إشكالية الملاحقة الجزائية في الجرائم الإلكترونية

إعداد
د. فيصل جعيلان العازمي
دكتوراه في القانون العام
كلية الحقوق – جامعة القاهرة

موجز عن البحث

بات من الممكن ارتكاب الجريمة الإلكترونية في أي مكان على وجه الأرض، وقدرة الجاني على تنفيذ جريمته دون ترك أي أثر يمكن تتبعه، تجعل من الضروري اتخاذ إجراءات فورية لحماية الأدلة، حيث يزيد التحدي عند وجود أدلة الجريمة على أجهزة الحاسوب الموجودة في دول أخرى، مما يتطلب تعاونًا فوريًا بين السلطات القانونية للدول المتصلة بتلك الجريمة، وتتطلب هذه المهمة مستوى عالٍ من الصعوبة والتعقيد، حيث يمكن أن تختفي الأدلة إذا لم يتم اتخاذ الإجراءات اللازمة بسرعة. لذلك، يصبح من الضروري تعزيز التعاون الدولي بين الدول المتضررة والدول التي يمكن أن يمر فيها الجاني أو تتواجد فيها الأدلة، ولذلك تعتمد فعالية مكافحة هذا النوع من الجرائم على التعاون الفعّال بين الدول، حيث يتوجب عليها تقاسم المعلومات والتقنيات القانونية لضمان الوصول إلى الأدلة وتحديد الجناة، وبالتالي معاقبتهم وتحقيق العدالة.

وتحقيق هذا التعاون الدولي يشكل جزءًا أساسيًا في تحقيق أمن الرقمي ومكافحة التهديدات الإلكترونية، ومن هذا المنطلق سلطنا الضوء في دراستنا على إشكالية الملاحقة

الجزائية في الجرائم الإلكترونية وموقف قانون مكافحة جرائم تقنية المعلومات الكويتي رقم ٦٣ لسنة ٢٠١٥ من تلك الإشكالية، **ومن ثم كان لابد من بيان خلاصة موجزة لما احتواه هذا البحث، والذي قسمناه إلى مبحثين مبحثين رئيسيين.**

أما المبحث الأول فقد ناقشنا من خلاله أهم الأحكام العامة للجرائم الإلكترونية، ثم انتقلنا في **المبحث الثاني** لمناقشة الإشكاليات الموضوعية والإجرائية للجرائم الإلكترونية، وتناولنا فيه أهم الإشكاليات والتحديات التي تواجه الجرائم الإلكترونية سواء كانت خاصة بالأحكام الموضوعية أو الإجرائية في ضوء مواجهتها بالسياسة التشريعية التي تبناها قانون مكافحة جرائم تقنية المعلومات الكويتي رقم ٦٣ لسنة ٢٠١٥ ، وسُبل مواجهة تلك الإشكاليات.

الكلمات المفتاحية : الجرائم الإلكترونية، تقنية المعلومات، الملاحقة الجزائية للجرائم، الأدلة الإلكترونية ، الاختصاص الجزائي .

The Problem Of Criminal Prosecution For Cybercrimes

Faisal Jailan Al-Azmi
Doctorate in Public Law, Faculty of Law - Cairo University, Egypt
E-mail : faisal-alazmi47@gmail.com

Abstract:
It has become possible to commit cybercrime anywhere on the face of the earth, and the ability of the perpetrator to carry out his crime without leaving any traces makes it necessary to take immediate measures to protect the evidence, as the challenge increases when evidence of the crime is found on computers located in other countries, which It requires immediate cooperation between the legal authorities of the countries involved in the crime, and this task requires a high level of difficulty and complexity, as evidence can disappear if the necessary measures are not taken quickly. Therefore, it becomes necessary to strengthen international cooperation between the affected countries and the countries through which the perpetrator may pass or where evidence is present. Therefore, the effectiveness of combating this type of crime depends on effective cooperation between countries, as they must share information and legal techniques to ensure access to evidence and identify the perpetrators. , thus punishing them and achieving justice.
Achieving this international cooperation constitutes an essential part in achieving digital security and combating electronic threats. From this standpoint, we shed light in our study on the problem of criminal prosecution for cybercrimes and the position of the Kuwaiti Information Technology Crimes Law No. 63 of 2015 on that problem, and then it was necessary to clarify A brief summary of what this research contains, which we divided into two main sections.
As for the first section, we discussed the most important general provisions for cybercrimes. Then we moved in the second section to discuss the substantive and procedural problems of cybercrimes. In it, we discussed the most important problems and challenges facing cybercrimes, whether they were specific to substantive or procedural provisions, in light of confronting them with the legislative policy adopted by the Anti-Cybercrime Law. Kuwaiti Information Technology Crimes No. 63 of 2015, and ways to confront these problems.

Keywords: Electronic Crimes, Information Technology, Criminal Prosecution Of Crimes, Electronic Evidence, Criminal Jurisdiction.

مقدمة

شهد التطور المستمر والمتجدد لدور الحاسوب في المجتمع المعلوماتي تزايد الوعي حول أهمية المعلومات كمصدر للقوة والثروة. وارتبط هذا التحول بشمولية استخدام الإنترنت على مستوى العالم، حيث قدمت شبكة الاتصالات وتكنولوجيا المعلومات العديد من المزايا، وبات بالإمكان القيام بالكثير من الأمور التقليدية بشكل أفضل، بالإضافة إلى إمكانية التواصل بين الأفراد دون قيود مكانية أو زمانية، إلا أنه ومع ذلك، جلبت هذه التطورات خطرًا غير محدودًا في عالم الإنترنت، حيث يمكن استخدام الشبكة بشكل غير قانوني، مما أدى إلى حالة من الفوضى المعلوماتية عبر العالم الافتراضي، الأمر الذي زاد معه انتشار الجرائم الإلكترونية التي تفتقر إلى رقابة فعّالة بسبب عدم قدرة القوانين الجزائية على مواكبة التطور السريع في هذا العالم الرقمي.

ففي ظل تقدم التكنولوجيا وزيادة استخدام شبكة الإنترنت، بات من الأسهل على الجناة استغلالها في ارتكاب الجرائم. فشبكة الإنترنت تميزت بعدم وجود حدود جغرافية، مما يسمح للأفراد والمؤسسات بالتنقل بين دول العالم وهم في منازلهم، ونتيجةً لهذه الطبيعة الدولية لشبكة الإنترنت، تكتسب الجرائم التي ترتكب باستخدامها صفة دولية، حيث يمكن لأفراد من دول مختلفة المشاركة في ارتكاب جريمة واحدة، ويمكن أن يكون الضحايا في بلدان متعددة.

تلك الظروف وغيرها ساهمت في تعقيد التحقيق في الجرائم الإلكترونية، حيث قد تكون الأدلة الرقمية ضعيفة أو تتلاشى بسرعة، الأمر الذي يتطلب معه اتخاذ إجراءات سريعة لحفظ تلك الأدلة ومنع تلفها، وهذا لا يتأتى إلا من خلال تعاون السلطات في البلد الذي نشأت فيه الجريمة أو البلدان التي تم من خلالها النشاط الإجرامي.

وما زاد الأمر تعقيدا أن هذه الجرائم المستحدثة سريعة الحدوث بل وعابرة للحدود، ومن ثم تزيد الصعوبة بسبب اختلاف التشريعات في الدول المختلفة، وهو ما قد يحدث معه تنازع في الاختصاص الجنائي بشأن الجرائم الإلكترونية التي تتخطى الحدود الوطنية، حيث يمكن أن ترتكب جريمة في إقليم دولة معينة، ويكون الجاني أجنبيًا، مما يجعل الجريمة تخضع لاختصاص الدولة الثانية بناءً على مبدأ الاختصاص الشخصي، وقد تكون الجريمة التي ترتكب على إقليم دولة معينة تهديدًا لأمان دولة أخرى، مما يؤدي إلى اختصاص جنائي إقليمي ووطني في نفس الوقت بناءً على مبدأي الاختصاص العيني [١].

(١) فتحي محمد عزت، الحماية الجنائية والموضوعية والإجرائية، الاعتداء على المصنفات والحق في الخصوصية والكمبيوتر والإنترنت في نطاق التشريعات الوطنية والتعاون الدولي، دار النهضة العربية، ٢٠٠٧م، ص٤٠٧، وما بعدها.

بالإضافة إلى ما تطرحه هذه الجرائم من مشاكل قانونية أخرى تتعلق بالجهات المخول لها متابعة المجرم، أو من خلال المحكمة المختصة، فقد ترتكب الجريمة في دولة وتكون آثارها في دولة أخرى، وقد يكون الجاني يحمل جنسية دولة أخرى وتكون أدلة الجريمة موجودة في دولة أخرى وخارج النطاق الإقليمي لجهة التحقيق، فكيف يتم جمع الأدلة وضبطها وما هو القانون الواجب التطبيق.

ومن هذا المنطلق وفي ظل هذا التقدم الرهيب للتكنولوجيا واعتماد الكثير من العمليات والمعاملات على الوسائل الإلكترونية، أصبحت الجريمة الإلكترونية تشكل تحديًا كبيرًا للأمن السيبراني وحماية المعلومات.

وقد حاول المشرع الكويتي بدوره مسايرة التشريعات المقارنة الحديثة في شأن مواجهة تلك الإشكاليات والتحديات من خلال تبني سياسات تشريعية تهتم بمكافحة الجرائم الإلكترونية وتكنولوجيا المعلومات بهدف مواكبة التقنيات الحديثة والتحديات الكبيرة في هذا العالم الرقمي المتسارع، وقد أصدر المشرع الكويتي القانون رقم (٦٣) لسنة بشأن مكافحة جرائم تقنية المعلومات ٢٠١٥ للتصدي لهذه الظاهرة المتزايدة.

حيث تناول المشرع في هذا القانون مختلف أشكال الجريمة الإلكترونية، ووفر نصوصًا تجريمية تتعامل مع التحديات الفريدة لهذا النوع من الجرائم. وفي هذا السياق، يتساءل الباحث عما إذا كان المشرع الكويتي نجح في وضع قوانين شاملة

تغطي جوانب متعددة للجريمة الإلكترونية، وهل استفاد من الخبرات والتجارب الدولية والإقليمية في هذا المجال.

هل تمكّن المشرع الكويتي من سد الثغرات والنقائص التي قد تظهر في التشريعات المقارنة؟ وكيف يتفاعل القانون مع التحديات المستجدة والتطورات في مجال الجريمة الإلكترونية؟ وهل يلبي القانون احتياجات المجتمع في ظل التطور السريع للتكنولوجيا؟ هذه أسئلة تستدعي تقييمًا دقيقًا للقانون الكويتي المعلوماتي وفاعليته في مكافحة الجريمة الإلكترونية وحماية أمن السيبراني.

وهذا ما جعلنا نسلط الضوء في هذا البحث على أهم الإشكاليات التي تتعلق بالجرائم الإلكترونية.

سبب اختيار موضوع البحث:

ترجع أسباب اختيار موضوع البحث إلى محاولة لإيجاد تعريف واضح لمفهوم الجريمة الإلكترونية، مع التركيز على التحديات القانونية والإجرائية المرتبطة بها في التشريع الكويتي مع تقديم حلول للمشكلات العملية والتشريعية المتعلقة بهذا النوع من الجرائم، وتسليط الضوء على نواحي القصور في التشريع الكويت.

ووضع ما توصل إليه الباحث بين يدي المشرع الكويتي وأن يأخذ بعين الاعتبار النتائج والتوصيات التي توصل إليها، وذلك بهدف محاربة الجرائم الإلكترونية وتقليل انتشارها حفاظًا على حقوق الأفراد والحكومات، سواء على الصعيدين

الوطني والدولي، ومواكبة التطورات السريعة في هذا المجال.

أهمية البحث:

تتزايد أهمية هذ البحث نظرًا لاستغلال المرتكبين للجرائم وسائل الاتصال الحديثة، بهدف تسهيل ارتكابهم لتلك الجرائم. يتناول موضوع البحث قضية ذات أهمية نظرية وعملية، إذ يلمس مصالح المجتمع على المستوى الدولي والوطني، يظهر أهميته في تحديد مصادر المخاطر التي تهدد النظام المعلوماتي وتحديد أشكال الاعتداء على المعلومات عبر الإنترنت، بالإضافة إلى فحص الأنماط المتنوعة للجرائم الإلكترونية المستحدثة المتعلقة بتقنية المعلومات. وليس ذلك وحسب، بل له أهميته في فهم الاتجاهات التشريعية الدولية والإقليمية لحماية المعلومات وأنظمتها الإلكترونية، مع تسليط على الضوء على المشكلات العملية والقانونية في التشريع الكويتي. بحيث يمكن للمشرع الاستفادة من نتائج البحث لتحسين تشريعاتهم، وتسليط الضوء على التحديات الموضوعية والإجرائية التي تطرأ نتيجة لتلك الجرائم المتقدمة. كما يعتبر البحث مهم لكافة القانونين المعنيين سواء من رجال القضاء أو الباحثين المعنيين بهذا الشأن، وتوفير أساس لإجراء دراسات متقدمة في مجال تكنولوجيا المعلومات.

إشكالية البحث:

التقدم التكنولوجي في أساليب ارتكاب الجرائم، خاصةً عبر شبكة الإنترنت والحاسوب، يستلزم من الجهات المختصة التعامل مع أشكال جديدة من الأدلة في

ميدان الإثبات الجنائي. ومن ثم تكمن إشكالية البحث في التساؤل حول كيفية تقديم دليل رقمي إلكتروني فعّال ومعترف به أمام القاضي الجزائي. وتظهر مشكلة أخرى متعلقة بكفاءة القواعد التقليدية في التشريع الجزائي الكويتي لمواجهة التحديات المنبثقة عن الجرائم الإلكترونية، وذلك نتيجة القصور التشريعي في التشريع الجزائي. وليس هذا فقط، بل هناك مشكلة تتعلق بطبيعة المشكلات الموضوعية والإجرائية التي تثيرها هذا النوع من الجرائم ومدى كفاية معالجتها من قبل المشرع الكويتي، في ظل قوانين مكافحة جرائم تقنية المعلومات التي تفتقر إلى التعديل اللازم، والذي لم يسعفنا هذا البحث المتواضع لتناولها.

منهجية البحث:

يعتمد هذا البحث على المنهج التحليلي والوصفي المقارن، حيث يتم إدراج النصوص ذات الصلة بموضوع البحث في التشريع الكويتي، ومن ثم تحليلها ومقارنتها بالأنظمة المختلفة. يهدف ذلك إلى الوصول إلى نتائج وتوصيات تكشف عن نقاط الضعف في التشريع الكويتي في مواجهة التحديات والمشكلات المتعلقة بجرائم تقنية المعلومات.

خطة البحث:

قسمنا بحثنا إلى مبحثين رئيسيين. **في المبحث الأول**، تناولنا أهم الأحكام العامة المتعلقة بالجرائم الإلكترونية. **أما المبحث الثاني**، فقد ألقينا الضوء على أهم

الإشكاليات الموضوعية والإجرائية المتعلقة بقانون مكافحة جرائم تقنية المعلومات الكويتي رقم ٦٣ لسنة ٢٠١٥ وسُبل مواجهة تلك الإشكاليات المتعلقة بالجرائم الإلكترونية.

المبحث الأول: الأحكام العامة للمواجهة الجزائية للجرائم الإلكترونية.

المطلب الأول: ماهية الجرائم الإلكترونية

المطلب الثاني :أركان الجرائم الإلكترونية

المبحث الثاني: الإشكاليات الموضوعية والإجرائية للجرائم الإلكترونية وسُبل مواجهتها

المطب الأول: الإشكاليات الموضوعية والإجرائية للجرائم الإلكترونية

المطلب الثاني: سُبل مواجهة إشكاليات الملاحقة الجزائية للجرائم الإلكترونية

المبحث الأول

الأحكام العامة للمواجهة الجزائية للجرائم الإلكترونية

تمهيد وتقسيم:

تباينت مواقف الدول المختلفة في التعامل مع الجرائم الإلكترونية، فبينما توجد في بعض الدول نصوص قانونية قابلة للتطبيق على تلك الجرائم، نجد أن دولًا أخرى لا تتعامل تشريعاتها مع مثل هذه الجرائم، ويرجع ذلك بشكل أساسي إلى اختلاف تجارب تلك الدول مع الجرائم الإلكترونية، ويمكن بشكل عام التمييز بين اتجاهين رئيسيين في هذا الشأن:

أما الاتجاه الأول: ينظر هذا الاتجاه إلى الجرائم الإلكترونية على أنها جرائم تقليدية لا تتميز بخصائص تميزها عن غيرها من الجرائم بحيث تتطلب نصوصًا جديدة وقوانين جديدة لمواجهتها[1]، بحيث يمكن تطبيق النصوص القانونية التقليدية وتطويعها للتعامل مع الجرائم الإلكترونية.

أما الاتجاه الثاني: ينظر هذا الاتجاه إلى الجرائم الإلكترونية على أنها تتمتع

(١) نائلة عادل قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي، بيروت، ٢٠٠٥م، ص٤٠٦، وما بعدها، انظر أيضًا: ناصرمحمد البقمي، فاعلية التشريعات العقابية في مكافحة الجرائم المعلوماتية، مجلة البحوث الأمنية، المجلد ١٧، العدد٤، أغسطس ٢٠٠٨، ص١٢١، وما بعدها

بصفات تميزها عن غيرها من الجرائم. ويرى أيضًا ضرورة إصدار قوانين جديدة تتعامل مع الجرائم الإلكترونية، أو تعديل نصوص القوانين التقليدية بحيث تستطيع التعامل مع هذا النوع من الجرائم المستحدثة، وقد قامت الدول التي اتبعت هذا الاتجاه وهي غالبية الدول الصناعية واتبعتها في ذلك بعض الدول العربية منها الكويت ومصر والمملكة العربية السعودية والإمارات العربية المتحدة وغيرها من الدول بإصدار قوانين خاصة تعنى بجميع الأفعال التي ترتكب من خلال النظام المعلوماتي، أو التي تقع عليه، لمواجهة تلك الجرائم والحد من ارتكابها، كما قامت دول أخرى بتعديل قوانينها أو الإضافة إليها لذات الغرض[1].

