جامعة الشرقية
A' SHARQIYAH UNIVERSITY

المواجهة الجزائية للجرائم السيبرانية في القانون العُماني

"دراسة وصفية تحليلية"

خليل بن ناصر بن مسلم الرقادي

رسالة مقدمة لاستكمال متطلبات الحصول على درجة
الماجستير في القانون الجزائي

قسم القانون العام
كلية الحقوق
جامعة الشرقية
سلطنة عُمان

٢٠٢٤م / ١٤٤٥هـ

الإشراف على الرسالة

المواجهة الجزائية للجرائم السيبرانية في القانون العُماني

"دراسة وصفية تحليلية"

رسالة مقدمة لاستكمال متطلبات الحصول على درجة

الماجستير في القانون الجزائي

إعـــــداد

خليل بن ناصر بن مسلم الرقادي

إشـــــراف

الدكتور/ نــزار حمــدي قشطــة

٢٠٢٤م / ١٤٤٥هـ

لجنة مناقشة الرسالة

" المواجهة الجزائية للجرائم السيبرانية في القانون العماني

"دراسة وصفية تحليلية"

أعدها الباحث:

خليل بن ناصر الرقادي

نوقشت هذه الرسالة وأجيزت بتاريخ 7 من ربيع الأول 1446هـ، الموافق 10 من سبتمبر 2024م،

المشرف

د. نزار حمدي قشطة

أعضاء لجنة المناقشة

م	صفته في اللجنة	الاسم	الرتبة الأكاديمية	التخصص	الكلية/ المؤسسة	التوقيع
1	رئيس اللجنة	د. نزار حمدي قشطة	أستاذ مشارك	القانون الجزائي	جامعة الشرقية	
2	المناقش الداخلي	د. أحمد بن صالح البرواني	أستاذ مساعد	القانون الجزائي	جامعة الشرقية	
3	المناقش الخارجي	د. أحمد حسنية	أستاذ مشارك	القانون الجزائي	جامعة ظفار	

بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ

قَالَ تَعَالَىٰ:

﴿ ۞ يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ كُونُواْ قَوَّٰمِينَ بِٱلْقِسْطِ شُهَدَآءَ لِلَّهِ وَلَوْ عَلَىٰٓ أَنفُسِكُمْ أَوِ ٱلْوَٰلِدَيْنِ وَٱلْأَقْرَبِينَ ۚ إِن يَكُنْ غَنِيًّا أَوْ فَقِيرًا فَٱللَّهُ أَوْلَىٰ بِهِمَا ۖ فَلَا تَتَّبِعُواْ ٱلْهَوَىٰٓ أَن تَعْدِلُواْ ۚ وَإِن تَلْوُۥٓاْ أَوْ تُعْرِضُواْ فَإِنَّ ٱللَّهَ كَانَ بِمَا تَعْمَلُونَ خَبِيرًا ﴿١٣٥﴾ ﴾

صَدَقَ اللهُ العَظِيمُ

سورة النساء: ١٣٥

إقــرار الباحث

أقر بأن المادة العلمية الواردة في هذه الرســـالة قد حُدِدَ مصـــدرها العلمي وأن محتوى الرســـالة غير مقدم للحصـــول على أي درجة علمية أخرى، وأن مضـــمون هذه الرسالة يعكس آراء الباحث الخاصة وهي ليست بالضرورة الآراء التي تتبناها الجهة المانحة.

الباحث: خليل بن ناصر بن مسلم الرقادي التوقيع: خليل الرقادي

إهداء

إلى من كانوا سندي وعوني في هذه الحياة...

إلى والديّ الأعزاء، الذين لم يدخروا جهدًا في دعمي...

إلى أسرتي الكريمة، التي تحملتني بكل حب وصبر...

إلى كل من ساهم في إكمال هذا العمل...

أهدي هذه الرسالة تعبيرًا عن امتناني واعتزازي بكم.

الباحث

اعترافًا بالفضل والشكر لأهله، أسجل خالص شكري وامتناني وتقديري **للدكتور/ نزارقشـــطة**، لتفضـــله بقبول الإشـــراف على هذه الرســـالة، الذي لم يكن مجرد مشـــرف أكاديمي، بل كان بوصلةً في بحر المعرفة، شكرًا على صبرك، ورؤيتك وتوجيهاتك التي أضاءت لي الطريق.

كما أود أن أشـــكر جميع أســـاتذتي في كلية الحقوق بجامعة الشـــرقية، الذين كانوا مصدر إلهام ودعم لي طوال فترة الدراسة.

وختامًا، أقدم شـــكري وامتناني لأســـرتي وأصـــدقائي، الذين ســـاندوني في إنجاز هذه الدراسة.

الباحث

قائمة المحتويات

المواجهة الجزائية للجرائم السيبرانية في القانون العُماني "دراسة وصفية تحليلية"

إعـداد: خليل بن ناصر بن مسلم الرقادي

إشــراف

الدكتور/ نـزار حمـدي قشطـة

الملخص:

تواجه ســـلطات إنفاذ القانون حول العالم بما فيها الســـلطنة تحديًا متزايدًا في مواجهة الجرائم الســيبرانية، التي تتميز بتطورها الســريع وتعقيدها المســتمر، مما يتطلب معها الاســتجابة القانونية الفعالة لمواكبة هذا التطور، ومكافحة الجرائم الناشـــئة عنها، ومن هنا تبرز أهمية هذه الدراســـة والحاجة لتطوير الإطار القانوني العُماني لمواجهة الجرائم السيبرانية بفعالية، في ظل الزيادة المستمرة في استخدام التكنولوجيا الرقمية والإنترنت، وسد الفجوات القانونية القائمة، وتقديم توصيات عملية للتصدي لهذه الجرائم.

سعت الدراسة إلى تحليل النصوص الجزائية المتعلقة بالجرائم السيبرانية في السلطنة وتقييم مدى كفايتها في التصــدي لهذه الجرائم، وقد ركزت الإشـكالية الرئيسـية على مدى قدرة التشـريع العُماني على مواكبة التطورات الســريعة في الجرائم الســيبرانية، بالإضـــافة إلى التحديات الموضـــوعية والإجرائية التي صـــاحبت هذا التطور، وأوجه القصـــور القائمة في النصـــوص القانونية، وتقديم مجموعة من التوصـــيات لتعزيز فعاليتها وتحسين قدرتها على التصدي لهذه الجرائم بشكل أكثر فاعلية.

اعتمدت الدراســة على المنهج الوصــفي التحليلي، عبر تحليل النصــوص والقواعد القانونية العُمانية ذات الصـــلة، وخلصـــت إلى أن التشـــريعات الجزائية العُمانية بحاجة إلى تحديث شـــامل وتكامل بين القوانين المختلفة لتوفير حماية قانونية شاملة وفعالة ضد الجرائم السيبرانية، وأوصت بضـــرورة إصـــدار قانون جزائي متكامل خاص بمواجهة الجرائم الســـيبرانية، مع الأخذ في الاعتبار الاســـتفادة من التجارب الدولية الناجحة في هذا المجال، وضـــمان توفير آليات قانونية واضـــحة وسريعة للتعامل مع هذه الجرائم.

الكلمات المفتاحية: الجرائم السيبرانية، المواجهة الجزائية، القانون العُماني، تقنية المعلومات، الأدلة الرقمية.

Penal Response to Cybercrimes in Omani Law: A Descriptive and Analytical Study

Prepared by: Khalil bin Nasser bin Muslim al-Ruqadi

Supervised by: Dr. Nizar Hamdi Qishta

Abstract:

Law enforcement authorities around the world, including in Oman, face increasing challenges in addressing cybercrimes, which are characterized by their rapid evolution and ongoing complexity. This necessitates an effective legal response to keep pace with these developments and combat the emerging crimes. Thus, the importance of this study and the need to develop the Omani legal framework to address cybercrimes effectively becomes evident, especially given the continuous rise in the use of digital technology and the internet, and the need to close existing legal gaps.

The study aimed to analyze the criminal texts related to cybercrimes in Oman and assess their adequacy in addressing these crimes. The main issue focused on the extent to which Omani legislation can keep up with the rapid advancements in cybercrimes, the associated objective and procedural challenges, and the existing shortcomings in legal texts, offering recommendations to enhance effectiveness and improve the ability to combat these crimes more effectively.

The study relied on a descriptive-analytical approach, analyzing relevant Omani legal texts and rules, and concluded that Omani criminal legislation requires comprehensive updating and better integration among various laws to provide comprehensive and effective legal protection against cybercrimes. It recommended enacting a comprehensive criminal law specifically for cybercrimes, taking into account successful international experiences and ensuring clear and rapid legal mechanisms to handle these crimes.

Keywords: Cybercrimes, penal response, Omani law, information technology, digital evidence.

المقدمـــــة

يســـعى الإنســـان إلى تحقيق الاســـتفادة المثلى من التكنولوجيا مع ضـــمان أمانها وســـلامة استخدامها واستثمارها بشكل آمن لتحقيق الفوائد بكل يسر وأمان وتكاملها في خدمة الرفاهية العامة، لذلك فإن تعزيز الأمان الإلكتروني أصـبح ضـرورة حيوية لأمن الإنسـان واسـتقراره، والحد من مخاطر التقنية والتحكم في ســـلبياتها، وتحرير الفرد من مخاوفه المتعلقة بالأمان الرقمي، حيثُ ظهرت الجرائم السـيبرانية كنتيجة طبيعية لتطور الاتصـالات والتكنولوجيا وانتشـارها الواسـع، والتي تتميز بأسـلوبها الحديث والمبتكر، وباتت وتشـــكل تهديدًا كونها تتجاوز الإطار الزمني والحدود الإقليمية وتعتمد على عوامل افتراضية معقدة يصعب التنبؤ بأبعادها وخفاياها ومصادرها[1].

لا يخفى على أحد المكانـة التي تحتلهـا تكنولوجيـا المعلومـات ومـدى ارتبـاط الأشـــخـاص والمؤســـســـات العامة بتقنية المعلومات والانترنت في تنظيم كافة المصـــالح وأوجدت عوالم افتراضـــية تختلف في طبيعتها عن العالم المادي الذي نعيشـه، وتحولت طرق التفاعل فيه على كافة المسـتويات بما فيها الجريمة التي أصـبحت ترتكب على ذلك العالم الافتراضـي، مما يحتم عند دراسـة أي جريمة وخاصـــة المســـتحدثة منها اســـتقراء مدى انتشـــارها وأنواعها وطرق ارتكابها بما يمكن الســـلطات من مواجهتها ووضع التدابير المناسبة لذلك.

تعتبر الجرائم الســـيبرانية أحد التحديات الحديثة التي تواجه المجتمعات، لكثرة اعتماد أنشـــطة الإنســـان على التكنولوجيا الرقمية وشـــبكة الإنترنت، مما يجعل هذه الجرائم تشـــكل تهديدًا للأفراد والمؤســـســـات والدول، وتشـــمل مختلف الأنشـــطة غير القانونية التي تســـتهدف الأنظمة الإلكترونية والبيانات، وانتهاك الحقوق والحريات العامة، بالإضـــافة إلى الخســـائر المالية الكبيرة التي قد تنشـــأ عن هذه الجرائم، مما يتطلب تحديث وتطوير التشريعات الجزائية لمواكبة هذا التطور التكنولوجي.

---

[1] محمد مســعد حميد، رؤية إســتراتيجية لمكافحة الجرائم الســيبرانية: اليمن دراســة حالة، المجلة العربية الدولية للمعلوماتية، اتحاد الجامعات العربية، جمعية كليات الحاسبات والمعلومات، المجلد ٧، العدد ١٢، ٢٠١٩، ص٨٤.

تشهد الجرائم السيبرانية تفاوتًا في أشكالها وتنوعها، مما يستدعي تسليط الضوء على طبيعتها وتفاصيلها وتحديد الأحكام القانونية المتعلقة بها، لذلك سعت الدول المعاصرة بما فيها السلطنة إلى مكافحة هذه الجرائم من خلال إصدار قوانين جزائية تتناسب مع طبيعتها التقنية، وتطوير استراتيجيات فعّالة للتصدي لها وتحقيق الأمان الشامل وحماية المجتمع والأفراد من تأثيراتها الخطيرة[١].

تتباين النظرة إلى التطور التقني الذي يعيشه عالمنا المعاصر، إلا أن النظرة القانونية تبقى مؤطرة بمبدأ الشرعية الجزائية وهو مبدأ مقدس يحمي الحقوق والحريات العامة من أي انتهاك، والذي يقضي بأنه " لا جريمة ولا عقوبة إلا بمقتضى القانون، وهو ما جاءت به المادة (٢٦) من النظام الأساسي للدولة[٢] التي نصت على أنه: "لا جريمة ولا عقوبة إلا بناء على قانون، ولا عقاب إلا على الأفعال اللاحقة على العمل بالقانون الذي ينص عليها، والعقوبة شخصية".

جاءت الجريمة السيبرانية كنتيجة طبيعية للانتشار الواسع للتقنية ودخول التكنولوجيا في كافة أنشطة الإنسان اليومية، وما تشكله الهجمات السيبرانية من تهديد على مصالح أي دولة سواء كانت اقتصادية أو مالية أو أمنية، وانتهاك صريح لحياة الأفراد الخاصة، فضلًا عن التحديات الناتجة عن ارتكاب هذه الجرائم لدى جهات الضبطية القضائية، والسلطة القضائية في الحصول على الأدلة وصعوبة الإثبات بالوسائل التقليدية.

في ظل تزايد وتيرة الهجمات السيبرانية على الفضاء الافتراضي العُماني، والذي يأتي كنتيجة طبيعية للانتشار الواسع لاستخدام التكنولوجيا والتقنية[٣]، فإن الدراسة سوف تسعى إلى بيان ماهية الجريمة السيبرانية ومدى كفاية التشريع العُماني في التصدي لها، والتحديات والصعوبات التي تواجه السلطات في ملاحقة مرتكبيها.

---

[١] عبد العزيز بن فهد بن محمد ابن داود، الجرائم السيبرانية: دراسة تأصيلية مقارنة، مجلة الاجتهاد للدراسات القانونية والاقتصادية، معهد الحقوق والعلوم السياسية، المجلد ٩، العدد ٣، الجزائر، ٢٠٢٠، ص١٤٦.

[٢] النظام الأساسي للدولة الصادر بالمرسوم السلطاني رقم (٢٠٢١/٦)، نشر هذا المرسوم في ملحق عدد الجريدة الرسمية رقم (١٣٧٤) الصادر في ١٢ / ١ / ٢٠٢١م.

[3] Over 400,000 Cyber Attacks Thwarted in Oman in 2020, Newspaper Times of Oman, Publication Date: 13 January 2021.

أهمية الدراسة:

أخذت التطورات الهائلة في تكنولوجيا المعلومات والاتصالات مكانًا بارزًا في عصرنا الحاضر، وأدت إلى تعقيدات جديدة وتحديات في سياق القانون الدولي والقانون الوطني، وتزايدت حاجة المجتمعات إلى التكيف مع هذا التقدم، وتحديد الإطار القانوني الذي يحكم استخدام التكنولوجيا وتأثيرها على الحياة اليومية، الأمر الذي دفع الدول إلى مكافحة الجرائم السيبرانية من خلال إقرار قوانين جزائية تتناسب مع طبيعة هذا النوع من الجرائم، ويتمثل التحدي الرئيسي في تحقيق التوازن بين تطوير التكنولوجيا وحقوق الفرد والمجتمع ، وضمان تبني استخدام آمن وأخلاقي للتكنولوجيا، وذلك من خلال تطوير استراتيجيات فعّالة لمكافحتها، وتحقيق التعاون الدولي وضمان الالتزام بالقوانين والمعايير الدولية(١).

رغم الإيجابيات المصاحبة للتطور التقني المذهل الذي خدم البشرية في شتى المجالات، وما صاحبه من طفرة في سرعة إنجاز المعاملات، إلا أن له تداعيات سلبية ناتجة عن الاستغلال غير المشروع لهذه التقنيات أدت إلى انتشار هذه الممارسات التي أصبحت تؤرق الأفراد والدول والمنظمات، مما حدا بالدول إلى وضع التشريعات الرادعة لمواجهتها، عليه فإن الدراسة تكتسب أهميتها في دراسة وتحليل النصوص الجزائية المواجهة لهذه الجرائم في السلطنة، ومدى كفايتها وفاعليتها في مكافحة الجرائم السيبرانية، وتبرز أهمية الدراسة العلمية في ندرة الدراسات والبحوث العُمانية التي تناولت هذا الجانب، وإثراء البحث العلمي في تقديم دراسة تحليلية شاملة للأحكام المتعلقة بالمواجهة الجزائية للجرائم السيبرانية في القانون العُماني، ويسهم في رفع مستوى الوعي القانوني لدى الأفراد والمجتمع حول هذا النوع من الجرائم.

---

(١) كريم احليحل، الجريمة السيبرانية والجهود الدولية في مواجهتها، المجلة الإلكترونية الدولية لنشر الأبحاث القانونية، المجلد ١، العدد ٣، المغرب، ٢٠٢٣، ص٧.

أهداف الدراسة:

مع تطور التكنولوجيا أصبحت الجرائم السيبرانية مجالًا خصبًا للمجرمين لتحقيق أغراض غير مشروعة، الأمر الذي دفع التشريعات الدولية والإقليمية إلى تنظيم الجرائم السيبرانية، ومن بينها التشريع العُماني، وتهدف هذه الدراسة إلى تحليل الأحكام المتعلقة بالمواجهة الجزائية للجرائم السيبرانية في القانون العُماني، وذلك من خلال تسليط الضوء على العناصر المكونة لهذه الجرائم، وتعريفها وتحديد أنواعها وخصائصها، وبيان جوانبها الموضوعية والإجرائية.

كما أن هناك أهداف عملية تسعى هذه الدراسة إلى تحقيقها من خلال تقديم توصيات ومقترحات عملية لمعالجة المشكلات المتعلقة بالمواجهة الجزائية لهذه الجرائم، وبيان مدى الحاجة إلى مراجعة القوانين المنظمة لها. عليه فإن الدراسة تركز على تحقيق الأهداف الآتية:

١. تحديد مفهوم الجريمة السيبرانية وخصائصها وطبيعتها القانونية وأركانها.
٢. تحليل الأحكام الموضوعية والإجرائية المتعلقة بمواجهة الجرائم السيبرانية في القانون العُماني.
٣. عرض التحديات التي يواجها المشرع العُماني في التصدي لهذه الجرائم، وتقييم فعالية النصوص القانونية في مكافحتها.
٤. تقديم توصيات عملية لتحسين الإطار القانوني لمكافحة الجرائم السيبرانية، ومعالجة الفجوات القانونية القائمة في القوانين العُمانية.

مشكلة الدراسة:

نظرًا للانتشار الواسع للجريمة السيبرانية، والتحديات التي تواجهها السلطات في مواكبة التطور المتسارع للتكنولوجيا الحديثة، وتقدم الوسائل المستخدمة في ارتكاب الجرائم السيبرانية، فإن المشكلة الأساسية للدراسة تتمثل في مدى مواكبة المشرع العُماني للتطور المتسارع للتقنية والتصدي للجرائم الناشئة عنها، التي تتسم بالسرعة والتنوع والتخفي، وتبرز مشكلة الدراسة في الإجابة على التساؤلات الآتية:

١. ماهية الجريمة السيبرانية وخصائصها وطبيعتها القانونية وأركانها؟
٢. مدى استيعاب التشريعات الجزائية العُمانية للجريمة السيبرانية؟
٣. ما هي أبرز الصعوبات والتحديات التي تواجهها السلطات العُمانية في مواجهة هذه الجرائم؟

منهجية الدراسة:

يُعد المنهج الوصـــفي التحليلي من المناهج العلمية التي تعتمد على وصـــف الظواهر والأحداث وتحليلها، وذلك من خلال دراسة البيانات والمعلومات المتعلقة بالموضوع، وتفسيرها واستخلاص النتائج منها.

فيما يتعلق بدراســـة المواجهة الجزائية للجرائم الســـيبرانية في القانون العُماني، فإن اســـتخدام المنهج الوصفي التحليلي من الأساليب المناسبة لدراسة هذا الموضوع، وذلك لما يلي:

- يسمح هذا المنهج بوصف أركان المسؤولية الجزائية للجرائم السيبرانية وتحليلها، وذلك من خلال دراسة النصوص القانونية والقواعد العامة المتعلقة بالموضوع.
- يمكن من خلال هذا المنهج اسـتعراض القانون العُماني والأحكام القضـائية المتعلقة بالموضـوع، بغية الوصول إلى أهداف الدراسة.

الدراسات السابقة:

- **الدراســـة الأولى:** مجمع البحوث والدراســـات، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، أكاديمية السلطان قابوس لعلوم الشرطة، نزوى – سلطنة عُمان، ٢٠١٦.

استعرضـت الدراسـة أنواع الجرائم الإلكترونية، وواقع الجريمة الإلكترونية وحجم الخسـائر في دول مجلس التعاون لدول الخليج العربية، ومدى تأثير برامج التواصل الاجتماعي على مجتمعات هذه الدول.

وقد توصـلت الدراسـة إلى نتائج واقعية ومن أهمها تزايد مخاطر الجريمة الإلكترونية على أمن الأفراد والمؤسسات والمجتمعات، والحاجة إلى استراتيجية موحدة لمكافحة الجريمة الإلكترونية في دول مجلس التعاون، وقدمت مجموعة من التوصـــيات البناءة، ومن أبرزها ضـــرورة تطوير التشـــريعات والقوانين لمكافحة الجريمة الإلكترونية وتغليظ العقوبات على مرتكبيها، والتركيز على التعاون الدولي لمكافحة الجريمة الإلكترونية، ورفع وعي المجتمعات حول الجريمة الإلكترونية ومخاطرها وطرق الوقاية منها، وتعزيز البنية التحتية لتكنولوجيا المعلومات والاتصالات في دول مجلس التعاون.

تختلف الدراسة عن هذه الدراسة في تركيزها على واقع الجريمة الإلكترونية بصورة عامة وحجم الخسـائر التي تسـببها وضـرورة التعاون الدولي لمكافحتها، وتركز الدراسـة على دول مجلس التعاون

الخليجي، بينما تركز هذه الدراسة على المواجهة الجزائية للجرائم السيبرانية في القانون العُماني بصورة خاصة، وتسعى إلى تسليط الضوء على القوانين الوطنية المنظمة لهذه الجريمة.

- **الدراسة الثانية:** عبد الله بن على بن سالم الشبلي، الجريمة الإلكترونية في سلطنة عُمان: التحديات والحلول القانونية، مجلة العلوم الاقتصادية والإدارية والقانونية، المركز القومي للبحوث، غزة، المجلد ٣، العدد ٢، ٢٠١٩.

تناولت الدراسة مفهوم الجريمة الإلكترونية وخصائصها في إطار التشريع العُماني، مع التركيز على الحلول المناسبة لها.

توصلت الدراسة إلى أن التقدم الحضاري في المجتمع العُماني، يقابل التحديات الناشئة من جراء تطور جرائم الإلكترونية، ويقترح عدة توصيات أبرزها أهمية إجراء دراسات ميدانية تحدد أنماط وأنواع الجرائم الإلكترونية، والتي يمكن أن تسهم في تطوير القوانين الحالية، كما يُشدد على ضرورة توعية المجتمع بخطورة هذه الجرائم، وتبني استراتيجيات للوقاية منها، بالإضافة إلى التركيز على الأخلاقيات والتأثيرات الاجتماعية لهذه الجرائم.

تركز الدراسة على الجريمة الإلكترونية بشكل عام والتحديات التي تواجه مكافحة الجريمة الإلكترونية، أما هذه الدراسة فهي أكثر تركيزًا على تناول الأحكام الموضوعية والإجرائية الخاصة بمواجهة الجرائم السيبرانية، والتحديات التي تواجه السلطات المختصة بمكافحتها، وتسعى إلى وضع الحلول القانونية لمكافحة الجريمة السيبرانية.

- **الدراسة الثالثة:** المعمر محمد أحمدي، صور الجريمة السيبرانية في التشريع الموريتاني: قانون الجريمة السيبرانية رقم ٠٠٧ – ٢٠١٦ نموذجا، رسالة مقدمة لنيل مؤهل الماجستير، كلية العلوم القانونية والاقتصادية، جامعة نواكشوط، موريتانيا، ٢٠٢٢م.

استعرضت الدراسة صور الجريمة السيبرانية في التشريع الموريتاني، وتحليل قانون الجريمة السيبرانية، والتحديات التي تواجه مكافحة الجريمة السيبرانية في موريتانيا واقترحت لمواجهتها مجموعة

من التوصـيات، أبرزها إطلاق حملات توعية واسـعة لرفع الوعي بمخاطر الجريمة السـيبرانية، وتأهيل وتدريب الكفاءات المتخصصة، وتخصيص الموارد المالية اللازمة لمكافحتها.

تركز الدراســة على صــور الجريمة الســيبرانية في التشــريع الموريتاني وفقًا لقانون الجريمة السيبرانية الموريتاني، في حين هذه الدراسة تتناول تنظيم الجريمة السيبرانية في القانون العُماني.

خطة الدراسة

تناولت الدراسة فصلين مقسمين إلى أربع مباحث وثمان مطالب على النحو الآتي:

الفصل الأول: التأصيل النظري للجرائم السيبرانية.

المبحث الأول: ماهية الجريمة السيبرانية.

المطلب الأول: مفهوم الجريمة السيبرانية.

المطلب الثاني: أنواع الجرائم السيبرانية.

المبحث الثاني: الطبيعة القانونية للجريمة السيبرانية.

المطلب الأول: أركان الجريمة السيبرانية.

المطلب الثاني: الطبيعة الخاصة لارتكاب الجريمة السيبرانية.

الفصل الثاني: المواجهة القانونية للجرائم السيبرانية في القانون العُماني.

المبحث الأول: الجهود الوطنية المتخذة في مواجهة الجرائم السيبرانية.

المطلب الأول: المواجهة التشريعية للجرائم السيبرانية.

المطلب الثاني: المواجهة التقنية للجرائم السيبرانية.

المبحث الثاني: إجراءات مواجهة الجرائم السيبرانية وتحدياتها في القانون العُماني.

المطلب الأول: إجراءات التحقيق الخاصة بالجرائم السيبرانية في القانون العُماني.

المطلب الثاني: التحديات القانونية في مواجهة الجرائم السيبرانية في القانون العُماني.

الخاتمـــــــــة.

النتائـــــــــج.

التوصيـــــات.

الفصل الأول

التأصيل النظري للجرائم السيبرانية

في عصر يتسم بالاعتماد المتزايد على التكنولوجيا والاتصالات الرقمية، أصبح الفضاء السيبراني جزءًا لا يتجزأ من الحياة اليومية، رغم فوائد وأهمية الثورة الرقمية إلا أنها أفرزت نوعًا جديدًا من الجرائم المعروفة بالجرائم السيبرانية، التي تستهدف الأفراد والمؤسسات والدول عبر استغلال الثغرات في الأنظمة الرقمية، وتعد الجرائم السيبرانية أحد أكبر التحديات التي تواجه الحكومات والجهات المعنية بالأمن في الوقت المعاصر، حيث تتنوع أساليبها وأدواتها بطرق سريعة ومبتكرة، لذا سعت التشريعات إلى تجريم هذه الأفعال، وأصبح من الضروري فهم التأصيل النظري للجرائم السيبرانية، باعتبارها ميدانًا حديثًا ومتطورًا يتطلب استجابة فعالة وشاملة.

تشمل الجرائم السيبرانية مجموعة متنوعة من الأفعال غير القانونية التي تُنفذ باستخدام التكنولوجيا الرقمية، مثل الهجمات الإلكترونية، وسرقة الهوية، والاحتيال المالي، والاختراقات الأمنية، وعلى الرغم من تعدد أنواع هذه الجرائم وتنوع أساليبها، إلا أنها تشترك في اعتمادها الكبير على الفضاء الإلكتروني والاعتماد على الثغرات التقنية لاستغلال الضحايا، هذا التنوع والتعقيد يجعل من الصعب تحديد تعريف دقيق وشامل للجرائم السيبرانية، مما يستدعي وضع إطار مفاهيمي واضح يمكن أن يساعد في تصنيف هذه الجرائم وفهمها بشكل أعمق.

ويهدف هذا الفصل إلى تقديم إطار مفاهيمي شامل للجرائم السيبرانية، من خلال استعراض مختلف التعريفات والتصنيفات المتعلقة بهذا النوع من الجرائم، والتركيز على تحليل العناصر الأساسية التي تميز الجرائم السيبرانية عن الجرائم التقليدية، وتبيان خصائصها وأركنها وأنواعها، مع مناقشة طبيعتها القانونية وطرق ارتكابها وأطرافها، عليه سيتناول الفصل الأول من خلال مبحثين: الأول حول ماهية الجريمة السيبرانية، والثاني حول أنواع الجرائم السيبرانية.

المبحث الأول

ماهية الجريمة السيبرانية

شـهدت التطورات في مجال التكنولوجيا والاتصـالات ظهور أشـكال جديدة من الجرائم لم تكن معروفة من قبل، وتتميز هذه الجرائم بخصـــوصـــيتها، إذ تختلف عن الجرائم التقليدية التي تحدث في العالم الواقعي، ونظرًا للتهديد الذي تشـــكله هذه الجرائم على الأفراد والدول، فقد أصـــدرت العديد من الدول التشريعات التي تجرم الاعتداء على حقوق الأفراد والمنظمات باستخدام الوسائل الإلكترونية، ولم تتفق التشريعات على مصطلح محدد للدلالة عليها، فهناك من يطلق عليها اسم "الجرائم السيبرانية"، أو "الجرائم المعلوماتية"، أو "الجرائم الإلكترونية" ، أو "الجرائم التقنية"[١] .

سـوف يسـلط هذا المبحث الضـوء على بيان ماهية الجريمة السـيبرانية من خلال تقسـيمه إلى مطلبين: الأول حول مفهوم الجريمة السيبرانية، والثاني حول أنواع الجرائم السيبرانية.

المطلب الأول

مفهوم الجريمة السيبرانية

إزاء تعدد المصـــطلحات التي تدل على الجرائم الســـيبرانية فقد تنوعت التعريفات التي قدمها الفقهاء والباحثون وفقًا للمنهجيات الفلســـفية والفقهية التي يعتمدونها، وتباين المعايير التي يســـتندون إليها، ويعود الاختلاف في هذه المصـــطلحات إلى تطور الظـاهرة الإجرامية المرتبطـة بـالتكنولوجيا الحديثة، وسـيتناول المطلب في فرعين: الأول حول تعريف الجريمة السـيبرانية والثاني حول خصـائص الجريمة السيبرانية، وفقًا للآتي".

[١] هلالي عبد اللاه أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست، دار النهضة العربية، القاهرة، ٢٠١١، ص١٠٧.

الفرع الأول

تعريف الجريمة السيبرانية

بالنظر إلى الجريمة السيبرانية نجد عدم وجود تعريف موحد ومحدد لها، ويرجع ذلك إلى تسارع تطور مجال التكنولوجيا والاتصالات باستمرار، ويتضح التباين في تعريف الجريمة السيبرانية من خلال استخدام مصطلحات متعددة للإشارة إليها، والمعايير المعتمدة في تعريفها.

يقدم الفقه القانوني تعريفات متنوعة للجريمة السيبرانية، ويمكن تصنيفها إلى خمسة اتجاهات رئيسية، كما يلي:

الاتجاه الأول:

يُعرف الجريمة السيبرانية بأنها: "أي سلوك غير قانوني يتم ارتكابه باستخدام الحاسوب"[١]، ويُلاحظ أن هذا التعريف يركز على وسيلة ارتكاب الجريمة، وهي استخدام الحاسوب، لتصنيف الفعل كجريمة سيبرانية.

فمصطلح "جرائم الحاسوب "، الذي يُقصد به الجرائم التي ترتكب باستخدام أجهزة الحاسوب، يُعد من بين أقدم المصطلحات المستخدمة لوصف هذا النوع من الجرائم، حيث ظهرت أول جريمة من هذا النوع في الولايات المتحدة الأمريكية، ورغم استمرار استخدام هذا المصطلح حتى الآن، إلا أنه يعاني من نقص في الدقة، حيث يستثني جميع الجرائم التي تتم باستخدام الأجهزة الإلكترونية الأخرى[٢].

يعتمد أصحاب هذا الاتجاه على الحاسب الآلي والوسائل الأخرى المرتبطة به في ارتكاب الجرائم، فعندما تكون وسيلة ارتكاب الجريمة تتمثل في استخدام الحاسوب أو التكنولوجيا الحديثة، ويُضيق أنصار هذا الاتجاه تعريف الجريمة السيبرانية ويقتصرونه على الحالات التي تتعلق بمكونات الحاسوب غير المادية، مثل البرامج والبيانات المخزنة في الذاكرة[٣].

---

[١] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦، ص١٤.

[٢] محمود رجب فتح الله، شرح قانون مكافحة جرائم تقنية المعلومات في ضوء القانون المصري ١٧٥ لسنة ٢٠١٨ دراسة تحليلية مقارنة، دار الجامعة الجديدة، الإسكندرية، ٢٠١٩، ص٥٥١.

[٣] عبد العال الدريبي، محمد صادق إسماعيل، الجرائم الإلكترونية: دراسة قانونية قضائية مقارنة: مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١٢، ص٤٢

وعلى الرغم من تركيز أصحاب هذا الاتجاه على وسيلة ارتكاب الجرائم إلا أنه يتعين الإشارة إلى أن القانون في العادة يركز على خطورة الفعل والسلوك المكون للجريمة أكثر من تركيزه على الوسيلة المستخدمة في ارتكابها[١].

الاتجاه الثاني:

يُعرف الجريمة السيبرانية بأنها " أي نشاط غير قانوني يهدف إلى نسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي يتم تحويلها عبره"[٢].

يُلاحظ أن هذا التعريف يركز على ضرورة أن يكون الحاسوب موضوع الجريمة السيبرانية، وقد فسّرَ جانب من الفقه القانوني هذه الجريمة كاعتداء على الأموال المعلوماتية، والتي تشمل الأدوات والبرامج والمعدات المتعلقة بالحاسوب[٣].

ويركز أصحاب هذا الاتجاه على الجرائم التي تستهدف نطاق المعلومات، كإحداث تلف البيانات المخزنة في الأنظمة المعلوماتية، أو النسخ أو الوصول إلى المعلومات، وبذلك فإن مجرد الدخول على نظام معلوماتي لا يجرم وفق هذا التعريف[٤].

الاتجاه الثالث:

يُعرّف الجريمة السيبرانية بأنها "أي فعل غير قانوني يتطلب معرفة بتقنيات المعلومات، حيث يكون الجاني ملمًا بالتكنولوجيا الإلكترونية لكي يرتكب الجريمة، ويتم التحقيق فيه وملاحقته قضائيًا.[٥].

ويُلاحظ أن هذا التعريف يشدد على أهمية فهم الفاعل لتقنيات المعلومات الإلكترونية، وخاصة استخدام الحاسوب، لكي تُعتبر جريمته جريمة سيبرانية.

---

[١] رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، الإسكندرية، ٢٠١٨، ص٢٢.

[٢] هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، ١٩٩٢، ص٥.

[٣] محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، ٢٠١٠، ص١٧٠.

[٤] خالد حازم إبراهيم، دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية(الإنترنت) دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠١٤، ص١٢.

[٥] محمد سامي الشوا، الغش المعلوماتي، جامعة نايف العربية للعلوم الأمنية، المجلد (٢٤)، العدد (٢٨٠)، ٢٠٠٥، السعودية، ص٤٤ – ٤٧.

الاتجـــاه الرابـــع:

يعرف هذا الاتجاه الجريمة الســـيبرانية بأنها " الاعتداءات القانونية التي يمكن أن تُرتكب باستخدام الوسائل الإلكترونية بهدف تحقيق الربح"[١].

وقد وصـــفت منظمة التعاون والتنمية الاقتصـــادية التابعة للأمم المتحدة الجريمة الســـيبرانية بأنها: "كل فعل أو امتناع من شـــأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجًا مباشـــرة أو غير مباشرة عن تدخل التقنية الإلكترونية"[٢].

ومن الملاحظ في هذين التعريفين أن التعريف الأول يشترط تحقيق ربح، وهو الأمر الذي لا يتوافق دائمًا مع الجرائم الســـيبرانية، كما أن الفعل المرتكب قد لا يكون عمديًا، بل قد تتحقق بدون قصـــد، كما أن تعريف منظمة التعاون والتنمية الاقتصـــادية يشـــمل الأموال المادية، والتي قد تكون محمية بالفعل بموجب قوانين العقوبات التقليدية، مما يثير تساؤلات حول ضرورة إصدار قوانين خاصة لحمايتها[٣].

الاتجاه الخامس:

يعرف الجريمة السـيبرانية بأنها كل فعل أو امتناع، سـواء كان مباشـرًا أو غير مباشـر، يُعتبر اعتداءً على الأموال المعنوية من خلال استخدام البيانات المخزنة على أجهزة الكمبيوتر[٤].

يُلاحظ أن هذا التعريف يشـمل الأموال المعنوية دون الأموال المادية، على اعتبار أن الاعتداء على الأموال المادية يكون مشمولًا بالقواعد التقليدية المجرمة للاعتداء على أموال الغير[٥].

هناك الكثير من المصطلحات لوصف هذه الجرائم فقد أُطلق عليها الجرائم الإلكترونية، وجرائم الحاســـوب، وجرائم التقنية، وأدى ظهور الانترنت إلى ظهور مصـــطلحات مثل: الجرائم الســـيبرانية أو جرائم الانترنت أو جرائم الشبكات، وهناك مصطلحات أخرى مثل الجريمة الرقمية، والجرائم الافتراضية،

---

[١] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت (الجرائم الالكترونية)، منشورات الحلبي الحقوقية، لبنان، ٢٠٠٧، ص١٥.

[٢] محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمّان، ٢٠٠٥، ص١٧.

[٣] محمود أحمد عبابنة، المرجع السابق، ص١٧.

[٤] سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، الإسكندرية، ٢٠٠٧، ص١٢.

[٥] محمود أحمد عبابنة، مرجع سابق، ص١٩.

وجرائم تكنولوجيا المعلومات، ولا يواجه المتخصص صعوبة في هذه المصطلحات، ومع ذلك قد يسبب تعدد المصطلحات حيرة للأشخاص العاديين والمبتدئين الذين يحاولون فهم الجرائم السيبرانية.

لم تخل التشريعات العربية أيضًا من مشكلة تعدد المصطلحات، حيث استخدمت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠ مصطلح "جرائم تقنية المعلومات"، والذي اعتمدته عدة دول عربية مثل السلطنة والإمارات ومصر، ومع ذلك فإن باقي التشريعات العربية لم تلتزم بنفس المصطلح واختارت استخدام مصطلحات مختلفة حيثُ استخدمت المملكة العربية السعودية والسودان وسوريا مصطلح "الجرائم المعلوماتية"، بينما اختار المشرع الجزائري استخدام مصطلح "الجرائم المتصلة بتكنولوجيا الإعلام والاتصال"، واستخدم المشرع القطري مصطلح "الجرائم الإلكترونية".

عرّف المشرع العُماني "جرائم تقنية المعلومات" بأنها "الجرائم المنصوص عليها في قانون مكافحة جرائم تقنية المعلومات"، وعرف "تقنية المعلومات" بأنها "الاستخدام العلمي للحوسبة والإلكترونيات والاتصالات لمعالجة البيانات بصيغها المختلفة"[١].

يرى الباحث أن اقتصار التعريف على الجرائم المنصوص عليها في قانون مكافحة جرائم تقنية المعلومات، دون باقي الجرائم السيبرانية الواردة في القوانين الوطنية الأخرى، يعكس محدودية قدرة هذا التعريف على استيعاب التطورات الجديدة في مجال الجرائم السيبرانية، والتي قد تتطلب تعريف أكثر شمولية ومرونة.

وقد اعتمد مصطلح "الجريمة السيبرانية" في النطاق الأوروبي ليشمل جرائم الحواسيب والشبكات، حيث يُعتبر هذا المصطلح شاملًا لكل منهما، حيثُ تُستخدم كلمة "سيبران" لتشير إلى العالم الافتراضي وشبكة الإنترنت نفسها، وتم تبني مصطلح "الجريمة السيبرانية" بشكل شائع من قبل المشرعين في الدول

---

[١] نصت المادة (١) من قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم ١٢ / ٢٠١١ على أنه: "في تطبيق أحكام هذا القانون يكون للكلمات والعبارات الآتية المعنى المبين قرين كل منها ما لم يقتض سياق النص معنى آخر: ب- تقنية المعلومات: الاستخدام العلمي للحوسبة والإلكترونيات والاتصالات لمعالجة وتوزيع البيانات والمعلومات بصيغها المختلفة. ج- جرائم تقنية المعلومات: الجرائم المنصوص عليها في هذا القانون. د- البيانات والمعلومات الإلكترونية: كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات أيا كان شكله كالكتابة والصور والأصوات والرموز والإشارات. و- وسيلة تقنية المعلومات: جهاز إلكتروني يستخدم لمعالجة البيانات والمعلومات الإلكترونية أو تخزينها أو إرسالها أو استقبالها كأجهزة الحاسب الآلي وأجهزة الاتصال.

التي أصدرت قوانين لتجريم هذا النوع من الجرائم، بالإضافة إلى غالبية الفقهاء القانونيين، ويعتبر هذا المصطلح هو الأكثر دقة في تعريف هذه الجرائم، حيث يشمل وسائل ارتكاب الجرائم وجميع التقنيات المستخدمة في التعامل مع المعلومات[١].

باستقراء ما تقدم، يقترح الباحث التعريف الآتي:" كل سلوك مجرم يتم في الفضاء الرقمي، أو باستخدام التكنولوجيا الرقمية أو شبكة الإنترنت أو أنظمة المعلومات والبيانات الرقمية".

الفرع الثاني

خصائص الجريمة السيبرانية

الجرائم السيبرانية كظاهرة حديثة ومعقدة في العالم الرقمي، تتميز بخصائص فريدة تجعلها تختلف جذريًا عن الجرائم التقليدية، فهي عابرة للحدود ويمكن ارتكابها من أي مكان في العالم دون التقيد بالحدود الجغرافية، بالإضافة إلى الخصائص الأخرى التي تجعلها تشكل تهديدًا معقدًا وصعب التنبؤ به، مما يستدعي تحليلًا دقيقًا لفهم أبعادها وآلياتها بشكل أعمق.

نظرًا لارتباط الجريمة السيبرانية بالتكنولوجيا الرقمية والفضاء الإلكتروني بشكل عام، فإن ذلك أضفى عليها مجموعة من الخصائص المميزة التي تميزها عن الجرائم التقليدية، ومن بين هذه الخصائص:

أولًا: الجريمة السيبرانية عابرة للحدود:

الجرائم السيبرانية تتجاوز الحدود الجغرافية وتتم في بيئة افتراضية، مما يجعلها عابرة للحدود الدولية[٢].

هذا النوع من الجرائم يمكن أن يتم تنفيذه من أي مكان في العالم، ويمكن للمجرمين السيبرانيين التحرك بحرية دون تقييدات جغرافية، وذلك يشكل تحديًا كبيرًا للسلطات القضائية والتنفيذية في مكافحة هذه الجرائم وملاحقة المجرمين[٣].

---

[١] محمود رجب فتح الله، مرجع سابق، ص٥٤٩، ٥٥١.

[٢] محمد علي العريان، مرجع سابق، ص٧٨.

[٣] عبد العال الديربي، محمد صادق إسماعيل، مرجع سابق، ص٥٣.

انتشار شبكة الإنترنت أتاح إمكانية ربط أعداد هائلة من أجهزة الحاسوب دون قيود زمانية أو مكانية، مما يجعل من السهل على المجرم أن يكون في بلد معين بينما يكون المجني عليه في بلد آخر، وهذا يتطلب وجود تنظيم قانوني دولي وداخلي لمكافحة هذا النوع من الجرائم وضبط فاعليتها، ونظرًا لاختلاف التشريعات الداخلية بين الدول يظهر العديد من التحديات المتعلقة بالاختصاص القضائي وإجراءات الملاحقة القانونية[١].

ثانيًا: الجريمة صعبة الاكتشاف والإثبات:

يكمن تحدي إثبات مثل هذه الجرائم في عدم تركها أثرًا ماديًا ظاهرًا يمكن التحقيق فيه، وتنعقد المشكلة أيضًا بسبب التباعد الجغرافي، إذ تشير الدراسات إلى أن ما يتم اكتشافه من جرائم السيبرانية يصل إلى نسبة ١٪، ومن هذه النسبة يتم الإبلاغ عن نسبة لا تتجاوز ٥٪ فقط[٢]، ويتم ارتكاب الجريمة باستخدام وسيلة إلكترونية تنتهي وظيفتها في زمن قصير جدًا، مما يجعل من الصعب اكتشافها وإثباتها، وهو مختلف تمامًا عن الجرائم التقليدية التي نعرفها[٣].

فالجريمة السيبرانية تتميز بوقوعها في بيئة رقمية، وهذا يثير العديد من التحديات لسلطات تطبيق القانون، حيث إن سلطة الضبط القضائي كانت تعتمد عادة على الأدلة المادية في التحقيقات، ولكن في البيئة الرقمية تصبح الأدلة غالبًا غير مادية، هذه التحديات تشمل صعوبة جمع الأدلة الرقمية ونقلها إلى العالم المادي لعرضها أمام المحكمة، كما أن طبيعة الجرائم السيبرانية تتم بطرق فنية معقدة، بالإضافة إلى ذلك فإن معظم الآثار المترتبة على الجرائم السيبرانية تكون آثارًا رقمية، وتحتاج إلى استخدام تقنيات متخصصة لاكتشافها وتحليلها، وبالنظر إلى ضخامة حجم البيانات والملفات الإلكترونية المتواجدة في البيئة الرقمية، قد يكون من الصعب تحديد البيانات والملفات المجرمة بين هذا الكم الهائل وفصلها عن غيرها من البيانات[٤].

