

خطورة الجرائم الإلكترونية على الأمن القومي

The threat of cybercrime to national security

وردية طاشت

Ourdia Tachet

جامعة الجزائر 1 الجزائر

University of Algiers 1, Algeria

مخبر العلوم الجنائية

Criminal Sciences Research Laboratory

ourdiatachet@gmail.com

تاريخ النشر: 2026/05/31

فرحة أبوبكر المهدي *

Farha Aboubakar Elmahdi

جامعة الجزائر 1 الجزائر

University of Algiers 1, Algeria

مخبر العلوم الجنائية

Criminal Sciences Research Laboratory

ferha.elmahdi@univ-alger.dz

تاريخ الاستلام: 2025/11/15

تاريخ القبول للنشر: 2025/12/10

ملخص:

تشكل الجرائم الإلكترونية تهديداً متصاعداً للأمن القومي، لما تتميز به من طابع عابر للحدود وصعوبة في التتبع والإثبات. تعتمد هذه الجرائم على تقنيات رقمية متقدمة لاختراق الأنظمة وسرقة أو تخريب البيانات، مما ينعكس سلباً على الاستقرار السياسي والاقتصادي والاجتماعي. وعلى الرغم من الإيجابيات التي توفرها الإنترنت ومواقع التواصل، إلا أنها أصبحت بيئة خصبة لهذه الأنشطة الإجرامية. ويقام ضعف التنسيق الدولي وغياب تشريعات موحدة من صعوبة التصدي لها، ما دفع بعض الدول، مثل ليبيا ومصر، إلى إصدار قوانين خاصة لمواجهتها. الكلمات المفتاحية: الجرائم الإلكترونية؛ الأمن القومي؛ الجرائم المعلوماتية؛ الشرعية الجنائية.

Abstract:

Cybercrimes represent an escalating threat to national security due to their cross-border nature and the difficulty of tracking and proving them. These crimes rely on advanced digital technologies to infiltrate systems, steal or sabotage data, and thereby undermine political, economic, and social stability.

Despite the many benefits offered by the internet and social media platforms, they have become fertile ground for such criminal activities. The lack of international coordination and unified legislation further complicates efforts to combat them, prompting some countries, such as Libya and Egypt, to enact specific laws to address this growing challenge.

Keywords: Cybercrimes; National Security; Information Crimes; Criminal Legitimacy.

* المؤلف المراسل

مقدمة:

تُعَدّ الجرائم الإلكترونية، أو جرائم الحاسوب، من جرائم المعلومات المعاصرة والعابرة للحدود الوطنية التي ظهرت مؤخرًا مع انتشار التكنولوجيا، لا سيما لارتباطها الوثيق بالحوسبة. والأداة الرئيسية لهذه الجرائم هي الإنترنت. وي طرح هذا النوع من الجرائم تحديات عديدة، لا سيما فيما يتعلق بالكشف والإثبات. بل إنه يتميز بمكر وخداع مرتكبيه، الذين يستخدمون تقنيات معلوماتية متطورة للغاية. تتيح لهم هذه التقنيات اختراق الشبكات وأجهزة الحاسوب المتصلة بالإنترنت، وتجاوز أنظمة الأمان، والوصول إلى الأجهزة للكشف عن محتوياتها، أو إتلافها، أو تغيير المعلومات المخزنة عليها.

ونظرًا لخطورة هذه الجريمة وصعوبة اكتشافها وعدم وجود أدلة مادية لإدانة مرتكبها فقد أصبحت منتشرة بشكل كبير في العالم الإجرامي نتيجة لغياب استراتيجية فعالة لمكافحتها والحد منها وخاصة على المستوى الدولي نظرًا لندرة الاتفاقيات الدولية وصعوبة التعاون الدولي للحد منها وهذا بطبيعة الحال نظرًا لطبيعتها الخاصة.

أصبح الاستخدام الواسع لشبكات التواصل الاجتماعي، مثل فيسبوك وتويتر، جزءًا أساسيًا من حياتنا، وأداة فعالة لتطوير وتحسين استراتيجيات المؤسسات العامة والخاصة، وكذلك الأفراد، وتمكينهم من التقدم. وكانت الدول المتقدمة من أوائل الدول التي استفادت من هذه المنصات وواكبتها، وأصبح من الصعب الاستغناء عنها.

رغم المزايا التي توفرها هذه البرامج والشبكات الإلكترونية، إلا أنها أدت أيضًا إلى ظهور أنواع جديدة من الجرائم، وهي الجرائم الإلكترونية، التي تهدد جميع المجتمعات البشرية بتسببها في أزمات سياسية واقتصادية واجتماعية، وثقافية، وأمنية. ينتشر القراصنة في كل مكان؛ إذ يخترقون أجهزة الكمبيوتر والهواتف الذكية لسرقة المعلومات، وابتزاز الأفراد والمؤسسات أو تشويه سمعتهم، بالإضافة إلى سرقة الحسابات المصرفية واستغلال الثغرات الأمنية لتجنيد الشباب والشبان، وحتى الأطفال، للقيام بأعمال تخريبية.

تُعَدّ الجرائم الإلكترونية من الجرائم الحديثة التي ظهرت مع ظهور أنظمة المعلومات. وتُعَدّ هذه الظاهرة نتيجة طبيعية لتطور الحياة بشكل عام، فكلما تطور المجتمع تكنولوجياً، ظهرت أشكال جديدة من الجرائم.

بُذلت جهود دولية لمكافحة الجرائم الإلكترونية، لا سيما من خلال اتفاقيات ومؤتمرات تشجع الدول على تجريم هذه الجرائم. ونتيجةً لذلك، سارعت العديد من دول العالم، بما فيها عدة دول

عربية، إلى سنّ قوانين لمكافحة الجرائم الإلكترونية، مُحاكياً بذلك التوجه السائد في دول أخرى تشهد موجةً من التطور والتقدم. فعلى سبيل المثال، أصدر البرلمان الليبي القانون بشأن مكافحة الجرائم الإلكترونية، وهو من أحدث القوانين في هذا المجال. وبالمثل، أصدر البرلمان المصري القانون رقم 175 لسنة 2018.

أهمية الدراسة:

تكمن أهمية هذا البحث في النقاط التالية:

- تسليط الضوء على القانون رقم 5 لسنة 2022 بشأن الجرائم الإلكترونية، وتحديدًا أحكامه، نظرًا لحداثته النسبية مقارنةً بالتشريعات الأخرى.
- إبراز خطورة الجرائم الإلكترونية وما تُشكله من مخاطر جسيمة على الأمن والنظام في ليبيا والدول العربية الأخرى.
- تحديد المعوقات التي قد تُعيق فعالية التشريعات العربية في مكافحة الجرائم الإلكترونية.
- ندرة الدراسات والبحوث العربية حول الجرائم الإلكترونية وفعالية التدابير المُتخذة لمكافحتها.

أهداف الدراسة:

يهدف هذا البحث إلى تقييم فعالية القوانين والتشريعات العربية في مكافحة الجرائم الإلكترونية، بالإضافة إلى تحليل الطبيعة القانونية والعناصر المكونة للجرائم الإلكترونية، والجوانب الإجرائية لمعالجتها، بدءًا من ارتكابها وحتى مرحلتي التحقيق والمحاكمة.

إشكاليات الدراسة

- سارعت العديد من الدول العربية إلى اعتماد تشريعات خاصة لمكافحة الجرائم الإلكترونية، استكمالاً للاتفاقيات الدولية الهادفة إلى تعزيز التعاون الدولي والإقليمي للحد من مخاطر هذه الجرائم والحفاظ على أمن الدول العربية. لذا، يمكن صياغة سؤال البحث على النحو التالي:
- ما مدى فعالية القوانين والتشريعات العربية في مكافحة الجرائم الإلكترونية؟
- ينبثق من هذا السؤال الرئيسي الأسئلة الفرعية التالية:
- ما خصائص الجريمة الإلكترونية في التشريعات العربية؟
- ما آليات مكافحة الجريمة الإلكترونية التي توفرها التشريعات العربية؟

منهجية الدراسة:

اعتمد الباحث المنهج التحليلي لتحليل ومناقشة نصوص وأقوال الخبراء القانونيين، ثم مقارنتها لتحديد مواطن الضعف ومعالجتها أو إبراز مواطن القوة. ولدعم الدراسة وتقويتها، اعتمد الباحث

المنهج المقارن مع القوانين العربية المتعلقة بمكافحة الجرائم الإلكترونية، وخاصة القانون المصري رقم 175 لسنة 2018 بشأن الجرائم الإلكترونية.

المبحث الأول:

ماهية الجرائم الإلكترونية

يُعدّ التعريف بموضوع البحث من الركائز الأساسية في أي دراسة علمية، إذ يُبرز هذا التعريف أهمية الموضوع ويُمدّد لفهم أبعاده المختلفة، كما يُعدّ مدخلاً ضرورياً لتحديد محاور الدراسة وزوايا تناولها. ونظراً لهذه الأهمية البالغة، لم يحظ أي موضوع بتعريف موحد بين الفقهاء والمفكرين، وذلك نتيجة لاختلاف وجهات النظر وتباين الزوايا التي يعتمدها كل باحث كمنطلق لتعريفه. ويمكن تمييز اتجاهين رئيسيين في هذا السياق: أحدهما يركّز على الجانب الشكلي أو البنيوي للموضوع، بينما ينصرف الآخر إلى البعد الموضوعي أو الوظيفي.

وفي هذا الإطار، يبرز تساؤل جوهري لدى الكثيرين: ما المقصود بالجرائم الإلكترونية؟ ولماذا تُوصف بأنها "جرائم"؟ ما هي صورها المختلفة؟ وما الدوافع الكامنة وراء ارتكابها؟
تعريف القانون: "الجريمة هي كل فعل يعود بالضرر على المجتمع ويقرر له القانون عقوبة جنائية"

تعريف علم الاجتماع: "الجريمة هي نوع من الخروج على قواعد السلوك التي تهدد المجتمع، وهي مسألة اعتبارية محضة يرجع في تقديرها إلى المجتمع الذي له السلطة العليا في التمييز بين أنواع السلوك، وفي الحث على الالتزام ببعض أنواعها، وفي تحريم أنواع أخرى فيها خروج عن النظم التي وضعها وانحراف عن الطرق التي شرعها إذ هو يرى فيها تهديداً لكيانه"¹
ولا يوجد إجماع على تعريف الجريمة الإلكترونية من حيث كيف تُعرف أو ما هي الجرائم التي تتضمنها الجريمة الإلكترونية.

ويقول فان دير هيلست وونيف "هناك غياب لتعريف عام وإطار نظري متسق في هذا الحقل من الجريمة وفي أغلب الأحيان تستخدم مصطلحات الافتراضية والحاسوب والإلكترونية والرقمية".