وأيًا كان الاتجاه الذي تتبعه دول العالم فإن المواجهة الجزائية تطلب تجريم سوء استخدام أدوات تقنية المعلومات وشبكة الإنترنت، ولابد من أن تكون القوانين المتعلقة بمكافحة الجرائم الإلكترونية على قدر من التناسق، بحيث تمكن تلك الدول من التنسيق والتعاون فيما بينها في مكافحة هذا النوع من الجرائم المستحدثة التي تتطلب قدرًا كبيرًا من التعاون بين الدول للتعامل معها، فلابد أن تنص قوانين

(١) سليمان أحمد فضل، المواجهة التشريعية والأمنة للجرائم الناشئة عن استخدام المعلومات الدولية (الإنترنت) دار النهضة العربية، القاهرة ٢٠٠٧م، ص٤٢١، وما بعدها. انظر: أيضًا ناصر البقمي، المرجع السابق، ص١٢٠ وما بعدها.

دول العالم كافة على جميع الأفعال المجرمة فيما يتعلق بالجرائم الإلكترونية بحيث لا تستثني أيًا منها، وأن تقوم بتسليم الأدلة والمجرمين للدول المجني عليها أو محاكمتهم بنفسها حتى لا يفلت المجرم من العقاب تحت ذريعة عدم النص على الفعل في النصوص القانونية، أو عدم إمكانية تسليمه للدولة الطالبة في حالة عدم محاكمته في الدولة التي يتواجد فيها[١].

وقد سار المشرع الكويتي في هذا السياق وفقًا للتشريعات العقابية الأخرى المتعلقة بمكافحة الجرائم الإلكترونية، وتشمل هذه التشريعات مجموعة من القوانين، بعضها يعتبر تقليديًا وبعضها الآخر يعتبر مستحدثًا [٢].

وسنحاول في هذا المبحث التعرف على الأحكام العامة للمواجهة الجزائية للجرائم الإلكترونية والوقف على موقف المشرع الكويتي من قانون مكافحة جرائم

(1) Doon paker, fighting computer crime John wiley publishing U. K. 1998, at 241.Gina Angelis, Cyber Crmes, Chelsea house publishers, New York 2000, At 139

(٢) واجه المشرع الكويتي جرائم تقنية المعلومات من خلال قوانين موجودة ضمن المدونة الجزائية في التشريع الكويتي كقانون إساءة استعمال أجهزة الاتصالات الهاتفية وأجهزة التنصت وتعديلاته الصادر سنة ٢٠٠١ وقانون المطبوعات والنشر الصادر سنة ٢٠٠٦ وقانون الاعلام المرئي والمسموع الصادر ٢٠٠٧، ثم أصدر مؤخرا قوانين مستحدثة تدعم تلك القوانين وهي: قانون التعاملات الإلكترونية الصادر سنة ٢٠١٤ ، وقانون إنشاء هيئة تنظيم الاتصالات الصادر سنة ٢٠١٤، وقانون مكافحة جرائم تقنية المعلومات الصادر سنة ٢٠١٥ ، وقانون الإعلام الإلكتروني الصادر سنة ٢٠١٦.

تقنية المعلومات الكويتي رقم ٦٣ لسنة ٢٠١٥ منها، وذلك على التفصيل التالي:

المطلب الأول
ماهية الجرائم الإلكترونية

ما زال الفقه يسعى إلى تحديد مصطلح ومفهوم يتناسبان مع طبيعة الجرائم المرتبطة بتقنية المعلومات، فبينما هناك ألفاظ استخدمها للتعبير عن تلك الجرائم، مثل الجرائم الإلكترونية، والجرائم المعلوماتية، والجريمة السيبرانية، نجد بالنسبة للمفهوم تعددًا في التعاريف وتباين، حيث تكون بعض التعاريف ضيقة أحيانًا وتتسع تارة أخرى. ويرجع هذا التعدد لطبيعة تلك الجرائم التي ارتبطت بتطور التقنية، بدءًا من ظهور الحاسوب الآلي، ومن ثم تباينت هذه المصطلحات والتسميات مع تطوير شبكة الإنترنت [1]، وهذا الاختلاف للأسف يمثل إشكالية ولا يزال قائما حتى يومنا هذا، وسنحاول في هذا المطلب إلقاء الضوء على تحديد مفهوم الجرائم الإلكترونية

(١) د. علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة دراسة مقارنة، ط١، مكتبة زين الحقوقية، بيروت، ٢٠١٣، ص ٧٥ وما بعدها أسامة أحمد المناعسة وجلال محمد الزعبي جرائم ، تقنية نظم المعلومات الإلكترونية : دراسة مقارنة، ط٢، دار الثقافة للنشر، عمان، الأردن، ٢٠١٤، ص ٦٦ وما بعدها. وانظر في الفقه المقارن :

Johannes Xingan Li, Cyber Crime and Legal Countermeasures: A Historical Analysis, International Journal of Criminal Justice Sciences (IJCJS), Official Journal of the South Asian Society of Criminology and Victimology (SASCV), July-December 2017, Vol. 12 (2), p. 196; P. Sai Sheela and Nitika Sharma and Bhanu Bharadwaj, Cyber Crime Definition - challenges and the cost, International Journal of Computer & Mathematical Sciences (IJCMS), Volume 3, Issue 2 April 2014, p. 34; Paul Day, Cyber Attack - The truth about digital crime, cyber warfare and government snooping, Carlton Books, UK, 2014, p. 2.

وموقف التشريع الجزائي الكويتي من ذلك ، ثم بعد أن نبرز أهم الخصائص والصور التي تميز تلك النوعية من الجرائم لاسيما بعد ظهور تكنولوجيا الذكاء الاصطناعي كمطور لأداء أدوات تقنية المعلومات الذي ساعد على تفاقم أضرار وقوعها.

الفرع الأول
مفهوم الجرائم الإلكترونية

يتأسس تعريف الجريمة بصفة عامة على بيان عناصرها التي يحددها القانون، حيث إنه من دون النص على النموذج القانوني للجريمة لا يمكن المساءلة عنها وهو ما يستوجب التمييز بين مصطلحين وهما: الظاهرة الإجرامية والجريمة، فظاهرة الإجرام الإلكتروني هي الأفعال غير المشروعة المرتبطة بنظم الحاسبات، أما الجريمة الإلكترونية فقد اختلف الفقه الجنائي في تعريفها:

فمنهم من عرفها على أساس السلوك الإجرامي بأنها سلوك غير مشروع معاقب عليه قانونـًا، صادر عن إرادة إجرامية آثمة، محله معطيات الحاسب الآلي، فالسلوك يشمل الفعل والامتناع عن الفعل، وهذا السلوك غير المشروع معاقب عليه قانونـًا، لأن إسباغ الصفة الإجرامية لا يتحقق في مجال القانون الجنائي إلا بإرادة المشرع ومن خلال النص على ذلك حتى لو كان السلوك مخالفـًا للأخلاق، ومحل الجريمة

الإلكترونية هو دائماً معطيات الكمبيوتر بدلالتها الواسعة (بيانات مدخلة معلومات معالجة ومخزنة البرامج، المعلومات المستخرجة والمتبادلة بين النظم) [١].

ومنهم من عرفها على أساس وسيلة ارتكاب الجريمة، حيث عرفها الفقيه "توم فورستر [٢] بأنها فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية، واجتهد أخر بتعريفها أنها: مجموعة من الأنشطة الإيجابية والسلبية التي تكون فيها وسائل تقنية المعلومات أداة لارتكاب الأنشطة الإجرامية أو بيئة لها أو هدفا لها[٣].

كما عرفها الفقيه "تيدمان" بأنها كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب [٤].

وهناك من عرف الجريمة الإلكترونية على أساس سمات شخصية الجاني كتعريف الفقيه الأمريكي دون باركر الذي عرفها على أنها " الجرائم التي يستخدم فيها الجاني معرفته الخاصة بتكنولوجيا الكمبيوتر والفضاء الإلكتروني " [٥] .

---

(١) د. يونس خالد عرب مصطفى، صور الجرائم الإلكترونية واتجاهات تبويبها، ورقة عمل (٣) مقدمة لورشة عمل عن تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، مسقط، سلطنة عمان، المدة من ٢-٤ / ٤ / ٢٠٠٦م، ص ٧.

(2) Tom Forester and Perry Morrison, Computer Ethics: Cautionary Tales and (١٤) Ethical Dilemmas in Computing, 2nd ed., Cambridge, Massachusetts: MIT Press, 1994, p.29.

(٣) معاذ سليمان الملا، التعليق على أحكام القانون رقم ٦٣ لسنة ٢٠١٥ بشأن مكافحة جرائم تقنية المعلومات، ط ١ ، لجنة التأليف والتعريب مجلس النشر العلمي، جامعة الكويت، ٢٠١٩، ص ٤٢.

(4) Klaus Tiedeman, Fraude et autres délits d'affaires commis à l'aide d'ordinateurs électroniques, Rev. D.P.C. 1984, p.612.

(5) Donn B. Parker, Fighting Computer Crime: A New Framework for Protecting Information, 1998 Wiley computer Publishing, United States of America, p.72.

وإذا كانت تعريفات الجريمة عموماً تقوم على أساسين هما عناصر الجريمة «السلوك، ووصفه والنص القانوني على تجريم هذا السلوك وإيقاع العقوبة، فإن الجديد في مجال الجرائم الإلكترونية أو المعلوماتية هو إضافة عنصر ثالث يبرز محل الاعتداء في هذه الظاهرة المستحدثة متمثلاً في معطيات الحاسب الآلي [1].

وتحت وصف الجريمة الإلكترونية عرّف المشرع الكويتي هذه الجرائم في إطار المادة الأولى من القانون رقم ٦٣ لسنة ٢٠١٥ بشأن مكافحة جرائم تقنية المعلومات، بأنها: «كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية، أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون».

ومن وجهة نظر الباحث أن المشرع الكويتي قيد من نطاق هذه الجرائم حين اختزلها في دور الوسيلة وأسس تعريفه لها على أساس وسيلة ارتكاب الجريمة في حين أن هذه النوعية من الجرائم أوسع نطاقا بالنظر إلى الأدوار التي تؤدي إلى ارتكاب الجريمة، ونلمس هذا القصور في إيراد المشرع مصطلحات عديدة في المادة ذاتها تدخل ضمن نطاق هذه الجرائم.

(١) د. يونس خالد عرب مصطفى المرجع السابق، ص٦-٧.

ويجدر الإشارة إلى أن المشرع الكويتي للأسف لم يكن موفقاً في اختياره وعَنْونة هذا النوع من الجرائم في القانون رقم (٦٣) لسنة ٢٠١٥ بشأن مكافحة جرائم تقنية المعلومات ، فعبارة "تقنية المعلومات تدل على أنظمة تشغيل المعلومات ولا تشمل المعلومات، وذات الملاحظة توجه ايضاً إلى المشرع الجزائري الذي عنون هذه الجرائم بـ "الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات"، وكأن الأمر يتعلق بحماية الأنظمة فقط دون المعلومات أو المعلومات الموجودة داخلها، ورغم أن التسمية المعتمدة من طرف المشرّع السعودي أقرب للصواب وأشمل وهي "قانون مكافحة الجريمة المعلوماتية"، إلا أنه ومع ذلك نجد أيضاً أن مصطلح معلوماتية لا يشمل كل الجرائم التي تقع في عالم افتراضي، وإنما تقتصر على الجرائم الماسة بالمعلومات.

ومن هنا يكون الأصح تسمية هذا النوع من الجرائم بـ "الجرائم الإلكترونية"، وذلك لعدة أسباب أهمها:

١- ضرورة تسمية الجرائم بشكل يعكس الطابع الإلكتروني للجريمة، و تسمية "الجرائم الإلكترونية" تعكس بشكل أوسع الطبيعة الفعلية لهذه الجرائم لتشمل الأفعال التي تتعلق بالأنظمة والمعلومات.

٢- تسمية "الجرائم الإلكترونية" يمكن من خلالها تحسين التعريفات المتعلقة بالجرائم لتشمل تفاصيل أكثر حول الأفعال والمفاهيم المرتبطة بها، مما يجعلها

أكثر وضوحًا وشمولًا، ومن ثم توضيح بعض النصوص لضمان فهم دقيق للقوانين، وتحديدًا فيما يتعلق بالتصرفات المحظورة والعقوبات المتوقعة.

٣- أن تسمية "الجرائم الإلكترونية" يحقق تنسيق وانسجام القانون الكويتي مع التشريعات الإقليمية والدولية المتعلقة بمكافحة الجرائم الإلكترونية، لضمان تطابقه والتنسيق الفعّال.

٤- أن تسمية "الجرائم الإلكترونية" تحقق الحماية الشاملة، حيث يتعين على المشرع النظر في توسيع نطاق الحماية ليشمل المعلومات والأنظمة، مع التركيز على أمن السيبراني بشكل شامل.

بناءً على ذلك يمكن تكامل القانون ليعكس بشكل أفضل التحديات والتطورات في مجال مكافحة الجرائم الإلكترونية، ولذلك ومن وجهة نظر الباحث يمكن تعريف الجريمة الإلكترونية بأنها "كل سلوك غير مشروع محله المعلومات المعالجة آليًا أو نظم ووسائل إلكترونية تعتمد على تقنية المعلومات بطريقة مباشرة أو غير مباشرة، مما ينتج عنه إلحاق ضرر بالضحية أو حصول الجاني على مكاسب لا يستحقها ".

وفي هذا التعريف، يعتمد على عناصر الركن المادي للجريمة، والتي تتضمن السلوك غير المشروع الذي يشمل جميع صور السلوك الإجرامي المستحدثة في جرائم الاعتداء على المعلومات المعالجة آليًا، سواء كان ذلك بطريقة مباشرة أو غير مباشرة (كالفعل أو الامتناع). ويشمل أيضًا محل الجريمة، الذي يمثله كيانات معنوية

متمثلة في المعلومات المعالجة آليًا أو نظم ووسائل تقنية المعلومات، وأخذنا أيضًا في اعتبارنا النتيجة الإجرامية، والتي يمكن أن تكون إما إلحاق ضرر بالضحية، سواء كان هذا الضرر ماديًا أو أدبيًا، أو حتى حصول الجاني على فوائد أو مكاسب لا يستحقها بغض النظر عن نوعها. وتشمل النتيجة أيضًا قيام علاقة السببية بين السلوك والنتيجة، مع توافر الركن المعنوي للقائم بارتكاب الجريمة، ومن ثم سيوفر هذا التعريف إطاراً شاملاً يشمل مختلف أوجه الجرائم الإلكترونية ويظهر التفاعل المعقد بين تكنولوجيا المعلومات والأنشطة الإجرامية، وهذا ما يتوافق مع طبيعة هذه الجرائم وخصوصيتها.

الفرع الثاني
خصائص الجريمة الإلكترونية

تتميز الجريمة الإلكترونية بعدة خصائص تميزها عن الجريمة التقليدية ومن أهمها:

١- الجريمة الإلكترونية عابرة للحدود ذات طابع عالمي:

تعد هذه الجرائم صورة صادقة من صور العولمة وذلك باعتبار العالم قرية مصغرة، حيث يمكن ارتكاب الجرائم عن بعد، وقد يتعدد المكان إلى أكثر من دولة بل أكثر من قارة وهذا من شأنه أن يطرح إشكالية القانون الواجب التطبيق -التي

سنتعرض لها لاحقـًا–[١].

ولذلك باتت الجريمة الإلكترونية جريمة عالمية، الأمر الذي يستوجب معه السعي نحو زيادة التعاون الدولي في المجالين الاتفاقي والقضائي وهذا في سبيل تطويق هذه الظاهرة الإجرامية الخطيرة[٢].

هذا الوضع يعرضنا للعديد من التحديات القانونية، حيث إن التحدي الرئيسي الذي يواجه مجتمع القانون الجنائي في مواجهة جرائم الإلكترونية يتمثل في تباين القوانين الجنائية بين الدول.

٢- الجريمة الإلكترونية مستحدثة وقابلة للتطوير المستمر:

فهذا النوع من الجرائم يتميز بقابليته للتطور المستمر، حيث اعتمد المجرمون على تكنولوجيا الذكاء الاصطناعي لتعزيز أنشطتهم الإجرامية. في الوقت الحاضر، لا نتحدث عن جريمة إلكترونية أو جريمة معلوماتية فقط، بل نشهد تطورًا تقنيًا يجعل تلك الأنشطة "ذكية" بفضل استخدام تكنولوجيا الذكاء الاصطناعي. هذا يعني أن

(١) فغالبا ما يكون لهذه الجرائم طابع عالمي، لأن كل الدول مرتبطة وفي حالة اتصال دائم، ولذلك فالجريمة الإلكترونية لا تعرف حدود وبذلك أصبح مسرح الجريمة الإلكترونية عالميا. عبد الله حسين على محمود، سرقة المعلومات المخزنة في الحاسب الآلي ، دار النهضة العربية، الإسكندرية، ٢٠٠٢، ص ٣٥١

(٢) ثروت جلال، شرح قانون العقوبات القسم العام، منشأة المعارف، الإسكندرية، ١٩٨٩، ص ١٠٤. مأمون محمد سلامة، شرح قانون العقوبات القسم العام ط ٠٣ دار النهضة العربية، الإسكندرية ٢٠٠٢ص٨٠

الآلة نفسها تسهم في تنفيذ الجريمة دون التدخل المباشر من قبل الإنسان، وتقوم بتنظيم النشاط الإجرامي وتنفيذه تحت شعار الآلة وليس البشر فحسب[١]؛ أي أن الآلة سترتكب نشاطًا إجراميًا دون أي تدخل من الإنسان ذاته[٢]، ولذلك يشير الخبراء في مجال الذكاء الاصطناعي إلى أنه على الرغم من إمكانية استخدام هذه التكنولوجيا لتقديم حلاً فعّالًا، إلا أن هناك من يسيء استخدامها في ارتكاب جرائم مختلفة. يمكن وصف الوضع، وفقًا لبعض الأفراد، بأنه سباق بين الخير والشر للفوز في معركة التطور التكنولوجي [٣].