---

[١] مصعب القطاونة، الإجراءات الجنائية الخاصة في الجرائم المعلوماتية، بحث مقدم لشبكة قانوني الأردن، الأردن، ٢٠١٠، ص٥.

[٢] مصعب القطاونة، المرجع السابق، ص٦.

[٣] مفتاح بو بكر المطردي، الجريمة الإلكترونية، مؤتمر رؤساء المحاكم العليا الثالث في الدول العربية، السودان، ٢٠١٢، ص٨.

[٤] جميل عبد الباقي الصغير، الجوانب الاجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٢، ص٤.

على ضـــوء ذلك يتعين على تلك الســـلطات تطوير القدرات والمهارات الخاصـــة في التحقيق الرقمي، والاســـتفادة من التقنيات المتقدمة والخبرات الفنية لمواجهة التحديات الناتجة عن الجريمة السيبرانية وضمان تحقيق العدالة بكفاءة.

إضـــافة إلى ذلك فإن الجريمة الســـيبرانية في كثير من الأحيان لا يُبلَّغ عنها أو تُقدَّم عليها شـكوى بسـهولة، يمكن أن يكون ذلك بسـبب عدم اكتشـاف الضـحية للجريمة، أو خوفًا من التعرض للتشـهير، ونتيجة لذلك فإن معظم الجرائم يتم اكتشـافها بشـكل عرضـي، وفي بعض الأحيان بعد مرور فترة زمنية طويلة من ارتكابها، ومن المهم أيضًا التنويه إلى أن الجرائم التي لم يتم اكتشافها تكون أكثر بكثير من تلك التي تم الكشـف عنها، مما يُشـير إلى وجود فارق بين عدد الجرائم الفعلية وعدد الجرائم التي تم اكتشـافها، وتتجلى هذه الظاهرة بشـكل أكبر في المؤسـسـات المالية، مثل البنوك والمؤسـسـات الادخارية والمؤســسـات المالية الأخرى، حيث تخشـى مجالس الإدارة عادة من أن يؤدي كشـف هذه الجرائم أو اتخاذ الإجراءات القضائية بشأنها إلى تقليل ثقة العملاء في المؤسسة وانصرافهم عنها[١].

ثالثًا: تمتع المجرم السيبراني بمهارات تقنية:

المجرم السـيبراني يتمتع عادةً بمهارات تقنية متقدمة في مجال تقنية المعلومات، ويسـتخدم هذه المهارات لاختراق الأنظمة والشـبكات الحاسـوبية والقيام بأنشـطة غير قانونية، يمكن أن يكون للمجرم السيبراني خلفية تقنية قوية في مجال البرمجة والشبكات وأمن المعلومات[٢].

من المهم أن نلاحظ أن الكثير من المخترقين اكتســـبوا مهاراتهم التقنية من خلال الاطلاع والتعلم الذاتي، ســـواء من خلال دراســـة المواد عبر الإنترنت أو من خلال الانضـــمام إلى مجتمعات التقنية عبر الإنترنت، ولا يشترط أن يكون للمجرم السيبراني درجة أكاديمية في مجال تقنية المعلومات، ولكن يمكنه أن يكون قادرًا على تطوير مهاراته من خلال التجارب العملية والتعلم المستمر.

---

[١] محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، ط٢، ٢٠٠٩م، ص٣٧.

[٢] مدحت عبد الحليم رمضان، جرائم الاعتداء على الأشخاص والإنترنت دار النهضة العربية، القاهرة، ٢٠١٥م، ص٨٩.

فقد لا تتأثر الجرائم التقليدية بالمستوى العلمي للمجرم بشكل عام، ولكن الأمر مختلف تمامًا بالنسبة للمجرم السيبراني الذي يكون عادة من ذوي الخبرة والمعرفة في مجال تقنية المعلومات.

وقد تم تصنيف مجرمي الجرائم السيبرانية إلى الفئات التالية:

أ. **المخترقون:** الذين يتمتعون بمهارات عالية في استخدام الحاسوب ويكون لديهم فضول غير مشروع في اختراق حسابات الآخرين، وغالبًا ما يكونوا متطفلين، ويكون معظمهم في سن المراهقة[١].

ب. **المحترفون:** هم الأكثر خطورة، حيث يهدف بعضهم إلى تحقيق مكاسب مادية غير مشروعة عبر اختراق حسابات البنوك، بينما يستخدم البعض الآخر مهاراتهم لأغراض سياسية[٢] .

ج. **الحاقدون:** وهم الذين يسعون للانتقام والتأثير في الأمور الطائفية دون وجود أهداف سياسية أو مادية[٣].

رابعًا: مسرح الجريمة افتراضي:

بينما يسهل التحديد التقليدي لمكان ارتكاب الجريمة في الجرائم العادية، يُعتبر تحديد مكان وقوع الجريمة في الجرائم الإلكترونية أمرًا صعبًا، نظرًا لسرعة انتقال المعلومات عبر الشبكة العنكبوتية وانعدام الحدود الجغرافية، ونتيجة لذلك طفت على السطح إشكاليات تحديد القانون الذي يجب تطبيقه والمحكمة التي ينبغي تقديم القضية إليها مشكلة دولية تتطلب التعاون بين الدول المختلفة[٤].

خامسًا: الجريمة السيبرانية جريمة متطورة:

الجرائم السيبرانية تعتمد بشكل أساسي على استخدام التكنولوجيا المتطورة مثل الحواسيب، والشبكات اللاسلكية، والإنترنت، وهذه التقنيات الجديدة تسمح بارتكاب جرائم بأساليب غير مسبوقة، وتشكل خطرًا جسيمًا في ظل دخول التقنية في كافة مجالات الحياة، التي جعلت العالم يبدو وكأنه قرية صغيرة، ومع التطور السريع للتقنيات تتطور وسائل ارتكاب هذه الجرائم، مما جعل هذا التقدم يفوق

---

[١] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٤، ص١٧٨.

[٢] خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط١، ٢٠٠٩، ص٧٨.

[٣] خالد ممدوح إبراهيم، المرجع السابق، ص٧٩.

[٤] عفيفي كامل عفيفي، فتوح الشاذلي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، لبنان، ٢٠٠٣م، ص٧٦.

قدرات سـلطات الدول في مكافحة الجريمة، وإضـعاف قدرتها على تطبيق القوانين بشـكل يكفل أمنها وسلامة مواطنيها[١].

سادسًا: احتمال تعدد الأوصاف القانونية لمحل الجريمة السيبرانية

قد يتجلى محل الجريمة السيبرانية بشكلين: مادي ومعنوي، فقد تكون محمولة في صـورة غير مادية مثل البيانات المخزنة في ذاكرة الأنظمة الإلكترونية، أو تكون متجسدة في صورة مادية من خلال تخزينها على وسـائط إلكترونية، ونتيجة لطبيعة المعلومات غير المادية قد تخضـع لأكثر من تصـنيف قانوني، فعلى سـبيل المثال قيام شـخص بتوزيع برامج خبيثة عبر الإنترنت بهدف اختراق أجهزة الكمبيوتر الشـخصـية للآخرين دون إذنهم، يمكن وصـف هذا الفعل بأوصـاف مختلفة كانتهاك الخصـوصـية، والاختراق السـيبراني، وسـرقة المعلومات، والاحتيال الالكتروني في حال قام المرتكب بالاستيلاء على معلومات مالية بهدف ارتكاب احتيال مالي[٢].

باستقراء خصائص الجرائم السيبرانية، والتحديات التي تواجه السلطات في مكافحتها، فإن ذلك يشكل إغراءً كبيرًا للمجرمين، في ظل ما يمكن تحقيقه من مكاسب مالية هائلة مما يجعلها جذابة للعديد من الأشخاص بسبب سهولتها، وصعوبة تعقب مرتكبيها[٣].

وتتميز الجرائم التي تنشأ عن استخدام التقنية بأنها تعتمد على مهارات التخطيط والتنفيذ الذكية باسـتخدام الأجهزة الذكية والأنظمة الحاسـوبية، وتتضـمن هذه الجرائم سـرقة البيانات، والتلاعب بالمعلومات، والتجسس، وغيرها من الأنشطة التي يمكن تنفيذها بواسطة أوامر رقمية[٤].

وبسـبب هذا التحول نحو ارتكاب هذه الجرائم، فإنها قد تكون أكثر تعقيدًا في الكشـف عنها ومكافحتها، ويتطلب التعامل معها مهارات تقنية متقدمة وتحديد نقاط الضـعف في الأنظمة الإلكترونية، وسد الثغرات التشريعية لمكافحتها والتصدي لها.

---

[١] خالد ممدوح إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص٨٦.

[٢] خالد ممدوح إبراهيم، المرجع السابق، ص٨٧-٨٨.

[٣] محمود أحمد عبابنة، مرجع سابق، ص٣٠.

[٤] تميم عبد الله سيف التميمي، الجرائم المعلوماتية في الاعتداء على الأشخاص، مكتبة القانون والاقتصاد، الرياض، ٢٠١٦م، ص٦٦.

المطلب الثاني

أنــواع الجرائــم السيبرانيــة

تتسم الجرائم السيبرانية بتنوعها الكبير، حيث تشمل مجموعة واسعة من الأفعال غير القانونية التي تُنفذ باستخدام التكنولوجيا الرقمية، من أبرز هذه الجرائم الهجمات الإلكترونية التي تستهدف البنى التحتية الحيوية، وجرائم الاحتيال المالي التي تعتمد على اختراق البيانات الشــخصــية، وصــولًا إلى الجرائم المتعلقة بالقرصـــنة وانتهاك حقوق الملكية الفكرية، هذا التنوع يعكس الطبيعة المتطورة لهذه الجرائم، وتبرز الحاجة إلى فهم شامل لكل نوع منها للتصدي بفعالية للتهديدات التي تفرضها.

تتنوع أشكال الجريمة السيبرانية وتعبر الحدود الزمانية والمكانية، حيث يمكن أن تُمارَس ضد الأفراد أو المنظمات أو حتى الدول، وتزداد معدلاتها في الوقت الحالي بفضـــل التقنيات الحديثة التي فتحت أمامها فرصًـا غير مسـبوقة للانتشـار[1]، ويتم تناول المطلب في فرعين: الأول تقسـيم الجرائم السيبرانية من حيث نطاق وقوعها، والثاني تقسيم الجرائم السيبرانية من حيث أسلوب ارتكابها.

الفرع الأول

تقسيم الجرائم السيبرانية من حيث نطاق وقوعها

يتطلب تقسيم الجرائم السيبرانية تصنيفًا دقيقًا لفهم نطاق تأثيرها بشكل أفضل من خلال تقسيم الجرائم السـيبرانية وفقًا لنطاق وقوعها، التي تشـمل الاعتداءات على المعلومات الشـخصـية والأمن الفردي، أو تلك التي تسـتهدف الأصـول المالية مثل الاحتيال المالي وسـرقة البيانات البنكية، أو التي تؤثر على البنى التحتية الحيوية والأمن الوطني، بالإضـــافة إلى الجرائم التي تخل بالمعايير الأخلاقية والقانونية في المجتمع، هذا التصـــنيف يســـاعد في توضـــيح طبيعة الجرائم الســـيبرانية وتوجيه جهود المكافحة بشكل فعال لمواجهة كل نوع منها بما يتناسب مع خصائصه وأبعاده.

---

[1] علي جبار الحسناوي، جرائم الحاسوب والإنترنت، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، ٢٠٠٩، ص٤٦- ٤٧.

وبذلك يمكن تقسيم الجرائم السيبرانية من حيث نطاق وقوعها إلى أكثر من صورة، وذلك على النحو التالي:

أولًا: الجرائم السيبرانية الواقعة على الأموال:

الجريمة المادية تشمل أي نشاط مجرم يتسبب في إلحاق أضرار مادية بالضحايا، سواء كانت هذه الأضرار ناتجة عن السرقة والنصب والتزوير، أو أي نوع آخر من الأنشطة الإجرامية التي تتسبب في فقدان موارد مالية أو ممتلكات، ومن بين الأمثلة على الجرائم المادية، السرقة الإلكترونية لماكينات الصراف الآلي وحسابات البنوك، وإنشاء صفحات إلكترونية مزيفة للتستر على هوية البنوك وابتزاز الضحايا، وكذلك إرسال رسائل بريد إلكتروني مزيفة تدعو إلى التبرع بالأموال مع وعود زائفة بالحصول على نسبة من المبلغ، هذه الأنشطة تعتمد على التلاعب بالتكنولوجيا واستغلال الثغرات في الأنظمة الإلكترونية وضعف التوعية لدى الضحايا؛ الأمر الذي يدفع الأفراد والمؤسسات إلى تبني تدابير أمنية وقائية لحماية أنفسهم من هذه الأنشطة الإجرامية[١].

ويثور التساؤل حول الطبيعة المالية للبرامج والمعلومات محل الجرائم السيبرانية، ما إذا كانت لها قيمة في حد ذاتها أم أنها مجموعة من البيانات لا يقع عليها مفهوم السرقة، وانقسم الفقه في ذلك إلى اتجاهين:

- **الاتجاه الأول:** يرى أن الأشياء المادية فقط هي التي يمكن حيازتها واستحواذها وفقًا للقواعد العامة، إذ يجب أن يكون الشيء المسروق ماديًا، له وجود مادي ملموس ويمكن نقله وحيازته بشكل غير شرعي، ونظرًا للطبيعة غير المادية للمعلومات والبيانات فهي تخرج عن مفهوم الممتلكات المادية إلا في سياق حقوق الملكية الفكرية، وبالتالي فهي مستبعدة من مجال السرقة ما لم تكن مسجلة على وسائط مادية مثل الأقراص ووسائل التخزين الأخرى[٢].

---

(1) Osman Goni. Haidar Ali, Showrov. Mahbub Alam, & Abu Shameem . The Basic Concept of Cyber Crime, Journal of Technology Innovations and Energy,2022, Vol . 1 No . 2,p . 29 .

(٢) مفتاح بو بكر المطردي، مرجع سابق، ص١٧.

- **الاتجاه الثاني** يرى المعلومات كمجموعة قيم يمكن استحواذ عليها مستقلة عن وسائطها المادية تُعتبر المعلومات لها قيمة اقتصادية يمكن الاستحواذ عليها بشكل غير شرعي وترتبط بمؤلفها، أي أن المعلومات تُعتبر مالًا قابلًا للتملك أو الاستغلال بناءً على قيمتها الاقتصادية وليس على أساس كيانها المادي، وبالتالي فهي مشمولة بالحماية القانونية بصفتها أموال[١].

ويرى البعض ضرورة الفصل بين المال الذي يحتوي على المكونات المادية الملموسة، وبين المال المادي الذي يحتوي على مضمون معنوي يعطيه قيمة إضافية، ويشمل الأجهزة ومتعلقات الحاسوب مثل وحدة العرض البصري ووحدة الإدخال والتخزين، ففي جرائم التجسس عن بعد على سبيل المثال، يتم سرقة البيانات دون الإضرار بالأجهزة المادية، وفي مثل هذه الحالة فإن المال الذي يتم سرقته ليس الأجهزة بقيمتها المادية، وإنما القيمة المالية للمحتوى الذي يتم سرقته من هذه الوسائط[٢].

يتطلب التحليل المنطقي اعتبار البيانات الرقمية محل جرائم السرقة السيبرانية كيانًا ماديًا، كونها قابلة للانتقال والاستحواذ، ويمكن رؤيتها على الشاشة بعد تشغيل الجهاز، ومن ثم تُنقل الأفكار والمعلومات التي تحتويها إلى ذهن المتلقي، وبالتالي فإن هذه المعلومات لها أصل ووجود مادي قابل للسرقة[٣].

أدى التقدم التكنولوجي إلى ظهور العديد من وسائل التقنية المستخدمة في ارتكاب الجرائم السيبرانية الواقعة على الأموال، ولعل أخطرها جريمة الاحتيال الإلكتروني.

السلطنة كحال باقي الدول سعت إلى اتخاذ الإجراءات اللازمة للحد من الجرائم السيبرانية بصفة عامة، وجريمة الاحتيال الإلكتروني بصفة خاصة، ومن أهمها الخطوات التشريعية التي اتخذها المشرع في إصدار العديد من التشريعات من بينها قانون المعاملات الإلكترونية الصادر بالمرسوم السلطاني رقم (٩٦/ ٢٠٠٨)، وقانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم (٢٠١١/١٢)، حيث جرمت المادة (١٢) منه "استخدم وسائل تقنية المعلومات في ارتكاب جريمة تزوير معلوماتي، بتغيير الحقيقة في البيانات أو المعلومات الإلكترونية بالإضافة أو الحذف أو

---

[١] محمد عبد الله ابو بكر سلامة، موسوعة جرائم المعلوماتية "جرائم الكمبيوتر والإنترنت"، المكتب العربي الحديث، مصر، ٢٠١١، ص٤٣- ٤٤.

[٢] جلال الزعبي، أسامة المناعسة، جرائم تقنية نظم المعلومات الإلكترونية – دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمّان، ٢٠١٧، ص٣٦- ٣٧.

[٣] هدى حامد قشقوش، مرجع سابق، ص٥١-٥٢.

الاستبدال بقصد استعمالها كبيانات صحيحة تكون مقبولة قانونا في نظام معلوماتي ما من شأنه تحقيق منفعة لنفسه أو لغيره أو إلحاق ضرر بالغير، وتشدد العقوبة إذا كانت تلك البيانات أو المعلومات الإلكترونية حكومية، أو استعمال البيانات الإلكترونية المزورة رغم علمه بتزويرها".

وفي ذلك قررت المحكمة العليا: "إدانة المتهم بجنايتي التزوير الإلكتروني في البيانات الحكومية واستعمالها المؤثمتين بنص المادة (١٢) من قانون مكافحة جرائم تقنية المعلومات استخدام وسيلة تقنية معلومات لارتكاب جريمة تزوير معلوماتي في البيانات والمعلومات الإلكترونية الحكومية وذلك بطريق التغيير بالإضافة وجعل واقعة مزورة في صورة واقعة صحيحة مع علمه، وذلك بأن اعتمد سندات الصرف محل جريمة الاختلاس في النظام المالي الإلكتروني التابع لوزارة المالية، دون أن يكون لها مؤيدات حقيقية وصحيحة، بصفته الموظف المعني باعتماد سندات الصرف بدائرة التدقيق الداخلي بالوزارة وحول تلك السندات بعد اعتمادها إلى وزارة المالية"[١].

ثانيًا: الجرائم السيبرانية المتعلقة بالأشخاص:

قد تحدث الجرائم التي ترتكب من خلال النظام الإلكتروني، وتعتبر هذه الجرائم جزءًا من جرائم الأشخاص، ولكن لا تجد هذه النوعية من الجرائم الكثير من التطبيقات العملية في الحياة الواقعية، إذ ينحصر تأثير هذه الجرائم في نطاق محدود من الأنشطة الإجرامية التي تتضمن الذم والقدح والتحقير، وجرائم التهديد والتحريض، بالإضافة إلى جريمة الاعتداء على الحياة الخاصة، ويشمل الاعتداء السيبراني على حرمة الحياة الخاصة للأفراد عبر الإنترنت عدة أشكال من الانتهاكات، منها[٢]:

١. الإفشاء العلني للمعلومات الخاصة: يتمثل هذا في نشر معلومات حساسة عن الشخص دون إذنه، مثل نشر معلومات عن مرض مخزي يعاني منه الفرد، أو عن عجزه عن سداد ديونه، أو نشر صور شخصية دون موافقته، هذا النوع من الاعتداءات يمكن أن يؤدي إلى خسارة الثقة والكرامة الشخصية للأفراد.

---

[١] الطعن رقم ١٠٢٥ / ٢٠٢٠م جلسة ٣٠ / ٠٣ / ٢٠٢١ مجموعة الأحكام الصادرة عن الدائرة الجزائية بالمحكمة العليا والمبادئ المستخلصة منها في الفترة من ٢٠٢٠/١٠/١م حتى ٢٠٢١/٩/٣٠.

[٢] على نعمة جواد الزرفي، الجريمة المعلوماتية الماسة بالحياة الخاصة، دراسة مقارنة، المكتب الجامعي الحديث،الإسكندرية،٢٠٢٠، ص٣٨.

٢. التشهير والإساءة إلى السمعة: يتضمن ذلك نشر معلومات كاذبة أو مشوهة عن الشخص بهدف النيل من سمعته وتقديمه بشكل سلبي في نظر العامة، ويمكن أن يؤدي هذا النوع من الاعتداءات إلى تأثير سلبي على حياته المهنية والشخصية.

٣. الاستيلاء على البيانات الشخصية: يشمل هذا استخدام تقنيات القرصنة أو الاحتيال للحصول على معلومات شخصية عن الفرد مثل الاسم والصورة والبيانات الشخصية الأخرى، لاستخدامها في أنشطة احتيالية أو الإضرار بالآخرين.

تجدر الإشارة إلى أن المشرع العُماني قد وسع نطاق الحماية ليشمل الأشخاص الاعتباريين بجانب الأفراد الطبيعيين، فقد تناول قانون مكافحة جرائم تقنية المعلومات في المادة (٦) منه الاعتداء على البيانات والمعلومات الإلكترونية التابعة للمؤسسات الحكومية والمصارف والمؤسسات المالية، مما يعزز حماية الأشخاص الاعتباريين من التهديدات السيبرانية، وهذا يعكس التزام المشرع بتوفير إطار قانوني شامل يضمن الحماية لكل من الأفراد والكيانات القانونية.

ويتضمن هذا النوع من الجرائم اختراق الأنظمة الإلكترونية للحصول على معلومات أو تعديلها أو تدميرها دون إذن، حيث إن كمية البيانات الشخصية الهائلة الساكنة في العالم الافتراضي، تمثل خطرًا داهمًا على خصوصية أصحابها، لاسيما وأن هذا العصر هو عصر التكنولوجيا، وخاصة بعد ظهور البرامج والتطبيقات التي تشترط الحصول على معلومات خاصة للعملاء مقابل استخدامها وأدى ذلك إلى ظهور تجارة البيانات الشخصية، من خلال استغلالها وعرضها للبيع لأغراض مختلفة، حيث أنها تتعرض عند معالجتها أثناء الجمع أو التخزين أو النقل للعديد من المخاطر التي تنتهك خصوصية تلك البيانات، بالإضافة إلى انتشار الوسائل الإلكترونية التي سهلت السبل لذلك مع ضعف الوازع الأخلاقي أو غياب القاعدة القانونية التي تعمل على حماية تلك البيانات، مما أدى إلى تدخل المشرع في كثير من البلدان لوضع إطار قانوني يحكم معالجة البيانات الشخصية، بحيث تكون هذه المعالجة ظاهرة ويعلم بها الكافة، فضلًا عن حقهم في الاعتراض عليها[١].

[١] سامح عبد الواحد التهامي، ضوابط معالجة البيانات الشخصية، دراسة مقارنة بين القانون الفرنسي والقانون الكويتي، مجلة كلية القانون الكويتية العالمية، المجلد ٣، العدد ٩، ٢٠١٥، ص٣٩٨.

وفي السلطنة رخصت المادة (٤٣) من قانون المعاملات الإلكترونية، لأية جهة حكومية أو مقدم خدمات تصديق أن يجمع بيانات شخصية مباشرة من الشخص الذي تجمع عنه البيانات أو من غيره بعد الموافقة الصريحة لهذا الشخص، وذلك لأغراض إصدار شهادة أو المحافظة عليها أو تسهيل ذلك، ولا يجوز جمع البيانات أو معالجتها أو استخدامها لأي غرض آخر دون الموافقة الصريحة للشخص المجموعة عنه البيانات[١].

كما ألزمت المادة (١٤) من قانون حماية البيانات الشخصية المتحكمَ قبل البدء في معالجة أي بيانات شخصية أن يخطر صاحب البيانات الشخصية بتفاصيل المعالجة والغرض منها ودرجة الإفصاح عن بياناته وحقوقه في الوصول لتلك المعلومات، وأي معلومات مفيدة لاستيفاء المعالجة[٢].

ونصت المادة (١٩) من القانون ذاته على أنه: "يلتزم المتحكم، عند حدوث اختراق للبيانات الشخصية، يؤدي إلى تدميرها أو تغييرها أو الإفصاح عنها أو الوصول إليها أو معالجتها بصورة غير قانونية، بإبلاغ الوزارة وصاحب البيانات الشخصية عن الاختراق، وذلك وفقًا للضوابط والإجراءات التي تحددها اللائحة".

ثالثًا: الجرائم السيبرانية المتعلقة بجرائم أمن الدولة والجرائم المخلة بالثقة العامة والآداب العامة:

بسبب الطبيعة الخاصة لجرائم أمن الدولة واحتمالية وقوع العديد منها عبر الوسائل الإلكترونية، فإنها تعتبر مرشحة للحدوث عبر الفضاء الإلكتروني، سواء كانت تتعلق بأمن الدولة الداخلي أو الخارجي من الأمثلة على ذلك: جرائم التجسس، وجرائم التواصل مع العدو، وجرائم إثارة الفتن والتحريض، وجرائم المساس بالوحدة الوطنية، والتحريض على التمرد ضد السلطات[٣].

---

[١] قانون المعاملات الإلكترونية الصادر بالمرسوم السلطاني رقم (٦٩ / ٢٠٠٨)، نُشر في الجريدة الرسمية العدد ٨٦٤ بتاريخ ١ / ٦ / ٢٠٠٨م.

[٢] قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم (٦/ ٢٠٢٢)، نُشِر في الجريدة الرسمية، العدد رقم (١٤٢٩) الصادر في ١٣ / ٢ / ٢٠٢٢م.

[٣] محمد حسين منصور، المسؤولية الإلكترونية، منشأة المعارف، الإسكندرية، ٢٠٠٦، ص١٤٨.

أما بالنسبة للجرائم المخلة بالثقة العامة والآداب العامة، فهي أيضًا قابلة للحدوث عبر الوسائل الإلكترونية، مثل جرائم التزوير، وتقليد الأختام، وتزوير الأوراق البنكية، وانتحال الشخصية[1].

ويُعتبر الإرهاب في السلطنة من جرائم أمن الدولة وفقًا لأحكام قانون الجزاء وقانون مكافحة الإرهاب، وقانون مكافحة غسل الأموال وتمويل الإرهاب، وأحد أهم صوره الإرهاب الإلكتروني الذي يتمثل في استخدام التكنولوجيا الرقمية والإنترنت لتنفيذ أعمال إرهابية أو الترويج للأفكار الإرهابية وتأييدها.

وفي هذا السياق فقد حددت المادة (٢٠) من قانون مكافحة جرائم تقنية المعلومات العقوبات التي تواجه أي فرد يتورط في استخدام التكنولوجيا لأغراض إرهابية وحددت الأفعال المكونة للجريمة، وهي: "إنشاء موقعًا إلكترونيًا على الشبكة المعلوماتية لتنظيم إرهابي أو استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات لأغراض إرهابية أو في نشر أفكار ومبادئ تنظيم إرهابي والدعوة لها أو في تمويل العمليات الإرهابية والتدريب عليها أو في تسهيل الاتصالات بين تنظيمات إرهابية أو بين أعضائها وقياداتها أو في نشر طرق صناعة المتفجرات والأسلحة والأدوات التي تستخدم خاصة في عمليات إرهابية".

---

[1] عبدالفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت: دراسة متعمقة في جرائم الحاسب الألي والانترنت، دار الكتب القانونية، مصر، ٢٠٠٢، ص٥٨.

الفرع الثاني

تقسيم الجرائم السيبرانية من حيث أسلوب ارتكابها

الجريمة السـيبرانية هي نوع من أنواع الجريمة تشـمل اسـتخدام التكنولوجيا وتقنيات الحاسـب الآلي بشكل مباشر أو غير مباشر لتنفيذ أعمال إجرامية، ويمكن استخدام التقنيات السيبرانية كوسيلة لتنفيذ الجرائم أو كهدف لتحقيق أهداف إجرامية مختلفة[١].

وتعتبر الجريمة السيبرانية مظهرًا جديدًا للسلوك الإجرامي ويمكن تصورها في صورتين، إما أن تكون جريمة تقليدية تُرتكب باستخدام وسائل إلكترونية أو رقمية، أو أن تكون مستحدثة ليس لها صورة في الجرائم التقليدية كاستهداف الوسائل المعلوماتية نفسها مثل قواعد البيانات والبرامج المعلوماتية[٢].

وبذلك تقسم الجرائم السيبرانية من حيث أسلوب ارتكابها إلى **صورتين**[٣]:

أولًا: الجرائم التقليدية التي ترتكب بوسائل إلكترونية:

تمتاز الجرائم السيبرانية باستخدام التقنية الرقمية والانترنت في ارتكابها، وبالتالي يتوقف إمكانية المجرم السـيبراني على اسـتخدام أجهزة الحاسـوب المتصـلة بالإنترنت والأجهزة المحمولة الذكية لتنفيذ هجماته، ويتطلب ارتكاب هذه الجرائم توافر وسـائل التكنولوجيا الحديثة، بالإضـافة إلى معرفة ودراية المجرم بكيفية التعامل مع هذه الأجهزة[٤].

يتم اسـتخدام الحاسـوب والإنترنت في الجرائم السـيبرانية كأداة لتحقيق أهداف غير مشـروعة، يشـمل ذلك العديد من الأنشـطة المحظورة كالنصـب والاحتيال، وانتهاك حقوق الملكية الفكرية، وانتهاك الخصـوصـية، والاتجار في المواد الإباحية للأطفال، وتزوير العملة والمسـتندات الرسـمية أو الاختلاس أو الاعتداء على بيانات ومعلومات حواسـيب أخرى عبر الإنترنت للحصـول على فوائد مالية أو غيرها

---

[١] محمود أحمد القرعان، الجرائم الإلكترونية، دار وائل للنشر والتوزيع، عمّان، ط١، ٢٠١٧، ص١٩.

[٢] أيمن محمد عبداللطيف، إشكالية إثبات الجرائم الإلكترونية، الموقع الإلكتروني:(https://ae.linkedin.com/pulse)، تم الاستيراد بتاريخ ٢٠ مارس ٢٠٢٣م.

[٣] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمّان، ٢٠٠٨، ص٦٤.

[4] David Wall, Cybercrimes: New Wine, No Bottles, Invisible Crimes, pp 105–139 .

من الجرائم تتسبب في أضرار جسيمة للأفراد والمؤسسات، وتشكل تهديدًا على الأمن السيبراني والاقتصاد الرقمي[١].

الاعتداء السيبراني على حقوق الملكية الفكرية يشمل الاعتداء على العلامات التجارية وبراءات الاختراع، وكذلك نسخ وتقليد البرامج وإعادة إنتاجها وصنعها دون ترخيص، مما يؤدي إلى انتهاك الحقوق المالية والحقوق الأدبية لصاحب الأعمال الفكرية، أما الاستيلاء والنصب والاحتيال السيبراني، فهو يشمل استيلاء الأفراد على مال منقول أو على سند مالي، أو تزوير هذا السند، أو توقيعه بطرق غير قانونية عبر الإنترنت، ويتم ذلك عن طريق الاحتيال واستخدام معلومات كاذبة أو انتحال صفة غير صحيحة[٢].

المجرم السيبراني يستخدم تقنية الاختراق للوصول إلى الأنظمة المعلوماتية والأمنية بهدف تنفيذ جريمته، ويتم ذلك عادةً عن طريق استغلال ثغرات في نظام الحماية، باستخدام برنامجين رئيسيين لتحقيق ذلك: الأول الخادم الذي يتصل بجهاز المجني عليه وينفذ المهام الموكلة إليه، والثاني برنامج المستفيد الذي يوجد بجهاز المخترق، وتتضمن طرق الهجوم السيبراني المتعددة الذي يتسبب في ضغط كبير على الموقع، والاختناق المروري السيبراني الذي يمنع تبادل المعلومات، واستغلال الأبواب الخلفية التي يتركها مصمم النظام عمدًا للتسلل إليه عند الحاجة، ويستخدم المجرم السيبراني العديد من البرامج ، منها: حصان طروادة الذي يزرعه المبرمج داخل النظام لإطلاق الفيروسات أو تعطيل الجهاز أو الشبكة، وفيروسات حجب الخدمات (DDOS) التي تستخدم لتعطيل شبكات الخدمات، وحقن (SQL) التي تُستخدم لاستغلال الثغرات في قواعد البيانات، والتعدين الخبيث (Crypto Jacking) الذي يستخدم لاختراق جهاز الكمبيوتر واستخدامه في إصدار العملات الرقمية المشفرة[٣].

وفي هذا السياق فقد قام شخص في عام ١٩٨٩م بتوزيع عدد كبير من النسخ الخاصة ببرنامج، والذي بدا أنه يحتوي على معلومات حول مرض نقص المناعة المكتسبة، وكان يحمل فيروس حصان

---

[١] محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع، عمّان،٢٠٠٤، ص٤٦.

[٢] غانم مرضي الشمري، الجرائم المعلوماتية، الدار العلمية الدولية، عمّان، ط١، ٢٠١٦ م، ص٥٢.

[3] Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace, School of Law Faculty Publications, University of Dayton University of Dayton, 2010, P12.

طروادة، وعند تشغيل البرنامج يؤدي الفيروس إلى تعطيل جهاز الحاسوب وظهور رسالة على الشاشة تطلب دفع مبلغ مالي إلى عنوان في دولة "بنما" ليتمكن المتضرر من الحصول على "مفتاح" فك الفيروس، وفي عام ١٩٩٠ تم القبض على المشتبه به في ولاية أوهايو بالولايات المتحدة الأمريكية، وقدمت بريطانيا طلبًا لتسليمه ومحاكمته أمام القضاء الإنجليزي، لأن البرنامج تم إرساله من داخل المملكة المتحدة[١].

ثانيًا: الجرائم السيبرانية المستحدثة:

يقصد بها الجرائم التقنية التي لا يوجد لها صور في الجرائم التقليدية، مثل تعديل أو تحريف برامج الحاسوب أو تدمير البيانات والمعلومات المخزنة فيه، وهي تلك الجرائم التي تنشأ بفعل التطورات التكنولوجية الجديدة وتستهدف نقاط ضعف جديدة في الأنظمة والتكنولوجيا الرقمية، وتتطور باستمرار مع تطور التكنولوجيا وتشمل مجموعة متنوعة من الأنشطة الإجرامية التي يمكن تنفيذها باستخدام الحوسبة والشبكات والإنترنت[٢].

وتعتبر برامج الحاسوب مجموعة من الأوامر والبيانات التي تتضمن تطبيقات تقوم بأداء الوظيفة المطلوبة عند تشغيلها في الحاسب الآلي، بناءً عليه فإن الجريمة السيبرانية تشمل الأنشطة الإجرامية التي تشتمل على دخول الأجهزة الإلكترونية المعاصرة ضمن نطاق الحاسب الآلي، بالإضافة إلى ارتباطها بالشبكات الخاصة والعامة والعالمية، ويمكن للجرائم السيبرانية أن تشمل الاعتداء على البيانات والانتهاكات الإلكترونية في العالم الافتراضي[٣].

تناول قانون مكافحة جرائم تقنية المعلومات الجرائم المتعلقة بالتدخل غير المشروع في الأنظمة الإلكترونية، فحدد عقوبات السجن والغرامة لمن يقوم بدخول أو تعديل أو نشر بيانات أو معلومات

---

[١] طارق ابراهيم دسوقي عطية، عولمة الجريمة، الشركات العالمية في الممارسات الاجرامية، دار الجامعة الجديدة، الإسكندرية، ٢٠١٠، ص٢٣٠.

[٢] جلال الزعبي، أسامة المناعسة، مرجع سابق، ص٣٨.

[٣] محمود عمر محمود، الجرائم المعلوماتية والإلكترونية، خوارزم العلمية، السعودية، ط١، ٢٠١٥، ص٥٠.

إلكترونية بطريقة غير مشروعة، مع تشديد العقوبات إذا كانت البيانات ذات طبيعة شخصية[١]، وشدد العقوبات إذا ارتكبت من قبل موظف أثناء أداء واجباته الوظيفية[٢].

ومن الجرائم المستحدثة التي نص عليها المشرع العُماني القيام بتغيير أو تعديل أو إتلاف البيانات الطبية عبر استخدام تقنيات المعلومات بدون وجه حق[٣]، يعني ذلك أنه إذا قام شخص ما، على سبيل المثال، بتعديل تقرير طبي إلكتروني بطريقة غير مشروعة، فإنه يتعرض للملاحقة الجزائية، وذلك بغرض حماية سرية وصحة البيانات الطبية، حيث يعد الوصول غير المشروع إليها أو تغييرها خطيرًا على سلامة المرضى ومصداقية المعلومات الطبية.

كما جرم المشرع العُماني الدخول إلى مواقع إلكترونية أو أنظمة معلوماتية بشكل غير قانوني بهدف الحصول على بيانات حكومية سرية أو وفقًا لتعليمات معينة، وتشدد فيها العقوبة إذا تسبب في إلغاء أو تغيير أو تعديل أو تشويه أو إتلاف أو نسخ أو تدمير أو نشر البيانات أو المعلومات الإلكترونية[٤].

ولا شك أن ذلك يهدف إلى حماية سرية البيانات الحكومية، خاصة البيانات المالية والمعلومات الحساسة، وتعزيز الأمن الإلكتروني للمؤسسات المالية والمصارف لضمان عدم تعرضها للتجسس أو الاختراق من قبل أفراد غير مخولين.

كما نص المشرع العُماني على صور أخرى للجرائم السيبرانية المستحدثة كالدخول إلى موقع إلكتروني بشكل غير قانوني بهدف تغيير تصميمه أو تعديله أو إتلافه أو إلغائه أو تغيير عنوانه، وعرقلة خط سير البيانات الإلكترونية أو المعلومات المرسلة عبر الشبكة المعلوماتية بدون وجه حق، سواءً بقطع بثها أو استقبالها أو التنصت عليها، أو إدخال برامج أو بيانات غير مصرح بها في نظام معلوماتي أو شبكة معلوماتية بهدف تعطيلها أو تعطيل عملها، أو إعاقة الوصول إلى خدمات مقدم الخدمة أو دخول نظام معلوماتي أو وسائل تقنية المعلومات[٥].

---

[١] المادة الثالثة من قانون مكافحة جرائم تقنية المعلومات.

[٢] المادة الرابعة من قانون مكافحة جرائم تقنية المعلومات.

[٣] المادة الخامسة من قانون مكافحة جرائم تقنية المعلومات.

[٤] المادة السادسة من القانون العُماني لمكافحة جرائم تقنية المعلومات.

[٥] المواد (٧ – ١٠) من قانون مكافحة جرائم تقنية المعلومات.

بالإضـــافة إلى ما تقدم فقد نص قانون تنظيم الاتصـــالات على تجريم اســـتخدام الوســـائل الاحتيالية في الحصـول على خدمات الاتصـالات، أو الوصـول غير القانوني إلى الخدمات، ويشـمل ذلك الموردين عند اللجوء إلى وسائل غير مشروعة[1].

[1] المواد (٥٧ – ٥٩) من قانون تنظيم الاتصالات الصادر بالمرسوم السلطاني العُماني رقم (٣٠/ ٢٠٠٢).

المبحث الثاني

الطبيعة القانونية للجريمة السيبرانية

تمثل الجريمة السيبرانية أحد التحديات الرئيسية التي تواجهها المجتمعات الحديثة في عصر التكنولوجيا، حيث تتسم بالتطور المستمر، وذلك يجعل للجريمة السيبرانية طبيعة قانونية خاصة تستوجب على الباحثين دراسة وتحليل تلك الطبيعة بشكل دقيق لإيجاد السبل الكفيلة لمكافحتها.

وتأتي أهمية فهم الطبيعة القانونية للجريمة السيبرانية من ضرورة معالجة تلك الظاهرة بشكل شامل وفعال، والتكيف والتطور مع الثورة التقنية التي يعيشها العالم المعاصر.

ويهدف هذا المبحث إلى الوقوف على الجوانب القانونية المتعلقة بالجريمة السيبرانية، وسيتم تناول المبحث من خلال المطلبين: الأول حول أركان الجريمة السيبرانية، والثاني حول الطبيعة الخاصة لارتكاب الجريمة السيبرانية.

المطلب الأول

أركان الجريمة السيبرانية

تستند الجريمة بشكل عام على ثلاثة أركان أساسية وهي الركن الشرعي، الذي يُعتبر الصفة غير المشروعة للفعل، وتكون قواعد التجريم والعقاب للجرائم الإلكترونية موضوعة في القانون لجرائم أنظمة المعلومات، والركن المادي الذي يشير إلى الأفعال المكونة للجريمة التي تظهر من خلالها للعالم الخارجي، والركن المعنوي الذي يرتبط بالإرادة المتعلقة بالفعل، سواء كان ذلك قصدًا أو خطأ[1].

فالجريمة السيبرانية من الجرائم العمدية التي لا يكفي لتحققها توفر الركن المادي فقط، أو الفعل المكون للجريمة، الركن المعنوي هو القصد الجنائي بشقيه العلم والإرادة، وهو ما سيوضحه المطلب من خلال الفرعين التاليين.

---

[1] محمد الجبور، الوسيط في قانون العقوبات (القسم العام)، دار وائل، عمّان، ط١، ٢٠١٢، ص٥٩.

الفرع الأول

الركـــــن المـــــادي

يعتبر الركن المادي عنصرًا جوهريًا في تكوين الجريمة السيبرانية، إذ يشمل الفعل أو الامتناع عن الفعل الذي يؤدي إلى وقوع الضـرر أو التهديد في البيئة الرقمية، ويأخذ أشـكالًا متعددة تتراوح بين اختراق الأنظمة الإلكترونية، والاحتيال عبر الإنترنت، وســـرقة البيانات، وتدمير أو تعطيل البنى التحتية الرقمية، ويتم تنفيذها باســـتخدام أدوات وتقنيات رقمية، مما يميزها عن الجرائم التقليدية ويُعقِد عملية تحديدها وملاحقة مرتكبيها، وحيثُ أن فهم الركن المادي في هذا الســياق ضـــروري لإثبات وقوع الجريمة وتطبيق العقوبات المناسبة، خاصة في ظل التطور السريع للتكنولوجيا الذي يُغير باستمرار طبيعة هذه الجرائم.

الركن المادي للجريمة أشارت إليه المادة (٢٧) من قانون الجزاء التي نصت على أنه: "يتكون الركن المادي للجريمة من نشاط مجرم قانونًا بارتكاب فعل، أو امتناع عن فعل"[١].

ويعد الركن المادي أحد الدعامات التي تقوم عليها المســؤولية الجزائية، ويعد تخلف هذا الركن مانعًا لقيام الجريمة، والركن المادي هو المظهر الخارجي الذي تقوم به الجريمة إلى حيز الوجود، وهو الفعل المجرم بموجب نصـــوص قانون الجزاء والقوانين الجزائية الأخرى، إذ يعد الركن المادي تجســـيد للإرادة الجرمية للفاعل[٢]، ويتكون من السلوك والنتيجة الإجرامية والعلاقة السببية بينهما، وسيتم تناولها تباعًا على النحو الآتي:

أولا: السلـــوك:

من بين التحديات العملية التي تثيرها الجريمة السيبرانية هو طبيعة الركن المادي في هذا النوع من الجرائم، فمفهوم التجريم يتمركز حول اسـتخدام غير قانوني للنظام الإلكتروني أو اختراقه، مما ينتج عن ذلك تأثيرًا ملموسًـا قد يظهر على شـكل تدمير للبيانات، وهذا ما يثير احتمالية الخسـارة المتعمدة

---

[١] قانون الجزاء الصـــادر بالمرســوم الســلطاني رقم ٧ / ٢٠١٨، الباب الثالث تقســيم الجرائم وأركان الجريمة، الفصـــل الثاني الركن المادي، المادة (٢٧).

[٢] ضاري خليل، الوجيز في شرح قانون العقوبات، دار القادسية للنشر والطباعة والتوزيع، بغداد، ٢٠٠٥، ص٦٦.

للممتلكات أو السـرقة، عبر اسـتغلال بطاقات الائتمان بطرق غير قانونية، أو التلاعب ببيانات الحاسوب، أو غيرها من الأفعال الجرمية.

والسـلوك في الركن المادي للجريمة قد يكون إيجابيًا أو سـلبيًا بالترك، وتقع جرائم الترك بدون أن يتحقق عنها نتيجة إيجابية مباشرة، ويرى جانب من الفقه أن الركن المادي في الجريمة السيبرانية لا يقوم بسـلوك سـلبي، وإنما بفعل إيجابي، وبذلك تعد الجريمة السـيبرانية من الجرائم ذات السـلوك الإيجابي، التي تتكون من إتيان عمل أو فعل نهى القانون عن فعله، وذكر جانب من الفقه أن الركن المادي في الجريمة السـيبرانية يتكون من مجموعة أفعال متعددة[١]، إلا أن الباحث يرى إمكانية قيام الجرائم السـيبرانية بفعل سـلبي، كإهمال الموظف المعهود إليه إدارة الأنظمة أو الشـبكات الإلكترونية عمدًا أو تقصـيرًا القيام بإجراءات تأمين الشـبكات أو تحديثها حسـب البروتكولات التقنية المعتمدة وأدى ذلك إلى الإضـرار بهذه الشـبكات والأنظمة، أو نتج عن اهماله في القيام بواجبه تسـهيل ارتكاب الغير لجرائم أخرى كالاختراق وغيرها من الجرائم السيبرانية.

