانة أحد الأشخاص بجريمة الدخول إلى النظام المعلوماتي بقصد ارتكاب جريمة التزوير، كما أيدت المحكمة ذاتها إدانته بالجريمة المنصوص عليها في المادة الثالثة أيضاً، وتتلخص وقائع تلك الدعوى بقيام شخص يدعى (Levin) بالدخول إلى النظام المعلوماتي الخاص ببنك (City Bank) في مدينة نيوجرسي من مدينة سانت بطرسبرغ، حيث يقيم باستخدام جهاز الحاسوب الخاص به، وتمكن من تحويل بعض الأموال من الحسابات العائدة لبعض عملاء البنك إلى حسابات خاصة به في بريطانيا[4].

---

(1) الشوا، محمد سامي، مرجع سابق، ص165.

(2) الرواشدة، سامي والهياجنة، أحمد، مرجع سابق، ص133.

(3) الشوا، محمد سامي، مرجع سابق، ص165.

(4) أشار إليها: الرواشدة، سامي والهياجنة، أحمد، مرجع سابق، ص152.

المطلب الرابع

المشكلات المتعلقة بجريمة سرقة المال المعلوماتي

لا تثور المشكلة عندما يتم سرقة المعلومات المخزنة على أدوات التخزين ذات الكيان المادي المحسوس، كاسطوانات الحاسب، لأن السرقة هنا تنصرف إلىمال منقول مادي يتم إخراجه من حيازة مالكه أو حائزه الشرعي إلى الغير وهو الاسطوانة بما عليها من معلومات.

ولن يثور الخلاف عندما يتم الاستيلاء على المعلومات المخزنة داخل الجهاز دون وجه حق أو نسخ هذه المعلومات، وهو ما يعبر عنه حالياً بالقرصنة، وقد عرف البعض القرصنة بأنها: "سرقة المعلومات من برامج وبيانات مخزنة في دائرة الكمبيوتر بصورة غير شرعية، أو نسخ برامج معلوماتية بصورة غير شرعية بعد تمكن مرتكب هذه العملية من الحصول على كلمة السر، أو بواسطة التقاط الموجات الكهرومغناطيسية الصادرة عن الحاسب الآلي أثناء تشغيله وباستخدام هوائيات موصلة بحاسبة خاصة"[1].

ونظراً لما تمثله القرصنة في وقتنا الحاضر من تهديد لمستقبل التقنية وصناعة المعلومات، كان لا بدّ من دراسة هذه الظاهرة الإجرامية لمحاولة تحديد النصوص القانونية الواجب الاستناد إليها للتجريم، ذلك أن القرصنة تثير إشكالاً يتعلق بطبيعة المعلومات الخاصة، ذلك أن ليس لها كيان مادي محسوس وتبقى في حيازة مالكه، وبالتالي يثور تساؤل حول ما إذا كانت المعلومات تصلح محلاً لجريمة السرقة أم لا؟ وبعبارة أخرى هل تعدّ المعلومات مالاً منقولاً مملوكاً للغير حتى يمكن سرقتها؟

لم يرد في قانون الجزاء الكويتي وقانون العقوبات الأردني تعريف للمال لغايات تطبيق القانون، هذا ويعرف المال بأنه: كل عين أو حق له قيمة مادية في التعامل ويمكن

---

[1] المناعسة وآخرون (2001). جرائم الحاسب الآلي والإنترنت، دار وائل، عمان، ط1، ص146.

حيازته مادياً أو معنوياً وبالانتفاع به انتفاعاً مشروعاً ولا يخرج عن التعامل بطبيعته أو بحكم القانون، يصح أن يكون محلاً للحقوق المالية، وتمّ تعريف العقار بأنه: كل شيء مستقر بحيزه ثابت فيه لا يمكن نقله منه، دون تلف أو تغير هيئتته فهو عقار، وكل ما عدا ذلك فهو منقول[1].

مما لا شك فيه أن المعلومات وإن كانت تثير إشكالاً يتمثل في مدى اعتبارها من الأموال التي يمكن سرقتها، إلا أنه من المسلم فيه أن هذه المعلومات ابتداءً يمكن أن تترجم إلى قيم مالية نظراً لقابليتها للاستغلال مقارنة بالبرامج التي هي نوع من الإبداع الذهني والفكري، وبما أن البرامج عبارة عن أسلوب ينظم العمل والمعالجة، فإن استخدام هذا الأسلوب بصورة غير مصرّح بها من قبل مالكها أو حائزها الشرعي يشكل اعتداءً على حقوق الاستغلال المالي[2].

وبتحليل عناصر جريمة السرقة التي تتفق التشريعات العربية على عناصرها من وجوب كون المال منقولاً ومملوكاً للغير، ونقل حيازته من حائزه الشرعي إلى السارق، فإن البعض يرى وجوب عدم قياس نصوص السرقة التقليدية على سرقة المعلومات، وعدم إطلاق وصف السرقة على هذه الجريمة، وذلك للاعتبارين التاليين:

أولاً: المشرّع الأردني عرّف السرقة في المادة (399) بأنها: "أخذ مال الغير المنقول دون رضاه، وتعني عبارة (أخذ المال) إزالة تصرف المالك فيه، برفعه من مكانه ونقله، وإذا كان متصلاً بغير منقول فبفصله عنه فصلاً تاماً ونقله، وتشمل لفظة (مال) القوى المحرزة"، أما قانون العقوبات الليبي فجاء في المادة (444) منه: كل من اختلس منقولاً مملوكاً لغيره يعاقب

---

[1] انظر المواد (53، 54، 57) من القانون المدني الأردني رقم (43) لسنة 1976م.

[2] العبابنة، محمود أحمد، مرجع سابق، ص95.

بالحبس ويعدّ من الأموال المنقولة في حكم قانون العقوبات الطاقة الكهربائية وجميع أنواع الطاقة ذات القيمة الاقتصادية.

والغاية من إيراد هذين النصين تتمثل في أن الركن المادي المكوّن لجريمة السرقة في التشريعين السابقين يتمثل في أخذ مال الغير المنقول دون رضاه (الاختلاس)، وهو محور ارتكاز هذه الجريمة، فانهياره يؤدي إلى انهيار الجريمة لتخلف ركنها المادي، وبالرجوع إلى الأحكام الخاصة بجريمة السرقة، وبتحليل عناصر الاختلاس والتي تتمثل في سلب الحيازة وإنهائها مع عدم رضاء الحائز وإنشاء حيازة جديدة، وذلك بأن يقوم الحائز الجديد بإنشاء حالة واقعية تتيح له السيطرة على الشيء دون عقبات تحول بينه وبين التمتع بهذه السيطرة بنية احتباسه، كذلك وجوب أن تكون هذه الحيازة الجديدة مستقلة بشكل تقطع فيه حيازة الحائز السابق، ولا يكون بإمكانه ممارسة الرقابة عليه، وتطبيق هذا على سرقة المعلومات أمر لا يستقيم لأن السارق إن جاز التعبير، نادراً ما يخرج حيازة هذه المعلومات من حرز صاحبها أو من سلطته عليها.

والاعتبار الثاني يتعلق بموضوع السرقة، إذ يجب أن تنصرف السرقة إلأى مال منقول له كيان مادي محسوس يشغل حيز في الفضاء الخارجي المحيط بنا، وعلى ذلك فإن هذا الرأي لا يرى إمكانية صلاحية المعلومات لأن تكون موضوعاً للسرقة، وهذا لتجردها من صفة المواد المحسوسة ما لم تثبت على أجزاء أخرى مادية كالاسطوانات الخاصة بالحاسب، إضافة إلى أن المعلومات بحد ذاتها لا تعدّ من قبيل الأموال إلا إذا كان لها قابلية للاستغلال.

وبالرجوع إلى المادة (249) من قانون الجزاء الكويتي، نجد أن هذه المادة جاءت تحت عنوان: "الإتلاف والقرصنة"، وقد جاء نصها: "كل من أتلف أو خرب مالاً منقولاً أو ثابتاً مملوكاً لغيره، أو جعله غير صالح للاستعمال في الغرض المخصص له، أو أنقص من

قيمته أو فائدته، وكان ذلك عمداً وبقصد الإساءة، يعاقب بالحبس مدة لا تتجاوز ثلاثة أشهر وبغرامة لا تتجاوز ثلاثمائة روبية أو بإحدى هاتين العقوبتين".

وأرى بأن هذا النص، وإن جاء تحت عنوان: "الإتلاف والقرصنة" إلا أنه لا يصلح أساساً للتجريم والعقاب في جريمة سرقة المال المعلوماتي، نظراً لأن المعلومات ليس لها كيان مادي محسوس ولا تصلح لأن تكون محلاً للسرقة، كما أن المعلومة لا تعدّ مالاً منقولاً، إنما تعدّ مالاً معنوياً.

لهذا، فإن القواعد التقليدية في قانون الجزاء الكويتي لا تصلح لمواجهة جريمة سرقة المال المعلوماتي.

أما عن موقف بعض التشريعات الغربية، فلم يرد في قانون العقوبات الفرنسي الجديد ما يشير إلى جريمة سرقة المعلومات، عندما تناول في المادة (323) بفقراتها المعالجة الآلية للبيانات، وكأن في هذا إشارة إلى سريان القواعد العامة للسرقة على سرقة المعلومات من جانب المشرّع[1].

أما في الولايات المتحدة الأمريكية، وبالرغم من تباين واختلاف القوانين المتعلقة بجرائم الكمبيوتر من ولاية إلى أخرى، حيث صدر القانون الفيدرالي عام 1984م والذي يعاقب على الوصول غير المرخص إلى المعلومات، ثم صدر قانون حماية البنية التحتية للمعلومات الذي عدّل في القانون رقم (18) المتعلق بالغش والاحتيال المرتبط بالكمبيوتر، وينظم القانون رقم (18) الجرائم المرتبطة بالحاسب الآلي، فالمادة (1029) تتعلق بالاحتيال والنشاطات المتعلقة بالاتصال مع أدوات الاتصال، والمادة (1030) تتعلق بالاحتيال المرتبط بالكمبيوتر، والمادة (1362) التي تتعلق بخطوط الاتصال والمحطات والأنظمة، والمادة

---

[1] قشقوش، هدى، مرجع سابق، ص164.

(2511) التي تتعلق باعتراض وإفشاء المعلومات بعد الاطلاع عليها من خلال الأسلاك، والمادة (2701) التي تتعلق بالنشاطات غير القانونية تجاه الاتصالات المخزنة[1].

ويرتبط بجريمة سرقة المال المعلوماتي مسألة أخرى تتعلق بإتلاف المعلومات وبرامج الحاسب الآلي.

إن الأشكال المختلفة لأساليب إتلاف المعلومات وبرامج الحاسب الآلي تتمثل بالآتي[2]:

أولاً: الفيروسات:

ومن أبرز الفيروسات التي تستخدم للاعتداء على معلومات وبرامج الحاسب الآلي فيروس حصان طروادة، وهو عبارة عن برنامج يتمتع بقدرته الفائقة على الاختفاء داخل البرنامج الأصلي ليعمل أثناء التشغيل بحيث يؤدي إلى تعديل البرنامج أو تغييره ومحو المعلومات وتدميرها[3].

ثانياً: برامج الدودة:

وهي عبارة عن برامج تستغل أية فجوات في نظم التشغيل كي تنتقل من حاسب إلى آخر ومن شبكة إلى أخرى عبر الوصلات التي تربط بينهما وتتكاثر أثناء عملية انتقالها كالبكتيريا بإنتاج نسخ منها[4]، ومن أبرز هذه البرامج ذلك الذي أنتجه روبرت موريس عام 1988م[5] الذي كان طالباً في مرحلة الدكتوراه (علم الكمبيوتر) بجامعة كورنيل، وأراد موريس أن يثبت عدم ملائمة أو فعالية الإجراءات الأمنية القائمة لحماية شبكات الكمبيوتر

---

(1) الشوا، محمد سامي، مرجع سابق، ص520-521.

(2) الصغير، جميل عبد الباقي (2010). الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، ص104-105.

(3) الصغير، جميل، مرجع سابق، ص104.

(4) الشوا، محمد سامي، مرجع سابق، ص193.

(5) رمضان، مدحت، مرجع سابق، ص50.

وإظهار العيوب فيها، وقام بتصميم برنامج لذلك بحيث ينتشر بشبكة وطنية بعد تشغيله عن طريق حاسب محلي مرتبط بالإنترنت، ويربط بين مجموعة من شبكات الكمبيوتر الأمريكية المتصلة مع الجامعات والجهات الحكومية والعسكرية، وبعد أن تم برنامج الدودة، اكتشف موريس أنه يقوم بالانتشار بسرعة كبيرة، الأمر الذي ترتب عليه تلف الكثير من برامج الكمبيوتر وتوقيفها عن العمل.

وبعد إلقاء القبض عليه تمت محاكمته بمقتضى النص الذي يجرم الدخول إلى الأجهزة الفيدرالية وبدون تصريح، وتمت إدانته والحكم عليه بالوضع ثلاث سنوات تحت المراقبة، والقيام بعمل لخدمة المجتمع لمدة 400 ساعة وغرامة عشرة آلاف وخمسين دولاراً أمريكياً.

ثالثاً: القنابل المنطقية أو الزمنية:

تعرف القنابل المنطقية بأنها: "برنامج أو جزء من برنامج ينفذ في لحظة محددة، أو كل فترة زمنية منتظمة، يوضع على شبكة معلوماتية بهدف تحديد ظروف أو حالة فحوى النظام بغرض تسهيل عمل غير مشروع"[1].

ولعل ما حدث في جامعة مونماوث في الولايات المتحدة الأمريكية يعطينا صورة عن الأثر المدمر للقنابل الإلكترونية، فبعد انفجار قنبلة إلكترونية استهدفت نظام البريد الإلكتروني للجامعة الذي ترتبط به أعمال وأنشطة على درجة عالية من الأهمية، كالتسجيل وتبادل الأبحاث ودفع الرسوم، انهار نظام البريد الإلكتروني وقدرت الخسائر بعشرات الآلاف من الدولارات، غير أن فريق تحقيق فيدرالي تمكن من تحديد اليوم والساعة وعنوان الكمبيوتر المستخدم في الجريمة، وبعد مواجهة المتهم اعترف وحاول تبرير فعلته بأنه لم يقصد

---

[1] الشوا، محمد سامي، مرجع سابق، ص194.

التخريب، إلا أن ذلك لم يسعفه، فاعتبرته مذنباً وحكمت عليه بالسجن لمدة ثلاث سنوات وغرامة مالية مقدارها مائة ألف دولار[1].

أما بخصوص موقف المشرّع الأردني والكويتي من هذه المسألة فقد استلزما لتحقيق جريمة الإتلاف أن يقع الاعتداء على مال منقول أو عقار[2].

فوجوب كون المال المتلف من العقارات، أو المنقولات، يخرج المعلومات والبرامج من إطار الحماية الجنائية التي يوفرها قانون العقوبات للأموال، لأن المعلومات والبرامج – وبالرغم من أن لها قيمة اقتصادية قابلة للاستغلال – إلا أنها لا تعدّ من الأموال المنقولة المادية.

وعلى هذا فالبحث عن نصوص في قانون العقوبات التقليدي لإمكانية انطباق جريمة إتلاف المعلومات والبرامج قد يكون أمراً ليس بذي جدوى، وهذا ما دفع بالمشرّع الأردني للتصدي لمعالجة هذه الصورة من صور الجرائم الإلكترونية في قانون جرائم أنظمة المعلومات، إذ تنص المادة (3/ب) منه على أنه: "ب- إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات أو تغيير موقع إلكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه، فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار أو بكلتا هاتين العقوبتين".

---

[1] نعناع، فاطمة (1998). مقال بعنوان: "قنبلة إلكترونية في بريد الجامعة"، منشورة في مجلة إنترنت العالم العربي، السنة الأولى، العدد السابع، إبريل، ص64-65.

[2] انظر: المادة (443) من قانون العقوبات الأردني، والمادة (249) من قانون الجزاء الكويتي.

وكذلك ما نصت عليه المادة (4) من نفس القانون بأنه: "كل من أدخل أو نشر أو استخدم قصداً برنامجاً عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات بهدف إلغاء 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 إتلافه 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 أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار أو بكلتا هاتين العقوبتين".

