ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639
Volume 11 issue 3
N:64 June 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

الجريمة الإلكترونية في ظل التحولات الرقمية: مقاربة قانونية معاصرة

Cybercrime in Light of Digital Transformations: A Contemporary Legal Approach

الدكتورة: هاجر العباسي

دكتورة في القانون الخاص، كلية العلوم القانونية والسياسية، جامعة الحسن الأول سطات/المغرب.

ملخص:

تتناول هذه الدراسة موضوع الجريمة الإلكترونية في ظل التحولات الرقمية المتسارعة، باعتبارها إحدى أبرز الظواهر الإجرامية المستحدثة التي أفرزها التطور التكنولوجي الحديث، والذي شمل مختلف مجالات الحياة الاجتماعية والاقتصادية والسياسية والثقافية. وقد أسهم هذا التحول الرقمي في إحداث تغييرات عميقة في بنية المجتمعات وأنماط تفاعلها، بما أفرز ما يُعرف بالثورة المعلوماتية.

ولا شك أن الظاهرة الإجرامية تتأثر بطبيعة التطور الذي تعرفه المجتمعات، ولا سيما في ظل التطور التكنولوجي، حيث إن هذا الأخير، رغم ما يقدمه من مزايا وخدمات إيجابية، قد أتاح في المقابل فرصًا جديدة لاستغلاله في ارتكاب أفعال إجرامية ذات طابع تقني معقد، يصعب ضبطها بالآليات التقليدية.

وفي هذا السياق، برزت الجريمة الإلكترونية كصورة حديثة من صور الإجرام، تمثل تهديدًا متزايدًا لأمن الأفراد والمؤسسات وحتى الدول، الأمر الذي يثير إشكالات قانونية متعددة تتعلق بمدى قدرة المنظومة القانونية على مواكبة هذه التحولات الرقمية المتسارعة.

وتعتمد هذه الدراسة على المنهج الوصفي التحليلي، من خلال تحليل مظاهر العلاقة بين التحول الرقمي وتطور الجريمة الإلكترونية، بهدف إبراز طبيعة هذه الظاهرة والتحديات القانونية التي تطرحها.

الكلمات المفتاحية: التحولات الرقمية، الجريمة الالكترونية، الثورة المعلوماتية، التطور التكنولوجي، الإجرام المستحدث.

Abstract :

This study examines cybercrime in light of rapid digital transformations shaping the contemporary world. Cybercrime has emerged as a key modern criminal phenomenon driven by technological development across social, economic, and political domains, leading to profound changes in societal structures and interactions within the information revolution era.

While technological advancement provides significant benefits, it also creates opportunities for new forms of sophisticated criminal activity that are difficult to address through traditional legal frameworks. In this context, cybercrime represents a growing threat to individuals, institutions, and states, raising important legal challenges regarding the adaptability of existing legal systems to digital developments.

The study adopts a descriptive and analytical approach to explore the relationship between digital transformation and the evolution of cybercrime, highlighting its nature and the legal issues it raises.

Keywords : Digital transformation, cybercrime, information revolution, technological development, modern criminality

جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

Volume 11 issue 3
N:64 June 2026

ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

مقدمة:

شهد العالم المعاصر تحولات رقمية متسارعة غير مسبوقة، نتيجة التطور الهائل في تكنولوجيا المعلومات[537] والاتصال، مما أدى إلى إدماج التكنولوجيا الحديثة في مختلف مجالات الحياة اليومية للأفراد والمؤسسات. وقد انعكس هذا التحول بشكل مباشر على الأنماط الاجتماعية والاقتصادية والثقافية، حيث أضحت الرقمنة أحد أبرز مظاهر العصر الحديث، بما وفرته من تسريع للتواصل وتسهيل للمعاملات وإتاحة فرص واسعة للابتكار والتطور. غير أن هذه التحولات، رغم إيجابياتها، أفرزت في المقابل تحديات جديدة، من أبرزها تنامي الجريمة الإلكترونية كظاهرة إجرامية مستحدثة تستغل الفضاء الرقمي والوسائل التكنولوجية الحديثة.

ومع التطور الهائل في عالم تكنولوجيا المعلومات ودخول وسائلها إلى شتى مجالات الحياة والذي أدى إلى تعاظم دورها بشكل غير محدود، فقد باتت الحواسيب الآلية[538] والتقنيات الالكترونية وشبكة الانترنت[539] لغة العصر التي لا يمكن الاستغناء عنها، وأصبح الاعتماد عليها كبيرا في أدق التفاصيل التي تتعلق بتسيير المرافق الاقتصادية والاجتماعية والعسكرية والطبية وغيرها (إبراهيم، 2003، ص. 7)، وقد أصبحت هذه الوسائل من الأهمية بمكان بحيث تعاظمت الضرورة في توفير أقصى درجات الحماية لما يحيط بها وذلك تجنبا لتعطيل سير تلك المرافق والمصالح الحيوية أو الاعتداء عليها بما يؤثر على المصالح الجوهرية في حياة الجماعة.

ويُلاحظ أن التطور الرقمي لم يقتصر على تسهيل حياة الأفراد، بل أسهم في إعادة تشكيل بنية المجتمع الحديثة، حيث أصبح الفضاء الرقمي مجالًا مفتوحًا لتبادل المعلومات والمعطيات، لكنه في الوقت ذاته أتاح فرصًا جديدة للاستغلال غير المشروع لهذه الوسائل، مما أدى إلى بروز أنماط إجرامية جديدة تتسم بالتعقيد والتطور المستمر، وتندرج ضمن ما يُعرف بالجريمة الإلكترونية، التي لم تعد تقتصر على الاعتداء على الأنظمة المعلوماتية فحسب، بل امتدت لتشمل صورًا متعددة من الإجرام التقليدي في قالب رقمي حديث.

فتختلف الجرائم الإلكترونية، المرتكبة باستخدام التكنولوجيا الحديثة والإنترنت، عن الجرائم التقليدية في وسائل ارتكابها ودوافعها وخصائصها المميزة. فقد شهد العالم تقدماً ملحوظاً في استخدام تقنيات المعلومات والاتصالات، بما في ذلك الحواسيب، والهواتف الذكية، ومنصات التواصل الاجتماعي، حتى أصبح التنافس بين الدول قائمًا على مدى استثمارها وإتقانها لهذه

---

537 يُشتق مصطلح "المعلومات" من كلمة "علم"، ويدل على المعرفة التي يمكن نقلها واكتسابها. ويعود أصل المصطلح في اللغات الأوروبية إلى الكلمة اللاتينية informare، التي تعني الإبلاغ والتوضيح. وقد تناول عالم الرياضيات الأمريكي Claude Shannon مفهوم المعلومات من منظور رياضي، معتبرًا أنها ترتبط بعملية الاختيار بين بدائل ممكنة وبدرجة عدم التحديد في الرسائل. وفي الاصطلاح، يمكن تعريف المعلومات بأنها الحقائق أو الرسائل أو الإشارات أو المفاهيم التي تُعرض بطريقة صالحة للإبلاغ أو التفسير، عبر الإنسان أو الوسائل التقنية، أو بأنها "الصورة المحوّلة للبيانات بعد تنظيمها ومعالجتها بطريقة تسمح باستخلاص النتائج".