٣- صعوبة اثبات الجريمة الإلكترونية:

حيث يصعب العثور على أثر مادي للجريمة الإلكترونية، ولعل السبب في ذلك يعود الى الاستخدام الجاني وسائل فنية تقنية معقدة في كثير من الأحيان، كما يتمثل

(1)Thomas C. King and Nikita Aggarwal and Maria rosaria Taddeo and Luciano Floridi, Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions, Science and Engineering Ethics, Springer, 2020, p. 90. DOI: 10.1007/s11948- 018-00081-0

(٢) أثار فقهاء القانون الجنائي منذ زمن ليس ببعيد مشكلة المسؤولية الجزائية إذا ارتكب النشاط الإجرامي بواسطة الآلة .

للمزيد من التفاصيل حول هذا الموضوع راجع:

Jerry Kaplan, Op. Cit., p.105; Gabriel Hallevy, Liability for Crimes Involving Artificial Intelligence Systems, Springer, USA, 2015, p. 1.

(3)Thomas C. King and Nikita Aggarwal and Maria rosaria Taddeo and Luciano Floridi, Op. Cit., p. 91. See also: Roman Zhidkov, The Future Impact of AI on Cyber Crime, 14 Feb 2020.
https://becominghuman.ai/the-future-impact-of-ai-on-cyber-crime-f9659cf354a6

سلوك المكون للركن المادي فيها عمل سريع قد لا يستغرق أكثر من بضع ثوان[١].

٤- الجرائم الإلكترونية بانها اقل عنفاً:

تتسم الجرائم الإلكترونية بأنها اقل عنفا من نظيرتها التقليدية، حيث لا تحتاج الى مجهود عضلي وتعتمد على الدراية الذهنية والتفكير العلمي المدروس القائم على معرفة بتقنيات الحاسب الالي[٢] لذا يطلق عليها جرائم ناعمة[٣].

لذلك، يمكننا القول إن التقدم العلمي والتكنولوجي في ظل العولمة قد تجاوز قدرات الدولة الرقابية، وأدى إلى ضعف قدرتها على تطبيق قوانينها بطريقة فعّالة، مما يشكل تهديدًا لأمنها وسلامتها[٤]. وبناءً على هذا الاستنتاج، سارعت الدول إلى إقرار تشريعات خاصة تستهدف الوقاية ومكافحة هذه الجريمة المتقدمة [٥]. كما

---

(١) د. هشام رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني، بحث منشور في مجلة الأمن والقاون، والقانون، العدد ٢، كلية الشرطة دبي، ١٩٩٩م ، ص٨٢.

(٢) أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلى والانترنت، دراسة تحليلية مقارنة، ط١، دار وائل للنشر، عمان، ٢٠٠١م ، ص١٠٧.

(٣) د. عبد الستار الكبيسي المسؤولية الجنائية الناشئة عن استعمال الحاسوب، سلسلة المائدة الحرة من ندوة القانون والحاسوب بيت الحكمة، ١٩٩٩م.

(٤) نبيلة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي ، الإسكندرية، ٢٠٠٦، ص٣٥

(٥) حيث أن وقوع الجريمة الإلكترونية غالباً ما تقع أثناء المعالجة الآلية للبيانات وهذه الخاصية الفعلية والضرورية

قامت هذه الدول بالمشاركة في عقد اتفاقيات دولية تهدف إلى التعاون في مجال مكافحة هذه الجرائم وتعزيز أمن السيبراني على المستوى العالمي.

إلا أنه، بالرغم من أهمية تقدم التشريعات والتكنولوجيا في مكافحة هذه الجرائم المستحدثة، إلا أن طبيعة وخصائص هذه الجرائم تثير العديد من الإشكاليات القانونية، خاصة في مجالات الاختصاص القضائي وتطبيق القوانين. لذا، يهدف هذا البحث إلى إيجاد رؤية توافقية تعمل على الحد من انتشار هذه الجرائم. يتعين تحقيق هذا الهدف من خلال متابعة وملاحقة الجناة ومنعهم من التهرب من العقوبات؛ وفي ذات الوقت يجب حماية حقوق الأفراد وضمان حرياتهم الأساسية، بما في ذلك سرية المعلومات وحرية الاتصال.

لارتكاب الجريمة الإلكترونية تظهر بشكل واضح في جميع مراحل ارتكاب الجريمة، سواء أثناء إدخال البيانات، أو أثناء معالجتها، أو خروج المعلومات، وحتى بعد تخزينها. الأمر الذي يُعتبر معه اعتماد هذه الخاصية في تشريعات الدول بات ضروريًا لفهم وتعريف الجريمة الإلكترونية، ولذلك استخدم المشرع الفرنسي على سبيل المثال هذه الفكرة في تعديل قانون العقوبات لسنة ١٩٩٤. ويمكن الاستفادة من هذه النهج عند وضع قوانين خاصة تتعامل مع الجرائم الإلكترونية في سياق معين. نائلة عادل، محمد فريد، جرائم الحاسوب والجريمة الاقتصادية، منشورات الحلبي الحقوقية، لبنان، ٢٠٠٥م، ص٥٥

الفرع الثالث
صور الإجرام الإلكتروني

الجريمة ليست ظاهرة جديدة في التاريخ، بل هي واقع قديم، لكن الجريمة الحديثة عبر الإنترنت تمثل تهديداً أكبر بفضل تطور التكنولوجيا، خاصةً الحواسيب والهواتف المحمولة، أصبحت الجرائم الإلكترونية أكثر خطورة وتطورًا. تشمل هذه الجرائم استخدام الإنترنت لارتكاب أفعال إجرامية بشكل سريع ومتقدم، مما يشكل تهديداً كبيرًا على مستوى الفرد والمجتمع. وليس هذا وحسب، بل يمتد تأثير هذا النوع من الجرائم إلى أمان واستقرار الدول، من هنا ركز مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعالجة المجرمين الذي انعقد في فيينا للفترة ١٠ – ١٧ نيسان ٢٠٠٠ على مواجهة الجرائم المتصلة بشبكة الحواسيب، ورأى المؤتمر أن الجرائم الحاسوبية تقسم إلى نوعين:

النوع الأول: الجرائم الحاسوبية بالمعنى الضيق، وهي أي سلوك غير مشروع يوجه بواسطة عمليات إلكترونية تستهدف أمن نظم الحواسيب والبيانات التي تعالجها تلك النظم.

النوع الثاني: الجرائم المتصلة بالحواسيب (بالمعنى الأوسع) وهي أي سلوك غير

مشروع يرتكب بواسطة نظام أو شبكة حواسيب بما في ذلك جرائم حيازة المعلومات أو عرضها وتوزيعها بصورة غير مشروعة [١].

وهناك عدة صور محتملة لجرائم الحاسوب تتمثل في [٢]:

١. أن النفاذ غير المشروع وغير المرخص به الى نظم وشبكات الحاسوب أو ما تسمى بالقرصنة.
٢. إلحاق الضرر ببيانات وبرامج الحاسوب أو إفسادها.
٣. ج. جريمة نشر الفايروسات لغرض إتلاف محتويات الحاسوب.
٤. د. التجسس بواسطة الحواسيب أي الحصول على سر تجاري وإفشائه دون إذن أو مبرر قانوني.
٥. جرائم الغش والتزوير بواسطة الحاسوب.
٦. سرقة وقت الحاسوب من خلال الدخول غير المصرح به أو استخدام الكومبيوتر لأغراض شخصية.
٧. جريمة استخدام بيانات شخصية غير صحيحة.

---

(١) د. أكرم عبد الرزاق المشهداني، "الجرائم التكنولوجية"، بغداد، مطبعة الوفاق، ٢٠٠٥ م.

(٢) ذياب البدائنة، التقنية والإجرام المنظم بحث مقدم إلى الندوة العلمية ٤٧ (الجريمة المنظمة وأساليب مواجهتها في الوطن العربي) جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٠م.

٨. جرائم الاعتداء على الحريات الشخصية وحقوق الملكية الأدبية للبرمجيات (النسخ غير المشروع). ويقدر حجم الخسائر السنوية للشركات المنتجة للبرامج الكمبيوترية من جراء أعمال القرصنة بنحو ٣٠٠ مليون دولار سنوياً.

الفرع الرابع
حجم الخسائر الناتجة عن الإجرام الإلكتروني عالمياً

تعد الجرائم الإلكترونية من أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل أخطارا جسيمة في ظل العولمة، حيث أن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة، بحيث يتجاوز هذا التقدم بقدراته وإمكاناته أجهزة الدولة الرقابية، بل أنه أضعف من قدراتها في تطبيق قوانينها، بالشكل الذي أصبح يهدد أمنها وأمن مواطنيها [1]

حيث صارت الجريمة الإلكترونية بمختلف صورها وإشكالها خطرا يهدد الأمن في مختلف دول العالم، وتأتي خطورتها بعد جرائم الاتجار بالمخدرات وبالأسلحة وبالبشر، بل إن تلك الجرائم تتعاظم خطورتها باستخدام التكنولوجيا الاتصالية وسيلة لتنفيذها أو تسهيل وقوعها، فتقنيات المعلومات صارت اليوم أدوات بيد

(١) الأمم المتحدة، مجموعة وثائق وأعمال مؤتمر الأمم المتحدة العاشر لمنع الجريمة والعدالة الجنائية فبينا ٢٠٠٠م.

مجرمي الاتجار بالمخدرات والأسلحة والأشخاص والجرائم الاقتصادية وغيرها، حيث قدرت الخسائر المترتبة على عمليات الاحتيال المالي على المستوى العالمي بنحو ٣.٥ تريليون دولار سنوياً[١]، وتعادل نحو ٥ في المائة من دخل الاقتصاد العالمي، المقدر بنحو ٧٠ تريليون دولار، الأمر الذي يفسر الجهود المتنامية لمكافحة أساليب الاحتيال المالي وتضافر جهود المجتمع الدولي لعرقلة تفشيها في أسواق العالم، في ظل التطور المتسارع الذي تشهده التقنيات المصرفية والنمو

(١) يُطلق مصطلح "احتيال الإنترنت" على أي نشاط يستخدم خدمات الإنترنت، مثل الدردشة والبريد الإلكتروني والمنتديات ومواقع الويب، لتوجيه خدع وحيل نحو ضحايا محتملين عبر الشبكة. يهدف هذا الاحتيال غالبًا إلى خداع المستخدمين وسلب أموالهم، سواء عبر سرقة معلومات بطاقات الائتمان أو إقناعهم بإرسال تحويلات مالية أو شيكات، أو الكشف عن معلومات شخصية بهدف التجسس أو انتحال الهوية أو الوصول إلى معلومات حساباتهم الحساسة، ومن ثم فالاحتيال الإلكتروني أو الاحتيال عبر الأنترنت هو طريقة لسرقة الهوية بالاحتيال عن طريق الأنترنت بالكشف عن معلومات شخصية أو مالية. يستخدم المحتالون مواقع أنترنت مزيفة، أو رسائل مضللة عن طريق البريد الإلكتروني، وذلك بتقليد العلامات التجارية والشركات الموثوق بها من أجل سرقة معلومات شخصية مثل: أسماء المستخدمين، وكلمات السر وأرقام بطاقات الائتمان ومعلومات الفواتير. زياد سويدان، انتحال الهوية الرقمية قاضي التحقيق بالمحكمة الابتدائية بتونس ٢٠١٠. وقد انتشرت في الآونة الأخيرة جرائم النصب والاحتيال المالي الإلكتروني على شبكة الأنترنت من خلال رسائل البريد الإلكتروني التي ترد للمتعاملين مع الشبكة وهذا الأسلوب يعرف باسم التصيد المالي phishing. أسامة أحمد المناعسة، جلال الزغبي صايل الهواوشة، "جرائم الحاسب الآلي والأنترنيت-دراسة تحليلية مقارنة، دار وائل للنشر عمان الأردن ٢٠٠١م.

اللافت في معدل الاعتماد على الشبكة العنكبوتية من قبل الأفراد والمؤسسات في تنفيذ العمليات المصرفية والمالية[١].

غير أن اندفاع مستخدمي أدوات تقنية المعلومات نحو شراء مقتضياتهم عبر شبكة الإنترنت ومنصات شبكات التواصل الاجتماعي يتزايد، مما يستلزم إدخال البيانات الشخصية للمستخدمين، بما في ذلك أرقام بطاقاتهم الائتمانية لإتمام العمليات الشرائية. كما يشهد القطاع العام والخاص في بعض البلدان تنامي بيئة الأعمال والمؤتمرات عن بُعد، حيث يعتمد المشاركون على التراسل الإلكتروني كتطبيق لفكرة التباعد الاجتماعي[٢]، وهذا بطبيعة الحال أسهم في تعريضهم لهجمات إلكترونية مختلفة[٣]، كالاحتيال أو التصيد الإلكتروني وهجمات البرامج الخبيثة

(١) ويشير متتبعو الأخبار ووسائل الإعلام إلى استمرار حوادث الاحتيال المالي، وهي مؤشر على استمرار ضعف الوعي المالي وثقافة الاستثمار، وقلة الوعي القانوني لدى فئة من المدخرين. يظهر أن المحتالين يطوّرون أساليبهم ووسائلهم، ويستخدمون التكنولوجيا الحديثة لاستهداف ضحاياهم. الطمع يظل الدافع الرئيسي وراء نجاح عمليات الاحتيال، رغم التحذيرات المتكررة من الجهات الأمنية والاستثمارية. تعمل الجهات الأمنية على نشر تفاصيل عمليات الاحتيال والأساليب المستخدمة، بهدف توعية المواطنين وحثهم على تجنب الوقوع في فخ المحتالين. راجع في ذلك: الغش التجاري في المجتمع الإلكتروني ورقة عمل مقدمة إلى الندوة الرابعة لمكافحة الغش التجاري والتقليد في دول مجلس التعاون الخليجي، من الغرفة التجارية الصناعية بالرياض خلال الفترة ٢٠١٨ سبتمبر عام ٢٠١٢م.

(2)Chi Tran, Recommendations for Ordinary Users from Mitigating Phishing and Cybercrime Risks During COVID-19 Pandemic, Security Research Blog, Writeups , P1.

(٣)بينت آيكان» في تقرير لها أنه في شهر مارس ٢٠٢٠ فقط ، تم تسجيل ١٠٠ ألف موقع الكتروني جديد على الأقل

واختراقات الأنظمة وغيرها سيما وأن شبكة الإنترنت الخفي تعتبر نافذة حقيقية لتلك الاعتداءات[1].

وقد حذرت هيئة شبكة الإنترنت للأسماء المعروفة بـ "الآيكان" من انتشار هذه الأنشطة، خاصة أثناء فترة تفشي جائحة كرونا ، حيث تم رصد ما يقرب من ١٠٠,٠٠٠موقع إلكتروني تحت أسماء نطاقات مرتبطة بكلمات تتعلق بجائحة كورونا[2].

ورغم أن حجم عمليات الاحتيال المالي على الصعيد الدولي لا تتعدى ١ ٪ من إجمالي العمليات المالية الكلية المنفذة، إلا أن تلك النسبة تبقى مصدر قلق بالنظر

تحت أسماء نطاقات تشمل كلمات مثل «كوفيد و كورونا، و فيروس. راجع تقرير-يحذر – تنامي – الاحتيال – الالكتروني-زمن-كورونا **على الرابط الإلكتروني التالي**:

www.skynewsarabia.com/varieties/1334977-

(١)الإنترنت الخفي إما أن يكون عميقا وإما أن يكون أعمق، وقد أطلق عليه وصف المظلم، وشبكة الإنترنت الخفي تمثل ما نسبته ٩٠ إلى ٩٥٪، بينما الشبكة العامة أو الظاهرة التي نستخدمها تشكل الجزء المتبقي أي ٥ إلى ١٠٪ فأين نحن من هذا العالم وكيف نواجه الأنشطة الإجرامية الخفية، نديم منصوري، مرجع سابق، ص٥٢. وانظر أيضا : وليد بن صالح، الإنترنت المظلم والعملات الافتراضية ، مجلة كلية القانون الكويتية العالمية، ملحق خاص ، أبحاث المؤتمر السنوي الدولي الخامس (الجزء الثاني)، العدد ٣ أكتوبر ٢٠١٨، ص ٣٨٩ وما بعدها. يشير خبراء تقنيون إلى أن هذه الشبكة ساهمت في الأنشطة الإجرامية خلال فترة تفشي جائحة كورونا، انظر هذا التقرير :

IntSights Defend forward, The Cyber Threat Impact of COVID-19 to Global Business, p. 2.

(٢) للاطلاع على مزيد من طبيعة وأنواع الهجمات الإلكترونية منذ بداية تفشي جائحة كورونا وتطورات هذه الهجمات، راجع الرابط الإلكتروني التالي:

https://cyware.com/blog/live-updates-covid-19-cybersecurity-alerts-b313

إلى حجم الخسائر المالية الجسيمة المترتبة على حقوق ومدخرات عملاء المصارف في العالم، وهو ما يدعو إلى ضرورة مواصلة الجهود الكفيلة بالتصدي لأساليب التحايل المالي التي لا يقتصر وجودها على العمليات المصرفية الخاصة بالمصارف فقط، وإنما يتعدى نطاقها ليشمل مختلف مجتمعات الأعمال ومنظماتها الخاصة والعامة والفردية حتى الأسرة كذلك لارتباطها بعنصر "المال والمادة" وضعف العنصر البشري أمامه [1].

وقد أعلنت شركة ماكافي McAfee الشركة العالمية الأميركية المتخصصة في تقنيات حماية وأمن المعلومات عن تزايد وانتشار هجمات الجرائم الإلكترونية على مستوى العالم خلال الربع الثالث من العام الجاري، وتضاعف الهجمات الضارة على الأجهزة المحمولة مقارنة بالربع الثاني من العام، وتزايد معدلات عمليات الاحتيال المالي الإلكتروني عالميـًا، وذلك وفق أحدث نتائج تقرير التهديدات للربع الثالث الذي أصدرته الشركة. وأوضحت الشركة بأن التقنيات المستخدمة في الجرائم الإلكترونية شهدت تطوراً وتحديثـًا متواصلاً من مجرمي الإنترنت الذين يسعون دومـًا لاستغلال واكتشاف الثغرات الإلكترونية في الأنظمة العالمية، مشيرة إلى

(١) جريدة الإتحاد الإماراتية ٣/ ١٢/ ٢٠١٣.