وبشأن موقف بعض التشريعات الغربية، ففي الولايات المتحدة الأمريكية لا تثور مشكلة بهذا الخصوص، لأن القانون رقم (18) المتعلق بجرائم الحاسب الآلي يعالج هذه المسألة، وتطبيقاً لذلك فلقد أدانت محكمة ولاية نيوجيرسي في الولايات المتحدة المتهم ديفيد سميث، حيث أسند إليه تهمة إنتاج فيروس ميليسا الذي اجتاح الولايات المتحدة عام 1999م وتسبب في عطل أكثر من مليون جهاز حاسب آلي، وخسارة مالية قدرت بحوالي ثمانين مليون دولار، وتمّ الحكم عليه وفقاً للفقرة (A 1030) البند الخامس من المرسوم رقم (18) الذي يعاقب على إتلاف البرامج والتسبب في الإضرار إلى أجهزة الحاسب الآلي المحمية والتي عرفها ذلك القانون بأنها أجهزة الحاسب الآلي العاملة لدى الحكومة أو لدى المؤسسات المالية والتجارية، وبعد الرجوع إلى قرار المحكمة بشأن المتهم (سميث)، يلاحظ أنه تمت إدانته وفقاً للقانون وبموجب المادة (1030) لإطلاقه فيروس ميليسا الذي سبب أضراراً لأجهزة الحاسب الآلي وأتلف البرامج وعطل الخدمة وصدر حكم بحقه من محكمة ولاية

نيوجيرسي بالحبس مدة 5 سنوات وغرامة 250000 دولار، وبعد أن طعن في الحكم تم تخفيض مدة الحبس إلى ثلاث سنوات مع الغرامة من قبل المحكمة العليا[1].

أما في فرنسا، فإن قانون العقوبات الفرنسي الصادر عام 1993م نظم هذه المسألة أيضاً، ونص في المادة (3/323) "كل من يدخل بطريقة مخادعة لمعطيات داخل نظام المعالجة الآلية أو من يحذف أو يعدل بطريقة مخادعة معطيات موجودة في النظام، فإنه يعاقب بالسجن لمدة ثلاث سنوات وغرامة قيمتها ثلاثمائة ألف فرنك فرنسي".

وبذلك تكون التشريعات الغربية والتشريع الأردني قد قطعت شوطاً متقدماً في مجال حماية المال المعلوماتي الذي نتمنى أن يحذو المشرّع الكويتي حذو هذه التشريعات واللحاق بها في هذا المجال.

ومن التطبيقات القضائية بهذا الشأن قضية Zezev V. United States، وتتلخص وقائع هذه الدعوى: "بقيام شخص يعمل في شركة مقرّها كازاخستان باختراق النظام المعلوماتي العائد لشركة تعمل في ولاية نيويورك الأمريكية تقوم بتزويد الأخبار والمعلومات المالية إلى كافة أرجاء العالم، وتمكن المشتكى عليه من الدخول إلى البريد الإلكتروني الخاص بمدير الشركة ومدير الأمن فيها، الأمر الذي مكنه من الحصول على معلومات بالغة السرية، بعد ذلك قام بإرسال عدد من الرسائل الإلكترونية إلى مدير الشركة لإخباره بأن النظام المعلوماتي الخاص بالشركة قد تم اختراقه، وطالب بمبلغ وقدره مائتي ألف دولار مقابل عدم قيامه بنشر واقعة اختراق النظام المعلوماتي الخاص بالشركة وهو أمر لو تحقق فإنه سيضر بسمعة الشركة، وسيلحق بها خسائر مالية كبيرة، تم اعتقال المشتكى عليه في مدينة لندن أثناء حضوره لاستلام المبلغ المتفق عليه بعد أن أخبر مدير الشركة الشرطة بذلك، وطلبت الولايات

---

[1] نقلاً عن: العبابنة، محمود أحمد، مرجع سابق، ص105-106.

المتحدة ترحيله إليها لمحاكمته بعد أن تم توجيه ست تهم إليه من بينها التآمر لإتلاف البيانات المخزنة وهي الجريمة التي يعاقب عليها بمقتضى المادة الثالثة من القانون، وقضت محكمة الاستئناف بتأييد قرار محكمة الدرجة الأولى بالموافقة على تسليم المشتكى عليه إلى الولايات المتحدة الأمريكية باعتبار أن فعل الشخص المطلوب تسليمه ارتكب جريمة يعاقب عليها بموجب المادة الثالثة من قانون إساءة استخدام الحاسوب لعام 1990م، وقد جاء في حيثيات الحكم أن إرسال بريد إلكتروني بطريقة يفهم منها أنه مرسل من شخص ما إلا أنه في الواقع تم إرساله من شخص آخر، الأمر الذي أدى إلى جعل جهاز الحاسوب يسجل معلومات غير صحيحة أضرت بشكل واضح بمصداقية البيانات المخزنة في الحاسوب، بناءً على ذلك فإن هذا التصرف يدخل ضمن نطاق المادة 3/2/ج من القانون باعتبار أن المعلومات هي بيانات بدون أدنى شك، كما قضت المحكمة بأن إدخال بيانات غير صحيحة إلى النظام المعلوماتي من خلال التظاهر بأنه صاحب البريد الإلكتروني مع أنه في الواقع ليس كذلك، يفسد عمل الحاسوب، ويعتبر تعديلاً لمحتوياته من المعلومات، ولهذا لا يقبل الاحتجاج بأن نص المادة الثالثة يقتصر على إتلاف الحاسوب وأن تعديل المعلومات يتحقق بإضافة معلومات أخرى إليها، ويرى الفقه أن قرار المحكمة يشير بكل وضوح إلى أن نص المادة الثالثة يتطلب قصداً جرمياً ذا طبيعة مزدوجة، اتجاه الإرادة نحو تعديل محتويات الحاسوب والمعلومات المخزنة فيه، وانصراف الإرادة نحو الإضرار بمصداقية المعلومات، إلا أنه عندما يتطلب الأمر أن يترتب على تعديل المعلومات الإضرار بمصداقيتها، فإن كلا القصدين يتداخلان ليصبح القصد المتمثل بإرادة تسجيل معلومات غير صحيحة في الحاسوب يعني أن الإرادة الجرمية قد اتجهت حتماً نحو الإضرار بمصداقية البيانات"[1].

---

[1] أشار إليها: الرواشدة، سامي والهياجنة، أحمد، مرجع سابق، ص152-153.

وفي قضية أخرى هي قضية (Whitaker) في إنجلترا بإدانة المدعو (Whitaker) بارتكابه الجريمة المنصوص عليها في المادة الثالثة من قانون إساءة استخدام الحاسوب، وتتلخص وقائع هذه الدعوى: "بقيام (Whitaker) بتطوير بنرامج لأحد زبائنه مقابل مبلغ من المال، وقد تم إبرام عقد بينهما لهذه الغاية، إلا أنه نتيجة لخلاف حول دفع قيمة البرنامج، قام المشتكى عليه بزرع فيروس في البرنامج، الأمر الذي أدى إلى عدم إمكانية استخدامه، أثار المشتكى عليه دفعاً مفاده بأنه يملك الحق في فعل ذلك بدعوى أنه لا يزال يملك حقوق التأليف الخاصة بالبرنامج، ولم تقبل المحكمة هذا الدفع بدعوى أن هذا الأمر لم يرد النص عليه في العقد المبرم بينهما"[1].

بالإضافة إلى الصور سالفة الذكر، فقد عالج المشرّع الأردني صوراً أخرى للجرائم الإلكترونية، وهي:

أولاً: التغرير والاستدراج والأعمال الإباحية والدعارة، وهما من أشهر جرائم الإنترنت وأكثرها انتشاراً خاصة بين أوساط صغار السن من مستخدمي الشبكة، وهذه الجريمة تقوم على عنصر الإيهام في تكوين علاقات من قبل المجرمين (المادة 8 والمادة 9 من قانون جرائم أنظمة المعلومات الأردني).

ثانياً: استخدام نظام المعلومات أو الشبكة المعلوماتية لإنشاء المواقع الإلكترونية لتسهيل القيام بأعمال إرهابية، أو دعم جماعة، أو تنظيم، أو جمعية تقوم بأعمال إرهابية، أو الترويج لاتباع أفكارها، أو تمويلها (المادة 10 من قانون جرائم أنظمة المعلومات الأردني).

ثالثاً: الدخول غير المصرّح به إلى موقع إلكتروني أو نظام معلومات بأي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني، أو علاقات

---

[1] أشار إليها: الرواشدة، سامي والهياجنة، أحمد، مرجع سابق، ص155-156.

دولة بغيرها من الدول، أو المساس بالسلامة العامة، أو الاقتصاد الوطني (المادة 11 من قانون جرائم أنظمة المعلومات الأردني).

ومن وجهة نظر الباحث فإن المشرّع الأردني قد عالج الأعم الأغلب من صور الجرائم الإلكترونية، وأرى بأنه كان ينبغي على المشرّع الأردني أن ينص على قاعدة عامة بخصوص صور الجريمة الإلكترونية وأن ينص على أمثلة بشأنها ومن ثم يكون التعداد الوارد في القانون على سبيل المثال لا الحصر، بخاصة أن هناك صور لم يعالجها المشرّع الأردني مثل الملاحقة الإلكترونية، والتشهير، وتشويه السمعة سواء في غرف الدردشة أو مواقع التواصل الاجتماعي وبخاصة "تويتر" و "الواتسب" وكذلك الاحتيال الإلكتروني.

المبحث الثاني

المشكلات الإجرائية التي تثيرها الجريمة الإلكترونية

هناك مشكلات قانونية وعملية تواجه الجهود المبذولة لمكافحة الجرائم الإلكترونية على الصعيد الإجرائي، وهذه المشكلات تتعلق بضبط الجريمة وإثباتها، وبسلطات التحري والملاحقة، وأخيراً الاختصاص القضائي والقانون واجب التطبيق، وعليه سأتناول هذه المشكلات ضمن ثلاثة مطالب.

المطلب الأول

المشكلات المتعلقة بضبط الجريمة الإلكترونية وإثباتها

لعل من أهم العناصر التي ترتبط بالجريمة هو مسرحها أو مكان وقوع أركانها، وهو العنصر الرئيس لضبط وتحري الجريمة وملاحقة مرتكبيها، وهذا هو الحال نفسه فيما يتعلق بالجريمة الإلكترونية، حيث إن مسرحها متوفر وحتى إن كان مختلفاً عن المسرح المادي للجريمة التقليدية كونه مسرحاً معنوياً، فتجول الشخص في الشبكة العنكبوتية يعني أن يترك آثار أقدامه وبصماته المعنوية في الموقع الذي يزوره، إذ يتم تحديد عنوانه الإلكتروني الدائم له، ويتم تحديد نوع الجهاز الذي يستخدمه والمكان الذي يدخل منه[1].

ويمكن تتبع هذه العناصر بطرق بسيطة أحياناً وبعضها متوفر للمستخدمين العاديين والتي تكشف معلومات المستخدم ويجعلها متاحة لأي شخص يود تتبع تحركات المجرم، فضلاً عن أن يقوم بذلك المتخصصون، وحتى أن جهاز المجرم الشخصي نفسه يحتفظ بملفات الكوكيز للمواقع التي دخلها.

---

[1] السعيد، كامل (2002). جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، دراسات جنائية معمقة في القانون والفقه والقضاء المقارن، دار الثقافة للنشر والتوزيع، عمان، ص46.

ولكن الأمر ليس بهذا القدر من البساطة، فيمن اكتشاف المجرمين البسطاء ربما بمثل هذه الطرق، أما المجرمين المتخصصين بل وحتى الهواة منهم يقومون بمحو آثارهم التي تمّ تسجيلها من خلال عدة طرق، منها: مسح ملفات الكوكيز الموجودة على أجهزتهم، وأيضاً القيام بإخفاء عناوينهم الإلكترونية الخاصة بأجهزتهم بطرق مختلفة[1].

وتحاول مختلف الدول والشركات المقدّمة لخدمات الإنترنت التغلب على هذه الاختراقات عبر برامج خاصة أحياناً وعبر رموز أخرى، وهذا يتطلب عند محاولة الاستفادة منه لغايات التحري تعاوناً من مزودي الخدمة، لأن هذه الرموز تخص مزود الخدمة يتعرف من خلالها على هوية المتصلين عبر خطوطهم[2].

هذا ويعتمد ضبط الجريمة وإثباتها في المقام الأول على جمع الأدلة التي حدّد المشرّع وسائل إثباتها على سبيل الحصر، وذلك لما فيها من مساس بحرية الأفراد وحقوقهم الأساسية، فلا يجوز أن تخرج الأدلة التي يتم تجميعها عن تلك التي اعترف لها المشرّع بالقيمة القانونية، وتتمثل في وسائل الإثبات الرئيسة، وفي المعاينة، والخبرة، والتفتيش، وضبط الأشياء المتعلقة بالجريمة، أما غيرها من وسائل الإثبات كالاستجواب، والمواجهة، وسماع الشهود فهي مرحلة تالية من إجراءات التحقيق وجمع الأدلة، ولما كنا بصدد تناول الجريمة الإلكترونية وما تثيره من مشكلات إجرائية، فسنتعرض للمشكلات القانونية التي يثيرها إثبات هذه الجرائم دون غيرها من الإجراءات كالاستجواب، والمواجهة، وسماع الشهود، لأن هذه الأخيرة تتم في مواجهة البشر، أما المعاينة، والخبرة، والتفتيش فهي إجراءات فنية محلها الأشياء لا الأفراد وهو ما يهمنا في هذا الموضوع.

---

[1] القطاونة، مصعب، مرجع سابق، ص7.

[2] موسى، مصطفى محمد (2005). دليل التحري عبر شبكة الإنترنت، دار الكتب القانونية، مصر، ص48.

وسوف أبحث ضمن أدلة الإثبات حجية المستندات الإلكترونية في الإثبات الجنائي، ومن ثم أبحث إشكاليات المعاينة والخبرة والتفتيش في الجرائم الإلكترونية، وذلك في فرعين.

الفرع الأول: حجية المستندات الإلكترونية في الإثبات الجنائي:

تخضع المستندات كغيرها من الأدلة التي تقدم أثناء نظر الدعوى إلى تقدير المحكمة حيث يسود مبدأ حرية القاضي في تكوين عقيدته، وهو ما يختلف فيه القاضي المدني حيث يتقيد هذا الأخير بطرق معينة في الإثبات، فالقاضي الجنائي له مطلق الحرية في تقدير الدليل المطروح أمامه، وله أن يأخذ به أو يطرحه، ولا يجوز تقييده بأي قرائن أو افتراضات[1].

لما كانت المستندات أحد الأدلة التي قد يلجأ إليها القاضي في الإثبات فهي تخضع كغيرها من الأدلة لتقدير المحكمة، إلا إذا كان الإثبات متعلقاً بمواد غير جنائية، ففي هذه الحالة يكون على القاضي الجنائي أن يتقيد بطريق الإثبات المحددة في ذلك الفرع من القانون، مثال ذلك حق الملكية في جريمة السرقة، والعقود التي تثبت التصرف في الحق في جريمة خيانة الأمانة أو صفة التاجر في جريمة الإفلاس بالتدليس[2].

ولما كان المشرّع الكويتي لا يزال عازفاً عن التدخل التشريعي في هذه المسألة، فلا بدّ من تطبيق القواعد العامة في هذا الصدد، فالمشرّع الكويتي لا يزال يعتمد على مبدأ سيادة الدليل الكتابي على غيره من الأدلة، ولا يجوز الاعتماد على الدليل غير الكتابي في غير المسائل الجنائية، إلا على سبيل الاستئناس، ولا يخفى ما يؤدي ذلك من تقييد للقاضي الجنائي، لأن الإثبات في المسائل الجنائية كثيراً ما يعتمد على مسائل غير جنائية، فمواجهة الجرائم الإلكترونية لا تتأتى إلا عن طريق نظام قانوني متكامل أهم عناصره التدخل لضبط

---

[1] مصطفى، معوان (2009). مكافحة الجريمة المعلوماتية، قواعد الإثبات، دار الكتاب الحديث، القاهرة، ط1، ص36.

[2] مصطفى، معوان، مرجع سابق، ص36.

المعاملات، والتجارة الإلكترونية، وإضفاء الحجية القانونية على المستندات الإلكترونية، شأنها شأن المستندات الورقية، حتى يتاح للقاضي الجنائي الاعتماد عليها واتخاذها دليلاً جنائياً كغيره من الأدلة، وقد كان المشرّع التونسي من السبّاقين في هذا المجال، حيث صدر في تونس قانون التجارة والمعاملات الإلكترونية الذي اعترف للمستندات الإلكترونية سنة 2000م بحجيتها في الإثبات، كما أصدر المشرّع الأردني قانون المعاملات الإلكترونية سنة 2001م، كما أصدرت إمارة دبي قانون التجارة الإلكترونية سنة 2002م، وكذلك المشرّع المصري سنة 2004م الذي أصدر قانون التوقيع الإلكتروني، وكل هذه القوانين أعطت للمستند الإلكتروني ذات الحجية التي يتمتع بها المحرر الورقي، وتجدر الإشارة أيضاً إلى أن لجنة الأمم المتحدة للقانون التجاري الدولي (اليونسترال) قد نصت على هذه الحجية، وقد كان ذلك سنة 2000م، أما القانون العربي النموذجي للتوقيع الإلكتروني سنة 2003م فنص في المادة الأولى منه على تعريف الكتابة بأنها: كل عملية تسجيل للبيانات على وسيط لتخزينها، والمقصود بالوسيط في هذه الحالة هو الوسيط الإلكتروني، لأن الوسيط الورقي المتمثل في الأوراق التقليدية لا يحتاج إلى تعريف.

