المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (69) ديسمبر 2025
Volume (69) December 2025
IJOHSS

التعاون الدولي في مكافحة الجريمة الإلكترونية (اتفاقية بودابست ودور دولة قطر)

سعود جاسم المرزوقي
طالب ماجستير، اكاديمية الشرطة، كلية الدراسات العليا، قطر
البريد الالكتروني: Almarzouqi.1995@hotmail.com

الملخص

يشكّل الفضاء الرقمي اليوم أحد أكثر البيئات خصوبة لارتكاب أنماط إجرامية غير تقليدية، تتجاوز الحدود الجغرافية وتستغل التفاوت التشريعي بين الدول و تعتبر الجرائم الإلكترونية من الظواهر الحديثة في عالم الجريمة، حيث ترتبط ارتباطًا وثيقًا بالتطورات التكنولوجية التي يشهدها العالم، تعتمد هذه الجرائم على تكنولوجيا المعلومات والاتصالات، وتتسم بطبيعة معقدة تجعلها تختلف جوهرياً عن الجرائم التقليدية ، سواء من حيث نطاقها أو الضحايا المتضررين منها أو تقنيات الكشف عنها، ويُلاحظ أن الاستخدام السلبي للتكنولوجيا قد ساهم في زيادة احترافية المجرمين، مما يجعل ضبطهم أكثر صعوبة.

إن انشغال المجتمعات في رفاهية الحياة السريعة، وتوافر الأدوات الرقمية وأجهزة الاتصال، قد ساهم في زيادة معدل هذه الجرائم وتوسع دائرة مستهدفيها، وأن الجرائم الإلكترونية ليست محصورة ضمن حدود دولة واحدة، بل تتسم بالطابع العابر للحدود، مما يعني أنها تضم أفرادًا، ومتخصصين وأساليب متنوعة ومتطورة، ولذلك يتطلب الأمر إعادة النظر في مفهوم هذه الجرائم، وفهم مسبباتها، وايجاد آليات فعالة للتعامل القانوني مع تحدياتها، ودراسة أطر التعاون بين الدول وتطوير الاتفاقيات والتشريعات الدولية.

تعد اتفاقية بودابست من أبرز الجهود الدولية في مجال مكافحة الجرائم الالكترونية ، والتي جاءت كأول إطار قانوني متعدد الأطراف يعالج الجريمة الإلكترونية، محددةً آليات التجريم، والإجراءات، وقنوات التعاون القضائي والأمني بين الدول.

على مستوى دولة قطر، بادر المشرع القطري بإيلاء أهمية خاصة للأمن السيبراني، وهو ما ظهر في صدور قانون مكافحة الجرائم الإلكترونية لعام 2014، وإطلاق الاستراتيجية الوطنية للأمن السيبراني، بالإضافة إلى الجهود المؤسسية التي تبذلها وزارة الداخلية القطرية ووحدة مكافحة الجرائم الإلكترونية، ومع ذلك تبقى مسألة توافق التشريعات والسياسات الوطنية مع المعايير الدولية، وعلى رأسها اتفاقية بودابست، موضوعاً لنقاشات علمية وقانونية تتسم بالعمق، خاصة في ظل التحديات القانونية والسياسية والتقنية ، إذ اننا نلاحظ تقدم سريع ومواكبة منظمة في تطوير السياسات التشريعية والمؤسسية لمواجهة الجرائم الالكترونية، سواء على المستوى التشريعي الدولي والوطني، أو على المستوى المؤسسي أو التقني.

الكلمات المفتاحية: الجريمة الإلكترونية، التعاون الدولي، اتفاقية بودابست، التشريعات القطرية، الأمن السيبراني، السياسة الجنائية، القانون الدولي.

DOI: https://doi.org/10.33193/IJoHSS.69.2025.896

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (69) ديسمبر 2025
Volume (69) December 2025
IJOHSS

International Cooperation in Combating Cybercrime (The Budapest convention and the role of state of Qatar)

Saoud Jassem Al-Marzouki
Police Academy, College Of Graduate Studies, Qatar
Email: Almarzouqi.1995@hotmail.com

ABSTRACT

The digital landscape today enables unconventional criminal activities that transcend borders and exploit legal gaps between countries. Cybercrime, closely linked to technological advancements, relies on information and communication technology, and presents unique challenges that set it apart from traditional crimes. Its complexity complicates detection efforts and has led to heightened criminal professionalism, making apprehension more difficult. Societal reliance on fast-paced digital living and available technology has increased the prevalence of cybercrime and expanded its target audience. Notably, cybercrime operates transnationally, involving diverse individuals and sophisticated methods. This necessitates a re-evaluation of these crimes, understanding their root causes, and developing legal frameworks to tackle associated challenges while promoting international cooperation and enhancing treaties. One of the most prominent international efforts to combat cybercrime is the Budapest Convention, which serves as the first multilateral legal framework addressing cybercrime, specifying mechanisms for criminalization, procedures, and channels for judicial and security cooperation among countries. The Budapest Convention stands out as a key international initiative against cybercrime, establishing a multilateral legal framework that outlines criminalization, procedures, and cooperation among nations. In Qatar, the government has prioritized cybersecurity, evident in the 2014 Cybercrime Prevention Law and the National Cybersecurity Strategy, The Qatari Ministry of Interior and its Cybercrime Unit have also made significant institutional efforts. However, aligning national laws and policies with international standards, particularly those set by the Budapest Convention, continues to be a topic of legal and academic discussion due to various challenges. There is notable progress in aligning legislative and institutional policies to address cybercrime effectively on both national and international fronts.

Keywords: cybercrime, international cooperation, Budapest convention, legislation Qatari, cyber, international law.

 DOI: https://doi.org/10.33193/IJoHSS.69.2025.896

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (69) ديسمبر 2025
Volume (69) December 2025
IJOHSS

المقدمة:

تعد الجريمة ظاهرة اجتماعية ظهرت بظهور الانسان وارتبطت ارتباطاً وثيقاً به، فأصبحت بذلك الوجه السلبي الذي يتنقل عبر العصور مع تطور فيها الانسان، وكان من البديهي أن تظهر أنماط جديدة من الجرائم لم تكن معهودة في السابق.

شهد العالم منذ منتصف القرن العشرين تحولاً جذرياً تمثّل في ظهور الثورة المعلوماتية، التي جاءت امتداداً للثورة الصناعية، لكنها تجاوزتها في الأثر والانتشار والتأثير على صور وانماط الحياة البشرية، فقد أصبح تدفّق المعلومات وتخزينها وتنظيمها ضرورة حيوية، بل عاملاً أساسياً في بناء الحضارة الحديثة.

أظهر عجز الفكر البشري عن مواكبة الكم الهائل من المعطيات، الحافز الأبرز لابتكار أدوات وتقنيات متطورة مكّنت الإنسان من السيطرة على تدفق البيانات، وتحويلها إلى رصيد معرفي منظم، ومع التوسع في تطبيقات تكنولوجيا الاتصال والمعلومات، ظهر ما يمكن تسميته بالعصر المعلوماتي، الذي بات أحد أبرز ملامح المرحلة الحضارية الراهنة، بحيث غدا الإنسان فيه أمام وسائط متجددة لا تعرف التوقف، ابتداءً من النقش على جدران المعابد، مروراً بالكتابة على الورق، وصولاً إلى الأقراص الإلكترونية المعقدة التي تمثل قمة التطور التقني المعاصر.

إلا أنّ هذا التطور لم يكن خالياً من التحديات، فكما أنتج وابتكر فرصاً هائلة لخدمة الإنسان، فتح المجال أمام أنماط جديدة من الانحراف والجريمة، حيث نشأت ظاهرة الجريمة الإلكترونية بوصفها أحد أخطر نتائج عصر التكنولوجيا، فهي جريمة ذات طابع متطور، تواكب الأدوات والوسائط المستحدثة، وتعكس بوضوح حقيقة أن الجريمة ، بمختلف صورها هي نتاج ملازم لمسيرة التطور الإنساني، فكلما تقدمت البشرية في بناء أدواتها، أبدع المجرمون أساليب غير تقليدية لاستغلالها بما يتناسب مع أهدافهم غير المشروعة.

إن المفهوم العام للجريمة الالكترونية لم تنص عليه صراحة معظم قوانين العقوبات بشكل مباشر ومفصل ، لذلك لجأ العديد من الفقهاء الى وضع تعريف لها " كل فعل او امتناع غير مشروع يهدد بخطر، يتخذ من الانترنت عبر مختلف الأجهزة وسيلة لارتكابه، وذلك إذا نص القانون على جزاء في صورة عقوبة أو تدبير احترازي. (عالية، 2018،ص4).

تكمن خطورة الجريمة المعلوماتية في طبيعتها غير التقليدية، وفي امتداد آثارها إلى مجالات الحياة كافة، سواء الاقتصادية أو الاجتماعية أو الأمنية، فهي ليست امتداداً للجريمة بالمفهوم العام فحسب، بل تمثل نقلة نوعية في أسلوب التعدي على القيم والمصالح المحمية قانوناً، بما يفرض على المجتمعات والأنظمة القانونية مواجهة هذا التحدي بوعي، وأدوات متجددة، وتشريعات قادرة على ضبط الظاهرة والحد من آثارها.

في هذا السياق تعتبر اتفاقية بودابست لعام 2001 أول وأهم صك دولي شامل يهدف إلى توحيد الجهود التشريعية والإجرائية لمكافحة الجرائم الإلكترونية، وتعزيز التعاون القضائي والشرطي بين الدول.

أما على مستوى دولة قطر، فقد سارع المشرع القطري بإيلاء أهمية خاصة للأمن السيبراني، وهو ما ظهر من خلال اصدار قانون مكافحة الجرائم الإلكترونية لعام 2014، وإطلاق الاستراتيجية الوطنية للأمن السيبراني، بالإضافة إلى الجهود المؤسسية التي تبذلها الوزارات المعنية القطرية في مكافحة الجرائم الإلكترونية.

إشكالية البحث:

تعد الجريمة الالكترونية واحدة من أكبر التحديات التي نواجهها في وقتنا هذا، وعلى الرغم من الطابع العابر للحدود الذي تتميز به الجريمة الإلكترونية، ما يزال التعاون الدولي في مواجهتها يواجه عقبات متعددة تتعلق بتفاوت التشريعات الوطنية، وتباين القدرات التقنية، وضعف التنسيق بين الدول، ومن هنا تبرز إشكالية البحث في التساؤل الرئيسي:

DOI: https://doi.org/10.33193/IJoHSS.69.2025.896

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (69) ديسمبر 2025
Volume (69) December 2025
IJOHSS

- **إلى أي مدى يسهم التعاون الدولي في مواجهة الجريمة الالكترونية، ولا سيما من خلال اتفاقية بودابست، ، وما هي التحديات والفرص التي نواجهها في هذا الإطار.**
وقدرة دولة قطر على مكافحة الجريمة الإلكترونية؟

وتتفرع من هذه الإشكالية مجموعة من التساؤلات الفرعية يمكننا عرضها على الشكل التالي:

1- ما طبيعة الإطار القانوني الدولي الذي أقرته اتفاقية بودابست لمكافحة الجرائم الإلكترونية؟

2- كيف يمكن تقييم موقع ودور دولة قطر في ضوء هذه الاتفاقية، وما مدى انسجام تشريعاتها الوطنية مع أحكامها؟

3- ما هي أبرز التحديات التي تواجه دولة قطر في مجال التعاون الدولي لمكافحة الجريمة الإلكترونية؟

4- ما الطرق الممكنة لدعم فعالية التعاون الدولي، وضمان تكامل الجهود الوطنية مع الالتزامات الدولية في هذا المجال؟

أهمية الموضوع:
تكمن أهمية هذا البحث في تناوله موضوعًا حديثًا ومتجددًا يتطور بمستوى متسارع يوميًا، هذا التطور السريع لا يؤثر فقط على المجالات التقنية والتشريعية والاجتماعية، بل يتيح أيضًا فهمًا أعمق للتحديات والفرص التي أمامنا، وتكمن أهمية البحث ايضاً في دراسة شمولية للعلاقة بين الطابع العابر للحدود للجريمة الإلكترونية وبين الحاجة الملحة إلى تعاون دولي منظم، والى تسليط الضوء على التغيرات التي تساهم في دعم إدراكنا، ووعينا بالمسائل المرتبطة بموضوع هذا البحث، ما يجعله ذا صلة وثيقة بالواقع الذي نعيشه اليوم.

أسباب اختيار البحث:
يتطلب التصدي للجرائم الإلكترونية تعاونًا دوليًا موسعًا وفعّالًا، حيث أصبحت هذه الجرائم تتخطى الحدود الجغرافية وتؤثر على الأمن السيبراني عالميًا، لذلك ينبغي تسليط الضوء بشكل شامل على أهمية هذا التعاون، مع التركيز على تبادل المعرفة والخبرات بين الدول لتحقيق فاعلية أكبر في مكافحتها.
إضافة الى ذلك يتوجب دراسة القوانين المقارنة المتعلقة بالجرائم الإلكترونية، حيث يمكن أن تسهم في توضيح كيفية التعامل مع هذه القضايا، كما ينبغي شرح السبل التي تتبناها مختلف الدول لمواجهة هذه التحديات، من خلال تحليل التشريعات القائمة وإجراءات إنفاذها، هذا سيمكننا من استكشاف نماذج ناجحة لأفضل الممارسات، ويساعد على بناء إطار عمل دولي متين للتصدي للجرائم الإلكترونية بفعالية وكفاءة.