تجاوز معدلات الاختراق الأمني القواعد البيانات في عام ٢٠١٣ الأرقام المسجلة في عام ٢٠١٢، حيث قام مطورو قواعد البيانات بالكشف والتصحيح السري لما يقارب ١٠٠ ثغرة أمنية في قواعد البيانات هذا العام. وكشف أن مختبرات "مكافي" رصدت حاليًا ١٠٠٫٠٠٠ نموذج لبرامج ضارة جديدة، وهو ما يمثل متوسط عدد نماذج البرامج الضارة الجديدة لكل يوم حيث تضاعف عدد البرامج الضارة المتوقعة منذ شهر يناير، مما أثر على البنية التحتية للائتمان العالمي [1].

من ناحية أخرى، كشف تقرير الرقمية العالمية لشهر أبريل ٢٠٢٠م أن عدد مستخدمي الإنترنت في العالم وصل إلى ٤.٥٧ مليار مستخدم، بنمو يبلغ ٧٪ عن أبريل ٢٠١٩. وأظهر التقرير زيادة بنسبة أكثر من ٨٪ في عدد مستخدمي منصات شبكات التواصل الاجتماعي، حيث وصل عددهم إلى ٣.٨١ مليار خلال الفترة نفسها. كما ارتفع عدد مستخدمي الهواتف المحمولة إلى ٥.١٦ مليار مستخدم، بزيادة ١٢٨ مليون مستخدم منذ أبريل ٢٠١٩، وهو ما يمثل ثلثي إجمالي سكان العالم تقريبًا. وشهدت استخدامات البريد الإلكتروني زيادة بنسبة ٣٠٪ منذ مارس ٢٠٢٠. أظهر التقرير أيضًا أن أكثر من ثلثي مستخدمي الإنترنت الذين تتراوح

(١) د. أكرم المشهداني، الجرائم التكنولوجية، مصدر سابق، ٥٣.

أعمارهم بين ١٦ و ٦٤ عامًا يخصصون وقتًا لألعاب الفيديو، حيث تم تحميل أكثر من ١٣ مليار لعبة في الأشهر الثلاثة الأولى من عام ٢٠٢٠، بإجمالي نفقات قدره ١٧ مليار دولار. ولاحظ التقرير زيادة في معدل التسوق عبر الإنترنت، حيث أظهر أن ثلثي مستخدمي الإنترنت يهتمون أكثر بشراء السلع الاستهلاكية والغذائية من خلال مواقع السوبر ماركت، وسجل معدل نمو في عدد زيارات هذه المواقع بنسبة ٢٥١٪ من ٨ إلى ١٥ أبريل ٢٠٢٠.[١].

وقد أظهرت التقارير في دولة الكويت أن عدد مستخدمي شبكة الإنترنت فيها قد بلغ ٤.٢٠٠ مليون مستخدم في تلك الفترة. وقد ارتفع بمقدار ٢٤ ألف مستخدم بين ٢٠١٩ و ٢٠٢٠، وبلغ معدل انتشار شبكة الإنترنت ٩٩٪ وازداد عدد معدل مستخدمي شبكات التواصل الاجتماعي نحو ١٥٥ ألف مستخدم بين ٢٠١٩ – ٢٠٢٠ ومعدل انتشار شبكات التواصل الاجتماعي ٩٩٪ . وقد بلغ عدد مستخدمي

(١)اعتمد التقرير على محاور أساسية في الربع الأول من عام ٢٠٢٠، وهذه المحاور كان أولها يشير إلى القفزات الهائلة والكبيرة في الأنشطة الرقمية، وجاء المحور الثاني مستعرضا نتائج استخدام شبكات التواصل الاجتماعي، فيما خصص المحور الثالث لبيان النتائج المتعلقة باستخدام تطبيقات التجارة الإلكترونية، وجاء الرابع مستعرضـًا نتائج الوقت الذي يقضيه المستخدمون في الألعاب التفاعلية، وأما الخامس والأخير فكان مخصصا لعرض بعض الفرص غير المتوقعة للمعلنين الرقميين. راجع الموقع الإلكتروني على الرابط التالي :
https://datareportal.com/reports/digital-2020-april-global-statshot

الهواتف المحمولة في الكويت ٧.٣٨ مليون مستخدم في يناير ٢٠٢٠، بزيادة مقدارها ٣١٧ ألفا بين ٢٠١٩ و ٢٠٢٠ ما يعادل ١٧٤٪ من إجمالي عدد السكان[١].

المطلب الثاني
أركان الجرائم الإلكترونية
الفرع الأول
الركن المادي للجرائم الإلكترونية

يقصد بالركن المادي للجريمة السلوك الإنساني الذي تترتب عليه نتيجة يعاقب عليها القانون الجنائي [٢]، ومن ثم فإن عناصر الركن المادي هي السلوك الإنساني والنتيجة وعلاقة السببية بينهما. ويتمثل الركن المادي في مجموعة العناصر المادية التي ينتج عنها الخطر أو تلحق الضرر بمصلحة يحميها القانون جنائيـًا، فلا جريمة دون ركن مادي حتى يكون إقامة الدليل عليها ميسوراً [٣].

يتطلب ارتكاب الجريمة الإلكترونية بالضرورة فهمـًا للمنطق التقني، حيث يكون ذلك ضروريًا للقيام بالأنشطة الجرمية عبر الإنترنت. يمكن أن يكون هذا المنطق التقني إيجابيًا، حيث يمثل الفهم الفعّال له جزءًا من الجريمة الإلكترونية، سواء كان

---

(١)للاطلاع راجع الرابط الإلكتروني التالي:

https://datareportal.com/reports/digital-2020-kuwait

(٢) د. محمود نجيب حسني، شرح قانون العقوبات القسم العام، ط / جامعة القاهرة، ١٩٧٨م، ص٢٧٩.

(٣) د. يسر أنور علي، شرح قانون العقوبات، النظريات العامة، ١٩٨٨م، ص ٢٧٦.

ذلك من خلال الدخول غير المشروع إلى أنظمة الحواسيب أو الاتصال بشبكات المعلومات، وعالج المشرع الكويتي صراحة هذا الجانب الفني للجريمة الإلكترونية، حيث يحظر بشكل صريح على أي شخص دخول جهاز حاسوب أو نظام معالجة إلكترونية للبيانات أو نظام إلكتروني مؤتمت أو شبكة معلوماتية بطريقة غير مشروعة. بذلك يعتبر المشرع الكويتي التورط في أنشطة جريمة إلكترونية أو استخدام الحاسوب المتصل بالإنترنت لارتكاب جرائم محددة يعكس القيمة الموحدة للشروع في تلك الجرائم(١).

حيث تنص المادة (٢) من القانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات الكويتي على أنه: "يعاقب بالحبس... كل من ارتكب دخولاً غير مشروع إلى جهاز حاسب آلي أو إلى نظامه أو إلى نظام معالجة إلكترونية للبيانات أو إلى نظام إلكتروني مؤتمت أو إلى شبكة معلوماتية " (٢).

(١) د. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيًا، دار الجامعة الجديدة للنشر، ١٩٧٧م، ص ٢٥-٢٦.

(٢) وهي المقابلة للمادة (٢) من المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ شأن مكافحة في جرائم تقنية المعلومات الإماراتي والتي تنص على أنه: "يعاقب بالحبس... كل من دخل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات من دون تصريح أو بتجاوز حدود التصريح أو بالبقاء فيه بصورة غير مشروعة ".

وقد تستخدم عبارات مثل "استخدام الحاسوب الآلي" أو "المعالجة الآلية للبيانات" أو "الدخول إلى موقع إلكتروني" أو "نظام معالجة إلكترونية" أو "شبكة معلوماتية"، وجميع هذه التعبيرات تعكس نشاطًا تقنيًا، حيث يتعلق الأمر بالاستفادة من الحواسيب والتكنولوجيا الإلكترونية لارتكاب الجرائم. لذلك، يعد وجود نشاط تقني أمرًا أساسيًا لإمكانية ارتكاب الجريمة المعلوماتية، وعدم وجود هذا النشاط يمكن أن يعتبر دفاعًا فعّالًا عند اتهام الفرد بارتكاب جريمة معلوماتية. في حالة عدم وجود نشاط تقني، يمكن أن يعتبر حكم المحكمة القاضي بارتكاب جريمة معلوماتية عيبًا في التسبيب، مما يستوجب نقضه أو تمييزه[1].

ففي الجرائم الإلكترونية، يكون النشاط التقني جزءًا حيويًا من ارتكاب الجريمة. يجب أن يكون الشخص الممارس للجريمة ملمًا بالتكنولوجيا والأنظمة الإلكترونية بما يكفي لتنفيذ فعله. على سبيل المثال، في جريمة اختراق نظام معلوماتي، يحتاج الفاعل إلى مهارات تقنية عالية لتخطي الحمايات والوصول إلى المعلومات بطريقة غير مشروعة. لذلك، يعتبر النشاط التقني والفهم العميق للأنظمة والتكنولوجيا جزءًا حاسمًا في ارتكاب جرائم الإلكترونية. يعكس هذا الفهم العميق قدرة الجاني على

(١) د. علاء محمود يسن حراز، الحماية الجنائية للمعلومات المعالجة آليـاً، دراسة مقارنة في القانون الوضعي والشريعة الإسلامية رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ص٢٠٢-٢٠٣.

التلاعب بالأنظمة الرقمية والاستفادة من الثغرات الأمنية، مما يبرز أهمية وجود تقنيات فعّالة لمكافحة هذه الجرائم وتأمين الأنظمة والبيانات[١].

والفعل الذي يقوم به مرتكب الجريمة الإلكترونية يجب أن يكون السبب الذي يؤدي إلى النتيجة، مما يشير إلى وجود علاقة سببية بين الفعل والنتيجة. وبناءً على ذلك، يتحقق شرط المسؤولية عندما يكون مرتكب الفعل مسؤولًا عن النتيجة ويكون هناك ارتباط سببي بينهما. [٢].

ولثبوت الركن المادي في الجرائم الإلكترونية، يجب بالضرورة إثبات وجود علاقة سببية بين النشاط المعلوماتي والنتيجة الإجرامية. ومن ثم يلزم أن يثبت بالضرورة قيام علاقة السببية بين النشاط المادي وبين النتيجة الإجرامية، فمثلاً لقيام جريمة انتهاك الحق في الخصوصية عبر الإنترنت يجب أن يكون هناك دخول على الإنترنت باستخدام حاسب آلي عامل واختراق الخوادم المختلفة في مسارها، ثم بعد ذلك التعدي على خصوصية موقع ما أو إعداد موقع ما، ثم بعد ذلك يبث عليه صوراً ذات خصوصية لأشخاص مشهورين [٣].

---

(١) د. محمد أمين الرومي، جرائم الكمبيوتر والإنترنت دار المطبوعات الجامعية، ٢٠٠٣م، ص١٨٢.

(٢) د. محمود نجيب حسني، المرجع السابق، ص٢٩٣.

(٣) د. علاء محمود يسن حراز، رسالة دكتوراه المرجع السابق، ص، ٢١.

والعنصر الثاني من عناصر الركن المادي هو النتيجة الإجرامية، وهي كل أثر للسلوك الإنساني يسفر عن تغيير في المحيط الخارجي [1]. وفي إطار بحث النتيجة في الجريمة الإلكترونية ينبغي التعرض لفكرة جرائم الضرر وجرائم الخطر والنتيجة المحتملة، فجرائم الضرر المعلوماتية هي التي يتحقق فيها هلاك المال أو الإنقاص منه أو التضحية بمصلحة إنسانية يحميها القانون، أما جرائم الخطر المعلوماتية فهي تلك الجرائم التي يكون الهدف فيها حماية المال من احتمال التعرض للخطر فهي جرائم وقائية [2]، ومن المشاكل التي تواجه تحديد الضرر أو الخطر كنتيجة إجرامية عبر الإنترنت تلك المتعلقة بجرائم العدوان الفيروسي، وفي هذا النوع من الجرائم يصعب تحديد المجني عليه [3].

ومن حيث النتيجة المحتملة وهي حالة إذا ما ترتب على النشاط الإجرامي أكثر

(١) د. محمد عمر مصطفى، النتيجة وعناصر الجريمة مجلة العلوم القانونية والاقتصادية، ع٢، س ٧ يوليو ١٩٦٥، كلية الحقوق جامعة عين شمس، ص ٣٢٤.

(٢) د. علي أحمد راشد القانون الجنائي، المدخل والنظرية العامة، ١٩٨٤م، ص ٢٥٩.

(٣) د. يونس خالد عرب مصطفى، تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، ورقة عمل مقدمة لورشة عمل عن تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، هيئة تنظيم الاتصالات، مسقط عمان -٢-٤ / ٤/ ٢٠٠٦، ص ٥.

من نتيجة لا يسعى الجاني إلا إلى صورة واحدة منها وهي التي يتوقعها ويريدها [١] وتنتشر فكرة النتيجة المحتملة في الجرائم الإلكترونية، ذلك أن النشاط التقني له منطق تفكيري واسع المجال يمكن أن يترتب عليه نتائج متعددة وليس مجرد النتيجة المقصودة من الجريمة وهذا الأمر متوافق بالضرورة مع الطبيعة التي عليها تقنية المعلومات، فمن يقصد القرصنة ويتحقق معها انتشار فيروسات من أي نوع نتيجة لوجود دفاع فيروسي في البرمجة أو الموقع، فمثل هذه النتائج تتحقق مع النتيجة الأصلية وهي الشروع في القرصنة إلى جواز نتائج أخرى يبدو الاحتمال واضحاً في حدوثها كنتائج لكنها ليست النتائج المقصودة من النشاط الإجرامي [٢] .

الفرع الثاني
الركن المعنوي للجرائم الإلكترونية

الركن المعنوي في الجرائم الإلكترونية له صور عديدة منها القصد الجنائي وهو علم الجاني واتجاه إرادته إلى مخالفة القانون الجنائي، ويكون ذلك في الجريمة العمدية، ولذا يجب على الجاني أن يكون عالماً بحقيقة ما يرتكبه، مدركاً أن عمله

(١) د. عبد الأحد جمال الدين د. جميل الصغير، ، النظرية العامة للجريمة، دار النهضة العربية، القاهرة، ٢٠٠٦ م.

(٢) د. عمر يونس، الجرائم الناشئة عن استخدام الإنترنت الأحكام الموضوعية والجوانب الإجرائية، دار النهضة العربية، ٢٠٠٤م، ص ٢٧٥.

هذا يجرمه القانون ويعاقب عليه به [1]، حيث يمثل ذلك الركن المسلك الذهني أو النفسي للجاني، وفي إطار هذا الركن تتوافر كافة مقومات المسؤولية الجنائية [2].

ومفهوم القصد الجنائي يظل أمرًا معقدًا في سياق الجرائم الإلكترونية، حيث تعترض العديد من المشكلات التي ترتبط بتحديد مدى تطلب القصد الجنائي وكيفية تحقيق هدف المشرع في بنية الإدانة، يظهر هذا بشكل واضح عند مناقشة مدى إمكانية توسيع نطاق التحقيق في الركن المعنوي للجرائم ذات الصلة بالجريمة الأولى في مجال الجرائم الإلكترونية، وتحديداً جريمة الاختراق. بخلاف هذه الجريمة، قد يتطلب المشرع في الجرائم الأخرى ذات الصلة ببناء الركن المعنوي فيها العمد أو قد لا يتطلبه، وذلك وفقًا للظروف والسياق [3].

وتتحقق جريمة الاختراق للنظام المعلوماتي في صورتها البسيطة بمجرد فعل الدخول غير المشروع[4]، وهذه الجريمة قد نص عليها المشرع الكويتي في المادة الثانية فقرة أولى من القانون رقم ٦٣ لسنة ٢٠١٥ الكويتي، حيث نص على أنه:

---

(١) د. أحمد المجذوب، مشكلة تقنين القصد الجنائي، المجلة الجنائية القومية، العدد الأول، المجلد ١٣، ١٩٧٠م، ص ٤١٠.

(٢) د. محمود نجيب حسني، المرجع السابق، ص٩.

(٣) د. عمر يونس، المرجع السابق، ص ٢٨٩-٢٩١

(٤) د. علي القهوجي، المرجع السابق، ص ٥٤.

"يعاقب بالحبس مدة لا تجاوز ستة أشهر وبغرامة لا تقل عن خمسمائة دينار ولا تجاوز ألفي دينار أو بإحدى هاتين العقوبتين، كل من ارتكب دخولاً غير مشروع إلى جهاز حاسب آلي أو إلى نظامه أو إلى نظام معالجة إلكترونية للبيانات أو إلى نظام إلكتروني مؤتمت أو إلى شبكة معلوماتية " [١]، بينما تتحقق في صورتها المشددة متى ترتب على الدخول غير المشروع محو أو تعديل البيانات التي يحتويها النظام، أو عدم قدرة النظام ذاته على تأدية وظيفته، وقد شدد كل من المشرع الكويتي والإماراتي العقاب في تلك الحالة نظراً لخطورة الأضرار الجسيمة المترتبة على تلك الأفعال [٢].

والصورة الثانية من صور الركن المعنوي، الخطأ غير العمدي في الجرائم الإلكترونية، ويتكون الركن المعنوي في هذه الجرائم من الخطأ بسبب الإهمال وعدم الاحتياط والرعونة، وهو المسلك الذهني للجاني الذي يؤدي لنتائج إجرامية لم يردها الجاني وكان بإمكانه أن يتوقاها، وكان يتوقع النتيجة الإجرامية ولكنه لم يبذل العناية الواجبة عليه لتلافيها [٣].

