المجلة الالكترونية الشاملة متعددة المعرفة لنشر الابحاث العلمية و التربوية (MECSJ)
العدد الواحد و العشرون (كانون الثاني) 2020
ISSN: 2617-9563

WWW.mecsj.com/ar

الجرائم المعلوماتية وسبل مواجهتها على المستويين الوطني والدولي

د. شريهان ممدوح حسن
أستاذ القانون المساعد
جامعة شقراء – المملكة العربية السعودية
Dr_s_mamdouh@yahoo.com

ملخص البحث:

على الرغم من الأهمية التي تلعبها المعلوماتية وشبكة الانترنت في كونها الوسيلة الأسرع والأذكى في استحضار المعلومات المتدفقة، إلا أنها وللأسف الشديد تعد أيضاً أداة قوية لارتكاب الجريمة، ففي ظل غياب الأمن والمراقبة والتحكم، تظهر وتنموا كافة عمليات التجسس على المعلومات المعالجة إلكترونيا وسرقتها، الأمر الذي يشكل تهديداً غاية في الخطورة لسائر المؤسسات والهيئات الحكومية والخاصة التي تعتمد أعمالها على الحاسبات والشبكات، ومما يزيد من خطورة الأمر أنه بجانب صعوبة السيطرة على شبكة الإنترنت وعلى الجرائم التي ترتكب خلالها، فإنه يصعب أيضا اكتشاف هذه الجرائم أو تحديد مصدرها حيث يستخدم الجاني اسماً مستعاراً أو يرتكب فعله من خلال إحدى مقاهي الإنترنت، كما يصعب إيقافها بالنظر إلى سرعة نشر المعلومات وتسجيلها أوتوماتيكيا على الحاسبات الخادمة في الخارج.

الأمر الذي يتعين معه تكاتف الجهود المحلية والدولية في محاولة القضاء على مثل هذا النوع من الجرائم لخطورته وسرعة ارتكابه، وهو ما تصدى له المنظم السعودي في نظام مكافحة جرائم المعلومات السعودي الصادر بالمرسوم الملكي م/17 في 1428/3/8هـ، وكذا الاتفاقيات والمعاهدات الدولية.

الكلمات الافتتاحية: المعلوماتية، الجرائم الالكترونية، مكافحة الجرائم المعلوماتية.

Abstract:

Despite of the importance of the internet and informatics as the fastest and smartest way to evoke the flow of information, it is considered unfortunately a powerful tool to commit crimes. In the absence of security, observation and control, many operations of espionage appear and increase on information which are edited electronically and steal them. That issue makes a serious threat to all the governmental and private institutions whose work depends on computers and networks. What makes it more serious is that beside the difficulty of controlling the internet and the crimes committed through it. It is also difficult to discover these crimes or to determine their source, as the perpetrator uses a pseudonym or commits his crime through an internet café. It is also difficult to stop them, according to the speed of disseminating information and recording them automatically on servers abroad.

Domestic and international efforts must join together to eradicate this type of crime because of its seriousness and its speedy of commission. The Saudi organizer has tackled to these crimes in the Saudi Information Crime Prevention System which is issued by a royal decree (M/17) in 8/3/1428 Hijri and also in the international conventions and protocols.

Keywords: Informatics, Electronic crimes, Combating information crimes.

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الابحاث العلمية و التربوية (MECSJ)
العدد الواحد و العشرون (كانون الثاني) 2020
ISSN: 2617-9563
WWW.mecsj.com/ar

المقدمة:

لقد أصبحت المعلوماتية تتزايد بصورة كبيرة ومتتالية، حيث بدأت تغزو العالم منذ حدوث الثورة الصناعية وصارت حيث صار الاعتماد على الطرق التقليدية لجمع وتنظيم المعلومات قاصرة وبشدة عن تلبية احتياجات المستفيدين من المعلومات بكفاءة وفاعلية، وأصبح محتما استخدام أساليب علمية وتقنية متطورة لمواجهة فيض المعلومات المتدفق والتعامل معه.

وتعتبر شبكة الإنترنت من أبرز مظاهر هذا المجتمع المعلوماتي، فقد حدثت طفرة في الاتصالات حولت العالم إلى قرية صغيرة، فأصبح الإنسان يستطيع أن يرصد ما يجرى على الطرف الآخر من الكرة الأرضية بالصوت والصورة في لحظة قيام الحدث، وأصبحت عملية تبادل المعلومات سهلة وميسورة، وأدى الانتشار السريع للمعلومات عبر وسائل الاتصال المختلفة إلى تدفق هائل في المعلومات والأخبار والمعارف والأبحاث والرسائل الثقافية.

وعلى الرغم من الأهمية التي تلعبها المعلوماتية وشبكة الانترنت في كونها الوسيلة الأسرع والأذكى في استحضار المعلومات المتدفقة، إلا أنها وللأسف الشديد تعد أيضاً أداة قوية لارتكاب الجريمة، وخاصة منها عمليات التجسس على المعلومات المعالجة إلكترونيا وسرقتها وذلك بسبب غياب الأمن والمراقبة والتحكم، الأمر الذي يشكل تهديداً غاية في الخطورة لسائر المؤسسات والهيئات الحكومية والخاصة التي تعتمد أعمالها على الحاسبات والشبكات، ومما يزيد من خطورة الأمر أنه بجانب صعوبة السيطرة على شبكة الإنترنت وعلى الجرائم التي ترتكب خلالها، فإنه يصعب أيضا اكتشاف هذه الجرائم أو تحديد مصدرها حيث يستخدم الجاني اسماً مستعاراً أو يرتكب فعله من خلال إحدى مقاهي الإنترنت، كما يصعب إيقافها بالنظر إلى سرعة نشر المعلومات وتسجيلها أوتوماتيكيا على الحاسبات الخادمة في الخارج.

الأمر الذي يتعين معه الى ضرورة تكاتف الجهود المحلية والدولية في محاولة القضاء على مثل هذا النوع من الجرائم لخطورتها وسرعة ارتكابها، وهو ما تصدى له المنظم السعودي في نظام مكافحة جرائم المعلومات السعودي الصادر بالمرسوم الملكي م/17 في 1428/3/8هـ، وكذا الاتفاقيات والمعاهدات الدولية.

أهمية البحث:

مع انتشار المعلوماتية في كافة دول العالم ومنها الدول العربية، حيث صاحب انتشار استخدام الانترنت سلبيات وإيجابيات كثيرة، على كافة المستويات وخصوصاً على المستوى الأمني، وإدراكا لتجاوب الواقع الأمني مع الثورة المعلوماتية وما يصاحبها من حدوث جرائم وما يتبعها من مخاطر، وفى مقدمتها "الجريمة الإلكترونية" المتولدة من استخدام شبكة الإنترنت حتى يمكن بقدر الإمكان تفاديها والتقليل من حدة آثارها على شتى مناحي الحياة في المجتمع.

مشكلة البحث:

موضوع جرائم الإنترنت موضوع دقيق وشائك ويثير مشكلات جديدة كما أنه يعد مشكلة ذات طبيعة خاصة، فضلا عن مسألة صعوبة ملاحقة الجناة إذا ما كانوا يقيمون في دولة أخرى لا تربطها اتفاقية بالدولة التي تحقق فيها السلوك الإجرامي أو جزء منه، الأمر الذي يثير مسالة مدى فاعلية نظام مكافحة جرائم المعلومات السعودي والاتفاقيات الدولية في مكافحة مثل هذا النوع من الجرائم.

أهداف البحث:

يهدف هذا البحث إلى بيان الآتي:

- ✓ موضوع الجرائم الإلكترونية وخصائصها.
- ✓ المواجهة الدولية للجرائم الإلكترونية.
- ✓ مواجهة للجرائم الإلكترونية في النظام السعودي.

منهج البحث:

نظرا لخصوصية موضوع الدراسة، وتحقيقا لهذه الغاية نتبع المنهج التحليلي للنصوص النظامية القائمة، وذلك في دراسة الجرائم الالكترونية في ضوء نصوص الاتفاقيات والمعاهدات الدولية ونظام مكافحة جرائم المعلومات السعودي الصادر بالمرسوم الملكي م/17 في 1428/3/8هـ.

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الابحاث العلمية و التربوية (MECSJ)
العدد الواحد و العشرون (كانون الثاني) 2020
ISSN: 2617-9563
WWW.mecsj.com/ar

خطة البحث:

المقدمة.

المبحث الأول: ماهية الجرائم المعلوماتية.

المطلب الأول: تعريف الجرائم المعلوماتية وخصائصها.

المطلب الثاني: أنواع الجرائم المعلوماتية.

المطلب الثالث: أركان الجريمة المعلوماتية ومخاطرها.

المبحث الثاني: طرق مكافحة الجرائم المعلوماتية.

المطلب الأول: مكافحة الجرائم المعلوماتية على المستوى الوطني.

المطلب الثاني: الجهود الدولية لمكافحة الجرائم المعلوماتية.

المطلب الثالث: الصعوبات التي تواجه التعاون الوطني والدولي وكيفية القضاء عليها.