منهجية البحث:
سوف نعتمد من أجل معالجة هذا الموضوع على المنهج الوصفي التحليلي ، وذلك لتحليل جملة من النصوص القانونية المتعلقة بموضوع التعاون الدولي في مكافحة الجريمة الإلكترونية ضمن إطار اتفاقية بودابست ودور دولة قطر ، وسنعتمد المنهج المقارن في ظل التشريعات والنصوص القانونية الأجنبية.

خطة البحث :
تم تقسيم هذا البحث على الشكل التالي :
- المقدمة
- المبحث الأول سنتناول فيه مفهوم الجريمة الالكترونية خصائصها /مميزاتها.
- المطلب الأول سنتناول فيه أنماط وأساليب الجريمة الالكترونية.
- المطلب الثاني سنتناول فيه دوافع وآثار الجريمة الالكترونية على المستوى الامني / الاجتماعي /النفسي/الاقتصادي.

DOI: https://doi.org/10.33193/IJoHSS.69.2025.896

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (69) ديسمبر 2025
Volume (69) December 2025
IJOHSS

- المبحث الثاني سنتناول فيه الأسس القانونية للتعاون الدولي في مواجهة الجريمة الالكترونية.
- المطلب الأول سنتناول فيه أهمية التعاون الأمني الدولي ونتائجه.
- المطلب الثاني سنتناول فيه اتفاقية بودابست (2001) أهدافها ومبادئها .

- المبحث الثالث سنتناول فيه طرق مكافحة الجرائم الالكترونية / التشريعات العربية والأجنبية نموذجاً .
- المطلب الأول سنتناول التحديات التي تواجه التعاون الدولي /دور المنظمات الدلية والإقليمية لمكافحة الجرائم الالكترونية.
- المطلب الثاني سنتناول فيه التعاون الدولي في مجال التدريب لمكافحة الجرائم المعلوماتية/ جهود دولة قطر العملية
- الخاتمة والتي تشمل جملة من النتائج والتوصيات.

المبحث الأول: مفهوم الجريمة الالكترونية خصائصها /مميزاتها

الجريمة الإلكترونية تُعتبر تطورًا حديثًا للجريمة التقليدية، حيث تمتلك خصائصها الفريدة، برزت هذه الجرائم بشكل خاص في عصر الحواسيب والعولمة والإنترنت، مما يجعلها مختلفة تمامًا عن الجرائم التقليدية، فالجرائم الإلكترونية تتميز بعدد من الخصائص التي تميزها عن الأنواع الأخرى من الجرائم.

تعد الجريمة الإلكترونية بأنها اعتداءات قانونية يرتكبها الجاني باستخدام الوسائل الإلكترونية بهدف تحقيق الربح، وتتمثل هذه الاعتداءات في استهداف أموال معنوية، مثل البيانات والمعلومات الحاسوبية، من خلال تدخل تقني إلكتروني، تتشابه الجريمة الالكترونية مع الجريمة التقليدية في أطراف الجريمة من مجرم ذي دافع لارتكاب الجريمة وضحية والذي قد يكون شخص طبيعي أو شخص اعتباري وأداة ومكان الجريمة، وهنا يكمن الاختلاف الحقيقي بين نوعي الجريمة ففي الجريمة الالكترونية الاداة ذات تقنية عالية وأيضا مكان الجريمة الذي لا يتطلب انتقال الجاني اليه انتقالا جسدياً حضورياً، ولكن في الكثير من تلك الجرائم تتم عن بعد باستخدام خطوط وشبكات الاتصال بين الجاني ومكان الجريمة (الديري، 2012،ص47).

تتمثل اركان هذه الجريمة ب الركن المادي حيث ترتبط طبيعة الركن المادي في الجرائم الإلكترونية بالمشكلات المُثارة، ويقصد بذلك سوء استخدام الأنظمة الإلكترونية بطريقة غير مشروعة، أو اقتحام آثار مادية ملموسة تساهم في تدمير المعلومات، أو السرقة لبطاقات الائتمان أو التزوير والتلاعب في البيانات المرتبطة بالحواسب الآلية، وإن السلوك الإجرامي يعتبر عنصر أساسي في الركن المادي في الجرائم التقليدية، كمشاهدة الجاني ورؤيته رؤية العين في قيامه بالقتل أو السرقة أو التزوير، أمّا في الجرائم الإلكترونية فيكون من الصعب الإمساك بالجاني مادياً، لأنَّها ترتكب عبر المعلومات والبيانات المتوافرة عبر أنظمة الحواسيب الآلية.

والركن المعنوي ويقصد به الحالة النفسية والمزاجية لمرتكبي الجرائم الإلكترونية، مع أهمية التركيز على العلاقات التي تكون مرتبطة ما بين ماديات الجريمة وشخصية الجاني.

تتسم الجرائم الإلكترونية بشكل عام بعدد من الخصائص مثل سهولة الانخراط فيها، إذ يسهم غياب الرقابة الأمنية الفعالة في انتشارها بشكل واسع، إضافة الى ذلك فإن الأضرار الناتجة عن الجرائم الإلكترونية يصعب قياسها وغالباً ما تكون جسيمة، مما يؤثر على الأفراد والشركات والمجتمعات بشكل عام.

يحتاج كشف مرتكبي الجرائم الإلكترونية إلى استخدام تقنيات وأساليب أمنية متقدمة، حيث تتطلب هذه الجرائم مهارات خاصة ومعرفة متعمقة بالتكنولوجيا، كما تصنف ك سلوكيات غير تقليدية وغير أخلاقية على المستوى الاجتماعي، ما يثير القلق حول تأثيرها على القيم والمبادئ الاجتماعية.

يستنتج مما سبق ان جرائم الاحتيال الإلكتروني تتميز بأنها تتطلب مستويات أقل من العنف والجهد مقارنة بالجرائم التقليدية، مما يجعلها أكثر جذباً للعديد من الأفراد، كما أنها لا تتقيد بزمان أو مكان معين، مما يسمح لها بالانتشار عبر مسافات جغرافية كبيرة وبسرعة، يمكن بسهولة إخفاء الأدلة وآثار الجريمة بفضل التقنيات مثل التشفير والرموز، مما يعقد من مهمة التحقيق وكشف الجناة، ويتطلب ايضاً لمواجهة هذه الظاهرة فهمًا عميقًا للتكنولوجيا المستخدمة، وكذلك تطوير استراتيجيات جديدة في مكافحة الجرائم الإلكترونية، ويرى الخبراء أنه من الضروري أن تتعاون الحكومات والجهات المختصة لتعزيز الأمن السيبراني وتوفير بيئة آمنة للمستخدمين على الإنترنت.

DOI: https://doi.org/10.33193/IJoHSS.69.2025.896

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (69) ديسمبر 2025
Volume (69) December 2025
IJOHSS

المطلب الأول : أنماط وأساليب الجريمة الالكترونية:

تتزايد الجرائم الإلكترونية مع اتساع استخدام التكنولوجيا والتواصل الرقمي في مختلف جوانب الحياة اليومية، وتعتبر هذه الجرائم معضلة عالمية خطيرة تهدد الأفراد والمؤسسات والدول على حد سواء، تشتمل الجرائم الإلكترونية على مجموعة متنوعة من الأنماط والأساليب التي تهدف إلى تحقيق مكاسب غير قانونية من خلال استغلال الثغرات الأمنية والذهنية للضحايا، وتتضمن هذه الجرائم استهداف الأفراد بشكل مباشر، مثل عمليات الاحتيال وسرقة الهوية، بالإضافة إلى استهداف الملكية الفكرية والمعلومات السرية للجهات الحكومية والخاصة، كما تشمل الهجمات الإلكترونية التي تستهدف الحكومات بهدف إلحاق الضرر بالبنية التحتية الرقمية، سنستعرض في هذا المطلب أبرز الأنماط والأساليب المرتبطة بالجريمة الإلكترونية، ونبرز المخاطر المرتبطة بكل نوع منها.

تتعدد أنواع جرائم الاحتيال الإلكتروني وتتنوع استهدافاتها، حيث يمكن تصنيفها كما يلي:

أولا جريمة إلكترونية تستهدف الأفراد ويُطلق عليها أيضاً مسمى جرائم الإنترنت الشخصية والتي تقتضي على الحصول بطريقة غير شرعية على هوية الأفراد الإلكترونية كالبريد الإلكتروني وكلمة السر الخاصة بهم وكما تمتد لتصل إلى انتحال الشخصية الإلكترونية وسحب الصور والملفات المهمة من جهاز الضحية لتهديده بها وإخضاعه للأوامر، كما تُعتبر سرقة الاشتراك أيضاً من الجرائم ضد الأفراد.

ثانياً جريمة إلكترونية تستهدف الملكيّة يستهدف هذا النوع من الجريمة الجهات الحكوميّة والخاصة والشخصية ويركّز على تدمير الملفات الهامة أو البرامج ذات الملكية الخاصة ويكون ذلك عبر برامج ضارة يتم نقلها إلى جهاز المستخدم بعدة طرق من أبرزها الرسائل الإلكترونية.

ثالثاً جريمة إلكترونية تستهدف الحكومات وهي هجمات يشنّها القراصنة على المواقع الرسميّة الحكومية وأنظمة شبكاتها والتي تركز جل اهتمامها على القضاء على البنية التحتيّة للموقع أو النظام الشبكي وتدميره بالكامل ومثل هذه الهجمات في الغالب يكون الهدف منها سياسيّا (مرعي،2025،ص24).

رابعاً النصب والاحتيال الإلكتروني، وتصنيف اللائحة والتعداد يطول ليشمل الجرائم السياسية الإلكترونية والتى تركز على استهداف المواقع العسكرية لبعض الدول لسرقة المعلومات التي تتعلّق بأمن الدولة، وسرقة المعلومات الموثّقة إلكترونياً ونشرها بطرق غير شرعيّة، إضافة الى جرائم القذف/ الشتم والسبّ والقدح والذم، مثل جرائم التشهير التي يكون هدفها الإساءة لسمعة الأفراد، وجرائم الاعتداء على الأموال أو الابتزاز الإلكتروني أو الوصول إلى مواقع محجوبة.

خامساً الإرهاب الإلكتروني، والجرائم الجنسية الإلكترونية، وجرائم الاعتداء على الاموال (مؤسسات مصرفية ومالية وبنوك).

أما على مستوى الأساليب او الطرق والصور التي يعتمدها المجرمون في تنفيذ أهدافهم، نجد ان أساليب جرائم الاحتيال الإلكتروني تتطور بسرعة، مستفيدةً من الثغرات التقنية والنفسية، وفيما يلي أبرز هذه الأساليب:

التصيد الاحتيالي حيث يقوم المحتالون بانتحال هوية مؤسسات موثوقة من خلال رسائل بريد إلكتروني أو نصية مزيفة، بهدف خداع المستخدم وسرقة بياناته الحساسة مثل كلمات المرور ومعلومات البطاقات الائتمانية.

انتحال الشخصية حيث يكتسب المحتالون معلومات شخصية من الضحية لإنشاء هوية رقمية مزورة، مستخدمين إياها في الابتزاز أو لارتكاب عمليات احتيالية.

احتيال مواقع التسوق المزيفة حيث ينشئ المحتالون متاجر إلكترونية وهمية بأسعار مغرية، ويقومون بسرقة بيانات الدفع عندما يدخل الضحية معلوماته على هذه المواقع.

احتيال الدعم الفني حيث يتصل المحتالون بالضحايا مزعمين أنهم من الدعم الفني، ويطلبون منهم دفع مبالغ مالية مقابل خدمات غير موجودة أو الوصول إلى أجهزتهم لسرقة البيانات.

DOI: https://doi.org/10.33193/IJoHSS.69.2025.896

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (69) ديسمبر 2025
Volume (69) December 2025
IJOHSS

الابتزاز الإلكتروني حيث يهدد المحتالون الضحايا بنشر معلومات حساسة ما لم يتم دفع فدية، ومن أبرز أشكاله هجمات الفدية الخبيثة.

جرائم الاعتداء على الأموال حيث يعد المحتالون الضحايا بعوائد مالية سريعة من استثمارات وهمية، ويبنون ثقة قبل الاختفاء بعد الحصول على أموال الضحية.(الصويلح،2025،ص.ص 20-25).

يتضح من التحليل أن أنماط جرائم الاحتيال الإلكتروني تظهر بشكل متنوع ومعقد، مما يجعلها تحديًا كبيرًا يتطلب اهتمامًا خاصًا من المجتمع ككل، حيث تركز الجرائم على الأفراد من خلال استغلال هوياتهم الرقمية، وعلى الملكية الفكرية من خلال تدمير المعلومات والبيانات الحيوية، كما تستهدف الحكومات بهدف تنفيذ برامج وغايات معينة، ويمكن القول إن خطورة هذه الجرائم تكمن في قدرتها على التأثير على الأمان الشخصي والمؤسسي، وتدمير سمعة الكيانات المستهدفة، لذلك من الضروري أن يتم دعم الوعي العام حول هذه الأنماط وأساليبها، بالإضافة إلى تحسين استراتيجيات الحماية والتقنيات المستخدمة لمكافحة تلك الجرائم على كافة المستويات.