---

(١) وهي المقابلة لنص المادة الثانية فقرة (١) من القانون الإماراتي رقم ٥ لسنة ٢٠١٢.

(٢)نص م (٢) فقرة ثانية من القانون رقم ٦٣ لسنة ٢٠١٥ الكويتي، والمادة (٢/ ٢) من مرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ الإماراتي.

(٣) د. محمود نجيب حسني، المرجع السابق، ص ٦٦٤.

المبحث الثاني

الإشكاليات الموضوعية والإجرائية للجرائم الإلكترونية وسُبل مواجهتها

تمهيد وتقسيم:

تتعدد الإشكاليات الموضوعية والإجرائية باعتبارها تمثل صعوبات وتحديات تعيق مكافحة ومواجهة الجرائم الإلكترونية، فأول تلك الإشكاليات عدم اتفاق التشريعات المقارنة على مفهوم موحد للجرائم الإلكترونية؛ بل يمكن تجريم ذات الفعل في التشريعات الوطنية ذاتها، الأمر الذي ينعكس بطبيعة الحال على المسؤولية الجزائية الناشئة عن الجرائم الإلكترونية. وسنحاول في هذا المبحث إبراز تلك الإشكاليات وملامح القصور في معالجتها التشريعية، وسُبل مواجهتها، **وذلك على التفصيل التالي**:

المطب الأول: الإشكاليات الموضوعية والإجرائية للجرائم الإلكترونية

المطلب الثاني: سُبل مواجهة إشكاليات الملاحقة الجزائية للجرائم الإلكترونية

المطلب الأول
الإشكاليات الموضوعية والإجرائية للجرائم الإلكترونية
الفرع الأول : عدم وجود مفهوم محدد ومشترك للجرائم الإلكترونية

لا تتفق الأنظمة القانونية والتشريعات في دول العالم كافة على الأفعال المجرمة فيما يتعلق بالجرائم الإلكترونية، فما يكون مشروعًا في أحد الأنظمة قد يكون مجرمًا وغير مشروع في نظام أخر، مما يشكل نوعا من التخبط لا بد من إزالته بهدف توحيد المسميات والمفاهيم [1].

ويمكن عزو ذلك إلى عدة أسباب أهمها اختلاف الفكر القانوني حول حماية

(١) حيث أطلق عليها المشرع السعودي الجرائم المعلوماتية»، والمشرع القطري «الجرائم الإلكترونية»، وهناك من أطلق عليها جرائم تقنية المعلومات» كما فعل القانون العماني والقانون الإماراتي. أما على المستوى الدولي فقد أطلق عليها المشرع البلجيكي جرائم الكمبيوتر»، وكذلك فعل المشرع الإنجليزي، والمشرع الياباني، والمشرع الفرنسي، والعديد من الولايات في الولايات المتحدة الأمريكية. أما المشرع البلغاري فأطلق عليها «جرائم العالم الافتراضي»، وكذلك فعل المشرع الكندي، والمشرع الألماني والمشرع الهنغاري، والمشرع الإيطالي. أما المشرع الدنماركي فأطلق عليها «جرائم تكنولوجيا المعلومات»، وكذلك فعل المشرع الهندي. انظر في ذلك: أنور محمد صدقي مساعدة، إضاءات وتأملات في قانون الجرائم الإلكترونية القطري الجديد الصادر بالقانون رقم ١٤ لسنة ٢٠١٤، العدد الثاني مجلة مركز الدراسات القانونية والقضائية، وزارة العدل، قطر (السنة الثامنة ٢٠١٦)، ص. ٣٠٥؛ أنور محمد صدقي مساعدة، مدى كفاية أحكام التجريم الإلكتروني في قانون الجرائم الإلكترونية الأردني الجديد رقم ٢٧ لسنة ٢٠١٥ العدد ،٧٤ السنة ٣٢، رجب ١٤٣٩ هـ، إبريل ٢٠١٨، مجلة الشريعة والقانون جامعة الإمارات العربية المتحدة ص. ٤٥٥.

New German Laws on Cybercrime: www.securityfocus.com. The World Information Technology and Services Alliance: www. witsa.org. National Belgium Information Technology Center: www.nitc.gov. National English Information Technology Center: www.nitc.gov.np. Science links japan website: http://sciencelinks.jp/j-east. Website of Athabasca University: www.atha-bascau.ca/policy/computingservices. James M. Thomas, The Computer Fraud and Abuse Act: A Powerful Weapon vs. Unfair Competitors and Disgruntled Employees, In-House Defense Quarterly, Chicago, 2007, &1.

المعلومات، إضافة إلى قصور التشريع ذاته في العديد من دول العالم وعدم مسايرته لسرعة التقدم المعلوماتي التقني ومن ثم الجرائم الإلكترونية [1].

وكما سبق أن أشرنا أن المشرع الكويتي لم يكن موفقاً في اختياره عَنْوان هذا النوع من الجرائم في القانون رقم (٦٣) لسنة ٢٠١٥ بشأن مكافحة جرائم تقنية المعلومات ، فعبارة "تقنية المعلومات" تدل على أنظمة تشغيل المعلومات ولا تشمل المعلومات، وذات الملاحظة توجه ايضاً إلى المشرع الجزائري الذي عنون هذه الجرائم بـ "الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات"، وكأن الأمر يتعلق بحماية الأنظمة فقط دون المعلومات أو المعلومات الموجودة داخلها، ورغم أن التسمية المعتمدة من طرف المشرّع السعودي أقرب للصواب وأشمل وهي "قانون مكافحة الجريمة المعلوماتية"، إلا أنه ومع ذلك نجد أيضاً أن مصطلح معلوماتية لا يشمل كل الجرائم التي تقع في عالم افتراضي، وإنما تقتصر على الجرائم الماسة بالمعلومات.

ومن هنا يكون الأصح تسمية هذا النوع من الجرائم بـ (الجرائم الإلكترونية)،

(١) عبد الفتاح بيومي حجازي- الإثبات الجنائي في جائم الكمبيوتر والإنترنت، دار الكتب القانونية القاهرة، ٢٠٠٧م، ص١٨٨، وما بعدها. أنظر أيضًا: حسين سعيد الغافري، السياسية الجنائية في مواجهة جرائم الإنترنت (دراسة مقارنة) دار النهضة العربية، القاهرة، ٢٠٠٩م، ص٦٩٠ وما بعدها.

ليعكس بشكل أفضل التحديات والتطورات في مجال مكافحة الجرائم الإلكترونية.

ولذلك فإنه بات لزامًا على الدول أن تتحرك على محورين من أجل مكافحة الجريمة الإلكترونية:

المحور الأول:- يمكن تحقيق التصدي للجرائم المستحدثة عبر وضع قوانين تتماشى مع طبيعة هذه الجرائم، ومن ثم يتعين تطوير تشريعات فعّالة وشاملة تغطي مجالات متعددة مثل الوصول غير المشروع إلى الأنظمة الحاسوبية، والاحتيال الإلكتروني، وسرقة الهوية، والتهديدات السيبرانية الأخرى.

المحور الثاني:- فيكون على المستوى الدولي، حيث يمكن تعزيز مكافحة الجرائم المستحدثة من خلال وضع اتفاقيات دولية وإقليمية فعّالة. يجب أن تتيح هذه الاتفاقيات التعاون الفعّال بين الدول لمواجهة التحديات السيبرانية العابرة للحدود. يمكن أن تشمل هذه الاتفاقيات مجموعة واسعة من المسائل، مثل تبادل المعلومات، وتسليم المجرمين، وتعزيز التحقيقات الدولية بهدف تطوير إطار قانوني دولي فعّال يتناسب مع التحديات السيبرانية المتزايدة وبما يسهم في توحيد الجهود للقضاء على هذه الجرائم[١].

(١)خالد محمد كدفور المهيري، جرائم الكمبيوتر والانترنت والتجارة الالكترونية، دار العزيز للطباعة والنشر، دبي، ٢٠٠٥، ص١٣٥.

الفرع الثاني
مدى كفاية المعالجة التشريعية لأشكال الجرائم الإلكترونية

حاول المشرع الكويتي من خلال القانون رقم (٦٣) لسنة ٢٠١٥ بشأن مكافحة جرائم تقنية المعلومات التصدي لهذه الظاهرة المتزايدة للإجرام الإلكتروني، حيث تناول المشرع في هذا القانون مختلف أشكال الجريمة الإلكترونية، ووفر نصوصًا تجريميه تتعامل مع التحديات الفريدة لهذا النوع من الجرائم.

ويجب أن نشير إلى أن المشرع الكويتي كان له فرصة أكثر من غيره في سنّ مثل هكذا قانون، حيث توجد أمامه العديد من التشريعات المقارنة التي تناولت مكافحة الجريمة المعلوماتية، وكذا العديد من الاتفاقيات الدولية على رأسها الاتفاقية العربية لمكافحة الجريمة المعلوماتية، واتفاقية بودابست لمكافحة الجريمة الإلكترونية. ولكن هل وفق المشرّع الكويتي في سن قانون شامل لمختلف جوانب وأشكال الجريمة الإلكترونية أو المعلوماتية كما فضل تسميتها؟ وهل استفاد من ثغرات ونقائص القوانين المقارنة باعتباره قانون حديث النشأة ؟ هذا ما سنحاول تسليط الضوء عليه على النحو التالي:

أولاً: فيما يتعلق بالمفاهيم الواردة بقانون مكافحة جرائم تقنية المعلومات الكويتي:

نصت المادة الأولى من هذا القانون على أنه: "تطبيق أحكام هذا القانون يقصد بالمصطلحات التالية، المعنى الموضح قرين كل منها:....."، بالرجوع إلى نص

المادة المشار إليها نجد المشرع الكويتي يحاول شرح بعض المصطلحات المتعلقة بهذا النوع من الجرائم، حيث قام بتعريف عدد من المصطلحات وهى: البيانات الإلكترونية؛ النظام الإلكتروني؛ نظام المعالجة الإلكترونية للبيانات؛ الشبكة المعلوماتية؛ المستند أو السجل الإلكتروني؛ الموقع؛ ووسيلة تقنية المعلومات؛ الجريمة المعلوماتية؛ نظام الحاسب الآلي؛ التوقيع الإلكتروني؛ الالتقاط ألمعلوماتي؛ والاحتيال الإلكتروني، وهذا يعد بلا شك أمر يخدم مبدأ الشرعية، ويبعد القاضي الجنائي عن التفسير والقياس، ويسهل عليه الوصول إلى التكييف المناسب، إلا أنه هل كانت هذه المفاهيم شاملة أم أن هناك مصطلحات كان على المشرع الكويتي تضمينها في الماد الأولى؟

وفي الواقع، يظهر أن المشرع الكويتي قد قدّم شروحًا وتعاريف دقيقة ومفصلة للمفاهيم المتعلقة بالجرائم الإلكترونية، متفوقًا بذلك على بعض التشريعات الأخرى كالقانون الجزائري أو السعودي أو الاتفاقية العربية في هذا الصدد[1]، إلا أن

(١)على سبيل المثال نجد المشرع الكويتي عرَّف البيانات الإلكترونية : بأنها بيانات ذات خصائص إلكترونية في شكل نصوص أو رموز أو أصوات أو رسوم أو صور أو برامج حاسب آلي أو قواعد للبيانات، في حين نجد المشرع السعودي يستعمل مصطلح البيانات للدلالة على البيانات الإلكترونية، لذلك نجد أن التعبير الذي استعمله المشرع الكويتي أفضل لأنه مركز، كما أن المشرع السعودي لم يكن موفقًا كنظيره الكويتي في شرح هذه العبارة، حيث نجد أن التعريف المذكور أعلاه مختصر ودقيق ، هذا ولم ينص المشرع الجزائري على هذا التعريف بينما نصت عليه الاتفاقية العربية لمكافحة الجرائم المعلوماتية تحت مسمي ا البيانات.

هناك بعض نوردها فيما يلي:

١- المشرع الكويتي لم يعرف مفهوم "التداخل"، الذي يختلف عن الدخول غير المشروع وكذلك عن الالتقاط. حيث يتعلق التداخل بمحاولة الجاني اعتراض الموجات أو الإشارات بقصد الاطلاع على محتواها أو التشويش، ويحدث غالبًا في البث التلفزيوني المشفر.

٢- المشرع الكويتي لم يُعرِّف مفهوم "الحاسب الآلي"، على الرغم من أن جهاز الحاسب الآلي معروف. يفضل في هذا السياق توضيح مفهوم جهاز الحاسوب، كما فعل المشرع السعودي. في المادة الأولى فقرة (٠٦)، عرَّف المشرع السعودي جهاز الحاسوب على أنه: "أي جهاز إلكتروني ثابت أو محمول، سلكي أو لاسلكي، يحتوي على نظام معالجة للبيانات، أو تخزينها، أو إرسالها، أو استقبالها، أو تصفحها، يؤدي وظائف محددة بحسب البرامج والأوامر المعطاة له".

٣- ربط المشرع الكويتي مفهوم الاحتيال الإلكتروني بقصد الحصول على منفعة دون وجه حق أو الإضرار بالغير[1]، وهو جانب الصواب إلى حد ما. ومن الأفضل أن

(١)حيث عرف المشرع الكويتي الاحتيال الإلكتروني بأنه: «التأثير في نظام إلكتروني مؤتمت أو نظام معلوماتي إلكتروني أو شبكة معلوماتية أو مستند أو سجل إلكتروني أو وسيلة تقنية معلوماتية أو نظام أو جهاز حاسب آلي أو توقيع إلكتروني أو معلومات إلكترونية وذلك عن طريق البرمجة أو الحصول أو الإفصاح أو النقل أو النشر الرقم أو كلمة أو رمز سري أو بيانات سرية أو خاصة أخرى، بقصد الحصول على منفعة دون وجه حق أو الإضرار بالغير»

يكون التعريف أكثر شمولًا دون الربط الحصري بوجود قصد خاص، نظرًا لأن العديد من عمليات الاحتيال الإلكتروني تتم بدافع المتعة والتحدي وليس فقط بهدف الحصول على منفعة أو الإضرار.

٤- المشرع الكويتي لم يعرِّف مفهوم "الوسيط في خدمة الإنترنت"؛ حيث يلعب الوسيط دورًا كبيرًا في نقل المعلومات أو توفيرها أو حفظها، ويتحمل جزءًا من المسؤولية الجنائية في بعض الجرائم الإلكترونية. ويُعرَّف الوسيط في التشريع الجزائري على أنه "أي كيان عام أو خاص يقدم المستعملين خدمات الاتصال عبر منظومة معلوماتية و/ أو نظام للاتصالات، وأي كيان آخر يقوم بمعالجة أو تخزين معلومات لصالح خدمة الاتصال المشار إليها أو لصالح مستخدميها."[1].

ثانياً: النصوص التجريمية المتعلقة بجرائم الدخول غير المشروع الواردة بقانون مكافحة جرائم تقنية المعلومات الكويتي:

تنص المادة الثانية من القانون رقم (٦٣) لسنة ٢٠١٥ بشأن مكافحة جرائم تقنية

(١)بينما عرفته الاتفاقية العربية تحت مسمى مزود الخدمة بأنه: «أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها...، وللاستفادة أكثر يمكن إجراء مقارنة مع اتفاقية بودابست، هلالي عبد اللاه أحمد ٢٠٠٨، مكافحة الجرائم المعلوماتية، دار النهضة العربية، ط ٠١.

المعلومات الكويتي على أنه : «يعاقب بالحبس مدة لا تجاوز ستة أشهر، وبغرامة لا تقل عن خمسمائة دينار ولا تجاوز ألفي دينار أو إحدى هاتين العقوبتين، كل من ارتكب دخولاً غير مشروع إلى جهاز حاسب آلي، أو إلى نظامه، أو إلى نظام معالجة إلكترونية للبيانات، أو إلى نظام إلكتروني مؤتمت ، أو إلى شبكة معلوماتية، فإذا ترتب على هذا الدخول إلغاء أو حذف أو إتلاف أو تدمير أو إفشاء أو تغيير أو إعادة نشر بيانات أو معلومات، فتكون العقوبة الحبس مدة لا تجاوز سنتين، والغرامة التي لا تقل عن ألفي دينار، ولا تجاوز خمسة آلاف دينار أو إحدى هاتين العقوبتين، فإذا كانت تلك البيانات أو المعلومات شخصية ؛ فتكون العقوبة الحبس مدة لا تجاوز ثلاث سنوات والغرامة التي لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين».

يبدو أن المشرع الكويتي يهدف من خلال المادة الثانية من القانون رقم (٦٣) لسنة ٢٠١٥ بشأن مكافحة جرائم تقنية المعلومات الكويتي **إلى حماية الأنظمة والبرامج من عمليات التطفل والقرصنة. حيث يُحظر الدخول غير المشروع إلى أي جزء من النظام أو النظام بأكمله، وقد يكون ذلك بعد فوات الوقت المحدد للدخول. هذا يشير إلى رغبة المشرع في تقييد ومعاقبة أي دخول غير مشروع يمكن أن يؤدي إلى إلغاء أو تدمير البيانات أو التلاعب بها، مما يعزز الحماية للأنظمة والبرامج من الاعتداءات**

السيئة [١].

