الجرائم المعلوماتيّة والضوابط القانونيّة لمكافحتها على الصعيدين الوطني والدولي

Cyber Crimes and Legal Regulations to Combat Them at the National and International Levels

الدكتور حمزه بن فهم السلمي

DR. Hamzah Faham Alsulami

كلية القانون والدراسات القضائية، قسم القانون العام

College of Law and Judicial Studies, Public Law

جامعة جدة

University of Jeddah

جدة، المملكة العربية السعودية

Kingdom of Saudi Arabia, Jeddah

E : Hfalsulami1@uj.edu.sa

الملخص:

يشهد العالم منذ منتصف القرن العشرون ثورة معلوماتيّة تجسّدت في التطوّر الكبير في مجالي تكنولوجيا المعلومات والإتّصالات، وأصبحت الشبكة المعلوماتيـة الدوليّة هي أهم ما يميّز العصر الحديث، والحضارة الإنسانية الحاليّة هي حضارة معلوماتيّة، فالعالم كلّه يقوم على تبادل المعلومات، وبناء الخبرات، وترتيب البيانات. إلاّ أنّه وعلى الرغم من الإيجابيات والتطوّرات الهائلة التي تحققت بفضل تقنية المعلومات، فإنّ الثورة المعلوماتية صاحبتها في المقابل جملة من الإنعكاسات السلبية الخطيرة، لعل أهمّها ظهور صنف جديد من الجرائم المستحدثة العابرة للحدود، والتي تسمّى بالجرائم المعلوماتيّة أو الإلكترونية أو جرائم الإنترنت التي تستهدف الأشخاص والدول حيث طالت، في الآونة الأخيرة، المؤسسات المالية والحكوميّة والأفراد، وأصبحت تمثّل تهديداً حقيقيّاً لأمن الدول وسلامة مواطنيها والبنى التحتية الأساسية. وهكذا فإنّ الجرائم المعلوماتيّة أصبحت من التحدّيات الكبرى التي تواجهها المملكة، كغيرها من دول العالم التي بدأت رحلة التحول الرقمي، على الصعيدين الإقليمي والعالمي. وفي هذا الإطار يأتي هذا البحث ليبرز الصعوبات والتحدّيات التي تطرحها مكافحة الجرائم المعلوماتيّة وذلك من خلال بيان ماهيّة هذه الجرائم وخصوصيّتها ومدى نجاعة الجهود الوطنيّة والدوليّة في مواجهتها. وتوصلت الدراسة إلى عدد من النتائج التوصيات ومنها إبرام إتّفاقية دوليّة لتعزيز التعاون الدولي بجميع صوره لمواجهة التحديات الإجرائية الناجمة عن الجرائم المعلوماتية عبر الوطنية.

الكلمات المفاتيح: الجرائم المعلوماتيّة – المجرم المعلوماتي – الإنترنت – الحاسوب – الآليات – المكافحة – التعاون الدولي.

Abstract:

Since the middle of the twentieth century, the world has been witnessing an information revolution embodied in the breakthroughs in the fields of information and communication technology. The international information network has become the most important characteristic of the modern era, making of the current human civilization an information civilization as the whole world became based on exchanging information, building experiences, and managing data. However, despite the tremendous positive advances that have been achieved thanks to information technology, this information revolution was accompanied by several serious negative repercussions, the most important of which is probably the emergence of a new category of modern cross-border crimes, usually referred to as cybercrimes that target both people and countries. This new category of crimes has recently not only affected financial and governmental institutions and individuals, but also it has become a real threat to the security of states and the safety of their citizens as well as to basic infrastructures. Thus, cybercrimes have grown into one of the major challenges facing the Kingdom, which, just like other countries in the world, has begun the journey of digital transformation at the regional and global levels. In this context, this research comes to highlight the difficulties and challenges posed by the fight against cybercrimes, by stressing the nature and specificity of these crimes and the extent of the effectiveness of national and international efforts in confronting them. The study reached a number of findings and recommendations, including the conclusion of an international agreement to enhance international cooperation in all its forms to face the procedural challenges resulting from transnational cybercrimes.

Keywords: Cyber Crimes - Information Criminal - Internet - Computer - Mechanisms - Combat - International Cooperation

المقدمة:

بدخول العالم عصر الثورة المعلوماتيّة وتوجّهه نحو التحول الرقمي الذي شمل شتى المجالات ومختلف القطاعات الحيوية الإدارية والإقتصاديّة والعسكرية تغيّرت كل معالم الحياة الإنسانيّة وزادت هيمنة تكنولوجيا المعلومات والإتّصالات على نسق الحياة العام. وأدّى التطوّر المستمر للتقنية الرقميّة إلى ظهور الفضاء الإلكتروني الذي يُمكن مزايا التحوّل الرقمي وتعطي فوائده في شتى مجالات الحياة، وأصبح له دور إستراتيجي في المجتمع الدولي حيث تُعتبر المعلومات، في هذا العصر الرقمي، موردًا اقتصاديًا وعاملا رئيسيّا للتطوّر، وأداة أساسيّة للنجاح أو الفشل على مستوى الفرد والمجتمع وعلى المستويين الوطني والدولي. وتعتبر المملكة العربية السعوديّة من أولى الدول على مستوى العالمي التي إختارت التوجّه نحو التحوّل الرقمي وتنمية البنية التحتيّة الرقميّة، لمواكبة التقدّم العالمي المتسارع في الخدمات الرقميّة وفي الشبكات العالميّة المتجدّدة وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، وخاصّة لتحقيق رؤيتها الطموحة 2030، التي تبنتها منذ عام 2016إلاّ أنّه وبالرغم من المزايا والتطوّرات الهائلة التي تحققت على جميع الأصعدة بفضل الثورة التكنولوجية[1]؛ فإنّ هذا التطور التقني السريع صاحبته في المقابل جملة من الإنعكاسات السلبيّة الخطيرة نتيجة إساءة إستخدام التقنية الحديثة والإنحراف بها عن

أهدافها الحقيقيّة وتوظيفها في ممارسات غير مشروعة[٢]، فقد أصبح الفضاء الإلكتروني بيئة المجتمع الحديث ينتج مثلما ينتجه الواقع المادي أنواع جديدة من الجرائم سُميت بالجرائم المعلوماتية أو الإلكترونية أو جرائم الإنترنت[٣]، من خلال خلق فضاء جديد للمجرمين مكّنهم من تصفح الإنترنت وإرتكاب طائفة جديدة من الجرائم العابرة للحدود، مثل القرصنة، والإحتيال، والتخريب، والتعامل في معلومات العدالة والأمن والنظم البنكيّة، السرقة والتزوير وإختراق المواقع الإلكترونيّة وتدميرها والتجسّس والجرائم الأخلاقيّة والجنسيّة والدينيّة وجرائم الإرهاب الإلكتروني[٤]، والّتي باتت من الظواهر الإجراميّة الخطيرة الّتي تهدّد أمن المجتمعات والدول وسلامة مواطنيها والبنى التحتيّة الأساسيّة وبالتالي تهدّد السلم والأمن الدوليين[٥]. وفي هذا الإطار يندرج موضوع هذا البحث حول:" **الجرائم المعلوماتيّة والضوابط القانونيّة لمكافحتها على الصعيدين الوطني والدولي.**" **وتُعرّف الجرائم المعلوماتيّة** بأنّها تلك الأفعال الإجرامية الناتجة من خلال أو بواسطة إستخدام المعلوماتيّة والتقنية الحديثة المتمثّلة في الكمبيوتر والمعالجة الآلية للبيانات، أو بنقلها[٦]. كما عرفتها منظمة التعاون الإقتصادي والتنمية بأنّها: " كل فعل أو إمتناع من شأنه الإعتداء على الأموال الماديّة والمعنويّة يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية."[٧]وتُعرّف أيضا بأنّها: " كلّ فعل أو إمتناع عمدي ينشأ عن الإستخدام غير المشروع لتقنية المعلومات ويهدف إلى الإعتداء على الأموال الماديّة أو المعنويّة."[٨]ومن خلال كل ما تقدّم يمكن تعريف الجرائم المعلوماتية بأنّها كل فعل أو إمتناع قصدي ينشأ نتيجة الإستخدام غير المشروع لتقنية المعلومات ويهدف إلى الإضرار بالمصالح الماديّة أو المعنويّة التي يحميها النظام.

أهميّة موضوع البحث:

يكتسب هذا البحث أهميّته من خطورة ظاهرة الجرائم المعلوماتيّة التي تمسّ بشكل مباشر مصالح أفراد المجتمع والدول والمصارف والبنوك من خلال السطو على الأموال والتلاعب في كشوفات وحسابات العملاء، ونقل الأرصدة من حساب إلى آخر وسرقة البطاقات البنكيّة، وأيضا إنتهاك حرمة الحياة الخاصة للأفراد، كما أنّ الإجرام الإلكتروني أصبح يُستخدم من قبل المنظمات الإرهابيّة ويمسّ الحكومات ويُهدّد مصالح الدول الإقتصادية والعسكريّة والأمنيّة ويعتبر الخطر الّذي يمثّل المرتبة الثالثة بعد الأسلحة الكيميائيّة والنووية. ومن هنا تتجلى الأهميّة النظرية والعملية لهذا البحث الّذي يأتي ليحدّد ماهيّة هذه الجرائم ومدى خطورتها ويبيّن الصعوبات والتحدّيات الأمنيّة والتقنيّة والقانونيّة التي تواجه مكافحتها ويبحث في الآليات والسبل الكفيلة بالتصدي لها على المستويين الوطني والدولي.كما يُمثّل هذا البحث أيضا إضافة إلى رصيد الدراسات القانونية التي تناولت موضوع مكافحة الجرائم المعلوماتيّة، ويهدف لزيادة وعي الشعوب والمجتمع الدولي بخطورة هذه الجرائم وضرورة تجريمها دوليّا والتعاون في مواجهتها من خلال بعض التوصيات العلمية والتصوّرات العمليّة، لتفعيل دور المنظمات والإتّفاقيات والمعاهدات والجهود الدولية لتحقيق حماية أفضل للفضاء الإلكتروني والأمن السيبراني.

أسباب إختيار موضوع البحث:

يرجع إختيار الموضوع، بالرغم ممّا يكتنفه من صعوبات، إلى الإعتبارات الذاتيّة والموضوعيّة التالية:

– تتمثّل الأسباب الذاتيّة أساساً في الإهتمام بالبحث في خصوصيّة هذه الجرائم المستحدثة وصورها المختلفة نظراً وأنّها أصبحت من أهم القضايا الدُوليّة الّتي تهدّد الأمن المعلوماتي للأفراد والمؤسسات والحكومات.

– أمّا الأسباب الموضوعية فتعود إلى الإنتشار الواسع للجرائم المعلوماتيّة على الصعيدين الوطني والدولي مع التطوّر السريع والهائل في مجال تكنولوجيا الإتّصالات والمعلومات، حيث أصبحت تشكّل تحدّياً كبيراً يواجه أجهزة إنفاذ القانون، ليس في دولة واحدة، بل في جميع دول العالم، ممّا يقتضي ضرورة فهم هذا النوع من الجرائم والصعوبات التي تواجه مكافحتها والبحث في مدى نجاعة الآليات والجهود الوطنيّة والدوليّة لمواجهتها وتفعيل التعاون الدولي في جميع مجالاته أمنيّاً وتشريعيّاً وقضائيّاً.[٩]

أهداف موضوع البحث:

يأتي هذا البحث في وقت تفشّت فيه الجرائم المعلوماتيّة وتفاقمت مخاطرها وتخطى مداها حدود الدول بل والقارات لمحاولة تحديد ماهيّة الجرائم المعلوماتيّة والتعرّف على خصائصها وصفات المجرم المعلوماتي وتمييزها عن الجرائم التقليديّة وبيان الآثار السلبيّة والتداعيات الخطيرة لهذه الجرائم. كما يهدف البحث إلى إبراز الجهود الوطنيّة والدوليّة المبذولة في مكافحة الجرائم المعلوماتيّة والتحدّيات التي تواجهها والتأكيد على ضرورة التعاون الإقليمي والدولي للتصدّي لها والحدّ منها والبحث في الآليات والوسائل الممكنة للقضاء عليها.

منهج البحث :

لمعالجة الموضوع اعتمدنا المنهج الوصفي التحليلي لتحديد ماهيّة الجرائم المعلوماتيّة وطبيعتها وخصائصها ثمّ تقييم الآليات والجهود الوطنيّة والدوليّة في مجال مكافحتها.

إشكاليّة البحث :

من خلال ما سبق تتمثّل الإشكالية أو بالأحرى الإشكاليات الرئيسية التي يطرحها هذا البحث، فيما يلي : **ماهي الجرائم المعلوماتيّة ؟ وما مدى نجاعة وفعاليّة الآليات والجهود الوطنيّة والدوليّة في مكافحة الجرائم المعلوماتيّة والحدّ منها ؟**

خطة البحث :

للإجابة عن هذه الإشكالية لابدّ من ماهيّة الجرائم المعلوماتيّة وخصائصها، ثم بيان مدى الجهود الوطنيّة والدوليّة في مواجهتها والتصدّي لها. لذلك تناولنا هذا البحث من خلال مبحثين أساسيين:

- **المبحث الأوّل : ماهيّة الجرائم المعلوماتيّة.**
- **المبحث الثاني : مدى نجاعة الآليات والجهود الوطنيّة والدوليّة في مكافحة الجرائم المعلوماتيّة.**

المبحث الأوّل ماهيّة الجرائم المعلوماتيّة

تُعدّ الجرائم المعلوماتيّة جرائم مستحدثة، وضرباً من ضروب الذكاء الإلكتروني الإجرامي، نظراً لإرتباطها بتكنولوجيا المعلومات، ووسائل الإتصالات الحديثة ممّا أدى إلى تغيُّر أنماط الجريمة وتنوّع الإعتداءات وإتّساعها بحيث لم تعد تقتصر فقط على النفس والمال، بل طالت أيضا المعلومات. وقد إنتشرت هذه الجرائم لما لها من سمات تدفع المجرمين إلى إرتكابها، وتميّزها كثيرا عن الجرائم التقليدية من حيث طبيعتها وأنواعها وخصائصها ممّا يصعب معه إدراجها ضمن الأوصاف الجنائيّة التقليديّة في القوانين الجنائية الوطنية والأجنبيّة كما تصعب مكافحتها. ولذلك كان لا بدّ من توضيح ماهيّتها وذلك من خلال تعريف الجرائم المعلوماتيّة **(المطلب الأوّل)**، ثمّ بيان الصعوبات والتحدّيات الّتي تواجه مكافحتها **(المطلب الثاني)**.

المطلب الأوّل : تعريف الجريمة المعلوماتيّة

إنّ مفهوم الجريمة المعلوماتيّة من المفاهيم الحديثة التي لا يوجد لها إلى الوقت الحالي تعريف موحّد وشامل متّفق عليه من كافّة دول العالم، فهي تعتبر من الظواهر الحديثة الّتي إرتبط ظهورها وإنتشارها بالتطوّر المستمر في تكنولوجيا المعلومات والإتّصالات[١٠] مع "غياب لتعريف عام وإطار نظري متّسق في هذا الحقل من الجريمة ... وفي أغلب الأحيان تستخدم مصطلحات الإفتراضيّة والحاسوب والإلكترونيّة والرقميّة"[١١]. وقد أطلقت عليها تسميات مختلفة ومنها جرائم الحاسب[١٢]، جرائم الإنترنت، جرائم الكمبيوتر[١٣]، جرائم تقنية المعلومات، جرائم المعالجة الآلية للبيانات، جرائم إلكترونية، جرائم المعلوماتيّة، وغيرها. كما اختلف الفقه القانوني في تعريفها، أمّا بالنسبة للتشريعات فنجد بعضها عرّفت الجرائم المعلوماتيّة بطريقة غير مباشرة وبعضها لم يتعرّض لتعريفها.ويقتضي تعريف الجريمة المعلوماتيّة تحديد مفهومها **(الفرع الأوّل)**، ثمّ بيان أركانها **(الفرع الثاني)**.

الفرع الأوّل ـ مفهوم الجريمة المعلوماتية:

لتحديد مفهوم الجريمة المعلوماتيّة لابدّ من تعريفها من الناحية الفقهيّة **(أوّلاً)**، ثمّ التعرّض إلى تعريفها التشريعي **(ثانياً)**.