المطلب الثاني : دوافع وآثار الجريمة الالكترونية على المستوى الامني / الاجتماعي /النفسي/الاقتصادي:

في عصر التكنولوجيا الحديثة هذا والاعتماد المتزايد على الإنترنت، أصبحت الجريمة الإلكترونية واحدة من أخطر التحديات التي تواجه المجتمعات على مستوى العالم، فمع توسع نطاق الاستخدام الرقمي، تنامت أيضًا الأنشطة غير القانونية التي تهدف إلى استغلال هذه الوسائل التكنولوجية لتحقيق مكاسب شخصية. تثير الجرائم الإلكترونية القلق ليس فقط بسبب تأثيراتها المالية الكبيرة، ولكن أيضًا بسبب تعقيداتها القانونية والاجتماعية.

إن فهم دوافع هذه الجرائم يكشف عن جوانب متعددة تسهم في انتشار هذه الظاهرة، مما يجعل من الضروري دراسة الأسباب وراء ارتكابها، حيث تتنوع دوافع الأفراد المنخرطين في هذه الأنشطة وتتعدد غاياتهم لارتكاب الجرائم الإلكترونية، مما يجعلها ظاهرة معقدة شائكة ومتنوعة، من بين هذه الدوافع نجد:

الدوافع المادية حيث تُعتبر هذه الدوافع من أكثر وأكثر الأسباب شيوعًا في ارتكاب الجرائم الإلكترونية. يسعى الأفراد من خلال هذه الدوافع إلى الحصول على مكاسب مالية سريعة، مما يدفعهم للقيام بأعمال مثل سرقة الأموال وتحويلها إلى حساباتهم الشخصية، وغالبًا ما تنشأ هذه الدوافع من ضغوط مالية أو حاجات اقتصادية.

الدوافع الشخصية حيث تتعلق هذه الدوافع برغبة الأفراد في التعلم واستكشاف القدرات التقنية المتعلقة باختراق الأنظمة، حيث يقضي العديد من الأشخاص أوقاتًا طويلة في دراسة كيفية تجاوز الحواجز الأمنية وتعلم تقنيات الاختراق، مما يدفعهم إلى الانخراط في أنشطة غير قانونية.

الدوافع الذهنية أو النمطية ويتمثل هذا النوع من الدوافع في رغبة الأفراد في إثبات الذات وتحقيق الانتصارات في مجالات التقنيات المعلوماتية، ويسعى هؤلاء الأفراد إلى تطوير مهاراتهم في الاختراق كوسيلة لإظهار براعتهم وكفاءتهم في هذا المجال.

دافع الانتقام ويعتبر هذا الدافع من أخطر الأسباب التي تدفع الأفراد لارتكاب الجرائم الإلكترونية، يحدث ذلك عندما يمتلك هؤلاء الأفراد معلومات حساسة حول شركات أو مؤسسات معينة، مما يمكنهم من توجيه هجمات تستهدف تلك الكيانات بغرض الانتقام أو الرد على أفعال سابقة.

دافع التسلية حيث يسعى بعض الأفراد إلى ارتكاب الجرائم الإلكترونية بدافع التسلية فقط، يعتبر هؤلاء الأشخاص هذه الأنشطة بمثابة نوع من الترفيه، مما يعكس افتقارهم للوعي بمخاطر هذه الأفعال وعدم تقدير العواقب المحتملة.

الدافع السياسي ويشمل هذا الدافع استخدام الجرائم الإلكترونية لأغراض سياسية، كفبركة الأخبار والمعلومات، أو دعم معلومات مجتزأة من الحقيقة، غالبًا ما تُستهدف الحكومات من خلال نشر أخبار ملفقة على منصات سياسية معارضة، حيث تستغل هذه الأنشطة لتسليط الضوء على المحاولات الدولية لاختراق الشبكات الحكومية في مختلف أنحاء العالم.

ويتبين لنا من خلال ما ذكرنا أن الجرائم الإلكترونية من الظواهر المتزايدة التي تؤثر بشكل كبير على الأفراد والمجتمعات، وتشمل آثار هذه الجرائم مجموعة من الجوانب السلبية التي تتراوح من الأضرار النفسية إلى الآثار الاقتصادية والاجتماعية، سنستعرض فيما يلي بعض من هذه الآثار بالتفصيل:

الأضرار النفسية على الضحايا حيث تتسبب الجرائم الإلكترونية في آثار نفسية عميقة على الضحايا، حيث يشعر العديد منهم بالقلق المستمر، والاكتئاب، والرهاب الاجتماعي، ويمكن أن يؤدي الابتزاز أو التشهير إلى تدهور الحالة النفسية، مما يسبب فقدان الثقة بالنفس والشعور بالعزلة، كما قد يعاني الضحايا من اضطرابات في النوم أو مواجهة صعوبات في التركيز، مما يؤثر سلبًا على حياتهم اليومية وعلاقاتهم الاجتماعية.

DOI: https://doi.org/10.33193/IJoHSS.69.2025.896

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (69) ديسمبر 2025
Volume (69) December 2025
IJOHSS

الخسائر المالية المباشرة وغير المباشرة حيث تشكل الجرائم الإلكترونية عبئًا ماليًا كبيرًا، حيث تتضمن الخسائر المباشرة سرقة الأموال من الحسابات البنكية أو سرقة البيانات المالية، بالإضافة إلى ذلك تواجه الشركات والأفراد تكاليف باهظة لاستعادة البيانات والحماية من الهجمات المستقبلية، هذه النفقات قد تشمل التعاقد مع متخصصين في الأمن السيبراني، وكذلك تكلفة إصلاح الأنظمة المتضررة.

تشويه السمعة الشخصية أو المهنية، بالمبدأ يمكن أن تؤدي الجرائم الإلكترونية إلى تدمير السمعة الشخصية أو المهنية للأفراد أو المؤسسات، فعندما تتعرض البيانات الحساسة للتسريب أو تتم إساءة استخدامها، قد يجد الضحايا أنفسهم في وضع صعب، حيث يصعب إعادة بناء الثقة بالسيرة الذاتية والأعمال، وهذا قد يتطلب وقتًا وجهودًا كبيرة لعلاج الأضرار التي حدثت.

انتهاك الخصوصية حيث تعد سرقة البيانات الحساسة أو نشر معلومات خاصة دون إذن انتهاكًا صارخًا لحقوق الأفراد في الخصوصية، فالأشخاص الذين يتعرضون لهجمات إلكترونية قد يفقدون السيطرة على معلوماتهم الشخصية ويواجهون أخطار تتعلق بهويتهم، والتي قد تؤدي إلى تداعيات تتخطى الفضاء الرقمي إلى حياتهم اليومية وعلاقاتهم الأسرية.

إرباك الأمن الوطني حيث لا تقتصر تأثيرات الجرائم الإلكترونية على الأفراد والمؤسسات فحسب، بل تمتد لتشمل الأمن الوطني أيضًا، تسعى بعض الهجمات إلى استهداف البنية التحتية الحيوية، مما يخلق خطرًا مباشرًا على استقرار الدولة، كما يجوز أن تؤثر على الرأي العام من خلال نشر معلومات مضللة، مما يؤدي إلى زعزعة الثقة في المؤسسات والسلطات الحكومية.

يمكن القول أن دوافع ارتكاب الجرائم الإلكترونية تعكس تنوعًا واسعًا، يتراوح بين الرغبات المالية والشخصية إلى الأغراض الأنانية والدوافع السياسية، مما يستدعي ضرورة البحث عن حلول فعالة لمكافحة، وتبرز الآثار المتنوعة للجرائم الإلكترونية الحاجة الملحة إلى اتخاذ تدابير أمنية فعالة، وتعزيز الوعي العام حول المخاطر المرتبطة بالتكنولوجيا الحديثة، ويتطلب ذلك تكامل الجهود بين الأفراد، والشركات، والدول لحماية الحقوق الفردية وتعزيز الأمن السيبراني كوسيلة أساسية لتحصين المجتمعات ضد هذه التحديات المتزايدة. (مهدي،2013،ص45)

المبحث الثاني : الأسس القانونية للتعاون الدولي في مواجهة الجريمة الالكترونية:

الجريمة الإلكترونية هي واحدة من الظواهر التي تتجاوز الحدود الوطنية وفقاً للدراسات السابقة، مما يستدعي اطلاق التنبيه على أهمية التعاون القانوني الدولي بين السلطات المعنية كافة، لأن هذه الأهمية لا تنحصر في الدولة التي نشأت فيها الجريمة فحسب، بل تمتد وتشمل أيضًا البلدان التي تم تنفيذ الأنشطة الإجرامية داخلها، فقد أثبتت التجارب الواقعية أن مواجهة هذه الجرائم لا يمكن أن تتم بنجاح عبر جهود فردية، خاصةً في ظل التسارع الهائل في تقنيات الاتصال وتكنولوجيا المعلومات، وكذا الطبيعة العالمية التي يتمتع بها عالم الإنترنت.

وبناءً عليه فإن تحقيق مكافحة فعالة يتطلب إنشاء إطار أو شبكة تعاون دولي مدعومة بآليات إجرائية جنائية تسهل التواصل المباشر بين الأجهزة في مختلف الدول، على سبيل المثال، في حالات الجرائم المتعلقة بالبث والنشر الفيروسي، قد يتواجد المهاجم في دولة معينة، ولكنه يستهدف دولة أخرى، مما يجعل آثار هذه الجرائم مدمرة وتتخطى الحواجز الجغرافية.

لذا، يتطلب الأمر إزالة العوائق المتعلقة بالحدود والولايات القضائية، لضمان الكشف الفوري عن الجرائم الإلكترونية ومعاقبة مرتكبيها بشكل فعّال.(المظلوم،2013،ص165).

يظهر من خلال الدراسة ان المجتمع الدولي واجه هذه الظاهرة الإجرامية بمجموعة من التشريعات وذلك عن طريق المعاهدات والاتفاقيات، وعلى كافة المستويات.

أولا جهود منظمة الأمم المتحدة ومنظمة اليونيسكو في مكافحة الجريمة الإلكترونية حيث تعتبر منظمة الأمم المتحدة منظمة دولية حكومية، وتُشكل النواة الأولى لتنظيم عالمي، تم توقيع ميثاق الأمم المتحدة في 26 يوليو 1945، ودخل حيز التنفيذ في 26 أكتوبر من نفس العام وتعتبر الأمم المتحدة هيئة مستقلة تتمتع بشخصية قانونية دولية، تأسست من خلال اتفاق بين مجموعة من الدول ذات السيادة، وتفتح باب العضوية لكل دولة تتمتع بالسيادة، لقد بذلت الأمم المتحدة جهودًا كبيرة في مكافحة جرائم الإنترنت، نظرًا لما تسببه هذه الجرائم من

DOI: https://doi.org/10.33193/IJoHSS.69.2025.896

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (69) ديسمبر 2025
Volume (69) December 2025
IJOHSS

أضرار وخسائر جسيمة على الإنسانية جمعاء، وتؤمن المنظمة بأن منع هذه الجرائم ومكافحتها يتطلبان استجابة دولية قائمة على فهم الطابع والأبعاد الدولية للإساءة لاستخدام الكمبيوتر والجرائم المرتبطة بها.

تتمثل أهداف الأمم المتحدة في الحفاظ على السلام والأمن الدوليين، وتعزيز العلاقات الودية بين الدول، وتحقيق التعاون الأمني لمواجهة الجرائم ذات البعد الدولي، وخاصة الجرائم الإلكترونية، من خلال المصادقة على العديد من الاتفاقيات الدولية ذات الصلة.
ومنذ تأسيسها، عملت الأمم المتحدة على وضع سياسة ناجحة لمنع الجريمة وتحقيق العدالة الجنائية، وقد قامت بتشكيل لجان متخصصة، من بينها اللجنة الاستشارية لخبراء منع الجريمة ومعاملة المجرمين، التي تتولى مهمة تقديم المشورة للأمين العام، ورسم السياسات المتعلقة بتدابير دولية تهدف إلى تطوير برامج فعالة في مجال منع الجريمة ومعاملة المجرمين. (الزناتي،2008،ص14).

ثانياً المؤتمرات الدورية لمنظمة الأمم المتحدة لمكافحة الجريمة حيث تعقد منظمة الأمم المتحدة مؤتمرات دورية كل خمس سنوات لتعزيز التعاون الدولي والإقليمي في مجال مكافحة الجريمة، حيث يتبادل الخبراء والمعنيون المعرفة والخبرات. وفيما يلي ملخص لبعض هذه المؤتمرات:

أ- مؤتمر الأمم المتحدة الخامس (جنيف 1975) ناقش المؤتمر تغيرات الجريمة الوطنية والدولية، ودور الشرطة والتشريعات في منع الجريمة، وكيفية معايير معاملة المجرمين داخل السجون، والآثار الاقتصادية والاجتماعية للجريمة.