المبحث الأول: ماهية الجرائم المعلوماتية

تمهيد وتقسيم:

نظراً للازدياد المستمر والمطرد لاستخدام شبكات المعلوماتية، في المقال أصبح هناك ازديدا كبير أيضاً للجرائم المعلوماتية، ونظراً للخطورة التي تمثلها الجرائم المعلوماتية، كان ولا بد بداية التصدي لوضع تعريف للجرائم المعلوماتية مع بيان خصائصها، مع إلقاء الضوء على أهم أنواع تلك الجرائم، وأخيراً بيان أركان تلك الجرائم، وذلك وفق التقسيم التالي:

المطلب الأول: تعريف الجرائم المعلوماتية وخصائصها.

المطلب الثاني: أنواع الجرائم المعلوماتية.

المطلب الثالث: أركان الجريمة المعلوماتية ومخاطرها.

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الابحاث العلمية و التربوية (MECSJ)
العدد الواحد و العشرون (كانون الثاني) 2020
ISSN: 2617-9563
WWW.mecsj.com/ar

المطلب الأول: تعريف الجرائم المعلوماتية وخصائصها

إن التطور السريع لتقنيات الإعلام والاتصال وتنوع شبكات الربط أدى بطبيعة الحال إلى توسع ميادين استعمال هذه التقنيات سواء على المستوى الثقافي أو الاقتصادي أو الاجتماعي أو الإداري ...إلخ، وهذا بدوره أدى إلى الاستخدام السيء للإنترنت الذي ترتب عليه ارتفاع الجرائم المرتكبة بواسطته والتي تعرف بـ "الجرائم المعلوماتية أو الجرائم الالكترونية"، التي تطورت تطورا ملحوظا ومذهلا في عصرنا هذا سواء في شخصية مرتكبها أو في أسلوب ارتكابها.

فنظرا للأهمية البالغة في مجال مكافحة الجريمة المعلوماتية وما فرضته من تحديات خاصة في عصرنا الحالي الذي يعرف تطورا سريعا في مجال تكنولوجيات الإعلام والاتصال، لذلك حاولنا في دراستنا هذه إلى محاولة المساهمة في وضع الخطوط العريضة بالتعرف على مفهوم الجريمة الالكترونية وخصائصها.

أولا: تعريف الجريمة المعلوماتية (الالكترونية):

إن إيجاد تعريف للجريمة المعلوماتية كان محلاً لاجتهادات الفقهاء والباحثين، فقد ذهبوا في ذلك لمذاهب مختلفة ووضعوا تعريفات شتى وبالتالي فلا نجد تعريفاً محدداً للجريمة المعلوماتية.

الجريمة: فالجريمة في اللغة "الجيم والراء والميم" أصل واحد، يرجع إلى الفروع، والأصل هو القطع، إذ هو حمل الشئ لقطعه **(ابن فارس، 445)**، قال الله تعالى " يَا أَيُّهَا الَّذِينَ آمَنُوا كُونُوا قَوَّامِينَ لِلَّهِ شُهَدَاءَ بِالْقِسْطِ ۖ وَلَا يَجْرِمَنَّكُمْ شَنَآنُ قَوْمٍ عَلَىٰ أَلَّا تَعْدِلُوا ۚ اعْدِلُوا هُوَ أَقْرَبُ لِلتَّقْوَىٰ ۖ وَاتَّقُوا اللَّهَ ۚ إِنَّ اللَّهَ خَبِيرٌ بِمَا تَعْمَلُونَ"[1]، ومن معاني الجريمة في اللغة: القطع، يقال: جرمه يجرمه جرماً: قطعه، والتمام، يقال: سنة مجرمة، أي تامة، من تجرم الليل ذهب، والكسب، يقال: جرم لأهله: كسب لهم، والذنب والتعدي، يقال جرم فلان جرماً: أذنب**(الزبيدي، 1205هـ:385)**، والجريمة اصطلاحاً كل معصية أو مخالفة لأوامر الله تعالى ونواهيه**(أبو زهرة، 1976م:24)**، أي أن الجريمة تطلق على "إتيان فعل محرم معاقب على فعله أو ترك فعل محرم الترك معاقب على تركه، وهي فعل أو ترك نصت الشريعة على تحريمه والعقاب عليه"**(عوده، 2005م:44)**، والجريمة لدى فقهاء القانون: عبارة عن الواقعة التي ترتكب بالمخالفة لقانون العقوبات، ويترتب عليها عقوبة جنائية**(الجندي، 1998م:191)**.

(1) سورة المائدة، الآية 8.

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الابحاث العلمية و التربوية (MECSJ)
العدد الواحد و العشرون (كانون الثاني) 2020
ISSN: 2617-9563
WWW.mecsj.com/ar

وعرفت الجريمة بصفة عامة على إنها كل فعل غير مشروع صادر عن إرادة آثمة يقرر له القانون عقوبة أو تدبيراً احترازياً، وتعتمد الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت على المعلومة بشكل رئيسي، وهذا الذي أدى إلى إطلاق مصطلح الجريمة المعلوماتية على هذا النوع من الجرائم(**الكعبي، 2009م:32**).

المعلوماتية: لقد ذهب البعض إلى القول انه من الصعب أو من المستحيل وصف المعلومة بدقة وما يمكن فقط هو إدراك أثرها **(بدر، 2003م:17)**، المعلومات: مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلاً للتبادل والاتصال أو للتفسير والتأويل أو للمعالجة سواء بواسطة الأفراد أو بواسطة الأنظمة الالكترونية(**قوره، 2005م:97**)، وهناك من عرفها بأنها رسالة معبر عنها في شكل يجعلها قابلة للنقل والإبلاغ للغير أو بكونها رمزاً أو مجموعة رموز تنطوي على إمكانية الإفضاء إلى معنى(**الشوا، 1998م:117**)، كما عرفت أيضاً بأنها النقل المجرد لوقائع معينة ثم الحصول عليها من مصادر متعددة **(إبراهيم، 2008م:17)**.

الجريمة المعلوماتية "الالكترونية": لقد اختلف الفقهاء في تعريف الجريمة المعلوماتية، حيث تعددت التعريفات الخاصة بالجريمة المعلوماتية فمنها من عرفها بأنها "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات"، أو هي "الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية"، وهناك من عرفها بانها "الجريمة التي تقع بواسطة الحاسب الآلي أو عليه أو بواسطة شبكة الانترنت"، وهناك من عرف الجريمة المعلوماتية بأنها "كل سلوك إجرامي يتم بمساعدة الكمبيوتر أو كل جريمة تتم في محيط أجهزة الكمبيوتر" **(غازي، 2014م:118)**، وهناك من عرفها بأنها " كل فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية"(**الحلبي، 2011م:29**).

وهناك من يطلق عليها اسم جرائم استخدام تكنولوجيا المعلومات والاتصال ويسميها آخرون جرائم الكمبيوتر في حين يذهب آخرون إلى تسميتها الجرائم الالكترونية وهناك من يطلق عليها اسم الجرائم المستحدثة.

وقد عرفت الجريمة المعلوماتية طبقا لما جاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا سنة 2000 "بأنها أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية"(**الحلبي، 2011م:30**).

وقد تبنى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين تعريف الجريمة المعلوماتية بأنها "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية"**(المناعسة، وآخرون، 2001م:77)**.

كما ذهب مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية في عام 1983 إلى تعريف الجريمة المعلوماتية بأنها "كل سلوك غير مشروع أو غير أخلاقي أو مصرح به يتعلق بالمعالجة الآلية للبيانات أو ينقلها".

وفي تقرير الجرائم المتعلقة بالحاسوب أقر المجلس الأوروبي بقيام المخالفة (الجريمة) في كل حالة يتم فيها تغيير معطيات أو بيانات أو برامج الحاسوب أو محوها أو كتابتها أو أي تدخل آخر في مجال إنجاز البيانات أو معالجتها، وتبعاً لذلك تسببت في ضرر اقتصادي أو فقد حيازة ملكية شخص آخر أو بقصد الحصول على كسب اقتصادي غير مشروع له أو لشخص أخر **(السعيد، 1993م:324-325).**

يذهب اتجاه آخر في الفقه إلى التركيز على الجانب الموضوعي في تعريف الجريمة المعلوماتية باعتبار أن هذه الجريمة التي يستخدم الحاسب الآلي كأداة في ارتكابها فحسب بل تقع على الحاسب الآلي أو في داخل نظامه **(حجازي، 2006م:25)**.