أوّلا – المفهوم الفقهي للجريمة المعلوماتية:إنّ مسألة وضع تعريف للجريمة المعلوماتية كانت محلاً لإجتهادات الفقهاء، حيث ذهب الفقهاء في تعريف الجريمة المعلوماتيّة مذاهب شتى ووضعوا تعريفات مختلفة، وبالتالي لا نجد تعريفاً محدّداً للجريمة المعلوماتية. فقد تعدّدت التعريفات والإتّجاهات بحسب وجهة النظر إلى الزاوية التي تشكّل الجريمة المعلوماتيّة. فالنّظر إلى الجانب التقني عرّفها جانب أوّل من الفقه بأنها ذلك النوع من الجرائم التي تتطلب إلماماً خاصّاً بتقنيات الحاسب الآلي ونظم المعلومات لإرتكابها أو التحقيق فيها ومقاضاة فاعلها.[١٤] وعرّفها آخر بأنّها كل جريمة ترتكب في محيط أجهزة الحاسوب، أو كل سلوك غير مشروع أو غير أخلاقي، أو غير مصرح به يتعلق بالمعالجة الآليّة للبيانات أو نقلها.[١٥] وعرّف إتّجاه ثاني من الفقه الجريمة المعلوماتيّة بالنظر إلى وسيلة ارتكابها على أنّها "الجرائم الّتي لا تعرف الحدود الجغرافيّة والّتي يُستخدم الكمبيوتر أداة رئيسيّة في إرتكابها عن طريق شبكة الإنترنت وبواسطة شخص على دراية واسعة بها "[١٦] أي أنّها الجرائم التي يكون فيها الحاسوب وسيلة إرتكاب فعل غير مشروع، أو محل لوقوع الفعل غير المشروع، وذلك بالقيام بعمل أو الإمتناع عن أدائه من شأنه الإعتداء على الأموال الماديّة أو المعنويّة، شريطة أن يكون مرتكبها على معرفة بتقنية إستخدام الحاسوب والتعامل مع معطياته.[١٧] وهي بذلك "كل أشكال السلوك أو الفعل غير المشروع والذي يرتكب بواسطة جهاز الحاسوب"[١٨]، أو هي كل فعل

غير مشروع يؤدي فيه جهاز الحاسوب دوراً مهماً لإتمام السلوك غير المشروع على أن يكون هذا الأداء أو الدور مؤثراً ومؤدياً إلى ارتكاب الجريمة.[١٩] ومن هذا المنظور تشمل الجرائم المعلوماتيّة كل أشكال السلوك أو الأفعال التي تضر بالمجتمع والتي ترتكب باستخدام الحاسب الآلي والإنترنت.[٢٠] أمّا من حيث موضوع الجريمة، فقد عرّف إتّجاه ثالث من الفقه الجريمة المعلوماتية بأنّها مجرد نشاط موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه[٢١]. كما يمكن تعريفها أيضا بأنّها الإعتداء الواقع على البيانات أو المعلومات أو المعالجة الآلية للبيانات في جهاز الحاسوب بطريقة غير مشروعة. فجرائم المعلوماتية فيها جميع أوجه الإعتداء الإلكترونية الموجهة للمعلوماتية مثل سرقة البيانات المعلوماتية وجرائم الملكية الفكرية وغيرها من الأساليب غير المشروعة الإلكترونية الموجهة لقواعد البيانات والمعلومات.[٢٢]ونظرا لعدم نجاعة التعاريف السابقة للجريمة المعلوماتيّة لإعتمادها على أحد المعايير، فقد ذهب إتّجاه آخر من الفقه إلى تعريف الجريمة المعلوماتيّة بالنظر إلى عدّة معايير بأنّها:" الجريمة الّتي يُستخدم فيها الحاسب الآلي كوسيلة أو أداة لإرتكابها أو تُمثّل إغراء بذلك، أو جريمة يكون الحاسب نفسه ضحيّتها.[٢٣]

ثانيا – المفهوم القانوني للجريمة المعلوماتية:

نظراً لما تتّسم به الجرائم المعلوماتيّة من سهولة وخطورة، إهتمّت بعض التشريعات بتعريفها في المواد الأولى من النظام الذي يعالج هذا النوع من الجرائم. ففي المملكة العربية السعودية تمّ سن تشريع خاص بمكافحة الجرائم المعلوماتية أُطلق عليه ما يسمى بـ" نظام مكافحة جرائم المعلوماتية " الصادر وفقا لقرار مجلس الوزراء رقم (79) وتاريخ 1428/03/07هـ[٢٤] والّذي عرّف الجريمة المعلوماتية في المادّة الأولى (8) بأنّها: "أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتيّة بالمخالفة لأحكام هذا النظام."أمّا المشرع القطري فقد عرّفها بأنّها: " أي فعل ينطوي على إستخدام وسيلة تقنية المعلومات أو نظام معلوماتي، أو الشبكة المعلوماتيّة، بطريقة غير مشروعة بما يخالف أحكام القانون"[٢٥]. ويتشابه هذا التعريف مع ما ورد بالمادّة الأولى من قانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات الكويتي الذي عرّفها كما يلي: " في تطبيق أحكام هذا القانون يُقصد بالمصطلحات التالية المعنى الموضح قرين لكل منها: الجريمة المعلوماتية: كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لحكام هذا القانون. "وفي المقابل خلت التشريعات الجنائية لبعض الدول من كلّ تعريف للجريمة المعلوماتيّة، ومنها قانون الجرائم المعلوماتية السوداني لسنة 2007، وقانون مكافحة جرائم تقنية المعلومات الإماراتي رقم 5 لسنة 2012، وقانون جرائم تقنية المعلومات البحريني رقم 60 لسنة 2014، وأيضا قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015. ويتضّح بذلك أنّ المشّرعين السعودي والكويتي متقدّمين على العديد من الأنظمة الأخرى حيث عَرّفا الجريمة المعلوماتية، وهي مسألة مهمّة جدّا نظراً وأنّ الجريمة المعلوماتية تقتضي تحديد مفهومها وتعريفها صلب النصوص القانونيّة.وعُرفت الجريمة المعلوماتيّة أيضا في الإتّفاقيّة العربية وقانون الجرائم الأمريكيّة وإتّفاقيّة بودابست والإتّحاد الدولي للإتّصالات بأنّها " كلّ جناية أو جنحة ترتكب ضد فرد أو جماعة بدافع جرمي ونيّة الإساءة لسمعة الضحيّة أو جسده أو فكره أو ماله أو حياته، سواء كان ذلك بطريقة مباشرة أو طريقة غير مباشرة بإستخدام وسائل الإتّصالات الحديثة الإنترنت."[٢٦] كما عرّفتها أيضا منظمة التعاون والتنمية الإقتصاديّة «OCDE» بأنّها : "كل فعل أو امتناع من شأنه الإعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية."[٢٧]ويلاحظ من جملة التعريفات المقدّمة أنّه تستخدم مصطلحات مختلفة في اللفظ مثل الجريمة المعلوماتية، الجريمة الإلكترونية، جرائم الكمبيوتر أو جرائم الانترنت ولكنها لها نفس المعنى. ولهذا يطرح السؤال التالي: **أيّ من المصطلحات المذكورة هو الأشمل من حيث المفهوم والمضمون؟**يرى البعض أنّ إستخدام مصطلح جرائم الكمبيوتر أعم وأشمل من إستخدام مصطلح جرائم المعلوماتية، لأن جرائم المعلوماتية تشمل من حيث المفهوم الإعتداء على المعلومات والبرامج داخل جهاز الكمبيوتر، بينما مصطلح جرائم الكمبيوتر أعم وأشمل من حيث المفهوم والمضمون، فهي جرائم ترتكب على جهاز الحاسوب وبواسطة الحاسوب كأداة ويشمل الإعتداء على الحاسوب الإعتداء على المعلومات والبرامج من حيث المضمون.[٢٨] والحقيقة أنّ سرّ هذا الخلاف يكمن في النسق الذي يعالج فيه الباحث موضوع بحثه أو موضوع الحق الذي حصل عليه الاعتداء وذلك على النحو التالي:

– فمن يستخدم مصطلح الجريمة المعلوماتيّة أراد التعبير عن الجريمة التي يكون فيها موضوع الحق المعتدى عليه المعلومة.

– أمّا من يستخدم مصطلح جرائم الإنترنت فهو إستخدام ضيّق لأنّه سيقصر هذه الجرائم على سلوكيات غير مشروعة ترتكب عن طريق الدخول إلى شبكة الإنترنت، كما أنّ من شأن هذا المصطلح أن يوحي بإخراج الجرائم التي يمكن أن نتصوّر إمكانية إرتكابها عن طريق جهاز الكمبيوتر دون الحاجة لإستخدام شبكة الإنترنت. – أمّا من يستخدم مصطلح الجريمة المعلوماتيّة فيقصد بها الجرائم المرتكبة

عن طريق الكمبيوتر وغيره من وسائل الإتّصال الحديث. وعلى هذا الأساس فإنّ إستخدام مصطلح الجريمة المعلوماتيّة أشمل وأعم مفهوما ومضمونا ونتفّق في هذا الإطار مع المنظم السعودي وغيره من الأنظمة والباحثين في هذا المجال على إستخدام مصطلح الجريمة المعلوماتيّة وذلك لأنّ مصطلح الجريمة المعلوماتيّة له دلالة واسعة ويستوعب كافّة مستجدات الإختراعات الإلكترونية ووسائل الإتّصال والمنظومات المعلوماتية من تجهيزات وشبكات حاسوبيّة أي كل ما يخدم المعلومة، كما يضمن هذا المصطلح إستيعاب جرائم الكمبيوتر وغيرها من السلوكيات الضارة بالأفراد والجماعة.

الفرع الثاني – أركان الجريمة المعلوماتية تُعرف الجريمة عموما بأنّها " فعل غير مشروع أو فعل خطير محظور يرتكب عن إرادة جنائية يعاقب عليها القانون."[٢٩] وتشترك الجرائم المعلوماتيّة مع الجرائم التقليديّة من حيث الأركان الثلاثة المكوّنة للجريمة وهي الركن الشرعي أو القانوني، الركن المادي والركن المعنوي.

أوّلاً– الركن القانوني للجريمة المعلوماتيّة :إنّ الجريمة هي نتيجة لأفعال الماديّة الصادرة عن الإنسان، وهذه الأفعال تختلف حسب نشاطات الإنسان. وهذا ما جعل المشرّع يتدخل لتجريم هذه الأفعال الضارّة بموجب نص قانوني يحدّد فيه الفعل الضار أو المجرم والعقوبة المقررة لإرتكابه.[٣٠] وينطبق مبدأ الشرعية على تعريف الجرائم وعلى تحديد العقوبات وتدابير الأمن التي تطبق على شخص معيّن، فالقاعدة الأساسيّة الناتجة عن هذا المبدأ هي عدم رجعيّة القانون الجنائي فلا يجوز للقاضي تجريم الفعل ما لم يجرم بنص، ولا توقيع عقوبة.[٣١] فالقاضي الجنائي عند تفسيره لنصوص القانون يفسّره تفسيراً ضيقاً، أي عدم لجوء القاضي الجنائي لقياس فعل لم يرد نص بتجريمه على فعل ورد نص بتجريمه فيقرّر القاضي الجنائي للأوّل عقوبة الثاني للتشابه بين الفعلين.[٣٢]والركن القانوني للجريمة هو الركن الذي يضع النص القانوني أو الشرعي الذي يجرم الفعل أو يعاقب على إتيانه. ويعتبر وجود النص القانوني المحدد لنوع الجريمة الركيزة الأساسية لوصف السلوك جريمة معاقب عليها أم لا، وذلك تطبيقاً لمبدأ شرعية التجريم والعقاب أو ما يصطلح عليه في المجال القانوني بمبدأ "لا جريمة ولا عقوبة إلا بنصّ"، ومفاد هذا المبدأ حصر نصوص مصادر التجريم والعقاب في القانون المكتوب[٣٣]. وعلى هذا الأساس تستمد الجرائم المعلوماتيّة شرعيّتها من مختلف التشريعات الوطنيّة الصادرة بشأن الجرائم المعلوماتيّة. وهذا ما نصّ عليه المنظم السعوي في نظام مكافحة الجرائم المعلوماتية السعودي حيث جرّم في المادّة الأولى منه "أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتيّة بالمخالفة لأحكام هذا النظام"[٣٤].

ثانياً– الركن المادي للجريمة المعلوماتية :الركن المادي هو الفعل الظاهري الذي يبرز الجريمة ويعطيها وجودها وكيانها في الخارج. ويعرف هذا الركن أيضا بأنّه وقوع فعل أو امتناع عن فعل حرمة القانون بما يجعل الجريمة تبرز إلى الوجود تامّة كانت أو ناقصة. وعليه فإنّ وجود الجريمة يتحقق بوجود الركن المادي وهو مبدأ عام لا يرد عليه استثناء. ويعتمد هذا الركن على ثلاثة عناصر أساسيّة:

– **الفعل:** وهو عبارة عن نشاط أو سلوك إجرامي يصدر من الجاني، ويتّخذ مظاهر خارجية يسهل الاستدلال عليها. ويلاحظ أنّ هذا السلوك ضروري في جميع الجرائم، ولكن صورته تختلف من فعل لآخر تبعا لإعتبارات متعدّدة أهمّها طبيعة السلوك ذاته، مدّة التنفيذ، عدد الأفعال المكوّنة للفعل والظروف الملابسة لمباشرة الفعل.

– **النتيجة:** يقصد بها الأثر جنائياً وقانونياً عن نتيجة الفعل.

– **العلاقة السببية:** هي تلك الرابطة التي دفعت إلى الإتيان بهذا الفعل، وما يترتّب عليه من نتيجة.[٣٥]

ولكي يكون الجاني مسؤولاً قانونياً على إرتكاب الفعل يجب أن تكون هناك نتيجة حتمية لذلك الفعل، وفي حال إنتفاء هذه العلاقة لا تكون هناك علاقة سببية، وبالتالي لا تترتّب أيّة مسؤوليّة.[٣٦] ونظرا للطبيعة الخاصّة للجرائم المعلوماتيّة، يطرح في هذا الإطار السؤال التالي : **كيف يتحقّق الركن المادّي في الجريمة المعلوماتيّة؟**

الركن المادي للجريمة المعلوماتية :

المشكلة الأساسية التي تثيرها الجريمة المعلوماتيّة هي طبيعة الركن المادي فيها، حيث أنّ مناط التجريم ينصب على إساء إستعمال نظام إلكتروني أو إقتحامه على نحو غير مشروع. ويلاحظ أنّ هذا الاستعمال أو الإختراق له أثر مادي ملموس يتمثّل في تدمير المعلومات، وهو ما يثير إمكانية الإتلاف العمدي للمنقولات أو السرقة وذلك عن طريق إساءة إستعمال بطاقات الإئتمان، أو يثير شبهة التزوير عن طريق التلاعب في بيانات الحاسب أو تدميرها.ويلاحظ أنّ هناك فرق بين السلوك الإجرامي في الجريمة التقليديّة العاديّة والجريمة المعلوماتيّة المترتب على السلوك الإجرامي وهي العدوان الواقع على الحق الذي حماه النظام وأقرّ بعقوبة على من إعتدى عليه. فالسلوك الإجرامي في

الجريمة التقليدية يتمّ رؤيته والتأكد منه مثل فعل القتل، فالجريمة هنا لها ملامح واضحة. أمّا السلوك الإجرامي في الجريمة المعلوماتيّة فهو يرتبط دائما بالمعلومة المخزنة في الحاسب أو التي يتمّ إدخالها إليه، ومن خلال الضغط على زر في الحاسب يتمّ تدمير النظام المعلوماتي أو حصول السرقة أو التسلل إلى نظام أرصدة العملاء في البنوك. وتكمن صعوبة الركن المادي في الجريمة المعلوماتيّة في أنّ الجريمة ترتكب عن طريق معلومات تتدفق عبر نظام الحاسب الآلي لا يمكن الإمساك بها ماديّاً.كما أنّ السلوك الإجرامي في هذه الجريمة يتطلب وجود بيئة رقمية، جهاز كمبيوتر، شبكة إنترنت، ومعرفة بداية هذا النشاط والشروع فيه ونتيجته.[٣٧] ومثال ذلك أن يقوم مرتكب الجريمة بتجهيز الكمبيوتر لكي يُحقّق له حدوث الجريمة، فيقوم بتحميل الحاسب ببرامج إختراق أو يقوم بجريمة إعداد برامج فيروسات تمهيداً لبثها.وتجدر الإشارة أيضا إلى أنّه وبالنسبة للجرائم التقليديّة، ليس كل جريمة تتطلب وجود أعمال تحضيرية، والقانون أيضا لا يعاقب على الأعمال التحضيرية فشراء الرجل لأداة الجريمة مثلا لتنفيذ جريمة قتل لا يعتبر جريمة في حدّ ذاته؛ ولكن الأمر يختلف في الجرائم المعلوماتيّة فشراء برامج إختراق ومعدات لفك الشفرات يمثل جريمة في حدّ ذاتها، وذلك يرجع إلى صعوبة الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في الجرائم المعلوماتية. كما أنّ السلوك المادي في الجريمة المعلوماتية المتمثل في الطابع التقني يجعل الجريمة عبر الإنترنت ذات طابع موحد بالضرورة، وهذه الطبيعة الموحدة من حيث إتّحاد جميع أشكالها الماديّة تدفع بالضرورة إلى إستخدام الآلة كوسيط إلى إرتكابها، وهنا تتّصف الجريمة بالطابع التقني.[٣٨]وتثير أيضا مسألة النتيجة الإجرامية في الجريمة المعلوماتية مشاكل عديدة، ومنها ما يتعلق بمكان وزمان تحقُّق النتيجة الإجرامية. فلو قام أحد المجرمين في بلد ما باختراق جهاز خادم (Server) أحد البنوك في بلد آخر، وهذا بلد موجود في مكان ثالث فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الجهاز الخادم، وما هو القانون الواجب التطبيق في هذا الشأن ؟ كلّ هذه الإشكاليّات المتعلّقة بخصوصيّة الجرائم المعلوماتيّة تطرح صعوبات حقيقيّة أمام الجهود الوطنيّة والدوليّة لمكافحة هذا النوع المستحدث من الجرائم، وهو موضوع الجزء الثاني من هذا المبحث.