ب- مؤتمر الأمم المتحدة السادس (كاراكاس 1980) تناول هذا المؤتمر المعدلات الجديدة للجريمة واستراتيجيات مكافحتها، وآليات قضاء الأحداث وإساءة استعمال السلطة، وحقوق الإنسان والمسائل الإصلاحية، والعلاقة بين الجريمة والتنمية الاجتماعية والاقتصادية.

ج- مؤتمر الأمم المتحدة السابع (ميلانو 1985)حيث تم التركيز على استخدام التكنولوجيا في منع الجريمة، وضرورة وجود تدابير لحماية الخصوصية، وتحديث التشريعات لمكافحة جرائم الحاسوب.

د- مؤتمر الأمم المتحدة الثامن (هافانا 1990) حيث دعا المؤتمر لتحديث القوانين الجنائية وتحسين الأمن الإلكتروني، وضرورة تدريب العاملين في مجال مكافحة الجرائم الإلكترونية، ودعم التعاون الدولي لمحاربة الجرائم المتعلقة بالتكنولوجيا.(البدراوي،2011،ص307).

وأما على المستوى الإقليمي فإن الجهود التشريعية الدولية لمكافحة جرائم الإنترنت تتبلور في
جامعة الدول العربية والتي تأسست قبل إنشاء الأمم المتحدة في عام 1944م، حيث تعتبر جامعة الدول العربية أول منظمة دولية إقليمية تُؤسس في العالم، وقد نص ميثاق الجامعة والوثائق المتعلقة بلجانها التحضيرية على دعم الروابط بين الدول العربية، وعقد الاجتماعات الدورية لتوثيق الصلات بينها، وتنظيم خطط التعاون، وتستمر هذه الجهود في إطار دعم تعاون الدول العربية لمواجهة تحديات جرائم الإنترنت، وهو ما يتطلب تطوير الأطر القانونية والتشريعية المناسبة.
بالنتيجة تعتبر الجريمة الإلكترونية من الظواهر التي تتجاوز الحدود الوطنية، مما يستدعي دعم التعاون القانوني الدولي بين الدول لمواجهتها بشكل فعّال، ويتطلب الأمر إنشاء إطار تعاون مدعوم بآليات جنائية تسهل التواصل بين السلطات المختلفة، نظرًا لأن آثار هذه الجرائم يمكن أن تتخطى الحدود الجغرافية بسهولة، لقد بذلت منظمة الأمم المتحدة جهودًا كبيرة في هذا المجال عبر مؤتمرات متكررة واتفاقيات دولية تهدف إلى مكافحة الجريمة الإلكترونية، مشددة على أهمية تطوير استراتيجيات فعالة لمواجهة التحديات الحالية، كما أن الجامعة العربية تسعى إلى دعم التعاون بين الدول العربية لمواجهة هذه الجرائم عن طريق تطوير الأطر القانونية اللازمة.(رجب،1976،ص6).

DOI: https://doi.org/10.33193/IJoHSS.69.2025.896

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (69) ديسمبر 2025
Volume (69) December 2025
IJOHSS

وبرأيي الشخصي إن الاستجابة الفعّالة للجريمة الإلكترونية تتطلب تضافر الجهود وتعاونًا دوليًا حقيقيًا وجدياً، خاصة في ظل التطورات التكنولوجية السريعة، ويجب على الدول أن تتجاوز الإجراءات المنفصلة وأن تعمل بشكل جماعي لاستحداث وإنشاء تدابير شاملة تشمل التشريعات والتدريب وتبادل المعلومات.

الخلاصة تستمر الجريمة الإلكترونية في النمو والتعقيد والتطور، ويجب على المجتمع الدولي، بما في ذلك الدول العربية، أن تعد وتجهز الأطر والتشريعات بطرق جديدة ومتطورة للتعامل معها، وهذا الامر يتطلب التزامًا جادًا من الحكومات والمنظمات الدولية لتطوير القواعد القانونية وتشجيع ودعم المبادرات التعاونية.

المطلب الأول : أهمية التعاون الأمني الدولي ونتائجه:

يعرف التعاون الدولي بأنه تبادل العون والمساعدة والتعاون المشترك بين طرفين دوليين، أو أكثر لتحقيق نفع ، أو خدمة، أو تسهيل في مجال التصدي لمخاطر الجريمة، وما يرتبط بها من مجالات أخرى مثل مجال العدالة الاجتماعية ، ومجال الامن، أو لتخطي مشكلات الحدود والسيادة التي قد تعترض الجهود الوطنية لملاحقة المجرمين وتعقب مصادر التهديد، سواء كانت مساعدة تتمثل قانونًا أو قضائيًا أو إداريًا، وسواء اقتصر على دولتين فقط أو امتدت اقليمياً او عالمياً.

منطقياً يمكن القول ان الجريمة الإلكترونية أصبحت تمثل ظاهرة تتطلب اهتمامًا دوليًا متزايداً كما ذكرنا سابقاً.

ويمثل التعاون الدولي بين الدول وبين الأجهزة المختصة في مكافحة الجرائم الإلكترونية أداة رئيسية للتخفيف من هذه التهديدات، إذ يمكن من خلال هذا التعاون تبادل المعلومات والخبرات، مما يعزز القدرات على التعرف على الأنماط والتوجهات الإجرامية، وبذلك يسهم في تقليل فرص وقوع الجرائم الإلكترونية أو على الأقل الحد منها. (القحطاني،2006،ص38).

تشمل هذه الإجراءات التعاون مع الدول الأخرى لتنفيذ عمليات تتعلق بالتحقيقات التي تحدث خارج حدود الدولة المعنية، مثل مراقبة الأنشطة على الإنترنت، أو الوصول إلى البيانات المحفوظة على الخوادم الأجنبية، أو حتى القيام بعمليات التنصت على اتصالات المجرمين المشتبه بهم.

ولا بد من التأكيد على أهمية التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، حيث لا يمكن للدولة بمفردها أن تعالج هذه القضايا العديدة والمعقدة، فعندما تعبر الجرائم حدود الدول، يصبح من الصعب على الأجهزة المحلية تعقب المجرمين ومتابعتهم بسبب القيود المتعلقة بالسرية والاختصاص القضائي، لهذا السبب يتطلب معالجة هذه الجريمة إجراءات قانونية دولية تهدف إلى تقوية القدرة على التحقيق والملاحقة القضائية للمجرمين عبر الحدود.

لذلك فإن تفعيل التعاون الدولي وتأسيس أطر قانونية ملائمة لمكافحة الجريمة الإلكترونية ليست فقط إجراءات ضرورية، بل هي أيضًا استثمار حيوي للحفاظ على الأمن السيبراني والحد من المخاطر التي تواجه الأفراد والمؤسسات في عصر التكنولوجيا الحديثة.(العبيد،2021،ص514).

وبطبيعة الحال ان التحديات المتزايدة المتعلقة بالجرائم الالكترونية، تبرز الحاجة الملحة لبناء أسس التعاون الأمني الدولي لمكافحة هذه الظاهرة، حيث تُعد الدراسات العلمية عن جرائم المعلوماتية من العناصر الأساسية التي ينبغي تعزيزها، حيث يمكن من خلالها جمع بيانات إحصائية دقيقة حول الجرائم المرتكبة، مما يسهم في فهم الحجم الحقيقي لهذه الظاهرة وتأثيراتها.

إضافة الى ذلك يجب تحديد أنماط واضحة للتعاون بين الأجهزة الامنية على المستويات الدولية، لضمان تحقيق التنسيق الفعال بين الدول في مواجهة هذه التحديات، حيث يتطلب ذلك أيضًا تطوير اتفاقيات دولية تضمن توحيد التشريعات والقوانين المتعلقة بجرائم المعلوماتية، مما يسهل عملية التعاون ويعزز فعالية التصدي لهذه الجرائم. (خراشي،2015،ص.ص23-24).

وأما على المستوى الإقليمي، تم توقيع "الاتفاقية العربية لمكافحة جرائم تقنية المعلومات" في 23 ديسمبر 2010 من قبل مجلس وزراء الداخلية والعدل العرب، وتأتي هذه الاتفاقية في إطار الجهود الحثيثة التي تبذلها جامعة الدول العربية لتعزيز التدابير الأمنية لمكافحة الجرائم المرتبطة بتقنية المعلومات، وذلك ضمن الأسس النظامية والبيئة القانونية القائمة.

تتكون الاتفاقية من ثلاثة وأربعين مادة تمثل التزام الدول الأطراف بإدخال تعديلات قانونية تهدف إلى تجريم مجموعة متنوعة من الجرائم المتعلقة بتقنية المعلومات، والتي تشمل:

- الاختراقات غير المشروعة
- الاعتراض غير المشروع على أسرار البيانات

DOI: https://doi.org/10.33193/IJoHSS.69.2025.896

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (69) ديسمبر 2025
Volume (69) December 2025
IJOHSS

- الاعتداء على سلامة البيانات
- الاعتداء على حرمة الحياة الخاصة
- الاعتداء على الملكية الفكرية
-إساءة استخدام وسائل تقنية المعلومات
-التزوير والاحتيال
-الجرائم المرتبطة بالإرهاب وغسل الأموال والمخدرات
- الاتجار بالجنس البشري وأعضائه والأسلحة
- المساس بالقيم الدينية أو النظام العام
- التهديد والابتزاز
- الاتجار في الآثار والتحف الفنية
- الاستخدام غير المشروع لأدوات الائتمان والوثائق الإلكترونية.

وفي ذات الإطار تتناول الاتفاقية العربية لمكافحة جرائم تقنية المعلومات العديد من الجرائم الرئيسية، ومنها:

- الدخول غير المشروع
- الاعتراض غير المشروع على سريّة البيانات
- الاعتداء على سلامة البيانات
- إساءة استخدام وسائل تقنية المعلومات
- جرائم التزوير والاحتيال
- الجرائم الإباحية وجرائم الاستغلال.

بالنتيجة تعكس هذه الاتفاقية الالتزام الجماعي للدول العربية بمواجهة التحديات المتزايدة في الفضاء الرقمي، مما يضمن سلامة وأمان المجتمعات في عصر الانترنت وتقنية المعلومات.

وأما على المستوى العالمي تبنّت العديد من الدول نماذج رئيسية في سن تشريعات لمواجهة الجرائم الالكترونية، ومن أبرزها دولة السويد والولايات المتحدة الأمريكية وجمهورية فرنسا.

ويتبين لنا بأن دولة السويد كانت رائدة في هذا المجال، حيث أصدرت قانون البيانات عام 1973، الذي تناول قضايا الاحتيال عبر الحاسوب وجرائم الدخول غير المشروع على البيانات، والتزوير وتحويل المعلومات بشكل غير قانوني.

تبعتها الولايات المتحدة، التي شرعت مجموعة من القوانين لحماية أنظمة الحاسوب بين عامي 1976 و1985، وفي عام 1985، قسم معهد العدالة الوطني الجرائم المعلوماتية إلى خمسة أنواع:

- الجرائم الداخلية على الحاسوب.
- الاستخدام غير المشروع عن بعد.
- التلاعب بالحاسوب.
- دعم الأنشطة الإجرامية.
- سرقة البرمجيات والمكونات الفيزيائية للحاسوب.

كما أصدرت الولايات المتحدة عدة تشريعات في عام 1986 لتعريف المصطلحات ذات الصلة بالجرائم المعلوماتية، وفي عام 2000، اعتمدت وزارة العدل الأمريكية تصنيفاً للجرائم المرتبطة بالحاسوب، والذي يتضمن السطو على البيانات وقرصنة البرمجيات والتزوير باستخدام الحاسوب.(الغياثين،2013،ص65).

المطلب الثاني: اتفاقية بودابست (2001) أهدافها ومبادئها:

تناولنا في السابق الجهود التي تبذلها جامعة الدول العربية في سبيل إبرام اتفاقية عربية لمكافحة الجرائم ذات الصلة بتقنية المعلومات، وذلك بهدف حماية المواطن العربي كشخص ضحية ومعرض للجرائم المعلوماتية العابرة للحدود.

ومع تطور الجريمة الدولية واستغلال الأطفال في المواد الاباحية ، وغياب تشريع دولي ملزم للدول لمكافحة الجرائم الإلكترونية بشكل عام، أدى الى فتح مجلس أوروبا باب التوقيع على اتفاقية بودابست في 23 نوفمبر 2001، والتي دخلت حيز النفاذ في 1 يوليو 2004، حيث تعتبر هذه الاتفاقية أول صك دولي يجسد الالتزام

DOI: https://doi.org/10.33193/IJoHSS.69.2025.896

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (69) ديسمبر 2025
Volume (69) December 2025
IJOHSS

بتجريم جميع أشكال الجرائم الإلكترونية، خصوصًا الجرائم المعلوماتية، وتعتبر اتفاقية بودابست المعروفة أيضا باسم اتفاقية الجريمة الإلكترونية، أول معاهدة دولية تسعى إلى معالجة الإنترنت وجرائم الحاسوب عن طريق موائمة القوانين الوطنية لكل دولة، وتحسين أساليب التحري وزيادة التعاون بين الدول.

