



الجريمة الإلكترونية في ضوء اتفاقية بودابست: الإطار المفاهيمي والتصنيفي Cybercrime in Light of the Budapest Convention: Conceptual and Typological Framework

د. سعيد مسعود الكثيري¹

جامعة ظفار - سلطنة عُمان

smalkathiri@du.edu.com

تاريخ القبول للنشر: 2025-12-15

تاريخ الاستلام: 2025-12-03

ملخص

أصبحت الجريمة الإلكترونية من أبرز التحديات التي تواجه المجتمع الدولي نظرًا لتطور تكنولوجيا المعلومات واتساع الفضاء الرقمي، وما نتج عنه من جرائم عابرة للحدود يصعب ضبطها بالآليات التقليدية، فقد تعددت أشكال هذه الجرائم لتشمل اختراق الأنظمة، وتزوير المعطيات، والاحتيال الإلكتروني وانتهاك الخصوصية واستعمال تكنولوجيا المعلومات في أنشطة إرهابية أو إجرامية منظمة وهو ما أدى إلى ضرورة البحث عن إطار دولي موحد لمعالجتها.

على المستوى الدولي، برزت عدة جهود من أجل وضع قواعد قانونية وآليات تعاون فعّالة، وقد مثّلت اتفاقية بودابست لعام 2001 (الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية) الإطار القانوني الأكثر أهمية، كونها أوّل معاهدة دولية تنظم هذا النوع من الجرائم، وتحدّد إجراءات البحث والتحري الرقمية، إضافة إلى وضع أسس للتعاون الدولي في مجال تبادل المعلومات وتسليم المجرمين، وقد انضمت إليها العديد من الدول خارج القارة الأوروبية، ممّا أكسبها طابعًا عالميًا.

رغم هذه الجهود لا تزال المعالجة الدولية تواجه صعوبات تتعلق باختلاف التشريعات الوطنية وببطء التعاون القضائي وصعوبة تحديد مرتكبي الجرائم في بيئة

¹ د. سعيد مسعود الكثيري



افتراضية لا تعترف بالحدود، ومع ذلك يُعدّ التعاون الدولي وتحديث التشريعات واعتماد معايير تقنية مشتركة الطريق الأمثل لمواجهة هذا التهديد المتزايد. الكلمات المفتاحية: الجريمة المعلوماتية، اتفاقية بودابست، الجرائم العابرة للحدود، الجريمة الإلكترونية.

Abstract:

Cybercrime has become one of the most pressing challenges facing the international community due to the rapid development of information technology and the expansion of the digital space. These advancements have given rise to transnational offenses that are difficult to control using traditional legal mechanisms. The forms of cybercrime have diversified to include system intrusions, data forgery, online fraud, privacy violations, and the use of information technologies for terrorist or organized criminal activities. This growing complexity has made it necessary to search for a unified international framework capable of addressing such threats.

At the international level, multiple efforts have emerged to establish legal standards and effective mechanisms for cooperation. The 2001 Budapest Convention (the Council of Europe Convention on Cybercrime) stands as the most significant legal instrument in this regard. It is the first international treaty dedicated to combating cybercrime, outlining digital investigative procedures and establishing rules for international cooperation, particularly in information exchange and extradition. Its adoption by several non-European states has reinforced its relevance and granted it a global dimension.

Despite these significant efforts, international responses still face obstacles, such as differences in national legislation, slow judicial cooperation, and the difficulty of identifying perpetrators in a borderless virtual environment. Nevertheless, enhanced international collaboration, updated legal frameworks, and the adoption of shared technical standards remain the most effective path forward to confront this rapidly escalating threat.

Keywords: Cybercrime, Budapest Convention, Transnational Crimes, Electronic Crime.

مقدمة

إن الثورة المعلوماتية التي يشهدها العالم في عصرنا هذا ساهمت وبشكل كبير في تطور معاملات الأفراد، وتسهيلها ذلك في شتى مجالات الحياة المختلفة؛ لاسيما بعد ظهور الانترنت التي وضعت العالم كله في قرية صغيرة نظرا لما ميزها من سرعة في تبادل البيانات والمعلومات.

إلا أن هذه الأخيرة ورغم ما تركته من آثار إيجابية نتيجة للتقنيات العالية التي تقوم عليها، إلا أنها ولدت جرائم جديدة اختلفت عن الجرائم التقليدية حيث

اتسمت بخطورتها الكبيرة نظراً لسهولة ارتكابها وأن آثارها ليست محصورة في النطاق الإقليمي لدولة بعينها، فضلاً على أن مرتكبيها يتسمون بالذكاء والدراسة في التعامل مع مجال المعالجة الآلية للمعطيات والإلمام بالمهارات والمعارف التقنية، ليس هذا فحسب بل إنها تستهدف محلاً من طبيعة خاصة ونعني بذلك المعلومات التي يحتوي عليها نظام المعالجة الآلية.

تعد الجريمة المعلوماتية من الظواهر الحديثة في عصر الثورة الرقمية، إذ ترتبط باستخدام التقنيات الحديثة ووسائل الاتصال الإلكترونية في ارتكاب الأفعال المخالفة للقانون. ومن هنا تبرز إشكالية البحث في السؤال عن ماهية الدققة لهذه الجرائم، فماذا يُقصد بالجريمة المعلوماتية؟ وما هي الأنواع والأشكال التي تتخذها، سواء كانت اختراقاً للأنظمة المعلوماتية، احتيالاً إلكترونياً، أو إساءة استخدام للبيانات الرقمية؟ كما تثير هذه الظاهرة تساؤلات مهمة حول استجابة الدول والمجتمع الدولي لهذه التحديات، وكيفية وضع الأطر القانونية والإجرائية الكفيلة بمكافحتها، وضمان حماية الأفراد والمؤسسات من أضرارها. وتتمثل أهمية هذا التساؤل في كونه يمس الأمن الرقمي والاقتصادي والاجتماعي، ويستلزم دراسة شاملة لتحديد الإجراءات الوقائية والتشريعية الفعالة لمواجهة الجريمة المعلوماتية والحد من انتشارها في ظل عالم رقمي متسارع التطور.