الفرع الثاني: الخبرة والمعاينة والتفتيش في الجرائم الإلكترونية:

تعتبر كل من الخبرة والمعاينة أكبر العقبات التي تواجه الإثبات في الجرائم الإلكترونية، فالمعاينة إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد آثارها بنفسه، فيقوم بجمعها وجمع أي شيء يفيد في كشف الحقيقة، وتقتضي المعاينة إثبات حالة الأشخاص والأشياء الموجودة بمكان الجريمة، ورفع الآثار المتعلقة بها كالبصمات، والدماء، وغيرها مما يفيد التحقيق، والمعاينة تكون شخصية إذا تعلقت بشخص المجني عليه، أو مكانية إذا تعلقت بالمكان الذي تمت فيه الجريمة، ووضع الشهود والمتهم والمجني عليه، أما المعاينة

العينية فهي التي تتعلق بالأشياء أو الأدوات المستخدمة في ارتكاب الجريمة، وقد يقتضي الأمر الاستعانة بخبير للتعرف على طبيعة المادة أو نوعها إذا كان ذلك يحتاج لرأي المتخصص، وفي هذه الحالة يتم إرسال هذه الأشياء إلى الخبير لنكون بصدد إجراءآخر من إجراءات التحقيق وهو الخبرة، فالخبرة هي أحد أهم وسائل جمع الأدلة، يلجأ إليها المحقق عند وجود واقعة مادية أو شيء مادي يحتاج التعرف عليه إلى حكم الخبير المتخصص، فهو يأخذ حكم الشاهد من حيث الحجية أو القوة في الإثبات[1].

يثور التساؤل هنا عن مدى إمكانية معاينة الجريمة الإلكترونية، وإذا كانت المادة (76) من قانون الإجراءات الجنائية الكويتي تنص على انتقال المحقق لأي مكان ليثبت حالة الأمكنة والأشياء والأشخاص، ووجود الجريمة مادياً، فهل يكون للجريمة الإلكترونية وجود مادي يمكن للمحقق الكويتي معاينته؟ نجد في هذه المادة أن المشرّع الكويتي سن هذا النص لضبط جريمة لها وجود مادي محسوس في العالم الخارجي، وما يؤكد ذلك هو أن المادة (91) من ذات القانون أوجبت على المحقق وضع الأشياء والأوراق التي تضبط في حرز مغلق وتربط كلما أمكن، فالحرز المغلق الذي يتم ربطه هو الإجراء العام الذي تخضع له كل الأشياء المضبوطة، وهنا نصطدم بالعقبة الأساسية أمام معاينة الجريمة الإلكترونية التي ترتكب داخل الفضاء الافتراضي، فالمحقق في هذه الحالة يتعامل مع بيئة مليئة بالنبضات الإلكترومغناطيسية والبيانات المخزنة داخل نظام معلوماتية شديدة الحساسية، ولا يتعامل مع أوراق أو أسلحة أو أشياء قابلة للربط وهو ما يؤكد القواعد الإجرائية التقليدية لتواجه سلوكاً مادياً يرتكب بواسطة آلات وأدوات قابلة للربط والتحريز.

---

[1] حجازي، عبد الفتاح (2007). مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص158-159.

أما السلوك الإجرامي في الجريمة الإلكترونية فهو عبارة عن بيانات مخزنة في نظام معلوماتي يتطلب إثباته انتقال محقق متخصص، حيث يتم التفتيش عن البيانات عن طريق نقل محتويات الاسطوانة الصلبة الخاصة بالجهاز، ويجب على المحقق أو ضباط الشرطة المتخصصين استخراج المعلومات التي من شأنها أن تساعد التحقيق، وأن يطلعوا زملائهم عليها، مثل القيام بالبحث في بنوك المعلومات، وفحص كل الوثائق المحفوظة، ومراسلات مرتكب الجريمة مثل الرسائل الإلكترونية، وفك شفرات الرسائل المشفرة[1]، وهو ما يحدث عندما ترتكب الجريمة عبر شبكة الإنترنت، ولكي ينجح المحققون في عملهم يجب أن يتتبعوا أثر الاتصالات منذ الحاسب المصدر إلى الحاسب أو المعدات الأخرى التي تملكها الضحية، مروراً بمؤدي الخدمة والوساطة في كل دولة، كما يقتضي ذلك أيضاً أن يعمل المحقق على الوصول إلى الملفات التاريخية التي تبين لحظات مختلف الاتصالات، من أين صدرت؟ ومن الذي يحتمل إجراؤها، بالإضافة إلى ضرورة إلمام المحقق بالحالات التي يكون عليه فيها التحفظ على الجهاز أو الاكتفاء بأخذ نسخة من الاسطوانة الصلبة للحاسب، والأوقات التي يستخدم فيها برامج استعادة المعلومات التي تم إلغاؤها[2].

فالمحقق الذي يقوم بمعاينة الجريمة الإلكترونية يجب أن يكون ملماً بمهارات هذه التقنية، أما الخبير ففي هذه الحالة يجب أن يكون ملماً بمهارات تحليل البيانات ومهارات التشفير التي تتيح له فكر الرموز واستعادة البيانات الملغية[3].

ولما كانت الجرائم ترتكب عبر الشبكة الدولية، فقد نصت المادة (23) من اتفاقية بودابست على أن: "تتعاون كل الأطراف، وفقاً لنصوص هذا الفصل، على تطبيق الوسائل

---

(1) العنزي، سليمان، مرجع سابق، ص98-99.

(2) موسى، مصطفى، مرجع سابق، ص143.

(3) عبد الله، عبد الله عبد الحكيم، مرجع سابق، ص46.

الدولية الملائمة بالنسبة للتعاون الدولي في المجال الجنائي والترتيبات التي تستند إلى تشريعات موحدة ومتبادلة، وكذلك بالنسبة للقانون المحلي على أوسع نطاق ممكن بين بعضهم البعض بغرض التحقيقات والإجراءات المتعلقة بالجرائم الجنائية للشبكات، والبيانات المعلوماتية، وكذلك بشأن الحصول على الأدلة في الشكل الإلكتروني لمثل هذه الجرائم"، كما نصت المادة (30) من الاتفاقية على الكشف السريع عن البيانات المحفوظة، حيث نصت على: "أنه عند تنفيذ طلب حفظ البيانات المتعلقة بالتجارة غير المشروعة والمتعلقة باتصال خاص تطبيقاً لما هو وارد في المادة (29) فإن الطرف المساند إذا اكتشف وجود مؤدي خدمة في بلد آخر قد شارك في نقل هذا الاتصال، فإن عليه أن يكشف على وجه السرعة إلى الطرف طالب المساعدة كمية كافية من البيانات المتعلقة بالتجارة غير المشروعة حتى يمكن تحديد هوية مؤدي الخدمة هذا والطريق الذي تم الاتصال من خلاله"، كما أشارت المادة (31) إلى المساعدة المتعلقة بالدخول إلى البيانات المحفوظة، حيث أجازت لأي طرف أن يطلب من أي طرف آخر أن يقوم بالتفتيش أو أن يدخل بأي طريقة مشابهة وأن يضبط أو يحصل بطريقة مماثلة، وأن يكشف عن البيانات المحفوظة بواسطة شبكة المعلومات داخل النطاق المكاني لذلك الطرف والتي يدخل فيها أيضاً البيانات المحفوظة وفقاً للمادة (29) من الاتفاقية.

ويرى بعض الفقه أننا نواجه اليوم أخطر مظاهر العولمة، فالتعاون الدولي في المجال الجنائي لم يعد مقتصراً على نظام الإنتربول، فأصبح على الدولة أن تستخدم بروتوكولات موحدة لنظم التخزين والحماية المعلوماتية، كما حدث على مستوى الاتصالات الهاتفية، لأن التعاون بين دولة وأخرى سوف يتم بين أجهزة الخبرة الجنائية بشكل مباشر وبطريقة متشابكة، وهو ما نصل معه إلى أن تطوير البنية التحتية المعلوماتية لأي دولة اليوم أصبح ضرورة

ملحة، ومطلباً أساسياً قد يترتب على غيابه انعزال الدولة وصيرورة نظامها المعلوماتي – إذا كان متواضعاً – مباحاً لمرتكبي الجرائم الإلكترونية[1].

نخلص من كل ما تقدم إلى أن الخبرة والمعاينة الجنائية في الجرائم الإلكترونية اليوم تحتاج إلى إدارة خاصة يعمل بها متخصصون في أنظمة المعلومات ويتمتعون بصفة الضبطية القضائية، وهو ما يتطلب إنشاء إدارة خاصة للخبرة والمعاينة في الجرائم الإلكترونية، ولا يجب الاكتفاء بمجرد تدريب القائمين على إدارة الخبرة الجنائية، أما رجال القضاء والنيابة والضبطية القضائية فلا شك أنهم يحتاجون للتدريب على استخدام مهارات الحاسب الآلي.

أما بالنسبة لإجراءات التفتيش، ففي هذا النمط من الجرائم يتم عادة على شبكات المعلومات، وقد يتجاوز النظام المشتبه به إلى أنظمة أخرى مرتبطة، وهذا هو الوضع الغالب في ظل شيوع الشبكات الداخلية على مستوى الشركات أو المؤسسات والشبكات المحلية والإقليمية والدولية على مستوى الدول[2].

يعتبر امتداد نطاق التفتيش إلى نظام غير النظام محل الاشتباه محل تحديات كبيرة أولها مدى قانونية هذا الإجراء ومدى مساسه بحقوق الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش.

وبالنسبة لإجراءات الضبط فإن عملية الضبط لا يتوقف على تحريز جهاز الكمبيوتر فقد يمتد من ناحية ضبط المكونات المادية إلى مختلف أجزاء النظام التي تزداد يوماً بعد يوم، والأهم أن الضبط ينصب على المعطيات والبيانات والبرامج المخزنة في النظام أو النظم المرتبطة بالنظام محل الاشتباه، وأي أدوات دفع إلكترونية أو أي أشياء ذات طبيعة معنوية

---

[1] الشوا، محمد سامي، مرجع سابق، ص520.

[2] حجازي، عبد الفتاح (2006). مكافحة جرائم الكمبيوتر والإنترنت، دراسة معمقة في القانون المعلوماتي، دار الفكر الجامعي، الإسكندرية، ط1، ص14.

معرضة بسهولة للتغيير والإتلاف، وهذه الحقائق تثير مشكلات متعددة، منها المعايير المقبولة للضبط المعلوماتي ومعايير التحريز إضافة إلى مدى مساس إجراءات ضبط محتويات نظام ما بخصوصية صاحبه – وإن كان المشتبه به – عندما تتعدى أنشطة الضبط إلى كل محتويات النظام التي تضم عادة معلومات وبيانات قد يحرص على سريتها أو أن تكون محل حماية بحكم القانون أو لطبيعتها أو تعلقها بجهات أخرى[1].

ومن ثم فإنّ القواعد العامة التقليدية الواردة في المواد (من 78 إلى 97) من قانون الإجراءات الجنائية الكويتي لا تصلح أساساً للتطبيق في مجال التفتيش بخصوص الجرائم الإلكترونية، وهذا بخلاف الوضع عليه لدى المشرّع الأردني الذي عالج موضوع التفتيش في الجرائم الإلكترونية بموجب نصوص خاصة في قانون جرائم أنظمة المعلومات، إّ تنص المادة (12) منه على أنه: "أ- مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة ومراعاة حقوق المشتكى عليه الشخصية، يجوز لموظفي الضابطة العدلية، بعد الحصول على إذن من المدعي العام المختص أو من المحكمة المختصة، الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم، وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضراً بذلك ويقدمه إلى المدعي العام المختص، ب- مع مراعاة الفقرة (أ) من هذه المادة، ومراعاة حقوق الآخرين ذوي النية الحسنة، وباستثناء المرخص لهم وفق أحكام قانون الاتصالات ممن لم يشتركوا بأي جريمة منصوص عليها في هذا القانون، يجوز لموظفي الضابطة العدلية ضبط الأجهزة والأدوات والبرامج والأنظمة والوسائل المستخدمة لارتكاب أي من الجرائم

---

[1] حجازي، عبد الفتاح، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص148.

المنصوص عليها أو يشملها هذا القانون والأموال المتحصلة منها والتحفظ على المعلومات والبيانات المتعلقة بارتكاب أي منها، ج- للمحكمة المختصة الحكم بمصادرة الأجهزة والأدوات والوسائل وتوقيف أو تعطيل عمل أي نظام معلومات أو موقع إلكتروني مستخدم في ارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون، ومصادرة الأموال المتحصلة من تلك الجرائم والحكم بإزالة المخالفة على نفقة مرتكب الجريمة".

يتضح لنا من هذا النص أن المشرّع الأردني قد أجاز تفتيش مكان الجريمة الإلكترونية والأجهزة والأدوات والبرامج والوسائل المستخدمة في هذه الجريمة، وقد أعطى المحكمة المختصة الحكم بمصادرتها وتوقيف أو تعطيل عمل أي نظام معلومات أو موقع إلكتروني مستخدم في ارتكاب الجريمة الإلكترونية، وبهذا النص يكون المشرّع الأردني قد أوجد حماية جزائية للمشتكي بما يتناسب مع طبيعة الجريمة الإلكترونية.

المطلب الثاني

المشكلات المتعلقة بسلطات التحري والملاحقة

إن خصوصية الجرائم الإلكترونية انعكست على الإجراءات الجزائية المطبقة عليها؛ ومنها السلطة المختصة بالتحري والملاحقة.

فمن المعروف أن صفة الضابطة العدلية لا تمنح إلا بموجب نص خاص، ولقد أشار قانون أصول المحاكمات الجزائية الأردني رقم (9) لسنة 1960م، وكذلك قانون الإجراءات الجنائية الكويتي رقم (17) لسنة 1960م إلى أن هناك قسمين لرجال الضابطة العدلية؛ أولهما أعضاء الضابطة العدلية ذوي الاختصاص العام، والقسم الآخر هو الأعضاء المخولون بهذه الصفة بموجب قوانين خاصة، وخولهم المشرّع اختصاصات ووظائف محددة في القانون تبدأ باستقصاء الجرائم وتنتهي مع انتهاء المحاكمة[1].

ولعل الجرائم الإلكترونية لم تجد بعد لها نصاً خاصاً يحدد من هي الضابطة العدلية المختصة بها، وإن كانت بعض الجهات التي منحها المشرّع صفة الضابطة العدلية الخاصة مثل موظفي مكتب حماية حق المؤلف، حيث يختصون ببعض الانتهاكات التي تقع على حقوق المؤلفين الواقعة باستخدام الوسائل المختلفة ومنها الوسائل الإلكترونية، وعليه فإن الضابطة العدلية العامة بحسب التشريع الأردني والكويتي هي المختصة قانوناً بتقصي الجرائم الواقعة في البيئة الإلكترونية ما لم يحدد سواهم للقيام بذلك وخصوصاً بوجود النصوص التي تسمح للمدعي العام الاستعانة بالخبراء في أي مجال ومنها المجال الإلكتروني.

وقد أعطى المشرّع الأردني بموجب المادة (12) من قانون جرائم أنظمة المعلومات لموظفي الضابطة العدلية بعد الحصول على إذن المدعي العام المختص أو المحكمة المختصة،

---

[1] انظر: المواد (8-10) أصول جزائية أردني، والمواد (39-44) إجراءات جنائية كويتي.

صلاحية الدخول إلى المكان الذي تشير الدلائل إلى ارتكاب الجريمة الإلكترونية من خلاله والقيام بأعمال التفتيش بمعناه الواسع.

ومن الجدير ذكره وجود جمعية أردنية متخصصة بالجرائم الإلكترونية هي الجمعية الأردنية للحد من الجرائم الإلكترونية والإنترنت، والتي تم توقيع نظامها. وفي ظل الفراغ التشريعي بخصوص هذه المسألة في التشريع الكويتي، فإنني أرى بأن النصوص القانونية الواردة في قانون الإجراءات الجنائية المتعلقة بالضابطة العدلية تكفي في الوقت الحاضر بخصوص التحري والملاحقة لمرتكبي الجرائم الإلكترونية أن يقوم المشرّع الكويتي بالتدخل بسن قانون خاص يعالج فيه هذه المسألة.

هذا وتثير الجرائم الإلكترونية إشكاليات تتعلق بعمل سلطات الاستدلال والتحقيق، وهذه مردها الإحجام عن الإبلاغ ونقص خبرة هذه السلطات، هذا ولم يلزم المشرّع الأردني في قانون جرائم أنظمة المعلومات الإبلاغ عن الجريمة الإلكترونية، إلا أن القواعد العامة في قانون أصول المحاكمات الجزائية جعلت الإبلاغ عن الجرائم إلزامي كقاعدة عامة[1].

وهذه القواعد برأي تكفي في حال ارتكاب الجرائم الإلكترونية دون حاجة للنص على ذلك في قانون جرائم أنظمة المعلومات.

المطلب الثالث

المشكلات المتعلقة بالاختصاص والقانون واجب التطبيق

يطرح في هذا المجال التساؤل الآتي: هل تستجيب القواعد التقليدية لتحديد نطاق تطبيق القانون من حيث المكان؟ وهل هناك تحديات مرتبطة بالاختصاص بنظر الجريمة الإلكترونية؟

---

[1] راجع: المادة (25، 26) أصول جزائية أردني، وراجع أيضاً: المادة (35، 36) إجراءات جنائية كويتي.

