



جامعة مستغانم

كلية الحقوق والعلوم السياسية

أطروحة

للحصول على شهادة الدكتوراه الطور الثالث في الحقوق تخصص القانون الدولي الجنائي

حماية النظم المعلوماتية وفق الاتفاقيات الدولية والتشريعات الوطنية

تحت إشراف الأستاذ:

طاهر عباس

من إعداد الطالب:

هاني مطر أبو سعود

لجنة المناقشة:

رئيسا	جامعة مستغانم	أستاذة	حميدة نادية
مشرفا مقرر	جامعة مستغانم	أستاذ	عباس طاهر
ممتحنا	جامعة مستغانم	أستاذة محاضرة أ	و افي حاجة
ممتحنا	جامعة مستغانم	أستاذ محاضراً	بن عودة نبيل
ممتحنا	جامعة بلعباس	أستاذ	فرعون محمد
ممتحنا	جامعة وهران 2	أستاذة محاضرة أ	طاهير فاطمة الزهراء

السنة الجامعية: 2025 / 2026 .



قال تعالى

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

﴿ أَقْرَأْ بِاسْمِ رَبِّكَ الَّذِي خَلَقَ ﴾⁽¹⁾ خَلَقَ الْإِنْسَانَ مِنْ عَلَقٍ

﴿2﴾ أَقْرَأْ وَرَبُّكَ الْأَكْرَمُ ﴿3﴾ الَّذِي عَلَّمَ بِالْقَلَمِ ﴿4﴾

عَلَّمَ الْإِنْسَانَ مَا لَمْ يَعْلَمْ ﴿5﴾.

صدق الله العظيم.

سورة العلق

الآيات 1 - 5.

الإهداء

إلى من أوصاني الله بهما برا وإحسانا
" أمي " رحمة الله عليها، " أبي " اطل الله في عمره.
الذين زرعوا في قلبي بذور العلم والصبر، ورويا أحلامي بماء الدعاء والحنان.
فكانا الريح الدافعة في رحلتي الطويلة نحو النجاح.

إلى زوجتي العزيزة " أم مطر " رفيقة الدرب التي شاركتني الصعاب والافراح
وأضاءت لي الطريق فكانت نجما في ليالي الجهد والسهرة، مشاركة في كل خطوة
مؤنسة في كل لحظة.

إلى ورود قلبي أبنائي الغاليين "مطر" و "أمير"، اللذان يملآن قلبي بالفرح والأمل.

إلى إخواني و أخواتي حبا وتقديرا و وفاء .

إلى شهداء فلسطين الحبيبة وفي مقدمتهم
(أبن اختي :حمزة خيرى أبو سعود، وأبن أخي: هاني رامز أبو سعود).

و إلى زميلي بن علي لمنور وكل يد امتدت لمساعدتي في بناء هذا الإنجاز.

أهدي هذا العمل المتواضع رمزا للعتاء ، في سبيل علم يعلو و وطن يزدهر
إليكم جميعا بكل امتنان وود أهديه.

هاني مطر أبو سعود

الشكر والعرفان

أول من يستحق الشكر والإجلال في أي حال من الأحوال هو الله سبحانه وتعالى على توفيقه في إنجازي لهذه الدراسة، فالحمد لله والشكر لله أولاً وأخيراً ودائماً وأبداً،،،

كما أتقدم بالشكر والتقدير واعبر عن عميق أمتناني للأستاذ الدكتور عباسة طاهر المحترم لتفضله بالإشراف على هذه الأطروحة، فجهوده الدؤوبة في التوجيه والإرشاد ودقة تعليقاته ونصائحه السديدة، كانت بمثابة الدليل الذي أثار طريقي وسهل مسيرتي نحو أنجاز هذا العمل، فجزاه الله عني خير الجزاء،،،

كما أتقدم بجزيل الشكر للسادة الدكاترة الأكارم أعضاء لجنة المناقشة، كل باسمه ولقبه، على قبولهم الكريم لمناقشة هذه الدراسة وتقييمها وتصويبها، فلکم مني كل الاحترام والعرفان.

وأنتقدم بجزيل الشكر لمدير جامعة عبد الحميد بن باديس (مستغانم) المحترم، ولعميد كلية الحقوق والعلوم السياسية الاستاذ فنينخ عبدالقادر المحترم، ولنائب عميد كلية الحقوق الاستاذ بن عديدة نبيل المحترم، ولجميع أساتذة ودكاترة كلية الحقوق والعلوم السياسية— مستغانم، ولجميع القائمين على إدارة هذه الكلية بما فيهم العاملين في مكتبة الكلية لما قدموه من خدمات لي أثناء أعداد هذا العمل.

وأخيراً أتقدم بالشكر والعرفان إلى كل من عرفني وعرفته.

وبارك الله فيكم جميعاً.



شهد العالم خلال العقود الأخيرة ثورة رقمية غير مسبوقة أثّرت في مختلف مناحي الحياة، وأصبحت النظم المعلوماتية الركيزة الأساسية لعمل الحكومات والمؤسسات والشركات والأفراد، ولا ريب أن لهذه الثورة آثاراً إيجابية واسعة امتدت لتشمل جميع جوانب الحياة، إذ أصبحت القطاعات المختلفة تعتمد اعتماداً أساسياً على الأنظمة المعلوماتية في أداء أنشطتها، لما توفره من سرعة ودقة في جمع المعلومات وتخزينها ومعالجتها، بالإضافة إلى سهولة تداولها وتبادلها بين الأفراد والمؤسسات داخل الدولة الواحدة أو بين الدول، كما تحولت هذه الأنظمة إلى مستودع حيوي للمعلومات الشخصية والمالية للأفراد، فضلاً عن كونها خزاناً لأسرار الدول في المجالات العسكرية والصناعية والاقتصادية، ما يعكس أهميتها البالغة في العصر الرقمي.

وهنا ومع هذا الاعتماد المتزايد على التقنيات الرقمية وتبادل البيانات عبر الشبكات، برزت تحديات جديدة تتعلق بسلامة المعلومات، وحماية البنية التحتية الرقمية، والحدّ من الجرائم المعلوماتية التي تتنامى بوتيرة سريعة وتزداد تعقيداً واتساعاً، ولم يعد تهديد الأمن المعلوماتي مسألة تقنية فحسب، بل أصبح قضية ذات أبعاد قانونية واقتصادية وسياسية تتطلب إطاراً تشريعياً واضحاً واستجابة دولية مشتركة.

إذ ولدت الثورة المعلوماتية نمطاً جديداً من الجرائم يُعرف بـ"الجريمة المعلوماتية"، والتي تعد من أخطر السلبات المصاحبة للتقدم التكنولوجي، بل وأعادت تشكيل الجرائم التقليدية نفسها، محولة إياها من أشكالها المألوفة إلى أفعال إجرامية ذات أبعاد مبتكرة تعتمد على استغلال الأنظمة المعلوماتية، وقد أصبحت هذه الجرائم تهدد القيم الأساسية للأفراد والمؤسسات والدول، كما تمثل أخطر التحديات للنظم المعلوماتية ذاتها، إذ يمكن أن تتسبب في شلل كامل للأنظمة المدنية والعسكرية، واختراق المنظومات المالية والمصرفية، وإتلاف المعدات الحيوية، ونتيجة لذلك، تركت هذه الجرائم أثراً عميقاً في النفوس، مؤلدة شعوراً متزايداً بعدم الثقة تجاه التعامل مع الثورة الرقمية والاستفادة من إمكانياتها.

وتعود جذور جرائم النظم المعلوماتية إلى البدايات الأولى لاستخدام الحاسوب في أربعينيات وخمسينيات القرن العشرين، حين اقتصرَت على محاولات بسيطة للتلاعب بالأنظمة الكبيرة في المختبرات العسكرية والجامعات، قبل أن تتطور في سبعينيات وثمانينيات القرن الماضي مع ظهور الشبكات الأولى مثل ARPANET وظهور الفيروسات البدائية وعمليات الاختراق الموجهة نحو المؤسسات الحكومية والمصرفية، ومع الانتشار الواسع للإنترنت في تسعينيات القرن العشرين، انتقلت الجريمة المعلوماتية من نطاق محدود إلى ظاهرة عالمية، وهكذا تطورت جرائم النظم المعلوماتية من مجرد تجارب تقنية محدودة إلى تهديد عالمي متعدد الأبعاد، عابر للحدود، يواكب تطور التكنولوجيا ويستدعي استجابة قانونية دولية ووطنية ديناميكية وفعّالة.

وفي هذا السياق، سعت الدول إلى تطوير تشريعات وطنية تنظّم أمن المعلومات، وتحدد المسؤوليات القانونية، وتكافح الاعتداءات الإلكترونية بمختلف صورها، كما برزت الحاجة إلى اتفاقيات ومعايير دولية تتسق الجهود بين الدول وتوحّد الرؤى وتوفّر آليات فعّالة للتعاون العابر للحدود، خاصة أن الجرائم المعلوماتية غالباً ما تتجاوز النطاق الإقليمي التقليدي للسلطات القضائية.

فبرزت الحاجة الملحة إلى وضع إطار قانوني دولي قادر على مواكبة هذا التطور ووضع قواعد مشتركة للتصدي للمخاطر الناشئة، وفي هذا السياق جاءت اتفاقية بودابست لمكافحة الجرائم المعلوماتية بوصفها أول وثيقة دولية مخصّصة بشكل شامل لتنظيم الجريمة الإلكترونية وتعزيز التعاون بين الدول في هذا المجال.

لقد جاءت هذه الاتفاقية نتيجة مخاوف متنامية من قدرة جرائم النظم المعلوماتية على تجاوز الحدود الوطنية، مما جعل التشريعات المحلية عاجزة وحدها عن مواجهتها، حيث بادر مجلس أوروبا (Council of Europe) إلى إطلاق مفاوضات دولية منذ منتصف التسعينيات، شاركت فيها عدة دول غير أوروبية، معتمدة منهجاً متعدد الأطراف هدفه وضع قواعد موحدة تُيسّر الملاحقة الجنائية، وتتسق آليات تبادل الأدلة، وتوفر أدوات استجابة سريعة للجرائم التي تتم في فضاء لا تعترف حدوده بالسيادة التقليدية.

وانعقدت المفاوضات بحساسية عالية نظراً لتضارب القيم بين الأنظمة القانونية المختلفة، خاصة فيما يتعلق بحدود التدخل في الخصوصية، وحرية التعبير، والسيادة الرقمية، والاختلافات في تعريف الجريمة المعلوماتية بين دولة وأخرى، ورغم ذلك، تمكنت الدول المفاوضة من التوصل إلى صيغة توافقية اعتمدت رسمياً في بودابست بتاريخ 23 نوفمبر 2001، لتصبح منذ ذلك الحين مرجعاً عالمياً في مكافحة جرائم نظم المعلومات، وتستمر في استقطاب دول جديدة للتصديق والانضمام إليها.

وعلى المستوى العربي أدركت جامعة الدول العربية الحاجة إلى إيجاد إطار قانوني عربي موحد لمكافحة الجرائم المعلوماتية، فصدر المشروع القانوني للاتفاقية العربية لمكافحة الجرائم الإلكترونية عام 2010، بهدف توحيد التشريعات الوطنية وتوفير أدوات قانونية فعالة للتصدي لهذه الجرائم، وسعت الاتفاقية إلى حماية الأفراد والمؤسسات وتعزيز الأمن الرقمي، عبر تعريف الجرائم الإلكترونية ووضع معايير للتعاون القضائي والأمني بين الدول العربية، فضلاً عن تعزيز الوقاية والتحقيق والملاحقة القانونية، وتكتسب هذه الاتفاقية أهمية خاصة، كونها تشكل أول محاولة رسمية على مستوى الجامعة العربية لتوحيد المفاهيم القانونية المتعلقة بالجرائم الإلكترونية، ولكن بالرغم من ذلك مازالت تواجه الدول العربية تحديات عملية وقانونية في تطبيق الاتفاقية، نظراً لاختلاف مستويات التطور الرقمي والتشريعي بينها وحاجة الأنظمة القانونية إلى تحديث مستمر لمواكبة تقنيات الجريمة الجديدة.

فالجزائر عملت على تطوير إطار قانوني متخصص لمكافحة الجرائم المعلوماتية، وكان القانون رقم 04-09 الصادر في 5 أوت 2009¹ حجر الزاوية في هذا المسعى، فقد نص هذا القانون على تعريف الجرائم المرتبطة بتكنولوجيا المعلومات والاتصال، وحدد إجراءات الوقاية والتحقيق، بما يضمن حماية الأفراد والمؤسسات من الأفعال الإجرامية المرتكزة على التكنولوجيا الرقمية، ويُعد هذا القانون أول خطوة رسمية لتجريم الأفعال التي لم تكن مغطاة بالقوانين التقليدية،

1- القانون رقم 04-09 والمؤرخ في 05/08/2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والمنشور بالجريدة الرسمية عدد 47 بتاريخ 2009/08/16.

مثل اختراق الأنظمة الحاسوبية، التلاعب بالبيانات، أو استخدام الإنترنت كوسيلة لارتكاب الجرائم.

وفي نفس السياق عملت المملكة العربية السعودية على إصدار نظام مكافحة جرائم المعلوماتية بموجب المرسوم الملكي رقم م/17 بتاريخ 8 ربيع الأول 1428هـ، الموافق 26 مارس 2007، بهدف تنظيم مواجهة الجرائم الإلكترونية وحماية النظم المعلوماتية والأفراد والمؤسسات من الاستخدام غير المشروع للتكنولوجيا الرقمية، إذ يغطي النظام مجموعة واسعة من الجرائم، مثل الدخول غير المصرح به إلى أنظمة الحاسوب، الإتلاف أو التلاعب بالبيانات، الاحتيال الإلكتروني، ونشر المحتوى المخالف للأداب العامة أو الدينيّة، بما في ذلك دعم الأنشطة الإرهابية، ويمثل هذا النظام خطوة أساسية في تأمين البيئة الرقمية في السعودية، كما يعكس حرص الدولة على مواءمة سياساتها الوطنية مع المعايير الدولية للأمن المعلوماتي وحماية البيانات، مع مراعاة التوازن بين الأمن القومي وحرية التعبير الرقمي.

• أهمية الموضوع:

تكمن الأهمية العلمية لهذه الدراسة "حماية النظم المعلوماتية وفق الاتفاقيات الدولية والتشريعات الوطنية" في كونها تتناول واحدة من أكثر القضايا المعاصرة حساسية وتعقيداً في مجال القانون والتقنية، وهي حماية النظم المعلوماتية في ظل تزايد التهديدات المعلوماتية وانتشار الجرائم الإلكترونية على الصعيدين الوطني والدولي، إذ لم تعد النظم المعلوماتية مجرد أدوات تقنية مساعدة، بل أصبحت العمود الفقري للبنى الاقتصادية، والمؤسسات الحكومية، والبنى التحتية الحيوية، ما يجعل أي اختراق أو استغلال لها يشكل تهديداً مباشراً للأمن القومي واستقرار الدولة، وتكتسب الدراسة أهميتها أيضاً من خلال التركيز على الربط بين الإطار القانوني الدولي والتشريعات الوطنية، الأمر الذي يساهم في كشف نقاط القوة والقصور في حماية الأنظمة المعلوماتية، وتقديم حلول عملية لتجاوز الثغرات القانونية والتطبيقية، علاوة على ذلك، فإن هذه الدراسة تمثل إضافة علمية قيمة من خلال تقديم توصيات ملموسة لتعزيز منظومة الأمن المعلوماتي، بما يحقق توازناً بين حقوق الأفراد واحتياجات الدولة، ويواكب التطورات التقنية

المستمرة، وبالتالي فهي تساهم في تعزيز الأمن الرقمي والاستراتيجي للدول، كما وتساهم في تطوير رؤية قانونية متكاملة تضمن أمن الفضاء المعلوماتي وتدعم الجهود الوطنية والدولية في مواجهة المخاطر المعلوماتية المستمرة والمتزايدة.

ومن جانب آخر، تسلط الضوء على أهم الاتفاقيات الدولية والقوانين العربية الحديثة في مجال مكافحة الجريمة المعلوماتية ومثال ذلك قوانين دول " الجزائر، السعودية، الأردن، الإمارات" التي تناولت حديثاً معالجة جرائم النظم المعلوماتية في قوانينها الوطنية وقدمت نصوصاً تجريمية شاملة وحديثة تتماشى مع حداثة الجريمة.

• أسباب اختيار الموضوع:

- بالنسبة للأسباب الذاتية: جاء اختياري لموضوع حماية النظم المعلوماتية وفق الاتفاقيات الدولية والتشريعات الوطنية من جملة أسباب ذاتية ترتبط باهتمامي المتزايد بمجال القانون الرقمي وتطوراتهِ المتسارعة، ورغبتي في التعمق في أحد أهم التحديات القانونية المعاصرة التي أصبحت تمسّ مختلف قطاعات الدولة، فقد شكّل الاطلاع المستمر على القضايا الحديثة المتعلقة بالجرائم الإلكترونية بمناسبة عملي في مجال المحاماة وما تثيره من إشكالات قانونية معقدة دافعاً قوياً للاهتمام بهذا المجال، خاصة في ظل الفجوة الواضحة بين التطور التقني السريع وبين قدرة التشريعات على مواكبته، كما أن ميلي الشخصي لدراسة الموضوعات القانونية الحديثة وغير التقليدية، وما تحمله من أبعاد تحليلية عميقة، أسهم في توجيه اهتمامي نحو هذا الموضوع تحديداً، إضافة إلى ذلك، فإن احتكاكي الأكاديمي والميداني عزز لديّ القناعة بأن هذا المجال لا يزال بحاجة إلى دراسات معمقة تسهم في تطوير المعرفة القانونية وتقديم حلول موضوعية قابلة للتطبيق، الأمر الذي جعل تناول هذا الموضوع خياراً مناسباً يلائم ميولي العلمية ويستجيب لتطلعاتي البحثية.

- أما بالنسبة للأسباب الموضوعية: تتبع الأسباب الموضوعية لاختيار موضوع " حماية النظم المعلوماتية وفق الاتفاقيات الدولية والتشريعات الوطنية " من الأهمية المتزايدة التي اكتسبها الأمن المعلوماتي في السنوات الأخيرة، وما يطرحه من تحديات قانونية معقدة نتيجة تزايد حجم الجرائم المعلوماتية وتطور أساليبها بشكل يفوق قدرة العديد من الدول على المواكبة التشريعية، كما أن اتساع الاعتماد على التقنيات الرقمية الحديثة في مختلف القطاعات الحيوية—مثل المالية والصحة والطاقة والإدارة الحكومية—جعل من حماية النظم المعلوماتية مسألة ذات بعد استراتيجي، تتطلب دراسة معمقة للإطار القانوني الذي ينظمها، إذ أنه تم ربط هذه الدراسة من الناحية القانونية بالشق الموضوعي لحماية النظم المعلوماتية موضوعيا "تشريعيا"، ويضاف إلى ذلك وجود فجوة واضحة بين الاتفاقيات الدولية التي تحاول وضع معايير موحدة لمواجهة جرائم نظم المعلومات، وبين التشريعات الوطنية التي تختلف في مدى شموليتها وفعاليتها في التطبيق، ما يستدعي القيام ببحث علمي يوضح نقاط الالتقاء والاختلاف بينها، كما أن عدم كفاية الدراسات العربية المتخصصة في هذا المجال، مقارنة بالتطورات التقنية والقانونية المتسارعة، شكّل دافعاً موضوعياً لتناول هذا الموضوع بهدف سد النقص المعرفي وتقديم تحليل قانوني يسهم في تطوير منظومة الحماية على الأقل على المستوى الوطني.

• أهداف الموضوع:

تهدف هذه الدراسة إلى تحديد وفهم الإطار القانوني لحماية النظم المعلوماتية من منظور موضوعي بحث، عبر التركيز على نصوص الاتفاقيات الدولية والتشريعات الوطنية وتقييم فعاليتها في مواجهة الجرائم الإلكترونية، ويكمن الهدف الأول في تحليل الاتفاقيات الدولية، مثل اتفاقية بودابست والاتفاقية العربية لمكافحة الجرائم الإلكترونية، بهدف تقييم مدى شموليتها ودقتها في تنظيم الجرائم المعلوماتية وتوحيد المعايير القانونية بين الدول، أما الهدف الثاني، فهو فحص التشريعات الوطنية المعتمدة في الدراسة المعمول بها في حماية النظم المعلوماتية، للكشف عن مواطن القوة والقصور، وبيان مدى انسجامها مع المعايير الدولية، ويهدف الهدف الثالث إلى

تقييم الجوانب القانونية والتطبيقية لهذه التشريعات، بما في ذلك تحديد المسؤوليات الجنائية والإجراءات القانونية المعتمدة ومدى قدرة التشريعات على مواجهة التهديدات الإلكترونية المستحدثة وأخيراً، تسعى الدراسة إلى تقديم توصيات قانونية دقيقة وموضوعية لتعزيز فعالية الإطار القانوني الوطني والدولي، بما يحقق حماية متكاملة للنظم المعلوماتية، مع التركيز التام على البعد القانوني دون الانحراف إلى الجوانب التقنية أو الاجتماعية.

• إشكالية الموضوع:

على الرغم من تعدد المبادرات الدولية واعتماد العديد من الدول تشريعات تنظم حماية للنظم المعلوماتية والأمن المعلوماتي، لا يزال التهديد المعلوماتي يمثل تحدياً متصاعداً يتجاوز القدرات القانونية التقليدية، وي طرح هذا الواقع عدة تساؤلات حول مدى فعالية الأطر القانونية—الدولية والوطنية—في تحقيق حماية حقيقية للنظم المعلوماتية، خاصة في ظل الطبيعة العابرة للحدود للجريمة الإلكترونية، وتعدد الفاعلين غير الحكوميين، وتطور التقنيات المستخدمة في الاعتداءات المعلوماتية.

ومن هنا تنطلق إشكالية هذه الدراسة من السؤال الرئيس الآتي:

إلى أي حد تسهم الاتفاقيات الدولية والتشريعات الوطنية في حماية النظم المعلوماتية، وما مدى كفايتها وفعاليتها في مواجهة التحديات المتجددة للأمن المعلوماتي؟

• الدراسات السابقة:

أنت الدراسات السابقة لموضوع بحثنا المتمثل في " حماية النظم المعلوماتية وفق الاتفاقيات الدولية والتشريعات الوطنية " في سياق عملية البحث عما له علاقة أو ارتباط بموضوع الدراسة، إذ لم أجد مواضيع في هذا السياق نفسه، إلا أن يوجد عدد محدود من الدراسات التي تتقارب مع بعض جوانب هذه الدراسة، إلا أنها تظل محدودة في التفاصيل والعمق، ويرجع ذلك أساساً إلى أن الغالبية العظمى من الأبحاث السابقة قد ركزت على الجرائم المعلوماتية أو الإلكترونية بشكل عام، أو انحصرت في استكشاف إحدى مظاهرها دون الأخرى،

في حين اهتمت فئة أخرى بآليات مواجهة هذه الجرائم مع التركيز الرئيسي على الجوانب الإجرائية والتنفيذية، ومن بين هذه الدراسات نذكر:

- بشأن عبد النور، الجوانب الموضوعية لمعالجة الجريمة المعلوماتية، أطروحة لنيل شهادة الدكتوراه في الحقوق، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 01، الجزائر، السنة الجامعية 2017-2018.

- ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة لنيل شهادة الدكتوراه في الحقوق، قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، الجزائر، السنة الجامعية 2015-2016.

- بلال بن جامع، الجرائم المعلوماتية على شبكة الانترنت دراسة حالة جامعة عبد الحميد مهري قسنطينة 2، أطروحة لنيل شهادة الدكتوراه علوم في علم المكتبات والتوثيق، معهد علم المكتبات والتوثيق، جامعة قسنطينة 2، الجزائر، السنة الجامعية 2016-2017.

- بعقيقي عبير، مكافحة الجريمة المعلوماتية في التشريعين الجزائري و الإماراتي دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد خضير بسكرة، الجزائر، العام الدراسي 2017-2018.

• الصعوبات التي اعترضت الموضوع:

واجهت هذه الدراسة عدداً من الصعوبات التي أثّرت على مسار إنجازها، سواء على الصعيد العلمي أو العملي، فقد تمثلت إحدى أبرز الصعوبات في قلة المراجع العربية المتخصصة في مجال حماية النظم المعلوماتية، ما اضطرني إلى الاعتماد بشكل أكبر على المقالات العلمية والبحوث والوثائق الدولية لسدّ هذا النقص، كما برزت صعوبة أخرى تتعلق بتعدد وتباين التشريعات الوطنية بين الدول، سواء من حيث تعريف الجريمة المعلوماتية أو من حيث آليات التجريم والعقاب، مما تطلّب دقة عالية في إجراء المقارنات القانونية والتمييز بين المدارس التشريعية المختلفة، وكان لظروف جائحة كورونا تأثير واضح في الحد من القدرة على الوصول إلى بعض المكتبات والجهات البحثية، إضافة إلى تعطيل العديد من الأنشطة الأكاديمية

التي كان يمكن أن أشارك فيها وتدعم الجانب المعرفي للدراسة، وإلى جانب ذلك، واجهت الدراسة تحديات مرتبطة بـ الظروف العائلية الصعبة التي رافقت فترة البحث، وما فرضته من ضغوط نفسية وزمنية أثّرت في وتيرة الإنجاز، كما لا يمكن إغفال تأثير الحرب في غزة وما رافقها من أوضاع إنسانية صعبة، وصعوبات في التركيز والاستمرار في العمل البحثي بشكل منتظم، وعلى الرغم من هذه التحديات مجتمعة، فقد حرصت على تجاوزها بالإصرار والمتابعة، وتنظيم الوقت، وتنويع مصادر البحث، والاعتماد على التحليل القانوني المقارن، والاستناد إلى أحدث ما توفر من مراجع موثوقة بما يضمن تحقيق معالجة علمية دقيقة ومتكاملة للموضوع.

• المناهج المعتمدة في الموضوع:

1- المنهج التحليلي القانوني:

الوصف: حيث اعتمد الباحث على تحليل النصوص القانونية والاتفاقيات الدولية المتعلقة بحماية النظم المعلوماتية.

الأهداف: فهم محتوى النصوص القانونية والالتزامات الدولية، تفسير البنود القانونية وربطها بمستجدات الجرائم المعلوماتية، وذلك بدراسة النصوص القانونية، القوانين الوطنية، الاتفاقيات الدولية، والأحكام القضائية.

2- المنهج المقارن:

الوصف: مقارنة الاتفاقيات الدولية مع التشريعات الوطنية المختلفة لتحديد نقاط الالتقاء والاختلاف.

الاهداف: تقييم مدى انسجام التشريعات الوطنية مع المعايير الدولية واستخلاص أفضل الممارسات القانونية الدولية لتطوير التشريعات الوطنية مثل تحليل قوانين الجزائر والسعودية والاردن والامارات.

3- المنهج الوصفي:

الوصف: وصف الوضع القانوني الحالي للنظم المعلوماتية على المستوى الدولي و الوطني.
الاهداف: تقديم خلفية موضوعية حول القوانين والاتفاقيات، وتسهيل الضوء على الثغرات والمشكلات الموضوعية والتطبيقية في النصوص القانونية، وتقديم أمثلة ملموسة لدعم التحليل القانوني والنقدي.

• خطة البحث:

لقد ارتأينا تقسيم هذه الدراسة إلى بابين، يحتوي كل باب على فصلين، وكل فصل من هذه الأبواب على مبحثين، ولكل مبحث ثلاثة مطالب، ولكل مطلب منها فروع، وهذا بالإضافة إلى المقدمة والخاتمة وقائمة المصادر والمراجع العربية والأجنبية وقائمة الملاحق، وجاء التقسيم كالآتي:

- جاء الباب الأول بعنوان "الإطار المفاهيمي للنظم المعلوماتية"، يعالج النظم المعلوماتية بمفهومها العام ومقسما إلى فصلين، خُصص الفصل الأول فيه لبيان النظم المعلوماتية بالمفهوم العلمي والتقني، بداية من التعريف اللغوي و الاصطلاحي وتمييز المعلومات عن شبيهاتها مع تحديد طبيعتها القانونية، إضافة إلى تناول النظم المعلوماتية بالمفهوم التقني والجنائي لتحديد مفهوم النظم المعلوماتية ومكوناتها المادية وتحديد جرائم نظم المعلومات وخصائصها وارتباطاتها وسمات و دوافع مرتكبيها، أما الفصل الثاني فتناول نظامها القانوني وتقسيماتها تبعا لدورها في الجريمة أو لعلاقتها بالنظام المعلوماتي، كما بينا تصنيفاتها حسب الآراء الفقهية وحسب رأي الوكالات الدولية المتخصصة، بالإضافة إلى علاقتها بالجريمة المنظمة.