وهنا طرح الإشكال، فما المقصود بالجريمة المعلوماتية؟ وفيما تتمثل أنواعها؟ وكيف اهتمت الدول بمعالجة الجريمة المعلوماتية؟

المحور الأول: ماهية الجريمة المعلوماتية

إن الجرائم الناشئة في البيئة الرقمية جرائم حديثة، ارتبط مفهومها ولا يزال يرتبط بتكنولوجيا الحاسبات وتطوراتها المستخدمة في تشغيل وتخزين ونقل المعلومات في شكل إلكتروني، وكذا بتكنولوجيات وسائل الاتصال وشبكات الربط، لذلك فإنه من الضروري أن يكون أي تعريف لهذا النمط من الجرائم متسماً بالمرونة بما يسمح باستيعابه وتواكبه مع سائر التقنيات المبتكرة الراهنة والمستقبلية في مجال تكنولوجيا التعامل مع المعلومات إن الجرائم الناشئة في البيئة

الرقمية جرائم حديثة، ارتبط مفهومها ولا يزال يرتبط بتكنولوجيا الحاسبات وتطور المستخدمة في تشغيل وتخزين ونقل المعلومات في شكل إلكتروني، وكذا بتكنولوجيات وسائل الإتصال وشبكات الربط، لذلك فإنه من الضروري أن يكون أي تعريف سمياً لهذا النمط من الجرائم مت بالمرونة بما يسمح باستيعابه وتواكبه مع سائر التقنيات المبتكرة الراهنة والمستقبلية في مجال تكنولوجيا التعامل مع المعلومات (نعيم، 2013، ص 25).

ولقد تعددت تعريفات الجريمة المعلوماتية وتباينت فيما بينها ضيقاً واتساعاً وقد أسفر ذلك عن تعذر إيجاد مفهوم مشترك لظاهرة الجريمة المعلوماتية، وما يستتبع ذلك من تسهيل التوصل إلى الحلول المناسبة لمواجهتها. وسوف نحاول من خلال هذا المبحث الوصول إلى تعريف يتلاءم مع طبيعة الجريمة المعلوماتية (أولاً)، لننتقل بعد ذلك إلى خصائص هذه الجريمة (ثانياً).

أولاً: تعريف الجريمة المعلوماتية

تقع هذه الجريمة على الكمبيوتر وشبكة الانترنت ونظمها، وهي جريمة ناعمة ترتكب دون عنف، وفي الخفاء، ولا أثر خارجي لها، وممكن تدمير أي دليل عليها في ثانية واحدة أو عدة ثواني، ويكون اكتشافها في الغالب بالصدفة وكثيراً ما تحجم الضحية عن إبلاغ السلطات الحكومية عنها إما لعدم الثقة، أو لتفادي آثار العلم بها وانتشارها، وتأثير ذلك على زبائن المؤسسة وثقة الجمهور بها (مؤسسات مالية، مصرفية....) وإما لضعف ثقافة الضحية في هذا المضمار، وهذا ما جعل نسبة الجرائم المعلوماتية المكتشفة ضئيلة (فريد، 2016، ص 183).

وفي هذا الإطار يعرف الفقه للجريمة المعلوماتية نجد أن الاتجاهات تباينت في هذا السياق بين موسع لمفهومها وبين مضيق لها:

1-الاتجاه المضيق من مفهوم الجريمة المعلوماتية

عرف أنصار هذا الاتجاه الجريمة المعلوماتية بأنها: "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازماً لارتكابه من ناحية، وملاحقته وتحقيقه من ناحية أخرى" (Parker, 1973, P 517)، ومن خلال هذا

التعريف يتبين لنا أنه لا يكفي فقط أن تتوافر معرفة تكنولوجيا الحاسبات الآلية بدرجة كبيرة من أجل ارتكاب الجريمة المعلوماتية ولكن أيضا من أجل ملاحقتها ومتابعتها

والتحقيق فيها بمعنى لا بد أن يتوافر قدر كبير من العلم بهذه التكنولوجيا لدى الجناة والقائمون على معاينة وملاحقة مرتكبها (سفيان، 2011، ص 12).

وقد انتقد هذا التعريف لكونه يحصر الجريمة المعلوماتية في الحالات التي تتطلب قدرا كبيرا من المعرفة التقنية في ارتكابها، إذ أنه في كثير من الحالات يرتكب الفعل دون الحاجة إلى هذا القدر من المعرفة ورغم ذلك لا يمكننا إنكار أن هذه الأفعال تدخل في عداد الجرائم المعلوماتية كإتلاف البيانات المخزنة داخل النظام المعلوماتي، كما أن هذا الفعل مجرم قانونا عند معظم التشريعات (سفيان، 2011، ص 13).

2-الاتجاه الموسع لمفهوم الجريمة المعلوماتية

فعلى عكس من الاتجاه السابق فإن أنصار هذا الاتجاه يذهبون إلى التوسيع من مفهوم الجريمة المعلوماتية باعتبار أن مجرد مشاركة الحاسب الآلي في النشاط الإجرامي يصيب عليه وصف الجريمة المعلوماتية. وقد تباينت مواقف أنصار هذا الاتجاه في تعريف الجريمة المعلوماتية بحسب المعايير التي اعتمد عليها كل فريق في تعريف الجريمة المعلوماتية، وتباين مواقف الفقهاء أنصار هذا الاتجاه حسب نظرتهم إلى الدرجة التي يمكن أن تمتد إليها الجريمة المعلوماتية فيذهب فريق من الفقهاء إلى تعريف الجريمة المعلوماتية بأنها كل سلوك إجرامي يتم بمساعدة الحاسب الآلي. وفريق آخر يعتبرها أنها كل جريمة تتم في محيط الحاسبات الآلية، ومن هذه التعريفات ما جاء به الفقيه MERWE الذي يرى أن الجريمة المعلوماتية تتمثل في الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي (نعيم، 2013، ص 28).

ومن المعلوم أن التشريع العماني قد مر بمراحل متعددة في مكافحة الجريمة الإلكترونية، فبدأ بتجريمها من خلال إضافة فصل خاص بها وفق قانون

الجزء العماني رقم 1974/7 بموجب التعديل الذي تم بمرسوم سلطاني رقم 2001/72، بإضافة الفصل الثاني مكرر إلى الباب السابع تحت عنوان جرائم الحاسب الآلي، وفي ذات السياق تناولها قانون الاتصالات رقم 2002/30 وتعديلاته، وكذلك قانون المعاملات الإلكترونية 2008/69، ولكن نظراً للطبيعة الخاصة التي تتميز بها الجريمة الإلكترونية فقد اتجه المشرع إلى إصدار قانون خاص بالجرائم الإلكترونية وهو قانون مكافحة جرائم تقنية المعلومات رقم 2011/12.

كما ذهب البعض إلى القول بأن الجريمة المعلوماتية هي كل عمل أو امتناع يأتيه الإنسان إضراراً بمكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به باعتبارها من المصالح والقيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها (نعيم، 2013، ص 29).