إلا أنه يجدر الملاحظة إلى أن المشرع الكويتي لم يضف جوانب جديدة تخص جريمة الدخول غير المشروع في قانون مكافحة جرائم تقنية المعلومات، مما يعكس تشابهًا كبيرًا مع نظرائه في الجزائر والمملكة العربية السعودية والاتفاقية العربية في هذا الشأن، ولذلك غفل مثل نظرائه من المشرعين عن الكثير من السلوكيات التي تتشابه

---

(١)حصل نقاش واسع في الولايات المتحدة الأمريكية حول عبارة «الدخول» وذلك سنة ١٩٩٦ أمام محكمة كانساس العليا في قضية Allen، حيث حاولت التضييق من مفهوم الدخول، وتتلخص وقائع القضية في قيام المتهم Allen باستخدام حاسبه الآلي للاتصال بحاسب شركة الهاتف الجنوبية الغربية التي تتحكم في تحويل الاتصالات البعيدة المدى، حيث تلاعب المتهم بنظامها بطريقة تسمح بالاتصال الهاتفي مجانا ، وقد اتضح للمحققين أن Allen اخترق النظام عن طريق فك كلمته السرية ، ومن ثمة إزالة الدليل على نشاطه بإلغاء السجلات ..، وقد دافع المتهم عن نفسه أمام المحكمة بأنه لا يوجد دليل على دخوله إلى الحاسب الآلي للشركة، إلا أن الادعاء اعتمد على تعريف التشريع الواسع لعبارة الدخول Access) والتي تقر بأن الدخول يعني الاقتراب أو إصدار أمر أو الاتصال بـ.. أو أي أشياء أخرى تؤدي إلى استخدام مصادر الحاسب الآلي... لكن المحكمة أجابت بأن هذا التعريف كان واسعا يؤدي إلى القول بعدم دستورية التشريع لغموضه..، وانتهت المحكمة إلى أن المعنى الكامل والعادي يجب أن يطبق عوضا عن الترجمة المشوهة للتعريف المتوافر .... والقول إن دخول المتهم إلى النظام يظهر في قيامه بالبحث عن كلمة العبور الخاصة بنظام الشركة المذكورة للوصول إلى المعلومات قول لا دليل عليه، وهو ما يؤدي إلى القول بعدم دخول المتهم إلى حاسبات الشركة . انظر : خليفة محمد، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، رسالة دكتوراه كلية الحقوق جامعة باجي مختار عنابة٢٠١٠، ص ١٤٠ وما بعدها.

انظر أيضا:

Samia Bet Ismail Kamoun. La formation du contrat de vente électronique et le droit commun des contrats. Revue Tunisienne de Droit. Centre de Publication Universitaire 2004.p 132.

مع الدخول غير المشروع، وسنحاول الإشارة إليها فيما يلي:

١- لم ينص المشرع الكويتي على فعل (البقاء) الذي يتحقق في حالة ما إذا كان الجاني مسموحـًا له بالدخول لفترة زمنية، لكنه يتعمد البقاء بعد نفاذ تلك الفترة، ففي هذه الحالة يُعد بقاؤه غير مشروع [١].

٢- أن المشرع الكويتي نص في الفقرة الثانية من ذات المادة على تشديد العقوبة في حالة ترتب على فعل الدخول إلغاء أو حذف أو إتلاف أو تدمير أو إفشاء أو تغيير أو إعادة نشر بيانات أو معلومات، إلا أنه لم يبين أو يحدد نوع معلومات؛ هل المعلومات المتعلقة بسير النظام أو المعلومات المحفوظة داخل النظام ؟ [٢]، ولذلك كان من الأفضل تدارك ذلك وإعادة صياغة نص المادة لتتلاءم مع قصد المشرع الكويتي في الفقرتين الأولى والثانية من المادة الرابعة حيث نجد أنه يقصد

---

(١) وهو فعل لم يشر إليه المشرّع السعودي ايضـًا، ولكن نص عليه المشرع الجزائري، حيث جاء في المادة (٣٩٤ مكررا) من قانون العقوبات أنه : يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة مالية من ٥٠.٠٠٠ د.ج إلى ١٠٠.٠٠٠ د. ج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك».وهو ما نصت عليه الاتفاقية العربية لمكافحة الجريمة المعلوماتية حيث جاء في المادة (١/ ٦) منها: "الدخول أو البقاء، وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به". د. إبراهيم عبد العزيز شيما، الإدارة العامة، مؤسسة شباب الجامعة، بدون سنة طبع، الإسكندرية ص ١٧٠.

(٢)تنص بقية الفقرة وهي صياغة لا غبار عليها : «فإذا وقع التزوير على مستند رسمي أو بنكي أو بيانات حكومية أو بنكية إلكترونية تكون العقوبة الحبس مدة لا تجاوز سبع سنوات، وبغرامة لا تقل عن خمسة آلاف دينار ولا تجاوز ثلاثين ألف دينار أو بإحدى هاتين العقوبتين. ويعاقب بذات العقوبة بحسب الأحوال كل من استعمل أيـًا مما ذكر مع علمه بتزويره أو فقده لقوته القانونية».

البيانات الموجودة داخل النظام، وليس بيانات سير النظام.

٣- الملاحظ أيضـًا أن المشرع الكويتي لم يُوفَّق عندما نص على حماية المعلومات سواء كانت عامة أو شخصية ضمن جريمة الدخول، حيث اعتبر المساس بهذه البيانات. مجرد ظرف تشديد، ويكون من الأفضل لو نص على الجرائم الماسة بالبيانات المخزنة داخل الأنظمة والبرامج بصفة مستقلة، وذلك نظراً لتعدد وتنوع هذه الجرائم، فالأمر لا يتعلق فقط بمجرد المساس بهذه المعلومات بل هناك أشكال أخرى من الأفعال الماسة بالبيانات مثل: جريمة عدم اتخاذ الإجراءات الأولية لإجراء معالجة البيانات، جريمة عدم اتخاذ الاحتياطات اللازمة لحماية البيانات المعالجة، جريمة المعالجة غير المشروعة للبيانات...الخ.

٤- أن المشرع الكويتي لا يُعترف بقيام جريمة الاحتيال الإلكتروني إلا إذا كانت الوسائل المستخدمة في الاحتيال قادرة على خداع المجني عليه. ويُعتبر هذا الشرط مناسبًا في جرائم النصب التقليدية، ولكنه قد يكون صعب التطبيق في جريمة الاحتيال الإلكتروني، حيث يعتمد العالم الإلكتروني على معرفة متقدمة بتقنيات المعلومات، وهو ما قد يكون مجهولًا للكثير من مستخدمي الإنترنت. من هنا، كان من الأفضل عدم ربط شروط الجريمة بهذا الشرط، مما يتيح حرية التقييم لقاضي الموضوع.

٥- ويلاحظ في هذا السياق ايضـًا أن هناك وجود تفاوت بين نص هذه الجريمة

وتعريف الاحتيال الإلكتروني الوارد في المادة الأولى من ذات القانون. ففي تعريف الاحتيال الإلكتروني، ربط المشرع الكويتي بين الاحتيال وقصد الحصول على منفعة، بينما توسع نص المادة في الفقرة الثالثة والفقرة الأخيرة ليشمل المال أو مستندًا أو توقيعًا على مستند. يمكن أن يكون نص المادة الثالثة أكثر دقة لتغطية مجموعة واسعة من السلوكيات وضمان عدم إفلات المجرم من العقوبة.

ثالثاً: النصوص التجريمية المتعلقة بجرائم تعطيل الأنظمة أو المواقع الواردة بقانون مكافحة جرائم تقنية المعلومات الكويتي:

نص المشرع الكويتي في الفقرة الأولى من المادة الرابعة من قانون مكافحة جرائم تقنية المعلومات الكويتي رقم ٦٣ لسنة ٢٠١٥ على أنه : «يعاقب بالحبس مدة لا تجاوز سنتين، وبغرامة لا تقل عن ألفي دينار ولا تجاوز خمسة آلاف دينار، أو بإحدى هاتين العقوبتين كل من : أعاق أو عمل عمداً الوصول إلى موقع خدمة إلكترونية، أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات الإلكترونية بأي وسيلة كانت، وذلك عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات..»، ولقد تميز المشرع الكويتي بالنص على هذا السلوك المجرم بهذه الصياغة، إذ لا نجد لها مثيلا عند المشرع الجزائري، أما

المشرع السعودي فقد نص على هذا السلوك المجرم، ولكن صياغة المشرع الكويتي أفضل[١]، حيث نصت المادة الخامسة نظام مكافحة جرائم المعلوماتية ١٤٢٨هـ على" يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:١- الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها.٢- إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها. ٣-إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت".

أما فيما يخص حماية المواقع الإلكترونية، **فقد أسهب المشرع الكويتي في ذكر الأفعال التي يمكن أن تشكل السلوك المجرم، وقد أحسن في صياغتها**. وعلى الجانب الآخر، كان المشرع السعودي غير دقيق عندما نص على حماية المواقع الإلكترونية [٢]. **بينما يظهر أن المشرع الجزائري قد غفل عن هذه الجرائم في تشريعاته.**

(١)قارن ما بين الفقرة الأولى من المادة الرابعة من قانون مكافحة جرائم تقنية المعلومات الكويتي، والفقرة الثالثة من المادة الخامسة من قانون مكافحة الجرائم المعلوماتية السعودي.

(٢)المادة الخامسة من قانون مكافحة الجرائم المعلوماتية السعودي.

والملاحظ أن المشرع الكويتي لم ينص في المادة الثانية على المساس العمدي بالبيانات المتعلقة بسير النظام الإلكتروني، وإنما نص عليه كظرف تشديد إذا تم بغير قصد ويمكن أن يكون ذلك قصورًا في التجريم، حيث يقتصر على المواقع الإلكترونية دون غيرها من الأنظمة المعلوماتية، وكان من الأفضل أن تشمل الجريمة جميع الأنظمة المعلوماتية لضمان فاعلية أكبر في مكافحة المساس بالبيانات.

رابعاً: النصوص التجريمية المتعلقة بجرائم الاستخدام غير المشروع للأنظمة المعلوماتية والمواقع الواردة بقانون مكافحة جرائم تقنية المعلومات الكويتي:

نص المشرع الكويتي على هذه الجرائم في المادة الرابعة حتى المادة العاشرة من قانون مكافحة جرائم تقنية المعلومات الكويتي رقم ٦٣ لسنة ٢٠١٥ ، وهي تتعلق باستخدام الأنظمة المعلوماتية والمواقع للاعتداء على المراسلات أو المقدسات الدينية ورموز الدولة أو الأموال والأمن.

جاء في الفقرة الثالثة من المادة الرابعة في القانون الكويتي ما يلي: «تنصت أو التقط أو اعترض عمدا، دون وجه حق، ما هو مرسل عن طريق الشبكة المعلوماتية أو وسيلة من وسائل تقنية المعلومات..». **وقد أحسن المشرع الكويتي صياغة هذا السلوك المجرم، وكذلك المشرع السعودي، حيث نص كليهما على التصنت أو التقاط أو اعتراض الموجات أو الترددات، والذي يشمل التداخل، وهو سلوك**

يتعلق بالتشويش على موجات البث التلفزيوني المشفر، وهو ما يشكل تهديدًا لبعض القنوات التلفزيونية المعروفة.

أما الفقرة الرابعة من المادة الرابعة فقد جاء فيها: «كل من أنشأ موقعاً أو نشر أو أنتج أو أعد أو هيأ أو أرسل أو خزن معلومات أو بيانات ، بقصد الاستغلال أو التوزيع أو العرض على الغير عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات وكان ذلك من شأنه المساس بالآداب العامة ، أو أدار مكاناً لهذا الغرض». **وهنا يحاول المشرع الكويتي من خلال هذه الفقرة حماية الأخلاق والآداب العامة من نشر المواد الإباحية، إلا أنه يلاحظ في هذا الشأن الملاحظات التالية:**

١- أن المشرع الكويتي قد ربط كل هذه السلوكيات بالمعلومات أو البيانات، وتجاهل الصور أو الفيديوهات كمادة يتم إعدادها وعرضها، ومن ثم كان من الأفضل لو نص على عبارة : «ما من شأنه» مكان عبارة «معلومات أو بيانات»، حتى تكون الجريمة شاملة لكل الصور بكل أشكالها.

٢- إن المشرع الكويتي ذكر عبارة بالآداب العامة»، وكان من الأفضل لو أضاف لها عبارة والنظام العام والقيم الدينية والحياة الخاصة»، وهو ما نص عليه المشرع

السعودي الذي كانت صياغة لهذه الجريمة أفضل[1]، وكذا الاتفاقية العربية لمكافحته الجرائم المعلوماتية[2].

٣- كان من الأفضل إضافة مصطلح «اشترى» بعد مصطلح «خزن»، حتى تطال الجريمة المشتري أيضاً، وبدرجة أقل يستحسن إضافة مصطلح «البيع» بعد مصطلح «العرض».

ومن ناحية أخرى، حاول المشرع الكويتي توسيع دائرة التجريم لتشمل المحرض على أعمال الفجور والدعارة باستخدام الشبكة المعلوماتية، أو بإحدى وسائل تقنية المعلومات، حيث جاء في الفقرة الأخيرة من المادة الرابعة ما يلي: «كلُّ من حرَّض أو أغوى ذكراً أو أنثى لارتكاب أعمال الدعارة والفجور، أو ساعده على ذلك باستخدام الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، فإذا كان الفعل موجهاً إلى حدث فتكون العقوبة الحبس مدة لا تجاوز ثلاث سنوات والغرامة التي لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين»، **وقد حسن ما فعل المشرع الكويتي، إلا أنه ومع ذلك يلاحظ أنه شدد العقوبات فيما تعلق التحريض بحدث، ولم يشدِّد العقوبات في الفقرة الرابعة إذا تعلق**

(١)الفقرتان الأولى والثالثة من المادة السادسة من قانون مكافحة الجرائم المعلوماتية السعودي.

(٢)المادة ١٢ من الاتفاقية.

الأمر بأفعال مخلة بالآداب متعلقة بالأحداث، مع أن جل التشريعات تنص على ذلك.

وقد نصت المادة الخامسة من قانون مكافحة جرائم تقنية المعلومات الكويتي رقم ٦٣ لسنة ٢٠١٥ على أنه : يعاقب بالحبس مدة لا تجاوز سنة و وبغرامة لا تقل عن ألف دينار ولا تجاوز ثلاثة آلاف دينار أو بإحدى هاتين العقوبتين ، كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات للوصول دون وجه حق إلى أرقام أو بيانات بطاقة ائتمانية أو ما في حكمها من البطاقات الإلكترونية فإذا ترتب على استخدامها الحصول على أموال الغير، أو على ما تتيحه هذه البطاقة من خدمات، يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين»، **ويجب أن نشيد هنا بالصياغة القانونية لتلك المادة المشار إليه التي نفتقدها في الكثير من التشريعات العربية سيما وأن حماية بطاقات الائتمان باتت ضرورة ملحة باعتبارها من أكثر وسائل الدفع عرضة للقرصنة والتزوير.**

أما فيما يتعلق بجريمة الاعتداء على الأمن العام باستعمال وسيط إلكتروني، فقد نص المشرّع الكويتي في قانون مكافحة جرائم تقنية المعلومات الكويتي رقم ٦٣ لسنة ٢٠١٥ على مجموعة من الجرائم والمتعلقة في مجملها بالأمن العام وذلك في المواد من السادسة إلى العاشرة، **ورغم أننا ندعو المشرع الجزائري، وكذا السعودي بالنص على هذه الجرائم والاقتداء بالمشرع الكويتي في هذا الصدد سيما وأن الاتفاقية**

العربية لمكافحة الجريمة المعلوماتية لم تشر إلى هذه الجرائم. إلا أننا لاحظنا أن المشرع الكويتي يحيل إلى نصوص قانونية ورادة في قانون المطبوعات والنشر، وكذا القانون المعدل لقانون الجزاء، وكان من الأجدر به إدراج الأفعال المنصوص عليها في : تلك القوانين في المادتين بدل الإحالة إليها أو إلى عقوباتها.

ومن ناحية أخرى، فإن المشرّع الكويتي حاول مواجهة جريمة الاتجار بالبشر وهي من أخطر الجرائم ضد الإنسانية، وكذلك جريمة ترويج المخدرات أو المؤثرات العقلية لما لها من آثار سلبية على الفرد والمجتمع، وذلك من خلال ما نصت المادة الثامنة من قانون مكافحة جرائم تقنية المعلومات الكويتي رقم ٦٣ لسنة ٢٠١٥ على أنه: «يعاقب بالحبس مدة لا تجاوز سبع سنوات وبغرامة لا تقل عن عشرة آلاف دينار ولا تجاوز ثلاثين ألف دينار أو بإحدى هاتين العقوبتين، كل من أنشأ موقعاً أو نشر معلومات باستخدام الشبكة المعلوماتية أو بأي وسيلة من وسائل تقنية المعلومات المنصوص عليها في هذا القانون، بقصد الاتجار بالبشر أو تسهيل التعامل فيهم، أو ترويج المخدرات أو المؤثرات العقلية وما في حكمها ، أو تسهيل ذلك في غير الأحوال المصرح بها قانونا»، **إلا أنه يلاحظ أن هناك بعض الجرائم الأخرى كان من الأفضل لو نص عليها المشرع الكويتي في هذه المادة نظراً لخطورتها أيضاً ، وهي جريمة إنشاء موقع أو نشر معلومات باستخدام الشبكة المعلوماتية أو بأي وسيلة من وسائل تقنية المعلومات بقصد الاتجار بالأعضاء البشرية أو تهريب**

المهاجرين ... وهي جرائم لم ينص عليها المشرع السعودي ولا المشرع الجزائري ولا حتى الاتفاقية العربية لمكافحة الجريمة المعلوماتية.

والجدير بالذكر أن المشرع الكويتي يعتبر التشريعات التي تفطّنت لتجريم جريمة تبييض الأموال عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات، من خلال نص المادة السابعة من قانون مكافحة جرائم تقنية المعلومات الكويتي رقم ٦٣ لسنة ٢٠١٥ التي جاء شامل لكل صور التجريم المتعلقة بتبييض الأموال عن طريق وسيط إلكتروني. فالجناة على حدّ تعبير البعض في جرائم غسل الأموال قد اتجهوا إلى ارتكاب جرائمهم عن طريق الوسائط الإلكترونية وأهمها استعمال الحاسب الآلي وشبكة الإنترنت وبرامج الاختراق التي يمارسها الجناة لحسابات البنوك والقدرة على التلاعب بها ونقلها وتحويلها عن بعد، فلا أن تستعمل الأجهزة المصرفية الأنظمة المضادة لهذا بد الاختراق، وأن تراقب حركة الحسابات إلكترونيا سواء حركات السحب أو الإيداع أو التحويل أو النقل من الداخل أو الخارج أو العكس[١].