بالنسبة للاختصاص بالنظر في الجريمة فإنه يلاحظ أن اختصاص القضاء بنظر الجرائم الإلكترونية والقانون الواجب تطبيقه على الفعل لا يحظى دائماً بالوضوح أو القبول أمام حقيقة أن غالبية هذه الأفعال ترتكب من قبل أشخاص من خارج الحدود، أو أنها تمر عبر شبكات معلومات وأنظمة معلومات خارج الحدود حتى عندما يرتكبها شخص من داخل الدولة على نظام في الدولة نفسها، وهو ما يبرز أهمية اختبار مدى ملاءمة قواعد الاختصاص والقانون واجب التطبيق، وما إذا كانت النظريات والقواعد القائمة في هذا المجال تطال هذه الجرائم، أم يتعين أفراد قواعد خاصة بها في ضوء خصوصيتها، وما تثيره من مشكلات في حقل الاختصاص القضائي، ويرتبط بمشكلات الاختصاص وتطبيق القانون مشكلات امتداد أنشطة الملاحقة، والتحري، والضبط، والتفتيش خارج الحدود وما يحتاجه ذلك إلى تعاون دولي شامل للموازنة بين موجبات المكافحة ووجوب حماية السيادة الوطنية[1].

هذا وقد أورد المشرّع الأردني نصاً خاصاً بخصوص الاختصاص القضائي بالجرائم الإلكترونية، هو نص المادة (16) من قانون جرائم أنظمة المعلومات، وجاء نصها: "يجوز إقامة دعوى الحق العام والحق الشخصي على المشتكى عليه أمام القضاء الأردني إذا ارتكبت أي من الجرائم المنصوص عليها في هذا القانون باستخدام أنظمة معلومات داخل المملكة أو ألحقت أضراراً بأي من مصالحها أو بأحد المقيمين فيها أو ترتبت آثار الجريمة فيها، كلياً أو جزئياً، أو ارتكبت من أحد الأشخاص المقيمين فيها".

ففي ضوء هذا النص وضع المشرّع الأردني معاييراً لكي يكون القضاء الأردني مختصاً بنظر الجريمة الإلكترونية، وتتمثل في الآتي:

---

[1] الشوابكة، محمد، مرجع سابق، ص13.

1. إذا ارتكبت الجريمة الإلكترونية داخل المحكمة وكان منصوصاً عليها في القانون المذكور آنفاً.
2. أو ألحقت أضراراً بأي من مصالح المملكة الأردنية.
3. أو بأحد مصالح المقيمين في المملكة الأردنية.
4. أو ترتبت نتائجها وآثار الجريمة كلياً أو جزئياً داخل المملكة الأردنية.
5. أو ارتكبت الجريمة من أحد الأشخاص المقيمين فيها.

وفي ظل الفراغ التشريعي في الكويت بخصوص هذه المسألة؛ فأرى بأن القواعد العامة التي تحكم نطاق تطبيق النصوص الجنائية من حيث المكان والتي تتمثل في مبدأ إقليمية النص الجنائي، والاستثناءات الواردة عليه تقتضي تطبيق النص الجزائي على كل الجرائم الإلكترونية الواقعة في إقليم دولة الكويت، إلا في أحوال خاصة نص عليها المشرّع الكويتي في المواد (11، 12، 13) من قانون الإجراءات الجنائية، والتي تبين حالات يطبق فيها القانون الكويتي على جرائم ارتكبت خارج إقليم دولة الكويت، وهي:

1. ارتكاب جريمة خارج إقليم الكويت، ويكون مرتكبها فاعلاً أصلياً أو شريكاً في جريمة وقعت كلها أو بعضها في إقليم الكويت.
2. كل شخص كويتي الجنسية يرتكب خارج الكويت فعلاً معاقباً عليه طبقاً للقانون الكويتي، وطبقاً للقانون الساري في المكان الذي ارتكب فيه هذا الفعل.

الفصل الرابع

الحلول التشريعية والعملية لمواجهة المشكلات الناجمة عن الجريمة الإلكترونية

سأقوم من خلال هذا الفصل ببيان بعض الحلول على الصعيد التشريعي، وكذلك بيان بعض الحلول العملية للحد من المشكلات التي تثيرها الجرائم الإلكترونية، لذلك سأقسم هذا الفصل إلى مبحثين:

المبحث الأول

الحلول التشريعية في مكافحة الجريمة الإلكترونية

لا هروب من الواقع الذي يشهد تنامي ظاهرة الجرائم الإلكترونية والتي أصبحت تأخذ أنماطاً جديدة كلما زاد الذكاء الإجرامي عبر الوسائل الإلكترونية، ولهذا لا بدّ من معرفة دور بعض التشريعات المقارنة من الحماية الجزائية من الجريمة الإلكترونية ودورها في الحد من مشكلاتها القانونية سواء الموضوعية منها وأيضاً الإجرائية.

وكذلك لا بد من معرفة دور التعاون التشريعي الدولي والإقليمي من هذه المسألة، وأخيراً الوقوف على الجهود الوطنية المؤسسية بهذا الشأن، وعليه سأقسم هذا المبحث إلى ثلاثة مطالب:

المطلب الأول

دور بعض التشريعات المقارنة في الحماية الجزائية من الجريمة الإلكترونية

إن بيان الدور المنوط ببعض التشريعات المقارنة بشأن الحد من مشكلات الجريمة الإلكترونية يتطلب من الباحث استعراض موقف بعض هذه التشريعات سواء الغربية منها وكذلك العربية.

ففي فرنسا صدر قانون 6 يناير 1978م خاص بالمعالجة الإلكترونية للبيانات الاسمية، وبينما كان مطروحاً للنظر أمام مجلس الشيوخ مشروع قانون أعد لتعديل قانون حرية الاتصالات الصادر 1986م ليتفق مع التوجيهات الأوروبية الجديدة، تقدمت الحكومة الفرنسية بتعديل هذا المشروع يتعلق بإضافة مواد جديدة للقانون المذكور بشأن الإذاعة والتلفزيون مستهدفة الحكومة من هذا التعديل تعريف القائم على تقديم خدمة الإنترنت، وشروط التقدم لممارسة هذه الخدمة التي منها ضرورة الحصول على موافقة مسبقة كغيره ممن يقومون بتوفير خدمات الاتصالات السمعية والبصرية من المجلس الأعلى للإذاعة والتلفزيون، وقد اعتبر جانب من الفقه أن المشروع عندما قام بتعريف الاتصالات السمعية والبصرية قد وسّع في التعريف بحيث شمل خدمات الإنترنت من بين وسائل الاتصال، وعندما عرض المشروع على المجلس الدستوري قرر عدم دستورية الفقرتين (2، 3) من المادة (43) من المشروع استناداً إلى أن نص هاتين الفقرتين يخل ويقيد حرية الاتصال وتبادل الأفكار والآراء التي تعد من أسمى حقوق الإنسان الذي من حقه أن يتكلم ويكتب ويطبع بحرية طالما لم يسيء استخدام هذه الحرية التي حددها القانون، وكانت مآخذ المجلس الدستوري على المشروع أنه لم يضع ضوابط يتم بمقتضاها إصدار الموجهات العامة والقرارات التي تصدر بناءً عليها وخصوصاً أنه قد يترتب عليها قيام المسؤولية الجنائية.

وعقب فشل المشرّع الفرنسي تنظيم استعمال الإنترنت في عام 1996م صدر القانون رقم (19) لسنة 1988م المتعلق ببعض الجرائم المعلوماتية مع التعديل الذي أدخل في سنة

1992م، ثم صدر قانون رقم (230) لسنة 2000م في شأن الإثبات والمتعلق بالتوقيع الإلكتروني[1].

وفي الولايات المتحدة الأمريكية صدر في 8 فبراير 1996م قانون بشأن الاتصالات يستهدف تقييد حرية القصر في الاطلاع على الصور والمواد المخلة بالآداب أو التي يكون الأولاد القصر طرفاً فيها، ويمكن الاطلاع عليها من خلال التعامل مع الإنترنت، ورغم أن هذا القانون لم يقم إلا بمد نطاق العقوبات الجنائية السارية بشأن الأعمال الفاضحة التي تتم باستخدام اتصال هاتفي ليشمل أي اتصال يتم بأية وسيلة من وسائل الاتصالات، وجعل من سوء النية ركناً في تلك الجرائم واستحقاق العقاب عنها حينما قرر المشرّع عدم مسؤولية المستعمل أو من يقوم بتوفير خدمات الإنترنت إذا وقع منه بحسن نية، إلا أن بعض الجماعات المدافعة عن الحقوق المدنية اعتبرت أحكام هذا القانون تخالف التعديل الأول للدستور الأمريكي الذي يكفل حرية التعبير عن الرأي وطالبت هذه الجماعات من القضاء وقف العمل بهذا القانون لحين الفصل في عدم دستوريته، وفي 12 يونيو 1996م، وبناءً على دعوى أخرى بوقف العمل بذلك القانون، صدر حكم من محكمة فيلادلفيا الاتحادية ليؤكد أن جماعات الحقوق المدنية أثبتت أن النصوص الخاصة بقانون آداب الاتصال تخالف التعديل الأول للدستور الأمريكي، وبتاريخ 26 يونيو 1997 أصدرت المحكمة العليا الأمريكية حكمها القاضي بعدم دستورية بعض نصوص قانون آداب الاتصالات، وعولت هذه المحكمة في حيثيات حكمها على أنه لا يجوز ترتيب المسؤولية الجنائية على توجيهات أو قرارات عامة لم

---

(1) وعرفت دول أخرى هذا النوع من القوانين مثل ألمانيا منذ عام 1986م، والنمسا والنرويج واليابان منذ عام 1987م، واليونان منذ عام 1988م، الدانمرك، ولكسمبورج وإيطاليا منذ عام 1993م، وسويسرا منذ عام 1994م، وإسبانيا وكندا والدانمرك وفنلندا منذ عام 1995م، راجع تفصيلاً: المطردي، مفتاح بو بكر، مرجع سابق، ص6-7.

توضح الأسباب التي تقوم عليها، أو عبارات نصوص عامة غير محددة الألفاظ من شأنها أن تقيد حرية التعبير عن الرأي التي يكفلها الدستور[1].

وهكذا، وعلى الرغم من فشل محاولة المشرّع الفرنسي والمشرّع الأمريكي وضع ضوابط وتنظيم استعمال الإنترنت، إلا أن النصوص القائمة كانت في أغلبها منطبقة على الجرائم التي تقع عن طريق الإنترنت، إلا أن النصوص القائمة كانت في أغلبها منطبقة على الجرائم التي تقع عن طريق الإنترنت، كتلك النصوص الخاصة بحماية حرية الحياة الخاصة، والنصوص المتعلقة بتجريم القذف والسب، والنصوص التي تحمي الصغار من الاستغلال الجنسي.

وفي المملكة المتحدة، جرت تحقيقات أولية على يد لجنة القانون الاسكتلندي ضمنتها مذكرة استشارية مسببة نشرت عام 1982م، وفي عام 1987م تم نشاط مماثل فيما أعدت فيه ورقة قامت بوضعها لجنة القانون في عام 1988م، ووضعت تقريرها النهائي في عام 1989م، وقد أسفر عن هذه الانشطة توصيات وضع على أساسها قانون أطلق عليه إساءة استخدام الحاسب الآلي الذي تمت الموافقة عليه في يونيو 1990م ودخل حيز التنفيذ في أغسطس من السنة ذاتها[2].

يبدو أن هذه الجهود والمبادرات لمواجهة الجرائم الإلكترونية كانت متأخرة بمنظور الزمن، وذلك على خلفية أن أول جريمة إلكترونية وقعت في الولايات المتحدة الأمريكية كانت عام 1956م، وأن أول جريمة وقعت في البلاد الإسكندنافية كانت في فنلندا عام 1968م متعلقة بتقليد برامج الحاسب الآلي، في حين أن المبادرة الأولى بإصدار تشريع يتعلق بمعلومات

---

[1] مدحت، رمضان (2000). مرجع سابق، ص17 وما بعدها.

[2] الرواشدة، سامي والهياجنة، أحمد، مرجع سابق، ص132-133.

الحاسب الآلي كانت من السويد التي أَدرت قانوناً بشأن حماية المعلومات الشخصية الخاصة المخزنة في الحاسب الآلي والإنترنت عام 1973م، وعدلت تشريعاتها في سنة 1982م، وتلتها الولايات المتحدة الأمريكية التي أصدرت في عام 1976م قانوناً خاصاً بحماية الحاسب الآلي، وفي عام 1984م تبنى الكونجرس قانوناً متعلقاً بالتحليل المعلوماتي، عدّل بالقانون رقم 1986/1213 لمواجهة جرائم الحاسب الآلي، ومن ذعام 1993م وجميع ولايات الولايات المتحدة الأمريكية لها تشريعات خاصة بجرائم الحاسب الآلي، وأخيراً صدر في 14 فبراير 2002م قانون للمعاملات التجارية الرقمية[1].

أما على مستوى الدول العربية، فهناك قرار صادر عن مجلس وزراء العدل العرب بجامعة الدول العربية بشأن مشروع قانون عربي استرشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها، يتكون من 27 مادة وضع من خلالها القواعد الأساسية التي يتعين على التشريعات العربية الاستعانة به عند وضع قانون لمكافحة الجرائم الإلكترونية[2]، كما تسعى الدول العربية إلى إنشاء منظمة عربية تهتم بالتنسيق في مجال مكافحة الجرائم الإلكترونية والتشجيع على قيام اتحادات عربية تهتم بالتصدي لتلك الجرائم، وتفعيل دور المنظمات والإدارات والحكومات العربية في مواجهتها عن طريق نظام الأمن الوقائي[3].

---

(1) وعرفت دول أخرى هذا النوع من القوانين مثل ألمانيا منذ عام 1986م، والنمسا والنرويج واليابان منذ عام 1987م، واليونان منذ عام 1988م، والدانمرك، ولكسمبورج وإيطاليا منذ عام 1993م، وسويسرا منذ عام 1994م، وإسبانيا وكندا والدانمرك وفنلندا منذ عام 1995م، راجع: المطردي، مفتاح بو بكر، مرجع سابق، ص8-9.

(2) اعتمده مجلس وزراء العدل العرب في دورته التاسعة عشرة بالقرار رقم 495-د 19- 2003/10/8؛ ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم 417 – د 2004/21، راجع: قشقوش، هدى، مرجع سابق، ص102-103.

(3) كما بدأ الإدراك بأهمية الموضوع يتزايد في بعض التشريعات العربية مثل: التشريع التونسي الذي كان له فضل البق بين الدول العربية في سن قانون خاص بالتجارة الإلكترونية وهو القانون رقم (83) لسنة

في ضوء ما سبق، فإن الحلول التشريعية تعد أولوية ملحة لمواجهة تحديات ومشكلات الجرائم الإلكترونية، وكما يرى بعض الفقه[1] ينبغي إنجازها على الصعيد التشريعي، وتتمثل هذه الأولويات في الآتي:

أولاً: تحديد الطبيعة القانونية للجريمة الإلكترونية:

إن المال ينقسم إلى نوعين منفصلين وفقاً لطبيعته، فهو إما مال معلوماتي ذو طبيعة معنوية ويتمثل في البرامج والمعلومات أياً كان نوعها، وإما أن يكون المال المعلوماتي ذو طبيعة مادية ويتمثل في أدوات وآلات الحاسب الآلي الملموسة، إذ قد يترتب على اختلاف هذه الطبيعة القانونية للمال المعلوماتي اختلافاً في النتائج المترتبة على تطبيق بعض نصوص القانون الجنائي التقليدي، ولذلك ظهرت هذه الخلافات الفقهية وتبعها في ذلك عدم استقرار الأحكام القضائية، فالاعتداء على برامج ومعلومات الحاسب الآلي يجعلنا أمام مشكلة تقنية ذات طبيعة خاصة يتطلب فيه البحث في تطبيق الجزاء الجنائي الواجب في حالة الاعتداء على المال المعلوماتي المعنوي أي المحتوى الداخلي للشريط الممغنط أو الاسطوانة الممغنطة، وهي ما سميت في فرنسا بجريمة التوصل بطريق التحايل لنظام المعالجة الآلية للبيانات، وهي جريمة مستحدثة تناولها المشرّع الفرنسي بموجب القانون رقم (19) لسنة 1988م بشأن بعض جرائم المعلوماتية في مادته (2/462) [2].

2000م الصادر في أغسطس سنة 2000م في شأن المبادلات والتجارة الإلكترونية، حيث تم بموجب الفصل 8 من إنشاء، كما أصدرت الأردن قانوناً رقم 2001/85م بشأن المعاملات الإلكترونية، راجع: مصطفى، معوان، مرجع سابق، ص46.

[1] انظر: عبد الله، عبد الله عبد الكريم، مرجع سابق، ص165-167؛ والمطردي، مفتاح بو بكر، مرجع سابق، ص21-28.