يتفاوت تعريف الجريمة الإلكترونية بين من يراها جرائم تُرتكب عبر الحاسوب تحديداً، وبين من يوسّع نطاقها لتشمل كل الأفعال غير المشروعة التي تُرتكب باستخدام أي نوع من الأجهزة الرقمية. ويمكن تلخيص مفهوم الجريمة الإلكترونية بأنها تلك الأفعال الإجرامية التي تُنفَّذ بواسطة

الحاسوب أو الشبكات أو الوسائل التقنية المختلفة، مثل الهواتف الذكية وغيرها من المعدات الرقمية².

وسوف نتناول هذا المبحث في المطالب الآتية: -

المطلب الأول: تعريف الجريمة الإلكترونية

قبل الخوض في موضوع الجريمة الإلكترونية، من الضروري أولاً التعرف على مفهوم شبكة الإنترنت، باعتبارها البيئة الحاضنة لهذا النوع من الجرائم. يُشتق مصطلح "الإنترنت" من كلمتين إنجليزيتين هما: *International* و *Network*، ويقصد به شبكة الاتصالات الدولية التي تربط بين الحواسيب والمعدات الرقمية حول العالم، مما يتيح تبادل المعلومات والبيانات بسرعة وفعالية غير مسبوقة³.

ولعل من أهم التعريفات التي قيلت في شأن الإنترنت ما يلي:

تُعدّ شبكة الإنترنت منظومة ضخمة من أجهزة الحاسوب المترابطة عبر خطوط الاتصال العالمية، وتشكل ما يُعرف بـ "شبكة الشبكات" نظراً لاحتوائها على عدد هائل من الشبكات المتزايدة في مختلف أنحاء العالم. فالإنترنت في جوهره هو تجمع عالمي لشبكات الحواسيب والأجهزة الرقمية المنتشرة في الدول كافة، والتي تتواصل فيما بينها من خلال أنظمة الاتصالات الإلكترونية المخصصة لنقل البيانات والمعلومات. ويمكن لأي فرد يمتلك جهاز حاسوب، وخطاً هاتفياً، واشتراكاً لدى أحد مزودي خدمة الإنترنت، أن يصل إلى هذه الشبكة العالمية ويستفيد من خدماتها المتعددة⁴.

يُنظر إلى الإنترنت على أنه تطور متقدم في استخدام الحاسوب، قائم على الربط الدولي عبر شبكات الاتصالات، ويتطلب توفر تقنيات خاصة لضمان فعاليته. فهو يشكل شبكة عالمية ضخمة تتألف من عدد هائل من شبكات الحواسيب المنتشرة في مختلف أنحاء العالم، والمتصلة فيما بينها بواسطة خطوط الهاتف أو الأقمار الصناعية. وتتم عملية تبادل المعلومات بين المستخدمين من خلال بروتوكول موحد يُعرف باسم "بروتوكول نقل الإنترنت. (Internet Protocol)"⁵ وفي هذا السياق، تجدر الإشارة إلى أن للإنترنت استخدامات متعددة، من أبرزها:

تُوفّر شبكة الإنترنت مجموعة واسعة من الخدمات التي أحدثت نقلة نوعية في التواصل وتبادل المعلومات، ومن أبرز هذه الخدمات:

البريد الإلكتروني: يتيح إرسال واستقبال الرسائل النصية بسرعة فائقة لا تتجاوز بضع ثوانٍ، مما يجعله وسيلة فعالة للتواصل المهني والشخصي.

المحادثات الشخصية: تُمكن المستخدم من التواصل المباشر مع طرف واحد أو عدة أطراف عبر الصوت والصورة والنص، مما يعزز التفاعل الفوري.

خدمة نقل الملفات: تسمح بنقل البيانات والمعلومات الرقمية، بغض النظر عن حجمها، بين المستخدمين أو الأجهزة المختلفة.

الأرشفة الإلكترونية: يُمكن من خلاله إنشاء وتخزين المعلومات والوثائق بطريقة منظمة، مع إمكانية الرجوع إليها في أي وقت بسرعة وسهولة.

خدمة البحث: تُعد من أهم وظائف الإنترنت، حيث تتيح الوصول إلى المعلومات، البرامج، المواقع الإلكترونية، المنتجات، وسائل الترفيه، الإعلانات الوظيفية، وغيرها من الموارد التي يحتاجها الإنسان في حياته اليومية.

لم يضع المشرع تعريفاً دقيقاً ومحددًا للجريمة الإلكترونية، ولا يزال الجدل قائماً حول ماهيتها وحدودها، إلا أنه يمكن النظر إليها بوصفها سلوكيات غير مشروعة يرتكبها فرد أو مجموعة أفراد باستخدام الأجهزة الذكية أو المنصات الإلكترونية، بهدف تحقيق مكاسب مادية أو معنوية. وغالباً ما تتجسد هذه السلوكيات في صور من الابتزاز، والتهديد، وتشويه صورة الضحية أمام المجتمع الواقعي والافتراضي.⁶

أما من منظور المجتمع الدولي، فقد تم توصيف الجريمة الإلكترونية بأنها مجموعة من الأفعال والممارسات المرتبطة باستخدام الحاسوب، تهدف إلى تحقيق منافع شخصية أو مالية، أو إلحاق الضرر بالآخرين أو بالمؤسسات.⁷

لغويًا، تُشتق كلمة "جريمة" من الفعل "جَزَمَ" على وزن "فَعَلَ"، والذي يدل على الذنب واكتساب الإثم. أما اصطلاحاً، فالجريمة تُعرّف بأنها ارتكاب فعل محترّم نهى عنه الشارع، أو الامتناع عن أداء فعل مأمور به، ولا يُعدّ الفعل أو الترك جريمة إلا إذا رُصدت له عقوبة قانونية محددة.⁸

ما يهمننا في هذا البحث هو الوقوف على مفهوم الجريمة المرتبطة بشبكة الإنترنت العالمية، والتي تُعرف بتسميات متعددة مثل: الجريمة المعلوماتية، الجريمة الإلكترونية، جريمة الإنترنت، أو جريمة الحاسب الآلي. وتُرتكب هذه الجرائم من خلال استغلال الفضاء الرقمي كوسيلة أو بيئة لتنفيذ أفعال غير مشروعة.

وفي هذا السياق، يمكن الاستعانة بعدد من التعريفات التي تسهم في توضيح أبعاد هذه الظاهرة، من أبرزها:

أنها تشمل جميع أنماط السلوك غير القانوني أو الضار بالمتجمع، والتي تُرتكب باستخدام الحاسوب أو أي وسيلة رقمية، وتشمل كل فعل إجرامي متعمد يرتبط بشبكة المعلومات، ويترتب عليه إلحاق ضرر بالمجني عليه أو تحقيق منفعة غير مشروعة للمجاني⁹.

كما تُعرّف بأنها سلوك احتيالي، أو خداعي، أو تخريبي أو تخريضي، يتم عبر استخدام الحاسوب المتصل بالإنترنت، ويهدف مرتكبه إلى تحقيق مصلحة مادية أو شخصية، أو إلحاق الأذى بالغير بطرق غير قانونية¹⁰.

أما بالنسبة لخبراء "المنظمة الأوروبية للتعاون والتنمية الاقتصادية" فإن المقصود بالجريمة المعلوماتية كل سلوك غير مشروع أو مناف للأخلاق أو غير مسموح به يرتبط بالمعالجة الآلية للبيانات أو بنقلها أو تحويلها¹¹.

وعرفت وزارة العدل في الولايات المتحدة الأمريكية "التي عرفت الجريمة عبر الإنترنت بأنها "أي جريمة لفاعلها معرفة فنية بتقنية الحاسبات تمكنه من ارتكابها"¹²

أما منظمة التعاون الاقتصادي للجريمة المرتكبة عبر الإنترنت "هي كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به، يتعلق بمعالجة آلية للبيانات ونقلها"

ويعرفها قانون مكافحة الجريمة المعلوماتية السعودي "بأنها أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية المخالفة لأحكام هذا النظام"¹³

حسب اللجنة الأوروبية فإن مصطلح الجريمة الإلكترونية" يضم كل المظاهر التقليدية للجريمة مثل الغش وتزييف المعلومات، ونشر مواد إلكترونية ذات محتوى مخل بالأخلاق أو دعوى لفتن طائفية"¹⁴

يتفق الفقهاء على أن الغش المعلوماتي يُعدّ مظلة واسعة تشمل طيفاً من الأفعال غير المشروعة، التي تستغل ما يُنتجه الحاسوب من بيانات ومعلومات بهدف ارتكاب جرائم رقمية. وتنوّع صور هذا الغش لتشمل إدخال بيانات أو ملفات مزوّرة، أو إتلاف البرامج والمعلومات المثبتة، أو الاستيلاء على الخدمات والأموال والمنافع الرقمية الأخرى، فضلاً عن استخدام الوسائط الإلكترونية لبث الإشاعات ضد الأفراد، أو المؤسسات، أو الدول، أو التحريض على الانحلال الأخلاقي ونشر المحتوى الذي يُخلّ بالآداب العامة.

وتعرف بانها "الاعتداء غير القانوني الذي يرتكب بواسطة المعلومات الحاسوبية بغرض تحقيق الربح¹⁵ كما عرفت بأنها" كل فعل إجرامي متعمد أياً كانت صلته بالمعلومات ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل "¹⁶

وعرفت أيضا بأنها "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابها من ناحية، وملاحقته وتحقيقه من ناحية أخرى"¹⁷. كما عرفت بانها: "جرائم الشبكة العالمية التي يستخدم الحاسب وشبكاته العالمية كوسيلة مساعدة لارتكاب جريمة مثل استخدامه في النصب والاحتيال وغسل الأموال وتشويه السمعة والسب"¹⁸.

او هي "كل جريمة تتم في محيط أجهزة الكمبيوتر" أو هي "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها"¹⁹. "كل نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"²⁰.

إن النمو المتزايد والانتشار المتسارع للجرائم الإلكترونية التي ترتكب من خلال شبكة الإنترنت هو الذي قاد رغبة الخبراء والمختصين إلى تحديد تصنيفاتها الداخلية على النحو التالي:-

الفرع الأول: جرائم التحريف والتزوير

تتمثل خلاصة الجرائم الإلكترونية في الاعتداء على المعلومات المخزنة داخل ذاكرة الحاسوب، سواء بسرقتها أو تحريفها أو التلاعب بمحتواها. كما تشمل هذه الجرائم اعتراض البيانات أثناء انتقالها عبر شبكة الإنترنت، مما يُعد انتهاكاً لسرية المعلومات. ومن أبرز أساليب التخريب أيضاً، استخدام برامج خبيثة تستهدف أنظمة المعلومات بهدف تدميرها أو التعديل على برامج أخرى، وهي الممارسات التي تُعرف اليوم باسم "القرصنة المعلوماتية".²¹

الفرع الثاني: جرائم الاختلاس والسرقة

تتجسد صورة هذه الجرائم في قيام الجاني باستخدام الحاسوب للولوج إلى شبكة الإنترنت بهدف الوصول غير المشروع إلى الأنظمة الرقمية للبنوك والمصارف والمؤسسات المالية. ويُنفذ هذا الاعتداء من خلال إدخال بيانات مزيفة، أو التلاعب بالبيانات الأصلية عبر تعديلها أو حذفها، وذلك بقصد اختلاس الأموال، أو تحويلها إلى حسابات أخرى، أو إتلافها، مما يُشكل انتهاكاً صارخاً لسلامة المعلومات المالية وحقوق أصحابها.²²

الفرع الثالث: الجرائم الجنسية والممارسات الإباحية

يشهد العالم المعاصر موجة جارفة من الانفلات الجنسي تجاوزت الحدود الأخلاقية والثقافية، ما جعل هذه الظاهرة تُطرح بوصفها من أخطر التحديات التي تهدد الكيان الإنساني والمجتمعات على حد سواء. وقد عبّر المفكر "جيمس رستون" في مجلة نيويورك تايمز عن هذا القلق

بقوله: "إن خطر الطاقة الجنسية قد يفوق في نهاية المطاف خطر الطاقة الذرية"²³، في إشارة إلى التأثير العميق للمحتوى الجنسي على البنية الاجتماعية العالمية.