ثالثاً– الركن المعنوي :يمثّل الركن المعنوي الجانب الذاتي الخاص بالجريمة مباشرة، فهو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني. ولا يكتمل الوجود القانوني للجريمة إلاّ بإقتران ركنها المادي بالركن المعنوي الذي قوامه الإرادة المجرمة والتي تتّجه نحو الفعل الإجرامي، وبالتالي تحقيق النتيجة الإجرامية.[٣٩] وهذه الإرادة تتمثّل في القصد الجنائي. ويعني القصد الجنائي تعمد إتيان الفعل المحرم أو تركه مع العلم بأنّ الشارع يحرم الفعل أو يوجبه. ويقوم القصد الجنائي على عنصري العلم والإرادة، وهذان العنصران يمتدان ليشملا كل الوقائع الماديّة التي تتكوّن منها الجريمة. وبالنظر إلى خصوصيّة الجرائم المعلوماتيّة عن الجرائم التقليديّة، يُطرح التساؤل في هذا الصدد حول **كيفيّة تحقُّق الركن المعنوي في الجريمة المعلوماتيّة؟**

الركن المعنوي للجريمة المعلوماتية : إنّ توافر الركن المعنوي في الجرائم المعلوماتيّة يعدّ من الأمور الهامّة في تحديد طبيعة السلوك المرتكب وتكييفه لتحديد النصوص التي يلزم تطبيقها. فالجرائم الإلكترونية تُرتكب بشكل قصدي، وذلك بسبب طبيعة هذه الجرائم، حيث يكون لدى الجاني القدرة على إستخدام الحاسوب، والبيئة الإلكترونية، وغالبا ما يكون مرتكب هذه الجرائم من أشخاص أذكياء لديهم مهارات عالية في إستخدام الإنترنت، وبالتالي يكون لديه العلم والإرادة الكاملة بتحقيق النتيجة الإجرامية. وتطبيقا لذلك فإنّ المشرّع الأمريكي قد راوح في تحديد الركن المعنوي للجريمة بين مبدأ الإرادة، كما هو الشأن في قانون العلامات التجاريّة في القانون الفيدرالي الأمريكي، ومبدأ العلم، كما الأمر في قانون مكافحة الإستنساخ الأمريكي.وقد برزت هذه المشكلة في قضية موريس الّذي كان متّهما في قضية دخول غير مصرّح به على جهاز حاسب فيدرالي، وقد دفع محامي موريس بإنتفاء الركن المعنوي للجريمة. الأمر الذي جعل المحكمة تطرح السؤال التالي: "هل يلزم أن يقوم الإدعاء بإثبات القصد الجنائي في جريمة الدخول غير المصرّح به، بحيث تثبت نيّة المتهم في الولوج إلى حاسب فيدرالي، ثم يلزم إثبات نيّة المتّهم في تحدي الحظر الوارد على إستخدام نظم المعلومات في الحاسوب وتحقيق خسائر، ومثل هذا الأمر يستدعي التوصل إلى تحديد أركان جريمة الدخول دون تصريح." وقد ذهبت المحكمة إلى تبنّي معيارين هنا هما الإرادة بالدخول غير المصرّح به، وكذا معيار العلم بالحظر الوارد على إستخدام نظم معلومات فيدرالية دون تصريح.[٤٠] أمّا بالنسبة للقضاء الفرنسي فإنّ منطق سوء النية هو الأعم في شأن الجرائم المعلوماتية، حيث يشترط المشرّع الفرنسي وجود سوء نية في الإعتداء على بريد إلكتروني خاص بأحد الأشخاص. كذلك الحال بالنسبة للمشرع البريطاني، فالركن المعنوي في الجريمة المعلوماتية يتطلب أن تنصرف إرادة الجاني إلى الدخول إلى البيانات أو المعطيات المخزنة في أي حاسوب، إذ جرم المشرع البريطاني الدخول غير المصرح به للنظام الالكتروني.[٤١]

المطلب الثاني : الصعوبات والتحديات التي تواجه مكافحة الجرائم المعلوماتية

تُمثّل جرائم المعلوماتيّة أفعال إجراميّة مستحدثة أنتجتها تقنية المعلومات[٤٢]، فهي ترتبط بها وتقوم عليها. وهذا ما أكسبها لوناً وطابعاً قانونياً خاصاً يُميّزها عن غيرها من الجرائم غير المستحدثة التقليدية بمجموعة من السمات أضفت عليها خصوصيّة غير عاديّة تعكس، في الوقت ذاته، مدى التحدّيات والصعوبات الّتي تواجه إثبات الجرائم المعلوماتية ومكافحتها[٤٣] والّتي يمكن حصرها إجمالاً فيما يلي:

أوّلاً – صعوبة إثبات الجرائم المعلوماتيّة : تتمثّل المشكلة الأساسية التي تثيرها الجريمة المعلوماتية في طبيعة الركن المادي فيها، حيث أنّ مناط التجريم ينصب على نظام الكتروني يساء استعماله أو يتمّ اقتحامه على نحو غير مشروع. ويلاحظ أنّ هذا الإستعمال أو الاقتحام له أثر مادي ملموس يتمثل في تدمير المعلومات، وهو ما يثير إمكانية الإتلاف العمدي للمنقولات أو السرقة وذلك عن طريق إساءة استعمال بطاقات الائتمان، أو يثير شبهة التزوير عن طريق التلاعب في بيانات الحاسب.ويلاحظ أنّ هناك فرق بين السلوك الإجرامي في الجريمة العادية والجريمة المعلوماتية المترتب على السلوك الإجرامي وهي العدوان الواقع على الحق الذي حماه النظام وأقرّ بعقوبة على من إعتدى عليه. فالسلوك الإجرامي في الجريمة التقليدية يتمّ رؤيته والتأكد منه مثل فعل القتل، فالجريمة هنا لها ملامح واضحة. أمّا السلوك الإجرامي في الجريمة المعلوماتية يرتبط دائما بالمعلومة المخزنة في الحاسب أو التي يتمّ إدخالها إليه، ومن خلال الضغط على زر في الحاسب يتمّ تدمير النظام المعلوماتي أو حصول السرقة أو التسلل إلى نظام أرصدة العملاء في البنوك.[٤٤]وتتميّز الجرائم المعلوماتيّة بصعوبة إثباتها[٤٥] من حيث عدم إيجاد الدليل الذي يُدين مرتكب الجريمة بطريقة سهلة ومنهجية ذلك أن الجرائم المعلوماتية يسهل فيها محو الدليل، والتلاعب فيه، خصوصاً مع عدم وجود الدليل المادي للجرائم المعلوماتية (كالدم والشعر، والبصمة، ... الخ)[٤٦] بالإضافة إلى عدم توفر الخبرة الكافية لدى رجال الشرطة في الأمور الفنية والتفصيلية ذات الصلة بالجرائم المعلوماتية.[٤٧]وتكمن صعوبة الركن المادي في الجريمة الالكترونية في أنّ الجريمة ترتكب عن طريق معلومات تتدفق عبر نظام الحاسب الآلي لا يمكن الإمساك بها ماديّاً. كما أنّ السلوك الإجرامي في هذه الجريمة يتطلب وجود بيئة رقمية لا علاقة لها بالورق أو المحررات، جهاز كمبيوتر، شبكة انترنت، ومعرفة بداية هذا النشاط والشروع فيه ونتيجته[٤٨] فهي بيئة افتراضية من خلال الشبكة العنكبوتية بعيداً عن الأدلة المادية والآثار الملموسة.[٤٩] وبذلك فإنّ الجاني لا يترك أدلّة خلفه تقود الجهات المختصة لضبط مسرح الجريمة نظرا لفضائية العالم الإفتراضي بالإضافة الى مهارة المجرم المعلوماتي في بعض الجرائم الإلكترونية مثل نشر الفيروسات وإختراق المواقع والوصول الى المعلومات السرية والبنكية والإئتمانية كما يساعد على ذلك تطوّر برامج تغيير المواقع وعدم التتبع وظهور وتنامي الأنشطة الإجراميّة الإلكترونية وتوسل مرتكبيها بتقنيات جديدة غير مسبوقة في مجال تكنولوجيا المعلومات والإتّصالات حيث أنّ ظاهرة الجرائم المعلوماتيّة باتت تتخذ أنماطاً جديدة وضرباً من ضروب الذكاء الإجرامي وهذا بلا شك يمثل تحديّاً جدياً وجديداً في الوقت الحاضر.[٥٠]

ثانياً– صعوبة إكتشاف الجرائم المعلوماتية : تُعدّ الجرائم المعلوماتية من الجرائم غير المقيدة والمرتبطة بمنطقة جغرافية معينة فمن الممكن أن ترتكب الجريمة في أي وقت دون الإلتزام والتقيد بدولة ما أو منطقة ما أو بقرب المسافات أو تباعدها، ويتم إرتكاب الجرائم المعلوماتية بواسطة الحواسيب وعن طريق الشبكة المعلوماتيّة.[٥١] وهذه الجرائم لا تعرف الحدود بين الدول والقارات[٥٢] وهي بذلك شكل جديد من أشكال الجريمة العابرة للحدود الإقليمية بين دول العالم بأكمله[٥٣]، حيث أنّ القائم على النظام المعلوماتي في أيّ دولة يمكنه أن يحول مبلغا من المال لأيّ مكان في العالم مضيفاً له صفر أو بعض الأصفار لحسابه الخاص، بل يستطيع أيّ شخص أن يعرف كلمة السرّ لأيّ شبكة في العالم ويتّصل بها ويغيّر ما بها من معلومات.[٥٤]وينتج عن تباعد المسافات بين الفعل غير المشروع الذي يرتكبه المجرم المعلوماتي والنتيجة الإجرامية لهذا الفعل صعوبة في اكتشاف الجريمة المعلوماتية[٥٥] نظراً لعدم وجود الفاعل أي المجرم المعلوماتي ولإرتكاب جريمته عن بعد ومن ثم تباعد المسافات بين الفعل الذي يرتكب من خلال جهاز الحاسوب وبين النتيجة الإجرامية حيث لا تقف الجريمة المعلوماتية عند حدود دولة معينة، بل تمتد إلى حدود الدول الأخرى، وبالتالي يصعب اكتشافها والوصول إلى الحقيقة.[٥٦]

ثالثاً – الطابع التقني للجرائم المعلوماتية :

تعود صعوبة إكتشاف الجرائم المعلوماتية وإقامة الدليل على مرتكبيها إلى الطابع التقني لهذا النوع من الجرائم الذي يضفي عليها الكثير من التعقيد والصعوبة في الإثبات، وإقامة الدليل على من يرتكب هذه الجرائم[٥٧]، كما أن سهولة تدمير المعلومات وسرعة التخلص منها سمة من سمات هذه الجريمة التي يصعب اكتشافها. ولذلك من الضروري تكاتف الجهود الدولية والوطنية للدول في مجال إعداد وتدريب رجال الشرطة الدولية (الأنتربول)، والشرطة المحلية للدول إعداداً تقنياً وفنياً في مجال مكافحة الجرائم المعلوماتية عن طريق تأهيلهم بعمل دورات متخصصة في موضوع هذا النوع من الجرائم، كما يلزم أيضاً إيجاد محاكم متخصصة يمتاز قضاتها بدرجة عالية من التأهيل العلمي والتقني

في موضوع هذه الجرائم أو على الأقل وجود هيئات قضائية متفرغة متخصصة بالنظر في مثل هذا النوع من الجرائم[٥٨]، بالإضافة إلي تحديد أدلة الإثبات في قوانين مكافحة الجرائم المعلوماتية بالتنسيق مع الدول والأمم المتحدة في هذا الإطار، وذلك لصعوبة إثبات هذا النوع من الجرائم والكشف عن مرتكبيها.

رابعاً – قلّة الإبلاغ عن الجرائم المعلوماتيّة :

نظراً لحساسية هذا النوع من الجرائم وما يتعرض له المجني عليه كطرف في الجريمة من تشهير فيما لو أبلغ عن الجريمة، فإنّ الإبلاغ عن هذا النوع من الجرائم ضعيف مقارنة مع غيرها من الجرائم[٥٩]، حيث أنّ معظم جرائم الإنترنت والجرائم المعلوماتية يتم اكتشافها على سبيل الصدفة، وقد يكون هذا الإكتشاف بعد مدّة طويلة من ارتكاب الجريمة بل أن أغلب الشركات والمؤسسات في مجتمع الأعمال تحجم عن الإبلاغ تجنباً للإساءة إلى السمعة وهزّ الثقة فيها. وبذلك فإنّ الفجوة بين عدد هذه الجرائم الحقيقي وبين ما تم اكتشافه فجوة كبيرة فنقص الخبرة لدى الجهات المختصة أدى إلى ازدياد عدد الجرائم المعلوماتية بشكل ملحوظ، وذلك بسبب عدم قدرة هذه الجهات على التعامل مع هذا النوع من الجرائم المستحدثة بالوسائل الإستدلالية والإجراءات الجنائية التقليدية[٦٠].ولذلك من الضروري اليوم وبصفة ملحة تعديل قوانين مكافحة الجرائم المعلوماتية بوجود نصوص تحمي المبلغ في هذه الجرائم من حيث سريّة التبليغ وسرية التحقيق والمحاكمة في هذا النوع من الجرائم، كذلك اشتمال النصوص على حوافز لمن يُبلغ عن هذه الجرائم كمبلغ مالي مثلا يُعطى للشخص الذي يبلغ عن هذه الجرائم تشجيعاً للتبليغ عنها وبالتالي مكافحتها.

خامساً– غياب مفهوم موحّد للجرائم المعلوماتيّة :

يعود عدم وجود إتّفاق عام بين الدول على مفهوم موحد وشامل للجرائم المعلوماتيّة إلى أنّ الأنظمة القانونيّة في دول العالم كافّة لا تتفّق على الأفعال المجرّمة فيما يتعلّق بالجرائم المعلوماتيّة. فبالرجوع إلى التشريعات المختلفة المتعلّقة بمكافحة الجرائم المعلوماتيّة يتبيّن عدم وجود إتّفاق مشترك بين الدول حول الأفعال الإجراميّة الّتي تُمثّل إساءة إستخدام للنظم المعلوماتيّة وشبكات الإنترنت وبالتالي تكوّن جرائم معلوماتيّة. وعلى هذا الأساس فإنّ الأفعال المشروعة في أنظمة بعض الدول قد تكوّن مجرّمة وغير مشروعة في قوانين دول أخرى.[٦١] ويرجع ذلك إلى إختلاف البيئات والعادات والتقاليد والأعراف والثقافات والديانات وأيضا مستوى التقدّم المعلوماتي من مجتمع إلى آخر، هذا بالإضافة إلى قصور التشريعات ذاتها في كثير من الدول وعدم مواكبتها للتطوّر التكنولوجي والتقني وغياب التوافق بين قوانين الإجراءات الجنائية للدول بشأن التحقيق في تلك الجرائم.[٦٢]ومهما يكن من أمر، يستخلص ممّا سبق بسطه أنّه بالنظر خاصّة لصعوبة الكشف عن الجرائم المعلوماتية وغياب الدليل المادي الذي يدين مرتكبها، فإنّ الجرائم المعلوماتية أصبحت تطغى على ساحة الإجرام وبشكل كبير[٦٣]. وقد ترتّب على إنتشار هذا النوع من الجرائم تحدّيات واجهت المجتمع الدولي، فتزايد الأنشطة الإجرامية الإلكترونية وتسلح مرتكبيها بتقنيات جديدة غير مسبوقة في مجال تكنولوجيا المعلومات والإتّصالات يسّرت لهم إرتكاب هذه الجرائم داخل حدود الدولة وخارجها، الأمر الذي أدى إلى إنشغال الدول والمنظمات والمؤتمرات الدولية بهذا النوع من الجرائم وسبل مكافحتها، إذ أصبحت الحاجة ملحّة لحماية المعلوماتيّة والتصدّي للإجرام المعلوماتي على الصعيدين الوطني والدولي[٦٤]. وهنا يطرح التساؤل عن الآليات والجهود الوطنيّة والدوليّة في مكافحة الجرائم المعلوماتيّة ومدى نجاعتها؟

المبحث الثاني مدى نجاعة الآليات والجهود الوطنية والدولية في مكافحة الجرائم المعلوماتية

في ظلّ التطور التكنولوجي السريع وما إقترن به من إساءة استخدام التكنولوجيا الإلكترونية ووسائل الإتّصال الحديثة، أصبح واقعاً إنتشار وتطوّر الجرائم المعلوماتيّة، كما أصبحت هذه الجرائم خطراً يهدّد المجتمع الدولي، خاصّة بعد لجوء التنظيمات الإرهابية لإستخدام الفضاء الإلكتروني وإستقطاب عناصر جديدة لهجمات عابرة للحدود والقارّات، إضافة إلى جرائم السطو والقرصنة على المؤسسات الماليّة سواء الوطنيّة أو الدوليّة[٦٥]. وهذا ما جعل الدول تقف وقفة جادّة من أجل وضع الحلول لمعالجة المشكلات والحدّ من هذه الظواهر الإجراميّة المستحدثة والخطيرة الّتي أصحت تهدّد أمن المجتمعات والدول وحرمة وسلامة مواطنيها والبنى التحتيّة الأساسيّة، وهو ما نبّهت إليه الأمم المتّحدة وغيرها من التنظيمات الدوليّة ذات العلاقة على المستويات العالميّة والإقليميّة. ففيما تتمثّل الآليات والجهود الوطنيّة والدوليّة لمكافح الجرائم المعلوماتيّة؟ وما مدى فاعليّتها في الحدّ من هذه الجرائم ومقاومتها؟ تقتضي التحدّيات والصعوبات التي تطرحها مكافحة الجرائم المعلوماتيّة جهوداً على المستوى الداخلي والخارجي وتعاوناً دوليّاً. لذلك فإنّ هذا المبحث سيتناول بالدراسة مطلبين أساسيين: آليات وجهود

مكافحة الجرائم المعلوماتيّة على المستوى الوطني **(المطلب الأوّل)** ثمّ آليات وجهود مكافحة الجرائم المعلوماتيّة على المستوى الدولي **(المطلب الثاني)**.