[2] الشوا، محمد سامي، مرجع سابق، ص521.

ومن خلال تحديد الطبيعة القانونية للمال المعلوماتي المعتدى عليه، يمكن تحديد الطبيعة القانونية للجريمة الإلكترونية والوضع القانوني للبرامج والمعلومات، وهل لها قيمة في ذاتها أم أن قيمتها تتمثل في أنها مجموعة مستحدثة من القيم القابلة للاستثناء يمكن الاعتداء عليها بأية طريقة كانت، وقد سبق للباحث التعرض لهذا الموضوع.

ثانياً: تكريس التطور الحاصل في نطاق تطبيق القانون الجنائي الوطني من حيث المكان:

غالباً ما يتحدد السريان المكاني للقانون الجنائي الوطني وفقاً لأحد مبادئ أربعة: مبدأ الإقليمية، ومبدأ الشخصية، ومبدأ العينية، ومبدأ العالمية، وتتفاوت أهمية هذه المبادئ فيما بينها، وتتدرج في أهميتها بحسب ترتيبها، وتأخذ معظم التشريعات الجنائية بمبدأ الإقليمية كأصل عام ثم تكمله بالمبادئ الأخرى[1].

وتحديد مكان وقوع الجريمة إعمالاً لمبدأ الإقليمية، جاء بشيء من الغموض في بعض من التشريعات، كقانون الجزاء الكويتي الذي نص في المادة (11) بأن: "تسري أحكام هذا القانون أيضاً على الأشخاص الآتي ذكرهم: أولاً كل من ارتكب خارج البلاد فعلاً يجعله فاعلاً لجريمة وقعت كلها أو بعضها في الكويت أو شريكاً فيه ..."، في حين أن البعض الآخر من التشريعات جاءت مفصلة في تحديد متى تعتبر الجريمة واقعة على إقليم الدولة كما هو الحال في قانون العقوبات الأردني[2].

وكان الفقه والقضاء وخاصة في فرنسا لا يميلان إلى أن يقتصر تحديد مكان وقوع الجريمة على الحالات المعروفة[3]، بل كانا يميلان إلى التوسع في تحديد مكان وقوع الجريمة

---

[1] شقير، رامي، مرجع سابق، ص30-31.

[2] انظر: المواد من (7 إلى 11) من قانون العقوبات الأردني.

[3] وهي: 1- وقوع الجريمة بكامل ركنها المادي على إقليم الدولة، 2- تحقق أحد عناصر الركن المادي فحسب على إقليم الدولة، 3- تحقق جزء من عنصر السلوك على إقليم الدولة، 4- وقوع جريمة أصلية

الذي من مظاهره تدويل فكرة مكان وقوع الجريمة من حيث الواقع، واعتبار كل دولة مختصة بنظر هذه الجريمة، ويمكن رصد مظاهر ذلك التوسع في مجال الجرائم الوقتية متعدية الآثار، فعلى الرغم من تنفيذ الجريمة على إقليم الدولة إلا أن آثار هذه الجريمة قد تتعدى حدود دولة التنفيذ، ولم يتنكر القضاء الفرنسي لانعقاد اختصاصه بنظر مثل هذه الجريمة لكون آثارها قد تحققت على الإقليم الفرنسي، كما في إحدى جرائم النشر التي وقعت بواسطة صحيفة تم طبعها وتوزيعها في دولة أجنبية، لكن بعضاً من نسخها قد وزع في فرنسا، كما أجاز القانون والقضاء الفرنسيين بنظر جريمة اعتداء على الملكية الفكرية وقعت في الخارج متى كانت آثارها قد تحققت في فرنسا[1].

وإعمال السريان المكاني للقانون الجنائي وفقاً لأحد المبادئ الأربعة سالفة الذكر، لا يخلو من صعوبات، تفضي إلى إثارة تنازع إيجابي في الاختصاص بين أكثر من تشريع وطني، وأيضاً يقوم تنازع سلبي في الاختصاص يخرج معه اختصاص أي من الدول بملاحقة الجاني، وهذا النوع الأخير من التنازع نادر الوقوع لأن التشريعات الوطنية تعقد اختصاصها وفقاً لمعايير الاختصاص المعروفة، أما في حالة قيام تنازع إيجابي في الاختصاص بين أكثر من دولة لملاحقة نفس النشاط الإجرامي، أو في حالة يثور فيها التنازع كما في الجرائم عبر الوطنية التي يتوزع فيها السلوك المادي للجريمة في إقليم أكثر من دولة، أو في حالة تجرد بعض عناصر هذا السلوك من خصيصتها المادية، كما هو الحال في القرصنة في مجال الحوسبة، وصور المساهمة الجنائية التي تتم باستخدام أجهزة الاتصالات الحديثة؛ مثل هذه

على إقليم الدولة من جانب شخص في الخارج يعتبر فاعلاً لها أو شريكاً فيها، 5- البدء في تنفيذ فعل مكون لجريمة الشروع على إقليم الدولة، وتمثل الحالة الثالثة مظهراً ملحوظاً للتوسع في إعمال مبدأ الإقليمية نص عليها المشرّع الفرنسي في المادة (113-2) من قانون العقوبات الفرنسي الجديد، راجع: المطردي، مفتاح بو بكر، مرجع سابق، ص22.

[1] عبد الله، عبد الله عبد الكريم، مرجع سابق، ص165.

الظاهرة تفرض تنازعاً في الاختصاص بل غموضاً في تحديد معياره، تتطلب بطبيعة الحال حلولاً مستحدثة وابتكاراً لمفاهيم قانونية جديدة دون إخلال بمبادئ الشرعية الجنائية التي ترتكز عليها معظم النظم الجنائية الوطنية[1].

للتغلب على التنازع الإيجابي للاختصاص يوجد حلاّن؛ الأول: يتمثل في محاولة إعطاء الأولوية لأي من الدول المتنازعة وفقاً لأحد معايير الاختصاص الأكثر جدوى وفعالية لضمان ملاحقة الجريمة، ويبدو أن مبدأ الإقليمية هو الأكثر قبولاً، فالدولة التي في إقليمها تقع الجريمة كلها أو الجزء الأكبر من النشاط المكون لركنها المادي، أو النشاط التبعي كله، أو بصفة عامة الدولة التي في إقليمها توجد متحصلات الجريمة، تبدو أرجح الدول اختصاصاً بملاحقة الجريمة ومحاكمة فاعلها، ولا يجد هذا الحل مبرراً فقط في اعتبارات السيادة الوطنية اللصيقة بمبدأ الإقليمية، وإنما أيضاً في جدواه العملية، وأنه حيث تقع الجريمة كلها أو جلها، تصبح أدلة الإثبات متوافرة، ويغدو من اليسير إجراء التحقيقات الكفيلة لإظهار الحقيقة، ويأتي من بعد مبدأ الإقليمية، ومبدأ العالمية، حيث يكون هو الملائم لمعظم الجرائم الإلكترونية التي يتوزع النشاط المكون للركن المادي لها في أكثر من دولة، ثم يلحقه في أولوية الترتيب مبدأ الشخصية في شقه الإيجابي، بحيث ينعقد الاختصاص بنظر الجريمة للدولة التي يحمل جنسيتها مرتكب هذه الجريمة، فإن تعددت جنسياته، فيكون من حق الدول التي يحمل جنسياتها حتى لا يأخذ البعض من اكتساب جنسية جديدة سبيلاً للإفلات من الملاحقة، كما يمكن اللجوء إلى هذا المعيار تفادياً لإفلات المتهم من الملاحقة حين لا يتيسر ملاحقته وفقاً لأي من المعايير السابقة[2].

---

[1] رستم، هشام محمد، مرجع سابق، ص70-71.

[2] شقير، رامي، مرجع سابق، ص143.

أما الحل الثاني في محاولة التغلب على التنازع الإيجابي المتصور في الاختصاص الجنائي بين دولتين أو أكثر، فيتمثل في تدعيم وتأكيد الملاحقة الجنائية في كل حالة يخشى فيها لسبب إجرائي أو لآخر إفلات مرتكب الجريمة من المحاكمة، ومثال ذلك حين تقع الجريمة في إقليم دولة معينة ويتم إلقاء القبض على المتهم في دولة أخرى يكون متمتعاً بجنسيتها، ففي هذا الفرض يثور التنازع في الاختصاص وفقاً لمبدأين متعارضين: مبدأ الإقليمية الذي يمنح الاختصاص لدولة مكان وقوع الجريمة، ومبدأ عالمية حق العقاب الذي يعطي الاختصاص بملاحقة الجريمة لدولة مكان القبض على المتهم، ويبيح لها في الوقت نفسه التنصل من تسليمه استناداً إلى أن معظم الدول ليست ملزمة – بغير اتفاق – بتسليم رعاياها[1].

ثالثاً: اعتبار بعض صور المساهمة في دورها وآثارها من قبيل الجرائم الإلكترونية المستقلة:

جعل اكتمال البناء القانوني لبعض الأنشطة الإجرامية الإلكترونية يستند إلى قيام جريمة أصلية سابقة عليها، كجريمة الاعتداء على الملكية الفكرية، وجريمة تسلم أو إخفاء أشياء مسروقة أو محصلة بأي وجه من الوجوه من جناية أو جنحة (أي المحصلة من مصدر غير مشروع الذي يشكل الجريمة الأصلية)؛ فثمة قوانين وطنية تعاقب على مثل هذه الأنشطة بوصفها من قبيل المساهمة التبعية في الجريمة الأصلية، بمعنى أن مصير ملاحقة مرتكبيها وعقابهم يكون متوقفاً على مصير ملاحقة وعقاب الفاعلين الأصليين للجريمة الأصلية، وقد تتعذر ملاحقتهم لعدم خضوعهم للاختصاص الإقليمي للدولة التي ارتكبت عليه الجريمة التبعية، وهو نهج يترتب عليه التقليل من الحماية الجنائية ويضعف من نظام الملاحقة، على

---

[1] حجازي، عبد الفتاح، مرجع سابق، ص665.

عكس لو اعتبرت هذه الأنشطة جرائم مستقلة بذاتها وليست من الجرائم المساهمة التبعية[1]، والذي من شأنه التقليل من فرص الإفلات من الملاحقة والعقاب أمام مرتكبي الجرائم الإلكترونية، إضافة إلى أن يكون لهذه الأنشطة مدة تقادم خاصة بها، تعطي مدة زمنية أطول للملاحقة، كما لا ينحصر الاختصاص القضائي بنظرها في الدائرة التي وقعت فيها الجريمة الأصلية، بل حسب القاعدة العامة في تحديد الاختصاص[2].

رابعاً: تطوير نظام تقادم الجرائم والعقوبات:

يمثل نظام تقادم الجرائم والعقوبات وسيلة لمرتكبي الجرائم والمحكومين للإفلات من الملاحقة أو تنفيذ الأحكام، وللحد من اختراق ثغرات هذا النظام ينبغي تجريم بعض الأنشطة كالجرائم التبعية باعتبارها جرائم ذات طبيعة مستقلة كما سبقت الإشارة، على الأقل فيما يتعلق بالقواعد المنظمة لتقادم الجرائم، وكذلك اعتبار الجريمة الإلكترونية مرتكبة في وقت اقتراف السلوك أو وقت حدوث النتيجة الإجرامية، أي اعتبار تاريخ السلوك وكذلك تاريخ حدوث النتيجة الإجرامية كنقطة بداية لسريان مدة التقادم، أو باعتبار بعض الجريمة الإلكترونية من قبيل الجرائم المستمرة، بما يكفل مدة تقادم أطول، وأخيراً رفع تباين التشريعات الوطنية فيما يخص تحديد مدة التقادم وتدقيق فكرة انقطاعه ووقفه[3].

خامساً: الاعتراف في بعض الحالات بحجية للتشريعات والأحكام الجنائية غير الوطنية:

القاعدة التقليدية هي تلازم السيادتين التشريعية والقضائية في المجال الجنائي، بما يعني أن كل دولة لا تعترف سوى بأحكام قانونها الجنائي الوطني، ولا تعتد، ولا تنفذ على إقليمها سوى

---

(1) راجع: المادة 1/465 مكررة (أ) من قانون الجزاء الكويتي، وانظر: شقير، رامي، مرجع سابق، ص144.

(2) المطرودي، مفتاح بن بكر، مرجع سابق، ص26.

(3) إبراهيم، خالد ممدوح، مرجع سابق، ص158.

الأحكام الجنائية الصادرة عن إحدى محاكمها الوطنية، ويجد ذلك سنده في أن تطبيق القانون الجنائي يعدّ تعبيراً عن سيادة الدولة بوصفه يحمي المصالح الأساسية للمجتمع والدولة والحقوق الجوهرية لأفراده، إضافة إلى أن قواعد القانون الجنائي تتعلق في جملتها بالنظام العام، وهو ما يحول دون الخضوع لحكم قانون أجنبي وتطبيقه[1].أما فيما يتعلق بحجية الأحكام الجنائية الأجنبية في شقها الإيجابي، فإنه يجب أن يفسح لها مكان بين أحكام المعاهدات الدولية ذات الصلة، وهكذا يمكن أن يؤخذ في الاعتبار بالآثار الجنائية غير المباشرة للأحكام الجنائية الأجنبية لا سيما في الاعتبار بالآثار الجنائية غير المباشرة للأحكام الجنائية لا سيما في مجال العود، ووقف التنفيذ وتقدير العقوبة في ضوء ما يثبت من الخطورة الإجرامية للجاني، أما بالنسبة لحجية الأحكام الجنائية في شقها السلبي، فقد اعترف بها بعض المشرّعين، إذ يمتنع إقامة الدعوى الجنائية ضد من ارتكب جريمة في الخارج متى ثبت أن المحاكم الجنائية الأجنبية قد برأته أو أدانته نهائياً واستوفى عقوبته، فكأن هؤلاء المشرّعين يعترفون بقوة الشيء المحكوم فيه ولو تعلق الأمر بحكم أجنبي تطبيقاً لقاعدة امتناع محاكمة الشخص عن ذات الفعل مرتين[2].أرى أنه حان الأوان لتجاوز بعض المفاهيم التقليدية، وخاصة فيما يتعلق بتلازم السيادتين التشريعية والقضائية في المجال الجنائي في الجرائم الإلكترونية، وذلك بالتوجه نحو الاعتراف في بعض الحالات وعلى نحو ما بحجية لتشريع جنائي عبر وطني، وبحجية لحكم جنائي صادر عن محاكم دولة أخرى، وتتجلى أهمية ذلك على وجه الخصوص في مجال الجرائم الإلكترونية التبعية التي تفترض ارتكاب جريمة أصلية على إقليم دولة ما، ثم وقوع الجريمة التابعة على إقليم دولة أخرى، ومثال ذلك جريمة الاعتداء إلكترونياً على حقوق الملكية الفكرية.

---

(1) المطردي، مفتاح بو بكر، مرجع سابق، ص27.

(2) سلامة، محمد عبد الله، مرجع سابق، ص148-149.

المطلب الثاني

التعاون التشريعي الدولي والإقليمي لمكافحة الجريمة الإلكترونية

ترتكب الجريمة الإلكترونية في مسرح غير قابل للتحديد الجغرافي، إلا أنه يضم أكبر تجمع إنساني يتميز بارتباط وتشابك معقد، وتتمثل أهم خصائصه في خلق آليات خاصة لفرض الالتزامات والإذعان لها مثل قطع الاتصال على مخترقي بعض القواعد، أو طردهم من المنتديات، لكن هذا التجمع الإنساني الضخم يفتقر إلى المعايير الأخلاقية المشتركة، وهو ما حدا المجلس الأوروبي إلى عقد اتفاقية بودابست عام 2001م بشأن الجرائم الإلكترونية، والتي قدّمت صوراً لمكافحة الجرائم الإلكترونية، ونصت المادة (22) منها على: "أن لكل طرف اتخاذ الإجراءات التشريعية وغيرها التي يراها لازمة لكي يحدد اختصاصه بالنسبة لكل جريمة تقع وفقاً لما هو وارد في المواد من (2 إلى 11) من الاتفاقية الحالية عندما تقع الجريمة:

أ. داخل نطاق المحلي للدولة.

ب. على ظهر سفينة تحمل علم تلك الدولة.

ج. على متن طائرة مسجلة في هذه الدولة.

د. بواسطة أحد رعاياها، إذا كانت الجريمة معاقباً عليها جنائياً في المكان الذي ارتكبت فيه، أو إذا كانت الجريمة لا تدخل في أي اختصاص مكاني لأي دولة أخرى.

ولكل طرف أن يحتفظ لنفسه بالحق في عدم تطبيق، أو عدم التطبيق إلا في حالات وفي ظل شروط خاصة، قواعد الاختصاص المنصوص عليها في الفقرة الأولى (ب و د) من هذه المادة أو في أي جزء من هذه الفقرات.

