الجامعة العربية الأمريكية

كلية الدراسات العليا

قسم العلوم القانونية

برنامج الماجستير في العلوم الجنائية

مكافحة الجريمة الإلكترونية
(دراسة في ظل التشريع الفلسطيني والإتفاقيات الدولية)

محمد باسم إبراهيم الخالدي

202113518

أسماء لجنة الإشراف:

د. علاء خلايلة

د. أحمد الأشقر

د. محمود الشيخ

تم تقديم هذه الرسالة استكمالًا لمتطلبات درجة الماجستير في تخصص العلوم الجنائية

فسطين، 2025/1

لجامعة العربية الأمريكية

كلية الدراسات العليا

قسم العلوم القانونية

برنامج الماجستير في العلوم الجنائية

صفحة إجازة الرسالة

مكافحة الجريمة الإلكترونية

(دراسة في ظل التشريع الفلسطيني والإتفاقيات الدولية)

محمد باسم إبراهيم الخالدي

202113518

نوقشت هذه الرسالة وأجيزت بتاريخ 15.1.2025 من لجنة المناقشة التالية أسماؤهم وتواقيعهم:

الإسم :		التوقيع
1.د. علاء خلايلة	المشرف الرئيس	.....
2.د. أحمد الأشقر	عضو لجنة الرسالة	.....
3.د. محمود الشيخ	عضو لجنة الرسالة	.....

فلسطين، 1 /2025

الإقرار

انا الموقع أدناه مقدم الرسالة الموسومة:

مكافحة الجريمة الإلكترونية
(دراسة في ظل التشريع الفلسطيني والإتفاقيات الدولية)

أقر بأن ما اشتملت عليه الرسالة إنما هو نتاج جهدي الخاص، بإستثناء ما تمت الاشارة إليه حيثما ورد، وإن هذه الرسالة ككل، أو جزء منها لم يقدم من قبل لنيل درجة علمية أو بحث لدى أي مؤسسة تعليمية أو بحثية اخرى.

إسم الطالب: محمد باسم ابراهيم الخالدي

الرقم الجامعي: 202113518

التوقيع:

تاريخ تسليم النسخة النهائية من الرسالة: 2025/04/13م

الإهداء

إلى أرواحٍ ارتقت في ربوع الوطن كله "خاصة غزة المنبت والديار" التي تطل علينا من عليائها كل مساء لتذكرنا أن الشهداء لا يموتون بل يمهدون طريقة الحرية والعودة والاستقلال

إلى قدوتي وسندي وصديقي أبي حفظه الله وبارك في عمره

إلى سيدة نساء الأرض من كانت ولم تزل نبراس حياتي والدتي الحبيبة حفظها الله

إلى شريكة الأمل ورحلة الحياة، ملهمتي الداعمة والمحفّزة إلى دروب العلا/ زوجتي الغالية

إلى قرّة عيني وأملي المتجدد ونبض القلب صغيرتي سما

إلى إخوتي الأحبة كرم ومجد السند والعضد المتين

إلى من حملوا هموم الوطن ورسموا الطّريق للسّمو بمؤسّساتنا التّعليمية في فلسطين

إلى جميع الأحبّة من الأهل والأصدقاء وزملاء الدّراسة الدّاعمين، وجميع محبّي العلم والمعرفة

إلى دكتوري الفاضل صاحب الفضل الكبير الدّكتور القدير علاء خلايلة

إلى كل هؤلاء في وطني الغالي الذي لم يزل رغم الظلم و محاولات طمس هويته على موعد مع فجر الحرية والانعتاق أهدي ثمرة جهدي المتواضع.

الباحث: محمد باسم ابراهيم الخالدي.

الشكر والتقدير

الحمد لله والصلاة والسلام على رسولنا الكريم صلى الله عليه وسلم

أتقدم بالشكر والعرفان إلى:

أستاذي الفاضل الدكتور علاء خلايلة الذي أشرف على رسالتي ومد لي يد العون بالنصح والإرشاد وتقديم الأفكار السديدة.

كما أتقدم بجزيل الشكر إلى الأساتذة عضوي لجنة المناقشة الكريمين:

د.أحمد الاشقر

د.محمود الشيخ

على كل ما بذلاه من وقت وجهد في سبيل تقويم هذه الرسالة، وهم الأقدر على تصويب اعوجاجها.

لا أنسى توجيه الشكر لكل من دعمني وشجعني وقدم لي المساعدة والجهد؛ لإخراج هذه الرسالة بالطريقة الصحيحة.

فجزاهم الله كل خير،،،

الباحث: محمد باسم ابراهيم الخالدي.

مكافحة الجريمة الإلكترونية

(دراسة في ظل التشريع الفلسطيني والإتفاقيات الدولية)

محمد باسم إبراهيم الخالدي

د. علاء خلايلة

د. أحمد الأشقر

د. محمود الشيخ

ملخص

تناولت الرسالة موضوع مواءمة التشريع الجزائي الفلسطيني مع الاتفاقيات الدولية لمكافحة الجريمة الإلكترونية، وتأتي أهمية هذا الموضوع نتيجةً للتوسع في استخدام الشبكة العنكبوتية وازدياد أعداد المستخدمين لها، أصبح الإنترنت وسطاً ملائماً لتخطيط وتنفيذ عدداً من الجرائم، والتي عرفت فيما بعد باسم الجرائم الإلكترونية ،لقد أدرج المشرع الفلسطيني القرار بقانون رقم (10) لعام 2018م بشأن الجرائم الإلكترونية، ليعتبر تشريعاً خاصاً لمكافحة الجريمة الإلكترونية ووضع حد لها، بحيث يكون قادراً على تكييف الجرائم الإلكترونية لحماية الحقوق المنتهكة ومتلائماً مع التشريعات الدولية ذات العلاقة، لذلك ناقشت الرسالة مفهوم الجرائم الإلكترونية وخصائصها والمفاهيم ذات الصلة المرتبطة بها، والتنظيم القانوني للجرائم الإلكترونية، ونظراً لما تثيره الجرائم الإلكترونية من المشكلات الإجرائية من الناحية القانونية والعملية، فقد تناولت الرسالة الإجراءات القانونية المتبعة في مكافحة الجريمة الإلكترونية على المستوى الدولي والإقليمي وكذلك الوطني، ثم مسألة الإثبات الجنائي في الجرائم الإلكترونية الكلمات المفتاحية: مواءمة، الجرائم الإلكترونية، الإتفاقيات الدولية، التشريع الجزائي، الإثبات الإلكتروني.

فهرس المحتويات

المقدمة

مع بزوغ فجر الثورة التكنولوجية وما شهده العالم من ثورة في التطور الهائل والسريع في مختلف جوانب الحياة وعلى رأسها تكنولوجيا المعلومات والاتصالات، ظهرت تقنيات عالية مثل: أجهزة الكمبيوتر، والهواتف الذكية، والبرمجيات وشبكة الإنترنت والمواقع الإلكترونية، وما أحدثت تلك التقنيات والتطورات من تسهيل الاتصال وطرق تنقل الأفراد والسع ورؤوس الأموال بين الدول، حتى أظهرت العولمة العالم وكأنه قرية صغيرة[1].

ويعد الإنترنت من أكبر شبكات الكمبيوتر ذات الارتباط الوثيق بالجرائم الإلكترونية؛ شبكة تربط مجموعة من الأجهزة الإلكترونية المتصلة ببعضها البعض ويمكن لها تبادل المعلومات فيما بينها[2]. وهو ما يدعو إلى ضرورة تنبيه الدول إلى المخاطر الكبيرة التي تشكلها هذه الجرائم التي تتطور بشكل سريع، لدرجة أن بعض أنواعها أصبحت تتميز بدرجة عالية من الخطورة والتعقيد، ومن أبرزها الجريمة المنظمة العابرة للحدود الوطنية[3].

ونشير هنا إلى صعوبة التحديد الدقيق لبداية ظهور الجريمة الإلكترونية، غير أن هناك من يرجح أن البداية الحقيقية لظهور الجريمة الإلكترونية تعود إلى عام 1958، وذلك مع رصد معهد

---

[1] العولمة: مصطلح يعني تسارع وتكثيف آليات وعمليات ونشاطات، ومن الممكن أن تعزز التبعية العالمية المتبادلة، وربما الاندماج السياسي والاقتصادي العالمي في النهاية، وتحمل العولمة بعض السمات التي يمكن التعرف إليها، على الرغم من عدم وجود إجماع في هذا المجال حول أي من هذه السمات، وتتضمن العولمة أولاً إدراكاً متزايداً لكون العالم مكاناً واحداً. وينعكس هذا الأمر في جمل مثل القرية العالمية والاقتصاد العالمي. للمزيد أنظر: مارتن غريفتش وتيري أوكالاهان، المفاهيم الأساسية في العلاقات الدولية، مركز الخليج للأبحاث، دبي، الإمارات العربية المتحدة، 2008، ص361.

[2] محمد عبيد الكعبي، الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت دراسة مقارنة، دار النهضة العربية، ط2، القاهرة، 2009، ص20.

[3] Finckenauer, J.O. "Problems of definition: What is organized crime?", First edition, By Routledge, USA, NewYork, 2005, P:34

ستانفورد الدولي للأبحاث في الولايات المتحدة الأمريكية وبصورة منظمة لما كان يعرف في ذلك الوقت بإساءة استخدام الحاسوب[1].

وهناك العديد من الأسباب التي يمكن حصرها كأسباب للجريمة الإلكترونية، منها ما يقع على مستوى كوني، ومنها ما يقع على مستوى مجتمعي، ومنها ما يقع على مستوى فردي أو شخصي، كما أن أسباب الجريمة الإلكترونية تتفاوت وفق نوعها ونوع المستهدف ونوع الجاني ومستوى تنفيذه (فردي، مجتمعي، كوني)[2].

ودراسة الدوافع وراء ارتكاب الجريمة الإلكترونية له فائدة مزدوجة، فهي تساعد في إيجاد الحلول المناسبة في إطار مكافحة الجريمة الإلكترونية والتغلب عليها، كما يسهم ذلك في تحديد التكييف القانوني الذي قد تضيفه تلك الدوافع عليها. فقد يكون الدافع لارتكاب الجريمة الإلكترونية يتمحور في السعي وراء الربح، وقد يكون دافعاً سياسياً، كما قد يكمن الدافع في الرغبة في تحدي النظام التقني المعلوماتي[3].

وتزامنا مع تطور صناعة الحاسبات الإلكترونية، فقد أصبحت الطريقة الميكانيكية المتبعة سابقاً غير قادرة على القيام بالعمليات المتطورة، ولذلك تم تطوير جهاز الكمبيوتر والهواتف النقالة، والذي شمل تغيير وحدة المعالجة المركزية والذاكرة[4].

---

[1] مجمع البحوث والدراسات، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، أكاديمية السلطان قابوس لعلوم الشرطة، جامعة نزوى، سلطنة عمان، 2016، ص25.

[2] ذياب البداينة، الجرائم الإلكترونية: المفهوم والأسباب، كلية العلوم الإستراتيجية، كلية الشرطة، وزارة الداخلية، قطر، 2014، ص9 وما بعدها.

[3] سعد فهد سعد ادبيس المطيري، مفهوم الجرائم الإلكترونية وسماتها، المجلة القانونية، العدد 5، المجلد 16، جامعة القاهرة، كلية الحقوق، فرع الخرطوم، 2023، ص1254.

[4] عبير بعقيبي، مكافحة الجريمة المعلوماتية في التشريعين الجزائري والإماراتي–دراسة مقارنة– أطروحة دكتوراه، كلية الحقوق، جامعة محمد خيضر، بسكرة، الجزائر، 2018، ص11.

لذلك تقدم وكالات إنفاذ القانون الدولية مثل اليوروبول والإنتربول، والمنظمات الإقليمية مثل الاتحاد الأفريقي ومنظمة الدول الأمريكية معلومات حول اتجاهات الجريمة الإلكترونية والأمن السيبراني، ويمكن أيضًا تحديد هذه الاتجاهات للجريمة الإلكترونية من التقارير السنوية أو البيانات التي يتم تحليلها من مختلف أدوات قياس الجريمة الرسمية واستقصاءات الإيذاء[1]. ويوفر اليوروبول (2018) العديد من التوعية العامة وأدلة الوقاية[2].

واستناداً لكل ما سبق، بدء العالم يشهد ومنذ سبعينيات القرن المنصرم، ظهور بعض التشريعات والقوانين التي تجرم بعض الممارسات المتعلقة بإساءة استخدام الحاسوب وحددت لها العقوبات اللازمة، كما هو الحال في السويد التي تعتبر أول دولة تصدر قانوناً يجرم بعض الأفعال المتعلقة بإساءة استخدام الحاسوب[3].

---

[1] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، على الرابط التالي:
https://www.unodc.org/e4j/ar/cybercrime/module-1/key-issues/cybercrime-trends.html، تاريخ الإطلاع: 2024/5/9، على الساعة 6:00 مساءاً.

اليوروبول: هي وكالة إنفاذ القانون للاتحاد الأوروبي، هدفها هو المساعدة في تحقيق أوروبا أكثر أمانا من خلال دعم وكالات إنفاذ القانون في أوروبا، وتهدف الدول الأعضاء فيها إلى مواجهة الجرائم الدولية الخطيرة والإرهاب. أنظر الموقع الرسمي لليوروبول: http://www.europol.eurpa.eu، تاريخ الإطلاع: 25\9\2024، على الساعة 7:00 مساءاً.

الإنتربول: وهي المنظمة الدولية للشرطة الجنائية، تهدف إلى تأمين وتنمية التعاون المتبادل على أوسع نطاق بين كافة سلطات الشرطة الجنائية، وذلك في إطار القوانين القائمة في مختلف البلدان وبروح الإعلان العالمي لحقوق الإنسان، و إنشاء وتنمية كافة المؤسسات القادرة على المساهمة الفعالة في الوقاية من جرائم القانون العام وفي مكافحتها. أنظر: القانون الأساسي للمنظمة الدولية للشرطة الجنائية (الإنتربول).

الاتحاد الإفريقي: تأسس عام 2002 ومقره في أديس أبابا، يضم 55 دولة ويهدف إلى معالجة القضايا السياسية والإجتماعية والاقتصادية وتعزيز التنمية والتكامل في عموم إفريقيا. للمزيد أنظر الموقع الرسمي للإتحاد على الرابط التالي: https://au.int/en/overview، تاريخ الإطلاع: 25\9\2024، على الساعة7:30 مساءاً.

منظمة الدول الأمريكية: هي منظمة إقليمية تأسست عام 1889، وتضم دول الأميركتين الشمالية والجنوبية في إطار الإمم المتحدة، وتسعى إلى خلق نوع من التضامن والتقارب والتعاون بين الدول الأعضاء فيها، ونشر وترسيخ الديمقراطية بين البلدان الأعضاء، والدفاع عن مبادئ حقوق الإنسان، وتكريس مقاربة أمنية متعددة الجوانب، ودعم التعاون الإقليمي بين بلدان المنظمة.

[2] الموقع الرسمي لليوروبول على الرابط التالي: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides، تاريخ الإطلاع: 2024/5/9، على الساعة 5:00 مساءاً.

[3] عبد الله حسين القحطاني، تطوير مهارات التحقيق الإلكتروني في مواجهة الجرائم المعلوماتية دراسة تطبيقية في هيئة التحقيق والإدعاء العام في مدينة الرياض، رسالة ماجستير، الرياض، السعودية، 2014، ص30.

وقد سارعت العديد من دول العالم إلى بذل الجهود المضنية لعقد العديد من الاتفاقيات والمؤتمرات الدولية المتعلقة بالجرائم الإلكترونية، ودعت إلى تجريم الجرائم الإلكترونية، وذلك بهدف تعزيز التعاون الدولي لدرء مخاطر هذه الجرائم وذلك في سبيل الحفاظ على الأمن والنظام العام وإنشاء بيئة مستقرة عبر الإنترنت محلياً وإقليمياً ودولياً.

وتماشياً مع الجهود الدولية لمواجهة تحديات الجرائم الإلكترونية، وفي إطار الدعوة الدولية للتعاون الدولي لمكافحة الجرائم الإلكترونية من خلال سن القوانين والتشريعات التي من شأنها مواجهة تلك الجرائم والحد منها، أدرج المشرع الفلسطيني تشريعياً خاصاً لمكافحة الجريمة الإلكترونية ووضع حد لها، فجاء القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات رقم 10 لسنة 2018 وتعديلاته. وذلك تماشياً مع القانون الأساسي الفلسطيني، وتحقيقاً للمصلحة العامة.

أهمية الدراسة

تأتي أهمية الدراسة إنطلاقاً من أهمية التحديات الأمنية والتقنية والقانونية المرافقة لاستخدامات التقنيات الإلكترونية، وذلك على اعتبار أن الجريمة الإلكترونية تتسم بالمرونة والتطور المستمر في مختلف المجالات.

وكذلك اعتباراً لمدى خطورة الجرائم الإلكترونية على البنيات التحتية لأنظمة المعلومات والاتصالات وتهديد الاختراقات لمؤسسات القطاع العام والخاص وحتى للأفراد.

وكذلك قدرة التشريع الفلسطيني على تكييف الجرائم الإلكترونية لحماية الحقوق المنتهكة استناداً إلى القوانين الخاصة المستحدثة والمتعلقة بالجرائم الإلكترونية. كما تتضح أهمية البحث في موضوع

الدراسة من خلال النظر في مدى ليونة المشرع الفلسطيني لمواءمة التشريعات القانونية الفلسطينية المتعلقة بالجرائم الإلكترونية مع التشريعات الدولية ذات العلاقة.

أهداف الدراسة

تهدف الدراسة إلى التعريف بماهية الجرائم الإلكترونية، وبيان مدى خطورة الجرائم الإلكترونية على المستوى المحلي والإقليمي والدولي، وكذلك التحديات التي قد تحول دون فاعلية التشريعات والقوانين سواء على الصعيد المحلي أو على الصعيد الدولي. ثم تسليط الضوء على قانون مكافحة الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات الفلسطيني رقم (10) لسنة 2018م وتعديلاته، باعتباره قانوناً حديثاً نسبياً، كما تهدف الدراسة إلى التعمق في كيفية مجابهة الجرائم الإلكترونية في المجتمع الفلسطيني من خلال سن القوانين والتشريعات التي يراعى فيها الاتفاقيات الدولية المختصة. وبالتالي تهدف الدراسة إلى التأكيد على ضرورة التعاون الإقليمي والدولي لمواجهة الجريمة الإلكترونية.

أسباب اختيار الموضوع

للباحث رغبة كبيرة للبحث في موضوع الدراسة؛ وذلك نظراً لأهمية موضوع الجرائم الإلكترونية وحداثته في المجتمع الفلسطيني، وكذلك، لندرة الأبحاث حول مسألة مواءمة التشريع الفلسطيني مع الاتفاقيات الدولية المتعلقة بالجرائم الإلكترونية، وبالتالي فإن الباحث يطمح إلى تقديم رؤية قانونية متكاملة حول الجرائم الإلكترونية في ظل التشريع الفلسطيني والاتفاقيات الدولية.

دراسات سابقة

استندت الدراسة إلى مجموعة من الدراسات الحديثة التي تناولت موضوع الجريمة الإلكترونية، ووقفت على مفهومها وخصائصها وأركانها وأضرارها الاجتماعية والاقتصادية وسبل مواجهاتها والحد منها على المستوى الدولي والآخر الوطني، ومنها على سبيل المثال لا الحصر نذكر منها:

1- مصطفى عبد الباقي، التحقيق في الجرائم الإلكترونية وإثباتها في فلسطين: دراسة مقارنة، دراسات علوم الشريعة والقانون، الجامعة الأردنية، الأردن، المجلد 45، العدد 4، 2018.

2- سعد فهد سعد ادبيس المطيري، مفهوم الجرائم الإلكترونية وسماتها، المجلة القانونية، جامعة القاهرة، كلية الحقوق، فرع الخرطوم، العدد 5، المجلد 16، 2023.

3- عبير بعقيبي، مكافحة الجريمة المعلوماتية في التشريعين الجزائري والإماراتي-دراسة مقارنة-، أطروحة دكتوراه، كلية الحقوق، جامعة محمد خيضر، بسكرة، الجزائر، 2018.

4- نايف شافي المظافرة الهاجري، جرائم تقنية المعلومات في التشريع الأمريكي مقارنة بالتشريعات العربية، مجلة البحوث القانونية والاقتصادية، المنصورة، العدد 83، مارس، 2023.

وتميزت هذه الدراسة عن غيرها من الدراسات السابقة كونها ناقشت مقتضيات القرار بقانون رقم (10) لسنة 2018م وتعديلاته ومدى ملائمته مع الاتفاقيات الدولية والإقليمية، في ظل تطور الجريمة الإلكترونية وتنوع أساليب ارتكابها وتزايد مخاطرها وحجم الخسائر الناجمة عنها، حتى باتت تشكل تهديداً للإقتصاد والأمن الوطني.

إشكالية الدراسة

إلى أي حد كان المشرع الفلسطيني موفقاً في مكافحة الجريمة الإلكترونية في ضوء الاتفاقيات الدولية ذات العلاقة؟

ويتفرع عن إشكالية الدراسة الرئيسة مجموعة من الأسئلة الفرعية التي يمكن طرحها على الشكل التالي:

أسئلة الدراسة

1- ما هي ماهية الجرائم الإلكترونية؟

2- ماهو الإطار القانوني الناظم للجرائم الإلكترونية على المستوى الدولي والوطني؟

3- ما هي السياسة العقابية المتبعة في محاربة الجريمة الإلكترونية؟

4- ما هي الإجراءات القانونية المتبعة في مكافحة الجريمة الإلكترونية؟

5- ماهي الخصوصية التي تتمتع بها الجرائم الإلكترونية عن الجرائم التقليدية؟

6- ماهي التحديات التي تواجه المشرع الفلسطيني في مواجهة الجرائم الإلكترونية؟

7- ما هي الاجراءات الخاصة التي فرضها المشرع الفلسطيني بشأن الجرائم الالكترونية للسير في الدعوى الجزائية المترتبة على هذه الجريمة؟

منهج الدراسة

اعتمد الباحث في دراسته على المنهج الوصفي التحليلي والمنهج المقارن للوقوف على النصوص القانونية ذات الصلة بالجرائم الإلكترونية والاتفاقيات الدولية.

فرضية الدراسة

لغرض الإجابة عن إشكالية الدراسة والأسئلة الفرعية المتعلقة بها، ينطلق الباحث من فرضية رئيسة مفادها: أن الجريمة الإلكترونية تشكل ظاهرة عالمية عابرة للحدود ونوع مختلف عن أشكال الجرائم الأخرى التي تهدد أمن المجتمعات، لذلك لا بد من إدماج ما توصلت إليه الجهود الدولية في سبيل الحد من سلبيات ومخاطر ظاهرة الجريمة الإلكترونية في القوانين والتشريعات الداخلية، وبالتالي معالجة أي قصور تعاني منه القوانين الداخلية للإحاطة بكافة جوانب ظاهرة الجريمة الإلكترونية.

تقسيم الدراسة

ولغرض الإحاطة بكافة جوانب الموضوع، وسعياً للإجابة عن الإشكالية المطروحة، ارتأى الباحث تقسيم الموضوع إلى فصليين رئيسيين:

الفصل الاول: السياسة العقابية المتبعة في محاربة الجريمة الإلكترونية

الفصل الثاني: الإجراءات القانونية المتبعة في مكافحة الجريمة الإلكترونية

الفصل الاول: السياسة العقابية المتبعة في محاربة الجريمة الإلكترونية

مع توسع شبكة الإنترنت وامتدادها وازدياد عدد الجرائم الإلكترونية وتعدد صورها وأشكالها، الشيء الذي جعل الإنترنت نموذجاً للإجرام فيه ثغرات قانونية، فقد توسعت الجريمة الإلكترونية وامتدت لتشمل العديد من الأفعال الإجرامية كالتشهير والنصب والاحتيال وغيرها من الجرائم.

وقد تأخر المشرعون في إصدار القوانين التي من شأنها مواجهة الجرائم الإلكترونية، وبالرغم من أن بعض الدول كانت سباقة لسن قوانين للوقاية من مخاطر الجريمة الإلكترونية، فمعظم الدول استشعرت خطورة هذه الجريمة بعد استفحالها، وبدأت العمل على تحصين قوانينها، ولذلك تعتبر أغلب التشريعات المتعلقة بمكافحة الإجرام الإلكتروني حديثة نسبيا.

إذ عملت جل الدول على ملاءمة قوانينها بما يتناسب مع طبيعة الجريمة الإلكترونية، وسداً للقصور الذي كان يعانيه القضاء في مكافحة الجريمة الإلكترونية بالنصوص القانونية التقليدية، وهي ملاءمة مخالفة لمبدأ الشرعية، باعتباره مبدأ يحقق الحماية لحقوق المتهم من تجريمه على أفعال وعقابه بعقوبات لم ينص عليها القانون.

لذلك ونتيجةً لحداثة الجرائم الإلكترونية وارتباطها بالتطور التكنولوجي واعتباراً لطبيعتها العابرة للحدود وإمكانية ارتكابها في دولة ما وإحداث نتائجها في دولة أخرى، وكذلك سرعة وسهولة إخفاء أدلتها، فلكل هذا التداخل، كان من الأهمية بمكان دراستها ومواجتها، فقد تناول الباحث في الفصل الأول الحديث حول مفهوم الجرائم الإلكترونية، وتوضيح أركانها وتبيان خصائصها، حيث تطرق في المبحث الأول إلى ماهية الجريمة الإلكترونية.

ولتحقيق نتائج إيجابية في مكافحة الجرائم العابرة للحدود، والتي تمثل الجريمة الإلكترونية أحد صورها، كان على المجتمع الدولي أن يخلق نوع من التعاون الدولي في مكافحتها؛ وذلك لأن توافق

التشريعات والسياسات الجنائية الوطنية مع التشريعات والسياسات الجنائية الدولية يعتبر مقدمة طبيعية لتحقيق تلك النتائج الإيجابية. وعليه، فقد تناول الباحث هذا الجانب من خلال التطرق في المبحث الثاني إلى التنظيم القانوني الخاص للجريمة الإلكترونية.

المبحث الأول: ماهية الجريمة الإلكترونية

انطلاقاً من التطور التاريخي الذي عرفته الجريمة الإلكترونية وما ساهمت به من إنتاج السلوكيات التي تعد إجراماً وفقاً لقواعد وقوانين التجريم، وما أحدثه ذلك من أثر في كافة مناحي الحياة الإنسانية، لذلك فقد كان مفهوم الجريمة الإلكترونية محلاً لاجتهادات فقهية وقانونية كثيرة، إذ تميزت هذه الجريمة بمجموعة من الخصائص التي تميزها عن غيرها من الجرائم التقليدية، وهو ما يدعو إلى تبيان أركان الجريمة الإلكترونية وصورها.

وقد ارتأى الباحث بدايةً تناول هذا المبحث من خلال التطرق إلى مفهوم الجريمة الإلكترونية (المطلب الأول)، مروراً بخصائص الجريمة الإلكترونية (المطلب الثاني)، وصولاً إلى أركان الجريمة الإلكترونية (المطلب الثالث).

المطلب الأول: مفهوم الجريمة الإلكترونية

مع تطور وسائل الاتصالات والمعلومات في العصر الحديث وارتباطها بأجهزة الكمبيوتر والإنترنت وما نتج عنه من جرائم غير مسبوقة، أصبح لزاماً على الفقه والقانون تبيان مفهوم الجريمة الإلكترونية. ونشير هنا إلى أن الفقه الجنائي لم يتفق على تسمية موحدة للجريمة الإلكترونية[1]،

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، ط1، 2008، ص46.

فالبعض يطلق عليها الجريمة المعلوماتية، وآخرون يطلقون عليها مسمى جرائم الكمبيوتر والإنترنت، إلا أن العديد من الاتفاقيات الدولية والتشريعات الوطنية قد اعتمدت مصطلح الجريمة الإلكترونية، وهو المصطلح الذي سيعتمده الباحث في هذه الرسالة.

ووفقاً لهذا المطلب، سنتطرق إلى تناول مفهوم الجريمة الإلكترونية من خلال تناول المفهوم الفقهي للجريمة الإلكترونية (الفرع الأول)، ثم تناول المفهوم القانوني للجريمة الإلكترونية (الفرع الثاني).

الفرع الأول: المفهوم الفقهي للجريمة الإلكترونية

إن تحديد مفهوم الجريمة الإلكترونية كان محل اجتهاد الفقهاء، فقد نتج عن ذلك مذاهب مختلفة وضعت تعريفات عديدة لمفهوم الجريمة الإلكترونية، لذلك فلا نجد معياراً محدداً متفقا عليه لبيان مفهوم الجريمة الإلكترونية، إذ إن بعض الفقهاء تناول مفهوم الجريمة الإلكترونية من الناحية التقنية أو الفنية، والبعض الآخر تناول مفهوم الجريمة الإلكترونية من الناحية الاصطلاحية.

وبناءً على ما تقدم، فقد ظهرت محاولات فقهية لتحديد مفهوم الجريمة الإلكترونية انطلاقاً من الزاوية التي يتم النظر من خلالها لهذا النوع من الجرائم، فالتعاريف الواردة للجريمة الإلكترونية حاولت أن تشمل أي فعل أو نشاط غير مشروع، ورأت في الجريمة الإلكترونية أنها كل فعل أو نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة في الحاسب الآلي أو تلك التي يتم تحويلها من خلاله[1]. ويعاب على هذا المفهوم أنه يخرج من نطاق الجريمة الإلكترونية عدداً كبيراً من الأفعال غير المشروعة التي يستخدم فيها الحاسب الآلي كأداة لارتكاب الجريمة الإلكترونية من قبيل الاحتيال الإلكتروني.

[1] هشام فريد رستم، جريمة الحاسب الآلي كصورة من صور الجرائم الاقتصادية المستحدثة، مؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاملة المجرمين، مجلة الأمن العام، لبنان، العدد 151، 1995، ص31.

وفي إطار تخطي عيوب المفهوم أعلاه ذهب أحد الفقهاء في تحديده لمفهوم الجريمة الإلكترونية إلى اعتبار كل فعل أو سلوك غير مشروع يكون العلم بتكنولوجيا الحاسب الآلي بقدر كبير لازماً لارتكابه من جهة، وملاحقته وتحقيقه من جهة أخرى[1]. غير أن هذا التعريف للجريمة الإلكترونية أوضح أنه يجب أن تتوافر معرفة بتكنولوجيا الحاسب الآلي بدرجة كبيرة لارتكاب الجريمة الإلكترونية، وليس ذلك فحسب، بل أيضاً من أجل ملاحقتها وتحقيقها، وهو ما كان سبباً لانتقاد هذا المفهوم.

ويرى جانب آخر من الفقه أن مفهوم الجرائم الإلكترونية يشمل كل أشكال الفعل أو النشاط أو السلوك غير المشروع الذي يرتكب بواسطة الحاسوب والذي يهدف إلى الاعتداء على الأموال المادية والمعنوية. وبناءً على ذلك تم تعريف مفهوم الجريمة الإلكترونية على اعتبار أنها كل نشاط إجرامي يؤدي فيه نظام الحاسب الآلي دوراً لإتمامه، شريطةً أن يكون هذا الدور على قدر من الأهمية[2].

وفي رأي الباحث، فإن ما يؤخذ على هذا المفهوم أنه عام وبحاجة إلى توضيح المقصود بجملة القدر من الأهمية، فما هي الأهمية المطلوبة حتى يتحقق شرط الإجرام؟.

كذلك ذهب جانب من الفقه إلى تعريف الجريمة الإلكترونية على أنها الجريمة التي تقع بواسطة الحاسب الآلي أو عليه أو بواسطة الإنترنت[3]. وفي ذات السياق عُرفت أيضاً على أنها المخالفات التي ترتكب ضد فرد أو مجموعة من الأفراد بقصد إلحاق الضرر المادي أو المعنوي المباشر أو

---

[1] محمد عبدالله أبو بكر، موسوعة جرائم المعلوماتية (جرائم الكمبيوتر والإنترنت)، المكتب العربي الحديث، الإسكندرية، 2011، ص10.

[2] نائلة محمد فريد قورة، جرائم الحاسب الاقتصادية: دراسة نظرية تطبيقية، منشورات الحلبي الحقوقية، القاهرة، ط1، 2005، ص25.

[3] محمد عبد الرحيم سلطان العلماء، جرائم الإنترنت والاحتساب عليها، مؤتمر القانون والكمبيوتر والإنترنت، كلية الحقوق والشريعة، جامعة الإمارات، مايو، 2005، ص5.

غير المباشر باستخدام شبكات الاتصالات والإنترنت[1]. ودعا بعض الفقهاء إلى ضرورة تعريف المفردات الضرورية المتعلقة بارتكاب الجرائم الإلكترونية كنظام الحاسب الآلي والممتلكات والبيانات والخدمات[2].

واستناداً لما ورد أعلاه من تعاريف للجريمة الإلكترونية فإنها تركز على النشاط الإجرامي الذي تدخل فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المقصود. وهو ما اتجه إليه بعض الفقهاء الذين عرفوا الجريمة الإلكترونية على أنها كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي[3].

وذهب الفقيه الفرنسي Masse إلى اعتبار الجريمة الإلكترونية بأنها الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية ولغرض تحقيق الربح[4]. إلا أن هذا التعريف يشترط تحقيق الربح، وفي رأي الباحث، فإنه ليس شرطاً أن يحقق الاعتداء ربحاً، فقد يكون الاعتداء لأجل التعطيل أو التخريب.

ويرى ديفد ثوميسون أن الجريمة الإلكترونية هي جريمة تتطلب لاقترافها توافر معرفة لدى فاعلها معرفة بتقنية النظام المعلوماتي. وذهب في ذات الاتجاه سلوري الذي عرفها على أنها: "أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبيها"[5]. وقد عرفها الأستاذ Rosemblat أنها: "نشاط غير مشروع موجه لنسخ أو الوصول المعلومات المخزنة داخل الحاسوب أو تغييرها أو

---

[1] بوزيدي مختارية، ماهية الجريمة الإلكترونية، الملتقى الوطني حول آليات مكافحة الجريمة الإلكترونية، الجزائر، 29/مارس/2017، ص9.

[2] محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، مؤتمرات القانون والكمبيوتر والإنترنت، مرجع سابق، ص6.

[3] قال في هذا التعريف الفقيه الألماني تاديمان، أنظر: عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشريعة الجزائية، مركز دراسات الكوفة، العراق، 2008، ص112-113.

[4] محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مطابع الهيئة المصرية العامة للكتاب، مصر، 2003، ص19.

[5] سعد فهد سعد ادبيس المطيري، مفهوم الجرائم الإلكترونية وسماتها، مرجع سابق، ص1242.

حذفها"[1]، كما عرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها: "الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيسياً"[2].

وقد عرف الفقه المصري الجريمة الإلكترونية بأنها: كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات يهدف إلى الاعتداء على الأموال المادية او المعنوية أو أنها نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود[3].

ولم تأت الاتفاقية الأوروبية للجريمة عبر العالم الافتراضي المؤرخة في 2001/11/23م على تعريف محدد للجريمة عبر الإنترنت، وإنما اعترفت بنوعية من الجرائم يمكن ارتكابها عبر الإنترنت.