ومن الناحية القانونية، اهتمت بعض التشريعات بتعريف المعلومات، مثل القانون الفرنسي رقم 82-652 الصادر بتاريخ 1982/07/26، الذي نص على أن المعلومات تشمل جميع صور الوثائق والبيانات والرسائل مهما كانت طبيعتها، وكذلك القانون الأمريكي المنظم للمعاملات التجارية الإلكترونية الصادر سنة 1999، الذي عرف المعلومات بأنها: "كل البيانات والكلمات والصور والأصوات والوسائل وبرامج الكمبيوتر، بما في ذلك البرامج المضغوطة، سواء على أقراص مرنة أو قواعد بيانات أو ما شابه ذلك".

للمزيد من المعلومات انظر: (ربيعي، 2016، ص. 6–7).

538 يعرف جهاز الحاسوب بكونه: "جهاز إلكتروني له القدرة على تلقي البيانات وتخزينها داخليا وتنفيذ مجموعة من التعليمات في صورة برنامج، كما يقوم بتأدية العمليات الحسابية والمنطقية المطلوبة على تلك العمليات، واستخراج النتائج". للتوسع أكثر راجع: (بني غازي، 2011/2010، ص. 28).

539 الإنترنت هو مجموعة مترابطة من شبكات الحاسوب حول العالم، حيث تتبادل الحواسيب المعلومات والبيانات فيما بينها عبر تبادل الحزم باتباع بروتوكول الإنترنت الموحد (IP). ويتكون مصطلح "الإنترنت" من كلمتين: Inter وتعني "بين"، وNet وتعني "شبكة"، أي "الشبكة البينية"، وشبكة الإنترنت هي شبكة ما بين عدة شبكات تُدار بشكل لا مركزي، بحيث لا تعتمد أي شبكة على الأخرى لتشغيلها، وتستخدم كل شبكة تقنيات حاسوبية وشبكية مختلفة. وما يجمع هذه الشبكات هو ارتباطها عبر بوابات تستخدم بروتوكول الإنترنت القياسي. ويقدم الإنترنت العديد من الخدمات مثل الشبكة العنكبوتية العالمية (الويب)، وتقنيات التخاطب، والبريد الإلكتروني، وبروتوكولات نقل الملفات (FTP). كما أصبحت الإنترنت اليوم ظاهرة اجتماعية وثقافية تؤثر في جميع أنحاء العالم، وأدت إلى تغيير المفاهيم التقليدية في مجالات اقتصادية واجتماعية وسياسية وفكرية (اليحياوي، 1999، ص. 2).

Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

التكنولوجيا. كما أدى هذا التطور إلى تراجع الحدود الجغرافية التقليدية، وأضحى معيار تقدم الدول مرتبطاً بقدرتها على مواكبة هذا التحول الرقمي والتفاعل معه بكفاءة عالية.

وبناءً عليه، تبرز أهمية دراسة الجريمة الإلكترونية في ظل التحولات الرقمية لفهم طبيعة هذا التطور الإجرامي، واستجلاء العلاقة بين التقدم التكنولوجي وتنامي هذا النوع من الجرائم، إضافة إلى استشراف أبرز التحديات القانونية والتقنية التي تطرحها.

وتتجلى إشكالية هذه الدراسة في مدى مساهمة التحولات الرقمية في تطور الجريمة الإلكترونية وظهور أنماط إجرامية مستحدثة، وإلى أي حد تستطيع المنظومة القانونية مواكبة هذا التطور المتسارع؟

كما تسعى هذه الدراسة إلى تحقيق مجموعة من الأهداف، من بينها تحديد مفهوم الجريمة الإلكترونية وخصائصها، وتحليل العلاقة بين التطور التكنولوجي وتنامي هذا النوع من الجرائم، إلى جانب إبراز أهم التحديات القانونية والتقنية المرتبطة بها، مع اقتراح بعض الآليات الكفيلة للحد من آثارها.

ولمقاربة هذه الإشكالية، سيتم الاعتماد على المنهج الوصفي التحليلي من خلال دراسة وتحليل العلاقة بين التحول الرقمي وتطور الجريمة الإلكترونية، وتفسير مختلف أبعادها القانونية والتقنية.

ولمعالجة هذه الإشكالية، سيتم تقسيم هذه الدراسة إلى محورين رئيسيين: يتناول الأول العلاقة بين التحولات الرقمية والجريمة الإلكترونية، بينما يخصص الثاني لبحث أهم الإشكالات القانونية التي تطرحها هذه الظاهرة في ظل التحول الرقمي.

المحور الأول: الجريمة الإلكترونية في سياق التحولات الرقمية

يُعد التحول الرقمي من أبرز مظاهر التطور التكنولوجي المعاصر، لما أحدثه من تغييرات عميقة مست مختلف جوانب الحياة الاجتماعية والاقتصادية والثقافية، الأمر الذي انعكس بشكل مباشر على طبيعة الظاهرة الإجرامية وأساليب ارتكابها. وفي هذا السياق، برزت الجريمة الإلكترونية كأحد أهم صور الإجرام المستحدث المرتبط بالبيئة الرقمية. ومن هذا المنطلق، سيتم التطرق في هذا المحور إلى طبيعة العلاقة بين التحولات الرقمية والجريمة الإلكترونية، من خلال بيان أثر التطور التكنولوجي في ظهور هذا النوع من الجرائم، ثم الوقوف على مفهوم الجريمة الإلكترونية وأبرز خصائصها.

أولًا: التحولات الرقمية و أثرها في تطور الجريمة

شهد التطور التكنولوجي خلال العقود الأخيرة تسارعًا ملحوظاً في مجال تكنولوجيا المعلومات والاتصال، حيث عرفت هذه المرحلة انتشاراً واسعاً للأدوات الرقمية وتوسعا كبيراً استخدام شبكة الإنترنت في مختلف مجالات الحياة. وقد أسهم هذا التطور في إعادة تشكيل أنماط التفاعل الاجتماعي والاقتصادي والثقافي، وأصبح عنصرا أساسيًا في تنظيم حياة الأفراد والمؤسسات.