المطلب الأول: آليات وجهود مكافحة الجرائم المعلوماتية على المستوى الوطني

أمام تزايد إنتشار الجرائم المعلوماتيّة والتهديدات الخطيرة الّتي تُهدّد أمن الدول من خلال إختراق المواقع الإلكترونية لرؤساء الدول والحكومات والوزارات والتجسّس عليها وتدميرها، والإطلاع على مختلف المعلومات الأساسيّة والسريّة للدول خاصّة الأمنيّة منها، إضافة إلى المؤسسات الإقتصادية كالبنوك والبورصات العالمية، وحتّى الجوانب الإجتماعية والثقافية بتدمير مواقع المستشفيات ومصانع توليد الطاقة، والماء، والغاز، ونشر ثقافة التطرف الديني والإرهاب[٦٦]، عملت العديد من الدول على مواجهتها لتحقيق أمنها وإستقرارها. وفيما يلي نعرض أهمّ الجهود الوطنيّة في مكافحة الجرائم المعلوماتيّة:

أوّلا- المملكة العربية السعودية تعتبر المملكة العربية السعودية من أبرز الدول المتقدّمة عالمياً في توفير الخدمات الحكومية الإلكترونية من خلال البوابات والمنصات الحكومية؛ وهي أيضا من أكثر الدول عرضة للتهديدات الإجراميّة والهجمات الإلكترونيّة[٦٧]، لذلك إتّخذت المملكة العديد من الإجراءات والآليات مكافحة الجرائم المعلوماتيّة وتتمثّل فيما يلي:

1- إصدار تشريع خاص بمكافحة الجرائم المعلوماتيّة : " نظام مكافحة جرائم المعلوماتيّة " لمكافحة أي جريمة من الجرائم لابد أن يكون هناك بنية قانونية عقابيّة تحكمها، وأن يكون هناك جهة قضائية تطبّق الجزاء على من يقوم بإرتكابها. لذلك، وعلى الرغم من أنّ المملكة تعتمد على القوانين الشرعيّة والتي تستمدّ أصولها من كتاب الله والسنة النبوية، فإنّها سبقت نظيراتها من الدول العربيّة في إصدار قانون خاصّ بمكافحة جرائم المعلوماتية، بمقتضى المرسوم الملكي رقم م/17 في 1428/03/08هـ بناء على قرار مجلس الوزراء رقم 79 بتاريخ 1428/03/08هـ[٦٨]. ويتألف النظام من 16 مادّة؛ تشمل المادّة الأولى بعض التعريفات الرئيسة، وتوضح المادّة الثانية الهدف من القانون، وتضمّنت المواد من 3- 13 الجرائم والعقوبات، وتُبيّن المادّتين 14 و15 دور الهيئات المختصة، أمّا المادّة 16، فقد أوضحت تاريخ دخول القانون حيز النفاذ وقد حددته في مائة وعشرين يومًا من تاريخ نشره. والجدير بالذكر، أنّ للقانون العديد من نقاط القوّة حيث نصّ على الإلتزام بمدأ الشرعيّة الجنائيّة الذي يقضي بأن لا جريمة ولا عقوبة إلا بنص، وإشتمل على غالبيّة الجرائم المعلوماتيّة وعقوباتها التي تنوعت بين السجن لمدد مختلفة والغرامات المالية بحسب نوع وطبيعة كل جريمة منها، ويهدف إلى حماية المجتمع من جرائم المعلوماتية والحد منها والمساعدة على تحقيق الأمن المعلوماتي وحفظ الحقوق المترتّبة عن الإستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية وحماية المصلحة العامّة والأخلاق والآداب العامّة وحماية الإقتصاد الوطني.

2- المصادقة والإنضمام إلى الإتّفاقية العربيّة لمكافحة جرائم تقنية المعلومات[٦٩] :صادقت السعودية على هذه الإتّفاقيّة العربية لمكافحة جرائم تقنية المعلومات الصادرة سنة 2010، الّتي تضمّ العديد من الجرائم المعلوماتيّة مثل سرقة بطاقات الإئتمان، وجرائم الإنترنت والإرهاب الإلكتروني، وتصنيع الفيروسات أو نشرها، والقرصنة وإختراق الأنظمة، والوصول والإختراق غير المشروع، وغير ذلك. وتأتي هذه الإتّفاقيّة ضمن الجهود العربية الحثيثة التي تقوم بها جامعة الدول العربيّة لوضع التدابير الأمنية اللازمة لمكافحة الجرائم في شتّى أشكالها وصورها ومنها جرائم تقنية المعلومات عبر إيجاد الأسس النظامية والبيئة القانونية، وتعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، وترسيخ الهدف النبيل والغاية في المحافظة على الأمن والمصير المشترك الذي يتطلّب تضافر الجهود للحفاظ على أمن وإستقرار المجتمعات الإنسانيّة. وتُعدّ هذه الإتفاقية نقطة تحول في التعاون العربي لمكافحة الجرائم السيبرانية، حيث نصّت الإتّفاقية على التعاون العربي في مكافحة الجرائم المعلوماتية في العديد من المجالات منها: التعاون القضائي، تبادل المعلومات، تبادل الخبرات، الإختصاص القضائي، تسليم المجرمين، المساعدة القضائية وغيرها من الموضوعات ذات الصلة[٧٠]، وأوضحت المادة الثالثة من الإتّفاقية مجالات تطبيقها على النحو التالي: " تنطبق الإتّفاقيّة على جرائم تقنية المعلومات بهدف منعها والتحقيق فيها وملاحقة مرتكبيها.

3 -الجهود الحكوميّة في مكافحة جرائم المعلوماتيّة :لا شك أنّ القوانين لا يكفي في حدّ ذاتها ولا يتحقّق الهدف منها إلاّ بإحداث أجهزة ومؤسّسات حكوميّة لتنفيذها. وفي هذا الإطار تقوم الوزارات والهيئات الحكوميّة السعوديّة المختلفة بجهود جبّارة في مكافحة الإجرام الإلكتروني بمختلف أشكاله، ونذكر منها على سبيل المثال:

أ- وزارة الإتّصالات وتقنية المعلومات السعودية : هي الوزارة المسؤولة عن جميع وسائل الإتّصال وتقنية المعلومات في المملكة، ولها سلطة إقتراح مشاريع الأنظمة المتعلقة بالإتّصالات وتقنية المعلومات ورفعها إلى مجلس الوزراء، وقد قامت الوزارة بإصدار العديد من

القرارات المنظمة للتعاملات الإلكترونية منها: القرار رقم 7/ب/33181 لسنة 2003، المتضمن وضع خطة لتقديم الخدمات والمعاملات الحكوميّة، والقرار رقم م/ب/8189 لسنة 2005، الخاص بتشكيل لجنة داخل كل جهة حكوميّة للتعاملات الإلكترونيّة [٧١]. وقد أسهمت الوزارة بصورة كبيرة في الجهود التي تبذلها الدولة لمكافحة الجرائم المعلوماتيّة، من خلال إقتراحها للإستراتيجية الوطنيّة لأمن المعلومات الخاصّة بالمملكة العربية السعودية في عام 2011 الّتي تُقدّم رؤية واضحة للمملكة هدفها توفير بيئة رقميّة آمنة وقويّة، من خلال العمل على:

- تطوير بنية تحتية لتكنولوجيا المعلومات آمنة ومرنة وموثوق فيها.
- توفير موارد بشرية قادرة على تحقيق الأمن المعلوماتي بأعلى درجاته.
- تهيئة بيئة لأمن المعلومات ملهمة قائمة على الثقة والشفافية والتعاون.
- دعم خدمات الحكومة الإلكترونية ودعم البنية التحتية للمملكة من أجل الإيفاء بأهداف الأمن المعلوماتي وخطط واستراتيجيات تكنولوجيا المعلومات والاتصالات.
- تعزيز النمو الاقتصادي من خلال البحث والتطوير [٧٢].

ب- وزارة الداخلية السعودية : تُعتبر وزارة الداخلية الوزارة المسؤولة عن مراقبة شؤون الأمن الداخلي، وفي هذا الصدد تسعى الوزارة إلى التصدي للجرائم المعلوماتية، وتقوم بعمل إجتماعات لبحث إستعداداتها لمباشرة إستقبال بلاغات هذه الجرائم، وأسلوب تحريز الأدلة الرقميّة[٧٣]، وتحديد هوية المجرمين الرقميين، ومراقبة الإنترنت للأغراض الجنائية، وقد تصدّت الوزارة إلى العديد الأنشطة الإجراميّة الإلكترونية الخطيرة[٧٤].

ج- وزارة العدل السعودية :تختص وزارة العدل بالإشراف على النظام القضائي في المملكة، كما لها سلطة ضمان الإمتثال لمتطلبات مكافحة غسل الأموال وتمويل الإرهاب. ولقد شهدت المحاكم السعودية زيادة هائلة في عدد القضايا المتعلّقة بالجرائم المعلوماتيّة؛ حيث تعمل المحاكم على مكافحة هذه الجرائم وذلك بمعاقبة مرتكبيها.والجدير بالذكر، أن مكافحة الجرائم المعلوماتيّة لم تقتصر على الوزارات المذكورة، بل إن هناك الكثير من الجهود التي تبذلها الوزارات والأجهزة الأخرى، من بينها وزارة التعليم، من خلال ما تقوم به من مجهودات في التوعية بخطورة هذه الجرائم وذلك بتنظيمها للعديد من المؤتمرات في الغرض.

4- الهيئة الوطنيّة للأمن السيبراني : استشعارا لأهميّة البيانات والأنظمة التقنية والبنى التحتية الحساسة وإرتباطها بالمصالح الوطنيّة، وأهميّة حمايتها من أي تهديدات أو مخاطر يشهدها الفضاء المعلوماتي، أنشأت السعودية الهيئة الوطنية للأمن السيبراني التي ترتبط بالملك –حفظه الله– وتمّت الموافقة على تأسيسها وتنظيمها بمقتضى الأمر الملكي بتاريخ1439/02/11هـ الموافق لـ2017/02/11م، لتكون " الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه، وتهدف إلى تعزيزه؛ حمايةً للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية." وقد كان هذا القرار نتيجة لما تتعرّض إليه المملكة من الهجمات السيبرانية[٧٥]. وتتمثّل الأهداف والمهام الرئيسيّة للهيئة في حماية مصالح المملكة العربية السعوديّة الحيويّة من الهجمات السيبرانية وتعزيز الأمن السيبراني وحماية الأمن الوطني والبنى التحتية الحساسة في المملكة، والحفاظ على سريّة وخصوصيّة وجاهزيّة تكامل البيانات والمعلومات في المملكة العربية السعودية، وتحقيق التكامل بين أجهزة الدولة المعنية بذلك المجال مثل (المركز الوطني للأمن الإلكتروني في وزارة الداخلية، ومركز التميّز في جامعة الملك سعود، ومركز الأمن السيبراني في مدينة الملك عبد العزيز للعلوم التقنية) حرصاً أن تكون جميع الأجهزة والأعمال والبيانات مَحكومة بنظام أمني قوي.[٧٦]

5- هيئة الإتّصالات وتقنية المعلومات السعوديّة :نصّت المادّة 14 من نظام مكافحة جرائم المعلوماتيّة المشار إليه على أنّه:" تتولى هيئة الإتّصالات وتقنية المعلومات وفقًا لإختصاصها تقديم الدعم والمساندة الفنيّة للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة." وإدراكاً منها للحاجة الملحة للتوعية بمخاطر هذا النوع من الجرائم، وإساءة إستخدام خدمات الإتّصالات وتقنية المعلومات، تقوم الهيئة بدور هامّ في رفع مستوى الوعي بسبل مكافحة الجرائم المعلوماتيّة، فضلاً عن تبيان حقوق المستخدمين وفق ما كفله لهم النظام، مع التوعية بسبل الوقاية من خطر الوقوع ضحايا لأيّ نوع من هذه الجرائم. وفي هذا الإطار أطلقت الهيئة أكثر من 1435 حملة توعية للتعريف بنظام مكافحة جرائم المعلومات[٧٧]. يتّضح ممّا سبق، أن المملكة وضعت مهمّة

مكافحة الجرائم المعلوماتيّة ضمن أولويتها واتّخذت عديد الإجراءات وتبنّت الخطط والإستراتيجيات التي تهدف إلى محاربة هذا النوع من الجرائم.

ثانياً – الإمارات العربية المتّحدة تحظر دولة الإمارات العربية المتّحدة الجرائم المعلوماتيّة بإعتبارها جرائم مستحدثة، وقد أصدرت القانون الإتّحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات وهو من القوانين الريادية الأولى في العالم العربي الذي تضمن تفاصيل كثيرة، حيث وضح معاني المصطلحات المستعملة وذات الدلالة القانونية وهي المعلومات الإلكترونية، البرنامج المعلوماتي، نظام المعلومات الإلكتروني، الشبكة المعلوماتيّة، المستند الإلكتروني، الموقع وغيرها من المصطلحات، كما بيّن النظام الجرائم المعلوماتيّة والعقوبات المقرّرة لها والتدابير لمكافحة هذه الجرائم[٧٨]. وقد صدر مؤخّرا قانون الجرائم الإلكترونية الجديد، الذي تم تبنيه بموجب المرسوم بقانون إتّحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية ليحل محل القانون الإتّحادي السابق لعام 2012.[٧٩]

ثالثاً– الأردن الأردن مثل باقي دول العالم يعاني من تفشي مختلف أنواع الجرائم المعلوماتيّة، ولهذا تبرز جهود الأردن في مقاومة هذه الجرائم من خلال عدّة جوانب. فمن الناحية القانونيّة تمّ في البداية إصدار قانون المعاملات الإلكترونية المؤقت رقم 85 لسنة 2001 المنشور على الصفحة 6010 من عدد الجريدة الرسميّة رقم 4524 بتاريخ 2001/12/03[٨٠] الذي تمّ إلغائه وتعويضه بقانون المعاملات الإلكترونية رقم 15 لسنة 2015[٨١]. كما أقرّ مجلس الوزراء قانون جرائم أنظمة المعلومات لسنة 2010 [٨٢]، ويأتي هذا النظام في ظلّ إستفحال الجرائم المعلوماتيّة وتهديداتها الخطيرة للأمن الوطني والمؤسسات والأفراد لوضع آليات قانونيّة لمكافحتها. كما قامت مديريّة الأمن العام بدرء فعال في هذا المجال من خلال إنشاء قسم خاص للجرائم الإلكترونيّة في مديريّة الأمن العام تتبع إدارة البحث الجنائي في عام 2008 [٨٣] حيث تقوم بملاحقة مرتكبي هذه الجرائم والتصدي لها والحدّ منها. كما وقّعت المملكة الأردنيّة إتّفاقيات للحدّ من هذه الجرائم، بالإضافة إلى إطلاق مشروع تطوير قدرات التعامل مع الجرائم الإلكترونيّة[٨٤] وغيرها من المجهودات.

رابعاً– قطر نص قانون العقوبات القطري الصادر بالقانون رقم 11 لسنة 2004 على جرائم الحاسب الآلي، وأدرجها ضمن الجرائم الواقعة على المال، ونظمها في 18 مادّة تبدأ بالمادّة 370 وتنتهي بالمادّة 387، حيث احتوت على أحكام تتعلق بنظام المعالجة الآليّة للبيانات، وفيروس الحاسب الآلي، وبطاقات الدفع الممغنطة. وتعتبر دولة قطر من أوائل الدول العربية التي وضعت أحكاماً في قانون العقوبات تتعلق بالجرائم ذات الصلة بالحاسب الآلي[٨٥]. كما اهتم المشرع القطري أيضا بالتعاون القضائي الدولي في مجال الجريمة وهذا يتجلى من خلال ما تضمنه قانون الإجراءات الجنائية القطري رقم 23 لسنة 2004 من أحكام. كما أولى المشرع القطري إهتماماً كبيراً للتعاون الدولي في مجال مكافحة الجريمة. كما أصدر القانون رقم 14 لسنة 2014 المتعلّق بمكافحة الجرائم الإلكترونية لمواجهة الإعتداءات التي يتعرض لها النظام المعلوماتي، ومواكبة الوسائل الحديثة التي يرتكب بها هذا النوع من الجرائم والذي تضمن كل الأحكام والآليات وسبل التعاون الدولي لمكافحتها. وفي نفس الصدد أصدر المشرّع القطري القانون رقم 20 لسنة 2019 المتعلّق بمكافحة غسل الأموال وتمويل الإرهاب، هذا بالإضافة إلى الأجهزة المتعدّدة المختصة في مكافحة الجرائم المعلوماتيّة ومنها نيابة الجرائم الإلكترونية، نيابة التعاون الدولي، إدارة مكافحة الجرائم الإقتصادية والإلكترونية، إدارة الإتّصال للشرطة العربية والدولية (الإنتربول) بوزارة الداخليّة التي تقوم بجهود كبيرة في هذا المجال وغيرها[٨٦]

خامساً – العراق بهدف توفير الحماية القانونية وإيجاد نظام عقابي لمرتكبي جرائم الحاسوب وشبكة المعلومات ولغرض تنظيم ومعالجة الجرائم المرتكبة عن طريق الإنترنت تولى البرلمان العراقي تقديم مسودة قانون مكافحة الجرائم المعلوماتية منذ سنة 2011 ولكنّه بقي إلى اليوم معلّقا وعلى الرغم من معالجة الجرائم المعلوماتيّة في أكثر من قانون عقابي ومنها قانون العقوبات وقانون مكافحة الإرهاب وغيره من القوانين الأخرى؛ يظلّ العراق في حاجة إلى التسريع بإصدار نظام خاص بمكافحة الجرائم المعلوماتيّة[٨٧].تختلف سياسات وتشريعات مواجهة الجرائم المعلوماتيّة على المستوى الوطني من دولة إلى أخرى، حسب الطبيعة السياسية، الإقتصادية والإجتماعية لكلّ دولة، ولكن على الرغم من تلك الجهود المبذولة وطنيّا في مجال مكافحة الجرائم المعلوماتيّة فهي ما زالت دون المستوى المطلوب سواء من حيث إيجاد محاكم متخصصة أو دوائر تحقيق تكون مساندة للقضاء ومتخصصة للنظر في هذا النوع من الجرائم، أو من حيث الإهتمام بالجانب التدريبي لكوادر الأمن العام أو القضاة خاصة وأن الجرائم المعلوماتية تُعدّ من الجرائم التي تحتاج إلى معرفة فنيّة دقيقة من أجل التعامل مع مرتكبيها. كما أن الجانب التشريعي في مكافحة الجرائم المعلوماتية يعتريه الكثير من النقص في العديد من المحاور وخاصة فيما يتعلق بالإجراءات

الجزائية للتعامل مع هذا النوع من الجرائم. كما أنّه أيضاً لا يكفي وضع حلول لضبط هذه الجرائم على المستوى الوطني، بل لا بدّ من إيجاد إطار شمولي يضمن عدم تكرار هذه الجرائم على المستوى الدولي، وهو ما يتطلب جهودًا دولية بالتعاون مع الدول بعضها البعض.