ومجمل القول، فإن المفهوم الفقهي للجريمة الإلكترونية استند إلى مجموعة من المعايير، إذ إن بعض الفقهاء حدد المفهوم انطلاقاً من وسيلة ارتكاب الجريمة الإلكترونية، والبعض الآخر استند إلى موضوع الجريمة الإلكترونية في تحديد المفهوم، وبعضهم استند إلى السمات الشخصية لمرتكب الجريمة الإلكترونية، في حين أن البعض استند إلى الهدف من الجريمة الإلكترونية.

ونخلص من خلال التعاريف الواردة أعلاه للجريمة الإلكترونية إلى أنها ترتكز إلى عاملين رئيسيين، الأول: أنها جريمة ترتكب بواسطة جهاز إلكتروني، والثاني: أنها تلحق ضرراً مادياً أو معنوياً بالأفراد. لذلك وبالإطلاع على التعريفات السابق ذكرها، يرى الباحث أن الجريمة الإلكترونية تعني: كل سلوك غير مشروع يرتكب بوساطة الأجهزة الإلكترونية لغرض إلحاق الضرر المادي والمعنوي المباشر أو غير المباشر بحقوق الأشخاص المحميين قانونياً.

---

[1] نسرين سيد سلامة، الجرائم الإلكترونية وأثرها على المجتمع، مجلة القاهرة للخدمة الإجتماعية، العدد 39، القاهرة، 2023، ص404.

[2] نسرين سيد سلامة، الجرائم الإلكترونية وأثرها على المجتمع، ص405.

[3] سعد فهد سعد ادبيس المطيري، مفهوم الجرائم الإلكترونية وسماتها، مرجع سابق، ص1242.

الفرع الثاني: المفهوم القانوني للجريمة الإلكترونية

يجد التأطير القانوني للجريمة الإلكترونية أهميته في الدور الذي تلعبه الإلكترونيات في الحياة اليومية، وما ينتج عنها من خطورة إساءة استخدامها، وأبرز الجهود التي تقوم بها كل الدول لتوحيد تشريعات مكافحة الجريمة الإلكترونية نظرا لطابعها العابر للحدود الوطنية.

وقد جاءت التشريعات المتعلقة بمكافحة الجريمة الإلكترونية حديثة نسبيا، حيث إن الدول السباقة في سن تشريعات خاصة بهذا المجال لم تتعدى السبعينات من القرن الماضي مثل القانون الفرنسي رقم 78-17 بشأن الحريات والمعلوماتية الصادر في 6 يناير عام 1978[1]، وقانون جرائم الحاسوب الصادر عام 1978 بولاية فلوريدا أول قانون في الولايات المتحدة الأمريكية[2]، وكذلك أصدر المشرع الإنجليزي بتاريخ 12/يوليو/1984 قانون حماية البيانات[3].

وقد اختلف نهج التشريعات القانونية المتعلقة بمكافحة الجرائم الإلكترونية بحسب توجهات الأنظمة القانونية، ويعتبر قانون جرائم الحاسوب الصادر عام 1978 بولاية فلوريدا أن كل دخول غير مخول إلى الحاسوب هو بمثابة جريمة، حتى ولو لم يكن هناك نية عدائية من هذا الدخول.

أما على الصعيد الفيدرالي، فقد صدر في عام 1984 قانون الاحتيال وسوء استخدام الكمبيوتر « Computer fraud and abuse act»، وتم تعديله في الأعوام 1986 و 1988 و 1989 و 1990 و 1994، ثم تم تعديله أخيراً عام 2001 بمقتضى القانون الوطني المؤرخ في

[1] القانون الفرنسي رقم 17 الصادر بتاريخ 6\يناير\ 1978 بشأن معالجة المعلومات والملفات والحريات، والذي جرى تعديله بموجب القانون رقم 493 الصادر بتاريخ 20\يونيو\2018.

[2] وهو أول قانون في الولايات المتحدة الأمريكية يخاطب الاحتيال والتطفل على الحاسوب

[3] عبد المنعم إبقال، الإطار القانوني لمكافحة الجريمة الإلكترونية: دراسة مقارنة، مجبة المنارة للدراسات القانونية والإدارية، المغرب، عدد خاص، 2017، ص118.

«The patrioty act»20/11/26 ، حيث تم إدراجه في القسم 1030 من الباب 18 من القانون الفدرالي للولايات المتحدة الأمريكية[1].

ونشير هنا إلى أن القانون الأمريكي ميز بين مصطلحي حاسوب Computer وبين حاسوب مشمول بالحماية computer Protected ، فهذا الأخير يعني ذلك الحاسب الآلي المتصل بغيره عن طريق الشبكة الدولية للمعلومات "الإنترنت" في حين إن إيراد مصطلح حاسوب Computer فقط فإنه يعني مجرد الحاسب الآلي غير المتصل بأي شبكة ولو داخلية (حيث يعد هنا أداةً للتخزين فقط)[2].

وقد عالج المشرع الفرنسي في القانون رقم 17/78 الصادر بتاريخ 6/يناير/1978 مسألة تخزين البيانات في الحاسب الآلي وأنواع هذه البيانات ومدة تخزينها وكذلك البيانات التي يجوز تخزينها والبيانات التي لا يجوز تخزينها[3].

وعمد المشرع الفرنسي إلى سن القانون رقم 19/88 الصادر بتاريخ 5/ يناير/ 1988 المتعلق بجرائم الغش المعلوماتي، وأصدر المشرع الفرنسي قانون العقوبات الفرنسي الجديد رقم 1336 لسنة 1992 والذي بدأ العمل به في الأول من مارس سنة 1994، وتضمن أحكام جديدة لمواجهة ظاهرة الإجرام الإلكتروني، وأضاف فصل ثالث للباب الثاني من القسم الثالث من قانون العقوبات،

---

[1] عبد المنعم إبقال، الإطار القانوني لمكافحة الجريمة الإلكترونية: دراسة مقارنة، مرجع سابق، ص119.

[2] نايف شافي المظافرة الهاجري، جرائم تقنية المعلومات في التشريع الأمريكي مقارنة بالتشريعات العربية، مجلة البحوث القانونية والاقتصادية، المنصورة، العدد 83، مارس، 2023، ص344.

[3] يمكن ذكر هذه الجرائم على النحو التالي: 1- الجرائم الخاصة بالمعالجة الإلكترونية للبيانات بدون ترخيص، ونصت عليها المادة 41 من هذا القانون. 2- لجرائم الخاصة بالتسجيل أو الحفظ غير المشروع للبيانات الاسمية، ونصت عليها المادة 42. 3 – الجرائم الخاصة بالإفشاء غير المشروع للبيانات الاسمية و تحكمها المادة 43. 4- الجرائم الخاصة بالانحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات الاسمية وتنظمها المادة 44.

ويأخذ الفصل المضاف عنوان "الاعتداءات على نظم المعالجة الآلية للمعلومات"، وذلك في المادة323-1 - 323-7[1].

واتجه المشرع الكويتي إلى تحديد مفهوم الجريمة الإلكترونية، وذلك من خلال القانون رقم 63 لعام 2015 بشأن مكافحة جرائم تقنية المعلومات، حيث حددت المادة الأولى منه مفهوم الجريمة المعلوماتية (الإلكترونية) على أنها: "كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون"[2].

كما عرف المشرع السعودي الجريمة (المعلوماتية) الإلكترونية على أنها: "أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة العنكبوتية بالمخالفة لأحكام هذا النظام"[3].

كذلك فقد حدد المشرع القطري مفهوم الجريمة الإلكترونية على أنها: "أي فعل ينطوي على استخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو شبكة معلوماتية بطريقة غير مشروعة وخالفة لأحكام القانون"[4].

---

[1] نصت هذه المادة على مجموعة من الجرائم التي تقع على أنظمة معالجة البيانات وهي: نص البند 1 من المادة 323 على جريمة الدخول بطريق الغش أو التدليس إلى نظام المعلومات أو بقاء الاتصال بطريقة غير مشروعة به. ونص البند 2 من المادة 323 على جريمة إعاقة أو التسبب في تحريف تشغيل نظام معالجة البيانات. ونص البند 3 من المادة 323 على جريمة إدخال البيانات بطريقة غير مشروعة في نظام معالجة البيانات أو إلغاء أو تعديل البيانات التي يحتوي عليها النظام بطريقة غير مشروعة. ونص البند 4 من المادة 323 على تجريم المساهمة في جماعة أو اتفاق بين مجموعة من الأشخاص للتحضير بعمل أو أعمال مادية لارتكاب جريمة أو أكثر من الجرائم السابقة. وكذلك جريمة تزوير الوثائق المعالجة معلوماتيا فقد أضاف المشرع في قانون العقوبات الجديد نص المادتين (462و 625) في شأن الغش ألمعلوماتي إلى نص المادة (441) التي تجرم تزوير الوثيقة المعلوماتية واستخدامها، وجعل المشرع الفرنسي نص هذه المادة يستوعب التزوير العادي في المحررات إلى جانب تزوير الوثيقة المعلوماتية وذلك بالنص على لفظ "سند أو دعامة وبأية وسيلة" فلم يحدد المشرع طريقة معينة للتزوير، ومن تم فهذه المادة شاملة لما جاء في المواد (462 و625) بخصوص التزوير الواقع على الوثيقة المعالجة معلوماتيا.

[2] القانون رقم 63 لعام 2015 الكويتي بشأن مكافحة جرائم تقنية المعلومات، المادة الأولى منه المعنونة بالتعريفات.

[3] هيئة الاتصالات وتقنية المعلومات، نظام مكافحة جرائم المعلوماتية السعودي، المادة الأولى.

[4] قانون مكافحة الجرائم الإلكترونية القطري رقم 14 لعام 2014، صادر عن الديوان الأميري القطري، تاريخ النشر :15\9\2014.لا

في حين عرف مكتب الأمم المتحدة المعني بالمخدرات والجريمة، الجريمة الإلكترونية، على أنها فعل ينتهك القانون، والذي يُرتكب باستخدام تكنولوجيا المعلومات والاتصالات (ICT) لاستهداف الشبكات والأنظمة والبيانات والمواقع الإلكترونية و/أو التكنولوجيا أو تسهيل ارتكاب جريمة[1].

وعرفتها منظمة التعاون الاقتصادي للتنمية بأنها: كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة او غير مباشرة عن تدخل التقنية المعلوماتية[2].

ونشير إلى أن بعض الدول لم تحدد في تشريعاتها مفهوم محدد للجريمة الإلكترونية: كالتشريع المصري، والتشريع الإماراتي، والتشريع الفلسطيني على اعتبار أنه ليس من اختصاص المشرع وضع التعريفات، إنما هو من اختصاص رجال الفقه والقضاء. في حين اكتفى التشريع المصري والإماراتي والمغربي والجزائري والفلسطيني بوضع أسس عامة أو أركان للجريمة، وتحديد بعض المصطلحات، بحيث يمكن من خلالها تحديد السلوك الإجرامي المستحدث. وهو ذات الاتجاه الذي سارت نحوه الاتفاقيات الدولية كاتفاقية بودابست لمكافحة الجرائم المعلوماتية لعام 2001 واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية وبروتوكولاتها عام 2003. وفي رأي الباحث، فإن عدم وضع تعريف للجريمة الإلكترونية في التشريعات هو التوجه الأسلم، وذلك نظراً لطبيعة الجريمة الإلكترونية وما يمكن أن تعرفه من حالات متطورة.

[1] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، على الرابط التالي: https://www.unodc.org/e4j/ar/cybercrime/module-1/key-issues/cybercrime-in-brief.html، تاريخ الإطلاع: 3/ابريل/2024

[2] يوسف المصري، الجرائم المعلوماتية والرقمية للحاسوب والإنترنت، دار العدالة، القاهرة، 2010، ص48.

المطلب الثاني: خصائص الجريمة الإلكترونية

تعد الجريمة الالكترونية إفرازا ونتاجا لتقنية المعلومات التي اتسع نطاق استعمالها في المجتمع؛ لذلك فهي ظاهرة إجرامية مستحدثة ذات طبيعة خاصة تتميز بمجموعة من الخصائص التي تختلف عن تلك التي تتميز بها الجرائم التقليدية.

والجريمة الإلكترونية ذات طابع خاص تستهدف معنويات وليست ماديات محسوسة، إلا أن آثارها قد تكون مادية محسوسة كما قد تكون معنوية أيضاً، غير إن الجريمة الإلكترونية تتشابه مع الجريمة التقليدية في أطراف الجريمة، وتختلف عنها في أداة ومكان الجريمة، حيث إن الأداة في الجريمة الإلكترونية عالية التقنية، والمجرم في الجريمة الإلكترونية لا يحتاج إلى التنقل الحركي لمكان وقوع الجريمة، بل يقوم بالفعل الإجرامي عن بعد باستخدام خطوط وشبكات الاتصال[1].

فالجرائم الإلكترونية تختلف عن الجريمة التقليدية حيث إنها لا تعرف حدودًا مادية أو جغرافية، ويمكن تنفيذها بجهد أقل وسهولة أكبر وبسرعة أكبر من الجريمة التقليدية. ونظراً للطبيعة الخاصة بالجريمة الإلكترونية، فإنها تتسم ببعض الخصائص المتعلقة بمرتكب الجريمة، وأخرى تتعلق بالجريمة الإلكترونية في حد ذاتها.

إذ إن مرتكب الجريمة الإلكترونية يتمتع بصفات مميزة من حيث الثقافة الإلكترونية وخبرة تقنية عالية في المجال، فالمجرم الإلكتروني يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها قبل أن ينفذ جريمته[2]، كما أن مرتكب الجريمة الإلكترونية يمتلك شعوراً بأن ما يقوم به لا

[1] حسين فريجة، الجرائم الإلكترونية والإنترنت، مجلة المعلوماتية، العدد 36، السعودية، أكتوبر، 2011، ص3.

[2] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت (الجرائم الإلكترونية)، منشورات الحلبي الحقوقية، ط1، بيروت، 2007، ص32.

يشكل جريمة؛ حيث يفرق بين الإضرار بالأشخاص والذي يعده عملاً غير أخلاقي، وبين الإضرار بمؤسسة أو جهة الذي يعده عملاً طبيعياً[1].

وفي هذا البحث سيتناول الباحث الخصائص التي تتسم بها الجريمة الإلكترونية بحد ذاتها، إذ تتميز الجريمة الإلكترونية بمجموعة من الخصائص التي تميزها عن غيرها من الجرائم التقليدية، وهو ما أكسبها لوناً وطابعاً قانونياً خاصاً، فالجريمة الإلكترونية عابرة للحدود (الفرع الأول)، كما أنها جريمة مركبة (الفرع الثاني).

الفرع الأول: الجريمة الإلكترونية جريمة عابرة للحدود

جعل نظام الإنترنت من معظم دول العالم في حالة اتصال دائم، لذلك فإن الجريمة الإلكترونية تتسم بالطابع الدولي؛ إذ إنه من المتوقع أن ترتكب الجريمة الإلكترونية في أي وقت دون الالتزام والتقيد بدولة ما أو بمدى قرب المسافة أو بعدها، فهذا النوع من الجرائم لا يعترف بالحدود، إذ تمتد هذه الجريمة إلى خارج حدود دولة مرتكبيها إلى دولة أخرى أو عدة دول، من خلال ربط الحواسيب عبر العالم بشبكة الإنترنت، مما يثور معها مجموعة من الإشكالات كالمشاكل المتعلقة بالاختصاص وتلك المتعلقة بالإجراءات والتحري وغير ذلك من الإشكالات التي تثيرها[2].

وقد انعكست قدرة الإنترنت على اختصار المسافات على طبيعة الأعمال الإجرامية، إذ ساعدت على ارتكاب الجريمة عن بعد، ومن ثم تتباعد المسافة بين الفعل الإجرامي الذي يتم من خلال الكمبيوتر وبين معطيات الجريمة ونتائجها، وبذلك فالجريمة الإلكترونية تعتبر شكلا جديدا من أشكال الجريمة العابرة للحدود التي يمكن من خلال الأجهزة الإلكترونية المرتبطة بشبكة الإنترنت

[1] نائلة محمد فريد قورة، جرائم الحاسب الاقتصادية: دراسة نظرية تطبيقية، مرجع سابق، ص54.

[2] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت (الجرائم الإلكترونية)، مرجع سابق، ص33.

ارتكاب العديد من الجرائم الإلكترونية من قبيل التعدي على البيانات، والتزوير، وغسل الأموال، وإتلاف المستندات الإلكترونية، والقرصنة، والاحتيال المعلوماتي.

غير أن الجرائم الإلكترونية تتميز عن جرائم غسل الأموال أو جرائم المخدرات في أنها لا تحتاج إلى الحركة والتنقل بين الدول، فيمكن ارتكابها دون مغادرة المقعد المقابل للحاسب الآلي، كأن يتم التعدي على البيانات البنكية لشخص ما، في دولة ما، أو أن يتم التعدي على شركات أو مؤسسات ووزارات في دولة أخرى.

هذا التباعد أحدث تشتت في الجهود الرامية إلى مكافحة هذا النوع من الإجرام، فعندما يكون مرتكب الجريمة في دولة ما أو في قارة ما ونتائج الجريمة في دولة أخرى أو في قارة أخرى، يكون التصدي لهذا الفعل الإجرامي أمراً عسيراً؛ وذلك لاختلاف الجراءات الجنائية أو النزاع حول القانون واجب التطبيق.

الفرع الثاني: صعوبة إثبات الجريمة الإلكترونية

تتميز الجريمة الإلكترونية وتتصف بصعوبة الكشف عنها، وذلك لعدم وجود آثار مادية بصورة مرئية يمكن متابعتها، إذ يمكن للجاني تدمير دليل الإدانة بسرعة كبيرة، بالإضافة إلى أن هذا النوع من الجرائم يرتكب بالخفاء وعدم وجود أثر كتابي لما يتم خلال تنفيذها. ناهيك عن صعوبة تحديد مكان فحصها[1].

وهناك مجموعة من العوامل التي يعزى إليها صعوبة إثبات الجريمة الإلكترونية من قبيل أن الجريمة الإلكترونية لا تترك أثراً مادياً، حيث إن بيئتها إلكترونية يتم فيها نقل البيانات وتداولها

[1] عبد الحكيم مولاي إبراهيم، الجرائم الإلكترونية، مجلة الحقوق العلوم الإنسانية، جامعة زيان عاشور بالجلفة، العدد 23، الجزائر، 2015، ص213.

بنبضات إلكترونية دون وجود مستندات ورقية، كما أنها جريمة في الغالب لا تترك شهوداً يمكن استجوابهم ولا أدلة يمكن فحصها. كما أن صعوبة الإثبات في هذه الجرائم تأتي من صعوبة الاحتفاظ بأدلة الجريمة الإلكترونية، إذ يمكن لمرتكب الجريمة أن يمحو أو يحرف أو يغير في البيانتا لموجودة على جهاز الحاسوب في أقل من ثانية[1].

كما أن الجريمة الإلكترونية بحاجة الإلمام بالخبرة الفنية والتقنية للكشف عنها والتحقيق فيها، إذ إن عدم امتلاك الخبرة من قبل الجهة التي تحقق فيها قد يتسبب عن غير قصد بإتلاف الدليل الإلكتروني، وهو ما يعيق مسألة مكافحة مثل هذه الجرائم[2].

ونشير هنا إلى أن من خصائص الجريمة الإلكترونية أنها جريمة هادئة أو ناعمة ، فهي لا تحتاج إلى مجهود عضلي في تنفيذها، وإنما هي تحتاج إلى القدرة الذهنية والخبرة العلمية والفنية[3]، بالإضافة إلى أن من خصائص الجريمة الإلكترونية أنها قد تكون جريمة مركبة، إذ اتفقت التشريعات الوطنية والدولية على أن الدخول العمد غير المصرح به لموقع إلكتروني واستمرار التواجد فيه بعد العلم بذلك يشكل جريمة بحد ذاته من حيث المبدأ ويعاقب عليها القانون، وفي حال ترتب عن هذا الدخول أضرار معينة تصبح الجريمة مشددة ويعاقب عليها القانون بعقوبة أشد[4].

وهو الأمر الذي أكدت عليه الاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست) عام 2001 في الباب الثاني منها الموسوم بالتدابير الواجب اتخاذها على الصعيد الوطني في المادة 2 منه المعنونة بالنفاذ غير المشروع والتي جاء فيها "تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق: النفاذ

---

[1] حسين فريجة، مرجع سابق، ص3.

[2] أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2005، ص113 وما يليها.

[3] محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع، عمان، الاردن، ط1، 2004، ص166.

[4] أنظر على سبيل المثال لا الحصر القرار بقانون الفلسطيني بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات رقم 10 لسنة 2018 وتعديلاته، المادة 4 منه.

الكامل أو الجزئي إلى نظام (كمبيوتر). يجوز لطرف أن يستلزم أن تُرتكب الجريمة عن طريق مخالفة التدابير الأمنية، بنِية الحصول على بيانات الكمبيوتر أو بأي نية غير صادقة أخرى، أو في ارتباط بنظام كمبيوتر متصل بنظام حاسوبي آخر".

في حين أشارت المادة 3 من الاتفاقية المعنونة بالاعتراض غير المشروع إلى أن "تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق: الاعتراض باستخدام وسائل فنية، للإرسال غير العمومي لبيانات الكمبيوتر إلى أو من أو داخل نظام كمبيوتر، بما في ذلك الانبعاثات الكهرومغناطيسية الصادرة عن نظام كمبيوتر يحمل هذه البيانات. ويجوز للدولة الطرف أن يستلزم أن تُرتكب الجريمة عن طريق مخالفة التدابير الأمنية، بنِيَّة غير صادقة أو في ارتباط بنظام كمبيوتر متصل بنظام حاسوبي آخر".

هو ذات الأمر الذي علق عليه التقرير التفسيري لاتفاقية الجرائم الإلكترونية الصادر في نوفمبر 2001 [1]، فقد أكد على أن "التسلل غير المرخص، بمعنى "قرصنة" أو "كسر" أو "اختراق الكمبيوتر"، غير قانوني في حد ذاته من حيث المبدأ، حيث إن مثل هذا السلوك قد يضع عوائق أمام المستخدمين الشرعيين للأنظمة والبيانات، وقد يتسبب في إحداث تغيير أو تدمير يسفر إصلاحه عن كلفة عالية. وقد يترتب عن مثل هذا الاختراق النفاذ إلى بيانات سرية (بما في ذلك، كلمات المرور ومعلومات عن النظام المستهدف)، وأسرار، بالإضافة إلى استخدام النظام بدون مقابل أو حتى إلى تشجيع القراصنة على ارتكاب أشكال أكثر خطورة من الجرائم المتصلة بالكمبيوتر، مثل الاحتيال أو التزوير المتصل بالكمبيوتر".

[1] التقرير التفسيري لاتفاقية الجرائم الإلكترونية، مجلس أوروبا، سلسلة المعاهدات الأوروبية رقم 185، بودابست، 23\نوفمبر\2001.

وفي ذات الاتجاه تبنت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الصادرة بتاريخ 2010/12/21، ودخلت حيز النفاذ بتاريخ 2014/2/6، في الفصل الثاني منها، المادة 6 والمعنونة بجريمة النفاذ غير المشروع، إذ جاء في البند الثاني منها "تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال: أ: محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الإلكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين. ب: الحصول على معلومات حكومية سرية.

وأخيراً نشير إلى أن هناك مجموعة من الصعوبات التي تواجه عملية مكافحة الجريمة الإلكترونية، من قبيل: سهولة إخفاء معالم الجريمة، وعدم خبرة الأجهزة الأمنية الكافية لتمحيص عناصر الجريمة، بالإضافة إلى اختلاف مفاهيم الجريمة الإلكترونية على المستوى الدولي، ناهيك عن عدم كفاية الاتفاقيات الدولية والثنائية ذات العلاقة بتسليم المجرمين.

المطلب الثالث: أركان الجريمة الإلكترونية

لاعتبار أي سلوك جريمة بمعناها القانوني، لا بد من توافر الأركان التي تدل على أن هذا السلوك يشكل جريمة، حيث تعد أركان الجريمة الأساس والأصل لقيام أي جريمة، ففي أي سلوك يعتبر جريمة، لا بد من وجود أركان لهذا السلوك وهما الركن المادي والركن المعنوي، بالإضافة للركن الشرعي، وبدون وجود هذه الأركان لا تقوم الجريمة.

إذ إن الركن المادي هو السلوك الإجرامي ويتكون من الفعل والنتيجة والعلاقة السببية التي تربط بين الفعل والنتيجة، فلا جريمة دون وجود فعل غير مشروع. كما أن الركن المادي يمكن تحقيقه دون تحقيق النتيجة، وذلك مثلاً في حالة الإبلاغ عن الجريمة قبل أن تحقق الجريمة النتيجة[1].

أما الركن المعنوي فهو القصد الجنائي، أي العلم بطبيعة السلوك وبالنتيجة التي يُفضي إليها وإرادة السلوك والنتيجة معاً، فالركن المعنوي للجريمة يتكون من العلم والإرادة، بحيث ينصب علم الجاني على مضمون السلوك غير المشروع ، إذ إن العلم والإرادة عنصران يتعلقان بنفسية الجاني[2].

في حين أن الركن الشرعي يشير إلى النص القانوني المجرم للسلوك أو الفعل، وذلك تطبيقاً للمبدأ الشرعي لا جريمة ولا عقوبة إلا بنص[3]. وكذلك هي الجريمة الإلكترونية تتكون من الركن الشرعي (الفرع الأول)، والركن المادي (الفرع الثاني)، والركن المعنوي (الفرع الثالث). وهو ما سنتناوله في هذا المطلب.

الفرع الأول: الركن الشرعي للجريمة الإلكترونية

يعني الركن الشرعي السند القانوني لتجريم الفعل أو السلوك طبقاً لمبدأ الشرعية الذي ينص على أنه "لا جريمة ولا عقوبة إلا بنص"، وإعمالا لذلك فإنه من غير الممكن للقاضي بأي حال من الاحوال القياس في التجريم، فلا بد من وجود نص قانوني يجرم الفعل ويعتبره غير مشروع[4].

وفي إطار الجريمة الإلكترونية فإن الركن الشرعي لها يتحقق من خلال ما أكدت عليه نصوص الاتفاقيات الدولية[1]، والاتفاقيات الإقليمة[2] والتشريعات الوطنية من أن النفاذ الكلي أو الجزئي غير

[1] علي إبراهيم بن دراج، محاضرات في الجرائم المعلوماتية، المركز الجامعي آفلو، معهد الحقوق والعلوم السياسية، الجزائر، 2021، ص14

[2] علي ابراهيم بن دراج، مرجع سابق، ص14-15.

[3] علي إبراهيم بن دراج، مرجع سابق، ص12.

[4] حنان ريحان مبارك المضحكي، الجرائم المعلوماتية دراسة مقارنة، منشورات الحلبي الحقوقية، ط1، بيروت، 2014، ص56.

المشروع يشكل جريمة يعاقب عليها القانون، فلا تكاد تخلو التشريعات العربية والأجنبية من النص على تجريم الدخول غير المشروع للنظام المعلوماتي. وتأتي أهمية تجريم الدخول غير المصرح به للنظام المعلوماتي على اعتبار أنها مرحلة سابقة تشكل بوابة مرور لارتكاب جرائم أخرى.

إذ ذكر القانون الفلسطيني رقم (10) لسنة 2018م وتعديلاته والمتعلق بالجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات في المادة (4) الفقرة (1) منه أن كل دخول عمداً بغير وجه حق يعاقب بالحبس أو الغرامة أو بكلتا العقوبتين.

وهو ذات المضمون الذي أكدت عليه التشريعات العربية من قبيل القانون المصري بشأن مكافحة جرائم تقنية المعلومات رقم (175) لسنة 2018م، والتشريع السعودي من خلال قانون مكافحة الجريمة الإلكترونية، والقانون القطري رقم (14) لسنة 2014م المتعلق بمكافحة الجرائم الإلكترونية، والقانون الإماراتي بشأن مكافحة جرائم تقنية المعلومات، والقانون الكويتي رقم (63) لسنة 2015م بشأن مكافحة جرائم تقنية المعلومات، وغيرها من التشريعات العربية كالقانون المغربي وكذلك الجزائري.

لذلك باتت هذه القوانين تمثل الركن الشرعي للجرائم الإلكترونية في كل دولة، وذلك لما تشكله من اعتداء على حرمة الحياة الخاصة للإنسان وانتهاكاً لخصوصيته، لذلك فقد كرس المشرع الفلسطيني من خلال القرار بقانون رقم 10 لسنة 2018 وتعديلاته، تجريم مجموعة من الأفعال التي نص عليها وعلى عقوباتها ومنها على سبيل المثال لا الحصر جريمة غسل الأموال وجريمة التزوير

---

[1] القسم الأول من الباب الثاني من الاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست)، 2001/11/23. وكذلك التقرير التفسري لها.

[2] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الصادرة بتاريخ 2010/12/21، ودخلت حيز النفاذ بتاريخ 2014/2/6، الفصل الثاني، المادة 6 والمعنونة بجريمة النفاذ غير المشروع وجاء في البند الأول منها "الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به".

الإلكتروني وغيرها العديد من الجرائم، وهو ما يعتبر الركن الشرعي الذي يؤسس لتجريم هذه الأفعال.

الفرع الثاني: الركن المادي للجريمة الإلكترونية

تتكون الجريمة الإلكترونية كغيرها من الجرائم من الركن المادي للجريمة والذي هو السلوك الجرمي أي فعل أو امتناع عن فعل، ونتيجة جرمية، وعلاقة سببية تربط بينهما، غير أن هناك من الجرائم التي يكتفي فها السلوك الجرمي للمعاقبة عليها، وذلك دون شرط إحداث نتيجة جرمية وتسمى بجرائم السلوك المحض أو الجرائم الشكلية. ومن الأمثلة على ذلك جريمة الدخول غير المشروع[1]. فالركن المادي يشير إلى الجريمة التامة أو الكاملة، وبالتالي فإن الركن المادي للجريمة الإلكترونية يتكون من مكونات ثلاث وهي: السلوك الجرمي (أولاً)، والنتيجة الجرمية (ثانياً)، والعلاقة السببية (ثالثاً).

أولاً: السلوك الجرمي: بحكم أن الجاني في الجرائم الالكترونية يختلف عنه في غيرها من الجرائم، فإن السلوك الجرمي الذي سيصدر منه في مجال ارتكاب الجريمة الالكترونية حتما سيختلف عن الجاني التقليدي، إذ يتطلب لقيام الجريمة الإلكترونية وجود جهاز إلكتروني متصل بشبكة الإنترنت، ويفترض كذلك معرفة الجاني بإدارة النشاط ومعرفته باستخدام الجهاز الإلكتروني، ويفترض قدرته على تجهيز الجهاز الإلكتروني، كأن يقوم الجاني بتحميل برامج الإختراق[2].

[1] خالد سليمان عبدالله الحمادي، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري: دراسة مقارنة، كلية القانون، جامعة قطر، يناير، 2019، ص46.

[2] عبد الإله أحمد هلالي، المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست، مجلة الحقوق، جامعة البحرين، المجلد السادس، العدد13، 2009، ص25.

ومن الناحية القانونية فإن فعل السلوك الجرمي له صور عديدة ومختلفة، حددتها الاتفاقيات الدولية والإقليمية والتشريعات الوطنية، وتختلف هذه الصور من تشريع إلى آخر، غير أن مختلف التشريعات الوطنية جاءت متفقة مع نصوص الاتفاقيات الدولية المتعلقة في هذا المجال، كاتفاقية بودابست لمكافحة الجرائم الإلكترونية فجميعها اتفقت على أن السلوك الجرمي في الجرائم الإلكترونية يتمثل في النفاذ غير المشروع وكذلك الاعتراض غير المشروع.

ونأخذ على سبيل المثال لا الحصر التشريع الفلسطيني الذي أشار إلى صور السلوك الجرمي، ونشير هنا إلى نص المادة 4 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات، فقد أكدت المادة 4 في البند 1 منها على أن الدخول العمد غير المشروع يعاقب عليه القانون، كما نص البند 2 من ذات المادة على صور السلوك الجرمي، وذكرت أن كل ما يترتب عن هذا الدخول غير المشروع من إلغاء للبيانات أو نقلها أو تعديلها أو إتلافها أو نسخها أو نشرها...إلخ، يعاقب عليه القانون بحكم مشدد.

ثانياً: النتيجة الجرمية: وهي أحد أهم مكونات الركن المادي، وتعني ما يترتب على الفعل أو السلوك الجرمي غير المشروع الذي قام به الجاني، ويطلق على هذه النتيجة المدلول المادي للنتيجة الجرمية، أما الدلول القانوني للنتيجة الجرمية فيكمن في الاعتداء على الحق الذي يحميه القانون، وبذلك فهو يمثل التكييف القانوني للنتيجة المادية التي خلفها الفعل غير المشروع[1].

وكذلك هي الجرائم الإلكترونية تفترض وجود النتيجة الجرمية فيها كونها مكون من مكونات الركن المادي للجريمة، وعلى اعتبار أن الجريمة الإلكترونية تتعدد وتتنوع، فإن النتيجة الجرمية تختلف باختلاف نوع الجريمة الإلكترونية المرتكبة؛ فالنتيجة الجرمية الناتجة عن جريمة التزوير أو

[1] ذياب البداينة، الجرائم الإلكترونية: المفهوم والأسباب، الملتقى العلمي حول: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، عمان، الأردن، 2-2014/9/4.

التحريف الإلكترونية ليست هي النتيجة الجرمية الناتجة عن جريمة القتل من خلال أجهزة الحاسوب والإنترنت.

وهنا يثور النقاش بشأن النتيجة الجرمية في الجرائم الإلكترونية فيما إذا كانت نتيجة الفعل الجرمي في العالم الإلكتروني أم في العالم الواقعي، فالنتيجة الجرمية الناتجة عن سرقة البيانات أو سرقة موقع إلكتروني هل هي نتيجة مادية أم معنوية؟

نشير هنا إلى أن الفقه انقسم في ذلك إلى عدة اتجاهات، إذ يرى جانب من الفقه أن سرقة البيانات أو تزويرها لها مدلول مادي وليس معنوي؛ وذلك على اعتبار أن تلك البيانات لها أصل صادرة عنه، ولها مقابل مادي[1]، وجانب آخر من الفقه يرى بأن سرقة البيانات أو تزويرها لها مدلول معنوي وبالتالي يجب وضع نصوص قانونية تتناسب مع طبيعة الجريمة[2].

ويميل الباحث إلى الرأي الفقهي الذي يعتبر أن النتيجة الجرمية الناتجة عن سرقة البيانات لها مدلول مادي؛ إذ إن القاعدة القانونية هي كل شيء يصلح محلاً لحق عيني، وبالتالي فالحيازة التي تنالها السرقة بالاعتداء على البيانات، يراد منها الحيازة المادية، حيث إن الصفة المادية لشيء هو إمكان السيطرة المادية عليه، وصلاحيته لأن تستخلص منه مباشرة المزايا المادية التي تشكل السرقة اعتداء عليها وهو ما ذهب إليه الفقه الفرنسي والبلجيكي[3].

والنتيجة الجرمية لفعل القتل بواسطة الحاسوب، كأن يقوم الجاني بتغيير نوعية الدواء وكميته للمريض وبالتالي قتله، فهنا مدلول النتيجة الجرمية مادي تحققت في الواقع، كذلك هو الحال

---

[1] لورنس سيعيد الحوامدة، الجرائم المعلوماتية أركانها وآلية مكافحتها: دراسة تحليلية مقارنة، مجلة الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية العالمية، عمان، الأردن، 2017، ص20.