وتُعدّ المواقع الإلكترونية ذات الطابع الإباحي من أبرز مظاهر هذه الظاهرة، لما لها من دور في تعزيز مظاهر الانحلال الأخلاقي، لا سيما بين فئة الشباب، والمساهمة في ارتفاع معدلات الجرائم ذات الطابع الجنسي. وتشير التقديرات إلى أن الصفحات الإباحية تمثل نحو 3.2% من إجمالي محتوى شبكة الإنترنت²⁴، ويُسجّل أن بعض هذه الصفحات تستقطب ما يقارب 280 ألف زائر يوميًا، في حين يُقدّر أن 20% من سكان الولايات المتحدة الأمريكية يترددون بانتظام على هذه المواقع. وقد بلغت قيمة المشتريات المتعلقة بالمواد الجنسية المعروضة عبر الإنترنت في عام 1999 نحو 18 مليار دولار أمريكي²⁵. ولا تقتصر هذه الظاهرة على المواقع الإباحية فحسب، بل تشمل أيضًا توزيع الصور الفاضحة عبر البريد الإلكتروني، فضلًا عن المنصات التي تروج للفسق والفجور والسياحة الجنسية. وتجدر الإشارة إلى أن هذه الأفعال، وإن لم تُشكّل جريمة دعارة بالمعنى التقليدي، فإنها تسهم بوضوح في نشر الفساد الأخلاقي وتشويه وعي الشباب.

الفرع الرابع: جرائم القذف والتشهير

تتخذ الجرائم الإلكترونية صورًا متعددة، من أبرزها استخدام شبكة الإنترنت كوسيلة للتشهير بالأفراد، وانتهاك خصوصيتهم من خلال نشر أخبارهم الشخصية والدعاية الكاذبة بحقهم. وقد يتطور الأمر إلى التسلل غير المشروع إلى مواقع خاصة بشخصيات عامة أو مؤسسات حساسة، وسرقة الصور والمعلومات الخاصة بهم، ثم نشرها بطريقة تسيء إلى سمعتهم وتلحق بهم الضرر²⁶.

ولا يقتصر هذا النوع من الجرائم على الأفراد فحسب، بل يمتد ليطال الدول والشركات والمؤسسات، من خلال نشر بيانات ومعلومات تسيء إلى صورتها العامة، سواء عبر كشف سلبياتها أو إفشاء أسرارها التنظيمية دون إذن مسبق، وقد يصل ذلك إلى حد الابتزاز والتشهير والقذف بأسلوب متهور وغير مسؤول.

ومن هنا، يمكن القول إن الجريمة الإلكترونية هي كل فعل غير قانوني يُرتكب باستخدام الحاسوب وشبكة الإنترنت، من قبل أشخاص يمتلكون معرفة تقنية تؤهلهم لاستغلال هذه الوسائل في تنفيذ أفعال ضارة. وهي تُعد امتدادًا لما يُعرف بجرائم الحاسوب، والتي يُقصد بها كل سلوك إجرامي يُستخدم فيه الحاسوب كأداة رئيسية، سواء كان هو الهدف المباشر للجريمة أو الوسيلة لتنفيذها.²⁷

يتفق الباحث مع التعريف الذي يرى أن الجريمة الإلكترونية هي مجموعة من الممارسات التي تُوجّه ضد فرد أو جماعة بدافع إجرامي، بهدف الإضرار المتعمد بسمعة الضحية، أو إلحاق الأذى النفسي أو الجسدي بها، سواء تم ذلك بشكل مباشر أو غير مباشر، عبر استخدام وسائل الاتصال الحديثة مثل الإنترنت، والبريد الإلكتروني، وغرف المحادثة، والهواتف المحمولة.²⁸

المطلب الثاني: خصائص الجرائم الإلكترونية

تتميز الجرائم الإلكترونية²⁹ بعدد من الخصائص تميزها عن غيرها من الجرائم التقليدية هي:

1- ترتكب بواسطة شبكة الإنترنت: "أي تستخدم شبكة الإنترنت كأداة لارتكاب الجريمة أو تسهيل ارتكابها؛ إذ تعد شبكة الإنترنت حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم كالبنوك والشركات بكافة أنواعها والأشخاص وغيرها، والتي غالباً ما تكون الضحية"³⁰.

2- مرتكب الجريمة مجرم ذو خبرة في استخدام الحاسب الآلي والإنترنت.

3- الجرائم الإلكترونية لا تعرف الحدود المكانية ولا الحدود الزمنية

4- الجرائم الإلكترونية تنسم بالخطورة البالغة: وذلك من عدة نواح فمن ناحية:

الحسائر الناجمة عنها كبيرة جداً قياساً بالجرائم التقليدية وبصفة خاصة جرائم الأموال، ومن ناحية ثانية: نجدها ترتكب من فئات إجرامية متعددة تجعل من الصعب معرفة الفاعل، ومن ناحية أخيرة: تنطوي على سلوكيات غير مألوفة".

5- صعوبة التحري والتحقيق في هذه الجرائم ومن ثم محاكمة مرتكبيها:

هناك صعوبة في ملاحقة مرتكب هذه الجرائم، ولو تم التوصل إليه فمن السهل اتلاف الأدلة من قبل الجناة، كما أن هذه الجرائم لا تحدها حدود، فهي جرائم عابرة للحدود مما يثير تحديات ومعوقات في حقل الاختصاص القضائي والقانون الواجب التطبيق ومتطلبات التحقيق والملاحقة والضبط والتفتيش".

6- يتميز الدافع وراء ارتكاب الجرائم الإلكترونية عن ذلك المرتبط بالجرائم التقليدية، إذ غالباً ما يكون مدفوعاً بعوامل غير نمطية. فبعض الأفراد، لا سيما القراصنة، يُقدمون على هذه الأفعال بدافع الفضول المعرفي أو الرغبة في الوصول إلى معلومات جديدة. بينما يسعى آخرون إلى الاستيلاء على البيانات المخزنة في أجهزة الحاسوب، أو حذفها، أو تدميرها، أو إلغائها بشكل نهائي. وقد يكون الحافز أيضاً محاولة اختراق الأنظمة الإلكترونية بهدف إثبات التفوق التقني أو تحقيق شهرة شخصية، وهي ظاهرة شائعة بين فئة الشباب. كما قد تُرتكب هذه الجرائم بدافع استهداف أفراد أو جهات معينة، لأغراض انتقامية أو تخريبية.³¹

ومن خصائص الجرائم الإلكترونية أيضا

- تُعدّ الجرائم الإلكترونية نمطًا حديثًا ومستحدثًا ضمن أنماط السلوك الإجرامي، وتمتاز بخصوصية تميزها عن الجرائم التقليدية، إذ تنصبّ اعتدائها بشكل رئيسي على المعلومات والبيانات الرقمية، مما يمنحها طابعًا تقنيًا فريدًا يتطلب أدوات ومعالجات قانونية متخصصة.
- الجرائم التي ترتكب بأداة الكمبيوتر، وتكون عن طريق شبكة الإنترنت، بواسطة شخص على دراية بها.
- هي جزء من العمل الإلكتروني الرقمي الذي يقوم به المجرم بالتقنية الإلكترونية الرقمية، وشبكة الإنترنت لتحقيق غرض إجرامي محدد³²
- تُعدّ الجرائم الإلكترونية من الجرائم العابرة للحدود، إذ لا تخضع لقيود جغرافية أو سيادة وطنية محددة. فبيئة الإنترنت، القائمة على الانتشار العالمي لشبكات الاتصالات، أفرزت نمطًا من الإجرام يتجاوز الحدود التقليدية للدول، مما جعل هذه الجرائم تُصنّف ضمن فئة الجرائم العابرة للأوطان³³.
- تُعاني الجرائم الإلكترونية من غموض في طبيعتها وصعوبة في إثباتها، الأمر الذي يدفع العديد من الضحايا إلى التردد في الإبلاغ عنها. ويرجع ذلك إلى تعقيد وسائل ارتكابها وافتقارها غالبًا إلى الأدلة المادية المباشرة، على خلاف الجرائم التقليدية التي تترك آثارًا ملموسة تُسهّل عملية تتبع الجناة. كما أن تنوع الجرائم الإلكترونية واتساع نطاقها يجعل من الصعب حصرها أو كشفها بسهولة، مما يُشكل تحديًا كبيرًا أمام الجهات المختصة في ملاحقة مرتكبيها³⁴.
- إن الخسارة الاقتصادية التي تسببها الجرائم الإلكترونية عادة ما تكون باهظة في أغلبية الجرائم.
- تُعدّ الجرائم الإلكترونية من أكثر أنماط الجرائم جذبًا لمرتكبيها، نظرًا لسهولة تنفيذها وسرعتها، وإمكانية ارتكابها عن بُعد دون الحاجة إلى التواجد الفعلي في مسرح الجريمة. كما أن هذا النوع من الجرائم يتميز بطبيعته "الناعمة"، إذ لا يتطلب جهدًا عضليًا أو أدوات مادية تقليدية، في مقابل ما يحققه من مكاسب ومنافع كبيرة. كل هذه العوامل مجتمعة تجعل الجرائم الإلكترونية خيارًا مغريًا للعديد من الجناة، خاصة في ظل ضعف الرقابة وصعوبة التتبع³⁵.

سمات المجرم المعلوماتي: يتميز المجرم الإلكتروني بعدد من السمات والخصائص التي تجعله مختلفاً عن المجرم التقليدي والتي منها

1- مجرم ذكي: يُعد الذكاء من أبرز السمات التي تميز مرتكب الجريمة المعلوماتية، إذ تتطلب هذه الجرائم إلماماً عميقاً بتقنيات وتكنولوجيا المعلومات، إلى جانب القدرة على التعامل مع أنظمة الحاسوب، وتعديل أو تغيير برامجها بمهارة عالية.

2- مجرم محترف: يتمتع المجرم الإلكتروني بمستوى عالٍ من الخبرة والمهارة في استخدام الحاسوب والتقنيات الحديثة، مما يُمكنه من تنفيذ جرائمه بدقة وفعالية..