وفي إطار التغيرات العميقة التي أحدثتها الثورة الرقمية والعولمة المستمرة لشبكات المعلومات، أوضحت الوثيقة التفسيرية للاتفاقية الأثر المترتب على تطور التكنولوجيا والاتصالات، فقد تحولت وسائل الاتصال التقليدية، مثل الهاتف، من مجرد تبادل الصوت إلى إمكانية نقل كميات ضخمة من البيانات التي تشمل الصوت والنصوص والصور والفيديو، مما أدى إلى ارتباط الحواسيب بشكل أكبر مع بعضها البعض.

وخلال صياغة الاتفاقية، أولت الدول أهمية خاصة للتوصيات الصادرة عن لجنة الوزراء بالاتحاد الأوروبي، ومن أبرزها:

- التوصية رقم 85/10، المتعلقة بتنفيذ الاتفاقية الأوروبية للمساعدة المتبادلة في مسائل الجرائم.
- التوصية رقم 88/2، المتعلقة بمسألة القرصنة في حقوق التأليف والنشر.
- التوصية رقم 87/15، التي تناولت تنظيم استخدام البيانات الشخصية في قطاع الشرطة.
- التوصية رقم 95/4، حول حماية البيانات الشخصية في خدمات الاتصالات.
- التوصية رقم 89/9، التي قدمت مبادئ توجيهية لتعريف بعض جرائم الحاسوب.

وتحتوي اتفاقية بودابست الأوروبية لعام 2001 على 44 مادة، حيث يتناول الباب الأول المصطلحات المستخدمة في الاتفاقية، وتُعتبر هذه الاتفاقية من بين أولى الاتفاقيات التي تصدت للاستخدام غير المشروع للحاسبات وشبكات المعلومات، كما تحدد معيارًا مشتركًا لوضع حد أدنى يعتبر بموجبه بعض التصرفات بمثابة جرائم جنائية، مما يستدعي التنسيق التشريعي بين الدول لمكافحة التصرفات غير المشروعة، خصوصًا تلك التي تعتمد تشريعات أقل صرامة من الاتفاقية.

بالتالي يهدف إبرام اتفاقية بودابست لمكافحة الجرائم الإلكترونية إلى إكمال المعاهدات أو الترتيبات الثنائية أو متعددة الأطراف بين الدول، ومن أبرز هذه المعاهدات:

1- الاتفاقية الأوروبية لتسليم المجرمين، التي فتحت للتوقيع في باريس في 13 ديسمبر 1957.
2- الاتفاقية الأوروبية للمساعدة المتبادلة في المسائل الجنائية، التي فُتِحَت في ستراسبورغ في 20 أبريل 1959.
3- البرتوكول الإضافي للاتفاقية الأوروبية المتعلقة بالمساعدة المتبادلة، الذي فُتِحَ في ستراسبورغ في 17 مارس 1978. (أحمد،2011،ص5).

ومن هذا المنطلق تُستكمل الاتفاقية ببروتوكولات إضافية تعمل على توسيع نطاقها وتعزيز فعاليتها في مكافحة الجرائم الإلكترونية، مع ضمانات لحقوق الإنسان.

تجدر الإشارة الى أن المغرب هي إحدى الدول العربية التي صدقت على اتفاقية بودابست، حيث تمت المصادقة في 29 يونيو 2018، ودخلت حيز التنفيذ في 1 أكتوبر 2018.(المطيري، 2020،ص47).

ونخلص إلى القول، إن الاتفاقية الأوروبية (بودابست) لمكافحة الجريمة الإلكترونية لعام 2001 تهدف إلى تحقيق الحماية الإجرائية والعقابية للنظم المعلوماتية، وذلك من خلال إلزام الدول الأطراف اتخاذ التدابير التشريعية الإجرائية والعقابية ضد كل من يرتكب جرائم معلوماتية على النظم المعلوماتية، بهدف حذف تقنية المعلومات، أو تغييرها، أو إلغائها، أو إتلافها دون وجه حق، وفقاً للمادة 5 والمادة 2 من الاتفاقية.

أما على مستوى دولة قطر أو العلاقة بين دولة قطر واتفاقية بودابست لمكافحة الجرائم الإلكترونية تظهر النتائج ان دولة قطر ليست طرفًا في اتفاقية بودابست بشأن الجرائم الإلكترونية، التي تم إبرامها في عام 2001 والتي تُعتبر أول معاهدة دولية تعالج قضايا جرائم الإنترنت كما ذكرنا ، بدلاً من ذلك تبذل دولة قطر جهودها على مكافحة الجريمة السيبرانية من خلال دعم التعاون مع الأمم المتحدة، وهو ما يتجلى ويظهر في إنشاء مركز الأمم المتحدة الإقليمي لمكافحة الجريمة السيبرانية في الدوحة حيث يسعى المركز إلى دعم وتطوير البرنامج العالمي لمكافحة الجريمة السيبرانية من خلال تقديم التدريب وبناء القدرات للدول الأعضاء.

وتسعى دولة قطر بذلك إلى تفعيل دورها في مكافحة الجريمة السيبرانية ودعم التعاون الدولي في هذا المجال الحساس.

DOI: https://doi.org/10.33193/IJoHSS.69.2025.896

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (69) ديسمبر 2025
Volume (69) December 2025
IJOHSS

المبحث الثالث : طرق مكافحة الجرائم الالكترونية /التشريعات العربية والأجنبية نموذجاً :

نشأت الجريمة مع ظهور المجتمع البشري وازدهرت مع تطور الحياة فيه، بما في ذلك التطورات في جميع المجالات الاقتصادية والاجتماعية والصناعية، وقد أدى ذلك إلى ظهور ثقافات جديدة ساهمت في تحفيز أنماط سلوكية اجرامية منحرفة، ومع ظهور هذه الأنماط انتشرت الجريمة وأصبحت تهديدًا جديًا للنظام العام ككل في المجتمع، مما دفع الدول العربية والاجنبية إلى إصدار تشريعات لمواجهة الجرائم الحديثة، وفي مقدمتها الجرائم المعلوماتية.

أولاً التشريع الكويتي:

أظهرت بعض الدراسات الأمنية التي أجرتها السلطات الأمنية في دولة الكويت خطورة وحجم جرائم الإنترنت التي تزايدت في الآونة الأخيرة، حيث تم ضبط مواقع إباحية في العديد من الدول الغربية، بما في ذلك أوروبا وأمريكا، وحاول بعض المشبوهين استغلال هذه الجرائم داخل الكويت من خلال توزيع الصور الفاضحة والمخلة، كما أظهرت الإحصائيات وجود بعض الأنشطة الإجرامية التي ترتكب ضد البيانات والحسابات المصرفية الشخصية .(المري،2013،ص48).

ولم يكن المشرع الكويتي، بمعزل عن هذا التطور الجديد في شكل الجرائم والأنشطة الإجرامية الحديثة التي جعلت العالم أشبه بقرية صغيرة، فقد كان القضاء الكويتي سابقًا يطبق القواعد العامة في القانون الجزائي على الجرائم المعلوماتية، ومن أبرز تلك القوانين القانون رقم 9 لسنة 2001 بشأن إساءة استعمال أجهزة الاتصالات الهاتفية وأجهزة التنصت، وقد تم إضافة فقرة إلى المادة الأولى منه بتاريخ 1 يوليو 2007، وذلك بموجب القانون رقم 40 لسنة 2007، وجاءت المادة الأولى مكرر منه على النحو التالي:

" يعاقب بالحبس مدة لا تجاوز سنتين وبغرامة لا تتجاوز ألفي دينار أو بإحدى هاتين العقوبتين كل من تعمد الإساءة أو التشهير بغيره عن طريق استعمال جهاز أو وسيلة من وسائل الاتصال الهاتفية أو غيرها في التقاط صورة أو أكثر أو مقاطع فيديو له دون علمه أو رضاه، أو استغل إمكانات هذه الأجهزة واستخرج صوراً منها دون إذن أو علم أصحابها، أو قام باصطناع صور تخدش الآداب العامة لأشخاص آخرين".

و"يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تتجاوز ثلاثة آلاف دينار أو بإحدى هاتين العقوبتين كل من قام عن طريق هذه الأجهزة أو الوسائل بإرسال الصور المذكورة في الفقرة السابقة، أو أي صورة أو مقطع فيديو تخدش الآداب العامة إلى أشخاص آخرين، أو قام بنشرها أو تداولها بأي وسيلة كانت".

وتكون العقوبة الحبس مدة لا تجاوز خمس سنوات والغرامة التي لا تتجاوز خمسة آلاف دينار إذا اقترنت الأفعال المذكورة في أي من الفقرتين السابقتين بالتهديد أو الابتزاز أو تضمنت استغلال الصور بأي وسيلة في الإخلال بالحياة أو المساس بالعراض أو التحريض على الفسق والفجور.

ويحكم في جميع الأحوال بمصادرة أجهزة ووسائل الاتصال أو غيرها مما استخدم في ارتكاب الجريمة.(المادة الأولى مكرر من القانون رقم 9 لسنة 2001 ، والمضافة بالقانون رقم40 لسنة 2007).

ثانياً التشريع المصري:

في ظل التطورات المتلاحقة للإنترنت واختلاف أشكال الجريمة المعلوماتية العابرة للحدود، لم تكن جمهورية مصر العربية بمعزل عن هذا التطور، فقد أصدر رئيس الجمهورية قرارًا برقم 276 لسنة 2014 بالموافقة على انضمام جمهورية مصر العربية إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، كما أصدر رئيس مجلس الوزراء ثلاثة قرارات، الأول برقم 2259 لسنة 2014 بإنشاء مجلس أعلى لأمن البنى التحتية للاتصالات وتكنولوجيا المعلومات، والثاني برقم 1453 لسنة 2015 بشأن إنشاء مجلس أعلى للمجتمع الرقمي وتحديد اختصاصاته، والثالث برقم 994 لسنة 2017 والمتعلق بتنفيذ الجهود الحكومية لقرارات وتوصيات المجلس الأعلى للأمن السيبراني.

DOI: https://doi.org/10.33193/IJoHSS.69.2025.896

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (69) ديسمبر 2025
Volume (69) December 2025
IJOHSS

وايمانًا من المشرع المصري بضرورة مكافحة الجرائم المعلوماتية، فقد وضع العديد من العقوبات لبعض الجرائم التي تنطوي على المساس بالنظم والبيانات المعلوماتية، ولعل أبرز ما تم تضمينه في القانون رقم 175 لسنة 2018 هو العقوبات التالية: (الهاجري،2025،ص 498)

- جريمة الانتفاع بدون وجه حق بخدمات الاتصالات والمعلومات وتقنيتها.
- جريمة تجاوز حدود الحق في الدخول إلى الحسابات الخاصة والنظم المعلوماتية.
- جريمة الدخول غير المشروع على نظام معلوماتي محظور الدخول عليه أو على موقع أو حساب خاص.
- جريمة الاعتراض غير المشروع بدون وجه حق على المعلومات والبيانات أو كل ما هو متبادل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي.
- جريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية سواء بتعطيلها، أو إتلافها، أو تعديلها، أو إلغاء كلي ،أو جزئي للبرامج والبيانات والمعلومات المخزنة، أو المعالجة، أو المولدة، أو المنشئا على أي نظام معلوماتي وما في حكمه.
- جريمة الاعتداء على البريد الإلكتروني أو المواقع أو الحسابات الخاصة.
- جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة.
- جريمة الاعتداء على سلامة الشبكة المعلوماتية.
- جرائم الاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإلكتروني.
- الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي غير المشروع.(المادة السادسة من القانون رقم 175 لسنة 2018).

ثالثاً تشريعات المملكة العربية السعودية :

أثبتت الدراسات في العاصمة السعودية الرياض أن هناك أكثر من 23 مليون عملية هجوم إلكتروني جاءت من 126 دولة على أنظمة الحاسب الآلي، وفقاً لدراسة أمن الإنترنت خلال الملتقى العلمي لمكافحة المعلوماتية في مدينة الرياض، واجه مستخدمو أجهزة الحاسب الآلي في 215 دولة في عام 2010/2009 حوالي 32.6 مليون عملية هجوم إلكتروني، وقد احتلت الدول العربية، بما في ذلك السعودية، مركزاً متقدماً بين الدول المستهدفة بهذه العمليات غير المشروعة، حيث وصل معدل الانتهاكات المعلوماتية في السعودية إلى 2.27 من إجمالي الاعتداءات.

بالتالي صدر قرار رئيس مجلس الوزراء رقم 79 بتاريخ 7/3/1428هـ، المتعلق بنظام مكافحة الجرائم المعلوماتية، وصدق عليه بالمرسوم الملكي رقم (م/17) بتاريخ 8/3/1428، الموافق 8/3/2007، الذي تضمن نظاماً لمكافحة الجرائم المعلوماتية.

حيث تضمن المرسوم نصوصاً تُجرم التنصت على ما يُرسل إلى أجهزة الحاسب الآلي دون مسوغ نظامي صحيح، والدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عن القيام به، وكذلك إعاقة الوصول للخدمة أو مسح البرامج أو البيانات المستخدمة، بالإضافة إلى جرائم أخرى تتعلق بأنشطة إجرامية.(العنزي،2021،ص112).