[2] لورنس سيعيد الحوامدة، مرجع سابق، ص20.

[3] حابس يوسف زيدات، حدود قانون العقوبات في السيطرة على السرقة الإلكترونية "اختلاس المعلومات والبيانات الالكتروني" في ضوء التشريعات الوطنية والدولية، المؤتمر الدولي لكافحه الجرائم الالكترونية في فلسطين، كلية الحقوق، جامعة النجاح الوطنية، فلسطين، 2016/4/17، ص9.

بالنسبة لسرقة البيانات، فإن النتيجة الجرمية لها تحققت في الواقع من خلال ما يحصل عليه الجاني من مقابل أو حتى من خلال أن هذه البيانات يمكن تحليلها إلى معلومات معينة لها أصل صادرة عنه.

ثالثا: علاقة السببية: أشرنا إلى أن العلاقة السببية تشير إلى العلاقة بين سلوك الجاني وبين النتيجة التي ترتبت على فعله، وبالتالي لا بد أن تتحق العلاقة السببية حتى تكتمل أركان الجريمة، حيث إنه بوقوعها تتحقق المسؤولية التامة لارتكاب الجريمة، إذ إنها تسند النتيجة الجرمية وهو ما يعني أن للعلاقة السببية أهمية بالغة لإكتمال الركن المادي. فالسببية هي العلاقة بين العلة والمعلول تربط بين ظاهرتين حسيتين مرتبطتين على شكل ضروري في تعاقب زمني يفيد أن أحدهما سبباً للآخر[1].

وفيما يتعلق في العلاقة السببية في الجرائم الإلكترونية، فيمكن تطبيق ذات القواعد العامة المطبقة على الجرائم العادية في حال انطبقت عليها، إذ إن سرقة المعلومات والبيانات واختلاسها يتحقق بالنشاط المادي الصادر عن الجاني سواء بتشغيله للجهاز للحصول على المعلومة أو البرنامج أو الاستحواذ عليها، وبتشغيله للجهاز تتحقق النتيجة بحصوله عليها، لذلك فالرابطة السببية متوفرة بين نشاطه المادي والنتيجة الإجرامية[2].

الفرع الثالث: الركن المعنوي للجريمة الإلكترونية

الجريمة كذلك كيان نفسي، فإذا كان الركن المادي يتكون من السلوك الجرمي والنتيجة الجريمة والعلاقة السببية، فإن الركن المعنوي يتكون من العلم والإرادة، وذلك يعني أن الجاني يكون محل

[1] محمود حسني، شرح قانون العقوبات القسم العام، دار النهضة العربية، القاهرة، 1979، ص280.

[2] هدى حامد قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992، ص61 –62.

للمساءلة إذا قامت الصلة بين الركن المادي للجريمة والركن المعنوي لها[1]، وعليه يمكن تعريف الركن المعنوي على أنه: العلاقة بين ماديات الجريمة وشخصية مرتكب الجريمة، وهي العلاقة التي يستوجب معها العقاب القانوني[2].

والعلم هي حالة ذهنية يكون عليها الجاني وقت ارتكاب الجريمة ويتمثل ذلك في أن ينصرف علم الجاني على العناصر التي تتألف منها الركن المادي بأن يحيط علمه بالواقعة المكونة للسلوك الإجرامي والعلم بالتكيف أو بالمدلول[3]. وكذلك علم الجاني بالظروف المشددة وعلمه بالأركان الخاصة.

والإرادة هي العنصر الثاني من عناصر توافر القصد الجرمي فهو ركن لا يتعلق بالماديات إنما متعلق بالحالة النفسية أو المزاجية لمرتكب الجريمة الالكترونية، إذ إن الإرادة هي سبب الفعل، وبنظر القانون لا قيام للفعل ما لم يكن صادراً عن الإرادة، فهي التي تسيطر على الفعل وبالتالي تضفي الصفة الإرادية على جميع أجزائه[4]

فلا بد وأن يتم التركيز على العلاقات بين مادية الجريمة وشخصية مرتكب الجريمة؛ وذلك على اعتبار أن المنهج النفسي والذهني هو محور القانون الجنائي، ففي إطار الركن المعنوي تتحقق مقومات المسؤولية الجنائية، وبالتالي يتوجب حق الدولة في العقاب الذي يبنى على هذه المقومات. وكذلك هو الحال بالنسبة للجريمة الإلكترونية، فهي من الجرائم التي يشترط لقيامها توافر القصد الجرمي أي لا بد من علم الجاني بتوافر عناصر الجريمة، فإذا كان الجاني جاهلاً بالوقائع المادية

[1] محمود نجيب حسني، النظرية العامة للقصد الجنائي دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، دار النهضة العربية، القاهرة، 2006، ص56.

[2] محمود نجيب حسني، النظرية العامة للقصد الجنائي دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية مرجع سابق، ص61.

[3] محمود نجيب حسني، النظرية العامة للقصد الجنائي دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، مرجع سابق، ص60.

[4] محمود نجيب حسني، النظرية العامة للقصد الجنائي دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، مرجع سابق، ص7.

للجريمة ووقع في عنصر من عناصرها، ولم تنصرف إرادته للفعل الجرمي، فإن ذلك يمنع من توافر القصد الجرمي[1]. وهذا هو المقصود بالقصد العام للجريمة.

فيجب أن يكون الجاني على علم بحقيقة الواقعة الجرمية، وأن فعله يشكل عدواناً على الحقوق التي هي محمية بموجب القانون، كما يجب أن تنصرف إرادته إلى ذلك الفعل. ونشير هنا إلى أنه إذا كان الفعل الجرمي مجرم بنص القانون ومنشور في الجريدة الرسمية، فإن ذلك كفيل بانتفاء صفة جهل الجاني بسلوكه الجرمي، فلا مجال للجاني للتعذر بعدم علمه.

أما فيما يتعلق بالقصد الخاص في الجرائم الإلكترونية، فهو يرجع بالدرجة الأولى إلى طبيعة الجريمة ونية الجاني الخاصة التي دفعته للقيام بالفعل غير المشروع، لذلك فليست كل الجرائم الإلكترونية على درجة واحدة، فكل جريمة إلكترونية تختلف عن الأخرى من حيث أركانها وماهيتها وطبيعتها، فنرى أن القضاء الأمريكي لم يستقر على حال بالنسبة لبعض الجرائم الإلكترونية من حيث تحديد ما إذا كانت تتطلب قصداً عاماً أو خاصاً[2].

من الملاحظ أن معظم الجرائم الإلكترونية تقوم بتوافر القصد العام أي بعلم الجاني وإرادته، كالتعدي على برامج الحاسب الآلي، والدخول غير المشروع للبريد الإلكتروني أو المواقع التجارة الإلكترونية وهو ما نص عليه القانون الفرنسي والقانون السويسري والقانون البرتغالي والقانون الدنماركي. أما القصد الخاص في مثل هذه الجرائم فإنه يتمثل بنية الإضرار بالغير أو الحصول على الربح غير المشروع[3].

كما أن القصد الخاص يتوافر في بعض الجرائم الإلكترونية، فعلى سبيل المثال في حالة سرقة البيانات وهي من الجرائم الإلكترونية فجيب أن ينصرف علم الجاني وإرادته إلى أن سرقة البيانات

---

[1] محمود حسني، شرح قانون العقوبات القسم العام، مرجع سابق، ص57.

[2] خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر العربي، الإسكندرية، ط1، 2009، ص109 وما يليها.

[3] خالد ممدوح إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص259.

يعتبر فعلاً غير مشروع. ويترافق مع هذا القصد العام لسرقة البيانات القصد الخاص المتمثل في نية الجاني بتملك المعلومة أو البيانات وهو ما أخذت به محكمة النقض الفرنسية[1].

ونخلص مما سبق إلى أن القصد العام والقصد الخاص في الجرائم الإلكترونية هو أساس تحديد المسؤولية الجنائية، وما يحدد توافر القصد الخاص في بعض الجرائم الإلكترونية هو طبيعة الجريمة ونية الإضرار بالغير ونية التملك أو النية الخاصة لمرتكب الجريمة والتي يمكن تحديدها من مكونات كل جريمة بشكل مستقل، وبالتالي فإن الجرائم الإلكترونية باعتبارها جرائم مستحدثة تعتبر كغيرها من الجرائم التقليدية يشترط فيها توافر الركن المعنوي لقيام الجريمة، فلا يتصور قيام جريمة إلكترونية بمختلف أنواعها دون توافر الركن المعنوي.

وانطلاقاً من كل ما سبق، يتضح أن الجرائم الإلكترونية تمتاز بمجموعة من الخصائص التي تميزها عن غيرها من الجرائم التقليلدية والتي تعتبر من التحديات التي توجهها مختلف التشريعات، غير أن الجرائم الإلكترونية كغيرها من الجرائم التقليدية تقوم بتوافر ركنيها المادي والمعنوي، ولكي تقع الجريمة الإلكترونية يشترط وجود أركان الجريمة المشار إليهما أعلاه. يبقى لنا أن نتساءل عن التنظيم القانوني الخاص بالجريمة الإلكترونية وهو ما سنتناوله في المبحث الثاني من البحث.

[1] بلال أمين زين الدين، جرائم أنظمة المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية، دار الفكر العربي، الإسكندرية، ط1، 2008، ص117.

المبحث الثاني: التنظيم القانوني الخاص بالجريمة الإلكترونية

نتيجةً للتطوررات الهائلة خاصة في مجال نظم المعلومات والاتصالات وما رافقها من تطورات في جانبها السلبي، ظهرت الجريمة الإلكترونية، لذلك أصبح المشرع الدولي والمشرع الوطني على حدٍ سواء أمام ضرورة إيجاد نصوص قانونية تحدد تلك الأفعال المجرمة والعقوبات المناسبة لها.

لذلك، تُستمد شرعية مكافحة الجريمة الإلكترونية من القوانين الجنائية التي تتخذها الدول وتستقيها من الاتفاقيات الدولية لحماية مصالحها المهددة، الأمر الذي فرض ضرورة تبادل الخبرات بين المشرعين الجنائيين من باب إقرار قوانين أكثر نجاعة في التصدي لمختلف أشكال الجرائم الإلكترونية، وذلك بالاستفادة من التشريعات المقارنة، وخاصة للدول السباقة لاستحداث قوانين خاصة بالجرائم الإلكترونية.

وعلى مستوى الجهود التشريعية الدولية لمكافحة الجرائم الإلكترونية، فقد بذلت منظمة الأمم المتحدة جهوداً جمة في رسم سياسات ناجحة في سبيل العمل على مكافحة جرائم الإنترنت وتحقيق العدالة الجنائية عبر إقرار العديد من التوصيات، وإنشاء اللجان المتخصصة ومن بينها اللجنة الإستشارية لخبراء منع الجريمة ومعاملة المجرمين الذي عهد إليها مهمة مكافحة الجريمة وتقديم المشورة للأمين العام، وإيجاد البرامج ووضع الخطط ورسم سياسات لتدابير دولية في مجال منع الجريمة، ومعاملة المجرمين.

وعقدت منظمة الأمم المتحدة العديد من المؤتمرات لتعزيز وتبادل المعارف والخبرات بين الأخصائيين من مختلف الدول من أجل تدعيم التعاون الدولي والإقليمي في مجال مكافحة الجريمة، ومن هذه المؤتمرات: مؤتمر جنيف الخامس عام 1975، والمؤتمر الدولي السادس بكركاس في فنزويلا عام 1980، ومؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين

عام 1985، ومؤتمر الامم المتحده الثامن لمنع الجريمه ومعامله السجناء وقرارات بشأن الجرائم ذات الصله بالكمبيوتر هافانا عام 1990، ومؤتمر الأمم المتحده التاسع لمنع الجريمة ومعاملة المجرمين عام 1995[1].

واعتمدت لجنة الأمم المتحدة عام 1996 قانون الانسيترال النموذجي بشأن التجارة الالكترونية، والذي جاء إعداده في الأساس استجابة للتغير الرئيسي الذي حدث في الوسائل التي تتم فيها الاتصالات بين أطراف يستخدمون في أعمالهم التقنيات الحاسوبية أو غيرها من التقنيات الحديثة، وكان القصد منه أن يكون أنموذجاً تهتدي به الدول لتقييم وتحديث جوانب معينة من قوانينها وممارساتها في ميدان العلاقات التجارية، وتدارك المساوئ الناجمة عن قصور التشريعات الوطنية[2]. كما اهتمت مجموعة الدول الثمانية G8 بالجرائم التي تتم باستخدام أو ضد الكمبيوتر، وصدر عنها مجموعة من التوصيات والقرارات في مجال مكافحة هذا النوع من الجرائم، ومن أبرز هذه القرارات ما صدر عن مجموعة العمل المعروفة باسم Group Lyon التي شكلت في أثناء قمة "هاليفاكس" في كندا عام 1995، تحت مسمى توصيات من أجل مكافحة الجريمة المنظمة عبر الوطنية بفعالية[3].

ولأن الجرائم الإلكترونية التي ترتكب بواسطة النظام المعلوماتي تتنوع ما بين جرائم اقتصادية أو قرصنة المعلومات وجرائم ذات طابع سياسي، لذلك تقع الجرائم الإلكترونية على الأموال كما قد تقع على الأشخاص سواء كانوا أشخاصاً طبيعيين أو اعتباريين. وبناء عليه، فإن الباحث سيتناول هذا

---

[1] أشرف لبيب صادق شحاته البدراوي، التعاون الدولي في مجال مكافحة الجريمة المنظمة، أطروحة دكتوراة، كلية الحقوق، جامعة أسيوط، 2011، ص307-311. وكذلك: منير محمد الجنبيهي وممدوح محمد الجنبيهي، تزوير التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006، ص155.

[2] أمجد حسن مرشد الدعجه، استيراتيجيه مكافحه الجرائم المعلوماتيه، رساله ماجيستير، معهد البحوث والدراسات الاستيراتيجيه، جامعه ام درمان الاسلامية، السودان، 2014، ص54.

[3] محمود محمد صفاء الدين علي شرشر، الجهود الدولية والتشريعية لمكافحة جرائم الانترنت، مجلة البحوث القانونية والاقتصادية، مجلد54، عدد3، أكتوبر،2021، ص540-543.

الموضوع من خلال البحث في التنظيم القانوني للجرائم الإلكترونية المتعلقة بالأشخاص (المطلب الأول)، ثم يتناول الباحث التنظيم القانوني للجرائم الإلكترونية المتعلقة بالأموال (المطلب الثاني).

المطلب الأول: التنظيم القانوني للجرائم الإلكترونية المتعلقة بالأشخاص

تعتبر الجرائم الإلكترونية التي تستهدف الحياة الخاصة للأشخاص من أكثر الجرائم إنتشاراً، وتأخذ صوراً وأشكالاً عدة، وأطلقت التشريعات الدولية والوطنية على هذا النوع من الجرائم الاعتداء على الحياة الخاصة للأفراد، فحق حماية الحياة الخاصة من أهم الحقوق؛ وذلك لارتباطه ارتباطاً وثيقاً بخصوصية الأفراد، وبالتالي تشكل الجريمة الإلكترونية خطراً وتهديداً حقيقياً لإحترام حياة الأفراد الخاصة.

ومن صور الاعتداء على الحياة الخاصة للأفراد، كأن يقوم الجاني بجمع البيانات وتخزينها على نحو غير مشروع، والإفشاء غير المشروع لتلك البيانات أو إساءة استعمالها، وكذلك الاعتداء على سرية المكالمات والاتصالات والمراسلات، الاعتداء على حقوق الملكية الفكرية والأدبية، كالسطو على بنوك المعلومات دون إذن صاحبها، ناهيك عن الذم والتشهير والتهديد التي تعتبر من أكثر الجرائم ذيوعاً وانتشاراً[1].

كما قد يتخذ الاعتداء على الأفراد صوراً أخطر من ذلك، فقد يصل إلى حد القتل، كأن يقوم الجاني باختراق النظام الإلكتروني لمستشفى ما ويجري تغيراً على ذلك النظام بما يتسبب بموت أحد المرضى.

[1] عبد الحكيم مولاي إبراهيم، الجرائم الإلكترونية، مرجع سابق، ص216.

إجمالاً يهدف هذا النوع من الجرائم إلى الحط من المكانة الإجتماعية للأشخاص والإساءة لهم بشكل مباشر أو غير مباشر، إذ تعتبر شبكة الإنترنت المكان الأفضل لمثل هذه الجرائم؛ ويعزا ذلك لسرعة ارتكابها، وسهولة انتشارها، عدا عن البعد المكاني بين الجاني والمجني عليه، بالإضافة إلى كافة الخصائص التي تتميز بها الجريمة الإلكترونية، وكذلك صعوبات الحد منها والتي أشرنا لها في المبحث الأول من البحث.

وقد جاء تجريم هذا النوع من الجرائم في التشريعات الدولية، وكذلك على مستوى التشريعات الوطنية، وسيتناول الباحث ذلك من خلال التطرق إلى التنظيم القانوني للجريمة الإلكترونية المتعلقة بالأشخاص في الاتفاقيات الدولية والإقليمية (الفرع الأول)، على أن يتطرق إلى التنظيم القانوني للجريمة الإلكترونية المتعلقة بالأشخاص وفقاً للقانون الفلسطيني رقم 10 لسنة 2018 وتعديلاته (الفرع الثاني).

الفرع الأول: التنظيم القانوني للجريمة الإلكترونية المتعلقة بالأشخاص في الاتفاقيات الدولية والإقليمية

من جملة المواضيع الدولية التي اهتم بها المجتمع الدولي وتطرق إلى البحث والتفصيل فيها وما زال الجرائم الإلكترونية؛ إذ أُبرمت الاتفاقيات الدولية ذات العلاقة بالجريمة الإلكترونية، فتناولت ماهيتها وأركانها وخصائصها، وحددت الإطار القانوني الذي ينظمها، عدا عن أنها فصّلت في الجرائم الإلكترونية الواقعة على الأشخاص وتلك الواقعة على الأموال.

ومن بين الجرائم التي من الممكن أن ترتكب بواسطة الإنترنت والشبكات الإلكترونية والتي ترتبط بالأشخاص جرائم السب والقذف عبر الإنترنت، وجرائم التعدي على الحياة الخاصة، وكذلك الجرائم

المتعلقة بالإخلال بالآداب العامة عبر الإنترنت، وغيرها من الجرائم التي تناولتها الاتفاقيات الدولية.

وسنتناول في هذا الفرع التنظيم القانوني للجرائم الإلكترونية الواقعة على الأشخاص في الاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست) (أولاً)، كما سنتطرق لتناول التنظيم القانوني للجريمة الإلكترونية الواقعة على الأشخاص من خلال الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (ثانياً).

أولاً: الجريمة الواقعة على الأشخاص في الاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست):

إدراكاً لخطورة الجريمة الإلكترونية ومدى إمكانية استخدام شبكات الكمبيوتر لارتكاب جرائم جنائية، وأن الأدلة المتعلقة بمثل هذه الجرائم يمكن تخزينها ونقلها عبر هذه الشبكات، ومما يزيد من خطورة الجرائم الإلكترونية اعتبارها جريمة عابرة للحدود، لذلك فقد توجهت العديد من الدول نحو التوقيع على الاتفاقية المتعلقة بالجريمة الإلكترونية بتاريخ 2001/11/23 في العاصمة المجرية بودابست، وقد اهتمت هذه الاتفاقية بحماية المجتمعات من خطر الجريمة الإلكترونية من خلال تبني تشريعات ملائمة لعمق التغييرات التي أحدثتها الرقمنة والالتقائية والعولمة المتواصلة لشبكات الكمبيوتر.

وتأتي أهمية اتفاقية بودابست من كونها جاءت كضرورة لردع الأعمال الموجهة ضد سرية وسلامة النظم الحاسوبية والشبكات والبيانات وإساءة استخدامها، وذلك من خلال النص على تجريم مثل تلك السلوكيات، بالإضافة إلى اعتماد كافة الصلاحيات اللازمة من اجل تحقيق مكافحة فعالة للجرائم الإلكترونية، من خلال تيسير إجراءات كشفها والتحقيق بشأنها ومقاضاة مرتكبيها على المستويين الدولي والوطني. ناهيك عن خلق ترتيبات لأجل تحقيق تعاون دولي موثوق وسريع.

وقد أكدت ديباجة اتفاقية بودابست على أن هذه الاتفاقية إنما جاءت مكملة للاتفاقيات المتعلقة بحقوق الإنسان وحقوق الطفل والاتفاقيات المتعلقة بحماية الأفراد فيما يخص المعالجة الآلية للبيانات الشخصية، لذلك فقد حرصت على تأمين توازن ملائم بين إنفاذ القانون من جهة واحترام حقوق الإنسان والحريات الأساسية من جهة أخرى، بالإضافة إلى تعزيز فعالية التحقيقات والإجراءات الجنائية المتعلقة بنظم وبيانات الحاسوب، والتمكن من جمع الأدلة في الجرائم الإلكترونية[1].

وبالاستناد إلى بند النفاذ غير المشروع وبند الاعتراض غير المشروع الوارد ذكرهما في الفصل الأول من الباب الأول من اتفاقية بودابست، فقد ألزمت الاتفاقية في فصلها الثاني المتعلق بالجرائم ذات الصلة بالكمبيوتر الدول الأطراف باتخاذ التدابير التشريعية اللازمة لمواجهة جريمة التزوير والاحتيال المرتبطة بالكمبيوتر وكذلك الجرائم ذات الصلة بمواد إباحية عن الأطفال[2].

كذلك فقد تضمنت اتفاقية بودابست المتعلقة بالجريمة الإلكترونية بين فصولها ما ينسب إلى الجرائم المتعلقة بانتهاكات حقوق الأشخاص كحقوق النشر والتأليف وحقوق الملكية الفكرية، وهو ما أكدت عليه المادة 10 في الفصل الرابع من الاتفاقية[3].

فمن خلال هذه المادة يتضح مدى حرص التشريعات الدولية على إلزام الدول باتخاذ التدابير اللازمة في تشريعاتها الوطنية لتجريم الأفعال التي تنتهك حقوق النشر والتأليف، وذلك انطلاقاً من وثيقة باريس المؤرخة بتاريخ 24/يوليو/1971، وكذلك تجريم الأفعال التي تمس حقوق الملكية

---

[1] الاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست)، الديباجة، مجلس أوروبا، مجموعة المعاهدات الأوروبية، رقم 185، 2001/11/23، ص2.

[2] المادة 7 و8 و9 من الاتفاقية المتعلقة بالجريمة الإلكترونية، مرجع سابق. وكذلك: محمود محمد صفاء الدين علي شرشر، مرجع سابق، ص547.

[3] الاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست)، الفصل الرابع، المادة 10.

الفكرية، وذلك انطلاقاً من الاتفاق الخاص بجوانب حقوق الملكية الفكرية المتصلة بالتجارة، ومعاهدة حقوق المؤلف للمنظمة العالمية للملكية الفكرية[1].

كما تطرقت اتفاقية بودابست إلى إلزام كل دولة طرف فيها باتخاذ التدابير التشريعية اللازمة التي من شأنها أن تجرم كل فعل يمس حقوق الفنانيين الأدائيين ومنتجي الاسطوانات وكذلك هيئات البث الإذاعي، وذلك وفقاً لاتفاقية روما المتعلقة بحقوق الفنانيين الأدائيين ومنتجي الاسطوانات وهيئات البث الإذاعي، وكذلك معاهدة الويبو الخاصة بالأداء والتسجيلات الصوتية[2].

علماً أن الاتفاقية منحت الدول الأطراف بالاحتفاظ بحق عدم فرض المسؤولية الجنائية على ما ورد في الفقرتين 1 و2 من المادة 10 منها، وذلك مع ضمان توافر سبل فعالة لتحقيق الإنصاف، على أن تلتزم الدولة بالالتزامات الدولية من المنصوص عليها في الاتفاقيات والمعاهدات الواردة في

---

[1] المنظمة العالمية للملكية الفكرية (WIPO) أنشأت عام 1967 في مدينة ستوكهولم، وأصبحت إحدى وكالات هيئة الأمم المتحدة المتخصصة بتاريخ 17\12\1974، على الرابط التالي: https://www.wipo.int/portal/ar/، تاريخ الإطلاع:8\10\2024، على الساعة 8 مساءاً.

والاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست)، نصت في المادة 10، الفقرة 1، على أنه" تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني: انتهاك حقوق النشر والتأليف، وفقا لتعريفها بموجب القانون الخاص بتلك الدولة الطرف، وتبعاً لالتزاماتها بموجب وثيقة باريس المؤرخة في 24 يوليو/تموز 1971 والمنقحة لاتفاقية برن لحماية المصنفات الأدبية والفنية، والاتفاق الخاص بجوانب حقوق الملكية الفكرية المتصلة بالتجارة، ومعاهدة حقوق المؤلف للمنظمة العالمية للملكية الفكرية باستثناء أي حقوق معنوية مخولة بموجب هذه الاتفاقيات، عندما تُرتكب هذه الأفعال عمداً على نطاق تجاري وبواسطة نظام الكمبيوتر".

[2] بهدف حماية حقوق المؤلفين على مصنفاتهم الأدبية بأكثر الطرق فعالية تم إبرام اتفاقية برن الدوليةبتاريخ 9\9\1886، والمكملة في باريس في مايو 1896، والمعدلة في برلين بتاريخ 13\9\1908، والمكملة ببرن بتاريخ 20\3\1914، والمعدلة في روما عام 1928، وبروكسل عام 1948، واستوكهولم عام 1967، وباريس عام 1971. أنظر: محمود محمد صفاء الدين علي شرشر، مرجع سابق، ص538.

وتنص الفقرة 2 من المادة 10 من اتفاقية بودابست، على أنه " تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني :انتهاك الحقوق ذات الصلة، وفقا لتعريفها بموجب القانون الخاص بتلك الدولة الطرف، وتبعاً لالتزاماتها بموجب الاتفاقية الدولية لحماية الفنانين الأدائيين ومنتجي الاسطوانات وهيئات البث الإذاعي (اتفاقية روما)، والاتفاق الخاص بجوانب حقوق الملكية الفكرية المتصلة بالتجارة، ومعاهدة الويبو بشأن الأداء والتسجيلات الصوتية، باستثناء أي حقوق معنوية مخولة بموجب هذه الاتفاقيات، عندما تُرتكب هذه الأفعال عمداً على نطاق تجاري وبواسطة نظام الكمبيوتر".

الفقرات 1 و2 من المادة 10[1]. ونلاحظ في ذلك مدى حرص التشريعات الدولية على ضمان عدم التعدي على حقوق الأشخاص من خلال شبكات الإنترنت والكمبيوتر.

وحرصاً على حماية الأشخاص من الجرائم الإلكترونية التي قد ترتكب ضدهم، نشير إلى أن اتفاقية بودابست في فصلها الخامس المتعلق بالمسؤولية الإضافية والعقوبات، قد ألزمت الدول الأطراف باتخاذ التدابير التشريعية اللازمة لتجريم الأفعال المرتبطة بالمحاولة والمساعدة والتحريض على أي جريمة من الجرائم الوارد في المواد 2–10 من الاتفاقية إذا ما ارتكبت بشكل متعمد وبسوء نية[2].

وعلى الرغم من أن التقرير التفسيري لاتفاقية بودابست لا يشكل تفسيراً ذي حجية للاتفاقية، فهو ذو طبيعة تسهل تطبيق البنود الواردة في الاتفاقية[3]، فقد أكد على ضرورة أن يواكب القانون الجنائي التطورات التكنولوجية التي تتيح الفرصة لإساءة استخدام مرافق الفضاء الإلكتروني فيُرتكب من خلالها جرائم تقليدية ضد سلامة الأشخاص المحميين وفقاً للقانون الجنائي[4].

وأشار التقرير التفسيري للاتفاقية إلى أهم التهديدات الأساسية المتصلة بالكمبيوتر والمخلة بسرية وسلامة البيانات وأنظمة الكمبيوتر، حيث تستخدم أنظمة الحاسوب والاتصالات كوسيلة للهجوم على المصالح المحمية بموجب القانون الجنائي كالغش والتزوير واستغلال الأطفال في المواد الإباحية من خلال أجهزة الحاسوب والإنترنت[5].

---

[1] وهو ما أكدت عليه الفقرة 3 من المادة 10 من اتفاقية بودابست، إذ نصت على أنه " يجوز للدولة الطرف الاحتفاظ بالحق في عدم فرض المسؤولية الجنائية بموجب الفقرتين1 و2 من هذه المادة في ظروف محدودة شريطة توافر سبل فعالة أخرى للانتصاف، وأن يتقيد هذا التحفظ بالالتزامات الدولية للدولة الطرف المنصوص عليها في الصكوك الدولية المشار إليها في الفقرتين 1 و2 من هذه المادة".

[2] المادة 11 من اتفاقية بودابست المتعلقة بالمحاولة والمساعدة والتحريض.

[3] جاء في ثانياً من التقرير التفسيري لإتفافية الجريمة الإلكترونية الصادر عن مجلس أوروبا بتاريخ 8/نوفمبر/2001، في الصفحة الأولى منه أنه " لا يشكل نص هذا التقرير التفسيري أداة توفر تفسيرا ذي حجية للاتفاقية، على الرغم من أنه قد يكون ذا طبيعة تسهل تطبيق الأحكام الواردة فيه".

[4] الفقرة 8 و9 من التقرير التفسيري لاتفاقية الجريمة الإلكترونية، مرجع سابق، ص2

[5] الفقرة 35 من التقرير التفسيري لاتفاقية الجريمة الإلكترونية، مرجع سابق، ص7.

ثانياً: الجرائم الواقعة على الأشخاص في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[1]

في إطار مواجهة الجرائم الإلكترونية ودرء مخاطرها جاءت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من أجل تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة الجرائم الإلكترونية، وذلك حفاظاً على أمنها وسلامة مجتمعها وأفرادها، موضحةً مجالات تطبيق هذه الاتفاقية مع مراعاة صون مبدأ سيادة الدولة.

واستناداً إلى مبدأ النفاذ غير المشروع وكذلك الاعتراض غير المشروع الوارد ذكرهما في المادة 6 و7 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، فقد ألزمت الاتفاقية الدول الأطراف بتجريم الأفعال المنصوص عليها في الفصل الثاني من الاتفاقية، وذلك وفقاً لتشريعاتها وأنظمتها الداخلية[2].

وتجدر الإشارة في هذا الصدد إلى أن جريمة الدخول إلى تقنية المعلومات جريمة قصديه، تقوم بالقصد الجنائي العام، أي بتوافر العلم والإرادة، إذ يكفي أن يعلم الجاني أنه يدخل أو يقوم بالاتصال غير المشروع بنظام تقنية معلومات خاصة بالغير دون أن يكون له الحق في ذلك[3].

ومن ضمن الأفعال المجرمة، نظمت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات تلك الأفعال المتعلقة بالأشخاص، كجريمة التزوير وجريمة الاحتيال والجرائم المرتبطة بالاعتداء على حرمة الحياة الخاصة، وغيرها من الجرائم التي تناولتها بنود الاتفاقية.

حيث أكدت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على التزام الدول الأطراف باتخاذ كافة التدابير اللازمة لمنع كل ما يتعلق بالجرائم الإلكترونية وضرورة التحقيق فيها وملاحقة مرتكبيها،

---

[1] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الأمانة العامة لجامعة الدول العربية، القاهرة، 2010/12/21، الفصل الأول، المواد 1 و3 و4.

[2] المادة 5 المتعلقة بالتجريم من الفصل الثاني من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[3] أحمد حمي، وزهيرة كيسي، صور جرائم تقنية المعلومات وفقا لالتفاقية العربية لسنة 2014، مجلة العلوم القانونية والسياسية، مجلد10، عدد1، كلية القانون والعلوم السياسية، جامعة ديالي، العراق، ابريل، 2019، ص781.

فتناولت المادة 10 من الاتفاقية جريمة التزوير، وأوضحت المقصود بجريمة التزوير الإلكترونية على أنها استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييراً من شأنه إحداث ضرر، وبنية استعمالها كبيانات صحيحة"[1].

فيما تناولت المادة 11 من الاتفاقية جريمة أخرى من الجرائم الإلكترونية والمتعلقة بالاحتيال الإلكتروني، وأوضحت أن جريمة الاحتيال تقع بمجرد التسبب بالضرر للمستخدمين عن قصد وبدون وجه حق لتحقيق مصلحة أو منفعة بطريقة غير مشروعة سواء للفاعل أو لغيره، ويكون ذلك من خلال مجموعة من الإجراءات الواردة بنص المادة 11، كإدخال أو تعديل أو محو أو حجب للمعلومات، أو إجراء تعطيل في وظيفة أنظمة التشغيل وأنظمة الاتصالات ومحاولة تغييرها، أو من خلال تعطيل الأجهزة والبرامج والمواقع الإلكترونية[2].

كذلك فقد تطرقت الاتفاقية العربية لجريمة أخرى أكدت عليها اتفاقية بودابست، ويتعلق الأمر بجريمة الإباحية، وذلك بنص المادة 12 منها، إذ أشار نص المادة إلى أن كل إنتاج أو توزيع أو عرض أو توفير أو شراء أو بيع أو نشر أو استيراد لمواد إباحية من خلال التقنيات الإلكترونية يعتبر جريمة إباحة[3]. وقد شدد نص المادة 12 على عقوبة الجرائم المتعلقة بالإباحية التي تستغل الأطفال والقصر، إذ أكدت على أن العقوبة تتشدد بمجرد حيازة مواد إباحية متعلقة بالأطفال والقصر عن طريق التقنيات الإلكترونية[4].

ومن الملاحظ هنا أن نص المادة 12 من الاتفاقية جرمت مواد الإباحية بشكلٍ عام ولم تقتصرها فحسب على المواد الإباحية المتعلقة بالأطفال القصر، باعتبارها جريمة مخلة بالآداب والحياء

---

[1] المادة 10 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

وكذلك: أحمد حمي، وزهيرة كيسي، مرجع سابق، ص783.

[2] المادة 11 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[3] البند 1 من نص المادة 12 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[4] البند 2 و3 من نص المادة 12 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

العام، فميزت في العقوبة بين حيازة المواد الإباحية وبين حيازة المواد الإباحية المتعلقة بالأطفال والقصر، وهو ما لم تعمل به اتفاقية بودابست المتعلقة بالجرائم الإلكترونية، وربما ذلك راجع لاختلاف طبيعة الثقافة والقيم التي تحكم المجتمعات، إذ إنه لكل مجتمع قيمه وثقافته الخاصة به التي تميزه عن غيره من المجتمعات.

وأشارت المادة 13 من الاتفاقية كذلك إلى أساليب أخرى مرتبطة بالإباحية كالمقامرة والإستغلال الجنسي وهي بذلك امتداد لنص المادة 12 التي جرمت الفعل الإباحي بكافة أشكاله وأساليبه[1]. وقد أكدت الاتفاقية على أن الاعتداء على حرمة الحياة الخاصة بواسطة التقنيات الإلكترونية، يشكل جريمة يعاقب عليها القانون، حيث ورد ذلك بنص المادة 14 من الاتفاقية والتي تناولت جريمة الاعتداء على حرمة الحياة الخاصة بواسطة تقنيات إلكترونية[2].