وتنص الفقرة (4) من المادة نفسها على عدم استبعاد أي اختصاص ينعقد للقضاء الوطني طبقاً للقانون المحلي، الفقرة (5) تنص على أنه في حالة حدوث تنازع في الاختصاص فإنه يجب أن يتم حله بالتشاور بين الدول الأطراف حول المكان الأكثر ملائمة، كما أفردت الاتفاقية بنداً خاصاً لضرورة التعاون بين الدول[1].

هذا ولم ينص القانون العربي النموذجي بشأن الجرائم الإلكترونية[2] على أي قواعد لتحديد الاختصاص بنظر هذه الجرائم، فإن كان الفقه الجنائي اليوم قبل فكرة تطبيق القانون الأجنبي لمواجهة الجريمة عبر الوطنية ما أظهر ضرورة تجاوز فكرة تلازم الاختصاص الجنائي القضائي والتشريعي، فيلزم من باب أولى قبول هذه الفكرة والتوسع فيها بالنسبة لجرائم ترتكب في القضاء الافتراضي الذي يتجاوز الحدود والقارات، وبذلك نصل إلى ضرورة التفكير في وضع ضوابط إسناد جنائية لتحديد الاختصاص الموضوعي والإجرائي بعد أن تصنف الجرائم الإلكترونية إلى فئات مختلفة تشكل كل فئة فكرة مسندة تتضمن المصالح الواجب حمايتها جنائياً على المستوى العالمي لوضع ضوابط إسناد تشير إلى القانون واجب التطبيق[3].

إلا أن هذه القواعد يجب أن تتم صياغتها في إطار اتفاقيات دولية لأن الجريمة الدولية لا يمكن مواجهتها إلا بالتعاون الدولي، وهو أهم ما جاء في اتفاقية بودابست بشكل يسمح بتبادل التعاون سواء كان ذلك على مستوى جمع الأدلة أو تسليم المجرمين، وهو ما يعني أن المجتمع الدولي مقبلاً على توسع في مجال التعاون القضائي الذي يتوقع أن يتم بين الأجهزة

---

(1) تفصيلاً راجع: عبد الله، عبد الله عبد الكريم، مرجع سابق، ص105 وما بعدها.

(2) اعتمدت جامعة الدول العربية عبر الأمانة الفنية لمجلس وزراء العدل العرب ما سمي بقانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها، وقد اعتمده بموجب قرار رقم 417/ د21/ 2004م، للتفصيل راجع: عبد الله، عبد الله عبد الكريم، مرجع سابق، ص140 وما بعدها.

(3) المطرودي، مفتاح بو بكر، مرجع سابق، ص27.

القضائية والأمنية بشكل مباشر نظراً لأن عامل الوقت في حفظ الأدلة الإلكترونية سوف يكون حرجاً ومتطلباً لسرعة الإنجاز[1].

وعلى الرغم من ضرورة التعاون الدولي بشأن مواجهة تحديات الجرائم الإلكترونية، وتضافر الجهود من أجل تفعيله، إلا أن هناك العديد من العقبات التي تعترض سبيله، من أبرزها: عدم وجود اتفاق عام بين الدول على مفهوم الجرائم الإلكترونية، وعدم وجود توافق بين قوانين الإجراءات الجنائية للدول بشأن التحقيق في تلك الجرائم، والنقص الظاهر في مجال الخبرة لدى الشرطة وجهات الادعاء والقضاء[2].

المطلب الثالث

الجهود الوطنية المؤسسية في مجال مكافحة الجريمة الإلكترونية

سأقوم ببيان بعض الجهود الوطنية التي من شأنها الحد من مشكلات الجرائم الإلكترونية، ولعل من أبرزها: التجربة المصرية والأردنية، ولذلك سأقسم هذا المطلب إلى فرعين.

الفرع الأول: مكافحة الجرائم الإلكترونية في مصر:

لقد وضع المؤتمر الأول لجمعيات قانون الإنترنت والذي عقد بالقاهرة في 27 سبتمبر 2004م اللبنة الأولى لإنشاء جمعيات ومنظمات أهلية للعمل التطوعي في مجال قانون الإنترنت، ومن هنا جاء تأسيس الجمعية المصرية لمكافحة جرائم المعلوماتية والإنترنت تلبية سريعة لدعوة المؤتمر التأسيسي لجمعيات ومنظمات قانون الإنترنت من جانب نخبة من

---

(1) البشري، محمد الأمين (2009). التحقيق في جرائم الحاسب الآلي، دار الكتب القانونية، مصر، ص178.

(2) عوض، محمد محيي الدين (2011). مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات، دار الفكر العربي، القاهرة، ط1، ص326-327.

القضاة ووكلاء النائب العام، والمحامون، والمحاسبون، والمصرفيون، والإعلاميون، ومهندسي تكنولوجيا المعلومات والاتصالات[1].

تعتبر الجمعية المصرية لمكافحة جرائم المعلوماتية والإنترنت منظمة غير حكومية خاضعة للقانون المصري ومشهرة تحت رقم (2176) لسنة 2005م وصدر قرار إشهارها بتاريخ 2005/8/5م[2].

إن انتشار تكنولوجيا المعلومات والاتصالات الجديدة على نطاق العالم أدى إلى ظهور أشكال من الجرائم المتصلة بالحواسيب والتي تشكل خطراً على سرية النظم الحاسوبية أو سلامتها أو توافرها بل يتعدى ذلك ليشكل خطراً متعاظماً على أمن البنى الأساسية الحرجة، وفضلاً عن ذلك فإن الابتكارات التكنولوجية تسفر عن أنماط مختلفة من الابتكار الإجرامي، فعند مكافحة هذه الجرائم يواجه المحققون وممثلو الادعاء العام والقضاة على السواء عدداً من المشاكل التي تنجم جزئياً عن الطابع غير الملموس للأدلة الرقمية وسرعة اختفائها، وعلاوة على ذلك فإن التحقيق في الجرائم المتصلة بالحواسيب وملاحقتها قضائياً غالباً ما يقتضيان تتبع النشاط الإجرامي وإثارته من خلال مجموعة متنوعة من مقدمي خدمات الإنترنت أو الشركات التي تقوم بذلك، ويتجاوز هذا التتبع أحياناً الحدود الوطنية، الأمر الذي يثير أسئلة صعبة تتعلق بالولاية القضائية والسيادة، وتفرض التحديات الخاصة بالجرائم المتصلة بالحواسيب إقامة تعاون دولي فعّال في هذا المجال، وبالتالي فإن ذلك يقتضي أن يكون لدى كل دولة في العالم الأدوات القانونية والإجرائية والتنظيمية اللازمة لذلك، كما أن زيادة وكثافة تكنولوجيا المعلومات والاتصالات وجني فوائد مجتمع المعلومات يؤدي أيضاً لزيادة الجرائم

---

[1] عبد الله، عبد الله عبد الكريم، مرجع سابق، ص94.

[2] انظر الموقع الآتي: www.eapiic.org.

المتصلة بالحواسيب، وبالتالي فإنه من مصلحة الأمن الاقتصادي والأمن العام سن تشريعات محلية لمكافحة الجرائم المتصلة بالحواسيب[1].

وتتمثل الأهداف المتوخاة من الجمعية بالتالي[2]:

1. نشر الوعي والقيام بحركة تـــثـــقيف اجتماعية، وقانونية، واقتصادية، وتنموية، للتعريف بالجرائم الناشئة عن استخدام الإنترنت.
2. إعداد الدراسات والبحوث حول العلاقة الرقمية بالقاعدة الموضوعية والإجرائية في القانون الجنائي والحث على تطويره.
3. إعداد ومتابعة التجمعات العلمية والأكاديمية، وحضور المؤتمرات والندوات المتعلقة بالجرائم ضد المعلوماتية، والجرائم الناشئة عن استخدام الإنترنت.
4. إعداد قاعدة إحصائية للجرائم ضد المعلوماتية والجرائم الناشئة عن استخدام الإنترنت.
5. تقديم الدعم والعون العلمي للمؤسسات والأفراد وكل من له مصلحة في مكافحة الجرائم الناشئة عن استخدام الإنترنت.
6. تنمية الكوادر البشرية في مجال مكافحة الإجرام عبر الإنترنت.
7. متابعة التقارير والدراسات والبحوث، والعمل على تشجيع البحث العلمي في مجال دراسة الجرائم الناشئة عن استخدام الإنترنت.

أما بخصوص أنشطتها[3]، فهي:

1. إعداد المؤتمرات والندوات وورش العمل وإلقاء المحاضرات والمشاركة في كل ذلك والمساهمة مع المؤسسات الأخرى ذات العلاقة بأغراض الجمعية.

---

(1) عوض، محمد محيي الدين، مرجع سابق، ص158.

(2) انظر الموقع الآتي: www.eapiic.org.

(3) انظر الموقع الآتي: www.eapiic.org.

2. متابعة الفقه والقضاء المقارن في كل ما ينشر والمبادرة إلى تعميمها عن طريق إصدار المصنفات والمطبوعات.
3. التـــثـــقيف والتدريب وإنشاء مؤسسات تدريبية والمساهمة مع الغير فيها بقصد السعي إلى تطوير قانون الإجراءات الجنائية لكي يتفاعل مع الأدلة الرقمية.
4. إصدار الدوريات والنشرات والبحوث والعمل على نشرها، وتعميمها وبثها عبر الإنترنت.
5. تقديم الاستشارات والخدمات، وإعداد وتنفيذ الدراسات المتخصصة في مجالات عمل الجمعية.
6. المساهمة في تقديم خدمات البلاغ الرقمي ومتابعة هذا البلاغ.
7. تبادل الخبرات والزيارات والدراسات المشتركة مع الجهات المعنية بأهداف وأنشطة الجمعية.
8. نشر فكر ووعي قانون الإنترنت والسعي لدى المشرّعين على كافة المستويات لقيام فرع قانون الإنترنت.
9. مكافحة كافة أشكال الجرائم التي تقع ضد المعلوماتية في كافة أشكالها (الأجهزة، والبرامج، والشبكات، والمعلومات، والبيانات، والأموال، ووسائل الاتصال، والجرائم ضد السمعة، والجرائم ضد الشخصية، والجرائم ضد الإنسانية، والجرائم الموجهة للأمن القومي في كافة أشكالها وصورها)، وبالعموم مكافحة كافة الجرائم التي يكون الحاسب أداة من أدواتها أو هدفاً من أهدافها أو وسطاً لها.

وتسعى الجمعية للتعاون مع كافة قطاعات المجتمع وعلى الأخص كليات الحقوق، وكليات المعلومات والحاسبات، وشركات القطاع الخاص العاملة في مجال تكنولوجيا

المعلومات، والنقابات المهنية، والاتحادات العمالية، وكافة الوزارات والهيئات المعنية بميدان عمل الجمعية، ومنظمات العمل المدني في مصر.

كما تسعى الجمعية لعقد اتفاقيات تعاون فيما بينها وبين كافة الجهات المماثلة لها في كافة الدول العربية، كما تسعى الجمعية لدى جامعة الدول العربية لإنشاء جمعيات مثيلة في الأقطار العربية، وتؤكد الجمعية على دعمها ومؤازرتها للجمعية العربية لقانون الإنترنت والالتزام بنظامها الأساسي، والالتزام بمقررات المؤتمر الدولي الأول لقانون الإنترنت الذي انعقد في مدينة الغردقة بجمهورية مصر العربية في شهر أغسطس سنة 2011م، وتؤكد على حصرها للانضمام لعضوية الجمعية العربية لقانون الإنترنت، وتسعى الجمعية للحصول على عضوية الجمعية الدولية لقانون الإنترنت فور الإعلان عن تأسيسها وقيامها خلال فعاليات المؤتمر الدولي الثاني لقانون الإنترنت، كما تسعى للتعاون مع الجهات المثيلة لها في كافة دول العالم للاستفادة بالخبرات السابقة في مجال عمل الجمعية[1].

الفرع الثاني: مكافحة الجرائم الإلكترونية في الأردن:

أتى إنشاء الجمعية الأردنية للحد من جرائم المعلوماتية والإنترنت متوائماً مع مبادئ الأمم المتحدة، بحيث أن الجمعية الأردنية للحد من جرائم المعلوماتية والإنترنت أكدت التزامها بالقيم التي أرساها المؤتمر التأسيسي لجمعيات قانون الإنترنت الذي عقد بالقاهرة في 27 سبتمبر 2004م، والمؤتمر التأسيسي الثاني الذي عقد بالقاهرة في 2006/7/31م، إضافة إلى الالتزام بمقررات المؤتمر الدولي الأول لقانون الإنترنت الذي انعقد في مدينة الغردقة بجمهورية مصر العربية في شهر أغسطس سنة 2011م[2].

---

(1) انظر الموقع الآتي: news.moffed.com.

(2) الشوابكة، محمد، مرجع سابق، ص143.

والأسباب التي دعت لإنشاء الجمعية، هي[1]:

1. إن انتشار تكنولوجيا المعلومات والاتصالات الجديدة على نطاق العالم أدى إلى ظهور أشكال من الجرائم المتصلة بالحواسيب والتي تشكل خطراً على سرية النظم الحاسوبية أو سلامتها أو توافرها بل يتعدى ذلك ليشكل خطراً متعاظماً على أمن البنى الأساسية الحرجة، وفضلاً عن ذلك فإن الابتكارات التكنولوجية تسفر عن أنماط مختلفة من الابتكار الإجرامي.
2. تفرض التحديات الخاصة بالجرائم المتصلة بالحواسيب إقامة تعاون دولي فعّال في هذا المجال، وبالتالي فإن ذلك يقتضي أن يكون لدى كل قطاع في العالم الأدوات القانونية والإجرائية والتنظيمية اللازمة لذلك.
3. إن زيادة وكثافة تكنولوجيا المعلومات والاتصالات، وجني فوائد مجتمع المعلومات يؤدي أيضاً لزيادة الجرائم المتصلة بالحواسيب، وبالتالي فإنه من مصلحة الأمن الاقتصادي والأمن العام سن تشريعات محلية لمكافحة الجرائم المتصلة بالحواسيب والإنترنت.
4. لقد تطورت القوانين الوطنية على مدى قرون بينما تطور الإنترنت على مدى عقود قليلة فقط، وغني عن القول أن القانون يواصل التكيف مع تغير المجتمع وربما تحتاج التشريعات الوطنية إلى التحديث للتصدي للجرائم المتصلة بالحواسيب والإنترنت.
5. إن تنامي اعتماد الحكومات والأعمال التجارية والمنظمات الأخرى أدى المعتمدين على تكنولوجيا المعلومات لتوفير السلع والخدمات الأساسية، وتسيير الأعمال، وتبادل المعلومات يحتم التعاون بين الحكومات وممثلي القطاع الخاص، والمجتمع المدني والمجتمع بأكمله.

---

[1] انظر الموقع الخاص بالجمعية على شبكة الإنترنت: www.uaegrap.net.

6. لقد أصبحت مشاركة القطاع المدني والعمل الأهلي التطوعي في التصدي للمشكلات التي تواجه المجتمع العامل الحاسم لضمان النجاح في التصدي لهذه المشكلات، من خلال تنمية الوعي المجتمعي وإيجاد ثـــقافة عامة على صعيد المجتمع بكامله ترفض السلبيات وتعمل على تنمية الإيجابيات.

انطلاقاً مما تقدم وفي 2006/4/1م أسس الموقعون على النظام الأساسي ومن ينظم إليهم، في المملكة الأردنية الهاشمية جمعية تحت اسم الجمعية الأردنية للحد من جرائم المعلوماتية والإنترنت، ويكون مركز عملها عمّان، وفق الأهداف والغايات التالية[1]:

1. نشر الوعي والقيام بحركة تـــثـــقيف اجتماعية وقانونية، واقتصادية وتنموية للتعريف بالجرائم الناشئة عن استخدام الإنترنت.
2. إعداد الدراسة والبحوث حول العلاقة الرقمية بالقاعدة الموضوعية والإجرائية في القانون الجنائي والحث على تطويره.
3. إعداد ومتابعة التجمعات العلمية والأكاديمية وحضور المؤتمرات والندوات المتعلقة بالجرائم ضد المعلوماتية والجرائم الناشئة عن استخدام الإنترنت.
4. إعداد قاعدة إحصائية وبنك معلومات للجرائم ضد المعلوماتية والجرائم الناشئة عن استخدام الإنترنت.
5. تقديم الدعم والعون العلمي للمؤسسات والأفراد وكل من له مصلحة في مكافحة الجرائم الناشئة عن استخدام الإنترنت.
6. تنمية الكوادر البشرية في مجال مكافحة الإجرام عبر الإنترنت.

---

[1] انظر أيضاً موقع الجمعية على شبكة الإنترنت: www.uaegroup.net.

7. دعم الاهتمام بقانون الإنترنت والتعاون مع الأطراف ذات العلاقة لبحث جوانبه والتعرف على موضوعات المتعددة والمتطورة.
8. متابعة التقارير والدراسات والبحوث والعمل على تشجيع البحث العلمي في مجال دراسة الجرائم الناشئة عن استخدام الإنترنت.