- أما الباب الثاني فقد جاء بعنوان: "جرائم النظم المعلوماتية والآليات الدولية لحمايتها"، ويتضمن تفصيل دقيق لجرائم النظم المعلوماتية وبدوره مقسم إلى فصلين، تناولنا في الفصل الأول جرائم النظم المعلوماتية المرتكبة ضد النظام المعلوماتي ويشمل عدد من الجرائم كالولوج غير المشروع والاعتراض غير المشروع والإتلاف المعلوماتي، أما الفصل الثاني فتناول جرائم نظم المعلومات المرتكبة بواسطة النظام المعلوماتي وتشمل عدد من الجرائم كالتزوير المعلوماتي

والاحتيال المعلوماتي واستغلال الاطفال في الجرائم الاباحية، وجريمة التعدي على الملكية الفكرية المعلوماتية.

وانتهت هذه الدراسة بخاتمة احتوت على مجموعة من النتائج التي توصلت إليها هذه الدراسة، وتتضمن أيضا مجموعة من التوصيات والاقتراحات الهامة والموجهة إلى الجهات المعنية في مكافحة جرائم نظم المعلومات.

الباب الأول:

الإطار المفاهيمي للنظم

المعلوماتية.

تعد النظم المعلوماتية جزءاً أساسياً من البنية التحتية للعديد من الدول والمؤسسات والمنظمات في العالم، فهي تلعب دوراً حيوياً وحاسماً في تحقيق التنمية والتقدم للدول، بما تشكله من نظاماً متكامله تهدف إلى جمع وتخزين ومعالجة وتوزيع المعلومات بطريقة فعالة ومنظمة، بما يعزز ويطور الخدمات الحكومية للدول والمنظمات ويحسن كفاءة العمل ويحقق التنمية المستدامة.

ويتكون الإطار المفاهيمي للنظم المعلوماتية من مجموعة من المفاهيم والمكونات التي تعمل سوية لتحقيق أهداف النظام المعلوماتي، بما يعود بالنفع بالدرجة الأولى على العنصر البشري والبشرية جمعاء، وبما تشكله النظم المعلوماتية من بنية تقنية تحتية مكونة من شبكات الاتصال وأجهزة الحاسب الآلي والانترنت والبرامج وقواعد البيانات والتي تعمل معاً من أجل تخزين ومعالجة ونقل المعلومات.

ويهدف الإطار المفاهيمي للنظم المعلوماتية إلى توفير إحاطة فهم وتحليل وتقييم وهيكلية ومفهومية لفهم النظم المعلوماتية وعلاقتها المختلفة، من أجل الإلمام بجميع الجوانب المفاهيمية والقانونية والتقنية للنظم المعلوماتية، ولهذا ارتأينا في دراستنا إلى تقسيم هذا الباب إلى فصلين، الفصل الأول نبحث فيه عن النظم المعلوماتية بالمفهوم العلمي والتقني لندرس فيه مفهوم النظم المعلوماتية وتعريفاتها وتمييزها عن غيرها من المصطلحات، أما الفصل الثاني فحاولنا البحث فيه عن النظام القانوني لجرائم نظم المعلومات بما يشمل تقسيماتها وعلاقتها بالجرائم الأخرى ممثلة بالجريمة المنظمة وجرائم الإرهاب الإلكترونية، والتركيز على أهم وأخطر صورها التي ترتكبها الجماعات الإجرامية التقليدية أو الحديثة.

الفصل الأول : النظم المعلوماتية بالمفهوم العلمي والتقني.

أحاط بالنظم المعلوماتية شأنها في ذلك شأن كل ظاهرة جديدة العديد من التساؤلات التي تتعلق بتعريفها وتحديد مفهومها وخصائصها، وتحديد حجمها وهو الخطوة الأولى للتعرف على هذه الظاهرة من جميع جوانبها القانونية، وحيث تعددت مفاهيم وتعريفات النظم المعلوماتية وتباينت فيما بينها ضيقاً واتساعاً ما أسفر عن تعذر إيجاد فهم مشترك ودقيق للنظم المعلوماتية.

وفي هذا الفصل من الدراسة سنعرض مفهوم النظم المعلوماتية وسوف نحاول الوصول إلى التعريف الذي يتلاءم مع طبيعة نظم المعلومات وذلك بعد التعرض للاتجاهات المختلفة في تعريف النظم المعلوماتية بمفهومها العلمي والتقني ويتطلب ذلك التعرض للجوانب المحيطة بالنظم المعلوماتية والاتجاهات والآراء المختلفة في تعريفها، وتمييز المعلومات عن غيرها من شبيهاتها من المصطلحات فقهاً وقانوناً، وكذلك بيان مدلولها التقني ومكوناتها المادية وخصائصها، وسنتناول ذلك من خلا بحثين كما يلي:

- المدلول العلمي للنظم المعلوماتية.

المدلول التقني والجنائي للنظم المعلوماتية

المبحث الأول: المدلول العلمي للنظم المعلوماتية.

لعل مفهوم النظم المعلوماتية من أكثر المفاهيم جدلاً في الوسط الأكاديمي بتفرق الفقه حوله نظراً للتطور السريع والهائل للتكنولوجيا الحديثة واختلاف النظرة لفكرة المعلومات ومحتواها من وسط لآخر وبهذا يعتبر التعريف اللغوي والاصطلاحي أول باب يطرق لرفعه (المطلب الأول) وعرض مختلف التعريفات التي توصل لها الفقهاء واعتمدتها المنظومات التشريعية، وهنا اظهرت هذه التعاريف أنواع متعددة من المعلومات وشببياتها تختلف بعضها عن بعض من حيث الأنواع والخصائص (المطلب الثاني)، وهذا ما دعانا إلى دراسة الطبيعة القانونية للمعلومات (المطلب الثالث).

المطلب الأول: التعريف اللغوي والاصطلاحي للمعلومات.

كما سبق الإشارة إليه أن النظم المعلوماتية تعرضت للكثير من محاولات التعريف لتحديد ماهيتها وأدواتها على مدي السنين التي واكبت التطور التكنولوجي ومسألة الخلافية لا يفسر المجهودات المبذولة لحلها إلا ما يشكله التعريف من ضرورة ملحة على المستوى الدولي والقانوني (الفرع الأول) ثم أن الخلاف هذا لا يظهر على المستوى اللغوي (الفرع الثاني) بقدر ما هو بارز عند آراء الفقه والفقهاء.

الفرع الأول : تعريف المعلومات في اللغة.

قد يبدو للوهلة الأولى أنه لا صعوبة في تعريف المعلومات كونها منتشرة بشكل كبير في مجالات الحياة كافة، غير أنه بظهور تكنولوجيا الحاسبات و وسائل الإتصال المتقدمة وشبكات المعلومات جعل لها بعد آخر واكساها حلة جديدة بل تسمية جديدة فأصبحت تعرف بالمعلوماتية إشارة إلى ارتباطها بهذه التكنولوجيا الحديثة¹، هذه القيمة العظيمة للمعلومات تدفعنا إلى أن نتناول تعريفها.

1- دلخار صلاح بوتاني، الحماية الجنائية الموضوعية للمعلوماتية، دار الفكر الجامعي، الاسكندرية، جمهورية مصر العربية، الطبعة الاولى، 2016، ص 14.

أولاً: التعريف اللغوي للمعلومات.

المعلومات كلمة لم تفتأ أذاننا تخفي يوماً سماع صداها يدوي في آفاق وسائل الاتصال المسموعة، ولم تعد أبصارنا من رؤية حروفها مطبوعة على صفحات وشاشات وسائل الاتصال المقروءة والمرئية، ولم تخل مجالسنا ومحافلنا من تجاذب أطراف الحديث عن التغني بأهميتها البالغة ودورها الحاسم وأثرها الواسع في مختلف جوانب حياتنا¹.

وبالرجوع إلى القرآن الكريم كونه مصدر اللغة العربية وجامع ألفاظها، وحيث أنه قديم قدم الإنسانية فإنه احتوى على ألفاظ المعلومات والعلم في العديد من الآيات القرآنية، إذ قال سبحانه وتعالى " وَتَعَلَّمَ آدَمُ الْأَسْمَاءَ كُلَّمَا نُفِثَ مِنْ عَرْصِهِمْ عَلَى الْمَلَكَةِ فَقَالَ أَنْبِئُونِي بِأَسْمَاءِ هَؤُلَاءِ إِنْ كُنْتُمْ صَادِقِينَ (31) قَالُوا سُبْحَانَكَ لَا يِلْمُ لَنَا إِلَّا مَا عَلَّمْتَنَا إِنَّكَ أَنْتَ الْعَلِيمُ الْحَكِيمُ (32) قَالَ يَا آدَمُ أَنْبِئْهُمْ بِأَسْمَائِهِمْ فَلَمَّا أَنْبَأَهُمْ بِأَسْمَائِهِمْ قَالَ أَلَمْ أَقُلْ لَكُمْ إِنِّي أَعْلَمُ غَيْبِ السَّمَاوَاتِ وَالْأَرْضِ وَأَعْلَمُ مَا تُبْدُونَ وَمَا كُنْتُمْ تَكْتُمُونَ"²، وكذلك قال تعالى " الرَّحْمَنُ (1) عَلَّمَ الْقُرْآنَ (2) خَلَقَ الْإِنْسَانَ (3) عَلَّمَهُ الْبَيَانَ (4)"³، من ما سبق يتضح بأن كلمة (علم) ، هي لفظ مذكور في القرآن الكريم لدلالة على الإحاطة ببواطن الأمور والوعي والادراك والمعرفة.

المعلومات جمع كلمة معلومة، وهي أسم مفعول مؤنث لكلمة العلم وقد ألحقت به التاء المربوطة للدلالة على صيغة المبالغة، ومعناها في السياق اللغوي مستمد من كلمة "علم"، ودلالاتها تدور حول المعرفة القابلة للتبادل والاكتساب، فمثلاً يقال "أعلم فلانا الخبر" أي أخبره به بمعنى إبلاغه، و "أعلم فلانا أمراً واقعاً" أي جعله يعلمه ويدرك، ويعتبر العلم ضد الصريح للجهل، و "علمت الشيء" أي أعلمه علماً أي عرفه⁴.

1- خالد ممدوح أبراهيم، أمن الجريمة الالكترونية، الدار الجامعية، الإسكندرية، 2008، ص 25.

2 - سورة البقرة الآيات 31-32.

3 سورة الرحمن الآيات 1-4.

4- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية بيروت، لبنان، الطبعة الأولى 2012، ص 6.

فالمعلومة من الفعل "علم"، "وعلم بالشيء" "شعر به"، "وعلم الأمر وتعلم" أي أتقن الأمر، "وعلم الرجل" أي أخبره، واجب أن يعلمه أي أن يخبره¹، فهي مادة غنية بالكثير من المعاني كالعلم والإحاطة بباطن الأمور والوعي والادراك واليقين والارشاد وتحديد المعالم.

وبالتعريض على تعريف المعلومات في اللغات الأجنبية، نجد أن المعلومات في اللغة الإنجليزية مشتقة من كلمة "INFORMATION" وهي مشتقة من كلمة "INFORM" بمعنى يبلغ أو يعلم، وتحمل كلمة "Information" معنى (معلومات - استعلامات - إعلام - إطلاع - معرفة - أنباء - إستخبارات) وتصنف ضمن أقسام الكلام على أنها أسم "Noun" والرمز الصوتي لها (r) mer(e) inf.

أما اللغة الفرنسية يشير مصطلح "Information" على العملية الاتصالية التي ترمي إلى نقل وتوصيل إشارة أو محتوى أو الاعلان عنه، وإتخاذ وظيفتها في نقل المعارف، إذا فالمعلومة حالة ذهنية وظاهرة كونية جوهرية، لا نستطيع التعرف على كنهها وجه اليقين إلا أننا ندرك أثرها الملموس، وأثرها موجود في كافة المجالات المتعلقة بالإنسانية²، إذ أصبحت المعلومات في عصرنا الحديث كنز عظيم واستراتيجي لاسيما في ظل وجود تكنولوجيا المعلومات التي أسهمت بفاعلية كبيرة في معالجة وتخزين، وبث المعلومات³، وبالتالي فامتلاكها والسيطرة عليها يشكل مصدر قوة لصاحبها.

ثانيا: التعريف الاصطلاحي للمعلومات.

والمصطلح هو ما أصطلح عليه القوم، وغالبا تتمثل التعريفات الاصطلاحية فيما ورد في معاجم و موسوعات التخصص، إلا أنه فيما يتعلق بالمعلومات لا يوجد إجماع في الفقه على

1 - بلال بن جامع، الجرائم المعلوماتية على شبكة الانترنت دراسة حالة جامعة عبد الحميد مهري قسنطينة2، أطروحة لنيل شهادة الدكتوراه علوم في علم المكتبات والتوثيق، معهد علم المكتبات والتوثيق، جامعة قسنطينة2، الجزائر، السنة الجامعية 2016-2017، ص 54.

2- ضياء مصطفى عثمان، السرقة الالكترونية، دراسة مقارنة، دار النفائس للنشر والتوزيع، الاردن، الطبعة الاولى 2011، ص 94.

3- وعرفت المعلومة في قاموس المعلوماتية بأنها " الركيزة الاساسية لنقل المعرفة" أو بيانات تمت معالجتها من أجل تحقيق غاية معينة أو لاستعمال محدد"، رشدي محمد على محمد عيده، الحماية الجنائية الموضوعية للمعلومات عبر شبكة الانترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، 2013، ص 10-11.

تعريف جامع مانع للمعلومة، فقد اختلفت آراء الفقهاء في تناولهم هذا المصطلح، وفيما يلي بعض التعريفات الاصطلاحية:

عُرفت المعلومات وفقاً للمعجم الموسوعي لمصطلحات المكتبات والمعلومات أنها "البيانات التي تمت معالجتها لتحقيق هدف معين أو لاستعمال محدد، لأغراض اتخاذ القرارات، أي البيانات التي أصبح لها قيمة بعد تحليلها، أو تفسيرها، أو تجميعها في شكل ذي معنى والتي يمكن تداولها وتسجيلها ونشرها وتوزيعها في صورة رسمية أو غير رسمية وفي أي شكل"، وعرفت المعلومات كذلك على أنها المقومات الجوهرية في أي نظام للتحكم¹.

وكان التعريف المرجح أنها "مجموعة من الرموز أو الوقائع أو المفاهيم أو التعليمات القابلة لأن تكون محلاً للتبادل والاتصال، أو للتفسير والتأوي، أو للمعالجة سواء بواسطة الأفراد أو عبر الأنظمة الإلكترونية، وهي تتميز بدرجة عالية من المرونة، إذ يمكن تعديلها، أو تجزئتها وجمعها أو نقلها بوسائل و وسائل وأشكال مختلفة"².

وحاول الفقه من جانبه وضع تعريف للمعلومات من خلال بيان المعنى المقصود بها، إذ ذهب الفقيه الفرنسي "Fliry" في معرض محاولته تعريف المعلومة، إلى القول "أنه من الصعب إعطاء تعريف بسيط لفكرة المعلومة التي هي رسالة تحمل إلى من يتلقاها عددا من التعليمات".

بينما قدم الاستاذ "Mackaay" عام 1969 تعريفا للمعلومات بأنها "تلك التي تضيف شيئاً ما إلى النموذج العقلي وإلى الانطباع الذهني الذي نعرفه عن العالم الخارجي في لحظة معينة"³.

ويعرفها الأستاذ "Catala" بأنها "رسالة معبر عنها في شكل يجعلها قابلة للنقل أو الإبلاغ للغير، فهي تعبير يستهدف جعل رسالة قابلة للتوصيل إلى الغير بفضل علامة أو إشارة

1- رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الانترنت، مذكرة لنيل شهادة الماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة ابي بكر بلقايد، الجزائر، السنة الجامعية 2011-2012، ص 33.

2- رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائرية، أطروحة لنيل شهادة الدكتوراه علوم في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة ابي بكر بلقايد، الجزائر، السنة الجامعية 2017-2018، ص 25.

3- دلخار صلاح بوتاني، المرجع سابق، ص 17-18.

من شأنها أن توصل المعلومة للغير بالتعبير وتوصيله للغير يحقق وظيفة المعلومة وهي انتقال أو نقل المعرفة¹، والملاحظ هنا ان تعريفه واسعا للغاية.

الفرع الثاني: تعريف المعلومات في التشريع.

لم يكن التشريع غائبا عن النقاشات التي تدور حول تعريف المعلومات على مستوى الدول أو في نطاق الاتفاقيات الدولية بل سعى جاهدا لوضع تعريف للمعلومات، وكان من هذه المحاولات بسيطة بدايتاً إلا أنها بمرور الوقت أصبحت أكثر تطوراً، ونستعرضها فيما يلي:

أولاً: تعريف المعلومات في التشريعات الغربية.

كان المشرع الفرنسي في سباقاً، على الصعيد الغربي، في وضع تعريف للمعلومات أذ عرفها في المرسوم الصادر بتاريخ 22 ديسمبر 1981 المتعلق بإثراء المصطلحات المعلوماتية في فرنسا بأن " المعلومات إحدى عناصر المعرفة القابلة للأداء بموجب الاتفاق من أجل حفظها ومعالجتها وإيصالها للغير"²، كما تناول تعريف المعلومات القانون الصادر في 29 يوليو سنة 1982 المتعلق بالاتصالات السمعية والبصرية، حيث قدم أول تعريف عام للمعلومة، والذي ينظر إليها بوصفها " رنين صور الوثائق والبيانات أو الرسائل من أي نوع"، وعلى هذا الأساس تعنى المعلومة وتفهيم على أنها رمزا أو مجموعة من الرموز القادرة على الإفضاء إلى معنى و دلالة³.

أما المشرع الأمريكي فقد تناول تعريف المعلومات في قانون المعاملات التجارية الالكترونية لسنة 1999، حيث نصت الفقرة العاشرة من المادة الثانية على تعريفها بأنها " تشمل البيانات والكلمات والصور والأصوات والرسائل، إلى جانب برامج الكمبيوتر والبرامج المخزنة والموضوعة على الأقراص المرنة وقواعد البيانات أو ما يماثلها"⁴.

1- الفقيه الفرنسي "Catala" مذكور من قبل رصاع فتيحة، المرجع السابق، ص18.

2- محمد عطية علي محمد الرزازي، الحماية القانونية لقواعد البيانات في القانون المصري والتشريعات المقارنة، دار الجامعة الجديدة، مصر، سنة الطبع 2013، ص 102.

3- حسين محمد الغول، جرائم شبكة الانترنت والمسؤولية الجزائية الناشئة عنها - دراسة مقارنة، مكتبة بدران الحقوقية، لبنان، الطبعة الاولى 2017، ص 124.

4- رصاع فتيحة، المرجع السابق، ص 17.

ثانيا: تعريف المعلومات في التشريعات العربية.

عرف المشرع الأردني المعلومات في قانون المعاملات الالكترونية رقم 85 لسنة 2001 في المادة الثانية منه على أنها "البيانات والنصوص والصور والأشكال والأصوات والرموز وقواعد البيانات وبرامج الحاسوب وما شابه ذلك"، إضافة إلى ذلك عرفها في قانون المعاملات الالكترونية لسنة 2015 في المادة الثانية منه على أنها "البيانات أو النصوص أو الصور أو الرسوم أو الأشكال أو الأصوات أو الرموز أو قواعد البيانات وما شابه ذلك"، كما عرفها في قانون جرائم أنظمة المعلومات رقم 30 لسنة 2010 في المادة الثانية منه على أنها "المعلومات التي تمت معالجتها وأصبح لها دلالة".

ومن القوانين العربية أيضا التي عرفت المعلومات القانون الاتحادي لدولة الإمارات العربية المتحدة رقم 1 لسنة 2006 المتعلق بالمعاملات التجارية الإلكترونية في مادته الأولى بنصه على أنها "بيانات ومعلومات إلكترونية في شكل نصوص أو رموز أو أصوات أو رسوم أو صور أو برامج الحاسب الآلي أو غيرها"¹.

وفي إطار التشريعات العربية نص قانون التجارة الالكترونية البحريني رقم 28 لسنة 2002 في المادة الأولى منه أن المعلومات هي "البيانات والنصوص والصور والأشكال والأصوات والرموز وقواعد البيانات وبرامج الحاسوب وما شابه ذلك"².

أما المشرع الجزائري فقد عرف المعلومات في نص المادة الثانية الفقرة "ج" من القانون 04-09 المؤرخ في 05 اوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، بالقول بأن المعطيات المعلوماتية "أي عملية عرض للوقائع والمعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج التي تجعل من المنظومة المعلوماتية تؤدي وظيفتها"، ويلاحظ أن تعريف المشرع الجزائري يتسم بقدر من العمومية المفرطة، فهو تعريف يبتعد عن الدقة المطلوبة، ولا سيما في مجال تحديد تعريف

1- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، الجزائر، السنة الجامعة 2012-2013، ص 14.

2- دلخار صلاح بوتاني، المرجع سابق، ص 17.

المعلومة على وجه الخصوص، ومن ثم تبرز ضرورة إعادة صياغة تعريف المعلومة بما يضمن تمييزها وفصلها عن غيرها من المفاهيم المتقاربة، خصوصاً وأن ميدان المعلوماتية يتسم بالدقة ولا يحتمل الخلط أو التداخل بين المفاهيم¹.

ثالثاً: تعريف المعلومات في التشريعات الدولية.

• تعريف منظمة التعاون والتنمية الاقتصادية.

أخذت منظمة التعاون والتنمية الاقتصادية (OCDE)² في توصياتها الصادرة في 1992 و 1997 و 2002 والمتعلقة بأمن نظم المعلومات والشبكات بالترقية بين المعلومات والبيانات وذلك على أساس أن البيانات هي عبارة عن تمثيل أو تصور للحقائق أو المفاهيم أو التعليمات في شكل وقالب معياري يلاءم عملية الاتصال أو النقل أو التفسير أو الترجمة أو المعالجة بواسطة الحاسب الآلي، أما المعلومات فهي النتائج النهائية لهذه العملية، بما معناه أن البيانات هي المادة الخام التي تنقل وتعالج بوسائل معينة لتنتج عنها المعلومات³.

• تعريف اتفاقية بودابست.

عرفتها اتفاقية بودابست لمكافحة الجريمة المعلوماتية بتعريفها أنها تعني " كُلُّ تَمَثِيلٍ لِلْوَقَائِعِ أَوْ الْمَعْلُومَاتِ أَوْ الْمَفَاهِيمِ تَحْتَ أَيِّ شَكْلِ ، وَتَكُونُ مُهَيَّأَةً لِلْمُعَالَجَةِ الْآلِيَّةِ بِمَا فِي ذَلِكَ بَرْنَامَجٌ مُعَدٌّ مِنْ ذَاتِ الطَّبِيعَةِ وَيَجْعَلُ الْحَاسِبُ يُؤَدِّي الْمُهْمَةَ "4.

1- ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة لنيل شهادة الدكتوراه في الحقوق، قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، الجزائر، السنة الجامعية 2015-2016، ص 8.

2- منظمة التعاون الاقتصادي والتنمية OECD هي منظمة دولية تهدف إلى التنمية الاقتصادية وإلى إنعاش التبادلات التجارية، تتكون المنظمة من مجموعة من البلدان المتقدمة التي تقبل مبادئ الديمقراطية التمثيلية واقتصاد السوق الحر، أنشأت منظمة التعاون الاقتصادي والتنمية في 30 من سبتمبر سنة 1961 بعد ان حلت محل منظمة التعاون الاقتصادي الأوروبي OEEC التي أسست سنة 1948 للمساعدة على إدارة مشروع مارشال لإعادة إعمار أوروبا بعد الحرب العالمية الثانية وبعد فترة تم توسيعها لتشمل عضويتها بلدان غير أوروبية.

3- دلخار صلاح بوتاني، المرجع سابق، ص 18.

4- اتفاقية بودابست انبثقت عن اجتماع المجلس الأوروبي بتاريخ 23 نوفمبر 2001 تحت رقم 185 وذلك بوصف "اتفاقية بودابست لمكافحة الجريمة المعلوماتية، وهي اتفاقية تخص دول النطاق الأوروبي وكذلك دول

ومن الملاحظ أن ما يتبين من التعريفات السابقة أنها أعطت مفهوماً موسعاً للمعلومات من خلال إضافتها لعبارة "من أي نوع" كما في تعريف القانون الفرنسي أو بعبارة "ما شابه ذلك" كما في تعريف القانون الأمريكي، وهذا ربما تحسباً لما قد يظهر من أشكال جديدة للمعلومات وذلك لارتباطها بتقنية الحاسوب والتطور التكنولوجي الذي قد تظهر معه وسائل أخرى تنقل بواسطتها المعلومة، ويمكن القول من خلال التعاريف للمعلومة أنها أنصبت كلها عند مفهوم مشترك لها، إذ اعتبرت أن المعلومة هامة وفعالة ذات أهمية وتأثير على المجتمع ككل في العصر الحالي، لكونها تحيط بنا من كل جانب وتتعلق بكافة مجالات الحياة، وارتباطها بالتكنولوجيا أضاف من أهميتها ما جعلها محط انظار المجرمين.

وتتسم المعلومات بوجه عامة بقابليتها للدمج، إذ يمكن إضافة معلومة إلى أخرى لتتشأ عنهما معا معلومة جديدة تختلف من حيث قيمتها وأهميتها، وبالتالي من حيث مستوى الحماية القانونية الواجب توفيره لها مقارنة بما كانت عليه قبل عملية الدمج، فعلى سبيل المثال يُعد رقم حساب العميل لدى البنك معلومة ذات أهمية تستوجب الحماية، إلا أن إرفاقها بمعلومات أخرى كاسم البنك وأسم العميل وقيمة الرصيد، يؤدي إلى تضاعف قيمة المعلومة وأهميتها، الأمر الذي يستلزم من ناحية أخرى توفير درجة أعلى من الحماية¹.

العالم و دخلت حيز التنفيذ في 01 جويلية 2004، أيمن عبدالله فكري، جرائم نظم المعلومات دراسة مقارنة، دار الجامعة الجديدة، الاسكندرية، جمهورية مصر العربية، طبعة 2007، ص 43.

1- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، الطبعة الاولى 2005، بيروت لبنان، ص 99.

المطلب الثاني: تمييز المعلومات وخصائصها.

من خلال ما سبق من تعريفات للمعلومات من جانب فقهاء القانون والتشريعات الوطنية والدولية، ونظر إلى الأهمية الكبيرة للمعلومات و الاستغلال الكبير لها في الميدان العلمي والتكنولوجي وميدان البرامج الالكترونية وقواعد البيانات والحاسبات الآلية، فكان لا بد من التمييز بين المعلومة وبعض المصطلحات الشبيهة لها كالبيانات والمعطيات من جهة، والمعلومة وبرامج الكمبيوتر من جهة أخرى، وإبراز أنواعها وخصائصها.

الفرع الأول: تمييز المعلومات عن شبيهاتها من المصطلحات.

• أولاً: تمييز المعلومات عن البيانات والمعطيات.

البيانات من الفعل "بين" و "البيان" ما يبين به الشيء من الدلالة، أي أتضح، والبيانات مصدرها بين، حيث تعرف في اللغة العربية "حقائق أو أشياء معروفة يقينا ويمكن منها الوصول إلى نتيجة معينة"، وهي كلمات أو أرقام أو رموز، ويميز البعض في تعريف المعلومات بينها وبين البيانات فالبيانات والمعطيات تعبر عن الأرقام والكلمات والرموز أو الحقائق أو الاحصائيات الخام التي لا علاقة بين بعضها البعض، ولم تخضع بعد للتفسير أو التجهيز للاستخدام، إذ تخلوا من المعنى الظاهر في أغلب الأحيان¹، وتصف فكرة أو موضوع أو حدث أو هدف معين، ويتم تحويلها كمواد خام لغرض إستخراج معلومات معينة، أما المعلومات فهي المعنى الذي يستخلص من هذه المعطيات.