وقد نصت المادة 16 من الاتفاقية العربية على الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات وهي: 1- القيام بعمليات غسل أموال أو طلب المساعدة أو نشر طرق القيام بغسل الأموال. 2- الترويج للمخدرات والمؤثرات العقلية أو الاتجار بها. 3- الاتجار بالأشخاص.4- الاتجار بالأعضاء البشرية.5- الاتجار غير المشروع بالأسلحة.

ويتضح أن المادة 16 اشترطت أن تكون الجرائم المنظمة الواردة أعلاه مرتكبة بواسطة تقنية المعلومات لتأخذ وصف الجرائم المعلوماتية أو جرائم تقنية المعلومات، إذ يمكن تطبيق الأحكام الموضوعية والإجرائية عليها، التي جاءت بها الاتفاقية العربية[3].

---

[1] المادة 13 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[2] المادة 14 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[3] وردة شرف الدين، الأحكام الإجرائية لمكافحة جريمة الاتجار بالأشخاص المرتكبة بواسطة تقنية المعلومات دراسة ضمن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 ، مجلة الإجتهاد القضائي، عدد16، كلية الحقوق، جامعة محمد خيضر بسكرة، الجزائر، ص98.

وقد تناولت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات شكل آخر من أشكال الجرائم المتعلقة بالأشخاص، وهنا يتعلق الأمر بالجرائم الإلكترونية المرتبطة بانتهاك حقوق المؤلف وكذلك حقوقه المجاورة، إذ أكدت المادة 17 من الاتفاقية تجريم انتهاك حق المؤلف في حال تم ارتكاب الفعل عن قصد ولغير الاستعمال الشخصي، وكذلك تجريم كل فعل يمس الحقوق المجاورة للمؤلف في حال تم ارتكاب الفعل عن قصد ولغير الاستعمال الشخصي، وذلك حسب القانون المعمول به في كل دولة طرف[1].

ويُفهم من عبارة الحقوق المجاورة للمؤلف أي الحقوق الناشئة عن استغلال المصنفات الأدبية والفنية والصناعية والتجارية، لذلك سعت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من خلال المادة 17 إلى حماية الملكية الفكرية للمؤلف، كحماية الحقوق الواردة على براءات الاختراع، وحماية الحقوق الواردة على العلامات التجارية والصناعية.

ومن الملاحظ أن نص المادة 17 ذكرت مسألة الحقوق المجاورة للمؤلف دون التفصيل فيها، بل تركت مسألة التفصيل فيها للقانون المطبق في كل دولة طرف في الاتفاقية، وذلك تجنباً للاختلاف بين التشريعات الوطنية للدول الأطراف، فقد تتناولها بعض التشريعات الوطنية بنوع من التوسع، في حين أن تشريع وطني آخر قد يتناولها دون التوسع في جميع الحالات التي تطرق لها تشريع آخر، وفي ذلك نوع من ترك المساحة للتشريعات الوطنية في تناول الحالات التي تندرج تحت مسمى الحقوق المجاورة للمؤلف.

[1] المادة 17 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

الفرع الثاني: التنظيم القانوني للجريمة الإلكترونية المتعلقة بالأشخاص وفقاً للقانون رقم 10 لسنة 2018م وتعديلاته

أخذ المشرع الفلسطيني بالنهج الذي سارت عليه الاتفاقيات الدولية بعدم وضع تعريفاً محدداً لمفهوم الجريمة الإلكترونية، وذلك على اعتبار أنها جريمة حديثة ما زالت تشهد تطورات وحالات كثيرة، ومن الممكن أن يؤدي وضع تعريف محدد لها حالياً إلى عدم اشتمال هذا التعريف على حالات مستقبلية يمكن أن تصنف على أنها جرائم إلكترونية.

كذلك فإن فهم الجرائم الإلكترونية ووضع تعريف محدد لها يعتمد بالأساس على الحالات التي يمكن اعتبارها جريمة إلكترونية، وبالتالي فإن وضع مفهوم محدد للجريمة الإلكترونية بناء على الحالات المعروفة حالياً، من الممكن أن يؤدي إلى عدم اعتبار حالات جديدة مستقبلاً ضمن الجرائم الإلكترونية لكون المفهوم لم يحددها.

ونظراً لما تشكله الجرائم الإلكترونية من مخاطر عديدة تهدد أمن المجتمع واستقرار الأفراد، فإن المشرع الفلسطيني أصدر قانوناً يتعلق بالجرائم الإلكترونية بحد ذاتها، وعلى الرغم من هذه الخطوة جاءت متأخرة نوعاً ما، تبقى خطوة صحيحة في المسار الصحيح، وتجد أساسها في القانون الأساسي الفلسطيني المعدل لسنة 2003، الذي أشار إلى مسألة حظر الاعتداء على الحريات الشخصية وحرمة الحياة الخاصة، وجاء ذلك وفقاً لنص المادة 32 من القانون الأساسي الفلسطيني[1].

[1] نصت المادة 32 من القانون الأساسي الفلسطيني المعدل لسنة 2003 على أنه "كل اعتداء على أي من الحريات الشخصية أو حرمة الحياة الخاصة للإنسان وغيرها من الحقوق والحريات العامة التي يكفلها القانون الأساسي أو القانون، جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم، وتضمن السلطة الوطنية تعويضاً عادلاً لمن وقع عليه الضرر".

وعملاً بمضمون المادة 3(2) من القانون الأساسي الفلسطيني المعدل لسنة 2003، واستناداً لقانون العقوبات رقم (74) لسنة 1936م ولقانون العقوبات رقم (16) لسنة 1960م، فقد أصدر المشرع الفلسطيني القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، ونظراً للتطورات التي تعرفها التقنيات الإلكترونية، وبروز العديد من الحالات التي تصنف على أنها جرائم إلكترونية، فقد ألغى المشرع الفلسطيني القرار بقانون رقم 16 لسنة 2017، وأصدر القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية، والذي خضع بدوره لتعديلات عديدة، فصدر القرار بقانون رقم 28 لسنة 2020 بشأن الجرائم الإلكترونية.

وحرصاً من المشرع الفلسطيني على مراعاة التطورات الواقعة على موضوع الجرائم الإلكترونية، وحرصاً منه كذلك على مواءمة التشريع الوطني الفلسطيني مع الاتفاقيات الدولية وإحداث التناغم بينهما، فقد أجرى المشرع الفلسطيني بتاريخ 2021/12/23 تعديلاً أخراً على القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية ورمز إليه بالقرار رقم 38 لسنة 2021، فأصدر القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات رقم 10 لسنة 2018 وتعديلاته.

وقد تناول القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية في مواده تنظيم الجرائم الإلكترونية المتعلقة بالأشخاص من قبيل جرائم التزوير والتهديد والابتزاز والسب والقذف الخادش للشرف والاعتبار من خلال التقنيات الإلكترونية، وكذلك الجرائم المتعلقة بالإباحية، وجرائم التعدي على حرمة الحياة الخاصة، وجريمة الاتجار بالبشر والأعضاء البشرية، وجريمة الاتجار أو الترويج للمخدرات والمؤثرات العقلية، وسنتناول كل جريمة من هذه الجرائم بنوع من التفصيل.

وقد جرم القرار بقانون رقم 10 لسنة 2018 وتعديلاته كل حيازة لأي جهاز أو برنامج أو بيانات إلكترونية أو كلمة سر أو ترامیز دخول أو قدمها أو وزعها أو أنتجها أو روج لها أو استدوردها أو أصدرها بغرض اقتراف أي من الجرائم المنصوص عليها في القانون رقم 10 لسنة 2018 وتعديلاته، وحدد عقوبة ذلك بالسجن مدة لا تزيد عن 5 سنوات، وبغرامة مالية لا تقل عن 3000 آلاف دينار أردني ولا تزيد عن 5000 آلاف دينار أردني أو ما يعادلها بالعلمة المتداولة قانوناً[1].

إذ أشارت المادة (11) ضمن بنودها (7) إلى جريمة تزوير المستندات التي من شأنها أن تحدث ضرراً، وأكد على أن هذه الجريمة يعاقب عليها القانون بالعقوبة السالبة للحرية (الحبس) أو بفرض الغرامة المالية[2]، فيما تناول البند 1 من المادة 12 من القانون، تجريم استخدام الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات دون وجه حق للوصول إلى أرقام أو بيانات وسيلة التعامل الإلكترونية أو التلاعب فيها، وحددت عقوبتها بالحبس مدة لا تقل عن ستة أشهر أو بغرامة مالية لا تقل عن 500 دينار أردني ولا تزيد عن 1000 دينار أردني أو ما يعادلها بالعملة المتداولة أو بكلتا العقوبتين[3].

فيما أشار البند (2) من المادة (12) من القانون إلى أن ذات العقوبة المقررة في البند 1 من المادة 12 تنطبق على كل من زور وسيلة تعامل إلكترونية بأي وسيلة كانت أو حاز بدون ترخيص أجهزة تستخدم لإصدار أو تزوير بطاقة التعامل الإلكتروني[4]. كما أكد البند 3 من المادة 12 من القانون على أن تسهيل استخدام وسيلة تعامل إلكترونية مزورة مع العلم بذلك أو قبل وسيلة تعامل

---

[1] المادة 26 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[2] بنود المادة 11 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[3] البند 1 من المادة 12 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[4] البند 2 من المادة 12 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

إلكترونية منهية الصلاحية أو مسروقة مع العلم بذلك توجب العقوبة المنصوص عليها في البند 1 من المادة 12[1].

أما في حال أخذ الشخص أموالاً مقابل أي فعل من الأفعال الواردة في نص المادة 12، فإن المشرع الفلسطيني شدد العقوبة في هذه الحالة، حيث أشار البند 4 من المادة 12 إلى أن ارتكاب أي فعل من الأفعال الواردة بحكم المادة 12 بقصد الحصول على أموال أو بيانات الغير أو ما تتيحه من خدمات، تعتبر جريمة يعاقب عليها بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن 1000 دينار أردني ولا تزيد عن 3000 آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً أو بكلتا العقوبتين[2].

وفي حال ارتكب الشخص أي فعل من الأفعال الواردة في نص المادة 12 من القانون لغرض الإستيلاء على أموال الغير لنفسه أو لغيره، فإن عقوبته تكون مشددة، إذ تصل إلى الحبس مدة سنتين على الأقل أو بغرامة مالية لا تقل عن 3000 آلاف دينار أردني ولا تزيد عن 5000 آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً أو بكلتا العقوبتين[3].

ومن الجرائم الإلكترونية المتعلقة بالأشخاص والتي نظمها القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات الجرائم الخادشة للشرف والاعتبار وكذلك جريمة التهديد والابتزاز، إذ أشارت المادة 15 من القانون إلى أن جريمة تهديد أو ابتزاز شخص آخر من خلال الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات

---

[1] البند 3 من المادة 12 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[2] البند 4 من المادة 12 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[3] البند 5 من المادة 12 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات. أنظر كذلك: أحمد البراك، عبد القادر جرادة، الجرائم الإلكترونية في التشريع الفلسطيني دراسة تحليلية تأصيلية مقارنة، دار الشروق للنشر والتوزيع، رام الله، 2019، ص167.

لحمله على القيام بفعل ولو كان مشروعاً أو الامتناع عن فعل ولو كان مشروعاً، يعاقب عليها بالحبس مدة لا تقل عن سنة ولا تزيد عن سنتين، بالإضافة إلى سنتين حبس مع وقف التنفيذ لمدة خمس سنوات تبدأ من انتهاء العقوبة الفعلية وبغرامة مالية لا تقل عن 1000 دينار أردني ولا تزيد عن 3000 آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً[1].

وكذلك أشارت المادة 15 إلى جريمة السب والقذف الخادش للشرف والاعتبار من خلال الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات والتي تصل إلى درجة الجناية، إذ أقرت عقوبتها بالحبس مدة لا تقل عن سنتين ولا تزيد عن ثلاث سنوات، بالإضافة لثلاث سنوات حبس مع وقف التنفيذ لمدة خمس سنوات تبدأ من انتهاء العقوبة الفعلية، وبغرامة مالية لا تقل عن خمسة آلاف دينار أردني ولا تزيد عن عشرة آلالف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً[2].

ومن الملاحظ أن المشرع الفلسطيني وفي إطار تطبيق العقوبة على جرائم التهديد والابتزاز وجرائم السب والقذف الخادش للشرف والاعتبار أخذ بتطبيق عقوبة الحبس والغرامة معاً، وذلك نظراً لخطورة هذه الجرائم وما قد ينتج عنها من أضرار تمس كرامة الأشخاص.

كما وقد نظم القرار بقانون رقم 10 لسنة 2018 وتعديلاته الجرائم المتعلقة بالأعمال الإباحية، وقد أخذ المشرع الفلسطيني بالتوجه الذي سارت عليه الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في التمييز بين الأعمال الإباحية لمن أعمارهم فوق الثامنة عشر سنة ميلادية، وبين الأعمال الإباحية لمن أعمارهم دون الثامنة عشر سنة ميلادية.

---

[1] البند 1 من المادة 15 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

أنظر القضية رقم 332\2023، المنعقدة أمام محكمة النقض، رام الله، 24\سبتمبر\2023، وموضوعها: استعمال الشبكة العنكبوتية أو إحدى وسائل تكنولوجيا المعلومات وإسناد أمور خادشة للشرف أو الإعتبار.

[2] البند 2 من المادة 15 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

إذ نصت المادة 16 من القانون على تجريم كل من يرسل عمداً أعمالاً إباحية مسموعة كانت أو مقروءة أو مرئية من خلال الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات لمن هم فوق الثامنة عشر سنة ميلادية دون رضاهم، وأقر عقوبتها بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد عن سنتين، أو بغرامة مالية لا تقل عن 200 دينار أردني ولا تزيد عن 1000 دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً أو بكلتا العقوبتين[1].

في حين نصت المادة 16 من القانون على تجريم كل من يرسل عمداً أعمالاً إباحية مسموعة كانت أو مقروءة أو مرئية من خلال الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات لمن هم دون الثامنة عشر سنة ميلادية أو تتعلق بالإستغلال الجنسي لهم، وأقر عقوبتها بالحبس مدة لا تقل عن سنة، أو بغرامة مالية لا تقل عن 1000 دينار أردني ولا تزيد عن 3000 دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً أو بكلتا العقوبتين[2].

وقد جرم القانون رقم 10 لسنة 2018 وتعديلاته كل من يستخدم الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات قاصداً إعداد أو حفظ أو عرض أو معالجة أو ترويج أو نشر أنشطة إباحية بهدف التأثير على من هم دون الثامنة عشرة سنة ميلادية أو من هم من ذوي الإعاقة، وحددت المادة 16 عقوبة ذلك بالحبس مدة لا تقل عن سنتين أو بغرامة مالية لا تقل عن 1000 دينار أردني ولا تزيد عن 3000 آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً أو بكلتا العقوبتين[3].

---

[1] البند 1 من المادة 16 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[2] البند 2 من المادة 16 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات. راجع كذلك: أحمد البراك، عبد القادر جرادة، مرجع سابق، ص292.

[3] البند 3 من المادة 16 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

ومن بين السلوكيات المرتبطة بالجرائم الإلكترونية المتعلقة بالأموال، جريمة المخدرات والمؤثرات العقلية فقد نظم القرار بقانون رقم 10 لسنة 2018 وتعديلاته المتعلق بالجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات، جريمة المخدرات والمؤثرات العقلية، وذلك من خلال نص المادة 19 منه، الذي أكد على أن كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو إحدى وسائل تكنولوجيا المعلومات بغرض الاتجار أو الترويج للمخدرات والمؤثرات العقلية وكل ما يرتبط بها أو سهل التعامل فيها من بيع أو شرح أو عرض طرق إنتاج المواد المخدرة، يعاقب بالسجن مدة لا تقل عن 10 سنوات أو بغرامة مالية لا تقل عن 3000 آلاف دينار أردني ولا تزيد عن 5000 آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً أو بكلتا العقوبتين[1].

وكذلك فقد اهتم القرار بقانون رقم 10 لسنة 2018 وتعديلاته بحماية الحياة الشخصة وتجريم الأفعال التي تشكل اعتداءاً على حرمة الحياة الخاصة للأفراد، إذ نص البند 1 من المادة 22 من القانون على أنه "يحظر التدخل التعسفي أو غير القانوني في خصوصيات أي شخص أو في شؤون أسرته أو بيته أو مراسلاته".

إذ أكدت المادة 22 من القانون على أن كل من ينشأ موقعاً أو حساباً إلكترونياً أو تطبيقاً أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات بغرض نشر صور أو أخبار أو تسيجلات مرئية أو صوتية سواء كانت مباشرة أو مسجلة تصنف على أنها تدخل غير قانوني في الحياة الخاصة أو العائلية للأشخاص حتى وإن كانت صحيحة، يعاقب بالحبس لمدة لا

[1] المادة 19 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته المتعلق بالجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات. وكذلك: أحمد البراك، عبد القادر جرادة، مرجع سابق، ص207.

تقل عن سنة أو بغرامة مالية لا تقل عن 1000 دينار أردني ولا تزيد عن 3000 دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً أو بكلتا العقوبتين[1].

واستناداً لما ورد أعلاه فيمكن القول أن المشرع الفلسطيني كان موفقاً في ملائمة القرار بقانون رقم 10 لسنة 2018 وتعديلاته، إذ أنه جاء متماشياً مع الاتفاقيات الدولية والإقليمية ذات العلاقة، غير أنه بحاجة إلى إعادة النظر في مسألة العقوبات بحيث تكون عقوبات أكثر ردعاً.

المطلب الثاني: التنظيم القانوني للجرائم الإلكترونية المتعلقة بالأموال

من بين أحد أهم الخصائص التي تتميز بها الجرائم الإلكترونية والتي أشرنا لها سابقاً في المبحث الأول من الرسالة أنها تتم بطرق سهلة ولا تحتاج إلى مجهود جماعي كما في الجرائم التقليدية، وكذلك هو الحال بالنسبة للجرائم الواقعة على الأموال، فهي جرائم تحتاج لشخص متخصص في برامج الحاسب الآلي، عدا عن أنها توقع خسائر ضخمة أكبر بكثير من الجرائم التقليدية.

وانطلاقاً من مبدأ النفاذ غير المشروع ومبدأ الاعتراض غير المشروع ومبدأ إساءة استخدام الأجهزة الإلكترونية وما تحتويه من بيانات، فيصبح كل إرسال للبيانات الحاسوبية أو إتلاف أو تعديلها أو حذفها أو تدميرها جريمة إلكترونية يعاقب عليها القانون، ومن الأمثلة على الجرائم الإلكترونية المتعلقة بالأموال تزوير بطاقة الصراف الآلي والسحب عليه، إذ تعد هذه الحالة من حالات السرقة التي تتم من خلال وسيلة إلكترونية وهي بكاقة الصراف الآلي[2].

وسيتناول الباحث من خلال هذا المطلب التنظيم القانوني لبعض الجرائم الإلكترونية الواقع على الأموال، وذلك من خلال التطرق إلى التنظيم القانوني للجريمة الإلكترونية المتعلقة بالأموال في

---

[1] البند 2 من المادة 22 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات. وكذلك: أحمد البراك، عبد القادر جرادة، مرجع سابق، ص259.

[2] هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، مرجع سابق، ص114-115.

الاتفاقيات الدولية والإقليمية (الفرع الأول)، على أن نتناول التنظيم القانوني للجريمة الإلكترونية المتعلقة بالأموال وفقاً للقانون رقم 10 لسنة 2018 وتعديلاته (الفرع الثاني).

الفرع الأول: التنظيم القانوني للجريمة الإلكترونية المتعلقة بالأموال في الاتفاقيات الدولية والإقليمية

سنتطرق من خلال هذا الفرع إلى التنظيم القانوني للجرائم الإلكترونية المتعلقة بالأموال من خلال اتفاقية بودابست المتعلقة بالجرائم الإلكترونية (أولاً)، وكذلك تنظيم الجرائم الإلكترونية المتعلقة بالأموال من خلال الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (ثانياً).

أولاً: التنظيم القانوني للجرائم الإلكترونية المتعلقة بالأموال في اتفاقية بودابست المتعلقة بالجرائم الإلكترونية

إدراكاً للمخاطر الناجمة عن إساءة استخدام الحاسب الآلي والشبكة الإلكترونية، واقتناعاً بضرورة ردع الأعمال الموجهة ضد سلامة وسرية الأنظمة الحاسوبية والشبكات الإلكترونية وبياناتها، فقد نظمت اتفاقية بودابست مجموعة من المواد العامة التي من شأنها أن تحد من الجرائم التي تستهدف الأموال.

وقد سعت اتفاقية بودابست إلى وضع قائمة بالجرائم والتي كانت عبارة عن مبادئ توجيهيه بحيث تشمل الحد الأدنى من التوافق الدولي، دون استبعاد توسيع نطاق القانون المحلي بشأن الجرائم المتصلة بالكمبيوتر، فقد اشتملت اتفاقية بودابست على أهم الجرائم الإلكترونية التي تمثل التهديدات الأساسية لأمن الكمبيوتر وسلامة البيانات التي تتعرض لها معالجة البيانات الإلكترونية وأنظمة الاتصال.

وفي هذا الإطار، قدمت الاتفاقية وصفاً لنوع الجرائم التي تؤدي دوراً أكبر في الممارسة، بحيث تستخدم أنظمة الكمبيوتر والاتصالات كوسيلة للهجوم على بعض المصالح القانونية التي يحميها القانون الجنائي في معظم الأحيان من الهجمات التي تستخدم طرقاً تقليدية.

فقد ألزمت اتفاقية بودابست الدول الأطراف باتخاذ التدابير التشريعية ضد كل فعل يرتكب عمداً وبغير وجه حق بشكل كلي أو جزئي يستهدف الأنظمة والشبكات الإلكترونية[1]، كما أن الاتفاقية ألزمت الدول الأطراف باتخاذ التدابير التشريعية اللازمة لتجريم الأفعال التي ترتكب عمداً وتستهدف البيانات التي تحتويها الأجهزة الإلكترونية سواء بإرسالها أو إتلافها أو حذفها أو تدميرها[2].

وأشارت المادة 4 من اتفاقية بودابست إلى مسألة التدخل في البيانات، إذ ألزمت الدول الأطراف باتخاذ التدابير التشريعية لتجريم الأفعال التي ترتكب عمداً ودون وجه حق لإتلاف بيانات الحاسوب أو تعديلها أو حذفها أو تدميرها أو إفسادها.

كما أكدت المادة 5 من الاتفاقية على مسألة التدخل في النظام، وألزمت الدول الأطراف باتخاذ التدابير اللازمة لتجريم الأفعال التي ترتكب عمداً لإعاقة اشتغال التقنيات الإلكترونية من خلال إدخال بيانات حاسوبية وتغييرها وإرسالها وإتلافها وحذفها.

لكل ذلك فقد نصت المادة 6 من الاتفاقية على مسألة إساءة استخدام الحاسوب، فألزمت الدول الأطراف باتخاذ التدابير اللازمة لتجريم كل فعل متعمد منصوص عليه في المواد 2-5، لإنتاج أو بيع، أو شراء بغرض الاستخدام، أو استيراد، أو توزيع أو إتاحة بأي طرق أخرى من خلال جهاز بما في ذلك برنامج كمبيوتر، تم تصميمه أو ملاءمته مبدئياً، أو من خلال كلمة سر خاصة

[1] المادة 2 من اتفاقية بودابست المتعلقة بالجرائم الإلكترونية لعام 2001.

[2] المادة 3 من اتفاقية بودابست المتعلقة بالجرائم الإلكترونية لعام 2001.

بكمبيوتر، أو رمز الولوج، أو بيانات مماثلة يمكن بواسطتها النفاذ بشكل كامل أو جزئي إلى نظام كمبيوتر[1].

وحول الجرائم ذات الصلة بالكمبيوتر فقد أشارت اتفاقية بودابست إلى جريمة التزوير المرتبطة بالكمبيوتر، إذ ألزمت الدول الأطراف باتخاذ التدابير التشريعية اللازمة لتجريم كل فعل متعمد وبدون وجه حق يقضي بإدخال أو تعديل أو حذف أو إتلاف لبيانات الحاسوب بحيث تبدو البيانات غير الأصلية أصلية بقصد استخدامها لأغراض قانونية، بصرف النظر عما إذا كانت البيانات قابلة للقراءة والفهم بشكل مباشر أم لا[2].

وكذلك نظرت الاتفاقية بمسألة الاحتيال المرتبط بالكمبيوتر، وكذلك ألزمت الدول الأطراف باتخاذ التدابير التشريعية اللازمة لتجريم كل فعل يرتكب بشكل متعمد ودون وجه حق وتسببت في إلحاق الضرر بملكية شخص آخر، كأي إدخال أو تعديل أو إتلاف لبيانات الحاسوب، أو أي تدخل في وظيفة نظام الكمبيوتر للحصول على منفعة اقتصادية ذاتية أو لمصلحة شخص آخر[3].

ومن الملاحظ على نصوص مواد الاتفاقية أنها حددت خصائص للجرائم التي أدرجتها ضمن بنودها من أجل تطبيق المسؤولية الجنائية، ومن بين هذه الخصائص اشترطت بنود الاتفاقية أن يكون ارتكاب الفعل المجرم عمداً، وكذلك الشرط الصريح بأن يكون السلوك المعني بدون وجه حق، وفي ذلك إشارة إلى أنه قد يكون السلوك الموصوف قانونياً أو مبرراً كالموافقة أو الضرورة أو الدفاع عن النفس، وبالتالي تشير عبارة دون وجه حق إلى السلوك الذي يتم دون سلطة سواء تشريعية أو

[1] البند 1 من المادة 6 من اتفاقية بودابست المتعلقة بالجرائم الإلكترونية.

[2] المادة 7 من اتفاقية بودابست المتعلقة بالجرائم الإلكترونية.

[3] المادة 8 من اتفاقية بودابست المتعلقة بالجرائم الإلكترونية.

قضائية أو تنفيذية أو توافقية أو إدارية أو تعاقدية، أو أي سلوك لا تشمله خلاف ذلك الدفوع القانونية، كالأعذار، أو المبررات أو المبادئ ذات الصلة القائمة بموجب القانون المحلي[1].

وقد سعت الجهود الدولية إلى زيادة تعزيز التعاون بشأن الجرائم الإلكترونية وجمع الأدلة في شكل إلكتروني عن أي جريمة جنائية، وذلك لغرض التحقيقات أو إجراءات جنائية محددة من خلال أدوات إضافية تتعلق بالمساعدة المتبادلة الأكثر كفاءة، بالإضافة لأشكال التعاون الأخرى بين السلطات المختصة؛ وإلى تعزيز التعاون في حالات الطوارئ والتعاون المباشر بين السلطات المختصة ومقدمي الخدمات والكيانات الأخرى التي تمتلك أو تتحكم في المعلومات ذات الصلة. وهو ما جاء من أجله البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الإلكترونية بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية[2].

بقي أن نشير أخيراً إلى أن اتفاقية بودابست كانت عبارة عن مبادئ توجيهيه لمكافحة الجرائم الإلكترونية، لذلك فموادها لم تشمل سوى 9 حالات من الجرائم الإلكترونية، ومنها جرائم التزوير والاحتيال من خلال التقنيات الإلكترونية، فلم تشر هذه الاتفاقية إلى مجموعة من الحالات المتعلقة بالأموال كالتجارة الإلكترونية والتحويلات الإلكترونية، وكذلك جرائم غسل الاموال والإرهاب، لذلك لا بد من بذل الجهود لبناء اتفاقية دولية تخص الجرائم الإلكترونية وتتوسع في تناول الحالات المرتبطة بالجريمة الإلكترونية مع مراعاة التطور الهائل الذي عرفه مجال تكنولوجيا المعلومات.

وعلى الرغم من ذلك، أوصت اتفاقية بودابست بضرورة أن تصاغ القوانين والتشريعات الوطنية بأكبر قدر ممكن من الوضوح والخصوصية، وذلك لغرض توفير الإستشراف الملائم لنوع السلوك

---

[1] التقرير التفسيري لاتفاقية الجريمة الإلكترونية، مجلس أوروبا، سلسلة المعاهدات الأوروبية رقم 185، بودابست، 23/نوفمبر/2001، ص8.

[2] البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الإلكترونية بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية، سلسلة معاهدات مجلس أوروبا، 2022، ص2.

المعاقب عليه بعقوبة جنائية. وفي ذات الإطار أكدت الاتفاقية على ضرورة تجريم أي سلوك من غير السلوكات المحددة في مواد الاتفاقية، بما في ذلك ما يسمى باحتلال الفضاء الإلكتروني أو السطو الإلكتروني[1].

كما أن اتفاقية بودابست أكدت على ضرورة أن تعتمد كل دولة طرف فيها مجموعة من التدابير التشريعية وغيرها من التدابير للتأكد من أن الجرائم المنصوص عليها ضمن بنود المادة معاقب عليها بعقوبات فعالة رادعة ومتناسبة بما في ذلك العقوبات السالبة للحرية، بالإضافة إلى مساءلة الأشخاص الاعتباريين وإخضاعهم لتدابير وعقوبات فعالة رادعة ومتناسبة سواء كانت تدابير أو عقوبات جنائية او مالية[2].

ثانياً: تنظيم الجرائم الإلكترونية المتعلقة بالأموال من خلال الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

تطرقت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى تنظيم الجرائم الإلكترونية المتعلقة بالأموال، وذلك من خلال تناولها لموضوع الجرائم المتعلقة بالإرهاب والمرتكبة من خلال تقنية المعلومات، إذ أكدت المادة 15 من الاتفاقية على مجموعة من السلوكيات من قبيل نشر أفكار جماعات إرهابية والدعوة لها، أو تمويل عمليات إرهابية وتسهيل الاتصالات بين التنظيمات الإرهابية، أو نشر طرق صناعة المتفجرات التي تستخدم في عمليات إرهابية، وكذلك نشر الفتن والنعرات الطائفية والاعتداء على الأديان والمعتقدات[3].

[1] التقرير التفسيري لاتفاقية الجريمة الإلكترونية، مرجع سابق، ص8.

[2] المادة 13 من اتفاقية بودابست لمكافحة الجرائم الإلكترونية.

[3] بنود المادة 15 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

واعتبرت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات أن الاستخدام غير المشروع لأدوات الدفع الإلكترونية تشكل جريمة الإلكترونية، إذ أكدت المادة 18 منها على أن تزوير أو وضع أجهزة تساعد على تزوير أو تقليد أي أداة من أدوات الدفع الإلكترونية أو بأي وسيلة كانت تعتبر جريمة إلكترونية تتعلق بالأموال. وكذلك الحال بالنسبة لأي فعل يستولي على بيانات أي أداة من أدوات الدفع واستعملها أو قدمها للغير أو سهل للغير الحصول عليها، أو كل استخدام للشبكة الإلكترونية أو إحدى وسائل تقنية المعلومات في الوصول دون وجه حق إلى أرقام أو بيانات أي أداة من أدوات الدفع، وكذلك كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك. فكل هذه السلوكيات تشكل جرائم إلكترونية يعاقب عليها القانون[1].

ونص الفصل الثالث من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والمعنون بالأحكام الإجرائية، على جملة من الإجراءات الجزائية التي تكفل مكافحة الجريمة المعلوماتية، وتتمثل هذه الإجراءات في: التحفظ العاجل على البيانات المخزنة في تقنية المعلومات، أمر تسليم المعلومات، تفتيش وضبط المعلومات المخزنة، الجمع الفوري للمعلومات[2].

وأخيراً، فإن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ألزمت الدول الاطراف بترتيب المسؤولية الجنائية على الأشخاص الطبيعية والاعتبارية في حال ارتكب ممثلوها سواء باسمها أو لصالحها جريمة إلكترونية، وذلك دون الإخلال بفرض العقوبة على الجاني الذي ارتكب الجريمة

[1] بنود المادة 18 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. كذلك: وردة شرف الدين واحميدة هنية، الحماية الإجرائية للمستهلك من جريمة الاستخدام غير المشروع لأدوات الدفع الإلكترونية وفقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، مجلة المنار للبحوث والدراسات القانونية والسياسية، عدد4، مارس، 2018، ص41.

[2] للإستزادة في ذلك أنظر: وردة شرف الدين واحميدة هنية، مرجع سابق، ص46.

شخصياً[1]، كما أن الاتفاقية شددت العقوبة على الجريمة التقليدية التي ترتكب بواسطة تقنية المعلومات[2].

ومن خلال ما تطرقنا إليه أعلاه، يتضح لدى الباحث أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، أشارت بالنص إلى مسألة التزوير الواقع على بيانات الدفع الإلكتروني، وهو ما لم تتطرق له اتفاقية بودابست المتعلقة بالجرائم الإلكترونية، وهذا في نظر الباحث إنما يدل على التطور في الجرائم الإلكترونية خلال فترة عقد من الزمن –بين عامي 2001–2010–. ومع استمرار التطور والتقدم في المجال الإلكتروني، فبالتأكيد ظهرت حالات جديدة تستدعي معها إجراء تعديلات على النصوص القانونية تراعي الحالات الجديدة، وذلك في إطار مكافحة الجريمة الإلكترونية.

وهو ما يؤكد في نظر الباحث على ضرورة عقد المزيد من الاتفاقيات في الفترة الحالية، بحيث يتم دراسة الطرق والأساليب الحديثة في مجال الجريمة الإلكترونية، والتي لم يتم تناولها وتدارسها في الاتفاقيات السابقة، وهو ما يعني كذلك ضرورة إجراء التعديلات على القوانين الوطنية بحيث يتم التنبه إلى السلوكيات الحديثة في مجال الجريمة الإلكترونية.

الفرع الثاني: التنظيم القانوني للجريمة الإلكترونية المتعلقة بالأموال وفقاً للقانون رقم (10) لسنة 2018م وتعديلاته

تناول المشرع الفلسطيني من خلال القرار بقانون رقم 10 لسنة 2018 وتعديلاته المتعلق بالجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات تنظيم الجريمة الإلكترونية المتعلقة بالأموال،

[1] المادة 20 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[2] المادة 21 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

وذلك من خلال التطرق لمجموعة من السلوكيات ذات الصلة بهذه الجريمة، ومنها: جريمة اتلاف البيانات الإلكترونية، وجريمة غسل الأموال والإرهاب، وجريمة الاعتداء على حقوق الملكية الفكرية، وجريمة سرقة الأموال أو إختلاسها من خلال الشبكة الإلكترونية.

إذ أشارت المادة (4) من القرار بقانون رقم (10) لسنة 2018م وتعديلاته المتعلق بالجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات إلى مسألة الدخول العمد غير المصرح به لأي موقع إلكتروني أو شبكة إلكترونية وترتب عن هذا الدخول إلغاء لبيانات أو معلومات إلكترونية أو حذفها أو إفشائها أو إتلافها أو تغييرها أو نقلها أو نسخها أو التقاطها أو نشرها أو ألحق ضررا بالمستخدمين أو المستفيدين او انتحال شخصية مالك الموقع الإلكتروني، يعاقب بالحبس مدة لا تقل عن سنة او بغرامة مالية لا تقل عن 1000 دينار أردني ولا تزيد عن 3000 آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً أو بكلتا العقوبتين[1].