وأخيراً ورغم ما نصت عليه المادة العاشر من قانون مكافحة جرائم تقنية

(١)مراد رشدي، غسل الأموال عبر الوسائل الإلكترونية، ٢٠٠٧.مقال منشور على الموقع التالي:
http://www.f-law.net/law/threads.

المعلومات الكويتي رقم ٦٣ لسنة ٢٠١٥ من أنه :» يعاقب بالحبس مدة لا تجاوز عشر سنوات وبغرامة لا تقل عن عشرين ألف دينار ولا تجاوز خمسين ألف دينار أو بإحدى هاتين العقوبتين، كل من أنشأ موقعا لمنظمة إرهابية، أو لشخص إرهابي، أو نشر عن أيهما معلومات على الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، ولو تحت مسميات تمويهية، لتسهيل الاتصالات بأحد قياداتها أو أعضائها، أو ترويج أفكارها، أو تمويلها ، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرة، أو أية أدوات تستخدم في الأعمال الإرهابية»، **كذلك ورغم أن هذا النص ولم يكن له مثيل في التشريع الجزائري أو السعودي**[1]، **وكذا الاتفاقية العربية لمكافحة الجريمة المعلوماتية**[2]، **إلا أن نص هذه المادة يمكن أن يخلق عدة إشكاليات كثيرة من حيث التطبيق سيما صعوبة تحديد المقصود بالمنظمات الإرهابية أو الشخص الإرهابي، وكان من الأفضل تحديد المقصود بالعمل الإرهابي والمنظمات الإرهابية.**

ويجدر بنا الملاحظة أنه وعلى الرغم من أن قانون مكافحة جرائم تقنية المعلومات الكويتي حديث الصدور ويتميز بصياغة ممتازة، إلا أن هناك بعض الجرائم التي لم

(١)المادة السابعة من قانون مكافحة الجريمة المعلوماتية السعودي.

(٢)المادة ١٥ من الاتفاقية.

يتضمنها القانون، ومن بينها الأفعال المتعلقة بتصميم أو صنع أو الاتجار بمعطيات أو برامج تستخدم في الجرائم الإلكترونية. كما تشمل هذه النقصان الأفعال المتعلقة بحيازة أو نشر أو استخدام المعطيات المتحصل عليها من الجرائم الإلكترونية. ويشترك المشرع السعودي في تفاقم هذا النقص، حيث لم ينص على هذه الجرائم أيضًا.

ومع ذلك، فقد نص كلاً من المشرع الجزائري وكذلك الاتفاقية العربية لمكافحة الجريمة المعلوماتية على هذه الجرائم، حيث قدر أن تجميع معلومات مستخدمة في ارتكاب جرائم إلكترونية يمكن أن يزيد من مستوى الخطر الذي تشكله هذه الجرائم ويسهم في تسهيل ارتكابها، ويُعرف هذا النوع من التشريع بالتشريع الوقائي.

الفرع الثالث
الصعوبات العملية في إثبات الجرائم الإلكترونية

واجهت الجرائم الإلكترونية صعوبات عملية كثيرة، بما في ذلك صعوبة إثبات وقائعها وضبط مرتكبيها، خاصةً إذا تم تنفيذ الاعتداءات خارج إقليم الدولة ، حيث تعد أدلة الإثبات والإدانة في شأن تلك الجرائم وهي كلها بيانات معنوية كسجلات الكمبيوتر ومعلومات الدخول والاشتراك والنفاذ وهي تثير جملة من الإشكاليات

أمام القضاء من حيث مدى قبولها وحجيتها مع وسائل الإثبات التقليدية أن أهم التحديات التي تواجه الجريمة الإلكترونية تتمثل في[1] الحاجة إلى سرعة الكشف عن الجريمة و تعقبها وخشية ضياع الدليل بالإضافة إلى خصوصية قواعد التفتيش والضبط الملائمة لهذه الجرائم، ومدى قانونية وحجة الأدلة في الجرائم الإلكترونية التي تقع عن الانترنت سيما في ضوء عدم وجود التعاون الدولي في مجال التحقيق وتسليم المجرمين وتنفيذ الأحكام القضائية.

فما يميز هذه الجريمة أنها تتصف بالخفاء وعدم وجود أثار مادية يمكن متابعتها مما يجعلها صعبة الاكتشاف، وعليه فمن الصعب تحديد مكان وقوعها، حيث إنها جريمة لا تترك أثار مادية بعد ارتكابها، وغالبا ما يتم اكتشافها بالمصادفة وبعد وقت طويل من حدوثها سيما مع صعوبة الاحتفاظ بالدليل الفني على ارتكابها[2]، وذلك لان الجاني يستطيع في ظرف وجيز جدا أن يمحوا أو يحرف أو يغير أو يتلف البيانات والمعلومات وجميع المعطيات الموجودة في قاعدة البيانات وعلى هذا الأساس كان للمصادفة دور كبير في اكتشافها.

كذلك فإن تلك الجرائم تحتاج إلى خبرة فنية وتقنية عالية، وذلك من خلال معرفة

(١)محمد الشكوابة، جرائم الحاسوب والانترنت دار الثقافة للنشر، الأردن، ٢٠٠٤، ص١٣.

(2)John Eaton & jermy smithers, A managers Guide to information Technology, London, Philip Allan, 1982,p263

تقنيات الكمبيوتر ونظم المعلومات سواءً في مجال جمع الأدلة والتحقيق أو المتابعة القضائية، لذلك فإن رجال الضبطية القضائية غير قادرين على التعامل مع هذه الفئة من الجرائم بالطرق التقليدية، بالإضافة إلى صعوبة تتبع مسار العمليات الكترونيا خصوصا إذا كانت عابرة للقارات، فهذه الجرائم تعتمد في المقام الأول على الخداع في ارتكابها والتضليل مما يساعد على عدم التعرف على الفاعل الحقيقي، والشيء الملاحظ هو أن المؤسسات والبنوك خصوصا تحجم عن الإبلاغ وهذا تجنبا للإساءة إلى السمعة والخوف من هز ثقة العملاء فيها، بالإضافة إلى إخفاء أسلوب ارتكاب الجريمة خوفا من تكرارها مما يزيد في فرص إفلات الجاني من العقاب[1].

بالإضافة إلى ذلك تعتمد تلك الجرائم على الذكاء ولهذا تسمى (جرائم الذكاء) وهي غالبا ما ترتكب بصفة فردية، واهم دوافعها الطمع والجشع والانتقام وأحيانا بدافع إثبات الذات، وعلى هذا الأساس نقول أن الإجرام المعلوماتي هو إجرام الأذكياء الذي يعتمد على مهارات فنية وتقنية وإلمام بنظم المعلوماتية بالمقارنة مع الإجرام التقليدي الذي يعتمد على العنف[2].

وتتجلى تلك الإشكالية في ضعف الشق الإجرائي لمكافحة هذه الجرائم سيما في

(١)خالد ممدوح إبراهيم، امن الجريمة الالكترونية، الدار الجامعية، الإسكندرية، ٢٠٠٨، ص٤٧

(٢)جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات، دار البداية، ليبيا، ٢٠٠٧، ص١٤٤.

القانون رقم ٦٣ لسنة ٢٠١٥ بشأن مكافحة جرائم تقنية المعلومات في الكويت.

حيث اقتصر المشرع الكويتي في هذا القانون على المادة (١٥) التي تحدد من لهم صفة الضبط القضائي، حيث نصت على أنه "للموظفين الذين يصدر بتحديدهم قرار من الوزير المختص ضبط الجرائم التي تقع بالمخالفة لأحكام هذا القانون وتحرير المخالفات عنها، وإحالتها الى النيابة العامة، وعلى جميع الجهات ذات الصلة تقديم التسهلات اللازمة لهؤلاء الموظفين."

وكذلك المادة (١٧) التي تنص على اختصاص النيابة العامة في التحقيق والتصرف والادعاء في هذه الجرائم، حيث نصت على أنه "تختص النيابة العامة وحدها، دون غيرها، بالتحقيق والتصرف والادعاء في جميع الجرائم المنصوص عليها في هذا القانون".

أما إجراءات الضبط والتفتيش، فقد اكتفى المشرع الكويتي بشأنها بتطبيق الأحكام الواردة في قانون الإجراءات والمحاكمات الجزائية الصادر سنة ١٩٦٠، وهو ما يصطدم عمليا مع طبيعة هذه النوعية من الجرائم فيما يتعلق بالدليل المتحصل منها[1].

(١)معاذ سليمان الملا، مرجع سابق، ص٢٢٩ وما بعدها.

الفرع الرابع
الصعوبات التي تتعلق بالإجراءات الجنائية

يشكل عدم وجود تنسيق في الإجراءات الجنائية المتعلقة بالجرائم الإلكترونية بين الدول، وبشكل خاص فيما يتعلق بأعمال الاستدلال والتحقيق، تحديًا كبيرًا، خاصة أن عملية الحصول على دليل في مثل هذه الجرائم قد تحدث خارج إقليم الدولة[١]، فبالنظر لطبيعة هذه الجرائم فإنها لا تترك اثرا ماديا في مسرح الجريمة بالإضافة إلى قدرة الجاني على إتلاف وتشويه الدليل في وقت قصير.**ومن هنا تظهر جملة من الصعوبات والتحديات أهمها:**

١. فيما يتعلق بإجراءات التفتيش المتعلق بتلك الجرائم يعتمد على نظم المعلومات وقد تتجاوزها إلى أنظمة أخرى غير نظام المشتبه به. حيث يعتمد هذا الإجراء على تمديد نطاق التفتيش على نظام غير المشتبه به، ويثير ذلك جملة من التحديات القانونية فيما يتعلق بمدى احترام حقوق الأفراد وعدم المساس بالحريات الشخصية، ومبدأ سرية الاتصالات بالنسبة للأفراد الذين يمتد إليهم التفتيش[٢].

---

(١) خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص٤٠٨، وما بعدها. انظر أيضًا عبد الفتاح حجازي، المرجع السابق، ص١٩٨ وما بعدها.

(٢)عبد الفتاح حجازي، مكافحة جرائم الكمبيوتر والانترنت، دراسة معمقة في القانون ألمعلوماتي، ط٠١، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦، ص١٤.

٢. فيما يتعلق بالنسبة لإجراءات الضبط فإنه لا تتوقف إجراءات الضبط على جهاز الكمبيوتر بل تمتد من ضبط المكونات المادية إلى مختلف أجزاء النظام، ومن ثم فتمتد إلى المعلومات والمعطيات والبيانات والبرامج المخزنة في النظام أو إلى النظم المرتبطة بالنظام محل الاشتباه وكل الأشياء ذات الطبيعة المعنوية لأنها معرضة بسهولة للتلف والضياع وهذا ما يثير إشكالية من الجهة القانونية خصوصا ما تعلق بالحقوق المحمية قانونا وكذا الحق في سرية البيانات واحترام سرية الاتصالات [1].

٣. ونظرًا لتنوع واختلاف النظم القانونية الإجرائية، فإن طرق الاستدلال والتحقيق والمحاكمة التي تثبت فائدتها وفاعليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى، أو قد لا يسمح بإجرائها فيها، كما هو الوضع بالنسبة للمراقبة الإلكترونية (Electronic Monitoring)، والتسليم المراقبة والعمليات المستترة، وغيرها من الإجراءات المماثلة، فإذا ما اعتبرت طريقة ما من طرق جمع الاستدلالات أو التحقيق على أنها مشروعة في دولة ما فقد تكون غير مشروعة في دولة أخرى،

(١)عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والانترانت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا، ط٠١، منشورات الحلبي الحقوقية، لبنان، ٢٠٠٧، ص ٤٧.

إلى جانب ذلك، يُضاف إلى التحديات القانونية أن هناك العديد من الدول التي تعاني من فقدان تشريعات تُجرم هذا النوع من الجرائم، أو أن التشريعات الموجودة قد تكون غير كافية للتعامل مع هذا التحدي الناشئ. ينعكس ذلك في صعوبة تقديم العقوبات للمرتكبين وتطبيق القانون بشكل فعّال. ومن ثم تظهر الجرائم الإلكترونية كتحدي دولي يتطلب تعاونًا فعّالًا بين الدول لتطوير إطار قانوني شامل وفعّال يمكن من مواجهة هذه التحديات المتزايدة وضمان حماية أمن الرقمي والمعلوماتية على الساحة الدولية [١].

٤. بالإضافة إلى ذلك، فإن عدم وجود قنوات اتصال (Communication Channels) بين الدول يشكل ايضاً مشكلة تعيق التعاون الدولي في مكافحة الجريمة، ولتحقيق هذا الهدف يجب أن يكون هناك قنوات اتصال تسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة أو معلومات هامة[٢].

٥. ويجب أن نشير إلى ايضاً أن عدم وجود معاهدات ثنائية أو جماعية (Bilateral

(1) Miquelon Weismann, Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, August 27-September 7, 1990, 335 &. Dominic Carucci, David Overhuls & Nicholas Soares, Computer Crimes, 48 AM. CRIM. L. REV. 375, 378, 2011, 417 &.

(٢) عبد الفتاح حجازي، المرجع السابق، ص١٨٩، وما بعدها أنظر أيضًا: حسين الغابق، المرجع السابق، ، ص٦٩١ وما بعدها. أنظر أيضا: خالد إبراهيم، المرجع الساق، ص٤١١، وما بعدها انظر أيضًا

John Nadelman, The Evoluion of United States Involvement in the International Rendition of fugitive Criminals, 25 N. Y. U, J, int l. 817- 122

Agreements) بين الدول على نحو يسمح بالتعاون الفعال في مكافحة الجرائم الإلكترونية، وحتى في حال وجودها فإن هذه المعاهدات قد لا تكون فعالة في توفير الحماية المطلوبة في ضوء التطور السريع للنظم والبرامج المعلوماتية[1].

(١) وقد حث مؤتمر الأمم المتحدة الثامن لمنع الجريمة والمجرمين- والذي تم عقده في هافانا بكوبا عام ١٩٩٠م- في قراره المتعلق بجرائم الحاسب الآلي الدول الأعضاء على تكثيف جهودها في مكافحة إساءة استخدام الحاسب الآلي، كما حث القرار الدول الأعضاء على الدخول كاطراف في المعاهدات المتعلقة بتسليم المجرمين وتبادل المساعدة في مكافحة جرائم الحاسب الآلي، كما حث القرار الدول الأعضاء بالعمل على أن تكون تشريعاتها المتعلقة بتسليم المجرمين وتبادل المساعدة في المسائل الجنائية تنطبق بشكل تام على جرائم الحاسب الآلي ودعا القرار أيضا إلى وضع معايير دولية لأمن المعالجة الآلية للبيانات، واتخاذ تدابير ملائمة لحل مشكلات الاختصاص القضائي التي تثيرها الجرائم المعلوماتية العابرة للحدود، كما دما القرار الدول الأعضاء إلى الدخول في اتفاقيات دولية تنطوي على نصوص وأحكام تنظم إجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الأنظمة المعلوماتية المتصلة فيما بينها، والأشكال الأخرى للمساعدة المتبادلة مع ضرورة كفالة الحماية لحقوق الأفراد وحرياتهم واحترام سيادة الدول، كذلك فقد نص المجلس الأوروبي (Council of Europe) في توصيته رقم(١٢/ ٩٥) على أن إجراءات التحقيق في البيئة التقنية تقتضي التدخل السريع لمد الإجراءات إلى أنظمة حاسبات قد تكون موجودة خارج الدولة، وحتى لا يمثل هذا الأمر اعتباه على سيادة الدولة يجب وضع قواعد قانونية صريحة تسمح بمثل هذا الإجراء، ولذلك فثمة حاجة ملحة لاتفاقية تنظم كيفية القيام بمثل هذه الإجراءات، كما يجب أن تتوافر إجراءات عاجلة ومناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع الأدلة، وهو ما يتطلب أن تسمع السلطات الأخيرة بإجراءات التفتيش والضبط. انظر حسين سعيد الغافري، المرجع السابق. ص٦٩٢، وما بعدها. أنظر أيضًا: عبد الفتاح حجازي، المرجع السابق، ص١٨٨ وما بعدها. انظر أيضًا:

Jack Brown, Jurisdiction to Prosecute Crimes Committed by use of the Internet, 38 Jurimetrics J. 611. 1998

الفرع الخامس
إشكالية تنازع الاختصاص القضائي

الاختصاص هو السلطة التي يقرها القانون للقضاء في أن ينظر في دعاوى من نوع معين [١]، وبالنظر لطبيعة وخصائص الجريمة الإلكترونية فليس لها مقر ثابت أو دولة معينة بل تنتشر في كل دول العالم، وليست لها أية هيئة أو جهة تشرف عليها ومسؤولة عنها مما يترتب عن ذلك عدم وجود قانون جنائي محدد أو موحد يحكم الجريمة بل بالعكس هناك العديد من القوانين الجنائية بتعدد الدول والأنظمة القانونية وذلك يرجع أساسا لارتباط القانون الجنائي بالسيادة الوطنية.

ومن هنا تكمن الإشكالية التي تثيرها الجرائم الإلكترونية تجاه مسألة الاختصاص (Jurisdiction) على المستويين الوطني والدولي، ولا توجد مشكلة بالنسبة للاختصاص على المستوى الوطني، حيث يتم الرجوع إلى القواعد المحددة قانونًا لذلك، ولكن المشكلة تثار فيما يتعلق بالاختصاص على المستوى الدولي حيث يوجد اختلاف بين الدول فيما يتعلق بالجرائم الإلكترونية التي تتميز بكونها عابرة للحدود، فقد يحدث أن ترتكب الجريمة في إقليم دولة ما من قبل شخص أجنبي، ففي هذه الحالة تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى استنادًا إلى مبدأ

(١)محمود نجيب حسني، شرح قانون الإجراءات الجزائية، دار النهضة العربية، ٢٠٠٢، ص ٧٢٣

الإقليمية، كما تخضع أيضا لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي.