ورغم ما حققه هذا التطور من إيجابيات متعددة، تتجلى في تسهيل المعاملات وتسريع تبادل المعلومات وتعزيز الابتكار، إلا أنه أفرز في المقابل آثارًا سلبية تمثلت في استغلال الفضاء الرقمي في أنشطة غير مشروعة، الأمر الذي أدى إلى بروز أنماط إجرامية جديدة تتسم بالتعقيد والتطور المستمر، وهو ما يعكس العلاقة الوثيقة بين التطور التكنولوجي وظهور الجريمة الإلكترونية.

أ- ضبط المفاهيم:

1. **تعريف التطور التكنولوجي:** يُعرف التطور التكنولوجي بأنه العملية المستمرة لتحسين وتطوير الأدوات والأنظمة التقنية، بما يسهم في زيادة الكفاءة الإنتاجية، وتيسير الاتصال، وتوسيع إمكانيات الوصول إلى المعلومات والخدمات في مختلف مجالات الحياة. ويرى Ellul (1964) أن التكنولوجيا لا تقتصر على مجرد الأدوات، بل تصبح عنصرًا مركزيًا في تنظيم النشاط البشري وعلاقات المجتمع، وتشمل التغيرات التي تصاحب التحولات الرقمية الحديثة.
2. **تعريف التكنولوجيا:** لقد تم تعريف التكنولوجيا technologie من الناحية اللغوية: بأنها كلمة يونانية الأصل تنقسم الى قسمين théchné ومعناها: الفن والحرفة، و logie وتعني: علم والدراسة، وتعد علما تطبيقيا يهتم بدراسة الإضافات والتطورات في العديد من المجالات، مثل الصناعة، والفنون، والحرف، وكل ما تحتاجه من وسائل وتقنيات مادية (scridan, 1999, p. 17).

جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال
Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

أما اصطلاحا فقد وردت في (المعجم الموسوعي الفرنسي) بأنها: "دراسة التقنيات الصناعية من وسائل ومناهج الصناعة التي تستعمل في إطارها عام أو في المجال الجزيئي" (Encyclopédique, 2001, p. 1841). ومن هنا تعتبر التقنية نتيجة حتمية من نتائج العلم، أي هي التطبيق الفعلي والبراغماتي لما وصل إليه العلماء من نظريات وقوانين علمية، لهذا فإن تطورها في علاقة وطيدة بالتطور العلمي والحضاري الذي بلغه الإنسان أو المجتمع، حيث تظهر لنا أن العلاقة بين العلم والتقنية هي علاقة سببية متلازمية (أودينة، 2025، ص. 510).

وفي هذا السياق، يعرفها جميل صليبا: "بأنها علم التقنيات، وهو يدرس الطرق التقنية من جهة ما هي مشتملة على مبادئ عامة أو من جهة ما هي متناسبة مع تطور الحضارة. ومن بين مسائلها دراسة تطور الطرق التقنية في أحد المجتمعات الإنسانية أو في المجتمع الإنساني العام (صليبا، 1982، ص. 333). ومنه، فالتكنولوجيا تُعد نتاجًا عمليًا للتوجه الفكري الإنساني البراغماتي، الذي يهدف إلى السيطرة على الطبيعة واستغلالها لصالح الإنسان، وذلك من خلال تحويل المعارف العلمية النظرية إلى تطبيقات عملية تُستخدم بطريقة عقلانية ومنظمة، خدمة لأغراض حيوية سوسيولوجية وحضارية. ويتجلى ذلك في المفهوم الوارد في المعجم الفلسفي عند لالاند، حيث تُعرّف التكنولوجيا باعتبارها علم التقنية الذي يدرس الطرق التقنية من حيث اشتمالها على مبادئ عامة، ومدى اتساقها مع الحضارة، كما يهتم بدراسة تطور الطرق التقنية داخل المجتمعات الإنسانية (لالاند، 2001، ص. 1429).

وبناءً على ما سبق، يمكن القول إن التكنولوجيا هو علم التقنية التي تساعد أسلوب الإنسان في التعامل مع الطبيعة، وتدعم استمرار حياته.

ومن المسلّم به أن التقدم العلمي والتكنولوجي أحدث تنوعا وتطورا في وسائل العيش وفي نمط الحياة بصفة عامة، وفي توفير العديد من الوسائل التي ساعدت الانسان في مختلف المجالات، وانطلاقاً من ذلك، يمكن بيان بعض الايجابيات التي توفرها التكنولوجيا فيما يلي:

- ساعدت التكنولوجيا العلمية الحديثة في ابتكار تقنيات جديدة لم تكن معروفة سابقًا، والتي تُسهم في كشف غموض العديد من الجرائم الخطيرة، سواء التقليدية أو المخفية، وكذلك الجرائم المرتكبة في الفضاء الافتراضي، مما يُسهل ضبط مرتكبيها.
- تساهم التكنولوجيا في تقديم العديد من الخدمات الجليلة لأجهزة العدالة الجنائية من خلال دخول التقنيات والوسائل العلمية المتطورة في عمل الشرطة واكتساحها لمجموع الإدارات والمؤسسات الأمنية والقضائية[540]، وذلك من خلال ما وفرته من آليات تقنية جد متطورة في تتبع أحداث الجريمة ومراقبة الجناة وتحديد أماكنهم مما يسهل إلقاء القبض عليهم.
- تبرز أهمية استخدام الأجهزة الأمنية للتكنولوجيا الحديثة في تسهيل عملها وتعزيز التنسيق بين إداراتها، كما تمكن من حفظ الأمن للفرد والمؤسسات وهو ما يساعد الجهات المعنية والأجهزة الأمنية على الخصوص في وضع السياسات والاستراتيجيات وإعداد الخطط والبرامج الاستباقية للرفع من جودة عملها في مجال تطويق الظواهر الإجرامية (موسى، 2002، ص. 74).
- ساهمت الثورة المعلوماتية بشكل كبير في تعزيز التعاون الدولي لمكافحة الظواهر الإجرامية، وخصوصًا الجرائم العابرة للحدود، وجرائم الإرهاب، والجريمة المعلوماتية.