ثانياً: خصائص الجريمة المعلوماتية:

تختلف الجريمة المعلوماتية عن الجرائم التقليدية من حيث الأفعال الاجرامية، هذا الاختلاف اكسبها خصوصية غير عادية مما حد بنا إلى بيان أهم خصائص الجريمة المعلوماتية في ما يلي:

1) الجريمة المعلوماتية جريمة عابرة للحدود الدولية:

الجريمة المعلوماتية جريمة لا تعترف بالحدود الجغرافية**(المومني، 2008م:50)**، فهي جريمة عابرة للحدود وبالتالي لا تعترف بعنصر المكان والزمان فهي تتميز بالتباعد الجغرافي واختلاف التوقيتات بين الجاني والمجني عليه، وبذلك اكسبها طبيعة دولية أو كما يطلق عليها جرائم ذات طبيعة متعدية الحدود**(إبراهيم، 2016م:76-77)**، فلا يقتصر الضرر المترتب عن الجريمة على المجني عليه وحده وإنما قد يتعداه إلى متضررين آخرين في دول أخرى نتج عن ذلك العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة وحول تحديد القانون الواجب تطبيقه بالإضافة إلى اختلاف إجراءات الملاحقة القضائية **(المومني، 2016م:52)،(Larent, 2008:6).**

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الابحاث العلمية و التربوية (MECSJ)
العدد الواحد و العشرون (كانون الثاني) 2020
ISSN: 2617-9563
WWW.mecsj.com/ar

2) سرعة وسهولة تنفيذ الجريمة المعلوماتية مع سهولة إخفاء وإتلاف الجناة لأدلة الجريمة وعدم الوقوف على دليل واضح يمكن التوصل إلى الجناة لا سيما وأن الجاني يتعمد إلى عدم ترك أثر لجريمته **(Ali,2010:20)**، بالإضافة إلى سهولة محو الدليل من على شبكات الانترنت والحاسب الآلي في زمن قياسي وبلمسة واحدة على لوحة المفاتيح بجهاز الحاسب الآلي على اعتبار أن الجريمة تتم في صورة أوامر تصدر إلى الجهاز مما يؤدي إلى عدم تحديد مرتكبيها **(أرحومة، 2009م:3)** وإثبات الجريمة وعدم وجود أي أثر كتابي ملموس لما يجري خلال تنفيذها من عمليات وأفعال إجرامية حيث يتم استخدام النبضات الالكترونية في نقل المعلومات **(سلامة، 2006م:97)**.

3) اختلاف طبيعة الجاني في الجرائم المعلوماتية: لا يمكن تحديد نموذج محدد للمجرم المعلوماتي يوضح شخصيته ومدى جسامة جرمه كأساس لتبرير وتقدير العقوبة، وإنما يتوافر لدى معظم مجرمي المعلوماتية مجموعة من الصفات تميزهم عن سواهم من الجناة المتورطين في أنماط الانحراف الأخرى، ومن هذه الصفات:

أ) الذكاء: يعتبر الذكاء من أهم صفات المجرم المعلوماتي حيث يمتلك المجرم المعلوماتي مهارة الذكاء التي تؤهله إلى القيام بتعديل وتطوير الأنظمة الأمنية والتقنية بالمقارنة بالمجرم التقليدي الذي يميل إلى العنف، فالمجرم المعلوماتي إنسان على مستوى عالي من الذكاء ومتكيف اجتماعياً لا يناصب العداء للمجتمع**(حجازي، 2006م:83)**.

ب) المهارة والاحتراف: تعتبر مهارة الاحتراف من أبرز خصائص المجرم المعلوماتي التي تؤهله لأن يوظف مهاراته في الاختراق والسرقة والاعتداء على حقوق الملكة الفكرية ومستوى المهارة التي يكون عليها المجرم المعلوماتي هي التي تحدد الأسلوب الذي يرتكب به الجرائم فإذا كان المجرم يتمتع بقدر ضئيل من مستوى المهارة والاحتراف نجد أن الجرائم التي يرتكبها لا تتعد الاتلاف المعلومات أو نسخ البيانات والبرامج **(إبراهيم، 2009م:135)**، أما إذا كان على درجة عالية من المهارة والاحتراف فإن أسلوبه في ارتكاب الجرائم المعلوماتية يكون مختلف حيث يمكنه استخدام الشبكات في الدخول إلى الحاسب الآلي لسرقة الأموال أو ارتكاب جرائم تجسس وزرع الفيروسات، فالظروف التي تحيط بالجريمة المراد تنفيذها وإمكانيات نجاحها واحتمالات فشلها تساعد في تحديد درجة مهارة المجرم التي يتمتع بها **(قوره، 2005م:58)**.

ج) التخصص: لابد أن يتوافر لدى الجناة مرتكبي الجرائم المعلوماتية قدر من المعرفة المعلوماتية بمعنى أنهم متخصصون في هذا الشكل من الانحراف والاجرام **(الشوا، 1998م:54)**.

د) يتراوح اعمار جناة مرتكبي الجريمة المعلوماتية ما بين (18-46) عاماً.

هـ) شديد الرغبة للعودة في ارتكاب الجرائم المعلوماتية.

5) صعوبة قياس الأضرار الناتجة عن الجريمة المعلوماتية: تعتبر الأضرار الناجمة من الجرائم المعلوماتية غير قابلة للقياس في حالة إثبات الجريمة المعلوماتية، نضف إلى ذلك في أن المجني عليهم في الجرائم المعلوماتية لا يعلمون شيئاً عنها إلا بعد أن تقع وحتى عندما يعلمون فهم يفضلون الكتمان وعدم الابلاغ لتجنب إنشاء وسر انتهاك النظام المعلوماتي للمؤسسة أو الشركة العائدة لهم**(الشوا، 1998م:65).**

6) اختلاف الدافع من الجرائم المعلوماتية: ذهب الفقه القانوني إلى نوعين من دوافع ارتكاب الجرائم المعلوماتية فهناك دوافع شخصية وأخرى خارجية:

أ) **الدوافع الشخصية:** فتنقسم لدى مرتكبي الجرائم المعلوماتية إلى دوافع مادية (يعتبر من أهم دوافع ارتكاب الجريمة المعلوماتية لما فيه من تحقيق الربح والثراء والكسب المادي بأعلى المكاسب وأقل مجهود دون أن يترك المجرم أثر وراءه) **(الحمود، والمجالي، 2005م:30)**، ودوافع ذهنية أو نمطية (كالمتعة والتحدي والرغبة في فهم النظام المعلوماتي وإثبات الذات والرغبة في قهر الأنظمة الالكترونية والتغلب عليها) **(الملط، 2006م:98).**

ب) **الدوافع الخارجية:** قد يسعى المجرم المعلوماتي في بعض الجرائم لا لكسب المال ولا للمتعة والتسلية، ومن أهم هذه الدوافع فيما يلي:

- **دافع التعاون والتواطؤ:** يعتبر هذا الدافع كثير التكرار في الجرائم المعلوماتية حيث قد تدفع الحاجة إلى بعض الدول أو المنشآت إلى الاتصال بأفراد يشغلون أماكن حساسة في إحدى الدول أو المنشآت الأخرى وذلك بهدف الاطلاع على بعض المعلومات والتقنيات المتوفرة لديها للاستفادة منها والتي قد يصل في بعض الأحيان إلى زرع جواسيس في تلك الأماكن مع استخدام عدة أساليب منها الرشوة أو الاقناع والإغراء المقترن بالتهديد **(الشوا، 1998م:61-62).**
- **دافع الانتقام:** يعتبر من أخطر الدوافع التي يمكن أن تدفع المجرم في ارتكابه للجريمة للمعلوماتية، وغالباً ما يكون هذا الدافع لأسباب تتعلق بالحياة المهنية لشخص يمتلك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها كالحرمان من بعض الحقوق المهنية أو الطرد من الوظيفة، فيتولد هنا دافع الانتقام من رب العمل أو أحد الزملاء **(الملط، 2006م:90).**

- هناك دوافع أخرى يكون الهدف منها سياسي كتهديد الأمن القومي والعسكري للدولة فيما يعرف بالتجسس الالكتروني والإرهاب الالكتروني والحرب المعلوماتية كما هو الحاصل بين الدول المتقدم الكترونياً.

7) وقوع الجريمة في بيئة المعالجة الآلية للبيانات والمعلومات.

يشترط لقيام الجريمة المعلوماتية التعامل مع بيانات مجمعة ومجهزة للدخول للنظام المعلوماتي وذلك من أجل معالجتها الكترونياً بما يمكن المستخدم من إمكانية كتابتها من خلال العمليات المتبعة والتي يتوافر فيها إمكانية تصحيحها أو تعديلها أو محوها أو استرجاعها، وهذه العمليات وثيقة الصلة بارتكاب الجرائم المعلوماتية ولابد من فهم واتقان الفاعل لها أثناء ارتكابها وخاصة في جرائم التزوير والتقليد.**(الملط، 2006م:105)**

المطلب الثاني: أنواع الجرائم المعلوماتية

تعد مسألة حصر الجرائم في أنواع محددة مسألة غاية في الصعوبة وذلك نتيجة للتطور الشديد والسريع التي تشهده مثل تلك الجرائم الأمر الذي يظهر معه أنواع جديدة مستحدثة لم تكن معروفة من قبل، وإن كان يمكن لنا تعديد أنواع الجرائم المعلوماتية وتقسيمها في المجمل إلى ثلاثة أنواع وهم الآتي:

النوع الأول: الاعتداء على المكونات المادية للنظام المعلوماتي:

ويتثمل هذا النوع من أنواع الجرائم المعلوماتية في الاعتداء على المكونات المادية للنظام المعلوماتي، من إتلاف الأجهزة والمعدات الملحقة بالنظام المعلوماتي، كما يتمثل هذا النوع من الجرائم في تلك الجرائم التقليدية التي ترتبط بالجرائم المعلوماتية أو النظام المعلوماتي، ولكنها فقط ترتبط بالأجهزة وملحقاتها محل الجريمة، غير أنه أثناء ارتكاب تلك الجريمة التقليدية يتعرض من خلالها النظام المعلوماتي إلي السرقة أو الإتلاف العمدي، وذلك عن طريق إتلاف المكونات بالضرب بالات حادة أو ثقيلة أو إشعال الحرائق بها أو تفجيرها أو العبث بمفاتيح التشغيل أو محو بطاقات التعريف بما فيها من معلومات مخزنة وغير ذلك مما يعود بالسلب على البرامج المعلوماتية أو البيانات المخزنة عليها، وأبرز مثال على ذلك ما حدث من تنظيم "الألوية الحمراء" بإيطاليا عندما قامت مجموعة من المتخصصين من ذلك التنظيم في التكنولوجيا بتدمير مركز المعالجة الآلية لأحد الشركات بالديناميت مما أدى إلى خسائر بلغت قيمتها أربعة مليون دولار**(الملط، 2005م:202)،(حسونة، 1993م:471)،(صابر، 2010م:3-4)،(الدباس، 2007م:90).**