وتهتم هذه الجمعية بالقضايا الآتية[1]:

1. نشر فكر ووعي قانون الإنترنت والسعي لدى المشرّعين على كافة المستويات لقيام فرع قانون الإنترنت.
2. الحد من كافة أشكال الجرائم التي تقع ضد المعلوماتية في كافة أشكالها (الأجهزة والبرامج والشبكات والمعلومات والبيانات والأموال ووسائل الاتصال والجرائم ضد السمعة، والجرائم ضد الشخصية، والإرهاب عبر الإنترنت)، والجرائم ضد الإنسانية، والجرائم الموجهة للأمن القومي في كافة أشكالها وصورها، وبالعموم المساهمة في الحد من كافة الجرائم التي يكون الحاسب أداة من أدواتها، أو هدفاً من أهدافها، أو وسيلة لها.

---

[1] انظر موقع الجمعية: www.uaegroup.net.

المبحث الثاني

الحلول العملية في مكافحة الجريمة الإلكترونية

سأقوم من خلال هذا المبحث ببيان بعض الحلول العملية فيما يتعلق ببعض الإجراءات المتطلبة في هذا المجال وفيما يتعلق بضبط وتفتيش الآليات التي تنفذ من خلالها الجرائم الإلكترونية، وذلك من خلال مطلبين:

المطلب الأول

الحلول العملية فيما يتعلق ببعض الإجراءات المتطلبة لمكافحة الجريمة الإلكترونية

يطرح بعض الفقه[1] حلولاً عملية لمواجهة تحديات ومشكلات الجرائم الإلكترونية، وتتمثل بالآتي:

أولاً: لا بدّ من اتخاذ وسائل الحيطة والحذر في تعامل البنوك مع الأنشطة المصرفية التي تتم عبر الإنترنت نظراً لأن تركيز غاسلي الأموال يتم على هذه البنوك، وبهذه الأساليب باعتبارها مرتعاً خصباً لتجارتهم خصوصاً إذا كانت الدول التي ترعى هذه البنوك أو التي في ضيافتها تعاني من عجز في النظام الرقابي العام للدولة.

ثانياً: إصدار قوانين واضحة وصارمة تلزم جميع المصارف بوضع الخطوات العملية الضرورية لمنع غسل الأموال فيها خاصة تلك الأموال التي يتم التعامل بها عبر الإنترنت.

ثالثاً: ضرورة قيام المصارف بتدابير عملية من شأنها تكشف محاولات غسل الأموال فيها، ومراقبة جميع التعاملات الإلكترونية.

---

[1] انظر: الألفي، محمد (2005). المسؤولية الجنائية عن الجرائم الأخلاقية عبر الإنترنت، المكتب المصري الحديث، القاهرة، ص203-204؛ وعوض، محمد محيي الدين، مرجع سابق، ص153-155؛ وعبد الله، عبد الله عبد الكريم، مرجع سابق، ص54-55.

رابعاً: ضرورة قيام المصارف بإنشاء أجهزة أو إدارات تتولى مراقبة ومتابعة البلاغات التي تصلها عن أي عملية أو نشاط مشبوه، وبالتالي الإبلاغ عنها للجهات المختصة في الدولة خاصة إن كانت تلك العمليات المصرفية تتعلق بأنشطة تتم عبر الإنترنت.

خامساً: ضرورة تدريب العاملين في المباحث الجنائية على تفحص الأدلة الإلكترونية.

سادساً: ضرورة تدريب المحققين على القيام بالكشف عما تحتويه أجهزة الكمبيوتر من برامج مخزنة عند الضرورة مما ييسر عمليات التفتيش التي تتم على كمبيوتر المتهم.

سابعاً: ضرورة الاستعانة بخبراء في الكمبيوتر والشبكات أثناء عمليات التقصي والتحقيق في الجرائم المعلوماتية والإنترنت.

المطلب الثاني

الحلول العملية فيما يتعلق بضبط وتفتيش الآليات التي تنفذ من خلال الجريمة الإلكترونية

إن الانتشار الكبير للإنترنت في الحياة العملية أظهر الحاجة في وضع الحلول العملية للمشاكل الناتجة عن استخدام الإنترنت في ضوء القواعد العامة للقانون، إضافة إلى أهمية توجيه نظر المشرّع للتدخل لوضع قواعد خاصة لتنظيم استخدام الإنترنت في بعض المجالات الحيوية واستخلاص القواعد الرئيسة في هذا المجال والتي يمكن للمشرّع أن يستهدي بها إذا ما أراد يوماً تنظيم مجال أو أكثر من مجالات استخدام الإنترنت بقواعد خاصة كالإثبات، وكذلك بيان الأحكام القانونية لاستخدام الإنترنت في بعض المجالات.

يشار في هذا المجال إلى أن شركة مكافئ المتخصصة في تقنيات حماية أنظمة المعلومات أعلنت عن النتائج التي توصلت إليها آخر الأبحاث، والتي تثبت أن الجريمة الإلكترونية المنظمة تعمل على إغواء الجيل الجديد من مستخدمي الكمبيوتر وإعداده لتنفيذ الجرائم الشبكية المدهشة باستخدام تكتيكات تشبه تكتيكات الكي جي بي، المخابرات الروسية، لتجنيد العملاء خلال الحرب الباردة، فقد أظهر تقرير مكافي السنوي الثاني حول الإنترنت والجريمة والمنظمة، والذي يعتمد على النتائج التي توصلت إليها أهم وحدات مكافحة جرائم التقنية الرفيعة في أوروبا والأف بي آي، أن عصابات الجريمة المنظمة قد أصبحت تستهدف أوائل طلبة المعاهد الأكاديمية الشهيرة لكي يحصلوا على المهارات التي تتيح لهم تنفيذ جرائمهم الجديدة ذات التقنية الرفيعة والنطاق الواسع، كما تظهر الدراسة أيضاً أن المراهقين الماهرين في استخدام الإنترنت، والذي قد لا تتجاوز أعمارهم في بعض الحالات الرابعة عشرة قد صاروا ينجذبون إلى جرائم الشبكة العالمية نتيجة الصيت الواسع الذي يحظى به مجرمو التقنية الرفيعة وإمكانية اكتساب بعض المال دون التعرض لمخاطر الجرائم التقليدية.

ويذكر التقرير أيضاً أن مجرمي الشبكة العالمية قد بدأوا يغادرون أماكنهم الخاصة إلى الأماكن العامة، كمقاهي الإنترنت، والمقاهي المزودة بشبكات الواي فاي، ومن النتائج الهامة الأخرى التي توصل إليها تقرير مكافحي حول الجريمة في العالم الافتراضي لعام 2006م:

1. جماعة جرائم الشبكة العالمية: لقد نجحت الجريمة الشبكية في تأسيس جماعة لها أتباع، تضم بعض مجرمي الإنترنت الذين ارتقوا لكي يحتلوا مكانة رفيعة في أوساط المتسللين غير الشرعيين.
2. أساليب جديدة لتطوير البرامج الضارة: أصبحت جماعات الجريمة المنظمة تلجأ إلى أساليب تشبه أساليب الكي جي بي لاستقطاب الأجيال الجديدة من المتسللين لكتابة البرامج الضارة.
3. جرائم داخلية: مستغلين ضعف الإجراءات الأمنية في الشركات، أصبح الموظفون الحاليون والسابقون، والمتعاملون مع الشركة من المتعهدين والمقاولين، من أكثر من ينظم عمليات الهجوم على شبكات الشركة والتسلل إليها، بل صار مجرمو الشبكة العالمية يتوجهون إلى الخريجين الجدد وتجنيدهم لكي يستفيدوا من معرفتهم الداخلية بشبكات الشركات التي سيعملون بها، ويلقي تقرير مكافي للجرائم الافتراضية لعام 2006م الأضواء على إمكانات التسلل وإخفاء الهوية التي تقدمها بيئة الشبكة العالمية، وكيف أصبح كشف هويات المجرمين أمراً في غاية الصعوبة على هيئات تطبيق القانون، كما أورد التقرير القائمة التالية التي تشمل أخطر التهديدات والأدوات والفرص التي تستكشفها حالياً عصابات الجريمة المنظمة، حسب رأي مكافحي:
    - **الألعاب الذهنية:** يزداد توجه مجرمو الشبكة العالمية إلى أساليب الحرب النفسية لكي ينجحوا في مساعيهم، لقد ارتفع حجم رسائل سرقة المعلومات الشخصية

بنسبة تقترب من 25% خلال العام الماضي، ويوماً بعد يوم يصبح من الصعب كشفها وتزداد أعداد الناس الذين تنجح في خداعهم من خلال لجوئها إلى قصص واقعية بدلاً من الوعود الخلابة التي لا يمكن أن يصدقها أحد، كالفوز بملايين الدولارات.

- **الحيل الاجتماعية:** إن مجرمي الشبكة العالمية تجتذبهم التجمعات الكبيرة في الشبكات الاجتماعية والمواقع الجماعية، فيملأون هوياتهم وصفحاتهم المزيفة بالبرامج الإعلانية والتجسسية وأحصنة طراودة، حتى أصبح مؤلفو البرامج الضارة يقبضون ثمن شعبيتهم، كما يقومون أيضاً بتجميع المعلومات الشخصية المبثوثة عبر الإنترنت ليخلقوا لأنفسهم هوية ثانية مزيفة ويستخدمونها في أغراضهم الشريرة.
- **تسرب البيانات:** إن الكثير من البيانات مكشوفة ولا يتطلب الاستيلاء عليها أساليب معقدة، ومجرمو الشبكة العالمية لها بالمرصاد، إن انتشار استخدام كلمات السر في مواقع الشراء والعمل قد جعل من قليل من التخمين كافياً لفتح الباب الموصد، أما أجهزة تخزين البيانات غير المحمية، كأصابع اليو أس بي، فهي تفتح المجال أمام نقل المعلومات بسهولة، بينما أدى تقارب التقنيات المختلفة إلى مضاعفة التهديدات وجعل من أنظمة الحماية لا تقوم بمهمتها على الوجه المطلوب.
- **البوتنت:** أصبحت شبكات البوتنت وهي شبكات آلية متصلة بشكل غير شرعي ويتم التحكم بها عن بُعد، هي الأسلوب المفضل للصوص الإنترنت من أجل تنفيذ هجماتهم، هنالك على الأقل 12 مليون كمبيوتر على مستوى العالم قد تم تسخيرها لهذه الأغراض، وتستخدم في تنفيذ عمليات إرسال رسائل صيد المعلومات،

والرسائل غير المرغوب فيها، ونشر المواد الإباحية، وسرقة كلمات السر والهويات.

- **المستقبل:** لقد ركز التقرير على التهديدات التي من المتوقع أن تشهد أوسع قد رمن الانتشار خلال السنة القادمة، لقد جعلت الهواتف الذكية والهواتف متعددة الاستخدامات من الكمبيوترات المحمولة واحدة من أساسيات الحياة العصرية ومن المتوقع أن تتزايد جهود مجرمي الشبكة العالمية لاستخلاص المعلومات الثمينة منها خلال الأشهر المقبلة، أما الانتشار المتواصل لتقنيات البلوتوث والاتصالات الهاتفية عبر بروتوكول الإنترنت فسوف يؤدي إلى ظاهرة جديدة من التسلل إلى الشبكات الهاتفية[1].

إن التدخل التشريعي الوطني في دولة الكويت والدولي مطلوب بقوة في هذه المرحلة بشكل أكبر من أي وقت مضى في ظل سرعة إتلاف الدليل وطبيعة ما يثبت الجريمة ذاتها من الأدلة، وفي ظل الحاجة للتدخل السريع لضبط متعلقات الجريمة، وفي ظل ارتباط مادة الجريمة أو وسيلتها بأنظمة أطراف أخرى لا صلة لهم بها أو بشبكات ونظم معلومات خارج الحدود، فإن المكافحة الفاعلة قد تنطوي على إهدار لحقوق وحريات الكثيرين والتفريط بضمانات المتهم وما توجبه قرينة البراءة المقررة له، وهذا التناقض لا مجال لفضه إلا بإقامة معيار تعكسه القواعد التشريعية، فالاستثناء على الحرية والقيد المقرر عليها يعدو مقبولاً في ضوء اعتبارات مصلحة المجتمع وأمنه متى ما توفر بحق هذا المبرر ومتى ما كان المعيار مدركاً أن الاستثناء لا يجوز التوسع فيه، ويتعين تقييده بالقيد التشريعي الواضح الذي لا يتيح

---

[1] انظر الموقع الآتي: www.alkhaleei.ae.

للسلطات استخدامه عبثاً بما منحها القانون من حقوق أو بما تفسره هي وفق رؤيتها لما قرره القانون لها من صلاحيات[1].

فالتفتيش بصورته التقليدية يتطلب مذكرة قضائية، أما في حالة اتصل ذلك بجريمة تتم عبر الإنترنت، فلا بدّ أن تشمل المذكرة القضائية ما مفاده جواز تفتيش أنظمة الكمبيوتر والقواعد التي ترعى التعامل عبر الإنترنت، وأما إجراء التفتيش دون مذكرة قضائية أو الحصول على بيانات من جهات ليست محلاً للاشتباه لتعلقها بالمشتبه به، فإنها مسائل تثير الكثير من المعارضة خاصة في ظل ما تقرر من قواعد تحمي الخصوصية وتحمي حقوق الأفراد، وتوجب مشروعية الدليل وسلامة مصدره، أو تبطل كل إجراء يتم خلافاً للقواعد الأصولية المتعلقة بالتفتيش والضبط المنصوص عليها في القانون، لذلك يجب أن يتضمن إذن التفتيش الإجازة بالبحث عن كيان البرنامج وأنظمة تشغيله والسجلات التي تثبت استخدام الأنظمة الآلية لمعالجة البيانات والسجلات المستخدمة في عملية الولوج في النظام الآلي لمعالجة البيانات[2].

تعتبر هذه المسائل محور قصور يحاول أن ينفذ من خلالها الجناة عند عدم إجازة القانون هذا المسلك الاستثنائي وعلى نحو يجعل من الضرورة بمكان التمسك بضرورة عدم اللجوء إلى هذا السلوك لأن المشروعية الإجرائية توجب تحقيق أقصى ضمانات للمتهم تتفق ومقتضيات قرينة البراءة، لذلك نجد أنه ونظراً لحداثة تلك الجرائم ولتنوعها وللطابع التقني

---

(1) العنزي، سليمان، مرجع سابق، ص158.

(2) عوض، محمد محيي الدين، مرجع سابق، ص146.

الذي يستخدم في ارتكابها، تواجه السلطة القضائية والأجهزة الأمنية صعوبات عديدة في اكتشاف وملاحقة مرتكبيها[1].

هذا ولا يمكن إلزام أية جهة بتقديم أية بيانات بشأن الخدمات المقدمة للزبائن أو علاقتهم به، لأن هذه البيانات في الأصل سرية ولا يجوز إفشاؤها إلا وفق القانون، فإن الحاجة ماسة للتدخل التشريعي في دولة الكويت لإتاحة آلية الضبط المستعجل للنظم المشتبه بها مع أمر كف يد المشتبه به عن استخدام النظام فوراً بمجرد البدء بإجراءات التفتيش، إضافة إلى الحق في ضبط الأجهزة لإجراء التفتيش عليها في مقار التحقيق باستخدام التقنيات التي تتيح ذلك والتي قد لا تتوفر في مكان التفتيش، خاصة إذا ما علمنا أن تفتيش جزء صغير جداً من الذاكرة قد يحتاج ساعات، فكيف هو الحال وقد أصبحت ذاكرات الكمبيوترات قادرة على تخزين ملايين الملفات، إضافة إلى أن التفتيش الأولي قد لا يحل مشكلة الملفات المخبأة أو المحمية أو المشفرة، وندعو المشرّع الكويتي للسير على هدي المشرّع الأردني بهذا الخصوص في قانون جرائم أنظمة المعلومات.

لكن هذه الحلول العملية في نطاق التفتيش تناقض القواعد المقررة قانوناً في حقل ضمانات المتهم وضمانات احترام حقوق الإنسان والحريات الفردية وفي مقدمتها الخصوصية، فمثل هذه الإجراءات قد تؤدي إلى كشف بيانات شخصية أو كشف أسرار العمل أو الوصول إلى ملفات يحرص أصحابها على سريتها أو يتيح لهم القانون ذلك، وتعدو المسألة أكثر خطورة عندما يمتد التفتيش إلى نظم مرتبطة بالنظام موضوع الاشتباه، فتطال ملفات وبيانات جهات لا علاقة لها بالجريمة قد تكون خاضعة لسرية مهنية أو قواعد حماية سرية بيانات

---

[1] عبد الله، عبد الله عبد الكريم، مرجع سابق، ص59.

العملاء كما في حالة نظم الكمبيوتر الخاصة بمزودي الخدمات أو نظم كمبيوترات البنوك أو كمبيوترات مزودي خدمات الإنترنت أو الشركات التي تتعاطى البيع عبر الإنترنت[1].

هذا ويرى الباحث أن الوقاية من إشكاليات الجرائم الإلكترونية خير من العلاج، لذلك أرى من الأفضل لمستخدمي الوسائل الإلكترونية بمختلف أشكالها وصورها أن يحصنوا أجهزتهم وبياناتهم ضد هذه الجرائم، وأقترح عدة طرق في ذلك ومنها:

أولاً: منع المطاردة في الإنترنت: ويقصد بذلك الامتناع عن كشف المعلومات الشخصية للغرباء مثل رقم الهوية، رقم الضمان الاجتماعي، رقم الحساب البنكي، ورقمه السري.