وقد عرفت الوكالة الفرنسية للتقييس (Afnor) المعطيات (Les donnees) بأنها "كُلُّ حَادِثٍ مَفْهُومٍ أَوْ تَعْلِيمَةٍ تَقْدُمُ فِي شَكْلِ مُنَقِّحٍ عَلَيْهِ قَابِلٍ لِلتَّبَادُلِ عَنْ طَرِيقِ الْبَشَرِ أَوْ بِوَسِطَةِ الْحَاسُوبِ أَوْ يُنْتَجِجُهَا الْحَاسُوبُ"، وفي هذا الشأن ذهبت اتفاقية بودابست للجريمة المعلوماتية إلى ما اخذت به هيئة التوصيف العالمية الايزو، حيث نصت في مادتها الأولى على أن "المُعْطَيَاتُ هِيَ كُلُّ تَمَثِيلٍ لِلْوَقَائِعِ أَوْ الْمَعْلُومَاتِ أَوْ الْمَفَاهِيمِ تَحْتَ أَيِّ شَكْلٍ وَتَكُونُ مُهَيَّأَةً لِلْمُعَالَجَةِ بِمَا فِي ذَلِكَ بَرْنَامَجٍ مُعَدٍّ مِنْ ذَاتِ الطَّبِيعَةِ وَيَجْعَلُ الْحَاسِبَ يُؤْذِي الْمُهْمَّةَ"².

1- بلال بن جامع، المرجع السابق ص 53.

2- المادة الأولى من اتفاقية بودابست بشأن مكافحة الجريمة المعلوماتية عام 2001.

وقد أخذت التوصية الصادرة عن منظمة التعاون الاقتصادي والتنمية في 1992/11/26 الخاصة بحماية أنظمة الحاسبات الآلية وشبكات المعلومات بالترقية المشار إليها، حيث عرفت المعطيات بأنها "مجموعة من الحقائق أو المفاهيم أو التعليمات تتخذ شكلاً محدداً يجعلها قابلة للتبادل أو للمعالجة بواسطة الأفراد أو بوسائل إلكترونية ، أما المعلومات فهي المعنى المستخلص من هذه المعطيات"¹.

أما المشرع الجزائري على غير العادة عمد إلى وضع تعريف للمعطيات بموجب المادة الثانية من القانون 04-09 بنصها في الفقرة "ج" من هذه المادة على أن "المعطيات المعلوماتية هي أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية ، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها"².

إلا أنه لا جدوى من التمييز بين المعلومات والبيانات في مقام دراستنا، إذ أن الاهتمام الأساسي ينصب على حماية المعلومات بشكل عام، وبما أن المعلومات تمثل المعنى المستخلص من البيانات فإن الحماية تشمل كلاهما معاً، ومن ناحية أخرى قد لا تكون المعلومة مفهومة لدى متلقيها وهو ما يجعلها تخرج عن دائرة المعلومات طبقاً لهذه التفرقة ورغم ذلك يكون الوصول إليها والتلاعب بها على قدر كبير من الخطورة، فالذي يعنينا هو حماية المعلومات بغض النظر عن فهم محتواها، فلذلك نحن نرى استخدام المعلومات والبيانات في هذا المقام كمترادفين³.

إذ أنه ليس من الضروري بيان الفرق بين مصطلح البيانات (Data) ومعرفة مدى اختلافها مع مصطلح (Information) وذلك أن نقطة التمايز بين كلا المصطلحين تكمن في جهة المعالجة، فالمعلومات هي نتائج بيانات أخضعت للمعالجة أو التنظيم، في حين أن البيانات

1- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، المرجع السابق ص20.

2- المادة الثانية من القانون رقم 04-09، المرجع السابق.

3- طارق إبراهيم الدسوقي عطيه، الامن المعلوماتي النظام القانوني لحماية المعلوماتية، دار الجامعة الجديدة الاسكندرية، مصر، طبعة 2009، ص 39.

تشير إلى وصف أولي للأشياء أو الاحداث أو الأنشطة، لكنها ليست منظمة أو ذات معنى، ولهذا يُطلق على العلاقة بينهما (البيانات والمعلومات) مصطلح الدورة الاستراتيجية للمعلومات¹، إذ يتم في إطارها تجميع البيانات ومعالجتها لاستخلاص المعلومات، والتي تستخدم بدورها في اتخاذ القرارات والتي تنادي إلى توليد مجموعة جديدة من البيانات التي يتم تجميعها ومعالجتها مرة أخرى للحصول على معلومات إضافية يعتمد عليها في إصدار قرارات جديدة، ومن هنا يرتبط مصطلح البيانات ارتباطاً وثيقاً بالاستخدام المعلوماتي، وبناء عليه يمكن القول إن كل البيانات هي معلومات، والعكس غير صحيح أي أن كل المعلومات لا تُعد بالضرورة بيانات.

• ثانياً: تمييز المعلومات عن برامج الحاسب الآلي.

تحظي برامج الحاسب الآلي بأهمية كبيرة حيث يعتبر البرنامج من العناصر الرئيسية للكيان المنطقي لأي حاسوب، والذي بدونه - أي البرنامج - يصبح الحاسوب مجرد مجموعة من المعدات والآلات الصماء، وقد حظي برنامج الحاسوب بالعديد من التعريفات العلمية والقانونية ومنها أنه "مجموعة من الأوامر والتعليمات التي تقوم بمعالجة وتشغيل المعطيات أو البيانات والتي تصدر إلى الحاسب الآلي لتنفيذها"، بمعنى أنه مجموعة البيانات الداخلية طبقاً لبرنامج قد تم وضعه مسبقاً للحصول على نتائج معينة.

كما عرف برنامج الحاسب الآلي بعدة تعريفات نضيف منها تعريف المشرع المصري الوارد بالقرار الوزاري رقم 28 لسنة 1993 حيث عرفه بأنه "مَجْمُوعَةُ تَعْلِيمَاتٍ يُعْبَرُ عَنْهَا بِأَيِّ لُغَةٍ أَوْ رَمَزٍ مُتَّخَذٍ أَيْ شَكْلٍ مِنَ الْأَشْكَالِ يُمَكِّنُ اسْتِخْدَامَهَا بِطَرِيقَةٍ مُبَاشِرَةٍ فِي الْحَاسِبِ الْآلِيِّ لِإِدَاءِ وَظِيفَةٍ أَوْ الْوُصُولِ إِلَى نَتِيجَةٍ سِوَاءٍ كَانَتْ هَذِهِ التَّعْلِيمَاتُ فِي شَكْلِهَا الْأَصْلِيِّ أَوْ فِي شَكْلِ أُخَرَ تَتَحَوَّلُ إِلَيْهِ بِوَاسِطَةِ الْحَاسِبِ"، وشمل المشرع المصري برامج الحاسب الآلي بالحماية حين تناولها بالقانون رقم 82 لسنة 2002 في المادة 140 فقرة 2 بالنص "تَتَمَتَّعُ بِحِمَايَةِ هَذَا الْقَانُونِ حُقُوقَ الْمُؤَلِّفِينَ عَلَى مُصَنَّفَاتِهِمُ الْأَدَبِيَّةِ وَالْفَنِّيَّةِ، وَبِوَجْهِ خَاصٍّ الْمُصَنَّفَاتِ الْآتِيَةُ : 1 - 2... بَرَامِجُ

1 - رابحي عزيزة، المرجع السابق، 29.30.

الحَاسِبِ الآلِيَّ"¹، وتشمل الحماية جميع أنواع برامج الحاسب الآلي سواء برامج المصدر أو الترجمة أو الهدف كما تشمل برامج التطبيق والتشغيل².

ومن الواضح أن المشرع الجزائري، عند سنه القانون رقم 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة، قد أدرج المصنفات المعلوماتية ضمن فئة المصنفات الأصلية المشمولة بالحماية، حيث عبر عنها بمصنفات قواعد البيانات وبرامج الإعلام الآلي، وهنا كان المشرع مواكبًا للاتجاه الذي تبنته معظم البلدان، فقد عمل على أعمال قواعد البيانات والبرامج الإعلامية الآلية، بعيدًا عن الدراسة المتعمقة لمفهوم تعريف البرنامج، يرجع ذلك إلى تعقيد فكرة البرنامج نفسه، لأنها مرتبطة بتطوير تقنية نظم المعلومات واستخدامها، فمن الصعب حصرها في نطاق محدد³، كما أنه أدرج برامج الحاسوب ضمن مفهوم المعطيات وهذا في نص المادة 2 من القانون رقم 04/09، الذي ينص على أن " أَيْ عَمَلِيَّةَ عَرْضِ اللُّوَقَائِعِ أَوْ المَعْلُومَاتِ بِمَا فِي ذَلِكَ البرَامِجُ المُنَاسِبَةُ الَّتِي مِنْ شَأْنِهَا أَنْ تَجْعَلَ المُنظُومَةَ المَعْلُومَاتِيَّةَ تُؤَدِّي وَظِيفَتَهَا " ⁴.

علما أن البعض يستعمل مصطلح البرامج المعلوماتية، والبعض الآخر مصطلح برامج الحاسب، وترجع هذه التفرقة إلى أن برامج الحاسب الآلي هي منتج فاعل متميز بالإمكانات والمهام التي يؤديها أو بتركيبته الخارجية، في حين أن البرامج المعلوماتية تتميز بتركيبتها الداخلية، ويمكن أن لا تشمل إلا على لائحة بيانات البرنامج المصدري، وعليه تعد برامج الحاسب الآلي من أوائل وأهم المصنفات المعلوماتية أو مصنفات تقنية المعلومات التي حظيت باهتمام بالغ، سواء من حيث وجوب الاعتراف بطبيعتها أو توفير الحماية القانونية لها، فالبرمجيات تمثل الكيان المعنوي لنظام الحاسب الآلي، ودونها لا تتحقق أية فائدة من المكونات المادية للأجهزة و الوسائط، وتنقسم البرمجيات بوجه عام إلى نوعين أولهما برمجيات التشغيل التي تتولي تنسيق وإتاحة عمل مكونات النظام معا لتوفير بيئة عمل مناسبة لتشغيل البرمجيات

1- المادة 140 من القانون رقم 82 لسنة 2002 الخاص بقانون حقوق الملكية الفكرية المصري.

2- محمد عطية علي محمد الرزازي، المرجع السابق، ص 112.

3- سعيداني نعيم، المرجع السابق ص 19.

4- المادة الثانية من القانون رقم 04-09 المتضمن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها سابق الذكر.

التطبيقية وهي النوع الثاني والتي تؤدي وظائف محددة مثل برامج معالجة النصوص و الجداول الحسابية وبرامج الرسم¹.

أما من ناحية الدراسات والتشريعات القانونية فقد أثر فيها عدد من المفاهيم المتصلة بأنواع البرمجيات أبرزها:

1- برنامج المصدر: ويطلق عليه كذلك الصورة القابلة للقراءة الآدمية وهي مجموعة الأوامر والتعليمات التي يضعها المبرمج أو مؤلف البرنامج، وتكون مفهومة له لكنها غير قابلة للإدراك المباشر من قبل الآلة، أي الحاسب الآلي بوصفه جهازاً مادياً، ويتم إعداد برامج المصدر باستخدام لغات البرمجة، التي تختلف فيما بينها من حيث السهولة والتعقيد في إنجاز البرنامج لتحقيق الغرض المخصص له.

2- برنامج الآلة: يُعد برنامج الآلة نقيضاً لبرنامج المصدر، إذ يكون قابلاً للإدراك الآلة ومهيأً للتعامل معها وتشغيله من قبل الحاسب الآلي، وبين برنامجي الآلة والمصدر توجد برامج ذات غرض تحويلي أو ما يعرف (برامج الترجمة) والتي يتم بموجبها تحويل برامج المصدر إلى برامج آلة قابلة للتنفيذ.

3- الخوارزميات: تتمثل في العناصر والرموز الرياضية التي يقوم عليها البناء المنطقي للبرنامج، وهي من حيث الأصل تشبه الأفكار والحقائق العلمية في كونها غير قابلة للحماية القانونية لأنها ليست موضعاً للاستثمار، غير أنها متى نُظمت في شكل أوامر وتعليمات ابتكارية تهدف لتحقيق غرض معين، فإننا نكون بصدد برنامج حاسوب، والذي يصبح متى توافرت فيه عناصر الجدة والابتكار والأصالة محلاً للحماية القانونية، شأنه في ذلك شأن سائر مصنفات الملكية الفكرية الأدبية الأخرى².

1- حسين محمد الغول، المرجع السابق ص 127.

2- حسين محمد الغول، نفس المرجع السابق ص 131.

الفرع الثاني: المعلومات انواعها وخصائصها.

• أولاً: أنواع المعلومات .

للمعلومات أنواع متعددة تختلف عن بعضها البعض من حيث الطبيعة، والهيئة التي تظهر فيها، وكذلك من حيث مدى إتاحتها للجمهور، وبصفة عامة صنف الاستاذ "Catala" المعلومات إلى ثلاث أنواع رئيسية وهي: المعلومات الأسمية، والمعلومات المتمثلة في المصنفات الفكرية، والمعلومات المباحة، نتناولها بشيء من التفصيل على النحو التالي:

1- المعلومات الاسمية: هي المعلومات المرتبطة بأسماء الأشخاص والهيئات والمرتبطة بهم، وتشمل كلاً من المعلومات الشخصية والمعلومات الموضوعية، وقد نصت المادة الرابعة من القانون الفرنسي رقم 17 المتعلق بالمعلوماتية، الصادر في 06 جانفي 1978 على أن "المعلومات تُعد أسمية، إذا كانت تتيح بصورة مباشرة أو غير مباشرة، وتحت أي شكل بالتعرف على الشخص محل هذه المعلومات، أو تجعله قابلاً للتعرف عليه"¹، وتنقسم المعلومات الاسمية بدورها إلى نوعين:

أ- المعلومات الشخصية: ويقصد بها المعلومات التي تتعلق بشخص طبيعي بعينه، من حيث أسمية، لقبه، موطنه، وحالته الاجتماعية، وتدخل هذه المعلومات في إطار الخصوصية أو الحياة الخاصة، وهي تلك المرتبطة بشخص ما وعلى الرغم من أنها ليست من صنع صاحبها، غير أنه يملك السلطة عليها، فلا يمكن للغير الاطلاع عليها إلا في حالة موافقته الشخصية، أو بأمر من السلطات العامة المختصة، وهذا الأمر اكدت عليه نصوص القانون الفرنسي رقم 17 سالف الذكر والذي أعترف ضمناً بحق صاحب هذه المعلومات عليها، كحماية للأشخاص الطبيعيين مما قد يترتب من نتائج على معالجة معلوماتهم الأسمية آلياً، وقصر هذا الحق على صاحب المعلومات مراعاة للحق في الخصوصية².

1- رصاع فتيحة، المرجع السابق، ص 28.

2- دلخار صلاح بوتاني، المرجع السابق، ص 20.

والخصوصية وجهان يتمثلان في الاعتراف للشخص الذي تتعلق به المعلومات، بسلطته في الاعتراض على التدخل أو التقصي في خصوصيته¹، وسلطته في الاعتراض على الوصول إلى المعلومات الخاصة المتعلقة بخصوميته، وبمفهوم آخر فالخصوصية لها وجهان (الأول) مادي وقوامة عدم اقحام النفس في خصوصيات الآخرين والتدخل في شؤونهم الخاصة، (والثاني) إعلامي بالنسبة للغير وذلك بعد استخدام الآخرين لمعلومات تتعلق بالحياة الخاصة للفرد².

ب- المعلومات الموضوعية: وهي تلك المعلومات المرتبطة بشخص آخر ويعبر بها الشخص عن رأيه، فهي لا تتعلق بالشخص الصادرة منه بل تتعلق بشخص آخر، بمعنى أن الشخص المؤلف للمعلومات يختلف عن الشخص موضوع هذه المعلومات، ومن الأمثلة على ذلك المقالات الصحفية والملفات الإدارية، وتتفق هذه المعلومات مع المعلومات الشخصية في أنها خاصة بشخص معين، وتختلف عنها في كونها موجهة إلى الغير، وغير لصيقة بشخصية صاحبها³.

2- المعلومات المتمثلة بالمصنفات الفكرية:

هذه المعلومات عبارة عن نتاج لعمل ذهني ولها صفة الابتكار، وتظهر في صورة مصنفات فكرية محمية بتشريعات الملكية عادةً، سواءً التشريعات الخاصة بالملكية الأدبية

1- يقصد بالحق في الخصوصية أو ما يعرف في النظام اللاتيني بالحق في الحياة الخاصة حق الفرد في احترام سرية وخصوصية شؤونه وحمايتها من أي تدخل مادي أو معنوي، ويعد هذا الحق ذا جذور تاريخية عميقة، إذ يمكن القول أن مفهوم الخصوصية نشأ في البيئة الإنجليزية، حيث تطور مفهوماً في بريطانيا وظل لفترة محصورة المفهوم المادي للخصوصية، في حين عرف تطورا أوسع في الفقه الدستوري والقضائي في الولايات المتحدة الأمريكية سواء من حيث مضمونه أو نطاق حمايته، وهي فرنسية الاعتراف كحق عام، فقها وقضاء وتشريعا تجاوز في نطاقه المفاهيم المادية فأحاط المعنويات بالحماية من كافة مظاهر التدخل، وتعرضت لها أول مدونة دستورية لحقوق الإنسان تتمثل بوثيقة الحقوق البريطانية الصادرة في 1215 والمعروفة بالعهد الأعظم (الماجنا كارتا)، وفي إطار المعلوماتية يعرفها البعض أنها الحياة الخاصة وحق الفرد في الاستئثار بمباشرة السيطرة على كل المعلومات التي تتلف به أو بمعنى آخر هي حق الفرد في الرقابة على تداول ما يتعلق به من معلومات، أنظر أيمن عبدالله فكري، جرائم نظم المعلومات دراسة مقارنة، المرجع السابق، الصفحات 30 و 613-614.

2- أيمن عبدالله فكري، المرجع السابق، ص 30.

3- درار نسيم، الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني -دراسة مقارنة، أطروحة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان الجزائر، السنة الجامعية 2015-2016، ص 36.

والفنية أو الصناعية، ويتمتع مؤلفو هذه المعلومات بحقوق مالية وأدبية عليها، منها حق الاستنثار والاستغلال لهذه المعلومات أو المصنفات¹، بحكم علاقة الابوة التي تربط المؤلف بالمصنف، وقد عرفها قانون حماية الملكية الفكرية المصري في المادة 138 فقرة 1 بأنها "كُلِّ عَمَلٍ مُبْتَكِرٍ أَدَبِيٍّ أَوْ فَنِّيٍّ أَوْ عِلْمِيٍّ أَيْ كَانَتْ نَوْعُهُ أَوْ طَرِيقَةُ التَّعْبِيرِ عَنْهُ أَوْ أَهَمِّيَّتُهُ أَوْ الْغَرَضُ مِنْ تَصْنِيفِهِ"².

3- المعلومات المباحة:

يقصد بها تلك المعلومات التي تكون متاحة للجميع الحصول عليها ولا تنسب إلى مالك معين، ومن أمثلتها التقارير اليومية للبورصة والنشرات الجوية، وثبتت ملكية هذه النوع من المعلومات لمن يسبق إلى جمعها وصياغتها، وتقديراً للجهد الفكري المبذول في عمليتي الجمع والصياغة، ويلاحظ أنه متى جرى تجميع هذه المعلومات بقصد معالجتها وتشغيلها بواسطة الحاسب الآلي وتخزينها، فإن ذلك يؤدي إلى إنتاج معلومات جديدة³، وتنقسم هذه المعلومات إلى قسمين، وذلك على النحو الآتي:

- أ- **المعلومات المعالجة:** هي المعلومات التي تجمع وتعالج كي يتسنى تشغيلها على الحاسب بعد تخزينها واسترجاعها كلما دعت الحاجة، وينعقد حق الملكية على هذا النوع من المعلومات لمن قام بهذا العمل، وذلك دون الإخلال بحقوق المالك الأصلي.
- ب- **المعلومات المنتجة:** وهي تلك التي تنتج مع معالجة مجموعة من المعلومات، ولا ينعقد حق الملكية على هذه المعلومات لمالك واحد، إذ يحول اختلاط ملكية المعلومات الأصلية المتعددة وتداخلها دون ذلك، حيث يتقرر حق الملكية على هذه المعلومات وفق قاعدة حيازة المال المنقول، فتتعقد الملكية لمالكي المعلومات الأصلية جميعاً وتبعا إلى حجم ونوعية وقيمة إسهام كل واحد منهم.

1- دلخار صلاح بوتاني، المرجع السابق، ص 22.

2- المادة 138 من القانون رقم 82 لسنة 2002 الخاص بقانون حقوق الملكية الفكرية المصري.

3- درار نسيم، المرجع السابق، ص 36.

• ثانيا: خصائص المعلومات.

يلزم أن تتوفر في المعلومة بصفة عامة سواً أكان التعبير عنها يتم من خلال وسط مادي أم كانت بمعزل عن هذا الوسيط، فالمعلومات من حيث الطبيعة لا تتشابه مع أي شيء آخر، إذ لها خصائص فريدة تجعلها متميزة عن غيرها، وفي مجال تحديد خصائص المعلومات تتنازع نظريتان كل واحد منهما تحدد خصائص معينة للمعلومات تختلف عن الأخرى وهاتان النظريتان هما: نظرية التداول الحر للمعلومات، ونظرية القيمة الاقتصادية للمعلومات.

1- خصائص المعلومات تبعاً لنظرية التداول الحر للمعلومات.

بحسب هذه النظرية فإن من خصائص المعلومات أنها ذات طابع غير مادي، كما أن لها قابلية للنقل والتداول.

أ. المعلومات ذات طابع غير مادي: وهنا ينبغي أن لا يتم الخلط بين الدعامات المادية المثبتة عليها المعلومات، وبين المعلومات ذاتها، فالدعامة عبارة عن شيء مادي، بينما تنتمي المعلومات إلى مجموعة الأشياء المعنوية.

فكان أول تصوير للمعلومات هو الكلام والتبادل الشفوي، ثم ظهرت الكتابة بعد ذلك، التي أدت إلى تثبيت المعلومات على دعامة مادية كالحجار والخشب والردى و الورق وصولاً إلى الاسطوانات وغيرها من الوسائل الحديثة، وقد أدى ذلك إلى إحداث لبس بين المعلومات ذاتها وبين الدعامات المادية المثبتة عليها، والتمييز بينهما لم يكن بالأمر السهل¹.

ت-المعلومات قابلة للنقل و التداول: تتميز المعلومات بقابليتها للنشر والتداول حيث باتت تتنقل بمعزل عن دعاماتها المادية في ظل التكنولوجيا الحديثة، فنقل المعلومات وانتشارها أصبح يتم في نفس اللحظة وفي جميع أرجاء المعمورة بفضل شبكات المعلومات والوسائل التقنية الحديثة، مما أضفى صفة العالمية على المعلومات التي غدت تتكاثر وتتضاعف باستمرار.

1- دلخار صلاح بوتاني، المرجع السابق، ص24.

2- خصائص المعلومات تبعا لنظرية القيمة الاقتصادية:

وفق هذه النظرية فإن المعلومات لها أهمية اقتصادية كبيرة، تجعلها جديرة برفعها إلى مصاف الأموال، فهي حقيقة في حد ذاتها، يتحدد سعرها بوصفها سلعة، بيد أن هذا القول لا ينطبق على جميع المعلومات، ولكي نكون أمام معلومات ذات قيمة اقتصادية وتحظى بالحماية القانونية و الجنائية لابد أن تتوفر فيها عدة خصائص¹، وهي التحديد والابتكار والسرية والاستثناء.

أ- التحديد والابتكار:

إذا كانت المعلومة تمثل تعبيراً أو صياغة محددة تجعل رسالة ما قابلة للتبليغ والتداول من خلال علامات أو اشارات مختاره، فإنه يتعين أن تتسم بقدر من التحديد، وذلك بحصرها ضمن نطاق خاص وتعيين عناصرها وجوانبها بدقة، ذلك أن المعلومة التي تفتقد لصفة التحديد لا يمكن أن تكون معلومة حقيقية، وتبرز أهمية ذلك بوجه خاص في حالة الاعتداء على الأموال، حيث يشترط أن ينصب الاعتداء على شيء معين محدد، وأن يكون هذا الشيء بدوره محلاً لحق محدد²، فإذا كانت المعلومة عامة وأنعدم الحصر، كالمعلومات المتعلقة بكارثة طبيعية أو أحداث جارية في منطقة معينة وغيرها من الاحداث المتاحة للجميع لمعرفتها، فلا تدخل ضمن المعلومات التي تدخل ضمن صور الاعتداءات والأعمال الجرمية التي تستهدفها³.

أما فيما يخص صفة بالابتكار، فينبغي أن تنصرف إلى الرسالة التي تحملها المعلومة ذاتها، فالمعلومة غير المبتكرة تبقى في نطاق المعلومات العامة المتاحة للكافة، ولا يمكن أسنادها إلى شخص معين أو فئة محددة من الأشخاص، وتبدو أهمية هذه الرابطة عند تناولنا للصفتين الاتيتين.

1- يرى البعض أن هذه الخصائص هي بمثابة الشروط اللازمة توافرها في المعلومات كي تتمتع بالحماية القانونية، راجع: طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الاسكندرية مصر، سنة الطبع 2009، ص 40.

2- سعيداني نعيم، المرجع السابق، ص 24.

3- حسين محمد الغول، المرجع السابق، ص 131.

ب- السرية والاستئثار:

أن الصفة السرية للمعلومات تعني حصرها ضمن دائرة محدودة من الأشخاص، وبالتالي لا يتصور وقوع جرائم السرقة والنصب وخيانة الأمانة في مجال المعلومات إذا انعدم هذا الحصر¹، وبدون هذا التحديد لا يمكن أن تكون المعلومة محلاً يعتدى عليه، فالمعلومة غير السرية تكون صالحة للتداول، ومن ثم تكون بمنأى عن أي حيازة كالمعلومات التي تتعلق بحقيقة معينة أو بحدث معين.

وقد تستمد المعلومات سريتها من طبيعتها (اكتشاف في أحد المجالات التي تتميز بالسرية)، أو لرغبة صاحبها في ذلك، أو للسببين معا كما في حالة الشفرة السرية الخاصة باستعمال بطاقة الائتمان، وفي جميع الحالات فإن السرية التي تتمتع بها المعلومة هي التي تحدد نطاق إستعمالها في دائرة محددة، بحيث يستفيد أصحابها من الخاصية الثانية، وهي الاستئثار بالمعلومة².

و تعد خاصية الاستئثار بالمعلومة أمراً ضرورياً، لأنه في مختلف الجرائم التي تنطوي على إعتداء قانوني على الأموال، فإن الفاعل يعتدى على حق يخص الغير على سبيل الاستئثار.

ويتوافر للمعلومة هذه الصفة، إذا كان الوصول إليها غير مصرح به إلا لأشخاص محددين، إلا أن الاستئثار بالمعلومة قد يرجع إلى سلطة شخص ما على المعلومة في التصرف فيها، وفي هذه الحالة يكون الاستئثار لمؤلف المعلومة، ويرتبط هذا الشكل من أشكال الاستئثار بالمعلومة نوع من الرابطة نجدها محققة في حالتين:

- الحالة الاولى: تتعلق بالمعلومات التي ينصب موضوعها على بيان حقيقة أو واقعة ما، وهذا النوع من المعلومات هو بحسب الأصل غير سري ومتاح للجميع، أما إذا قام شخص

1- دلخار صلاح بوتاني، المرجع السابق، ص 26.

2- نائلة عادل محمد فريد قورة، المرجع السابق، ص 114.

بتجميع وحفظ هذه المعلومات ذاتها، فهو ينشئ عن طريق هذا التجميع والحفظ معلومة جديدة، يمكن أن يستأثر بالتصرف فيها بمفرده¹.

- **الحالة الثانية:** وتتحقق لتوافر الرابطة بين المعلومة وصاحبها، وعندما يكون موضوع هذه المعلومة فكرة أو عمل ذهني، ففي هذه الحالة ينظر مؤلف المعلومة إليها باعتبارها ملكاً خاصاً له، فإذا تمكن الغير من الاستيلاء عليها وعلى نحو غير مشروع²، فسوف يشعر صاحبها بأنه قد سلب³.