رابعاً التشريعات الأجنبية:

تعتبر أهم نماذج التشريعات التي شرعت قوانين مواجهة الجرائم المعلوماتية الولايات المتحدة الأمريكية، والقانون الفرنسي، والقانون السويدي، وغيرهم، ونوضح ذلك:

في البداية، كانت دولة السويد هي أول دولة تقوم بسن تشريعات خاصة بجرائم الحاسب الآلي والإنترنت، فصدر قانون البيانات السويدي عام 1973 م، الذي اختص بمعالجة قضايا الاحتيال بواسطة الحاسب الآلي، شمل القانون نصوصًا عامة خاصة بجرائم الدخول غير المشروع على البيانات الحاسوبية، أو تزويرها، أو تحويلها، أو الحصول غير المشروع عليها.

ثم تأتي الولايات المتحدة الأمريكية خلف دولة السويد حيث وضعت قواعد لقوانين متعلقة بحماية أنظمة الحاسب الآلي (1976 – 1985)، وفي عام 1985 قسم معهد العدالة القومي الجرائم المعلوماتية لخمسة أنواع وهي

DOI: https://doi.org/10.33193/IJoHSS.69.2025.896

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (69) ديسمبر 2025
Volume (69) December 2025
IJOHSS

جرائم الحاسب الآلي الداخلية، وجرائم الاستخدام غير المشروع عن بعد، وجرائم التلاعب بالحاسب الآلي، ودعم التعاملات الإجرامية، سرقة البرامج والأجهزة والمكونات المادية للحاسب.

وبالتالي أصدرت الولايات المتحدة الأمريكية عدة تشريعات لمواجهة الجرائم المعلوماتية، منها:
- قانون حماية أنظمة الحاسب الآلي عام 1976.
- قانون الاحتيال وإساءة استغلال الحاسب الآلي عام 1984.
- قانون أمن الحاسب الآلي عام 1987.
- عدة قوانين أخرى خاصة بالولايات، نذكر منها قانون ولاية تكساس لجرائم الحاسب الآلي.

وصولا الى العام 2000، حيث أقرّت وزارة العدل الأمريكية تصنيفًا لأنواع الجرائم المتعلقة بالحاسوب، وذلك في إطار تطبيق قانون الحاسوب الفيدرالي من قبل مكتب التحقيقات الفيدرالي (FBI)، ومن أهم هذه التصنيفات، السطو على بيانات الحاسوب، الاحتيال باستخدام كلمات السر، انتهاك حقوق الطبع والنشر، بما في ذلك الأفلام والبرامج والتسجيلات الصوتية، بالإضافة إلى جرائم القرصنة.

وسرقة الأسرار التجارية من خلال استخدام الحاسوب، تزوير العلامات التجارية باستخدام الحاسوب، تزوير العملة بوسائل الحاسوب، الاحتيال والازعاج من خلال استخدام الحاسوب.

أيضا في الجهة المقابلة قامت كندا في عام 1985، بتعديل قانونها الجنائي وأدرجت مواد خاصة بجرائم الحاسوب والإنترنت، وحددت العقوبات المتعلقة بهذه الجرائم، بما في ذلك الجرائم الحاسوبية وجرائم التدمير أو الدخول غير المشروع إلى أنظمة الحاسوب.(المراغي،2016،ص54).

وفي عام 1986، أصدرت ألمانيا الاتحادية القانون الثاني لمكافحة الجرائم الاقتصادية، الذي جرم إتلاف أو تعديل أو تزوير البيانات معالجة إلكترونيًا، وشدد العقوبات على البيانات ذات الأهمية الأساسية لقطاع الأعمال أو السلطة الإدارية، لتصل العقوبات إلى السجن لمدة خمس سنوات والغرامة. كما جرم القانون النصب والاحتيال باستخدام الحاسوب وفرض عقوبة لذلك.

وفي عام 1988، طورت فرنسا القوانين الجنائية الخاصة بها بإضافة جرائم الحاسوب إلى القانون الجنائي الفرنسي. وفي عام 1994، أصدرت فرنسا قانون العقوبات الجديد الذي نظم معالجة البيانات إلكترونيًا في المادة 323 بفقراتها الأربعة. كما منحت النيابة العامة سلطات التحقيق، ومواجهة الشهود، والقيام بالتحريات في الجرائم المعلوماتية.(القاضي،2011،ص58).

يتبين لنا من خلال ما ذكرنا أن التشريعات القانونية لمواجهة الجرائم السيبرانية قد تطورت بشكل ملحوظ في البلدان المختلفة، ونجد أن القوانين التي تم وضعها لمكافحة الجرائم الإلكترونية تتمحور حول عدة نقاط أساسية مثل حماية البيانات، تجريم الدخول غير المشروع إلى الأنظمة، والتعويض عن الأضرار الناتجة عن الجرائم الحاسوبية، بالإضافة إلى ذلك، فإن هذه التشريعات تتيح للجهات القانونية ووسائل التحقيق القدرة على معالجة الجرائم بشكل فعال، وتشير هذه التشريعات إلى وعي متزايد بمخاطر الفضاء الإلكتروني والجرائم المرتبطة به، حيث تسعى الحكومات إلى توفير حماية قانونية فعالة لكل من الأفراد والمؤسسات في هذا السياق، ومع ذلك، يبقى التحدي في توافق هذه القوانين مع التطورات السريعة للتكنولوجيا والممارسات السيبرانية الجديدة، وأرى أن هناك حاجة ماسة لتطوير هذه القوانين باستمرار لتتناسب مع قاعدة التكنولوجيا المتسارعة وتطبيق أساليب جديدة لمكافحة الجرائم السيبرانية، يجب أن تتعاون الحكومات مع شركات التكنولوجيا والتعليم لزيادة الوعي العام حول الأمان الرقمي.

المطلب الأول: التحديات التي تواجه التعاون الدولي ودور المنظمات الدولية والإقليمية لمكافحة الجرائم الإلكترونية:

التعاون الدولي في مجال مكافحة الجريمة الإلكترونية هو مجموع الآليات القانونية والمؤسسية والإجرائية التي تتخذها الدول والمنظمات الدولية لتبادل المعلومات، والمساعدة القضائية، وتنسيق الجهود في التحقيق والملاحقة والمعاقبة على الجرائم التي تُرتكب عبر الفضاء الإلكتروني، والتي غالبًا ما تتجاوز الحدود الجغرافية للدول، بمعنى آخر لا يمكن لأي دولة بمفردها أن تواجه الجريمة الإلكترونية لأن الأدلة والمجرمين والضحايا قد يكونوا في دول مختلفة.

من جهة أخرى تظهر أهمية أسباب الحاجة للتعاون الدولي وذلك بسبب ان الجريمة الإلكترونية غالبًا لا ترتكب داخل إقليم واحد، مثلًا يمكن أن يكون الجاني في آسيا، والضحية في أوروبا.

DOI: https://doi.org/10.33193/IJoHSS.69.2025.896

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (69) ديسمبر 2025
Volume (69) December 2025
IJOHSS

تعتبر الجرائم الإلكترونية واحدة من أكبر التحديات التي تواجه الدول في العصر الرقمي الحالي الحديث، وذلك نظرًا لتعقيدها وسرعتها في التطور، وبالتالي أصبح من الضروري فهم ودراسة التحديات التي تعترضها في سبيل التعاون الوطني والدولي في هذا المجال.

أولا ترتكب الجريمة الإلكترونية في بيئة النظم المعلوماتية ، وما يميز الجريمة الإلكترونية عن الجرائم التقليدية هو استخدامها للأدوات الرقمية مثل الحاسوب والشبكة الإلكترونية، وتتجلى هذه الجرائم في النظام المعلوماتي، حيث تُرتكب خلال مراحل مختلفة من معالجة المعلومات، سواء كانت في مرحلة الإدخال أو المعالجة أو الإخراج. هذا النمط من الجرائم يجعل التعقب والملاحقة القانونية أمورًا معقدة، إذ تختبئ الأفعال الإجرامية خلف الستار الرقمي.

ثانياً أهداف المجرم المعلوماتي، الهدف الأساسي لمجرم المعلوماتية هو النظم المعلوماتية نفسها، ومع تزايد اعتماد الأفراد والقطاعين العام والخاص على المعلوماتية، أصبحت هذه الأنظمة عرضة للهجمات. يمكن للمجرمين تجاوز الرقابة الأمنية المتبعة، مما يزيد من المخاطر المترتبة على هذه الجرائم. بالإضافة إلى ذلك، فإن استخدام الشبكات الإلكترونية يمنح المجرمين القدرة على التسلط على أنظمة التحكم والدفاع، مما قد يؤدي إلى تعطيل الأنظمة الحيوية، مثل شبكات الكهرباء والمياه والمصارف.(شاهين،2018،ص41).

ثالثاً التأثيرات الأمنية السلبية في الجرائم الإلكترونية حيث تظهر المخاطر المرتبطة بالجرائم الإلكترونية بوضوح في الجوانب الأمنية؛ إذ يمكن لقراصنة المعلومات اختراق مواقع التجارة الإلكترونية وسرقة البيانات الحساسة، مثل أرقام بطاقات الائتمان، أو تخريب المواقع برموز ضارة. هذه الأفعال لا تؤثر فقط على الأفراد، بل تؤثر أيضًا سلبًا على التجارة الإلكترونية، مما يؤدي إلى تردد المستخدمين في إجراء المعاملات عبر الشبكة. ووفقًا لاستبيانات أُجريت، يعود سبب إحجام 53% من المستخدمين عن استخدام التجارة الإلكترونية إلى عدم وجود أمان كافٍ، بينما يعاني الآخرون من صعوبات في التصفح وارتفاع الأسعار . (الكعبي، 2010،ص.ص 177-179).

رابعاً الجريمة العابرة للحدود الوطنية ،لم تعد الجرائم الإلكترونية مقصورة على حدود دولة واحدة؛ بل أصبحت تجري عبر الحدود بتعقيد متزايد. بفضل التكنولوجيا الحديثة، يمكن أن تنفذ الجريمة في دولة، وتحقق تأثيراتها في دولة أخرى في غضون ثوانٍ، مما يعكس حتمية ضرورة التعاون الدولي لمكافحتها.

خامساً نقص الاتفاقيات الدولية ، يعد غياب الاتفاقيات والمعاهدات الدولية اللازمة للتعاون في الجريمة الإلكترونية واحدة من أبرز العوائق، رغم وجود بعض الاتفاقيات، مثل الاتفاقية الأوروبية في بودابست لعام 2001 وغيرها من المعاهدات العربية، إلا أنها تظل غير كافية، فعدم وجود إطار قانوني موحد يشكل تحديًا كبيرًا، إذ لا توجد نماذج متفق عليها عالميًا لتحقيق التعاون الفعال بين الدول.(إبراهيم،2009، ص87).
أما بالنسبة الى مسألة التحديات في الجرائم الإلكترونية على المستوى الدولي، يظهر في اختلاف التشريعات الوطنية، يعتبر اختلاف التشريعات الوطنية من أبرز العوائق التي تؤثر على تحقيق التعاون الدولي في مكافحة الجرائم الإلكترونية، حيث تتطلب المعاهدات القانونية تجريم الفعل نفسه في التشريعات المحلية، وتعاني معظم الدول من عدم وجود آليات مناسبة لمواجهة الجرائم الإلكترونية وتطبيق القواعد التقليدية، مما يؤدي إلى عدم توافق فيما يتعلق بنماذج الجرائم الواجب تجريمها، يرجع ذلك إلى اختلاف البيئات والعادات والثقافات، مما يعقد التشريعات من مجتمع إلى آخر. (دورماز،2024،مقال)
أيضاً اختلاف النظم القانونية الإجرائية الجنائية، حيث تتميز النظم القانونية الإجرائية بتنوعها، مما يؤدي إلى أن أساليب التحقيق قد تكون فعالة في دولة واحدة وغير مفيدة في أخرى. قد تعتبر بعض الإجراءات القانونية مثل المراقبة الإلكترونية غير مقبولة في دول معينة، مما يعرقل تحقيق العدالة، هذا التباين يترك السلطات القانونية في موقف صعب، خاصة حين يتعلق الأمر باستخدام الأدلة التي قد تكون ملتزمة بشروط قانونية مختلفة من دولة لأخرى.

DOI: https://doi.org/10.33193/IJoHSS.69.2025.896

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (69) ديسمبر 2025
Volume (69) December 2025
IJOHSS

ايضاً تنازع الاختصاص القضائي الدولي من التحديات البارزة وعلى الرغم من وجود معاهدات تسهل تبادل الأدلة، إلا أن عدم تحديد الاختصاص يتسبب في مشكلات خلال عمليات الاستدلال والتحقيق في الجرائم الإلكترونية، بحكم طبيعتها العابرة للحدود، تجعل الكشف عن الأدلة واستخدامها معقدًا، مما يتطلب تنسيقًا قانونيًا دوليًا أفضل، والصعوبات في المساعدات القضائية الدولية حيث تتبع تحديات المساعدات القضائية الدولية من بطء الإجراءات الدبلوماسية، مما يتعارض مع الطبيعة السريعة للجرائم الإلكترونية، كما قد يتسبب التباطؤ في الردود من الدول المتلقية في فقدان الفرصة لجمع الأدلة الضرورية، مما ينجم عنه إغلاق قضايا مهمة بدون تحقيق العدالة.