3. **تعريف الجرائم المستحدثة:** تعددت التعاريف حول تحديد ماهية الجرائم المستحدثة، فقد عرفت على أنها: "عبارة عن ظواهر إجرامية أفرزتها تيارات إنحرافية، نتيجة تغير أنماط الحياة ووسائل العيش والرفاه، حيث برزت على الساحة الإجرامية في عهدنا هذا، وهي وليدة التحولات التي شهدتها الحياة المعاصرة في كل ماله من صلة بالمسائل الاجتماعية والاقتصادية والثقافية والسياسية وغيرها (الردايدة، 2013، ص.25). وعرفت أيضاً على أنها: "تلك الجرائم الحديثة التي ظهرت مؤخراً ولازمت التقدم

540 ومن بين الوسائل والتقنيات الحديثة والمتقدمة التي أفرزها التطور التكنولوجي نجد جهاز الحاسب الآلي والذي يلعب دورا كبيرا في تخزين المعلومات والبيانات ومعالجتها بدقة وسرعة فائقة، وتصنيفها وفهرستها، ناهيك عن الدور البارز الذي أصبح يحتله في المجال الأمني لاستخدامه في مكافحة الجريمة وضبط مرتكبها.

العلمي والتكنولوجي فأصبحت تشكل خطراً على المجتمع، ولذلك لابد من مواجهتها وردعها بأعنف الوسائل الفعالة للقضاء عليها" (شهاني، بدون سنة، ص. 291).

وعرفها آخرون بأنها: "أنماط من الجريمة تستخدم فيها التكنولوجيا الحديثة من أجل تسهيل عملية الإجرام مثل جرائم الإرهاب وجرائم العنف وجرائم غسل الأموال وجرائم الياقات البيضاء والجرائم الاقتصادية وأنماط الفساد الإداري والجرائم الكمبيوترية وجرائم تزوير بطاقات الإئتمان والجرائم الناتجة عن التعامل غير المشروع بجسد الإنسان وجرائم العنف العائلي وغيرها من أنماط الجرائم المستحدثة" (اليوسف، 1999، ص. 198).

ب: التطور التكنولوجي والتغيير في أساليب ارتكاب الجريمة

أدى التطور التكنولوجي والتقدم العلمي إلى تغيير جذري في أساليب ارتكاب الجريمة. فقد أخذت الجرائم أبعادًا جديدة في عصر العولمة نتيجة ظهور مجموعة من التكنولوجيات الحديثة، مثل تقنيات المعلومات والاتصال. ورافق ذلك العديد من الإنجازات العلمية التي أسهمت في تغيير نمط الحياة وفرضت أنماطًا جديدة من السلوك الفردي والجماعي في ظل الظروف الاجتماعية والاقتصادية والثقافية المتغيرة. ومن ثم، أصبح للتقنية الحديثة والتكنولوجيا بصفة عامة تأثير كبير على توسع وتطور الجريمة.

كما أن التطور التكنولوجي أدى إلى تحول نسبة كبيرة من الجرائم التقليدية إلى جرائم ذوي الياقات البيضاء، التي يقوم بها مجرم مثقف يستخدم بالإضافة إلى الأساليب التكنولوجية الحديثة ذكاءه وإمكانياته العلمية والعملية بدون إراقة الدماء (السيد، 1999، ص. 70-71).

وبناءً على ما سبق، يتضح أن التحولات الرقمية وما رافقها من تطور تكنولوجي متسارع قد أسهما بشكل كبير في إعادة تشكيل البيئة الإجرامية، سواء من حيث الوسائل أو الأساليب، مما أفرز أنماطًا جديدة من السلوك الإجرامي تتسم بالتعقيد والارتباط الوثيق بالفضاء الرقمي. وفي هذا الإطار، يستدعي فهم هذه الظاهرة التطرق إلى مفهوم الجريمة الإلكترونية وبيان خصائصها، باعتبارها الإطار المفاهيمي الذي يحدد ملامح هذا النمط المستحدث من الإجرام.

ثانيا: تعريف الجريمة الإلكترونية وخصائصها

من المُسلم به في السياسة الجنائية أن الجريمة ظاهرة اجتماعية تتطور بتطور المجتمعات، وتتأثر بالتحولات التي تعرفها مختلف المجالات، ولا سيما المجال التكنولوجي والرقمي. وفي هذا الإطار، برزت الجريمة الإلكترونية باعتبارها أحد أبرز مظاهر الإجرام المستحدث المرتبط بالفضاء الرقمي، حيث أصبحت تشكل تهديدًا حقيقيًا لأمن الأفراد والمؤسسات والدول، بالنظر إلى ما تنطوي عليه من اعتداءات تمس المعطيات والأنظمة المعلوماتية والمصالح المرتبطة بها.

وقد أدى التطور المتسارع لتكنولوجيا المعلومات والاتصال إلى تنامي هذا النوع من الجرائم واتساع نطاقه، الأمر الذي أفرز مجموعة من الإشكالات القانونية المرتبطة بطبيعتها ووسائل ارتكابها وصعوبة ضبط مرتكبيها، مما جعل الجريمة الإلكترونية تتميز بخصوصيات تجعلها تختلف عن الجرائم التقليدية من حيث الوسيلة والمحل والطابع العابر للحدود.

ومن ثم، فإن الإحاطة بهذا النوع من الإجرام تقتضي بداية الوقوف على مفهوم الجريمة الإلكترونية، ثم بيان أبرز الخصائص التي تميزها عن غيرها من الجرائم التقليدية.

أ- تعريف الجريمة الإلكترونية

رغم الأهمية البالغة التي يحظى بها مصطلح الجريمة الإلكترونية (Cybercrime) في الدراسات الأكاديمية المعاصرة التي تتناول التهديدات الرقمية، إلا أنه لا يوجد اتفاق موحّد حول تعريف دقيق يحدد ماهيتها وعناصرها وأشكالها المختلفة، الأمر الذي يفسره تعدد التسميات التي أطلقت عليها نجد تسمية الجريمة الالكترونية، جرائم الانترنت، جرائم الكمبيوتر، جرائم المعالجة الآلية للبيانات والمعطيات (شوقي، 2019، ص. 18).

ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639
Volume 11 issue 3
N:64 June 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

عرفها البعض بأنها: "كل سلوك غير مشروع يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات، أو هي كل نشاط غير مشروع موجه لنسخ او حذف او الوصول إلى المعلومات المخزنة داخل الحاسوب او التي تحول عن طريقه" (الشكري، 2008، ص. 113). حيث تم التركيز على موضوع الجريمة المعلوماتية.

بينما ذهب البعض الآخر لتقديم تعريف قائم على وسيلة ارتكابها يتمثل في أنها نشاط اجرامي تستخدم فيه تقنية الحاسب بطريقة مباشرة أو غير مباشرة بهدف تنفيذ العمل الاجرامي المقصود (وهيب، 2014، ص. 338).

فمنهم من يعرف الجريمة المعلوماتية كل أنها: "كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات بهدف للاعتداء على الأموال أو الأشياء المعنوية في كل فعل اجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق جني عليه او كسب يحققه الفاعل" (مومني، 2008، ص. 20).