كما اعتبرت المادة (6) من القرار بقانون رقم (10) لسنة 2018م وتعديلاته المتعلق بالجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات أن أي فعل من شأنه إيقاف الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات أو تعطيلها أو إتلاف للبرامج أو حذفها أو تعديلها، يعاقب بالسجن مدة لا تزيد عن 5 سنوات وبغرامة مالية لا تقل عن 3000 آلاف دينار أردني ولا تزيد عن 5000 آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً[2].

وعملاً بما أكدت عليه الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وتماشياً مع أهدافها وتوجهاتها، أكد القرار بقانون رقم 10 لسنة 2018 وتعديلاته المتعلق بالجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات، على تجريم بعض السلوكيات التي تعتبر من الجرائم الإلكترونية

[1] البند 3 من المادة 4 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته المتعلق بالجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[2] المادة رقم 4 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته المتعلق بالجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

المتعلقة بالأموال، إذ أقرت المادة 17 من القرار بقانون رقم 10 لسنة 2018 بتجريم على كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً ونشر معلومات بقصد الاتجار في البشر أو الأعضاء البشرية أو حتى سهل التعامل فيها، ودذلك دون الإخلال بأحكام القرار بقانون بشأن تنظيم نقل وزراعة الأعضاء البشرية النافذ. كما أكدت المادة 17 على أن عقوبة ذلك السجن مدة لا تزيد عن 7 سنوات وبغرامة مالية لا تقل عن 3000 آلاف دينار أردني ولا تزيد عن 5000 آلاف دينار أردني أو ما بعادلها بالعملة المتداولة قانوناً[1].

وكذلك فقد نصت المادة 18 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته المتعلق بالجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات على تجريم كل فعل متعلق بغسل الأموال وتمويل الإرهاب، فقد جرمت المادة 18 كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو استخدم إحدى وسائل تكنولوجيا المعلومات لغرض ارتكاب جريمة غسل الأموال، وحددت المادة 18 عقوبته بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن 1000 دينار أردني ولا تزيد عن 3000 آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً أو بكلتا العقوبتين[2]

كما أقرت المادة 18 بالعقوبة الجنائية على كل فعل متعلق بتمويل الإرهاب بالسجن أو بغرامة مالية لا تقل عن 3000 آلاف دينار أردني ولا تزيد عن 5000 آلاف أردني أو ما يعادلها بالعملة المتداولة قانوناً أو بكلتا العقوبتين[3]. ومن الملاحظ هنا على أن المشرع الفلسطيني لم يحدد مدة الحبس على الأفعال المرتبطة بتمويل الإرهاب، وبالتالي كان لا بد من تحديد مدة الحبس على مثل هذه السلوكيات.

---

[1] المداة 17 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته المتعلق بالجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[2] البند 1 من المادة 18 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته المتعلق بالجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[3] البند 2 من المادة 18 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته المتعلق بالجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

وقد جرم القانون رقم 10 لسنة 2018 وتعديلاته كل استعمال للشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات لغرض سرقة الأموال أو اختلاسها، وحدد القانون من خلال المادة 13 منه عقوبتها بالسجن أو بغرامة مالية لا تقل عن 3000 آلاف دينار أردني ولا تزيد عن 5000 آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً أو بكلتا العقوبتين[1]

ومن الملاحظ أن المادة 13 لم تحدد مدة السجن لجريمة سرقة الأموال أو اختلاسها، ويرى الباحث أنه لا بد من تحديد مدة العقوبة، باعتبار جريمة السرقة والاختلاس عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات كسائر الجرائم المنصوص عليها في القانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

كذلك فقد أشارت المادة 14 من القانون إلى تجريم كل استيلاء من خلال الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات على أي مال منقول أو سند أو توقيع إلكتروني أو بيانات أو منظومة إنشاء توقيع إلكتروني عن طريق الاحتيال أو انتحال صفة غير صحيحة للخداع، وقد حددت المادة عقوبة هذه الجريمة بالحبس مدة لا تقل عن سنة أو بغرامة مالية لا تقل عن 1000 دينار أردني ولا تزيد عن 3000 آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً أو بكلتا العقوبتين[2].

وتناول القرار بقانون رقم 10 لسنة 2018 وتعديلاته تنظيم جريمة الاعتداء على حقوق الملكية الفكرية أو الأدبة أو الصناعية، فأشار وفقاً للمادة 20 من القانون إلى أن كل من ينتهك أي حق من حقوق الملكية الفكرية طبقاً للتشريعات النافذة من خلال الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، يعاقب بالحبس مدة لا تزيد عن 6 أشهر أو بغرامة مالية لا تقل عن 500

[1] المادة 13 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[2] المادة 14 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

دينار أردني ولا تزيد عن 1000 دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً أو بكلتا العقوبتين[1].

بقي أن نشير أخيراً إلى أن القانون رقم 10 لسنة 2018 وتعديلاته لم يأت على ذكر الجرائم المتعلقة بالتجارة الإلكترونية والتحويلات الإلكترونية للأموال (بالنص)، على الرغم من أن تلك الجرائم لها وسائل مختلفة يمكن أن ترتكب من خلالها، إذ إن من جرائم التجارة الإلكترونية تلك التي ترتكب ضد المستهلك إذ يستطيع المستهلك التعامل في الأسواق المحلية والعالمية بكبسة واحدة على جهاز الكمبيوتر لطلب السلعة أو الخدمة المعروضة، فأصبحت الإعلانات تؤثر على توجه المستهلك ويبنى عليها قراره في الإقبال على التعاقد أم لا، فإذا كانت الدعاية الإعلانية كاذبة أو مضللة، فإنها بلا شك تؤثر على المستهلك.

وكذلك الحال بالنسبة للتحويلات الإلكترونية للأموال، إذ يتم التلاعب في نظام التحويل الإلكتروني للأموال عن طريق أي وسيلة من وسائل الاحتيال المعلوماتي، كالتلاعب من خلال إدخال البيانات أو في برامج الكمبيوتر أو في المكونات المادية له أو أثناء عملية نقل البيانات إلكترونياً.

بعد أن اهتم الفصل الأول من الرسالة بالسياسية العقابية لمحاربة الجريمة الإلكترونية، وانطلق من ماهية الجريمة الإلكترونية ووضح التنظيم القانوني لها على المستوى الدولي والإقليمي والوطني، تبيَّن أن كافة التشريعات فصلت في تنظيم الجريمة الإلكترونية بحيث شملت الجرائم الواقعة على الأجهزة الإلكترونية والتي تستهدف الأشخاص وتلك الجرائم الواقعة على الأموال من خلال التقنيات الإلكترونية.

[1] المادة 20 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

ومن خلال البحث اتضح أن كافة التشريعات اتفقت على المبادئ العامة للجريمة الإلكترونية كمبدأ الدخول غير المصرح به ومبدأ اعتراض البيانات والمعلومات، غير أنه كلما كانت التشريعات حديثة، كلما تناولت حالات أكثر دقة من الجرائم الإلكترونية، وهو ما يفسر سبب التغيير وتعديل في التشريعات الوطنية كما هو الحال في التشريع الفلسطيني، وفي ذات الوقت يدعو إلى ضرورة استحداث اتفاقيات دولية جديدة تراعي التطور والتقدم الحاصل في مجال الجرائم الإلكترونية. ويبقى أن نتسائل حول الإجراءات القانونية المتبعة في مكافحة الجريمة الإلكترونية وهو ما سنتناوله في الفصل الثاني من الرسالة.

الفصل الثاني: الإجراءات القانونية المتبعة في مكافحة الجريمة الإلكترونية

يعتبر الشق الإجرائي في مكافحة الجريمة الإلكترونية من الموضوعات ذات الأهمية؛ وذلك نظراً لحداثتها، إذ إن إجراءات التحقيق في الجرائم الإلكترونية وكيفية ضبط الأدلة الرقمية وجمعها من الموضوعات المستجدة في مختلف دول العالم، عدا عن أن طبيعة الأدلة الرقمية وكيفية التعامل معها من قبل جهات التحقيق تعتبر من الموضوعات ذات الأهمية القانونية والعملية.

وانطلاقاً من أن الدول وحكوماتها تتحمل مسؤولية حماية المجتمع والأفراد من الجريمة التقليدية وكذلك الجريمة المرتكبة من خلال الإنترنت، بما في ذلك من خلال التحقيقات الجنائية والملاحقات القضائية الفعالة، وإدراكاً لكون الأدلة المتعلقة بأي جريمة جنائية يتم تخزينها بشكل متزايد في شكل إلكتروني على أنظمة الحاسوب في مختلف الدول، ظهرت الحاجة إلى اتخاذ تدابير إضافية للحصول على مثل هذه الأدلة بشكل قانوني وذلك ضماناً للاستجابة الجنائية الفعالة وتعزيزاً لسيادة القانون.

لذلك سعى المجتمع الدولي إلى زيادة تعزيز التعاون بشأن الجرائم الإكترونية وجمع الأدلة في شكلها الإلكتروني عن أي جريمة جنائية لغرض إجراءات التحقيق أو إجراءات جنائية محددة من خلال أدوات إضافية تتعلق بالمساعدة المتبادلة الأكثر كفاءة وأشكال التعاون الأخرى بين السلطات المختصة؛ وإلى تعزيز التعاون في حالات الطوارئ والتعاون المباشر بين السلطات المختصة ومقدمي الخدمات والكيانات الأخرى التي تمتلك أو تتحكم في المعلومات ذات الصلة.

ولم يغفل المجتمع الدولي في إطار مكافحته للجريمة الإلكترونية وما يتبع ذلك من إجراءات الاستدلال والتحقيق والمحاكمة في الجرائم الإلكترونية عن الحاجة إلى ضمان خضوع تدابير العدالة الجنائية الفعالة بشأن الجرائم الإلكترونية وجمع الأدلة في شكل إلكتروني لشروط وضمانات توفر

الحماية الكافية لحقوق الإنسان والحريات الأساسية، بما في ذلك الحقوق المنبثقة عن الالتزامات التي تعهدت بها الدول بموجب صكوك حقوق الإنسان الدولية المعمول بها، على غرار اتفاقية عام 1950 لحماية حقوق الإنسان، والعهد الدولي التابع للأمم المتحدة الخاص بالحقوق المدنية والسياسية لعام 1966، وغيرها من المعاهدات الدولية المتعلقة بحقوق الإنسان والحريات العامة.

إن مسألة التصدي للجرائم الإلكترونية يتطلب القدرة على جمع الأدلة والإثبات الجنائي وهو ما يتطلب كذلك نموذج تحقيقي فعال يحقق المحاكمة العادلة للجاني ويحفظ حقوق المجني عليه، وفي إطار ذلك يسعى الباحث إلى البحث في إجراءات الاستدلال والتحقيق في الجرائم الإلكترونية من خلال تحليل ومقارنة تلك الإجراءات في الإنفاقيات الدولية والإقليمية والوطنية وذلك في (المبحث الأول)، ليتطرق الباحث إلى إجراءات المحاكمة في الجرائم الإلكترونية والآثار المترتبة عن بطلان تلك الإجراءات وذلك في (المبحث الثاني).

المبحث الأول: إجراءات الاستدلال والتحقيق في الجرائم الإلكترونية

تثير الجرائم الإلكترونية بعضاً من المشكلات الإجرائية من الناحية القانونية والعملية، وذلك لما تتسم به هذه الجرائم من حداثة من حيث أساليب ارتكابها وسرعة تنفيذها وإخفاء معالمها ومحو آثارها، وهو ما نتج عنه جملة من الصعوبات والإشكاليات العملية التي تقف حائلة أمام أجهزة البحث والتحري من أجل إثبات واستيفاء الدليل الإلكتروني[1].

وتتعلق هذه المشكلات بضبط الجريمة الإلكترونية وإثباتها وما يتعلق بسلطات التحري والملاحقة، فمن أبرز العناصر التي ترتبط بالجريمة هو مكان وقوع أركانها، فهو العنصر الأساس لضبط وتحري الجريمة وملاحقة مرتكبيها، وهو ذات الحال فيما يخص الجريمة الإلكترونية؛ إذ إن مسرح الجريمة الإلكترونية وإن كان مسرحاً معنوياً، فإن تجول الشخص في الشبكة الإلكترونية يترك أثراً وبصمات معنوية في الموقع الذي يدخله، حيث يتم تحديد عنوانه الإلكتروني الدائم، كما يتم تحديد نوع الجهاز الذي يستخدمه بالإضافة للمكان الذي يدخل منه[2].

غير أن صعوبة ضبط الجريمة وإثباتها تكمن في حال تمكن الجاني من محو آثاره، كأن يتمكن الجاني من مسح الملفات، وإخفاء عناونه الإلكتروني الخاص بجهازه بطرق مختلفة. لذلك تسعى مختلف الدول والشركات ذات الاختصاص بالمجال الإلكتروني والإنترنت إلى التغلب على هذه الإختراقات من خلال برامج خاصة أو عبر رموز أخرى يتم من خلالها التعرف على هوية المتصل، فلغرض ضبط الجريمة وتحريها يستلزم وجود تعاوناً من قبل مزودي الخدمة[3].

---

[1] مصطفى عبد الباقي، التحقيق في الجرائم الإلكترونية وإثباتها في فلسطين: دراسة مقارنة، دراسات علوم الشريعة والقانون، الجامعة الأردنية، الأردن، المجلد 45، العدد 4، 2018، ص284.

[2] يوسف خليل يوسف العفيفي، الجرائم الإلكترونية في التشريع الفلسطيني (دراسة تحليلية مقارنة)، رسالة ماجستير، كلية الشريعة والقانون، الجامعة الإسلامية، غزة، فلسطين، ص16.

[3] يوسف خليل يوسف العفيفي، مرجع سابق، ص16.

وقد ظهرت وسائل حديثة في مجال الإثبات الجنائي للجريمة الإلكترونية كالدليل الرقمي، ويُعرف على أنه الدليل الذي يأخذ من أجهزة الحاسوب ويكون على شكل مجال أو نبضات كهربائية أو مغناطيسية يمكن تجميعها وتحليلها عن طريق برامج تكنولوجية خاصة، ويمكن أن تقدم على شكل دليل من الممكن أن يعتمد أمام القضاء[1].

أمام هذا الحال ولغرض تناول موضوع إجراءات الاستدلال والتحقيق في الجرائم الإلكتررونية على كافة المستويات الدولية والإقليمية والوطنية، يسعى الباحث لتناول هذا الموضوع من خلال ما جاءت به الاتفاقيات الدولية والإقليمية في هذا المضمار (المطلب الأول)، على أن ينظر الباحث كذلك فيما تناوله التشريع الفلسطيني في موضوع إجراءات الاستدلال والتحقيق في الجرائم الإلكترونية من خلال القانون رقم 10 لسنة 2018 وتعديلاته (المطلب الثاني).

المطلب الأول: إجراءات الاستدلال والتحقيق في الجرائم الإلكترونية وفقاً للاتفاقيات الدولية والإقليمية

يعتمد ضبط الجريمة الإلكترونية وإثباتها في المقام الأول على ما يتم جمعه من الأدلة التي حدد المشرع وسائل إثباتها، وذلك لما فيها من مساس بحرية الأفراد وحقوقهم الأساسية، وقد أفرد الاهتمام الدولي قسماً خاصاً بمسألة جمع الأدلة والتحقيق في الجرائم الإلكترونية، إذ تناولتها اتفاقية بودابست لمكافحة الجرائم الإلكترونية من خلال القسم الثاني من الاتفاقية (الفرع الأول)، وكذلك تناولتها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من خلال الفصل الثالث من الإتفاقية (الفرع الثاني).

[1] رعد فجر فتيح و ياسر عواد، إثبات الجريمة الإلكترونية بالدليل العلمي، مجلة جامعة تكريت للحقوق، العراق، عدد 3، مجلد 1، آذار، 2017، ص485.

الفرع الأول: إجراءات الاستدلال والتحقيق في الجرائم الإلكترونية وفقاً لاتفاقية بودابست

إن اتفاقية بودابست ترمي بشكل أساسي إلى مواءمة عناصر القانون الموضوعي الجنائي المحلي والأحكام المتصلة بالجرائم في مجال الجريمة الإلكترونية، والتنصيص على صلاحيات القانون الإجرائي الجنائي المحلي اللازمة للتحقيق في هذه الجرائم ومتابعتها قضائياً علاوةً على الجرائم الأخرى التي ترتكب عن طريق الكمبيوتر أو التي تكون الأدلة المتصلة بها في شكل إلكتروني[1]. فقد تناولت الاتفاقية في قسمها الثاني المسائل المتعلقة بالقانون الإجرائي ذو العلاقة بالجرائم الإلكترونية.

وقد تجاوز نطاق تطبيق القانون الجنائي الجرائم التي حددتها الاتفاقية، إذ إنه ينطبق على أية جريمة ترتكب بواسطة أجهزة وأنظمة الحاسوب أو تكون الأدلة المتصلة بها في شكل إلكتروني، حيث أشارت الاتفاقية إلى الشروط والضمانات المشتركة التي تنطبق على جميع الصلاحيات الإجرائية، ثم حددت الصلاحيات الإجرائية والتي تتمثل في: التعجيل بحفظ البيانات المخزنة؛ والتعجيل في حفظ بيانات الحركة والإفصاح الجزئي عنها؛ أمر تقديم البيانات؛ البحث عن بيانات الكمبيوتر ومصادرتها، وجمع بيانات الحركة في الوقت الحقيقي؛ اعتراض بيانات المحتوى[2]، وهي ذات الإجراءات التي فصّل فيها البروتوكول الثاني للاتفاقية المتعلقة بالجريمة الإلكترونية بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية، والذي صدر عن مجلس أوروبا لعام 2022.

فقد أكدت المادة 15 من الاتفاقية والمعنونة بالشروط والضمانات على ضرورة أن توفر الدول الأطراف الحماية الملائمة لحقوق الإنسان والحريات الأساسية، وذلك بما يشمل الحقوق الناشئة عن الالتزامات التي تعهدت بها بموجب اتفاقية مجلس أوروبا لعام 1950 الخاصة بحماية حقوق

[1] التقرير التفسيري لاتفاقية الجريمة الإلكترونية، مرجع سابق، ص4.

[2] نادين محمود محمد الشايب، التفتيش في الجرائم الإلكترونية: دراسة تحليلية مقارنة، رسالة ماجستير، جامعة النجاح الوطنية، نابلس، فلسطين، 2023، ص79-81.

الإنسان والحريات الأساسية، وكذلك العهد الدولي للأمم المتحدة لعام 1966 الخاص بالحقوق المدنية والسياسية، وغيرها من الصكوك الدولية ذات الصلة بحقوق الإنسان، وذلك مع ضمان إدماج مبدأ التناسب[1]، وبالتالي لا بد أن تعمل صلاحيات السلطات المختصة والإجراءات على "تضمين مبدأ التناسب"، وهو المبدأ الذي تطبقه كل دولة طرف وفقاً للمبادئ ذات الصلة في قانونه الوطني.

وقد أشارت المادة 15 من الاتفاقية إلى ضرورة أن تشمل تلك الشروط والضمانات النظر إلى طبيعة الإجراءات أو السلطات المعنية، الإشراف القضائي أو بواسطة أي هيئة مستقلة أخرى، والأسس المبررة للتطبيق، وحدود نطاق تلك الإجراءات أو السلطات ومدتها، وذلك حسب الإقتضاء[2]. ومراعاةً للمصلحة العامة والإدارة السليمة للعدالة ألزمت الاتفاقية الدول الأطراف بتدارس تأثير السلطات والإجراءات القانونية الواردة في الاتفاقية على حقوق الأغيار ومسؤولياتهم ومصالحهم المشروعة[3].

وتطبيقاً للإجراءات القانونية المتبعة في مكافحة الجريمة الإلكترونية، نصت المادة 16 من الاتفاقية على ضرورة التعجيل في حفظ البيانات المخزنة على الكمبيوتر، إذ ألزمت الدول الأطراف باتخاذ التدابير التشريعية وغيرها من التدابير لتمكين السلطات المختصة بالحفظ المعجل لبيانات الكمبيوتر، بما في ذلك بيانات الحركة المُخزنة بواسطة نظام الكمبيوتر، خاصةً في حال وجود اعتقاد أن تلك البيانات معرضة بشكل خاص للضياع أو التعديل[4].

---

[1] البند 1 من المادة 15 من اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

[2] البند 2 من المادة 15 من اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

[3] البند 3 من المادة 15 من اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

للإستزادة راجع: هلالي عبداللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية: معلقاً عليها هلالي عبداللاه أحمد، ط1، دار النهضة العربية، القاهرة، 2011.

[4] البند 1 من المادة 16 من اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

وفي حال ألزمت الدولة شخصاً ما بحفظ بيانات محددة على الكمبيوتر، وذلك تفعيلاً للبندا 1 من المادة 16 من الاتفاقية، فقد ألزمت الاتفاقية الدول الأطراف باتخاذ التدابير التشريعية اللازمة وغيرها من التدابير لإلزام ذلك الشخص بحفظ بيانات الكمبيوتر المعنية مع الإبقاء على سلامتها لأطول مدة زمنية ممكنة على ألا تتجاوز تسعين يوماً، وذلك لغرض تمكين السلطات المختصة من التماس الكشف عنها، وقد أجازت الاتفاقية للدول الأطراف التنصيص على تجديد المدة الزمنية[1].

كما تنبهت الاتفاقية إلى مسألة سرية إجراءات حفظ البيانات، إذ ألزمت الدول الأطراف باتخاذ التدابير التشريعية وغيرها من التدابير اللازمة لإلزام القيّم على حفظ بيانات الكمبيوتر أو كل من أُوكلت إليه هذه المهمة بالحفاظ على سرية هذه الإجراءات طيلة الفترة الزمنية المنصوص عليها في قانون الدولة الوطني[2]. وذلك مع ضرورة أن تخضع تلك السلطات والإجراءات لنطاق الأحكام الإجرائية الواردة في المادة 14 من الاتفاقية، وكذلك أن تخضع للشروط والضمانات التي نصت عليها المادة 15 من الاتفاقية[3].

كما ألزمت الاتفاقية الدول الأطراف بالإضافة إلى مسألة التعجيل بحفظ بيانات الكمبيوتر بضرورة الكشف الجزئي عن بيانات الحركة، وهو ما أكدت عليه المادة 17 من الاتفاقية، إذ ألزمت الدول الأطراف بضرورة اتخاذ التدابير التشريعية وغيرها من التدابير اللازمة لغرض ضمان توفر إمكانية التعجيل في حفظ بيانات الحركة بصرف النظر عن مشاركة مزود خدمة واحد أو أكثر في عملية نقل هذا الاتصال، وكذلك ضمان تعجيل الكشف للسلطة المختصة أو الشخص الذي تعينه تلك السلطة، عن القدر الكافي من بيانات الحركة من أجل تمكين الدولة الطرف من تحديد مزود

---

[1] البند 2 من المادة 16 من اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

[2] البند 3 من المادة 16 من اتفاقية بودابست لمكافحة الجريمة الإلكترونية. للإستزادة حاتم أحمد محمد بطيخ، تطورالسياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات دراسة تحليلية مقارنة، على الرابط التالي:
file:///C:/Users/user/Downloads/JDL_Volume%207_Issue%201_Pages%201-143.pdf- ص20.

[3] البند 4 من المادة 16 من اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

الخدمة والمسار الذي تم من خلاله نقل الاتصال[1]. وذلك مع تأكيد الاتفاقية على أن تخضع تلك السلطات والإجراءات لأحكام المواد 14 و15 من الاتفاقية[2].

كذلك فقد أشارت الاتفاقية إلى مسألة الأمر بإبراز البيانات، حيث ألزمت الدول الأطراف وفقاً للمادة 18 منها بضرورة إتخاذ ما يلزم من تدابير تشريعية وغيرها من التدابير لغرض تمكين سلطاتها المختصة إصدار أمر إلى أي شخص داخل أراضي الدولة بتقديم بيانات كمبيوتر محددة بحوزته أو تحت سيطرته، ومخزنة على نظام الكمبيوتر أو على أي دعامة أخرى لتخزين بيانات الكمبيوتر، كما يمكن للسلطات المختصة أن تصدر أمراً إلى أي مزود خدمة يعرض خدماته داخل أراضي الدولة بتقديم معلومات عن المشترك ذات الصلة بتلك الخدمات الموجودة بحوزته أو تحت سيطرته[3]. وذلك على أن تخضع تلك السلطات والإجراءات لأحكام المواد 14 و15 من الاتفاقية[4].

وقد أدرجت الاتفاقية المقصود بعبارة "بيانات عن المشترك" على أنها تلك المعلومات المدرجة في شكل بيانات على الكمبيوتر أو في أي شكل آخر يحفظها مزود الخدمة وتتعلق بالمشتركين في الخدمات التي يزودها بخلاف بيانات الحركة أو المضمون من قبيل: نوع خدمة الاتصال والشروط الفنية ومدة الخدمة، وكذلك هوية المشترك وعنوانه البريدي أو الجغرافي ورقم هاتفه وأي معلومات أخرى عن موقع تركيب أجهزة ومعدات الاتصال[5].

وفي إطار الاهتمام الدولي بإجراءات جمع المعلومات، أكدت اتفاقية بودابست لمكافحة الجريمة الإلكترونية على ضرورة البحث عن بيانات الكمبيوتر المخزنة ومصادرتها، إذ ألزمت الدول الأطراف باتخاذ التدابير التشريعية وغيرها من التدابير اللازمة لغرض تمكين سلطاتها المختصة من

---

[1] البند 1 بفرعيه (أ، ب) من المادة 17 من اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

[2] البند 2 من المادة 17 من اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

[3] البند 1 بفرعيه (أ، ب) من المادة 18 من اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

[4] البند 2 من المادة 18 من اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

[5] البند 3 من المادة 18 من اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

البحث أو النفاذ إلى أي نظام كمبيوتر أو أي جزء منه والبيانات المخزنة فيه؛ وإلى أي دعامة تخزين بيانات الكمبيوتر يمكن أن تكون بيانات الكمبيوتر مخزنة داخلها على أراضي تلك الدولة[1].

وفي حال أنجزت سلطات الدولة عمليات البحث أو النفاذ إلى نظام الكمبيوتر أو إلى جزء منه، ووجدت أن البيانات المطلوبة مخزنة داخل نظام كمبيوتر آخر ويمكن النفاذ إلى تلك البيانات، فإنه ينبغي أن تتمكن السلطات من تعجيل توسيع نطاق البحث أو النفاذ إلى النظام الآخر[2].

وبذلك تتخذ الدولة ما يلزم من التدابير التشريعية وغيرها من التدابير لغرض تمكين سلطاتها المختصة من مصادرة أو تأمين تلك البيانات، كتمكينها من مصادرة أو تأمين نظام الكمبيوتر أو جزء منه أو دعامة تخزين بيانات الكمبيوتر، وإجراء نسخة من هذه البيانات الحاسوبية والاحتفاظ بها، والحفاظ على سلامة بيانات الكمبيوتر المخزنة ذات الصلة، وجعل تلك البيانات الحاسوبية غير قابلة للنفاذ على نظام الكمبيوتر الذي تم الولوج إليه أو إزالتها[3].

ولهذا الغرض ألزمت الاتفاقية الدول الأطراف باتخاذ التدابير التشريعية وغيرها من التدابير اللازمة لتمكين سلطاتها المختصة بأمر أي شخص لديه معرفة بتشغيل نظام الكمبيوتر بتقديم المعلومات اللازمة لتمكين إجراء التدابير المشار إليها في الفقرة 1 و 2 من المادة 19 من الاتفاقية[4]، على أن تخضع السلطات المختصة والإجراءات المشار إليها لأحكام المواد 14 و15 من الاتفاقية[5].

وعلى اعتبار أن البيانات في البيئة الإلكترونية ليست دائماً ثابتة، بل تتدفق في خضم عملية الاتصال، فقد ركزت اتفاقية بودابست على مسألة جمع البيانات في الوقت الحقيقي، حيث ألزمت الاتفاقية في المادة 20 منها الدول الأطراف باتخاذ التدابير التشريعية وغيرها من التدابير اللازمة

---

[1] البند 1 بفرعيه (أ،ب) من المادة 19 من اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

[2] البند 2 من المادة 19 من اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

[3] البند 3 من المادة 19 من اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

[4] البند 4 من المادة 19 من اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

[5] البند 5 من المادة 19 من اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

لغرض تمكين سلطاتها المختصة من جمع أو تسجيل بيانات الحركة في الوقت الحقيقي، وكذلك إجبار مزود الخدمة في نطاق قدرته الفنية على جمع وتسجيل بيانات الحركة في الوقت الحقيقي، والتعاون مع السلطات المختصة لأجل هذا الغرض، وذلك مع ضرورة إلزام مزود الخدمة بالحفاظ على سرية التنفيذ، وأن تخضع السلطات المختصة والإجراءات المشار إليها في المادة 20 لأحكام المواد 14 و 15 من الاتفاقية[1]. وهو ما ينطبق كذلك على مسألة اعتراض بيانات المحتوى التي أشارت إليها المادة 21 من الاتفاقية.

وأخيراً نشير إلى أن اتفاقية بودابست لمكافحة الجرائم الإلكترونية هدفت إلى تمكين الحصول على البيانات أو جمعها لأغراض التحقيقات أو الإجراءات الجنائية الخاصة، وتشير الإجراءات الواردة في المواد أعلاه بوجه عام إلى جميع أنواع البيانات، بما في ذلك ثلاثة أنواع محددة من بيانات الكمبيوتر وهي: بيانات الحركة، وبيانات المحتوى، وبيانات المنخرطين.

ومن الملاحظ على بنود الاتفاقية التي تختص بالتحقيق وجمع الأدلة في شكلها الإلكتروني، إلا أنه لا يوجد في الاتفاقية ما يطلب أو يدعو الدول الأطراف إلى إنشاء سلطات أو إجراءات غير تلك الواردة في هذه الاتفاقية، كما أنه لا يوجد ما يمنع الدول الأطراف من القيام بذلك. وفي رأي الباحث كان من باب الأولى أن يتم التنصيص على حث الدول الأطراف على إنشاء تلك السلطات أو الإجراءات خاصة تلك الإجراءات ذات العلاقة بالتحقيق ورفع الأدلة الجنائية الإلكترونية.

[1] المادة 20 من اتفاقية بودابست لمكافحة الجريمة الإلكترونية.

الفرع الثاني: إجراءات الاستدلال والتحقيق في الجرائم الإلكترونية وفقاً للاتفاقية العربية لمكافحة جرائم تقنية المعلومات

في نطاق إجراءات الجمع والاستدلال والتحقيق في الجرائم الإلكترونية، سارت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على النهج الذي جاءت به اتفاقية بودابست لمكافحة الجريمة الإلكترونية، حيث شملت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في الفصل الثالث منها على مجموعة من المواد (22–29) التي تتعلق بالأحكام الإجرائية فيما يخص الجرائم الإلكترونية أو التقنية لغرض جمع الأدلة في شكلها الإلكتروني والتحقيق فيها[1].

حيث أكدت الاتفاقية العربية على مجموعة من الإجراءات التي تضمن عملية جمع الأدلة بشكلها الإلكتروني، وتمثلت هذه الإجراءت في: التحفظ العاجل على البيانات المخزنة في تقنية المعلومات، والكشف الجزئي لمعلومات تتبع المستخدمين، وتسليم المعلومات، وتفتيش المعلومات المخزنة، وضبط المعلومات المخزنة، والجمع الفوري لمعلومات تتبع المستخدمين، واعتراض معلومات المحتوى[2].

وقد تناولت المادة 22 من الاتفاقية نطاق تطبيق تلك الأحكام الإجرائية، فألزمت الدول الأطراف أن تتبنى في قانونها الداخلي التشريعات والإجراءات الضرورية لتحديد الصلاحيات والإجراءات الواردة في الاتفاقية كالجرائم المنصوص عليها في المواد 6–19 من الاتفاقية، وكذلك أية جرائم أخرى ترتكب بواسطة تقنية المعلومات، وجمع الأدلة عن الجرائم بشكل إلكتروني[3].

---

[1] حاتم أحمد محمد بطيخ، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات دراسة تحليلية مقارنة، مرجع سابق، ص25–26.

[2] نادين محمود محمد الشايب، التفتيش في الجرائم الإلكترونية: دراسة تحليلية مقارنة، مرجع سابق، ص82–84.

[3] المادة 22 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

وهو ما يضمن الحصول على الأدلة في شكل إلكتروني على أي جريمة جنائية أو جمعها عن طريق تلك الصلاحيات والإجراءات، كما يوفر قدرة موازية للحصول على بيانات الكمبيوتر أو جمعها طبقا لما يتم في إطار الصلاحيات التقليدية والإجراءات المتعلقة بالبيانات غير الإلكترونية.

ونصت الاتفاقية العربية على إجراء التحفظ العاجل على البيانات المخزنة في تقنية المعلومات، فألزمت المادة 23 من الاتفاقية الدول الأطراف باتخاذ التدابير اللازمة والضرورية لتمكين السلطات المختصة من إصدار الأمر بالحصول على الحفظ العاجل للبيانات المخزنة، خاصةُ في حال وجود اعتقاد بأن تلك المعلومات عرضة للفقدان أو التعديل، كما يشمل الحفظ العاجل للمعلومات التي تتبع المستخدمين والمخزنة على تقنية المعلومات[1].

وقد حددت الاتفاقية إلزامية الحفظ العاجل للبيانات وصيانتها وسلامتها لمدة 90 يوم قابلة للتجديد، وذلك لغرض تمكين السلطات المختصة من البحث والتقصي[2]، فيما ألزمت الاتفاقية الدول الأطراف بتبني التدابير اللازمة لإلزام الشخص المسؤول عن حفظ بيانات تقنية المعلومات بالسرية التامة للإجراءات طوال الفترة القانونية المنصوص عليها في القانون الوطني[3].

كما أشارت الاتفاقية العربية لمسألة الكشف الجزئي للبيانات التي تتعلق بالمستخدمين، إذ أكدت المادة 24 من الاتفاقية على الحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين، وألزمت الدول الأطراف باتخاذ التدابير اللازمة من أجل ضمان توفر الحفظ العاجل لمعلومات تتبع المستخدمين بصرف النظر عن عدد المشتركين من مزودي الخدمة في بث تلك الاتصالات، وكذلك لغاية ضمان الكشف العاجل للسلطات المختصة أو لأي شخص تعينة السلطات لقدر كافٍ

[1] البند1 من المادة 23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[2] البند 2 من المادة 23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[3] البند 3 من المادة 23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

من البيانات التي تخص المستخدمين، وذلك لغرض لتمكين الدولة الطرف من تحديد مزودي الخدمة ومسار بث الاتصالات[1].

ووفقاً لنص المادة 25 من الاتفاقية العربية، فإنه يتعين على الدول الأطراف اتخاذ الإجراءات والتدابير الضرورية لغرض لتمكين السلطات المختصة من إصدار الأوامر لأي شخص في إقليمها من أجل تسليم معلومات معينة في حيازته والمخزنة على تقنية معلومات أو وسيط تخزين معلومات، وكذلك تمكين السلطات المختصة بأمر مزودي الخدمة الذي يقدم خدماته في إقليم الدولة الطرف لتسليم بيانات المشترك المتعلقة بتلك الخدمات والتي تكون في حوزة مزود الخدمه أو تحت سيطرته[2].