السـلوك الإجرامي في هـذه الجرائم يتمحور عـادةً حول المعلومـات المخزنـة على الأجهزة الحاسـوبية، أو تلك التي يتم إدخالها إليها، والتحدي الرئيسـي يكمن في أن السـلوك الإجرامي يمكن أن يتحقق بسـهولة من خلال النقرة على زر في الحاسـوب، مما يؤدي إما إلى تدمير النظام المعلوماتي أو التلاعب بالبيانات أو السرقة[٢].

وإذا كان السلوك الإجرامي كعنصر في الركن المادي في الجريمة التقليدية يمكن رؤيته بوضوح والتأكد منه، كما في حالات القتل أو السرقة أو التزوير، إلا أن السلوك الإجرامي في الجريمة السيبرانية يُعتبر أمرًا أكثر تعقيدًا، حيث يتم ارتكابها باسـتخدام معلومات تنتقل عبر أنظمة الحاسـوب، والتي لا

---

[١] حسـام محمد السـيد محمد، المواجهة الجنائية لظاهرة الثأر الإباحي، دراسـة مقارنة بين النظامين الأنجلو أمريكي واللاتيني، مجلة الدراسـات القانونية والاقتصادية، عدد ٩(٥)، ٢٠١٩، ص١٨٥.

[٢] سميرة معاشـي، ماهية الجريمة المعلوماتية، بحث منشور في مجلة المنتدى القانوني، العدد السـابع، جامعة محمد خيضـر بسكرة، الجزائر، ٢٠١١، ص٢٨٠.

يمكن الإمساك بها ماديًا، لذلك يتطلب أن يولى تحليل السلوك الإجرامي في الجريمة السيبرانية اهتمامًا خاصًا، وعلى وجه الخصوص جرائم الاعتداء على المال العام أو الخاص[١].

إضافة إلى أن النشاط أو السلوك المادي في الجريمة السيبرانية تثير العديد من التساؤلات بشأن وقت بدء الجريمة، حيث يختلف هذا النشاط عن العالم المادي، فالجريمة السيبرانية تتطلب إعدادًا تقنيًا، وبدونه لا يمكن للشخص حتى الاتصال بالإنترنت، سواء كان ذلك لارتكاب جريمة معينة أو لمجرد التصفح أو المشاركة في الاتصال المباشر كالمحادثات وغيرها[٢].

ويمثل السلوك المادي جانبًا أساسيًا في الجريمة السيبرانية، حيث يتضمن ذلك السلوك أو النشاط المادي وفقًا لطبيعة الأفعال المكونة للركن المادي في الجريمة السيبرانية، وقد حاول المشرع في النظم المتعددة تدارك هذا الأمر عندما استخدمت التشريعات مصطلحات صريحة للإشارة إلى استخدام التقنية في ارتكاب الجريمة، ومنها على سبيل المثال: " إذا ارتكبت الجريمة باستخدام نظام معلومات أو الشبكة المعلوماتية" أو "باستخدام المعالجة الآلية للبيانات"، وهذا يعكس وعي المشرع بأهمية مفهوم الشروع في ارتكاب الجريمة عبر الشبكة المعلوماتية المتصلة بالإنترنت[٣].

لذا، فإن الدفع بعدم وجود قدرات تقنية في حالة الاتهام بارتكاب جريمة عبر الإنترنت يعتبر جزءًا أساسيًا من الدفوع الموضوعية التي يتعين على المحكمة الرد عليها تفصيلًا، وإلا فإن عدم توفر هذا الرد يمكن أن يُعتبر عيبًا في التسبيب يجعل حكمها قابلًا للنقض، وقد أدت الطبيعة الموحدة للجريمة السيبرانية في أشكالها المادية وارتكابها عبر الإنترنت، إلى إضفاء طابع تقني على هذه الجرائم[٤].

ثانيا: النتيجة الإجرامية:

لكي يتوافر الركن المادي في الجريمة السيبرانية، لابد من حصول النتيجة الإجرامية المرتبطة بالسلوك الإجرامي، وتثير مسألة النتيجة الإجرامية في الجرائم السيبرانية جدلًا كبيرًا بين أنصار المذهب

---

[١] عبد الفتاح حجازي، صراع الكمبيوتر والانترنت، دار الكتب القانونية، مصر، ٢٠٠٧، ص١١٤.

[٢] كاميران عزيز حسن، الجهود الدولية في مواجهة الجرائم السيبرانية، منشورات الحلبي الحقوقية، ط١، ٢٠٢٠، ص٣٥.

[٣] عبد الكريم الردايدة، الجرائم المستحدثة واستراتيجية مواجهتها، دار ومكتبة حامد للنشر والتوزيع، عمّان، ط١، ٢٠١٣، ص٢٣.

[٤] خالد ممدوح إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص١٠٠.

المادي وأنصار المذهب القانوني حول تحديد الجريمة السيبرانية هل هي جرائم مرتكبة سلوكًا أو كنتيجة في العالم الافتراضي، أم أن هناك امتدادًا للنتيجة لتحقيق وجودها المادي[١].

وتنقسم النتيجة الإجرامية إلى قسمين[٢]:

١. **جرائم الضـــرر**: هي التي يطلب القانون في ركنها المادي حصـــول ضـــرر معين، وذلك مثل حصول الضرر في الجرائم السلبية والإيجابية.

٢. **جرائم الخطر**: هي جرائم السلوك المجرد حتى لو لم تقع النتيجة الإجرامية، وجرائم الشروع التي يعاقب عليها المشـرع العُماني طبقًا لنص المادتين (٣٠، ٣١) من قانون الجزاء في الجنايات أو الجنح إذا نص عليها القانون صـراحة، وذلك لما يمثله السـلوك الإجرامي من خطر دون النظر في نتيجة ذلك الفعل، ولا يعاقب عليها في المخالفات؛ نظرًا لقلة خطورة الدافع الإجرامي في نفس الفاعل، كما نصـــت المادة (٣٠) من قانون مكافحة جرائم تقنية المعلومات، على تجريم الشـروع في ارتكاب إحدى الجرائم المنصـوص عليها في القانون بنصـف الحد الأعلى للعقوبة المقررة للجريمة.

ثالثًا: العلاقة السببية:

العنصـر الثالث من عناصـر الركن المادي في الجريمة السـيبرانية يتمثل في العلاقة السـببية، أي تكون النتيجة الإجرامية التي تحققت نتيجةً لسـلوك الجاني مباشـرة، وقد عبَّرت عنها المحكمة العليا بأن العلاقة السـببية عنصـرًا في الركن المادي، فإذا كانت هذه العلاقة منتفية فلا يسـأل الجاني عن النتيجة التي لم يكن فعله سـببها[٣]، أي تبدأ بالسـلوك وتنتهى بالنتيجة الإجرامية، أو تمثل صـلة بين ظاهرتين ماديتين، هما الفعل والنتيجة[٤]، ومن ثم فإن تحقق العلاقة السـببية يرجع إلى الماضـي، أي منذ لحظة وقوع الفعل، وإن تحققت النتيجة مستقبلًا.

---

[١] محمود أحمد القرعان، مرجع سابق ص٣٤.

[٢] روان بنت عطية هلا الصحفي، الجرائم السيبرانية، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد ٢٤، الأردن، ٢٠٢٠، ص٢٣.

[٣] الطعن رقم ٥١٩/ ٢٠١٤م جزائي عليا (أ) جلســة ٢٥ / ١١ / ٢٠١٤، مجموعة الأحكام الصـــادرة عن الدائرة الجزائية بالمحكمة العليا والمبادئ المستخلصة منها للسنتين القضائيتين الخامسة عشر والسادسة عشر.

[٤] محمود نجيب حسني، علاقة السببية في قانون العقوبات، دار نادى القضاة، مصر، ١٩٨٤، ص٥.

وقد وجدت العديد من النظريات التي تفسر العلاقة السببية، منها نظرية العامل الأقوى، الذي يساهم بقدر أكبر في وقوع النتيجة الإجرامية، ونظرية السببية المباشرة، التي تقتضي أن تكون النتيجة الإجرامية متصلة اتصالًا مباشرًا بسلوك الجاني، ونظرية تعادل الأسباب[١] التي أخذ بها المشرع العُماني، وأيًا كانت النظرية التي يمكن التعويل عليها في إسناد العلاقة السببية، دون الدخول في تفاصيلها فإنها تشكل عنصرًا من عناصر الركن المادي للجريمة، ومنها الجريمة السيبرانية.

الفرع الثاني

الركن المعنوي

الركن المعنوي يتعلق بالحالة النفسية للمتهم والعلاقة بينها وبين الفعل الذي ارتكبه يُعتبر الركن المعنوي محورًا أساسيًا في القانون الجزائي، حيث يتم من خلاله تحديد المسؤولية الجزائية للمتهم بناءً على عوامل مثل المعرفة والنية الإجرامية والقصد الجنائي، ويمكن تعريف الركن المعنوي بأنه العلاقة التي تربط بين الجاني والجريمة التي ارتكبها، حيث يُعتبر هذا العنصر جوهريًا في تحديد جوهر العقوبة والوقوع تحت طائلة التجريم والعقاب[٢].

والركن المعنوي للجريمة وفقًا لما نصت المادة (٣٣) من قانون الجزاء، هو:" العمد في الجرائم المقصودة، والخطأ في الجرائم غير المقصودة، ويتوفر العمد باتجاه إرادة الجاني إلى ارتكاب فعل أو الامتناع عن فعل متى كان هذا الارتكاب أو الامتناع مجرمًا قانونًا، وذلك بقصد إحداث نتيجة مباشرة أو أي نتيجة أخرى مجرمة قانونًا يكون الجاني قد توقعها وقبل المخاطرة بها، وتكون الجريمة عمدية كذلك إذا وقعت على غير الشخص المقصود بها، ويتوفر الخطأ إذا وقعت النتيجة الإجرامية بسبب خطأ الفاعل، أو عدم مراعاة القوانين أو الأنظمة"[٣].

---

[١] ماهر عبد شويش وآخرون، نظرية تعادل الأسباب في القانون الجنائي، دار ومكتبة الحامد للنشر، عمّان، ٢٠٠٠، ص١٩.

[٢] محمود نجيب حسني، النظرية العامة للقصد الجنائي، دار النهضة العربية، مصر، ط٢، ١٩٧١، ص٩٠.

[٣] قانون الجزاء الصادر بالمرسوم السلطاني رقم (٧ / ٢٠١٨)، الباب الثالث تقسيم الجرائم وأركان الجريمة، الفصل الثالث الركن المعنوي، المادة (٣٣).

ووفقًا للنص المتقدم فإن قيام الركن المعنوي لا يتوقف على الجرائم العمدية وحسب، وإنما يشمل جرائم الخطأ أو الجرائم غير العمدية، وهي جرائم محصورة في بنص القانون ومنها على سبيل المثال: جرائم القتل وإحداث الحريق والإيذاء وإحداث كسرًا أو إتلافًا أو نحو ذلك بالمرافق العامة، والتسبب في نقل عدوى مرض متلازمة العوز المناعي المكتسب، والتسبب في موت أو إيذاء حيوان أو طير مملوك للغير[١]، وهو ما تناولته المحكمة العليا في قولها: "الجرائم غير العمدية يتوقف تحققها على توافر ثلاثة أركان هي الخطأ والضرر والرابطة السببية بين ركن الخطأ والضرر، والخطأ الذي يقع من الأفراد عمومًا في الجرائم غير العمدية يتوافر متى تصرَّف الشخص تصرفًا لا يتفق والحيطة والحذر اللذين تقضيان بهما ظروف الحياة العادية وبذلك فهو عيب يشوب مسلك الإنسان لا يأتيه الفرد العادي المتبصر الذي أحاطت به ظروف خارجية مماثلة للظروف التي أحاطت بالجاني مرتكب الخطأ، وأما الضرر فهو الأثر الخارجي المترتب على الخطأ المعاقب عليه، وأما رابطة السببية وهي ركن من أركان هذه الجريمة فيجب أن تتوافر بين خطأ الجاني والضرر، وتتطلب إسناد النتيجة إلى خطأ الجاني ومساءلته عنها طالما كانت تتفق والسير العادي للأمور"[٢].

من المتفق عليه فقهًا وقضاءً يستلزم لقيام الجريمة وجود ركنًا معنويًا، وهو ما دعا جانبًا من الفقه إلى القول بأنه لا توجد مسؤولية ما لم يتوفر القصد[٣]، فإذا انتفى هذا الركن المعنوي انتفت معه الجريمة العمدية[٤]، وهذا الركن المعنوي هو الإثم الذي يدور في نفس الجاني، وهو ما دعا المفكر (Edward Coke) إلى القول بأنه لا يكون الفعل إثمًا إلا إذا كانت النفس آثمة[٥]، وتشكل الجريمة عدوانًا على المجتمع عندمًا تكون جميع العناصر المادية للجريمة مرتكبة عن عمد[٦].

---

[١] المواد (١٥٨، ١٦٦، ٣١٢، ٣٢١، ٣٧٣) من قانون الجزاء الصادر بالمرسوم السلطاني رقم (٧/ ٢٠١٨).

[٢] الطعن رقم ١١٢٩ / ٢٠١٧ الصادر عن الدائرة الجزائية جلسة ١٠ / ٠٤ / ٢٠١٨، مجموعة الأحكام الصادرة عن الدائرة الجزائية بالمحكمة العليا والمبادئ المستخلصة للسنتين القضائيتين السابعة عشر والثامنة عشر.

[3] Hosni, M .N ., L' Erreur de droit et son influence sur la responsabilité pénale, Rev . Sc . Crim ., Vol . 4, 1999, p .711 .

[٤] أشرف توفيق شمس الدين، المسئولية الجنائية والركن المعنوي للجريمة، الضوابط الدستورية لنصوص التجريم والعقاب في قضاء المحكمة الدستورية العليا، مجلة الدستورية، العدد (١٤)، مصر، ٢٠٠٨، ص١.

[5] Bonne, R ., Coughlin, A .M ., Jeffries, J ., and Peter, L ., Criminal Law, 2 *ed* ed ., New York, 2004, p .170.

[٦] طارق سرور، الوجيز في قانون العقوبات، القسم الخاص، جرائم الاعتداء على الأشخاص، مطبوعات جامعة القاهرة، القاهرة، ٢٠٠٩، ص٣١.

يكون القصد الجنائي موجودًا لدى الجاني في ثلاث حالات[١]:

- **الحالة الأولى:** عندما يكون الجاني يتوقع ويرغب في أن يترتب على فعله أو امتناعه حدوث الضرر أو الخطر الذي ينص عليه القانون.
- **الحالة الثانية:** عندما ينجم عن الفعل أو الامتناع ضرر أو خطر أكبر مما كان يقصده الجاني، وينص القانون صراحة على إمكانية ارتكاب هذا النوع من الجرائم.
- **الحالة الثالثة:** عندما يربط القانون الفعل بالفاعل نتيجة لفعله أو امتناعه، حيث يفترض القانون توافر القصد الجنائي لدى الجاني افتراضًا، ويُفترض أنه طالما تم إحداث النتيجة الجسيمة نتيجة لفعل الجاني، فإنه يجب أن يتحمل نتائج هذا الفعل، سواءً كان متوقعًا أم لا.

وتكمن أهمية القصد الجنائي في كونه يدخل في تركيب البنيان القانوني للجريمة، وركن أساسي فيها، وعبر المشرع الفرنسي عن أهمية القصد الجنائي في المادة (٣/١٢١) من قانون العقوبات بقوله " لا توجد جناية أو جنحة ما لم يكن هناك قصد على ارتكابها"[٢].

وترجع أهمية القصد الجنائي إلى أنه وسيلة القانون في تحديد الأفراد الذين ينزل بهم العقوبة، وتتحقق غايته في الردع العام والخاص[٣]، ولإدانة المتهم بالجريمة يجب التزامن بين ارتكاب الفعل وبين القصد الجنائي، فإذا انتفى القصد الجنائي انتفى العمد، وجاز معاقبة المتهم عن جريمة غير عمدية[٤]، بالإضافة إلى كونه معيارًا لتقييم السلوك الإجرامي تقييمًا نهائيًا، ويعد القصد الجنائي وسيلة لتحديد العقوبة وشدتها باعتباره مؤشرًا لدرجة ونوعية الإرادة الآثمة لدى الجاني[٥].

ومن ثم يمكننا القول بأن القصد مؤشرًا يكشف عن نفسية إجرامية آثمة، يمكن للمحكمة استخدامه في تقدير العقوبة الموقعة، كما يعد ضابطًا لتقسيم الجرائم ما بين جرائم عمدية وأخرى غير عمدية.

---

[١] محمد الجبور، مرجع سابق، ص٢٣٨.

[2] Act no . 1996-393 of 13 May 1996 Article 1 Official Journal of 14 May 1996; Act no . 2000-647 of 10 July article 1 Official Journal of 11 July 2000.

[٣] أشرف توفيق شمس الدين، مرجع سابق، ص٣.

[4] Duff, R .A ., Intention, agency and criminal liability, Basil Blackwell, 1989, p .8.

[٥] عبد الله محمد كريرى، الركن المعنوي في الجرائم المعلوماتية في النظام السعودي، دراسة تأصيلية، رسالة لنيل درجة الماجستير، جامعة نايف للعلوم الأمنية، السعودية، ٢٠١٣، ص٩٣.

ويمكن استخلاص قصد الفرد من سلوكه، فإذا استخدم الجاني سكين للقتل أو إحداث عاهة مستديمة، وفى ظل غياب ظروف أخرى، فإن النتيجة التي يمكن استخلاصها هي أنه قد ارتكب جريمة القتل عن علم وإرادة[١].

وبسبب أهمية القصد الجنائي باعتباره ركنًا من أركان الجريمة عرفه المشرع العُماني وفقًا للمادة (٣٣) من قانون الجزاء بأنه:" اتجاه إرادة الجاني إلى ارتكاب فعل أو الامتناع عن فعل، وذلك بقصد إحداث نتيجة مباشرة أو أي نتيجة أخرى مجرمة قانونًا يكون الجاني قد توقعها وقبل المخاطرة بها"[٢].

وفي ذلك قالت المحكمة العليا: " إن الركن المعنوي يتمثل في القصد الجنائي العام في جريمة السب والقذف وليس الخاص، كون المشرع لم يتطلب القصد الخاص وبالتالي يكفي لتوافر القصد الجنائي أن تتجه إرادة الجاني إلى استخدام الشبكة المعلوماتية أو سائل تقنية المعلومات في نشر عبارات تحمل معنى السب والقذف حتى ولو لم تتجه إرادته إلى الإهانة أو تشويه السمعة أو المساس بالغير طالما أقدم على الفعل بإرادة صحيحة مختارة غير مشوبة بإكراه"[٣].

وأخيرًا، فقد أثار البعض تساؤلًا بشأن أثر الباعث على القصد الجنائي في الجرائم السيبرانية؟

وخلال الإجابة على هذا التساؤل فقد انقسم الرأي إلى اتجاهين:

- **<u>الاتجاه الأول</u>**: ويرى أنصاره أنه لا ارتباط بين القصد الجنائي وبين الباعث، وهو ما عبرت عنه المحكمة العليا بقولها: "يقوم الركن المعنوي في جنحتي استخدام وسائل تقنية المعلومات في نشر وتوزيع ما من شأنه المساس بالنظام العام وإهانة الموظفين على عنصرين العلم والإرادة المتجهين

---

(1) Lydon, M , Criminal law - rehabilitation, A Thesis; punishment, the Antithesis - Insanity Defense in the Balance, De Paul Law Review, Vol ., 140, 1969, p .142 .

(٢) كما عرف المشرع اللبناني وفقًا للمادة (١٨٨) من قانون العقوبات " بأنها إرادة ارتكاب الجريمة على ما عرفها القانون، وبينت المادة (١٨٩) من ذات القانون أن " الجريمة تعد مقصودة وإن تجاوزت النتيجة الإجرامية عن الفعل أو عدم الفعل إذا كان قد توقع حصولها فقبل بالمخاطرة".

(٣) الطعن رقم ٦٦١/ ٢٠١٦ الصادر عن الدائرة الجزائية جلسة ٠٧/ ٠٣/ ٢٠١٧، مجموعة الأحكام الصادرة عن الدائرة الجزائية بالمحكمة العليا والمبادئ المستخلصة منها للسنتين القضائيتين السابعة عشر والثامنة عشر.

إلى عناصر الجريمة، وإن جريمة إهانة الموظف يستقيم ركنها المعنوي بتعمد الجاني توجيه تلك الألفاظ التي تحمل بذاتها معنى الإهانة إلى الموظف بغض النظر عن الباعث"[١].

- **<u>الاتجاه الثاني</u>:** يرى أن الباعث يرتبط ارتباطا وثيقًا ولا يقبل التجزئة بالقصد الجنائي، وذلك استنادًا إلى كون الباعث هو الذي يشكل القصد الجنائي في ذهن الإنسان فيدفعه إلى ارتكاب الجريمة، واستدل أنصار هذا الاتجاه بمثال الفقير الذي يسرق ليأكل، فإن باعث الجوع والحاجة هو الذي دفعه إلى السرقة، والتي هي من الجرائم العمدية، التي يشترط لارتكابها توفر القصد الجنائي[٢].

وفي ذلك فإن الباحث يساير موقف المشرع العُماني، الذي نص صراحة على عدم الاعتداد بالباعث على ارتكاب الجريمة ما لم ينص القانون على خلاف ذلك، طبقًا للمادة (٣٦) من قانون الجزاء.

ويلزم لقيام القصد الجنائي العلم اليقيني لدى الجاني بكافة الوقائع المادية المكونة للجريمة، لا ظني أو افتراضي[٣]، وهو ما يتطلب الرجوع إلى وقائع كل جريمة على حدة واستخلاص ما يُعد داخلًا في بنيانها وما لا يعد كذلك[٤]، والأصل العام هو انصراف العلم إلى كل واقعة يقوم عليها كيان الجريمة، ذلك أن القصد الجنائي يعنى اتجاه الإرادة الواعية إلى الجريمة في كل أركانها وعناصرها، فإذا تطلب القانون العلم بواقعة لتوفر القصد الجنائي، فمعنى ذلك أن الجهل أو الغلط المتعلق بها نافٍ لهذا القصد، وبالتالي لا يسأل الجاني عن فعله، فالجهل بهذا النوع من الوقائع أو الغلط فيها يعد جهلًا أو خطأ جوهري ينتفى به القصد الجنائي[٥].

وتوافر الركن المعنوي فيما يتعلق بالجرائم السيبرانية يعتبر أمرًا بالغ الأهمية لتحديد طبيعة سلوك المتهم وضبطه بما يتناسب مع التكييف القانوني الصحيح، على سبيل المثال يُعتبر التمييز بين

---

[١] الطعن رقم ٩٩٩ /٢٠١٥م جزائي عليا (أ) جلسة ٠٥ / ٠١ / ٢٠١٦، مجموعة الأحكام الصادرة عن الدائرة الجزائية بالمحكمة العليا والمبادئ المستخلصة منها في الفترة للسنتين القضائيتين الخامسة عشر والسادسة عشر.

[2] Bangara, A., Bangara, A., Determinisim and the annihilation of mens rea, Nimera University Law Journal, Vol. 4 (1), 2014.p 39-40.

[٣] أشرف توفيق شمس الدين، مرجع سابق، ص١٧.

[٤] أحمد عوض بلال، م مرجع سابق، ص٦٧٠.

[٥] أحمد شوقي أبو خطوة، مرجع سابق، ص٢٠٩.

الاختراق غير المشروع لنظام معالجة البيانات وبين جريمة تجاوز الصلاحيات في الوصول إلى هذا النظام تمييزًا دقيقًا[١].

في جريمة تجاوز الصلاحيات في الوصول إلى الشبكات أو الأنظمة، ينبغي لتوافرها أن يكون للشخص صلاحية للوصول إلى نظام محدد، ولكن يجب أن تكون هناك أنظمة داخل هذا النظام تمنع الوصول إليها بدون صلاحية، وعندما يقوم المتهم بالوصول إليها بالفعل، يُعد ذلك جريمة تجاوز الصلاحيات، في هذه الحالة يكون هناك متهم يمتلك صلاحية الوصول إلى النظام الأساسي، ولكنه لا يمتلك صلاحية الوصول إلى الأنظمة الفرعية داخله[٢].

ونتيجة لذلك فإن القضاء في الولايات المتحدة لم يصل إلى تحديد دقيق بشأن بعض الجرائم السيبرانية حول ما إذا كانت تتطلب قصد عامًا أم خاصًا، فعلى الرغم من أن بعض الجرائم مثل جريمة التهديد قد يتطلب وجودها قصد جنائي خاص، إلا أنه يتم الاعتراف من جديد بأن القصد العام قد يكفي في بعض الحالات، مثل جريمة التهديد عبر البريد الإلكتروني والمجموعات الإخبارية، حيث يتم استنتاجه من خلال التحليل الموضوعي للسلوك الشخصي للمتهم والظروف المحيطة بالجريمة، بما في ذلك فحص الحالة العقلية للمتهم[٣].

أما في القضاء الفرنسي، يسود مفهوم سوء النية في النصوص فيما يتعلق بالجرائم السيبرانية، بمعنى القصد الخاص ونية إلحاق الضرر[٤]، وبالمثل يتبنى المشرع البريطاني مفهوم الركن المعنوي في الجرائم السيبرانية، ولتحقق الركن المعنوي يجب أن يكون لدى الجاني نية واضحة للدخول إلى البيانات أو المعلومات المخزنة على أي حاسوب، فعلى سبيل المثال تعتبر جريمة بموجب المادة الأولى من قانون إساءة استخدام الحاسوب البريطاني لعام ١٩٩٠ أي دخول غير مصرح به إلى النظام الإلكتروني، وكذلك تُعد جريمة بموجب المادة الثانية من نفس القانون أي دخول غير مصرح به إلى النظام الإلكتروني بهدف ارتكاب جريمة أخرى[٥].

---

[١] روان بنت عطية هللا الصحفي، مرجع سابق، ص٣٠.

[٢] روان بنت عطية هللا الصحفي، المرجع السابق، ص٣١.

[٣] خالد ممدوح إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص١٠٩.

[٤] مصطفى محمد موسى، دليل التحري عبر شبكة الإنترنت، دار الكتب القانونية، مصر، ٢٠١٠، ص١٤٣.

[٥] سامي الرواشدة وأحمد الهياجنة، مكافحة الجريمة المعلوماتية بالتجريم والعقاب المجلة الأردنية في القانون والعلوم السياسية، جامعة مؤتة، المجلد (١)، العدد (٣)، الأردن، ٢٠٠٩، ص١٢٨.

المطلب الثاني

الطبيعة الخاصة لارتكاب الجريمة السيبرانية

في عصر الرقمنة المتسارع، يشهد العالم زيادة كبيرة في حجم البيانات وتعقيد الأنظمة الرقمية، مما جعلها عرضة لمختلف أنواع الهجمات السيبرانية، تتنوع هذه الهجمات بين الاختراقات الإلكترونية المتطورة والاحتيال الإلكتروني الذكي، مما يتطلب استراتيجيات أمنية متعددة الأوجه لحماية الأفراد والشركات والحكومات من التهديدات السيبرانية.

إضافة إلى ذلك، يمكن أن تكون الأطراف المشاركة في الجرائم السيبرانية متنوعة ومتعددة الأشكال، حيث تشمل المخترقين والقراصنة والمحتالين السيبرانيين بجانب الموظفين السابقين أو الحاليين وحتى الحكومات والمنظمات الاستخبارية.

ومن الضروري إدراك الأساليب والتقنيات المستخدمة لارتكاب الجرائم السيبرانية، والأشخاص القائمين عليها، لوضع الأدوات التشريعية لمكافحتها، لذا سوف يتم تقسيم هذا المطلب إلى فرعين: الأول حول وسائل ارتكاب الجرائم السيبرانية، والثاني حول أطراف الجرائم السيبرانية.

الفرع الأول

وسائل ارتكاب الجريمة السيبرانية

يتمتع المجتمع الرقمي بمزايا هائلة في التواصل والتبادل والوصول إلى المعلومات بسرعة وسهولة، ومع ذلك فإن هذا الانتشار الواسع للتكنولوجيا يفتح الباب أمام الجرائم السيبرانية التي تستهدف الضعف في الأمن الرقمي.

ويستخدم المجرم السيبراني تقنية الاختراق لتنفيذ جريمته وذلك من خلال التحايل على الأنظمة المعلوماتية، فيكون الاختراق بالقدرة على وصول هدف معين عن طريق ثغرات في نظام الحماية الخاصة، وتتم عن طريق برنامجين الأول الخادم وهو بجاهز الضحية إذ ينفذ المهام الموكلة إليه، والثاني يوجد بجهاز المخترق ويسمى بالبرنامج المستفيد كما أنهم يستخدمون برامج عدة[1].

---

[1] محمد أمين البشري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، ط١، ٢٠٠٤، ص٩٤.

وتجدر الإشارة إلى أن وسائل ارتكاب الجرائم السيبرانية تتنوع بشكل كبير، فالنشاط أو السلوك المادي في هذه الجرائم يتضمن عادةً استخدام بيئة رقمية وجهاز كمبيوتر، واتصال بشبكة الإنترنت، بالإضافة إلى معرفة أدواتها وكيفية تنفيذها ونتائجها، فقد يقوم الفاعل بتجهيز الحاسوب لتحقيق هدف الجريمة، سواءً من خلال تحميل برامج اختراق جاهزة أو إعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلى إعداد صفحات تحمل محتوى مخل بالأخلاق العامة وتحميلها على الجهاز المستهدف، أو إعداد برامج فيروسية للنشر، ولا يشترط وجود عمليات تحضيرية واضحة، حيث يصعب في بعض الأحيان التمييز بين العمل التحضيري وبدء التنفيذ، ورغم أن القانون قد لا يعاقب على الأعمال التحضيرية، إلا أنه في مجال تكنولوجيا المعلومات، قد تعتبر بعض الأفعال كجرائم في حد ذاتها، مثل شراء برامج اختراق أو فك الشفرات وكلمات المرور، أو حيازة مواد إباحية تمثل جريمة بحد ذاتها[١].

بمطالعة قانون مكافحة جرائم تقنية المعلومات نجد أن نص المادة (١٢) منه[٢] قد جرمت "استخدم وسائل تقنية المعلومات في ارتكاب جريمة تزوير معلوماتي، وذلك بتغيير الحقيقة في البيانات أو المعلومات الإلكترونية بالإضافة أو الحذف أو الاستبدال بقصد استعمالها كبيانات أو معلومات إلكترونية صحيحة تكون مقبولة قانونًا في نظام معلوماتي بهدف تحقيق منفعة لنفسه أو لغيره أو إلحاق ضرر بالغير".

ولذلك فإن السلوك الإجرامي في هذه الجريمة يقوم بكل عمل ما من شأنه تحريف أو تزوير أو إرباك نظام معالجة البيانات[٣] التي تحتوي عليها التوقيع أو الوسيط أو المحرر الإلكتروني واستعمال البيانات والمعلومات الإلكترونية[٤] وبيان ذلك بالوسائل الآتية:

---

[١] عبد الفتاح حجازي، صراع الكمبيوتر والانترنت، مرجع سابق، ص١١٣.

[٢] الفصل الرابع، التزوير والاحتيال المعلوماتي، قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم (١٢ / ٢٠١١).

[٣] مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، ٢٠٠١، ص٥٤.

[4] ALAN BENSOUSSAN, INTERNET, Aspect Juridique, HERMES,1996, P. 109.

أولًا: وسائل تباطؤ أو ارباك عمل النظام:

في العالم المتصل بالإنترنت، أصبحت الأنظمة الرقمية للشركات والحكومات والأفراد عرضة لمخاطر متزايدة من هجمات الإنترنت التي تستهدف إعاقة وتباطؤ أو حتى تعطيل عمل هذه الأنظمة، ويُعَدّ تباطؤ أو ارباك عمل النظام من بين أكثر الاختراقات السيبرانية شيوعًا، حيث يهدف المهاجمون إلى خلق فوضى وتعطيل العمليات اليومية للمؤسسات والأفراد[١].

وقد يكون الاعتداء بمحو البيانات أو تعديلها لما أعدت له أو إفساد البرامج فلا تصلح للاستخدام، أو تغيير نتائجها عما كانت من المفروض أن تكون عليه في حالة صحتها، وقد ترد الإعاقة على برنامج من البرامج التي يحتويها النظام وليس على كل النظام[٢].

وقد جرم المشرع العُماني طبقًا لنص المادة (٨) من قانون مكافحة جرائم تقنية المعلومات "كل من اعترض عمدًا ودون وجه حق باستخدام وسائل تقنية المعلومات خط سير البيانات أو المعلومات الإلكترونية المرسلة عبر الشبكة المعلوماتية أو وسائل تقنية المعلومات أو قطع بثها أو استقبالها أو تنصت عليها".

ولم يشترط المشرع وسيلة معينة لحصول الإعاقة، فقد تكون بطريقة بإدخال فيروس على البرنامج أو تعديل كلمة السر أو تؤثر على كيفية أداء النظام لوظيفته، أو أعمال العنف المادية على أجهزة الحاسب وشبكة الاتصال وذلك عن طريق تخريبها بكسرها أو سكب مادة سائلة عليها أو أية مادة أخرى أو منع العاملين من الوصول إلى النظام[٣].

---

[١] طارق زين، الجريمة المنظمة العابرة للحدود الوطنية، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت، ط١، ٢٠١٧، ص١٥.

[٢] شيماء عبد الغنى، الحماية الجنائية للتعاملات الإلكترونية، اطروحة دكتوراه، كلية الحقوق جامعة المنصورة، مصر، ٢٠٠٥، ص١٤٩.

[٣] على عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات، الإمارات ٢٠٠٠، ص٥٦.

ويتحقق فعل الاعتراض كذلك بأي فعل يتســـبب في تباطؤ أو إرباك عمل النظام المعلوماتي الذي يتضمن التوقيع أو الوسيط أو المحرر الإلكتروني[١].

وعلى ذلك يمكن القول إن الجريمة التي نحن بصـددها في شـأن اعتراض أو تعطيل الوسـيط المعلوماتي تتحقق بأي عمل من شأنه إعاقة أو إفساد نظام التشغيل على نحو يؤدى إلى توقف النظام عن العمل بصفة دائمة أو مؤقتة[٢].

ثانيا: وسائل جعل النظام غير قادر على الاستعمال السليم:

وذلك بجعل النظام يعطى نتائج غير التي تلك كان من الواجب الحصـــول عليها[٣]، ومن وسائل التعطيل أو الإفساد استخدام القنبلة المعلوماتية[٤] أو استخدام البرامج التي تحمل فيروس يطلق عليه "حصـــان طروادة" وغير ذلك من الفيروســـات التي تؤثر على التوقيع أو الوســـيط أو المحرر الإلكتروني، بل إن الإفساد يمكن أن يتحقق عن طريق إتلاف بعض العناصر المادية في أي منهم[٥].

وقد جرمت المادة (٥٢) من قانون المعاملات الإلكترونية[٦] إجراء تعديل غير مرخص به في محتويات أي حاسـب آلي بقصـد إضـعاف فاعليته أو منع أو تعويق الدخول إلى أي برنامج أو بيانات محفوظة فيه أو إضـــعاف فاعلية ذلك البرنامج أو إضـــعاف الاعتماد على تلك البيانات أو التعديل بشطب البرامج والبيانات المخزنة أو إضافة بيانات أو برامج جديدة أو تعديلها.

---

(1) R .Gassin, informatique et libert repertorie, dalloz de droit penal, janiper, 1987, No . 522 .

(٢) أحمد حسام طه، مرجع سابق، ص٣٥١.

(٣) حسن إبراهيم، مرجع سابق، ص٦٥.

(٤) القنبلة المعلوماتية هو "مفهوم يستخدم لوصف حالة من الفوضى أو التشويش الناتجة عن إغراق الفرد أو المجتمع بكمية هائلة من المعلومات في وقت قصـير، بحيث يصـبح من الصـعب التفريق بين المعلومات الصـحيحة والمضـللة، في سياق الجرائم السيبرانية، القنبلة المعلوماتية يمكن أن تكون جزءًا من هجوم سيبراني يهدف إلى تعطيل النظام أو تشويش الرأي العام".

(٥) هدى حامد قشقوش، مرجع سابق، ص٩٥.

(٦) حيث نصـت المادة ٥٢ من قانون المعاملات الإلكترونية على أنه:" مع عدم الإخلال بأية عقوبة أشـد ينص عليها قانون الجزاء العُماني أو أي قانون آخر يعاقب بالسجن لمدة لا تتجاوز سنتين وبغرامة لا تتجاوز خمسة آلاف ريال عماني أو بإحدى هاتين العقوبتين كل من تسبب عمدًا في تعديل غير مرخص به في محتويات أي حاسـب آلي بقصـد إضـعاف فاعليته أو منع أو تعويق الدخول إلى أي برنامج أو بيانات محفوظة فيه أو إضعاف فاعلية ذلك البرنامج أو إضعاف الاعتماد على تلك البيانات إذا تم ذلك التعديل بإحدى الطرق الآتية:

أ . شطب أي برنامج أو بيانات محفوظة في الحاسب الآلي.

ب . إضافة أي برنامج أو بيانات إلى محتويات الحاسب الآلي.

ج . أي فعل يسهم في إحداث ذلك التعديل.

ويســتوي في هذه الجريمة أن يكون من شــأن نشــاط الجاني أن يؤدى إلى توقف النظام عن العمل بصورة دائمة أو مؤقتة، كما يستوي أن تكون الإعاقة أو الإفساد كلية أو جزئية [١].

كما جرم المشرع العُماني بموجب المادة (٣) من قانون مكافحة جرائم تقنية المعلومات الدخول عمدًا بدون وجه حق موقعًا إلكترونيًا أو نظامًا معلوماتيًا أو وســائل تقنية المعلومات أو جزءًا منها أو تجاوز الدخول المصرح به إليها أو استمر فيها بعد علمه بذلك.

وفي كاليفورنيا قضت المحكمة بمعاقبة أحد خبراء الحاسب الآلي بتهمه الدخول غير المشروع على قاعدة بيانات المستندات الإلكترونية المخزنة لطلاب جامعة كاليفورنيا وتوصل من خلال ذلك إلى فك شــفرة ورموز البيانات الخاصــة، تمهيدًا لاســتخدامها على نحو غير مشــروع، ومن خلال تلك المعلومات التي تم تمريرها إلى متهم آخر والذي كان يقيم خارج تلك الولاية تمكن هذا الأخير من الدخول على الموقع الإلكتروني للمؤتمر الصومالي وتدميره، كما تمكن من الاستيلاء على مبالغ ماليه طائلة من خلال برنامج يســتطيع اختراق نظام الأمن الإلكتروني للموقع وتدمير البيانات الموجودة به، ثم أنشأ لنفسه حسابًا بالبريد الإلكتروني ليتم تحويل المبالغ من ضحاياه مقابل عدم إتلاف بياناتهم أو إفشــائها [٢]، كما يتحقق الركن المادي لهذه الجريمة إذا قام الجاني بأحد أفعال الإدخال أو المحو أو التعديل للمعطيات الموجودة داخل أنظمة معالجة البيانات الخاصة بمواقع الإنترنت[٣].

ويقوم الركن المعنوي في جريمة اختراق أو إعاقة أو تعطيل نظام التوقيع أو الوسيط أو المحرر الإلكتروني على القصــد الجنائي العام بركنيه العلم والإرادة ، فيجب أن تتجه إرادة الجاني إلى اختراق أو إعاقة أو تعطيل التوقيع أو الوسيط أو المحرر الإلكتروني، وأن يعلم أن نشاطه غير مشروع وأنه يعتدي على صــاحب ذلك التوقيع أو الوســيط أو المحرر الإلكتروني محل الاعتداء، ولا تتطلب هذه الجريمة قصدًا جنائيًا خاصًا مثل قصد الإضرار بالغير[٤]؛ ولذلك إذا قام الشخص الذى يتعامل مع

---

[١] مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص٥٤.

[2] U .S . Department of Justice Central District of California Debra Wong Yang United States Attorney Thom Mrozek, Public Affairs Officer.

[٣] أحمد حسام طه تمام، مرجع سابق، ص٣٥١.

[٤] عبد الفتاح حجازي، التوقيع الإلكتروني في النظم المقارنة، دار الفكر الجامعي، الإسكندرية، ٢٠٠٤، ص١٣٣.

النظام بصورة مشروعة بإعاقة أو إفساد النظام نتيجة لخطأ في التشغيل أو التعامل مع البيانات، ينتفى القصد الجنائي لديه ولا يسأل عن هذه الجريمة[١].

ثالثا: وسائل بث ونشر معلومات وبيانات ضارة:

ويتم البث من خلال الوسائل المختلفة سواء كان عبر القنوات التليفزيونية أو عبر الإنترنت، وهي الوسيلة الغالب استخدامها في هذه الجريمة، نظرًا للقيود المفروضة على البث التلفزيوني، إضافة لما يحققه الإنترنت من سرعة وصول تلك الفيديوهات المفبركة، ووصولها إلى عدد كبير من المشاهدين، فضلًا عن صعوبة إزالة هذا المحتوى الإلكتروني، وهو ما يجعل النشر على الإنترنت أكثر تأثيرًا في النتيجة الإجرامية المتحققة[٢].

وقد عرف المشرع العُماني "وسيلة تقنية المعلومات" وفقًا للمادة (١/ و) من قانون مكافحة جرائم تقنية المعلومات بأنها "جهاز إلكتروني يستخدم لمعالجة البيانات والمعلومات الإلكترونية أو تخزينها أو إرسالها أو استقبالها كأجهزة الحاسب الآلي وأجهزة الاتصال، كما جرم استخدام الشبكة المعلوماتية أو وسائل تقنية المعلومات في إنتاج أو بيع أو شراء أو استيراد أو توزيع أو عرض أو إتاحة برامج أو أدوات أو أجهزة مصممة أو مكيفة لأغراض ارتكاب جرائم تقنية المعلومات أو كلمات سر أو رموز تستخدم لدخول نظام معلوماتي، أو حاز أدوات أو برامج مما ذكر، وذلك بقصد استخدامها في ارتكاب جرائم تقنية المعلومات".

---

(1) ABA Section Creates First Digital- Signature Guidelines To Aid In Security of The Internet, 1996.

(2) Isabelle Lolies, La protection pénale de la vie privée, Presses Universites d´Aix-Marseille, 1999, p.104.

الفرع الثاني

أطراف الجريمة السيبرانية

تلعب الأطراف المتورطة في الجرائم السيبرانية دورًا حاسمًا في تكوينها، وتشمل هذه الأطراف الجاني الذي قد يكون فردًا أو مجموعة أو منظمة، والمجني عليه الذي قد يكون شخصًا أو مؤسسة أو حتى دولة بأكملها، كما قد تتضمن أطرافًا أخرى مثل الوسطاء أو المتواطئين الذين يُسهمون في تنفيذ الجريمة أو تسهيلها، ويختلف دور كل طرف باختلاف نوع الجريمة وطبيعتها، مما يضيف أبعادًا متعددة إلى كيفية فهم الجرائم السيبرانية والتعامل معها قانونيًا وتقنيًا، وتحليل هذه الأطراف يساعد في تحديد المسؤوليات وتطوير استراتيجيات فعالة لمكافحة هذه الجرائم وحماية الضحايا.

لا بد للجريمة السيبرانية كغيرها من الجرائم أن يكون لها فاعل ومجني عليه، وسيتم تناولها بشيء من التفصيل على النحو التالي:

أولًا: الفاعل في الجريمة السيبرانية

بالإضافة إلى الشروط العامة التي يجب توافرها في مرتكب الجرائم السيبرانية، مثل السلوك المنحرف والعلم بنتائج هذا السلوك، يجب أن يكون هذا الشخص لديه معرفة وخبرة عملية محددة في مجال تقنية المعلومات وعلوم الحاسوب، وقد وُصف بعض هؤلاء الأشخاص بأنهم "المجرمين الإلكترونيين" أو "المجرمين المعلوماتيين[١].

بهذا فإنه لا يُمكن تصور أن يكون الجاني في الجرائم السيبرانية سوى شخصًا طبيعيًا، يمتلك القدرة والكفاءة لتحمل العواقب القانونية وتنفيذ العقوبة، وهو الأمر الذي لا ينطبق إلا على الأفراد الطبيعيين دون الأشخاص الاعتباريين، ويكون ذو خبرة ومعرفة في مجال علوم الحاسوب، سواء كان مستخدمًا عاديًا أو مبرمجًا أو مهوسًا بالتقنية، أو حتى محترفًا في جرائم الحاسوب وتقنية المعلومات[٢].

---

[١] محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، ١٩٩٤، ص٥١٧.

[٢] وليد الزيدي، القرصنة على الإنترنت والحاسوب، دار أسامة للنشر، عمّان، ط٣، ٢٠٠٩، ص٥٤.

المجرم السيبراني يتميز بمجموعة من الصفات والخصائص، منها: يتمتع بالمهارات والمعرفة والذكاء، وهو أيضًا شخص اجتماعي، يعمل على تبرير جريمته ويخشى كشفها في الوقت نفسه، بالإضافة إلى ذلك يتحلى الفاعل في هذه الجرائم بالسلطة على النظام الإلكتروني[١].

فالقراصنة السيبرانيون هم أفراد يتمتعون بقدرات فائقة في الإنترنت ومهارات عالية في التحكم بتقنيات المعلومات، يستغل هؤلاء الأفراد هذه القدرات لاختراق الشبكات وكسر كلمات المرور، حيث يسعون للاستيلاء على بيانات ومعلومات قيمة من الأجهزة المتصلة بالشبكات، ويقومون بتجوالهم في عالم الإنترنت بهدف جمع كل ما هو غالٍ وثمين، مما يشمل البيانات الحساسة والمعلومات المهمة التي يمكن العثور عليها على أجهزة الحواسيب المتصلة بالشبكات[٢].