3- مجرم غير عنيف: ينتمي هذا النوع من الإجرام إلى فئة الجرائم غير العنيفة، إذ يعتمد على الحيلة والخداع دون الحاجة إلى استخدام القوة أو التهديد الجسدي.

4- مجرم متكيف اجتماعياً: لا يُظهر المجرم الإلكتروني عداً مباشراً للمجتمع، بل يسعى إلى الاندماج فيه، ويُوظف ذكاءه للتكيف مع محيطه، مما يزيد من خطورته كلما تعمق هذا التكيف.

5- الميل إلى ارتكاب الجرائم: يُلاحظ لدى مرتكبي الجرائم الإلكترونية ميل واضح نحو ارتكاب الأفعال غير القانونية، مدفوعين برغبة مستمرة في تجاوز الحدود المسموح بها

6- الميل إلى التقليد: كثير من هذه الجرائم تنشأ نتيجة محاولة الفرد تقليد الآخرين في مهاراتهم التقنية، مما يدفعه إلى ارتكاب أفعال إجرامية دون إدراك كامل لعواقبها القانونية.³⁶

تصنيف الجرائم الإلكترونية:³⁷

تتخذ الجريمة الإلكترونية، أو ما يُعرف بالجريمة المعلوماتية، أشكالاً متعددة، إلا أنها تشترك جميعاً في الوسيلة التقنية المستخدمة لارتكابها، والمتمثلة في الأجهزة الحديثة كالحواسيب وغيرها، وُترتكب جميعها عبر شبكة الإنترنت³⁸، وقد تناولت اتفاقية بودابست، المعنية بالإجرام السيبراني والموقعة من قبل الاتحاد الأوروبي بتاريخ 23 نوفمبر 2001، أبرز صور هذه الجرائم. وتُعد هذه الصور التي حددتها الاتفاقية تمثيلاً دقيقاً لأشكال الجريمة المعلوماتية المعاصرة، والتي يمكن تلخيصها فيما يلي:³⁹

أولاً: الجرائم ضد سرية وسلامة وإتاحة البيانات والنظم المعلوماتية: عدت الاتفاقية صور هذه الجرائم في الآتي:

أ- الولوج غير القانوني: يقصد به الدخول غير المصرح به إلى نظام معلوماتي مملوك للغير، ويُعرف اصطلاحاً بـ "القرصنة". وقد يكون الهدف من هذا الفعل تخريبياً، كإتلاف أو تدمير النظام

المعلوماتي، أو استغلالياً، كالوصول إلى معلومات وبيانات سرية دون إذن، أو التلاعب بالبيانات المخزنة داخل النظام، وهو ما يُصنّف ضمن جرائم الغش أو التزوير المعلوماتي.

ب- **الاعتراض غير القانوني:** تمثل هذه الجريمة انتهاكاً صارخاً لحق الأفراد في الخصوصية، وتتحقق عندما يتم اعتراض الاتصالات أو المراسلات الإلكترونية الخاصة دون إذن. وتشمل هذه الجريمة جميع أشكال نقل البيانات إلكترونياً، سواء عبر الهاتف، أو الفاكس، أو البريد الإلكتروني، أو غيرها من الوسائل التقنية الحديثة.

ت- **الاعتداء على سلامة البيانات:** يقصد بها الأفعال العمدية التي تستهدف البيانات أو البرامج المخزنة على أجهزة الحاسب الآلي المملوكة للغير، وذلك بغرض تعطيل الجهاز، أو محو البيانات، أو تشويهها، بما يؤدي إلى فقدانها أو إفسادها بشكل كلي أو جزئي.

ث- **الاعتداء على سلامة النظام:** تتمثل هذه الجريمة في الأفعال التي تؤثر بشكل خطير على الأداء السليم لنظام الحاسب الآلي، مما يؤدي إلى تعطله أو توقفه عن العمل، ومن أبرز صورها إدخال الفيروسات أو البرمجيات الخبيثة التي تعيق تشغيل النظام أو تفسده.

ج- **إساءة استخدام أجهزة الحاسب:** ويشمل ذلك كل سلوك يُعد مجزماً قانوناً يتم من خلال استخدام الحاسب الآلي كوسيلة لارتكاب الجريمة، سواء تعلق الأمر بالاحتيال، أو التزوير، أو انتهاك الخصوصية، أو غيرها من الأفعال المخالفة للقانون الجرائم المرتبطة بالمحتوى "الأفعال الإباحية والأخلاقية"

ثانياً: **الجرائم المعلوماتية المتصلة بالحاسب:** وتتمثل في الآتي:

أ- **الاحتيال المعلوماتي أو التزوير و الغش المعلوماتيين**⁴⁰: ويقصد به "الخداع أو الغش المعلوماتي الذي يقوم علي التلاعب في نظم المعالجة الآلية للمعلومات بهدف الحصول دون وجه حق علي خدمات أو أموال أو أصول معينة، ويقوم الجاني في هذه الجريمة باستخدام التقنيات الحديثة بغية التلاعب في البيانات المصرفية ونتائج الميزانيات والمستحقات المالية، فيتم تحويل تلك الأموال في ثوانٍ معدودة من حساب إلى آخر، وتتمثل خطورة هذا الفعل الإجرامي في كونه يتم عبر الحدود الإقليمية لأكثر من دولة وفي ثوان معدودة، وهو ما يجعله بالغ الأثر السلبي على الاقتصاد القومي ؛ إذ من الممكن أن يؤدي ارتكاب مثل هذه الجريمة إلى إفلاس شركات أو بنوك كبرى في الدولة"⁴¹

ب- **الجرائم المتصلة بمحتوى الحاسب الآلي:** وهي تتعلق بجرائم إنتاج ونشر المواد الإباحية الخاصة بالأطفال وبيع الأطفال والاتجار فيهم والترويج لدعارة الأطفال.

لم تعتمد الاتفاقية العربية لمكافحة جرائم تقنية المعلومات تصنيفاً منهجياً مماثلاً لما ورد في اتفاقية بودابست، بل اكتفت بعرض نماذج من الجرائم الإلكترونية على سبيل المثال لا الحصر. ومن بين هذه النماذج: الجرائم المرتبطة باستخدام وسائل تقنية المعلومات، وجرائم الاحتيال والمحتوى الإباحي، وجرائم الاستغلال الجنسي، بالإضافة إلى انتهاك حرمة الحياة الخاصة، وما يتصل بجرائم الإرهاب والجريمة المنظمة⁴².

وهناك من الفقه من صنف الجرائم الإلكترونية تحت نوعين من الجرائم على حسب الأداة المستخدمة في ارتكابها⁴³

النوع الأول: جرائم الحاسب وشبكاته:

يرتبط هذا النوع من الجرائم بالانتهاكات التي تُرتكب عبر الشبكة العالمية، حيث يُستخدم الحاسب الآلي وشبكاته كأداة مساعدة في تنفيذ الجريمة. وتشمل هذه الأفعال جرائم النصب والاحتيال، وغسل الأموال، والتشهير، والسب، والقدف. ويتميّز هذا النمط من الجرائم بكون الحاسب الآلي يحتفظ بأدلة رقمية يمكن أن تسهم بشكل فعال في تحديد هوية الجاني وكشف ملابسات الجريمة.

النوع الثاني: جرائم الكمبيوتر

يرتبط هذا النوع من الجرائم بالحالات التي يكون فيها الحاسب الآلي ذاته هو محل الفعل الإجرامي، سواء من خلال الاعتداء على مكوناته المادية، أو على عناصره المعنوية كالبرمجيات (Software)، أو قواعد البيانات (Databases)، أو المعلومات المخزنة عليه. وتشمل هذه الأفعال الحصول غير المشروع على البيانات ونشرها، مما يُعد انتهاكاً لحقوق الملكية الفكرية، أو استخدام الحاسب لتخزين مواد إباحية، وهو ما يُشكل جريمة قائمة بذاتها.

وفي سياق التحليل الفقهي، انقسمت الاتجاهات إلى تصنيفات متعددة للجرائم الإلكترونية؛ فهناك من صنفها إلى جرائم تقليدية تُرتكب باستخدام الحاسب الآلي كوسيلة، مثل السرقة، والنصب، وخيانة الأمانة، والإتلاف، والتنصت، وغيرها من الجرائم المعروفة. في المقابل، ظهرت تصنيفات أخرى تعتبر بعض الجرائم الإلكترونية مستحدثة، كجرائم التجسس والقرصنة.

كما اتجه جانب من الفقه إلى تصنيف الجرائم الإلكترونية وفقاً للمصلحة القانونية المحمية، فميز بين: الجرائم التي تمثل اعتداءً على الأشخاص؛ الجرائم التي تستهدف الأموال؛ الجرائم التي تنال من البيانات والمعلومات؛ الجرائم التي تمس الآداب العامة وحقوق الملكية الفكرية؛ الجرائم ذات الصلة بالإجرام المنظم؛ والجرائم ذات الطابع السياسي⁴⁴.

الأهداف المقصودة من تلك الجرائم هي كالآتي:

1. صناعة ونشر الفيروسات: وهي أكثر الجرائم الإلكترونية انتشاراً وتأثيراً.
2. الاختراقات: يتمثل في الدخول غير المصرح به إلى أجهزة الحاسوب أو الشبكات الرقمية، بهدف الوصول إلى البيانات أو التحكم في الأنظمة.
3. تعطيل: انتشرت مؤخرًا عمليات تهدف إلى تعطيل أداء الأجهزة أو الشبكات دون تنفيذ اختراق فعلي، مما يؤدي إلى توقفها عن العمل.
4. انتحال الشخصية: تتجسد هذه الجريمة في استخدام هوية شخص آخر بشكل غير قانوني، إما للاستفادة من مكانته أو لإخفاء هوية الجاني وتسهيل ارتكاب جرائم إضافية.
5. المضايقة: تحدث غالبًا من خلال البريد الإلكتروني أو وسائل المصادقة الفورية، وتشمل إرسال رسائل تهديد أو تخويف أو إزعاج مستمر للضحية.
6. التشهير وتشويه السمعة أو المطاردة: يقوم الجاني بنشر معلومات سرية أو مضللة أو خاطئة عن الضحية، سواء كان فردًا أو مؤسسة، بهدف تعريضه للإحراج أو المضايقة العامة عبر الوسائل الإلكترونية.

7. النصب والاحتيال: أصبحت الإنترنت بيئة خصبة لعرض السلع والخدمات بطرق غير تقليدية، مثل البريد الإلكتروني أو المواقع الإلكترونية أو ساحات الحوار، مما يُستغل أحيانًا في عمليات احتيالية.