النوع الثاني: الاعتداء على المكونات المنطقية للنظام المعلوماتي:

يتمثل هذا النوع من الجرائم المعلوماتية في القيام بالاعتداء على المكونات الخاصة بالنظام المعلوماتي والبرامج والتي من خلالها يتم الوصول إلى هدف معين، ومثل هذا النوع من الجرائم يتمثل في القيام بالآتي:

1. **تعديل البرنامج المعلوماتي:** ويتم تعديل البرنامج المعلوماتي عن طريق التلاعب فيه بغرض اختلاس المال عن طريق البرامج المعلوماتية، كما حدث عندما قام أحد المبرمجين بأحدي البنوك الأمريكية بإدارة الحسابات بتعديل برنامج بوسيلته الخاصة حيث قام بإضافة 10 سنت لمصاريف إدارة الحسابات الداخلية على كل عشرة دولارات، دولار واحد على كل حساب يزيد عن عشرة دولارات وقام بقيد المصاريف الزائدة في حساب خاص به أسماه Zzwickوتمكن من الحصول علي مئات الدولارات كل شهر، وقد تم اكتشاف هذه الجريمة بالمصادفة فأراد البنك بمناسبة تأسيس شركة جديدة للدعاية والإعلان إن يكافئ أول وأخر عميل له وفقا للترتيب الأبجدي وحينئذ اكتشف عدم وجود ما يدعى"Zzwick". **(الملط، 2005م:205)، (صابر، 2010م:4)**
2. **التلاعب في البرنامج المعلوماتي:** ويتم التلاعب في البرنامج المعلوماتي عن طريق زرع برنامج فرعي غير مسموح به في البرنامج الأصلي ويسمح من خلاله الدخول إلى العناصر الأساسية للبرنامج الأصلي، كما حدث في فرنسا عندما قام تشكيل عصابي مكون من عدة أفراد يعملون في إحدى الشركات بالاستيلاء على مبالغ مالية من أرصدة وحسابات العملاء، وذلك من خلال استغلال النظام المعلوماتي للشركة **(فكري، 2014م:615).**
3. **الاعتداء على برامج التشغيل**: ويتم الاعتداء على برامج التشغيل عن طريق تزويد البرنامج بمجموعة من التعليمات الإضافية يسهل الوصول بواسطتها إلى التحايل على النظام المعلوماتي، مثل ما قامت به إحدى شركات التامين الأمريكية بمدينة لوس انجلوس بواسطة مبرمجيها والحاسب الآلي الخاص بها بتصميم برنامج وهمي يقوم بتصنيع وثائق تأمين لأشخاص وهميين بلغ عددهم 64,000 وثيقة تامين.

النوع الثالث: الاعتداء على البيانات الموجودة داخل النظام المعلوماتي:

تم الاعتداء على المعلومات المدرجة بالنظام المعلوماتي بوسيلتين اثنين **(صابر، 2010م:5)**:

الوسيلة الأولي: التلاعب في المعلومات: فالتلاعب في المعلومات يتم من خلال إدخال معلومات بمعرفة المسؤول عن القسم المعلوماتي لكي يحصل من خلال هذا الإدخال على غرضه الإجرامي.

الوسيلة الثانية: إتلاف المعلومات: ويتم إتلاف المعلومات عن طريق استبدالها أو محوها من على النظام وقد حدث ذلك حينما قام شخص باختلاس 61,000 دولار وهي عبارة عن مبالغ مرسله من شركات التامين إلى إحدى المراكز الجامعية حيث قام المحللون بمحو كل الحسابات القائمة في سجلات النظام المعلوماتي الخاص بالمركز وجعلها غير قابلة للتحصيل.

المطلب الثالث: أركان الجريمة المعلوماتية ومخاطرها

أولاً: أركان الجريمة المعلوماتية: تقوم أركان الجريمة المعلوماتية على ثلاثة أركان:

الركن الأول: الركن المفترض في الجرائم المعلوماتية:

ويتمثل هذا الركن في وجود جهاز إلكتروني في الغالب هو جهاز الكمبيوتر كركن مفترض يشكل الوسيلة المستخدمة لارتكاب السلوك في الركن المادي للجرائم المعلوماتية بوجود تلك البيئة الرقمية المتصلة بالإنترنت**(البقلي، 2010م:21).**

الركن الثاني: الركن المادي في الجرائم المعلوماتية:

يتمثل الركن المادي في الجرائم المعلوماتية في ذلك السلوك المادي الذي يتمثل بإتيان أفعال للجرائم الواقعة على العرض، وقد تتضمن تعدداً معنوياً لأكثر من جريمة بذات السلوك في بعضها أو تقتصر على السلوك المادي للجريمة المعلوماتية بالوسيلة الالكترونية وتحقق النتيجة بوقوع الجريمة بناء على ذلك السلوك، فمثلاً يقوم مرتكب الجريمة بتجهيز الحاسب لكي يحقق له حدوث الجريمة، فيقوم بتحميل الحاسب ببرامج اختراق، أو أن يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة وتحميلها على الجهاز المضيف، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيدًا لبثها. **(البقلي، 2010م:21)،(قطب، 2010م:3)**.

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الابحاث العلمية و التربوية (MECSJ)
العدد الواحد و العشرون (كانون الثاني) 2020
ISSN: 2617-9563
WWW.mecsj.com/ar

الركن الثالث: الركن المعنوي في جرائم المعلوماتية:

لا يمكن تصور وجود جريمة ما دون توافر الركن المعنوي إلي جانب الركن المادي، لذا يعد الركن المعنوي من العناصر الضرورية واللازمة لتحقق الجريمة المعلوماتية، ويراد بالركن المعنوي الإرادة الإجرامية أو الإرادة الآثمة المقترنة بالفعل سواء اتخذت صورة القصد الجرمي وعندئذ توصف الجريمة بالعمدية، أم اتخذت صورة الخطأ غير العمدي وحينئذ تكون الجريمة غير العمدية، فالركن المعنوي هو القصد الجنائي العام، فالركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني**(أحمد، 2018م:338)**.

ثانياً: مخاطر الجريمة المعلوماتية:

تتمثل مخاطر الجريمة المعلوماتية في الأضرار التي تسببها، حيث تزداد الجرائم المعلوماتية يوماً بعد يوم نظراً للتطور المستمر والحركة المستمرة لنمو نطاق تقنية المعلومات، فتكنولوجيا المعلومات تدخل في جميع مجالات الحياة العامة والاقتصادية والتجارية والدولية، فالاعتماد عليها يتزايد باستمرار، مما يجعل تكنولوجيا المعلومات هدفاً جذاباً لارتكاب الجرائم المختلفة، التي تؤثر علي الحياة العامة وتحمل جميع الدول خسائر فادحة تصل إلي مليارات الدولارات، كما تبرز خطورة تلك الجرائم في تعدد القضايا وتنوعها، بين الاستيلاء على أموال الغير والنصب والاحتيال، والتهديد والابتزاز وانتحال صفة الغير، وسرقة الخدمات الهاتفية أو استعمالها بغير حق، والقذف والسب وانتهاك حقوق الملكية، ولذا يتعين أن تعمل كافة الدول جاهدة على مكافحة هذا النوع من الجرائم خاصة قبل وقوعها لحماية الأفراد والمجتمع **(صابر، 2010م:7).**

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الابحاث العلمية و التربوية (MECSJ)
العدد الواحد و العشرون (كانون الثاني) 2020
ISSN: 2617-9563
WWW.mecsj.com/ar

المبحث الثاني: طرق مكافحة الجرائم المعلوماتية

تمهيد وتقسيم:

نظراً لما تتميز به الجرائم المعلوماتية من خطورة شديدة وذلك لسهولة ارتكابها، وصعوبة إثباتها، الأمر الذي يتعين معه ضرورة تضافر وتكاتف الجهود الدولية والوطنية لمكافحة مثل هذا النوع من الجرائم لما يمثله من خطورة شديدة على المجتمع الدولي والوطني، ونظراً لأهمية إبراز طرق ووسائل مكافحة الجرائم المعلوماتية خصصنا هذا المبحث للحديث عن تلك الطرق، حيث نتناول الحديث عن تلك الطرق وفق التقسيم التالي:

- **المطلب الأول:** مكافحة الجرائم المعلوماتية على المستوى الوطني.
- **المطلب الثاني:** الجهود الدولية لمكافحة الجرائم المعلوماتية.
- **المطلب الثالث:** الصعوبات التي تواجه التعاون الوطني والدولي وكيفية القضاء عليها.