وقد نصت المادة الثالثة من الفصل الثاني، من المرسوم السلطاني رقم 2011/12، على ما يلي:

يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد عن ستة أشهر وبغرامه لا تقل عن مائة ريال عماني ولا تزيد على خمسمائة ريال عماني أو بإحدى هاتين العقوبتين كل من دخل عمداً ودون وجه حق موقعا الكترونيا او نظاما معلوماتيا او وسائل تقنية المعلومات او جزء منها او تجاوز الدخول المصرح به اليها او استمر فيها بعد علمه بذلك فاذا ترتب على ما ذكر في الفقرة الاولى الغاء او تغيير او تعديل او تشويه او اتلاف او نسخ او تدمير او نشر او اعاده نشر بيانات او معلومات الكترونية مخزنة في النظام المعلومات او وسائل تقنية المعلومات او تدمير ذلك النظام او وسائل تقنية المعلومات او الشبكة المعلوماتية او الحاق ضرر بالمستخدمين او المستفيدين تكون العقوبة السجن مدة لا تقل عن ستة اشهر ولا تزيد عن سنة وغرامه لا تقل عن خمسمائة ريال عماني ولا تزيد على الف ريال عماني او بإحدى هاتين العقوبتين فاذا كانت البيانات او المعلومات المنصوص عليها في الفقرة الثانية شخصية تكون العقوبة السجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وغرامه لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة الاف ريال عماني او بإحدى هاتين العقوبتين

(المادة الثالثة من المرسوم السلطاني رقم 2011/12، المتعلق بمكافحة جرائم تقنية المعلومات).

ثانيا: خصائص الجريمة المعلوماتية

إن ظاهرة جرائم المعلوماتية ظاهرة جديدة مستحدثة أصبحت تدق ناقوس الخطر لتنبه مجتمعات العصر الراهن لحجم المخاطر و هول الخسائر الناجمة عن جرائم المعلوماتية التي تستهدف الاعتداء على المعطيات بدلائلها التقنية الواسعة (بيانات ومعلومات و برامج بكافة أنواعها)، وبما أن الجريمة المعلوماتية هي جريمة ذات ارتباط بجهاز الحاسوب و شبكة الانترنت أضفى عليها مجموعة من خصائص والسمات المميزة لهذه الجريمة عن الجرائم التقليدية هي (نهلا ، 2008 ، ص 50):

1- الجريمة المعلوماتية جريمة عابرة للحدود

الجريمة المعلوماتية تتصف غالبا بالطابع الدولي، ذلك لأن الطابع العالمي لشبكة الانترنت وما يرتبه من نتائج جعل معظم دول العالم في حالة اتصال دائم على الخطر، يسهل ارتكاب الجريمة من دولة إلى دولة أخرى، فالجريمة المعلوماتية لا تعترف بالحدود بين الدول والقارات لذلك فهي جريمة عابرة للقارات، فهي تعتبر شكلا جيدا من أشكال الجرائم العابرة للحدود الإقليمية بين ول العالم كافة، إذ يمكن من خلال النظام المعلوماتي ارتكاب العديد من الجرائم كالتعدي على قواعد البيانات خالد، 2008، ص 44).

هذه الطبيعة التي تتميز بها الجريمة المعلوماتية كونها عابرة للحدود خلقت العديد من المشاكل حول تحديد القانون الواجب تطبيقه بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام (نهلا ، 2008 ، ص 51).

2- صعوبة اكتشاف الجريمة المعلوماتية وإثباتها

تقع الجريمة المعلوماتية في بيئة افتراضية تقنية لا تترك أية آثار محسوسة، إذ يغلب عليها أنها تتم في الخفاء لأن الجناة يعمدون في كثير من الأحيان إلى إخفاء نشاطهم الجرمي عن طريق تلاعبهم بالبيانات، والذي يتحقق أحيانا إن لم نقل في

الغالب في غفلة من المجني عليهم. كما أنه من السهل عليهم تدمير الأدلة ومحوها مما يعقد أمر كشف الجريمة وإثباتها، وإذا ما قورنت حالات اكتشاف الجريمة المعلوماتية على ضوء ما يتم اكتشافه من الجرائم التقليدية فإن عددها قليل، فمعظم الجرائم المعلوماتية تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابه، ذلك أن هذا النمط الإجرامي لا يحتاج إلى عنف أو جثث أو اقتحام وإنما هي معلومات وبيانات تغير أو تعدل أو تمحى كلياً أو جزئياً من السجلات المخزونة في ذاكرة الحاسب الآلي فلا تترك أثراً خارجياً مرئياً أو ملموساً فهي كما وصفها بعض الفقهاء بأنها جريمة هادئة بطبيعتها لا تتطلب سوى عدد من اللمسات الخاطفة على لوحة المفاتيح حتى تؤدي إلى اختراق المعلومات المخزنة في الحاسب الآلي وهتك سريتها ومحوها أو تشويهها أو تعطيل الأنظمة التي تحتويها فالجريمة المعلوماتية من الجرائم المستحدثة التي لا تترك شهوداً يمكن الاستدلال بأقوالهم ولا أدلة مادية يمكن فحصها وإنما تقع في بيئة إلكترونية يتم فيها نقل المعلومات وتداولها بواسطة نبضات إلكترونية غير مرئية (نعيم، 2013، ص 33).

3- قلة الإبلاغ عن الجريمة المعلوماتية

لا يتم في الغالب الإبلاغ عن جرائم الانترنت إما لعدم اكتشاف الضحية لها وإما خشيته من التشهير، لذا نجد أن معظم جرائم الانترنت تم اكتشافها بالصدفة، بل وبعد وقت طويل من ارتكابها، زد ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها، فالرقم المظلم بين حقيقة هذه الجرائم المرتكبة والعدد الذي تم اكتشافه هو رقم خطير، وبعبارة أخرى، الفجوة بين عدد هذا الجرائم الحقيقي وبين ما تم اكتشافه فجوة كبيرة (نهلا، 2008، ص 54، 55).

4- الجريمة المعلوماتية جريمة مستحدثة

تعد الجرائم الإلكترونية من أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل أخطاراً جسيمة في ظل العولمة، فلا غرابة أن تعتبر الجرائم المعلوماتية سواء التي تتعرض لها أجهزة الكمبيوتر أو تلك التي تسخر تلك الأجهزة في ارتكابها من الجرائم

المستحدثة، حيث أن التقدم التكنولوجي التي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة، بحيث يتجاوز هذا التقدم بقدراته وإمكاناته أجهزة الدولة الرقابية، بل أنه اضعف من قدراتها في تطبيق قوانينها، بالشكل الذي أصبح يهدد أمنها وأمن مواطنيها (خالد محمود، 2011، ص 370).