كما ألزمت الاتفاقية العربية الدول الاطراف باتخاذ الإجراءات والتدابير اللازمة لتمكين سلطاتها المختصة من تفتيش المعلومات المخزنة أو الوصول إلى تقنية المعلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها، وكذلك الوصول إلى بيئة أو وسيط تخزين معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه[3]. وهو الحال الذي ينطبق فيما إذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانوناً أو متوفرة في التقنية الأولى، فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى[4].

---

[1] المادة 24 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[2] الفقرة 1 و 2 من المادة 25 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[3] الفقرات (أ،ب) من البند 1 من المادة 26 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[4] البند 2 من المادة 26 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. وكذلك إمكانية الوصول وضبط المكونات المادية لوسائل تكنولوجيا المعلومات وهي كافة الأجهزة الملموسة التي تستخدم في إدخال ومعالجة وإخراج البيانات والمعلومات. نورهان قرون وجهاد بوضياف ورحيمة العيفة، تكنولوجيا المعلومات والإتصال كركيزة أساسية لعملية التدريب الإلكتروني، مجلة التعليم عن بعد، جامعة بني سويف اتحاد الجامعات العربية، مجلد 8، عدد15، ديسمبر، 2020، ص46.

وحول مسألة ضبط المعلومات المخزنة، فقد ألزمت الاتفاقية العربية الدول الأطراف باتخاذ التدابير والإجراءات الضرورية واللازمة لغرض تمكين سلطاتها المختصة من ضبط وتأمين معلومات تقنية المعلومات، وتشمل إجراءات ضبط المعلومات صلاحية ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات، وعمل نسخة من معلومات تقنية المعلومات والاحتفاظ بها، والحفاظ على سلامة بيانات تقنية المعلومات المخزنة، وإزالة أو منع الوصول إلى تلك البيانات في تقنية المعلومات التي يتم الوصول إليها[1]. مع التأكيد على اتخاذ الإجراءات اللازمة لتمكين السلطات المختصة[2] 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 المتعلقة بتفتيش البيانات المخزنة الواردة في المادة 26 من الاتفاقية[3].

وفيما يخص الإجراء المتعلق بالجمع الفوري لبيانات تتبع للمستخدمين، فقد أكدت الاتفاقية العربية بنص المادة 28 منها، على أن تلتزم الدول الأطراف باتخاذ الإجراءات الضرورية لتمكين سلطاتها المختصة من جمع أو تسجيل بواسطة الوسائل الفنية على إقليم الدولة، وكذلك إلزام مزود الخدمة ضمن اختصاصة الفني بأن يجمع أو يسجل بواسطة الوسائل الفنية على إقليم الدولة، أو يتعاون ويساعد السلطات المختصة في جمع وتسجيل معلومات تتبع المستخدمين بشكل فوري مع الاتصالات المعنية في إقليمها والتي تبث بواسطة تقنية المعلومات[4].

---

[1] البند (1،2) من المادة 27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. وكذلك: محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، المكتب العربي الحديث، الإسكندرية، مصر، 2007، ص57.

[2] حول السلطات المختصة الأصلية بالتفتيش أنظر: نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الإستدلالات، دار الفكر الجامعي، الإسكندرية، مصر، 2007، ص241. وحول السلطات الإستثنائية بإجراء التفتيش أنظر: مصطفى عبد الباقي، شرح قانون الإجراءات الجزائية الفلسطيني، وحدة البحث العلمي والنشر، كلية الحقوق والإدارة العامة، جامعة بيرزيت، 2015 ص190.

[3] البند 3 من المادة 27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[4] البند 1 من المادة 28 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

وفي حال عدم تمكن الدولة من تحقيق ذلك بسبب نظامها الداخلي، فيمكنها اتخاذ إجراءات أخرى بشكل ضروري لضمان الجمع أو التسجيل الفوري للبيانات التابعة للمستخدمين المرافقة للاتصالات المعنية في إقليمها باستخدام الوسائل الفنية في الإقليم[1]. كل ذلك مع التأكيد على ضرورة اتخاذ الإجراءات والتدابير اللازمة لإلزام مزود الخدمة بالاحتفاظ بسرية أية معلومة عند تنفيذ تلك الصلاحيات[2].

وحول مسألة اعتراض معلومات المحتوى، فقد ألزمت الاتفاقية العربية الدول الأطراف، بضرورة اتخاذ الإجراءات والتدابير التشريعية وغيرها من التدابير اللازمة، فيما يخص الجرائم المنصوص عليها في قانونها الوطني من أجل تمكين سلطاتها المختصة من الجمع أو التسجيل من خلال الوسائل الفنية على إقليم الدولة، أو التعاون ومساعدة السلطات المختصة في جمع أو تسجيل بيانات المحتوى بشكل فوري للاتصالات المعنية في إقليمها والتي تبث بوساطة تقنية معلومات. وفي حال عدم تمكن الدولة من ذلك بسبب نظامها القانوني؛ فيمكنها تبني واتخاذ إجراءات أخرى بشكل ضروري لضمان التسجيل الفوري لبيانات المحتوى، كل ذلك مع التأكيد على اتخاذ التدابير الضرورية لإلزام مزود الخدمة بالاحتفاظ بسرية أية معلومة عند تنفيذ تلك الصلاحيات[3].

ويجوز لأي دولة طرف الاحتفاظ بحقها في تطبيق تلك الإجراءات فقط على الجرائم أو أصناف الجرائم المعنية بالتحفظ بشرط ألا يزيد عدد هذه الجرائم على عدد الجرائم التي تطبق عليها الإجراءات المذكورة في المادة 30 من الاتفاقية، كما يجوز للدولة أن تحتفظ بحقها في عدم تطبيق إجراءات المادة 29 كلما كانت غير قادرة بسبب محدودية التشريع على تطبيقها على الاتصالات

---

[1] البند 2 من المادة 28 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[2] البند 3 من المادة 28 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[3] البنود (1،2،3) من المادة 29 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. وكذلك: إبراهيم خالد ممدوح، إجراءات التفتيش في الجرائم المعلوماتية، دار الفكر الجامعي، مصر، 2022، ص65.

التي تبث بواسطة تقنية المعلومات لمزود الخدمة، وذلك في حال كانت التقنية يتم تشغيلها لصالح مجموعة مغلقة من المستخدمين. وكذلك في حال كانت التقنية لا تستخدم شبكات اتصال عامة وغير مرتبطة بتقنية معلومات أخرى عامة كانت أو خاصة، مع الأخذ بعين الاعتبار محدودية التحفظ؛ وذلك لإتاحة التطبيق الواسع للإجراءات الواردة في المادة 29[1].

ومن الملاحظ على مواد الاتفاقية المتعلقة بالأحكام الإجرائية أن المادة 22 منها احتوت على لفظ غامض وهو "أية جريمة أخرى ترتكب بوساطة تقنية المعلومات" وهو لفظ من خلاله يمكن تجريم أي نشاط رقمي. كما أن الاتفاقية لم تشمل على مواد من شأنها أن تراعي سرية وخصوصية بيانات المستخدمين وحقوقهم، وبذلك تكون الاتفاقية قد خالفة المعايير الدولية المتعلقة بالخصوصية. وفي رأي الباحث أنه من باب الأولى أن يتم إلحاق الاتفاقية ببروتوكول خاص بها يوضح مثل هذه الملاحظات.

إذ إن الاتفاقية تناولت في نص عام ومقتضب خصوصية المستخدمين وبياناتهم وحقوقهم، إلا أنها لم تضمن حق الشخص في إعلامه بالإجراءات التي يتم اتخاذها بشأن جمع البيانات والمعلومات حول نشاطه الرقمي، ولم تعطه الحق في الاعتراض على هذه الإجراءات. كذلك لم تضع الاتفاقية أي ضوابط قانونية للحصول على معلومات المشتركين، مثلاً كاستصدار أمر قضائي بذلك.

كما نصت الإتفاقية على أنه "يحتفظ في البيانات عن طريق شخص مسؤول بحفظها وصيانة سلامتها لمدة أقصاها 90 يوما قابلة للتجديد"، غير أنه لم يتم تحديد مرات التجديد، أو شروط التجديد، أو إطاره، أو إجراءاته، أو مدى ضرورته في أي من بنود الاتفاقية.

[1] البند (2،3) من المادة 22 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

المطلب الثاني: إجراءات الاستدلال والتحقيق في الجرائم الإلكترونية وفقاً للقانون رقم (10) لسنة 2018م وتعديلاته

في ضوء طبيعة وخصوصية الجريمة الإلكترونية وكيفية إثباتها، ثار النقاش حول ما إذا كان من الممكن الإكتفاء بقواعد الإثبات العادية من أجل إثبات الجريمة الإلكترونية، أم أن الأمر يتطلب وضع نصوص وقواعد إثبات خاصة بها تنسجم مع طبيعتها وخصوصيتها. وقد خلص هذا النقاش إلى ضرورة إستحداث وسائل حديثة تراعي التطور الحال في المجال الإلكتروني لإثبات الجريمة الإلكترونية، ونظراً لطبيعة الأدلة الرقمية وكيفية التعامل معها من قبل جهات التحقيق، فقد أصبح موضوع إثبات الجريمة الإلكترونية من الموضوعات ذات الأهمية القانونية والعملية.

وقد أدرك المشرع الفلسطيني هذه الأهمية، فوضع النصوص القانونية الخاصة بإجراءات جمع الأدلة والتحقيق فيها، ونظراً لحداثة موضوع الجريمة الإلكترونية وما يشهده من تطورات، فقد أجرى المشرع الفلسطيني تعديلات على القانون الخاص بالجرائم الإلكترونية، فأصدر القرار بقانون رقم 10 لسنة 2018 وتعديلاته.

وفي إطار هذا القانون سيناقش الباحث إجراءات الاستدلال في الجرائم الإلكترونية، من حيث السلطات المختصة بالاستدلال، وإجراءات الاستدلال (الفرع الأول)، كما سيتطرق الباحث إلى البحث في إجراءات التحقيق في الجرائم الإلكترونية، وذلك من حيث السلطات المختصة بالتحقيق، وإجراءات التحقيق (الفرع الثاني).

الفرع الأول: إجراءات الاستدلال في الجرائم الالكترونية والسلطة المختصة بها

سار المشرع الفلسطيني على النهج الذي تبنته الاتفاقيات الدولية والإقليمية فيما يتعلق بإجراءات الاستدلال والتحقيق في الجرائم الإلكترونية، حيث نص القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات، على مجموعة من الإجراءات التي تتعلق بجمع الأدلة الخاص بالجريمة الإلكترونية، من قبيل: تلقي البلاغات والشكايات، والمعاينه لمسرح الجريمه الاكتروني، والاستماع للمتهم في الجرائم الالكتروني، وإنجاز محاضر الاستدلال.

كما حدد المشرع السلطات المعنية التي تقوم بتلك الإجراءات. وسنتناول في هذا الفرع السلطات المختصة بالاستدلال في الجرائم الإلكترونية (الفقرة الأولى)، على أن نتطرق إلى إجراءات الاستدلال عن الجرائم الإلكترونية (الفقرة الثانية).

الفقرة الأولى: السلطات المختصة بالاستدلال في الجرائم الالكترونية

يقع نطاق تطبيق القرار بقانون رقم 10 لسنة 2018 وتعديلاته في حال ارتكاب أي جريمة من الجرائم الإلكترونية المنصوص عليها بالقانون، سواء ارتكبت بشكل كلي أو جزئي داخل فلسطين أو خارجها أو امتد أثرها داخل فلسطين، وكذلك سواء كان الفاعل أصلياً أو شريكاً أو محرضاً أو متدخلاً، على شرط أن تكون تلك الجرائم معاقب عليها خارج فلسطين[1].

ولهذا الغرض، نص القرار بقانون رقم 10 لسنة 2018 وتعديلاته على إنشاء وحدة متخصصة من مأموري الضبط القضائي عُرفت باسم وحدة بالجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات، وتتولى النيابة العامة مهمة الإشراف القضائي عليها، وتنظر المحاكم النظامية والنيابة

[1] الفقرة 1 من المادة 2 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

العامة كلاً وفقاً لإختصاصاتهما في دعاوى الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات[1].

وبذلك فقد حدد المشرع الفلسطيني السلطات المختصة في الجرائم الإلكترونية، وبناء عليه، سيتناول الباحث سلطة مأموري الضبط القضائي (أولاً)، ثم سلطة وحدة الجرائم الإلكترونية (ثانياً)

أولاً: مأموري الضبط القضائي

حددت المادة 21 من قانون الإجراءات الجزائية الفلسطيني[2] الأشخاص الذين منحهم القانون صفة مأمور الضبط وهم: مدير الشرطة ونوابه ومساعدوه ومديرو شرطة المحافظات والإدارات العامة، ضباط وضباط صف الشرطة، كلٌ في دائرة اختصاصه، رؤساء المراكب البحرية والجوية، الموظفون الذين منحوا صلاحيات الضبط القضائي بموجب القانون.

وعلى اعتبار أن الإشراف القضائي على الجرائم الإلكترونية يعتبر من مهام النيابة العامة، فإنه يحق لها أو لمن تنتدبه من مأموري الضبط القضائي أن تقوم بالإجراءات والتدابير اللازمة لضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة، وتنظيم محضر بالمضبوطات وعرضها على النيابة العامة لاتخاذ الإجراءات اللازمة بشأنها[3].

إذ يحق لمأموري الضبط القضائي النفاذ المباشر لأي وسيلة من وسائل تكنولوجييا المعلومات بقصد الحصول على البيانات أو المعلومات ذات الصلة بالجريمة الإلكترونية والتي من شأنها أن

[1] المادة 3 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[2] قانون الإجراءات الجزائية رقم 3 لسنة 2001. وكذلك: نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الإستدلالات، مرجع سابق، ص241.

[3] الفقرة 3 من المادة 52 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

تساعد في كشف الحقيقة[1]، على أنه يشترط أن يكون مأمور الضبط القضائي خصاً مؤهلاً للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات[2].

ويمكن لمأموري الضبط القضائي نسخ البيانات أو المعلومات المرتبطة بالجريمة وكذلك البيانات التي تؤمن قراءتها وفهمها على أي وسيلة من وسائل تكنولوجيا المعلومات[3]، ويتعين على مأموري الضبط القضائي استعمال كافة الوسائل لمنع الوصول أو النفاذ إلى البيانات المخزنة في نظام المعلومات؛ وذلك حفاظاً على أدلة الجريمة[4]، وتتخذ كافة الإحتياطات للحفاظ على سلامة المضبوطات المتحفظ عليها بما في ذلك الوسائل الفنية لحماية محتواها[5].

ويتعين على مأموري الضبط باعتبارهم الجهة المكلفة بالتنفيذ إعلام النيابة العامة بالتاريخ الفعلي لبدء عملية الاعتراض الفوري لمحتوى الاتصالات والتنسيق معها من أجل اتخاذ التدابير والإجراءات اللازمة لتحسين سيرها[6]. وفي حال رصد مأمورو الضبط أي مواقع إلكترونية ترتكب جريمة من الجرائم الإلكترونية التي نص عليها القانون رقم 10 لسنة 2018 وتعديلاته، أن تُعد محضراً وتقدمه للنائب العام أو أحد مساعديه، وتطلب الإذن بحجب تلك المواقع الإلكترونية[7].

---

[1] الفقرة 4 من المادة 52 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[2] الفقرة 5 من المادة 52 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات. وكذلك: إبراهيم خالد ممدوح، إجراءات التفتيش في الجرائم المعلوماتية، مرجع سابق، ص65.

[3] الفقرة 3 من المادة 53 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[4] الفقرة 4 من المادة 53 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[5] الفقرة 5 من المادة 53 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[6] الفقرة 3 من المادة 56 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[7] الفقرة 1 من المادة 59 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

ثانياً: وحدة الجرائم الإلكترونية

وفقاً لما نصت عليه المادة 3 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته آنفة الذكر، فإن وحدة الجرائم الإلكترونية التي أوصى بإنشائها القرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات رقم 10 لسنة 2018 هي وحدة تابعة لجهاز الشرطة وقوى الأمن وتتألف من مأموري الضبط القضائي، وتقوم بتلقي البلاغات والشكايات من أي شخص أو جهة معينة تفيد بوقوع جريمة إلكترونية.

وتعمل وحدة الجرائم الإلكترونية بشكل سري، وهي مختصة بمتابعة الجرائم الالكترونية المبنية على تقنية المعلومات والوسائل الالكترونية، ويعمل فيها أشخاص مختصون، تضم 26 وكيل نيابة متخصص، ومختبر مجهز بطاقم تقني مكون من 9 أشخاص مدربين على أحدث النظم الالكترونية، مهمتنا تحليل المعلومات التقنية وجمع الأدلة، ومن ثم بناء ملف تحقيقي مبني على الدليل الرقمي، وأخيرًا تنظيم لائحة الاتهام وتقديمها الى المحكمة وقد أنشأت موقعاً إلكترونياً لتقديم الشكاوي[1].

وقد بلغ عدد الشكاوى التي تلقتها دائرة الجرائم الإلكترونية في الشرطة الفلسطينية لغاية تاريخ 3067 جريمة إلكترونية، منها 422 جريمة إلكترونية غير مكتملة الأركان، وتم إنجاز 1548 ملف أي بنسبة إنجاز وصلت 58.5%، في حين بلغت عدد الجرائم المعلقة أو قيد المتابعة أو قيد الإجراء الإداري 1097 جريمة أي ما نسبته 41.5%[2].

[1] كيف تعمل وحدة مكافحة الجرائم الالكترونية الفلسطينية؟، مقابلة مع رئيسة نيابة الجرائم الإلكترونية، تاريخ النشر: 2017\1\20، على الرابط التالي: https://madar.news- تاريخ الإطلاع: 2024\9\30، على الساعة 7:20 مساءاً.

[2] إحصائية الشرطة الفلسطينية لعام 2022، على الرابط التالي: https://www.palpolice.ps/annual-statistics الصادر بتاريخ 2023/8/12، تاريخ الإطلاع: 2024/7/10، ص76-77.

الفقره الثانية: الإجراءات الخاصة في الاستدلال عن الجرائم الإلكترونية.

أنشأت وزارة الداخلية من خلال جهاز الشرطة الفلسطينية دوائر وأقسام مستقلة تم إرفادها بفرق عمل متخصصة للتعامل مع الأدلة الرقمية، مثل فرق عمل مسرح الجريمة، وجمع الأدلة الرقمية، وتحليل الأدلة الرقمية وفحصها، وبالتالي تهدف هذه الفقرة إلى معرفة إجراءات التعامل مع الجرائم الإلكترونية بشكل عام، إذ تعد إجراءات الاستدلال في الجرائم الإلكترونية من أهم وأخطر الإجراءات التي يتم التطرق إليها أثناء ملاحقة الجرائم الإلكترونية؛ وذلك نظراً لحساسية الإثبات وكذلك لخصوصية الأفراد.

وتعتبر إجراءات الاستدلال في الجرائم الإلكترونية من الإجراءات الأولية التي تساعد في تحريك الدعوى الجزائية، وتبدأ أولى إجراءات الاستدلال عن الجرائم الإلكترونية بتلقي البلاغات والشكايات، ثم المعاينه لمسرح الجريمه الإلكترونية، ثم الاستماع للمتهم في الجرائم الالكتروني، وأخيراً إنجاز محاضر الاستدلال. ووفقاً لنص المادة 22 من قانون الإجراءات الجزائية الفلسطيني، يتولى مأمورو الضبط القضائي البحث والاستقصاء عن الجرائم ومرتكبيها وجمع الاستدلالات اللازمة.

أولاً: تلقي البلاغات والشكايات

حرصاً من المشرع الفلسطيني على مكافحة الجريمة الإلكترونية ومواجهتها بكافة الطرق والسبل، فقد أنشأ وحدة الجرائم الإلكترونية التابعة للشرطة، والتي يقع على عاتقها تلقي البلاغات والشكاوي، وتحويلها لنيابة الجرائم الإلكترونية للتحقيق فيها.

إذ إن وجود بلاغ أو شكوى من شخص أو جهة معينة تفيد بوقوع جريمة إلكترونية أو على وشك الوقوع، هو أول ما يحرك الضابطة القضائية، حيث تبقى الجريمة الإلكترونية مستترة ومستمرة إلى

أن يتم إخبار السلطات المختصة بها، كما ألزم القرار بقانون رقم 10 لسنة 2018 وتعديلاته أجهزة الدولة ومؤسساتها وهيئاتها والجهات والشركات التابعة لها الإسراع في إبلاغ الجهات المختصة عن أي جريمة منصوص عليها في القرار بقانون فور اكتشافها، وتزويد الجهة المعنية بجميع المعلومات لغرض كشف الحقيقة[1].

والمقصود بالتبليغ عن الجريمة الإلكترونية إعلام وحدة الجرائم الإلكترونية عن وقوعها أو أنها على وشك الوقوع أو وجود اتفاق أو عزم على ارتكابها[2]، ويتم التبليغ عن الجريمة الإلكترونية بوسائل وطرق مختلفة، فقد يكون التبليغ كتابياً أو شفوياً من أي شخص سواء كان متضرراً أم لا، وهو ما يطلق عليه البلاغ المادي، وقد يكون البلاغ بواسطة البريد أو التلفون أو الصحف وهو ما يطلق عليه البلاغ المعنوي، وقد يكون البلاغ عن طريق الإنترنت من خلال إرسال رسالة إلكترونية إلى عنوان البريد الإلكتروني الخاص بالسلطات المختصة بالتحقيق وهو يطلق عليه البلاغ الرقمي[3].

ويجب أن يتضمن البلاغ تحديد مكان وقوع الجريمة وتحديد نوع الجريمة وكذلك تحديد محل الجريمة، وذلك حتى يتسنى لمأموري الضبط القضائي من تحديد معالم الجريمة ووضع خطة للتعامل معها[4]. ووفقاً للمادة 73 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته، فإنه يعفى من العقوبة المحددة كل من بادر من الجناة بإبلاغ السلطات المعنية بأي معلومات عن الجريمة وعن الأشخاص المشتركين فيها، وذلك قبل علم السلطات بها وقبل وقوع الضرر، كما يجوز للمحكمة أن

---

[1] الفقرة 2 من المادة 61 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية ووجرائم الاتصالات وتكنولوجيا المعلومات.

[2] جاسم خلف، نحو تطورات في الإجراءات الجزائية، منشورات زين الحقوقية، بيروت، 2017، ص76.

[3] الزهراء بخي، إجراءات التحقيق في الجرائم الإلكترونية، رسالة ماجستير، كلية الحقوق، جامعة المسيلة، الجزائر، 2014، ص54-55.

[4] منجد غيث وآخرون، أساليب ومهارات التحقيق في الجرائم الإلكترونية، جامعة فلسطين الأهلية، بيت لحم، فلسطين، 2014، ص18-19.

تقضي بوقف تنفيذ العقوبة في حال حصل الإبلاغ بعد علم السلطات وأدى إلى ضبط باقي الجناة[1].

ثانياً: المعاينة لمسرح الجريمه الإلكترونية

بعد أن تتلقى النيابة العامة البلاغ أو الشكوى حول الجريمة الإلكترونية، تصدر مذكرة لمأموري الضبط لمعاينة مسرح الجريمة الإلكترونية، ويقصد بالمعاينة أي رؤية المكان أو الشخص بالعين أو أي شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة.

ويجب على مأموري الضبط مراعاة مجموعة من القواعد والإجراءات الوقتية حتى تثمر المعاينة عن كشف الحقيقة ومقترفيها، فيقوم مأمورو الضبط بتوثيق حالة مسرح الجريمة، بمعنى تسجيل كافة التفاصيل المتعلقة بحالة الكمبيوتر، من قبيل تحديد ما إذا كان الحاسوب في وضع التشغيل، وإذا ما كان متصلاً بالإنترنت أم لا وقت ضبطه أم لا، وتحديد هوية وتوثيق جهاز الكمبيوتر والأجهزة الملحقة به التي يعثر عليها في مسرح الجريمة[2]، حيث أن رمز بروتوكول الإنترنت IP يلعب دوراً كبيراً في تحديد موقع ومكان المشتبه به، وتحديد هوية وتوثيق أجهزة التخزين (مثل CDs وDVDs) التي يعثر عليها في مسرح الجريمة[3].

---

[1] المادة 73 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية ووجرائم الاتصالات وتكنولوجيا المعلومات.

[2] مصطفى موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، القاهرة، 2009، ص172.

[3] IP: هو اختصار للكلمة الإنجليزية **Internet Protocol**: وتعني بروتوكول الاتصال الأساسي في حزمة بروتوكولات الإنترنت، فهو عبارة عن رقم يقوم بتعريف كل كمبيوتر عبر الإنترنت أو الشبكة.

CDS: هو اختصار Computer data storage وتسمى وحدة التخزين أو الذاكرة، وهي أقراص مصنوعة من مادة بلاستيكية ومغطاة بطبقة من الألمنيوم، تعمل بواسطة أشعة الليزر لتسجيل المعلومات أو قراءتها، لها قدرة هائلةعلى خزن المعلومات.

DVD: هو اختصار Digital Versatile Disc: وهو قرص بصري يستخدم كواسطة لتخزين البيانات، وبإمكانه حفظ الأفلام ذات جودة الوضوح والصوت العاليتين.

كما يقوم مأمورو الضبط لمعاينة مسرح الجريمة الإلكترونية بتصوير مسرح الجريمة، وحفظ الأدلة والمواد الرقمية، وحفظ الوثائق المطبوعة، وحفظ الأجهزة، وإجراء استرجاع للوثائق العالقة، من قبيل طباعة الأوراق العالقة في ماكنة الطباعة، وإجراء استرجاع للوثائق الملغاة أو التي تم مسحها، ونقل الأدلة التي يتم ضبطها[1].

ثالثاً: الاستماع للمتهم والشهود في الجرائم الإلكترونية

ألزم القرار بقانون مأموري الضبط القضائي بالتحفظ على أدوات الجريمة واتخاذ جميع الوسائل اللازمة للمحافظة على أدلة الجريمة، كما منح القانون مأموري الضبط القضائي صلاحية سماع أقوال المشتبه بهم والشهود بشروط معينة؛ وذلك على اعتبار أن الشاهد قد ينسى ما شاهده مع مرور الوقت أو قد يتأثر بالروايات التي يسمعها من شهود آخرين، كما أن تدوين أقوال المشتبه بهم يمنع من تلقينهم الأقوال مستقبلاً، لذلك يتم تثبيت أقولهم في محضر الإفادة.

ويكون الشاهد في الجرائم الإلكترونية الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي، ويكون لديه معلومات جوهرية لازمة تمكن من الولوج إلى نظام المعالجة الآلية للبيانات في حال اقتضت مصلحة التحري التنقيب عن أدلة الجريمة داخله ويطلق عليه الشاهد الإلكتروني. ويشمل الشاهد الإلكتروني مشغل الحاسب الآلي، والمبرمجين، والمحليون، ومهندسي الصيانة والاتصالات، ومديري النظم[2].

وقد ذهب المشرع الفلسطيني إلى إلزام مزود الخدمة بتزويد الجهات المختصة بمعلومات المشترك التي تساعد على كشف الحقيقة، وذلك بناءً على طلب النيابة العامة أو المحكمة المختصة،

[1] مصطفى عبد الباقي، التحقيق في الجرائم الإلكترونية وإثباتها في فلسطين: دراسة مقارنة، دراسات علوم الشريعة والقانون، الجامعة الأردنية، الأردن، المجلد 45، العدد 4، 2018، ص286.

[2] فيروز ميرغني، اجراءات التحري والضبط في الجريمة الإلكترونية، رسالة دكتوراه، جامعة شندى، السودان، 2017، ص58.

وحجب رابط أو محتوى أو تطبيق على الشبكة الإلكترونية، والاحتفاظ بمعلومات المشترك لمدة لا تقل عن ثلاث سنوات، ومساعدة الجهات المختصة في جمع أو تسجيل المعلومات والبيانات الإلكترونية والاحتفاظ المؤقت بها، وذلك بناءً على قرار قاضي المحكمة المختصة[1].

ويقوم مأمور الضبط كذلك بإعلام المشتبه به بالتهم المنسوبة إليه والأدلة الموجه ضده دون أن يتطرق إلى مناقشته تفصيلياً في حيثيات الجريمة، وسماع أقواله دون مواجهته، وكل شخص كان متواجداً في مسرح الجريمة أو يحوم حولها أو هناك أدلة ضده يعد من المشتبه بهم، ويتعين على مأمور الضبط أن يسمع أقواله وتدوينها مع إرسالها لوكيل النيابة خلال 24 ساعة، إذا دعت الحاجة لذلك[2]، ووفقاً لنص المادة 84 من قانون الإجراءات الجزائية الفلسطيني فإنه لوكيل النيابة مواجهة الشهود ببعضهم البعض، ومواجهتهم بالمتهم، إذا اقتضى الأمر ذلك.

رابعاً: إنجاز محاضر الاستدلال

تعتبر مسألة إنجاز محاضر الاستدلال خطوة في غاية الأهمية لما يليها من إجراءات؛ إذ بناء عليها يتم حفظ ملف الدعوى وإقامة الدعوى الجزائية، وتؤثر في مرحلة التحقيق ومرحلة المحاكمة كذلك، فلا تنتج إجراءات الاستدلال التي يقوم بها مأمورو الضبط أي قيمة أو أثر قانوني في حال لم يتم تنظيمها في محاضر تثبت ما تم اتخاذه من إجراءات، لذلك فهي من الضمانات الأساسية للوصول إلى الحقيقة، لأنها تحفظ الأدلة وتكون سبباً لعدم نسيانها. ولكل ذلك يتعين على مأموري الضبط توخي العناية والدقة عند تحرير مثل هذه المحاضر.

[1] المادة 51 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية ووجرائم الاتصالات وتكنولوجيا المعلومات.

[2] يوسف العفيفي، الجرائم الإلكترونية فيالتشريع الفلسطيني، رسالة ماجستير، الجامعة الإسلامية،غزة، فلسطين، 2013، ص103.

وفقاً لنص المادة 22 الفقرة 4 منها من قانون الإجراءات الجزائية الفلسطيني، فقد أوجب المشرع الفلسطيني في نهاية كل إجراء من إجراءات الاستدلال أن يقوم مأمور الضبط القضائي بتحرير هذه الإجراءات في محضر رسمي موقع عليه من مأمور الضبط وموقع من أي شخص اتخذ بحقه الإجراء كالشاهد أو المشتبه به، على أن يبين في المحضر وقت اتخاذ الإجراءات وتاريخها.

ويقع على عاتق مأموري الضبط تحرير قائمة بالمضبوطات المتحفظ عليها، وذلك بحضور المتهم أو من وجدت لديه تلك المضبوطات، ويحرر مأمور الضبط تقريراً بذلك، كما أنه يجب على مأمور الضبط أن يحفظ المضبوطات المتحفظ عليها حسب الحالة التي وجدت عليها في ظرف مختوم، ويضع عليه ورقة تبين تاريخ التحفظ وساعته وعدد المحاضر والقضية[1].

وقد أوجب المشرع الفلسطيني كتابة المحاضر، كي لا يتم الاعتماد على ذاكرة مأمور الضبط القضائي الشفهية لحين المحاكمة؛ لأن مأمور الضبط يصادف خلال عمله اليومي العديد من القضايا التي قد تختلط عليه مع مرور الوقت، وبالتالي تصبح عرضة للنسيان ويشوبها الشك وعدم اليقين مما يلحق ضرراً بكشف الحقيقة وتحقيق العدالة.

وتكمن أهمية إنجاز محاضر الاستدلال كذلك في أنها تكون حجة على المتهم، إذ يحتوي محضر الاستدلال على كيفية العثور على الأشياء المضبوطة والمكان الذي وجدت فيه وتاريخ إيجادها مما يفيد في كشف الحقيقة. ويجب على مأمور الضبط القضائي ذو الاختصاص إرسال المحضر الاستدلال وكافة المضبوطات إلى النيابة العامة المختصة بمباشرة إجراءات التحقيق في الجريمة[2].

ويُعرف محضر الاستدلال على أنه "الوثيقة المكتوبة التي يحررها مأمور الضبط القضائي أثناء ممارسة مهامه المتمثلة بإجراءات الاستدلال الإلكتروني، وتتضمن ما عاينه أو ما تلقاه من

[1] الفقرة 6 من المادة 53 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[2] الفقرة 4 من المادة 22 من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001.

تصريحات أو ما قام به من عمليات في حدود اختصاصه، ويثبت في المحضر المضبوطات المتحصل عليها"[1].

والمحضر الذي تعمل به الشرطة الفلسطينية يكون عبارة عن استمارة مطبوعة تعبأ بها المعلومات بخط يد مأمور الضبط، غير أن المادة 112 من التعليمات القضائية للنيابة العامة أجازت لمأمور الضبط القضائي أن يستعين بغيره من الإداريين الموجودين لديه في تحرير محضر الاستدلال على شرط أن يكون في حضرته وتحت بصره.

ومما يمكن ملاحظته أن المشرع الفلسطيني جعل الإجراءات الخاصة في الاستدلال وما ينتج عنها من جمع الأدلة وتحريرها في محاضر التحري والضبط هي جزء أصيل من مرحلة جمع الاستدلال، وهو ما يعني أن طبيعة الإجراءات الخاصة بالاستدلال تتصف بالشمول، حيث الاستقصاء والبحث والتحري وجمع الإيضاحات والتحفظ على الأدلة.

الفرع الثاني: التحقيق في الجرائم الإلكترونية

نص القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات، على مجموعة من الإجراءات التي تتعلق بجمع الأدلة الخاص بالجريمة الإلكترونية، من قبيل: إجراءات تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة، والضبط والتحفظ على كامل نظام المعلومات أو جزء منه أو أي وسيلة من وسائل تكنولوجيا المعلومات التي تساعد في كشف الحقيقة، والجمع والتزويد الفوري للبيانات بما فيها حركة

[1] قصي دويكات، حجية محاضر الاستدلال في الإثبات الجنائي، رسالة ماجستير، جامعة النجاح الوطنية، نابلس، فلسطين، 2018، ص23.

الاتصالات أو معلومات إلكترونية أو بيانات المشترك، والاعتراض الفوري لمحتوى الاتصالات. كما حدد المشرع السلطات المعنية التي تقوم بتلك الإجراءات.

وسيتعرض الباحث لهذا الفرع من خلال التطرق إلى السلطات المكلفة بالتحقيق في الجرائم الإلكترونية (الفقرة الأولى)، على أن يتم تناول إجراءات التحقيق الخاصة بالجرائم الالكترونية (الفقرة الثانية).

الفقرة الأولى: السلطات المكلفة بالتحقيق في الجرائم الإلكترونية

نظراً لتزايد استخدام وسائل تكنولوجيا المعلومات وما نتج عنه من تطور للجريمة الإلكترونية، وبالتالي اختلاف مسرح الجريمة الإلكترونية عن المسرح في الجرائم التقليدية، كما أن مكان ارتكاب الجريمة الإلكترونية قد لا يكون مكان تحقق النتيجة، فقد اتجه المشرع الفلسطيني نحو إصدار تشريع فلسطيني حديث يتعلق بوجود نيابة خاصة بالجرائم الإلكترونية، فظهر القرار بقانون رقم 10 لسنة2018 بشأن الجرائم الإلكترونية وجرائم الإتصالات وتكنولوجيا المعلومات وتعديلاته.