المطلب الأول: مكافحة الجرائم المعلوماتية على المستوى الوطني

عهد المنظم السعودي مسألة الجرائم المعلوماتية العناية الكافية نظراً لخطورتها الكبيرة في شتي المجالات، فلقد صدر المرسوم الملكي م/17 في 1428/3/8هـ في شأن مكافحة جرائم المعلومات، وهذا ان دل فإنما يدل على ما توليه المملكة العربية السعودية من أهمية كبري لمثل هذه النوعية من الجرائم المستحدثة، وقد واجه المنظم السعودي الجرائم المعلوماتية وتصدي لها وجرمها وفق الآتي:

أولا: جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات:

1. جريمة الدخول غير المشروع للمواقع أو اعتراضها:

يتمثل القصد الجنائي لهذه الجريمة في ركنين اثنين هما الدخول غير المشروع للموقع وقصد الحصول على المعلومات، ولا عبرة هنا باتجاه نية الجاني لتحقيق أثر محدد، يستوي في هذه الحالة توجه الإرادة إلى إحداث الاتلاف من عدمه.

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الابحاث العلمية و التربوية (MECSJ)
العدد الواحد و العشرون (كانون الثاني) 2020
ISSN: 2617-9563
WWW.mecsj.com/ar

حيث جرم نظام مكافحة الجرائم المعلوماتية السعودي فعل الدخول غير المشروع للمواقع الالكترونية، حيث عاقب بالسجن مدة لا تزيد عن سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب فعل الدخول عير المشروع لتهديد شخص أو ابتزازاه، وذلك لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً، أو إذا كان الدخول إلى الموقع الالكتروني بغرض تغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه [1].

أما المشرع المصري فقد فرق في العقاب بين مجرد الدخول غير المشروع سواء اكان هذا الدخول عمداً أو عن طريق الخطأ، وبين الدخول غير المشروع بقصد إحداث إتلاف أو محو او تغيير أو نسخ أو إعادة نشر للبيانات والمعلومات على ذلك الموقع.

2. جريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية:

هي جريمة تتعلق بالتلاعب في المعلومات داخل مواقع التواصل الاجتماعي كذلك مختلف النظم المعلوماتية بغرض تغيير الحقيقة فيها، وهذا التلاعب قد يتم عن طريق تعديل هذه المعلومات أو من خلال محو جزاء أو عدة اجزاء منها، فعملية تعديل المعلومات والمعطيات تقنية سهلة وشائعة من تقنيات الإجرام المعلوماتي **(المومني، 2008م:148).**

ففي النظام السعودي جرم فعل الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها، أو تغييرها، أو إعادة نشرها، حيث تكون العقوبة في تلك الجرائم السجن مدة لا تزيد على أربع سنوات، وبغرامة لا تزيد على ثلاثمائة ملايين ريال، أو بإحدى هاتين العقوبتين [2].

3. جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة:

لقد استغلت الكثير من الجماعات المتطرفة الطبيعة الاتصالية للإنترنت من اجل بث معتقداتها وأفكارها، بل تعداها الأمر إلى ممارسات تهدد أمن الدولة المعتدى عليها، خاصة المتمثلة في الارهاب والجريمة المنظمة، اللذان أخذا منحى آخر في استعمال الانترنت ووسائل التواصل الاجتماعي، التي ساعدتهم في ارتكاب جرائم غاية الفتك في حق المجتمعات والدول، بل الأخطر من ذلك أنها أتاحت للكثير من الدول ممارسة التجسس على دول أخري وذلك بالاطلاع على مختلف الأسرار العسكرية والاقتصادية لهذه الاخيرة **(اليوسفي، 2004م:25).**

---

[1] نص المادة 3-2/3 من نظام مكافحة جرائم المعلومات السعودي الصادر بالمرسوم الملكي م/17 في 1428/3/8هـ.
[2] راجع نص المادة 1/5 من النظام السعودي.

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الابحاث العلمية و التربوية (MECSJ)
العدد الواحد و العشرون (كانون الثاني) 2020
ISSN: 2617-9563
WWW.mecsj.com/ar

ولذلك جرم المنظم السعودي كل فعل من شأنه أن يؤدي إلى الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني، ففي كل تلك الجرائم تكون العقوبة السجن مدة لا تزيد على عشر سنوات، وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين [1].

4. جريمة الاعتداء على سلامة الشبكة المعلوماتية:

جرم المنظم السعودي كل فعل من شأنه أن يؤدي إلى إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدميرها، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها، أو إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها بأي وسيلة كانت، ففي كل تلك الجرائم تكون العقوبة السجن مدة لا تزيد على أربع سنوات، وبغرامة لا تزيد على ثلاثمائة ملايين ريال، أو بإحدى هاتين العقوبتين[2].

ثانياً: الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات:

1. جرائم الاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإلكتروني.

جرم النظام السعودي في نظام مكافحة الجرائم المعلوماتية كل فعل من شأنه الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة، وكذا كل فعل من شأنه الوصول دون مسوغ نظامي صحيح إلي بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات، حيث عاقب على تلك الأفعال بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين [3].

2. الجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإلكتروني بغرض الاتجار بالبشر أو المواد الاباحية أو المخدرات.

---

[1] راجع نص المادة 2/7 من النظام السعودي.
[2] راجع نص المادة 2/5-3 من النظام السعودي.
[3] راجع نص المادة 4 من النظام السعودي.

عاقب المنظم السعودي بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين [1] كل فعل ما من شأنه المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة، أو حرمة الحياة الخاصة، أو إعداده، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي، وايضا جرم كل فعل من شأنه إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره بغرض الاتجار في الجنس البشري، أو تسهيل التعامل به، أو إنشاء مواد أو بيانات متعلقة بالمواقع الاباحية، أو الأنشطة المتعلقة بالميسر والمخلفة بالآداب العامة وكذا العمل على نشرها أو ترويجها، أو إنشاء مواقع بغرض الاتجار بالمخدرات والمؤثرات العقلية، أو ترويجها، أو طرق تعاطيها، أو تسهيل التعامل معها.

3. جرائم التهديد المعلوماتي للحياة الخاصة.

تعد الحياة الخاصة قطعة غالية من كيان الإنسان لا يمكن انتزاعها منه، وإلا تحول في هذه الحالة إلي اداء صماء خالية من القدرة على الإبداع الإنساني، فالإنسان بحكم طبيعته له أسراره الشخصية ومشاعره الذاتية وصلاته الخاصة وخصائصه المتميزة ولا يمكن له أن يتمتع بها إلا في دائرة مغلقة يحفظها ويهيأ لها سبل البقاء، كما تقتضي حرمة هذه الحياة أن يكون للإنسان الحق في إفضاء السرية على مظاهرها، وفي إطار المعلوماتية تبرز خطورة التهديد المعلوماتي للحياة الخاصة بشكل أساسي في إساءة استخدام المعلومات والبيانات المتعلقة بالأفراد **(المومني، 2008م:172).**

وفي سبيل إضفاء المزيد من الحماية على الحياة الخاصة عاقب المنظم السعودي بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين كل فعل يرتكب بغرض التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد اجهزة الحاسب الآلي دون وجه حق أو التقاطه أو اعتراضه، أو المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا أو ما في حكمها، أو التشهير بالآخرين، وإلحاق الضرر بهم عبر وسائل تقنية المعلومات المختلفة [2].

---

[1] راجع نص المادة 6 من النظام السعودي.
[2] راجع نص المادة 3/1-4-5 من النظام السعودي.

كما عاقب المشرع المصري في قانون مكافحة جرائم تقنية المعلومات المصري كل من اعتدى على أي من المبادئ أو القيم الاسرية في المجتمع المصري، أو انتهك حرمة الحياه الخاصة أو ارسل بكثافة العديد من الرسائل الاليكترونية لشخص معين دون موافقته، أو منح بيانات إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته أو بالقيام بالنشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، لمعلومات أو اخبار أو صور وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة ام غير صحيحة بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين[1].

المطلب الثاني: الجهود الدولية لمكافحة الجرائم المعلوماتية

أصبح لكل شخص الحق في الاتصال بغيره، وتبادل المنافع المعرفية والمادية معه، ليس فقط داخل دولته، بل كذلك خارجها مع أبناء الدول الأخرى، وإذا كانت الدول فيما مضى استطاعت الحد من ذلك الاتصال والتبادل، في أوقات مضت تحت ستار حماية أمنها القومي الاقتصادي وغيره، إلا أنها لم تعد كذلك الآن بفعل تقدم وسائل الاتصال عبر الأقمار الصناعية، ووسائط نقل المعلومات والأخبار عبر الأثير والموجات الكهرومغناطيسية، لدرجة يمكن القول معها أن سيادة الدولة الإقليمية قد انحسرت عن الإقليم الفضائي أو الهوائي، واقتصرت على إقليمها الأرضي والمائي فقط.

فالجريمة الالكترونية أصبحت ألان متخطية للحدود الإقليمية للدول وتسير بمعدلات مضطردة نحو التعاظم، وتكمن النظرة الأساسية للتغلب على مسائل الجريمة متخطية للحدود الإقليمية في فضاء الانترنت لتعزيز التعاون فيما بين الدول.

ومع انتشار استخدام الانترنت والشبكات المعلوماتية، وتزايد استخدام الأفراد لها، أصبح هناك في المقابل تزايد كبير أيضاً في نسبة الجريمة المعلوماتية القائمة على الشبكات المعلوماتية، عن طريق منظمات اجرامية متخصصة في ارتكاب كافة الجرائم المعلوماتية عن طريق نشرها لشبكات دولية تتعاون فيما بينها في ارتكاب مثل تلك الجرائم، الأمر الذي يستوجب معه تضافر كافة الجهود الدولية والإقليمية والمحلية بغرض التصدي لتلك الجرائم المستحدثة لخطورتها الشديدة وصعوبة اثباتها،

[1] راجع نص المادة 25 من قانون مكافحة جرائم تقنية المعلومات المصري.