المحور الثاني: أنواع الجريمة المعلوماتية

أولاً: جريمة التحويل الالكتروني غير المشروع للأموال عبر شبكة الانترنت

بعد انتشار مفهوم التجارة الالكترونية في السبعينات استفادت من مزاياها الكثير من شركات الأعمال وأصبح من السهل الاستيلاء على بطاقات الائتمان وتم سرقة مئات الألوف من أرقام البطاقات في يوم واحد من خلال شبكة الانترنت ومن ثم بيع هذه المعلومات للآخرين، يتعدى الأمر المخاطر الأمنية التي تتعرض لها بطاقات الائتمان فنحن في بداية ثورة نقدية تعرف باسم النقود الالكترونية التي يتنبأ لها أن تكون مكملية للنقود الورقية، وأن هناك الأسهم والسندات الالكترونية المعمول بها في دول الاتحاد الأوروبي التي اقر الكونجرس الأمريكي التعامل بها عام، 1990 فالتعامل معها من خلال الانترنت سيواجه خطر أمنية ولا شك (عبد الفتاح، ص 106).

ثانياً: التزوير المعلوماتي

التزوير يقوم على تغيير الحقيقة بقصد الغش في محرر بطريقة بينها القانون، تغيير يؤدي إلى إلحاق الضرر بالغير (محمد صبحي، 2005، ص 3). وتغيير الحقيقة سواء كان في محرر رسمي أو عرفي، يمكن تصور حصوله في محررات في نطاق المعلوماتية، وهذه الحالة تسمى جريمة التزوير المعلوماتي، وهو ينصب على مخرجات الحاسب الآلي، عن طريق تغيير الحقيقة على الشرائط والمستندات طالما أن التغيير ذاته قد طال البيانات الموجودة في جهاز الحاسب الآلي، شرط حصول ضرر والذي يتمثل في اهتزاز الثقة المفترضة في المحررات الرسمية (عبد الفتاح، ص 146).

حيث تجاوز التزوير الإلكتروني التزوير الورقي أن كان هو نفسه في المفهوم الوظيفي لناحية تحريف الحقائق والبيانات، فهو لم يعد مجرد حك في مضمون السند وتعديل بعض كلماته، أو حذف بعض عباراته، بل أصبح يتطلب التعامل مع تقنيات المعلوماتية وذلك عن طريق محو بيانات وإضافة بيانات أخرى مكانها، ودمج بيانات مما يصعب من إمكانية كشفه، شأنه شأن سائر الأعمال الجرمية التي ترتكب في مجالا لمعلوماتية (بولين، 2009، ص 176، 177).

ثالثا: السرقة المعلوماتية

إن الصورة الغالبة لسرقة المال المعلوماتي المعنوي إن أمكن الوصف تأخذ صورة اختلاس البيانات و المعلومات والإفادة منها باستخدام السارق المعلومات الشخصية، مثل الاسم، اللقب، العنوان الأرقام السرية الخاصة بالمجني عليهم، والاستخدام غير الشرعي لشخصية المجني عليه ليبدأ بها عملية السرقة المتخفية عبر الانترنت بحيث تؤدي بالغير إلى تقديم الأموال الإلكترونية والمادية إلى الجاني عن طريق التحويل البنكي (محمد أمين، 2007، ص 138).

تتفق السرقة المعلوماتية مع السرقة التقليدية في أوجه كثيرة إلا أن اختلافهما يكون في محل السرقة ذاته، فمحل السرقة التقليدية مال منقول مملوك للغير، أما محل السرقة عبر الانترنت فهي المعلومات والبيانات المعالجة إلكترونيا (خديجة، 2013، ص 10).

رابعا: التجسس الإلكتروني

يعرف سلوك التجسس فعل ايجابي قوامه الكشف واستظهار الحقائق المخفية، ولكنه كشف واستظهار غير مشروع، إما بوسائله أو غاياته، وهو لذلك فعل لا يقره الشارع ويفرد لمرتكبه العقوبة الجزائية الرادعة دون تهاون انسجاما مع روح التشريع، وإدراكا لعظم خطورة هذا السلوك (جلال، 2010، ص 87).

فالحاسب الآلي خزانة بلا أبواب أو مستودع بلا حارس، ولذلك استطاع أطفال لم يتجاوزوا العاشرة من عمرهم التجسس على وزارة الدفاع الأمريكية، لأن اختراق شبكات المعلومات أمر يسير لمن يتوصل من خلال التجسس أو من خلال

الصدفة البحتة على كيفية هذا الاختراق ولذلك فإن الدول يجب أن تحمي معلوماتها ضد كل اختراق لها ولا انتهكت أسرارها لاسيما في المجال العسكري والأسرار السياسية وأسرار نظام الحكم داخل الدول، ففي المجال العسكري فأية دولة كانت تضع خططها العسكرية في عشرات المجلدات أن تضعها الآن في دعامه لا يزيد وزنها عن عشرين جراما بحيث يستطيع مخترقو الشبكات إذا وصل إلى هذه المعلومات أن يدمروا الأنظمة الدفاعية والعسكرية في الدول الأخرى (محمد محمد، 2001، ص 87).

أما الأسرار السياسية وأسرار نظم الحكم داخل الدول فيدخل في ذلك أيضا إدخال المعلومات المتعلقة بوثائق الدولة في الحاسب الآلي وعندئذ تقوم الدول الأخرى في الوصول إلى هذه البيانات المعالجة الكترونيا من أجل الوقوف على أسرار الدولة ونظام الحكم فيها (جلال، 2010، ص 265).

المحور الثالث: الجهود الدولية المبذولة التي اهتمت بمعالجة الجريمة المعلوماتية
لجأت أغلب الدول والأمم المتحدة والمنظمات الدولية إلى إيلاء اهتمام كبير بموضوع الجريمة المعلوماتية، نظراً لما تمثله من تهديد للأمن الرقمي والاقتصاد العالمي. وقد تجسد هذا الاهتمام من خلال مجموعة من الاتفاقيات الدولية المهمة، مثل اتفاقية برن لحماية الحقوق الأدبية والفنية، ومعاهدة الويبو، واتفاقية تربس، التي وضعت أسساً قانونية لحماية الملكية الفكرية في الفضاء الرقمي وتنظيم التعامل مع الانتهاكات الإلكترونية على المستوى الدولي (أحمد، 2002، ص 01، 02).

وتسعى هذه الجهود الدولية إلى تحقيق توازن بين مكافحة الجرائم المعلوماتية وضمان احترام حقوق الإنسان والحريات الأساسية في الفضاء الرقمي. كما تشجع على التعاون الإقليمي والدولي، وتطوير قدرات أجهزة الأمن والقضاء في التعامل مع القضايا الإلكترونية المعقدة، بما يعزز قدرة الدول على التصدي للجرائم السيبرانية بفعالية ويضمن استقرار نظم المعلومات وحماية البنى التحتية الحيوية.