المطلب الثاني : آليات وجهود مكافحة الجرائم المعلوماتيّة على المستوى الدولي

تُعتبر الجريمة المعلوماتية من الجرائم العابرة للحدود، ممّا يُؤدي إلى توزيع أركانها على عدّة دول، كما أنّ أدلة إثباتها يسهل طمسها ومحوها، ممّا يجعل القوانين الوطنية التقليدية عاجزة عن مواجهتها، ولهذا فإنّ مواجهتها تستدعي وجود كيان دولي يسعى إلى إتّخاذ كافة التدابير والإجراءات الضرورية للحد من إنتشارها ومعاقبة مرتكبيها، وهذا ما يتطلب وجود تعاون بين الهيئات الأمنية والقضائية الدوليّة[٨٨] إذ في ظل إنتشار الجرائم المعلوماتية وتزايد مخاطرها وتهديداتها، أصبح التعاون الدولي ضرورة ملحة، وليس الغرض منه معاقبة المجرمين أين ما كانوا وإنّما تشمل الردع والوقاية من هذه الجرائم.[٨٩] وهذا ما جعل المجتمع الدولي يتّجه نحو إنشاء أجهزة تعاونيّة تعمل على مستويات حكومية أو غير حكومية من أجل ضمان التنسيق والمتابعة فيما يُتخذ من تدابير دوليّة وداخليّة لمكافحة هذه الجرائم.[٩٠] **وفي هذا الإطار يُطرح التساؤل حول مدى فاعليّة آليات وجهود مكافحة الجرائم المعلوماتيّة ذات البعد العالمي؟**إدراكا من الدول للمخاطر والتحدّيات الّتي تشكّلها الجرائم المعلوماتيّة، فقد تعدّدت الآليات وتنوّعت الجهود المبذولة وإختلفت أوجه وصور التعاون الدولي في مكافحتها وتمثّلت خاصّة في التعاون الأمني الدولي **(الفرع الأوّل)**، التعاون الإتّفاقي الدولي **(الفرع الثاني)** والتعاون القضائي الدولي **(الفرع الثالث)**.

الفرع الأوّل : التعاون الأمني الدولي في مجال مكافحة الجرائم المعلوماتية

ويُعرّف التعاون الأمني الدولي بأنه "تبادل العون والمساعدة وتضافر الجهود المشتركة بين طرفين دوليين أو أكثر لتحقيق نفع أو خدمة أو مصلحة مشتركة في مجال التصدي لمخاطر الإجرام، وما يرتبط به من مجالات أخرى، مثل مجال العدالة الجنائيّة، ومجالات الأمن، أو لتخطي مشكلات الحدود والسيادة التي قد تعترض الجهود الوطنيّة لملاحقة المجرمين وتعقب مصادر التهديد، سواء أكانت المساعدة المتبادلة قانونيّة أو قضائية أو شرطيّة، وسواء اقتصرت على دولتين فقط أو امتدت إقليمياً أو عالمياً."[٩١] وبذلك يشمل التعاون الأمني الدولي مجالات مختلفة، كالمجال الشرطي، والمجال القانوني، والمجال القضائي.[٩٢] وعلى صعيد التعاون الأمني بين الدول في مجال جرائم المعلوماتية نشير إلى جهود المنظّمة الدوليّة للشرطة الجنائيّة "الأنتربول" (INTERPOL: The International Criminal Police Organization) تهدف هذه المنظمة إلى تأكيد التعاون الأمني بين الدول الأطراف في المنظمة وعلى نحو فعال في مكافحة الجرائم المعلوماتية من حيث تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة وذلك عن طريق المكاتب المركزية الموجودة في الدول الأطراف في هذه المنظمة[٩٣]. إنّ جهود الشرطة الدولية على الرغم من أهميّتها ما زالت دون المستوى المطلوب، ويجب عليها حثّ الدول الأطراف في منظمة الشرطة الدولية على التعاون معها عن طريق عقد الإتفاقيات الثنائية بما يبرهن التعاون الدولي في مجال الجرائم المعلوماتية والمنظمة، وإنشاء قسم متخصص في الأنتربول مهمّته متابعة الجرائم والكشف عنها وملاحقة المجرمين وتبليغ الدول ذات العلاقة بالجرائم المعلوماتية بوقوع الجرائم على أراضيها، والتنسيق مع أقسام الجرائم المعلوماتية في الدول من أجل تبادل الخبرات والمعلومات في مثل هذا النوع من الجرائم المستحدثة. أمّا على المستوى العربي، وفي المجال الأمني، فقد تم إنشاء قسم متخصص تابع للمكتب العربي للشرطة الجنائية بقرار من مجلس وزراء الداخلية العرب، بحيث يهتم هذا القسم بمتابعة كل ما يتعلق بالجرائم المعلوماتية بالإطار العربي؛ لكنّه ما زال دون المستوى المطلوب لعدم وجود اتّفاقية دولية صادرة عن الأمم المتّحدة في مكافحة هذا النوع من الجرائم.

الفرع الثاني : التعاون الإتّفاقي الدولي في مجال مكافحة الجرائم المعلوماتية تعتبر الإتّفاقيات الدولية أهم وسيلة في مجال مكافحة الجرائم المعلوماتيّة حيث تعمل على توحيد الجهود الدولية في هذا المجال. وتعمل الأمم المتّحدة بإعتبارها مركز لتنسيق الجهود بين الدول على ذلك من خلال جملة من القرارات والتوصيات والإتّفاقيات الدولية ونذكر منها على سبيل المثال :

أوّلاً- قرار هافانا 1990 المنبثق عن مؤتمر الأمم المتّحدة الثامن لمنع الجريمة ومعاملة المجرمين، هافانا، كوبا، في 27 آب/أغسطس إلى 7 أيلول/سبتمبر 1990 حيث وضع إطار دولياً لمكافحة لجرائم الكمبيوتر وجاء في هذا القرار بما يلي :

- التأكيد على وضع إطار قانوني دولي ملائم ممّا يتطلب جهداً جماعياً بين الدول.
- الطلب من الدول الأعضاء القيام بالإجراءات التالية :

1- تحديث القوانين لمواكبة المرحلة خصوصاً في مجال التحقيق وقبول الأدلة والإجراءات القضائية.

2- تحسين تدابير الأمن والوقاية المتعلقة بالحاسوب مع مراعاة الخصوصية وحقوق الإنسان.

3- زيادة الوعي لدى الجماهير من خلال إبراز أهمية مكافحة جرائم ذات صلة بالحاسوب.

4- إعتماد تدابير خاصة لتدريب القضاة والضبطية القضائية لمواكبة متطلبات المرحلة.

5- زيادة التعاون بين المنظمات ذات العلاقة ووضع قواعد للأخلاق للتعامل بها.[٩٤]

ثانياً- المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات في البرازيل 1984 : تم في هذا المؤتمر توقيع جملة من الأسس الواجب إحترامها ومراعاتها في مكافحة الجرائم المتعلّقة بالكمبيوتر ومنها :

1- وجوب تحديد السلطات التي تقوم بالتفتيش والضبط في بيئة تكنولوجيا المعلومات.

2- السماح للسلطات العامّة بإعتراض الإتّصالات داخل نظام الحاسوب ذاته مع إستخدام الأدلة المحصل عليها أمام المحاكم.

3- يجب مراعاة المسائل المرتبطة ببنية المعلومات وما يمثله ضياع الفرص الاقتصادية وانتهاك الحرمة والحياة الخاصة وكذا كلفة إعادة بناء قاعدة تحقيق.

4- إعادة النظر في الإثبات الالكتروني ومصداقية الأدلة مع مراعاة القواعد التشريعية.[٩٥]

ثالثاً- إتّفاقيّة بودابست الصادرة عن المجلس الأوروبي بتاريخ 23 نوفمبر 2001 لمكافحة الجرائم المعلوماتية[٩٦] :

تتعلّق هذه الإتّفاقيّة بمعالجة كل ما يهم الجرائم المعلوماتية في الإطار الأوروبي وتتلخص أهدافها فيما يلي:

1- السعي لتوحيد التدابير التشريعية بين الدول للوقاية من هذه الجرائم.

2- التأكيد على أهميّة التعاون الإقليمي والدولي للوقاية من هذه الجرائم.

3- العمل على تحقيق التوازن بين حقوق الإنسان الأساسية وحرية الرأي وحرية الرأي وحرية الوصول للمعلومة وحرية البحث والحق في الخصوصية وغيرها من الحقوق الأساسية الثابتة في العلاقات الدولية.[٩٧]

رابعاً - القانون العربي النموذجي لمكافحة جرائم تقنية أنظمة المعلوماتية الذي صادق عليه مجلس وزراء العدل العرب في 2003/08/10م، في دورته التاسع عشر :نصّ هذا القانون على جملة من الأحكام الموضوعية والإجرائية تعمل على الحدّ من الجريمة المعلوماتية وقد جاء في المادة 26 منه ما يلي:" تسري أحكام هذا القانون على أي من الجرائم المنصوص عليها فيه ولو أُرتكبت كليّاً أو جزئيّاً خارج إقليم الدولة متى أضرت بإحدى مصالحها ويختص القضاء الوطني بنظر الدعاوى المترتبّة عليه." ومن خلال هذا النص نلاحظ أنّ القانون أخذ بمبدأ العينية بإعتماده على المصلحة الوطنية كمعيار أساسي لثبوت الاختصاص وبالتالي تطبيق القانون الجنائي الوطني. كما أنّ هذا القانون لم يعيّن أي جهة تتولى عملية الضبط القضائي في جرائم المعلوماتية ممّا يعني أنّه ترك المجال مفتوحا للدول العربية من خلال إعطاء تلك السلطة لأي هيئة أو جهة تراها قادرة على إكتشاف ومتابعة تلك الجرائم.[٩٨]

خامساً - أما في إطار الدول العربية هنالك اتّفاقيّة الرياض للتعاون القضائي والصادرة في 1993/04/06م، وقد تم توقيع الإتّفاقية في مدينة الرياض، وتُعدّ هذه الإتفاقية النواة الأولى للتعاون العربي في المجال القضائي، كذلك اتّفاقية الأمم المتّحدة لمكافحة الجريمة المنظمة عبر الوطنية والصادرة من الأمم المتّحدة لسنة 2000م، كذلك هنالك الإتّفاقية القضائية والقانونية الصادرة عن مجلس التعاون الخليجي في الفترة من 21-2003/12/22م، في الكويت حيث تم اعتماد هذه الاتفاقية من المجلس الأعلى لمجلس التعاون الخليجي في دورته الرابعة.

الفرع الثالث : التعاون القضائي الدولي في مجال مكافحة الجرائم المعلوماتية:

لمّا كانت الجرائم المعلوماتية عابرة للحدود وتتعدى آثارها عدّة دول، فإنّ ملاحقة مرتكبي هذه الجرائم وتقديمهم للمحاكمة وتوقيع العقاب عليهم يستلزم القيام بأعمال إجرائية خارج حدود الدولة حيث أُرتكبت الجريمة أو جزء منها، مثل معاينة موقع الإنترنت في الخارج، أو ضبط الأقراص الصلبة الّتي توجد عليها معلومات غير مشروعة أو صور إباحيّة، أو تفتيش الوحدات الطرفية في حالة الإتّصال عن بعد، أو القبض على المتّهمين، أو سماع الشهود، أو اللجوء إلى الإنابة القضائية، أو تقديم المعلومات التي يمكن أن تساعدهم في التحقيق في هذه الجرائم، كل ذلك لا يمكن تحقيقه بدون تعاون قضائي دولي[٩٩]. وتتجلى الجهود الدوليّة أساساً من خلال المساعدة القضائيّة الدوليّة **(أوّلا)** وتسليم المجرمين **(ثانيا)** كما يلي :

أوّلاً- المساعدة القضائيّة الدوليّة في المواد الجنائية:

تُعرّف المساعدة القضائية الدوليّة بأنّها "كل إجراء قضائي تقوم به دولة من شأنها تسهيل مهمّة المحاكمة في دولة أخرى بصدد جريمة من الجرائم"[١٠٠]. وتتمثّل المساعدة القضائية في التعاون في مكافحة الجرائم في المجال الجنائي من خلال الإتّفاقيات. وبالنظر لطبيعة

جرائم المعلوماتية ذات الطابع العالمي فإنّ الإجراءات الجنائية وأعمال التحقيق والكشف عن هذه الجرائم، لا تتحقّق إلا بالمساعدة القضائية في إطار التعاون الدولي. ولهذا فقد نصت أغلب الإتّفاقيات الدولية على ضرورة المساعدة القضائية وذلك من خلال :

1- تبادل المعلومات: ويقصد بتبادل المعلومات تقديم كل البيانات والوثائق التي تطلبها سلطة قضائية أجنبيّة بصدد متابعة جريمة ما والرد على الاتهامات التي وجهت إلى رعاياه في الخارج وتبيان الإجراءات التي اتخذت ضدهم. ومن مظاهر تبادل المعلومات ما يتعلق بالمساعدة في الكشف عن السوابق القضائية للجناة من خلال التعريف بالماضي الجنائي لهم، وهذا من شأنه تكوين فكرة على طريقة عمل والتخطيط للمجرم مما يساعد في القبض عليه أثناء التحقيق، أو التخفيف والتشديد في العقوبة عند محاكمته.[١٠١]

2- نقل الإجراءات: ويقصد بها قيام دولة بناء على إتّفاقية بإتّخاذ إجراءات جنائية بصدد جريمة أُرتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة وهذا إذا ما توافرت شروط معيّنة وهي التالية:

- أن يكون الفعل المنسوب إلى الشخص يُشكّل جريمة في الدولة الطالبة والدولة المطلوب منها.
- أن يكون الإجراء المطلوب اتّخاذ قرار في قانون الدولة المطلوب إليها عن ذات الجريمة.
- أن يكون الإجراء المطلوب اتّخاذه يؤدّي إلى الوصول للحقيقة كأن تكون أدلة للجريمة موجودة بالدولة المطلوب إليها.[١٠٢]

وعليه فإنّه يجب على الدول المعنية أن تتعاون فيما بينها حتى يمكنها معالجة جرائم المعلوماتيّة، ومن هذا المنطلق شدّدت مسودة الإتّفاقية الأوربية لجرائم المعلوماتية من خلال القانون الجنائي على ضرورة تدويل هذه الجرائم وخاصة تلك العابرة للحدود، وضرورة قيام الدول الأطراف بتبني قوانين جنائية وطنية في هذا المجال. كما أوصت الإتّفاقية على المستوى الدولي بضرورة قيام الدول بالتعاون فيما بينها من أجل التصدّي لهذه الجرائم على ضوء المبادئ التالية:

- تقديم المساعدة في التحقيق الجاري في أي دولة بالنسبة لهذه الجرائم المنصوص عليها في المادة ٠٤ من هذه الإتفاقية.

– الإلتزام بالتعاون مع سلطات التحقيق.

– تقديم المساعدة الفنية والتقنية اللازمة في التحقيق الجنائي.

– تسهيل الإجراءات الإدارية والتقنية من أجل حل مشاكل الإثبات في جرائم المعلوماتية.[١٠٣]

3- تبادل الإنابة القضائية الدولية[١٠٤] : يقصد بالإنابة القضائية طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية، تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها لضرورة ذلك الفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة، ويتعذر عليها القيام بها بنفسها، وأنّ تنفيذ طلب الإنابة غير ملزم للدول المنابة لأنّ أساسها اعتبارات المجاملة الدولية.[١٠٥] وهذا الإجراء من شأنه تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة، والتغلب على عقبة السيادة الإقليمية التي تمنع الدول الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى، مثل ما جرى به العمل من سماع الشاهد المقيم بالخارج عن طريق الإنابة القضائية.وما يلاحظ أنّه غالباً ما يتمّ استبعاد تنفيذ أحكام الإنابة القضائية في المجال السياسي والضريبي والعسكري، لأنّها مجالات من شأنها المساس بالسيادة والنظام العام والمصالح الأساسية للدول، غير أنّ هذا النظام يبقى معيب لإرتباطه بالطرق الدبلوماسية والتي تتّسم بالبطء وكثرة الشكليات والبرتوكولات وهو ما يتعارض وطبيعة جرائم المعلوماتيّة التي تتميّز بالسرعة والتغير وتأخر ظهور نتيجتها الإجرامية أحيانا، وهذا من شأنه ضياع أدلة وبيانات أو اختفاءها والتي قد تشكل دليل مهمّا لإدانة المتهم.

ثانياً- تسليم المجرمين[١٠٦]:ويُعرّف تسليم المجرمين بأنّه الإجراء الذي تسلم به دولة استناداً إلى معاهدة أو تأسيساً على المعاملة بالمثل عادة إلى دولة أخرى شخصاً تطلبه الدولة الأخيرة لإتّهامه، أو لأنّه محكوم عليه بعقوبة جنائية[١٠٧]. هذا النوع من التعاون الدولي هو نتيجة طبيعية للتحولات التي حدثت في كافّة المجالات ومنها مجال الإتّصالات وتقنية المعلومات، بحيث لم تعد الحدود القائمة بين الدول تشكل حاجزاً أمام مرتكبي الجرائم، فالمجرم المعلوماتي أصبح مجرماً دولياً، لأنّ نشاطه الإجرامي لم يعد قاصراً على دولة معيّنة أو أقاليم، لأن المجرم قد يخطط لجريمته في دولة وينفذها في دولة أخرى ويهرب إلى دولة أخرى للإبتعاد عن أيدي العدالة.[١٠٨] والهدف من التسليم هو ضمان عدم الإفلات من العقاب في حالة ما إذا كان القانون الداخلي للدولة المتواجد على إقليمها المتهم لا يسمح لتلك الدولة بمحاكمته عن جريمته، وبالتالي فإنّ تسلم المجرمين هو أحد مظاهر التعاون الدولي في مكافحة الجريمة.[١٠٩]ومن خلال كلّ ما تقدّم يمكن القول أنّه وعلى الرغم من أهميّة التعاون الدولي والآليات والجهود المبذولة في مكافحة الجرائم المعلوماتيّة، فهي تبقى منقوصة ودون المستوى المطلوب

سواء من حيث عقد الإتّفاقيات الثنائية والدولية أو القضائية ذات العلاقة بالجرائم المعلوماتية خاصّة أمام تزايد خطورة هذا النوع من الجرائم العابرة للحدود والتي يصعب إثباتها ويسهل ارتكابها.