يتضح من التقسيمات السابقة أن إدراج الفعل ضمن إطار الجرائم الإلكترونية يتطلب أن يكون لجهاز الحاسب الآلي دور جوهري في ارتكاب الجريمة. ويُقصد بالحاسب الآلي هنا مكوناته المنطقية، مثل المعلومات والبرمجيات، إلى جانب العناصر المادية التي تساهم في تنفيذ المعالجة الآلية للبيانات. وتكمن أهمية هذا الدور في أن النظام المعلوماتي قد ساهم بشكل فعال في تسهيل ارتكاب الجريمة. ويختلف مدى تدخل الحاسب الآلي من جريمة إلى أخرى، تبعًا لطبيعة الفعل الإجرامي المرتكب.⁴⁵

على الرغم من الجهود المكثفة التي تبذلها الجهات المعنية بتطبيق القانون، يؤكد الخبراء أن الجرائم الإلكترونية تشهد نموًا متسارعًا يفوق في سرعته حتى تجارة المخدرات. وتشمل هذه الجرائم مجموعة من الأفعال غير القانونية، مثل الاتجار بالأطفال لأغراض جنسية، والتلاعب في أسواق المال، وسرقة البرمجيات، إضافة إلى جرائم الابتزاز الرقمي.

المطلب الثالث: التكيف القانوني للجريمة الإلكترونية

في الواقع، لا يزال الإطار القانوني المنظم لجرائم الإنترنت يعاني من فراغ شبه كامل، ويُعزى ذلك إلى حداثة هذه الظاهرة من جهة، وإلى تأخر المشرع في سنّ التشريعات ووضع الضوابط اللازمة لتنظيم استخدام تكنولوجيا المعلومات من جهة أخرى. وفي ظل هذا القصور، برزت مساهمات فقهية متفرقة كان لها دور محوري في بلورة المفاهيم القانونية المرتبطة بالفضاء الإلكتروني، واقتراح آليات للتعامل معه مستقبلاً.

الفرع الأول: تصنيف الجرائم الإلكترونية حسب طبيعة الأفعال المجرمة المنشأة لها

في هذا السياق، تبين أن جزءاً كبيراً من الجرائم الإلكترونية يُشابه إلى حدّ بعيد الجرائم التقليدية المنصوص عليها في قانون العقوبات، مما يستدعي تطبيق ذات المبادئ والضوابط القانونية المعتمدة في الجرائم العادية على نظيراتها الرقمية. فعلى سبيل المثال، تُعد جريمة التزوير والتحريف عبر الإنترنت امتداداً طبيعياً لنفس الجريمة في الواقع المادي، ويجب أن تُنظّم وفقاً للأسس القانونية ذاتها، نظراً لأن البرامج والمعلومات المخزنة في الحاسوب تُعدّ من قبيل الأموال، وتُشابه في طبيعتها بعض الحقوق التقليدية كحق الابتكار، والملكية الفكرية، والاسم التجاري. وتُعتبر برامج الحاسوب وسيلة للتعبير عن أفكار المؤلف، مما يجعلها خاضعة لحماية قانون حقوق المؤلف، وهو ما استقر عليه رأي غالبية الفقه القانوني⁴⁶.

وبناءً عليه، فإن أي شخص يقوم بالدخول إلى شبكة الإنترنت ويبعث بالبرامج المعروضة، سواء بتحريفها أو نسخها أو تدميرها، يُعدّ معتدياً على ملكية الغير، ويخضع للمساءلة القانونية بوصفه مرتكباً لفعل يستوجب العقوبة التعزيرية والتعويض عن الضرر الناتج⁴⁷.

أما بالنسبة لجريمة الاختلاس والسرقة تخضع جريمة السرقة عبر شبكة الإنترنت لنفس القواعد والأحكام المنصوص عليها في قانون العقوبات، لا سيما فيما يتعلق بالشروط والأركان اللازمة لقيام الجريمة. ويُعدّ العنصر الجوهري في هذه الجريمة هو انتقال المال من حيازة مالكه الشرعي إلى حيازة الجاني دون وجه حق. وينطبق هذا الوصف على السرقة المعلوماتية، حيث يعتمد الجاني على برمجة نظام الحاسب الآلي لتنفيذ عملية تحويل مالي من رصيد أحد الأشخاص، مستخدماً بيانات أو رموزاً تتيح له إتمام النقل، ليقيد المبلغ لاحقاً في حساب يسيطر عليه. ورغم أن هذا التحويل يتم في بيئة رقمية غير مادية، إلا أن الأثر القانوني الناتج عنه يُعادل تماماً التسليم الفعلي للمال، مما يُرتب على الجاني مسؤولية جنائية بوصفه معتدياً على ملكية الغير، ويستوجب توقيع العقوبة التعزيرية والتعويض عن الضرر.

أما العنصر الثاني في جريمة السرقة، يُعد القصد الجنائي عنصراً أساسياً، ويتحقق في الحالة المعروضة من خلال علم الجاني وإرادته في إخراج المال من حيازة صاحبه بقصد الاستيلاء عليه وتملكه، مما يدل على ارتكاب الفعل بشكل متعمد ومقصود. وبذلك، لا تختلف العناصر الجوهرية لجرمي السرقة والاختلاس بين المجال التقليدي والمجال المعلوماتي، إذ تتشابه في البنية القانونية والأساس الجنائي، باستثناء بعض الظروف الخاصة التي تحيط بكل حالة على حدة، والتي قد تؤثر في توصيف الجريمة أو في تقدير العقوبة.

الفرع الثاني: تحديد الاختصاص القضائي لنظر جرائم الإنترنت

رغم أن الجانب الشرعي للجرائم الإلكترونية قد حظي بمعالجة مبدئية كما تم بيانه سابقاً، إلا أن الإشكال الذي لا يزال قائماً حتى اليوم يتمثل في تحديد القانون الواجب التطبيق، والجهة القضائية المختصة بالنظر في هذه الجرائم. وفي الحالات التي يكون فيها أطراف الجريمة من نفس الدولة، فإن المسألة لا تثير إشكالاً يُذكر، إذ يُطبق قانون تلك الدولة وتُناط الولاية القضائية بمحاكمها. غير أن الطبيعة العابرة للحدود لشبكة الإنترنت تُعقد المسألة بشكل كبير، إذ تتجاوز هذه الجرائم الحدود الإقليمية التقليدية، مما يثير إشكالية تنازع القوانين والاختصاص القضائي على أكثر من صعيد.

وقد أدت هذه المرونة إلى تباين الآراء الفقهية، حيث انقسمت إلى عدة اتجاهات. فالاتجاه الأول يرى أن المحكمة المختصة هي محكمة الإقليم الذي وقعت فيه الجريمة، حتى وإن كان الجاني يحمل جنسية دولة أخرى. غير أن هذا الرأي تعرّض لانتقادات، أبرزها عجزه عن تقديم حل فعال في الحالات التي تُرتكب فيها الجريمة عبر أكثر من دولة في آن واحد⁴⁸.

الاتجاه الثاني -جعل المحكمة المختصة هي محكمة محل إقامة المدعى عليه، وقد أخذت معظم التشريعات العربية بهذا الاتجاه، بيد أنه لم يسلم من النقد هو الآخر، لا سيما إذا كان هذا الفعل لا يعد جرمًا في نظر الدولة محل ارتكابه، خاصة وأن صنفاً راجحاً من الدول لازال بعيداً عن السيطرة على أفعال الاعتداء على حقوق الملكية الفكرية، أو الدعاية الكاذبة أو المضللة...⁴⁹

يرى اتجاه فقهي أن المحكمة المختصة بنظر الجرائم الإلكترونية ينبغي أن تكون محكمة موطن المدعى عليه، وهو ما تبنته غالبية التشريعات العربية. غير أن هذا التوجه لم يخلُ من الانتقادات، خصوصاً في الحالات التي لا تُعد فيها الأفعال المرتكبة جرائم وفقاً لقانون الدولة التي وقعت فيها. ويزداد هذا الإشكال تعقيداً في ظل استمرار عدد معتبر من الدول في التباطؤ في تجريم بعض

الأفعال الرقمية، مثل انتهاك حقوق الملكية الفكرية أو نشر الدعاية الكاذبة والمضللة، مما يخلق فجوة قانونية تعيق تحقيق العدالة العابرة للحدود.

الاتجاه الثالث يرى أحد الاتجاهات الفقهية أن المحكمة المختصة بنظر الجريمة الإلكترونية ينبغي أن تكون محكمة جنسية مرتكب الجريمة. ورغم ما يتمتع به هذا الرأي من جاذبية نظرية، إلا أن تطبيقه العملي يواجه صعوبات جمة، نظرًا لما يتمتع به مرتكبو الجرائم الإلكترونية من قدرات تقنية ومعرفية عالية، تجعل من تعقبهم وتحديد هويتهم أمرًا بالغ التعقيد.

وفي نهاية المطاف، يخلص الباحث إلى أن هذا الإشكال "القديم-الجديد" لا يزال مطروحًا بقوة في الساحة القانونية، وأن الحل الأكثر واقعية يتمثل في إخضاع دعوى المسؤولية لقانون الدولة التي وقع فيها الفعل الإجرامي، شريطة أن يكون الفعل مجرمًا في كلا النظامين القانونيين: قانون المدعي وقانون المدعى عليه.

وقد تبنت هذا الحل عدد من الدول الصناعية الكبرى، رغم ما واجهته من تحديات على مستوى التطبيق، لا سيما في ظل تعقيدات التكيف القانوني وتباين الأنظمة القضائية.

المبحث الثاني:

الشرعية الجنائية للجريمة الإلكترونية

لا شك في أن التجريم والعقاب يعد من أخطر الأمور التشريعية التي تتصل بحرية المواطنين وذلك بسبب خطورة الآثار التي تترتب عليه، ولذلك فإن النصوص التشريعية التي تصدر به، يتعين أن تصدر دائماً وفقاً لمبدأ الشرعية الجنائية⁵⁰ الذي نحاول فيما يأتي إلقاء الضوء عليه.