كما عرفت بأنها: "تلك الجريمة التي يتم فيها استخدام الآليات والأسلحة الإلكترونية السابق ذكرها للقيام بهجوم إلكتروني بهدف تحقيق مكاسب مالية بالأساس" (Alnajim, 2009, p. 10–11).

وتعرف الجريمة الإلكترونية على أساس الاتفاقية العربية وقانون الجرائم الامريكية واتفاقية بودابست والاتحاد الدولي للاتصالات بأنها: " كل جناية أو جنحة ترتكب ضد فرد أو جماعة بدافع جرمي ونية الإساءة لسمعة الضحية أو جسده أو فكره أو ماله أو حياته سواء كان ذلك بطريقة مباشرة أم طريقة غير مباشرة باستخدام وسائل الاتصالات الحديثة الانترنيت"، ومع تزايد الانفتاح العالمي في مجتمع متحول من النظام الاجتماعي الطبيعي إلى النظام الاجتماعي المنفتح على العالم والأكثر تطوراً وسرعة واندماجاً بالعالم الخارجي والمجتمعات الداخلية المحلية بتقنيات ووسائل التواصل الاجتماعي المتاحة والمباحة وبحرية مطلقة دون قيود او ضوابط أو قوانين واضحة تحدد نطاق العقوبات الجرمية في حالة انتهاك الخصوصية أو الحقوق والحريات (عطية، 2009).

وبخصوص التعريف الدولي للجريمة الإلكترونية، فإنه يرتبط غالبًا بالغاية من استعمال المصطلح، إذ يُقصد به في معناه الضيق الأفعال التي تمس سرية البيانات وسلامتها وأنظمة الحاسوب، كما يمتد ليشمل استخدام النظم المعلوماتية لتحقيق مكاسب غير مشروعة أو إلحاق الضرر بالغير. وقد عرّف مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا سنة 2000 الجريمة الإلكترونية بأنها كل جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة معلوماتية أو داخلهما، وهو تعريف يتسم بالاتساع ليشمل مختلف الجرائم المرتكبة في البيئة الرقمية.

فمن خلال ما سبق ذكره، يمكننا إعطاء تعريف تقريبي للجريمة الإلكترونية أو المعلوماتية على أنها كل سلوك أو فعل إجرامي متعمد، مخالف للنصوص التشريعية، يتعلق بالبيانات الرقمية، ويكون الحاسوب و/ أو ملحقاته طرفا فيه بوصفه هدفا للجريمة أو وسيلة لها، سواء باستخدامه مباشرة أو بالاتصال به عن بعد بواسطة شبكة حاسوبية، ويترتب عليه خسارة لاحقة بالضحية أو حقق مكسبا غير مشروع للجاني.

ب- خصائص الجريمة الإلكترونية

تتميز الجريمة الإلكترونية بجملة من الخصائص التي تمنحها طبيعة خاصة تميزها عن الجرائم التقليدية، ويرجع ذلك أساسًا إلى ارتباطها بالبيئة الرقمية واعتمادها على الوسائل التقنية الحديثة. وقد أدى هذا الطابع التقني إلى بروز تحديات قانونية وأمنية جديدة، الأمر الذي دفع السياسة الجنائية إلى محاولة مواكبة هذه الخصوصيات من خلال وضع نصوص وآليات قانونية ملائمة لمواجهة هذا النوع من الجرائم المستحدثة.

Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

1. **حداثة الجريمة الإلكترونية:** تعد الجريمة الإلكترونية من الجرائم الحديثة والمتجددة كونها جاءت نتيجة لتطور تقني وتكنولوجي مستمر، مما يجعل وسائل تنفيذها وإخفاء نتائجها ومعالمها بشكل يصعب من اكتشافها في حد ذاتها أو اكتشاف فاعلها وتحديده بدقة.
2. **جريمة عابرة للحدود:** يمكن القول أن من أهم الخصائص التي تميز الجريمة الالكترونية هي تخطيها للحدود الجغرافية، فمن بين خصوصية هذا النوع من الجرائم هو إمكانية ارتكابها عن بعد، ومن ثم اكتسابها طبيعة دولية، أو كما يطلق عليها البعض الجرائم ذات طبيعة متعدية الحدود، فبعد ظهور شبكات المعلومات لم تعد الحدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة. وبعد ذلك من بين الأسباب التي تستدعي ضرورة تفعيل التعاون الدولي بشأن مكافحة الجريمة المعلوماتية.
3. **جريمة ناعمة:** بمعنى أن المجرم عند ارتكابه لأي فعل في جرائم الكمبيوتر، فإنه لا يحتاج إلى جهد بدني ووسائل مادية كالسكين أو الأسلحة النارية أو مواد سامة، وانما يعتمد على التقنية الحديثة وجهاز حاسوب، لان جرائمه تنتمي إلى جرائم الحيلة (يعيش، 2019، ص. 29)، والسبب في ذلك لكونها جرائم لا تترك أثراً لها، فلا توجد دماء أو جثة أو بصمات أو أداة إرتكاب الجريمة كالسكين أو الأسلحة، بالإضافة إلى طبيعة التطور التكنولوجي الذي يجعل من هذه الجرائم سهلة التنفيذ وعدم بذل أي جهد بدني يذكر مما يصعب أو يستحيل الوصول إلى الجاني (العبادي، 2018، ص. 94).
4. **خصوصية المجرم الالكتروني:** يتسم مرتكب الجريمة الإلكترونية غالبًا بدرجة من الذكاء والمهارة التقنية، إضافة إلى إلمامه بأنظمة الحاسب الآلي وآليات تشغيلها وتخزين البيانات واسترجاعها، وهو ما يفترض توفر قدر من المعرفة والخبرة التقنية. في المقابل، لا يشترط في مرتكب الجريمة التقليدية امتلاك مهارات تقنية متقدمة، إذ قد تصدر عن أشخاص بمستويات تعليمية وخبرات متباينة.
5. **جريمة صعبة الإثبات والاكتشاف:** الأصل في الجريمة إقامة الدليل وإسناده إلى المتهم، غير أنه وبفضل التطورات العلمية الحاصلة وظهور ما يسمى بالدليل الرقمي، يجعل إثبات هذا النوع من الجرائم أكثر صعوبة في الإثبات لأن الجاني مرتكب هذه الجريمة لا يترك وراءه أي أثر مادي خارجي ملموس يمكن فحصه، وهذا يعسر إجراءات اكتشاف الجريمة ومعرفة مرتكبها، إضافة إلى أنها جرائم مخفية وفي كثير من الأحيان لا يتم اكتشافها إلا صدفة -جريمة لا تتقيد بمكان وزمان معين-. وعليه تتميز جرائم الانترنت عن الجرائم التقليدية، بغياب الدليل وسهولة محو الآثار وهذا راجع إلى افتقاد وجود الآثار التقليدية للجريمة، وعدم كفاية القوانين القائمة (رستم، 1999، ص. 40).
6. **صعوبة إجراء التحقيق والمحاكمة:** أن أهم ما يميز الجرائم الإلكترونية، هو غموضها وصعوبة إثباتها والتحري عنها والتحقيق فيها، وذلك لسهولة إتلاف الأدلة وبالإضافة إلى صعوبة تحديد مكان ارتكاب الجريمة، وهذا ما يسبب إشكالية كبيرة في تحديد اختصاص المحكمة المختصة بالنظر في هذه الجرائم وإجراءات الضبط والتفتيش والملاحقة (الغافري، 2009، ص. 55).