إلى جانب شروط السرية والاستثناء والتحديد والابتكار، هناك بعض الشروط غير المتفق عليها يشترطها البعض في المعلومات للتمتع بالحماية الجزائية تتمحور فيما يلي:

- **المعالجة الآلية:** ويُقصد بها أن تكون المعطيات قد خضعت لمعالجة آلية حتى تدخل في نطاق التجريم، أي أن تكون موضوعاً لعمليات متعددة تتم بصورة آلية داخل النظام المعلوماتي.

- **اتخاذ تدابير جديّة للمحافظة على سرية المعلومات:** أذ يرى جانب من الفقه أنه لا تتحقق الحماية الجزائية للمعلومات الشريّة إلا إذا بادر صاحبها إلى اتخاذ تدابير فعالة تهدف إلى حمايتها وصون سرّيتها، خاصة إذا كانت تلك المعلومات على قدر من الأهمية كالمعلومات

1- راجي عزيزة، المرجع السابق، ص 33.

2- نائلة عادل محمد فريد قورة، المرجع السابق، ص 114 و 115.

3- لا تتسجم النصوص القانونية مع هذا الاتجاه، إذ إن تشريعات الملكية الفكرية لا تعدد بالأفكار المجردة ما لم تتجسد في شكل محدد تعبر عنه في قالب مصنف، ذلك أن أحكام الملكية الفكرية لا تمتد إلى حماية الأفكار في ذاتها، وعلى هذا الأساس ربط كل من القانون الفرنسي الصادر في 1957 والقانون المصري حماية حق المؤلف رقم 354 الصادر في 1954، الحماية القانونية للأفكار بتجسيدها في شكل معين، بحيث يصبح هذا الشكل هو محل الحماية المدنية والجنائية ضد أفعال التقليد، ويعد الرداء الذي يستر الفكرة، وهو الأمر الذي لا يتوافر للمعلومات في ذاتها في ظل النصوص التقليدية، وتعريجا على قانون حماية الملكية الفكرية المصري رقم 82 لسنة 2002 نجد أنه نص صراحة في المادة 141 منه على أنه " لا تشمل الحماية مجرد الأفكار والإجراءات وأساليب العمل و..."، وهو ذات التوجه الذي تبناه المشرع العراقي في قانون حماية حق المؤلف المرقم 3 لسنة 1971 حيث نص في المادة 2 منه على أنه " تشمل الحماية المصنفات المعبر عنها بطريقة الكتابة أو الصوت أو الرسم والتصوير أو الحركة..". راجع: طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، المرجع السابق، ص 42، دلخار صلاح بوتاني، المرجع السابق، ص 27.

السياسية والاقتصادية، ومن هذه التدابير استخدام كلمات المرور أو اللجوء إلى تقنيات التشفير¹.

المطلب الثالث: الطبيعة القانونية للمعلومات.

ظهر جليا من خلال تناولنا للمعلومة أنها تتمتع بقيمة اقتصادية، وأنها أصبحت محلاً للاعتداء في ظل التطور التكنولوجي الحاصل، خاصة بعد الازدياد الكبير في استخدام الشبكة المعلوماتية، ومن هنا ولكي تكون المعلومة مشمولة بالحماية ثار التساؤل عما إذا كانت المعلومات تعتبر أموالاً ذات طبيعة خاصة يمكن أن تكون محلاً لحق ملكية أدبية أو فنية؟ أم هل يمكن إعطاء المعلومات وصف المال بعيدا عن دعائها المادية؟ وعما إذا كانت المعلومات منفصلة عن الوسيط المادي الذي يعبر عنها؟ أنقسم الفقه في تحديد الطبيعة القانونية للمعلومات إلى اتجاهين، الأول تقليدي رأى أن المعلومات لها طبيعة من نوع خاص وهو ما سنوضحه في الفرع الأول، أما الثاني اتجاه حديث رأى أن المعلومات عبارة عن مجموعة من القيم وهو ما سنتناوله بالتوضيح في الفرع الثاني.

الفرع الأول: المعلومة لها طبيعة من نوع خاص.

ينطلق أنصار هذا الاتجاه من حقيقة مسلم بها وهي أن وصف القيمة يضيف أساساً على الأشياء المادية القابلة للاستحواذ، باعتبار أن ما يمكن الاستئثار به من أعيان مادية هو وحده ما يندرج ضمن القيم المادية، ولكون المعلومات لها طبيعة معنوية، فأنها لا تقبل الاستئثار بذاتها، وعلى ذلك فالمعلومات المعالجة آلياً والمختزنة لا تندرج في مجموعة القيم المحمية، ما لم تندمج في إطار المصنفات والمواد الأدبية أو الفنية أو الصناعية التي تحظى بالحماية المقررة بموجب قوانين حقوق الملكية الفكرية أو الصناعية².

غير أنه من المسلم به، في المقابل أن المعلومة لها قيمة اقتصادية لا يمكن أنكارها، الأمر الذي يتيح إدراجها ضمن نطاق الحقوق المالية دون اعتبارها من ضمن القيم المالية، وذلك من خلال تصنيفها ضمن طائفة المنافع والخدمات، فالمعلومة وفق هذا التصور وثيقة الصلة

1- رابحي عزيزة، المرجع السابق، ص34.

2- حسين محمد الغول، المرجع السابق، ص 139.

بالخدمة أو المنفعة القابلة للتقويم المالي، وهو ما قد يؤدي في بعض الأحيان إلى الخلط بينها وبين الأشياء ذات القيمة المالية ومن ثم وصفها على هذا الأساس بأنها ذات قيمة مالية¹.

ومن ناحية أخرى فإن عدم إدراج المعلومات ضمن القيم المالية لا يعني إنكار أنصار هذه النظرية للقيمة الاقتصادية للمعلومات، أو إنكار وجود خطأ عند الاستيلاء على معلومات الغير، أي أن الاستبعاد لا ينطوي على الرفض لكل حماية قانونية، حيث أعترف كل من الفقه والقضاء في فرنسا بوجود خطأ عند حيازة معلومات الغير على نحو غير مشروع، وحاول إيجاد حماية قانونية لها من خلال الاستعانة بدعوى المنافسة غير المشروعة، بأن يبرر العقاب على أساسها وليس على أساس الخطأ في الاستيلاء على معلومات تخص الغير، إذ يجد أساسه في الظروف المحيطة بالاستيلاء، وليس بالاستيلاء ذاته، وبذلك ابتعدوا عن الاعتراف بحق الاستئثار لمالك المعلومة، كون المعلومة غير قابلة للاستئثار بحسب مفهوم أنصار هذه النظرية².

كما ويستند أنصار هذا الاتجاه إلى المبدأ الذي أقرته محكمة النقض الفرنسية في حكمها الصادر في أكتوبر 1978 والمتعلق بالاستعمال غير المشروع لأفكار الغير، وتتلخص وقائع القضية في أن إحدى المؤسسات تمكنت، أثناء مفاوضات جرت بينها وبين أحد الأشخاص، من الاطلاع على بعض الأفكار التقنية التي قد توصل إليها ولم يبادر إلى تسجيلها بعد، ولما لم تقض تلك المفاوضات إلى أبرام عقد بين الطرفين، قامت المؤسسة إلي استغلال تلك الأفكار في عملها، وقد قضت المحكمة بإدانة هذه المؤسسة استناداً إلى دعوى المنافسة غير المشروعة، مؤكدة في حيثيات حكمها أن " الغاية من دعوى المنافسة غير المشروعة هي تأمين الحماية لكل من لا يستطيع أن ينتفع بحق استثنائي"³.

1- رصاع فتيحة، المرجع السابق، ص 40.

2- دلخار صلاح بوتاني، المرجع السابق، ص 37.

3- Cour de Cassation, Chambre commerciale Publié au bulletin Com. 3 octobre – 11.517-77 n° 1978.

117. ص 117. المرجع السابق، ص 117.

وفي قضية أخرى صادرة عن ذات المحكمة (محمة النقض الفرنسية)، أقرت محكمة النقض الفرنسية بوجود خطأ في واقعة الاستخدام غير المشروع لمعلومة تخص الغير، وبدون الإحالة إلى دعوى المنافسة غير المشروعة، حيث تتلخص وقائع هذه القضية في تقديم المؤسسة "X" بطلب إلى المؤسسات المتخصصة "Y"، بإجراء دراسة خاصة بمخفف السرعة يراعى فيه بعض الضوابط التقنية، وبالفعل قامت المؤسسة الأخيرة بإعداد البحث وقدمته إلى المؤسسة الأولى مع كافة التصميمات اللازمة، والتي بدوها قامت بتسليمه إلى مؤسسة ثالثة لتصنيع الجهاز، عندها ثار الخلاف بين المؤسستين حول أحقية المؤسسة المصممة في الاختراع، وحظي الحكم الصادر عن محكمة النقض في هذه القضية بإهتمام كبير من جانب الفقه وذلك للأسباب التالية:

➤ أن الحكم يرسى مبدأ مهما وهو أن القيمة الاقتصادية التي تعد ثمرة لأفكار وتم العمل عليها لإخراجها، لا يمكن أن يتم استغلالها بدون ضوابط محددة تتعلق بظروف هذا الاستغلال والقيام به.

➤ أن هذا الحكم لم يحيل القضية إلى دعوى المنافسة غير المشروعة كما اتجه الحكم السابق.

➤ أن هذه القضية هي المرة الأولى التي تنقرر فيها الحماية لمعلومات لا تحميها نصوص قانونية محددة¹.

و خلاصة القول أن هذا الاتجاه يدرج المعلومة ضمن نطاق الحقوق المالية، ونتيجة لهذا الحكم ظهر اتجاه فقهي حديث لم يتردد في رفع المعلومات إلى مصاف القيم المالية التي تجب حمايتها قانونياً.

1- نائلة عادل محمد فريد قورة، نفس المرجع السابق، ص 118.

الفرع الثاني: المعلومات ذات قيمة اقتصادية.

اعتبر أصحاب هذا الاتجاه أن المعلومات طائفة جديدة من القيم تضاف إلى غيرها من القيم الأخرى، وأخذو بفكرة ومعيار جديدين بعيداً عن المعيار المادي والمعنوي، وهذا المعيار هو معيار القيمة الاقتصادية للشيء محل الاعتداء، واعتبروا أن المعلومة هي من الأموال المعنوية ذات القيمة الاقتصادية التي يمكن الانتفاع بها واستغلالها وحيازتها بعيداً عن الوسط المادي الموجودة فيه¹.

ويُعد الاستاذ **"CATALA"** من أبرز أنصار هذا الاتجاه، إذ يرى أن للمعلومة قيمة مالية تقترب في طبيعتها من السلعة، بإعتبارها نتاجاً ذهنياً وبشريا، ولكي تكون قابلة للتملك يشترط أن يقوم من يملكها ويحوز عناصرها المكونة بطريقة مشروعة بإخراجها في شكل يسمح بالاطلاع عليها وتبليغها بصورة مفهومة، ويستند الاستاذ **"CATALA"** في ذلك إلى حجتين أساسيتين، أولهما أن للمعلومة قيمة اقتصادية يمكن تقويمها بسعر السوق متى لم تكن محظورة قانوناً، وثانيهما وجود علاقة التبعية بين المعلومة ومؤلفها، وهي علاقة تماثل تلك التي تربط المالك بالشيء المملوك، وهو ما يحقق ميزتين لصاحبها: حق صاحب المعلومة في ضمان سريتها، وحقه في المطالبة بالتعويض عن كل عمل غير مشروع يتعلق بها².

أما الأستاذ **"Vivant"** فيتفق مع الرأي السابق، إذ يرى أن المعلومات لها قيمة قابلة للتملك لما لها من قيمة اقتصادية، وأنها يمكن أن تكون محلاً لعقد بيع، ويستند بدوره في ذلك على حجتين: الأولى مستوحاة من الاستاذين **"Planial"** و **"Ripert"** وتتمثل في (أن فكرة الشيء أو القيمة لها صورة معنوية، وأن تنوع محل الحق يمكن أن ينتمي إلى قيمة معنوية ذات طابع اقتصادي، وأن تكون هذه القيمة جديرة بحماية القانون).

والحجة الثانية التي يقدمها الأستاذ **"Vinant"** نفسه، الذي يرى أن جميع الأشياء التي تكون محل ملكية معنوية ويعترف بها القانون تقوم على أساس الاقرار بقيمة المعلومات، متى كانت في صورة براءات أو رسومات أو نماذج أو التحصيلات الضرورية أو مصنغات مشمولة

1- حسين محمد الغول، المرجع السابق ص 140 و 141.

2- رصاع فتيحة، المرجع السابق، ص 34.

بحق المؤلف، والانسان الذي يقدم ويكشف ويطلع الجماعة على شيء ما - بصرف النظر عن الشكل أو الفكرة- يعد بذلك قد قدم لهم معلومة بالمعنى الواسع ولكنها خاصة به، ويجب أن تعامل هذه الاخيرة بوصفها قيمة وتصلح محلاً للحق، وينتهي إلى القول " أن المعلومة تعد قيمة بسبب أهميتها الاقتصادية، ولكن هذه القيمة لا تكون من قبيل القيم المستحدثة، لأنها تتدرج بحسب رأيه ضمن طائفة موجودة فعلاً وهي (طائفة القيم المعلوماتية) التي تحتاج إرساء نظرية عامة بشأنها"¹.

ومن خلال ما تقدم يظهر جلياً لنا أن الكفة تميل إلى الاتجاه الثاني الذي اعتبر المعلومات قيمة مالية قابلة للتملك والاستغلال، والمعلوماتية في جوهرها هي معلومات معالجة بطريقة آليه ولها قيمة اقتصادية، لذا تجب معاملتها معاملة المال المادي، ومنحها الحماية القانونية، بخلاف ذلك ستكون المعلوماتية عرضة للاعتداء عليها دون أي رادع.

1- دلخار صلاح بوتاني، المرجع السابق، ص 38 و39.

*- أن ما يؤكد القيمة الاقتصادية والمادية للمعلومات بشتى أشكالها، عدد من الاحكام نذكر منها، حكم محكمة استئناف باريس في 11 أيار 1995، برفض دعوى أقامها مصور مستقل في مواجهة المؤسسة الصحفية، مطالباً إياها بدفع حقوق المؤلف، عن قيامها بإعادة استغلال صوره الفوتوغرافية، التي تنازل عن حق استغلالها، مؤسساً دعواه على أن التنازل الصادر عنه لم يكن إلا بالنسبة للنشر الأول، حيث أكدت المحكمة على أن التنازل من المصور إلى الصحيفة لا يقتصر على النشر الأول، وما يعيننا هو أن أي معلومة لا بحق لأي شخص استثمارها دون إذن صاحبها أو مؤلفها، وهو ما يؤكد القيمة المادية للمعلومة بكافة أشكالها، وهذا ما يوجب حماية المال المعلوماتي بأي شكل ورد، إذ أن الموضوع القانوني للجريمة يقوم على أساس استحداث عملية ربط بين موضوعها المادي وبين المصلحة القائمة والمشروعة التي تمثل الموضوع القانوني للعدوان، خاصة وأن الغاية القانونية للقانون الجزائري هي حماية المصالح القائمة والمشروعة دائماً، أنظر في ذلك : حسين محمد الغول، جرائم شبكة الانترنت والمسؤولية الجزائية الناشئة عنها - دراسة مقارنة، المرجع السابق ص 145.

المبحث الثاني: المدلول التقني والجنائي للنظم المعلوماتية.

أن زيادة حجم المعلومات إلى جانب تنامي الحاجة إلى تبادلها ونقلها من مكان إلى آخر، قد أسهمت في انتشار تقنية المعلوماتية، التي تهدف إلى معالجة المعلومات بصورة آليه بفضل التقنيات التي تتوافر عليها، والتي تُعد ثمرة تقاطع علوم الحاسوب بعلم الاتصالات، فالنظم المعلوماتية ليست ظاهرة منقطعة الصلة عما سبقه من تطورات تكنولوجيه بل هي طفرة من طفرات التطور في الحياة البشرية، فالمعلومات ونظم معالجتها موجودة منذ زمن بعيد وشهدت طرق معالجتها مراحل متعددة، وبما إن النظم المعلوماتية تشكل الركيزة الأساسية لتقنية المعلومات، فبدونها كان من المستحيل إحراز هذا التقدم على المستوى الحضاري، وسنحاول أبرز مفهوم النظم المعلوماتية وتعريفها بشكل يتوافق مع موضوعنا (المطلب الأول)، وإبراز نظم المعلومات من الناحية الجنائية وعلاقتها بالجريمة (المطلب الثاني)، أما (المطلب الثالث) فخصصناه لدراسة المجرم المعلوماتي من خلال توضيح دوافعه وإبراز سماته.

المطلب الاول: مفهوم النظم المعلوماتية.

تعددت التعاريف الخاصة بنظم المعلومات باختلاف الخلفيات العلمية والعملية لأصحابها، وذلك تبعاً لتأثر كل واحد منهم بخلفيته فعرف بأنه مجموعة من الإجراءات التي تقوم بجمع واسترجاع وتشغيل وتخزين المعلومات واتخاذ القرارات حيث يمكن لنظم المعلومات أن تساعد المديرين والعاملين في تحليل المشكل وحلها، أما علم الموارد البشرية فقد أعتبر نظم المعلومات أنها اطار يتم من خلاله تنسيق المواد البشرية وتحويل المدخلات "البيانات" إلى "مخرجات" لتحقيق أهداف المشروع، وهذا ما يفرض علينا توضيح معنى النظم المعلوماتية تقنيا وفنيا وإبراز مكوناته بالمنظور الحديث وهذا ما سنتناوله في فروع هذا المطلب الثلاث.

الفرع الأول: تعريف النظم المعلوماتية.

نظم المعلومات هو اصطلاح نشأ منذ السبعينيات من القرن الماضي بهدف وصف الحالة التي نشأت باندماج تقنية نظم المعلومات وتقنية الاتصال عن بعد وهندسة التحكم، ما أدى إلى اختراع تقنيات باهرة ساعدت بشكل كبير على تطوير أنظمة معالجة البيانات بمختلف أشكالها وأنواعها، وأصبحت بالفعل عاملاً حاسماً في تحديد مصير عالمنا بدولة وأفراده¹، وهنا سنوضح التعريف الجامع للنظم المعلوماتية من الناحية الاصطلاحية والقانونية وإبراز خصائصه، ومكونات نظم المعلومات ومشتملاته.

أولاً: تعريف النظم المعلوماتية لغة و اصطلاحاً.

أن محاولة ضبط مفهوم نظام المعلومات تجعلنا نفصل في المصطلح ونشرح دلالاته وتركيباته المتعددة، فيطلق لفظ نظام في اللغة على عدة معانٍ، وبداية كلمة نظام هي الاسم من المصدر نظم، وجمعها نظم وأنظمة وأناظيم، والنظام هو الترتيب والاتساق، حيث يقصد بنظام الأمر قوامه وعماده، كما يعبر بالنظام على الطريقة، فمثلاً يقال النظام الاجتماعي هو جملة القوانين والقواعد التي يخضع لها المجتمع، ويمكن تعريف النظام في أبسط معانيه بأنه " أي مركب من مجموعة من الأجزاء المترابطة والمتفاعلة التي يختص كل جزء منها بوظيفة معينة، مع وجود درجة من التعاون والتكامل بين الأجزاء في ادائها لوظائفها"².

ويُعد النظام مصطلحاً مشتقاً من الكلمة اللاتينية "systema"، التي تفيد معنى الكل المركب من عدد من الأجزاء، و وفقاً للمعجم الشامل يُعرف النظام بأنه " عُنْصُرٌ مُرَكَّبٌ يَتِمُّ تَشْكِيلُهُ مِنْ عِدَّةٍ وَحَدَاتٍ مُنَمَّيَّةٍ مُنْصِلَةٍ مَعَ بَعْضِهَا الْبَعْضُ بِوَاسِطَةِ عَدَدٍ مِنَ الْعِلَاقَاتِ، الَّتِي تَنْشَأُ لِتَحْقِيقِ التَّفَاهُظِ وَالتَّرَاوُظِ بَيْنَ هَذِهِ الْمَكُونَاتِ أَوْ الْوَحْدَاتِ الْمُخْتَلَفَةِ "، وعرف أيضاً أنه " مَجْمُوعَةٌ مِنَ الْعَنَاصِرِ أَوْ الْإِجْزَاءِ الَّتِي تَعْمَلُ بِتَنْسِيقٍ تَامٍّ وَتَفَاعُلٍ، تَحْكُمُهَا عِلَاقَاتٌ وَآلِيَةٌ عَمَلٍ مُعَيَّنَةٌ فِي نِطاقٍ مُحَدَّدٍ لِتَحْقِيقِ غَايَاتٍ مُشْتَرَكَةٍ وَهَدَفٍ عَامٍ "³.

1- أيمن عبدالله فكري، المرجع السابق، ص25.

2- بلال بن جامع، المرجع السابق ص 66.

3- رابحي عزيزة، المرجع السابق، ص 53-54.

ثانيا: تعريف النظم المعلوماتية في التشريعات الدولية.

عرفت معاهدة بودابست لمكافحة الجريمة المعلوماتية لعام 2001 النظم المعلوماتية في نص المادة الأولى منها على أنها " كُلُّ آلَةٍ بِمُفْرَدِهَا أَوْ مَعَ غَيْرِهَا مِنْ الْآلَاتِ الْمُتَّصِلَةِ أَوْ الْمُزْنِطَةِ ، الَّتِي يُمَكِّنُ أَنْ تَقُومَ بِمُفْرَدِهَا ، أَوْ مَعَ مَجْمُوعَةٍ عَنَّا صِرَ أُخْرَى تَنْفِيزًا لِبَرْنَامَجٍ مُعَيَّنٍ ، بِإِدَاءٍ مُعَالَجَةٍ إِلَيْهِ لِلْمَعْلُومَاتِ "¹، حيث توضح هذه الاتفاقية أن النظم المعلوماتية عبارة عن جهاز يتكون من مكونات مادية، بهدف المعالجة الآلية للبيانات.

كما نجد تعريفا جاء في المذكرة التفسيرية لاتفاقية بودابست بمناسبة إنعقاد الدورة رقم 109 لاجتماع لجنة وزراء المجلس الاوروبي، بالقول بأنها " المقصودُ بِالنِّظَامِ المَعْلُومَاتِيّ هُوَ جِهَازٌ يَتَكَوَّنُ مِنْ مُكَوِّنَاتٍ مَادِيَّةٍ وَمُكَوِّنَاتٍ مَنْطِقِيَّةٍ، بِغَرَضِ الْمُعَالَجَةِ الْآلِيَّةِ لِلْبَيِّنَاتِ الرَّقْمِيَّةِ يَشْمَلُ هَذَا الْجِهَازُ عَلَى وَسَائِلِ الْإِدْخَالِ وَإِخْرَاجِ وَتَخْزِينِ الْبَيِّنَاتِ وَقَدْ يَكُونُ هَذَا الْجِهَازُ مُنْفَرِّدًا أَوْ مُتَّصِلًا بِمَجْمُوعَةٍ مِنَ الْأَجْهَازَةِ الْمُتَمَاثِلَةِ عَنْ طَرِيقِ شَبَكَةٍ وَتَعْنِي كَلِمَةُ آليَّةٌ دُونَ تَدْخُلٍ بَشَرِيٍّ "².

كما عرفت منظمة التعاون الاقتصادي والتنمية النظم المعلوماتية على أنها " تَشْمَلُ الْحَاسِبَاتُ الْآلِيَّةُ وَ وَسَائِلَ الْإِتِّصَالَاتِ وَشَبَكَاتِ الْمَعْلُومَاتِ وَالْبَيِّنَاتِ وَالْمَعْلُومَاتِ الَّتِي يُمَكِّنُ تَخْزِينُهَا وَمُعَالَجَتُهَا وَاسْتِزْجَاعُهَا وَنَقْلُهَا بِوَسِطَةِ هَذِهِ الْحَاسِبَاتِ وَ وَسَائِلِ الْإِتِّصَالَاتِ أَوْ شَبَكَاتِ الْمَعْلُومَاتِ بِمَا فِي ذَلِكَ بَرَامِجُ الْحَاسِبَاتِ الْآلِيَّةِ وَجَمِيعُ الْقَوَاعِدِ اللَّازِمَةِ لِتَشْغِيلِ هَذِهِ الْإِنْظَمَةِ وَالْمُحَافَظَةِ عَلَيْهَا "³.

أضافة إلى ذلك عرفتھا الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2012 في الفصل الأول منها في المادة الثانية في تعريفها لبعض المصطلحات "النِّظَامُ المَعْلُومَاتِيّ مَجْمُوعَةُ بَرَامِجٍ وَ أَدَوَاتٍ مُعَدَّةٍ لِمُعَالَجَةِ وَإِدَارَةِ الْبَيِّنَاتِ وَالْمَعْلُومَاتِ، وَمَهْمَا كَانَ إِسْلُوبُ مُعَالَجَتِهَا لِلْمُعْطَيَاتِ فَإِنَّهَا تُشَكِّلُ نِظَامًا مَعْلُومَاتِيًّا ".

1 - المادة الأولى من اتفاقية بودابست بشأن مكافحة الجريمة المعلوماتية عام 2001.

2- ربيعي حسين، المرجع السابق، ص12.

3- أيمن عبدالله فكري، المرجع السابق، ص27.

ثالثاً: تعريف النظم المعلوماتية في التشريعات العربية¹.

عرفها نظام مكافحة جرائم المعلوماتية السعودي في مادته الأولى بأنها "النظام المعلوماتي مجموعة برامج و أدوات مُعدّة لمُعالجة البيانات و إدارتها و تشمل الحاسبات الآليّة"²، بالإضافة إلى ذلك عرفها المشرع الأردني في قانون المعاملات الالكترونية تعريفاً صريحاً بقوله "نظم مُعالجة المعلومات هي ذلك النظام الإلكتروني المُستخدَم لإنشاء رسائل المعلومات أو إرسالها أو تسلمها أو مُعالجتها أو تخزينها أو تجهيزها على أي وجه آخر"³.

أما المشرع الجزائري فقد عرف النظم المعلوماتية في القانون الخاص بتكنولوجيا الاعلام والاتصال ومكافحتها 09-04 بالقول بأن النظم المعلوماتية⁴ هي " أي نظام مُفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمُعالجة الآلية للمعطيات تنفيذاً لبرنامج مُعَيّن "⁵.

1- بالتعريب على دول عربية أخرى نذكر ما جاء به قانون سلطنة عُمان بأنه " النظام المعلوماتي نظام الكتروني للتعامل مع المعلومات والبيانات بأجراء معالجة تلقائية لها لإنشاء أو إرسال أو تسلم أو تخزين أو عرض أ برمجة أو تحليل تلك المعلومات والبيانات"، أنظر في ذلك، المادة الاولى المخصصة للتعريفات من القانون رقم 69 لسنة 2008 بشأن المعاملات الالكترونية في سلطنة عُمان، والجدير بالذكر أن قانون التوقيع الالكتروني المصري رقم 15 لسنة 2004 صد خالياً تعريف للنظام المعلوماتي، أنظر في ذلك، د خالد ممدوح ابراهيم، الجرائم المعلوماتية، الطبعة الاولى، دار الفكر الجامعي، الاسكندرية، 2009، ص 21-22.

2- المادة الأولى من نظام مكافحة جرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم 17 بتاريخ 2007/03/23.

3- المادة الثانية من قانون المعاملات الاردني رقم 85 لسنة 2001، المنشور بالجريدة الرسمية على الصفحة 6010 عدد رقم 4524 بتاريخ 2001/12/3.

4- عند تناول مفهوم نظم المعلومات، يبرز مصطلح آخر يتكرر في العديد من المراجع محل الدراسة وهو قواعد البيانات فما المقصود منه؟ قواعد البيانات هو نظام للتخزين والمعالجة يقوم على الارتباط بنظام معالجة استرشادي يتخذ طبيعته أو شكله تبعاً لأسلوب إنشائه، مع العلم أنها تعرف من الناحية الفقهية أنها " مجموعة مهيكله من التسجيلات النصية أو غير النصية، تكون متاحة للقراءة الآلية عبر خط مباشر مرتبط"، أنظر في ذلك رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه، جامعة تلمسان، الجزائر، 2018، ص 56.

5- الفقرة "ب" من المادة الثانية من القانون رقم 09-04 سابق الذكر.