كذلك تعين الأمر العمل سوياً على رفع كفاءة الأجهزة المختصة بملاحقة مثل هذا النوع من الجرائم حتى تتمكن من ملاحقة التطور المستمر والسريع لتلك الجرائم ووسائل استخدامها بغرض القضاء على الصعوبات التي تواجه مكافحة مثل ها النوع من الجرائم.

وقد أولت الأمم المتحدة وكذا أغلب المنظمات الدولية اهتماماً كبيراً بالجرائم المعلوماتية لخطورتها الكبيرة، عن طريق إبرام مجموعة من الاتفاقيات الدولية التي تناولت الجرائم المعلوماتية وآليات مكافحتها والتصدي لها، وكانت أهم هذه الاتفاقيات ما يلي:

أولاً: اتفاقية برن: هي اتفاقية عالمية لحماية المصنفات الأدبية والفنية تعنى بحماية الحقوق الفكرية للمؤلفين وغيرهم، تم عقدها لأول مرة في برن، سويسرا عام 1886م تم التعديل عليها في مؤتمرات ومناقشات مختلفة وآخر نسخة تم اعتمادها كانت في باريس عام 1971م في سويسرا، وقد وقعت 120 دولة على هذه الاتفاقية، وقد وقعت المملكة العربية السعودية على هذه الاتفاقية في 11 ديسمبر 2003م، وبدء نفاذها في 11 مارس 2004م.

وبموجب هذه الاتفاقية تم منح برامج الحاسب الآلي الحماية القانونية باعتبارها أعمالاً أدبية وفقاً لما جاء فيها، حيث يتمتع بموجب هذه الاتفاقية مؤلف أو مصمم البرنامج الالكتروني بالحماية القانونية التي يتمتع بها مؤلفو المصنفات التي تدخل في نطاق هذه الاتفاقية وبمقتضاها يتمتع المؤلفون بحقوق مادية وأدبية.

والجدير بالذكر هنا أن اتفاقية برن لم تعالج مسألة النشر الالكتروني عبر شبكة الانترنت لان آخر تعديل طرأ عليها كان عام 1971 م في سويسرا قبل حدوث الثورة المعلوماتية الهائلة التي غزت العالم، وما ترتب عليها من انتشار الجرائم المعلوماتية، لذا جاءت هذه الاتفاقية قاصرة تماماً عن تقديم حلول قانونية لمكافحة هذا النوع من الجرائم ووضع الحلو القانونية الناتجة عنها.

ثانياً: معاهدة الويبو: الويبو عبارة عن منظمة دولية حكومية أصبحت في عداد الوكالات المتخصصة التابعة لمنظومة الأمم المتحدة سنة 1974.

وقد تم توقيع اتفاقية الويبو المنشئة للمنظمة العالمية للملكية الفكرية (الويبو) في استوكهولم في 14 يوليو 1967 ودخلت حيز التنفيذ سنة 1970 وعدلت سنة 1979 وبلغ مجموع أطرافها 192 دولة، وقد انضمت المملكة العربية السعودية إليها في 22 فبراير 1982م، وصارت سارية النفاذ في 22 مايو 1982م.

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الابحاث العلمية و التربوية (MECSJ)
العدد الواحد و العشرون (كانون الثاني) 2020
ISSN: 2617-9563
WWW.mecsj.com/ar

وتنقسم معاهدة الويبو إلى معاهدتين اثنين:

المعاهدة الأول: معاهدة الويبو بشأن حق المؤلف لسنة 1996م:

أبرمت هذه المعاهدة في عام 1996 ودخلت حيز التنفيذ عام 2002، وهي عبارة عن اتفاق خاص في إطار اتفاقية برن وتتناول حماية المصنفات وحقوق مؤلفيها في البيئة الرقمية، وكل طرف متعاقد (حتى وإن لم يكن ملتزما باتفاقية برن) يجب أن يمتثل للأحكام الموضوعية الواردة في وثيقة 1971 (باريس) لاتفاقية برن بشأن حماية المصنفات الأدبية والفنية (لسنة 1886). وفضلاً عن الحقوق المنصوص عليها في اتفاقية برن، تمنح هذه المعاهدة بعض الحقوق الاقتصادية للمؤلفين، ومدة الحماية المقررة بموجب هذه المعاهدة 50 سنة على الأقل لأي مصنف، وتتناول المعاهدة أيضا موضوعين يتعين حمايتهما بموجب حق المؤلف وهما [1]:

1. برامج الحاسوب، أيا كانت طريقة التعبير عنها أو شكلها.
2. مجموعات البيانات أو المواد الأخرى ("قواعد البيانات")، أيا كان شكلها، إذا كانت تعتبر ابتكارات فكرية بسبب اختيار محتوياتها أو ترتيبها (ولا تدخل في نطاق المعاهدة أية قاعدة للبيانات لا تعد بمثابة ابتكار من ذلك القبيل).

المعاهدة الثانية: معاهدة الويبو بشأن الأداء والتسجيل الصوتي لسنة 1996م:

وقد أبرمت المعاهدة في 1996 ودخلت حيز التنفيذ سنة 2002، وبلغ عدد أطرافها 103 طرف، ونصت على أنه يجب أن تكون مدة الحماية 50 سنة على الأقل، وتتناول معاهدة الويبو بشأن الأداء والتسجيل الصوتي حقوقاً لنوعين من المستفيدين، ولا سيما في البيئة الرقمية هما [2]:

1. فنانو الأداء (الممثلون والمغنون والموسيقيون وما إلى ذلك).
2. منتجو التسجيلات الصوتية (أي الأشخاص الطبيعيون أو المعنيون الذين يتم تثبيت الأصوات بمبادرة منهم وبمسؤوليتهم) وتتناول الوثيقة ذاتها هذين النوعين من أصحاب الحقوق لأن معظم الحقوق الممنوحة بموجب المعاهدة لفناني الأداء هي الحقوق المتصلة بما تم تثبيته من أدائهم السمعي البحت (أي موضوع التسجيلات الصوتية)، وتعطي المعاهدة فناني الأداء أربعة أنواع من الحقوق المالية في أوجه أدائهم المثبتة في تسجيلات صوتية و

---

[1] معاهدة الويبو بشأن حق المؤلف لسنة 1996م، الموقع الرسمي للـ WIPO https://www.wipo.int/treaties/ar/ip/wct/summary_wct.html، تاريخ الزيارة 10 اكتوبر 2019م، الساعة 10 صباحاً.
[2] معاهدة الويبو بشأن الأداء والتسجيل الصوتي لسنة 1996م، الموقع الرسمي للـ WIPO https://www.wipo.int/treaties/ar/ip/wppt/summary_wppt.html، تاريخ الزيارة 10 اكتوبر 2019م، الساعة 10 صباحاً.

ليس تسجيلات سمعية بصرية مثل الأفلام السينمائية). وتلك الحقوق هي: "1" حق الاستنساخ، "2" وحق التوزيع، "3" وحق التأجير، "4" وحق إتاحة الأداء المثبت.

وقد ألزمت تلك المعاهدتان كافة الأطراف المتعاقدة بالنص في قوانينها على جزاءات قانونية توقع ضد التحايل على التدابير التكنولوجية (مثل التجفير) التي يطبقها فنانو الأداء أو منتجو التسجيلات الصوتية لدى ممارسة حقوقهم وضد أي حذف أو تغيير في المعلومات الضرورية مثل بعض البيانات التي تسمح بتعريف فنان الأداء وأدائه أو منتج التسجيل الصوتي وتسجيله الصوتي لإدارة حقوقهم المذكورة مثل الترخيص وجني الإتاوات وتوزيعها أي معلومات بشأن إدارة الحقوق.

وكذلك تضمنت المعاهدة بالزام كل طرف متعاقد بأن يتخذ وفقاً لنظامه القانوني التدابير اللازمة لضمان تطبيق المعاهدة فيتعين على الطرف المتعاقد أن يكفل في قانونه إجراءات إنفاذ تسمح باتخاذ تدابير فعالة ضد أي تعد على الحقوق التي تغطيها المعاهدة ولا بد أن تشمل تلك الإجراءات توقيع الجزاءات العاجلة لمنع التعديات والجزاءات التي تعد رادعا لتعديات إضافية[1].

المعاهدة الثالثة: اتفاقية تريبس: تعد اتفاقية تريبس من المعاهدات التي قام المجتمع الدولي بإنشائها بغرض حماية الملكية الفكرية من السطو عليها خصوصاً مع انتشار الجرائم المعلوماتية الخاصة بالسطو الإلكتروني على الأعمال الفنية دون إعطاء مالكيها أي حق مادي أو معنوي، حيث جاءت تلك الاتفاقية لمنح الحماية القانونية والدولية والتصدي لمثل هذا النوع من الجرائم المعلوماتية.