أولاً: المعاهدات العامة

1- إتفاقية برن

تعد اتفاقية برن لحماية الحقوق الأدبية والفنية، الموقعة بتاريخ 1971 في سويسرا، حجر الأساس في إطار الحماية الدولية لحق المؤلف، وقد وقعت عليها أكثر من 120 دولة، ما جعلها المرجع القانوني الرئيسي لضمان احترام حقوق المؤلفين على المستوى العالمي. وتنص الاتفاقية على حماية المصنفات الأدبية والفنية من أي استغلال غير قانوني، سواء تمثل في النسخ أو العرض أو الأداء أو التوزيع، كما تفرض على الدول الأعضاء سن تشريعات محلية تتوافق مع المعايير الدولية، وتهدف الاتفاقية إلى توفير توازن بين حقوق المؤلفين في حماية أعمالهم وتحفيز الابتكار والإبداع، وبين مصلحة الجمهور في الوصول إلى المعرفة والثقافة، وهو ما يعكس رؤيتها الشاملة لدور الملكية الفكرية في التنمية الثقافية والاقتصادية.

2- معاهدة الويبو

تعتبر منظمة الويبو منظمة عالمية غير حكومية متخصصة في الملكية الفكرية، ويقع مقرها في جنيف، وقد تأسست بموجب اتفاقية ستوكهولم المبرمة عام 1967 ودخلت حيز التنفيذ عام 1970. وتتمثل مهمة المنظمة في وضع أطر قانونية دولية لحماية الملكية الفكرية بمختلف أشكالها، سواء الأدبية أو الصناعية، من خلال مراقبة الحقوق، وتقديم التوجيه الفني، وتسهيل التعاون بين الدول الأعضاء. كما توفر الويبو الدعم للدول النامية لتطوير تشريعاتها الوطنية بما يتماشى مع المعايير الدولية، إضافة إلى إدارة تسجيلات وبراءات الاختراع والعلامات التجارية والتصاميم الصناعية على المستوى العالمي. ويُعد عمل المنظمة محوريًا في مواجهة التحديات الناتجة عن التطور التكنولوجي وانتشار الجرائم السيبرانية المرتبطة بالانتهاكات الفكرية، مما يعزز الأمن القانوني للمبدعين والمستثمرين على حد سواء.

3- اتفاقية ترينس

تمثل اتفاقية الجوانب المتعلقة بالتجارة وحقوق الملكية الفكرية (ترينس) خطوة متقدمة في مجال حماية الملكية الفكرية، خاصة مع انتشار السطو

الإلكتروني على الأعمال الفنية والإبداعية في ظل الثورة الرقمية، وقد أبرمت الاتفاقية سنة 1994 ضمن إطار منظمة التجارة العالمية، وركزت على توحيد المعايير الدولية لحماية حقوق الملكية الفكرية، بما في ذلك حقوق المؤلف وبراءات الاختراع والعلامات التجارية والسر التجاري. كما تضمنت الاتفاقية آليات ملزمة للدول الأعضاء لفرض العقوبات على الانتهاكات، وتشجيع التدابير القانونية الفعالة لمكافحة القرصنة الإلكترونية والتقليد غير القانوني، ومن خلال هذه الاتفاقية يسعى المجتمع الدولي إلى خلق بيئة تجارية وتقنية عادلة تحمي المبدعين وتدعم الابتكار، مع ضمان التوازن بين مصالح المبدعين وحقوق المستهلكين في الوصول إلى المعرفة والإبداع (محمد الزعبي، 2002، ص5).

ثانياً: المعاهدات الخاصة (معاهدة بوادست)

شهدت العاصمة المجرية بودابست في أواخر عام 2001 اعتماد أولى المعاهدات الدولية لمكافحة الجرائم المعلوماتية، وهو ما شكل نقطة محورية في بلورة التضامن والتعاون الدولي لمواجهة هذه الظاهرة المتنامية التي أصبحت تهدد الأملاك والأفراد على حد سواء، وقد شارك في صياغة هذه المعاهدة عدد كبير من الخبراء القانونيين التابعين لمجلس أوروبا، بالتعاون مع دول أخرى أبرزها الولايات المتحدة الأمريكية، بعد سلسلة من المشاورات المكثفة بين الحكومات وأجهزة الشرطة وقطاع تقنية المعلومات على مستوى العالم، وانتهى هذا الجهد إلى توقيع الاتفاقية بتاريخ 23 نوفمبر 2001 من قبل 30 دولة لتفتح الباب لاحقاً أمام دول خارج مجلس أوروبا، مثل كندا واليابان والولايات المتحدة وجنوب أفريقيا، للانضمام إليها ما يعكس طبيعتها العالمية وأهميتها العابرة للحدود (هدى، 1992، ص6).

وتتكون هذه الاتفاقية من 48 مادة أكدت على ضرورة اتخاذ الدول لتدابير تشريعية فعالة لمكافحة جرائم الحاسوب وحماية أمنها الوطني، كما تضمنت مجموعة من التوصيات لدول الأعضاء لتطوير سياسات محكمة لمواجهة هذا النوع من الجرائم السيبرية، وركزت الاتفاقية على توحيد المعايير القانونية وتسهيل

التعاون بين السلطات القضائية والأمنية، بما في ذلك تبادل المعلومات وتسهيل جمع الأدلة الرقمية والتنسيق في التحقيقات عبر الحدود، ومن خلال هذا الإطار القانوني أسهمت اتفاقية بودابست في تعزيز القدرة الدولية على مواجهة التهديدات الرقمية وحماية الحقوق الرقمية للأفراد والمؤسسات، مع تعزيز الوعي الدولي بخطورة الجرائم المعلوماتية وضرورة مكافحتها بطريقة متكاملة ومنسقة.

ومن العناصر الأساسية لاتفاقية بودابست (خالد، محمد، 2009، ص 7):

- 1- أهمية التدابير التشريعية الموضوعية أي نصوص التجريم الموضوعية لهذا المجال
- 2- أهمية التدابير التشريعية الإجرائية المتلائمة مع طبيعة الجرائم الإلكترونية
- 3- أهمية تدابير التعاون الدولي و الإقليمي في مكافحة هذه الجرائم و الانطلاق أساسا من الانجازات و الجهود الدولية .

تتكون اتفاقية بودابست لمكافحة الجريمة المعلوماتية من أربعة فصول رئيسية تمثل هيكلها القانوني المتكامل، حيث يُقدّم كل فصل مجموعة من الأحكام التي تغطي جوانب مختلفة للجرائم السيبرانية، ويخصص الفصل الأول لتعريف المصطلحات الأساسية بما يضمن وضوح المفاهيم وتوحيد الفهم بين الدول الأعضاء.

أما الفصل الثاني فهو بعنوان "الخطوات الواجب اتخاذها على الصعيد الوطني"، وينقسم إلى ثلاثة أقسام: الأول (المواد 2 إلى 13) يعالج النصوص الموضوعية للجرائم المعلوماتية ويحدد طبيعة الأفعال المجرّمة، الثاني (المواد 14 إلى 21) يركز على القواعد الإجرائية اللازمة للتحقيق والملاحقة القضائية، أما القسم الثالث (المادة 22) فيتعلق بالاختصاص القضائي، بما يحدد نطاق السلطات الوطنية في معالجة هذه الجرائم.