ويتميز المجرم السيبراني أيضا بالعودة المستمرة للإجرام، حيث يستفيد من مهاراته وخبرته في مجال تكنولوجيا المعلومات وفهمه العميق لكيفية عمل الأجهزة وتخزين البيانات فيها، بالإضافة إلى قدرته على التحكم في أنظمة الشبكات، وعلى الرغم من أنه قد لا يقوم بارتكاب الجرائم بهدف الإيذاء أو سرقة البيانات دائمًا، إلا أنه يعتبر نوعًا من أنواع التحدي، حيث يهدف إلى اختبار مهاراته واستمرار تطويرها، وخاصة في حالة عدم القبض عليه[٣].

كذلك يتمتع بمهارات استثنائية ومعرفة عميقة بتقنيات الحاسوب والإنترنت، ومن بينهم الخبراء في مجال معالجة المعلومات آليًا، فهؤلاء المجرمون يتمتعون بمستوى عالٍ من الاحترافية في تنفيذ جرائمهم، ويسعون للتغلب على العقبات التي تواجههم من خلال الخبراء والمبرمجين الذين يحاولون حماية أنظمة الكمبيوتر، وهذا يظهر بوضوح في حالات الاختراق التي تطال البنوك والمؤسسات العسكرية ومواقع الحكومات[٤].

---

[١] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، ٢٠١٣، ص٤٧.

[٢] مليكة عطوي، الجريمة المعلوماتية، حوليات جامعة الجزائر، العدد ٢١، الجزائر ٢٠١٢، ص١٣.

[٣] عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، دار الكتب والوثائق المصرية، مصر، ٢٠٠٢، ص٤٥.

[٤] فتيحة رصاع، الحماية الجنائية للمعلومات على شبكة الأنترنت، رسالة لنيل درجة الماجستير، جامعة أبي بكر بلقايد، كلية الحقوق والعلوم السياسية، الجزائر، ٢٠١١ – ٢٠١٢، ص٥١

ويتمتع المجرم السـيبراني بذكاء فائق ونظرة غير تقليدية تجاه الجريمة، إذ يتمتع غالبًا بدرجة عالية من الذكاء المعلوماتي، بما يمكنه من تعديل وتطوير الأنظمة الأمنية بشـكل متقن، ويهدف إلى تجنب ملاحقته وتتبع أنشـطته الجرمية عبر الشـبكات وداخل أجهزة الحواسـيب، ويعتمد تحديد أنواع الجرائم التي يرتكبها على العديد من العوامل، من بينها مدى تطور وتعقيد الأنظمة التي يسـتهدفها وقدرته على التكيف مع التغيرات التكنولوجية الجديدة[١].

ويمكن تصنيف مرتكبي الجرائم السيبرانية، استنادًا إلى الدراسات السابقة في هذا المجال، إلى ثلاث فئات رئيسية:

الفئة الأولى: الموظفون العاملون في مجال تكنولوجيا المعلومات:

حيث يعمل النظام المعلوماتي كمجال أسـاسـي لهم، بفضـل مهاراتهم ومعرفتهم التقنية، قد يقترفون بعض الجرائم السيبرانية بهدف تحقيق مكاسب شخصية، بما في ذلك الربح المادي[٢].

الفئة الثانية: الحاقدون:

الذين يرتكبون أنشـطتهم الجرمية بدافع الرغبة في الانتقام والثأر، وينقسـم هؤلاء الأفراد إما إلى مسـتخدمي النظام الذين لهم علاقة مباشـرة بالنظام المسـتهدف، أو غرباء عن النظام ولديهم أسـباب شـخصـية للانتقام من الأفراد المسـتهدفين، على سـبيل المثال، يمكن أن يقوم بعضـهم بمسـح بعض المعلومات الخاصة بالشركة أو المؤسسة كوسيلة للانتقام منها لأسباب شخصية يعرفها المرتكب[٣].

الفئة الثالثة: القراصنة:

والمقصود بمصطلح "القراصنة" هم المتخصصون في مجال تكنولوجيا المعلومات الذين يسعون إلى اختراق الأنظمة المعلوماتية بطرق غير قانونية، هؤلاء الأفراد غالبًا ما يمتلكون مهارات برمجية

---

[١] عبد اللطيف معتوق، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، رسالة لنيل درجة الماجستير، جامعة العقيد الحاج لخضر بباتنة، الجزائر، ٢٠١١ – ٢٠١٢، ص١٦.

[٢] مليكة عطوي، مرجع سابق، ص١٣.

[٣] علي جعف، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشـخاص والحكومة، منشـورات زين الحقوقية، بيروت، ط١، ٢٠١٣، ص١١٧.

عميقة ويسعون لتجاوز الحواجز الأمنية المنصوص عليها لحماية تلك الأنظمة، ويمكن تصنيف القراصنة إلى فئتين رئيسيتين[١]:

١. القراصنة الهواة:

هم ذوو الاهتمام الشديد بمجال التكنولوجيا والحواسيب، وينطلقون من رغبة في التسلية والفضول والرغبة في الاطلاع والتعلم، يعتبرون اختراق الأنظمة المعلوماتية تحديًا لمهاراتهم الفردية، وغالبًا ما يكون لديهم دوافع غير تخريبية في بادئ الأمر، ومع ذلك قد تتحول هذه الأفكار إلى أعمال جرمية في بعض الأحيان بسبب عوامل مثل الضغط الاجتماعي أو التأثيرات السلبية[٢].

ومن سمات هذه الفئة من القراصنة هي اتجاههم لتبادل المعرفة والخبرات مع بعضهم البعض، ويتم ذلك عبر الإعلانات الإلكترونية والمنتديات ومجموعات الأخبار المخصصة لهذا الغرض، ويرى الهواة في هذا التبادل فرصة لتعزيز معرفتهم وتطوير مهاراتهم، ويتبادلون الأفكار والتقنيات لتحقيق ذلك الهدف[٣].

٢. القراصنة المحترفون:

المعروفين أيضًا "بالهاكرز"، يمثلون تهديدًا كبيرًا بالنسبة للأمن الرقمي، حيث يمتلكون المهارات والمعرفة اللازمة لتحقيق أهدافهم بدقة وفعالية، يفهمون تمامًا ما يريدون وكيفية الوصول إلى أهدافهم المحددة مسبقًا، ويستخدمون مهاراتهم ومعرفتهم التقنية لتنفيذ العمليات الإجرامية مثل سحب الأموال من الحسابات المصرفية واختراق المواقع الحساسة والتلاعب بالبيانات، سلوكيات هؤلاء القراصنة تظهر ميولًا إجراميًا واضحًا، حيث يظهرون رغبة واضحة في التخريب والسرقة والنهب، على الرغم من أن بعضهم قد يظهر تكيفًا اجتماعيًا وقد يبدو أنه عادي في المجتمع[٤].

ويتعين على سلطات مكافحة هذه الأنشطة الإجرامية مواكبة التقدم الرقمي، نظرًا لتعدد وتنوع الجرائم التي ترتكبها هذه الفئة وخطورتها[٥].

---

[١] يوسف صغير، الجريمة المرتكبة عبر الإنترنت، رسالة لنيل درجة الماجستير، جامعة مولود معمري بتيزي وزو، الجزائر،٢٠١٢ – ٢٠١٣، ص٢٦.

[٢] نائلة عادل محمد فريد قورة، مرجع سابق، ص٦١.

[٣] مليكة عطوي، مرجع سابق، ص١٣.

[٤] عبد الفتاح مراد، مرجع سابق، ص٠٤٧.

[٥] عبد اللطيف معتوق، مرجع سابق، ص١٦.

ثانيًا: المجني عليه في الجرائم الإلكترونية

بشكل عام، يكون مرتكب الجريمة الإلكترونية عادة شخصًا طبيعيًا، إلا أنه قد يكون المجني عليه شخصًا معنويًا مثل البنوك والشركات الكبرى والمؤسسات الحكومية والوزارات والمنظمات والهيئات المالية، وغيرها من الكيانات القانونية التي تعتمد على الحواسيب في إنجاز مهامها[١].

أدت الثورة المعلوماتية إلى ظهور المؤسسات المالية والمصرفية والتجارية العالمية التي تسعى بشكل دائم للتدخل المتنامي في الحياة الاقتصادية بشكل عام وحياة الأفراد بشكل خاص، وذلك بتسهيل إجراء معاملاتهم اليومية، ومساعدتهم على تخطي مخاطر حمل النقود، وتخطي إجراءات إصدار الأوراق التجارية وسهولة الحصول على الخدمات والوفاء بالمشتريات من مكان تواجدهم، بدون أن يبذلوا أي جهد أو عناء، وإذا كانت البيئة التجارية ومن ثم البيئة الاقتصادية تُعَرِّف النقود والأوراق التجارية باعتبارها الوسائل التي يتم بها ومن خلالها الوفاء بالمشتريات، فإن تلك المؤسسات قد ابتكرت وسائل للوفاء أكثر تقدمًا من الأوراق التجارية السائدة في البيئة التجارية، أو النقود السائدة في البيئة الاقتصادية، وهي بطاقات الوفاء المصرفية، التي يتم عن طريقها سداد أثمان المشتريات أو الحصول على الخدمات لحامليها إما بصورة فورية، وهذه هي بطاقات الوفاء الفوري، أو على شكل دفعات أو بعد مضي فترة وتلك هي بطاقات الائتمان[٢].

وفي السلطنة يشهد استخدام المواطنين لخدمات الحكومة الإلكترونية تطورًا ملحوظًا في السنوات الأخيرة، وذلك بفضل التحول الرقمي الذي تشهده البلد، وزيادة في عدد المواطنين الذين يستخدمون الخدمات الحكومية الإلكترونية للمعاملات المتعلقة بالتعليم والصحة والمالية والأعمال وغيرها من المجالات، ومن الملاحظ أن الحكومة العُمانية قد قامت بتطوير البنية التحتية الرقمية وتقديم خدمات إلكترونية مبتكرة لتلبية احتياجات المواطنين والمقيمين، وتشمل هذه الخدمات تسهيل إجراءات التسجيل، وتقديم الطلبات والدفع الإلكتروني[٣].

---

[١] محمد عبد الله قاسم، الحماية الجنائية للمعلومات الإلكترونية، دار الكتب القانونية، مصر، ط١، ٢٠١٠، ص١٤٨.

[٢] جلال محمد الزغبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الالكترونية دار الثقافة للنشر والتوزيع، عمّان، ط١، ٢٠١٠، ص٧٥.

[٣] نوال بنت علي بن عبدالله البلوشية، العوامل المساعدة على التحول الرقمي في سلطنة عُمان، الاتحاد العربي للمكتبات والمعلومات، العدد ٢٦، تونس، ٢٠٢٠، ص٤٨.

يمكن أن يتعرض الأفراد لأشـــكال مختلفة من الجرائم، ومن بينها الاعتداء على أســـرارهم التجارية أو شؤونهم الشخصية داخل أجهزتهم الحاسوبية، ولكي تتم الجريمة في هذا السياق يكون في الغالب المجني عليهم ضـمن الأفراد الذين يمكن أن يُجذبوا اهتمام الجناة، ومن أكثر الأشـخاص الذين ينجذبوا لهم الذين يشغلون مناصب سياسية رفيعة أو يتمتعون بشهرة عالمية في قطاعات اقتصادية أو اجتماعية أو عسكرية[١].

على الرغم من أن الجميع قد يتعرض للجرائم السـيبرانية، سـواء كانوا أشـخاصًـا معنويين أو طبيعيين، إلا أن معظم هذه الجرائم تُرتكب بهدفين رئيســـيين: المال والمعلومات. عليه يمكن القول إن المتضررين من الجرائم السيبرانية هم إما الأفراد أو المؤسسات المالية مثل البنوك والمصارف وشركات الصـرافة، أو شـركات معلومات بغض النظر عن نوعها أو قيمتها، والتي قد تكون تشـمل المعلومات العسكرية والسياسية، وقد تكون بسيطة مثل المعلومات الرياضية أو الفنية أو الاجتماعية[٢].

إن تحديد نطاق يضـــم جميع المتضـــررين في الجرائم الإلكترونية يعتبر أمرًا صـــعبًا بســـبب الطبيعة الخفية لهذه الجرائم، حيث يكتشف المتضـررون عادة الانتهاكات بعد وقوعها، مما يدفعهم إلى السـكوت والتسـامح معها، ويفضـلون عدم الإبلاغ عن اختراق أجهزتهم وانتهاك خصـوصـياتهم التي يعتبرونها آمنة وسرية، وهذا بحد ذاته يسهم في زيادة معدل الجرائم الإلكترونية وصـعوبة اكتشـافها أو الحد منها، مما يتسبب في تفاقم المشاكل على الصعيد القانوني والعملي[٣].

---

[١] محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية: دراسة مقارنة، دار الفكر والقانون، المنصورة، ط١، ٢٠١٧، ص٥٦.

[٢] محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مرجع سابق، ص١٥٨.

[٣] محمد سـليمان خوالدة، جريمة الدخول غير المشـروع إلى موقع إلكتروني أو نظام معلومات وفق التشـريع الأردني – دراسـة مقارنة، دار الثقافة، عمّان، ط١، ٢٠١٢، ص٥٠.

الفصل الثاني

المواجهة القانونية للجرائم السيبرانية في القانون العُماني

في عصر الرقمنة الذي نعيشه أصبحت الجرائم السيبرانية تشكل تحديًا متزايدًا على الصعيد العالمي، لذلك فإن السلطنة من الدول التي تسعى إلى تبني السياسات والتشريعات الرامية إلى مكافحة الجرائم السيبرانية وحماية المعلومات الرقمية والأمن السيبراني.

يتطلب التصدي للتحديات التي تطرحها الجرائم السيبرانية في السلطنة استراتيجية شاملة تشمل جوانب عدة، منها التشريع والتنفيذ الجزائي، ويُعتبر القانون من أبرز الأدوات التي تستخدم لمكافحة الجرائم السيبرانية، حيث يحتوي على تشريعات واضحة ومحددة تهدف إلى تحديد الجرائم وتحديد العقوبات المناسبة لمرتكبيها.

ويتناول الفصل الثاني من الدراسة استعراضًا لجهود السلطنة في مواجهة الجرائم السيبرانية على المستوى التقني والتشريعي، والإجراءات القانونية المتبعة في مكافحة هذه الجرائم في القانون العُماني، وذلك من خلال مبحثين: الأول يتناول الجهود الوطنية المتخذة في مواجهة الجرائم السيبرانية، وإبراز التدابير التي اتخذتها السلطنة على الصعيد الوطني لمكافحة الجرائم السيبرانية، بما في ذلك إنشاء الهيئات والأجهزة الخاصة بتعزيز الأمن السيبراني، وتطوير القوانين والتشريعات ذات الصلة، والثاني إجراءات مواجهة الجريمة السيبرانية وتحدياتها في القانون العُماني، وتسليط الضوء على التحديات التي تواجه هذه الإجراءات وكيفية التعامل معها بفعالية لضمان تحقيق العدالة وحماية المجتمع الرقمي في السلطنة.

المبحث الأول

الجهود الوطنية المتخذة في مواجهة الجرائم السيبرانية

في عصر التكنولوجيا الحديثة، واتساع استخدامها في كافة مناحي الحياة، أصبحت الجرائم السيبرانية تؤرق البشرية، وتتنوع هذه الجرائم بين اختراق الأنظمة الحاسوبية، وسرقة البيانات الشخصية، وتعطيل الخدمات الرقمية، مما يؤثر على أمن الدول واقتصادها وممارساتها اليومية، وبالتالي فإن مكافحة الجرائم السيبرانية باتت ضرورة ملحة تتطلب تعاونًا دوليًا وجهودًا مشتركة.

وتُعَدُّ الجرائم السيبرانية من أبرز التحديات التي تواجه السلطنة، حيث تتسبب في خسائر كبيرة تؤثر على الاقتصاد والأمن والاستقرار الوطني[١]، ومن أجل التصدي لهذه التحديات أصدرت السلطنة عدة تشريعات وعززت التعاون الدولي في هذا المجال[٢]، عليه سيتم في هذا المبحث استعراض الجهود الوطنية المتخذة في مواجهة الجرائم السيبرانية في السلطنة، من خلال مطلبين: الأول حول المواجهة التشريعية للجرائم السيبرانية والثاني المواجهة التقنية للجرائم السيبرانية.

المطلب الأول

المواجهة التشريعية للجرائم السيبرانية

تواجه جهود التشريع لمكافحة الجرائم السيبرانية تحديات كبيرة في العصر الرقمي، نتيجة للتقدم والتطور السريع لهذه التقنيات، على الرغم من أن القوانين والاتفاقيات الدولية وضعت القواعد والأحكام العامة لها، إلا أنها لم تتماشى بشكل كافٍ مع التطور التكنولوجي وتأثيره على هذا النوع من الجرائم، وتعتبر الجهود التشريعية أحد أهم السبل لمكافحة الجرائم السيبرانية، حيث تساهم في وضع الإطار القانوني الذي يحدد الأفعال المحظورة، وسيركز هذا المطلب على استعراض المواجهة التشريعية في

---

[١] صابرين جابر أحمد محمد، محمود بن علي بن سهيل المعشني، المواجهة الجنائية لجريمة الاحتيال الإلكتروني في التشريع العُماني، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، المركز الجامعي بأفلو، العدد (١٠)، مارس ٢٠٢٣، االجزائر، ص١٧١.

[٢] عبد الله بن على بن سالم الشبلي، الجريمة الالكترونية في سلطنة عُمان: التحديات والحلول القانونية، المركز القومي للبحوث، المجلد (٣)، العدد (٢)، غزة، ٢٠١٩م، ص٩٠.

فرعين الأول حول إصـدار القوانين العامة لمواجهة الجرائم السـيبرانية، والثاني سـيتناول إصـدار قانون مكافحة جرائم تقنية المعلومات، بصفته القانون الخاص بمواجهة الجرائم السيبرانية في السلطنة.

الفرع الأول

إصدار القوانين العامة لمواجهة الجرائم السيبرانية

يعتبر انتشـــار خدمة الإنترنت في الســـلطنة انطلاقة حديثة نحو الرقمنة والتكنولوجيا الحديثة، حيث تم إطلاق خدمة الإنترنت في البلاد عام ١٩٩٧م، ومنذ ذلك الحين شـــهدت البنية التحتية للإنترنت تطورًا ملحوظًا حيث بلغ عدد المشتركين في خدمة الإنترنت في نهاية عام ٢٠١٠م ما يقارب (٦٨٢٠١) مشترك، بينما بلغ عدد مشتركي خدمة الإنترنت المتنقل حوالي (١,٦٢٦,٨٩٦) مشترك في ذات الفترة، مما يوضح الانتشار الواسع للتكنولوجيا في البلاد واستخدامها المتزايد[١].

لمواجهة هذه التحديات، قامت السلطنة باتخاذ عدة إجراءات تهدف إلى تعزيز الأمن السيبراني وحماية المعلومات والأنظمة الحيوية للدولة[٢]، ومن تلك الإجراءات إصـــدار القوانين العامة لمكافحة الجرائم السيبرانية، ويتم استعراضها على النحو الآتي:

١. قانـــون الجـــزاء:

تم تعديل قانون الجزاء العُماني ليتناول جرائم الإنترنت، وذلك بموجب المرسوم السلطاني رقم (٢٠٠١/٧٢)، الذي أدخل تعديلات على القانون رقم (١٩٧٤/٧)، وتضـمنت هذه التعديلات إضـافة الفصل الثاني المكرر إلى الباب السابع ليتناول جرائم الحاسوب، وتم تضمين خمس مواد جديدة تعبر عن إرادة المشرع في مواجهة التطورات السريعة في تكنولوجيا المعلومات وشبكات الاتصال.

تم إلغاء الفصل الثاني مكرر من الباب السابع من قانون الجزاء العُماني السالف بيانة بموجب المادة الثانية من ديباجة المرسـوم السـلطاني رقم (١٢ / ٢٠١١) بإصـدار قانون مكافحة جرائم تقنية

---

[١] التقرير السنوي لهيئة تنظيم الاتصالات، ٢٠٠٩، ص٤٦.

[٢] خالد ظاهر عبدالله جابر السهيل المطيري، دور التشريعات الجزائية في حماية الامن السيبراني بدول مجلس التعاون الخليجي، مجلة البحوث الفقهية والقانونية، العدد ٣٨، مصر، ٢٠٢٢، ص١٠٤٤.

المعلومات، وبذلك أصـــبح قانون مكافحة جرائم تقنية المعلومات هو الإطار التشـــريعي الخاص الذي ينظم الجرائم السيبرانية في السلطنة.

في ١١ يناير ٢٠١٨م صـدر المرسـوم السـلطاني رقم (٧/ ٢٠١٨) بإصـدار قانون الجزاء، وألغى بموجبه قانون الجزاء العُماني الصادر بالمرسوم السلطاني رقم (٧ / ٧٤)، وخلا هذا القانون من تنظيم الجرائم السـيبرانية عدا المادة (٢٦٨) التي جرمت اسـتعمال أجهزة الاتصـالات السـلكية أو اللاسـلكية أو الوسـائط الإلكترونية أو أي وسيلة أخرى لنقل عبارات أو صور أو برامج منافية للآداب العامة أو الأخلاق[١].

يرى الباحث أن المشرع العُماني وفق في عدم إدراج الجرائم السيبرانية ضـمن قانون الجزاء، بصـفته قانون عام يحدد الأحكام العامة للجرائم والجزاءات، وأظهر بذلك المشرع حكمةً ووعيًا بطبيعة الجرائم السيبرانية وخصوصيتها، التي أحالها إلى القوانين الخاصة وفي مقدمتها قانون مكافحة جرائم تقنية المعلومات.

٢. قانون تنظيم الاتصالات الصادر بالمرسوم السلطاني رقم (٢٠٠٢/٣٠م):

عزز إصـدار قانون تنظيم الاتصـالات قطاع الاتصـالات وترسـيخ الشـفافية والثقة في البيئة التجارية، وصـدور لائحته التنفيذية بموجب القرار رقم (٢٠٠٨/١٤٤)[٢]، بالإضـافة إلى سـلسـلة من القرارات التنظيمية ذات الصلة التي تهدف إلى تعزيز المنافسة النزيهة وإيجاد بيئة مستقرة للاستثمار في قطاع الاتصالات بالبلاد.

فيما يتعلق بالجرائم السـيبرانية الواردة في قانون الاتصـالات فإنها تتنوع بين الأفعال المرتبطة بشبكة الإنترنت أو بسياقات أخرى للاتصالات الإلكترونية، وتتمثل في الآتي:

١. الاستخدام الخاطئ لأنظمة الاتصالات أو الأجهزة أو الوسائط بهدف توجيه رسالة معروفة بأنها غير صحيحة أو تسبب ضررًا لسلامة الأفراد أو لكفاءة الخدمة[٣].

---

[١] قانون الجزاء الصـادر بالمرسـوم السـلطاني رقم (٢٠١٨/٧)، نشـر هذا المرسـوم في ملحق عدد الجريدة الرسـمية رقم (١٢٢٦) الصـادر في ١٤ / ١ / ٢٠١٨م.

[٢] هيئة تنظيم الاتصالات، القرار رقم ١٤٤ / ٢٠٠٨ بإصدار اللائحة التنفيذية لقانون تنظيم الاتصالات.

[٣] نصـت المادة (٦٢) من قانون تنظيم الاتصـالات الصـادر بالمرسـوم السـلطاني رقم (٢٠٠٢/٣٠م) على أنه: " يعاقب بالعقوبة المنصـوص عليها في المادة (٦١) من هذا القانون كل شخص يستخدم أجهزة أو وسائل الاتصالات بقصد توجيه رسالة مع علمه بأنها غير صحيحة أو بأنها تتسبب في الإضرار بسلامة أي شخص أو بكفاءة أي خدمة".

٢. الاســـتخدام الغير المشـــروع للأجهزة الإلكترونية خارج الظروف المصـــرح بها من الجهات المختصــة، ســواء للحصــول على معلومات حول محتوى الرســائل أو المرســل أو المســتلم، أو للكشف عن سرية بيانات الرسائل، باستثناء الحالات المسموح لها بالكشف عن تلك البيانات وفقًا لأحكام القانون[١].

٣. إرسال رسالة تنتهك النظام العام أو الآداب العامة عبر الاتصالات مع العلم بهذا الانتهاك[٢].

تعتبر القضايا المتعلقة بالاحتيال في الحصول على خدمات الاتصالات من بين الجرائم الواردة في قانون الاتصــالات، وفي هذا الســياق نصــت المادة (٥٣) منه على تجريم إنشــاء أو تشــغيل نظام اتصــالات أو تقديم خدمات اتصــالات بدون الحصــول على الترخيص المطلوب طبقًا لأحكام القانون، كما جرمت المادة (٥٧) من ذات القانون الحصــول على خدمة اتصــالات باســتخدام وســائل احتيالية لتفادي دفع الرســوم المســتحقة على تلك الخدمة، ويضــاعف الجزاء عند التكرار، فيما جرمت المادتين (٥٨ و٥٩)، الحائز على أشياء تستخدم في الحصول على خدمة الاتصالات بقصد استخدامها بطرق احتيالية أو بقصــد ســماح شــخص آخر باســتخدامها بهذه الطريقة وتتبنى هذه المواد منظومة من العقوبات للتصــدي للأنشــطة غير المشــروعة في مجال الاتصــالات عبر الإنترنت وفي الفضــاء السيبراني، بهدف حماية المستهلكين وضمان توفير الخدمات بطرق قانونية وشفافة.

---

[١] نصت المادة (٦٣) من قانون تنظيم الاتصالات الصادر بالمرسوم السلطاني رقم (٢٠٠٢/٣٠م) على أنه: " يعاقب بالعقوبة المنصوص عليها في المادة (٦١) من هذا القانون كل شخص يستخدم أجهزة أو وسائل الاتصالات في غير الحالات المصرح بها من الهيئة أو في حالات تأدية مهام وظيفية لدى المرخص له بقصد: ١- الحصول على معلومات عن مضمون الرسالة أو عن مرسلها أو المرسل إليه إذا كان من يستخدم هذه الوسائل أو تلك الأجهزة أو من ينوب عنه غير مصرح له من الهيئة بتسلم الرسالة. ٢- إفشاء سرية أي بيانات متعلقة بمضمون الرسالة أو بمرسلها أو بالمرسل إليه تكون قد وصلت إلى علمه بسبب استخدام هذه الوسائل أو تلك الأجهزة سواء من قبله أو من قبل أي شخص آخر وذلك باستثناء الحالات التي يجوز فيها إفشاء سرية تلك البيانات بالتطبيق لأحكام القوانين المعمول بها".

[٢] نصت المادة (٦١) من قانون تنظيم الاتصالات الصادر بالمرسوم السلطاني رقم (٢٠٠٢/٣٠م) على أنه: " يعاقب كل شخص يرسل عن طريق نظام للاتصالات رسالة تكون مخالفة للنظام العام أو الآداب العامة أو تكون غير صحيحة مع علمه بذلك أو تهدف إلى إزعاج الغير بالسجن مدة لا تزيد على سنة، وبغرامة لا تزيد على ألف ريال عماني، أو بإحدى هاتين العقوبتين. وتضاعف العقوبة في حالة التكرار".

٣. قانون المعاملات الإلكترونية.

المحاولة الثالثة من المشـــرع العُماني لمواجهة الجرائم الســـيبرانية جاءت من خلال قانون المعاملات الإلكترونية[١]، حيث جرم المشـــرع في المادتين (٥٢، ٥٣) بعض الأنماط الســـلوكية التي تهدد ثقة الجمهور في التعاملات الرقمية، وتتضمن الجرائم الآتية:

الفئة الأولي: الإتلاف المادي:

ويشـــمل هذا النوع من الجرائم الأضـــرار التي قد تلحق بالمكونات المادية للحاســـب الآلي وملحقاته، مثل الشـاشـة، ولوحة المفاتيح وغيرها، وتسـري عليها أحكام الإتلاف في الجرائم التقليدية[٢]، إلا أن الخلاف قد يحصـــل في مدى قابلية الاعتداء على المكونات المعنوية لتحمل جريمة الإتلاف بالصورة التقليدية المتمثلة في تلف العناصر التي تتألف منها أنظمة المعالجة الآلية للحاسوب[٣].

لتجنب اللجوء إلى القياس، وضـــع المشـــرع العُماني حلًا تشـــريعيًا بتجريم إتلاف المكونات المعنوية لأنظمة الحاســـب الآلي ســـواءً بالتعديل غير المرخص في محتويات الحاســـب الآلي بهدف إضعاف فعاليته أو منع أو تعطيل الوصول إلى البرنامج أو البيانات المخزنة فيه طبقًا للمادة (٥٢) من قانون المعاملات الإلكترونية.

الفئة الثانية: الاختراق المعلوماتي:

يُعتبر الاختراق من بين أخطر الجرائم التي تهدد الأمن المعلوماتي[٤]، وقد ســـعى المشـــرع العُماني إلى تجريم الاختراق المعلوماتي من خلال إدراج بنود خاصـــة في قانون المعاملات الإلكترونية وذلك على النحو الآتي:

١. تجريم الاختراق الذي يؤدي إلى تعطيل أنظمة تشـــغيل الحاســـوب أو إتلاف البرامج أو البيانات الموجودة به، وسرقة المعلومات، واستخدام المعلومات بطرق غير مشروعة، أو إدخال معلومات غير صحيحة[٥].

---

[١] قانون المعاملات الإلكترونية الصـادر بالمرسوم سلطاني رقم ٦٩ / ٢٠٠٨، نشـر في الجريدة الرسـمية بتاريخ ١٧ من مايو سـنة ٢٠٠٨م، وعمل به من تاريخ نشره.

[٢] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت (دراسة مقارنة)، دار النهضة العربية، القاهرة، ٢٠٠٩، ص٤٠٧.

[٣] خالد حربي السعدي، جريمة إتلاف برامج ومعلومات الحاسب الآلي، دار النهضة العربية، القاهرة، ٢٠١٢، ص٤٩.

[٤] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت (دراسة مقارنة)، مرجع سابق، ص٣٣٥.

[٥] البند (٢) من المادة (٥٢) من قانون المعاملات الإلكترونية الصادر بالمرسوم السلطاني رقم (٦٩/ ٢٠٠٨).

٢. تجريم الدخول غير المصرح به إلى أجهزة الحاسوب بهدف ارتكاب جريمة أو تسهيل ارتكابها، سواء من خلال الفاعل نفسه أو من خلال شخص آخر[١].

الفئة الثالثة: الاعتداء على معلومات أو بيانات مشفرة:

يتم التلاعب بأنظمة المعلومات كأجهزة الصراف الآلي عبر إدخال البيانات بطرق غير مشروعة إلى النظام، واستخدام شفرة[٢] غير صحيحة للوصول إلى أنظمة دفع الأجور[٣].

ومن أجل حماية البيانات والمعلومات المشفرة، سعى المشرع العُماني إلى تجريم أي اعتداء عليها بموجب المادة (٥٢) من قانون المعاملات الإلكترونية.

الفئة الرابعة: التزوير الإلكتروني:

التزوير الإلكتروني يمثل تغييرًا متعمدًا للحقيقة في المستندات الإلكترونية، بهدف جلب المنفعة للنفس أو للغير أو الإضرار بالآخرين، ويتجلى التزوير في إعطاء صورة غير حقيقية للمعلومات أو التوقيع الإلكتروني[٤].

وجرم المشرع العُماني طبقًا للمادة (٥٢) من قانون المعاملات الإلكترونية، تزوير سجل إلكتروني[٥] أو توقيع إلكتروني[٦]، ويُعتبر التزوير الإلكتروني جريمة لا تقتصر على الفعل الفعلي للتزوير فقط، بل يشمل أيضًا استخدام المحتوى المزور إذا كان يعلم به.

---

[١] البند (١٣) من المادة (٥٢) من قانون المعاملات الإلكترونية الصادر بالمرسوم السلطاني رقم (٦٩/ ٢٠٠٨).

[٢] يقصد "بالتشفير" وفقًا للمادة الأولى من قانون المعاملات الإلكترونية أنه "عملية تحويل نص بسيط أو وثيقة نصية أو رسالة إلكترونية إلى رموز غير معروفة أو مبعثرة يستحيل قراءتها أو معرفتها بدون إعادتها إلى هيئتها الأصلية".

[٣] هدى حامد قشقوش، مرجع سابق، ص٩٥.

[٤] عبد الرحمن بن عبد الله السند، الأحكام الفقهية للتعاملات الإلكترونية (الحاسب الآلي وشبكة المعلومات الإنترنت)، دار الوراق للطباعة والنشر والتوزيع، الرياض، ٢٠٠٥، ص٣٧٥.

[٥] يقصد "بالسجل الإلكتروني" وفقاً للمادة الأولي من قانون المعاملات الإلكترونية السجل الإلكتروني أنه: "العقد أو القيد أو رسالة المعلومات التي يتم إنشاؤها أو تخزينها أو استخراجها أو نسخها أو إرسالها أو إبلاغها أو تسلمها بوسائل إلكترونية على وسيط ملموس أو أي وسيط آخر ويكون قابلا للتسلم بشكل يمكن فهمه".

[٦] يقصد "بالتوقيع الإلكتروني" وفقًا للمادة الأولي من قانون المعاملات الإلكترونية أنه: "التوقيع على رسالة أو معاملة إلكترونية في شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع متفرد يسمح بتحديد شخص الموقع وتمييزه عن غيره".

الفئة الخامسة: الاعتداء على التوقيع الإلكتروني:

الحماية الجزائية للتوقيع الإلكتروني يمثل خطوة أساسية في سلامة المعاملات الرقمية، وقد عمل المشرع العُماني على توفير الحماية اللازمة لها من خلال قانون المعاملات الإلكترونية[١].

ويقوم السلوك الإجرامي في هذه الجريمة بكل عمل من شأنه تحريف أو تزوير أو إرباك نظام معالجة البيانات[٢]، وقد يكون الاعتداء بمحو البيانات أو تعديلها لما أعدت له أو إفساد البرامج وجعلها غير صالحة للاستخدام، أو تغيير نتائجها عما كانت من المفروض أن تكون عليه، وقد ترد الإعاقة على أحد البرامج التي يحتويها النظام وليس على كل النظام[٣].

بالإضافة إلى ما تقدم جرمت المادة (٥٢) من قانون المعاملات الإلكترونية إجراء تعديل غير مرخص به في محتويات أي حاسب آلي بقصد إضعاف فاعليته أو منع أو إعاقة الدخول إلى أي برنامج أو بيانات محفوظة فيه أو إضعاف فاعلية الاعتماد على تلك البيانات إذا تم ذلك التعديل بشطب أي برنامج أو بيانات محفوظة في الحاسب الآلي، أو إضافة أي برنامج أو بيانات إلى محتويات الحاسب الآلي، أو أي فعل يسهم في إحداث ذلك التعديل.

ويقوم الركن المعنوي في هذه الجرائم على القصد الجنائي العام بركنيه العلم والإرادة[٤]، وتأسيسًا على ذلك إذا قام الشخص الذي يتعامل مع النظام بصورة مشروعة بإعاقة أو إفساد النظام نتيجة لخطأ في التشغيل أو التعامل مع البيانات، ينتفي القصد الجنائي لديه ولا يسأل عن هذه الجريمة[٥].

بعد استعراض القوانين العامة التي أصدرتها السلطنة لمكافحة الجرائم السيبرانية، يتضح حرص المشرع على وضع إطار تشريعي للتعامل مع التحديات التي تفرضها التكنولوجيا الحديثة، بما يعكس التزام السلطنة بمواكبة التطورات التقنية وحماية المجتمع من تهديداتها.

---

[١] البند (١٤) من المادة (٥٢) من قانون المعاملات الإلكترونية.

[٢] مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص٥٤.

[٣] شيماء عبد الغنى، مرجع سابق، ص١٤٩.

[٤] عبد الفتاح حجازي، التوقيع الإلكتروني في النظم المقارنة، مرجع سابق، ص١٣٣.

[5] ABA Section Creates First Digital- Signature Guidelines to aid in Security of The Internet, 1996.

الفرع الثاني

إصدار قانون متخصص بمواجهة الجرائم السيبرانية

تزايد مخاطر الجرائم السيبرانية دفع المشرع العُماني إلى اتخاذ خطوات حاسمة لمواجهتها بإصدار عدة قوانين من بينها قانون المعاملات الإلكترونية رقم (٩٦/ ٢٠٠٨)، وقانون مكافحة جرائم تقنية المعلومات رقم (١٢/ ٢٠١١)، كما انضمت السلطنة إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وصدقت عليها بموجب المرسوم السلطاني رقم (٥/ ٢٠١٥)[١].

وجاء إصدار قانون مكافحة جرائم تقنية المعلومات رقم (١٢/ ٢٠١١)، كقانون مستقل يعالج الجرائم السيبرانية بشكل أكثر تخصصًا وفعالية، تجسد هذه الخطوة حرص السلطنة على التصدي للجرائم السيبرانية بشكل جاد ومنظم[٢]، وعلى ضوء ذلك سوف يركز هذا الفرع على تناول الجرائم السيبرانية وفقًا لقانون مكافحة جرائم تقنية المعلومات على النحو الآتي:

أولًا: جرائم التعدي على سلامة وسرية وتوافر البيانات والمعلومات الإلكترونية والنظم المعلوماتية

سعى الفصل الثاني من القانون إلى حماية البيانات من كافة صور الاعتداء الإلكتروني، حيثُ جرم الدخول إلى المواقع الإلكترونية أو الأنظمة المعلوماتية أو تقنيات المعلومات بدون وجه حق، أو تجاوز المصرح له، وتشدد العقوبة إذا أدى الدخول إلى إلغاء أو تعديل أو نسخ المعلومات أو الإضرار بالبيانات أو الشبكات، أو تمت من قبل موظف أثناء تأدية عمله،[٣] ويفهم من ذلك أن الدخول غير المقصود غير مجرم، وذلك تجسيد للركن المعنوي الذي لا تقوم الجريمة إلا بتحققه.

كما جرم تغيير أو إتلاف البيانات والمعلومات الطبية، أو الدخول إلى المواقع أو الأنظمة الإلكترونية بقصد الحصول على المعلومات الحكومية السرية بطبيعتها[٤]، ويرى الباحث أن المشرع لم يوفق في استخدام مصطلح " **السرية** بطبيعتها"، وكان الأجدر به استخدام مصطلح "المعلومات والوثائق

---

[١] صابرين جابر أحمد محمد، محمود بن علي بن سهيل المعشني، مرجع سابق، ص١٧١.

[٢] خالد ظاهر عبدالله جابر السهيل المطيري، مرجع سابق، ص١٠٤٤.

[٣] المادتين (٣، ٤) من قانون مكافحة جرائم تقنية المعلومات.

[٤] المادتين (٥،٦) من قانون مكافحة جرائم تقنية المعلومات.

المصـنفة"، بما يتسـق مع قانون تصـنيف وثائق الدولة وتنظيم الأماكن المحمية[١]، ليشـمل جميع درجات التصــنيف[٢]، حيث أن النص بوضــعه الحالي قد يفهم منه أن الحماية تشــمل البيانات والمعلومات التي تحمل تصنيف "سري" دون غيرها من درجات التصنيف الواردة في القانون آنف الذكر.

وهنا يثور التســـاؤل إذا قام الولي بالدخول إلى نظام المعلومات أو الموقع الإلكتروني الخاص بالحدث أو فاقد الأهلية الذي يتولى أمره، هل يكون مشـــمولًا بهذا التجريم إذا كان ذلك الدخول لحماية من يتولى أمره والحفاظ عليه، ويرى الباحث ضرورة استثناء ولي الأمر من ذلك من خلال النص عليه صراحة.

يُعد الاعتداء على البيانات وأنظمة المعلومات من أكثر الجرائم الســيبرانية خطورة وتســببًا في إيقاع الخسائر للدول والمؤسسات الخاصة والأفراد[٣]، ويرى الباحث أن العقوبات التي حددها المشرع العُماني لا تتناسب مع جسامة بعض الجرائم التي قد ينتج عنها أضرار خطيرة وجسيمة[٤]، خاصة تلك التي تقع على أنظمة مؤســســات الدولة، أو تلك التي تؤدي إلى انقطاع الخدمات العامة، أو التي تقع على المؤسسات المالية كالبنوك، وما يترتب عليها من خسائر مالية كبيرة، والخطر الذي يقع على حياة الأفراد عند العبث بالأنظمة الإلكترونية في بعض القطاعات، كالمرافق الصحية.

ثانيًا: إساءة استخدام وسائل تقنية المعلومات

أفرد القانون الفصل الثالث منه لجرائم إساءة استخدام وسائل تقنية المعلومات[٥]، وذلك بتجريم "استخدام الشبكة المعلوماتية أو وسائل تقنية المعلومات في إنتاج أو بيع أو شراء أو استيراد أو توزيع أو عرض أو اتاحة برامج أو أدوات أو أجهزة لارتكاب جرائم تقنية المعلومات أو كلمات ســر أو رموز تستخدم لدخول نظام معلوماتي أو حيازتها بقصد استخدامها في ارتكاب جرائم سيبرانية"[٦].

---

[١] الصادر بالمرسوم السلطاني رقم (١١٨/ ٢٠١١)، نشر في عدد الجريدة الرسمية رقم (٩٤٩) الصادر في ٢٠١١/١٠/٢٩م.

[٢] نصت المادة (٣) من قانون تصنيف وثائق الدولة وتنظيم الأماكن المحمية على أنه: " تكون درجات تصنيف الوثائق على النحو الآتي: أ- سري للغاية. ب- سري. ج- محدود. د- مكتوم."

[٣] عزة الحسن، الجريمة المعلوماتية في القانون السوداني، الزيتونة للطباعة، السودان، ٢٠٠٩، ص٥١.

[٤] راشد الشيدي، الجرائم الإلكترونية، مكتبة الجيل الواعد، مسقط، ط١، ٢٠٢٢، ص٨٣.

[٥] يقصد بـــ "تقنية المعلومات" وفقًا للمادة الأولى من قانون مكافحة جرائم تقنية المعلومات بأنها "الاستخدام العلمي للحوسبة والإلكترونيات والاتصالات لمعالجة وتوزيع البيانات والمعلومات بصيغها المختلفة".

[٦] المادة (١١) من قانون مكافحة جرائم تقنية المعلومات.

قد يساعد الجناة في ارتكاب أفعالهم الإجرامية الثغرات التقنية في الشبكات والأنظمة التقنية، فضلًا عن الإهمال الذي قد يقع من قبل الموظف يجعلها عرضه للاختراق، كالإهمال في منح كلمات السر ورموز الاستخدام لغير المخول، وعلى ضوء ذلك يقترح الباحث تجريم إهمال الموظف الواضح الذي يتسبب في تسهيل ارتكاب أي من الجرائم الواردة في القانون.

ثالثًا: التزوير والاحتيال المعلوماتي

يتمثل الاحتيال الإلكتروني في استخدام الحاسب الآلي للوصول غير المشروع إلى بيانات مالية أو شخصية، أو تنفيذ عمليات احتيالية مثل الاحتيال الائتماني أو اختراق أنظمة الدفع الإلكتروني[١]، وقد تناول قانون مكافحة جرائم تقنية المعلومات هذه الجرائم في الفصل الرابع، بتجريم استخدام وسائل التقنية في تغيير الحقيقة في البيانات والمعلومات سواء بالحذف أو الإضافة أو الاستبدال، وجعلها مقبولة قانونًا لتحقيق النفع أو الإضرار بالغير[٢]، وفي ذلك قضت المحكمة العليا "بإدانة المتهم بجنحة إضافة بيانات ومعلومات غير صحيحة في نظام إلكتروني المؤثمة بنص المادة (١٢) من قانون مكافحة جرائم تقنية المعلومات، وذلك بعد إقدامه على إصدار فواتير وبوليصات شحن وهمية، ويتم صرف المبالغ باسم شركته، وقد وجدت بعض الشيكات المصروفة لشركته مخزنة بالنظام الإلكتروني للشركة المجني عليها، التي يعمل لديها بقسم المشتريات، ويقوم بحكم وظيفته بأعمال التخليص الجمركي واستلام الفواتير والإيصالات من الشركات التي تتعامل مع الشركة المجني عليها"[٣].

ويلاحظ أن المشرع فرق في العقوبة بين الاعتداء على البيانات الحكومية والمؤسسات المالية وبين غيرها من الأشخاص الطبيعية والمعنوية، وهي تفرقة جوهرية؛ نظرًا لأهمية المصلحة المعتدى عليها وجسامة الآثار المترتبة عليها.

---

[١] عبد الفتاح حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الفكر الجامعي، ٢٠٠٦، الإسكندرية، ص٧٣.

[٢] المادتين (١٢، ١٣) من قانون مكافحة جرائم تقنية المعلومات.

[٣] الطعن رقم ٩٠٤/ ٢٠٢٠م جلسة ١٩ / ٠١ / ٢٠٢١، مجموعة الأحكام الصادرة عن الدائرة الجزائية بالمحكمة العليا والمبادئ المستخلصة منها في الفترة من ٢٠٢٠/١٠/١م حتى ٢٠٢١/٩/٣٠.