وقد تم التوقيع على هذه الاتفاقية من قبل الدول الأعضاء عام 1994م، حيث تناولت تحرير التجارة الدولية من كافة مناحي النشاط التجاري على الصعيد الدولي، وشملت اتفاقية تريبس على مواد من شأنها مكافحة الجرائم المعلوماتية، حيث ورد في المادة 1/10 على أنه حيث تضمنت الحماية لبرامج الحاسب الآلي أو الكمبيوتر سواء كانت بلغة المصدر أو لغة الآلة باعتبارها أعمالاً أدبية بموجب معاهدة برن 1971، نصت في المادة 2/10 وأيضا حماية البيانات المجمعة أو المواد الأخرى بشروط معينة.

وأيضا فرضت اتفاقية التربس على الدول الأعضاء من منظمة التجارة العالمية التزامات عامة تتعلق بالإنفاذ، حيث ألزمت كل الدول الأعضاء بتوفير قواعد إجرائية في القانون الوطني تسمح باتخاذ تدابير فعالة سواء (دعوى قضائية- أمر قضائي- تظلم- شكوى إدارية) لمواجهة أي اعتداء على حق من حقوق الملكية الفكرية المنصوص عليها في هذه الاتفاقية واتخاذ إجراءات سريعة لمنع التعديات،

---

[1] معاهدة الويبو بشأن الأداء والتسجيل الصوتي لسنة 1996م، الموقع الرسمي للـ WIPO
https://www.wipo.int/treaties/ar/ip/wppt/summary_wppt.html، تاريخ الزيارة 10 اكتوبر 2019م، الساعة 10 صباحاً.

وكذلك تضمنت التشريعات الوطنية بأن تخول اتفاقية التريبس صلاحية أن تأمر المدعي بتقديم أدلة معقولة تفيد أنه صاحب حقوق الملكية الفكرية، وأن تأمره بتقديم تأمين أو كفالة بالقدر الذي يكفي لحماية المدعى عليه من إساءة استعمال المدعي لحقوقه أو لتنفيذها **(ثابت، 1439هـ:97)**.

المطلب الثالث: الصعوبات التي تواجه التعاون الوطني والدولي وكيفية القضاء عليها

نتيجة لما تمر به المعلوماتية من تطور غاية في السرعة، فضلاً عن اعتماد كافة المؤسسات والقطاعات بل والدول والأشخاص عليها في كافة نواحي الحياة، الأمر الذي أغرى أرباب الإجرام المعلوماتي للتعدي على جميع الأشخاص والمؤسسات بالجرائم المعلوماتية، الأمر الذي يتعين معه ضرورة مواجهة ومكافحة تلك الجرائم سواء على المستوي المحلي أو الدولي، غير أن مكافحة مثل هذا النوع من الجرائم يواجه مجموعة من الصعوبات التي تواجه التعاون الوطني والدولي للقضاء على تلك الجرائم، وتتمثل تلك الصعوبات فيما يلي:

أولاً: عدم كفاية الأنظمة الوطنية القائمة لمكافحة تلك الجرائم:

حيث أن الأنظمة الجزائية الوطنية لا تتطور بنفس السرعة التي تتطور بها المعلوماتية، وتزايد مهارة الذهن البشري في تسخير هذه المبتكرات لاستخدام سي، ومن هنا فإن النظام الجزائي التقليدي لا يكفي من حيث المبدأ لمواجهة مثل هذا النوع من الإجرام نظراً لحداثته واعتماده على تكنولوجيا غاية في التعقيد والتطور، ومن هنا استوجب على المنظم السعودي الاتمام بتنظيم مناخ نظامي وإعداده لمواكبة هذا التطور السريع للمعلوماتية وجرائمها ومكافحتها.

فتطبيق هذه الأنظمة والقوانين على أشكال جديدة للجرائم المعلوماتية لا يصطدم فقط بصعوبات ناجمة عن الطبيعة الخاصة والخصائص الفنية الفريدة للوسائل المعلوماتية المستخدمة في ارتكابها، وإنما تعترضه صعوبات رئيسية أخرى مرجعها أن نصوص التجريم التقليدية قد وضعت في ظل تفكير يقتصر إدراكه على الثروة الملموسة والمستندات ذات الطبيعة المادية مما يتعذر معه تطبيقها لحماية القيم الغير مادية المتولدة عن المعلوماتية **(الديربي، وإسماعيل، 2012م:12)**.

ونتيجة لذلك يتعين على الأجهزة الجزائية الإجرائية أن تتعامل مع أشكال محسوسة من الأدلة، وهو ما يلقي بظلاله على أساليب كشف الجرائم المعلوماتية وعمليات البحث الجنائي والتحقيق ومنظومة التدريب التخصصي اللازم لاكتساب المهارات الحقيقية اللازمة للتعامل مع هذه النوعية من الجرائم وضرورة تحديث الأساليب الإجرائية واستكمالها على نحو سيكفل استجابتها بشكل كاف دون تعريض حقوق الأفراد وحرياتهم للخطر لمتطلبات العملية الإثباتية في مجال الجرائم المعلوماتية. **(آل علي، 2009م:64)**

ثانياً: صعوبة إثبات الجريمة المعلوماتية أو اكتشافها:

تتميز الجرائم المعلوماتية بانها جريمة لا يتطلب لوقوعها حدوث عنف أو سفك للدماء ، فهي جريمة تقع دون وجود أي آثار لها عكس الجرائم التقليدية ، فهي عبارة عن مجموعة من الأرقام والبيانات التي تتغير أو يتم محوها من السجلات المخزنة في الحاسب الآلي ، ومن ثم فهي صعبة الاكتشاف لكونها لا تترك أي آثار خارجية تدل على وقوعها أو هوية مرتكبها ، فضلاً عن عدم وجود أي أثر كتابي لما يتم خلال تنفيذها ، نظراً لكونها تتم عن طريق نبضات إلكترونية وارتكابها عبر الدول يتم عن طريق شبكات الانترنت دون الحاجة إلي السفر وتخطي الحدود بين الدول. **(سككير، 2010م:42)**

ثالثاً: تمتع مرتكبي الجرائم المعلوماتية بمهارات فنية خاصة:

فمرتكبو الجرائم المعلوماتية يتميزون بكونهم مدربون على درجة عالية من المهارة في استخدام الأجهزة الإلكترونية الحديثة، وملمون بكافة المهارات الفنية في مجال المعلوماتية، فهم في الغالب من المتخصصين في مجال المعلومات.

رابعاً: دولية الجرائم المعلوماتية:

من الصعوبات التي تواجه الجرائم المعلوماتية مسألة دوليتها، فهي جرائم تقع متخطية لكافة الحدود الجغرافية، حيث تكتسب الطبيعة الدولية عن طريق القدرة التي تتميز بها أجهزة الحاسب الآلي والشبكات الالكترونية في نقل وتبادل المعلومات بسرعة فائقة، حيث يتم تداولها عبر تلك الأنظمة قاطعة كل تلك المسافات في سرعة فائقة، الأمر الذي يمثل عائق كبير في السيطرة عليها الحد منها**(قوره، 2003م:47).**

فالجرائم المعلوماتية لا تعترف بالحدود ولا بالحواجز بين الدول والقارات، فهي وبحق شكل من أشكال الجرائم العبارة للحدود، لذلك فإن هذا الأمر يتطلب تعاون دولي لمواجهة مشاكلها من حيث مكان وقوعها واختصاص المحاكم بها لجمع المعلومات والتحريات عنها والتنسيق بين الدول في معاينتها وتحديد صورها وقواعد التعامل معها وإيجاد الحلو لها، وتتمثل أهم العقبات التي تقف ضد آليات التعاون الدولي في مواجهة الجرائم المعلوماتية فيما يلي **(آل علي، 2009م:67)**:

1. لا يوجد مفهوم محدد ومشترك بين الدول لماهية الجريمة المعلوماتية.
2. لا يوجد مفهوم عام حول التعريف النظامي للنشاط الإجرامي المتعلق بالجرائم المعلوماتية.
3. اختلاف آليات التصدي للجريمة المعلوماتية وذلك لاختلاف التقاليد القانونية وفلسفة النظم القانونية المختلفة.
4. ضعف التنسيق بين أنظمة وقوانين الإجراءات الجنائية للدول المختلفة فيما يتعلق بالتحري والتحقيق في الجرائم المعلوماتية.
5. نقص الخبرة لدي الأجهزة الشرطية والقضائية في مجال المعلومات حول تلك الجرائم.
6. تعقد المشاكل القانونية والفنية الخاصة بتنفيذ إجراء معلوماتي معين خارج حدود الدولة، أو ضبط معلومة مخزنة فيه أو الأمر بتسلمها.
7. عدم وجود معاهدات للمعاونة الثنائية أو الجماعية بين الدول تسمح بالتعاون الدولي الكفؤ، أو عدم كفايتها إن كانت موجودة لمواجهة المتطلبات الخاصة بالجرائم المعلوماتية وسرعة إجراء التحريات فيها.

الخـــــــــاتمة

بعد الانتهاء من هذا البحث والذي تناول الحديث عن الجرائم المعلوماتية، حيث تناول الحديث في المبحث الأول ماهية الجرائم المعلوماتية، وذلك من خلال تعريف الجرائم المعلوماتية وخصائصها، مع إلقاء الضوء على أنواع الجرائم المعلوماتية، وأخيراً بيان أركان الجريمة المعلوماتية ومخاطرها.

وفي المبحث الثاني ألقي البحث الحديث عن طرق مكافحة الجرائم المعلوماتية، من خلال بيان آليات مكافحة الجرائم المعلوماتية على المستوى الوطني، وكذا الجهود الدولية لمكافحة الجرائم المعلوماتية، وأخيراً بيان الصعوبات التي تواجه التعاون الوطني والدولي وكيفية القضاء عليها.