يتضح مما سبق، أن التحولات التكنولوجية أسهمت بشكل مباشر في إعادة تشكيل الظاهرة الإجرامية من حيث طبيعتها ووسائل ارتكابها، إذ أفرزت نمطا جديدًا من الجرائم يقوم على البيئة الرقمية ويتسم بخصائص تميزه عن الجريمة التقليدية. ومن ثم، فإن دراسة الجريمة الإلكترونية لا تقتصر على تحديد مفهومها وخصائصها فحسب، بل تقتضي أيضا الوقوف على أبرز الإشكالات والتحديات التي تطرحها في ظل التحولات الرقمية المتسارعة.

المحور الثاني: الإشكالات القانونية للجريمة الإلكترونية في ظل التحول الرقمي

تُعد الجريمة الإلكترونية من أبرز صور الإجرام المستحدث التي أفرزتها التحولات الرقمية المتسارعة، حيث أضحت تطرح مجموعة من الإشكالات المعقدة على المستويين القانوني والإجرائي، بالنظر إلى ارتباطها ببيئة رقمية عابرة للحدود وسريعة التطور. وقد ترتب عن هذا الطابع الخاص صعوبات متعددة تتعلق بكيفية ضبطها، وإثباتها، وملاحقة مرتكبيها، فضلًا عن التحديات

جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال
Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

المرتبطة بتكييفها القانوني وتحديد الاختصاص القضائي الواجب التطبيق. ومن هذا المنطلق، سيتم التطرق في هذا المحور إلى أبرز الإشكالات القانونية والتقنية والإجرائية التي تثيرها الجريمة الإلكترونية في ظل التحول الرقمي.

أولاً: التحديات القانونية

تُثير الجريمة الإلكترونية جملة من الإشكالات القانونية المرتبطة أساسًا بطبيعتها العابرة للحدود، إذ غالبًا ما يتم ارتكاب الفعل الإجرامي عبر فضاء رقمي لا يعترف بالحدود الجغرافية، مما يؤدي إلى صعوبة تحديد الاختصاص القضائي والقانون الواجب التطبيق.

وفي هذا الصدد، سعت اتفاقية بودابست[541] حول الجريمة الإلكترونية إلى معالجة هذه الإشكالية من خلال وضع قواعد للاختصاص في المادة 22، غير أن التطبيق العملي يظل مرتبطًا بمدى انضمام الدول للاتفاقية وملاءمة تشريعاتها الداخلية (Council of Europe, 2001).

كما تبرز إشكالية التكييف القانوني للأفعال المستحدثة، حيث إن التطور السريع للتقنيات الرقمية يؤدي إلى ظهور صور إجرامية جديدة قد لا تكون منصوصًا عليها صراحة في التشريعات الوطنية، مما يثير إشكاليات تتعلق بمبدأ الشرعية الجنائية. وقد أكدت United Nations Office on Drugs and Crime أن التفاوت التشريعي بين الدول يشكل عائقًا أمام توحيد الجهود الدولية في مواجهة الجريمة السيبرانية (United Nations Office on Drugs and Crime [UNODC], 2013).

ويضاف إلى ذلك أيضاً التحدي المتعلق بتحقيق التوازن بين متطلبات مكافحة الجريمة وضمان حماية الحقوق والحريات الأساسية، خاصة الحق في الخصوصية وحماية المعطيات الشخصية، وهو ما حاولت تكريسه اللائحة العامة لحماية البيانات من خلال وضع معايير دقيقة لمعالجة البيانات الشخصية (European Parliament & Council, 2016). وهو ما يجعل مسألة التحديث التشريعي والتنسيق الدولي ضرورة ملحة لمواكبة تطور هذا النوع من الجرائم.

ثانياً: التحديات التقنية

تتميز الجريمة الإلكترونية باعتمادها على وسائل تكنولوجية متطورة ومتجددة باستمرار، مما يجعل مكافحتها رهينة بمدى توفر الخبرة التقنية والوسائل الرقمية الحديثة لدى أجهزة إنفاذ القانون. فالمجرمون يوظفون تقنيات التشفير وإخفاء الهوية والشبكات الافتراضية الخاصة، وهو ما يصعب عملية تعقبهم أو تحديد هوياتهم ومواقعهم الفعلية.

كما يتميز الدليل الرقمي بخصائص تقنية تجعله أكثر حساسية وهشاشة مقارنة بالدليل التقليدي، إذ يمكن نسخه أو تعديله أو إتلافه بسهولة، مما يستوجب اعتماد تقنيات دقيقة ومعايير صارمة في جمعه وحفظه وتحليله. وفي هذا السياق، تشير التقارير الدولية إلى أن الجرائم السيبرانية تتطور بوتيرة متسارعة تفوق أحيانًا قدرة الأجهزة الأمنية على مواكبتها، خاصة في الدول التي تعاني من ضعف الموارد التقنية والبنية التحتية الرقمية. وقد أكدت المنظمة الدولية للشرطة الجنائية (INTERPOL) [542] أن التطور

---

541 تعد معاهدة بودابست أولى المعاهدات الدولية المتعلقة بمكافحة جرائم الإنترنت، وقد أُبرمت في العاصمة المجرية بودابست بتاريخ 23 نوفمبر 2001 من طرف لجنة وزراء مجلس أوروبا خلال دورتها الـ109، بمناسبة انعقاد المؤتمر الدولي حول الجريمة الإلكترونية. وقد اعتُبر توقيع المعاهدة خطوة أولى من نوعها وغاية في الأهمية في مجال محاربة هذا النوع من الجرائم.

وقد وقعت على المعاهدة 26 دولة أوروبية، بالإضافة إلى كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية. وتوفر المعاهدة أسسًا لتعزيز الأمن العام وحماية المعلومات، حيث تضمنت 48 مادة موزعة على أربعة فصول.