ايضاً نقص قنوات الاتصال، بالتالي إن نجاح التعاون الدولي في مكافحة الجرائم الإلكترونية يتطلب وجود قنوات اتصال فعّالة لجمع المعلومات، وعدم وجود نظام يسهل الاتصال بين الجهات المعنية يعوق جهود جمع الأدلة، وبذلك تتلاشى فرص تحقيق النجاح في التصدي للمجرمين، وتفشل قيمة هذا التعاون.(إبراهيم،2009،ص.ص 414-415)

استناداً الى ما سبق عرضه يتبين لنا ان جهود التعاون الدولي في مكافحة الجرائم الإلكترونية تواجه مجموعة من التحديات الكبيرة على المستويين الدولي والوطني، ويمكن القول إن مكافحة الجرائم الإلكترونية تتطلب استراتيجية شاملة تتجاوز الحدود الجغرافية والتشريعية، وتحتاج الدول إلى العمل نحو توحيد القوانين وتطوير آليات التعاون الدولي لتسهيل تبادل المعلومات والأدلة، بالإضافة إلى ذلك، يجب تسريع الإجراءات القضائية وتطوير قنوات اتصال فعالة بين الهيئات القانونية في مختلف الدول.

ونستنتج ان النجاح في مكافحة الجرائم الإلكترونية على المستويين الوطني والدولي يعتمد على قدرة الدول على التغلب على الفجوات التشريعية والإجرائية التي تعوق التعاون، من خلال دعم الشراكات الدولية وتحقيق التنسيق بين الجهات القانونية، يمكن تحقيق نتائج أفضل في التصدي للجرائم التي تتجاوز الحدود التقليدية.

بالتالي تظهر المشكلة الأساسية في الفرق بين السرعة التي تتم بها الجرائم الإلكترونية وسرعة الاستجابة القضائية، حيث لا يمكن أن تستمر الدول في اعتماد المنهجيات التقليدية لمكافحة الجريمة، بل يجب عليها أن تتبنى نهجًا مبتكرًا يستفيد من التكنولوجيا الحديثة ويسمح بالاستجابة السريعة والمرنة للتحديات المتطورة، ويجب أيضًا أن يكون هناك مزيد من التوعية حول الجرائم الإلكترونية في المستويات الاجتماعية، مما يعزز من الوعي العام حول كيفية الوقاية والتعامل مع هذه التهديدات.

في الخلاصة، يتطلب الأمر استجابة متكاملة متعددة الأطراف للتصدي للجرائم الإلكترونية بفعالية، وهذا يتطلب إعادة تقييم التشريعات والآليات الحالية لضمان أنها تظل فعالة وملائمة للعصر الرقمي.

المطلب الثاني: التعاون الدولي في مجال التدريب لمكافحة الجرائم المعلوماتية/ جهود دولة قطر العملية

أدى ظهور أنماط جديدة في الجرائم المعلوماتية مثل القرصنة والاحتيال الالكتروني والابتزاز الالكتروني وغيره إلى وجود تحديات كبيرة لأجهزة العدالة، حيث تتميز هذه الجرائم بخصائص تجعلها تختلف عن باقي الجرائم ، مما يستدعي تأهيل العاملين في هذا المجال ليكونوا قادرين على التصدي لها بكفاءة.

بداية أهمية تأهيل القائمين على أجهزة مكافحة الجرائم المعلوماتية، حيث تعتبر برامج التدريب أداة حيوية لتحقيق الأهداف في مجال مكافحة الجرائم المعلوماتية، حيث تسهم في بناء الخبرات والمهارات اللازمة للعاملين، ويُعد التدريب ضرورة ملحة للجميع، سواء كانوا موظفين في الحكومة أو في القطاع الخاص، ويساعد في رفع كفاءة الأداء وتطوير الأساليب اللازمة لمواجهة هذه التحديات، في الوقت ذاته يحتاج العاملون في هذا المجال إلى تدريب متخصص يتضمن معرفة بأحدث التقنيات ووسائل التصدي للجرائم. ويجب أن تشمل البرامج التدريبية محتوى متنوعاً حول التهديدات ونقاط الضعف في الشبكات، بالإضافة إلى تحليل الجرائم الإلكترونية ووسائل الوقاية منها.

وتتطلب عملية التدريب أيضاً مهارات عملية تتعلق بالتحليل والتقييم، مما يضمن نتاجاً فعّالاً وقدرة أكبر على مواجهة الجرائم المعلوماتية. كما يجب أن تكون هذه البرامج مرنة وقابلة للتكيف مع التطورات السريعة في هذا المجال، مما يسهم في تعزيز الثقافة القانونية والتكنولوجية لدى المشاركين .

DOI: https://doi.org/10.33193/IJoHSS.69.2025.896

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (69) ديسمبر 2025
Volume (69) December 2025
IJOHSS

تمثل الاتفاقيات الدولية والإقليمية القادرة على دعم هذا التعاون ركيزة أساسية، حيث تدعو إلى تبادل المعرفة والخبرات بين الدول، على سبيل المثال، تنص المادة 1 من الاتفاقية العربية لمكافحة الجريمة المنظمة وتسلط الضوء على أهمية هذا التعاون، خاصة في التدريب على مواجهة الجرائم المرتبطة بشبكة الإنترنت.
في الولايات المتحدة الأمريكية، على سبيل المثال ايضاً، تُخصص برامج تدريبية لدعم قدرات العدالة الجنائية في دول أخرى، مما يُعزّز من فعالية الأنظمة القضائية، بالإضافة إلى زيادة الكفاءة في مواجهة الجرائم قبل أن تنتشر خارج الحدود، حيث تسهم هذه المبادرات في دعم التعاون الدولي وفتح أفق تبادل المعرفة على المستوى العالمي.
تقوم الدول المتقدمة بعقد الندوات والمؤتمرات وحلقات النقاش سواء داخل أراضيها أو خارجها، وتوفر برامج تدريبية متخصصة تُمكّن كفاءات رجال العدالة على سبيل الذكر وليس الحصر، كما يتم تبادل الخبرات وتطوير قدرات العاملين في العدالة الجنائية عبر إرسال فرق فنية للمشاركة في برامج تدريبية خارجية.(أبو نمر،2021،ص.ص36-37).
بناءً على ما تقدم تعود الفوائد العديدة لهذه البرامج على المشاركين، حيث تتيح لهم تبادل الآراء والخبرات، وترفع من مستوى الثقة بين الدول في قدراتها على التعاون في مكافحة الجرائم، ويُمكن أن تسهم هذه الجهود في زيادة مهارات ومسؤوليات المشاركين مما يُؤدي إلى تحسين فعالية جهودهم في مواجهة التحديات الجنائية، وبالتالي يمثل ذلك مرجعاً لتعزيز التعاون الدولي.
ومن هذا المنطلق لا بد من تسليط الضوء على جهود دولة قطر العملية في مواجهة الجرائم الإلكترونية حيث تتجلى فيما يلي من عدة جهات:

من جهة المؤسسات تتمتع دولة قطر بمجموعة متنوعة من المؤسسات المهمة الرئيسية التي تلعب دوراً حيوياً في مكافحة الجرائم المعلوماتية، من أبرز هذه المؤسسات وزارة الداخلية، والتي تدير قسم الجرائم الإلكترونية المُخصص لمتابعة والحد من هذه التهديدات، بالإضافة إلى ذلك، تسهم هيئة تنظيم الاتصالات بشكل كبير من خلال وضع السياسات والتشريعات اللازمة وتنظيم آليات الأمن السيبراني في الدولة. تشكل هذه الهيئات والتعاون بينها قاعدة صلبة لتطوير استراتيجيات فعالة لدعم الأمن السيبراني وحماية المعلومات الحساسة.
أما من جهة الاستراتيجيات، حيث وضعت دولة قطر استراتيجيات وطنية متكاملة تهدف إلى دعم الأمن السيبراني وحماية المعلومات الحيوية، وتشمل هذه الاستراتيجيات تطوير البنية التحتية الرقمية وتعزيز قدرات الاستجابة للتصدي للتهديدات السيبرانية، كما تتضمن توعية الجمهور بأهمية الأمان السيبراني، مما يُساهم في بناء مجتمع أكثر استعداداً للتفاعل مع التحديات الرقمية، من خلال هذه الاستراتيجيات، تسعى دولة قطر إلى تحقيق بيئة آمنة تتيح الاستخدام الآمن للتكنولوجيا في جميع القطاعات.

وجهة الشراكة الدولية حيث تدعم دولة قطر من شراكاتها الدولية من خلال توقيع اتفاقيات متعددة مع دول أخرى ومنظمات دولية متخصصة، بهدف تبادل المعلومات والخبرات الضرورية لمواجهة الجرائم الإلكترونية. يُعتبر هذا التعاون الدولي حيويًا، حيث يسمح بزيادة فعالية الاستجابة للتهديدات السيبرانية ودعم القدرات الوطنية، وذلك من خلال تبادل أفضل الممارسات وتعزيز التنسيق بين الدول، وتقوم دولة قطر بتوسيع نطاق جهودها لمكافحة الجريمة الإلكترونية بشكل فعّال.
في الختام ومن جهة المبادرات، أطلقت دولة قطر العديد من المبادرات التعليمية والتدريبية لأفراد القطاعين الحكومي والخاص لتعزيز مهاراتهم في مجال الأمن السيبراني، وتهدف هذه المبادرات إلى توفير المعرفة اللازمة للتصدي للتحديات الإلكترونية ونشر الوعي العام بالمخاطر، كما تُشجع هذه البرامج المجتمع على اتخاذ تدابير احترازية، مما يُقلل من المخاطر المحتملة، يعتبر الاستثمار في تدريب الكوادر البشرية عنصراً أساسياً في بناء قدرات وطنية قوية لمواجهة التهديدات السيبرانية.
بالرغم من الجهود المبذولة التي ذكرناها، تواجه دولة قطر مجموعة من التحديات المعقدة في مجال الأمن السيبراني، تتضمن هذه التحديات تطور الأساليب المستخدمة في الجرائم الإلكترونية، مما يجعل من الصعب متابعة ومواجهة هذه التهديدات بشكل فعّال، و بالإضافة إلى ذلك، يُعد قلة الوعي العام بالمخاطر أحد العوائق الرئيسية، فضلاً عن الحاجة إلى دعم التنسيق بين مختلف المؤسّسات الحكومية والخاصة لتحقيق الأمن السيبراني

DOI: https://doi.org/10.33193/IJoHSS.69.2025.896

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (69) ديسمبر 2025
Volume (69) December 2025
IJOHSS

بشكل فعّال، تواجه دولة قطر هذه التحديات بشكل نشط، وتبذل جهوداً مستمرة لتطوير استراتيجيات تتماشى مع البيئة الرقمية المتغيرة.
وفي المقابل تستمر دولة قطر في التزامها بتعزيز التعاون الدولي وتنمية قدراتها لمواجهة التحديات المستمرة في عالم الجرائم المعلوماتية. من خلال الاستمرار في تحديث وتطوير استراتيجياتها، تهدف الدولة إلى أن تكون نموذجًا يُحتذى به في مجال الأمن السيبراني على مستوى المنطقة والعالم.

الخاتمة:

خلص هذا البحث إلى أن الجريمة الإلكترونية تُعد تحديًا عالميًا يتطلب دعم التعاون الدولي، حيث قدمت اتفاقية بودابست نموذجًا متقدمًا من الناحيتين القانونية والإجرائية لمكافحة هذه المسألة او القضية، وقد أظهرت الدراسة أن دولة قطر أحرزت تقدمًا ملحوظًا في هذا المجال من خلال سن التشريعات الوطنية وإرساء الأطر المؤسسية الضرورية، ومع ذلك، هناك حاجة ملحة للتوافق بشكل أكبر مع المعايير الدولية لضمان فاعلية أعلى في التعاون عبر الحدود.
وعلى الرغم من القوانين المُتقدمة، لا تزال هناك ثغرات في تبادل المعلومات بين الدول لمواجهة الجرائم السيبرانية العابرة للحدود، وتتطلب التحديات المتعلقة بتطبيق هذه القوانين توازنًا دقيقًا بين الأمان والابتكار، وان القصور التشريعي للدول والتعارض بين مصالحها يعتبر أكبر تحدٍ يواجه مكافحة الجرائم المعلوماتية، لما ينجم عن ذلك من تعارض في تطبيق القانون من الناحية العملية، كما أن قصور التشريعات في وضع فهم وقواعد قانونية خاصة بالجرائم المعلوماتية يعوق التعاون في هذا المجال.
ونجد أن التحديات التي تواجه دولة قطر ليست محدودة بالجوانب التشريعية فحسب، بل تشمل أيضًا جوانب سياسية وسيادية وتقنية، لذا، من الضروري تبني مقاربة شاملة تقوم على تطوير، وتعزيز قدرات الأجهزة الأمنية والقضائية، وتعظيم التعاون الثنائي والمتعدد الأطراف مع الدول والمنظمات الدولية.
ويجب أن نكون واعين للمخاطر المتزايدة التي تمثلها الجرائم الإلكترونية، ولا ينبغي الانتظار حتى يصبح أحدنا ضحية لهذه الجرائم، حيث يتعين علينا اتخاذ إجراءات وقائية لحماية أنفسنا وعائلاتنا من خلال التعلم المستمر حول أحدث أساليب الاحتيال الإلكتروني ومشاركة هذه المعلومات مع مجتمعنا لبناء بيئة أكثر وعيًا.
وللحد من أخطار الجرائم الإلكترونية، ينبغي على الأفراد والشركات اتخاذ تدابير وقائية فعّالة، مثل تحديث البرامج والتطبيقات بشكل دوري، واستخدام كلمات مرور قوية وفريدة لكل حساب، وزيادة الوعي والتدريب لمعرفة كيفية التعرف على تهديدات الأمن السيبراني.
في الختام، يُعتبر دعم دور دولة قطر في إطار اتفاقية بودابست، سواء بالانضمام المباشر أو من خلال تبني المعايير والممارسات المثلى، خطوة استراتيجية تعزز مكانتها الإقليمية والدولية في مجال الأمن السيبراني، وتساهم في إنشاء بيئة رقمية أكثر أمانًا واستقرارًا.