وفي هذا السياق فإن الباحث يرى أهمية إضافة تجريم انتحال صفة الموظف العام أو أي صفة أخرى، وذلك لمواجهة الانتشار الواسع لانتحال الصفات لتحقيق أغراض شخصية في الوسط التقني، فضلًا عن الإشارة إلى تجريم الوسائل الاحتيالية بصورة عامة دون الحاجة إلى تفصيل الأفعال التي تشكل الاحتيال الإلكتروني كما هو الحال في المادة (١٣) من قانون مكافحة جرائم تقنية المعلومات، وذلك لصعوبة حصر وسائل الاحتيال الالكتروني المتجددة، بالإضافة إلى تجريم "التزييف العميق"[١]، نظرًا لدقة هذه التقنية وقابليتها للتصديق من قبل المشاهدين، وأثرها الكبير على المجني عليه.

رابعًا: جرائم المحتوى

تناول الفصل الخامس من القانون جرائم المحتوى وسيتم استعراضها بشيء من التفصيل على النحو الآتي:

١. ترويج المواد الإباحية، والتحريض على ارتكاب الفجور:

لقد أدى انتشار شبكة الإنترنت إلى خلق مجال واسع لارتكاب الجرائم المختلفة، بما في ذلك الجرائم المتعلقة بالآداب العام، حيث أظهرت الأبحاث الحديثة أن هناك طلبًا كبيرًا على المواقع الإباحية، وتستقبل بعض المواقع أكثر من ربع مليون زائر يوميًا [٢]، ولمواجهة ذلك حظر المشرع العُماني استخدام وسائل التقنية في عرض أو إنتاج أو نشر أو توزيع أو شراء أو بيع أو استيراد المواد إباحية ما لم يكن لأغراض علمية وفنية مصرح بها، كما جرم استخدام وسائل التقنية في إغواء أو تحريض الأنثى أو الذكر لارتكاب الفجور أو الدعارة وتشدد العقوبة إذا وقعت على الحدث[٣].

لا يرى الباحث أي مبرر أو جدوى من استثناء استيراد المواد الإباحية لأغراض فنية أو تعليمية، وأن المصلحة في إلغاء الاستثناء هي أكبر، خشية استغلال هذا الاستثناء بشكلٍ أو بآخر.

---

[١] "التزييف العميق Deep fakes : تعني قيام أشخاص محترفين باستخدام برامج إلكترونية لإنتاج مقاطع فيديو أو تعديل صورة، ويتم فيها استبدال وجه شخص ما بوجهٍ آخر تم إنشاؤه بواسطة جهاز الحاسوب وبرامج معينة، ويكون التزييف مقنعًا وقريبًا جدًا من الحقيقة من حيث الصوت والصورة، ويسهل تصديقه".

[٢] رضوى عبدالرحيم قنديل، الجرائم الإلكترونية ماهيتها وأنواعها وإجراءات الدعوى الجنائية في مكافحتها وفقًا لقانون سلطنة عُمان، دار الكتاب الجامعي، الإمارات العربية المتحدة، ط١، ٢٠٢١، ص١٢٠.

[٣] المادتين (١٥، ١٦) من قانون مكافحة جرائم تقنية المعلومات.

٢. الاعتداء على حرمة الحياة الخاصة

أصبحت البيانات الشخصية التي تنتشر بكميات هائلة عبر الإنترنت خطرًا على خصوصية أصحابها، وظهور تجارة البيانات الشخصية، عبر عمليات جمع ومعالجة البيانات الشخصية، سواء أثناء التحزين أو النقل، وتتعرض هذه البيانات لمخاطر عديدة تنتهك خصوصيتها، أدى ذلك إلى تدخل القانون لوضع إطار قانوني يضمن حماية البيانات الشخصية، حيثُ أجاز قانون المعاملات الإلكترونية لأية جهة حكومية أو مقدم خدمات جمع البيانات الشخصية مباشرةً من الشخص الذي تجمع عنه البيانات أو من غيره بعد موافقته الصريحة، وذلك فقط لأغراض إصدار شهادة أو المحافظة عليها أو تسهيل ذلك، ولا يجوز جمع البيانات أو معالجتها أو استخدامها لأي غرض آخر دون الموافقة الصريحة للشخص المجموعة عنه البيانات[١].

وألزم قانون حماية البيانات الشخصية المتحكم[٢] قبل البدء في معالجة أي بيانات شخصية أن يخطر صاحب البيانات الشخصية كتابة بكافة المعلومات الضرورية لاستيفاء شروط المعالج، وإلزام المتحكم عند حدوث اختراق للبيانات الشخصية، بإبلاغ الوزارة وصاحب البيانات[٣].

وفي ذات السياق نصت المادة (١٦) من قانون مكافحة جرائم تقنية المعلومات على تجريم استخدام وسائل التقنية في الاعتداء على حرمة الحياة الخاصة للأفراد بالتقاط الصور أو نشر التسجيلات المرئية أو الصوتية أو الأخبار ولو كانت صحيحة، أو في التعدي على الغير بالسب والقذف.

يلاحظ أن المشرع دمج جريمة السب والقذف مع جريمة الاعتداء على الحياة الخاصة في نص واحد، دون أن يكون أي رابط فيما بينها، وعلى ضوء ذلك يرى الباحث أنه من المناسب إفراد نص خاص لجريمة السب والقذف باستخدام الوسائل الإلكترونية باعتبارها جريمة مستقلة.

---

[١] المادة (٤٣) من قانون المعاملات الإلكترونية.

[٢] يقصد بالمتحكم وفقًا للمادة (١) من قانون حماية البيانات الشخصية: "الشخص الذي يتولى تحديد أهداف ووسائل معالجة البيانات الشخصية، ويقوم بهذه المعالجة بنفسه، أو يعهد بها إلى غيره".

[٣] المادتين (١٤، ١٩) من قانون حماية البيانات الشخصية.

في ضوء انتشار وسائل التواصل الاجتماعي، وسعي الكثيرين إلى تصوير كل واقعة لتحقيق السبق وكسب أعلى رقم من المتابعين والعائد المالي المتحقق من ذلك، يرى الباحث أنها أوجدت طرق جديدة للاعتداء على الحياة الخاصة، ويتعين على المشرع إدراجها ومن أمثلتها توثيق الجرائم بالتقاط ونشر الصور والفيديوهات للمجني عليهم، والتقاط ونشر مختلف الوقائع والأحداث التي تظهر الآخرين في مواضع ومواقف مختلفة، والأمر كذلك بالنسبة لاستخدام الوسائل التقنية في تحديد مواقع الأشخاص ورصد تحركاتهم.

٣. المقامرة والمساس بالآداب العامة والقيم الدينية والنظام العام

جرم المشرع العُماني استخدام الشبكات والتقنية في المقامرة، أو نشر أو توزيع أو إنتاج أو شراء أو حيازة ما من شأنه الإخلال والمساس بالآداب العامة أو القيم الدينية والنظام العام[١].

ويرى البعض أن استخدام المصطلحات العامة كالإخلال بالنظام العام والآداب العامة من شأنه التوسع في التجريم، بالإضافة إلى الغموض وعدم وضوح النصوص الجزائية، مما يتعين معه تعريف هذه المفاهيم ووضع أطر واضحة لها[٢]، في حين يرى البعض الآخر أن الأمن القومي والنظام العام والآداب العامة جميعها أمور نسبية متطورة ومتغيرة تتقدم وتتطور وتتغير من مجتمع لآخر وتضيق وتتسع من حضارة لأخرى وفقًا للموروث الثقافي والنظام الاجتماعي والسياسي السائد في كل مجتمع، ويصعب معه وضع تعريف جامع مانع لهذه المفاهيم على المستوى الدولي والإقليمي رغم اجتهاد فقهاء القانون في تعريفها، لذلك فإن التشريعات تعمل على إيراد هذه المفاهيم دون تعريفها أو وضع حدودها[٣]، وهو الرأي الذي يرجحه الباحث.

في ذلك ذهبت المحكمة العليا إلى قيام الركن المادي في جنحة استخدام تقنية المعلومات في نشر وتوزيع ما من شأنه المساس بالنظام العام عند إذاعة أخبار أو إشاعات كاذبة، إذا كان من شأن

---

[١] المادتين (١٧، ١٩) من قانون مكافحة جرائم تقنية المعلومات.

[٢] حمد الربيعي، القيود الجنائية على حرية التعبير عن الرأي من خلال وسائل الإعلام، دار النهضة العربية، القاهرة، ٢٠١٠، ص٢٠٢.

[٣] آية جمال المغربي، ضوابط حرية الرأي والتعبير عن الرأي في التشريع الفلسطيني والمواثيق الدولية، رسالة لنيل درجة الماجستير في الجامعة الإسلامية، غزة، ٢٠١٦، ص(٤١-٤٣).

ذلك تكدير وإثارة الرأي العام أو إلقاء الرعب بين الناس أو إلحاق الضرر بالمصلحة العامة[١]، واستقر القضاء العُماني إلى أن الحديث عن الأوضاع القائمة فعلا دون زيادة؛ بهدف تنوير الحكومة بما يعود بالنفع العام، لا يُعد مساسًا بالنظام العام[٢].

٤. التهديـــد والابتـــزاز

جرم المشرع العُماني استخدام الوسائل التقنية في التهديد والابتزاز لحمل الشخص على القيام بفعل أو الامتناع عنه ولو كان ذلك الفعل أو الامتناع عنه مشروع، وشدد العقوبة إذا كان الابتزاز أو التهديد بارتكاب جناية أو القيام بأفعال مخلة بالشرف والاعتبار[٣].

وحيثُ أن الفرق بين الابتزاز والتهديد هو أن الابتزاز يتضـــمن طلب القيام بأمر معين أو الامتناع عنه، بينما التهديد يهدف إلى إثارة الخوف لدى الضـــحية لإجبارها على القيام بأمر معين أو الامتناع عنه، وللابتزاز الإلكتروني آثار كبيرة على نفس المجني عليه يصـــل بعضـــها إلى حد إزهاق الروح بالانتحار، فضلًا عن أثرها على أمن المجتمع وهدم القيم وانتشار الفساد[٤].

واســـتقرت المحكمة العليا إلى أن " تقدير العبارات التي تشـــكل تهديدًا وابتزازًا من الأمور التي يقررها قاضـــي الموضـــوع بناءً على ظروف الواقعة وملابســـاتها، ويكفي أن يُثبت الحكم وجود الجريمة دون الحاجة إلى تفصيل الأركان المكونة لها[٥].

٥. الإرهاب وغسل الأموال

الإرهاب الإلكتروني يعتبر امتدادًا لجريمة الإرهاب التقليدية، حيث يتميز بالوسـيلة المسـتخدمة في تنفيذه والتي تشمل الوسائل الإلكترونية والتقنية وشبكات الإنترنت، ويتسم الإرهاب الإلكتروني بأنه

---

[١] الطعن رقم ٢٠١٥/٩٩٩م جزائي عليا (أ) جلســـة ٠٥ / ٠١ / ٢٠١٦، مجموعة الأحكام الصـــادرة عن الدائرة الجزائية بالمحكمة العليا والمبادئ المستخلصة منها للسنتين القضائيتين الخامسة عشر والسادسة عشر.

[٢] حكم المحكمة الابتدائية بمسقط – الدائرة الجزائية، الدعوى الجزائية رقم (٢٠٢٤/ ٥١٠٠/ ٢٠٢٢).

[٣] المادة (١٨) من قانون مكافحة جرائم تقنية المعلومات.

[٤] منصـور حسـان، جريمة الابتزاز الإلكتروني "دراسـة مقارنة بين القانون المصـري والفرنسـي والإماراتي والنظام السـعودي، المجلة القانونية، المجلد ١٧، العدد ٥، مصر، ٢٠٢٣، ص٩٣١.

[٥] الطعن رقم ٤٧٠/ ٢٠٢١م جلسة ٢٨ / ٠٩ / ٢٠٢١ مجموعة الأحكام الصادرة عن الدائرة الجزائية بالمحكمة العليا والمبادئ المستخلصة منها في الفترة من ٢٠٢٠/١٠/١م حتى ٢٠٢١/٩/٣٠م.

عابر للحدود ويتم ارتكابه عن بعد، مما يجعله صعب الكشف عنه قبل وقوعه، ويمكن أن تستهدف هذه الجرائم الأنظمة التقنية والشبكات الإلكترونية، بالإضافة إلى البنى التحتية والمؤسسات المالية المتصلة بشبكات الإنترنت، وهذا ما يجعلها تشكل خطرًا كبيرًا على الأفراد والمؤسسات والدول[١].

وتناول المشرع العُماني الإرهاب الإلكتروني عبر تجريم إنشاء المواقع الإلكترونية لتنظيمات إرهابية أو استخدام الشبكات أو وسائل التقنية لأغراض إرهابية أو نشر أفكارها أو تمويلها أو التدريب عليها أو تسهيل اتصالاتها أو نشر طرق صناعة الأسلحة المستخدمة في تنفيذ عملياتها، أو طلب المساعدة في غسل الأموال[٢].

٦. الاتجار بالبشر والأعضاء البشرية أو المخدرات والمؤثرات العقلية أو بالآثار والتحف الفنية

تصدى المشرع العُماني لجرائم الاتجار بالبشر عبر إصدار قانون مكافحة الاتجار بالبشر الصادر بالمرسوم السلطاني رقم (١٢٦/ ٢٠٠٨)، كما جاء قانون مكافحة جرائم تقنية المعلومات وجرم إنشاء موقع إلكتروني أو نشر المعلومات على شبكة الانترنت بقصد الاتجار بالبشر أو الاتجار في الأعضاء البشرية أو تسهيل التعامل بذلك، أو الاتجار في الأسلحة، وأحال في ذلك إلى قانون الأسلحة والذخائر الصادر بالمرسوم السلطاني رقم (٩٠/٣٦) ، أو الاتجار بالآثار والتحف الفنية بدون تصريح، أو الترويج للمخدرات والمؤثرات العقلية وفق الجداول الملحقة بقانون مكافحة المخدرات والمؤثرات العقلية[٣]، وحسنًا فعل المشرع عندما أحال إلى قانون مكافحة المخدرات والمؤثرات العقلية في تحديد أنواع المخدرات والمؤثرات العقلية التي تدخل في نطاق التجريم، ويرى الباحث أهمية إدراج المعادن ضمن المواد التي يحظر الاتجار بها باستخدام الوسائل الالكترونية وذلك في سبيل التصدي لمثل هذه التصرفات الضارة بالموارد الوطنية.

---

[١] توات عبدالحكيم، جريمة الإرهاب الإلكتروني، رسالة لنيل درجة الماجستير في جامعة العربي التبسي، الجزائر، ٢٠٢٢، ص٩٢.

[٢] المادتين (٢٠، ٢١) من قانون مكافحة جرائم تقنية المعلومات.

[٣] المواد (٢٢، ٢٣، ٢٤، ٢٥، ٢٧) من قانون مكافحة جرائم تقنية المعلومات.

خامسًا: التعدي على البطاقات المالية

رغم إيجابيات وسائل الدفع الإلكتروني التي سهلت التعاملات بين الأفراد والمؤسسات العامة والخاصة، التي أصبحت شائعة بفضل الراحة والأمان التي توفرها، إلا أنها محاطة بمجموعة من المخاطر ولعل أبرزها الاختراق أو التزوير أو سرقتها أو سرقة بياناتها[١]، وتصدى المشرع العُماني لجريمة التعدي على البطاقات المالية بدون وجه حق[٢].

وتجدر الإشارة أن وسائل الدفع الإلكتروني تطورت ولم تقتصر على البطاقات المالية التي تناولها المشرع العُماني بموجب المادة (٢٨) من قانون مكافحة جرائم تقنية المعلومات، الذي قصرها على الوسيط الإلكتروني الملموس، وهذا يعني أن الحماية لا تشمل وسائل الدفع الإلكتروني الأخرى كالبطاقات الافتراضية، والعملات الرقمية، والدفع عبر الرسائل النصية وغيرها، وفي ضوء ذلك يقترح الباحث على المشرع العُماني تعديل تعريف البطاقة المالية بما يشمل جميع وسائل الدفع الإلكتروني.

---

[١] ابتسام السايس، صفاء نيلي، وسائل الدفع في التجارة الإلكترونية، رسالة لنيل درجة الماجستير في جامعة قاصدي مرباح ورقلة، الجزائر، ٢٠٢٠، ص٨١.

[٢] المادة (٢٨) من قانون مكافحة جرائم تقنية المعلومات.

المطلب الثاني

المواجهة التقنية للجرائم السيبرانية

تتطلب مكافحة الجرائم السيبرانية جهودًا متعددة المستويات، لا تقتصر فقط على الجوانب التشريعية، بل تتطلب أيضًا اعتماد تقنيات حديثة لحماية الأنظمة الحاسوبية والبيانات للتصدي للهجمات السيبرانية بفعالية.

وتعد التقنيات الحديثة للحماية والأمن السيبراني أساسية في مواجهة التهديدات الإلكترونية المتزايدة، وتعمل على تعزيز القدرة على اكتشاف ومنع الهجمات السيبرانية قبل وقوعها، عليه سيتم في هذا المطلب استعراض الجهود التقنية في فرعين الأول حول تقنيات الحماية والأمن السيبراني، والثاني يتناول دور مركز الدفاع الإلكتروني في تعزيز الأمن السيبراني.

الفرع الأول

تقنيات الحماية والأمن السيبراني

تمثل التقنيات الحديثة جزءًا أساسيًا من الجهود المبذولة لتعزيز الأمن والحماية في العديد من الدول، ومن هذا المنطلق تعمل السلطنة جاهدة على استخدام أحدث التقنيات لتعزيز الأمن السيبراني الشامل على المستوى الوطني والمجتمعي، وتحقيق أعلى مستويات الحماية لفضائها الإلكتروني.

تشمل التقنيات مجموعة واسعة من الأدوات التي تستخدم لحماية الأنظمة الإلكترونية والشبكات من التهديدات الإلكترونية المختلفة، وعلى مستوى السلطنة تمثل هذه التقنيات جزءًا أساسيًا من استراتيجية الأمن الوطني، لحماية البيانات الحساسة والأنظمة الحيوية، وتعزيز الاستقرار السيبراني للدولة[١]، وتثبت بذلك التزامها ببناء مجتمع آمن ومستقر يعزز من مستقبل البلاد وتنميتها المستدامة[٢].

---

[١] عبد الله بن علي بن سالم الشبلي، مرجع سابق، ص٩١.

[٢] حسين بن سعيد الغافري، الحماية الجزائية للتوقيع الالكتروني "في ضوء التشريع العُماني والتشريع المقارن"، مجلة البحوث الفقهية والقانونية، العدد (٣٩)، مصر، أكتوبر ٢٠٢٢، ص١٧٣٤.

هذه الجهود تبرز الدور الحيوي في تحقيق الأمن والسـلامة العامة، في ظل دخول التكنولوجيا الحديثة في أغلب النشـاطات الإنسـانية، كاسـتخدام الروبوتات في الكشـف عن الألغام والمتفجرات، وتوظيف كاميرات المراقبة في الطرق العامة والفرعية[١].

في فرنسا عقب الهجمات الإرهابية في عام ٢٠١٥، التي سقط فيها عدد من القتلى، وضعت السـلطات الفرنسـية خطة لتأمين الانتخابات الرئاسـية عام ٢٠١٧، لمنع وقوع هجمات إرهابية، وقد اسـتخدم في خطة التأمين الذكاء الاصـطناعي[٢]، وكان من أهم أدواتها الضـبط الاسـتباقي، ذلك المصـطلح الذي يتم اسـتخدامه في الأمن الإقليمي، وهو الأمر الذي تحدث عنه الرئيس الفرنسـي "إيمانويل ماكرون" عام ٢٠١٨ بأنه سـوف يعتمد خطة الابتكار التكنولوجي من خلال تطبيقات الذكاء الاصطناعي في منع وقوع الجريمة[٣].

بعض تطبيقات الذكاء الاصـطناعي يمكن اسـتخدامها في الكشـف عن الجريمة، مثل تطبيق (Alexa) الذي أنتجته شـركة أمازون، يقوم بتسـجيل المكالمات التليفونية، التي يمكن الاسـترشـاد بها بشـأن علاقات المجني عليه مع الجناة، وإن كان هذا التطبيق يصـطدم بمعوقات قانونية، ولعل أبرزها سياسة الخصوصية التي تفرضها الشركات المالكة، وعلى سبيل المثال طلب المدعى العام من شركة أمازون أي تسـجيلات تكون قد قامت بها بموجب تطبيق ألكسـياAlexa في إطار التحقيق في جريمة قتل، إلا أن شركة أمازون رفضت وتذرعت بالأحكام الخاصة بالخصوصية[٤].

---

(١) حسين يوسف أبو منصور، الذكاء الإصطناعى وأبعاده، أوراق السياسة الأمنية، جامعة نايف للعلوم الأمنية، عدد ١، السعودية، ٢٠٢٠، ص١- ص١٨.

(2) Yamina Bouadi, Intelligence artificielle, justice pénale et protection des données à caractère personnel, M Sc Thése, Université de Strasbourg, 2020, pp .14-15.

(3) Marine Kettani, Predictive policing and Rule of technology, Webinaire IA and Law Breakfasts, organisé par le Conseil de l'Europe, le 02 .07 .2020.

(4) Eliott C . McLaughlin, Suspect Oks Amazon to Hand Over Echo Recordings in Murder Case, CNN (Apr . 26, 2017).

تمتلك السلطنة استراتيجية طويلة المدى لتحسين بيئة الأعمال الإلكترونية، تتضمن هذه الاستراتيجية توجيهات وإجراءات وممارسات متعلقة بالمجال الإلكتروني، بالإضافة إلى معايير نظام إدارة أمن المعلومات، بهدف الحماية والإشراف على المعلومات وتنفيذ إجراءات محددة من قبل الجهات الحكومية[١].

تهدف هذه التقنيات إلى حماية المعلومات من الوصول غير المصرح به والتلاعب بها، سواء أثناء تخزينها أو معالجتها أو نقلها، وتقييم المخاطر التي تواجهها المؤسسات الحكومية ووضع الخطط لمواجهتها، وحماية البيانات من الاختراقات، وبناء الثقة بين المؤسسات والعملاء والحد من الحوادث والتهديدات المتعلقة بالأمن السيبراني، وتبني التطوير المستمر لضمان دخول آمن للمستخدمين والاستفادة من الخدمات الحكومية[٢].

وتوجد عدة تقنيات وإجراءات تستخدمها السلطنة في الوقاية من الجريمة ومكافحتها، من بين هذه التقنيات[٣]:

١. **المراقبة بالكاميرات:** تستخدم الكاميرات الموزعة في الأماكن العامة والحيوية لمراقبة الأنشطة وتسجيل الأحداث، مما يسهم في رصد الجرائم وتوثيقها.
٢. **تحليل البيانات الضخمة(Big Data):** يتم جمع وتحليل كميات كبيرة من البيانات لتحديد الاتجاهات الجرمية، مما يسهل اتخاذ الإجراءات الوقائية المناسبة.
٣. **تطبيقات الهاتف الذكي والتقنيات الذكية:** يمكن استخدام التطبيقات المخصصة للسلامة العامة وتقارير الجريمة لتمكين المواطنين من الإبلاغ عن الجرائم بسرعة وفعالية، مما يزيد من فعالية الاستجابة الأمنية.
٤. **تحليل الوقت الحقيقي:** تقنيات متقدمة تستخدم لمراقبة الأحداث في الوقت الحقيقي، مما يتيح اتخاذ إجراءات سريعة لتفادي الجرائم أو الرد عليها.

---

[١] موقع (عماننا)، البوابة الإلكترونية للخدمات الحكومية الإلكترونية، الرابط الإلكتروني htpps://cut.us/vndts

[٢] خليل بن حمد البوسعيدي، السياسة العقابية التي اتبعها المشرع العُماني في قانون مكافحة الجرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم (١٢/ ٢٠١١)، مجلة ابن خلدون للدراسات والأبحاث، المجلد ٢، العدد ١٢، فلسطين، ٢٠٢٢، ص٥٠٠.

[٣] عبد الحميد الدوحاني، سليم القيسي، السياسات الجنائية في مواجهة جرائم تقنية المعلومات في المجتمع العُماني من وجهة نظر المحامين في سلطنة عُمان، حوليات آداب عين شمس، المجلد ٤٨، عدد أكتوبر – ديسمبر ٢٠٢٠، مصر, ٢٠٢٠ ص١٢٨.

٥. **التدريب والتوعية الأمنية:** يتم توعية المواطنين والمقيمين بأساليب الوقاية من الجريمة والتصرف الآمن عبر حملات توعية وبرامج تدريبية.

٦. **التعاون مع القطاع الخاص والمؤسسات الدولية:** يتم التعاون مع الشركات الخاصة لتطوير تقنيات الأمن والتصدي للتهديدات السيبرانية، بالإضافة إلى التعاون مع الجهات الدولية لتبادل المعلومات وتنسيق الجهود في مجال مكافحة الجريمة.

تعمل الجهات المختصة في السلطنة وبالشراكة بين القطاعين العام والخاص إلى تحقيق رؤية ومستقبل عمان الرقمية، حيثُ احتلت السلطنة في عام ٢٠٠٨م المرتبة (٨٤) في تصنيف الأمم المتحدة الدولي لجاهزية الحكومة الإلكترونية، وحققت بذلك تقدمًا بمقدار (٢٨) مركزًا مقارنة بالتصنيف في عام ٢٠٠٥م، وفي السنوات الأخير تقدمت السلطنة في هذا الجانب بشكل ملحوظ فقد حصلت على المركز الثالث عالميًا وفقًا لمؤشر الأمن السيبراني العالمي والأول عربيًا في جاهزية الأمن السيبراني في عام ٢٠١٧م[١]، كما أعلن الاتحاد الدولي للاتصالات نتائج نسخة عام ٢٠٢٤م للمؤشر العالمي للأمن السيبراني، وجاءت السلطنة في القائمة الأولى عالميًا ضمن الدول الأكثر جاهزية في الأمن السيبراني، وتضم القائمة الأولى الدول التي حصلت على مجموع أكثر من (٩٥) نقطة ، حيثُ ارتفعت السلطنة من (٩٦) نقطة في مؤشر عام ٢٠٢٠م، إلى (٩٧.٠٢) في مؤشر عام ٢٠٢٤.[٢]

ورغم ذلك فإن السلطنة ليست في مأمن من الهجمات السيبرانية، حيثُ سجلت السلطنة زيادة ملحوظة في عدد الهجمات السيبرانية التي استهدفت الفضاء السيبراني العُماني، وفي عام ٢٠٢٢م تم التصدي لأكثر من (٥,٧) مليون هجمة سيبرانية، بما في ذلك (١,٨) مليون هجمة عبر البريد الإلكتروني، بالإضافة إلى (١,٤) مليون عبر البرمجيات الخبيثة[٣]، وفي إطار مؤتمر الأمن السيبراني الذي انعقد في السلطنة في عام ٢٠٢٣م تم مناقشة أهمية تعزيز الحماية التقنية في السلطنة ضد التهديدات السيبرانية، وأشارت أوراق العمل التي قدمت إلى حجم الخسائر العالمية المرتبطة بالجرائم

---

[١] أمل بنت سعيد المشايخي، مستقبل الأمن السيبراني في سلطنة عُمان، رسالة لنيل درجة الماجستير في جامعة السلطان قابوس، مسقط، ٢٠١٧، ص٨.

[٢] وكالة الأنباء العُمانية، نشر في ١٢ سبتمبر ٢٠٢٤م.

[٣] حجب ٥.٧ مليون تهديد للأمن السيبراني في عمان، صحيفة عمان أوبزرفر الإلكترونية، نشر بتاريخ ١٢ أكتوبر ٢٠٢٢، تم استيراده بتاريخ ١٥ يونيو ٢٠٢٤م.

السـيبرانية التي بلغت حوالي (٦٠٠) مليار دولار سـنويًا، مما يؤكد على ضـرورة تطوير قدرات وطنية قوية في مجال الأمن السيبراني[١].

إن تحديد التهديدات والتنبؤ بها عامل مؤثر في مكافحة الجريمة السـيبرانية خاصـة بعض الهجمات الهادئة التي يصـعب اكتشـافها كسـرقة البيانات[٢] ويعتمد التنبؤ على برمجيات معينة في ملاحظة بعض الأفعال المكونة للجرائم السـيبرانية وتحديد مكان وزمان وقوعها، وتسـتخدم تلك البرمجيات خوارزميات متطورة خاصة بالتنبؤ بالجريمة حيث تحلل أنماط من قواعد البيانات الأمنية في محاولة لاكتشـاف متى وأين من المرجح حدوث جريمة مسـتقبلية، ويتم تسـليط الضـوء على النقاط المحتملة لارتكاب الجرائم على خريطة ذكية تنبه السـلطات لأهمية تكثيف تواجدها في تلك النقاط، وذلك من أجل منع وقوع الجريمة، وتوصـف نتائج هذه البرمجيات بأنها دقيقة[٣]، ونورد تاليًا أهم برمجيات التنبؤ:

أولًا: برمجية PREDPOL للتنبؤ بالجريمة:

يتم استخدام هذا البرنامج على نطاق واسع في الولايات المتحدة والمملكة المتحدة ، الذي يعتمد على تحديد "النقاط السـاخنة"، ويقوم بتحديد الأماكن والأوقات التي يرجح ارتكاب الجرائم خلالها وبدأت شـرطة نيويورك في اسـتخدامه في عام ٢٠١٣م، وتعتمد على خوارزميات يتم رفدها بالمعلومات عبر الشكاوى المتعلقة بالجرائم والوقائع والمكالمات التي ترد إلى الشرطة، بما يساعدها في إحباط الأنشطة الإجرامية[٤]، حيث يقوم بتحليل جريمة وقعت في منطقة ما، ويجمع البيانات في نمط يتبع تاريخ الجرائم في نفس المنطقة، مما يسـمح له بتوقع تاريخ ومكان وقوع الجريمة مسـتقبلًا، وقامت ولاية بنسـلفانيا بتجربة هذا البرنامج والتي كانت تعاني من معدلات عالية للفقر في سـنة ٢٠١١، الذي أدى

---

[١] المرجع السابق، نشر بتاريخ ٨ مارس ٢٠٢٣، تم استيراده بتاريخ ١٥ يونيو ٢٠٢٤م.

[٢] الذكاء الاصـطناعي والتعلم الآلي في الأمن السـيبراني، الموقع الالكتروني (https://me.kaspersky.com/resource) ، تم اسـتيراده بتاريخ ٢يوليو ٢٠٢٤م.

[3] Alexander Babuta, Innocent Until Predicted Guilty? Artificial intelligence and Police Decision – Making, Artificial intelligence and Policing, RUSI Newsbrief, March Vol . 38, No . 2, p.2.

[٤] عماد الدين محمد عبد الحميد، الشـرطة الذكية ودورها في ضـبط الجرائم في المجتمع الإماراتي، مجلة الدراسـات الإنسـانية والاجتماعية، المجلد رقم (٥٠)، العدد (٦/ ٢٠٢٣)، الإمارات، ٢٠٢٣، ص١٠٦.

إلى انتشار جرائم السطو، وبفضل استخدام البرنامج تم تقليل هذه الجرائم بنسبة تتعدى الربع خلال سنة واحدة فقط[١].

وينتقد البعض هذا البرنامج في أنه قد يؤدي إلى تحيزات عنصرية، من خلال تركيز السلطات على مناطق جغرافية معينة أو فئات محددة من المجتمع، حيث يمكن للخوارزميات تعزيز المواقف بشـــأن المواقع التي يكثر بها الإجرام مقابل الجيدة، حيث أن أحد روافد البيانات التي يعتمد عليها المداهمات السابقة للشرطة، وقد يؤدي ذلك إلى زيادة العنف من جانب الشرطة أثناء ممارسة أعمالها في استهداف تلك المناطق[٢].

ثانيًا: برنامج Hunch Lab للتنبؤ بالجريمة

البرنامج عبارة عن خوارزمية تحاول الجمع بين الجريمة والظروف المحيطة بمرتكب الجريمة والواقع الســلوكي والاجتماعي الذي يعيشــه، وتســاعد على تحديد المخاطر في مواقع وأزمنة محددة، وساهم ذلك في انخفاض الجرائم، وزيادة الشفافية والمساءلة[٣].

يمثل هذا البرنامج نظامًا لإدارة دوريات الشرطة عبر الإنترنت، ويستخدم البيانات غير المتعلقة بالجريمة كمتغيرات ضـــمن نظام التنبؤ بالجريمة، حيث تقوم النماذج الإحصـــائية المتقدمة فيه بتوقع موعد ومكان حدوث الجرائم، ويتعدى دوره في توقع الجريمة إلى معرفة أفضـل الطرق للاسـتجابة لتلك التوقعات، واقتراح الإجراءات المناسبة للتعامل معها[٤].

ثالثًا: التنبؤ الثبوتي بالجناة المحتملين وهوياتهم:

يمكن ادخال النظام الذكي في كاميرات المراقبة لا رســـال تنبيهات إلى الشـــرطة عند وجود تصـرف غير طبيعي في مكان معين، مما قد يشـير إلى إمكانية وقوع جريمة ما، وهي برامج ذكية من حيث قدرتها على تمييز الأنماط المعقدة من الســـلوك الاجرامي بدقة، وتكون بذلك قوة لردع الجريمة،

---

(1) Bilel Benbouzid, Values and Consequences in Predictive Machine Evaluation, op, cit, p .11.

(2) Bilel Benbouzid, the previous reference, p. 18.

(٣) استخدام التنبؤ لمنع الجريمة وتعزيز الأمان، الموقع الإلكتروني (fastercapital.com) تم استيراده بتاريخ ٢٠ يوليو ٢٠٢٤م.

(٤) أحمد لطفي مرعي، انعكاسات تقنيات الذكاء الاصطناعي على نظرية المسؤولية الجنائية، مجلة البحوث القانونية والاقتصادية، العدد (٨٠/ يونيو ٢٠٢٢)، المنصورة، ٢٠٢٢، ص٢٧٣.

وفي هذا الإطار تستخدم الشرطة البريطانية – في لندن ومانشستر – الدليل الإلكتروني في التنبؤ بطرفي جرائم العنف الخطيرة (الجاني – المجني عليه)، وتقوم فكرته على عرض تدخلات كوضع إشارات على الأشخاص الذين يحددهم النظام، وذلك من أجل تفادي سلوكهم الإجرامي المحتمل عبر نظام الحل الوطني لتحليلات البيانات "National Data Analytics Solution NDAS"، وفيه تم جمع بيانات هائلة من قواعد بيانات الشرطة المحلية والوطنية تتعلق بخمسة ملايين شخص بما في ذلك سجلات الذين تم القبض عليهم وتفتيشهم، وسجلات السوابق الجزائية والبلاغات المسجلة، وتمكن هذا البرنامج من استخرج ما يقرب من(١٤٠٠) مؤشر ساعد على التنبؤ بالجرائم[١].

ويرى الباحث أنه وعلى الرغم من أهمية هذه البرامج إلا أنها قد توجد بعض التحديات القانونية والأخلاقية، لأن استخدامها من قبل هذه الأجهزة دون ضوابط محددة قد يؤدي إلى فوضى يصعب السيطرة عليها، وتزداد المخاوف من استخدام هذه التقنيات دون قيود وضوابط في ظل انتشار تقنيات الذكاء الاصطناعي.

الفرع الثاني

إنشاء مركز الدفاع الإلكتروني

تعمل مراكز الأمن السيبراني من خلال وحدات متخصصة مزودة بالأجهزة والمعدات التكنولوجية المتطورة، يناط بها رصد ومراقبة المواقع المشبوهة على شبكة الإنترنت، وفحص شبكات وأنظمة المعلومات المراد حمايتها وتزويد تلك الوحدات بأحدث أجهزة الاتصالات السلكية واللاسلكية الالكترونية، وربطها بالأجهزة الأمنية المختصة لنقل وتبادل المعلومات ودعم اتخاذ القرار[٢].

بات الأمن السيبراني مصدر قلق كبير للعديد من الحكومات بسبب نمو الهجمات السيبرانية، حيثُ أصبحت الدول تضع مسائل الأمن السيبراني في أعلى هرم أولوياتها، في ظل تصاعد الحروب

---

(1) Fieke Jansen, Date Driven Policing in the Context of Europe, working paper, datajusticeproject, Cardiff University, May 2018, p. 6-7.

[٢] عبد الكريم درويش، نحو استراتيجية للموارد البشرية في المؤسسات الشرطية، مجلة الفكر الشرطي، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، المجلد التاسع، العدد الثاني، يوليو ٢٠٠٠م، ص٢٧.

السيبرانية التي تهدد سيادة الدول واستقلالها بصفته سلاح فعال للنيل من الخصوم،[١] ومن هنا جاء إنشاء مركز الدفاع الإلكتروني بموجب المرسوم السلطاني رقم (٦٤ / ٢٠٢٠) ويتبع جهاز الأمن الداخلي[٢]، ويلعب دورًا مهمًا وحيويًا في حماية البنية التحتية الرقمية ومكافحة التهديدات السيبرانية، ويكون الجهة المختصة بأمن الفضاء الإلكتروني في السلطنة[٣].

يهدف المركز إلى تعزيز مؤسسات الدولة والأفراد للتصدي للتهديدات السيبرانية، وفتح قنوات التعاون الإقليمي والدولي في هذا المجال، ويتولى المركز في سبيل تحقيق ذلك متابعة جاهزية البنى الأساسية الرقمية والجهات المختصة بها، ووضع الموصفات والمعايير التقنية ذات صلة باختصاصه، والتصدي لأي هجمات سيبرانية تتعرض لها مؤسسات القطاع العام والخاص، ويمارس دور الضبطية القضائية في الجرائم المتعلقة باختصاصه، وفحص أنظمة وشبكات المؤسسات العامة والخاصة للتأكد من سلامتها، والإشراف على تنفيذ التزاماتها طبقًا للاتفاقيات الدولية التي صادقت عليها السلطنة[٤].

وضع مركز الدفاع الإلكتروني استراتيجية وطنية للدفاع الإلكتروني وتم اعتمادها من قبل مجلس الأمن الوطني[٥]، لتحقيق أعلى مستويات الأمن الرقمي وتمكين السلطنة من فضاء إلكتروني آمن، يساعدها على تحقيق أهداف رؤية عمان ٢٠٤٠[٦].

في إطار تطوير قدرات المركز التقنية، وقع المركز عدة اتفاقيات مع شركات عالمية في مجال تقنية المعلومات ولعل أبرزها مع شركة مايكروسوفت في عام ٢٠٢٣م، من أجل توحيد الرؤى والجهود

---

[١] هيئة التحرير بمعهد الأمير سعود الفيصل للدراسات الدبلوماسية، درع المملكة الواقي لحماية مصالحها الحيوية وبنيتها التحتية الرقمية، مجلة الدبلوماسي، العدد (٩٠)، السعودية، ٢٠١٨، ص٩ –١٠.

[٢] جهاز الأمن الداخلي هو "إحدى المؤسسات الرسمية في سلطنة عُمان، مهمته حماية الدولة، وضمان استقرارها ووحدتها، وكفالة الأمن والطمأنينة للمواطن والمقيم، ويشرف على الأمن بصورة عامة ومن بينها أمن الفضاء الإلكتروني، فضلًا عن مكافحة جرائم أمن الدولة والإرهاب".

[٣] المادة (٢) من المرسوم السلطاني رقم ٦٤ / ٢٠٢٠ بإنشاء مركز الدفاع الإلكتروني.

[٤] المادتين (٥، ٦) من المرسوم السلطاني رقم ٦٤ / ٢٠٢٠ بإنشاء مركز الدفاع الإلكتروني.

[٥] يختص مجلس الأمن الوطني بالنظر في كافة الموضوعات المتعلقة بالأمن الوطني في سلطنة عُمان، ويترأسه جلال السلطان القائد الأعلى، انظر المرسوم السلطاني رقم (١٣/ ٢٠٢١).

[٦] الاستراتيجية الوطنية للدفاع الإلكتروني ٢٠٢٢ – ٢٠٢٥، المنشورة في الموقع الإلكتروني الرسمي لمركز الدفاع الإلكتروني (https://cdc.gov.om)

الرامية إلى حماية الفضـــاء الإلكتروني[١]، كما وقع مذكرة تفاهم مع شـــركة "وكاســـبرســـكي" في مايو ٢٠٢٤م، لتبادل التعاون في الأمن السيبراني، والتعاون في التنبؤات حول الهجمات السيبرانية، والتدريب والمؤتمرات المتعلقة بالأمن السيبراني[٢].

يقدم المركز برامج تدريبية عبر أكاديمية الأمن الإلكتروني المتقدم[٣] بالإضـافة الى محاضـرات توعويـة في مجـال الأمن الإلكتروني؛ لرفع مســـتوى الكفـاءات الوطنيـة العـاملـة في مجـال الأمن الإلكتروني، وتعزيز قطـاع تكنولوجيا المعلومـات والاتصـــــالات وتمكين القطـاعين العام والخـاص من الدفاع ضد الهجمات السيبرانية[٤].

يعمل مركز الدفاع الإلكتروني وفق اســتراتيجية وطنية معتمدة يتم تنفيذها بالتعاون مع مختلف الجهات لمواجهة التهديدات المتنامية، حيثُ أن المركز قد تعامل مع (٢٢٠) تهديد أمني من داخل وخارج الســـلطنة خلال عام ٢٠٢٣م، وتم التنســـيق بشـــأنها مع الجهات المتأثرة لســـد الثغرات الفنية ومعالجتها بأقل الأضـــرار وفق منهجية معتمدة للاســـتجابة مع الحوادث الإلكترونية، وتتم بعض هذه التهديدات بدافع الفضـــول وبعضـــها يتم من قبل مجموعات محترفة، وتشـــير الإحصـــاءات إن قطاع الخدمات أكثر القطاعات اسـتهدافًا، ويسـعى المركز إلى تحديد الأطر القانونية لملاحقة المخترقين من خارج السـلطنة عبر إبرام اتفاقيات التعاون مع المؤسـسـات النظيرة خارج السـلطنة وداخلها، ومذكرات التفاهم لتبادل المعلومات والتعاون في التحقيق وتقصي حوادث التهديدات الإلكترونية[٥].

---

[١] الموقع الإلكتروني الرســمي لشــركة مايكروســوفت (https://news.microsoft.com/en)، المنشــور بتاريخ ١٩ نوفمبر ٢٠٢٣م، تم استيراده بتاريخ ٢٣ يوليو ٢٠٢٤م.

[٢] الموقع الإلكتروني الرسمي لشركة كاسبرسكي (https://me.kaspersky.com) المنشور بتاريخ ٣٠ مايو ٢٠٢٤م، تم استيراده بتاريخ ٢٣ يوليو ٢٠٢٤م.

[٣] تم إنشـاء أكاديمية الأمن الإلكتروني المتقدم في عام ٢٠١٨م بهدف رفع القدرات الوطنية في مجال الأمن الإلكتروني، بالشـراكة مع جامعة التقنية والعلوم التطبيقية.

[٤] تدشين أول أكاديمية للأمن الإلكتروني المتقدم بالسلطنة، صحيفة الشبيبة الإلكترونية، نشر تاريخ ١٨ نوفمبر ٢٠١٨م، الموقع الالكتروني (https://shabiba.com) تم استيراده بتاريخ ٢٥ يوليو ٢٠٢٤م.

[٥] إذاعة الوصال، سلطنة عُمان، إيناس ناصر، الدكتور/ خميس الحجري – رئيس مركز الدفاع الإلكتروني، تمت المقابلة في ٢٨ مايو ٢٠٢٤م.

الجدير بالذكر أن المركز مسؤوليته تقتصر على حماية الفضاء الإلكتروني للمؤسسات الحكومية والقطاع الخاص، وفي حال تعرض الأفراد للاختراق أو الابتزاز الإلكتروني فإن ذلك لا يدخل في اختصاص المركز، وإنما ضمن اختصاص الادعاء العام أو شرطة عُمان السلطانية[١].

إضافة إلى مركز الدفاع الإلكتروني أنشأت السلطنة هيئات أخرى تضطلع بأدوار مشابهة في مكافحة الجرائم السيبرانية، ومنها:

أولًا: مركز السلامة المعلوماتية التابع لوزارة النقل والاتصالات وتقنية المعلومات

تم إطلاق أعمال المركز الوطني للسلامة المعلوماتية التابع لوزارة النقل والاتصالات وتقنية المعلومات في الربع الأول من عام ٢٠١٠م، الذي يُعتبر أحد أهم مشاريع مبادرة عمان الرقمية، بعد تفعيل العديد من المشاريع الأساسية مثل بوابة الدفع الإلكتروني ومركز البيانات الوطني ومركز أمن المعلومات والشبكة الحكومية الموحدة، ويهدف إنشاء هذا المركز إلى تعزيز الثقة في استخدام الخدمات الإلكترونية الحكومية عبر الإنترنت وبناء كوادر عمانية مؤهلة للتعامل مع الحوادث الأمنية وكشفها والاستجابة لها[٢].

ويسعى المركز أيضًا إلى بناء وتعزيز الوعي الثقافي بأمن المعلومات وأمن الحواسيب لدى مختلف شرائح المجتمع، وتوفير معلومات دقيقة وفي الوقت المناسب عن المخاطر والتهديدات ووسائل الحماية منها، كما يهدف إلى اتخاذ خطوات وتدابير احترازية لتجنب وتقليل التعرض للمخاطر والتهديدات الأمنية للحواسيب والاستجابة السريعة والفعالة لحوادث الحواسيب الأمنية[٣].

وتأتي جهود المركز في ظل تزايد مخاطر الجرائم المعلوماتية، خاصةً تلك المرتبطة بشبكة الإنترنت، وحصل المركز على اعتراف دولي من منظمات متخصصة في هذا المجال، وانضم إلى منظمات دولية متخصصة مثل التجمع العالمي لفرق الاستجابة لحوادث الأمن المعلوماتي، ولجنة

---

[١] اختصاصات مركز الدفاع الإلكتروني، الموقع الإلكتروني الرسمي لمركز الدفاع الإلكتروني (https://cdc.gov.om/)، تم استيراده بتاريخ ٢٥ يوليو ٢٠٢٤.