رابعاً: تعريف النظم المعلوماتية في التشريعات الغربية.

بالنسبة للمشرع الفرنسي لم يعرف النظم المعلوماتية، واقتراح مجلس الشيوخ الفرنسي مفهوم نظام معالجة البيانات الآلي عند تعديل القانون الجنائي "العقوبات"، وعرفها بأنها "كُلُّ مُرَكَّبٍ يَتَكَوَّنُ مِنْ وَحْدَةٍ أَوْ مَجْمُوعَةٍ مِنْ وَحَدَاتٍ مُعَالَجَةٍ ، وَتَتَكَوَّنُ كُلُّ وَحْدَةٍ مِنْ ذَاكِرَةٍ وَبَرَامِجٍ ، وَبَيِّنَاتٍ ، وَمُعَدَّاتٍ إِدْخَالٍ وَمُخْرَجَاتٍ ، وَأَجْهَزةٍ رِبْطٍ ، وَهِيَ مُرْتَبِطَةٌ بِبَعْضِهَا الْبَعْضُ مِنْ خِلَالِ مَجْمُوعَةٍ مِنَ الْعَلَاقَاتِ ، وَيَتِمُّ تَحْقِيقُ نَتَائِجٍ مُعَيَّنَةٍ مِنْ خِلَالِ هَذِهِ الْعَلَاقَاتِ ، وَهَذِهِ هِيَ مُعَالَجَةُ الْبَيِّنَاتِ ، وَعَلَيْهِ يَخْضَعُ الْمُرَكَّبُ لِنِظَامِ الْحِمَايَةِ الْفَنِّيَّةِ "، أما بالنسبة لقانون "قودفران" فقد غير أخيراً وجهة نظر المشرع الفرنسي لنظم المعلومات على أنها مال بحد ذاتها، ولا بد لها من حمايه القانون الجنائي من المساس غير المشروع¹.

كما تم تعريفها بتشريعات الولايات المتحدة الأمريكية من خلال تعريف الحاسب ونظام الحاسب وشبكة الحاسب، فالحاسب هو الجهاز الذي يقبل ويعالج ويخزن ويسترجع وينتج بيانات، عبر أجهزة اتصالات ترتبط بالحاسب، ويعرف نظام الحاسب بأنه أي مجموعة ذات علاقة متصلة أو غير متصلة بأجهزة حاسب أو برامج حاسب، أما شبكة الحاسب فعرّفها بأنها أي مجموعة ذات علاقة، أجهزة مرتبطة عن بعد و وسائل اتصالات ويتضمن ذلك أكثر من نظام حاسب، وتكون قادرة على إرسال البيانات فيما بينها من خلال وسائل الاتصال².

ويمكننا من خلال التعريفات السابقة وضع تعريف شامل للنظم المعلوماتية بأنها (النُّظُمُ الْمَعْلُومَاتِيَّةُ هِيَ كُلُّ نِظَامٍ مُكَوَّنٍ مِنْ مَجْمُوعَةٍ مِنَ الْآلَاتِ الْمُتَرَبِّطَةِ بِبَعْضِهَا الْبَعْضُ عَنِ الشَّبَكَاتِ اتِّصَالٍ، أَوْ آلَةٍ بِمُفْرَدِهَا يُمَكِّنُهَا الْقِيَامُ بِشَكْلِ آلِيٍّ عَنِ بَرَامِجٍ صُمِّمَتْ خِصَّيْصًا لِتَحْقِيقِ مُعَالَجَةِ آلِيَةٍ لِلْمَعْلُومَاتِ).

1- رابحي عزيزة، المرجع السابق، ص54.

2- أيمن عبدالله فكري، المرجع السابق، ص27.

خامسا: خصائص النظم المعلوماتية.

تتميز النظم المعلوماتية بعدد من الخصائص الفريدة، والتي تمنحها طابعاً خاصاً، ولعل من أبرز هذه الخصائص ما يأتي:

- **المرونة:** والمقصود بها امكانية إدخال التعديلات الضرورية للنظام لمواجهة المتغيرات المفاجئة والتي تحدث في حين عمل النظام.
- **التوازن:** ويقصد به تصميم نظام المعلومات بطريقة تسمح بتحقيق التوازن بين دقة المعلومات من جانب وكلفة الحصول عليها والنتيجة التي تحققها من جانب آخر.
- **التكامل بين عناصر النظام:** وهذا يعني أن يكون النظام وحدة متماسكة بحيث تكون مخرجات كل عملية مخرجات عملية لاحقة.
- **السهولة والبساطة:** يفقد النظام المعلوماتي فعاليته كلما تعقدت هيكلته، الأمر الذي يحد من قدرة المستفيد على استخدامه، ولذا يجب مراعاة البساطة في تصميم النظام، فيكون النظام سلسا بحيث يمكن ادراك عملة بسهولة ويسر، فالنظام المعلوماتي الناجح هو ذلك النظام الذي يتم بواسطته تطوير إجراءات وسبل الحصول على المعلومات ومعالجتها وتوصيل المعلومات إلى المستفيدين بطريقة بسيطة¹.

الفرع الثاني: المكونات المادية للنظم المعلومات.

إذا كانت المعلوماتية تعني المعلومات المعالجة آليا، فبالأكيد أن هذه المعالجة الآلية تقتضي توافر عدد من العناصر التي تتمثل في المعلومات، وأجهزة الحاسب الآلي وشبكات الاتصال، وبما أننا عرفنا المعلومات سابقا سنكتفي هنا بدراسة باقي العناصر والمتمثلة في الحاسوب وشبكات الاتصال.

أولا: الحاسب الآلي.

تعد الحواسيب من أهم المكونات الرئيسية للنظام المعلوماتي، إلا أنه هناك خلاف بين الباحثين من حيث تعدد التسميات لهذا الجهاز منها (الحاسب الآلي) و (الحاسب الإلكتروني) و

1- بلال بن جامع، المرجع السابق ص 71.

(الحاسوب)، ويطلق عليه البعض مصطلح (كمبيوتر) وهي تعريب للكلمة الانجليزية "Computer"¹ وترجمتها باللغة العربية (الحاسب) وهي مشتقة من الفعل "Compute" أي يحسب أو يحصي باللغة العربية، وهي إحدى وظائف هذا الجهاز، وبظهور الآلة العددية "Calculator" وخوفا من اختلاط الاسمين، أستخدم بعض الباحثين كلمة كومبيوتر².

وفي مجال دراستنا هذه سوف نستخدم المصطلحين (الحاسب الآلي) و (الكمبيوتر) كمترادفتين يدلان على نفس المعنى.

اصطلاحا يعرف الحاسب الآلي بأنه " آلة تقوم بإداء العمليات الحسابية واتخاذ القرارات المنطقية على البيانات الرقمية بوسائل إلكترونية وذلك تحت تحكم البرامج المخزنة فيه "، كما يعرف بأنه " جهاز إلكتروني يتكوّن من عنصرين ماديّ ومعنويّ ، ويشمل الأول كلّ المكونات المادية في حين يشمل الثاني البرامج ومعالجتها حيث يتم تشغيله على ضوء برنامج يتم تخزينه على ذاكرته ومن ثم يقوم باستقبال البيانات ومعالجتها على النحو المطلوب منه بغية الوصول إلى نتائج محدّدة ".

وتشريعا عرفت اتفاقية بودابست بشأن مكافحة الجرائم المعلوماتية لسنة 2001 الحاسب الآلي أنه " كلّ جهاز بمفرده أو مجموعة أجهزة مربوطة معا تؤدي بمفردها أو مع مجموعة عناصر أخرى ، وتنفيذا لبرامج معيّنة ، المعالجة الآلية للبيانات Data³ ".

1- تعددت الترجمات العربية للاصطلاح الانجليزي (Computer) فأطلق عليه أولا العقل الالكتروني ثم الحاسب الآلي واعتمدت المنظمة العربية للمواصفات والمقاييس اصطلاح الحاسوب وصدر معجم الحاسبات عن مجمع اللغة العربية سنة 1987 بدون اضافة كلمة إلكترونية او آليه إلى كلمة الحاسبات. أنظر في الحاسوب والانترنت، عبدالعال الديري و الاستاذ محمد صادق أسماعيل، الجرائم الإلكترونية دراسة قانونية قضائية مقارنة مع احداث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والانترنت، المركز القومي للإصدارات القانونية، الطبعة الاولى، القاهرة، مصر 2012، ص 15.

2- دلخار صلاح بوتاني، المرجع سابق، ص 31.

3- المادة الاولى من اتفاقية بودابست بشأن مكافحة الجريمة المعلوماتية عام 2001.

ومن التشريعات العربية التي عرفت الحاسب الآلي، نظام مكافحة جرائم المعلومات السعودي حيث عرفه " أيُّ جهازٍ ثابتٍ أو منقولٍ سلكيٍّ أو لاسلكيٍّ يحتوي على نظام معالجة آليّة للبيانات ، أو تخزينها أو إرسالها ، أو استقبالها ، أو تصفّحها ، يؤدي وظائف محدّدة بحسب البرامج ، والأوامر المُعطاة له "¹، أما من ناحية التشريع الجزائري فنجد أن القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، لم يتطرق لتعريف جهاز الحاسوب بالرغم من أنه يعتبر الوسيلة والقطعة الأساسية لأي نظام معلوماتي.

أما المشرع المصري فتدخل ليضع تعريف للحاسب الآلي في القرار بقانون رقم 109 لسنة 2005 بتاريخ 2005/05/15 الصادر بشأن اللائحة التنفيذية للقانون رقم 15 لسنة 2005 بشأن تنظيم التوقيع الالكتروني في المادة الأولى (... الحاسب الآلي جهاز إلكتروني قادر على تخزين ومعالجة وتحليل واسترجاع البيانات و المعلومات بطريقة إلكترونية...)².

أما من الناحية الفقهية فقد عرف الفقه المصري بانه " جهازٌ إلكتروني يستطيع أن يقوم بأدقّ العمليات الحسابية والمنطقية للتعليمات المُعطاة له بسرعة كبيرة قد تصل إلى عشرات الملايين من العمليات الحسابية في الثانية الواحدة ، وذلك على درجة عالية من الدقة ، له القدرة على التعامل مع كم هائل من البيانات وكذلك تخزينها واسترجاعها عند الحاجة إليها "³.

ولا يسعنا هنا إلا أن نتفق مع من ذهب للقول أن أفضل تعريفات للحاسب الآلي التعريف الذي جاءت به موسوعة دلتا كمبيوتر في مؤلفها المعنون بالموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، وذلك لشموله جميع الوظائف التي يؤديها الحاسب في الحياة العملية حيث عرفت الحاسب "Computer" بأنه " جهازٌ إلكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال بيانات (Data Input) أو إخراج معلومات Information output وإجراء عمليات حسابية أو منطقية وهو يقوم بالكتابة على أجهزة الإخراج Output

1- المادة الاولى الفقرة السادسة من نظام مكافحة جرائم المعلومات السعودي، سابق الذكر.

2- طارق أبراهيم الدسوقي عطيه، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة للنشر، الاسكندرية، مصر، ص 87.

3- ربيعي حسين، المرجع السابق، ص 13.

Devices أو التَّخزينِ والبياناتِ يَتِمُّ ادِّخالُها بِوَاسِطَةِ مُشغِّلِ الحاسبِ **Operator** عَنْ طَرِيقِ وَحَدَاتِ الإدخالِ ¹.

1- المكونات المادية للحاسب الآلي (Hard Ware).

من تعريف الحاسب الآلي الموضح لنا سابقا يظهر لنا جليا أن أجزاء الحاسب الآلي المادية تسمى بالمكونات المادية وتنقسم إلى ثلاث أجزاء رئيسية وهي:

أ- **وحدة الادخال:** وهي الوسائل التي تستخدم لإدخال البيانات أو المعلومات أو الاوامر أو المعطيات أو البرامج المراد معالجتها إلى ذاكرة الحاسوب، وقد تأتي هذه الوسائل في صورة أجهزة إدخال مباشرة، وتُعد لوحة المفاتيح إحدى أبرز هذه الوسائل، بالإضافة إلى شاشات اللمس والادخال المرئي بواسطة الكاميرا والادخال الصوتي بواسطة الميكروفون أو التلفون فيتم تحويل الصوت البشري إلى إشارات كهربائية ترسل إلى الحاسب، وقد تكون في شكل وسائل إدخال غير مباشرة كغرفة الاقراص المدمجة والماسح الضوئي.

ب- **وحدة المعالجة المركزية:** وهي محور الحاسب الآلي وأساسه، إذ تمثل الدماغ المسيطر على جميع أنشطته وعملياته، وتشمل وحدة الحساب والمنطق ووحدة التحكم، بالإضافة إلى وحدة الذاكرة التي تتألف بدورها من جزئين (ذاكرة القراءة فقط والذاكرة العشوائية أو المؤقتة) ².

ت- **وحدات الإخراج:** وهي الأجزاء و الوحدات التي يتم من خلالها إخراج البيانات بعد معالجتها من وحدة المعالجة المركزية إلى الخارج، ومن أبرز وحدات الإخراج شاشة العرض، وتُعرف أيضا بوحدة العرض المرئي، وتُعد من أكثر مكونات الحاسب الآلي استخدامًا، إذ تمكن المستخدم من استعراض البيانات أو المعلومات المدخلة عبر لوحة المفاتيح، فضلاً عن عرض النتائج والمتحصلة من معالجة البيانات في وحدة المعالجة المركزية، كما تُعد

1- عبدالعال الديري، محمد صادق أسماعيل، الجرائم الإلكترونية دراسة قانونية قضائية مقارنة مع احداث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والانترنت، المركز القومي للإصدارات القانونية، الطبعة الاولى، القاهرة، مصر 2012، ص 16-17.

2- دلخار صلاح بوتاني، المرجع سابق، ص33.

الطابعة من وحدات الإخراج الأساسية وهي عبارة عن جهاز يستخدم في لإنتاج نسخ مطبوعة من البيانات مثل التقارير والمنتجات العلمية¹.

2- المكونات المنطقية للحاسب (Software).

يقصد بالكيان المنطقي في الدلالة اللغوية مجموع المكونات غير المادية لنظام الحاسب الآلي، ويشمل ذلك برامج النظام و الكيانات المنطقية و التطبيقات العملية التي تجري داخل الكيان المادي للحاسوب، والمتمثلة في مجموع البيانات والمعلومات، إضافة إلى برمجيات الحاسوب²، وعرفه القانون الأمريكي الصادر سنة 1980 المتعلق بحماية حق المؤلف البرنامج بأنه " مَجْمُوعَةٌ مِنَ التَّوْجِيهَاتِ أَوْ التَّعْلِيمَاتِ الَّتِي يُمَكِّنُ لِلْحَاسِبِ إِسْتِخْدَامَهَا بِشَكْلِ مُبَاشِرٍ أَوْ غَيْرِ مُبَاشِرٍ لِلْوُصُولِ إِلَى نَتِيجَةٍ مُعَيَّنَةٍ "³.

وتعرف المنظمة العالمية للملكية الفكرية البرنامج بأنه " مَجْمُوعَةٌ تَعْلِيمَاتٍ يُمَكِّنُهَا إِذَا مَا نَقَلَتْ عَلَى رَكِيزَةٍ تَسْتَوِعِبُهَا آلَاءَةُ أَنْ تُشِيرَ - تُؤَدِّي - تُسَاعِدُ - فِي الْوُصُولِ إِلَى خَاصِيَّةٍ مَا أَوْ هَدَفٍ أَوْ نَتِيجَةٍ خَاصَةٍ بِوَاسِطَةِ آلَةٍ يُمَكِّنُهَا الْفَيَاؤُ بِالْعَامِلِ مَعَ الْمَعْلُومَةِ "، وهذه البرامج يمكن تصنيفها إلى نوعين وهي برامج التطبيقات وبرامج النظام.

1- طارق أبراهيم الدسوقي عطيه، المرجع السابق، ص 94-95.

2- من الصعب إعطاء تعريف شامل للبرنامج، شأنها في ذلك شأن الافكار المعنوية التي تستند في تعريفها على ذهن ومخيلة المعرف، لذلك هناك العديد من التعريفات سواء في التشريع أو الفقه ، على الرغم أن أغلب التشريعات قد نأت بنفسها عن التدخل المباشر في تعريف برامج الحاسب الآلي باعتبارها فكرة ويشكل تعريفها حدًا لامتصاص التطور التكنولوجي المستمر، غير أن المشرع الفرنسي عرف البرامج بموجب القرار الوزاري المتعلق بإثراء اللغة الفرنسية الصادر في 1981/12/22 بأنها "مجموعة البرامج والمراحل والقواعد وأحياناً الوثائق المتعلقة بسير مجموعة من استعلامات، حيث يقصد بالاستعلام مجموعة التقنيات التي تتيح تخزين المعلومات والوصول إليها وتنظيمها بغرض استغلالها"، وفي السياق ذاته تنص المذكرة التفسيرية لاتفاقية بودابست 2001 على أن البرنامج المعلوماتي هو " مجموعة من الأوامر التي يمكن ان تنفذها بواسطة الحاسب الآلي لتحقيق النتيجة المنشودة، ويمكن لجهاز الحاسب أن يقوم بتشغيل مختلف البرامج"، بينما عرف المشرع الاماراتي البرنامج المعلوماتي بأنه " مجموعة من التعليمات والاوامر، قابلة للتنفيذ بواسطة تقنية المعلومات ومعدة لإنجاز مهمة ما"، راجع في ذلك دلخار صلاح بوتاني، الحماية الجنائية الموضوعية للمعلوماتية، المرجع السابق، ص 34-35.

3- ربيعي حسين، المرجع السابق، ص 15.

أ- برامج التطبيقات (Applications program/ software): وهي البرامج التي تصمم لتنفيذ وظائف محددة إدارية أو علمية مثل المرتبات "Payroll" والدراسات الإحصائية "Statistical analysis" والصناعية "Manuactouring" والمحاسبة "Accounting" والعديد من البرامج الأخرى.

ب- برامج النظام (System program/ software): وهي برامج تعتبر أكثر عمومية من برامج التطبيقات وتكون عادة مستقلة عن أي تطبيق محدد فهي تخدم برامج التطبيقات عن طريق تحقيق أكبر استفادة ممكنة من مكونات الحاسب، فمثلا عند بدء تشغيل الحاسب يقوم برنامج معين بتجهيز الأجهزة والمكونات للعمل، ومن أهم برامج النظام مترجمات ومفسرات اللغات المختلفة، كما وتدخل نظم التشغيل " Operating systems " ضمن هذا التصنيف¹.

ثانيا: شبكات الاتصال.

تقوم شبكة الاتصالات بدور بالغ الأهمية بالنسبة للنظم المعلوماتية، إذ تقوم بنشر المعلومات وتوفر فرص نقلها وإتاحتها على نطاق واسع والتعامل معها، فتكنولوجيا الاتصالات هي التي قامت بربط النظم المعلوماتية المختلفة في أماكن شتى فسهلت الاتصالات فيما بينها، و بالإضافة إلى الحاسب يتكون النظام المعلوماتي من مجموعة من المكونات² منها ماديات وبرمجيات ومنها ما يتعلق بالشبكات أي شبكات الاتصال، فما هي طبيعة هذه الشبكات؟.

1- مفهوم شبكة الاتصال.

لشبكة الإتصال في مجال النظم المعلوماتية تعريف خاص بها فهي " أداة رَبطَ بَيْنَ حَاسُوبَيْنِ أَوْ أَكْثَرَ وَهَذِهِ الرَّابِطَةُ قَدْ تَكُونُ أَرْضِيَّةً بِالأَسْلاكِ أَوْ الكَابِلَاتِ ، كَمَا يُمَكِّنُ أَنْ تَكُونَ لاسِلكِيَّةً ، أَوْ بِالأَشْجَعَةِ تَحْتَ الحَمَرَاءِ أَوْ بِالأَقْمَارِ الصَّنَاعِيَّةِ "، وقد تقتصر شبكة الإتصال من حيث النطاق الجغرافي على مساحة محددة مقتصرة جغرافيا فتسمى شبكة (محلية) وهي نظام

1- عبدالعال الديربي، محمد صادق أسماعيل، المرجع السابق، ص 21-22.

2- غالبا ما تنصب الجريمة المعلوماتية على استغلال مكونات النظم المعلوماتية من حواسيب وشبكات اتصال، باعتبارها القناة الرئيسية للوصول إلى المعلومات المخزنة أو المتداولة، وذلك بقصد الاعتداء عليها أو المساس بها، أنظر في ذلك، ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 15.

يتم فيه إيصال مجموعة من الحاسبات داخل منطقة معينة في إطار الدولة كما هو الحال في الشركات والمؤسسات التي تقوم بإنشاء شبكة خاصة بها تربط بين مناطقها المختلفة من خلال ربطها بشبكة حاسبات متصلة ببعضها البعض، كما يمكن أن تمتد شبكة الاتصالات لتغطي نطاقاً جغرافياً واسعاً، فتوصف بأنها **(متسعة النطاق)**، ويمكن أن تكون متصلة ببعضها البعض، وتتميز بأنها ليست قاصرة على إقليم الدولة ولكنها تمتد لتشمل على نطاق واسع العديد من الدول، ولذلك تسمى بشبكة الشبكات، وذلك لقيامها بالربط بين الشبكات المحلية الموجودة في جميع أنحاء العالم أياً كانت مجالاتها أو تخصصات العمل بها، فهي ليست محدودة المكان ولا نوع المعلومات التي تتاح من خلالها¹، وتعد شبكة الانترنت شبكة عالمية لكونها تتكون من عدد كبير من الشبكات المترابطة فيما بينها، والتي تعتمد جميعها على نفس البروتوكولات، و وفقاً للتعرف السابق يمكن للنظم المعلوماتية أن تتصل بهذه الشبكة إما بوصفها نقاطاً نهائية أو نقاط خروج، أو كوسيلة لتسهيل نقل المعلومات وتبادلها.

2- تعريف شبكة الانترنت:

لغويًا تُعد كلمة الإنترنت مصطلحاً حديثاً في القاموس اللغوي لمختلف لغات العالم، وهي كلمة إنجليزية ومختصرة من مقطعين **"Inter"** وهي اختصار لمصطلح **"International"** وتعني دولي، و **"Net"** وهي اختصار لكلمة **"Network"** والتي تعني الشبكة²، وجمع الكلمتين يتضح المعنى الكامل المتحصل عليه وهو الشبكة الدولية وهذا من الناحية اللغوية¹.

1- أيمن عبدالله فكري، المرجع السابق، ص 68.

2- بدأت فكرة إنشاء شبكة معلومات عالمية على يد وكالة مشاريع الأبحاث المتقدمة الدفاعية الأمريكية (ARPA) عام 1969، عبر تمويل مشروع هدفه ربط أجهزة الحواسيب التابعة للإدارة الدفاعية بالمتقاعدين العسكريين وعدد كبير من الجامعات التي تجري أبحاثاً ممولة من وزارة الدفاع. وأُطلق على هذه الشبكة اسم أربانت (ARPANET)، وكان الهدف الأساسي منها تطوير تقنية تشبيك قادرة على الصمود في حال وقوع هجوم نووي أو عسكري، صُممت أربانت باستخدام تقنية إعادة التوجيه الديناميكي (Dynamic Packet Switching)، التي تتيح استمرار عمل الشبكة حتى عند تعطل بعض العقد أو الوصلات، حيث تُحوّل البيانات تلقائياً عبر مسارات بديلة. ومع مرور الوقت، لم يقتصر استخدام أربانت على الأغراض العسكرية، بل توسّع ليشمل الجامعات الأمريكية لأغراض البحث العلمي والتواصل الأكاديمي، مما أدى إلى ازدهار شديد تجاوز قدرة الشبكة، وفي عام 1983، تم فصل الجزء العسكري من الشبكة وإنشاء شبكة مخصصة للمواقع العسكرية أُطلق

أما اصطلاحاً فقد عُرِفَت شبكة الإنترنت بعدة مسميات، أبرزها "الشبكة العالمية" أو "شبكة الشبكات"، نظراً لطبيعتها المترابطة و امتدادها الواسع، فالإنترنت² جزء من ثورة الاتصالات ويعتبر أكبر شبكة حواسيب موسعة تغطي جميع أنحاء العالم، وتتصل بحواسيب شخصية وشبكات محلية وأخرى عامة، وبناء على ما تقدم فإن الإنترنت "شبكةً عملاقةً مكوّنةً من أجهزةٍ إلكترونيةٍ وميكانيكيةٍ وموادٍّ بَرْمَجِيَّةٍ وَعَنَاصِرٍ بَشَرِيَّةٍ تُسْتَخْدَمُ لِأَغْرَاضِ الْإِتِّصَالِ وَالْمَعْلُومَاتِ"، وتعني وصل جهازي حاسب أو أكثر معا عن طريق كوابل أو تقنيات خاصة من أجل تبادل المعلومات، مما يؤدي إلى تحقيق فوائد صعب الحصول عليها من خلال جاهز كومبيوتر واحد فقط، ما يعني أن شبكة الإتصال بالإنترنت وباقترانها بالحاسب الآلي تعتبر عنصراً مهماً في تكوين النظام المعلوماتي.

عليها اسم MILNET، بينما بقيت أربانت تخدم الاتصالات غير العسكرية. ومع انتشار أنظمة تشغيل يونكس (UNIX) التي تضمنت بروتوكولات الاتصال بالشبكة مثل TCP/IP، تزايد الضغط على أربانت مرة أخرى. وفي عام 1984، نُقلت مسؤولية الشبكة إلى مؤسسة العلوم الوطنية الأمريكية (NSF)، التي أنشأت عام 1986 شبكة أكثر سرعة وقدرة أُطلقت عليها اسم NSFNET، واستمرت هذه الشبكة في العمل بكفاءة حتى عام 1990، حين تم إيقاف تشغيل أربانت نهائياً بعد أكثر من 20 عاماً من الخدمة نتيجة قدم تقنياتها وكثرة مشكلاتها، بينما أصبحت NSFNET العمود الفقري الرئيسي لما نعرفه اليوم باسم الإنترنت. للمزيد، أنظر حسين محمد الغول، جرائم شبكة الإنترنت والمسؤولية الجزائية الناشئة عنها دراسة مقارنة، المرجع السابق، ص 13-14-15.

1- رصاع فتيحة، المرجع السابق، ص 7-8.

2- سعت الجزائر منذ وقت مبكر إلى الاستفادة من خدمات الإنترنت والتقنيات المرتبطة بها، حيث تم ربطها بالشبكة العالمية لأول مرة في مارس 1994 عبر مركز البحث على المعلومات العلمية والتقنية (CERIST) وقد أنشئ هذا المركز في أبريل 1986 بقرار من وزارة التعليم العالي والبحث العلمي، وكُلِّف منذ تأسيسه بمهمة محورية تمثلت في إنشاء شبكة وطنية للمعلومات وربطها بالشبكات الإقليمية والدولية، بما فيها الإنترنت، وفي إطار تنظيم هذا المجال وضمان تأطير استغلال خدمة الإنترنت، صدر المرسوم التنفيذي رقم 98-257 بتاريخ 25 أغسطس 1998 (منشور بالجريدة الرسمية عدد 63)، ثم جرى تعديل هذا المرسوم واستكمالته بموجب المرسوم التنفيذي رقم 307-2000 المؤرخ في 14 أكتوبر 2000 (منشور بالجريدة الرسمية عدد 60)، الذي حدد بدقة الشروط والكيفيات المتعلقة بتقديم خدمات الإنترنت واستغلالها داخل التراب الوطني الجزائري، أنظر درار نسيم، الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني -دراسة مقارنة، المرجع السابق، ص 8.

ولتحديد الأجهزة المرتبطة بهذه الشبكة العملاقة، فإن كل جهاز موصول بها مباشرة يكون له عنوان خاص يسمى عنوان الإنترنت "**Address IP**" وهذا العنوان عبارة عن رقم خاص يتكون من أربعة خانات وكل خانة يمكن أن تكون أي رقم في المدى من صفر إلى 255 من (00000000) إلى (11111111) بنظام العد الثنائي، وتكتب بهذه الطريقة مثلا (64,233,151,205).