وتختص نيابة مكافحة الجرائم الإلكترونية بمتابعة الطلبات المتعلقة بالجرائم الإلكترونية والاتصالات وكافة الطلبات ذات العلاقة الواردة من النيابات الجزئية والأجهزة الأمنية ذات العلاقة والدعاوى ذات العلاقة والتنسيق معها، وتتعاون كذلك مع وحدة مكافحة الجرائم الإلكترونية، وتتولى التواصل مع الجهات والمؤسسات والشركات ذات العلاقة فيما يتعلق بالجرائم الإلكترونية والاتصالات والحصول على الدليل الفني الإلكتروني وربط الجناة فيه، بحيث يتم التعامل بالقضايا الواردة لتلك النيابة بالسرعة الممكنة والسرية التامة[1].

[1] الموقع الرسمي لنيابة مكافحة الجرائم المعلوماتية، على الرابط التالي:

وكذلك تعمل النيابة على استقبال الاحتياج المعلومات من قبل النيابات المختلفة والأجهزة الأمنية وتحليل وتقيم الدليل الإلكتروني في العديد من الجرائم المختلفة وفقاً للاحتياجات التي ترد للنيابة، وتعمل النيابة على تنظيم الوقت اللازم لإنجاز الطلبات مع الأخذ بعين الاعتبار الطلبات العاجلة[1].

ويتولى أعضاء نيابة الجرائم الإلكترونية التحقيق في الشكاوي الواردة بالخصوص وفقاً للمعايير التي تتناسب مع طبيعة وخصوصية تلك الجرائم ومتطلباتها، علماً بأن الدور الذي تقوم به نيابة الجرائم الإلكترونية هو دور وقائي وعقابي في ذات الوقت، وذلك لصد ومكافحة الجرائم الإلكترونية وفقاً للقانون والأصول[2].

الفقرة الثانية: إجراءات التحقيق الخاصة بالجرائم الإلكترونية

يعتبر التحقيق أول مرحلة من مراحل الدعوى الجزائية، إذ أنه عبارة عن إجراءات تتخذها السلطات المختصة بالتحقيق من أجل جمع المعلومات والأدلة التي تساعد على التحقيق في الجريمة، وأشار القانون رقم 10 لسنة 2018 وتعديلاته إلى مجموعة من الإجراءات التي يجب اتباعها في هذا الإطار للحصول على الدليل على وقوع الجريمة.

وأشار قانون الإجراءات الجزائية الفلسطيني إلى العديد من إجراءات التحقيق، غير أن إجراءات التحقيق التي أشار لها القرار بقانون رقم 10 لسنة 2018 وتعديلاته تتلخص في: التفتيش الإلكتروني (أولاً)، والجمع والتزويد الفوري للبيانات بما فيها حركة الاتصالات أو معلومات

---

https://safeonline.najah.edu/ar/about/partners/the_public_prosecution/#gsc.tab=0، تاريخ الإطلاع: 30\9\2024، على الساعة 8:12 مساءاً.

[1] الموقع الرسمي لنيابة مكافحة الجرائم المعلوماتية، https://safeonline.najah.edu/ar/about/partners/the_public_prosecution/#gsc.tab=0، مرجع سابق.

[2] الموقع الرسمي لنيابة مكافحة الجرائم المعلوماتية، https://safeonline.najah.edu/ar/about/partners/the_public_prosecution/#gsc.tab=0، مرجع سابق.

إلكترونية أو بيانات المشترك (ثانياً)، ومراقبه المحادثات والاتصالات الإلكترونية (ثالثاً)، والاعتراض الفوري للبيانات (رابعاً).

اولاً: التفتيش الإلكتروني

يمكن تعريف التفتيش الإلكتروني بأنه إجراء تحقيقي تقوم به الضابطة القضائية بموجب مذكرة قضائية، أو بدون مذكرة في أحوال استثنائية، للبحث عن أدلة الجريمة الرقمية في جهاز كمبيوتر أو أي من أجهزة الاتصال الذكية[1].

وقد نوه القرار بقانون رم 10 لسنة 2018 وتعديلاته إلى إجراء تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة الإلكترونية[2]، وذلك على اعتبار أن هذا الإجراء من حق النيابة العامة أو من تنتدبه من مأموري الضبط القضائي[3]، على شرط أن يكون أمر التفتيش مسبباً ومحدداً مع إمكانية تجديده لأكثر من مرة ما دام هناك مبررات لذلك[4].

وفي حال أسفر إجراء التفتيش عن ضبط أجهزة وادوات أو وسائل ذات صلة بالجريمة، يتعين على مأمور الضبط تنظيم محضر بالمضبوطات وعرضها على النيابة العامة لاتخاذ ما يلزم من إجراءات بشأنها[5]، علماً أنه يجوز لوكيل النيابة أن يأذن بالنفاذ المباشر لمأموري الضبط أو كل من يسعينون به من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات وتفتيشها بقصد

---

[1] مصطفى عبد الباقي، التحقيق في الجرائم الإلكترونية وإثباتها في فلسطين: دراسة مقارنة، مرجع سابق، ص289.

[2] قضت محكمة النقض الفلسطينية بأنه "لا يرد القول باعتبار إجراءات تفتيش المنزل أهل المتهم الذي يقيم فيه أو المسؤول عن المكان المراد تفتيشه دون حضوره باطلة". نقض\ جزاء فلسطيني رقم 147 لسنة 2020.

[3] الفقرة 1 من المادة 52 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[4] الفقرة 2 من المادة 52 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات. وكذلك: أحمد حسام الدين محمد، الإذن بالتفتيش والضبط، دار النهضة العربية، ط3، مصر، 2003، ص286.

[5] الفقرة 3 من المادة 52 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

الحصول على البيانات او المعلومات[1]، ولذلك يشترط في مأمور الضبط القضائي أن يكون مؤهلاً للتعامل مع الطبيعة الخاصة بالجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات[2].

ثانيا: الجمع والتزويد الفوري للبيانات بما فيها حركة الاتصالات أو معلومات إلكترونية أو بيانات المشترك

نصت المادة 53 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته، على أنه يجوز للنيابة العامة أن تحصل على الأجهزة أو الوسائل أو الأدوات أو البيانات أو المعلومات الإلكترونية أو بيانات المرور أو تلك البيانات المتعلقة بحركة الاتصالات أو مستخدميها أو معلومات المشترك ذات العلاقة بالجريمة الإلكترونية[3]، وكذلك للنيابة العامة أن تأذن بضبط وتحفظ على كامل نظام المعلومات أو جزء منه أو ضبط أي وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها أن ساهم في الكشف عن الحقيقة[4].

وفي حال تعذر إجراء الضبط والتحفظ على نظام المعلومات، فإنه يمكن نسخ البيانات أو المعلومات ذات الصلة بالجريمة الإلكترونية، وكذلك نسخ البيانات التي تؤمن قراءتها وفهمها على

---

[1] الفقرة 4 من المادة 52 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات. وكذلك: محمد جمال مطلق الذنيبات، معن أحمد العناسوة، التفتيش في الجرائم الإلكترونية ماهيته وشروطه الشكلية، المجلة الأردنية في القانون والعلوم السياسية، مجلد 13، عدد3، 2021، ص100.

[2] الفقرة 5 من المادة 52 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[3] الفقرة 1 من المادة 53 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات. ونظراً لكون طبيعة الدليل الإلكتروني غير ملموس فيكون عبارة عن بيانات ومعلومات مخزنة على شكل إلكتروني، فقد تكون صوراً رقمية أو نصاً مكتوباً أو تسجيلاً صوتياً أو شكلاً أو رسماً أياً كان من ذلك فهو يحتاج إلى إجراءات تتناسب معه عند ضبطه. دليل الأدلة الإلكترونية، دليل أساسي لموظفي الشرطة والمدعين العامين والقضاة، صادر عن مجلس أوروبا، فرنسا، 2014، ص11.

[4] الفقرة 2 من المادة 53 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات. وكذلك: محمد جمال مطلق الذنيبات، معن أحمد العناسوة، التفتيش في الجرائم الإلكترونية ماهيته وشروطه الشكلية، مرجع سابق، ص100.

وسيلة من وسائل تكنولوجيا المعلومات[1]، وإذا استحال إجراء الضبط بصفة فعلية، يتعين استعمال كافة الوسائل المناسبة لمنع النفاذ إلى البيانات المخزنة في نظام المعلومات، وذلك حفاظاً على أدلة الجريمة[2]. كما تتخذ كافة الإحتياطات والتدابير الضرورية للحفاظ على سلامة المضبوطات متحفظ عليها، بما في ذلك الوسائل الفنية لحماية محتواها[3]. ويقوم مأمورو الضبط بتحرير قائمة بالمضبوطات بحضور المتهم أو من وجدت لديه تلك المضبوطات[4].

ثالثاً: مراقبة المحادثات والاتصالات الإلكترونية

تكون مراقبة المحادثات والاتصالات وتسجيلها والتعامل معها بأمر من قاضي الصلح، إذ يمكن لقاضي الصلح أن يأذن للنائب العام أو أحد مساعديه بمراقبة الاتصالات والمحادثات الإلكترونية وتسجيلها، وذلك في إطار البحث عن الدليل المتعلق بجناية أو جنحة المعاقب عليها بالحبس لمدة لا تقل عن سنة[5].

وقد اشترطت المادة 54 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات، أن يكون الإذن بمراقبة الاتصالات والمحادثات

---

[1] الفقرة 3 من المادة 53 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[2] الفقرة 4 من المادة 53 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات. والمقصود بالضبط بحسب الجرائم الإلكترونية: وضع اليد من قبل السلطات المختصة على المكونات المادية والمعنوية للأنظمة المعلوماتية وعلى كل شيء يفيد في الكشف عن الحقيقة. محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الإبتدائي، دار الجامعة الجديدة، الإسكندرية، مصر، 2018، ص319.

[3] الفقرة 5 من المادة 53 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[4] الفقرة 6 من المادة 53 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[5] الفقرة 1 من المادة 54 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

الإلكترونية وتسجيلها مبني على توافر دلائل جدية تشير إلى أهمية هذا الإجراء في كشف الحقيقة، وحددت المادة 54 أن يكون ذلك خلال 15 يوم قابلة للتجديد مرة واحدة، وألزمت من يقوم بالتفتيش أو المراقبة أو التسجيل بتنظيم محضراً يقدمه للنيابة العامة[1].

وأقرت المادة 54 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات، بحق النائب العام أو أحد مساعديه أن يأمر بالجمع والتزويد الفوري لأي بيانات بما في ذلك حركة الاتصالات أو معلومات إلكترونية أو بيانات مرور أو معلومات المشترك التي تتماشى مع مصلحة التحقيقات، وللنائب العام أو أحد مساعديه أن يستعمل الوسائل الفنية المناسبة ويستعين بمزودي الخدمات حسب نوع الخدمة التي يقدمها عند اقتضاء الحاجة[2].

رابعاً: الاعتراض الفوري للبيانات

بالاستناد إلى نص المادة 56 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات، فإنه يمكن للنائب العام أو أحد مساعديه أن يطلب من المحكمة المختصة أن تأذن بالاعتراض الفوري لمحتوى الاتصالات وتسجيلها أو نسخها، على أن يتضمن قرار المحكمة جميع العناصر التي من شأنها التعريف بالاتصالات موضوع طلب الاعتراض والأفعال الموجبة له وكذلك مدته[3].

---

[1] الفقرة 1 من المادة 54، من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[2] الفقرة 2 من المادة 54 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[3] الفقرة 1 من المادة 56 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

على شرط أن تكون مدة الاعتراض لا تزيد عن 3 أشهر وذلك من بداية تاريخ الشروع الفعلي في إنجاز الاعتراض، على أن تكون هذه المدة قابلة للتجديد لمرة واحدة[1]. وعلى الجهة المكلفة بتنفيذ إذن الاعتراض إعلام النيابة العامة بالتاريخ الفعلي لبدء عملية الاعتراض، والتنسيق معها في كل ما يتعلق باتخاذ التدابير اللازمة لضمان حسن سيرها[2]. وما يمكن ملاحظته في موضوع الاعتراض الفوري للبيانات هو طول مدة الاعتراض، وكذلك طول المدة التي تكون فيها الخصوصية مهددة.

خامساً: الالتزامات الملقاة على عاتق مزودي الخدمات في التحقيق الالكتروني

خص القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات مزود الخدمة بمجموعة من الالتزامات أوضحها بنص المادة 51 منه. وجاءت هذه الالتزامات وفقاً للإجراءات القانونية المقررة، إذ يقع على عاتق مزود الخدمة تزويد الجهات المختصة بمعلومات المشترك بناء على طلب النيابة العامة أو المحكمة المختصة، على شرط أن تكون هذه المعلومات تساعد في كشف الحقيقة، وبالتالي يجب أن تكون تلك المعلومات ذات صلة بموضوع الجريمة[3].كما أن مزود الخدمة ملزم بناء على الأوامر الصادرة إليه من الجهات القضائية حجب رابط أو محتوى أو تطبيق على الشبكة الإلكترونية، على شرط مراعاة أحكام المادة 59 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات[4].

---

[1] الفقرة 2 من المادة 56 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[2] الفقرة 3 من المادة 56 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[3] الفقرة 1 من المادة 51 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[4] الفقرة 2 من المادة 51 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

وتشير المادة 59 إلى أنه في حال رصدت جهات التحري والضبط مواقع إلكترونية داخل الدولة أو خارجها تضع عبارات أو صور أو أرقام أو أفلام أو أي مواد دعائية أو كل ما من شأنه تهديد الأمن القومي أو النظام العام أو الآداب العامة، أن تقدم للنائب العام أو أحد مساعديه محضراً بذلك، وتطلب الإذن بحجب المواقع الإلكترونية أو بعض روابطها من العرض[1].

ويقوم النائب العام أو أحد مساعديه بتقديم طلب الإذن لمحكمة الصلح خلال 24 ساعة مرفقاً بمذكرة برأيه، وتقوم المحكمة بإصدار قرارها بشأن الطلب في ذات اليوم الذي عرض عليها، على شرط ألا تزيد مدة الحجب عن 6 أشهر ما لم تتجدد المدة وذلك وفقاً للإجراءات المنصوص عليها في المادة 59 من القرار بقانون[2].

ويقع على عاتق مزود الخدمة الاحتفاظ بمعلومات المشترك مدة لا تقل عن 3 سنوات، وذلك لتزويد الجهات المختصة بتلك المعلومات التي تساعد في الكشف عن الحقيقة متى طلبتها[3]. وبناء على قرار قاضي المحكمة المختصة يتعاون مزود الخدمة مع الجهات المختصة في جمع وتسجيل المعلومات أو البيانات الإلكترونية والاحتفاظ المؤقت بها[4].

ونشير إلى أن الإثبات في الجرائم الإلكترونية يواجه صعوبات وتعقيدات كثيرة، لذلك فقد أكد القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات، على حجية الدليل الإلكتروني في الإثبات، واعتبر أن من أدلة الإثبات كل دليل ناتج

---

[1] الفقرة 1 من المادة 59 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[2] الفقرة 2 من المادة 59 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[3] الفقرة 3 من المادة 51 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[4] الفقرة 4 من المادة 51 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

عن أي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمتها أو شبكاتها أو المواقع الإلكترونية أو البيانات أو المعلومات الإلكترونية[1]، وكذلك فإن القرار بقانون اعتبر أن من أدلة الإثبات كل دليل متحصل عليه بمعرفة الجهات المختصة أو جهة التحقيق من أي دولة أخرى، طالما أن الحصول عليها تم وفقاً للإجراءات القانونية والقضائية للتعاون الدولي[2].

وأخيراً فإن القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات، لم يتطرق إلى تنظيم الخصوصية في الفضاء الإلكتروني، علماً أنها من أهم المواضيع التي تثير نقاشاً حاداً لدى الكثير من دول العالم، حيث إن مسألة الحق في الخصوصية فيما يتعلق بالمعلومات أو بيانات المشتركين، تعتبر من أهم التحديات التي تواجه التحقيق الإلكتروني. لذلك فإن الحفاظ على خصوصية المشتركين يجب أن يحظى بالاهتمام الكافي من قبل مؤسسات إنفاذ القانون.

كما ننوه إلى أن التحقيق الإلكتروني يحتاج إلى خبراء في هذا المجال، وهو ما تعاني منه الشرطة الفلسطينية، خاصة فيما يتعلق بمأموري الضبط القضائي الذين يضبطون أجهزة الكمبيوتر وأجهزة الهواتف الذكية في مسرح الجريمة قبل إحالتها الى الفرق المتخصصة في مراكز الشرطة، حيث أنه تنقصهم الخبرة والتدريب في مختلف جوانب التحقيق في بعض أنواع الجرائم الإلكترونية وكيفية ضبط والحفاظ على الأدلة الرقمية، وبالتالي لا بد من تأهيلهم للتعامل مع الأدلة الرقمية[3].

---

[1] المادة 57 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات. والأدلة الناتجة عن وسائل تكنولوجيا المعلومات تنقسم إلى أدلة إلكترونية مادية كجهاز الحاسوب والهواتف، وأدلة معنوية كالبانات المخونة عليها. صفاء حسن نصيف، التحديات الإجرائية المتصلة بالجرائم المعلوماتية، مجلة العلوم القانونية والسياسية، مجلد5، عدد2، 2016، ص258.

[2] المادة 58 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات. حول شروط قبول الدليل الإلكتروني أنظر: أحمد عبد الحكيم عبد الرحمن شهاب، شروط قبول الأدلة الإلكترونية أمام االقضاء المصري، مجلة الإجتهاد للدراسات القانونية والإقتصادية، مجلد7، عدد2، 2018، ص175.

[3] مصطفى عبد الباقي، التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين: دراسة مقارنة، مرجع سابق، ص287.

المبحث الثاني: إجراءات المحاكمة في الجرائم الإلكترونية

تعد السلطة القضائية السلطة المختصة للفصل في المنازعات التي تنشأ بين الأفراد، أو قد تنشأ بين الأفراد ومؤسسات الدولة، وقد منح القانون الأساسي الفلسطيني السلطة القضائية الإستقلالية في إصدار أحكامها[1]، فهي تصدر أحكامها في الوقائع التي تنظر فيها دون تدخل أي سلطة أخرى[2].

وتختلف مرحلة التحقيق الإبتدائي عن مرحلة المحاكمة، إذ إن مرحلة التحقيق الإبتدائي وتتولاه النيابة العامة، يهدف إلى البحث عن الأدلة التي تدين المتهم أو تبرءه، وإحالة الدعوى إلى المحكمة المختصة, أما المحاكمة فإن السلطة التي تقوم بها هي السلطة القضائية ممثلة بهيئة قضاة المحكمة، ويتمثل عمل المحكمة المختصة في الفصل في الدعوى القائمة أمامها ويكون الفصل فيها إما بالإدانة أو البراءة أو أي قرار آخر يصدر عنها مثل الإسقاط أو عدم الاختصاص[3].

وفي الوقائع فإن إجراءات المحاكمة في الجرائم الإلكترونية لا تختلف عن إجراءات المحاكمة في الجرائم التقليدية، علماً أن القاضي قد ينظر في قضايا ليس لديه الخبرة فيها، لذلك من الممكن للقاضي أن يستعين بخبراء أثناء المحاكمة. وسنتناول هذا المبحث من خلال التطرق إلى إجراءات محاكمة المتهم بارتكاب الجريمة الإلكترونية (المطلب الأول)، ثم تناول إجراءات الطعن في الحكم الصادر في الجرائم الإلكترونية (المطلب الثاني).

[1] المادة 97 من القانون الأساسي الفلسطيني المعدل لسنة 2003.

[2] المادة 98 من القانون الأساسي الفلسطيني المعدل لسنة 2003.

[3] مصطفى عبد الباقي، مرجع سابق، ص286.

المطلب الأول: إجراءات محاكمة المتهم بارتكاب جريمة إلكترونية

صنف المشرع الفلسطيني الجرائم الإلكترونية إلى جنح وجنايات، حيث جاء في الفقرة 2 من المادة 3 من القرار بقانون رقم 10 لسمة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات "تتولى المحاكم النظامية والنيابة العامة وفقاً لإختصاصاتهما النظر في دعاوى الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات".

وقد أصاب المشرع الفلسطيني في ذلك؛ إذ إنه لا تتساوى جريمة الدخول غير المشروع إلى النظام الإلكتروني مع جريمة الاتجار في الأعضاء البشرية أو جريمة الإباحة ضد الأفراد لمن هم دون سن الثامنة عشر.

وتعتبر محاكم الصلح مختصة بالنظر في جميع المخالفات والجنح الواقعة ضمن اختصاصها، ما لم ينص القانون على خلاف ذلك[1]. فيما تعتبر محاكم البداية مختصة بالنظر في جميع الجنايات، وجرائم الجنح المتلازمة معها والمحالة إليها بموجب قرار الاتهام[2]. وفي حال رأت محكمة البداية أن الواقعة كما هي مبينة في تقرير الاتهام وقبل تحقيقها في الجلسة تعد جنحة تحكم بعدم الاختصاص، وتحيلها إلى محكمة الصلح. وإذا تبين لمحكمة الصلح أن الجريمة المقدمة إليها من اختصاص محكمة البداية تحكم بعدم اختصاصها، وتحيلها إلى النيابة لاتخاذ ما تراه بشأنها[3].

وسيتناول الباحث هذا المطلب من خلال التطرق إلى إحالة ملف الدعوى للمحكمة المختصة وتبعاته القانونية (الفرع الأول)، ثم تناول مسألة الإثبات الجنائي في الجرائم الالكترونية (الفرع الثاني)، على أن يتم الحديث في (الفرع الثالث) عن مسألة إصدار الحكم في الجرائم الالكترونية.

---

[1] المادة 167 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[2] الفقرة 1 من المادة 168 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[3] المادة 169 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

الفرع الأول: إحالة ملف الدعوى للمحكمة المختصة والآثار المترتبة على ذلك

يترتب عن إحالة ملف الدعوى دخول الدعوى في حوزة المحكمة المختصة، وتختص النيابة العامة بسلطة إحالة ملف الدعوى للمحكمة المختصة، وفي حال صنفت الجريمة الإلكترونية على أنها جنحة، فإن قرار الإحالة من وكيل النيابة يعتبر قراراً نهائياً ولا يُشترط فيه عرضه على النائب العام، أما في حال صنفت الجريمة الإلكترونية على أنها جناية، فإن قرار الإحالة يكون من اختصاص النائب العام، وذلك وفقاً لما نصت عليه المواد 151 و152 من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001[1].

وفي حال كانت الجريمة الإلكترونية جناية، ورأى النائب العام وجوب إجراء المزيد من التحقيقات، يأمر بإعادة ملف الدعوى لوكيل النيابة لاستيفاء التحقيقات المطلوبة، وفي حال وجد النائب العام أو أحد مساعديه أن قرار الإحالة صحيح، يأمر بإحالة المتهم إلى المحكمة المختصة، أما إذا تبين للنائب العام أن الجريمة الإلكترونية لا تشكل جناية، فله أن يأمر بتعديل وصف التهمة وإعادة ملف الدعوى لوكيل النيابة ليتم تقديمها للمحكمة المختصة[2]. إضافةً لذلك، فإن قرار إحالة ملف الدعوى لا يقبل الطعن فيه من أي خصم من الخصوم، وللخصوم أن يتقدموا بدفوعهم أما المحكمة المختصة[3].

---

[1] نصت المادة 151 من قانون الإجراءات الجزائية رقم 3 لسنة 2001 والمتعلقة بالفعل الذي يشكل جنحة على أنه " إذا تبين لوكيل النيابة أن الفعل يشكل جنحة يقرر توجيه الاتهام إلى المتهم وإحالة ملف الدعوى إلى المحكمة المختصة لمحاكمته". فيما نصت المادة 152 من ذات القانون والمتعلقة بالفعل الذي يشكل جناية في الفقرة 1 منها على أنه " إذا تبين لوكيل النيابة أن الفعل يشكل جناية فإنه يقرر توجيه الاتهام إلى المتهم ويرسل ملف الدعوى إلى النائب العام أو أحد مساعديه".

[2] الفقرة 2 و الفقرة 3 و الفقرة 4 من المادة 152 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[3] المادة 53 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

ولا بد أن يشتمل قرار إحالة ملف الدعوى للمحكمة المختصة على مجموعة من البيانات من قبيل[1]: اسم المشتكي، اسم المتهم وشهرته وعمره ومحل ولادته، عنوان المتهم وعمله، تاريخ توقيف المتهم، موجز عن الجريمة المسندة إليه، تاريخ ارتكاب الجريمة، نوع الجريمة، ووصفها القانوني، المادة القانونية التي استند إليها الاتهام، الأدلة على ارتكاب الجريمة.

ونشير هنا إلى أن إجراءات سير المحاكمة في الجرائم الإلكترونية هي ذات الإجراءات التي تسير فيها المحاكمة في الجريمة التقليدية، وذلك من حيث علنية المحاكمات ما لم تقرر المحكمة إجراءها بشكل سري[2]، ويتولى وكيل النيابة تلاوة التهم على المتهم في الجرائم الواردة في قرار الاتهام[3].

كما يمكن للمحكمة أن تعدل التهمة بشرط أن لا يبنى هذا التعديل على وقائع لم تشملها البينة المقدمة، وفي حال كان التعديل يعرض المتهم لعقوبة أشد، تؤجل القضية للمدة التي تراها المحكمة ضرورية، وذلك لتمكين المتهم من تحضير دفاعه على التهمة المعدلة[4].

الفرع الثاني: الإثبات الجنائي في الجرائم الإلكترونية

يترك ارتكاب الجريمة الإلكترونية بصمات رقمية، وخلافاً للأدلة المادية فإن هذه البصمات الرقمية غير مرئية، أو أنها مرئية افتراضياً، كما أنها ذات طبيعة متقلبة، غير أنه يمكن العثور على الأدلة الرقمية في ذاكرة تخزين المعلومات، قد تكون وحدات تخزين دائمة، كما أنها قد تكون وحدات تخزين مؤقتة[5].

[1] المادة 154 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[2] المادة 237 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[3] المادة 239 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[4] المادة 270 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[5] مصطفى عبد الباقي، التحقيق في الجرائم الإلكترونية وإثباتها في فلسطين: دراسة مقارنة، مرجع سابق، ص292.

واختلفت أنظمة الإثبات في تقديرها لحجة الدليل الإلكتروني وتتمثل في نظام الإثبات الحر أو الإقتناع الذاتي، حيث يكون للقاضي الحرية الكاملة في البحث عن الحقيقة بكافة الوسائل الممكنة والمشروعة[1]، ونظام الإثبات المقيد، وهو نظام الأدلة القانونية يقضي بأن القاضي يستخدم وسائل الإثبات المحددة في القانون، بحيث لا يملك أن يقتنع إلا بهذه الأدلة المقررة قانوناً[2].

نشير هنا إلى أن هناك نوعان رئيسان لأدلة الإثبات: الأول، الأدلة التقليدية مثل شهادة الشهود والخبرة والأدلة المادية وغيرها؛ والثاني الأدلة غير التقليدية، وهي الأدلة الرقمية. وكل منهما يختلف عن الآخر في سلامته ودرجة مقبوليته.

ولنجاح أي تحقيق جنائي لا بد من سلامة الدليل، خاصةً عندما يتعلق الأمر بالدليل الرقمي سريع التحول، والذي يمكن أن يلحق به أذى وتتغير طبيعته، فإذا ما لحق الدليل ال قمي أي عطب يصبح غير مقبول في الإثبات الجنائي، لذلك يتوجب على مأموري الضبط والمحققين وأعضاء النيابة العامة التعامل مع الأدلة الرقمية بمسؤولية عالية حتى لا يتم فقدانها وخسارتها، مع الحفاظ على النسخة الأصلية؛ وذلك حتى لا يطعن المتهم بسلامة الدليل الرقمي.

ومع تنامي ظاهرة الجرائم الإلكترونية وتطور وسائل مؤسسات إنفاذ القانون في يخص الإثبات، لعبت الأدلة الرقمية دوراً متعاظماً في إثبات الجريمة الإلكترونية في الدول المتقدمة، وقد حذا المشرع الفلسطيني حذو الدول المتقدمة، إذ أكد على ضرورة أخذ كافة الإحتياطات اللازمة والضرورية للحفاظ على سلامة الأدلة لحماية محتواها المتحفظ عليها بما فيها الأجهزة والأدوات والأنظمة الإلكترونية والبيانات وكافة وسائل تكنولوجيا المعلومات[3].

---

[1] علي حسن محمد الطوالبة، التفتيش الجنائي على نظام الحاسوب والإنترنت، البحرين، 2010 ص201.

[2] عبدالله بن سعيد أبو داسر، إثبات الدعوى الجنائية، أطروحة دكتوراة، جامعة الإمام محمد بن سعود الإسلامية، 2021–2022، ص13.

[3] الفقرة 5 من المادة 53 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته، مرجع سابق. وكذلك المادة 55 من ذات القرار بقانون.

وقد أكد المشرع الفلسطيني على أن الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو المواقع الإلكترونية أو شبكات المعلومات أو البيانات والمعلومات الإلكترونية جميعها تعتبر من أدلة الإثبات[1]، وكذلك تعتبر من أدلة الإثبات الأدلة المتحصل عليها بمعرفة الجهة المختصة أو جهات التحقيق من دول أخرى[2]، وقد جرم المشرع الفلسطيني فعل العبث بالأدلة القضائية سواء من خلال اتلافها أو إخفائها أو تعديلها أو محوها، بالحبس مدة لا تقل عن سنة وبغرامة مالية لا تقل عن 1000 دينار أردني ولا تزيد عن 3000 دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً[3].

وقد ساوى المشرع الفلسطيني في الإثبات بين الوثيقة المادية المكتوبة والوثيقة الرقمية المكتوبة على الأجهزة الإلكترونية [4]، كما أكد قانون الإجراءات الجزائية على أن الإثبات بالوثائق الإلكترونية جائز في الدعاوى الجزائية بجميع طرق الإثبات ما لم ينص القانون على طريقة معينة للإثبات وطالما اقتنع القاضي بالدليل[5].

الفرع الثالث: إصدار الحكم في الجرائم الإلكترونية

أكد المشرع الفلسطيني على أن إجراءات إصدار الحكم في الجرائم العادية هي ذاتها المطبقة في الجرائم الإلكترونية، إذ نصت المادة 205 من قانون الإجراءات الجزائية رقم 3 لسنة 2001 على

---

[1] المادة 57 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته. للإستزادة: عدنان إبراهيم الحجار، فايز خضر بشير، الأدلة الرقمية وإثبات الجرائم السبرانية ما بين التأصيل والتأويل، مجلة جامعة الإستقلال للأبحاث، مجلد6، عدد1، تشرين أول\2021، ص134.

[2] المادة 58 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته.

[3] المادة 67 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته.

[4] قانون البينات في المواد المدنية والتجارية رقم 4 لسنة 2001. وكذلك: هلالي عبدالله أحمد، تفتيش نظام الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، ط2، 2008، ص121.

[5] المادة 206 من قانون الإجراءات الجزائية رقم 3 لسنة 2001. كذلك: علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، كلية الحقوق، جامعة حلوان، بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية الشرطة، دبي، مركز البحوث والدراسات، الإمارات العربية المتحدة 2003 / 22-28\ نيسان\ 2003، ص34-35.

عدم جواز الحكم بالعلم الشخصي، إذ لا يجوز للقاضي الحكم بعلمه الشخصي، وإنما يلتزم بما هو مقدم إليه من وثائق وأدلة، فلا يقوم الحكم إلا بناء على الأدلة المقدمة أثناء المحاكمة. وفي حال لم تقم البينة على المتهم يجب على القاضي الحكم ببراءته[1]. وهو ما أكدته عليه المادة 24 من القرار بقانون رقم (7) لسنة 2022م بشأن تعديل قانون الاجراءات الجزائية رقم (3) لسنة 2001م وتعديلاته.

ويصدر الحكم بالإجماع أو بالأغلبية (باستثناء عقوبة الإعدام التي تكون بالإجماع) بعد المداولة والتدقيق فيما طرح أمام المحكمة من بينات وادعاءات، ويصدر الحكم في ذات اليوم أو في يوم آخر تعينه المحكمة للنطق بالحكم[2].

وأكد المشرع الفلسطيني على أن الحكم يجب أن يكون مشتملاً على[3]: ملخص الوقائع الواردة في قرار الاتهام والمحاكمة، ملخص طلبات النيابة العامة والمدعي بالحق المدني ودفاع المتهم، الأسباب الموجبة للبراءة أو الإدانة، المادة القانونية المنطبقة على الفعل في حالة الإدانة، تحديد العقوبة ومقدار التعويضات المدنية.

كما يجب أن يكون الحكم موقعاً، إذ يوقع القضاة على الحكم، ويتلى علناً بحضور وكيل النيابة العامة والمتهم، ويفهم الرئيس المحكوم عليه بأن له الحق في استئناف الحكم خلال المدة المقررة قانوناً[4]. ثم لا بد من تسجيل الحكم في سجل الأحكام، حيث يسجل الحكم بعد صدوره في سجل

---

[1] المادة 205 والفقرة 2 من المادة 206 والمادة 207 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[2] المادة 23 من القرار بقانون رقم (7) لسنة 2022م بشأن تعديل قانون الاجراءات الجزائية رقم (3) لسنة 2001 وتعديلاته، القاضية بتعديل المادة 272 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[3] المادة 276 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[4] المادة 277 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

الأحكام الخاصة بالمحكمة، ويحفظ أصل الحكم مع أوراق الدعوى التي صدر فيها، كما تقوم المحكمة بإرسال قائمة بالأحكام التي صدرت إلى النائب العام[1].

المطلب الثاني: إجراءات الطعن في الحكم الصادر بحق المتهم في الجرائم الإلكترونية

بعد أن يصدر الحكم في موضوع الدعوى الجزائية، فإنه لا يمكن إعادة النظر في الدعوى إلا بالطعن في الحكم الصادر وذلك بطرق الطعن المقررة قانوناً[2]. كما يمكن الطعن كذلك من خلال: الاعتراض، والاستئناف، والطعن بالنقض، والنقض بأمر خطي، وإعادة المحاكمة.

وقد نظم قانون الإجراءات الجزائية رقم 3 لسنة 2001 وتعديلاته الإجراءات المتعبة للطعن في الحكم الصادر عن المحكمة في كافة الجرائم سواء التقليدية منها أو الإلكترونية، حيث يقبل الطعن في جميع الأحكام الجنائية الصادرة عن محكمة الاستئناف، وكذلك الأحكام والقرارات الصادرة من المحاكم الأخرى التي تنص قوانينها على أنها تقبل الطعن بطرق الطعن[3].

ويكون الطعن على حكم محاكم الاستئناف إذا ما شابهها مخالفة في القانون أو خطأ في تطبيقه أو تأويله أو في حالة وقوع بطلان في الحكم أو بطلان في الإجراءات. وسيتناول الباحث إجراءات الطعن في الحكم بحق المتهم في الجريمة الإلكترونية من خلال التطرق إلى مسألة طرق الطعن في الجرائم الإلكترونية (الفرع الأول)، وكذلك مسألة الأثر المترتب على الطعن بحق المتهم في الجريمة الإلكترونية (الفرع الثاني).