ثانياً: يجب على المستخدم أن يتجنب إرسال أي صور خاصة لا سيما للغرباء لتجنب حوادث سوء استخدام هذه الصور.

ثالثاً: تحميل واستخدام أحدث البرامج المضادة للفيروسات وتحديثها باستمرار تحسباً للهجمات الفيروسية.

رابعاً: الاحتفاظ بنسخ احتياطية للبيانات الموجودة في جهاز المستخدم في وحدات تخزين خارجية، حيث تحفظه من فقدان هذه البيانات نتيجة التعرض لهجوم إلكتروني.

خامساً: الامتناع عن إرسال رقم بطاقة الائتمان الخاصة على أي موقع غير مضمون لحمايتها من عمليات الاحتيال.

سادساً: مراقبة الأطفال عند استخدامهم شبكة الإنترنت والمواقع التي يتصفحونها، وذلك لمنع أي نوع من المضايقات والتحرشات.

سابعاً: ينبغي على أصحاب المواقع مراقبة مواقعهم باستمرار والتحقق من أي مخالفات، وتثبيت برامج تكشف الحركات غير الطبيعية والمشبوهة.

---

[1] عبد الله، عبد الله عبد الكريم، مرجع سابق، ص60.

الفصل الخامس

الخاتمة والنتائج والتوصيات

أولاً: الخاتمة:

لقد حاولت من خلال هذه الدراسة أن أعالج موضوعاً ذو أهمية على الصعيدين التشريعي والعملي، فقد عرضت في هذه الدراسة من خلال الفصل الثاني لمفهوم الجريمة الإلكترونية من خلال تعريفها وبيان خصائصها وطبيعتها القانونية، ثم المقصود بمحل الجريمة وأطرافها وآليات تنفيذها، بعد ذلك تعرضت في الفصل الثالث لدراسة المشكلات الموضوعية والإجرائية المتعلقة بالجريمة الإلكترونية، وقد استعرضت صور هذه الجريمة والمشكلات التي تثيرها وأوردت تطبيقات قضائية في مجال الجرائم الإلكترونية مع بيان موقف بعض التشريعات المقارنة من هذه المسألة.

أما الفصل الرابع فقد عرضت فيه الحلول التشريعية والعملية لمواجهة مشكلات الجريمة الإلكترونية، وقد بينت موقف بعض التشريعات المقارنة من هذه المسألة وما يجب أن تتضمنه من قواعد موضوعية وإجرائية للحد من مشكلات الجريمة الإلكترونية، وكذلك بينت الإطار الدولي والإقليمي في مجال مكافحة هذه المشكلات، كما عرضت للتجربة المصرية والأردنية في مجال مكافحة الجرائم الإلكترونية، ومن ثم بينت بعض الحلول العملية لمواجهة مشكلات الجريمة الإلكترونية وذلك فيما يتعلق ببعض الإجراءات المتطلبة في هذا المجال، وكذلك فيما يتعلق بضبط وتفتيش آليات تنفيذها.

ثانياً: النتائج:

1. إن الجرائم الإلكترونية هي من الجرائم التي تمس بالاقتصاد الوطني والدولي، كما أنها تمس منظومة الأخلاق في المجتمع.

2. تأخذ الجرائم الإلكترونية صوراً متعددة، وكل صورة من هذه الصور تثير مشكلات موضوعية وإجرائية.
3. تصدى المشرّع الأردني لمعالجة الجرائم الإلكترونية بموجب قانون خاص هو قانون المعاملات الالكترونية لسنة 2001، بخلاف المشرّع الكويتي الذي لم يواكب التطور التشريعي في هذا الشأن.
4. إن هناك حلولاً تشريعية وعملية يمكن من خلالها مواجهة تحديات ومشكلات الجريمة الإلكترونية.
5. تبين عجز النصوص التقليدية في التشريع الجزائي الكويتي عند مواجهة الجرائم الإلكترونية، وتعدّ قاصرة عن مواجهة هذه الجرائم المرتكبة بواسطة الحاسوب والإنترنت، لأن القواعد القانونية التقليدية في التشريع الجزائي الكويتي وضعت لحماية الأموال ذات الطبيعة المادية الملموسة التي لها كيان خارجي، وهذا يتعذر معه حماية الأموال غير المادية المتولدة عن المعلوماتية والجرائم الإلكترونية المرتبطة بها.
6. إن تضارب الجهود الوطنية والدولية في مواجهة تحديات ومشكلات الجرائم الإلكترونية يؤدي إلى جعل مكافحة هذه الجرائم هباءً منثوراً، لأن هناك قلة معرفة وخبرة لمواجهة هذا النوع من الجرائم.

ثالثاً: التوصيات:

انطلاقاً من الأهمية البالغة لهذا الموضوع، فإنني أتقدم بالتوصيات الآتية:

1. نوصي بضرورة تدخل المشرّع الكويتي لإصدار قانون خاص بالجريمة الإلكترونية، وفي هذا المجال أدعوه للاستفادة من التجربة التشريعية العربية، وبخاصة الأردنية في ضوء قانون جرائم أنظمة المعلومات لسنة 2010م، بحيث يحدد بشكل واضح ودقيق صور

الجرائم الإلكترونية والعقوبات المقررة لها، ومن الممكن عدم إصدار قانون جديد بهذا الخصوص، ولكن ندعو المشرّع الكويتي في مثل هذه الحالة، أن يتم تعديل قانون الجزاء بحيث يدرج قسم خاص بالجرائم الإلكترونية حتى يستجيب التشريع الكويتي للتطورات في مجال مكافحة هذا النوع من الجرائم.

2. أوصي بضرورة أن يتخلى المشرّعان الأردني والكويتي عن المفهوم التقليدي للمال بحيث يتبينا مفهوماً أوسع ليشمل المعلومات والبيانات، وهذا يتطلب تدخل تشريعي لهذه الغاية، لأن المال المعلوماتي المعنوي غير قابل للاستحواذ ولا يعد مالاً، ومن ثم غير قابل للسرقة، وهذا سيؤدي إلى تجريده من الحماية الجزائية ويفتح المجال واسعاً أمام مرتكبي الجرائم الإلكترونية وقراصنة البرامج والمعلومات.
3. أوصي المشرّع الكويتي بأن يعدّل قانون الإجراءات الجنائية بحيث يستوعب إجراءات التحري والملاحقة والتحقيق والاستدلال والضبط الإلكتروني والتفتيش الإلكتروني ووسائله وإجراء المعاينة والخبرة؛ لأن القواعد التقليدية الحالية لا تتلاءم وطبيعة الجرائم الإلكترونية.
4. أوصي المشرّع الأردني بتجريم ممارسات تشكل جرائم إلكترونية لم ينص عليها في قانون جرائم أنظمة المعلومات، ومنها: المضايقة، والملاحقة الإلكترونية، والتشهير، وتشويه السمعة سواء في غرف الدردشة أو مواقع التواصل الاجتماعي وبخاصة "تويتر" و "الواتسب" أو من خلال البريد الإلكتروني، وكذلك الاحتيال الإلكتروني.
5. ضرورة نشر الوعي بين الأشخاص سواء طبيعيين أو معنويين بمخاطر التعامل مع المواقع السيئة والمشبوهة على الشبكات الإلكترونية.

6. ضرورة تبني الدولة في الأردن والكويت فكرة إنشاء جهاز خاص بالخبرة الجنائية للجرائم الإلكترونية، لأن البحث داخل النظام الإلكتروني معقد يسهل فيه محو الأدلة.
7. أوصي الجهات ذات العلاقة في الأردن والكويت بضرورة تدريب أفراد الضابطة العدلية والنيابة العامة والقضاة وتأهيلهم على كيفية التعامل مع الجرائم الإلكترونية وآليات جمع الأدلة والتفتيش والتحري والملاحقة والتحقيق والاستدلال.

المراجع

أولاً: الكتب القانونية:

إبراهيم، خالد ممدوح (2009). **الجرائم المعلوماتية**، دار الفكر الجامعي، الإسكندرية، ط1.

الألفي، محمد (2005). **المسؤولية الجنائية عن الجرائم الأخلاقية عبر الإنترنت**، المكتب المصري الحديث، القاهرة.

بشري، محمد الأمين (2009). **التحقيق في جرائم الحاسب الآلي**، دار الكتب القانونية، مصر.

تمام، أحمد (2009). **الحماية الجنائية للحاسب الآلي**، دار النهضة العربية، القاهرة.

الجبور، محمد (2010). **الوسيط في قانون العقوبات – القسم العام**، دار وائل، عمان، ط1.

الجنبيهي، منير محمد والجنبيهي، ممدوح محمد (2005). **بروتوكولات وقوانين الإنترنت**، دار الفكر الجامعي، الإسكندرية، ط1.

الجنبيهي، منير محمد والجنبيهي، ممدوح محمد (2006). **جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها**، دار الفكر الجامعي، الإسكندرية، ط1.

حجازي، عبد الفتاح بيومي (دون سنة نشر). **جرائم الكمبيوتر والإنترنت**، دار الكتب القانونية، مصر.

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

حجازي، عبد الفتاح بيومي (2007). **الأحداث والإنترنت**، دار الكتب القانونية، مصر، ط1.

حجازي، عبد الفتاح بيومي (2007). **صراع الكمبيوتر والإنترنت**، دار الكتب القانونية، مصر، ط1.

حجازي، عبد الفتاح بيومي (2008). **التزوير في جرائم الكمبيوتر والإنترنت**، دار الكتب القانونية، مصر، ط1.

حسن، سعيد عبد اللطيف (1999). **إثبات جرائم الكمبيوتر والجرائم المرتبكة عبر الإنترنت**، دار النهضة العربية، القاهرة.

حسني، محمود نجيب (1971). **النظرية العامة للقصد الجنائي**، دار النهضة العربية، ط2.

حسني، محمود نجيب (1972). **شرح قانون العقوبات – القسم الخاص**، دار النهضة العربية، القاهرة.

خوالدة، محمد سليمان (2012). **جريمة الدخول غير المشروع إلى موقع إلكتروني أو نظام معلومات وفق التشريع الأردني – دراسة مقارنة**، دار الثقافة، عمان، ط1.

دسوقي، محمد (2003). **الحماية الجنائية لسرية المعلومات**، دار الكتب القانونية، مصر.

رستم، هشام محمد (1999). **جرائم الحاسب المستحدثة**، دار الكتب القانونية، مصر، ط1.

رمضان، مدحت (2007). **جرائم الاعتداء على الأشخاص والإنترنت**، دار النهضة

العربية، القاهرة.

رومي، محمد أمين (2003). **جرائم الكمبيوتر والإنترنت**، دار المطبوعات الجامعية، الإسكندرية، ط1.

زيدي، وليد (2009). **القرصنة على الإنترنت والحاسوب**، دار أسامة للنشر، عمان، ط3.

سعيد، كامل (2002). **جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات**، عمان.

سلامة، محمد عبد الله (2007). **موسوعة جرائم المعلوماتية**، المكتب العربي الحديث، الإسكندرية.

شقير، رامي سليمان (2005). **سريان القانون الجنائي من حيث المكان**، دار الإسراء، عمان، ط1.

شوا، محمد سامي (1994). **ثورة المعلومات وانعكاساتها على قانون العقوبات**، دار النهضة العربية، القاهرة.

شوابكة، محمد (2004). **جرائم الحاسوب والإنترنت**، دار الثقافة، عمان، ط1.

صغير، جميل عبد الباقي (2010). **الجرائم الناشئة عن استخدام الحاسب الآلي**، دار النهضة العربية، القاهرة.

عبابنة، محمود أحمد (2005). **جرائم الحاسوب وأبعادها الدولية**، دار الثقافة، عمان، ط1.

عبد الإله، أحمد هلالي (2003). **الجوانب الموضوعية والإجرائية لجرائم المعلوماتية**، دار النهضة العربية، القاهرة، ط1.

عبد الله، عبد الله عبد الكريم (2011). **جرائم المعلوماتية والإنترنت – الجرائم الإلكترونية**، منشورات الحلبي الحقوقية، بيروت، ط1.

عريان، محمد علي (2009). **الجرائم المعلوماتية**، دار الجامعة الجديدة، الإسكندرية، ط2.

عفيفي، كامل عفيفي (2010). **جرائم الكمبيوتر**، دار النهضة العربية، القاهرة.

عوض، محمد محيي الدين (2011). **مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات**، دار الفكر العربي، القاهرة.

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

قهوجي، علي (1999). **الحماية الجنائية لبرامج الحاسب الآلي**، الدار الجامعية، الإسكندرية.

قورة، نائلة عادل (2010). **جرائم الحاسب الآلي الاقتصادية**، منشورات الحلبي، بيروت، ط1.

كايد، أسامة عبد الله (1999). **الحماية الجنائية للحياة الخاصة وبنوك المعلومات**، دار النهضة العربية، القاهرة.

مرصفاوي، حسن صادق (1991). **قانون العقوبات الخاص**، منشأة المعارف، الإسكندرية.

مصطفى، معوان (2009). **مكافحة الجريمة المعلوماتية – قواعد الإثبات**، دار الكتاب الحديث، القاهرة، ط1.

ملط، أحمد خليفة (2006). **الجرائم المعلوماتية**، دار الفكر الجامعي، الإسكندرية، ط1.

مناعسة وآخرون (2001). **جرائم الحاسوب والإنترنت**، دار وائل، عمان، ط1.

منصور، محمد حسين (2010). **المسؤولية الإلكترونية**، دار المعارف، الإسكندرية، ط2.

موسى، مصطفى محمد (2005). **دليل التحري عبر شبكة الإنترنت**، دار الكتب القانونية، مصر.

هيتي، محمد حماد مرهج (2004). **التكنولوجيا الحديثة والقانون الجنائي**، دار الثقافة، عمان، ط1.

ثانياً: الرسائل والأبحاث والمقالات:

الحسيني، محمد (2013). **مقال بعنوان: "مختصون يطالبون بتشريع خاص للجرائم الإلكترونية في الكويت"**، منشور في جريدة "هنا الكويت"، الصادرة في 12 فبراير.

حميد، عبد الله قاسم (2010). **الحماية الجنائية للمعلومات الإلكترونية**، رسالة ماجستير، جامعة عين شمس.

الرواشدة، سامي والهياجنة، أحمد (2009). **مكافحة الجريمة المعلوماتية بالتحريم والعقاب**، بحث منشور في المجلة الأردنية في القانون والعلوم السياسية، جامعة مؤتة، الأردن، المجلد الأول، العدد الثالث.

الشوا، محمد سامي (1993). **الغش المعلوماتي**، بحث في مؤتمر الجمعية المصرية للقانون الجنائي، القاهرة (25 – 28 أكتوبر).

العنزي، سليمان بن مهجع (2003). **وسائل التحقيق في جرائم نظم المعلومات**، رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية، السعودية.

الفيل، علي عدنان (2012). **جريمة الاحتيال عبر البريد الإلكتروني**، مجلة الحقوق، الكويت، العدد الثاني، السنة 36.

القطاونة، مصعب (2010). **الإجراءات الجزائية الخاصة في الجرائم المعلوماتية**، بحث مقدّم لشبكة قانوني الأردن.

القهوجي، علي عبد القادر (2000). **الحماية الجنائية للبيانات المخزنة إلكترونياً**، بحث مقدّم إلى مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة (1 – 3 يوليو).

المطردي، مفتاح بو بكر (2012). **الجريمة الإلكترونية**، ورقة عمل مقدّمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، السودان (23 – 25 أيلول).

المعاشي، سميرة (2011). **ماهية الجريمة المعلوماتية**، بحث منشور في مجلة المنتدى القانوني، العدد السابع، جامعة محمد خيضر بسكرة – الجزائر.

الكندري، عبد الله (2013). مقال بعنوان "الجرائم الإلكترونية في التشريع الكويتي"، جريدة الأنباء الكويتية، العدد الصادر يوم الإثنين الموافق 22 يوليو 2013م.

ثالثاً: التشريعات الأردنية والكويتية:

أ- التشريعات الأردنية:

قانون العقوبات رقم (16) لسنة 1960م وتعديلاته.

قانون أصول المحاكمات الجزائية رقم (19) لسنة 1961م وتعديلاته.

القانون المدني رقم (43) لسنة 1976م.

قانون المعاملات الإلكترونية رقم (85) لسنة 2001م.

قانون جرائم أنظمة المعلومات المؤقت رقم (30) لسنة 2010م.

ب- التشريعات الكويتية:

قانون الجزاء رقم (16) لسنة 1960م وتعديلاته.

قانون الإجراءات والمحاكمات الجزائية رقم (17) لسنة 1960م وتعديلاته.

قانون الشركات الجديد رقم (25) لسنة 2012م.

مرسوم بقانون خاص بتنظيم الأوراق المالية رقم (7) لسنة 2010م.