وللاتصال بشبكة الانترنت فإنه يلزم توفير التجهيزات الخاصة بذلك، وكذلك يلزم الاشتراك مع مزود خدمة الانترنت (**Internet Service Provider-ISP**) المحلي الذي سيعطي المشترك أولا عنوان الانترنت (**Address IP**)، والذي سيكون عنوانا فريدا يميز المشترك من باقي المستخدمين لشبكة الانترنت على مستوى العالم، ثم يوصل المشترك بشبكة الإنترنت العالمية¹.

وهناك عدة طرق يمكن من خلالها الاتصال بشبكة الانترنت:

أ- **الاتصال الشبكي الهاتفي (Dial -up):** ويتم ذلك عن طريق الاتصال الهاتفي المباشر بمزود خدمة الانترنت من خلال رقم هاتفي محدد، وكل ما يحتاج إليه المستخدم في هذه الحالة هو خط هاتف عادي وجهاز حاسب آلي، وجهاز مودم خارجي "**Modem**"² لتحويل بيانات الحاسب الآلي الرقمية إلى إشارة تماثلية "**Analog**" يمكن نقلها عن طريق الهاتف كما لو كانت إشارة صوتية.

ب- **الاتصال عن طريق خطوط الاتصال الرقمية (Digital Subscriber Line -DSL):** ويتم ذلك عن طريق خط هاتف رقمي وليس عاديا تماثلها وجهاز موجه صغير

1- ذيب بن عايض القحطاني، أمن المعلومات، مدينة الملك عبد العزيز للعلوم والتقنية، الرياض، المملكة العربية السعودية، طبعة 2015، ص 40.

2- المودم هو جهاز توفيق يستخدمه المشترك للربط بين حاسبه الشخصي وجهاز الهاتف الذي يستخدمه في الإتصال بإحدى شركات الخدمة، وبمعنى آخر هو الوحدة التي تقوم بنقل المعلومات والبيانات من الحاسبات الآلية عبر خطوط التلغونات، والمودم نوعان أحدهما داخلي يثبت داخل الحاسب الآلي في شكل كارت، والآخر خارجي على شكل وحدة منفصلة توضع بجانب الحاسب لتتصل به عن طريق كابل، ولا يختلف النوعان في الوظائف التي يقومان بها. أنظر في ذلك، حسين محمد الغول، جرائم شبكة الإنترنت والمسؤولية الجزائية الناشئة عنها دراسة مقارنة، المرجع السابق، ص 12.

"Router" خارجي خاص بذلك، ويمكن أن يكون الجهاز الموجه سلكيا أو لاسلكيا في الوقت نفسه، و يوصل بالحاسب الآلي من خلال منفذ الشبكات **"RJ45"** ويمكن ربط أكثر من جهاز حاسب آلي على الموجه نفسه والخط نفسه في آن واحد معا، وكذلك يمكن إجراء المكالمات الهاتفية وتصفح الإنترنت على الخط نفسه في وقت واحد معاً، دون الحاجة إلى قطع الاتصال.

ت- **الاتصال اللاسلكي عن طريق شرائح شبكات الهاتف الجوال:** ويتم ذلك عن طريق بطاقات مزودة بشريحة هاتف جوال من الجيل الثالث (فأعلى) يوصل مباشرة بالحاسب الآلي عن طريق أحد منافذ (USB)، وتتميز هذه الطريقة بسرعة الاتصال حيث تصل في بعض الاحيان إلى 8.2 ميجابايت لكل ثانية، إلا أنها تعد عالية التكلفة ولا يمكن إجراء المكالمات الهاتفية من خلالها.

ث- **الاتصال عن طريق الشبكة المحلية (LAN):** يتم ذلك عن طريق توفير خدمة الإنترنت مركزيا، وبث هذه الخدمة من خلال شبكة الحاسب الآلي المحلية، وعند دخول المستخدم للشبكة المحلية يكون بإمكانه تصفح شبكة الإنترنت مباشرة، دون أن يكون لديه أي تجهيزات أو خطوط خاصة بذلك، وتطبق هذه الطريقة عادة لدى الشركات والجهات الحكومية التي لديها شبكات حاسب آلي محلية، ولديها عدد كبير من مستخدمي الإنترنت.

ج- **الاتصال عن طريق الأقمار الصناعية:** ويتم ذلك عن طريق طبق استقبال (دش، الصحن اللاقط) مزود برأس خاص بهذه الخدمة، موجه إلى القمر الصناعي المراد الاتصال عن طريقه، وكرت استقبال يوصل بالحاسب الآلي، ونظام تشغيل يدعم استقبال الإنترنت عن طريق الطبق، وتتميز هذه الطريقة بسرعة الاتصال، إلا أنها عالية التكلفة وتعد أقل أماناً من الطرق الأخرى¹.

1- ذيب بن عايض القحطاني، المرجع السابق، ص 41-42-43.

وخلاصة القول أن النظم المعلوماتية من الناحية التقنية يجب أن تتوفر فيها عدد من العناصر حتي ينطبق عليها هذا الوصف، وهذه العناصر هي المدخلات المعلوماتية والمعالجة المعلوماتية والمخرجات المعلوماتية، فضلا عن عنصر جديد أضاف بعداً جديداً للنظام المعلوماتي، وهو الاتصال (الانترنت) من خلال شبكات الاتصال ما بين النظم المختلفة، وبالتالي فإن مصطلح المعلومات والبيانات والمعطيات جميعها تعبر عن المدخلات للنظام المعلوماتي، وهذا ما عبرت عنه العديد من التشريعات حين استخدمت المصطلحات باعتبارها مترادفة تعبر عن بعضها، وأن التفرقة بينها هي تفرقة نظرية لا أثر لها في منظور القانون الجنائي، وإن اتخذت اشكالا متعددة وجب حمايتها جميعاً من أي اعتداء عليها.

المطلب الثاني: النظم المعلوماتية جنائيا.

في اللغة تعبر كلمة "جريمة" عن الجريمة أو عدم الشرعية أو الذنب، أما في سياق القانون الجنائي، تُعرّف الجريمة عادةً على أنها " فعل غير قانوني ناجم عن إرادة إجرامية"، وهو فعل غير قانوني، ويعترف القانون لها بعقوبة أو إجراء وقائي، أما في جانب المعلوماتية فكل باحث معروف له تعريفه الخاص لدراسة هذه الأفعال غير المشروعة، كما أن للفقهاء تعريفات عديدة لجرائم نظم المعلومات، بعضها يعتمد على الأساليب و الأفعال الإجرامية، وبعضهم يعتمد على موضوع الجريمة فقط، والبعض يؤكد أنها تعتمد على الطرفين أي الموضوع والوسيلة¹، وهنا نتناول تعريف جرائم نظم المعلومات بناء على وجهة نظر الفقه ومناهجه المختلفة في الفرع الاول، ونتناول خصائص جريمة نظم المعلومات في الفرع الثاني.

الفرع الاول: تعريف جرائم نظم المعلومات.

يشير تعدد المصطلحات المستعملة للتعبير عن هذه الجرائم إلى مدى أهمية هذا الموضوع، إذ ثمة اختلاف واسع بشأن الاصطلاحات المستخدمة للدلالة على الظاهرة الإجرامية الناشئة ضمن بيئة نظم المعلومات، وهو تباين واكب مسيرة تطور الظاهرة الإجرامية بداية من مصطلح إساءة استخدام الكمبيوتر، مروراً بمصطلح الاحتيال المعلوماتي والجريمة المعلوماتية، وصولاً إلى جرائم نظم المعلومات، فكل من المصطلحات يعكس مرحلة من مراحل تطور الفقه القانوني

1- أيمن عبدالله فكري، المرجع السابق، ص73-74.

والتقني للظاهرة الاجرامية، ولذلك تتبع أهمية معيار تحديد المصطلح المستخدم في التعريف إلى ما يلي:

➤ اختيار المصطلح يشترط فيه أن يجمع بين بعدي التكنولوجيا والقانون معاً، وإذا رجعنا إلى تقنية المعلومات سنجد أنها مرتبطة بفرعين يندمجان نتيجة التطور (أجهزة الكمبيوتر والاتصالات) فالحواسيب تعتمد على استخدام وسائل تقنية لإدارة وتنظيم معالجة البيانات في إطار تنفيذ مهام محددة مرتبطة ارتباطاً وثيقاً بعلمي الحاسوب والمنطق، أما الاتصال فتعتمد على وسائل نقل المعلومات بكافة دلالاتها العامة ومضامينها، ومع تزاوج واندماج الحاسبات ووسائل الاتصال يتجلى هذا الاندماج في صورة تقنية واطلق عليها مصطلح تقنية المعلومات **"Information Technology"**.

وفي مواجهة هذا الواقع، كان هناك العديد من المصطلحات التي تعبر عن الجرائم المتعلقة بالتكنولوجيا، بعضها يعبر عن السلوكيات المتعلقة بالحاسوب بطريقة معينة، والبعض الآخر يعبر عن السلوكيات التقنية، والبعض الآخر يعبر عن عموم التقنية باعتبار ما تحقق من التكامل والتناغم بين المجالات التقنية من ميادينها، ومع توسع الإنترنت، ظهرت مصطلحات جديدة ، تحاول دمج البيئة المشتركة للوسائط التقنية وطرق المعالجة ، وتبادل المعلومات.

➤ دقة اختيار الاصطلاح حيث يجب أن ينطلق من ضرورة التمييز بين الاصطلاحات الأخرى المنتمية لما يعرف بأخلاقيات الكمبيوتر وبين ما يعرف بإجرام التقنية أو جرائم الكمبيوتر، وهو ما يجيب عن التساؤل بشأن حدود انتهاء العبث وبداية المسؤولية عن الأفعال الجنائية، ولهذا نجد مصطلح إساءة استخدام الكمبيوتر ينتمي لطائفة الاصطلاحات ذات المحتوى الأخلاقي.

➤ ضرورة أن يكون المصطلح قادر على التعبير عن حدود محله بدقة، بحيث يكون شاملاً لما يعبر عنه، ومن هذا المنطلق، فإن كل اصطلاح وصف الظاهرة الإجرامية بدلالة إحدى جرائم الكمبيوتر كان قاصراً عن الإحاطة الشاملة بالظاهرة، فمصطلحات مثل، إحتيال الكمبيوتر أو غش الكمبيوتر وغيرها، أطلقت على أفعال محددة من بين أفعال جرائم

الكمبيوتر وصورها وليس على الظاهرة برمتها، كما أن تعبير جرائم التقنية العالية أو جرائم تقنية المعلومات هي تعبيرات في الفترة التي اطلقت فيها يقصد منها التعبير عن جرائم نظم المعلومات حتى قبل ولادة واتساع استخدام شبكة الإنترنت، وتظل تعبيرات واسعة الدلالة تحيط بأكثر مما تحتوى عليه ظاهرة جرائم نظم المعلومات¹.

وهنا ظهرت العديد من المصطلحات في بدايات الظاهرة واتسع استخدامها عند الفقهاء والدارسين كالغش المعلوماتي أو غش الحاسب والاحتيال المعلوماتي وغيرها، التي يجمعها التركيز على أن الظاهرة الاجرامية المستحدثة تتمحور رغم اختلاف أنماط السلوك الإجرامي حول فعل الغش أو النصب أو الإحتيال، ولكنها كما ذكرنا سابقا تستخدم الجزء للدلالة على الكل في حين أن هناك مصطلحات أخرى أكثر دقة للتعبير عن هذه الظاهرة الإجرامية.

ومن المصطلحات الشائعة في كثير من الدراسات مصطلح " الجرائم الاقتصادية المرتبطة بالحاسوب **Computer-Related Economic Crime**"، وهو تعبير يقتصر على الجرائم التي تستهدف معلومات قطاعات الأعمال أو التي تمس سرية المعلومات أو سلامتها أو توافرها، وبالتالي، يخرج من نطاق هذا المصطلح الجرائم التي تستهدف البيانات الشخصية، أو تلك التي تنتهك الحقوق المعنوية على المصنفات الرقمية (حقوق الملكية الفكرية)، وغيرها من الأنماط الأخرى. وعليه، فإن هذا الاصطلاح لا يعبر بشمولية ودقة عن جميع صور وأنماط جرائم نظم المعلومات والحاسوب.

وثمة كذلك العديد من المصطلحات التي غلب عليها الطابع الإعلامي كمصطلح "جرائم أصحاب الياقات البيضاء **White-Collar Crimes**" غير أن الدقة العلمية تقتضي أن ينطبق الوصف على الموصوف بدقة تامة، فجرائم أصحاب الياقات البيضاء أوسع نطاقاً بكثير من مجرد جرائم نظم المعلومات أو الحاسوب، إذ تشمل مختلف أشكال السلوك الإجرامي في بيئة الأعمال بجميع أنواعها وقطاعاتها، وعليه، فإن هذا المصطلح لا يُعد تعبيراً دقيقاً كافياً عن ظاهرة جرائم الحاسوب تحديداً، مع العلم بأن جرائم الحاسوب تندرج فعلاً تحت مظلة جرائم

1- أيمن عبدالله فكري، المرجع السابق، ص 75-76.

أصحاب الياقات البيضاء، لكنها لا تُمثل إلا جزءاً من طائفة واسعة ومتنوعة من الجرائم التي يشملها هذا التصنيف.

أما بالنسبة لمصطلحي "جرائم الكمبيوتر" **Computer Crimes** و "الجريمة ذات الصلة بالكمبيوتر" **Computer –related Crimes**، فلم يمكن التمييز بينهما في بداية الظاهرة متيسراً، ولكن من منظور تطور الظاهرة ونمط محاولة الفقهاء التعرف على جرائم نظم المعلومات، فإن البعض بدأ منهم استخدام مصطلح جرائم الكمبيوتر، وهنا يشير المصطلح إلى السلوكيات التي تستهدف أجهزة الكمبيوتر، مثل الوصول غير المصرح به وتدمير البيانات المخزنة، أما مصطلح الجرائم المرتبطة أو ذات الصلة بالكمبيوتر فهي تلك الجرائم التي تعد فيها أجهزة الكمبيوتر وسيلة من وسائل ارتكاب الجريمة ، مثل الاحتيال والتزوير عبر الكمبيوتر، ومع ذلك، فإن هذا الاستخدام ليس قاعدة، فالفقيه الألماني **Sieber Ulrich** و الأمريكي **Praker**، يستخدمون هذين المصطلحين بشكل مترادف للدلالة على جميع أشكال جرائم الكمبيوتر، سواء كان الكمبيوتر هو الهدف أو الوسيلة أو البيئة للجريمة، لكن هذين المصطلحين لا يزالان يمثلان هذه الظاهرة -نظم المعلومات- بشكل أكثر دقة، حتى وأن كانا ولدا قبل ولادة الشبكات على نطاق واسع و الإنترنت خاصة، وحتى بعد الإنترنت لا يزال الكثير من الناس يستخدمون نفس المصطلحين، وذلك لأن الإنترنت بمعناه الشامل ما هو إلا أحد مكونات هذا النظام، ولأن النظام من جديد أصبح يعبر عنه نظام الكمبيوتر فأصبح بعضهم يضيف تعبير الإنترنت إلى تعبير الكمبيوتر فيقول "جرائم الكمبيوتر والإنترنت" وهذا لمنع الإرباك لدى المتلقي ولكي يدرك المتلقي أن كافة الجرائم التي تقع على المعلومات متضمنة في التعبير¹.

1- أيمن عبدالله فكري، المرجع السابق، ص 77-78.

وهنا نرى تفضيل مصطلح جرائم نظم المعلومات على غيره من المصطلحات وذلك لسببين هما:

- أنه مصطلح يعبر عن محل الأنشطة الإجرامية ويمكنه أن يتواءم مع التطورات المستحدثة في مجال المعلوماتية و وظيفتها في الحياة الاجتماعية، دون أن يتم حصرها في نطاق وسيلة معينة.
- أن المصطلحات الأخرى تربط نفسها بأداة و وسيلة ارتكاب الأنشطة الإجرامية، أو تحصرها في نطاق نوع معين مما يؤدي إلى تجدد ظهور المشاكل القانونية في تطبيق النصوص على الوقائع.

ولغرض تحديد ماهية جرائم نظم المعلومات وتمييزها عن الجرائم التقليدية، فقد تعددت التعريفات التي قدمها الفقهاء والباحثون، وتتنوع هذه التعريفات تبعاً لتخصص الباحث وللمعيار المعتمد في التعريف، فمن جهة، اختلفت التعريفات بين من ينظرون إلى الظاهرة الإجرامية الناشئة عن استخدام الحاسوب من المنظور التقني، وبين من ينظرون إليها من المنظور القانوني، ومن جهة أخرى، وحتى ضمن المنظور القانوني نفسه، تختلف التعريفات حسب مجال الحماية المستهدفة؛ فتختلف التعريفات تبعاً لما إذا كان البحث يدور حول حماية النظام الجنائي العام، أو حماية الحياة الخاصة والخصوصية، أو حماية الملكية الفكرية والحقوق المعنوية على المصنفات الرقمية¹.

هنا تنقسم التعريفات إلى فئتين: الفئة الأولى هي مجموعة تعريفات تستند إلى معيار واحد، بما في ذلك التعريفات القائمة على المعايير القانونية، كتعريفها بدلالة موضوع الجريمة والسلوكيات محل التجريم، وتشمل أيضاً تعريفات قائمة على معيار شخصي، والفئة الثانية مجموعة من التعريفات مبنية على معايير متعددة، بما في ذلك التعريفات التي تسلط الضوء على موضوع الجريمة وأنماطها، وكذلك بعض العناصر المتعلقة بالأساليب الإجرامية، وبيئة ارتكابها².

1- شعبان سمير، الجريمة الإلكترونية مقارنة تحليلية لتحديد مفهوم الجريمة والمجرم، مجلة دراسات وأبحاث، العدد 1، جامعة الجلفة الجزائر، 2009، ص 115.

2- أيمن عبدالله فكري، المرجع السابق، ص 81-82.

1- التعريفات التي تستند إلى أداة ارتكاب الجريمة.

ينطلق أصحاب هذا الاتجاه من حقيقة أن جرائم نظم المعلومات تتحقق باستخدام الكمبيوتر كوسيلة إجرامية، وفي هذه التعريفات أنها " فِعْلٌ إجْرَامِيٌّ يَسْتَعْدِمُ الْكُمْبِيُوتَرُ فِي ارْتِكَابِهِ كَأَدَاةٍ رَئِيسِيَّةٍ "، وعرفها "Tiedemaun" بأنها " كُلُّ أَشْكَالِ السُّلُوكِ غَيْرِ الْمَشْرُوعِ الَّذِي يَرْتَكِبُ بِاسْتِخْدَامِ الْحَاسِبِ "، وانتقد البعض هذا التعريف للأسباب التالية:

- أن هذا التعريف عام و واسع للغاية، لأنه يشمل جميع الأعمال غير المشروعة التي تعرض المجتمع للخطر، ولأن الجريمة بمفهومها العام عمل غير قانوني يعرض المجتمع للخطر، فهي تنتمي إلى فئة جرائم المعلومات، وهو أمر غير مقبول، بالرغم من أن التعريف يحتفظ وينص على أن الأعمال غير القانونية مرتبطة باستخدام أجهزة الكمبيوتر، إلا أن ذلك لا ينفي أن يشمل أو ممكن أن يشمل كافة الجرائم التقليدية.
- أنه تعريف غير منطقي إذ لم يوضح أنه يخص بعض الجرائم التي لا يمكن تصور وقوعها إلا عبر الحاسب الآلي، ولو تم توضيح ذلك لكان قد قلل من عموميته وجعله أقرب للتعريفات العلمية الدقيقة، كما أن مجرد استخدام الحاسب الآلي لا يضيف أي جديد على السلوك غير المشروع، ولكن استخدام البيانات والمعلومات والبرامج هو الذي يمكن أن يضيف إلى الجريمة المعلوماتية سمتها الخاصة بها¹.

وعرفها كلاً من "A. Hardcasteg .R. Tattoy" من خلال تعريفهما للجرائم المرتبطة أو ذات الصلة بالحاسب بأنها " تِلْكَ الْجَرَائِمُ الَّتِي يَكُونُ قَدْ وَقَعَ فِي مَرَاجِلِ ارْتِكَابِهَا بَعْضُ عَمَلِيَّاتٍ فِعْلِيَّةٍ دَاخِلَ نِظَامِ الْحَاسِبِ، وَبِعِبَارَةٍ أُخْرَى تِلْكَ الْجَرَائِمُ الَّتِي يَكُونُ دَوْرَ الْحَاسِبِ فِيهَا إِجَابِيًّا أَكْثَرَ مِنْهُ سَلْبِيًّا ".

1- أيمن عبدالله فكري، المرجع السابق، ص 83-84.

وأخذ بهذا الاتجاه في التعريف لجرائم نظم المعلومات من ناحية وسيلة ارتكابها كلاً من الفقيهان **"Michel & Credo"** وذلك من خلال تعريفها بأنها " أَسْتَحْدَامُ الْحَاسِبِ كَأَدَاةٍ لِارْتِكَابِ الْجَرِيمَةِ فَضْلاً عَنِ الْحَالَاتِ الْمُتَعَلِّقَةِ بِالْوُلُوجِ غَيْرِ الْمُصَرَّحِ بِهِ لِحَاسِبِ الْمَجْنِيِّ عَلَيْهِ أَوْ بَيِّنَاتِهِ ¹".

بالرغم من عدم إمكانية إنكار دور الحاسب الآلي أو نظم المعلومات في ارتكاب الجريمة، فإن الفقه الجنائي ينتقد -بشكل عام- الاعتماد على "وسيلة ارتكاب الجريمة" كمعيار أساسي للتعريف، والسبب في ذلك أن القانون الجنائي لا يركز على الأداة أو الوسيلة التي استُخدمت في الجريمة، بل ينصبّ اهتمامه أساساً على طبيعة الفعل أو النشاط غير المشروع الذي ارتكبه الجاني على الحق أو المصلحة المحمية التي تمّ المساس بها، وبالتالي، فإن مجرد اشتراك الحاسب الآلي أو نظم المعلومات في عملية ارتكاب الجريمة لا يكفي وحده لاعتبارها "جريمة معلوماتية" أو جريمة خاصة بنظم المعلومات.

2- التعريفات التي تستند إلى محل أو موضوع ارتكاب الجريمة.

تستند هذه التعريفات إلى موضوع الجريمة أو أنماط السلوك محل التجريم كونها " نشاطٌ غَيْرُ مَشْرُوعٍ مَوْجَّهٍ لِنَسْخِ أَوْ تَغْيِيرِ أَوْ حَذْفِ أَوْ الْوُصُولِ إِلَى الْمَعْلُومَاتِ الْمُخَزَّنَةِ دَاخِلَ الْحَاسِبِ أَوْ الَّتِي تَحُولُ عَنْ طَرِيقَةٍ "، ولكن هذا الرأي لم يسلم من الانتقاد كون أن التعريف بدأ صحيحاً وانتهى معيباً فبعد أن بين أن جريمة الحاسب تعتبر من الجرائم المحصورة في إطار نشاط معين وهو ما يتوافق ومبدأ الشرعية الجنائية، لكنه أنهى إلى توسيع غير مقبول بنصه على أي نشاط غير مشروع يتعلق بالمعلومات التي يمكن أن تحول عن طريق الحاسب ليبقى الباب واسعاً أمام التفسيرات بما يتعارض ومبدأ المشروعية في تحديد النشاط الإجرامي.

وقد حاول كلاً من الاساتذة **"Le Stanc & Vivant"** أن يقوموا بصياغة تعريف يأخذ في الاعتبار موضوع الجريمة وذلك بوصفها بأنها " مجموعة الأفعال غير المشروعة والمرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب"، غير أن هذا التعريف يؤخذ عليه استناده إلى

1- رصاع فتيحة، المرجع السابق، ص 41.

معيّار احتمال جدارة الفعل للعقاب وهو معيار غير مضبوط ولا يتوافق مع التعريفات القانونية الدقيقة، وإن كان يصلح لتعريف في نطاق دراسات العلوم الاجتماعية¹.

ولم يقتصر الأمر على الفقه في محاولة وضع تعريفات لجرائم نظم المعلومات، بل ساهمت أيضاً الهيئات والمؤسسات المهتمة بدراسة الجريمة المعلوماتية بوضع تعريف لها، ففي اجتماع باريس عام 1983 ضمن حلقة "الاجرام المرتبط بتقنية المعلومات" عرف خبراء منظمة التعاون الاقتصادي والتنمية جرائم نظم المعلومات على أنها "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و/أو نقله"²، وتبنى هذا التعريف الفقيه الألماني "Ulrich Sieber" معتمداً في التعريف على معيارين أولهما وصف السلوك، وثانيهما اتصال السلوك بالمعالجة الآلية للبيانات.

وقد امتدح جانب من الفقه هذا التعريف فوصفه بأنه تعريف مرّن وعام وشامل، بينما رأى فيه بعضهم الآخر بأنه يتسبب بسبب اتساعه في أرباك الباحثين ويقلل النفع به بالنسبة للفقهاء، كما أنه يمد نطاق التجريم إلى دائرة الأخلاق التي تخرج عن نطاق التجريم وفقاً للقانون الجنائي³.

3- التعريفات تستند لأداة ارتكاب وموضوع الجريمة.

تعتمد هذه التعريفات على معايير متعددة، فيعرف جزء من الفقه جرائم نظم المعلومات بناءً على عدة معايير قانونية، المعيار الأول يعتمد على محل الجريمة، والمعيار الثاني يعتمد على وسيلة ارتكاب الجريمة، وكلا المعيارين يشملهم (نظام المعلومات) لأنه يلعب دور الضحية والوسيلة حسب الفعل المرتكب، حيث يعرفونها بأنها "أيّ صَرْبٍ مِنْ النَّشَاطِ الْمَوْجَّهٍ ضِدَّ أَوْ الْمُنْطَوِي عَلَى اسْتِخْدَامِ نِظَامِ الْحَاسِبِ"، فهي "كل جريمة تستخدم الحاسوب كأداة لارتكابها، أو تمثل الإغراء للقيام بذلك، أو جريمة يكون الكمبيوتر نفسه ضحية لها".

1- شعبان سمير، المرجع السابق، ص 119.

2- بلال بن جامع، المرجع السابق ص 115.

3- أيمن عبدالله فكري، المرجع السابق، ص 86-88.

وفي إجاباتهم على استبيان منظمة التعاون الاقتصادي والتنمية **OECD**، عرّف الخبراء في بلجيكا أيضًا جريمة نظام المعلومات على أنها "كُلُّ فِعْلٍ أَوْ امْتِنَاعٍ عَنِ فِعْلٍ مِنْ شَأْنِهِ الإِعْتِدَاءُ عَلَى ، الأَمْوَالِ المَادِّيَّةِ أَوْ المَعْنَوِيَّةِ يَكُونُ نَاتِجًا بِطَرِيقَةٍ مُبَاشِرَةٍ أَوْ غَيْرِ مُبَاشِرَةٍ عَنِ تَدَخُّلِ التَّقْنِيَّةِ المَعْلُومَاتِيَّةِ"¹، هذا التعريف تم تبنيه من قبل العديد من الفقهاء والباحثون، لأن لديهم بوصفهم أفضل تعريف، لأنه واسع وشامل بقدر الإمكان للتعريف بظاهرة جرائم نظم المعلومات، ولأن التعريف أعلاه يعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صورها كما يسمح أيضًا امكانية التعامل مع التطورات التقنية المستقبلية².

4- التعريفات وفقا لسمات الجاني الشخصية.

قدّم جانب من الفقه تعريفات لجرائم نظم المعلومات تستند إلى السمات الشخصية للجاني، وتحديدًا إلى درجته العالية من المعرفة والدراسة التقنية بتكنولوجيا الحاسوب ونظم المعلومات، ومن هذه التعريفات أنها "الجرائم التي يتطلب إلماها خاصا بتقنيات الحاسب ونظم المعلومات، لارتكابها أو التحقيق فيها ومقاضاة فاعلها"، وبمعنى آخر، هي الجرائم التي يستغل فيها الجاني معرفته المتخصصة بالحاسوب ونظم المعلومات للقيام بتصرف غير مشروع أو محظور قانوناً.