ويُكرس الفصل الثالث للتعاون الدولي، ويضم المواد من 23 إلى 35، حيث يشمل آليات تبادل المعلومات والتنسيق بين السلطات القضائية والشرطية على الصعيد العالمي لمواجهة الجرائم السيبرانية العابرة للحدود، أما الفصل الرابع، فيتضمن الأحكام الختامية (المواد 36 إلى 48)، التي تنظم الدخول حيز التنفيذ،

الانضمام إلى الاتفاقية، وتطبيقها بما يتوافق مع القوانين الوطنية لكل دولة عضو. ويعكس هذا الهيكل التنظيمي الشامل التوازن بين النصوص الموضوعية، الإجراءات الوطنية، والتعاون الدولي، بما يضمن فعالية مكافحة الجرائم المعلوماتية وحماية الحقوق الرقمية على الصعيد العالمي (يوسف، 2012، ص 17).

ثالثاً: الإجراءات الجنائية الجديدة لمكافحة الجريمة الإلكترونية في اتفاقية بودابست

تُعد اتفاقية بودابست لمكافحة الجريمة المعلوماتية (2001) علامة فارقة في القانون الدولي، إذ وضعت إطاراً متكاملاً للإجراءات الجنائية الحديثة لمواجهة الجرائم الإلكترونية، مبنية على مبدأ أساسي هو التزام الدول الأعضاء بدمج هذه الإجراءات في تشريعاتها الداخلية وأنظمتها القضائية، هذا الالتزام يعكس إدراك المجتمع الدولي للطبيعة العابرة للحدود للجرائم المعلوماتية، والتي لا يمكن مكافحتها بفاعلية إلا من خلال تنسيق تشريعي وإجرائي موحد بين الدول (بولين، 2009، ص 450).

أول هذه الإجراءات هو الحفظ السريع للمعطيات المخزنة (المواد 16 و 17)، الذي يهدف إلى ضمان الاحتفاظ بالمعلومات الرقمية وحمايتها من التلف أو فقدان، نظراً لأهمية هذه البيانات كأدلة رئيسية في التحقيقات الإلكترونية. ويعتبر هذا الإجراء من أصعب الإجراءات التطبيقية، بسبب الطبيعة المؤقتة للأدلة الرقمية وسرعة تغيرها أو محوها. لذلك، سمحت المادة 16 للسلطات الوطنية بإصدار أوامر قضائية أو إدارية للحفظ الفوري للبيانات، لضمان عدم فقدان المعلومات الضرورية لكشف الجريمة، وهو ما يعكس أهمية التوازن بين فعالية التحقيق وحماية حقوق الأفراد وخصوصيتهم الرقمية (الحلو، 2015، ص 35).

ثانياً، تناولت الاتفاقية تجميع المعلومات الخاصة بالمشاركين، مثل أرقام الهواتف وعناوين البريد الإلكتروني وعناوين المواقع، باعتبارها أدوات حاسمة لتحديد هوية مرتكبي الجرائم الإلكترونية، ويبرز هنا التحدي القانوني المتمثل في

حماية الخصوصية، إذ يجب أن يتم جمع هذه المعلومات وفق إجراءات رسمية وإذن قضائي، لضمان عدم انتهاك الحقوق المدنية أثناء التحقيق.

ثالثاً نصت الاتفاقية على التفتيش المعلوماتي، الذي يتطلب إذنًا رسميًا للوصول إلى البيانات في مواقع محددة، ويهدف إلى جمع الأدلة دون المساس بالحقوق الأساسية للأفراد. ويرتبط بهذا أيضًا إجراء التنصت، وهو أداة جديدة لمكافحة الجريمة المعلوماتية، تسمح باعتراض المراسلات أو تسجيل المكالمات أو التقاط الصور، ولكن مع ضرورة الحصول على موافقة السلطات القضائية، لضمان استخدامه بطريقة قانونية ومحدودة، ويظهر هذا التقدم التشريعي كيفية توافق القوانين مع التطورات التكنولوجية الحديثة لضبط الجرائم الرقمية دون تجاوز القانون.

رابعاً، شددت الاتفاقية على التعاون الدولي (المادة 23 وما بعدها) باعتباره الركيزة الأساسية لتفعيل الإجراءات السابقة، عبر تبادل المعلومات والأدلة بسرعة وفعالية، ووضع آليات لتسليم المجرمين، وأحكام خاصة بالجرائم المعلوماتية العابرة للحدود، ويعكس هذا البند أهمية التنسيق العالمي لمكافحة الجريمة السيبرانية، خصوصاً أن المجرمين غالباً ما يرتكبون جرائمهم من دول مختلفة عن ضحاياهم، مما يجعل التعاون الدولي ضرورة حيوية لنجاح التحقيقات وإحالة المجرمين للقضاء.

وأخيراً، ركزت الاتفاقية على تحديد المصطلحات القانونية الجديدة، مثل التفتيش الرقمي، الحفظ السريع للبيانات، والتنصت الرقمي، بما يتماشى مع التطورات التكنولوجية، ويعالج هذا البند مشكلة غموض القوانين التقليدية في مواجهة الجرائم الإلكترونية، ويضمن توحيد الإجراءات القضائية بين الدول الأعضاء، مما يعزز فاعلية مكافحة الجريمة المعلوماتية ويقوي الأمن السيبراني على المستوى الدولي.

تمثل اتفاقية بودابست رؤية قانونية دولية متكاملة لمكافحة الجريمة المعلوماتية، حيث وفرت سياقاً تشريعياً وإجرائياً شاملاً، مع تعزيز التعاون الدولي

وتطوير أدوات قانونية وتقنية حديثة، لضمان كشف الجرائم الرقمية ومعاقبة مرتكبيها بفعالية، مع الحفاظ على حقوق الأفراد وخصوصيتهم (مصطفى، 2005، ص23).

الخاتمة

تُظهر دراسة اتفاقية بودابست لمكافحة الجريمة المعلوماتية أن المجتمع الدولي قد أحرز تقدماً ملحوظاً في تطوير الإطار القانوني والإجرائي لمواجهة الجرائم الإلكترونية، فقد ساعدت الاتفاقية في توحيد التشريعات الوطنية وتوفير أدوات قانونية متقدمة مثل الحفظ السريع للبيانات، التفتيش المعلوماتي والتنصت الرقمي ما عزز قدرة الدول على كشف الجرائم السيبرانية ومعاقبة مرتكبيها بفاعلية. كما أثبتت الاتفاقية أهمية التعاون الدولي وتبادل المعلومات والأدلة بين الدول، مما ساهم في التصدي للجرائم العابرة للحدود وحماية الحقوق الرقمية للأفراد والمؤسسات.