تُعد الدولة محور الالتقاء بين القانون الدستوري والقانون الجنائي؛ إذ يتولى الدستور تنظيم نشاط الدولة من الزاوية السياسية، بينما يُعنى القانون الجنائي بتنظيم نشاطها من الناحية الجزائية، من خلال ضبط العلاقة بين الفرد والدولة، وكذلك بين الأفراد فيما بينهم. وتتجلى الصلة الوثيقة بين النظامين في تضمّن الدساتير لنصوص ذات طابع جنائي، تهدف إلى حماية الدستور ذاته ومنحه طابعاً من القدسية، بالنظر إلى ارتباطه الوثيق بحقوق الأفراد وحياتهم الأساسية. وتُسهم المبادئ الدستورية⁵¹ في رسم معالم القانون الجنائي، حيث يُستمد مضمون هذا الأخير بدرجة كبيرة من تطور المبادئ الدستورية، أكثر من اعتماده على تطور القيم أو المصالح الاجتماعية. وفي هذا الإطار، يؤدي القانون الجنائي وظيفته ضمن حدود الشرعية الدستورية، كما يحددها

الدستور، مستنداً إلى مجموعة من المبادئ الدستورية، في مقدمتها "مبدأ الشرعية الجنائية"⁵²، الذي يُعد الركيزة الأساسية للنظام الجنائي برمته. وينبثق عن هذا المبدأ، وتدور حوله، سائر المبادئ التي تحكم القواعد الجنائية، سواء الموضوعية منها أو الإجرائية⁵³. ويقصد به عموماً أن التشريع هو المصدر الوحيد للتجريم والعقاب، وأن السلطة التشريعية وحدها هي المخوّلة بتحديد الأفعال المجزّمة والعقوبات المقررة لها، دون تدخل من السلطتين القضائية أو التنفيذية، بينما تنحصر مهمة القاضي في تطبيق النصوص التي يستلزمها المشرّع.⁵⁴

يرتبط نشوء مبدأ الشرعية الجنائية في القانون الوضعي بتاريخ الفصل بين سلطات الدولة؛ إذ كانت سلطة التجريم والعقاب، قبل هذا الفصل، حكراً على الملك يمارسها بإرادته المطلقة⁵⁵. وفي العصور الوسطى، انتقلت هذه السلطة إلى القضاة الذين كانوا يملكون صلاحيات تقديرية واسعة لتجريم الأفعال ومعاينة مرتكبيها دون الاستناد إلى نص قانوني. وقد بدأ تكريس هذا المبدأ تدريجياً، بدءاً من ميثاق هنري الأول في إنجلترا، مروراً بدستور كلاريندون، ثم تأكيده في العهد الأعظم. وجاءت الثورة الفرنسية لتمنحه بعداً حقوقياً واضحاً، حيث نصت عليه المادة الثانية من إعلان حقوق الإنسان والمواطن لعام 1789. لاحقاً، تم ترسيخ هذا المبدأ في الوثائق الدولية، أبرزها الإعلان العالمي لحقوق الإنسان الصادر عام 1948، والاتفاقية الأوروبية لحقوق الإنسان لعام 1950، ثم العهد الدولي الخاص بالحقوق المدنية والسياسية لعام 1966، مما جعله أحد الركائز الأساسية للأظمة القانونية الحديثة.

يُعد مبدأ الشرعية الجنائية من المبادئ الدستورية ذات الطابع العالمي، وقد ساهم في ترسيخه الفقيه الإيطالي "شيزاري بيكاريا"، من خلال مؤلفه الشهير "الجرائم والعقوبات" الصادر عام 1764، حيث أكد فيه أن "القوانين وحدها هي التي تحدد العقوبات المقررة للجرائم"، وأن "القاضي لا يملك توقيع أي عقوبة خارج إطار النص القانوني"⁵⁶.

وبناءً على ما تقدم، سيتم تقسيم هذا المبحث إلى مطلبين رئيسيين: المطلب الأول: المحكمة الدستورية العليا في مصر ومبدأ الشرعية الجنائية في الجرائم الإلكترونية. والمطلب الثاني: مبررات تطبيق مبدأ الشرعية الجنائية على الجرائم الإلكترونية والنتائج المترتبة عليه.

المطلب الأول: إرساء دعائم مبدأ الشرعية الجنائية ودور المحكمة الدستورية العليا

لعبت المحكمة الدستورية العليا في مصر دوراً محورياً في ترسيخ مبدأ شرعية الجرائم والعقوبات، باعتباره أحد الركائز الأساسية لفكرة الأمن القانوني. فقد عملت المحكمة على توضيح مضمون هذا المبدأ، وكشف أبعاده ودلالاته وحدوده، كما وضعت الضوابط الدقيقة التي تحكم

تفويض السلطة التنفيذية في مجالي التجريم والعقاب. واستخلصت من ذلك قاعدة أساسية مفادها عدم جواز توقيع أي عقوبة إلا بموجب حكم قضائي، كما حددت مفهوم الجريمة من منظور قانوني، وأرست المعايير التي تمكّنها من ممارسة رقابتها على دستورية النصوص الجنائية.⁵⁷ وقد أكدت المحكمة على الأهمية البالغة لمبدأ الشرعية الجنائية، مشيرة إلى أنه أصبح ركيزة ثابتة في الأنظمة القانونية للدول المتحضرة، وهو ما انعكس في عدد من المواثيق الدولية، من بينها الفقرة (11) من الإعلان العالمي لحقوق الإنسان، والفقرة (1) من المادة (15) من العهد الدولي الخاص بالحقوق المدنية والسياسية، والمادة (7) من الاتفاقية الأوروبية لحماية حقوق الإنسان، فضلاً عن حضوره في العديد من الدساتير الوطنية.

وترى المحكمة أن هذا المبدأ يشكل ضمانة أساسية ضد التعسف، إذ يمنع القاضي من تجريم أفعال يختارها وفق هواه، أو من فرض عقوبات بناءً على تقدير شخصي لا يستند إلى نص قانوني. ومع زوال السلطة المطلقة، أصبح التأثيم من اختصاص السلطة التشريعية وحدها، فهي التي تحدد الأفعال المجزّمة وتقرّر العقوبات المناسبة لها. ويُفسّر هذا المبدأ في ضوء أن القيم الجوهرية التي يسعى القانون الجنائي لحمايتها لا يمكن تحديدها إلا من خلال الهيئة التشريعية المنتخبة، باعتبارها المعبرة عن الإرادة الشعبية. ومن ثم، فإن مبدأ الشرعية يُعدّ ضرورياً لربط المواطنين بتلك القيم التي يقوم عليها البناء المجتمعي، بما يعزز وحدتهم ويضمن تماسكهم الاجتماعي، ويحول دون ازدياد النظام القانوني.⁵⁸

أكدت المحكمة الدستورية العليا على الترابط الوثيق بين مبدأ الشرعية الجنائية والسياسة الجنائية للدولة، مشيرة إلى أن السياسة الجنائية الرشيدة ينبغي أن تُبنى على عناصر متجانسة ومتمكاملة. فإذا تأسست على عناصر متنافرة، فإن ذلك يؤدي إلى انفصام بين النصوص القانونية وأهدافها، مما يفقدها فعاليتها في تحقيق الغايات المرجوة، نتيجة لانعدام التناسق المنطقي بينها. ويستند هذا التوجه إلى الإيمان بأن الأصل في التشريعات، ضمن الدولة القانونية، هو ارتباطها العقلي والموضوعي بأهدافها، باعتبار أن التنظيم التشريعي لا يُقصد لذاته، بل يُعد وسيلة لتحقيق تلك الأهداف. ومن ثم، يتعين دائماً التحقق من مدى التزام النص المطعون فيه بإطار منطقي ينسجم مع الغايات التي يسعى إلى تحقيقها، دون أن يتناقض معها أو يتجاوزها، بما يخلّ بمبدأ خضوع الدولة للقانون.⁵⁹

كما شددت المحكمة على العلاقة الجوهرية بين مبدأ الشرعية الجنائية ومفهوم العدالة الجنائية، مؤكدة أن العدالة الجنائية، في جوهرها، لا تتحقق إلا من خلال قواعد قانونية محددة بدقة

وإنصاف، تُبنى عليها عملية الفصل في ما إذا كان المتهم مداناً أو بريئاً. ويتطلب ذلك تحقيق توازن دقيق بين مصلحة المجتمع في الحفاظ على أمنه واستقراره، ومصلحة الفرد في ألا تُفرض عليه عقوبة لا ترتبط بالفعل الذي ارتكبه، أو تفتقر إلى دليل قانوني يثبتها. ولا يجوز التفريط في هذه الضمانات أو التنازل عنها، لما تمثله من حماية جوهرية للحقوق والحريات.⁶⁰

أكدت المحكمة الدستورية العليا على أهمية الضمانات الملازمة لتطبيق مبدأ الشرعية الجنائية، مشيرة إلى أن النطاق الحقيقي لهذا المبدأ يتحدد من خلال ضمانتين أساسيتين تكفلان تحقيق أهدافه. أولهما: ضرورة أن تُصاغ النصوص العقابية بصياغة واضحة ومحددة، تخلو من الغموض أو الالتباس، بحيث لا تتحول إلى فخاخ أو شرك قانونية ينصبها المشرع باتساعها أو إبهامها، فيقع تحت طائلتها من لا يدرك حدودها أو يخطئ في تفسيرها. وتكمن الغاية من هذا الضمان في تمكين المخاطبين بتلك النصوص من إدراك مضمونها بدقة، بما يسمح لهم بمواءمة سلوكهم معها، لا بمخالفتها عن غير قصد.

وثانيهما: ومفترضها أن المرحلة الزمنية التي تقع بين دخول القانون الجنائي حيز التنفيذ والغاء هذا القانون يُشترط في تطبيق النصوص العقابية أن تكون نافذة في الفترة التي ارتكبت فيها الأفعال الإجرامية، فلا يجوز تطبيقها بأثر رجعي على أفعال سابقة لصدورها، إذ يجب أن يكون القانون سابقاً للفعل، ضماناً لمبدأ عدم رجعية النصوص الجنائية.⁶¹

وقد أكدت المحكمة الدستورية العليا على ضرورة احترام حدود تفسير القاضي للنصوص الجنائية، مشيرة إلى أنه لا يجوز تطبيق النصوص العقابية بما يُسيء إلى المركز القانوني القائم للمتهم، ولا تفسيرها على نحو يُخرجها عن معناها أو مقاصدها التشريعية. كما لا يجوز توسيع نطاق التجريم عن طريق القياس ليشمل أفعالاً لم يُجرّمها المشرع صراحة، حتى وإن بدا ذلك أكثر ضماناً للحرية الشخصية، ما لم يكن هناك ارتباط منطقي بين النص القانوني وإرادة المشرع، سواء كانت هذه الإرادة معلنة أو يُمكن استنباطها عقلياً.⁶²

المطلب الثاني: مبررات ونتائج مبدأ الشرعية الجنائية للجريمة الإلكترونية

طرح الفقه عدة مبررات ونتائج للترويج لمبدأ الشرعية الجنائية يمكن حصرها في الآتي:

الفرع الأول: مبررات مبدأ الشرعية الجنائية للجريمة الإلكترونية

أولاً: تحقيق مبدأ العدالة

يتطلب احترام الكرامة الإنسانية أن تُحصر الأفعال غير المشروعة المرتكبة عبر الوسائط الإلكترونية ضمن إطار الجرائم الإلكترونية، وأن تُحدّد العقوبات المقررة لها بدقة ووضوح، بما يتيح

للمشرع مواجهتها بفعالية. كما ينبغي إعلام المجتمع بهذه الجرائم والعقوبات المرتبطة بها، تعزيزًا للوعي القانوني العام.

ثانياً: تحقيق مبدأ الفصل بين السلطات

يتجلى هذا المبدأ من خلال توزيع الأدوار بين السلطات الثلاث: فالسلطة التشريعية، بصفتها ممثلة لإرادة الشعب، تتولى سنّ النصوص المتعلقة بالتجريم والعقاب في مجال الجرائم الإلكترونية؛ بينما تضطلع السلطة القضائية بتطبيق هذه النصوص على الوقائع المعروضة أمامها؛ وتتولى السلطة التنفيذية تنفيذ الأحكام القضائية الصادرة في هذا الشأن.