حيث تتسم الجرائم الإلكترونية بأنها تحدث في عالم افتراضي، حيث يتمتع سلطانها بطابع غير مادي وليس مقيدًا بالحدود الجغرافية. يظهر أن مرتكبي الجرائم الإلكترونية لا يلتزمون بالحدود السياسية والجغرافية، ولا يحترمون الاختصاص القانوني للدول، مما يعزز التحديات التي تواجه الدول عند محاولتها متابعة مرتكبي هذه الجرائم. ويظهر ذلك بشكل واضح عندما ترتكب الجرائم داخل إقليم دولة ما من قبل قراصنة محليين، الذين يستخدمون في الغالب مواقع أو وصلات إلكترونية في دول أخرى.

ففي مايو ٢٠١٧، شهدنا إحدى أبرز عمليات القرصنة والاختراق في تاريخ الإنترنت، حيث تعرضت مجموعة واسعة من المؤسسات والأفراد في حوالي ٧٤ دولة لهجمات إلكترونية هائلة، وكانت هذه الهجمات من بين أكبر الهجمات على الصعيدين الدولي والرقمي. تضمنت الدول المستهدفة بريطانيا، روسيا، فرنسا، ألمانيا، إيطاليا، بلجيكا، والولايات المتحدة. تم استخدام في هذه الهجمات فيروس "وانا ديكربتر" الذي يعتمد على تشفير محتويات الحواسيب، مطالبًا صاحبه بفدية من خلال البيتكوين. تحليلات "Forcepoint Security Labs" أكدت أن هذا الهجوم كان ذا بُعد عالمي، حيث طال منظمات في عدة دول، بما في ذلك أستراليا، بلجيكا، فرنسا،

ألمانيا، إيطاليا، والمكسيك. شمل الهجوم حملة واسعة من الرسائل الإلكترونية المؤذية.

وفي إسبانيا، تعرضت الشركات، بما في ذلك شركة الاتصالات الرائدة "تليفونيكا"، للاختراق، وكان للهجوم الإلكتروني تأثير كبير على العديد من الجوانب الاقتصادية والتكنولوجية في البلاد. ولم يكتفِ الهجوم بذلك، بل تم تأكيد تعرض وكالة الأنباء القطرية للاختراق، مما أدى إلى أزمة تأثرت بها جميع دول الخليج العربي بظلالها. علاوةً على ذلك، تم استهداف موقع قناة العربية لعملية اختراق مماثلة، إضافةً إلى محاولات متكررة لاختراق العديد من المواقع الإخبارية الأخرى[1].

وكمثال على هذه الإشكالية التي نحن بصددها، سيما التحديات التي تواجه الجهات القضائية، يمكن الإشارة إلى الأحداث التي وقعت في بدايات العقد الأول من القرن الواحد والعشرين، حيث اخترق اثنان من القراصنة مواقع إلكترونية لعدة مصارف أمريكية، قام القراصنة بسرقة بيانات العملاء ومعلومات لعدد كبير من

(١) أنور محمد صدقي، إشكالية الاختصاص في الجرائم الإلكترونية، المجلة الدولية للقانون، المجلد ٢٠١٨ العدد الرابع الخاص بالحصار، ص١٥٧ وما بعدها.

البطاقات الإلكترونية، ثم استخدموا هذه البيانات لابتزاز الأفراد واستخلاص أموال منهم مقابل الحفاظ على سرية بياناتهم فيما بعد، كشفت جهات التحقيق، بما في ذلك مكتب التحقيقات الفيدرالي"FBI" ، أن شخصين يقيمان في روسيا هما الفاعلان وراء هذه الجرائم. وبالرغم من تقديم السلطات الأمريكية عدة طلبات لتسليم هذين الفردَين من قبل السلطات الروسية، إلا أن هذه الطلبات تم تجاهلها تمامًا، ولتجاوز هذا العائق، قامت الشرطة الفدرالية الأمريكية بمؤامرة ذكية، حيث أُقنع هؤلاء القراصنة بوجود فرصة عمل مغرية لهما في الولايات المتحدة، وعندما حضرا لمقابلة العمل المزعومة، تم جمع كافة بياناتهم الإلكترونية، وتمت مراقبة أجهزة الحاسوب الخاصة بهما، مما أدى إلى اعتقالهما [1].

المطلب الثاني

سُبل مواجهة إشكاليات الملاحقة الجزائية للجرائم الإلكترونية

تمهيد وتقسيم:

لم ينص المشرع الكويتي على الجانب الإجرائي للجرائم الإلكترونية بالشكل اللازم. فهذه الجرائم تتطلب وجود إجراءات خاصة نظرًا لكونها تقع في عالم افتراضي، مما يخلق العديد من الصعوبات من الناحية التطبيقية. ويجعل طبيعة هذه الجرائم الإجراءات العادية عاجزة عن إثباتها والوصول إلى المجرمين، الأمر الذي

(1) Amalie M. Weber, The Council of Europe's Convention on Cybercrime, 18 Berkeley Tech. L.J. 227, 2003.

يتعذر معه الملاحقة الجزائية للجرائم الإلكترونية، **وسنحاول في هذا المطلب التعرف على سُبل التغلب على تلك الإشكاليات، وذلك على التفصيل التالي:**

الفرع الأول
سُبل التغلب على مشكلة الاختصاص

ندعو المشرع الكويتي للنص على مسألة الاختصاص، نظرًا لأنها ترتبط بسيادة الدول ومبدأ المعاملة بالمثل. يعتبر الجرائم الإلكترونية جرائمًا عابرة للحدود، وبالتالي يمكن أن تحدث في إحدى الدول وتتأثر دولًا مختلفة بنتائجها. يثير هذا مشكلة الاختصاص للمحققين والقضاة، خاصة مع تصدي الاتفاقية العربية لمكافحة الجريمة المعلوماتية لهذه التحديات، تنص المادة ٣٠ من الاتفاقية على أن كل دولة طرف يجب أن تتخذ الإجراءات اللازمة لتوسيع اختصاصها لتشمل الجرائم المنصوص عليها في الفصل الثاني من الاتفاقية عندما ترتكب هذه الجريمة كلياً أو جزئياً من قبل مواطني الدولة الطرف، ينبغي على المشرع الكويتي مراعاة هذه الجوانب لضمان فعالية مكافحة الجرائم المعلوماتية وتحقيق العدالة الدولية.

الفرع الثاني
سُبل التغلب على مشاكل الأدلة الإلكترونية

ندعو المشرع الكويتي إلى النص على عدة إجراءات هامة تتناسب مع طبيعة الجريمة الإلكترونية، ومن بينها النص على تنظيم مسألة التفتيش الإلكتروني، وذلك نظرًا لكونها من بين الإجراءات المهمة في إثبات هذا النوع من الجرائم. بحيث يجب

أن يكون من الممكن للسلطات القضائية المختصة وضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية، الدخول بغرض التفتيش، وحتى عن بُعد، إلى منظومة معلوماتية أو جزء منها، وكذلك المعطيات المخزنة فيها ومنظومة التخزين المعلوماتية، وإذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى يمكن الدخول إليها انطلاقًا من المنظومة الأولى، ويجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقًا بذلك، إذا تبين مسبقًا أن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقًا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة، وفقًا للاتفاقيات الدولية المعنية ومبدأ المعاملة بالمثل.

ويجب أن يكون التفتيش الإلكتروني موضوع رقابة وشروط دقيقة لضمان احترام حقوق الأفراد والحفاظ على الخصوصية[1]، يشمل ذلك وضع شروط وضوابط للتفتيش، مثل تحديد الميعاد المناسب لتنفيذه، الحصول على إذن قضائي قبل البدء

(١)عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والانترانت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا، ط٠١، منشورات الحلبي الحقوقية، لبنان، ٢٠٠٧، ص ٤٧.

في التفتيش، وضمان حضور المعني أو توفير وسيلة لحمايته في حالة عدم الحضور الشخصي، فهذه الضوابط تسعى إلى تحقيق توازن بين حقوق الأفراد والحاجة إلى مكافحة الجريمة وحماية المجتمع، يمكن أن تسهم هذه الإجراءات في تحقيق العدالة وضمان تطبيق القوانين بطريقة عادلة وفعّالة في عالم متزايد التكنولوجيا[1].

ويجب أن يكفل المشرع للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، وذلك قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

هذا وقد نصت الاتفاقية العربية لمكافحة الجريمة المعلوماتية على التفتيش الإلكتروني سيما جاء في ٢٦ منها، حيث تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها؛ بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه، وتظهر

(١)عبد الفتاح حجازي، مكافحة جرائم الكمبيوتر والانترنت، دراسة معمقة في القانون ألمعلوماتي، ط٠١، دار الفكر الجامعي، الإسكندرية،٢٠٠٦، ص١٤.

هذه المواد من الاتفاقية العربية لمكافحة الجريمة المعلوماتية أهمية وجود إطار قانوني للتفتيش الإلكتروني، ويتضح بوضوح التزام الدول الطرف باتخاذ الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى التقنيات والمعلومات المعينة، وينص على أهمية التعاون الدولي في هذا السياق، وهذه النصوص لا شك تسعى للتأكيد على الضرورة الملحة لتطوير القوانين والإجراءات لمكافحة الجرائم المعلوماتية، وتعزيز التعاون بين الدول لمواجهة هذه التحديات الحديثة.

ومن ناحية أخرى، ونظراً لخصوصية التفتيش والضبط في مجال الجرائم الإلكترونية، فإن المشرع من الضروري أن يجيز للجهة المكلفة بالتفتيش الاستعانة بذوي الخبرة من مقدمي خدمة الإنترنت، وهذا وقد نصت الاتفاقية العربية لمكافحة الجريمة المعلوماتية على مسالة ضبط المعلومات المخزنة حسب نص المادة ٢٧ التي جاء فيها أنه : ١ - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقرة (١) من المادة السادسة والعشرين من هذه الاتفاقية .. هذه الإجراءات تشمل صلاحيات :

أ) ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات ؛

ب) عمل نسخة من معلومات تقنية المعلومات والاحتفاظ بها؛

ج) الحفاظ على سلامة معلومات تقنية المعلومات المخزنة؛

د) إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها.

٢ – تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية المعلومات أو الإجراءات المطبقة لحماية تقنية المعلومات من أجل تقديم المعلومات الضرورية لإتمام تلك الإجراءات المذكورة في الفقرتين ٢ و١ من المادة السادسة والعشرين من هذه الاتفاقية».

غير أنه يجوز لها استعمال وسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

وجدير بالذكر أن من بين الإجراءات المهمة التي لم ينص عليها قانون مكافحة جرائم تقنية المعلومات الكويتي إجراء مراقبة الاتصالات الإلكترونية أو ما يعرف بالترصد الإلكتروني، إذ يعد الترصد الإلكتروني أحد الأدوات الرئيسية التي تستخدمها السلطات لمراقبة الاتصالات الإلكترونية وجمع المعلومات ذات الصلة بالجرائم المعلوماتية والأنشطة ذات الصلة، يمكن أن تتضمن هذه الأنشطة تحديد

هوية الأفراد، ومتابعة تحركاتهم عبر الإنترنت، ورصد التفاعلات الإلكترونية.

إلا أنه من الضروري التشدد على أهمية توازن بين الحاجة إلى حماية المجتمع وأمن السيبراني، وحقوق الأفراد في الخصوصية والحرية الشخصية. حيث أن تنظيم مثل هذه الإجراءات يتطلب عادة قوانين صارمة وآليات فعالة للرقابة والتحكم، ويجب أن يتم وفقًا لمعايير دولية ومحلية تحفظ حقوق الأفراد وتمنح السلطات اللازمة للتصدي للجرائم بشكل فعال.

الفرع الثالث

التعاون الدولي ضرورة حتمية في مجال مكافحة الجرائم الإلكترونية

يعتبر التعاون الدولي أمرًا حيويًا لمواجهة هذا النوع من الجرائم الذي يتجاوز الحدود الوطنية، التعاون الدولي يشمل مجموعة من الجوانب، مثل تبادل المعلومات، والمساعدة في التحقيقات، وتقديم المساعدة القانونية الدولية، حيث يسهم هذا التعاون في زيادة فعالية التحقيقات والمحاكمات وتحقيق العدالة.

وتشير العديد من الاتفاقيات والمعاهدات الدولية إلى أهمية التعاون الدولي في مكافحة الجرائم الإلكترونية، على سبيل المثال، يشدد البعض منها على ضرورة تبادل المعلومات بين الدول وتوفير الدعم القانوني عبر الحدود، يجب على الدول أن تضع آليات وإجراءات لتسهيل هذا التعاون وضمان فعاليته.

وإذا كان قانون مكافحة جرائم تقنية المعلومات في الكويت لا يشير بوضوح إلى قضايا التعاون الدولي، قد يكون من الملائم تعديل القانون ليتناسب مع متطلبات

التعاون الدولي ومكافحة الجرائم المعلوماتية على الساحة الدولية.

وتعتبر الاتفاقات الدولية وسيلة أساسية في مجال مكافحة جرائم تقنية المعلومات، حيث تعمل على توحيد الجهود الدولية لهذا الغرض، وتبرز دور الأمم المتحدة كمركز لتنسيق الجهود بين الدول. يظهر ذلك بوضوح من خلال مجموعة من القرارات والتوصيات والاتفاقيات الدولية، منها:

أ- قرار هافانا ١٩٩١ الناتج عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء.

ب- انعقاد المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات في البرازيل ١٩٨٤".

ج- اتفاقية بودابست ٢٠٠١ لمكافحة الجرائم المعلوماتية.

د- الاتفاقية العربية التي خصصت العديد من المواد لتنظيم مسالة التعاون الدولي بين جميع الدول الأطراف وتبادل المساعدة فيما بينها بأقصى مدى يمكن لغايات التحقيقات، أو الإجراءات المتعلقة بجرائم معلومات وتقنية المعلومات أو لجمع الأدلة الإلكترونية في الجرائم[1].

(١) الفصل الرابع من الاتفاقية.

الخاتمة

في ختام بحثنا، يظهر أن الجريمة الإلكترونية تمثل تحديًا حديثًا ومتقدمًا وغير تقليدي، مما يستدعي الحاجة إلى وضع تشريعات جنائية توفر الحماية الكافية من خلال إيجاد آليات جديدة تتلاءم مع طبيعتها، خاصة في الجانب الإجرائي. وفي هذا السياق، يمكن اتخاذ الإجراءات التالية:

١- توحيد الجهود لعقد مؤتمر دولي: العمل على تكامل الجهود الدولية من أجل عقد مؤتمر دولي يهدف إلى صياغة قانون موحد لمعالجة جرائم المعلوماتية، تحت رعاية الأمم المتحدة.

٢- الاعتماد على مبدأ العالمية: اعتماد مبدأ العالمية نظرًا لطبيعة الجرائم المعلوماتية التي تتجاوز الحدود، والنظر في كيفية تكامل هذا المبدأ في التشريعات الجنائية.

٣- تزويد الضبطية القضائية بوسائل تقنية متقدمة: منح الضبطية القضائية وسائل تقنية متقدمة، مع التركيز على التدريب والتأهيل المستمر، واستخدام الخبرات الفنية في التحقيقات.

٤- إنشاء هيئات وطنية وإقليمية وعالمية: إنشاء هيئات متخصصة على مستوى وطني وإقليمي وعالمي لتنسيق الجهود والعمل على الوقاية من هذه الجرائم.

٥- تأهيل وتكوين القضاة: تأهيل وتكوين قضاة متخصصين في جرائم المعلوماتية وإقامة محاكم مختصة في هذا المجال.

٦- تعزيز التعاون الدولي: تفعيل التعاون الدولي من خلال توقيع وتنفيذ المزيد من الاتفاقيات الدولية على المستوى الإقليمي والعالمي.

٧- تفعيل دور الأسرة والمجتمع: دور أساسي للأسرة في متابعة وحماية الأبناء من مخاطر الإنترنت، بالإضافة إلى توعية المجتمع المدني ووسائل الإعلام للمساهمة في الحد من هذه الجرائم.

رغم أن قانون مكافحة جرائم تقنية المعلومات الكويتي يُعد بحق من أكثر القوانين التي حاولت التطرق لمختلف صور جريمة الإلكترونية، إلا أننا نأمل من المشرع الكويتي أن يأخذ بعين الاعتبار التوصيات التالية: -

١- تعديل النصوص القانونية: يجب تحديث وتعديل النصوص القانونية لتغطية جميع جوانب الجرائم الإلكترونية وضمان عدم وجود ثغرات قانونية. هذا يساهم في تعزيز فعالية القانون وتحسين الحماية من التحديات الجديدة في مجال التكنولوجيا.

٢- توسيع نطاق الجرائم الإلكترونية: يمكن تعزيز القانون بتوسيع نطاق الجرائم الإلكترونية ليشمل تصميم وصنع واتجار بالمعطيات والبرامج المستخدمة في الجرائم الإلكترونية. هذا يضمن تغطية جميع الجوانب ذات الصلة.

٣- النص على الجوانب الإجرائية: يجب أن يشمل القانون نصوصًا واضحة حول الجوانب الإجرائية للجرائم الإلكترونية، مثل الاختصاص القضائي، والتفتيش

الإلكتروني، والأدلة الإلكترونية، والترصد الإلكتروني. ذلك يسهم في توفير إجراءات فعالة لمكافحة ومعالجة هذه الجرائم.

٤- إنشاء هيئة للوقاية والمكافحة: إنشاء هيئة أو جهاز خاص للوقاية من الجرائم الإلكترونية ومكافحتها يعزز التركيز على هذا النوع من الجرائم ويسهم في تطوير استراتيجيات الوقاية والردع.

٥- تدريب قضاة متخصصين: يجب توفير برامج تدريب متخصصة للقضاة لتمكينهم من التفاعل بفعالية مع قضايا الجرائم الإلكترونية. هذا يسهم في ضمان صدور أحكام قضائية متسقة وعادلة.

إذا تم تنفيذ هذه الاقتراحات، فإنها قد تعزز التشريع القائم وتعزز قدرته على التعامل مع التحديات الحديثة في مجال التكنولوجيا والجريمة الإلكترونية سيما التغلب على إشكالية الملاحقة الجزائية في الجرائم الإلكترونية.

فهرس المحتويات