الخاتمة:

تُعدّ الجرائم المعلوماتيّة من أخطر أنواع الجرائم حيث تمثّل إرهاباً إلكترونيّاً يهدّد الأمن، خاصة مع تطوّر الفضاء الإلكتروني التي أصبح له دور إستراتيجي في المجتمع الدولي على الصعيد الإقتصادي والسياسي والثقافي والأمني والإجتماعي. وتكمن خطورة الأعمال هذه الجرائم في إعتمادها على تقنيات متقدّمة مثل أجهزة التصنت على شبكات الإتّصال، وبرمجيات التشفير، وبرمجيات إختراق أنظمة أمن الشبكات والحاسبات، كما أن الشبكة الآلية الواحدة قد تضم عشرات أو مئات الآلاف أو ملايين الحواسب أو الأجهزة المتّصلة بالإنترنت والتي يمكن إستخدامها بصفة غير مشروعة لشن هجمات متنوّعة لأغراض إجرامية كالتخريب والسرقة والإرهاب والتهديد والإبتزاز. كما تكمن خطورة هذه الجرائم فيما تتميّز به من خصائص إستثنائيّة ومنفردة أضفت عليها لوناً وطابعاً قانونياً خاصاً وجعلها تشكّل تحدّياً كبيراً للقوانين والقضاء وجميع الجهود والآليات الوطنيّة والدوليّة لمكافحتها حيث ظلّت هذه الجهود رغم أهميّتها عاجزة عن التصدي لها والحدّ منها.ومن خلال ما تقدم توصلنا إلى جملة من النتائج والتوصيات والمقترحات كما يلي:

النتائج: تتمثل النتائج فيما يلي:

- أنّ الجرائم المعلوماتيّة ظاهرة إجرامية حديثة وليدة التطورات الهائلة في نظم تقنية المعلومات والإتّصالات وتُعدّ من أكبر السلبيات التي خلفتها الثورة المعلوماتية، لكونها تتمثّل في إعتداءات خطيرة على الأفراد والمؤسسات وأمن الدول، وهو ما يترك في النفوس شعوراً بعدم الثقة وإنعدام الأمن في التعامل والإستفادة من الثورة الرقميّة.
- أن الجرائم المعلوماتية تختلف عن الجرائم العادية من حيث أسلوب إرتكابها فهي جرائم ناعمة لا تحتاج مجهود بدني بل إلى الموهبة والمهارة الفنية والتقنية وكما تختلف من حيث شخص مرتكبها والوسيلة المستعملة في إرتكابها وهي من الجرائم الصعبة الاكتشاف والّتي تحتاج إلى خبراء مختصين في التحقيق فيها لأنّ المجرم لا يترك أثراً عند ارتكابها.
- أن الجرائم المعلوماتية كثيرة ومتشعبة وتتعدّد صور إرتكابها بين الإرهاب والمخدرات والإتّجار بالبشر إلى السب والقذف والقرصنة والجرائم المالية وإختراق المواقع ومنها ما يشكل جناية خطرة وتتدرج لتصل الى الجنح وهي جرائم يصعب حصرها.
- أنّ تنامي ظاهرة الجرائم المعلوماتية عبر الوطنية، وتخطي آثارها حدود الدول، أفرز جملة من التحدّيات القانونية على الصعيد الإجرائي تجسدت أساساً في بعض الصعوبات التي تكتنف إثبات هذه الجرائم وقبول الدليل بشأنها بإعتبارها لا تترك أثراً مادياً ملموساً.
- ورغم الجهود التي بُذِلت ولا تزال تُبذل، فإنّ هذه التحديات تبقى مستعصية على الحل في كثير من الأحيان في غياب إستراتيجية واضحة للتعامل مع هذه الطائفة من الجرائم ومرتكبيها لاسيما في الدول التي لم تبادر بعد إلى تعديل تشريعاتها بما يكفل تجاوز القوالب القانونية التقليدية التي لم تعد تناسب هذا العصر.

التوصيات والمقترحات:

في ختام هذه الدراسة، فإننا نورد بعض التوصيات قد يكون من المناسب العمل بها لمواجهة تهديدات الجرائم المعلوماتيّة المتزايدة. وتتمثّل فيما يلي:

- وجوب تعديل نظام مكافحة جرائم المعلوماتيّة ونظام الإجراءات الجزائية بما يتلاءم مع أنواع الجرائم المعلوماتيّة وخطورتها وطرق مكافحتها.
- إنشاء مركز دولي مقره الأمم المتحدة يسمى "المركز الدولي لمكافحة جرائم المعلوماتيّة"، لتنسيق الجهود في مجال مكافحة الجرائم المعلوماتية، وعقد المؤتمرات الدولية ذات العلاقة بالجرائم المعلوماتية وإعداد الإتّفاقيات الدولية أيضاً ذات الصلة بالموضوع.
- إبرام إتّفاقية دوليّة لتعزيز التعاون الدولي بجميع صوره لمواجهة التحديات الإجرائية الناجمة عن الجرائم المعلوماتية عبر الوطنية.
- إنشاء محاكم أو دوائر متخصّصة في الجرائم المعلوماتيّة في كل المجالس القضائية لمجابهة هذه الظاهرة.
- تعزيز التعاون والمساعدة الوطنية والدولية في مجال مكافحة جرائم الإنترنت.
- إعداد وتبني إستراتيجية موحدة من الأمانة العامّة لمجلس التعاون لدول الخليج العربيّة تنطلق من رؤيتها وأهدافها ومبادئها والخطط والبرامج التنفيذية لمواجهة الجرائم المعلوماتيّة.

- بناء القدرات في مجال تقنية المعلومات لرصد وتحليل التهديدات الأمنيّة المحتملة للجرائم المعلوماتيّة وآثارها والإنذار المبكر بإحتمالات وقوعها.
- بناء القدرات في مجال العدالة الجنائية (الشرطة والإدّعاء العام – القضاء) لتطوير التحقيقات الجنائية في مجال الجرائم المعلوماتيّة والأدلّة الرقمية وذلك بتوفير التدريب والتأهيل المناسب لرفع الكفاءة المهنية في هذا المجال الذي يواجه قصوراً نسبياً ملحوظاً.
- عقد اللقاءات في المدارس والجامعات، وحثّ دور العبادة والمؤسسات الدينية من أجل توعية المجتمع بمخاطر هذه الجرائم وأثرها على المجتمع، وعقد الورشات والمؤتمرات الوطنية في مجال مكافحة الجرائم المعلوماتية بهدف تبادل الخبرات والخروج بالتوصيات التي تساهم في حل المشكلات الناتجة عن هذه الجرائم وتشجيع البحث والتطوير في مجال الحماية من الجرائم المعلوماتيّة.
- إتّخاذ التدابير اللازمة لحماية البنيات التحتيّة الحساسة وتعزيز صمودها في وجه الإختراقات والهجمات الإلكترونية.
- التشجيع على التبليغ على هذه الجرائم بدل الصمت درءاً للفضيحة أو خوفاً من عدوانية المجرم.
- تحقيق تعاون دولي وتعزيز آليات المراقبة والمواجهة، مع فرض عقوبات زجرية في حق مرتكبي الجرائم المعلوماتيّة.

قـائمة المراجع

المراجع العربيّة:

١. إبراهيم بلبالي، الجريمة الإلكترونية بين وضوح معالم وأهداف التجريم وصعوبة التصنيف والتطبيق، دراسات وأبحاث، المجلّد الأوّل، العدد الأوّل، 2009، ص 133.

٢. إبراهيم رمضان إبراهيم عطايا، الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية (دراسة تحليلية تطبيقية)، مجلة كلية الشريعة والقانون بطنطا، العدد 30، الجزء الثاني، جامعة الأزهر، كلية الشريعة والقانون بطنطا، مصر، 2015، ص 360.

٣. أبو المعالي محمد عيسى، الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية، ورقة عمل مقدمة إلى المؤتمر المغاربي الأوّل حول المعلوماتية والقانون، بحث منشور على الرابط التالي: lefpedia.com

٤. أبو زيد، عبد الرحمان عاطف، الأمن السيبراني في الوطن العربي، المركز العربي للبحوث والدراسات، العدد 48، 2019.

٥. أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة، الطبعة 18، 2019.

٦. أحمد خليفة الملط، الجرائم المعلوماتية: دراسة مقارنة، دار الفكر الجامعي، القاهرة، الطبعة الثانية، 2006.

٧. أحمد خليفة الملط، الجرائم المعلوماتية، طبعة 2، دار الفكر الجامعي، الإسكندريّة، 2006.

٨. حمد عبد الحليم شاكر، دور الإنابة القضائية الدولية في مكافحة الجريمة، مجلة الفكر الشرطي، المجلد 17، العدد 4، 2008ص149.

٩. أحمد عبد الله الخشاشنة، تحريز الأدلّة الرقميّة وأثرها في كشف الجريمة، مجلّة الدراسات الأمنيّة، المجلّد الأوّل، العدد 16، الأردن، 2019، ص 1.

١٠. أسامة بن غانم العبيدي، الجهود الدوليّة في مكافحة الجرائم المعلوماتيّة، مجلّة الحقوق، العدد 4، 2015، ص 113.

١١. أمير فرج يوسف، الجرائم المعلوماتيّة على شبكة الإنترنت، الإسكندرية، دار المطبوعات الجامعيّة، 2010.

١٢. أيوب محمود عمار الرواشدة، التنظيم القانوني للتوقيع الإلكتروني: في ضوء قانون المعاملات الإلكترونية الأردني رقم 15 لسنة 2015: دراسة مقارنة، مجلة العلوم القانونية والسياسية، المجلّد 6، العدد 2، العراق، 2016، ص 167.

١٣. بدرة هويمل الزبن، الإرهاب في الفضاء الإلكتروني: دراسة مقارنة، رسالة دكتوراه منشورة، جامعة عمان العربية، كلية القانون، الأردن، 2012.

١٤. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأوّل: الجرائم الناشئة عن إستخدام الحاسب الآلي، دار النهضة العربية للنشر والتوزيع، القاهرة، 1992.

١٥. حاتم أحمد محمد بطيخ، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات (دراسة تحليلية مقارنة)، مجلّة الدراسات القانونيّة والإقتصاديّة، المجلد 7، العدد 1، أغسطس 2021، ص1.

١٦. خالد بن مبارك القريوي القحطاني، التعاون الأمني الدولي في مواجهة الجريمة المنظمة عبر الوطنية، رسالة دكتوراه، كلية الدراسات العليا، جامعة نايف العربيّة للعلوم الأمنيّة، الرياض، 2006.

١٧. خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتيّة، دار الفكر الجامعي، مصر، 2019.

١٨. خالد سليمان الحمادي، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري – دراسة مقارنة، رسالة ماجستير، جامعة قطر، 2019.

١٩. خالد عياد الحلبي، إجراءات التحقيق والتحري في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، الأردن، 2011.

٢٠. خالد ممدوح إبراهيم، حوكمة الإنترنت، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، 2011.

٢١. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، مصر، 2009.

٢٢. خليل يوسف جندي، المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني (دراسة مقارنة)، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد 07، العدد 26، 2018، ص 80.

٢٣. رستم هشام، أصول التحقيق الجنائي الفنّي، مجلّة الأمن والقانون أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين، أكاديميّة شرطة دبي، الإمارات العربيّة المتّحدة، العدد الثاني، 1999، ص 74.

٢٤. سالم محمد سليمان الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوطنية، رسالة دكتوراه، الدار الجماهيرية للنشر والتوزيع والإعلام، طرابلس، ليبيا، 2000.

٢٥. سامح أحمد موسى، الجوانب الإجرائية للحماية القضائية لشبكة الإنترنت، رسالة دكتوراه، جامعة الإسكندرية، 2010.

٢٦. سامي علي حامد عياد، الجرائم المعلوماتيّة وإجرام الإنترنت، مصر، دار الفكر العربي 2007.

٢٧. سفيان سويد، الجرائم المعلوماتية، رسالة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان الجزائر، 2010.

٢٨. شمس الدين إبراهيم محمد، وسائل مواجهة الإعتداءات على الحياة الشخصيّة في مجال تقنية المعلومات في القانون السوداني والمصري ـ دراسة مقارنة ـ دار النهضة العربية،، الطبعة الأولى، ،القاهرة، 2005.

٢٩. شيخة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، المجلّد 17، العدد1 ، جامعة الشارقة، الإمارات، 2020، ص 740.

٣٠. طارق أحمد صالح الخطيبي الفلاسي، أحكام تسليم المجرمين في قانون التعاون القضائي الدولي في المسائل الجنائية في ضوء الإتّفاقيات الدولية، رسالة ماجستير في القانون العام، أكاديمية شرطة دبي، كلية الدراسات العليا، 2015.

٣١. عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2015.

٣٢. عباس أبو شامة، التعريف بالظواهر الإجراميّة المستحدثة، حجمها، أبعادها، ونشاطها في الدول العربيّة، أكاديميّة نايف العربيّة للعلوم الأمنيّة، ندوة علميّة عقدت في تونس من 28 –1999/06/30.

٣٣. عبد الحميد محسن أحمد، مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المذنبين هافانا، كوبا 27 أغسطس – 7 سبتمبر 1990م، المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، المجلد 6، العدد 11، السعودية، 1991، ص131.

٣٤. عبد الرحمن عاطف أبو زيد، الأمن السيبراني في الوطن العربي، دراسة حالة المملكة العربية السعودية، المركز العربي للبحوث والدراسات، 2019/09/25، ص 55.

٣٥. عبد العزيز بن غرم الله بن جار الله الغامدي، جرائم الإنترنت وعقوباتها وفق نظام مكافحة الجرائم المعلوماتية السعودي: دراسة مقارنة، دار الكتاب الجامعي للنشر والتوزيع، 2017.

٣٦. عبد العزيز سالم السنيدي، السياسة العقابية للمشرّع الإماراتي في مواجهة الجرائم المعلوماتيّة في ظل المرسوم الإتّحادي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، رسالة ماجستير في القانون العام، Public Law Theses 7، 2018، ص 16 وما بعدها، متاح على الرابط: https://scholarworks.uaeu.ac.ae/public_law_theses

٣٧. عبد الفتّاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، دار الكتب القانونيّة، القاهرة، مصر، 2007.

٣٨. حسين سعيد الغافري، السياسة الجنائيّة في مواجهة جرائم الإنترنت (دراسة مقارنة)، دار النهضة العربيّة، القاهرة، مصر، 2009.

٣٩. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي، دار الكتب العربية، الطبعة الأولى، مصر،2007.

٤٠. عبد الفتاح محمد سراج، النظرية العامة لتسليم المجرمين، دار النهضة العربية للنشر والتوزيع، الطبعة الأولى، 1998.

٤١. عبد القدوس بوعزة، أيوب مخرمش، أساليب التعاون الدولي في القضاء على الجرائم الإلكترونية، المجلة الجزائرية للعلوم السياسية والعلاقات الدولية، المجلد 13، العدد 18، الجزائر، 2022، ص 155.

٤٢. عبد الله العلوي البليغثي، الإجرام المعاصر أسبابه وأساليب مواجهته، السياسة الجنائية بالمغرب واقع وآفاق، المجلّد الأوّل، (الأعمال التحضيرية)، منشورات جمعيّة نشر المعلومة القانونية والقضائية، سلسلة الندوات والأيام الدراسية، الطبعة الثانية، العدد 3، 2004، ص 222.

٤٣. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلّف والمصنّفات الفنيّة ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقيّة، بيروت، 2003.

٤٤. عكاشة محمد عبد العال، الإنابة القضائيّة في نطاق العلاقات الخاصّة، دراسة تحليليّة مقارنة في القانون المصري والقانون المقارن، دار المطبوعات الجامعيّة، الإسكندريّة، 1994.

٤٥. علي ثامر النويران، **الجرائم الإلكترونيّة وطرق الحد منها: تجربة الأردن، المؤتمر الدولي لمكافحة الجرائم المعلوماتيّة ICACC، جامعة الإمام محمد بن سعود الإسلاميّة – كليّة علوم الحاسب والمعلومات**، الأردن، 2015، ص174.

٤٦. علي جبار الحسيناوي، جرائم الحاسوب والإنترنت، دار اليازوري للنشر والتوزيع، الطبعة الأولى، عمان، الأردن، 2009.

٤٧. عمر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية للنشر والتوزيع، الطبعة الأولى، القاهرة، مصر، 2004.

٤٨. فادية حافظ جاسم، التعاون الدولي للحدّ من الجريمة المعلوماتيّة، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة النهرين، المجلّد 21، العدد 4، 2019، ص 377.

٤٩. فريد ناشف، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلّة البحوث في الحقوق والعلوم السياسيّة، المجلد 08، العدد الأوّل، 2022، ص 430.

٥٠. فؤاد الصلاحي، الأمن السيبراني، مجلّة الدوحة، وزارة الإعلام، 2015، ص 52.

٥١. كاظم عبد جاسم الزيدي، دراسة حول أهمية مكافحة الجرائم المعلوماتية وفقاً التشريع العراقي مكافحة الجرائم المعلوماتية في التشريع العراقي، استشارات قانونية مجانية، محاماة نت، 2017.