دخلت الاتفاقية حيز التنفيذ في شهر يوليو 2004، وتعد وثيقة دولية ملزمة للدول الأطراف فيها. وقد تناولت الفصول الأربعة للاتفاقية تعريفات فنية لبعض المصطلحات ذات العلاقة، وتحديد الجرائم الإلكترونية الأكثر شيوعًا عالميًا، ووضع الإجراءات الوطنية الواجب اتخاذها، لا سيما على الصعيد الجنائي، للحفاظ على المعلومات المخزنة، بالإضافة إلى تنظيم التعاون الدولي، وتسليم المجرمين، وجمع البيانات وإجراء التحقيقات، إلى جانب مسائل الانضمام والانسحاب وتعديل المعاهدة والتشاور بين الأعضاء (فضل، 2007، ص. 430).

وتهدف الاتفاقية بشكل أساسي إلى توحيد عناصر القانون الموضوعي الجنائي المحلي والأحكام المتعلقة بالجرائم الإلكترونية، ومنح صلاحيات للقانون الإجرائي الوطني للتحقيق في هذا النوع من الجرائم ومتابعتها قضائيًا، إضافة إلى الجرائم الأخرى التي ترتكب عن طريق نظم الحاسوب أو التي تكون أدلتها على شكل إلكتروني. كما تهدف إلى إنشاء نظام سريع وفعال للتعاون الدولي لمكافحة الجرائم الإلكترونية (خبراء، 2001، ص. 04).

542 تعد المنظمة الدولية للشرطة الجنائية (الأنتربول) من أهم المنظمات الدولية التي أخذت على عاتقها مكافحة الجريمة المنظمة عبر الوطنية، وتعمل المنظمة تحت إشراف الأمم المتحدة وتمتلك شبكة من المكاتب المركزية. كما تقدم المنظمة المساعدة الجنائية الدولية من معلومات وبيانات لوكالات الشرطة الجنائية الوطنية، التي تساعد في التصدي للجرائم

المستمر للتقنيات الرقمية وتنامي استخدام أدوات إخفاء الهوية والتشفير يزيد من تعقيد عمليات التتبع والكشف عن مرتكبي الجرائم الإلكترونية، الأمر الذي يفرض تعزيز القدرات التقنية وتطوير آليات التعاون الدولي في هذا المجال.

وفي السياق ذاته، يؤكد المؤشر العالمي للأمن السيبراني الصادر عن الاتحاد الدولي للاتصالات أن تفاوت البنية التحتية الرقمية بين الدول يؤدي إلى اختلاف مستويات الجاهزية في مواجهة التهديدات السيبرانية (International Telecommunication Union [ITU], 2020)، وهو ما ينعكس سلبًا على فعالية الجهود الدولية الرامية إلى مكافحة هذا النوع من الجرائم.

ثالثاً: التحديات الإجرائية

إلى جانب التحديات القانونية والتقنية، تثير الجريمة الإلكترونية مجموعة من الصعوبات الإجرائية المرتبطة بآليات البحث والتحري وجمع الأدلة الرقمية، ذلك أن الإجراءات التقليدية المنصوص عليها في قوانين المسطرة الجنائية قد لا تكون كافية لمواكبة خصوصية البيئة الرقمية، خاصة فيما يتعلق بسرعة الوصول إلى البيانات الإلكترونية والحفاظ عليها قبل تعرضها للإتلاف أو التعديل.

كما أن فعالية المتابعة الجنائية في الجرائم الإلكترونية ترتبط بشكل وثيق بسرعة التعاون الدولي، نظرًا لإمكانية انتقال البيانات والمعلومات عبر عدة دول في وقت وجيز، الأمر الذي قد يؤدي إلى صعوبة تعقب الجناة أو تحديد أماكن وجودهم. وفي هذا السياق، أكدت تقارير مكتب الأمم المتحدة المعني بالمخدرات والجريمة United Nations Office on Drugs and Crime أن بطء إجراءات المساعدة القضائية الدولية قد يساهم في ضياع الأدلة الرقمية أو إتلافها (UNODC, 2013)، مما ينعكس سلبًا على فعالية المتابعة الجنائية.

ومن جهة أخرى، حاولت اتفاقية بودابست بشأن الجريمة الإلكترونية تجاوز هذه الإشكالات من خلال إقرار مجموعة من آليات التعاون الدولي السريع وتبادل المعلومات بين الدول الأطراف، بما في ذلك نظام الاتصال المستمر على مدار 7/24 (Council of Europe, 2001)، بهدف تسهيل إجراءات البحث والتحري وتعزيز فعالية مكافحة الجرائم الإلكترونية العابرة للحدود.

ويُعد التعاون الدولي في هذا المجال ضرورة ملحة بالنظر إلى الطبيعة العابرة للحدود التي تتميز بها الجريمة الإلكترونية، إذ لم يعد بإمكان دولة واحدة مواجهة هذا النوع من الجرائم بشكل منفرد، بل أصبح الأمر يقتضي تنسيق الجهود الأمنية والقضائية والتشريعية بين مختلف الدول، من خلال تبادل المعلومات والخبرات وإبرام الاتفاقيات الدولية وتعزيز آليات المساعدة القضائية المتبادلة.

ومن ثم، فإن مواجهة التحديات الإجرائية المرتبطة بالجريمة الإلكترونية تقتضي تحديث القواعد الإجرائية التقليدية، وتطوير وسائل البحث والتحري الرقمي، وتعزيز التعاون الدولي بما يضمن سرعة الوصول إلى الأدلة الرقمية وملاحقة مرتكبي هذا النوع من الجرائم بفعالية أكبر.

صفوة القول، تثير الجريمة الإلكترونية تحديات متشابكة على المستويات القانونية والتقنية والإجرائية، بالنظر إلى طبيعتها الرقمية وطابعها العابر للحدود. فالتطور المتسارع للتكنولوجيا يفرض على التشريعات الوطنية مواكبة مستمرة لمختلف صور الإجرام المستحدث، كما أن خصوصية الدليل الرقمي تستوجب اعتماد وسائل تقنية متطورة لضمان سلامته وفعالية الاعتماد عليه في الإثبات. وإلى جانب ذلك، فإن فعالية مكافحة الجريمة الإلكترونية تظل رهينة بمدى تعزيز التعاون الدولي وتنسيق الجهود الأمنية والقضائية بين الدول، بما يضمن مواجهة فعالة لهذا النوع من الجرائم في ظل التحولات الرقمية المتسارعة، مما يجعل التصدي لهذه الجرائم يتطلب تنسيقًا متكاملًا بين الجوانب القانونية والتقنية والإجرائية.