بعد الانتهاء من بحث موضوع الجريمة المعلوماتية أوضحت هذه الدراسة النتائج الآتية :

- أن الجريمة المعلوماتية لم تحظ بالدراسة والتحليل في الفقه الجنائي إلا حديثاً لذا فإنها لم تكن محلاً لتنظيم تشريعي خاص إلا في بعض القوانين الغربية المقارنة وبهذه الصورة تتميز بخصوصية ذاتية من حيث صيغ هذه الحماية ومن حيث طبيعة الأحكام التي يجب أن تخضع لها واختلاف أثارها.
- أن الفكر القانوني المعاصر لم يستقر على رأي واحد يوضح تعريف المعلومة أو بيان خصائصها فضلاً عن أن التشريعات المختلفة لا تحتوي حالياً على نص يحدد مفهومها ويمكن الرجوع إليه وعليه فهي أفكار لا حدود لها وتستلزم تنظيماً قانونياً خاصاً بها .
- يطلق على الجرائم المعلوماتية جرائم عبر الوطنية لأنها تقع بين أكثر من دولة إذ غالباً ما يكون الجاني في بلد والمجني عليه في بلد آخر وقد يكون الضرر المتحصل في بلد ثالث مما يؤدي إلى صعوبة إثبات هذا النوع من الإجرام والملاحقة

القضائية نظرا إلى ما استحدثته التطور التقني من وسائل جديدة في ارتكاب هذه الجرائم وفي ضوء هذا أصبحت الإجراءات الجنائية التقليدية في الاستدلال والتحري عن هذه الجرائم غير قادرة في مواجهة هذا النوع إذ انه من غير الممكن العثور في هذا النوع من الجرائم على دليل مادي تقليدي .

وبناءً على هذه النتائج، تأتي التوصيات لتوجيه جهود الدول والمجتمع الدولي نحو تعزيز مكافحة الجريمة المعلوماتية. وتشمل التوصيات تحديث التشريعات الوطنية باستمرار، تأهيل وتدريب الكوادر القضائية والأمنية، وتطوير البنية التحتية التقنية لضمان فعالية جمع الأدلة الرقمية. كما تؤكد التوصيات على أهمية تعزيز التعاون الدولي والإقليمي، والحفاظ على التوازن بين مكافحة الجريمة وحماية الخصوصية، إضافةً إلى رفع مستوى الوعي العام حول الجرائم الإلكترونية وسبل الوقاية منها، بما يضمن نظاماً قانونياً وسيبرانياً متيناً ومستداماً.

- تعزيز التشريعات الوطنية: ينبغي على كل دولة عضو أن تواصل تحديث قوانينها الوطنية لتتماشى مع تطورات الجرائم الإلكترونية الجديدة، وضمان تطبيق فعال للإجراءات الجنائية الحديثة التي نصت عليها الاتفاقية.
- تدريب وتأهيل الكوادر القضائية والأمنية: ضرورة تنظيم برامج تدريبية مستمرة للقضاة، المحققين، وأجهزة الأمن السيبراني، لضمان القدرة على التعامل مع الأدلة الرقمية وتطبيق الإجراءات القانونية المعقدة بفاعلية.
- تطوير البنية التحتية التقنية: توفير نظم معلومات وتقنيات متقدمة للحفاظ السريع للبيانات، مراقبة الأنشطة المشبوهة على الشبكة، وتأمين الأدلة الرقمية، لضمان سرعة التحقيقات ومصادقتها.
- تعزيز التعاون الدولي والإقليمي: تشجيع توقيع مذكرات تفاهم واتفاقيات ثنائية أو إقليمية لدعم التعاون في التحقيقات السيبرانية، بما يشمل تبادل المعلومات، الأدلة، والخبرات التقنية.

- التوازن بين مكافحة الجريمة وحماية الخصوصية: ضرورة وضع ضوابط قانونية صارمة لضمان احترام حقوق الأفراد أثناء إجراءات التحقيق والتفتيش والتنصت، مع توفير آليات رقابية فعالة لمنع أي انتهاك للحقوق الرقمية.
- زيادة الوعي العام: تشجيع حملات توعية للمواطنين والمؤسسات حول الجرائم المعلوماتية، وحقوقهم وواجباتهم الرقمية، لتعزيز الوقاية وتقليل فرص وقوع الجريمة الإلكترونية

الهوامش

- نعيم سعيداني. (2012/2013). آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري. (رسالة ماجستير)، جامعة الحاج لخضر، باتنة، الجزائر، ص 25.
- فريد منعم جبور. (2016). حماية المستهلك عبر الانترنت ومكافحة الجرائم الإلكترونية: دراسة مقارنة. منشورات الحلبي الحقوقية، بيروت، لبنان، ص 183.
- Parker, D. B., Nycum, S., & Aura, S. (1973). Computer Abus: Stanford Research Institut. Taber, J. K. (1973). On Computer Crime. C.L.J, 1(1), 517.
- سفيان سوير. (2010/2011). جرائم المعلوماتية. (رسالة ماجستير)، جامعة أبو بكر بلقايد، تلمسان، الجزائر، ص 12.
- سفيان سوير. (2010/2011). مرجع نفسه، ص 13.
- نعيم سعيداني. (2012/2013). المرجع السابق، ص 28.
- مرجع نفسه، ص 29.
- سلطنة عُمان. (2011). المادة الثالثة من المرسوم السلطاني رقم 2011/12، المتعلق بمكافحة جرائم تقنية المعلومات.
- نهلا عبد القادر المومني. (2008). الجرائم المعلوماتية: ماجستير في القانون الجنائي أُمَلُومَاتِي. (الطبعة 1). دار الثقافة للنشر والتوزيع، ص 50.
- خالد ممدوح إبراهيم. (2008). امن الجريمة الإلكترونية. الدار الجامعية للنشر والتوزيع، الإسكندرية، ص 44.
- نهلا عبد القادر المومني. (2008). المرجع السابق، ص 51.
- نعيم سعيداني. (2012/2013). المرجع السابق، ص 33.
- نهلا عبد القادر المومني. (2008). المرجع السابق، ص 54، 55.
- خالد محمود إبراهيم. (2011). حوكمة الانترنت. دار الفكر الجامعي، الإسكندرية، مصر، ص 370.