---

[1] المادة 282 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[2] المادة 388 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[3] المادة 39 من القرار بقانون رقم (7) لسنة 2022م بشأن تعديل قانون الاجراءات الجزائية رقم (3) لسنة 2001.
على سبيل المثال لا الحصر: القضية رقم 41\2021، صادرة عن محكمة النقض، 4\إبريل\2021.

الفرع الأول: طرق الطعن في الجرائم الإلكترونية

حدد قانون الإجراءات الجزائية رقم 3 لسنة 2001، طرق معينة يتم من خلالها الطعن في الحكم الصادر عن المحكمة، إذ أن طرق الطعن تكون على نوعين: طرق الطعن العادية، كالإستئناف والإعتراض، وطرق الطعن غير العادية كإعادة المحاكمة، والنقض.

وبموجب المادة 349 من القانون، يكون الطعن بالنقض من خلال: النيابة العامة، المحكوم عليه، المدعي بالحق المدني، المسؤول عن الحقوق المدنية. ويكون الطعن بالنقض بحكم القانون في جميع الأحكام الصادرة بالإعدام أو بالحبس المؤبد حتى ولو لم يطلب الخصوم ذلك[1].

وقد أشار قانون الإجراءات الجزائية رقم 3 لسنة 2001 إلى الحالات التي يقبل فيها الطعن بالنقض وهي على النحو الآتي[2]: إذا وقع بطلان في الإجراءات أثر في الحكم، إذا لم تكن المحكمة التي أصدرته مشكلة وفقاً للقانون، أو لم تكن لها ولاية الفصل في الدعوى، إذا صدر حكمان متناقضان في وقت واحد في واقعة واحدة، الحكم بما يجاوز طلب الخصم، إذا كان الحكم المطعون فيه مبني على مخالفة للقانون، أو على خطأ في تطبيقه، أو في تفسيره، خلو الحكم من أسبابه الموجبة، أو عدم كفايتها، أو غموضها، أو تناقضها، مخالفة قواعد الاختصاص أو تجاوز المحكمة سلطاتها القانونية، مخالفة الإجراءات الأخرى إذا كان الخصم قد طلب مراعاتها ولم تستجب له المحكمة ولم يجر تصحيحها في مراحل المحاكمة التي تليها.

ويكون تقديم طلب الطعن بالنقض خلال 40 يوماً تبدأ من اليوم الذي يلي تاريخ صدور الحكم إذا كان حضورياً، أو من اليوم الذي يلي تبليغه إذا كان الحكم بمثابة الحضوري[3]، و يقدم طلب الطعن

[1] المادة 350 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[2] المادة 351 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[3] المادة 355 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

بالنقض إلى قلم المحكمة التي أصدرت الحكم أو إلى قلم محكمة النقض[1]، على أنه يجب أن يشمل طلب الطعن بالنقض على[2]:

1- يجب أن يكون طلب الطعن موقعاً من الطاعن أو من محام.

2- أن يتضمن أسباب الطعن، وأسماء الخصوم

3- أن يكون مرفقاً به إيصال دفع الرسوم المقررة

4- أن يؤشر إليه قلم المحكمة بتاريخ التسجيل

وفي حال لم يكن الطعن مقدماً من النيابة العامة أو من المحكوم عليه الموقوف لعقوبة سالبة للحرية فإنه يجب لقبوله أن يودع الطاعن في خزينة المحكمة مبلغ 50 ديناراً أردنياً أو ما يعادلها بالعملة المتداولة قانوناً، في حال لم يكن قد أعفي من الرسوم القضائية، ويعتبر المبلغ تأميناً يرد إلى الطاعن إذا كان محقاً في طعنه[3].

وعند إيداع طلب الطعن بالنقض لدى قلم المحكمة التي أصدرت الحكم، فإنه يتعين عليها أن ترسله إلى قلم محكمة النقض مع ملف الدعوى خلال أسبوع. وعندما تكتمل أوراق الطعن بالنقض، يقوم رئيس قلم المحكمة بإرسالها مع ملف الدعوى إلى النيابة العامة[4]، ويتم تسجل الأوراق في سجل النيابة العامة، وترفع مع الملف إلى النائب العام لتدوين مطالعته عليها، ويعيدها خلال 10 أيام من تاريخ وصولها إليه[5].

[1] المادة 356 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[2] المادة 357 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[3] المادة 358 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[4] المادة 362 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[5] المادة 363 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

وتقوم المحكمة بالنظر في الطعن تدقيقاً ويجوز لها أن تحدد جلسة لسماع أقوال النيابة العامة ووكلاء الخصوم إذا ارتأت ذلك[1]، وفي حال رفضت المحكمة جميع أسباب الطعن بالنقض التي تقدم بها الطاعن، ولم تجد من تلقاء نفسها سبباً للنقض ردت الطعن موضوعاً[2].

وفي حال كان الطعن بسبب الخطأ في ذكر نصوص القانون، فلا يجوز نقض الحكم إذا كانت العقوبة المحكوم بها هي المقررة في القانون للجريمة بحسب الوقائع المثبتة في الحكم وتصحح المحكمة الخطأ الذي وقع فيه وترد الطعن بالنتيجة، كما أنه لا يمكن للمحكوم عليه الاستناد إلى الطعن للامتناع عن تنفيذ الحكم المطعون فيه[3].

كما أن الطعن بالنقض يقتصر على الجزء المطعون فيه، إذ أنه لا ينقض من الحكم إلا الجزء الذي طعن فيه ما لم تكن التجزئة غير ممكنة[4]. وفي حال كان الحكم المطعون فيه صادراً بقبول دفع قانوني مانع من السير في الدعوى ونقضته محكمة النقض، وأعادت القضية إلى المحكمة التي أصدرته لنظر الموضوع، فإنه لا يجوز للمحكمة أن تحكم بعكس ما قضت به محكمة النقض[5].

ولا يقبل من الخصم أن يدفع ببطلان بعض الإجراءات التي تمت أمام محاكم الصلح والبداية إذا لم يحتج بها أمام محكمة الاستئناف[6]، كما أنه لا يقبل من الخصم أن يتقدم بدليل مستمد من وقائع لم يتطرق إليها أسباب الحكم المطعون فيه[7]. في حين أنه يمكن للمحكمة أن تنقض الحكم لمصلحة المتهم وذلك من تلقاء نفسها في حال تبين لها مما هو ثابت فيه أنه مبني على مخالفة القانون، أو على خطأ في تطبيقه أو في تأويله، أو أن المحكمة التي أصدرته لم تكن مشكلة وفقاً للقانون، أو

---

[1] المادة 366 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[2] المادة 367 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[3] المادة 369 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[4] المادة 370 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[5] المادة 371 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[6] المادة 352 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[7] المادة 353 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

لا ولاية لها للنظر في الدعوى، أو إذا صدر بعد الحكم المطعون فيه قانون يسري على واقعة الدعوى[1].

الفرع الثاني: الأثر المترتب على الطعن بحق المتهم في الجريمة الإلكترونية

يعتبر الحكم الصادر عن محكمة النقض حكماً قطعياً وباتاً، ففي حال قررت المحكمة رد طلب الطعن بالنقض، يصبح الحكم باتاً ولا يجوز بأي حال من الأحوال لمن رفعه أن يرفع طعناً آخر عن الحكم ذاته لأي سبب كان[2]. وفي حال طُعن في الحكم الصادر بعد النقض الأول، تنظر محكمة النقض في موضوع الدعوى[3].

ويمكن لوزير العدل أن يطلب من النائب العام خطياً عرض ملف الدعوى على محكمة النقض لوقوع إجراء فيها مخالف للقانون أو لصدور حكم أو قرار فيها مخالف للقانون، وكان الحكم أو القرار مكتسب الدرجة القطعية ولم يسبق لمحكمة النقض التدقيق في الإجراء أو الحكم أو القرار المطعون فيه، على أن يقدم ملف الدعوى إلى محكمة النقض مرفقاً بالأمر الخطي، وأن يطلب بالاستناد إلى الأسباب الواردة فيه إبطال الإجراء أو الحكم أو نقض الحكم أو القرار[4].

ولذات هذه الأسباب والشروط يحق للنائب العام إذا طلب منه ذلك المحكوم عليه أو المسؤول بالمال، أن يطعن بالنقض في الأحكام والقرارات القطعية في القضايا الجنحوية الصادرة عن محكمة البداية بصفتها الاستئنافية[5].

---

[1] المادة 354 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[2] المادة 373 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[3] المادة 374 من قانون الإجراءات الجزائية رقم 3 لسنة 2001.

[4] الفقرة 1 من المادة 40 من القرار بقانون رقم (7) لسنة 2022م بشأن تعديل قانون الاجراءات الجزائية رقم (3) لسنة 2001.

[5] الفقرة 2 من المادة 40 من القرار بقانون رقم (7) لسنة 2022م بشأن تعديل قانون الاجراءات الجزائية رقم (3) لسنة 2001.

الخاتمة

حاولت هذه الرسالة دراسة موضوع مواءمة التشريع الجزائي الفلسطيني مع الاتفاقيات الدولية لمكافحة الجريمة الإلكترونية بدراسة الأحكام الموضوعية للجرائم الناشة عن التقنيات الإلكترونية عن طريق بيان مفهوم الجريمة الإلكترونية وخصائصها وأركانها وطبيعتها القانونية، ولتبيان مدى مواءمة التشريع الفلسطيني مع الاتفاقيات الدولية فيما يخص الجرائم الإلكترونية تناولت الرسالة الإجراءات القانونية في مكافحة الجرائم الإلكترونية كإجراءات الإستدال والتحقيق وإجراءات المحاكمة وما يترتب عليها من آثار.

واتضح من سياق الرسالة أن موضع الجريمة الإلكترونية هو موضوع متجدد، إذ أنه في كل فترة يعرف تطورات جديدة؛ وذلك لما يتمتع به من خصائص ومميزات تميزه عن الجرائم التقليدية، وهو ما يجعل من مسألة مواجهة الجرائم الإلكترونية والحد منها، مسألة صعبة ومعقدة بحاجة إلى إستراتيجيات وآليات متطورة على المستوى الوطني، وكذلك بحاجة إلى تحقيق التعاون الدولي في مواجهة الجرائم الإلكترونية والحد منها من خلال الإلتزام بما نصت عليه الإتفقيات والمواثيق الدولية بخصوص هذا الشأن.

إن الدوافع وراء وجود الجريمة الإلكترونية مرتبط بما هو عالمي وبما هو مجتمعي وكذلك بما هو فردي، وتتفاوت وفق نوعها ونوع المستهدف ونوع الجاني ومستوى تنفيذه، وكذلك هو الحال بالنسبة لمواجهتها والحد منها، ولأجل أن تجني تلك المواجهة ثمارها، لا بد من مواجهة الجريمة الإلكتروني على مستوى الفرد وعلى مستوى المجتمع وعلى المستوى الدولي وتحقيق التعاون فيما بينهم.

وبعد البحث والتمحيص في كافة أطراف موضوع الرسالة، فقد تبين للباحث أن المشرع الفلسطيني ملتزم إلى حد كبير بمسألة مواءمة التشريع الجزائي الفلسطيني مع الاتفاقيات الدولية في إطار

مكافحة الجرائم الإلكترونية، وبالتالي فإن الباحث يؤكد صحة الفرضية التي انطلق منها وهي أن الجريمة الإلكترونية تشكل ظاهرة عالمية عابرة للحدود ونوعا مختلفا عن أشكال الجرائم الأخرى التي تهدد أمن المجتمعات، لذلك لا بد من إدماج ما توصلت إليه الجهود الدولية في سبيل الحد من سلبيات ومخاطر ظاهرة الجريمة الإلكترونية في القوانين والتشريعات الداخلية، وبالتالي معالجة أي قصور تعاني منها القوانين الداخلية للإحاطة بكافة جوانب ظاهرة الجريمة الإلكترونية.

فيما استخلص من الرسالة مجموعة من النتائج، وانتهت الرسالة إلى مجموعة من التوصيات التي بنيت على أساس ما توصلت إليه الرسالة من نتائج، وفيما يلي نستعرض أهم النتائج التي انتهت إليها الرسالة وما خلصت إليه الرسالة من توصيات.

النتائج

1. أصدر المشرع الفلسطيني تشريعاً خاصاً لمكافحة الجريمة الإلكترونية متماشياً بذلك مع الاتفاقيات الدولية.
2. أدرك المشرع الفلسطيني أهمية تكنولوجيا المعلومات في تحسين أداء الإدارة والأمن على حدٍ سواء، وعمل على إنشاء مؤسسات خاصة بالتحقيق في الجرائم الإلكترونية وجمع الأدلة الرقمية، وذلك تماشياً مع الاتفاقيات الدولية والإقليمية.
3. تكاثف الجهود الدولية لإنتاج اتفاقيات دولية أكثر شمولية وتوضيح في يخص الجريمة الإلكترونية في ضوء التطورات التكنولوجية.
4. عرف المجتمع الدولي العديد من الحالات التي تصنف على أنها جرائم إلكترونية والتي لم تعرفها الاتفاقيات الدولية من قبل.

5. ليس هناك تعرفياً فقهياً جامعاً مانعاً لمفهوم الجرائم الإلكترونية.
6. أغلب التشريعات لم تضع مفهوماً صريحاً للجريمة الإلكترونية، وإنما أشارت إلى الحالات التي تشكل جريمة الإلكترونية.
7. كانت المخاطر المختلفة للجرائم الإلكترونية الدافع وراء التفكير الجاد لمعالجة ومكافحة هذا الموضوع سواء على المستوى الدولي أو على المستوى الإقليمي والوطني.
8. التعاون الدولي بين الدول فيما بينها أو بين المؤسسات الدولية لم تصل إلى الحد المطلوب لمكافحة الجرائم الإلكترونية، سواء من حيث عقد الاتفاقيات الثنائية أو الدولية ذات الصلة بالموضوع، أو من حيث وجود هيئة دولية أو مركز دولي لتنسيق الجهود الدولية المتعلقة بموضوع الجرائم الإلكترونية.
9. ميز المشرع الفلسطيني في العقوبة بين جريمة الإباحية المتعلقة بالأشخاص لمن هم فوق عمر 18 عام، وبين جريمة الإباحية المتعلقة بالأطفال والقصر.
10. وجود بعض القصور القانونية في الاتفاقيات الدولية أو الإقليمية المتعلقة بالجرائم الإلكترونية ومكافحتها، كعدم تطرقها لمسألة الخصوصية وحق المشترك بإعلامه بالإجراءات التي يتم اتخاذها بشأن جمع البيانات والمعلومات حول نشاطه الرقمي والاعتراض عليها.
11. لم يتناول القرار بقانون رقم 10 لسنة 2018 وتعديلاته مسألة الخصوصية، باعتبارها من أهم التحديات التي تواجه المحقق الجزائي، حيث لا يجوز للمحقق ضبط وتفتيش أجهزة الكمبيوتر وأجهزة الاتصال الذكي التي تعود للمتهم إلا وفقا لقيود وضوابط

محددة. ويُخشى من ضياع الأدلة الرقمية خلال الفترة اللازمة للحصول على الإذن المطلوب، خاصة أنها من النوع سريع التغير والتلف.

توصيات الرسالة

1- الدعوة لعقد المزيد من المؤتمرات الدولية لبحث ما عرفه المجتمع الدولي من حالات متطورة تتعلق بالجرائم الإلكترونية.

2- إنشاء هيئة دولية لتنسيق الجهود الدولية الرامية لمكافحة الجرائم الإلكترونية.

3- ضرورة تظافر الجهود الدولية من أجل إعداد رجال الشرطة الدولية (الإنتربول)، بالإضافة لرجال الشرطة الوطنية، إعداداً تقنياً وفنياً وتأهيلهم في مجال مكافحة الجرائم الإلكترونية.

4- نقترج وجود محاكم متخصصة بالجرائم الإلكترونية يمتاز قضائها بدرجة عالية من التأهيل العلمي والتقني، أو على الاقل وجود هيئات قضائية متفرعة ومختصة بالنظر في موضوع الجرائم الإلكترونية على المستوى الوطني.

5- ضرورة وجود نصوص قانونية تحمي الجهات التي تبلغ عن الجرائم الإلكترونية سواء من حيث سرية التبليغ أو من حيث سرية التحقيق والمحاكمة على المستوى الوطني.

6- تعزيز القوانين الوطنية الفلسطينية لمكافحة الجرائم الإلكترونية من خلال نقل معارف المحاكم الجنائية الدولية وممارستها.

7- زيادة الخبرات المهنية لدى الأخصائيين الممارسين في مجال مكافحة الجريمة الإلكترونية من خلال تحديد مجالات تدخل رئيسية لدعم الكشف المبكرعن التهديدات الجديدة والناشئة التي تثيرها الجريمة الإلكترونية، واعتماد وتنفيذ سياسات تكفلِ التصدي بفعالية لتلك التهديدات.

8- ضرورة إجراء بعض التعديلات على القانون الفلسطيني رقم 10 لسنة 2018 وتعديلاته، وتحديد مدة الحبس كتلك المتعلقة بالسرقة والإختلاس في نص المادة 13.

9- إلحاق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ببروتوكول خاص بها يناقش القصور الذي شاب الاتفاقية مثل مسألة الخصوصية وحق المشترك في إعلامه بالإجراءات التي يتم اتخاذها بشأن جمع البيانات والمعلومات حول نشاطه الرقمي.

10- على اعتبار أن حماية الخصوصية من أهم التحديات التي يواجهها التحقيق الإلكتروني، فإنه لا بد من إصدار قانون للفصل في هذه المسألة.

11- إضافة نصوص قانونية تتعلق بمسألة الإثبات في الجرائم الإلكترونية، إذ ما يزال التشريع الفلسطيني يشوبه بعض القصور في هذا المجال.

المراجع

أولا: المصادر:

اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية وبروتوكولاتها، صادرة بموجب قرار الجمعية العامة للأمم المتحدة 25/55 المؤرخ في 15 تشرين الثاني/نوفمبر 2000، نفذت بتاريخ 29\سبتمبر\2003.

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الأمانة العامة لجامعة الدول العربية، القاهرة، 2010/12/21.

الاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست)، مجلس أوروبا، مجموعة المعاهدات الأوروبية، رقم 185، 2001/11/23.

البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الإلكترونية بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية، سلسلة معاهدات مجلس أوروبا، 2022.

التقرير التفسيري لاتفاقية الجرائم الإلكترونية، مجلس أوروبا، سلسلة المعاهدات الأوروبية رقم 185، بودابست، 23\نوفمبر\2001.

قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م وتعديلاته، صادر في مدينة غزة بتاريخ 2001\5\12.

القانون الأساسي الفلسطيني المعدل، الصادر في مدينة رام الله بتاريخ 2003\3\18.

قانون الجرائم الإلكترونية الفلسطيني رقم (10) عام 20م18 وتعديلاته، جريدة الوقائع الفلسطينية، عدد186، ص30، 2021\12\23.

القانون الفرنسي رقم 17 الصادر بتاريخ 6\يناير\ 1978 بشأن معالجة المعلومات والملفات والحريات، وجرى تعديله بموجب القانون رقم 493 الصادر بتاريخ 20\يونيو\2018.

القانون رقم 63 لعام 2015 الكويتي بشأن مكافحة جرائم تقنية المعلومات.

قانون مكافحة الجرائم الإلكترونية القطري رقم 14 لعام 2014.

هيئة الاتصالات وتقنية المعلومات، نظام مكافحة جرائم المعلوماتية السعودي

أحكام المحاكم:

محكمة النقض الفلسطينية– رام الله– (القضية رقم 2021/41)، الصادر بتاريخ 2021/4/4م.

محكمة النقض الفلسطينية– رام الله– (نقض/جزاء فلسطيني رقم 147 لسنة 2020)، الصادر بتاريخ 2020/4/30م.

محكمة النقض الفلسطينية– رام الله –القضية رقم (2023/332)، الصادر بتاريخ 24/سبتمبر/2023م.

ثانيا: المراجع:

1- الكتب:

إبراهيم خ، (2009)، *الجرائم المعلوماتية، دار الفكر العربي*، ط1، الإسكندرية.

أبو بكر م، (2011)، *موسوعة جرائم المعلوماتية (جرائم الكمبيوتر والإنترنت)*، المكتب العربي الحديث، الإسكندرية.

أحمد هـ، (2008)، *تفتيش نظام الحاسب الآلي وضمانات المتهم المعلوماتي*، دار النهضة العربية، القاهرة، ط2.

البراك أ، جرادة ع، (2019)، *الجرائم الإلكترونية في التشريع الفلسطيني دراسة تحليلية تأصيلية مقارنة*، دار الشروق للنشر والتوزيع، ط1، رام الله.

بن دراج ع، (2021)، *محاضرات في الجرائم المعلوماتية*، المركز الجامعي آفلو، معهد الحقوق والعلوم السياسية، الجزائر.

الجنبيهي م، (2006)، *تزوير التوقيع الإلكتروني*، دار الفكر الجامعي، الإسكندرية.

الحجار ع، بشير ف، (2011)، *الأدلة الرقمية وإثبات الجرائم السبرانية ما بين التأصيل والتأويل*، مجلة جامعة الإستقلال للأبحاث، مجلد6، عدد1.

حسني م، (1979)، *شرح قانون العقوبات القسم العام*، دار النهضة العربية، القاهرة.

حسني م، (2006)، *النظرية العامة للقصد الجنائي دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية*، دار النهضة العربية، القاهرة.

خلف ج، (2017)، *نحو تطورات في الإجراءات الجزائية*، منشورات زين الحقوقية، بيروت.

زين الدين ب، (2008)، *جرائم أنظمة المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية*، دار الفكر العربي، ط1، الإسكندرية.

سلامة م، (2007)، *جرائم الكمبيوتر والإنترنت، المكتب العربي الحديث*، الإسكندرية، مصر.

شاهين م، (2018) ، *الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الإبتدائي*، دار الجامعة الجديدة، الإسكندرية، مصر.

الشوا م، (2003)، *ثورة المعلومات وانعكاساتها على قانون العقوبات*، مطابع الهيئة المصرية العامة للكتاب، مصر.

الطوالبة ع، (2010)، *التفتيش الجنائي على نظام الحاسوب والإنترنت*، البحرين.

عبد الباقي م، (2015)، *شرح قانون الإجراءات الجزائية الفلسطيني*، وحدة البحث العلمي والنشر، كلية الحقوق والإدارة العامة، جامعة بيرزيت.

عبد الله ع، (2007)، *جرائم المعلوماتية والإنترنت (الجرائم الإلكترونية)*، منشورات الحلبي الحقوقية، ط1، بيروت.

قشقوش ه، (1992)، *جرائم الحاسب الالكتروني في التشريع المقارن*، دار النهضة العربية، القاهرة.

قورة ن، (2005)، *جرائم الحاسب الاقتصادية: دراسة نظرية تطبيقية*، منشورات الحلبي الحقوقية، ط1، القاهرة.

الكعبي م، (2009)، *الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت دراسة مقارنة*، دار النهضة العربية، ط2، القاهرة.

محمد أ ، (2003)، *الإذن بالتفتيش والضبط*، دار النهضة العربية، ط3، مصر.

المصري ي، (2010)، *الجرائم المعلوماتية والرقمية للحاسوب والإنترنت*، دار العدالة، القاهرة.

المضحكي ح، (2014)، *الجرائم المعلوماتية دراسة مقارنة*، منشورات الحلبي الحقوقية، ط1، بيروت.

الملط أ، (2005)، *الجرائم المعلوماتية*، دار الفكر الجامعي، الإسكندرية.

ممدوح إ، (2022)، *إجراءات التفتيش في الجرائم المعلوماتية*، دار الفكر الجامعي، مصر.

موسى م، (2009)، *التحقيق الجنائي في الجرائم الإلكترونية*، مطابع الشرطة، القاهرة.

المومني ن، (2008)، *الجرائم المعلوماتية*، دار الثقافة للنشر والتوزيع، ط1، عمان.

هروال ن، (2007) ، *الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الإستدلالات*، دار الفكر الجامعي، الإسكندرية، مصر.

هلالي أ، (2011)، *إتفاقية بودابست لمكافحة جرائم المعلوماتية*: معلقاً عليها هلالي عبداللاه أحمد، ط1، دار النهضة العربية، القاهرة.

الهيتي م، (2004)، *التكنولوجيا الحديثة والقانون الجنائي*، دار الثقافة للنشر والتوزيع، عمان، ط1، الاردن.

2- كتب مترجمة:

غريفتش م، أوكالاهان ت، (2008)، *المفاهيم الأساسية في العلاقات الدولية*، مركز الخليج للأبحاث، دبي، الإمارات العربية المتحدة،

3- مجلات علمية:

إبراهيم ع، (2015) الجرائم الإلكترونية، مجلة الحقوق العلوم الإنسانية، جامعة زيان عاشور بالجلفة، العدد 23، الجزائر.

إبقال ع، (2017)، الإطار القانوني لمكافحة الجريمة الإلكترونية: دراسة مقارنة، مجلة المنارة للدراسات القانونية والإدارية، المغرب، عدد خاص.
البداينة ذ، (2014)، الجرائم الإلكترونية: المفهوم والأسباب، كلية العلوم الإستراتيجية،
الحمادي خ، (2019)، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري: دراسة مقارنة، مجلة كلية القانون، جامعة قطر.
حمي أ، كيسي ز، (2019)، صور جرائم تقنية المعلومات وفقا لالتفاقية العربية لسنة 2014، مجلة العلوم القانونية والسياسية، مجلد10، عدد1.
الحوامدة ل، (2017)، الجرائم المعلوماتية أركانها وآلية مكافحتها: دراسة تحليلية مقارنة، مجلة الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية العالمية، عمان، الأردن.
دليل الأدلة الإلكترونية، (2014)، دليل أساسي لموظفي الشرطة والمدعين العامين والقضاة، صادر عن مجلس أوروبا، فرنسا.
الذنيبات م، العناسوة م،(2021)، التفتيش في الجرائم الإلكترونية ماهيته وشروطه الشكلية، المجلة الأردنية في القانون والعلوم السياسية، مجلد 13، عدد3.
رستم هـ، (1995)، جريمة الحاسب الآلي كصورة من صور الجرائم الاقتصادية المستحدثة، مؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاملة المجرمين، مجلة الأمن العام، لبنان، العدد 151.
سلامة ن، (2023)، الجرائم الإلكترونية وأثرها على المجتمع، مجلة القاهرة للخدمة الإجتماعية، العدد 39.
شرشر م، (2021)، الجهود الدولية والتشريعية لمكافحة جرائم الانترنت، مجلة البحوث القانونية والاقتصادية، مجلد54، عدد3.
شرف الدين و، (2018)، الأحكام الإجرائية لمكافحة جريمة الاتجار بالأشخاص المرتكبة بواسطة تقنية المعلومات دراسة ضمن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 ، مجلة الإجتهاد القضائي، عدد16.
شرف الدين و، هنية إ، (2018)، الحماية الإجرائية للمستهلك من جريمة الاستخدام غير المشروع لأدوات الدفع الإلكترونية وفقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، مجلة المنار للبحوث والدراسات القانونية والسياسية، عدد4.
الشكري ع، (2008) الجريمة المعلوماتية وأزمة الشريعة الجزائية، مركز دراسات الكوفة، العراق.
شهاب أ، (2018)، شروط قبول الأدلة الإلكترونية أمام االقضاء المصري، مجلة الإجتهاد للدراسات القانونية والإقتصادية، مجلد7، عدد2.
عبد الباقي م، (2018)، التحقيق في الجرائم الإلكترونية وإثباتها في فلسطين: دراسة مقارنة، دراسات علوم الشريعة والقانون، الجامعة الأردنية، الأردن، المجلد 45، العدد 4.

العلماء م، (2005)، جرائم الإنترنت والاحتساب عليها، مؤتمر القانون والكمبيوتر والإنترنت، مجلة كلية الحقوق والشريعة، جامعة الإمارات.
غيث م، (2014)، أساليب ومهارات التحقيق في الجرائم الإلكترونية، جامعة فلسطين الأهلية، بيت لحم، فلسطين.
فتيح ر، عواد ي، (2017)، إثبات الجريمة الإلكترونية بالدليل العلمي، مجلة جامعة تكريت للحقوق، العراق، مجلد 1، عدد 3.
فريجة ح، (2011)، الجرائم الإلكترونية والإنترنت، مجلة المعلوماتية، العدد 36، السعودية.
قرون ن وبوضياف ج ولعيفة ر، (2020)، تكنولوجيا المعلومات والإتصال كركيزة أساسية لعملية التدريب الإلكتروني، مجلة التعليم عن بعد، جامعة بني سويف اتحاد الجامعات العربية، مجلد 8، عدد15.
مجمع البحوث والدراسات، (2016)، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، أكاديمية السلطان قابوس لعلوم الشرطة، جامعة نزوى، سلطنة عمان.
محمد الأمين البشري، (2000)، التحقيق في جرائم الحاسب الآلي، المجلة العربية للدراسات الأمنية، مجلد15، عدد30.
المطيري س، (2023)، مفهوم الجرائم الإلكترونية وسماتها، المجلة القانونية، العدد 5، المجلد 16.
نصيف ص، (2016)، التحديات الإجرائية المتصلة بالجرائم المعلوماتية، مجلة العلوم القانونية والسياسية، مجلد5، عدد2.
الهاجري ن، (2023)، جرائم تقنية المعلومات في التشريع الأمريكي مقارنة بالتشريعات العربية، مجلة البحوث القانونية والاقتصادية، المنصورة، العدد 83.
هلالي ع، (2009)، المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست، مجلة الحقوق، جامعة البحرين، المجلد 6، العدد13.

4- الرسائل الجامعية

أبو داسر ع، (2022-2021)، إثبات الدعوى الجنائية، أطروحة دكتوراة، جامعة الإمام محمد بن سعود الإسلامية.
بخي أ، (2014)، إجراءات التحقيق في الجرائم الإلكترونية، رسالة ماجستير، كلية الحقوق، جامعة المسيلة، الجزائر.
البدراوي أ، (2011)، التعاون الدولي في مجال مكافحة الجريمة المنظمة، أطروحة دكتوراة، كلية الحقوق، جامعة أسيوط.

بعقيبي ع، (2018)، مكافحة الجريمة المعلوماتية في التشريعين الجزائري والإماراتي–دراسة مقارنة–، أطروحة دكتوراه، كلية الحقوق، جامعة محمد خيضر، بسكرة، الجزائر.

حاتم أحمد محمد بطيخ ح، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات دراسة تحليلية مقارنة.

حمودة ع، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، كلية الحقوق، جامعة حلوان.

الدعجه أ، (2014)، استيراتيجيه مكافحه الجرائم المعلوماتيه، رسالة ماجستير، معهد البحوث والدراسات الاستيراتيجيه، جامعه ام درمان الاسلامية، السودان.

دويكات ق، (2018)، حجية محاضر الاستدلال في الإثبات الجنائي، رسالة ماجستير، جامعة النجاح الوطنية، نابلس، فلسطين.

الشايب ن، (2023) التفتيش في الجرائم الإلكترونية، دراسة تحليلية مقارنة، رسالة ماجستير، جامعة النجاح الوطنية، نابلس، فلسطين.

العفيفي ي، (2013)، الجرائم الإلكترونية في التشريع الفلسطيني (دراسة تحليلية مقارنة)، رسالة ماجستير، كلية الشريعة والقانون، الجامعة الإسلامية، غزة، فلسطين.

القحطاني ع، (2014)، تطوير مهارات التحقيق الإلكتروني في مواجهة الجرائم المعلوماتية دراسة تطبيقية في هيئة التحقيق والإدعاء العام في مدينة الرياض، رسالة ماجستير، الرياض، السعودية.

ميرغني ف، (2017) ، اجراءات التحري والضبط في الجريمة الإلكترونية، رسالة دكتوراه، جامعة شندى، السودان.

5– المؤتمرات

البداينة ذ، (2–2014/9/4)، الجرائم الإلكترونية: المفهوم والأسباب، الملتقى العلمي حول: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، عمان، الأردن.

زيدات ح، (2016/4/17)، حدود قانون العقوبات في السيطرة على السرقة الإلكترونية "اختلاس المعلومات والبيانات الالكتروني" في ضوء التشريعات الوطنية والدولية، المؤتمر الدولي لكافحه الجرائم الالكترونية في فلسطين، كلية الحقوق، جامعة النجاح الوطنية، فلسطين.

مختارية ب، (29/مارس/2017)، ماهية الجريمة الإلكترونية، الملتقى الوطني حول آليات مكافحة الجريمة الإلكترونية، الجزائر.

مركز البحوث والدراسات، الإمارات العربية المتحدة ،(22–28\ نيسان\ 2003،)، للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية الشرطة، دبي.

6- المواقع الإلكترونية:

https://www.unodc.org/pdf/Manual_ComputerRelatedCrime.PDF,

international review of criminal policy, nos 43 and 44, united nations manual on the prevention and control of computer related crime, united nations, new York, 1994. See the following link:

إحصائية الشرطة الفلسطينية لعام 2022، على الرابط التالي: https://www.palpolice.ps/annual-statistics، الصادر بتاريخ 2023/8/12.

مدار، كيف تعمل وحدة مكافحة الجرائم الالكترونية الفلسطينية؟، مقابلة مع رئيسة نيابة الجرائم الإلكترونية، تاريخ النشر: 2017\1\20، https://madar.news.

المنظمة العالمية للملكية الفكرية (WIPO): https://www.wipo.int/portal/ar/.

الموقع الرسمي للإتحاد الإفريقي: https://au.int/en/overview

- الموقع الرسمي لليوروبول: http://www.europol.eurpa.eu.

الموقع الرسمي لنيابة مكافحة الجرائم المعلوماتية:

https://safeonline.najah.edu/ar/about/partners/the_public_prosecution/#gsc.tab=0.

الموقع الرسمي مكتب الأمم المتحدة المعني بالمخدرات والجريمة،

https://www.unodc.org/e4j/ar/cybercrime/module-1/key-issues/cybercrime-trends.html.

file:///C:/Users/user/Downloads/JDL_Volume%207_Issue%201_Pages%201-143.pdf

7- مراجع باللغة الأجنبية:

Finckenauer, J.O. "Problems of definition: What is organized crime?", First edition, By Routledge, USA, NewYork, 2005, P:34

Combating Cyber Crime (A study in light of Palestinian legislation and international agreements)

Mohammad Basem brahim Alkhaldi

Dr. Ala Khalayleh
Dr. Ahmad Alshqar
Dr. Mahmoud Alsheikh

Abstract

The thesis addresses the alignment of Palestinian criminal legislation with international conventions on combating cybercrime. The significance of this topic arises from the increasing use of the internet and the growing number of users, making cyberspace a suitable environment for planning and committing various crimes, later termed as cybercrimes.

In response, the Palestinian legislator enacted Decree-Law No. (10) of 2018 on Cybercrimes, establishing it as a specialized legal framework for combating cybercrime and curbing its proliferation. This legislation aims to effectively classify cybercrimes, ensure the protection of violated rights, and harmonize with relevant international legal frameworks; Accordingly, the thesis examines the concept of cybercrime, its characteristics, and related legal notions. It further explores the legal framework governing cybercrime, taking into account the procedural challenges posed by such offenses from both legal and practical perspectives. The study also delves into the legal measures adopted to combat cybercrime at the international, regional, and national levels, with a particular focus on the evidentiary aspects of cybercrime prosecution.

Keywords: Alignment, Cybercrime, International Conventions, Criminal Legislation, Electronic Evidence.