وفي تعقب المجرمين والقبض عليهم، لاسيما تلك العابرة للحدود ومرتكبها الذين يتنقلون عبر أقاليم دول متعددة ويشكلون جماعات إجرامية منظمة، وبالتالي يساعد نشاط الأنتربول في تحقيق الأمن وحماية المجتمع.

Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

خاتمة:

في ختام هذه الدراسة، يتبين أن التحولات الرقمية والتطور التكنولوجي المتسارع قد أسهما في بروز الجريمة الإلكترونية كأحد أبرز صور الإجرام المستحدث المرتبط بالفضاء الرقمي، حيث لم يعد الإجرام مقصورًا على الوسائل التقليدية، بل أصبح يعتمد على أدوات وتقنيات رقمية متطورة تتسم بالتعقيد وسرعة التطور.

وقد أظهرت الدراسة أن الجريمة الإلكترونية تتميز بخصائص تجعلها تختلف عن الجرائم التقليدية، خاصة من حيث الوسيلة والطبيعة والطابع العابر للحدود، وهو ما يفرز إشكالات قانونية وتقنية وإجرائية تتعلق بتحديد الاختصاص القضائي، وصعوبة جمع الأدلة الرقمية، ومواكبة التشريعات الوطنية لهذا التطور المتسارع.

كما خلصت الدراسة إلى أن مواجهة هذه الظاهرة لا يمكن أن تتم بالوسائل التقليدية وحدها، بل تتطلب مقاربة شاملة تقوم على تحديث الترسانة القانونية، وتعزيز القدرات التقنية للأجهزة المختصة، وتطوير آليات البحث والتحري الرقمي، إلى جانب تفعيل التعاون الدولي وتبادل المعلومات والخبرات بين الدول لمكافحة هذا النوع من الجرائم بفعالية أكبر.

وفي هذا الإطار، تبرز أهمية تعزيز الوعي المجتمعي بمخاطر الجريمة الإلكترونية، وترسيخ ثقافة الاستخدام الآمن للتكنولوجيا، باعتبارها عنصرًا مكملًا للجهود القانونية والأمنية في حماية المجتمع الرقمي في ظل التحولات الرقمية المستمرة.

قائمة المراجع

1. أندريه لالاند. (2001) موسوعة لالاند الفلسفية لبنان: منشورات عويدات.
2. أودينة، خالد. (2025). تأثير استخدام التكنولوجيا على الطفل: المخاطر والحلول. المجلة المغاربية للدراسات التاريخية والاجتماعية، 17(1).
3. بني غازي، محمد أحمد سيف. (2011/2010). التنظيم القانوني للعقود التجارية المُلزمة عبر الإنترنت: دراسة مقارنة (أطروحة دكتوراه، وحدة العقود والعطار، كلية العلوم القانونية والاقتصادية والاجتماعية بوجدة، جامعة محمد الأول.
4. جميل صليبا (1982) المعجم الفلسفي بيروت: دار الكتاب اللبناني.
5. ربيعي حسين. (2016). آليات البحث والتحقيق في الجرائم المعلوماتية (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة باتنة 1).
6. الردايدة، عبد الكريم. (2013). الجرائم المستحدثة واستراتيجية مواجهتها (الطبعة الأولى). الأردن: دار حامد للنشر والتوزيع.
7. رستم، هشام. (1999). الجرائم المعلوماتية: أصول التحقيق الجنائي الفني. مجلة الأمن والقانون، العدد 2. دبي: أكاديمية شرطة دبي.
8. السيد محمود وهيب. (1999). ظاهرة العولمة وانعكاساتها الأمنية. مجلة الأمن العام المجلة العربية لعلوم الشرطة، 164، القاهرة: مطابع الشرطة.
9. شيهاني، عمر. (بدون سنة). الجرائم المستحدثة وطرق التحري فيها. المجلة النقدية للقانون والعلوم السياسية، 12(1).
10. طالب، وهيب مشتاق. (2014). مفهوم الجريمة المعلوماتية ودور الحاسب في ارتكابها. مجلة العلوم القانونية والسياسية، 2(1)، جامعة ديالى، العراق.
11. العبادي، سلام عيسى. (2018). الإرهاب الإلكتروني: أخطاره وخصائصه وأهدافه ومكافحته (الطبعة الأولى).
12. عبد النبي، عادل يوسف الشكري. (2008). الجريمة المعلوماتية وأزمة الشرعية الجزائية. مجلة الكوفة، العدد (07)، مركز دراسات الكوفة، العراق.

13. عطية، طارق إبراهيم الدسوقي. (2009). الأمن المعلوماتي: النظام القانوني للحماية المعلوماتية. الإسكندرية: دار الجامعة الجديدة.
14. الغافري، حسين بن سعيد. (2009). السياسة الجنائية في مواجهة جرائم الإنترنت. القاهرة: دار النهضة العربية.
15. فضل، سليمان احمد (2007). المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية.
16. مجموعة خبراء (2001). التقرير التفسيري الاتفاقية الجريمة الالكترونية، مجلس أوروبا، بودابست.
17. موسى، مصطفى محمد. (2002). الجهاز الإلكتروني لمكافحة الجريمة. القاهرة: دار الكتب القانونية.
18. مومني، نهلا عبد القادر. (2008). الجرائم المعلوماتية (الطبعة الأولى). [مكان النشر غير مذكور]: دار الثقافة للنشر والتوزيع.
19. اليحياوي، يحيى. (1999). العولمة: أية عولمة (الطبعة الأولى). المغرب: إفريقيا الشرق.
20. يعيش، شوقي. (2019). الجريمة المعلوماتية: دراسة تأصيلية مقارنة (الطبعة الأولى). الوادي، الجزائر: مطبعة الرمال.
21. اليوسف، عبد الله عبد العزيز. (1999). التقنية والجرائم المستحدثة. ورقة علمية مقدمة إلى ندوة علمية بعنوان: الظواهر الإجرامية المستحدثة وسبل مواجهتها، تونس، 28–30 يونيو 1999.

المراجع الأجنبية

1. Alnajim, Abdullah M. (2009). Fighting internet fraud: Anti-phishing effectiveness for phishing websites detection (Doctoral thesis, Durham University). Durham University.
2. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). Strasbourg, France: Council of Europe.
3. Ellul, J. (1964). *The technological society*. Vintage Books.
4. European Parliament & Council. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). Official Journal of the European Union.
5. International Telecommunication Union (ITU). (2020). Global Cybersecurity Index 2020. Geneva, Switzerland: ITU.
6. Pradel, J. (1983). Conclusion du Colloque sur informatique et Droit pénal (p. 155). Paris, France: Cujas.
7. United Nations Office on Drugs and Crime (UNODC). (2013). Comprehensive Study on Cybercrime. Vienna, Austria: UNODC.