- عبد الفتاح بيومي حجازي. (بدون تاريخ). التجارة الإلكترونية وحمايتها القانونية، الكتاب الأول. دار الفكر الجامعي، الإسكندرية، ص 106.
- محمد صبيحي نجم. (2005). شرح قانون العقوبات "القسم الخاص". ديوان المطبوعات الجامعية، الجزائر، ص 3.
- عبد الفتاح بيومي حجازي. (2009). الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت. بهجات للطباعة والتجليد، مصر، ص 146.
- بولين انطونيوس أيوب. (2009). الحماية القانونية للحياة الشخصية في مجال المعلوماتية: دراسة مقارنة. منشورات الحلبي الحقوقية، بيروت، لبنان، ص 176، 177.
- محمد أمين الشوابكة. (2007). جرائم الحاسوب والانترنت، الجريمة المعلوماتية. (الإصدار 2). دار الثقافة للنشر والتوزيع، عمان، الأردن، ص 138.
- خديجة دحمان صبايحية. (2012-2013). جرائم السرقة والاحتيال عبر الانترنت: دراسة مقارنة بين الفقه الإسلامي والقانون الجزائري. (رسالة ماجستير)، جامعة الجزائر، كلية الشريعة والقانون، ص 10.
- جلال محمد الزعبي، وأسامة أحمد المناعسة. (2010). جرائم تقنية نظم المعلومات الإلكترونية: دراسة مقارنة. دار الثقافة للنشر والتوزيع، عمان، الأردن، ص 87.
- محمد محمد شتا. (2001). فكرة الحماية الجنائية لبرامج الحاسب الآلي. دار الجامعة الجديدة للنشر، الإسكندرية، مصر، ص 87.
- جلال محمد الزعبي، وأسامة أحمد المناعسة. (2010). المرجع السابق، ص 265.
- أحمد حسام طه تمام. (2002). الحماية الجنائية لتكنولوجيا الاتصالات: دراسة مقارنة. دار النهضة العربية، مصر، ص 01، 02.
- محمد الزعبي، وآخرون. (2002). الحاسوب والبرمجيات الجاهزة. (ط 1). دار وائل للنشر، عمان، ص 5.
- هدى حامد قشوش. (1992). جرائم الحاسب الإلكتروني في التشريع المقارن. دار النهضة العربية، القاهرة، ص 6.
- خالد الغنبر، و محمد القحطاني. (2009). أمن المعلومات بلغة ميسرة. (ط 1). جامعة الملك سعود، الرياض، ص 7.
- يوسف أبو فارة. (2012). الأعمال الإلكترونية. جامعة القدس المفتوحة، رام الله، ص 17.
- بولين أيوب. (2009). الحماية القانونية للحياة الشخصية في مجال المعلوماتية. (ط 1). منشورات الحلبي الحقوقية، بيروت، ص 450.
- أحمد الحلو، وآخرون. (2015). الأدلة الإلكترونية (الجوانب القانونية والتقنية). معهد الحقوق (جامعة بيرزيت)، رام الله، ص 35.

- مصطفى محمد موسى (2005). دليل التحري عبر شبكة الانترنت. دار الكتب القانونية، مصر (المحلة الكبرى)، ص 23.

قائمة المصادر والمراجع

1- الكتب والدوريات

- إبراهيم، خالد ممدوح. (2008). أمن الجريمة الإلكترونية. الدار الجامعية للنشر والتوزيع.
- إبراهيم، خالد محمود. (2011). حوكمة الانترنت. دار الفكر الجامعي.
- أيوب، بولين أنطونيوس. (2009). الحماية القانونية للحياة الشخصية في مجال المعلوماتية: دراسة مقارنة. منشورات الحلبي الحقوقية.
- جبور، فريد منعم. (2016). حماية المستهلك عبر الانترنت ومكافحة الجرائم الإلكترونية: دراسة مقارنة. منشورات الحلبي الحقوقية.
- حجازي، عبد الفتاح بيومي. (بدون تاريخ). التجارة الالكترونية وحمايتها القانونية: الكتاب الأول. دار الفكر الجامعي.
- حجازي، عبد الفتاح بيومي. (2009). الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت. بهجات للطباعة والتجليد.
- الحلو، أحمد، وآخرون. (2015). الأدلة الإلكترونية (الجوانب القانونية والتقنية). (معهد الحقوق) جامعة بيرزيت.
- الزعبي، جلال محمد، و المناعسة، أسامة أحمد. (2010). جرائم تقنية نظم المعلومات الالكترونية: دراسة مقارنة. دار الثقافة للنشر والتوزيع.
- الزعبي، محمد، وآخرون. (2002). الحاسوب والبرمجيات الجاهزة (ط. 1). دار وائل للنشر.
- الشوايكة، محمد أمين. (2007). جرائم الحاسوب والانترنت، الجريمة المعلوماتية (الإصدار 2). دار الثقافة للنشر والتوزيع.
- شتا، محمد محمد. (2001). فكرة الحماية الجنائية لبرامج الحاسب الآلي. دار الجامعة الجديدة للنشر.
- تمام، أحمد حسام طه. (2002). الحماية الجنائية لتكنولوجيا الاتصالات: دراسة مقارنة. دار النهضة العربية.
- الغنبر، خالد، و القحطاني، محمد. (2009). أمن المعلومات بلغة ميسرة (ط. 1). جامعة الملك سعود.



- قشوش، هدى حامد. (1992). جرائم الحاسب الالكتروني في التشريع المقارن. دار النهضة العربية.
- موسى، مصطفى محمد. (2005). دليل التحري عبر شبكة الانترنت. دار الكتب القانونية.
- نجم، محمد صبيحي. (2005). شرح قانون العقوبات "القسم الخاص". ديوان المطبوعات الجامعية.
- Taber, J. K. (1973). On Computer Crime. C.L.J, 1(1).

2- رسائل الماجستير

- دحمان صبايحية، خديجة. (2013). جرائم السرقة والاحتيال عبر الانترنت: دراسة مقارنة بين الفقه الإسلامي والقانون الجزائري. (رسالة ماجستير). جامعة الجزائر، كلية الشريعة والقانون.
- سعيداني، نعيم. (2013). آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري. (رسالة ماجستير). جامعة الحاج لخضر، كلية الحقوق والعلوم السياسية.
- سوير، سفيان. (2011). جرائم المعلوماتية. (رسالة ماجستير). جامعة أبو بكر بلقايد، كلية الحقوق والعلوم السياسية.
- المومني، نهلا عبد القادر. (2008). الجرائم المعلوماتية: ماجستير في القانون الجنائي أُمُلموماتي (الطبعة 1). دار الثقافة للنشر والتوزيع.
- أبو فارة، يوسف. (2012). الأعمال الالكترونية. جامعة القدس المفتوحة.
- Parker, D. B., Nycum, S., & Aura, S. (1973). Computer Abus: Stanford Research Institut. Stanford Research Institut.

3- الوثائق القانونية

- سلطنة عُمان. (2011). المرسوم السلطاني رقم 2011/12، المتعلق بمكافحة جرائم تقنية المعلومات.