[٢] الموقع الإلكتروني الرسمي لمركز السلامة المعلوماتية (https://cert.gov.om)

[٣] الموقع الالكتروني (https://cop.gov.om/about.aspx)، تم استيراده بتاريخ ٥ أغسطس ٢٠٢٤.

المراكز الوطنية للاستجابة لطوارئ الحواسيب في دول مجلس التعاون لدول الخليج العربي، ومنظمة المؤتمر الإسلامي لفرق الاستجابة لحوادث الحواسيب[١].

يقدم المركز مجموعة متنوعة من الخدمات التي تتناسب مع المهام الملقاة على عاتقه والأهداف المحددة له، ويمكن تلخيص هذه الخدمات على النحو التالي[٢]:

١. **الخدمات التفاعلية:** تم تصميم هذه الخدمات للاستجابة لطلبات المساعدة وتقارير الحوادث من المستفيدين من خدمة المركز الوطني للسلامة المعلوماتية، بالإضافة إلى استجابة فورية لأي تهديدات أو هجمات ضد نظم المركز.

٢. **الخدمات الاستباقية:** تم تصميم هذه الخدمات لتحسين الأمن الإلكتروني للمستفيدين من الخدمة قبل وقوع أي حادث أمني، وتتضمن توفير المساعدة التقنية والمراقبة الفنية، وتقييم الثغرات الخارجية واختبار الاختراق، وتوفير التوعية والتدريب للهيئات المستفيدة.

٣. **التنبيهات الأمنية والتحذيرات:** يتم نشر معلومات تشرح بعض الحوادث الأمنية وتوفير الإرشادات اللازمة للتعامل معها بشكل صحيح، بالإضافة إلى إخطار الوحدات المعنية وتبادل المعلومات حول كيفية التعامل مع التهديدات الأمنية.

٤. **تقييم الثغرات الخارجية واختبار الاختراق:** يتم تقييم الثغرات الخارجية واختبار الاختراق بشكل دوري لضمان تأمين البنية الأساسية للمؤسسة والتحقق من استمرار تحديثات الأمان.

٥. **اكتشاف تهديدات جديدة عبر البحث والتحليل:** يتم مراقبة التهديدات الجديدة في الفضاء السيبراني وتحليلها لاكتشاف أي نقاط ضعف في الأنظمة واتخاذ التدابير الوقائية المناسبة.

٦. **مراقبة المواقع الإلكترونية:** يتم مراقبة المواقع الإلكترونية لتحليل أي معلومات متعلقة بالحوادث الأمنية واتخاذ الإجراءات الضرورية.

---

[١] المركز الوطني للسلامة المعلوماتية – بوابة عماننا (https://omanportal.gov.om)، تم استيراده بتاريخ ٥ أغسطس ٢٠٢٤.

[٢] علي بن خلفان الهنائي، الحس الأمني لدى رجال الشرطة: تعريفه وأهميته وخصائصه وأهدافه، أكاديمية السلطان قابوس لعلوم الشرطة، سلطنة عُمان، ٢٠٢١، ص٢٢.

٧. **التدريب الأمني والتوعية:** تقديم التدريب والتوعية لزيادة الوعي بأهمية الأمان السيبراني والتحكم في مخاطر الأمن عبر الإنترنت.

في فبراير ٢٠١٦م دَشَّن المركز الوطني للسلامة المعلوماتية المختبر الوطني للأدلة الرقمية، مهمته مساعدة الجهات المختصة بإنفاذ القانون في توفير الأدلة الرقمية، وهو متخصص في إثبات ارتكاب الجرائم السيبرانية وتحليل الأدلة الرقمية، وتقديمها أمام السلطة القضائية، وقد حصل المختبر على الاعتراف الدولي في عام ٢٠١٧م، الأمر الذي يعزز مصداقية النتائج التقارير الصادر عنه في المحاكم المحلية والدولية، ويقوم المركز بتحليل البيانات الرقمية الصوتية والمرئية، وتحليل أجهزة الحاسب الآلي والهواتف الذكية واسترجاع البيانات، والابتزاز الإلكتروني[١].

ثانيًا: إدارة الدعم الفني التابعة للادعاء العام

إدارة الدعم الفني التابعة للادعاء العام، والتي كانت تُعرف سابقًا بمختبر الأدلة الجنائية، تلعب دورًا حيويًا في تقديم الدعم التقني والفني للتحقيقات الجنائية والقضايا القانونية، والمساهمة في توفير الأدلة الرقمية في القضايا المختلفة، وتم تفعيل قسم الأدلة الرقمية في عام ٢٠١٤م، ويختص بتحليل الأدلة المحالة إليه، وتم تأهيل مجموعة من الكفاءات الوطنية للعمل في هذه الإدارة، وتقوم بتحليل الأجهزة الإلكترونية وفحصها وتحليل بياناتها للوصول إلى الحقيقة وكشف ملابسات القضية[٢].

ثانيًا: إدارة الجرائم الاقتصادية بالإدارة العامة للتحريات والتحقيقات الجنائية التابعة لشرطة عمان السلطانية

أولت شرطة عمان السلطانية اهتمامًا خاصًا بالجرائم السيبرانية، حيثُ أنشأت قسم متخصص في تحليل الأدلة الرقيمة، يتبع إدارة الجرائم الاقتصادية بالإدارة العامة للتحريات والتحقيقات الجنائية اعتبارًا من ٩ مايو ٢٠٠٤م، بالإضافة إلى الجهود الرامية إلى تعزيز مكافحة هذه الجرائم، نوجزها في الآتي[٣]:

---

[١] المختبر الوطني للأدلة الرقمية، الموقع الإلكتروني الرسمي لمركز السلامة المعلوماتية، (https://cert.gov.om).

[٢] مختبر الأدلة الجنائية يتجه لإضافة (الوسائط المتعددة)، صحيفة الوطن العُمانية، نشر تاريخ ٢٥ أبريل ٢٠١٦، الموقع الالكتروني (https://alwatan.om)، تم استيراده بتاريخ ٣٠ يوليو ٢٠٢٤م.

[٣] الموقع الالكتروني (http://hussain-alghafri.blogspot.com/2011/07/blog-post_9603.html)، تم استيراده بتاريخ ٥ أغسطس ٢٠٢٤.

أ. عقد العديد من الندوات والدورات، أو المشـــاركة فيها، بالتعاون مع بعض الجهات المختصـــة، لنشر الوعي والتنبيه بمخاطر هذه الجرائم.

ب. إعداد الدراسات والبحوث والإحصاءات السنوية حول الجرائم السيبرانية في السلطنة.

ج. التنسـيق والتعاون مع السـلطات المختصـة في الدول الأخرى، ومع الهيئات والمنظمات الدولية والإقليمية، لتبادل الخبرات في مجال مكافحة هذا النوع المســـتحدث من الجرائم، مثل اللجنة العربية لأمناء العدل والإنتربول.

ويتضـح مما تقدم سـعي السـلطنة الجاد لمواجهة الجرائم السـيبرانية عبر إصـدار قانون مكافحة جرائم تقنية المعلومات، وتطوير مختبرات البحث الجنائي المختصـــة بالجرائم الســـيبرانية، مثل مختبر للأدلة الرقمية التابع للمركز الوطني للســلامة المعلوماتية التي تشــرف عليها وزارة النقل والاتصـــالات وتقنية المعلومات، وإدارة الدعم الفني التابعة للادعاء العام، بالإضـــافة إلى إدارة مكافحة الجرائم الاقتصـــادية والإلكترونية التابعة للإدارة العامة للتحريات والبحث الجنائي بشـــرطة عمان الســـلطانية، ومركز الدفاع الإلكتروني التابع لجهاز الأمن الداخلي، الصادر بالمرسوم السلطاني رقم (٢٠٢٠/٦٤).

المبحث الثاني

إجراءات مواجهة الجرائم السيبرانية وتحدياتها في القانون العُماني

مما لا شــك فيه أن المجرم الإلكتروني يتمتع بصــفات خاصــة من الذكاء والمهارة تمكنه من تنفيذ سلوكه الإجرامي بمنتهى الاحتراف مستغلا خبرته ومهارته في تنفيذ الجريمة، إلا أن ذلك لا يعني استحالة معاقبته أو إفلاته بجرمه[١].

ســوف يســعى هذا المبحث إلى تحليل إجراءات مكافحة الجريمة الســيبرانية والتحديات التي تواجهها في القانون العُماني، ويتناول المبحث في مطلبين رئيســيين، الأول حول إجراءات التحقيق الخاصة بالجريمة السيبرانية والثاني حول التحديات القانونية في مكافحة هذه الجرائم.

المطلب الأول

إجراءات التحقيق الخاصة بالجرائم السيبرانية في القانون العُماني

تعتبر الجرائم السيبرانية من التحديات الرئيسية التي تواجه السلطات القانونية في السلطنة[٢]، حيث تتطلب مكافحتها إجراءات خاصــة وفعالة للتحقيق وجمع الأدلة الرقمية ومعاقبة المتورطين وفقًا للقانون[٣]، وانطلاقًا من أهمية تبني إجراءات فعالة للتحقيق في جرائم الإنترنت والجرائم الســيبرانية في القانون العُماني، والاستعانة بالخبراء واستخدام التقنيات الرقمية المتطورة في هذا السياق، سوف يتناول هذا المطلب إجراءات التحقيق الخاصــة بالجريمة الســيبرانية في القانون العُماني، حيث يُقســم المطلب إلى فرعين رئيسيين: جمع الأدلة الرقمية وتحليلها، والاستعانة بالخبراء والمختبرات الرقمية.

---

[١] غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت "وجرائم الاحتيال المنظم باستعمال شبكة الإنترنت، دار الفكر والقانون، المنصورة، ٢٠١٧، ص١٣.

[٢] حفيظة بنت سليمان البراشدى، الفيسبوك والجرائم الإلكترونية في عمان، مجلة دراسات المعلومات والتكنولوجيا، المجلد (٢)، العدد (٢)، دار جامعة حمد بن خليفة للنشر، قطر، ٢٠١٩، ص٣.

[٣] محمد كمال محمود الدسوقي، مرجع سابق، ص١٤.

الفرع الأول

جمع الأدلة الرقمية وتحليلها

إن الاهتمام الذي يحظى به الدليل الرقمي مرده انتشـــار اســـتخدام تقنية المعلومات الرقمية، والتي تعاظم دورها مع دخول الانترنت شتى مجالات الحياة، وأصبح بذلك هذا الوسط مرتعًا لطائفة من الجناة يطلق عليهم اسم المجرمين المعلوماتيين أو السيبرانيين[١].

بشأن مراحل الإجراءات التي يبرز فيها استخدام وسائل التقنية الحديثة، فإن استخدام الأساليب والوسـائل العلمية للتقنية الحديثة في مجال الإثبات الجزائي يجعل عملية الإثبات قابلة للتجديد والتطور وفقًا لتطور العلوم التقنية والطبية والكيميائية وغيرها، التي يجب الأخذ بنتائجها بما لا يتعارض مع الضـمانات التشـريعية والطبيعية لحقوق الإنسـان والتي تحقق حرية وإرادة الإنسـان سـواء كان متهمًا أو شاهدًا أو مجنيًا عليه[٢].

اختلف الفقه في تعريف الدليل الرقمي، حيثُ اتجه البعض منه إلى التوســـع في التعريف، والبعض الآخر اتجه إلى تضييقه وحصره في جوانب محددة، وعرفه البعض بأنه: «دليل له أساس في العالم الافتراضـي التكنلوجي والتقني ويقود إلى الجريمة»[٣]، وكذلك عُرِّف بأنه: «معلومات يقبلها العقل والمنطق ويقرها العلم، يتحصـــل عليها بموجب إجراءات قانونية وعلمية بعد ترجمة البيانات الحســـابية المخزنة في أجهزة الحاسـب الآلي وملحقاتها وشـبكات الاتصـال، ويمكن اسـتخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شـــيء أو شـــخص له علاقة بجريمة أو جانٍ أو مجني عليه»[٤].

---

[١] خالد ممدوح إبراهيم، الدليل الإلكتروني في الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٨، ص٢.

[٢] أشرف سيد أبوالعلا، الحماية الجنائية لحق الإنسان في الصحة (دراسة مقارنة بين القانون الوضعي والشريعة الإسلامية)، دار النهضة العربية، القاهرة، ٢٠٢٢، ص٢١.

[٣] أشرف عبدالقادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، ٢٠١٥، ص١٢٣.

(٤) محمد الأمين البشري، التحقيق في الجرائم المستحدثة، جامعة نايف للعلوم الأمنية، الرياض، ط١، ٢٠٠٤، ص٢٣٤.

تحتوي البيئة الافتراضـــية للدليل الرقمي على بيانات رقمية متعددة، وهي التي يســـتمد منها الدليل، ونظرًا لطبيعته التقنية فإنه يتمتع بخصـــائص تميزه عن باقي الأدلة، ولعل أبرزها البيئة والنطاق الافتراضـــي الذي يتواجد به الدليل، ويتطلب الاســـتعانة بالأجهزة والأشـــخاص المختصـــين بالتعامل معها[١]، كما أنه متنوع ومتطور يظهر على هيئات مختلفة، ومع تقدم التكنولوجيا يتقدم الإجرام باستخدام هذه الوسائل، ويتطلب معها مواكبة هذا التطور بصورة مستمرة بالنسبة للسطات المعنية بمكافحة الجريمة[٢] كما أنه قابل للنســـخ، وحيث أن الأصـــل أنه عند إعداد نســـخة من محتوى الدليل التقليدي فإن قوته لن تكون مثل قوة الأصـــــل في حجية إثباته، إلا أن ذلك يختلف في مجال الدليل الرقمي فهو دليل يمكن اســـتخراج نســـخ منه مطابقة للأصـــل ويكون لتلك النســـخة ذات القيمة العلمية للأصل، وهي ضمانة للحفاظ على الدليل من الفقد أو الحذف أو التغيير أو التلف[٣].

يتميز الدليل الرقمي أنه دليل متنوع، وله صـــــور وأشـــــكال عديدة، لذلك فقد ذهب الفقه إلى تقسيمها إلى أربعة أقسام رئيسية، وهي[٤]:

١. الأدلة الرقمية المتعلقة بأجهزة الكمبيوتر وشبكاتها.

٢. الأدلة الرقمية المتعلقة بالإنترنت، ويشمل المحتوى الموجود على الويب، مثل الصفحات والمواقع الإلكترونية، والبيانات التي يتم تبادلها عبر الشبكة.

٣. الأدلة الرقمية المتعلقة ببرتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.

٤. الأدلة الرقمية الخاصـــة بالشـــبكة العالمية، كالبيانات التي تتعلق بالوصـــول إلى خدمات الشـــبكة العالمية، بما في ذلك سجلات الوصول والأنشطة المتعلقة بالمتصفح.

---

[١] عائشة بن قارة، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية، ٢٠١٠، ص٦١-٦٢.

[٢] حازم محمد حنفي، الدليل الإلكتروني ودوره في المجال الجنائي، دار النهضة العربية، القاهرة، ط١، ٢٠١٧، ص١٩ -٢٠.

[٣] عائشة بن قارة مصطفى، مرجع سابق، ص٦٤.

[٤] مسعود المعمري، الدليل الإلكتروني في إثبات الجريمة الإلكترونية، مجلة كلية القانون الكويتية العالمية، العدد (٣)، الكويت، ٢٠١٨، ص٢٠١.

هناك اتجاه فقهي آخر يقسم الدليل الإلكتروني إلى نوعينً رئيسيين، وهما:

١. **أدلة أعدت لتكون وسيلة إثبات:** وهذا النوع يتمثل في البيانات التي يتم إنشاؤها تلقائيًا بواسطة الأجهزة الإلكترونية كجهاز الحاسب الآلي والهاتف النقال وسجلات البطاقة البنكية، حيث أنها تحتفظ بالبيانات بصورة تلقائية دون تدخل شخص لحفظها[١].

٢. **أدلة لم تعد لتكون وسيلة إثبات:** ينشأ هذا النوع دون إرادة الشخص، ويسمى بالبصمةً الإلكترونية، ويتمثل فيما يتركه الشخص عند استخدام الأجهزة أو الشبكات من بيانات يتم تسجيلها بصورة تلقائية[٢].

إن التطور المتسارع في الجرائم السيبرانية ووسائل تنفيذها، يجعل السلطات القائمة على مكافحتها في سباق مع الزمن لمواكبة هذا التطور، ويدعو السلطات القضائية إلى مراجعة آلية التعامل مع هذه التطورات بسبب المشكلات التي تثيرها بسبب طبيعتها غير المادية والأدلة غير الملموسة التي تنتج عنها، على ضوء ذلك سوف يتم تقسيم إجراءات الحصول على الدليل الرقمي إلى الإجراءات التقليدية والإجراءات الحديثة، باستثناء الخبرة التي يتم تناولها في فرع مستقل، نظرًا لأهميتها في إثبات الجرائم السيبرانية.

أولًا: الإجراءات التقليدية في الحصول على الدليل الرقمي:

١. **المعاينة:** أول خطوة يقوم بها مأمور الضبط القضائي عند وقوع الجريمة هي الانتقال إلى مسرح الجريمة، للتحفظ على الأدلة المادية لها، وفي الجرائم السيبرانية يتعين أن نفرق بين مسرحين: **مسرح تقليدي:** وهو ما يقع خارج بيئة الحاسب الآلي والإنترنت، وهي الأدلة المادية المحسوسة التي يتحصل عليها في موقع ارتكاب الجريمة، كالأدوات المستخدمة في ارتكاب الجريمة والبصمات، والوسائط التخزينية الرقمية وغيرها[٣]، **ومسرح افتراضي** وهو ما يقع في البيئة الرقمية، وتتكون من بيانات رقمية في الحاسب الآلي وشبكة الإنترنت، والتعامل مع هذه الأدلة

---

[١] أمير فرج يوسف، الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها، مكتبة الوفاء القانونية، الإسكندرية، ط١، ٢٠١٦، ص٢٩٠.

[٢] أمير فرج يوسف، المرجع سابق، ص٢٩٠.

[٣] عائشة بن قارة، مرجع سابق، ص٨٤.

يتطلب كفاءات متخصصة عالية المهارة والكفاءة[١].

٢. **التفتيش:** للتفتيش في الجرائم الإلكترونية طبيعته خاصـــة تختلف عن التفتيش التقليدي، إلا أنه يخضـــع في إجراءاته لنصـــوص قانون الإجراءات الجزائية التي تتطلب وقوع الجريمة، والمتهمين بارتكابها بالإضـــافة إلى وجود قرائن تفيد في كشـــف الحقيقة عبر الأجهزة الإلكترونية[٢]، وترتبط الأجهزة الإلكترونية وأجهزة الحاسب الآلي مع بعضـها البعض بشـبكات اتصـال محلية أو دولية، وتحتاج هذه البيانات خبرات فنية لتفتيشـها، ويسـهل تفتيش البيانات المخزنة على هذه الأجهزة، أما المعلومات غير المخزنة على الأجهزة والمتداولة عبر الشـــبكات فإنها تتطلب مهارة عالية عند التعامل معها لاسـتخراج المعلومات والبيانات التي تحتويها، وذوي خبرة في هذه الشـبكات والتقنيات لاســـتخراجها عند تفتيش المحتوى المعنوي للأجهزة، كما أنها قد تحتاج إلى أذونات والتنســـيق مع أصحاب المواقع الإلكترونية للحصول على المعلومات التي تفيد في كشف الجريمة[٣].

وقد نص المشـــرع العُماني في المادتين (٣٣، ٨٨) من قانون الإجراءات الجزائية[٤] على اختصـاص مأمور الضـبط القضـائي بضـبط كل ما يتعلق بالجريمة وما يحتمل أن يكون اسـتعمل في ارتكابها أو يساعد في الكشف عن الحقيقة، وهو ما يعني أن المشرع العُماني أخذ كذلك بالاتجاه الذي يرى بأن ضـــبط الأدلة الإلكترونية يمكن أن يتم من جميع أشـــكال البيانات التي تتيحها الأجهزة الإلكترونية، ومنها المكونات المعنوية وبالتالي مشـروعية تفتيش هذه المكونات وإمكانية ضـبطها، وفقًا للإجراءات المقررة في هذا الشأن.

٣. **الشهادة:** فالشهادة من أدلة الإثبات التي يعتمد عليها القضاء، ويستمع القاضي إلى الذين شهدوا ارتكابها من غير أطراف الخصـومة؛ من أجل كشـف وقائعها والوصـول إلى الحقيقة، من خلال إفصـــاحهم عن البيانات ومعلومات حول الواقعة محل الاســـتدلال أو التحقيق أو المحاكمة،

---

[١] حازم محمد حنفي، مرجع سابق، ص٥٥-٥٦.

[٢] حازم محمد حنفي، المرجع سابق، ص٤١-٤٢.

[٣] سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية: دراسة تحليلية، دار الكتب القانونية، مصر ،٢٠١١، ص٢١٧-٢١٨.

[٤] قانون الإجراءات الجزائية الصادر بالمرسوم السلطاني رقم ٩٧ / ٩٩، نشر هذا المرسوم في عدد الجريدة الرسمية رقم (٦٦١) الصادر في ١٥ / ١٢ / ١٩٩٩م.

ويختلف الشاهد في الجرمية السيبرانية عن الشاهد في الجرائم التقليدية، الذي غالبًا ما يكون ذا خبرة فنية في التقنية والتكنولوجيا، ويكون ضمن فئات أو طوائف مختصة بذلك المجال مثل مشغلو الأجهزة، ومحللو البيانات، والمبرمجون، ومهندسو الصيانة والاتصالات، ومديرو النظم، ولا تختلف الإجراءات والشروط الواجب توافرها في الشاهد في الجرائم السيبرانية عنه في الجرائم التقليدية، وأصدرت بعض التشريعات لوائح وقرارات خاصة تحصر فيها شهود الجريمة الإلكترونية، من بينها المشرع في ولاية كاليفورنيا الأمريكية[١].

ثانيًا: الإجراءات الحديثة في الحصول على الدليل الإلكتروني:

أقر وزراء العدل العرب في مايو ٢٠٠٣م القانون العربي النموذجي الموحد لمكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات، وبادرت السلطنة في إصدار قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم (رقم ٢٠١١/١٢)، الذي اقتصر على بيان الجرائم، ولم يتناول طرق وإجراءات الحصول على الأدلة الرقمية، وهو الحال بالنسبة للتشريعات العربية النظيرة.

تُعتبر الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية (بودابست) من أبرز الاتفاقيات الدولية المعنية بمكافحة الجرائم السيبرانية، تحت إشراف المجلس الأوروبي ووقعت عليها (٣٠) دولة، منها أربع من خارج الاتحاد الأوروبي هي: اليابان وكندا والولايات المتحدة الأمريكية وجنوب أفريقيا، وهدفت إلى هو وضع سياسة جزائية مشتركة لمكافحة الجريمة السيبرانية عن طريق مواءمة القوانين الوطنية مع نصوص الاتفاقية لضمان توفير الحماية الكافية للمجتمع من هذه الجرائم، وفرقت اتفاقية "بودابست" بين نوعين من البيانات، وهي البيانات المخزنة أو الساكنة، والبيانات المتحركة أو البيانات المتعلقة بخط سير المعلومات، وأقرت الاتفاقية إجراءات جديدة لجمع الأدلة الرقمية [٢].

أقرت الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية (بودابست) إجراءات جديدة لجمع الأدلة الإلكترونية، ونبين تاليًا أهم تلك الإجراءات:

١. التحفظ السريع أو المستعجل على بيانات الحاسب المخزنة، بما يمكن السلطات المختصة ضبط

---

[١] هلالي عبد اللاه أحمد، التزام الشاهد بالإعلام في الجريمة المعلوماتية، دار النهضة العربية، القاهرة، ٢٠٠٠، ص٢٤.

[٢] عادل عزام، جرائم القدح والذم والتحقير المرتكبة عبر الوسائط الإلكترونية: دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمّان، ٢٠١٩، ص٣٦٥.

البيانات قبل تعرضها للفقد والتلف والتعديل[١].

٢. منح السلطات صلاحيات الكشف الجزئي على بيانات الحركة المخزنة لدى مزود الخدمة، لتحديد مصدرها وهوية مرتكب الجريمة السيبرانية[٢].

٣. منح السلطات صلاحيات في توجيه الأمر إلى أي شخص يتواجد في إقليم الدولة لتقديم البيانات الإلكترونية المتوفرة بحوزته أو تحت سيطرته، أو مخزنة داخل نظام حاسوبي، أو على أي وسيط تخزين بيانات آخر، وطلب أي بيانات من مزودي الخدمات داخل إقليم الدولة[٣].

٤. إعطاء السلطات صلاحية البحث في البيانات المعنوية المخزنة في أجهزة الحاسب الآلي ومصادرتها بهدف الحصول على الدلة الرقمية.[٤]

ويثور التساؤل حول مدى كفاية القواعد الإجرائية التقليدية في مواجهة الجرائم الإلكترونية المتطورة، أم أنها تتطلب إجراءات خاصة لمواجهتها وإثباتها، وفي ذلك قال البعض أن القواعد الإجرائية التقليدية تصلح في مواجهة جميع أنواع الجرائم بما فيها الجرائم السيبرانية، مع إجراء التعديلات عليها بما يتناسب مع طبيعة الجرائم السيبرانية[٥]، وهو الرأي الذي يرجحه الباحث، حيثُ أن إجراء التعديلات هو الأنسب في هذه المرحلة، بما يوفر المرونة اللازمة للتكيف مع التطورات المستقبلية، والحفاظ على وحدة القانون الإجرائي وبساطته وتجنب توزيعه وتعقيده، وتعزيز سرعة وفاعلية تطبيق القانون، مع تقييم فاعلية هذه التعديلات في سد الثغرات الإجرائية التي أفرزتها الجرائم السيبرانية، مما يجعله الخيار الأمثل في الوقت الراهن.

وهناك من يرى أن القواعد الإجرائية التقليدية باتت قاصرة في مواجهة الجرائم السيبرانية لأن مباشرتها تتم في بيئة رقمية لا تنسجم مع البيئة التقليدية، وقد يشكل ذلك مساسًا بالشرعية الإجرائية بصورة عامة وبحقوق الأفراد بصفة خاصة، وحق المجتمع في اقتضاء العقوبة، ويدعو أنصار هذا

---

[١] المادة (١٦) من اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

[٢] البند (١٦٦) من التقرير التفسيري لاتفاقية "بودابست"، المجلس الأوروبي، سلسلة المعاهدات الأوروبية رقم (١٨٥).

[٣] المادة (١٨) المرجع السابق.

[٤] البند (١٨٤) من التقرير التفسيري لاتفاقية "بودابست"، المجلس الأوروبي، سلسلة المعاهدات الأوروبية رقم (١٨٥).

[٥] محمد زروق، إشكالية الحصول على الدليل الإلكتروني في الجريمة المعلوماتية، مختبر البحث في قانون الأعمال، جامعة الحسن الأول، العدد (٣٣)، المغرب،٢٠١٨، ص١٥٠.

الاتجاه إلى إفراد قواعد خاصة بإجراءات البحث وجمع الأدلة في هذا النوع من الجرائم، وهو ما فرضته مجموعة من الاعتبارات، ومنها قصور الإجراءات التقليدية في التصدي للجرائم الإلكترونية، وما تثيره هذه الجرائم من صعوبات في تحديد الاختصاص والقانون الواجب التطبيق بين الدول التي ارتكبت على أراضيها، باعتبارها عابرة للحدود والجغرافيا[١].

الفرع الثاني

الاستعانة بالخبراء والمختبرات الرقمية

إذا كان للخبرة ذلك الدور والأهمية في الجرائم التقليدية، فإن تلك الأهمية تتضاعف وتصبح ضرورية في إجراءات جمع الأدلة الرقمية لإثبات الجريمة السيبرانية، حيث إن هذه الجرائم تتعلق بمسائل فنية غاية في التعقيد، كما أن محل الجريمة فيها ليس بصورة مادية، إضافة للتطور المستمر في أساليب ارتكابها وتطور وتنوع الأدوات المستخدمة فيها، فالأجهزة الإلكترونية متنوعة ومتعددة وكذلك شبكات الاتصال، بالإضافة إلى ارتباط التكنولوجيا والتقنية بعلوم مختلفة ولها تخصصات علمية وفنية دقيقة ومتعددة، وهذا ما يتطلب معه وجود الخبرة اللازمة لكشف غموض الجريمة ومعرفة مرتكبها والوصول لتحقيق العدالة[٢]، ويغدو بذلك اللجوء إلى الخبير الرقمي أمرًا مهمًا للوصول إلى كشف الجريمة ومرتكبها[٣].

لقد تعاظم دور الإثبات العلمي بالدليل مع ظهور الجرائم السيبرانية، وبَرَزت أهمية الخبرة في إثبات هذه الجرائم، وهو الدور الذي يضطلع به الخبراء القضائيون، وأصبح إنشاء المعامل الجنائية الرقمية مطلبًا ملحًا لفحص الأدلة الرقمية وتقييم عملية الإثبات الرقمي، وتحرير الجرائم في نطاق ما يعرف باسم نظم الخبرة الرقمية[٤].

---

[١] أحمد بن مالك، دور الأدلة الرقمية في الإثبات الجنائي، مجلة العلوم الإنسانية، المركز الجامعي علي كافي تندوف، المجلد (٥)، الإصدار الأول، الجزائر، ٢٠٢١، ص١١٠.

[٢] عائشة بن قارة مصطفى، مرجع سابق، ص١٣٨-١٣٩.

[٣] هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دار النهضة العربية، القاهرة ،١٩٩٤م، ص١٤٢.

[٤] ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب الوطنية، مصر، ٢٠٠٦، ص٨.

تكمن أهمية الخبرة في أنها تنير الطريق للقاضـــي الذي يهتدي به لتحقيق العدالة خاصـــة في القضـايا الجزائية، لذا فقد اهتمت التشـريعات بتنظيم أعمال الخبرة، لتحليل المسـائل الفنية التي يصـعب على المحقق أن يشق طريقه فيها، ويعجز عن جمع الأدلة بالنسبة لها بالوسائل الأخرى بالإثبات، ومنذ ظهور جرائم الحاسـب الآلي تسـتعين سـلطات التحقيق أو المحكمة بالمختبرات وأصـحاب الخبرة الفنية في مجال الحاسب الآلي والشبكات والاتصـالات وغيرها، وذلك بغرض كشف غموض الجريمة، وجمع أدلتها والتحفظ عليها، والمســـاعدة في إجلاء جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصـلة بالجريمة محل التحقيق، ويلاحظ أن نجاح الاسـتدلالات وأعمال التحقيق في هذه الجرائم يكون مرتهنًا بكفاءة وتخصـــص هؤلاء الخبراء[١]، ويجب الإشـــارة إلى أن البحوث الفنية التي يقوم بها أهل الخبرة في مرحلة جمع الاسـتدلالات بناء على طلب مأموري الضـبط القضـائي لا تعد من قبيل الخبرة، إذ تؤدى دون إتباع الإجراءات الشـكلية التي أوجبها القانون وهي الندب وأداء اليمين، إلا أنه يجوز لمأموري الضـبط القضـائي الاسـتعانة بالخبراء وتحليفهم اليمين إذا خيف ألا يسـتطيع فيما بعد سـماع شـهادتهم باليمين[٢]، وفي السـلطنة يسـتعين مأموري الضـبط القضـائي بمختبرات مجهزة تبعًا للاختصـاص، مثل مختبر للأدلة الرقمية، التابع لوزارة النقل والاتصـالات وتقنية المعلومات، وإدارة الدعم الفني التابعة للادعاء العام، وإدارة مكافحة الجرائم الاقتصـــادية والإلكترونية التابعة للإدارة العامة للتحريات والبحث الجنائي بشرطة عمان السلطانية، ومركز الدفاع الإلكتروني التابع لجهاز الأمن الداخلي.

أفرز التطور الهائل في مجال تكنولوجيا المعلومات العديد من الأنشـطة المسـتحدثة التي تتم باستخدام الوسائل الإلكترونية التي قوامها نظم وبرمجيات الحاسب الآلي والشبكات الحاسوبية وشبكات الاتصـــالات العالمية (الإنترنت)، كأعمال التجارة الإلكترونية، والمصـــارف والأعمال المصـــرفية الإلكترونية، والإدارة الإلكترونية، والحكومة الإلكترونية، مما ترتب عليه أن تتنوع الجرائم التي تقع على هذه العمليات، وفقًا لنوع الوسائل الإلكترونية المستخدمة في ارتكابها[٣].

---

(1)BOSSON, les regles de l'expertise elaboreespor le cade de procedure genol, D, 1960, P, 50.

(2) Robert Taylor, Computer crime . In criminal investigation edited "by Charles Swanson, n . chameleon and Territory, hill, ine, 5th edition 1992 . P1.

(3) Élise Ternynck, Le juge du contrat de travail et la preuve électronique: essai sur l'incidence des technologies de l'Information et de la communication sur le contentieux prud'homal, Ph D Thèse, PRES Université Lille Nord de France, 2014, pp.84-8.

ومن أمثلة هذه الجرائم (تزوير المستندات المدخلة في أنظمة الحاسب الآلي أو الناتجة عن التلاعب في البيانات، والتلاعب في البرامج الأساسية أو برامج التطبيقات، أو الغش أثناء نقل وبث البيانات)[١].

وحيثُ إن الاستعانة بخبير فني أمرًا يخضع لتقدير المحقق أو جهة التَحقيق أو الحكم، إلا أنه في المسائل الفنية البحتة التي لا يمكن للقاضي أن يقطع فيها برأي دون استطلاع رأي أهل الخبرة، ففي هذه الحالة يجب عليه أن يستعين بالخبير، فإذا تصدى للمسألة الفنية وفصل فيها دون تحقيقها بواسطة خبير كان حكمه معيبًا مستوجبًا نقضه [٢]، وفي ذلك استقرت المحكمة العليا على أن:" للمحكمة كامل السلطة في تقدير القوة التدليلية لعناصر الدعوى المطروحة على بساط البحث وهي الخبير الأعلى في كل ما تستطيع أن تفصل فيه بنفسها أو الاستعانة بخبير، ويخضع رأيه لتقديرها ما دامت المسألة المطروحة ليست من المسائل الفنية البحتة التي لا تستطيع المحكمة بنفسها أن تشق طريقها لإبداء الرأي فيها"[٣].

يرى جانب من الفقه بأنه ولئن كان للمحكمة السلطة التقديرية في تقرير ما إذا كانت الأدلة الموجودة في الدعوى كافية ويمكن الاستغناء بها عن تعيين خبير من عدمه، إلا أن ذلك مشروط بأن لا تتعرض للمسائل الفنية البحتة التي تكون في نطاق تحقيق دفاع المتهم[٤].

يظهر الواقع العملي أن القاضي غالبًا ما يسلم بما خلص إليه الخبير في تقريره، ويبني حكمه على أساسه، وهو ما يمليه الواقع، حيثُ أن رأي الخبير ورد في موضوع فني لا اختصاص للقاضي به، وليس من شأن ثقافته أو خبرته القضائية أن تتيح له الفصل فيه، بالإضافة إلى ذلك فهو الذي أنتدب الخبير ووثق في رأيه أنه مناسب لمهمته[٥].

---

[١] هشام فريد رستم، مرجع سابق، ص١٣٧.

[2] Ricordel, I., L'expertise en police scientifique, Dalloz, 2015, p.394.

[٣] الطعن رقم ١٧٩ / ٢٠٠٨ جلسة ٢١ / ١٠ / ٢٠٠٨ م، المبدأ رقم: (٥) – س (9) ، مجموعة المبادئ والقواعد القانونية التي قررتها المحكمة العليا في الفترة من ٢٠٠١ إلى ٢٠١٠.

[٤] سعيد حماد صالح قبائلي، حق المتهم في الاستعانة بمحام – دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٥، ص٨٩.

[5] Villard, M., La cybercriminalité et l’expertise judiciaire, La Jaune et la Rouge, Décembre 2005, p.36.

ذهب البعض إلى ضرورة إعطاء قوة إلزامية لتقرير الخبير، وذلك على أساس أن القاضي إذا رفض رأي الخبير فقد تعارض مع نفسه، إذ يعني ذلك أنه أراد أن يفصل بنفسه في مسألة سبق أن أعترف في بادئ الأمر بأن الخبير يتمتع فيها بمعرفة ودراية تفوق معرفته الشخصية[١].

في ذلك يذهب الباحث إلى عدم إلزامية تقرير الخبير، باعتبار أن القضـــاء هو الخبير الأعلى، وهو ما استقر عليه القضاء العُماني في تقدير تقارير الخبراء وإن ذلك مرجعه إلى محكمة الموضوع، التي لها كامل الحرية في تقدير قوة دليل تقرير الخبير شأنه في ذلك شأن سائر الأدلة[٢]، وفي الوقت ذاته يرى الباحث أهمية تـــأهيل قضاة متخصصين في القضايا السيبرانية وتعزيز معرفتهم بالجوانب التقنية، بما يمكنهم من الإحاطة بتقارير الخبراء، ورفع مستوى قدرتهم على تقدير تلك التقارير والفصل فيها.

تكاد تجمع كافة النظم القانونية، في الوقت الراهن على حجية الملفات المخزنة في الشبكات والنظم ومستخرجات الحاسوب والبيانات المسترجعة، وحجية الملفات ذات المدلول التقني، والإقرار بصحة التوقيع الإلكتروني والتسوية في الحجة مع التوقيع الفيزيائي، والعالم على أبواب الثورة الصناعية الرابعة سيشهد تطورًا نحو قبول الملفات الصـــوتية والتناظرية والملفات ذات المحتوي المرئي وغيرها من وســـائل الإثبات التقنية، لذا اتجهت معظم التشريعات إلى قبول الوسائل الإلكترونية كبينة في الدعاوى المصرفية[٣].

تتسم الجرائم السيبرانية بصعوبة اكتشافها وإثباتها، إذ أنها تتم في بيئة معقدة تمكن الجاني من العبث في بيانات الحاسب الآلي وبرامجه عن طريق نبضات إلكترونية لا ترى، وذلك في وقت قياسي قد يكون جزء من الثانية، كما يمكن محوها كذلك في زمن قياسي، قبل أن تصل يد العدالة إليه، لاسيما وأن عملية الضبط لا تتم سوى بمعرفة خبير فني أو متخصص[٤]، ويواجه الخبير صعوبات متعددة في سبيل جمع الأدلة الرقمية من أجهزة الحاسب الآلي أو الشبكات الرقمية نذكر منها:

---

[١] آمال عبد الرحيم عثمان، الخبرة في المسائل الجنائية، مطبوعات كلية الحقوق، جامعة المنصورة، القاهرة، ١٩٦٤، ص٣٠٧.

[٢] الطعن رقم ٩٠٤/ ٢٠٢٠م جلسة ١٩ / ٠١ / ٢٠٢١، مجموعة الأحكام الصادرة عن الدائرة الجزائية بالمحكمة العليا والمبادئ المستخلصة منها في الفترة من ٢٠٢٠/١٠/١م حتى ٢٠٢١/٩/٣٠.

[٣] يونس عرب، حجية الإثبات بالمستخرجات الإلكترونية في القضايا المصرفية، مجلة البنوك، الأردن، ٢٠١٠، ص٣٠٧.

[٤] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، ٢٠٠٤، ص٢٤.

١. **فقد جزء كبير من المعلومات والأوامر**، التي تشكل الأدلة الرقمية حال إغلاق جهاز الحاسب الآلي بطريقة غير صـــحيحة، أو في حالة القطع المفاجئ للتيار الكهربائي عن الجهاز، فعند إغلاق أو قطع التيار الكهربائي عن جهاز الكمبيوتر فإن مثل هذا الفعل قد يؤدي إلى محو المعلومات من ذاكرة الجهاز، أو تحريف بيانات هامة وحدوث ضـرر في أجهزة الكمبيوتر (hard ware)، أو منع نظام التشغيل من إعادة تحميل (Rebooting) وبالتالي فقدان الأدلة الجوهرية[١].

٢. **قيام الجاني بتهيئة جهاز الكمبيوتر للتفجير أو التدمير بمجرد تشغيله، بالضغط على زر توصيل الطاقة[٢].**

٣. **طبيعة مسـرح الجريمة:** قد لا يكون ممكنًا الحصـول علي الدليل في حالة توزيع مسـرح الجريمة بين أكثر من دولة، بسـبب تعقيد الإجراءات أو وجود مشـاكل عملية أو تشـريعية في بعض الدول، مما يحول دون الحصـول علي دليل رقمي، كما أن سرعة مرور البيانات الرقمية عبر الشـبكات في جزء من الثانية، مع مهارة المجرمون في تدمير الأدلة أو تحريف أو تعديل البيانات لحماية أنفسهم، وكذلك حجم البيانات الضـخمة التي تمر عبر الشـبكات، وهو ما يؤثر سـلبًا على جهود البحث عن دليل الإدانة أو البراءة[٣].

٤. **إخفاء الهوية:** عند اعتماد المسـتخدم إخفاء هويته حال اسـتخدام الإنترنت، سـواء القيام ببعض الإجراءات أو استخدام بعض البرامج والتطبيقات التي تؤدي إلى طمس الهوية، وهو ما يشكل عائقًا أمام المحقق الجنائي أو الخبير الفني[٤].

٥. **إخفاء المعلومات: وجود بعض البرامج الخاصـــة بإخفاء المعلومات أو البيانات، وذلك لخلق ما يعرف** بنظام ملفات الأمن عبر اســـتخدام الشـــبكة العالمية (الإنترنت)، الأمر الذي يجعل عملية استعادة الأدلة أو إعادة تركيبها في غاية الصعوبة أمام المحقق الجزائي[٥].

---

[١] براء منذر كمال، شرح قانون اصول المحاكمات الجزائية، دار الحامد للنشر والتوزيع، عمّان، ط١، ٢٠٠٩، ص١٠٢.

[٢] فخري عبد الحسن علي، المرشد العلمي للمحقق، منشورات مديرية الشرطة، بغداد، ١٩٩٩م، ص١٩٣.

[٣] عبد الفتاح حجازي، القانون الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص٢٦.

[٤] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٩م، ص٢٩٤.

[٥] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، القاهرة، ط١، ٢٠٠٩م، ص٢١٧.

ويتضح مما تقدم أن الحصول على الأدلة الرقمية أمر صعب الوصول إليه، لما يتطلبه من خبرة ومهارة كبيرة في المجالات التقنية.

تتنوع الوسائل الإلكترونية والأجهزة التي تستخدم نظم الحاسبات الآلية، كما تتنوع الشبكات التي تتميز بخصائص فنية وتتدرج تحت تخصصات فنية وعملية دقيقة، مما يستوجب توفر الإمكانيات والقدرات العلمية والفنية لدى الخبير في مجال التخصص الدقيق للحقل الذي يُطلب منه بحثه، التي تمكنه من تقديم تقارير دقيقة[١].

وبالنظر للطبيعة الفنية والعلمية للخبرة في مجال الجرائم المعلوماتية، فأنه يمكن تحديد هذه الخبرة في الموضوعات الآتية[٢]:

١. الإلمام بتركيب الحاسب وصناعته وطرازه ونظم تشغيله الرئيسية والفرعية، والأجهزة الطرفية الملحقة به، وكلمات المرور أو السر، وأكواد التشفير.

٢. طبيعة البيئة التي يعمل في ظلها الحاسب من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية، وتحديد أماكن التخزين والوسائل المستخدمة في ذلك.

٣. قدرة الخبير على إتقان مأموريته دون أن يترتب على ذلك أعطاب أو تدمير الأدلة المتحصلة من الوسائل الإلكترونية.

٤. التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة، أو المحافظة عليها، لحين القيام بأعمال الخبرة بغير أن يلحقها تدمير أو إتلاف، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على دعائمها الممغنطة.

ويرى الباحث أن هناك تحدٍ كبير قد يبرز فيما يتعلق بالخبراء المسجلين في قوائم الخبراء القضائيين حيثُ أن طبيعة هذه الجرائم تتسم بالتجدد الدائم وابتكار أساليب هجومية جديدة، مما يجعل

---

[١] هشام محمد فريد رستم، مرجع سابق، ص١٤٠.

[٢] المرجع السابق، ص١٤٢.

معرفة الخبير غير محددة بالمؤهلات وحسب، وإنما على مواكبة المتغيرات التقنية، وهذا يتطلب وجود أطر معينة لاعتماد قوائم الخبراء وضمان تحديث معارفهم.

وعادة ما توجد الأدلة الرقمية في مخرجات الطابعة والتقارير والرسوم، وفي أجهزة الكمبيوتر وملحقاتها، في الأقراص المرنة والصلبة وأشرطة تخزين المعلومات، وفى أجهزة المودم والبرامج وأجهزه التصوير ومواقع الويب والبريد الإلكتروني، ولذلك تستخدم عدة طرق أو أدوات تساهم في مجال الأدلة الرقمية منه [1]:

١. **برنامج إذن التفتيش:** وهو برنامج قاعدة بيانات يسمح بإدخال كل المعلومات الهامة لترقيم الأدلة، ويمكن لهذا البرنامج أن يصدر إيصالات باستلام الأدلة، والبحث في قوائم الأدلة المضبوطة، لتحديد مكان دليل معين أو تحديد ظروف ضبط هذا الدليل.
٢. **قرص بدء تشغيل الكمبيوتر:** وهو قرص يمكن المحقق من تشغيل الكمبيوتر إذا كان نظام التشغيل منه محميًا بكلمة مرور، ويجب أن يكون القرص مزودًا ببرنامج مضاعفة المساحة، فربما كان المتهم قد استخدم هذا البرنامج لمضاعفة مساحة القرص الصلب.
٣. **برنامج معالجة الملفات مثل (Xtree pro Gold)** وهو برنامج يمكن المحقق من العثور على الملفات في أي مكان على الشبكة أو على القرص الصلب، ويستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم.
٤. **برنامج النسخ مثل (lapt link)** وهو برنامج يمكن تشغيله في قرص مرن ويسمح بنسخ البيانات من الكمبيوتر الخاص بالمتهم ونقلها لقرص آخر، وهو برنامج مفيد للحصول على نسخة من المعلومات قبل تدميرها من جانب المتهم.