٥٢. لورنس سعيد الحوامدة، الجرائم المعلوماتيّة أركانها وآلية مكافحتها دراسة تحليلية مقارنة، مجلّة الميزان للدراسات الإسلامية والقانونية، المجلد 4، العدد الأوّل، 2017، ص 183.

٥٣. محروس نصار غايب، الجريمة المعلوماتيّة، مجلّة هيئة التعليم التقني الأكاديميّة، المجلد 24، 2011، ص1.

٥٤. محمد الصغير مسيكة، مفهوم الجرائم المستحدثة وطبيعتها القانونية (الجرائم الإلكترونية)، مجلّة الدراسات القانونية والسياسية، المجلد 08، العدد الأوّل، 2022، ص 132.

٥٥. محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2004.

٥٦. محمد بن أحمد بن علي المقصودي، الأمن السيبراني والجهود الدولية لمكافحة الجرائم عابرة القارات، جامعة نايف العربية للعلوم الأمنية، المجلّد 37، العدد 427، السعودية، 2017، ص102.

٥٧. محمد حجازي، جرائم الحاسبات والإنترنت (الجرائم المعلوماتيّة)، المركز المصري للملكيّة الفكريّة، القاهرة، 2005.

٥٨. محمد حماد مرهج الهيتي، الجريمة المعلوماتية نماذج من تطبيقها دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني، دار الكتب القانونيّة، مصر، 2014.

٥٩. محمد حماد مرهج الهيتي، جرائم الحاسوب ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها، دار المناهج للنشر والتوزيع، عمان، الأردن، الطبعة الأولى، 2006.

٦٠. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية للنشر والتوزيع، الطبعة الثانية، القاهرة، 1998.

٦١. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية للنشر والتوزيع، الطبعة الثانية، القاهرة، 1994.

٦٢. محمد عبد الله أبو بكر سلامة، موسوعة جرائم المعلوماتية ـ جرائم الكمبيوتر والإنترنت، منشأة المعارف، الاسكندرية، مصر، 2006.

٦٣. محمد محى الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، مصر، 1993.

٦٤. محمود علي عبد السلام وافي، الإنابة القضائيّة: دراسة مقارنة بين القانون المصري والنظام السعودي، مجلة العلوم القانونية والإقتصادية، المجلّد 58، العدد 02، 2016، ص 153.

٦٥. محمود عمر محمود، الجرائم المعلوماتية والإلكترونية: دراسة مقارنة بين الشريعة الإسلامية والقانون الوضعي، خوارزم العلمية للنشر والتوزيع، الطبعة الأولى، 2015.

٦٦. محمود مدين، فنّ التحقيق والإثبات في الجرائم الإلكترونية، المصرية للنشر والتوزيع، الطبعة الأولى، مصر، 2020.

٦٧. مخلد إبراهيم الزعبي، فاعلية القوانين والتشريعات العربية في مكافحة الجرائم الإلكترونية – دراسة مقارنة، المجلّة العربيّة للنشر العلمي، العدد 37، 2021، ص 275.

٦٨. مريم عبد اللطيف المسلماني، مظاهر التعاون الدولي لدولة قطر في مجال مكافحة الجرائم الإلكترونية، مجلّة القانون والمجتمع، المجلّد 10، العدد 2، 2022، ص14.

٦٩. مصطفي عبد الغفار، تطور آليات التعاون القضائي الدولي في المواد على ضوء الآليات الحديثة الجنائية في مجال القبض على الهاربين وإعادتهم لمكافحة الجريمة، مجلّة معهد الدراسات القضائية والقانونية، وزارة العدل، مملكة البحرين، العدد الأول، 2008، ص 1.

٧٠. مطهر جبران غالب المصري، التعاون الدولي في مكافحة الجريمة المنظمة، رسالة ماجيستر، حقوق أسيوط، مصر، 2008.

٧١. معهد دبي القضائي، قانون مكافحة الشائعات والجرائم الإلكترونية لدولة الإمارات العربية المتحدة مرسوم بقانون اتحادي رقم 34 لسنة 2021 التشريعات والقوانين لدولة الإمارات العربية المتحدة 16، معهد دبي القضائي، الطبعة الأولى، دبي، 2022.

٧٢. منير محمد الجنبيهي وممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، مصر، 2006.

٧٣. موسى مسعود ارحومة، السياسة الجنائيّة في مواجهة جرائم الإنترنت Cyber Crimes، مجلة دراسات قانونية (منشورات جامعة قاريونس)، العدد 17، 2008، ص 80.

٧٤. نائلة عادل محمد فريد قورة، جرائم الحاسب الإقتصادية ـ دراسة نظرية وتطبيقيّة ـ دار النهضة العربية، القاهرة، مصر، 2004.

٧٥. نائلة عادل محمد فريد قورة، الجرائم المعلوماتيّة على شبكة الإنترنت، لبنان، منشورات الحلبي الحقوقية، لبنان، 2005.

٧٦. نرمين سليمان، أثر الجرائم الإلكترونية على الأبعاد الداخلية للأمن القومي: دراسة حالة المملكة العربية السعودية خلال الفترة من 2006 إلى 2016، رسالة دكتوراه في العلوم السياسية، جامعة القاهرة، كلية الإقتصاد والعلوم السياسية، مصر، 2018.

٧٧. نظام توفيق المجالي، شرح قانون العقوبات– القسم العام– دراسة تحليلية في النظرية العامة للجريمة والمسؤولية الجزائية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005.

٧٨. هشام عبد العزيز مبارك، تسليم المجرمين بين الواقع والقانون، دار النهضة العربية، مصر، الطبعة الأولى، 2006.

٧٩. هلالي عبد اللاه أحمد، جرائم الحاسب والإنترنت بين التجريم الجنائي وآليات المواجهة، مجموعة محاضرات ألقيت على طلاب كليّة الحاسبات والمعلومات، دار النهضة العربية للنشر والتوزيع، القاهرة، 2016.

٨٠. وسيلة بوحية، صعوبات التحقيق وإثبات الجرائم المعلوماتية قانونا وقضاء وأساليب مواجهتها مع عرض وتقدير تجارب بعض الدول العربية والأجنبية، جامعة الإمام محمد بن سعود الإسلاميّة، المؤتمر الدولي الأوّل لمكافحة الجرائم المعلوماتيّة ICACC، كليّة علوم الحاسب والمعلومات، بحوث مؤتمرات، الرياض المملكة العربيّة السعوديّة، 2015، ص 114.

٨١. ياسمين أحمد صالح، الإرهاب الإلكتروني في ظل أزمة فيروس كورونا: الأنماط ... التداعيات، مجلة كلية السياسة والإقتصاد العدد التاسع، يناير 2021، ص 55.

٨٢. يوسف حسن يوسف، الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، الطبعة الأولى، مصر، 2011.
٨٣. يوسف صغير، الجريمة المرتكبة عبر الإنترنت، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسيّة، جامعة مولود معمري تيزي وزو، 2013.

الأنظمة والإتفاقيات:

١. نظام مكافحة جرائم المعلوماتية " الصادر وفقا لقرار مجلس الوزراء رقم (79) وتاريخ 1428/03/07هـ والمصادق عليه بالمرسوم الملكي رقم م/17 وتاريخ 1428/03/08هـ والمنشور في جريدة أم القرى، العدد رقم (4144) بتاريخ 1428/03/25 الموافق لـ 2007/04/13م. متاح على:
https://www.citc.gov.sa/ar/RulesandSystems/CITCSystem/Documents/LA-004-A-Anti-CyberCrime Law.pdf
٢. قانون جرائم أنظمة المعلومات لسنة 2010 المنشور على الصفحة 5334 من عدد الجريدة الرسميّة 5056 بتاريخ 2010/09/16.
٣. الإتّفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 المبرمة بالقاهرة بتاريخ 21 ديسمبر 2010، على الرابط التالي:
http://www.moj.gov.jo/EchoBusV3.0/SystemAssets/27adcb7a-5539-4b36-9d9a-28b91f578bac.pdf
٤. إستراتيجيّة الهيئة الوطنيّة للأمن السيبراني متاحة على:
https://nca.gov.sa/national_cybersecurity_strategy-ar.pdf

المراجع الأجنبيّة:

1. BUZUBAR Mohammed, “La Criminalité informatique sur l’internet”, Journal of Law, Kuwait University, N°1, Vol.26, March 2002, p. 21 et s.
2. Gabriel Weimann, " Terror on the Internet: The New Arena, the New Challenges", (Washington: United States Institute of Peace Press, 2006).
3. Manoharan, N. (2012). Abu Jundal’s Arrest and India-Saudi Arabia Counter-terrorism Cooperation. Vivekananda International Foundation. July, 6. Available at: https://www.vifindia.org/article/2012/july/06/abu-jundal-s-arrest-and-india-saudi-arabia-counter-terrorism-cooperation
4. Melissa Hathaway, Francesca Spidalieri, and Fahad Alsowailm, Kingdom of Saudi Arabia Cyber Readiness at a Glance, Potomac Institute for Policy Studies.

هوامش البحث

١) أُنظر : – جميل عبدالباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأوّل : الجرائم الناشئة عن إستخدام الحاسب الآلي، دار النهضة العربية للنشر والتوزيع، القاهرة، 1992، ص 4 . 5 ؛ محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الثانية، دار النهضة العربية للنشر والتوزيع، القاهرة، 1998، ص 3؛ عبدالله العلوي البلغيثي، الإجرام المعاصر أسبابه وأساليب مواجهته، السياسة الجنائية بالمغرب واقع وآفاق، المجلّد الأوّل، (الأعمال التحضيرية)، منشورات جمعيّة نشر المعلومة القانونية والقضائية، سلسلة الندوات والأيام الدراسية، الطبعة الثانية، العدد 3، 2004، ص222.
BUZUBAR Mohammed, “La Criminalité informatique sur l’internet”, Journal of Law, Kuwait University, N°1, Vol.26, March 2002, p. 21 et s.
٢) موسى مسعود ارحومة، السياسة الجنائيّة في مواجهة جرائم الإنترنت Cyber Crimes، مجلة دراسات قانونية (منشورات جامعة قاريونس)، العدد 17 ، 2008، ص. 80.
٣) أُنظر : محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2004، ص7 ؛ عمر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية للنشر والتوزيع، الطبعة الأولى، القاهرة، 2004؛ نائلة عادل محمد فريد، الجرائم المعلوماتية على شبكة الانترنت، لبنان، منشورات الحلبي الحقوقية، 2005 ؛ علي جبار الحسيناوي، جرائم الحاسوب والإنترنت، الطبعة الأولى، دار اليازوري العلمية للنشر والتوزيع، عمان، 2009 ؛ محمود عمر محمود، الجرائم المعلوماتية والإلكترونية : دراسة مقارنة بين الشريعة الإسلامية والقانون الوضعي، خوارزم العلمية للنشر والتوزيع، الطبعة الأولى، 2015 ؛ عبد العزيز بن غرم الله بن جار الله الغامدي، جرائم الإنترنت وعقوباتها وفق نظام مكافحة الجرائم المعلوماتية السعودي: دراسة مقارنة، دار الكتاب الجامعي للنشر والتوزيع، 2017.

[٤]) بدرة هويمل الزبن، الإرهاب في الفضاء الإلكتروني: دراسة مقارنة، رسالة دكتوراه منشورة، جامعة عمان العربية، كلية القانون، الأردن، 2012.

[٥]) نرمين سليمان، أثر الجرائم الإلكترونية على الأبعاد الداخلية للأمن القومي: دراسة حالة المملكة العربية السعودية خلال الفترة من 2006 إلى 2016، رسالة دكتوراه في العلوم السياسية، جامعة القاهرة، كلية الإقتصاد والعلوم السياسيّة، 2018، ص 27.

[٦]) محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية للنشر والتوزيع، الطبعة الثانية، القاهرة، 1994، ص7.

[٧]) أحمد خليفة الملط، الجرائم المعلوماتية: دراسة مقارنة، دار الفكر الجامعي، القاهرة، الطبعة الثانية، 2006، ص 87.

[٨]) عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلّف والمصنّفات الفنيّة ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقيّة، بيروت، 2003، ص 32.

[٩]) عكاشة محمد عبد العال، الإنابة القضائيّة في نطاق العلاقات الخاصّة، دراسة تحليليّة مقارنة في القانون المصري والقانون المقارن، دار المطبوعات الجامعيّة، الإسكندريّة، 1994، ص 7.

[١٠]) محمد حماد مرهج الهيتي، الجريمة المعلوماتية نماذج من تطبيقها دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني، دار الكتب القانونيّة، مصر، 2014، ص 24.

[١١]) محمد حجازي، جرائم الحاسبات والإنترنت (الجرائم المعلوماتيّة)، المركز المصري للملكيّة الفكريّة، القاهرة، 2005، ص 8.

[١٢]) هلالي عبد اللاه أحمد، جرائم الحاسب والإنترنت بين التجريم الجنائي وآليات المواجهة، مجموعة محاضرات ألقيت على طلاب كليّة الحاسبات والمعلومات، دار النهضة العربية للنشر والتوزيع، القاهرة، 2016.

[١٣]) عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلّف والمصنّفات الفنيّة ودور الشرطة والقانون، دراسة مقارنة، المرجع السابق، ص32.

[١٤]) علي جبار الحسيني، جرائم الحاسوب والإنترنت، دار اليازوري للنشر والتوزيع، الطبعة الأولى، عمان، الأردن، 2009، ص33.

[١٥]) خالد ممدوح إبراهيم، حوكمة الإنترنت، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، مصر، 2011، ص357-358.

[١٦]) منير محمد الجنبيهي وممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2006، ص13.

[١٧]) خالد عياد الحلبي، إجراءات التحقيق والتحري في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، الأردن، 2011، ص31.

[١٨]) يوسف حسن يوسف، الجرائم الدولية للإنترنت، مصر، المركز القومي للإصدارات القانونية، الطبعة الأولى، مصر، 2011، ص13.

[١٩]) نائلة عادل محمد فريد، الجرائم المعلوماتيّة على شبكة الإنترنت، منشورات الحلبي الحقوقية، لبنان، 2005، ص 28 وما بعدها.

[٢٠]) عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي، دار الكتب العربية، الطبعة الأولى، مصر،2007، ص24.

[٢١]) سامي علي حامد عياد، الجرائم المعلوماتيّة وإجرام الإنترنت، دار الفكر العربي، مصر، 2007، ص27.

[٢٢]) أمير فرج يوسف، الجرائم المعلوماتيّة على شبكة الإنترنت، دار المطبوعات الجامعيّة، الإسكندرية، 2010، ص 104 وما بعدها.

[٢٣]) يوسف صغير، الجريمة المرتكبة عبر الإنترنت، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسيّة، جامعة مولود معمري تيزي وزو، 2013، ص 18.

[٢٤]) نظام مكافحة جرائم المعلوماتية " الصادر وفقا لقرار مجلس الوزراء رقم (79) وتاريخ 1428/03/07هـ والمصادق عليه بالمرسوم الملكي رقم م/17 وتاريخ 1428/03/08هـ والمنشور في جريدة أم القرى، العدد رقم (4144) بتاريخ 1428/03/25 الموافق لـ 2007/04/13م.

[٢٥]) المادّة الأولى من قانون مكافحة الجرائم الإلكترونية القطري الصادر بالقانون رقم 14 لسنة 2014 المتعلّق بإصدار قانون مكافحة الجرائم الإلكترونية.

[٢٦]) فريد ناشف، آليات التعاون الدولي في مكافحة الجرائم الإلكترونيّة، مجلّة البحوث في الحقوق والعلوم السياسيّة، المجلّد 8، العدد 1، 2022، ص 432.

[٢٧]) عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، المرجع السابق، ص 5.

[٢٨]) لورنس سعيد الحوامدة، الجرائم المعلوماتيّة أركانها وآلية مكافحتها دراسة تحليلية مقارنة، مجلّة الميزان للدراسات الإسلامية والقانونية، المجلد 4، العدد الأوّل، 2017، ص 189 وما بعدها. أُنظر أيضا أمير فرج يوسف، المرجع السابق، ص 104 وما بعدها.

[٢٩]) إبراهيم بلبالي، الجريمة الإلكترونية بين وضوح معالم وأهداف التجريم وصعوبة التصنيف والتطبيق، دراسات وأبحاث، المجلّد الأوّل، العدد الأوّل، 2009، ص 134.

[٣٠]) أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة، الطبعة 18، 2019، ص 27.

[٣١]) أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، طبعة 2، الإسكندريّة، 2006، ص 78.

[٣٢]) نفس المرجع ص 10.

[٣٣]) نظام توفيق المجالي، شرح قانون العقوبات– القسم العام– دراسة تحليلية في النظرية العامة للجريمة والمسؤولية الجزائية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005، ص122–142.

[٣٤]) المادّة الأولى من نظام مكافحة جرائم المعلوماتية " السعودي الصادر وفقا لقرار مجلس الوزراء رقم (79) وتاريخ 1428/03/07هـ والمصادق عليه بالمرسوم الملكي رقم م/17 وتاريخ 1428/03/08هـ.

[٣٥]) مخلد إبراهيم الزعبي، فاعلية القوانين والتشريعات العربية في مكافحة الجرائم الإلكترونية – دراسة مقارنة، المجلّة العربيّة للنشر العلمي، العدد 37، 2021، ص 282.

[٣٦]) خالد سليمان الحمادي، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري – دراسة مقارنة، رسالة ماجستير، جامعة قطر، 2019، ص24.

[٣٧]) مخلد إبراهيم الزعبي، المرجع السابق، ص 283.

[٣٨]) لورنس سعيد الحوامدة، المرجع السابق، ص 197 وما بعدها.

[٣٩]) خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي الإسكندرية، الطبعة الأولى، مصر، 2009، ص 53.