ثالثاً: تحقيق مبدأ الردع العقابي

يتحقق هذا المبدأ من خلال إعلام المخاطبين بالقانون بمضامين النصوص الجنائية المتعلقة بالجرائم الإلكترونية، والعقوبات المقررة لها، مما يسهم في ردع الأفراد عن ارتكاب هذه الأفعال خشية العقوبة، ويعزز في الوقت ذاته قناعة الجاني بعدالة العقوبة الموقعة عليه.

رابعاً: تحقيق مبدأ المساواة في العقاب

تُصاغ النصوص الجنائية المتعلقة بالجرائم الإلكترونية بصيغة عامة ومجردة، بما يضمن تطبيقها على جميع الأفراد والوقائع دون تمييز. ويؤدي ذلك إلى تحقيق المساواة أمام القانون، بحيث لا يتأثر تطبيقه بالمركز الاجتماعي أو الوظيفي للجاني.⁶³

الفرع الثاني: نتائج مبدأ الشرعية الجنائية للجريمة الإلكترونية

يتحمّل المشرّع مسؤولية حصرية في مجال التشريع الجنائي للجرائم الإلكترونية، باعتبار أن السلطة التشريعية وحدها هي المختصة بوضع النصوص القانونية ذات الطابع الجزائي. ويُفترض أن يلتزم المشرّع، عند صياغة هذه النصوص، بعدم التعسف في استعمال سلطة التجريم، بحيث لا يُجرّم إلا الأفعال الإلكترونية التي تُشكّل اعتداءً فعلياً على المصالح الجوهرية للأمة. ورغم صعوبة تحديد هذه المصالح بدقة، إلا أنه يُشترط ألا تمتد الحماية الجنائية إلى مصالح لا تحظى بقيمة حقيقية لدى المجتمع أو لدى أغلبية أفراده.⁶⁴ كما يجب أن تُراعى قاعدة عدم رجعية النصوص الجنائية، بحيث لا تُطبّق أحكام التجريم على الوقائع السابقة لصدور النص، ويقتصر نطاق سريانها على المستقبل فقط، وهو ما يُجسّد مبدأ الشرعية الزمنية في التجريم الإلكتروني. ويُضاف إلى ذلك ضرورة التزام المشرّع بالوضوح والدقة في صياغة النصوص الجنائية⁶⁵، وتجنّب استخدام "النماذج المفتوحة" أو العبارات الفضفاضة التي تحتمل أكثر من تفسير، لما في ذلك من خطر على الأمن القانوني وحقوق الأفراد.⁶⁶

أولاً: بالنسبة للقاضي

يُعد القاضي ملزماً بتطبيق النصوص الجنائية الخاصة بالجرائم الإلكترونية كما وردت في التشريع، دون أن يُضيف إليها أو يُنقص منها، سواء في جانب التجريم أو العقاب. ويبدأ دوره بتحديد ما إذا كانت الواقعة المعروضة تندرج ضمن أحد الناذج الإجرامية التي نص عليها المشرع. فإن لم يتوافر هذا التكييف، وجب عليه الحكم ببراءة المتهم. أما إذا ثبت أن الفعل مجرم قانوناً، فيتعين عليه إسناد التكييف القانوني السليم للواقعة، بما يضمن تطبيق العدالة وفقاً للنصوص التشريعية

ثانياً: بالنسبة للسلطة التنفيذية

تلتزم الجهات المختصة بتنفيذ العقوبات الجنائية بتنفيذ الأحكام القضائية وفقاً لما نص عليه القانون، دون تجاوز أو تعديل. ولا يجوز للإدارة أن تُنقذ عقوبة لم يصدر بها حكم قضائي، أو أن تحل محل السلطة القضائية في تقرير العقوبة، أو أن تستمر في تنفيذها خلافاً لما قضى به الحكم. فالتنفيذ يجب أن يتم ضمن الحدود التي رسمها القضاء، احتراماً لمبدأ الفصل بين السلطات وضماناً للشرعية الإجرائية.⁶⁷

الخاتمة:

تناولت هذه الدراسة موضوع الجريمة الإلكترونية، حيث أظهرت كيف أن التطورات التكنولوجية الحديثة قد يَسَّرت سبل التواصل بين الجناة وضحاياهم، كما سهّلت التنسيق بين أعضاء الشبكات الإجرامية لوضع الخطط وتنفيذ الأفعال الإجرامية .

وقد تم التطرق إلى الخصائص الفريدة للجرائم الإلكترونية، التي تتجاوز الحدود المكانية والزمنية، وتتميز بخطورة بالغة وصعوبة في التحري والتحقيق، مما ينعكس على تعقيد إجراءات الملاحقة القضائية. كما أن الدوافع وراء ارتكاب الجرائم الإلكترونية تختلف عن تلك التي تحرك الجرائم التقليدية، وهو ما يطرح إشكالات قانونية متعددة.

وفي إطار التكييف القانوني للجريمة الإلكترونية، برزت تساؤلات محورية تتعلق بمسألتين أساسيتين: أولاهما تصنيف الجرائم الإلكترونية بناءً على طبيعة الأفعال المجرمة التي تنشأها والثانية تحديد الجهة القضائية المختصة بالنظر في هذه الجرائم، في ظل الطابع العابر للحدود الذي يميزها. وتواجه التشريعات العربية تحديات كبيرة في هذا المجال، أبرزها ضعف البنية القانونية المرتبطة بالجوانب التقنية والعملية، مما يجعل مواجهة الجرائم الإلكترونية تتجاوز مجرد إصدار نصوص قانونية، كما حاول قانون رقم 175 لسنة 2018 في مصر سدّ بعض الثغرات التشريعية السابقة.

وقد اختتمت الدراسة بتحليل يستند إلى مبدأ الشرعية الجنائية، بوصفه مبدأً دستوريًا راسخًا في مصر وسائر الدول المتحضرة، والذي ينص على أنه "لا جريمة ولا عقوبة إلا بنص". ونظرًا لحداثة الجريمة الإلكترونية وسرعة تطورها تبعًا لتطور التقنيات المستخدمة فيها، فقد بادرت بعض الدول المتقدمة إلى إصدار تشريعات دقيقة تُحدد عناصر الجريمة من حيث الركن المادي والمعنوي والعقوبة، وهي الدول التي نشأت فيها هذه التقنيات وتطورت تحت إشرافها. أما مصر، فقد وضعت إطارًا تشريعيًا شاملًا يغطي صور الجرائم الإلكترونية الراهنة، ويتيح في الوقت ذاته إمكانية استيعاب صور جديدة مستقبلية ضمن مظلتها القانونية.

المقترحات والتوصيات

- 1- ضرورة نشر الوعي بين الأفراد - ولا سيما الشباب - بمخاطر التعامل مع المواقع الخبيثة على شبكة الانترنت ودعم الوعي المجتمعي بالمخاطر النفسية والاجتماعية وغيرها الناجمة عن الاستخدامات غير الامنة للإنترنت.
- 2- تدريب رجال الضبط الجنائي والمحققين والقضاة المتخصصين بجرائم تقنية المعلومات على الأساليب الفنية المستخدمة في ارتكاب الجرائم وفيما يتعلق بالكشف عنها والدلائل المستحدثة في مجال اثباتها.
- 3- تفعيل دور المجتمع المدني ولا سيما الجمعيات الأهلية للقيام بدورها في وقاية الشباب من الوقوع في الممارسات الخاطئة للسلوكيات والممارسات الضارة أخلاقياً عبر شبكة الانترنت.
- 4- تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمكافحة الجرائم الإلكترونية من خلال الاتفاقيات الدولية الخاصة بمكافحة جرائم الانترنت وخاصة المعاهدة الدولية لمكافحة الجرائم الإلكترونية والانترنت مع متابعة المستجدات على الساحة العالمية
- 5- نأمل أن تسعى الدول العربية إلى انشاء منظمة عربية تهتم بالتنسيق في مجال مكافحة الجرائم الإلكترونية عبر الانترنت وتشجيع قيام اتحادات عربية تهتم بالتصدي لجرائم الانترنت وتفعيل دور المنظمات والادارات والحكومات العربية في مواجهة هذه الجرائم
- 6- إنشاء مدارس ومعاهد واقسام في الجامعات ومراكز بحثة خاصة تعني بالأمن المعلوماتي والتدريب فيه ومواكبة كل ما هو حديث في هذا المجال.
- 7- سن القوانين والأنظمة الخاصة التي تسد كافة ثغرت الجريمة الإلكترونية مثل القوانين المتعلقة بكيفية اكتشاف الأدلة الإلكترونية وحفظها والنص على طرق ثبوته

الهوامش:

- 1 السيد عوض، التطور التكنولوجي والجريمة، المؤتمر السنوي الرابع والثلاثون، قضايا السكان والتنمية المركز الديموغرافي بالقاهرة، 19-22 ديسمبر 2004، ص 6.
- 2 عبد الفتاح بيومي حجازي - مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية 2006.
- 3 يقصد بنطاق cyber بأنه هو نطاق ذو دلالة على شبكة الإنترنت يحدد بأن الكلمة التي ستلي هذا النطاق لها علاقة بشبكة الإنترنت مثل cyber cafe مقهى الإلكتروني الإرهاب الإلكتروني cyber terrorism النقود الإلكترونية cyber cash ومن هنا cyber crime هي الجرائم التي لها علاقة بالحاسب وشبكة الإنترنت.
- راجع مصطفى محمد موسي: التحقيق الجنائي في الجرائم الالكترونية، ط 1، دن، 2008، ص 111
- 4 راجع إبراهيم خالد ممنوح، إبرام العقد الإلكتروني، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2006، ص 13.
- 5 راجع- أحمد المناعسة وجمال محمد الزعبي، جرائم الحاسب الآلي والانترنت، دراسة تحليلية مقارنة، دار وائل للنشر، الطبعة الأولى، عمان، 2006، ص 60.
- 6 راجع- رشدي محمد السعيد، الإنترنت والجوانب القانونية لنظم المعلومات، دار الكتب للطباعة والنشر، الكويت 2002، ص 11.
- 7 راجع- عارف خليل أبو عيد، جرائم الإنترنت، دراسة مقارنة، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد 5 العدد الثالث، الإمارات العربية المتحدة، أكتوبر، 2008، ص 79.
- 8 المرجع السابق، ص 80.
- 9 راجع- قوره نائلة عادل، جرائم الحاسب الآلي، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، 2005، ص 17.
- 10 راجع- عارف خليل أبو عيد، المرجع السابق، ص 83.
- 11 راجع- قوره نائلة عادل، ص 17.
- 12 أحمد هلاي عبد الله، الحماية الجنائية للأخلاق من مظاهر الانحراف الجنسي، دار النهضة العربية، القاهرة، 1995، ص 36.

13 www.mcit.gov.sa

- 14 راجع- أحمد المناعسة وجمال محمد الزعبي، جرائم الحاسب الآلي والانترنت، دراسة تحليلية مقارنة، دار وائل للنشر، الطبعة الأولى، عمان، 2006، ص 60.