الخلاصة إذا واجهتك جريمة إلكترونية أو كنت تعرف شخصًا قريبًا تعرض لمثل هذه الجرائم، فإن الوعي هو مفتاح التصرف السليم، ومن الضروري التواصل مع وحدة مكافحة الجرائم الإلكترونية، والتحدث مع شخص موثوق، وتجنب التفاعل مع الجاني، ويجب عدم دفع أي مبالغ مالية أو الاستجابة لطلبات الابتزاز، التصرف الهادئ والحذر، وإغلاق أي ثغرات قد يستخدمها المجرم للتهديد، هي خطوات أساسية في مثل هذه المواقف.
ويجب على أي شخص أن يكون على دراية بأن الجرائم الإلكترونية قد تطال أي فرد، لذا ينبغي نشر الوعي المجتمعي حول مخاطرها وتأثيراتها، مما يساهم في تشكيل جبهة وقائية جماعية تقليل الخسائر المحتملة.
تهدف الجهود والاعمال المبذولة حالياً في مجال موضوع الجرائم السيبرانية على أهمية ملحة لمواكبة التغيرات المتزايدة التي تطرأ على هذا الفضاء، ويتطلب الأمر تطبيقًا حكيمًا للقوانين، مع الأخذ بعين الاعتبار الحاجة للتوازن بين الأمان والابتكار، وهو ما سيكون موضوعًا بارزًا في النقاشات المستقبل.

النتائج التي توصلنا اليها:

1- الجريمة الإلكترونية تمثل نمطًا جنائيًا عابرًا للحدود الوطنية، تتجاوز فيه الأفعال الإجرامية مفهوم الإقليم التقليدي للسلطة الجنائية، الأمر الذي يفرض إعادة النظر في مبادئ الاختصاص القضائي والتعاون الدولي .

DOI: https://doi.org/10.33193/IJoHSS.69.2025.896

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (69) ديسمبر 2025
Volume (69) December 2025
IJOHSS

2- اتفاقية بودابست لعام 2001 تُعد الإطار الدولي الأكثر شمولًا وفاعلية في مكافحة الجريمة الإلكترونية، إذ وضعت معايير موحدة للتجريم والإجراءات وجسورًا للتعاون القضائي بين الدول، مما جعلها مرجعًا تشريعيًا عالميًا في مواجهة الجرائم المعلوماتية.

3- يُلاحظ أن انضمام الدول إلى اتفاقية بودابست لا يزال محدودًا في المنطقة العربية، ما يؤدي إلى تفاوت في الأطر القانونية وضعف التنسيق الإقليمي، ويبرز الحاجة إلى مواءمة التشريعات الوطنية مع مبادئ الاتفاقية لتحقيق فعالية التعاون الدولي.

4- أكد البحث أن دولة قطر حققت تقدمًا نوعيًا في بناء منظومة وطنية لمكافحة الجريمة الإلكترونية، من خلال سن قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014، وإطلاق الاستراتيجية الوطنية للأمن السيبراني، وإنشاء وحدات متخصصة داخل وزارة الداخلية، ما يشكل نموذجًا تشريعيًا ومؤسسيًا رائدًا في المنطقة الخليجية.

5- رغم التطور التشريعي القطري، فإن عدم الانضمام الرسمي إلى اتفاقية بودابست يحدّ من فاعلية التعاون الدولي في المجال الجنائي الرقمي، خصوصًا فيما يتعلق بتبادل الأدلة الرقمية والمساعدة القضائية وتسليم المجرمين عبر الحدود.

6- تُظهر المقارنة القانونية بين التشريعات القطرية ومبادئ اتفاقية بودابست وجود توافقٍ جوهري في الأهداف والمبادئ العامة، غير أن الاتفاقية تتميز بتحديد إجراءات دولية دقيقة للملاحقة، مما يدعو إلى دراسة إمكانية تبني قطر لملاحق الاتفاقية أو إصدار قانون وطني مكمّل لها.

7- ضعف التنسيق الدولي واختلاف المفاهيم القانونية للجرائم المعلوماتية يشكّل تحديًا رئيسيًا أمام ملاحقة الجناة، إذ تؤدي الفجوات التشريعية وتباين النظم القانونية إلى تعطيل العدالة الجنائية وتأخير التعاون القضائي بين الدول.

8- يؤكد البحث أن التعاون الدولي لا يقتصر على التبادل التشريعي والقضائي، بل يمتد إلى بناء القدرات والتدريب التقني المتخصص، وهو ما بدأت دولة قطر بتطبيقه فعليًا من خلال مركز الأمم المتحدة الإقليمي لمكافحة الجريمة السيبرانية في الدوحة.

9- معالجة الجريمة الإلكترونية تتطلب مقاربة شاملة تجمع بين الأدوات القانونية، والمؤسسات الأمنية، والتقنيات الحديثة، بما يضمن تحقيق الأمن السيبراني دون المساس بحقوق الإنسان وحرياته الرقمية.

10- مكافحة الجريمة الإلكترونية لم تعد شأنًا وطنيًا محدودًا، بل هي التزام دولي مشترك يتطلب من الدول، وعلى رأسها دولة قطر، تعزيز الانخراط في الاتفاقيات الدولية وتطوير التعاون الثنائي والإقليمي لضمان أمن الفضاء الرقمي العالمي.

التوصيات المقترحة:

1- يجب تعزيز جهود العمل على انضمام دولة قطر رسميًا إلى اتفاقية بودابست لعام 2001 وبضرورة دراسة الجوانب القانونية والفنية للانضمام إلى الاتفاقية، أو تبنّي اتفاقية إقليمية عربية مكافئة، لما يمثله ذلك من دعم للثقة القانونية والتنسيق القضائي مع الدول الأخرى في مجال مكافحة الجريمة الإلكترونية

2-تحديث التشريعات الوطنية القطرية لتواكب التطور التقني المتسارع في أنماط الجرائم المعلوماتية وذلك عبر إدخال تعديلات دورية على قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014، لتشمل الجرائم الناشئة مثل الذكاء الاصطناعي الاحتيالي، والابتزاز عبر العملات الرقمية وغيرها.

DOI: https://doi.org/10.33193/IJoHSS.69.2025.896

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (69) ديسمبر 2025
Volume (69) December 2025
IJOHSS

3- إنشاء قاعدة بيانات وطنية موحدة للجرائم الإلكترونية بالتنسيق مع الجهات الأمنية والقضائية
تهدف هذه القاعدة إلى توثيق الجرائم، وأنماطها، وأساليب ارتكابها، وتبادل المعلومات مع الدول والمنظمات الدولية، بما يساهم في بناء مؤشرات دقيقة تساعد على وضع السياسات الوقائية الفعّالة.

4- دعم التعاون الإقليمي والدولي من خلال الاتفاقيات الثنائية والمتعددة الأطراف ويُوصى بتفعيل اتفاقيات تعاون جديدة بين دولة قطر والدول الصديقة في مجالات التحقيق الرقمي، وتبادل الأدلة، والتدريب المشترك، بما يضمن سرعة الاستجابة في مواجهة الجرائم الالكترونية.

5- أن تعمل الدول على الانضمام إلى اتفاقية بودابست، أو إصدار اتفاقية دولية جديدة ترتكز على الحماية الإجرائية والعقابية لنظم المعلومات، تشمل أغلب الدول لتحقيق تعاون دولي فعال في مكافحة الجرائم الإلكترونية.

7- تشجيع المجني عليهم أي الضحايا على الإبلاغ عن جرائم تقنية المعلومات، من خلال تضمين مواد في قانون مكافحة الشائعات والجرائم الإلكترونية تلزم الأفراد بذلك وتحفزهم على اتخاذ خطوات فعالة. ومن الضروري تطوير وصياغة الاتفاقيات لتستوعب جميع أنواع الجرائم الإلكترونية، وضمان تكامل القانون الوطني مع هذه الاتفاقيات.

المصادر والمراجع

1- اتفاقية بودابست لمكافحة الجرائم الالكترونية 2001.
2- المادة الأولى مكرر من القانون العقوبات الكويتي رقم 9 لسنة 2001 والمضافة بالقانون رقم40 لسنة 2007.
3- المادة السادسة من القانون رقم175 عقوبات المصري لسنة 2008.
4- أحمد، ه. (2011). اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقاً عليها. دار النهضة العربية. القاهرة.
5- إبراهيم، خ. (2009). الجرائم المعلوماتية. دار الفكر الجامعي. الإسكندرية.
6- الديري، ع. (2012). الجرائم الالكترونية، الطبعة الأولى. المركز القومي للإصدارات القانونية. القاهرة.
7- خراشي، ع. (2015). إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها. دار الجامعة الجديدة. طابق أول. الإسكندرية.
8- الكعبي، م. (2010). الحماية الجنائية للتجارية الإلكترونية. دار النهضة العربية. القاهرة.
9- المراغي، أ. (2016). الجريمة الالكترونية ودور القانون الجنائي في الحد منها. مصر.
10- مرعي، إ. (2025). الجرائم الالكترونية الأهداف الأسباب طرق الجريمة ومعالجتها. المركز الديمقراطي العربي.
11- الزناتي، ع. (2008). التنظيم الدولي. دار النهضة العربية.
12- شاهين، م. (2018). الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي. دار الجامعة الجديدة. الإسكندرية. الطبعة الأولى.
13- أبو نمر، س. (2021). مكافحة الجريمة المعلوماتية في إطار القانون الدولي. رسالة ماجستير. جامعة بسكرة.
14- البدراوي، إ. (2011). التعاون الدولي في مجال مكافحة الجريمة المنظمة. رسالة دكتوراة. كلية الحقوق. جامعة أسيوط.
15- العبيد، ف. (2021). الإجراءات الجنائية المعلوماتية. رسالة دكتوراة. كلية الحقوق عين شمس.
16- العنزي،خ. (2021). الجرائم الإلكترونية وتأثريها على الاقتصاد القومي. دراسة مقارنة. رسالة دكتوراة.
17- الغياثين، م. (2013). الجرائم المعلوماتية العابرة للحدود. أطروحة دكتوراة. جامعة القاهرة.
18- القحطاني،خ. (2006). التعاون الأمني الدولي في مواجهة الجريمة المعلوماتية عبر الوطنية. أطروحة دكتوراة. كلية الدراسات العليا. جامعة نايف العربية للعلوم الأمنية. دار النهضة العرب. الرياض.
19- المظلوم،ح. (2013). المواجهة الأمنية للجرائم العابرة للحدود. أكاديمية شرطة دبي. كلية الدراسات العليا.

 DOI: https://doi.org/10.33193/IJoHSS.69.2025.896

المجلة الدولية للعلوم الإنسانية والاجتماعية
International Journal on Humanities and Social Sciences
website:www.ijohss.com
Email:editor@ijohss.com
ISSN: 2415 – 4822
العدد (69) ديسمبر 2025
Volume (69) December 2025
IJOHSS

20- المري، ر. (2013). الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر. دراسة تحليلية تأصيلية مقارنة. أطروحة دكتوراة. جامعة القاهرة.
21- دورماز، م. (2024). اتفاقية الأمم المتحدة الجديدة لمكافحة الجرائم الالكترونية. مقال. موقع الكتروني. www.smex.orgتاريخ زيارة الموقع 2025/10/10 الساعة 15:00.
22- الهاجري، م. (2025). جريمة القرصنة الالكترونية في التشريع القطري. مجلة الحقوق للبحوث القانونية. قطر.
23- رجب، ي.(1976). الرابطة بين جامعه الدول العربية ومنظمه الوحدة الإفريقية. دراسة قانونية سياسية. دار الفكر العربي.
24- مطيري، خ.(2020). مواجهة الجرائم المعلوماتية في ضوء التشريعات الجنائية المعاصرة والاتفاقيات الدولية.
25- مهدي، ل.(2013). الجرائم الالكترونية أركانها أسبابها ودوافع ارتكابها. دراسات شرطية. الإمارات.
26- الصويلح، س. (2025). المواجهة الأمنية للاختراقات الالكترونية المستحدثة المؤثرة على الأمن القومي. المجلة العربية للدراسات الأمنية.

 DOI: https://doi.org/10.33193/IJoHSS.69.2025.896