كما عرفها الأستاذ **"Thompson"** بأنها "أَيُّ جَرِيْمَةٍ يَكُونُ مُتَطَلِّبًا لِإِقْتِرَافِهَا أَنْ تَتَوَافَرَ لَدَى فَاعِلِهَا مَعْرِفَةٌ بِتَقْنِيَّةِ الحَاسِبِ"، وحسب هذا التعريف فإنه يشترط أن يكون مرتكب الجريمة المعلوماتية على درجة كبيرة من العلم بتكنولوجيات الحاسبات³، أما الأستاذ **"Schjqlberg"** فقد عرفها بأنها "أَيُّ فِعْلٍ غَيْرِ مَشْرُوعٍ تَكُونُ المَعْرِفَةُ بِتَقْنِيَّةِ الكُمْبِيُوتَرِ أَسَاسِيَّةً لِإِرْتِكَابِهِ والتَّحْقِيقِ فِيهِ وَمَلاحَظَتُهُ قَضَائِيًّا"، إضافة إلى ذلك عرفها الفقيه **"Donn B. Parker"** الذي يرى بأنها "أَيُّ فِعْلٍ مُتَعَمِّدٍ مُرْتَبِطٌ بِأَيِّ وَجْهِ، بِالحَاسِبَاتِ، يَتَسَبَّبُ فِي تَكْبِيدِ أَوْ أَمْكَانِيَّةِ تَكْبِيدِ المَجْنِيِّ عَلَيْهِ لِخَسَارَةٍ أَوْ حُصُولٍ أَوْ امْكَانِيَّةِ حُصُولِ مُرْتَكِبِهِ عَلَى مَكْسَبٍ مِنْ إِسَاءَةِ اسْتِخْدَامِ الحَاسِبِ"⁴.

1- رصاع فتيحة، المرجع السابق، ص 40.

2- أيمن عبدالله فكري، المرجع السابق، ص 89.

3- سعيداني نعيم، المرجع السابق ص 27.

4- شعبان سمير، المرجع السابق، ص 117.

وفي دراسة وضعها معهد ستانفورد للأبحاث وتبنتها وزارة العدل الأمريكية في دليلها لعام 1979، حيث عرفت بأنها "أية جريمة يتمتع فاعلها بمعرفة فنية بالحواسيب تمكنه من ارتكابها"، إلا أن التعريفات وفق للسمات الشخصية الخاصة بمرتكب الفعل الإجرامي، هو أمر وإن كان له وجود فعلي بإعتباره من الشروط المفترضة فيمن يقوم بتلك الأفعال الإجرامية، إلا أن التعريف وفقاً لها يعد امراً قاصراً، إذ لا تحيط بحقيقة الأفعال غير المشروعة ولا تسهم في توضيح مفهوم جرائم نظم المعلومات بشكل كامل، كما أنها تتطلب البحث في ظروف خاصة بشخصية الجاني، وهذا ما لا يعتد به في القانون الجنائي إلا استثناء، باعتباره قانون موضوعي يركز على الفعل نفسه لا على صفات مرتكبه، فضلاً عن ذلك، فإن الأخذ بهذا المعيار يضيق نطاق الجريمة المعلوماتية إلى حد قد يجعلها شبه أسطورية، إذ يقتصر تعريفها على الحالات التي تتطلب فيها مستوى عالي من المعرفة التقنية لارتكابها.

وهنا نجد ان البعض من الفقه ذهب إلى التشكيك في إمكانية وضع تعريف يحدد مفهوم الجريمة المعلوماتية وأرجعوا صعوبة ذلك إلى عاملين رئيسيين هما:

- الخشية من حصر نطاق الجريمة داخل إطار يضر بها، وذلك لأن الطبيعة الفنية للجريمة المعلوماتية تفترض صعوبة في حصرها داخل غطاء قانوني تجريبي محدد.
- نظراً للطابع الدولي الواضح للجريمة المعلوماتية، يتعين أن يكون التعريف موحدًا ومقبولاً على نطاق دولي واسع، حتى يتسنى العمل به فعلياً وتنسيق التعاون الدول فيما بينها في كافة المجالات المتعلقة بمكافحة الإجرام المعلوماتي¹.

وهنا نتفق مع الرأي الثالث، أي من منظور شمولية مصطلح جريمة الكمبيوتر بالنسبة لمصطلح الجريمة المعلوماتية، فإنه يعتمد في تعريفه على الموضوع والأداة الإجرامية، ولأن الجريمة المعلوماتية تشمل من الناحية المفاهيمية الهجمات على المعلومات والبرامج داخل جهاز الكمبيوتر فهي محددة، أما مصطلح جريمة الكمبيوتر فهو أكثر عمومية وشمولية من حيث المفهوم والمحتوى، وهي جريمة تُرتكب على جهاز الكمبيوتر و باستخدام الكمبيوتر كأداة ويشكل الاعتداء عليه الاعتداء على المعلومات والبرامج من حيث المضمون.

1- أيمن عبدالله فكري، المرجع السابق، ص 91.

ونرى أن تعريف الجريمة المعلوماتية " هي جميع الأعمال غير القانونية التي تستخدم أجهزة الكمبيوتر أو أي وسيلة تقنية وتستهدف حذف المعلومات أو إضافتها أو معالجتها أو سرقتها أو تغييرها أو تعديلها لأغراض غير قانونية "، مع ملاحظة أن مسمى جرائم الكمبيوتر أو الجرائم الإلكترونية من حيث المنهج هي أشمل من جرائم المعلوماتية، لأن كل البيانات والمعلومات التي يتم تغييرها أو التلاعب فيها تتم بواسطة جهاز الحاسوب وعن طريقه، فالمعلومات محل الجريمة هي جزء من أجهزة الحاسوب مع الإشارة إلى أن مسمى الجرائم المعلوماتية، لا يعد أقل أهمية من مسمى الجرائم الإلكترونية، فالمعلومات وجهاز الحاسب هما الأساس في قيام هذا النوع من الجرائم.

الفرع الثاني: خصائص جرائم نظم المعلومات.

تتميز جرائم نظم المعلومات بمجموعة من الخصائص تميزها عن غيرها من الجرائم المستحدثة والتقليدية نظراً لحدثة هذه الجريمة والوسائل المستخدمة في إرتكابها وغياب المفهوم العام المتفق عليه بين الدول حول التعريف القانوني للنشاط الاجرامي المتعلق بهذا النوع من الإجرام، هذا ما يجعل الجريمة المعلوماتية تتميز بخصائص تميزها عن باقي الجرائم، ومن هذه الخصائص:

أولاً: الجرائم المعلوماتية جرائم عابرة للحدود.

تعد الجرائم المعلوماتية من الجرائم غير المحددة والمرتبطة بنطاق جغرافي محدد، فمن الممكن أن تُنفذ الجريمة في أي وقت دون التقيد بدولة ما أو منطقة ما أو بقرب المسافات أو بعدها، وترتكب عادة عبر شبكة الاتصالات العالمية أو من خلال الأقمار الصناعية بواسطة أجهزة الحاسوب، فمن المحتمل أن يرتكب الجاني جريمة في بلد ويكون المجني عليه في بلد آخر، وقد يلحق الضرر الناتج عن الجريمة المعلوماتية بأماكن عديدة، وهذا مفاده أن الجريمة المعلوماتية تتسم بالتباعد الجغرافي بين الفعل والمجني عليه، ومن الناحية التقنية التباعد بين أداة الجريمة ومحلها، وهذا التباعد قد يكون ضمن إطار الحدود الوطنية للدولة أو

خارجها ليصيب دولة أخرى يتواجد فيها نظام الحاسوب الذي حفظت فيه المعلومات محل الاعتداء¹.

أن هذه الطبيعة التي تتميز بها الجريمة المعلوماتية بكونها عابرة للحدود خلقت العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي لهذه الجريمة، وكذلك حول القانون الواجب التطبيق، فضلاً عن الإشكاليات المتعلقة بإجراءات الملاحقة والمتابعة القضائية².

وهنا يطرح السؤال اذا تجاوزت الجريمة المعلوماتية حدود دولة ما فأى الدول يحق لها تحريك دعوى الحق العام بحق المتهم، وكيف يتم تحديد الاختصاص القضائي؟

من المقرر قانوناً أن حكام الإجراءات الجنائية تحدد نطاق الاختصاص القضائي للجرائم أستناداً إلى موقع ارتكاب الفعل الإجرامي أو مكان اعتقال المتهم، أو موطنه، وفي الإطار العربي فقد نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2014 في المادة 30 منها على الآتي " تَلْتَزِمُ كُلُّ دَوْلَةٍ طَرَفٍ بِتَبْنِيِ الْإِجْرَاءَاتِ الصَّرُورِيَّةِ لِمَدِّ اخْتِصَاصِهَا عَلَى أَيِّ مِنْ الْجَرَائِمِ الْمَنْصُوصِ عَلَيْهَا فِي الْفَصْلِ الثَّانِي مِنْ هَذِهِ الْإِتِّفَاقِيَّةِ وَذَلِكَ إِذَا ارْتَكَبَتْ الْجَرِيمَةُ كُلِّيًّا أَوْ جُزْئِيًّا أَوْ تَحَقَّقَتْ أ - فِي أَقْلِيمِ دَوْلَةٍ طَرَفٍ ب - عَلَى مَتْنِ سَفِينَةٍ عَلَى الدَّوْلَةِ طَرَفُ ج - عَلَى مَتْنِ طَائِرَةٍ مُسَجَّلَةٍ تَحْتَ قَوَانِينِ الدَّوْلَةِ الطَّرَفِ د - إِذَا كَانَتْ الْجَرِيمَةُ تَمَسُّ أَحَدَ الْمَصَالِحِ الْعُلْيَا لِلدَّوْلَةِ "³.

إضافة إلى ذلك فقد أحيالت اتفاقية بودابست الموقعة في 23 نوفمبر 2001 بخصوص الجرائم المعلوماتية الإجراءات الجنائية ومنها الاختصاص القضائي إلى الدول الموقعة على الاتفاقية أو الأطراف فيها، فنصت المادة 14 من الاتفاقية على " يَجِبُ عَلَى كُلِّ طَرَفٍ أَنْ يَتَّخِذَ الْإِجْرَاءَاتِ التَّشْرِيعِيَّةَ، وَغَيْرَهَا مِنْ التَّدَابِيرِ، وَفَقَّ لِقَانُونِهَا الدَّاخِلِيَّ وَإِطَارِهَا الْقَانُونِيَّ،

1- سعيداني نعيم، المرجع السابق ص 32.

2- ربيعي حسين، المرجع السابق، ص 28.

3- المادة 30 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات عام 2014.

لإقرار السلطات والإجراءات المنصوص عليها في هذا القسم لأغراض التحقيقات أو الإجراءات الجنائية الخاصة¹.

ثانيا: الجرائم المعلوماتية جرائم صعبة الإثبات و الاكتشاف.

من المعروف أن الجرائم المعلوماتية حال وقوعها لا تخلف بصمات مادية ملموسة لأنها تُنفذ في الخفاء ودون ترك دليل يشير إلى فاعليها، خلافاً للجرائم التقليدية التي يخلف مرتكبها عادة آثار مادية وشواهد ملموسة كالدماء أو الجثة أو أدلة مادية كالشعر أو البصمات، كما أن الجاني في الجرائم المعلوماتية يستطيع طمس ومحو وإزالة الأدلة التي تدينه خلال ثوان، وتعتبر هذه الخاصية من أهم الخصائص المميزة لجرائم نظم المعلومات، فضلاً عن ذلك غالباً ما ترتكب الجريمة المعلوماتية دون أن يتلاقى طرفا الجريمة (الجاني والمجني عليه)، فقد لا ينتبه أو يعي المجني عليه ذاته أنه وقع ضحية لجريمة معلوماتية أو قد يدرك لكنه يتردد عن الإبلاغ عنها خوفاً من أن تلحقه أضرار أضاقه إذا ما أعلن عن ذلك، لاسيما في حالة كون الضحية أحد المصارف أو الهيئات المالية أو التجارية، فيفضي ذلك إلى الإخلال بالمركز المالي لها واهتزاز وزعزعة ثقة المتعاملين معها، وفي هذا الصدد يعتقد معظم الخبراء أن 15 بالمائة من جرائم الاحتيال والتلاعب المعلوماتي يتم الإعلان عنها من قبل الشركات والمؤسسات المجني عليها وإن العديد من هذه الجرائم تمر دون اكتشافها ويندر أن تتم إحالة الحالات المكتشفة للقضاء².

بالإضافة إلى ذلك يوجد العديد من الأسباب والعوامل تجعل من جرائم نظم المعلومات صعبة الاكتشاف والإثبات³ كوسيلة تنفيذها كما ذكرنا سابقاً التي تتميز في أغلب الأحيان

1- المادة 14 من اتفاقية بودابست بشأن مكافحة الجريمة المعلوماتية عام 2001.

2- دلخار صلاح بوتاني، المرجع سابق، ص51.

3- تعد صعوبة كشف جرائم نظم المعلومات قضية نسبية أمام كفاءة التحقيقات الدولية والمنسقة إذ نجح المحققون في الولايات المتحدة الأمريكية من تفكيك شبكة تجسس إلكتروني معقدة قادها متسللين "إسرائيليون" تمكنوا من الوصول إلى معلومات حساسة داخل أجهزة الكمبيوتر الأمريكية والإسرائيلية، حيث أثبت التحقيق أن مصدر الاختراق كان من داخل "إسرائيل" وبالتعاون مع سلطات التحقيق "الإسرائيلية" تم تحديد هوية الجناة وضبط جميع المعدات المستخدمة في الاختراق، وفي الوقت ذاته تمكنت السلطات الألمانية من تحديد مرتكبي جريمة الاحتيال المعلوماتي وهذا من خلال الاتصال بين أجهزة الكمبيوتر الألمانية وشبكة الاتصالات

بالطابع التقني الذي يضيف عليها الكثير من التعقيد، كما يتيح النظام الرقمي إمكانية اتلاف البيانات التي قد تستخدم كأدلة في سياق الأثبات القانوني خلال فترة زمنية لا تتجاوز الثانية الواحدة، حيث يكاد يكون الدليل الرقمي عملياً وسيلة الإثبات الرئيسية والوحيدة المتاحة التي يمكن من خلالها تعقب أثر الجاني، ومع ذلك تتميز بسهولة طمسها وإخفائها بالكامل¹، كما أنها صعبة الاكتشاف بسبب نقص الخبرة الفنية لدى المحققين في هذه الجرائم التي ترتكب في الغالب بوسائل تقنية متطورة، والتي تقتضي إماما واسعا باستخدام الحاسب الآلي وملحقاته.

وعلى سبيل التوضيح سجلت وزارة الداخلية الفرنسية عام 1986 نحو 1200 حالة جريمة معلوماتية، مقارنة بحوالي 53600 جريمة ضد الأشخاص، و18900 جريمة تصنف ضمن فئة الانتهاكات الأخلاقية، بالإضافة إلى ثلاثة ملايين جريمة تستهدف الأصول المالية، أما في التقرير الذي أصدره مركز شكاوى احتيال الانترنت (IFFC) الأمريكي مؤخراً، أظهر التحليل الشامل للشكاوى التي قدمت للمركز خلال سنة 2004 قد بلغت 6348 شكاوى منها 5273 حالة تتعلق باختراق أنظمة الحاسوب عبر شبكة الانترنت و 814 حالة أخرى تتعلق بوسائل الدخول والاقترام الأخرى، كالدخول عبر الاتصالات الهاتفية أو الدخول المباشر إلى النظام بشكل مادي.

وبالرغم من أن نسبة الجرائم المعلوماتية المكتشفة والمسجلة أقل بكثير من نظيرتها في الجرائم التقليدية، فإن حجم الخسائر المالية الناجمة عن الجرائم المعلوماتية يرتفع بشكل صاروخي ويتجاوز بمراحل الخسائر الناتجة عن سائر أنواع الجرائم الأخرى التقليدية؛ فعلى سبيل المثال، بلغت الخسائر الناجمة عن (8000) حالة سرقة بالإكراه في فرنسا خلال عام 1986 ما مجموعه 561 مليون فرنك فرنسي، في حين أن الخسائر الناتجة عن الجرائم المعلوماتية - رغم

السويسرية، حيث تم ضبط البيانات المخترقة داخل حواسيب المتسللين وذلك بالتعاون مع السلطات السويسرية، وهذا ما يؤكد أن الجريمة المعلوماتية مهما بلغت من تعقيدات لم تعد ملاذاً آمناً عندما تتكاثر أجهزة نفاذ القانون عبر الحدود، للمزيد أنظر في ذلك ضرغام جابر عطوش آل مواش، جريمة التجسس المعلوماتي-دراسة مقارنة-، المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع، القاهرة، جمهورية مصر العربية، الطبعة الأولى، 2017، ص 31-32.

1- عبد الإله النوايسة، جرائم تكنولوجيا المعلومات شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، دار وائل للنشر والتوزيع، عمان الاردن، الطبعة الأولى 2018، ص 80.

أن عددها المكتشف يقل عن ثمانية أضعاف عدد حالات السرقة بالإكراه - تتجاوز هذا الرقم بأكثر من الضعف، وفي الولايات المتحدة الأمريكية، وقد خلص مكتب التحقيقات الفيدرالي (FBI) إلى أن متوسط الخسارة الناجمة عن الجريمة المعلوماتية الواحدة يصل إلى حوالي نصف مليون دولار أمريكي (500,000 دولار)، بينما لا يتعدى متوسط الخسارة في جرائم السرقة العادية (3500) ثلاثة آلاف وخمسمائة دولار أمريكي¹.

وفي الأخير يتضح إن الغالبية العظمى من جرائم نظم المعلومات لا تُكتشف إلا بالمصادفة المحضة، أو بعد مضي فترة زمنية طويلة جداً على ارتكابها، بل إن الجرائم التي ظلت طي الكتمان تفوق بأضعاف مضاعفة تلك التي تم كشفها، مما يعني أن هناك "رقماً مظلماً" خطيراً يفصل بين العدد الحقيقي للجرائم المعلوماتية المرتكبة فعلياً وبين العدد الضئيل الذي تم اكتشافه ورصده رسمياً، وهي فجوة هائلة ومقلقة تؤكد أن الجزء المرئي من جبل الجرائم المعلوماتية لا يعدو أن يكون مجرد قمته البارزة.

1- الجرائم المعلوماتية جرائم ناعمة.

المعروف عن جرائم نظم المعلومات أنها لا تستلزم اللجوء إلى أي شكل من أشكال العنف البدني أو بذل جهد عضلي كبير كما هو الحال في الجرائم التقليدية مثل القتل أو الاختطاف أو السرقة بالإكراه، بل تُرتكب بأقل قدر ممكن من الجهد الجسدي وتعتمد بالأساس على المهارة الذهنية العالية والدراية التقنية المتقدمة بآليات عمل الحواسيب وبرمجياتها وشبكات الاتصال، ومن ثَمَّ، فإن الجاني هذه الجرائم يحتاج إلى معرفة دقيقة بكيفية تشغيل الحاسب الآلي وبرامجه، وإلى خبرة عملية يوظفها في اختراق الأنظمة أو التجسس الإلكتروني أو استغلال الشبكات للتغريب بالقاصرين وغيرها من الصور الإجرامية، ولهذا السبب تُصنّف جرائم نظم المعلومات ضمن الجرائم "النظيفة" أو "الناعمة" التي لا تترك وراءها أي آثار مادية خارجية ملموسة

1- خالد دوايدي، الجريمة المعلوماتية، دار الاعصار العلمي للنشر والتوزيع، عمان الاردن، الطبعة الاولى 2018، ص 27-28.

كالدماغ أو الأذى البدني، وإنما تقتصر آثارها على مجرد تعديل أو نسخ أو حذف أرقام وبيانات مخزنة في ذاكرة الأجهزة الإلكترونية، مما يجعلها جرائم خفية لا تُرى بالعين المجردة¹.

2- الجرائم المعلوماتية جرائم مزدوجة المحل.

باعتبار النظام المعلوماتي ذاته ليس متكون من طبيعة واحدة فهو يتكون من عدة عناصر مادية و أخرى غير مادية، ما يتيح امكانية أن يكون موضوع الجريمة ذو طابعين مختلفين، أحدهما مادي، والآخر يتمثل في جانب غير مادي، وذلك ليس على مكونات النظام ذاته بل يشمل ظهور المحل الواحد بمظهرين أحدهما مادي والآخر غير مادي كما هو الحال بالنسبة للمعلومات فمثلاً:

- قد تكون المعلومات في حالة انتقال أو موجودة في ذاكرة النظام المعلوماتي أي أنها في حالة غير مادية.

- وقد تكون تلك المعلومات مستجدة بصورة مادية وهذا بتخزينها على دعامة معلوماتية².

والملاحظ في هذا الصدد أن المعلومات، بفضل طبيعتها غير المادية الملموسة يمكن أن تخضع لأكثر من نص قانوني مختلف تبعاً لشكلها، سواء كانت في شكل مادي أم غير مادي، وفي السياق الآخر، قد تكون عرضة لتطبيق أكثر من نص قانوني، كما في حالة تصنيفها كمصنف أدبي، وهنا تبرز إشكالية التصنيفات القانونية المتعددة على ذات المحل.

1- محمد ممدوح بدير، مكافحة الجريمة المعلوماتية عبر شبكات الانترنت والاستدلال كوسيلة لإثبات الجريمة المرتكبة عبر الانترنت، مركز الدراسات العربية، القاهرة مصر، الطبعة الاولى 2019، ص 28-29.

2- طارق أبراهيم الدسوقي عطيه، المرجع السابق، ص 167.

المطلب الثالث: سمات و دوافع مرتكبي جرائم نظم المعلومات.

إن من الإفرازات السلبية للمعلوماتية أنها أضافت دون قصد نوع جديد من المجرمين إلى حياتنا البشرية، أطلق عليهم تسمية (مجرمي المعلوماتية) والذين يتميزون بخصائص وصفات تختلف عن مجرمي الجرائم التقليدية، وسوف نتناول دراسة المجرم المعلوماتي في هذا الفرع من حيث سماته أولاً، ثم دوافع ارتكابه للجرائم المعلوماتية ثانياً.

الفرع الأول: سمات مجرمي نظم المعلومات.

بما أننا ذكرنا سابقاً بأن جرائم نظم المعلومات تتميز عن غيرها من الجرائم ببعض السمات والخصائص معينة، فذلك هو الحال بالنسبة لمرتكبيها فإنه يتميز بسمات وصفات تميزه عن غيره من المجرمين التقليديين، وفي هذا المجال تباينت آراء لباحثين حول تحديد هذه السمات بدقة، ويعد الأستاذ "Parker" كواحد من أبرز الباحثين المتخصصين الذين يولون اهتمام كبيراً للجريمة المعلوماتية بشكل عام، وبشخصية المجرم المعلوماتي بشكل خاص، ومع ذلك ينتهي إلى وصفة لهذا المجرم باعتباره فاعلاً لسلوك إجرامي يستوجب فرض عقوبة عليه، مع الإشارة إلى أنه ينتمي إلى فئة متميزة من المجرمين تتقارب خصائصها مع أصحاب الياقات البيضاء¹، وفي معظم الحالات ينتمي المجرم المعلوماتي إلى وسط اجتماعي متميز ومناصب رفيعة المستوى ومن ذوي الكفاءات العليا المتمتعين بالذكاء والحكمة والقدرة على التكيف في المجتمع ويحظون باحترام وثقة عالية من الأشخاص المحيطين بهم، هذا القاسم المشترك بينهم دفع البعض إلى القول أن مجرمي المعلوماتية إنما ينتمون إلى طائفة المجرمين ذوي الياقات البيضاء².

1- خالد دواوي، المرجع السابق، ص 31.

2- يُعد مصطلح "مجرمو الياقات البيضاء" (White-Collar Criminals) تعبيراً حديثاً نسبياً صاغه عالم الاجتماع الأمريكي إدوين ساذرلاند (Edwin Sutherland) لأول مرة عام 1939، وذلك للدلالة على فئة المجرمين من ذوي المكانة الاجتماعية الرفيعة والمناصب الإدارية والتنفيذية العليا الذين يرتكبون جرائم اقتصادية ومالية خطيرة - كغسل الأموال، والاختلاس، والاحتيال المصرفي، وتزوير العلامات التجارية، والتلاعب في الأسواق المالية، وتجارة البشر، وغيرها من الجرائم المماثلة - دون الحاجة إلى عنف جسدي، وإنما من خلف

وهنا يرمز الاستاذ "Parker" إلى الخصائص التي يتميز بها المجرم المعلوماتي بكلمة S.K.R.A.M وهي تعني (المهارة Skills ، المعرفة Knowledge ، الوسيلة Resources ، السلطة Authority ، الباعث Motives).

أولاً: المهارة Skills.

تُعَدّ المهارة التقنية السمة الأبرز والأكثر تميزاً لدى مرتكبي جرائم نظم المعلومات، إذ يتعين على الجاني أن يمتلك مستوى متقدماً من الكفاءة في تكنولوجيا المعلومات، سواء اكتسبها من خلال التعليم الأكاديمي المتخصص أو من خلال الممارسة الذاتية المكثفة أو الاحتكاك المباشر بالوسط التقني والمتخصصين، غير أن هذه المهارة ليست متجانسة بين جميع المجرمين المعلوماتيين، بل تتباين شدتها ونوعيتها بحسب طبيعة الجريمة المرتكبة، فكل صورة من صور الجرائم المعلوماتية تتطلب حزمة مهارات محددة¹، ولكن الأهم أن يكون الجاني على قدر من الذكاء والمهارة لأنهم هم الذين يحددون الكيفية التي تتم بها الجريمة المعلوماتية.

ومع ذلك، أثبتت التجارب العملية والقضايا الواقعية أنه ليس شرطاً أن يكون الجاني المعلوماتي على درجة عالية جداً من العلم النظري أو الخبرة المهنية الرسمية، بل إن أخطر وأنجح مرتكبي هذه الجرائم وأكثرهم تأثيراً غالباً ما يكونون قد اكتسبوا مهاراتهم خارج إطار التعليم النظامي أو العمل المؤسسي، مما يؤكد أن الذكاء الحاد والإبداع التقني الذاتي هما العاملان الحاسمان في تحديد أسلوب ونجاح الجريمة المعلوماتية².

ثانياً: المعرفة Knowledge .

تعني المعرفة التعرف على كافة العوامل والظروف والملابسات التي تحيط بالجريمة المعلوماتية المراد ارتكابها والدراية الكاملة بكل تفاصيلها واحتمالات نجاحها أو فشلها، حيث أن

مكاتبهم الفاخرة وهم يرتدون بدلاتهم الأنيقة، مستغلين بذلك سلطتهم وثقة المجتمع وإلزامهم بتعقيدات النظم المالية والإدارية، للمزيد أنظر في ذلك: د دلخار صلاح بوتاني، المرجع سابق ، ص 54.

1- عبد الإله النوايسة، المرجع السابق، ص 85.

2- نائلة عادل محمد فريد قورة، المرجع السابق، ص 57.

المجرم يمكن أن يضع تصور كامل عن جريمته، ومن الممكن أن يقوم المجرم بتنفيذ جريمته على نظام حاسب آلي مماثل لتلك التي يريد استهدافها قبل تنفيذ جريمته¹.

ثالثاً: الوسيلة Resources .

أما الوسيلة فتشير إلى الإمكانيات التقنية والأدوات التي يمتلكها الجاني لإتمام جريمته، وفي حالة الجريمة المعلوماتية تتميز هذه الوسائل في أغلب الأحوال بالبساطة النسبية وسهولة التوافر، إذ يكفي المجرم المعلوماتي في كثير من الحالات حاسب آلي عادي متصل بالإنترنت وبعض البرمجيات المتاحة أو القابلة للتصميم الذاتي، ويتميز هذا النوع من المجرمين بقدرة فائقة على الحصول على الأدوات المطلوبة بسرعة، أو ابتكار وسائل بديلة تُقلّص الخطوات اللازمة وتُعجّل تنفيذ الفعل الإجرامي وتُيسّره إلى أقصى حد، غير أن الأمر يختلف جذرياً عندما يكون النظام المستهدف غير شائع أو عالي التحصين، ففي هذه الحالة تصبح الوسائل المطلوبة أكثر تعقيداً وأقل توافراً، إذ تقتصر معرفتها وإمكانية الوصول إليها عادةً على عدد محدود جداً من الأشخاص، وغالباً ما يكونون مشغلي النظام أو المطوّرين له، بخلاف الأنظمة واسعة الانتشار التي يتاح وسائل اختراقها لشريحة أوسع بكثير².

رابعاً: السلطة Anthority .