---

[1] Schuliar, Y., La coordination scientifiques dans les investigations criminalles, Proposition d' organization, aspects ethiques ou de la necessite d' un nouveau métier, Ph D these, Université Paris Descartes, 2009, p.87.

٥. **برنامج كشـــف الديســـك مثل (ama disk view disk)**: ويمكن من خلال هذا البرنامج الحصـــول على محتويات القرص المرن مهما كانت أســـاليب تهيئة القرص، وهذا البرنامج له نسختان، نسخه عادة خاصة بالأفراد ونسخة خاصة بالشرطة.

٦. **برامج الاتصالات مثل(lantastie)** : وهو يستطيع ربط جهاز حاسب المحقق بجهاز حاسب المتهم، لنقل ما به من معلومات وحفظها في جهاز نسخ المعلومات.

المطلب الثاني

التحديات القانونية في مواجهة الجرائم السيبرانية في القانون العُماني

تعد مكافحة الجريمة السـيبرانية تحديًا شـاملًا يتطلب جهودًا مشـتركة من السـلطات القانونية والمجتمع المدني، ويجب أن تكون هذه الجهود مدعومة بتشـريعات فعّالة وآليات إجرائية مناسـبة، وفي هذا السياق سعى المشرع العُماني إلى مواجهة التحديات التشريعية والإجرائية التي تعترض جهوده في مكافحة الجريمة السيبرانية.

يتطلب مكافحة الجريمة السـيبرانية في القانون العُماني تجاوز التحديات التشـريعية والإجرائية، وضـمان توافق التشـريعات والآليات القانونية مع التطورات التكنولوجية المسـتمرة لتحقيق العدالة والأمن السـيبراني، لذا سـوف يتناول هذا المطلب في فرعين رئيسـيين: الأول يتعلق بالتحديات التشـريعية، والمتمثلة في قدرة التشـريع على مواكبة التطورات التكنولوجية السـريعة ومكافحة الجريمة السـيبرانية بفعالية، وذلك في نطاق التشريعات القانونية وتحديد العقوبات المناسبة للمتسببين في الجرائم السيبرانية، والثاني يتناول التحديات الإجرائية بالآليات والإجراءات التي يتبعها النظام القانوني العُماني في التعامل مع حالات الجريمة السـيبرانية، من بينها تطوير القدرات الفنية والتقنية للأجهزة القضـائية وتدريب الكوادر القانونية على التعامل مع الجرائم السيبرانية.

الفرع الأول

التحديات التشريعية التي تواجه القانون العُماني في مواجهة الجرائم السيبرانية

القانون العُماني قد شهد تطورًا ملحوظًا في مواجهة ومكافحة الجرائم السيبرانية عبر عدة مراحل مختلفة بدأ بإضافة فصل في قانون الجزاء بموجب التعديل الذي أجراه على القانون رقم (١٩٧٤/٧)[١].

تناول القانون صورًا من الجرائم السيبرانية بواسطة قانون المعاملات الإلكترونية رقم (٢٠٠٨/٦٩)[٢]، حيث جرى تنظيم بعض الجوانب المتعلقة بالتعاملات الإلكترونية والتي شملت أنواعًا معينة من الجرائم الإلكترونية.

حاول المشرع معالجة بعض الصور من الجرائم السيبرانية من خلال قانون الاتصالات رقم (٢٠٠٢/٣٠)، الذي قدم تشريعات لحماية الاتصالات الإلكترونية والبيانات الشخصية ضد الاختراقات والاعتداءات الإلكترونية[٣].

أفرد المشرع العُماني قانونًا خاصًا لمكافحة الجرائم السيبرانية، وهو قانون مكافحة جرائم تقنية المعلومات رقم (٢٠١١/١٢)[٤]، وبعد مرور أكثر من (١٣) عامًا على صدوره، وفي ظل التطور المتسارع الذي يشهده العالم في مجال التكنولوجيا، يتعين على المشرع العُماني ملاحقة ذلك التطور، ومواجهة الجرائم الجديدة الناتجة عن الانتشار الواسع في استخدام التقنيات المتقدمة مثل الذكاء الاصطناعي والإنترنت، ونبين تاليًا المآخذ على قانون مكافحة جرائم تقنية المعلومات:

١. عرفت المادة الأولى من القانون الهيئة بأنها " هيئة تقنية المعلومات"، وهي الجهة التي يكون لموظفيها الذين يتم تحديدهم بقرار من وزير العدل وترشيح رئيس الهيئة صفة الضبطية القضائية في نطاق تطبيق أحكام القانون[٥]، وتم إلغاء الهيئة بموجب المرسوم السلطاني رقم (٦٣/ ٢٠١٩) وآلت

---

[١] عبد الله بن علي بن سالم الشبلي، مرجع سابق، ص٩١.

[٢] نشر هذا المرسوم في عدد الجريدة الرسمية رقم (٨٦٤) الصادر في ١ / ٦ / ٢٠٠٨م.

[٣] نشر هذا المرسوم في عدد الجريدة الرسمية رقم (٧١٥) الصادر في ١٧ / ٣ / ٢٠٠٢م.

[٤] نشر هذا المرسوم في الجريدة الرسمية رقم (٩٢٩) الصادر في ١٥ /٢ / ٢٠١١م.

[٥] المادة (٣٤) من قانون مكافحة جرائم تقنية المعلومات.

اختصاصاتها إلى وزارة التقنية والاتصالات جميع الاختصاصات، وفي أغسطس من عام ٢٠٢٠م تم إلغاء الوزارة ونقل اختصاصاتها إلى وزارة النقل والاتصالات وتقنية المعلومات، وذلك بموجب المرسوم السلطاني رقم (٢٠٢٠/٩٠) بإنشاء وزارة النقل والاتصالات وتقنية المعلومات، مما يتعين معه تعديل اسم الجهة التي يكون لموظفيها صفة الضبطية القضائية في نطاق تطبيق أحكام القانون.

٢. لم يعرف المشرع الجرائم السيبرانية، واكتفى بتعريف جرائم تقنية المعلومات بأنها "الجرائم المنصوص عليها في قانون مكافحة جرائم تقنية المعلومات"[١]، وبذلك أخرج كل الجرائم السيبرانية الواردة في القوانين الأخرى[٢]، وهذا الأمر يعني أنه لا توجد تعريفات قانونية واضحة وموحدة لما تشكله الجرائم السيبرانية من تحديات متزايدة، حيثُ أن التباين في تعريف الجرائم السيبرانية يمكن أن يؤثر على السياسات المتعلقة بمكافحة هذه الجرائم[٣].

٣. القانون لم يتبع سياسة الجمع بين عقوبتي السجن والغرامة على سبيل الوجوب والإلزام في كثير من النصوص، مما أدى إلى عدم كفاية العقوبات في بعض الجرائم، كالجرائم ذات الأبعاد الإلكترونية الكبيرة[٤]، فضلًا عن أن العقوبات التي وضعها القانون لا تتناسب مع خطورة بعض الجرائم[٥]، كالتي تقع على أنظمة المعلومات الخاصة بالمؤسسات الحكومية والخاصة التي تكبد خسائر مالية كبيرة، أو ينتج عنها انقطاع للخدمات الضرورية.

٤. لم يجرم القانون العديد من الأفعال التي تشكل اعتداء على أمن الدولة أو أمن الأفراد وحقوقهم، التي ترتكب باستخدام الوسائل التقنية، ونذكر منها على سبيل المثال لا الحصر:

أ. لم يتناول القانون استخدام وسائل التقنية في ارتكاب جرائم أمن الدولة بشكل مفصل رغم خطورة هذا النوع من الجرائم، وزيادة ارتكابها عبر وسائل التواصل الاجتماعي على وجه الخصوص، كإثارة الفتن والإضرار

---

[١] المادة (١) من قانون مكافحة جرائم تقنية المعلومات.

[٢] كقانون الجزاء، قانون المعاملات الإلكترونية، قانون تنظيم الاتصالات، قانون حماية البيانات الشخصية.

[٣] صابرين جابر محمد، الجريمة الإلكترونية ومكافحتها في القانون العُماني، المجلة المصرية للدراسات القانونية والاقتصادية، العدد ١٤، مصر، ٢٠٢٠، ص٢٢٣.

[٤] أشرف بن عبد الله الضويحي، المساهمة في الجرائم المعلوماتية المتعلقة بالاعتداء الشخصي، رسالة لنيل درجة الماجستير، جامعة الإمام محمد بن سعود الإسلامية، السعودية، ٢٠١٣، ص١٠٩.

[٥] راشد الشيدي، مرجع سابق، ص٨٣.

بسمعة الدولة ومركزها الاقتصادي، والوحدة الوطنية، وإعابة السلطان أو أفراد أسرته، وغيرها من الجرائم أمن الدولة الواردة في الفصلين الثاني والثالث من الكتاب الثاني من قانون الجزاء الصادر بالمرسوم السلطاني رقم (٧/ ٢٠١٨)، إلا أن زيادة وتيرة ارتكابها باستخدام وسائل التقنية يحتم تجريمها في نصوص خاصة متى كانت الرقمنة جزء من ارتكابها، ويحذو في ذلك حذو التشريعات النظيرة[١].

ب. الحاجة إلى تجريم بعض الأفعال المتعلقة بالإعلان والترويج عبر وسائل التقنية، كالتضليل ونشر بيانات غير صحيحة، ويتحقق التضليل عندما يكون السعر المذكور في الإعلان مخالف لسعر السعلة المعروضة، أو ترويج سلعة بياناتها غير واضحة، أو منتجات غير مرخصة، والمبالغة في الترويج بما يؤدي إلى عدم التمكن من استخدامها بذات الطريقة التي أُعلن عنها، أو تكون شروط الاتفاق مخالفة لما جاء في الإعلان كشرط الخدمة أو الصيانة لما بعد البيع، أو الادعاء الكاذب أن السلعة مطابقة للمواصفات[٢]، ورغم تجريم الإعلان المضلل بموجب المادة (٤٠) من قانون حماية المستهلك[٣]، إلا أن الانتشار الواسع في استخدام التقنية في الإعلان والترويج عبر نشطاء وسائل التواصل الاجتماعي وغيرها من الوسائل الإلكترونية فإن الباحث يرى ضرورة التدخل التشريعي في تجريم هذه الأفعال بما يعزز الرقابة وحماية المستهلك.

ج. لم ينظم المشرع تداول وترويج العملات الرقمية[٤]، رغم خطورتها على الأمن الاجتماعي، وتداعياتها المالية والاجتماعية على الأغلبية التي لا تحيط بالتعاملات الإلكترونية، وتكمن خطورة التعامل بهذه العملات في أنها افتراضية ليس لها وجود مادي، ولا تخضع لرقابة البنك المركزي، ويسهل بالتالي ممارسة الأنشطة المحظورة عبرها، فضلًا عن اعتبارها مجال خصب للاحتيال بالتداول بالعملات الرقمية المزورة[٥].

---

[١] أوردت المواد (٢٤، ٢٥، ٤٨) من قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي الصادر بالمرسوم الاتحادي رقم (٢٠٢١/٣٤) العديد من جرائم أمن الدولة.

[٢] متى يكون الإعلان مضللًا، منشور صادر عن الهيئة العامة لحماية المستهلك، صحيفة أثير الإلكترونية، https://www.atheer.om

[٣] قانون حماية المستهلك الصادر بالمرسوم السلطاني رقم (٦٦/ ٢٠١٤)، المنشور في الجريدة الرسمية العدد رقم (١٠٨١) الصادر في ٧/ ١٢ / ٢٠١٤م.

[٤] بدأ استخدام العملة الرقمية في عام ٢٠٠٩، لتفادي سلبيات النظام المالي التقليدي، وهو نظام نقدي رقمي يقوم على التعاملات المباشرة بدون وسطاء، يتم استخدامه بواسطة نظام حاسوبي مرخص.

[٥] دعاء أحمد توفيق، الأمن الاجتماعي وتداعيات العملة الرقمية، مجلة كلية الآداب والعلوم الإنسانية، جامعة قناة السويس، العدد (٣١)، مصر، ٢٠١٩، ص١٠٩ – ١١٠.

د. عدم تجريم جمع البيانات الشخصية بدون ترخيص، أو استغلال تلك البيانات لإضرار بالغير أو جلب النفع للنفس أو للغير، وقد حظر المشرع العُماني وفقًا لنص المادة (٤٣) من قانون المعاملات الإلكترونية العُماني جمع البينات الشخصية من قبل الجهات الحكومية أو مقدمو الخدمات، ولا ينصرف ذلك على الأشخاص أو غيرهم، على الرغم من أن ربط الأجهزة الإلكترونية بعضها البعض بواسطة جهاز مركزي أو عبر شبكات عامة للاتصال يؤدي إلى تبادل المعلومات والبيانات الشخصية للأفراد فيما بين الأنظمة المعلوماتية[١] ، أو جمع البيانات الشخصية دون علم الأشخاص عبر وسائل التكنولوجيا التي يتم من خلالها جمع البيانات الشخصية للمستخدمين وتخزينها عن طريق ملفات تعريف الارتباط (cookies)[٢].

كما تقوم شبكات التواصل الاجتماعي بجمع أكبر قدر من المعلومات عن مستخدميها حيث أصبحت هذه الشبكات بمثابة مستودع للمعلومات والتي من خلالها يتنازل المرء طواعية عن بياناته الشخصية للتسجيل في هذه المواقع، ومن ثم الحصول على حساب خاص به، ووفقًا لسياسات الخصوصية التي لا يقرأها عادة المستخدم قد يكون هناك تنازل صريح للفرد عن بياناته، فضلا عما يقوم به الشخص بشكل يومي من إفصاح عن حياته الشخصية[٣].

ومما لا شك فيه فإن جمع البيانات الشخصية في السلطنة يثير العديد من المخاطر، منها انتهاك الخصوصية حيث يمكن أن يؤدي إلى انتهاك خصوصية الأفراد، وقد يتم استغلال البيانات بطرق غير مشروعة مما يعرض المواطنين للمخاطر مثل الاحتيال والابتزاز، حيث يمكن أن يكون جمع البيانات هدفًا للمتسللين السيبرانيين بالتعدي عليها، أو تعديلها[٤].

---

[١] محمود عبدالرحمن، التطورات الحديثة لمفهوم الحق في الخصوصية "الحق في الخصوصية المعلوماتية" مجلة كلية القانون الكويتية العالمية، العدد التاسع، الكويت، ٢٠١٥، ص١٠٩.

[٢] ملفات تعريف الارتباط (cookies) "عبارة عن ملفات نصية تضعها معظم مواقع الويب على القرص الصلب في الخاص بالمتصفح (الزائر)، عند زيارته لهذه المواقع، بغرض جمع بعض المعلومات عن المستخدم، تتيح للموقع الذي أودعها أن يسترجعها عند الحاجة اليها، ومكمن الخطورة في هذه الملفات انه من الممكن استغلالها في انتهاك خصوصية المستخدمين وجمع معلومات عنهم خلال تصفحهم لمواقع الويب المختلفة".

[٣] دينا عبدالعزيز فهمي، المسؤولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي، مجلة كلية الحقوق، جامعة طنطا، مصر، ٢٠١٧، ص١٥.

[٤] رقية بنت خلفان بن ناصر العبدلية، حوكمة البيانات وفاعلية تطبيقها في المؤسسات الحكومية في سلطنة عُمان، رسالة لنيل درجة الماجستير، جامعة السلطان قابوس، ٢٠٢٢، ص٨٥ وما بعدها.

بالإضـافة إلى ما تقدم فإن المشـرع العُماني لم يضـع أطر قانونية خاصـة باسـتخدام تقنيات الذكاء الاصـطناعي والروبوتات، فضـلًا عن الانتهاكات التي لم يشـملها بالتجريم في الوسـط الرقمي، كانتحال صـفة الموظف العام أو أي صـفة أخرى، وترويج المنتجات الطبية بدون ترخيص، واسـتغلال النيازك وغيرها من المعادن الثمينة وترويجها وبيعها بدون ترخيص، والتسول الإلكتروني وغيرها.

على صـعيد متصـل وباسـتقراء التشـريعات المنظمة للجرائم السـيبرانية في السـلطنة يتضـح أن هناك ازدواج بين اختصـاصـات وزارة النقل والاتصـالات وتقنية المعلومات ومركز الدفاع الإلكتروني في مكافحة الجرائم السيبرانية ويتجلى ذلك في الآتي:

١. **تحديد الجهة المختصة بالموافقة على نقل البيانات ومعالجتها خارج السلطنة:** نصت المادة (٤) من نظام مركز الدفاع الإلكتروني على أنه:" تلتزم الجهات المعنية[١] بالآتي:... ٥- أخذ موافقة المركز قبل حفظ أي بيانات حساسة، أو معالجتها خارج السلطنة، ونصت المادة (٨) من قانون حماية البيانات الشخصية على أنه: "تتخذ الوزارة[٢] في سبيل حماية حقوق أصحاب البيانات الشخصية أيا من الإجراءات الآتية: د – وقف تحويل البيانات الشخصية إلى دولة أخرى، أو منظمة دولية"، كما نصت المادة (٢٣) من ذات القانون على نقل البيانات إلى خارج السلطنة وفق إجراءات محددة، ليس من بينها موافقة مركز الدفاع الإلكتروني.

٢. **الاختصاص بتلقي البلاغ عند حدوث اختراق أو تهديد الأمن السيبراني:** نصت المادة (٤) من نظام مركز الدفاع الإلكتروني على أنه: " تلتزم الجهات المعنية بالآتي:... ٢. إخطار المركز بشكل فوري بأي خطر أو تهديد أو اختراق لأمنها الإلكتروني واقع أو محتمل"، في حين أن المادة (١٩) من قانون حماية البيانات الشخصية نصت على إلزام المتحكم[٣]، عند حدوث اختراق للبيانات الشخصية، إبلاغ وزارة النقل والاتصالات وتقنية المعلومات وصاحب البيانات الشخصية عن الاختراق.

---

(١) عرفت المادة (١) من نظام مركز الدفاع الإلكتروني الصـادر بالمرسـوم السـلطاني رقم (٦٤/ ٢٠٢٠) **الجهات المعنية** بأنها: "الجهات الحكومية المدنية والعسكرية والأمنية ومؤسسات القطاع الخاص داخل السلطنة ذات الصلة باختصاصات المركز، وغير ذلك من الجهات التي يصدر بتحديدها قرار من رئيس جهاز الأمن الداخلي".

(٢) عرفت المادة (١) من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم (٢٠٢٢/٦) **الوزارة** بأنها: "وزارة النقل والاتصالات وتقنية المعلومات".

(٣) عرفت المادة (١) من قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم (٢٠٢٢/٦) **المتحكم** بأنه:" الشخص الذي يتولى تحديد أهداف ووسائل معالجة البيانات الشخصية، ويقوم بهذه المعالجة بنفسه، أو يعهد بها إلى غيره".

٣. **التعاون المحلي والدولي، وتمثيل السلطنة في المنظمات والمؤتمرات المتعلقة بالأمن السيبراني:** نصت المادة (٦) من نظام مركز الدفاع الإلكتروني على أنه:" يكون للمركز في سبيل تحقيق أهدافه ممارسة الاختصاصات الآتية:... ٢٠ – تبادل المعلومات في مجال الأمن الإلكتروني مع المراكز النظيرة المحلية أو الدولية. ٢١ – تمثيل السلطنة بالاشتراك والتنسيق مع الجهات الأخرى ذات العلاقة في المنظمات والمؤتمرات واللجان والاتحادات والاجتماعات الإقليمية والدولية ذات الصلة بالأمن الإلكتروني"، وفي الواقع العملي يتولى هذا الدور مركز السلامة المعلوماتية التابع لوزارة النقل والاتصالات وتقنية المعلومات[١]، وهنا تجدر الإشارة إلى أن الأمن الإلكتروني (السيبراني) لم يرد ضمن اختصاصات وزارة النقل والاتصالات وتقنية المعلومات الواردة بملحق المرسوم السلطاني رقم (٢٠٢٠/٩٠) بإنشاء وزارة النقل والاتصالات وتقنية المعلومات وتحديد اختصاصاتها واعتماد هيكلها التنظيمي[٢]، بل أن المادة الأولى من ديباجة المرسوم آنف الذكر نصت على ممارسة الوزارة لاختصاصاتها دون الإخلال بنظام مركز الدفاع الإلكتروني، وأن تؤدي بعض أعمالها بالتنسيق مع مركز الدفاع الإلكتروني[٣] صاحب الاختصاص الأصيل في منظومة الأمن السيبراني في السلطنة.

وإزاء ذلك يقترح الباحث إزالة هذا الازدواج ومنح جميع اختصاصات الأمن السيبراني لمركز الدفاع الإلكتروني، عملًا بأحكام القانون، وبما يحقق الأهداف الوطنية وتركيز الجهود الرامية إلى حماية الفضاء الإلكتروني العُماني.

وعلى صعيد متصل فقد أوردت هذه القوانين بعض المصطلحات التي يكتنفها الغموض وعدم الوضوح، ولم يرد لها تعريف في تلك القوانين، حيث نصت المادة (٣) من قانون حماية البيانات الشخصية على أنه: "لا تسري أحكام هذا القانون على معالجة البيانات الشخصية التي تتم في الأحوال الآتية: أ – حماية الأمن الوطني، أو المصلحة العامة. د – حماية المصالح الاقتصادية، والمالية للدولة."، حيث أن القانون لم يحدد الجهة التي يعهد إليها تحديد البيانات المتعلقة بالأمن الوطني

---

[١] الموقع الإلكتروني الرسمي لمركز السلامة المعلوماتية، https://cert.gov.om، تم استيراده بتاريخ ٠١ أغسطس ٢٠٢٤م.

[٢] نشر هذا المرسوم في عدد الجريدة الرسمية رقم (١٣٥٣) الصادر في ١٩ / ٨ / ٢٠٢٠م.

[٣] البندين (١١، ١٤) من ملحق المرسوم السلطاني رقم (٩٠/ ٢٠٢٠) بإنشاء وزارة النقل والاتصالات وتقنية المعلومات وتحديد اختصاصاتها واعتماد هيكلها التنظيمي.

والمصالح العامة والمصالح الاقتصادية، وهي مصطلحات نسبية يختلف تقديرها من شخص لآخر ومن مؤسسة لأخرى، والأمر ذاته بالنسبة للمادة (٤) من نظام مركز الدفاع الإلكتروني التي نصت على أنه:" تلتزم الجهات المعنية[١] بالآتي:... ٥-أخذ موافقة المركز قبل حفظ أي بيانات حساسة، أو معالجتها خارج السلطنة"، إذ أن القانون لم يُعرف البيانات الحساسة، وقد ينتج عنه عدم وضوح النص، وتباين في تحديد مفهومها سواء من قبل المخاطبين بها، أو القائمين على إنفاذ القانون.

بعد استعراض التشريعات العُمانية المواجهة للجرائم السيبرانية، يتبين أن هذه القوانين لم تواكب التهديدات السيبرانية المتزايدة والتحديات التي تفرضها التقنيات المتطورة، مما يتطلب معها وضع إطار قانوني شامل يمكنه التعامل مع الجرائم السيبرانية بكل أبعادها، حيثُ أن التشريعات الحالية لا تزال غير كافية لتوفير الحماية المطلوبة في عصر يشهد تحولًا كبيرًا نحو الرقمية، وتوجه العالم نحو الثورة الصناعية الرابعة، وهنا تبرز الحاجة لإصدار قانون جديد شامل يغطي كافة جوانب الجرائم السيبرانية، ويضمن تقديم الردع والعقاب المناسبين، إلى جانب تعزيز قدرات السلطنة في مجال الأمن السيبراني، بما يعزز الثقة في البيئة الرقمية وحماية المجتمع والاقتصاد من التهديدات السيبرانية.

الفرع الثاني

التحديات الإجرائية التي تواجه القانون العُماني في مواجهة الجرائم السيبرانية

أصدر المشرع العُماني العديد من القوانين والتشريعات لمواجهة الجرائم السيبرانية، ولعل أبرزها قانون مكافحة جرائم تقنية المعلومات، إلا أن تلك التشريعات لا تكفي وحدها لتحقيق الفاعلية المرجوة إذا كانت القواعد الإجرائية لا تتناسب مع طبيعتها التقنية، حيثُ أن قانون الإجراءات الجزائية الصادر بالمرسوم السلطاني رقم (٩٩/٩٧) لم ينص على إجراءات خاصة بالجرائم السيبرانية، مما يحد من فاعليته أمام التعقيدات التقنية وخصوصية هذا النوع من الجرائم.

---

[١] عرفت المادة (١) من نظام مركز الدفاع الإلكتروني الصادر بالمرسوم السلطاني رقم (٦٤/ ٢٠٢٠) **الجهات المعنية** بأنها: "الجهات الحكومية المدنية والعسكرية والأمنية ومؤسسات القطاع الخاص داخل السلطنة ذات الصلة باختصاصات المركز، وغير ذلك من الجهات التي يصدر بتحديدها قرار من رئيس جهاز الأمن الداخلي".

تتعدد التحديات الإجرائية التي يواجهها القانون العُماني في مواجهة الجرائم السيبرانية، ويسلط هذا الفرع الضوء على أهم تلك التحديات والمعوقات التي تواجه القائمين على مكافحة الجرائم السيبرانية وذلك على النحو الآتي:

أولًا: تحديات متعلقة بالجهات المختصة بإنفاذ القانون

تلعب الجهات المختصة بإنفاذ القانون دورًا محوريًا في مكافحة الجرائم السيبرانية، إذ تقع على عاتقها مسؤولية تنفيذ القوانين والتحقيق في الجرائم وضمان تقديم الجناة إلى العدالة، ومع ذلك فإنها تواجه تحديات في التعامل مع طبيعة الجرائم السيبرانية التي تتسم بالتعقيد والتطور السريع من بين هذه التحديات ما يأتي:

١. تعدد الجهات المختصة بممارسة دور الضبطية القضائية في الجرائم السيبرانية

يتمتع كل من وزارة النقل والاتصالات وتقنية المعلومات، وشرطة عمان السلطانية، ومركز الدفاع الإلكتروني، بصفة الضبطية القضائية في الجرائم السيبرانية، حيثُ أن المادة (٣٤) من قانون مكافحة جرائم تقنية المعلومات نصت على ممارسة صفة الضبطية القضائية من قبل موظفي هيئة تقنية المعلومات التي آلت اختصاصاتها إلى وزارة النقل والاتصالات وتقنية المعلومات[١]، كما أن شرطة عمان السلطانية تمارس ذات الاختصاص استنادًا للمادة (٣١) من قانون الإجراءات الجزائية[٢]، ونص البند (١٠) من المادة (٦) من نظام مركز الدفاع الإلكتروني على اختصاص المركز في الاستدلال والتحقيق في الجرائم السيبرانية، وهو ما قد يشكل تنازع في الاختصاص بالاستلال في هذه الجرائم، رغم اختلاف اختصاص الضبطية القضائية لكل منها.

---

[١] "تم إلغاء هيئة تقنية المعلومات بموجب المرسوم السلطاني رقم (٦٣/ ٢٠١٩) وآلت اختصاصاتها إلى وزارة التقنية والاتصالات، وفي أغسطس من عام ٢٠٢٠م تم إلغاء الوزارة ونقل اختصاصاتها إلى وزارة النقل والاتصالات وتقنية المعلومات، بموجب المرسوم السلطاني رقم (٢٠٢٠/٩٠)".

[٢] نصت المادة (٣١) من قانون الإجراءات الجزائية على أنه: "مأمورو الضبط القضائي في دوائر اختصاصهم:... ٢. ضباط الشرطة والرتب النظامية الأخرى بدءًا من رتبة شرطي".

٢. تعدد المختبرات المختصة بتحليل الأدلة الرقمية

سعت السلطنة إلى تطوير المختبرات الخاصة بتحليل الأدلة الرقمية، مثل مختبر للأدلة الرقمية التابع لوزارة النقل والاتصـــالات وتقنية المعلومات، وإدارة الدعم الفني التابعة للادعاء العام، بالإضـــافة إلى إدارة مكافحة الجرائم الاقتصـــــادية والإلكترونية التابعة للإدارة العامة للتحريات والبحث الجنائي بشرطة عمان السلطانية، ومركز الدفاع الإلكتروني التابع لجهاز الأمن الداخلي، ويرى الباحث أن تعدد هذه المختبرات تشتيت للجهود وزيادة في نفقات المباني والتجهيزات الفنية المخصصة لكل مختبر من هذه المختبرات، ويقترح إزاء ذلك إنشـــاء مختبر جنائي رقمي واحد مجهز بتقنيات عالية المســـتوى، ويسخر له أمهر الكفاءات الوطنية في هذا الجانب.

٣. نقص الخبرة التقنية لدى العاملين بالجهات المختصة بإنفاذ القانون

في الغالب يكون مرتكب الجريمة الســـيبرانية على دراية تامة بالتقنية والتكنولوجيا، وهذا الأمر يصعب مهمة القائمين على التعامل مع هذه الجرائم من مأموري الضبط القضائي والمحققين والقضاة في ظل نقص التدريب والخبرة في الجوانب التقنية[١]، بل أن ذلك قد يشـــكل تحدي حتى على الخبير التقني، بسبب تفرع التخصصات التقنية وتطورها السريع، وقد لا يمكنه التعامل مع جميع أنواع الأجهزة والبرامج والشبكات المختلفة؛ لذلك يتطلب الأمر الاعتماد على كفاءات متخصصـــة من ذوي القدرات العالية في التعامل مع التقنية وللحصول على الأدلة الرقمية منها[٢].

تتجلى هنا أهمية تأهيل العاملين في هذه الجهات بما يتماشـــى مع التطورات في مجالات تقنية المعلومات والجرائم السيبرانية وبالأخص القضاة، حيثُ أن هذه القضايا تتطلب تخصصًا دقيقًا يمكّن القضـــاة من الفصـــل في المســـائل الصـــعبة والمعقدة التي تحتاج إلى مهارات معينة وفهم عميق للتكنولوجيا، وذلك عبر تأهيل قضاة أكفاء قادرين على التعامل مع هذه النوعية من القضايا[٣].

---

[١] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمّان، ط١، ٢٠١١، ص٢٢٥.

[٢] خالد ممدوح إبراهيم، أمن الجريمة المعلوماتية، الدار الجامعية، الإسكندرية ،٢٠٠٨، ص٩٠.

[٣] نجلاء توفيق نجيب، القضـــاء المتخصـــص ودوره في تطوير النظام القضـــائي، مجلة الحقوق، جامعة البحرين، المجلد (١٦)، العدد (٢)، البحرين، ٢٠١٩، ص٣٨٠.

٤. ارتفاع تكاليف إجراءات مكافحة الجرائم السيبرانية

إعداد مختبرات متخصصة مزودة بأحدث الأجهزة والتقنيات والمواد التشغيلية التي تحتاجها، وتحديثها المستمر يتطلب موازنات مالية كبيرة جدًا، فضلا عما يحتاجه العاملين في هذه المختبرات، من تأهيل وتدريب مستمر[١].

ثانيًا: تحديات متعلقة بالضمانات العامة والحق في الحياة الخاصة واحترام مبدأ الإقليمية

يسعى المشرع إلى تحقيق التوازن بين مصلحة المجتمع في معاقبة الجاني ومكافحة الجريمة وبين مصلحة الأفراد في عدم الاعتداء على حياتهم الخاصة وحرياتهم الشخصية، والحق في سرية المراسلات والاتصالات، إلا وفق ضوابط وإجراءات محددة، وهو ما نص عليه النظام الأساسي للدولة[٢]، إلا أن تطبيق هذه الإجراءات في البيئة الرقمية يؤدي إلى عدم فاعلية الإجراءات الجزائية في هذه الجرائم، حيثُ أن عامل الوقت مهم جدًا في إثبات الجرائم السيبرانية[٣]، كما أن اعتراض المراسلات والمكالمات وبرامج التواصل الخاصة من أكثر الوسائل فعالية في ضبط الأدلة الرقمية، وإحباط الجرائم الكبيرة كجرائم أمن الدولة والإرهاب والتخريب[٤].

ينص المشرع العُماني كغيره من التشريعات النظيرة على مبدأ إقليمية القانون الجزائي، وهو ما أكدته المادة (١٥) من قانون الجزاء، وهو ما يثير إشكالية في مكافحة الجرائم السيبرانية العابرة للحدود الإقليمية، والجدل حول تطبيق قواعد قانون الإجراءات الجزائية في ظل عالمية هذه الجرائم، وما يتطلبه ذلك من تنسيق الجهود الدولية والتعاون في مكافحة هذه الجرائم.[٥]

رغم أهمية حقوق الإنسان والحقوق الشخصية والحريات العامة، إلا أنها قد تصطدم في الحقل التقني بسيادة القانون والأمن العام، الأمر الذي يثير الجدل حول أيهما أولى بالنظر والرعاية، وفي ذلك

---

[١] خالد عياد الحلبي، مرجع سابق، ص٢٢٨.

[٢] نصت المادة (٣٦) من النظام الأساسي للدولة على أنه "للحياة الخاصة حرمة، وهي مصونة لا تمس، وللمراسلات الإلكترونية بكافة أنواعها، والمراسلات الهاتفية، والبرقية، والبريدية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، فلا يجوز مراقبتها، أو تفتيشها، أو الاطلاع عليها، أو إفشاء سريتها، أو تأخيرها، أو مصادرتها، إلا في الأحوال التي يبينها القانون، ووفقا للإجراءات المحددة فيه.

[٣] محمد حبحب، تطبيق القواعد الجزائية الإجرائية على الجريمة الإلكترونية: تحديات وآفاق، مجلة كلية القانون الكويتية العالمية، المجلد (٦)، الكويت، ٢٠١٨، ص٤٠٨.

[٤] نادر عبد العزيز شافي، بين احترام الحريات الشخصية ومراعاة مصلحة الدولة والأمن الوطني، مجلة الجيش، العدد (٢٦٣)، لبنان، ص٢.

[5] Andre Huet, Le droit penal international et Internet, les petites affiches,1999,p39.

نصت اتفاقية "بودابست"[١] على وجوب مراعاة حقوق الإنسان إلا أنها أقرت مجموعة من الإجراءات التي تمس بهذه الحقوق، ومن أهمها ما يأتي:

١. التحفظ السريع أو المستعجل على بيانات الحاسب المخزنة، بما يمكن السلطات المختصة ضبط البيانات قبل تعرضها للفقد والتلف والتعديل[٢].

٢. منح السلطات صلاحيات في توجيه الأمر إلى أي شخص يتواجد في إقليم الدولة بتقديم البيانات الإلكترونية المتوفرة بحوزته أو تحت سيطرته، أو مخزنة داخل نظام حاسوبي، أو على أي وسيط تخزين بيانات آخر، وطلب أي بيانات من مزودي الخدمات داخل إقليم الدولة[٣].

٣. منح الدول الأعضاء حق الترخيص لسلطاتها بجمع البيانات من الوسائل الإلكترونية واعتراض البيانات والمحتوى الإلكتروني، وفقًا لضوابط محددة، وذلك عن طريق تسجيل البيانات والمعلومات باستخدام الوسائل التقنية[٤].

وهو ما يشير صراحة على إدراك الدول الموقعة على الاتفاقية لمخاطر الجرائم السيبرانية، بتقديمها المصلحة العامة على المصلحة الشخصية، وخطورة هذا النوع من الجرائم الذي يتطلب التدخل السريع لمواجهتها، ويرى جانب من الفقه إمكانية استخدام التكنولوجيا والتقنية لمساعدة مأموري الضبط القضائي وسلطات التحقيق في جمع الأدلة، ومنها على سبيل المثال استخدام برامج كسر "كلمات المرور" بما يمكن تلك السلطات الوصول السريع للبيانات[٥].

---

[١] اتفاقية بودابست "هي الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية، تم التوقيع عليها في نوفمبر ٢٠٠١م، ودخلت حيز النفاذ في يوليو ٢٠٠٤م، وهي أبرز الاتفاقيات الدولية المعنية بمكافحة الجرائم الإلكترونية، تحت إشراف المجلس الأوروبي، وهدفت إلى وضع سياسة جزائية مشتركة لمكافحة الجريمة الإلكترونية عن طريق مواءمة القوانين الوطنية مع نصوص الاتفاقية لضمان توفير الحماية الكافية للمجتمع من هذه الجرائم".

[٢] المادة (١٦) من اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

[٣] المادة (١٨) من اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

[٤] المادة (٢٠) من اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

[٥] حازم محمد حنفي، مرجع سابق، ص78.

ثالثًا: تحديات متعلقة بالدليل الرقمي

أسهمت ثورة تكنولوجيا المعلومات وتطورها في تعزيز استخدام شبكات المعلومات على مستوى العالم، حيثُ أصبحت معظم أجهزة الحاسوب محمولة وسهلة الاستخدام، وتنوعت هذه الأجهزة لتشمل أجهزة نقالة وأجهزة لوحية تحتوي على برامج مشابهة لتلك الموجودة في الحاسوب، وتُعتبر هذه الأجهزة بمثابة حواسيب مصغرة يمكن حملها واستخدامها في أي مكان، مما يسهل الوصول إلى شبكات المعلومات دون الحاجة إلى المكونات المادية المعقدة للحاسوب، نتيجة لذلك انتقل مسرح الجريمة إلى هذه الشبكات والأجهزة، مما أدى إلى تطور أدوات الجريمة، وأفرز ذلك العديد من التحديات والعقبات أمام سلطات التحقيق في مكافحة الجريمة السيبرانية، ومن أبرزها:

١. صعوبة تتبع الفاعل

تتواجد مسارح الجرائم السيبرانية والأدلة الرقمية في مواقع متعددة، مما يؤدي إلى صعوبات إجرائية في التحقيق وملاحقة الجناة، بالإضافة إلى ذلك تختلف القواعد الموضوعية والإجرائية بين الدول، مما يعني أنه إذا وُجدت أدلة في دولة أخرى فإنه غالبًا ما يكون من الصعب الحصول عليها، حتى مع اتخاذ إجراءات دولية لتسهيل تبادل الأدلة الرقمية فهذه الإجراءات غالبًا ما تكون معقدة وغير عملية، إلا في حالات الجرائم الخطيرة التي تتطلب طلب المعلومات بشكل رسمي من الدول المعنية[١] كجرائم الإرهاب.

ويستخدم بعض المجرمون تقنيات التخفي في ممارسة أنشطتهم الإجرامية كجرائم تمويل الإرهاب وغسل الأموال عبر تشفير عملة التحويلات المالية، أو التحويل بدون وسيط بفضل تقنيات متخصصة، أو التحويل عبر العملات الرقمية[٢]، ويتخفى المجرمون عبر وسائل التواصل الاجتماعي باستخدام أساليب مختلفة كانتحال صفات وممارسة أنشطتهم الإجرامية عبر الحسابات المزيفة[٣]، وهناك العديد من تقنيات التخفي التي يتطلب لمواجهتها تقنيات عالية، وإعداد كفاءات مناسبة للتعامل معها.

---

[١] ممدوح عبدالحميد عبدالمطلب، أدلة الصور الرقمية في الجرائم عبر الكمبيوتر، مركز بحوث الشرطة، الشارقة، 2005، ص١٢٠.

[٢] نادر عبدالعزيز شافي، المصارف والنقود الإلكترونية، المؤسسة الحديثة للكتاب، لبنان، ٢٠٠٧، ص٨٣.

[٣] سامي الرواشدة، الأدلة المتحصلة من مواقع التواصل الاجتماعي ودورها في الإثبات الجنائي، المجلة الدولية للقانون، المجلد(٦)، العدد (٣)، قطر، ٢٠١٧، ص١١.

٢. قابلية محو الدليل الرقمي

الجناة الذين يســـتخدمون الوســـائل الإلكترونية في ارتكاب جرائمهم يتميزون بالذكاء والإتقان الفني للعمل الذي يقومون به، والذي يتميز بالطبيعة الفنية، ولذلك فإنهم يتمكنون من إخفاء الأفعال غير المشروعة التي يقومون بها أثناء تشغيلهم لهذه الوسائل الإلكترونية، ويستخدمون في ذلك التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي يتم تسجيل البيانات عن طريقها[١].

الأمر الذي يتعين معه التعامل مع هذه الأدلة والتحفظ عليها بشـكل سـريع، حيثُ أن التعامل مع هذه البيانات لا يستغرق سوى كبسة زر، الأمر الذي يتيح مجال أكبر للمجرمين للتخفي، والهروب من العدالة وإخلاء ساحتهم من الأدلة التي تدينهم[٢].

٣. حجم البيانات الضخمة التي تستخلص منها الأدلة الإلكترونية

يتطلب البحث في كميات هائلة من البيانات جهودًا كبيرة وخبرة متقدمة، وتُعتبر البيانات المستخرجة من الشبكات والانترنت بيانات قابلة للنسخ، حيث يمكن الحصول على نسخة منها عبر نفس الشبكات، ويواجه بذلك أعضاء الادعاء العام أو الخبراء تحديات عند جمع الأدلة الإلكترونية من هذه الشـــبكات، تتمثل حجم البيانات التي يتطلب البحث فيها عن الدليل الرقمي، الأمر الذي يســـاعد المجرم على الإفلات من الملاحقة الجزائية[٣].

تواجه الســـلطات المعنية بإنفاذ القانون تحديًا في مواجهة الضـــخامة البالغة لكم البيانات التي يتعين فحصها أثناء التحقيق في الجرائم السيبرانية، وهو ما يتطلب استثمارات في البنية التحتية الرقمية واستخدام تقنيات الذكاء الاصطناعي لتحليل البيانات بصورة أسرع.

وبالإضـــافة إلى كل هذه التحديات تبرز إشـكاليات عديدة مصـــاحبة لتطبيق قواعد الإجراءات الجزائية التقليدية على الجرائم الســـيبرانية، كتفتيش المكونات المعنوية للحاســـب الآلي، وتطبيق أحكام التلبس بالجريمة الإلكترونية، والاختصاص المكاني لمأموري الضبط القضائي والادعاء العام والمحاكم

---

[١] هشام محمد فريد رستم، مرجع سابق، ص٥.

[٢] حازم محمد حنفي، مرجع سابق، ص٨٢.

[٣] حازم محمد حنفي، المرجع السابق، ص٨٣.

في ظل الجرائم التي ترتكب في الفضـــاء الإلكتروني، وغيرها من التحديات التي تؤكد ضـــعف فاعلية قواعد قانون الإجراءات الجزائية في مواجهة الجرائم السيبرانية.

الخاتمـــــــة

في ختام هذه الدراسة التي تناولت بشكل شامل موضوع المواجهة الجزائية للجرائم السيبرانية في القانون العُماني، حيث تم إبراز الأهمية المتزايدة لدراســـة هذا الموضـــوع في ظل التقدم التكنولوجي الســـريع الذي يشـــهده العالم، وتزايد الاعتماد على الإنترنت والتكنولوجيا الرقمية في مختلف جوانب الحياة، وإبراز الحاجة الملحة لتطوير الأطر القانونية القادرة على مواجهة الجرائم الســـيبرانية بفعالية، وتوفير الحماية اللازمة للمجتمع والأفراد من التهديدات التي تنشأ في الفضاء الإلكتروني.

سعت هذه الدراسة إلى تحليل النصوص القانونية ذات الصلة، وتبيّن أن السلطنة بذلت جهود كبيرة في مواجهة الجرائم السيبرانية سواء كان على مستوى التشريعات أو تطوير التقنيات اللازمة لذلك، إلا إن هذه التشـــريعات لا تزال بحاجة إلى تحديث وتطوير شـــامل لمواكبة التحديات الجديدة التي تفرضـها الطبيعة المتغيرة لهذه الجرائم، التي تتميز بتعقيداتها التقنية وصـعوبة اكتشـافها وملاحقتها، مما يحتم ضرورة وضع تشريعات مرنة وفعالة قادرة على التعامل مع هذه الجرائم باحتراف وكفاءة.

أظهرت الدراســة أن هناك فجوات قانونية قد تســتغل من قبل مرتكبي الجرائم الســيبرانية، بما يعزز من الحاجة إلى إصــدار قانون شــامل ومتكامل لمكافحة الجرائم الســيبرانية في الســلطنة يتســم بالشـــمولية ويغطي جميع أنواع الجرائم الســـيبرانية، مع الأخذ في الاعتبار أحدث التطورات التقنية والمعايير الدولية، لضمان فعاليته في مواجهة التهديدات السيبرانية المعاصرة.

من جانب آخر، تؤكد الدراســة على ضــرورة تأهيل وتطوير الكوادر القائمة على مكافحة هذه الجرائم، وتطوير اسـتراتيجيات فعالة لمكافحتها وملاحقة الجناة وتحقيق الردع العام والخاص، كما تبرز الحاجة إلى البحث المستمر في هذا المجال، بهدف تقييم فعالية التشريعات واستكشاف السبل المثلى لتحســينها بما يتناســب مع التحديات المســتقبلية، ويبقى الأمل في أن تســهم هذه الدراســة في تحفيز الجهود الوطنية الرامية إلى تعزيز الأمن الســيبراني في الســلطنة، وتطوير الســياســات والتشــريعات والإجراءات القانونية المتعلقة بمكافحة الجرائم السيبرانية، وقد توصلت الدراسة إلى مجموعة من النتائج والتوصيات، وهي كالآتي:

أولًا: النتائـــــــج

أسفرت الدراسة عن النتائج الآتية:

١. تعريف المشرع العُماني لـــــــ "جرائم تقنية المعلومات"، يعكس محدودية قدرة هذا التعريف على استيعاب التطورات الجديدة في مجال الجرائم السيبرانية.