- 15 هلال بن محمد بن حارب البوسعيدى، الحماية القانونية والفنية لقواعد المعلومات المحوسبة "دراسة قانونية وفنية مقارنة"، دار النهضة العربية، 2009، ص15، وما بعدها.
- 16 راجع: *D.B Parker, combattre la criminalité informatique, 1985, p18*.
- 17 نائلة عادل محمد فريد قوره، جرائم الحاسب الاقتصادية "دراسة نظرية وتطبيقية"، دار النهضة العربية، 2003-2004، ص21.
- 18 موسى، التحقيق الجنائي في الجرائم الإلكترونية، ط1، ص112
- 19 خالد ممدوح إبراهيم: الجرائم المعلوماتية، دار الفكر الجامعي، 2009، ص74.
- 20 مصطفى محمد موسى، مرجع سابق، ص112.
- 21 راجع- منصور حسين منصور، جرائم الكمبيوتر والإنترنت، دار الجامعة الجديدة، الإسكندرية، 2003 ص155.
- 22 المرجع السابق 156.
- 23 راجع- رشدي محمد السعيد، المرجع السابق، ص65.
- 24 راجع- عبد الله حسين علي محمود، "الجوانب القانونية والأمنية للعمليات الإلكترونية"، مجلة أكاديمية شرطة دبي، العدد الأول، الإمارات العربية المتحدة، مارس 2003، ص592.
- 25 ذكرت وزارة العدل الأمريكية في دراسة لها أن تجارة الدعارة والإباحية الخلقية تجارة رائجة جدا يبلغ رأس مالها ثمانية مليار دولارا ولها أواصر وثيقة تربطها بالجريمة المنظمة. وإن تجارة الدعارة هذه تشمل وسائل عديدة كالكتب والمجلات وأشرطة الفيديو والقنوات الفضائية الإباحية والإنترنت. وتفيد الإحصاءات الاستخبارات الأمريكية (BI) أن تجارة الدعارة هي ثالث أكبر مصدر دخل للجريمة المنظمة بعد المخدرات والقمار حيث إن بأيديهم 85% من أرباح المجلات والأفلام الإباحية. وهنالك في الوقت الحاضر في أمريكا وحدها أكثر من 900 دار سينما متخصصة بالأفلام الإباحية وأكثر من 15000 مكتبة ومحل فيديو تتاجر بأفلام ومجلات إباحية. وهذا العدد يفوق حتى عدد مطاعم ماكدونالد بنسبة ثلاثة أضعاف. ولقد كانت أمريكا في الماضي تحارب إلى درجة كبيرة انتشار الإباحية في مجتمعاتها بفرض بعض الأنظمة والقوانين، ولكن من الملاحظ في هذا العصر أن المعارضين لانتشار الإباحية بدأوا يخسرون هذه الحرب حيث نجحت الاستوديوهات بتخفيف المراقبة على الأفلام وتغيير مفهوم الإباحية لدى المقيمين فأصبحت الأفلام التي كانت لتندرج تحت بند الأفلام الإباحية (X) قبل قرن يعاد تقييمها اليوم وإدراجها تحت بند (R) الأخف. كما تم إنشاء فئات أخرى بينية كقئة (NC-17) للهدف نفسه. ولقد تم بنجاح مؤخرا في أمريكا قلب وإلغاء قانون "العفة في الاتصالات" (Communications Decency Act of 1996) ليتمكن الناس من الاستمرار في أعمال الإباحية دون أي قيود قانونية. ومن المعلوم أن أمريكا هي أولى دول العالم في إنتاج المواد الإباحية. فهي تصدر سنويا 150 مجلة من

- هذه النوع أو 8000 عددا سنويا. وتجارة تأجير الأفلام الإباحية قد زادت من 75 مليون سنة 1985 إلى 665 مليون سنة 1996. رابط المادة: <http://iswy.co/e2ei0m>.
- في تفصيل هذه المسألة راجع- الشوي محمد ساجي، " ثورة المعلومات وانعكاساتها على قانون العقوبات"، دار الفكر العربي، القاهرة، 2003، ص 122.
- 26 راجع- عارف خليل أبو عيد، المرجع السابق، ص 94.
- 27 Knittel, John, Soto, Micheal (2000). *The Danger o Computer Hacking*. New York: The Rosen Publishing Group
- 28 انظر: موسى، أساليب إجرامية بالتقنية الرقمية) ماهيتها ومكافحتها (، ص 56. صغير، الجريمة المرتكبة عبر الانترنت، ص 12.
- 29 طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، منشور في موقع ستار تايمز، <http://www.startimes.com/.aspx?t=30245909>
- 30 - <http://droit.moontada.com/t622-topic>
- 31 مصطفى محمد موسي، مرجع سابق، ص 134، 135. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت دراسة مقارنة، دار النهضة العربية، 2009، ص 53، وما بعدها.
- 32 منير الجنبيني، ومدوح الجنبيني، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، الإسكندرية، دار الفكر الجامعي 2006 ص 33.
- 33 أسامة المناعسة، جلال والزعبي وفاضل الهواوشة، جرائم الحاسب الآلي والإنترنت: دراسة تحليلية مقارنة، عمان: دار وائل للنشر 2001 ص 21.
- 34 مفيد الزبيدي، قضايا العولمة والمعلوماتية. عمان، دار أسامة للنشر والتوزيع. 2003 ص 54.
- 35 أسامة المناعسة، جلال والزعبي وفاضل الهواوشة، المرجع السابق ص 22.
- 36 أمين عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دار النهضة العربية للطبع والنشر والتوزيع، الأردن، 2005، ص 13، وما بعدها، رامي متولي القاضي، مرجع سابق، ص 54، وما بعدها. راجع
- 37 سينا عبد الله محسن، المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية، ورقة عمل مقدمة لندوة الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 19-20 يونيو، 2007، ص 5.
- 38 Hemraj Saini, Yerra Shankar Rao, T.C.Panda, *Cybercrimes and their Impacts : A Review International Journal o Engineering Research and Applications (IJERA) Vol. 2, Issue 2, Mar-Apr 2012, PP. 2020-203.*
- 39 هلال عبد الله أحمد: الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة 23 نوفمبر 2001، دار النهضة العربية، 2002، ص 67، وما بعدها.
- 40 مصطفى سمارة، الجريمة الالكترونية، مجلة المعلوماتية العدد 29- شهر تموز 2008.
- 41 محمد محمد شتات، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2001، ص 79، وما بعدها.

- 42 رامي متولي القاضي، مرجع سابق، ص 29.
- 43 مصطفى محمد موسي، مرجع سابق، ص 112.
- 44 راجع في تفاصيل هذا التقسيم رامي متولي القاضي، مرجع سابق، ص 31، وما بعدها
- 45 نائلة عادل محمد فريد قورة، مرجع سابق، ص 25.
- 46 راجع- عرب يونس، "جرائم الحاسوب"، رسالة ماجستير، فرع القانون الجنائي، جامعة عمان، الأردن 1998 ص 147
- 47 راجع- جميل عبد الباقي، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، 2004 ص 92.
- 48 أحمد سالم طه، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة
- 49 شمس الدين أشرف توفيق، "الحماية الجنائية للمستند الإلكتروني"، مؤتمر الأعمال المصرفية الإلكترونية، كلية الشريعة والقانون، جامعة الإمارات، الإمارات العربية المتحدة، 2003 ص 458.
- 50 محمود علي أحمد مدني، دور المحكمة الدستورية العليا في استجلاء المفاهيم الأساسية التي يقوم عليها النظام القانوني المصري "دراسة مقارنة" رسالة دكتوراه، حقوق حلوان، 2015، ص 349.
- 51 خالد عبد الله الشافي: المبادئ الجنائية الدستورية في النظام الأساسي للحكم في المملكة العربية السعودية دراسة مقارنة، رسالة دكتوراه، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية 2010، ص 58، 59.
- 52 عمر سالم، شرح قانون العقوبات المصري، دار النهضة العربية، 2010، ص 30.
- 53 عبد العظيم مرسي وزير، شرح قانون العقوبات، دار النهضة العربية، دت، ص 33.
- راجع ايضاً:
- BECCARIA: "Traité des délits et des peines". Nouvelle Traduction française, Introduction de ANCEL et STEANI, Paris, Cujas 1966, p. 67.
- 54 حسنى الجندي، شرح قانون العقوبات، دن، 1999، ص 76، هدى حامد قشقوش، مرجع سابق، ص 30.
- 55 ويرجع تاريخ الفصل بين السلطات في أوروبا إلى العصور الوسطى حيث كان ملوكها يتمتعون بصلاحيات واسعة ويحكمون حكماً مطلقاً، ووصل الاستبداد ذروته في عهد الأمير: لويس الرابع عشر الذي قال مقولته الشهيرة "أنا الدولة"، وكرد فعل لتلك السلطة المطلقة التي يتمتع بها الملوك نادى الكثير من المفكرين في أوروبا بمبدأ الفصل بين السلطات، منهم لوك وجان جاك روسو وغيرهم، راجع خالد عبد الله الشافي، مرجع سابق، ص 102
- 56 راجع أحمد فتحي سرور، القانون الجنائي الدستوري، دار الشروق، ط 2، 2002، ص 31، هدى حامد قشقوش، شرح قانون العقوبات، دار النهضة العربية، 2010، ص 30، 31. راجع:

J.P.Delms saint hilair: un probleme qui évolue, le principe de la légalité en matière d'attante à la liberté de l'ass.inter.de droit penal-bordeaux 1984,p12.ets.

57 راجع في تفاصيل دور المحكمة الدستورية في إرساء مبدأ الشرعية الجنائية محمود علي أحمد مدني، مرجع سابق، ص 348، وما بعدها.

58 راجع حكم المحكمة الدستورية العليا المصرية في القضية رقم 48 لسنة 17 قضاء دستوري جلسة 1997/2/22

59 راجع حكم المحكمة الدستورية العليا المصرية في القضية رقم 114 لسنة 21 قضاء دستوري جلسة 2001/6/2.

60 راجع حكم المحكمة الدستورية العليا المصرية في القضية رقم 49 لسنة 17 قضاء دستوري جلسة 1996/6/15.

61 راجع حكم المحكمة الدستورية العليا المصرية في القضية رقم 48 لسنة 17 قضاء دستوري جلسة 1997/2/22.

62 راجع حكم المحكمة الدستورية العليا المصرية في القضية رقم 48 لسنة 17 قضاء دستوري جلسة 1997/2/22، حكم المحكمة الدستورية العليا المصرية في القضية رقم 58 لسنة 18 قضاء دستوري جلسة 1997/7/5.

63 راجع إبراهيم حامد طنطاوي، علي محمود حمودة، شرح الأحكام العامة لقانون العقوبات الجزء الأول النظرية العامة للجريمة، دار النهضة العربية، د.ت، ص 17، 18.

64 عمر سالم، مرجع سابق، ص 35.

65 هدى حامد قشقوش، مرجع سابق، ص 36.

66 راجع. *BERNA RDINI(R.) ,Droit Pénal general,Paris,2003,No193,p171* :

67 عمر سالم، مرجع سابق، ص 39.