[٤٠]) خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتيّة، دار الفكر الجامعي، مصر، 2019، ص 51. أُنظر أيضا محمود مدين، فنّ التحقيق والإثبات في الجرائم الإلكترونية، المصرية للنشر والتوزيع، الطبعة الأولى، مصر، 2020، ص58.

[٤١]) خالد حسن أحمد لطفي، المرجع السابق، ص 52.

[٤٢]) تُعرف المعلومات بأنّها مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح أن تكون محلاً للتبادل والإتّصال أو التفسير والتأويل أو المعالجة بواسطة الأفراد أو الأنظمة الإلكترونيّة وهي تتميّز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها ونقلها بوسائل وأشكال مختلفة – نائلة عادل محمد فريد قورة، جرائم الحاسب الإقتصادية ـ دراسة نظرية وتطبيقيّة ـ دار النهضة العربية، القاهرة، مصر، 2004، ص 93. كما تُعرف بأنّها النقل المجرّد لوقائع معيّنة تم الحصول عليها من مصادر متعدّدة ـ أو هي بيان معقول أو رأي أو حقيقة أو مفهوم أو فكرة أو تجميعاً مترابطاً للبيانات والآراء والأفكار– شمس الدين إبراهيم محمد، وسائل مواجهة الإعتداءات على الحياة الشخصيّة في مجال تقنية المعلومات في القانون السوداني والمصري ـ دراسة مقارنة ـ دار النهضة العربية، الطبعة الأولى، القاهرة، 2005، ص 51 وما بعدها.

[٤٣]) محمد الصغير مسيكة، مفهوم الجرائم المستحدثة وطبيعتها القانونية (الجرائم الإلكترونية)، مجلّة الدراسات القانونية والسياسية، المجلد 08، العدد الأوّل، 2022، ص 138.

[٤٤]) عباس أبو شامة، التعريف بالظواهر الإجراميّة المستحدثة، حجمها، أبعادها، ونشاطها في الدول العربيّة، أكاديميّة نايف العربيّة للعلوم الأمنيّة، ندوة علميّة عقدت في تونس من 28 –1999/06/30، ص 110.

[٤٥]) محمد عبد الله أبو بكر سلامة، موسوعة جرائم المعلوماتية ـ جرائم الكمبيوتر والإنترنت، منشأة المعارف، الاسكندرية، مصر، 2006، ص97.

[٤٦]) رستم هشام، أصول التحقيق الجنائي الفنّي، مجلّة الأمن والقانون أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين، أكاديميّة شرطة دبي، الإمارات العربيّة المتّحدة، العدد الثاني، 1999، ص11.

[٤٧]) رستم هشام، المرجع السابق، ص 40.

[٤٨]) شمس الدين إبراهيم أحمد، المرجع السابق، ص 104.

[٤٩]) محمد الصغير مسيكة، المرجع السابق، ص 139 وما بعدها.

[٥٠]) إبراهيم رمضان إبراهيم عطايا، الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية (دراسة تحليلية تطبيقية)، مجلة كلية الشريعة والقانون بطنطا، العدد 30، الجزء الثاني، جامعة الأزهر، كلية الشريعة والقانون بطنطا، مصر، 2015، ص 374 وما بعدها.

[٥١]) فريد ناشف، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلّة البحوث في الحقوق والعلوم السياسيّة، المجلد 08، العدد الأوّل، 2022، ص 436.

[٥٢]) سويد سفيان، الجرائم المعلوماتية، رسالة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان الجزائر، 2010، ص 12.

[٥٣]) خليل يوسف جندي، المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني (دراسة مقارنة)، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد 07، العدد 26، 2018، ص90 .

[٥٤]) خليل يوسف جندي، المرجع السابق، ص90 .

[٥٥]) محمد الصغير مسيكة، المرجع السابق، ص 138 وما بعدها.

[٥٦]) شمس الدين إبراهيم محمد، وسائل مواجهة الإعتداءات على الحياة الشخصيّة في مجال تقنية المعلومات في القانون السوداني والمصري - دراسة مقارنة، المرجع السابق، ص 104.

[٥٧]) وسيلة بوحية، صعوبات التحقيق وإثبات الجرائم المعلوماتية قانونا وقضاء وأساليب مواجهتها مع عرض وتقدير تجارب بعض الدول العربية والأجنبية، جامعة الإمام محمد بن سعود الإسلاميّة، المؤتمر الدولي الأوّل لمكافحة الجرائم المعلوماتيّة ICACC، كليّة علوم الحاسب والمعلومات، بحوث مؤتمرات، الرياض المملكة العربيّة السعوديّة، 2015، ص 118.

[٥٨]) محمد حماد مرهج الهيتي، جرائم الحاسوب ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها، دار المناهج للنشر والتوزيع، الطبعة الأولى، عمان، الأردن، 2006، ص 238.

[٥٩]) المرجع نفسه، ص 117.

[٦٠]) محمد محى الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)، ورقة عمل مقدمة الى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، مصر، 1993، ص6.

[٦١]) أسامة بن غانم العبيدي، الجهود الدوليّة في مكافحة الجرائم المعلوماتيّة، مجلّة الحقوق، العدد 4، 2015، ص 119.

[٦٢]) عبد الفتّاح بيومي حجازي، الإثبات الجنائي في جرائم الكومبيوتر والإنترنت، دار الكتب القانونيّة، القاهرة، مصر، 2007، ص 177 وما بعدها. أُنظر أيضا حسين سعيد الغافري، السياسة الجنائيّة في مواجهة جرائم الإنترنت (دراسة مقارنة)، دار النهضة العربيّة، القاهرة، مصر، 2009، ص 690 وما بعدها.

[٦٣] Gabriel Weimann, " Terror on the Internet: The New Arena, the New Challenges", (Washington: United States Institute of Peace Press, 2006).

[٦٤]) أبو المعالي محمد عيسى، الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية، ورقة عمل مقدمة إلى المؤتمر المغاربي الأوّل حول المعلوماتية والقانون، بحث منشور على الرابط التالي: lefpedia.co

[٦٥]) مطهر جبران غالب المصري، التعاون الدولي في مكافحة الجريمة المنظمة، رسالة ماجيستر، حقوق أسيوط، مصر، 2008، ص 84.

[٦٦]) نرمين سليمان، أثر الجرائم الإلكترونية على الأبعاد الداخلية للأمن القومي: دراسة حالة المملكة العربية السعودية خلال الفترة من 2006 إلى 2016، رسالة دكتوراه في العلوم السياسية، جامعة القاهرة، كلية الإقتصاد والعلوم السياسية، مصر، 2018، ص 27.

[٦٧]) أبو زيد، عبد الرحمان عاطف، الأمن السيبراني في الوطن العربي، المركز العربي للبحوث والدراسات، العدد 48، 2019، ص 56.

[٦٨]) نظام مكافحة الجرائم المعلوماتية رقم بمقتضى المرسوم الملكي رقم م/17 في 1428/03/08هـ والمنشور في جريدة أم القرى، العدد رقم (4144) بتاريخ 1428/03/25هـ الموافق 2007/04/13م متاح على:

https://www.citc.gov.sa/ar/RulesandSystems/CITCSystem/Documents/LA_004_A_Anti-CyberCrime Law.pdf

[٦٩]) الإتّفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 المبرمة بالقاهرة بتاريخ 21 ديسمبر 2010، على الرابط التالي:

http://www.moj.gov.jo/EchoBusV3.0/SystemAssets/27adcb7a-5539-4b36-9d9a-28b91f578bac.pdf

٧٠) لورنس سعيد الحوامدة، الجرائم المعلوماتية، مرجع سابق، ص 211.

[٧١]) نرمين سليمان، المرجع السابق، ص 207.

[٧٢]) Melissa Hathaway, Francesca Spidalieri, and Fahad Alsowailm, Kingdom of Saudi Arabia Cyber Readiness at a Glance, Potomac Institute for Policy Studies. p.10.

[٧٣]) أحمد عبد الله الخشاشنة، تحريز الأدلّة الرقميّة وأثرها في كشف الجريمة، مجلّة الدراسات الأمنيّة، المجلّد الأوّل، العدد 16، الأردن، 2019، ص 7 وما بعدها.

[٧٤]) منها مثلا حادثة القبض على المواطن الهندي سيد ظبي الدين أنصاري، المعروف أيضًا باسم أبو جُنْدَل، بواسطة قوات الأمن السعوديّة عام 2012، والذي كان متعاونا مع منظمة "لشكر طيبة (LeT) الباكستانيّة" ومتورِّطًا في عدّة هجمات إرهابيَّة في مناطق مختلفة من الهند، وقد أرسلته لشكر طيبة إلى السعوديّة " لجمع التمويل والمجندين من المسلمين الهنود العاملين هناك، وتمّ القبض عليه من قوّات الأمن السعودية "بينما يعمل على مهمّته بإستخدام الإنترنت، خاصة موقع التواصل الاجتماعي فيسبوك.

Manoharan, N. (2012). Abu Jundal's Arrest and India-Saudi Arabia Counter-terrorism Cooperation. Vivekananda International Foundation. July, 6. Available at: https://www.vifindia.org/article/2012/july/06/abu-jundal-s-arrest-and-india-saudi-arabia-counter-terrorism-cooperation

[٧٥]) إستراتيجيّة الهيئة الوطنيّة للأمن السيبراني متاحة على : https://nca.gov.sa/national_cybersecurity_strategy-ar.pdf

– فؤاد الصلاحي، الأمن السيبراني، مجلّة الدوحة، وزارة الإعلام، 2015، ص 129.

[٧٦]) عبد الرحمن عاطف أبو زيد، الأمن السيبراني في الوطن العربي، دراسة حالة المملكة العربية السعودية، المركز العربي للبحوث والدراسات، 2019/09/25.

[٧٧]) نرمين سليمان، المرجع السابق، ص 202.

[٧٨]) عبد العزيز سالم السنيدي، السياسة العقابية للمشرّع الإماراتي في مواجهة الجرائم المعلوماتيّة في ظل المرسوم الإتّحادي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، رسالة ماجستير في القانون العام، Public Law Theses 7، 2018، ص 16 وما بعدها، متاح على الرابط: https://scholarworks.uaeu.ac.ae/public_law_theses

[٧٩]) معهد دبي القضائي، قانون مكافحة الشائعات والجرائم الإلكترونية لدولة الإمارات العربية المتحدة مرسوم بقانون اتحادي رقم 34 لسنة 2021 التشريعات والقوانين لدولة الإمارات العربية المتحدة 16، معهد دبي القضائي، دبي، 2022.

[٨٠]) علي ثامر النويران، **الجرائم الإلكترونيّة وطرق الحد منها : تجربة الأردن، المؤتمر الدولي لمكافحة الجرائم المعلوماتيّة ICACC، جامعة الإمام محمد بن سعود الإسلاميّة – كليّة علوم الحاسب والمعلومات**، الأردن، 2015، ص 178 وما بعدها.

[٨١]) أيوب محمود عمار الرواشدة، التنظيم القانوني للتوقيع الإلكتروني : في ضوء قانون المعاملات الإلكترونية الأردني رقم 15 لسنة 2015: دراسة مقارنة، مجلة العلوم القانونية والسياسية، المجلّد 6، العدد 2، العراق، 2016، ص 176.

[٨٢]) قانون جرائم أنظمة المعلومات لسنة 2010 المنشور على الصفحة 5334 من عدد الجريدة الرسميّة 5056 بتاريخ 2010/09/16.

[٨٣]) موقع مديرية الأمن العام الأردنيّة : http://www.psd.gov.jo

[٨٤]) علي ثامر النويران، المرجع السابق، ص181.

[٨٥]) مريم عبد اللطيف المسلماني، مظاهر التعاون الدولي لدولة قطر في مجال مكافحة الجرائم الإلكترونية، مجلّة القانون والمجتمع، المجلّد 10، العدد 2، 2022، ص 30 وما بعدها.

[٨٦]) المرجع السابق، ص 34 وما بعدها.

[٨٧]) كاظم عبد جاسم الزيدي، دراسة حول أهمية مكافحة الجرائم المعلوماتية وفقاً التشريع العراقي مكافحة الجرائم المعلوماتية في التشريع العراقي، استشارات قانونية مجانية، محاماة نت، 2017.

[٨٨]) محمد بن أحمد بن علي المقصودي، الأمن السيبراني والجهود الدولية لمكافحة الجرائم عابرة القارات، جامعة نايف العربية للعلوم الأمنية، المجلّد 37، العدد 427، السعودية، 2017، ص 103 وما بعدها.

[٨٩]) شيخة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، المجلّد 17، العدد1 ، جامعة الشارقة، الإمارات، 2020، ص 744 وما بعدها

[٩٠]) هشام عبد العزيز مبارك، تسليم المجرمين بين الواقع والقانون، الطبعة الأولى، دار النهضة العربية، مصر، 2006، ص 335.

[٩١]) خالد بن مبارك القريوي القحطاني، التعاون الأمني الدولي في مواجهة الجريمة المنظمة عبر الوطنية، رسالة دكتوراه، كلية الدراسات العليا، جامعة نايف العربيّة للعلوم الأمنيّة، الرياض، 2006، ص 38.

[٩٢]) سامح أحمد موسى، الجوانب الإجرائية للحماية القضائية لشبكة الإنترنت، رسالة دكتوراه، جامعة الإسكندرية، 2010، ص523.

[٩٣]) من بين إنجازات شرطة الأنتربول في مجال مكافحة الجرائم المعلوماتيّة، العمليّة التي قامت بها المباحث الفيدراليّة الأمريكيّة بالإشتراك مع الأنتربول في ملاحقة الشخص الذي نشر ما يعرف بفيروس "دودة الحب" الذي فتك بملايين الكومبيوترات حول العالم عبر الإنترنت في الفلبين. نذكر أيضا توقيف أحد الطلبة في الجمهورية اللبنانية من قبل القضاء اللبناني بتهمة إرسال صورة إباحية لقاصرة دون العشرة أعوام من موقعه على شبكة الإنترنت، كان هذا بفضل تلقي النيابة العامة اللبنانية بلاغاً أو برقية من الأنتربول في ألمانيا حول الواقعة أو القضية التي يحقق فيها القضاء اللبناني في 2005. أُنظر في هذا الإطار عادل عب العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتيّة وسبل التغلب عليها، دار الجامعة الجديدة، 2015، ص 28.

[٩٤]) عبد الحميد محسن أحمد، مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المذنبين هافانا، كوبا 27 أغسطس – 7 سبتمبر 1990م، المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، المجلد 6، العدد 11، السعودية، 1991، ص 131 وما بعدها.

[٩٥]) ياسمين أحمد صالح، الإرهاب الإلكتروني في ظل أزمة فيروس كورونا: الأنماط ... التداعيات، مجلة كلية السياسة والإقتصاد العدد التاسع يناير 2021، ص 83 وما بعدها.

[٩٦]) فادية حافظ جاسم، التعاون الدولي للحدّ من الجريمة المعلوماتيّة، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة النهرين، المجلّد 21، العدد 4، 2019، ص ص 395– 396.

[٩٧]) محروس نصار غايب، الجريمة المعلوماتيّة، مجلّة هيئة التعليم التقني الأكاديميّة، المجلد 24، 2011، ص20.

[٩٨]) حاتم أحمد محمد بطيخ، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات (دراسة تحليلية مقارنة)، مجلّة الدراسات القانونيّة والإقتصاديّة، المجلد 7، العدد 1، أغسطس 2021، ص 27 وما بعده.

[٩٩]) عبد القدوس بوعزة، أيوب مخرمش، أساليب التعاون الدولي في القضاء على الجرائم الإلكترونية، المجلة الجزائرية للعلوم السياسية والعلاقات الدولية، المجلد 13، العدد 18، الجزائر، 2022، ص 166 وما بعدها.

[١٠٠]) سالم محمد سليمان الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوطنية، رسالة دكتوراه، الدار الجماهيرية للنشر والتوزيع والإعلام، طرابلس، ليبيا، 2000، ص 425.

[١٠١]) أُنظر: عبد القدوس بوعزة، أيوب مخرمش، المرجع السابق، ص 166؛ وأيضا فريد ناشف، المرجع السابق، ص 440.

[١٠٢]) عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2015، ص ص 206–207.

[١٠٣]) أسامة بن غانم العبيدي، المرجع السابق، ص ص129– 130.

[١٠٤]) أُنظر: محمود علي عبد السلام وافي، الإنابة القضائيّة: دراسة مقارنة بين القانون المصري والنظام السعودي، مجلة العلوم القانونية والإقتصادية، المجلّد 58، العدد 02، 2016، ص 153 وما بعدها؛ أيضا أحمد عبد الحليم شاكر، دور الإنابة القضائية الدولية في مكافحة الجريمة، مجلة الفكر الشرطي، المجلد 17، العدد 4، 2008، ص 153.

[١٠٥]) أُنظر: عادل عبد العال إبراهيم خراشي، المرجع السابق، ص 208؛ أسامة بن غانم العبيدي، المرجع السابق، ص 130.

[١٠٦]) عبد الفتاح محمد سراج، النظرية العامة لتسليم المجرمين، دار النهضة العربية للنشر والتوزيع، الطبعة الأولى، 1998.

[١٠٧]) مصطفي عبد الغفار، تطور آليات التعاون القضائي الدولي في المواد على ضوء الآليات الحديثة الجنائية في مجال القبض على الهاربين وإعادتهم لمكافحة الجريمة، مجلّة معهد الدراسات القضائية والقانونية، وزارة العدل، مملكة البحرين، العدد الأول، 2008، ص 3.

[١٠٨]) عبد القدوس بوعزة، أيوب مخرمش، المرجع السابق، ص 166.

[١٠٩]) طارق أحمد صالح الخطيبي الفلاسي، أحكام تسليم المجرمين في قانون التعاون القضائي الدولي في المسائل الجنائية في ضوء الإتّفاقيات الدولية، رسالة ماجستير في القانون العام، أكاديمية شرطة دبي، كلية الدراسات العليا، 2015.