٢. تتميز الجرائم السـيبرانية بخصـائص تجعلها أكثر تعقيدًا في الكشـف عنها ومكافحتها، ويتطلب التصدي لها تشريعات وتقنيات متقدمة.

٣. تتنوع أشـكال الجريمة السـيبرانية وتعبر الحدود الزمانية والمكانية، حيث يمكن أن تُرتكب ضـد الأشخاص أو المؤسسات أو الدول.

٤. تختلف الطبيعة القانونية للجريمة السـيبرانية عنها في الجرائم التقليدية، من حيث تحقق أركانها، ووسائل ارتكابها وأطرافها.

٥. حرص المشـرع العُماني على وضـع إطار تشـريعي بإصـدار قوانين عامة للتعامل مع التحديات التي تفرضـها التقنيات الحديثة، كما أصـدر قانون مستقل لمكافحة جرائم تقنية المعلومات، وهي خطوة تعكس التزام السلطنة بالتصدي للجرائم السيبرانية وحماية المجتمع من تهديداتها.

٦. سعت السلطنة إلى تطوير تقنيات الأمن السيبراني، وإنشاء مراكز ومختبرات متخصصة بالأمن السيبراني، ومكافحة الجريمة السيبرانية.

٧. تزداد أهمية الخبرة والمختبرات الرقمية في إثبات الجريمة السـيبرانية، نظرًا لما يتطلب إثباتها من خبرة علمية وعملية في المجال التقني والرقمي، فضـلًا عن الحاجة الملحة إلى تأهيل وتدريب العاملين في السلطات المعنية بمكافحة هذه الجرائم على أحدث التقنيات، ومواكبة التطورات التقنية.

٨. التشريعات العُمانية المواجهة للجرائم السيبرانية لم تواكب التهديدات والتحديات المتزايدة التي تفرضـها التقنية، ولا تزال غير كافية لتوفير الحماية المطلوبة في عصر يشهد تحولًا كبيرًا نحو الرقمية.

٩. عدم كفاية قانون الإجراءات الجزائية الصادر بالمرسوم السلطاني رقم (٩٩/٩٧) للتصدي للجرائم السيبرانية، إذ أنه لم ينص على إجراءات خاصة بها، مما يحد من فاعليته أمام التعقيدات التقنية لهذه الجرائم.

ثانيًا: التوصيـــــات

في ضـوء النتائج التي توصـلت إليها هذه الدراسـة، يُقدّم الباحث التوصـيات التالية لتعزيز قدرة السلطنة على التصدي للجرائم السيبرانية:

١. **دعوة المشرع العُماني إلى وضع تعريف شامل ودقيق للجرائم السيبرانية يتضمن جميع الأنواع الحاليـة والمحتملـة في المســـتقبل:** تتبنى التشـــريعات نهجًا يقضـــي بترك تعريف بعض المصـــطلحات للاجتهاد الفقهي والقضـــائي، إلا أن التعقيد الذي يحيط بهذه الجرائم، وتنوعها المستمر، وما تتطلبه من إجراءات خاصة للتعامل معها، تفرض ضرورة تعريفها من قبل المشرع بوضـوح وبشـكل دقيق ومتكامل، بما يتيح اسـتيعاب جميع الأفعال المرتبطة بالجرائم السـيبرانية، وتعزيز فعالية التنفيذ، وحماية الأفراد والمؤسسات.

٢. **حث المشـرع العُماني على إصـدار قانون جزائي متكامل خاص بالجرائم السـيبرانية:** في ضـوء التحديات التي تعترض السلطات المختصـة بمواجهة الجرائم السيبرانية، وعدم مواكبة التشريعات الحالية للتهديدات المتزايدة المصـــاحبة للتطور التقني والتكنولوجي، فقد أصـــبح إصـــدار قانون شامل يقدم إطارًا قانونيًا متكاملًا يتماشى مع التحولات السريعة في البيئة الرقمية مطلبًا ضروريًا لتعزيز الثقة في البيئة الرقمية ويضمن حماية فعّالة للمجتمع والاقتصاد من المخاطر المتنامية.

٣. **دعوة المشـرع العُماني إلى تعديل قانون الإجراءات الجزائية:** تشـير نتائج الدراسـة إلى أن قانون الإجراءات الجزائية الصـادر بالمرسـوم السـلطاني رقم (٩٩/٩٧) لا يتضـمن إجراءات خاصـة بالتعامل مع الجرائم السـيبرانية، مما يحد من فاعليته في مواجهة التعقيدات التقنية لهذه الجرائم، ويتعين معه النظر في تعديل القانون لإدخال إجراءات تتناســـب مع الطبيعة التقنية للجرائم السـيبرانية، يتضـمن أحكام خاصـة بإجراءات الاسـتدلال والتحقيق الابتدائي والمحاكمة للجرائم السيبرانية، لتكون ملائمة للتحديات التقنية الجديدة، ويضمن استجابة قانونية أكثر ملاءمة.

٤. **العمل على إنشـــاء مختبر جزائي رقمي وطني:** حيث أن تعدد المختبرات الرقمية الحالية يمكن أن يؤدي إلى تباين في تقنيات العمل ومعايير التحقيق، مما يؤثر ســلبًا على دقة وفعالية الأدلة الرقمية، ولضـمان تحقيق أعلى مسـتويات الدقة والموثوقية في التعامل مع الأدلة الرقمية، ينبغي

إنشاء مختبر جزائي رقمي وطني، مزود بأحدث التقنيات وأفضل الكفاءات الوطنية، وإلغاء باقي المختبرات الرقمية الحالية، بما يسهم في توحيد المعايير والتقنيات، وتحسين جودة الأدلة الرقمية، وتحقيق فعالية واستجابة النظام القانوني في التصدي للجرائم السيبرانية بصورة أكثر دقة وموثوقية، فضلًا عن اسهامه في توفير النفقات وتركيز الجهود.

٥. **حث السلطة المختصة على اعتماد أطر قانونية خاصة باعتماد قوائم الخبراء في الجرائم السيبرانية:** تُبرز الحاجة إلى تعزيز فعالية التحقيقات في الجرائم السيبرانية أهمية وجود معايير محددة لاختيار الخبراء المؤهلين؛ لضمان اختيار الخبراء المناسبين وفقًا للتخصصات الدقيقة وتحديث معارفهم لمواكبة التطورات التقنية السريعة، وذلك باعتماد أُطر قانونية خاصة لإعداد قوائم الخبراء في هذا المجال، تساعد في تحسين جودة الأدلة الرقمية وتعزيز دقة الإجراءات القانونية، مما يدعم بدوره الأحكام القضائية من خلال توفير تقارير موثوقة ومبنية على أحدث التقنيات، ويعزز فعالية النظام القضائي في معالجة الجرائم السيبرانية ويضمن تقديم أحكام دقيقة ومستندة إلى أسس علمية قوية.

٦. **تعزيز التدريب والتأهيل المستمر للكوادر العاملة في مكافحة الجرائم السيبرانية:** نظرًا للتطور المتسارع في تقنيات الجرائم السيبرانية وتعقيداتها المتزايدة، يصبح تكثيف برامج التدريب والتأهيل المستمر للقضاة وأعضاء الادعاء العام ومأموري الضبط القضائي مطلب أساسي؛ لتمكينهم من مواكبة أحدث التحديات التقنية وتعزيز كفاءتهم في التعامل مع هذه الجرائم بشكل فعال، حيثُ أن الاستثمار في رفع مستوى التأهيل لهذه الكوادر يضمن جاهزيتهم وتسلحهم بالمعرفة والمهارات اللازمة لمواجهة التهديدات السيبرانية المتجددة، مما يسهم في تحقيق العدالة بكفاءة عالية وحماية المجتمع من المخاطر الرقمية.

قائمة المراجع

أولًا: المراجع العامة

الكتـــــــب:

١. أشرف سيد أبو العلا، (٢٠٢٢)، الحماية الجنائية لحق الإنسان في الصحة (دراسة مقارنة بين القانون الوضعي والشريعة الإسلامية)، دار النهضة العربية، القاهرة.

٢. آمال عبد الرحيم عثمان، (١٩٦٤)، الخبرة في المســـائل الجنائية، مطبوعات كلية الحقوق، جامعة المنصورة، القاهرة.

٣. براء منذر كمال، (٢٠٠٩)، شرح قانون أصول المحاكمات الجزائية، دار الحامد للنشر والتوزيع، عمّان، ط١.

٤. حمد الربيعي، (٢٠١٠)، القيود الجنائية على حرية التعبير عن الرأي من خلال وسائل الإعلام، دار النهضة العربية، القاهرة.

٥. ســعيد حماد صـــالح قبائلي، (٢٠٠٥)، حق المتهم في الاســتعانة بمحام: دراســة مقارنة، دار النهضة العربية، القاهرة.

٦. ضـــاري خليل، (٢٠٠٥)، الوجيز في شـــرح قانون العقوبات، دار القادســـية للنشـــر والطباعة والتوزيع، بغداد.

٧. طارق ابراهيم دســـوقي عطية، (٢٠١٠)، عولمة الجريمة، الشـــركات العالمية في الممارســـات الاجرامية، دار الجامعة الجديدة، الإسكندرية.

٨. طارق زين، (٢٠١٧)، الجريمة المنظمة العابرة للحدود الوطنية، المركز العربي للبحوث القانونية والقضائية جامعة الدول العربية، بيروت، ط١.

٩. طارق ســـرور، (٢٠٠٩)، الوجيز في قانون العقوبات (القســـم الخاص)، جرائم الاعتداء على الأشخاص، مطبوعات جامعة القاهرة، القاهرة.

١٠.عبد الرحمن بن عبد الله السـند، (٢٠٠٥)، الأحكام الفقهية للتعاملات الإلكترونية (الحاسـب الآلي وشبكة المعلومات الإنترنت)، دار الوراق للطباعة والنشر والتوزيع، الرياض.

١١.فخري عبد الحسن علي، (١٩٩٩)، المرشد العلمي للمحقق، منشورات مديرية الشرطة، بغداد.

١٢.ماهر عبد شويش وآخرون، (٢٠٠٠)، نظرية تعادل الأسباب في القانون الجنائي، دار ومكتبة الحامد للنشر، عمّان.

١٣.محمد الجبور، (٢٠١٢)، الوسيط في قانون العقوبات (القسم العام)، دار وائل، عمّان، ط١.

١٤.محمود نجيب حسنى، (١٩٨٤)، علاقة السببية في قانون العقوبات، دار نادي القضاة، مصر.

١٥.محمود نجيب حسني، (١٩٧١)، النظرية العامة للقصد الجنائي، دار النهضة العربية، مصر، ط٢.

١٦.نادر عبد العزيز شافي، (٢٠٠٧)، المصارف والنقود الإلكترونية، المؤسسة الحديثة للكتاب، لبنان.

١٧.نوال بنت علي بن عبد الله البلوشـية، (٢٠٢٠)، العوامل المسـاعدة على التحول الرقمي في سلطنة عُمان، الاتحاد العربي للمكتبات والمعلومات، العدد ٢٦، تونس.

الدراسات والرسائل الجامعية

١. ابتسام السايس، صفاء نيلي، (٢٠٢٠)، وسائل الدفع في التجارة الإلكترونية، رسالة لنيل درجة الماجستير في جامعة قاصدي مرباح ورقلة، الجزائر.

٢. أمل بنت سعيد المشايخي، (٢٠١٧)، مستقبل الأمن السيبراني في سلطنة عُمان، رسالة لنيل درجة الماجستير في جامعة السلطان قابوس، مسقط.

٣. آية جمال المغربي، (٢٠١٦)، ضـوابط حرية الرأي والتعبير عن الرأي في التشـريع الفلسـطيني والمواثيق الدولية، رسالة لنيل درجة الماجستير في الجامعة الإسلامية، غزة.

٤. رقية بنت خلفان بن ناصر العبدلية، (٢٠٢٢)، حوكمة البيانات وفاعلية تطبيقها في المؤسسات الحكومية في سلطنة عُمان، رسالة لنيل درجة الماجستير، جامعة السلطان قابوس، مسقط.

الأبحاث والمقالات والدوريات

١. إذاعة الوصـال، سـلطنة عُمان، إيناس ناصـر، الدكتور/ خميس الحجري – رئيس مركز الدفاع الإلكتروني، تمت المقابلة في ٢٨ مايو ٢٠٢٤م.

٢. أشـرف توفيق شـمس الدين، (٢٠٠٨)، المسـئولية الجنائية والركن المعنوي للجريمة، الضـوابط الدستورية لنصوص التجريم والعقاب في قضاء المحكمة الدستورية العليا، مجلة الدستورية، العدد (١٤)، مصر.

٣. بوابة عماننا (https://omanportal.gov.om)، المركز الوطني للسلامة المعلوماتية.

٤. التقرير التفسيري لاتفاقية "بودبست"، (٢٠٠١)، المجلس الأوروبي، سلسلة المعاهدات الأوروبية رقم (١٨٥).

٥. حسـام محمد السـيد محمد، (٢٠١٩)، المواجهة الجنائية لظاهرة الثأر الإباحي، دراسـة مقارنة بين النظامين الأنجلو أمريكي واللاتيني، مجلة الدراسات القانونية والاقتصادية، عدد ٩(٥)، ص١٨٥.

٦. حسـين يوسـف أبو منصـور، (٢٠٢٠)، الذكاء الاصـطناعي وأبعاده، أوراق السـياسـة الأمنية، جامعة نايف للعلوم الأمنية، عدد ١.

٧. دعاء أحمد توفيق، (٢٠١٩)، الأمن الاجتماعي وتداعيات العملة الرقمية، مجلة كلية الآداب والعلوم الإنسانية، جامعة قناة السويس، العدد (٣١)، مصر.

٨. سـامح عبد الواحد التهامي، (٢٠١٥)، ضـوابط معالجة البيانات الشـخصـية، دراسـة مقارنة بين القانون الفرنسي والقانون الكويتي، مجلة كلية القانون الكويتية العالمية، المجلد ٣، العدد ٩.

٩. صـحيفة أثير الإلكترونية، https://www.atheer.om، متى يكون الإعلان مضـللًا، منشـور صادر عن الهيئة العامة لحماية المستهلك.

١٠. صـــحيفة الشـــبيبة الإلكترونية، الموقع الالكتروني (https://shabiba.com)، تدشـــين أول أكاديمية للأمن الإلكتروني المتقدم بالسلطنة.

١١. صحيفة الوطن، سلطنة عُمان، مختبر الأدلة الجنائية يتجه لإضافة (الوسائط المتعددة).

١٢.عبد الفتاح حجازي، (٢٠٠٤)، التوقيع الإلكتروني في النظم المقارنة، دار الفكر الجامعي، الإسكندرية.

١٣.عبد الكريم درويش، (٢٠٠٠)، نحو استراتيجية للموارد البشرية في المؤسسات الشرطية، مجلة الفكر الشرطي، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، المجلد التاسع، العدد الثاني، يوليو ٢٠٠٠م.

١٤.علي بن خلفان الهنائي، (٢٠٢١)، الحس الأمني لدى رجال الشرطة: تعريفه وأهميته وخصائصه وأهدافه، أكاديمية السلطان قابوس لعلوم الشرطة، سلطنة عُمان.

١٥.مجموعة الأحكام الصادرة عن الدائرة الجزائية بالمحكمة العليا والمبادئ المستخلصة منها للسنتين القضائيتين السابعة عشر والثامنة عشر، المكتب الفني، مجلس الشؤون الإدارية للقضاء، ٢٠١٩.

١٦.مجموعة الأحكام الصادرة عن الدائرة الجزائية بالمحكمة العليا والمبادئ المستخلصة منها للسنتين القضائيتين الخامسة عشر والسادسة عشر المكتب الفني، مجلس الشؤون الإدارية للقضاء، ٢٠١٦.

١٧.مجموعة الأحكام الصادرة عن الدائرة الجزائية بالمحكمة العليا والمبادئ المستخلصة منها للسنة القضائية الحادية والعشرين، المكتب الفني، مجلس الشؤون الإدارية للقضاء، ٢٠٢٢.

١٨.مجموعة المبادئ والقواعد القانونية التي قررتها المحكمة العليا في الفترة من ٢٠٠١ الى ٢٠١٠، المكتب الفني، مجلس الشؤون الإدارية للقضاء.

١٩.الموقع الالكتروني (http://hussain-alghafri.blogspot.com/2011/07/blog-post_9603.html)،

٢٠.الموقع الالكتروني (https://cop.gov.om/about.aspx).

٢١.الموقع الالكتروني (https://me.kaspersky.com/resource).

٢٢.الموقع الإلكتروني الرسمي لشركة كاسبرسكي (https://me.kaspersky.com).

٢٣.الموقع الإلكتروني الرسمي لشركة مايكروسوفت (https://news.microsoft.com/en).

٢٤.الموقع الإلكتروني الرسمي لمركز الدفاع الإلكتروني (https://cdc.gov.om/).

٢٥.الموقع الإلكتروني الرسمي لمركز السلامة المعلوماتية (https://cert.gov.om).

٢٦.نادر عبد العزيز شافي، (٢٠٠٧)، بين احترام الحريات الشخصية ومراعاة مصلحة الدولة والأمن الوطني، مجلة الجيش، العدد (٢٦٣)، لبنان.

٢٧.نجلاء توفيق نجيب (٢٠١٩)، القضاء المتخصص ودوره في تطوير النظام القضائي، مجلة الحقوق، جامعة البحرين، المجلد (١٦)، العدد (٢)، البحرين.

٢٨.هيئة التحرير بمعهد الأمير سعود الفيصل للدراسات الدبلوماسية، (٢٠١٨)، درع المملكة الواقي لحماية مصالحها الحيوية وبنيتها التحتية الرقمية، مجلة الدبلوماسي، العدد (٩٠)، السعودية.

ثانيًا: المراجع المتخصصة

الكتـــــــب:

١.أشـــرف عبد القادر قنديل، (٢٠١٥)، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية.

٢.أمير فرج يوسف، (2016)، الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها، مكتبة الوفاء القانونية، الإسكندرية، ط١.

٣.تميم عبد الله سيف التميمي، (٢٠١٦)، الجرائم المعلوماتية في الاعتداء على الأشخاص، مكتبة القانون والاقتصاد، الرياض.

٤.جلال الزعبي، أسـامة المناعسـة، (٢٠١٧)، جرائم تقنية نظم المعلومات الإلكترونية: دراسـة مقارنة، دار الثقافة للنشر والتوزيع، عمّان.

٥.جلال محمد الزغبي، أسامة أحمد المناعسة، (٢٠١٠)، جرائم تقنية نظم المعلومات الالكترونية، دار الثقافة للنشر والتوزيع، عمّان، ط١.

٦. جميل عبد الباقي الصغير، (٢٠٠٢)، الجوانب الاجرائية للجرائم المتعلقة بالإنترنيت دار النهضة العربية، القاهرة.

٧. حازم محمد حنفي، (2017)، الدليل الإلكتروني ودوره في المجال الجنائي، دار النهضة العربية، القاهرة، ط١.

٨. حسين بن سعيد الغافري، (٢٠٠٩)، السياسة الجنائية في مواجهة جرائم الانترنت (دراسة مقارنة)، دار النهضة العربية، القاهرة.

٩. خالد حازم إبراهيم، (٢٠١٤)، دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية(الإنترنت) دراسة مقارنة، دار النهضة العربية، القاهرة.

١٠. خالد عياد الحلبي، (٢٠١١)، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمّان، ط١.

١١. خالد ممدوح إبراهيم، (٢٠٠٨)، الدليل الإلكتروني في الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية.

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

١٣. خالد ممدوح إبراهيم، (٢٠٠٩)، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط١.

١٤. خالد ممدوح إبراهيم، (٢٠٠٩)، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية.

١٥. راشد الشيدي، (٢٠٢٢)، الجرائم الإلكترونية، مكتبة الجيل الواعد، ط١، مسقط.

١٦. رشاد خالد عمر، (٢٠١٨)، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، الإسكندرية.

١٧. رضوى عبد الرحيم قنديل، (٢٠٢١)، الجرائم الإلكترونية ماهيتها وأنواعها وإجراءات الدعوى الجنائية في مكافحتها وفقًا لقانون سلطنة عُمان، دار الكتاب الجامعي، الإمارات العربية المتحدة، ط١.

١٨.سامي جلال فقي حسين، (2011)، التفتيش في الجرائم المعلوماتية: دراسة تحليلية، دار الكتب القانونية، مصر.

١٩.سامي علي حامد عياد، (٢٠٠٧)، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، الإسكندرية.

٢٠.عادل عزام، (2019)، جرائم القدح والذم والتحقير المرتكبة عبر الوسائط الإلكترونية: دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمّان.

٢١.عائشة بن قارة، (٢٠١٠)، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية.

٢٢.عبد العال الدريبي، محمد صادق إسماعيل، (٢٠١٢)، الجرائم الإلكترونية: دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت، المركز القومي للإصدارات القانونية، القاهرة، ط١.

٢٣.عبد الفتاح حجازي، (٢٠٠٤)، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة.

٢٤.عبد الفتاح حجازي، (٢٠٠٦)، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية.

٢٥.عبد الفتاح حجازي، (٢٠٠٧)، صراع الكمبيوتر والانترنت، دار الكتب القانونية، مصر.

٢٦.عبد الفتاح مراد، (٢٠٠٢)، شرح جرائم الكمبيوتر والإنترنت، دار الكتب والوثائق المصرية، مصر.

٢٧.عبد الكريم الردايدة، (٢٠١٣)، الجرائم المستحدثة واستراتيجية مواجهتها، دار ومكتبة حامد للنشر والتوزيع، عمّان، ط١.

٢٨.عبد الله عبد الكريم عبد الله، (٢٠٠٧)، جرائم المعلوماتية والانترنت (الجرائم الالكترونية)، منشورات الحلبي الحقوقية، لبنان.

٢٩.عبد الفتاح بيومي حجازي، (٢٠٠٢)، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت: دراسة متعمقة في جرائم الحاسب الآلي والانترنت، دار الكتب القانونية، مصر.

٣٠.عزة الحسن، (٢٠٠٩)، الجريمة المعلوماتية في القانون السوداني، الزيتونة للطباعة، السودان.

٣١.عفيفي كامل عفيفي، (٢٠٠٣)، فتوح الشـــاذلي، جرائم الكمبيوتر وحقوق المؤلف والمصـــنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، لبنان.

٣٢.على نعمة جواد الزرفي، (٢٠٢٠)، الجريمة المعلوماتية الماسة بالحياة الخاصة، دراسة مقارنة، المكتب الجامعي الحديث، الإسكندرية.

٣٣.علي جبار الحســـناوي، (٢٠٠٩)، جرائم الحاســـوب والإنترنت، دار اليازوري العلمية للنشـــر والتوزيع، عمّان.

٣٤.علي جعفر، (٢٠١٣)، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشـخاص والحكومة، منشورات زين الحقوقية، بيروت، ط١.

٣٥.غانم مرضي الشمري، الجرائم المعلوماتية، (٢٠١٦)، الدار العلمية الدولية، عمّان، ط١.

٣٦.غنـام محمـد غنـام، (٢٠١٧)، دور قـانون العقوبـات في مكـافحـة جرائم الكمبيوتر والإنترنـت "وجرائم الاحتيال المنظم باستعمال شبكة الإنترنت، دار الفكر والقانون، المنصورة.

٣٧.كاميران عزيز حسن، (٢٠٢٠)، الجهود الدولية في مواجهة الجرائم السيبرانية، منشورات الحلبي الحقوقية، لبنان، ط١.

٣٨.محمد الأمين البشري، (٢٠٠٤)، التحقيق في الجرائم المسـتحدثة، جامعة نايف للعلوم الأمنية، الرياض، ط١.

٣٩.محمد أمين البشـــري، (٢٠٠٤)، التحقيق في الجرائم المســـتحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، ط١.

٤٠.محمد حسين منصور، (٢٠٠٦)، المسؤولية الإلكترونية، منشأة المعارف، الإسكندرية.

٤١.محمد حماد مرهج الهيتي، (٢٠٠٤)، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشـــر والتوزيع، عمّان.

٤٢.محمد سامي الشوا، (١٩٩٤)، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة.

٤٣.محمد ســليمان خوالدة، (٢٠١٢)، جريمة الدخول غير المشــروع إلى موقع إلكتروني أو نظام معلومات وفق التشريع الأردني – دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمّان، ط١.

٤٤.محمد عبد الله ابو بكر ســـلامة، (٢٠١١)، موســـوعة جرائم المعلوماتية "جرائم الكمبيوتر والإنترنت"، المكتب العربي الحديث، مصر.

٤٥.محمد عبد الله قاســم، (٢٠١٠)، الحماية الجنائية للمعلومات الإلكترونية، دار الكتب القانونية، مصر، ط١.

٤٦.محمد عبيد الكعبي، (٢٠٠٩)، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، ط٢.

٤٧.محمد علي العريان، (٢٠١٠)، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية.

٤٨.محمد كمال محمود الدسوقي، (٢٠١٧)، الحماية الجنائية لسرية المعلومات الإلكترونية: دراسة مقارنة، دار الفكر والقانون، المنصورة، ط١.

٤٩.محمود أحمد القرعان (٢٠١٧)، الجرائم الإلكترونية، دار وائل للنشر والتوزيع، عمّان، ط١.

٥٠.محمود أحمد القرعان، (٢٠١٧)، الجرائم الإلكترونية، دار وائل للنشر والتوزيع، عمّان، ط١.

٥١.محمود أحمد عبابنة، (٢٠٠٥)، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمّان.

٥٢.محمود رجب فتح الله، (٢٠١٩)، شرح قانون مكافحة جرائم تقنية المعلومات في ضوء القانون المصري ١٧٥ لسنة ٢٠١٨ دراسة تحليلية مقارنة، دار الجامعة الجديدة، الإسكندرية.

٥٣.محمود عمر محمود، (٢٠١٥)، الجرائم المعلوماتية والإلكترونية، خوارزم العلمية، السعودية، ط١.

٥٤.مدحت عبد الحليم رمضـــان، (٢٠٠١)، الحماية الجنائية للتجارة الإلكترونية، دار النهضـــة العربية، القاهرة.

٥٥.مدحت عبد الحليم رمضان، (٢٠١٥)، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة،

٥٦.مصـطفى محمد موسـى (٢٠٠٩)، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشـرطة، القاهرة، ط١.

٥٧.مصطفى محمد موسى، (٢٠١٠)، دليل التحري عبر شبكة الإنترنت، دار الكتب القانونية، مصر.

٥٨.ممدوح عبد الحميد عبد المطلب، (٢٠٠٦)، البحث والتحقيق الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب الوطنية، مصر.

٥٩.ممدوح عبد الحميد عبد المطلب،) ٢٠٠٥)، أدلة الصـــور الرقمية في الجرائم عبر الكمبيوتر، مركز بحوث الشرطة، الشارقة، ط١.

٦٠.منير محمد الجنبيهي، (٢٠٠٦)، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاســـب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية.

٦١.نائلة عادل محمد فريد قورة، (٢٠٠٤)، جرائم الحاسـب الآلي الاقتصـادية، منشـورات الحلبي الحقوقية، بيروت.

٦٢.نبيلة هبة هروال، (٢٠١٣)، الجوانب الإجرائية لجرائم الانترنيت في مرحلة جمع الاســتدلالات دراسة مقارنة، دار الفكر الجامعي، الإسكندرية.

٦٣.نهلا عبد القادر المومني، (٢٠٠٨)، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمّان.

٦٤.هدى حامد قشـقوش، (١٩٩٢)، جرائم الحاسـب الإلكتروني في التشـريع المقارن، دار النهضـة العربية، القاهرة.

٦٥.هشام فريد رستم، (1994)، الجوانب الإجرائية للجرائم المعلوماتية، دار النهضة العربية، القاهرة.

٦٦.هشـام محمد فريد رسـتم، (١٩٩٨)، الجوانب الإجرائية للجرائم المعلوماتية: دراسـة مقارنة، دار النهضة العربية للنشر والتوزيع، القاهرة.

٦٧.هلالي عبد اللاه أحمد، (2000)، التزام الشاهد بالإعلام في الجريمة المعلوماتية، دار النهضة العربية، القاهرة.

٦٨.هلالي عبد اللاه أحمد، (٢٠١١)، كيفية المواجهة التشـــريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست دار النهضة العربية، القاهرة.

٦٩.وليد الزيدي (٢٠٠٩)، القرصنة على الإنترنت والحاسوب، دار أسامة للنشر، عمّان، ط٣.

الدراسات والرسائل الجامعية

١. أشـرف بن عبد الله الضـويحي، (٢٠١٣)، المسـاهمة في الجرائم المعلوماتية المتعلقة بالاعتداء الشخصي، رسالة لنيل درجة الماجستير، جامعة الإمام محمد بن سعود الإسلامية، السعودية.

٢. توات عبد الحكيم، (٢٠٢٢)، جريمة الإرهاب الإلكتروني، رســـالة لنيل درجة الماجســـتير في جامعة العربي التبسي، الجزائر.

٣. شـــيماء عبد الغنى، (٢٠٠٥)، الحماية الجنائية للتعاملات الإلكترونية، اطروحة دكتوراه، كلية الحقوق، جامعة المنصورة، مصر.

٤. عبد اللطيف معتوق، (٢٠١١ – ٢٠١٢)، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، رسالة لنيل درجة الماجستير، جامعة العقيد الحاج لخضر بباتنة، الجزائر.

٥. عبد الله محمد كريري، (٢٠١٣)، الركن المعنوي في الجرائم المعلوماتية في النظام الســـعودي، دراسة تأصيلية، رسالة لنيل درجة الماجستير، جامعة نايف للعلوم الأمنية، السعودية.

٦. فتيحة رصـاع، (٢٠١١ – ٢٠١٢)، الحماية الجنائية للمعلومات على شـبكة الأنترنت، رسـالة لنيل درجة الماجستير، جامعة أبي بكر بلقايد، كلية الحقوق والعلوم السياسية، الجزائر.

٧. يوسف صغير، (٢٠١٢ – ٢٠١٣)، الجريمة المرتكبة عبر الإنترنت، رسالة لنيل درجة الماجستير، جامعة مولود معمري بتيزي وزو، الجزائر.

الأبحاث والمقالات والدوريات

١. أحمد بن مالك، (٢٠٢١)، دور الأدلة الرقمية في الإثبات الجنائي، مجلة العلوم الإنسانية، المركز الجامعي علي كافي تندوف، المجلد (٥)، الإصدار الأول، الجزائر.

٢. أحمد لطفي مرعي، (٢٠٢٢)، انعكاسات تقنيات الذكاء الاصطناعي على نظرية المسؤولية الجنائية، مجلة البحوث القانونية والاقتصادية، العدد (٨٠/ يونيو ٢٠٢٢)، المنصورة.

٣. أيمن محمد عبد اللطيف، إشكالية إثبات الجرائم الإلكترونية، الموقع الإلكتروني:(https://ae.linkedin.com/pulse)، تم الاستيراد بتاريخ ٢٠ مارس ٢٠٢٣م.

٤. حسين بن سعيد الغافري، (٢٠٢٢)، الحماية الجزائية للتوقيع الالكتروني "في ضوء التشريع العُماني والتشريع المقارن"، مجلة البحوث الفقهية والقانونية، العدد (٣٩)، اكتوبر ٢٠٢٢، مصر.

٥. حفيظة بنت سليمان البراشدى، (٢٠١٩)، الفيسبوك والجرائم الإلكترونية في عمان، مجلة دراسات المعلومات والتكنولوجيا، المجلد (٢)، العدد (٢)، دار جامعة حمد بن خليفة للنشر، قطر.

٦. حكم المحكمة الابتدائية بمسقط – الدائرة الجزائية، الدعوى الجزائية رقم (٢٠٢٤/ ٥١٠٠/ ٢٠٢٢).

٧. خالد ظاهر عبدالله المطيري، (٢٠٢٢)، دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي، مجلة البحوث الفقهية والقانونية، العدد ٣٨، مصر.

٨. خليل بن حمد البوسعيدي، (٢٠٢٢)، السياسة العقابية التي اتبعها المشرع العُماني في قانون مكافحة الجرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم (١٢/ ٢٠١١)، مجلة ابن خلدون للدراسات والأبحاث، المجلد ٢، العدد ١٢، فلسطين.

٩. دينا عبدالعزيز فهمي، (٢٠١٧)، المسؤولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي، مجلة كلية الحقوق، جامعة طنطا، مصر.

١٠.روان بنت عطية هللا الصحفي، (٢٠٢٠)، الجـرائـم السيبـــرانيـة، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد ٢٤، الأردن.

١١.ســـامي الرواشـــدة وأحمد الهياجنة، (٢٠٠٩)، مكافحة الجريمة المعلوماتية بالتجريم والعقاب، المجلة الأردنية في القانون والعلوم السياسية، جامعة مؤتة، المجلد (١)، العدد (٣)، الأردن.

١٢.سامي الرواشدة، (٢٠١٧)، الأدلة المتحصلة من مواقع التواصل الاجتماعي ودورها في الإثبات الجنائي، المجلة الدولية للقانون، المجلد (٦)، العدد (٣)، قطر.

١٣.سميرة معاشي، (٢٠١١)، ماهية الجريمة المعلوماتية، بحث منشور في مجلة المنتدى القانوني، العدد السابع، جامعة محمد خيضر بسكرة، الجزائر.

١٤.صـابرين جابر أحمد محمد، محمود بن علي بن سـهيل المعشـني (٢٠٢٣)، المواجهة الجنائية لجريمة الاحتيال الالكتروني في التشـريع العُماني، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، المركز الجامعي بأفلو، العدد (١٠)، مارس ٢٠٢٣، الجزائر.

١٥.صـــابرين جابر محمد، (٢٠٢٠)، الجريمة الإلكترونية ومكافحتها في القانون العُماني، المجلة المصرية للدراسات القانونية والاقتصادية، العدد ١٤، مصر.

١٦.صحيفة عمان أوبزرفر الإلكترونية، سلطنة عُمان.

١٧.عبد الحميد الدوحاني، سـليم القيسـي، (٢٠٢٠)، السـياسـات الجنائية في مواجهة جرائم تقنية المعلومات في المجتمع العُماني من وجهة نظر المحاميـــن في سلطنة عُمان، حوليات آداب عين شمس، المجلد ٤٨، عدد أكتوبر – ديسمبر ٢٠٢٠، مصر.

١٨.عبد العزيز بن فهد بن محمد ابن داود، (٢٠٢٠)، الجرائم السـيبرانية: دراسـة تأصـيلية مقارنة، مجلة الاجتهاد للدراسات القانونية والاقتصـادية، معهد الحقوق والعلوم السياسية، المجلد ٩، ال عدد٣، الجزائر، ٢٠٢٠.

١٩.عبد الله بن على بن سالم الشبلي، (٢٠١٩)، الجريمة الالكترونية في سلطنة عُمان: التحديات والحلول القانونية، المركز القومي للبحوث، المجلد (٣)، العدد (٢)، غزة.

٢٠.علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيًا، مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات، الإمارات، مايو ٢٠٠٠

٢١.عماد الدين محمد عبد الحميد، (٢٠٢٣)، الشـــرطة الذكية ودورها في ضـــبط الجرائم في المجتمع الإماراتي، مجلة الدراسات الإنسانية والاجتماعية، المجلد رقم (٥٠)، العدد (٦/ ٢٠٢٣)، الإمارات.

٢٢.عماد الدين محمد عبد الحميد، (٢٠٢٣)، الشـــرطة الذكية ودورها في ضـــبط الجرائم في المجتمع الإماراتي، مجلة الدراسات الإنسانية والاجتماعية، المجلد رقم (٥٠)، العدد (٦/ ٢٠٢٣)، الإمارات.

٢٣.كريم احليحل، ٢٠٢٣، الجريمة الســـيبرانية والجهود الدولية في مواجهتها، المجلة الإلكترونية الدولية لنشر الأبحاث القانونية، المجلد ١، العدد ٣، المغرب.

٢٤.محمد حبحب، (٢٠١٨)، تطبيق القواعد الجزائية الإجرائية على الجريمة الإلكترونية: تحديات وآفاق، مجلة كلية القانون الكويتية العالمية، المجلد (٦)، الكويت.

٢٥.محمد زروق، (٢٠١٨)، إشـــكالية الحصـــول على الدليل الإلكتروني في الجريمة المعلوماتية، مختبر البحث في قانون الأعمال، جامعة الحسن الأول، العدد (٣٣)، المغرب.

٢٦.محمد ســامي الشــوا، (٢٠٠٥)، الغش المعلوماتي، جامعة نايف العربية للعلوم الأمنية، المجلد (٢٤)، العدد (٢٨٠)، السعودية.

٢٧.محمد مسعد حميد، (٢٠١٩)، رؤية إستراتيجية لمكافحة الجرائم السيبرانية: اليمن دراسة حالة، المجلة العربية الدولية للمعلوماتية، اتحاد الجامعات العربية، جمعية كليات الحاســـبات والمعلومات، المجلد ٧، العدد ١٢.

٢٨.محمود عبد الرحمن، (٢٠١٥)، التطورات الحديثة لمفهوم الحق في الخصـــوصـــية "الحق في الخصوصية المعلوماتية" مجلة كلية القانون الكويتية العالمية، العدد التاسع، الكويت.

٢٩.مســـعود المعمري، (٢٠١٨)، الدليل الإلكتروني في إثبات الجريمة الإلكترونية، مجلة كلية القانون الكويتية العالمية، العدد (٣)، الكويت.

٣٠.مصعب القطاونة، (٢٠١٠)، الإجراءات الجنائية الخاصة في الجرائم المعلوماتية، بحث مقدم لشبكة قانوني الأردن، الأردن.

٣١.مفتاح بو بكر المطردي، (٢٠١٢)، الجريمة الإلكترونية، مؤتمر رؤساء المحاكم العليا الثالث في الدول العربية، السودان.

٣٢.مليكة عطوي، (٢٠١٢)، الجريمة المعلوماتية، حوليات جامعة الجزائر، العدد ٢١، الجزائر.

٣٣.منصور حسان، (٢٠٢٣)، جريمة الابتزاز الإلكتروني "دراسة مقارنة بين القانون المصري والفرنسي والإماراتي والنظام السعودي، المجلة القانونية، المجلد ١٧، العدد ٥، مصر.

٣٤.الموقع الإلكتروني (fastercapital.com).

٣٥.يونس عرب، حجية الإثبات بالمستخرجات الإلكترونية في القضايا المصرفية، مجلة البنوك، الأردن، ٢٠١٠، ص ٣٠٧.

ثالثًا: القوانين

١. النظام الأساسي للدولة الصادر بالمرسوم السلطاني رقم (٢٠٢١/٦)، نشر في الجريدة الرسمية، العدد رقم (١٣٧٤) الصادر في ١٢ / ١ / ٢٠٢١م.

٢. قانون الجزاء الصادر بالمرسوم السلطاني رقم (٧ / ٢٠١٨)، نشر في الجريدة الرسمية، العدد رقم (١٢٢٦) الصادر في ١٤ / ١ / ٢٠١٨م.

٣. قانون الإجراءات الجزائية الصادر بالمرسوم السلطاني رقم ٩٧ / ٩٩، نشر في عدد الجريدة الرسمية العدد رقم (٦٦١) الصادر في ١٥ / ١٢ / ١٩٩٩م.

٤. قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم (١٢ / ٢٠١١)، نُشِر في الجريدة الرسمية، العدد رقم (٩٢٩) الصادر في ١٥ /٢ / ٢٠١١م.

٥. قانون المعاملات الإلكترونية الصادر بالمرسوم السلطاني رقم (٦٩ / ٢٠٠٨)، نُشر في الجريدة الرسمية، العدد (٨٦٤) بتاريخ ١ / ٦ / ٢٠٠٨م.

٦. قانون حماية البيانات الشخصية الصادر بالمرسوم السلطاني رقم (٦/ ٢٠٢٢)، نُشِر في الجريدة الرسمية، العدد رقم (١٤٢٩) الصادر في ١٣ / ٢ / ٢٠٢٢م.

٧. قانون تنظيم الاتصالات الصادر بالمرسوم السلطاني العُماني رقم (٣٠/ ٢٠٠٢)، نشر في الجريدة الرسمية، العدد رقم (٧١٥) الصادر في ١٧ / ٣ / ٢٠٠٢م.

٨. قانون تصنيف وثائق الدولة وتصنيف الأماكن المحمية الصادر بالمرسوم السلطاني رقم (١١٨/ ٢٠١١)، نشر في عدد الجريدة الرسمية رقم (٩٤٩) الصادر في ٢٠١١/١٠/٢٩م

٩. المرسوم السلطاني رقم (٦٤ / ٢٠٢٠) بإنشاء مركز الدفاع الإلكتروني، نشر في الجريدة الرسمية، العدد رقم (١٣٤٥) الصادر في ١٤ / ٦ / ٢٠٢٠م.

١٠. قانون حماية المستهلك الصادر بالمرسوم السلطاني رقم (٦٦/ ٢٠١٤)، نشر في الجريدة الرسمية العدد رقم (١٠٨١) الصادر في ٧/ ١٢ / ٢٠١٤م.

١١. اللائحة التنفيذية لقانون تنظيم الاتصالات، الصادر بالقرار رقم (١٤٤ / ٢٠٠٨).

رابعًا: المراجع الأجنبية

1. ABA Section Creates First Digital- Signature Guidelines to Aid in Security of The Internet, 1996.
2. Act no. 1996-393 of 13 May 1996 Article 1 Official Journal of 14 May 1996; Act no. 2000-647 of 10 July article 1 Official Journal of 11 July 2000.
3. ALAN BENSOUSSAN, INTERNET, Aspect Juridique, HERMES,1996.
4. Alexander Babuta, Innocent Until Predicted Guilty, Artificial intelligence and Police Decision – Making, Artificial intelligence and Policing, RUSI Newsbrief, March Vol . 38, No.
5. Andre Huet, Le droit penal international et Internet, les petites affiches,1999.
6. Bangara, A., Determinisim and the annihilation of mens rea, Nimera University Law Journal, Vol. 4 (1), 2014.
7. Bilel Benbouzid, Values and Consequences in Predictive Machine Evaluation.

8. Bonne, R ., Coughlin, A .M ., Jeffries, J ., and Peter, L ., Criminal Law, 2 ed ed ., New York, 2004.

9. BOSSON, les regles de l'expertise elaboreespor le cade de procedure genol, D, 1960.

10. Bouzat, P ., et Pinatel, J ., Traité de droit pénal et de criminologie, T . 1, Paris, 1963.

11. David Wall, Cybercrimes: New Wine, No Bottles, Invisible Crimes.

12. Duff, R .A ., Intention, agency and criminal liability, Basil Blackwell, 1989.

13. Eliott C . McLaughlin, Suspect Oks Amazon to Hand Over Echo Recordings in Murder Case, CNN (Apr . 26, 2017) .

14. Élise Ternynck, Le juge du contrat de travail et la preuve électronique: essai sur l'incidence des technologies de l'Information et de la communication sur le contentieux prud'homal, Ph D Thèse, PRES Université Lille Nord de France, 2014.

15. Fieke Jansen, Date Driven Policing in the Context of Europe, working paper, datajusticeproject, Cardiff University, May 2018.

16. Hosni, M .N ., L' Erreur de droit et son influence sur la responsabilité pénale, Rev . Sc . Crim ., Vol . 4, 1999.

17. Isabelle Lolies**,** La protection pénale de la vie privée, Presses Universites d´Aix-Marseille, 1999.

18. Lydon, M , Criminal law - rehabilitation, A Thesis; punishment, the Antithesis - Insanity Defense in the Balance, De Paul Law Review, Vol ., 140, 1969.

19. Marine Kettani, Predictive policing and Rule of technology, Webinaire IA and Law Breakfasts, organisé par le Conseil de l'Europe, le 02 .07 .2020

20. Osman Goni. Haidar Ali, Showrov. Mahbub Alam, & Abu Shameem . The Basic Concept of Cyber Crime, Journal of Technology Innovations and Energy,2022.

21. Over 400,000 Cyber Attacks Thwarted in Oman in 2020, Newspaper Times of Oman ,Publication Date: 13 January 2021.

22. R .Gassin, informatique et libert repertorie, dalloz de droit penal, janiper, 1987.

23. Ricordel, I., L'expertise en police scientifique, Dalloz, 2015.

24. Robert Taylor, Computer crime . In criminal investigation edited "by Charles Swanson, n . chameleon and Territory, hill, ine, 5th edition 1992.

25. Schuliar, Y., La coordination scientifiques dans les investigations criminalles, Proposition d' organization, aspects ethiques ou de la necessite d' un nouveau métier, Ph D these, Université Paris Descartes, 2009.

26. Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace, School of Law Faculty Publications, University of Dayton University of Dayton, 2010.

27. U .S . Department of Justice Central District of California Debra Wong Yang United States Attorney Thom Mrozek, Public Affairs Officer .

28. Villard, M., La cybercriminalité et l'expertise judiciaire, La Jaune et la Rouge, Décembre 2005.

29. Yamina Bouadi, Intelligence artificielle, justice pénale et protection des données à caractère personnel, M Sc Thése, Université de Strasbourg, 2020.