وخلص البحث إلى مجموعة من النتائج والتوصيات أهمها ما يلي:

النتائج والتوصيات:

تتمثل النتائج والتوصيات في الآتي:

1. تعد مسألة حصر الجرائم في أنواع محددة، وذلك نظراً لصعوبة هذا الحصر للتطور الشديد والسريع التي تشهده مثل تلك الجرائم.
2. من أنواع الجرائم المعلوماتية الاعتداء على المكونات المادية أو المنطقية أو البيانات المكونة والموجودة على للنظام المعلوماتي.
3. تقوم أركان الجريمة المعلوماتية على ثلاثة أركان، ركن مفترض، وركن مادي، وركن معنوي.
4. صعوبة إثبات الجريمة المعلوماتية، وذلك صعوبة حفظ الأدلة، صعوبة ملاحقة المجرم لأنه لا يترك أثرا ماديا ملموسا.
5. ضرورة ان تقوم مؤسسات المجتمع المدني المعنية بالمعلوماتية بحملات توعية للتحذير من مخاطر شبكة الانترنت وتثقيف الجميع لحمايتهم من مجرمي شبكة الانترنت وكذا عمل حملات إعلانية مكثفه لذلك.
6. ضرورة ان تتخذ المؤسسات مختلف الإجراءات لعمل الحماية الأمنية اللازمة والمقررة وفقا للمعايير العالمية لحماية بياناتها وأنظمتها الالكترونية من الاختراق ووضع سياسة أمنية يتم مراجعتها بشكل دوري.
7. ضرورة التعاون بين الدول والمنظمات الدولية، في نشر الثقافة القانونية بالمجتمع لكيلا يقع فريسة لهذه الجرائم.
8. ضرورة تدريب المحققين بشكل تقني أكثر لكشف هذه الجرائم التي لم يعهدونها من قبل أثناء حياتهم العملية.
9. ضرورة التعاون بين الجهات الأمنية والقضائية مع جهات وشركات خاصة متخصصة للاستعانة بخبراتها التقنية في الكشف عن الجرائم المعلوماتية.

المراجع والمصادر

أولاً: المراجع العامة والمتخصصة:

1. **ابن فارس،** معجم مقاييس اللغة، الجزء الأول.
2. **بدر، أحمد انور (2003م)،** الجديد في الاتصال العلمي، دار الثقافة العلمية، الإسكندرية.
3. **الملط، أحمد خليفة (2006م)،** الجرائم المعلوماتية، دار الفكر العربي، الإسكندرية.
4. **المناعسة، أسامة، والزعبي، جلال، والهواوشة، صايل فاضل (2001م)،** جرائم الحاسب الآلي والانترنت، دار وائل للطباعة والنشر والتوزيع، الطبعة الأولى، عمان.
5. **فكري، أيمن عبد الله (1435هـ/ 2014م)،** الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد، الطبعة الأولى، الرياض، المملكة العربية السعودية.
6. **الجندي، حسني (1998م)،** شرح قانون العقوبات، القسم العام.
7. **أحمد، خالد حسن (1439هـ/ 2018م)،** الحجية القانونية للمستندات الالكترونية بين الفقه الإسلامي والقانون الوضعي، مركز الدراسات العربية للنشر والتوزيع، الطبعة الأولى، الجيزة.
8. **الحلبي، خالد عياد (2011م)،** إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، الأردن.
9. **إبراهيم، خالد ممدوح (2019م)،** الجرائم المعلوماتية – دار الفكر الجامعي، الإسكندرية.
10. **إبراهيم، خالد ممدوح (2009م)،** الجرائم المعلوماتية، دار الفكر الجامعي، الطبعة الأولى، الاسكندرية.
11. **إبراهيم، خالد ممدوح(2008م)،** أمن الجريمة الالكترونية، الدار الجامعية للطباعة والنشر، القاهرة.
12. **ثابت، طارق (1439هـ)،** مدخل إلى قانون الملكية الفكرية، مركز الكتاب الأكاديمي.
13. عوده، عبد القادر(2005م)، التشريع الجنائي الإسلامي مقارناً بالقانون الوضعي، دار الكتب العلمية، الجزء الأول، لبنان.
14. **اليوسفي، عبد الله بن عبد العزيز(2004م)،** أساليب تطور البرامج والمناهج التدريبية لمواجهة الجرائم المستحدثة، جامعة نايف العربية للعلوم الامنية، الطبعة الاولي، الرياض.

15. **إسماعيل، عبدالعال الديربي ومحمد صادق (2012م)**، الجرائم الإلكترونية دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت، المركز القومي للإصدارات القانونية، الطبعة الأولى، القاهرة.
16. **حجازي، عبدالفتاح بيومي(2006م)**، مكافحة الكمبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، الاسكندرية.
17. **السعيد، كامل (1993م)**، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، القاهرة.
18. **أبو زهرة، محمد (1976م)**، الجريمة والعقوبة في الفقه الإسلامي، دار الفكر العربي، القاهرة.
19. **الشوا، محمد سامي (1998م)**، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة.
20. **سلامة، محمد عبدالله ابو بكر (2006م)**، موسوعة جرائم المعلوماتية، جرائم الكمبيوتر والانترنت، منشأة المعارف، الاسكندرية.
21. **الكعبي، محمد عبيد (2009م)**، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، القاهرة.
22. **سككير، محمد على (1431هـ/2010م)**، الجريمة المعلوماتية وكيفية التصدي لها، كتاب الجمهورية، القاهرة.
23. **قطب، محمد على (2010م)**، الجرائم المعلوماتية وطرق مواجهتا الجزء الثاني، الأكاديمية الملكية للشرطة، البحرين.
24. **الزبيدي، محمد مرتضى (1205هـ)**، تاج العروس من جوهر القاموس، دار الهداية.
25. **الدباس، محمد نور خالد (2007م)**، واقع الجريمة المنظمة في الأردن، دار يافا العلمية للنشر والتوزيع، الطبعة الأولى، عمان، الأردن.
26. **غازي، محمود إبراهيم (2014م)**، الحماية الجنائية للخصوصية والتجارة الالكترونية، مكتبة الوفاء القانونية، الطبعة الأولى، الاسكندرية.

27. **أرحومة، موسى مسعود (2009م)**، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس.
28. **قوره، نائلة عادل محمد فريد (2005م)**، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقيه، منشورات الحلبي القانونية، الطبعة الأولى، بيروت.
29. **المومني، نهلا عبد القادر (1429هـ/2008م)**، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن.
30. **البقلي، هيثم عبد الرحمن (1431هـ/ 2010م)**، الجرائم الالكترونية الواقعة على العرض بين الشريعة والقانون، دار القلم للنشر والتوزيع، الطبعة الأولى، القاهرة.
31. **الحمود، وضاح محمود الحمود، والمجالي، نشأت مفضي** (1426هـ/2005م)، جرائم الإنترنت: التعرض للأخلاق والآداب العامة، الحض على الفجور، جرائم الاستغلال الجنسي للأطفال، دار المنار، عمان.

ثانياً: الرسائل الدوريات:

1. **الملط، أحمد خليفة (2005م)**، الجرائم المعلوماتية، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة فرع بني سويف.
2. **صابر، دويب حسين (2010م)**، القوانين العربية وتشريعات تجريم الجرائم الالكترونية وحماية المجتمع، المؤتمر السادس لجمعية المكتبات والمعلومات، المملكة العربية السعودية.
3. **حسونة، ذكي ذكي أمين (1993م)**، جرائم الكمبيوتر والجرائم الأخرى في مجال التكنيك المعلوماتي، المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة.
4. **آل علي، مريم محمد (2009م)**، واقع الجرائم الإلكترونية المتعلقة بالآداب العامة عبر الانترنت دراسة ميدانية، مركز بحوث الشرطة، شرطة الشارقة، الشارقة.
5. **قوره، نائلة عادل (2003م)**، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية تطبيقية، رسالة دكتوراه، كلية الحقوق جامعة القاهرة.

ثالثاً: الأنظمة والمعاهدات والاتفاقيات الدولية:

1. معاهدة الويبو بشأن الأداء والتسجيل الصوتي لسنة 1996م، الموقع الرسمي للـ WIPO .https://www.wipo.int/treaties/ar/ip/wppt/summary_wppt.html
2. معاهدة الويبو بشأن الأداء والتسجيل الصوتي لسنة 1996م، الموقع الرسمي للـ WIPO .https://www.wipo.int/treaties/ar/ip/wppt/summary_wppt.html
3. معاهدة الويبو بشأن حق المؤلف لسنة 1996م، الموقع الرسمي للـ WIPO .https://www.wipo.int/treaties/ar/ip/wct/summary_wct.html
4. نظام مكافحة جرائم المعلومات السعودي الصادر بالمرسوم الملكي م/17 في 1428/3/8هـ.

المراجع الأجنبية:

1. **Larent, Grave Raulin (2008),** règles de conflits de juridications et règles de conflits de lois appliquées aux cybers délit, memoire de master 2 professionnel droit de l'internet publique, université paris 2-pantheon Sorbonne.
2. **Ali, El-Azzouzi (2010),** La cybercriminalité au Maroc, Edition Bishops solution, Casablanca.