تشير السلطة هنا إلى الحق أو الامتياز الذي يتمتع به الجاني تجاه النظام المعلوماتي والذي يمكنه من ارتكاب الجريمة، إذ يمتلك كثير من مجرمي المعلوماتية سلطة مباشرة أو غير مباشرة على المعلومات المستهدفة (محل الجريمة)، وقد تتجسد هذه السلطة في حيازة كلمة المرور أو الشيفرة الخاصة بالدخول إلى النظام، مما يتيح للفاعل صلاحيات متعددة تشمل فتح الملفات وقراءتها وتعديلها وحذفها أو نسخها، كما قد تتمثل في الحق المشروع باستخدام الحاسب الآلي أو إجراء معاملات معينة أو مجرد الوصول المادي إلى الأماكن التي تضم الأنظمة المعلوماتية،

1- دلخار صلاح بوتاني، المرجع سابق، ص 56.

2- نائلة عادل محمد فريد قورة، المرجع السابق، ص 58.

وقد تكون هذه السلطة غير مشروعة كما في حالة استعمال بيانات دخول شخص آخر دون إذن¹.

خامسا: الباعث² Motives .

ليس هناك فرق بين دوافع مرتكبي جرائم نظم المعلومات في معظم الحالات وبين دوافع مجرمي الجرائم التقليدية، إذ تبقى الرغبة في تحقيق كسب مادي غير مشروع الدافع الأساسي والأول، يليها الدافع الفكري المحض المتمثل في إثبات القدرة على قهر أنظمة الحاسب الآلي وتجاوز الحواجز الوقائية، ثم دافع الانتقام من صاحب العمل أو الزملاء.

ومهما كان الباعث، فإن الجاني المعلوماتي غالباً ما يفتقر إلى الشعور بالإجرام، بل يرى أن فعله لا يرقى إلى مستوى الجريمة أو لا ينطوي على مخالفة أخلاقية، خاصة إذا اقتصر السلوك على اختراق النظم أو تجاوز الحماية دون إلحاق ضرر مباشر بشخص طبيعي، إذ يميز كثير منهم بين الإضرار بفرد - وهو أمر يعتبرونه غير أخلاقي - وبين إلحاق الضرر بمؤسسة أو كيان كبير قادر على استيعاب الخسارة³، وهي الظاهرة المعروفة بمتلازمة روبن هود (The Robin Hood Syndrome).

وخلاصة لما سبق وصل الاستاذ "Parker" من خلال بحثه للأنماط المختلفة لمجرمي المعلوماتية أن الغالبية منهم غير قادرين على القيام بالجرائم التقليدية، وخاصة تلك الجرائم التي تتطلب لقاء ومواجهة فعلية مع المجني عليه، فالمجرم المعلوماتي لا يستطيع الاعتداء على المجني عليه بطريقة مباشرة، غير أنه يمكنه الاعتداء عليه عن طريق الحاسب الآلي.

1- خالد دواوي، المرجع السابق، ص 34.

2- الدافع أو الباعث هو العامل الذي يوجه إرادة الحب والشفقة والكراهية والانتقام والأفعال الإجرامية الأخرى، وهو القوة النفسية التي تدفع الإرادة إلى اتجاه الجريمة لتحقيق الهدف أو أهداف محددة، والتي تختلف من جريمة إلى أخرى، حسب طبيعة الإنسان من حيث العمر، والعلم، والثقافة، وما إلى ذلك، أنظر في ذلك دلخار صلاح بوتاني، المرجع السابق، ص 62.

3- نائلة عادل محمد فريد قورة، المرجع السابق، ص 58.

وبناء على ما تقدم فانه يمكننا تقسيم مجرمي المعلوماتية إلى فئات مختلفة، حيث توصلت الأبحاث المختلفة في هذا المجال إلى وجود سبعة فئات من مجرمي المعلومات، بالطبع هذا لا يعني أن كل مجرم ينتمي إلى فئة معينة دون غيرها، ولكن يمكن أن يكون المجرم خليطاً من عدة فئات:

- **الفئة الأولى المخادعون "Pranksters"**: وتشمل الجرائم المعلوماتية التي ترتكب بقصد التسلية والمزاح مع الآخرين مع عدم وجود نية لإيذاء الضحية، ومثالها الجرائم المعلوماتية التي ترتكب من قبل القصر¹.

- **الفئة الثانية المخترقون الهواة "Hackers"**: وهي تشمل الأشخاص الذين يهدفون إلى الوصول غير المصرح به إلى أنظمة الحاسبات الآلية وكسر الحواجز الأمنية الموضوعة لهذا الغرض، إما لاكتساب الخبرة أو بدافع الفضول أو لمجرد إثبات قدرتهم على اختراق تلك الأنظمة²، وهم غير مؤذيين فلا يقومون بالتدمير والاتلاف، ومنهم من يقوم بالدخول بدون تصريح بهدف الكشف عن مواقع الضعف الأمني في النظام ويطلق عليهم أسم المخترقون ذوي القبعات البيضاء³ **"White hat Hackers"**.

- **الفئة الثالثة المخترقون ذوي النوايا الخبيثة "Malicious Hackers"**: وتشمل الأشخاص الذين يسعون عمداً إلى إلحاق الضرر والخسائر بالضحايا دون تحقيق أنقعة مادية شخصية لأنفسهم، وتكون هذه الفئة في غالبيتها من مُبتكري فيروسات الحواسيب ومطلقها وناشريها.

الفئة الرابعة حلالو المشاكل الشخصية "Personal Problem Solvers": وهم الفئة الأكثر شيوعاً بين مرتكبي الجرائم المعلوماتية، والأشدّ خطورة من حيث حجم الخسائر التي تُحدثها للضحايا، ولا يقوم دافع هؤلاء على تحقيق كسب مادي مباشر، بل على البحث عن حلول فورية لمشكلاتهم المالية الشخصية التي عجزوا عن معالجتها بالطرق المشروعة أو

1- راجع في ذلك، د عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي - دراسة قانونية متعمقة في القانون المعلوماتي - دار الكتب القانونية المحلة الكبرى، القاهرة ، مصر، طبعة 2007، ص 90-91.

2- خالد دواوي، المرجع السابق، ص35.

3- عبد الإله النوايسة، المرجع السابق، ص 81.

حتى بالجرائم التقليدية، ويتمتع أفراد هذه الفئة عادةً بخبرة واسعة في مجال الحواسيب ناتجة عن طبيعة عملهم، ولا يتورعون عن تبرير أفعالهم بأن الضحية - وهي غالباً ما تكون مؤسسة المالية أو الجهة التي يعملون بها - قادرة على استيعاب الخسارة الناتجة عن جريمتهم.

- **الفئة الخامسة الممتهين المحترفين "Career Criminals"**: وهم فئة مرتكبي الجرائم المعلوماتية الذين يستهدفون تحقيق مكاسب مادية كبيرة بطرق غير مشروعة من خلال أنشطة إجرامية منظمة تنطبق عليها في أغلب الأحوال معايير الجريمة المنظمة¹، وقد يشترك فيها فرد واحد أو أكثر، ويتشابه الجاني في هذه الفئة إلى حد كبير مع نظيره في الجرائم التقليدية من حيث الدافع والأسلوب، غير أن الملاحظ أن التنظيمات الإجرامية التقليدية بدأت تنجذب بقوة نحو جرائم الحواسيب لما توفره من أرباح هائلة مع صعوبة بالغة في الكشف والإثبات، ومع ذلك، تبقى نسبة هذا النوع من الجرائم المعلوماتية المنظمة منخفضة نسبياً مقارنة بالجرائم التقليدية، ويعزى ذلك أساساً إلى اشتراط الجريمة المعلوماتية مستوى عالٍ من العلم والخبرة التقنية في مجال الحواسيب، وهو ما لا يتوافر عادة لدى معظم أفراد وقادة الجماعات الإجرامية من هذه الفئة.

- **الفئة السادسة المتطرفون "Extreme Advocates"**: وتشمل هذه الفئة الجماعات الإرهابية والتنظيمات المتشددة التي تضم أفراداً يحملون أفكاراً سياسية أو دينية أو أيديولوجية راديكالية، ويسعون لفرضها بالقوة، ويلجأ هؤلاء أحياناً إلى استخدام العنف ضد الأشخاص أو الممتلكات بهدف لفت الأنظار إلى قضاياهم، أذ بدأت التنظيمات الإرهابية، ولا سيما ذات البنية التنظيمية المحكمة، تتحول تدريجياً إلى استغلال الجرائم المعلوماتية بوصفها سلاحاً

1- وفقاً للمادة (2) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة فإنه المقصود بتعبير "جماعة إجرامية منظمة" الجماعة ذات الهيكل التنظيمي المؤلفة من ثلاثة أشخاص أو أكثر، موجودة لفترة من الزمن وتعمل بصورة متضافرة بهدف ارتكاب واحدة من الجرائم الخطيرة أو الأفعال المجرمة وفقاً لهذه الاتفاقية، من أجل الحصول بشكل مباشر أو غير مباشر على منفعة مادية أخرى، وتنص الفقرة (ج) من المادة 2 على أنه: يقصد بتعبير "جماعة ذات هيكل تنظيمي" جماعة غير مشكّلة عشوائياً لغرض ارتكاب الفوري لجرم ما، ولا يلزم أن تكون لأعضائها أدوار محددة رسمياً، أو أن تستمر عضويتهم فيها أو أن تكون ذات هيكل تنظيمي، أنظر في ذلك المادة 2 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة الصادرة بموجب قرار الجمعية العامة للأمم المتحدة 55/25 المؤرخ في 15/نوفمبر/2000 والتي بدأ نفاذها بتاريخ 29/سبتمبر/2003.

حديثاً، بعدما أدركت أن الاعتماد المتزايد للمؤسسات الحيوية والدول على الحواسيب والشبكات يوفّر هدفاً استراتيجياً مغرياً يمكن ضربه بتكلفة منخفضة وفاعلية كبيرة، ومن الأمثلة البارزة على ذلك ما قامت به الجماعة الإرهابية الإيطالية "الألوية الحمراء" "The Red Brigades" في ثمانينيات القرن الماضي، حين دمّرت أكثر من ستين مركزاً للحواسيب في أوروبا بهدف الترويج لأفكارها ومعتقداتها.

- الفئة السابعة المهملون جنائياً "The Criminally Negligent": ويشمل هذا التصنيف أحد أبرز التحديات المرتبطة بإساءة استخدام الحاسب الآلي وهي الإهمال، فلا يمكن إنكار أن الإهمال في قطاع تكنولوجيا المعلومات والنظم المعلوماتية غالباً ما يؤدي إلى عواقب وخيمة، قد تبلغ ذروتها في حوادث تؤدي إلى فقدان الأرواح، فعلى سبيل المثال وقعت حادثة في نيوزيلندا حيث قام اثنين من مبرمجي الحاسبات الآلية بتغيير برمجيات تحديد المسار بإحدى الطائرات، دون قدرتهم على إبلاغ قائد الطائرة بهذا التغيير مما نتج عنه تحطم الطائرة بعد اصطدامها بأحد الجبال وقتل 60 راكبا كانوا على متن الطائرة، وتمت محاكمة المتهمين بتهم القتل الخطأ¹.

في الواقع، بغض النظر عن مدى دقة حدود الطوائف المختلفة التي ينتمي إليها مجرمو الإنترنت، فإنه يظهر لنا إن الدوافع الرئيسية التي تحدد الجريمة المعلوماتية لأي فئة تنتمي من الفئات التي ينتمي إليها مجرمو المعلومات لا تتجاوز ثلاثة دوافع، الدافع الأول لجريمة المعلومات هو الهدف المشترك لجرائم الاعتداء على الأموال أي السعي وراء المصالح المادية، بينما الدافع الثاني لجريمة المعلومات يختلف عن الدوافع الأخرى وهو الرغبة في الدخول لأنظمة الحاسبات الآلية والمعلومات التي تحتويها أما للترفيه والتسلية أو لإثبات ما إذا كان الجاني لديه خبرة فنية وتقنية أو لغرض السعي وراء الكسب المادي أو تخريب هذه الأنظمة، وأخيراً يأتي الدافع الثالث وهو الرغبة في الإضرار بهذه الأنظمة بغض النظر عما إذا كانت الرغبة نابعة من الانتقام من المؤسسات التي تنتمي إليها هذه الأنظمة، أم أنها مجرد إلحاق الأذى بها لأسباب تنافسية أو لأسباب أخرى.

1- نائلة عادل محمد فريد قورة، المرجع السابق، ص 61-62.

الفرع الثاني: دوافع ارتكاب جرائم نظم المعلومات.

اهتم خبراء جرائم نظم المعلومات دائماً بدراسة دوافع هذه الجرائم وتحليل أسبابها العامة والخاصة، والتي تختلف جوهرياً في أغلب الأحوال عن دوافع الجرائم التقليدية، ومع ذلك، فإن وجود الدافع لا يترك أثراً قانونياً مباشراً على قيام الركن المعنوي للجريمة، إذ يكفي لتوافر القصد الجنائي مجرد العلم بالعناصر المكونة للجريمة وتوجيه الإرادة نحو تحقيقها أو قبول وقوعها، بغض النظر عن نبل الدافع أو دناءته، ومع هذا، تبقى دراسة الدوافع ذات أهمية عملية كبيرة في تضيق دائرة المشتبه بهم وتحديد الجناة المحتملين في الجرائم عموماً وفي جرائم نظم المعلومات على وجه الخصوص، وقد يُضفي القانون في بعض الحالات أهمية قانونية استثنائية على الدافع، فيشترط توافره لقيام الجريمة، فيصبح حينئذٍ جزءاً من القصد الجنائي ويُعرف بالقصد الخاص، كما يجوز للقاضي أن يتأثر بالدافع عند تقدير العقوبة، إذ يُعدّه عنصراً مؤثراً في تقييم درجة الخطورة الإجرامية للجاني¹.

وبناء على ما سبق سنحاول بيان الدوافع لارتكاب جرائم نظم المعلومات بوجه عام وهذا على سبيل المثال لا الحصر وذلك راجع إلى صعوبة تحديدها لكثرتها وتنوعها واختلافها من جانب إلى آخر وهي على النحو التالي:

أولاً: الدوافع المادية:

تتربع الدوافع المادية على قمة سلم دوافع جرائم نظم المعلومات، إذ يُعدّ السعي إلى الكسب المالي الدافع الأول والأقوى تحفيزاً لمرتكبي هذه الجرائم، فالرغبة الجامحة في الحصول على الثروة السريعة، أو الحاجة الملحة لتسديد ديون أو تمويل إدمان القمار أو تعاطي المخدرات، تدفع الجاني إلى توظيف كامل خبراته ومهاراته التقنية والفنية في استهداف المؤسسات المالية والبنوك والشركات، بهدف سرقة الأموال أو التلاعب بالحسابات أو تحويل مبالغ مالية إلى

1- دلخار صلاح بوتاني، المرجع السابق، ص 62-63.

حساباته الخاصة أو حسابات وسيطة، مستغلاً بذلك الربحية العالية التي تتميز بها هذه الجرائم مقارنة بغيرها¹.

إذ يحصل المجرمون على فوائد مالية وأرباح ضخمة دون عناء من خلال جرائم نظام المعلومات وجرائم الاحتيال الإلكتروني والاعتداء على الملكية الفكرية مقارنة بالجرائم التقليدية²، فسهولة ارتكاب الجريمة وصعوبة اكتشافها والعثور على الجناة هي عوامل جذابة لارتكاب جرائم نظم المعلومات، فعلي سبيل المثال في روسيا 60% من الشباب الجامعيين العاطلين عن العمل من خريجي الجامعات ينخرطون في القرصنة الإلكترونية كوسيلة لكسب دخل أعلى من دخل العمل في الوظائف³.

ثانياً: الدوافع الانتقامية:

يُعدّ دافع الانتقام من أخطر الدوافع وأكثرها شيوعاً في جرائم نظم المعلومات، إذ من الممكن أن يكون الجاني هو الموظف أو العامل السابق الذي يمتلك معرفة واسعة بأنظمة المؤسسة إلى استغلال هذه المعرفة لإلحاق أكبر ضرر ممكن بجهة عمله دون أن يسعى بالضرورة إلى كسب مادي، وينبع هذا الدافع عادةً من مشاعر الحقد والغبن والإحساس بالإهمال أو الظلم، كالفصل التعسفي أو الحرمان من الترقية أو الشعور بالدونية داخل بيئة العمل.

وتؤكد الإحصاءات أن نسبة كبيرة جداً من جرائم المعلومات ترتكب من داخل المؤسسة نفسها على يد موظفين حاليين أو سابقين، ومن الأمثلة الشهيرة في الولايات المتحدة أن موظفاً في إحدى شركات التأمين، بعد فصله من عمله، أدخل فيروساً خبيثاً إلى أنظمة الشركة، فأتلف مائة وستون سجلاً لعملاء مهمين، انتقاماً من الشركة، وقد أُحيل الموظف

1- محمد ممدوح بدير، المرجع السابق، ص 57-58.

2- ولقد ظهر هذا جلياً في فرنسا حيث أنه في عام 1986 كان العائد من جرائم السرقة بحمل السلاح ما يقارب من 70000 ألف فرنك فرنسي، في حين ان العائد من جرائم الغش المعلوماتي والمعالجة الآلية للمعلومات ما يقارب من 670000 ألف فرنك فرنسي أي ما يعادل الضعف 38 مرة، أنظر في ذلك: د خالد داودي، المرجع السابق، ص 37-38.

3- عبد الإله النوايسة، المرجع السابق، ص 88.

إلى القضاء وحُكم عليه بالسجن سبع سنوات وغرامة مالية قدرها مائة وخمسون ألف دولار أمريكي¹.

ثالثاً: الدوافع السياسية:

تُعَدُّ الآراء السياسية والميول القومية والأيدولوجية من الدوافع القوية التي تحفز بعض مرتكبي جرائم نظم المعلومات، حيث يستهدفون الإساءة إلى الدول والحكومات وقادتها من خلال نشر معلومات وبيانات وصور ملفقة أو مضللة لتشويه سمعتهم أمام الرأي العام، أو للنيل من خصومهم السياسيين والمعارضين، أو لزعزعة استقرار النظام الأمني والحاكم، كما قد يسعى هؤلاء الجناة إلى دعم فصيل أو تيار معين عبر الترويج لأفكاره وعقائده القومية أو الدينية أو السياسية، وذلك من خلال أعمال مثل تعطيل المواقع الحكومية الرسمية أو مواقع المعارضة السياسية أو اختراق قواعد البيانات الحساسة أو تسريب وثائق مزورة أو حقيقية بغرض إثارة الفتنة وإضعاف الثقة في مؤسسات الدولة².

رابعاً: الدوافع الشخصية:

يبرز لدى فئة من مرتكبي جرائم نظم المعلومات دافع نفسي قوي يتمثل في إثبات الوجود الشخصي والتفوق التقني، ويُعرف هذا الدافع بـ "قهر النظام"، يرى هؤلاء في كشف الثغرات واختراق الأنظمة الحساسة والاستراتيجية عملاً بطولياً يُظهر عبقريتهم وقدراتهم العلمية، مدفوعين بشغفهم الشديد بالمعلوماتية ورغبتهم في اكتساب المزيد من المعرفة والتباهي أمام أقرانهم بإنجازاتهم، ويشتد هذا الدافع خاصة لدى الشباب وصغار السن من الجناة الذين يقضون معظم أوقاتهم أمام الحواسيب في محاولات متكررة لتجاوز الحواجز الأمنية³، مما

1- محمد ممدوح بدير، المرجع السابق، ص 61.

2- دلخار صلاح بوتاني، المرجع السابق، ص 65.

3- يلاحظ أن الدافع المعروف بـ "قهر النظام" يصنف كواحد من أبرز الدوافع استغلالاً من قبل التنظيمات الإجرامية، حيث تتفنن هذه التنظيمات توظيفه لاستدراج المخترقين المحترفين وإغرائهم واقتناعهم بالمشاركة في عمليات اعتداء إلكتروني معقدة، أو لاستئجارهم بشكل مباشرة لتنفيذ الجرائم نيابةً عنها، مستثمرةً بذلك رغبتهم وحماستهم في إثبات الذات والتباهي والتفاخر بالقدرات التقنية، أنظر في ذلك: د. خالد داودي، المرجع السابق، ص 41.

دفع بعض الفقهاء والمتخصصين إلى وصف هذه الأفعال بأنها "بريئة" أو "غير مؤثمة" طالما لم تقترن بقصد الإضرار المتعمد أو تحقيق كسب مادي¹.

يجدر التنويه ختاماً بأن معظم الأبحاث الجنائية الحديثة في مجال الجريمة المعلوماتية تسعى جاهدةً إلى وضع تصنيف معياري موحد لمرتكبي جرائم نظم المعلومات، غير أن هذه المهمة تبقى صعبة للغاية بسبب التطور السريع والمستمر للظاهرة الإجرامية التي ترتبط ارتباطاً وثيقاً بالتطور التكنولوجي المتسارع في مجالي الحوسبة والإنترنت، فكل تقدم تقني جديد يُولد أساليب وأدوات وتكتيكات هجومية مبتكرة، مما يحدث تغييرات جذرية في أنماط الجريمة ويزيد من فعالية الهجمات وتعقيدها، ويترتب على ذلك بالضرورة تغير مستمر في خصائص مرتكبيها، ليس على مستوى الشخصية الفردية فحسب، بل - وبشكل أوضح - على مستوى السلوك الإجرامي ذاته، ولذلك، اتجه الباحثون في السنوات الأخيرة إلى الاعتقاد بأن التصنيف الأمثل والأكثر فائدة عملياً لمجرمي التكنولوجيا لا ينبغي أن يعتمد على التقنية المستخدمة أو الوسيلة التنفيذية أو حتى نوع الضحية، وإنما يجب أن يُبنى أساساً على الغرض أو الدافع من الهجوم، لأنه العنصر الأكثر ثباتاً نسبياً وسط هذا التغير التكنولوجي المتلاحق².

الفرع الثالث: الضحية في جرائم نظم المعلومات.

يقصد بالضحية (أو المجني عليه) في جرائم نظم المعلومات كل من يتعرض لاعتداء غير مشروع على نظام معلوماتي أو بياناته أو أمواله أو خصوصيته، وقد يكون الضحية شخصاً طبيعياً أو اعتبارياً (مؤسسة، شركة، جهة حكومية)، كما قد يمتد الضرر إلى أشخاص آخرين غير المستهدفين مباشرة ويُعرفون "بالمتضررين من الجريمة".

وقد أكد ذلك "الإعلان العالمي بشأن المبادئ الأساسية لتوفير العدالة لضحايا الجريمة وإساءة استعمال السلطة" الصادر عن الجمعية العامة للأمم المتحدة عام 1985، حيث عرّفت الفقرة (أ) منه مصطلح "الضحايا" بأنهم "كل من المجني عليه والضحية والمتضررين

1- دلخار صلاح بوتاني، المرجع السابق، ص 65.

2- جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة، دار البداية ناشرون وموزعون، عمان الاردن، الطبعة الاولى 2007، ص 156.

والمحرومين من التمتع بحقوقهم الأساسية كما ويمكن أن يشمل مصطلح الضحية عند الاقتضاء كل من العائلة المباشرة للضحية الأصلية أو معيلها المباشرين¹.

وبهذا يظهر أن مفهوم الضحية في الجريمة بصفة عامة (الإطار الجنائي) كل شخص طبيعي أو اعتباري تعرض لخسارة أو ضرر أو إعتداء نتيجة إرتكاب (فعل) جريمة سواء بفعل أو بالامتناع عن فعل، أما المقصود بالضحية في الجريمة المعلوماتية هو كل شخص طبيعي أو اعتباري أصابه ضرر مادي أو معنوي نتيجة الاستخدام غير المشروع لتقنية المعلومات، وقد يتجلى الضحية في صورة عامة ممثلاً بمؤسسات الدولة وهيئاتها، أو في صورة خاصة ممثلاً في الأشخاص الطبيعية أو المعنوية، وبحسب ذلك فإن الضحايا في الجريمة المعلوماتية يختلفون عن الضحايا في الجرائم التقليدية من مجرد كونهم أشخاص عادية إلى مؤسسات مالية أو عسكرية أو قطاعات حكومية، وهي مجالات يعجز المجرم التقليدي عن الاقتراب منها أو ارتكاب أي أعمال إجرامية ضدها.

وبشكل عام، يُعرّف الضحية في أي جريمة بأنه " كل شخص طبيعي أو اعتباري يتعرض لضرر مادي أو معنوي أو خسارة ناتجة عن فعل غير مشروع، سواء تمثل هذا الفعل في القيام بتصرف محظور أو في الامتناع عن واجب قانوني"، أما في جرائم نظم المعلومات، فيُقصد بالضحية " كل من أصابه ضرر مباشر أو غير مباشر - مادياً كان أو أدبياً - جزاء الاستخدام غير المشروع لتكنولوجيا المعلومات والاتصالات"، وقد يكون الضحية عامماً ممثلاً في

1- يقصد بمصطلح "الضحايا" الأشخاص الذين أصيبوا بضرر فردياً أو جماعياً، بما في ذلك الضرر البدني أو العقلي أو المعاناة النفسية أو الخسارة الاقتصادية، أو الحرمان بدرجة كبيرة من التمتع بحقوقهم الأساسية، عن طريق أفعال أو حالات إهمال تشكل انتهاكا للقوانين الجنائية النافذة في الدول الأعضاء، بما فيها القوانين لتي تحرم الإساءة الجنائية لاستعمال السلطة، ويمكن اعتبار شخص ما ضحية بمقتضى هذا الإعلان، بصرف النظر عما إذا كان مرتكب الفعل قد عرف أو قبض عليه أو قوضي أو أدين، وبصرف النظر عن العلاقة الأسرية بينه وبين الضحية، ويشمل مصطلح "الضحية" أيضاً، حسب الاقتضاء، العائلة المباشرة للضحية الأصلية أو معاليها المباشرين والأشخاص الذين أصيبوا بضرر من جراء التدخل لمساعدة الضحايا في محتنتهم أو لمنع الإيذاء، أنظر في ذلك الاعلان العالمي بشأن المبادئ الأساسية لتوفير العدالة لضحايا الجريمة وإساءة استعمال السلطة والصادر عن الجمعية العامة للأمم المتحدة بموجب القرار رقم 40/34 والصادر بتاريخ 1985/11/29.

أجهزة الدولة ومؤسساتها وهيئاتها الرسمية، أو خاصاً يتمثل في أفراد طبيعيين أو كيانات اعتبارية من القطاع الخاص.

ولذلك تختلف ضحايا الجرائم المعلوماتية جذرياً عن ضحايا الجرائم التقليدية، فالأخيرة كانت تقتصر غالباً على المؤسسات المالية أو العسكرية أو الإدارات الحكومية التي كان من المستحيل تقريباً على المجرم التقليدي الوصول إليها أو الاعتداء عليها بوسائله البدائية، بينما أصبحت هذه الجهات نفسها - وغيرها الكثير - هدفاً سهلاً ومباشراً أمام الجاني المعلوماتي بفضل طبيعة التكنولوجيا الحديثة¹.

وعليه وجب الإشارة إلى أن تقدير الحجم الحقيقي لجرائم نظم المعلومات يظل أمراً بالغ الصعوبة، نظراً لعدم إمكانية تحديد عدد الضحايا بدقة، وذلك لعاملين رئيسيين: أولهما يتعلق بالجريمة ذاتها، وهو غياب تعريف قانوني وإحصائي موحد ومقبول عالمياً لمفهوم "جريمة نظم المعلومات"، مما يُعيق إجراء دراسات إحصائية موثوقة تعكس انتشارها الفعلي، وثانيهما يرتبط بسلوك الضحايا أنفسهم، إذ يتمتع معظمهم - وخاصة المؤسسات المالية والبنوك - عن الإبلاغ عن الجرائم التي يتعرضون لها، خشية تلطيخ سمعتهم وفقدان ثقة العملاء والمساهمين، فالإدارات تفضل في الغالب امتصاص الخسائر المالية على الاعتراف لفكرة أن أنظمتها المعلوماتية قد تعرضت للاختراق أو الانتهاك، وهذا التكتّم يشكل حافزاً إضافياً للجناة لمواصلة نشاطهم الإجرامي دون خوف من الملاحقة²، وبالرغم من صعوبة التحديد الدقيق لضحايا هذه الجريمة، يمكن إيجاز أبرز فئاتهم على النحو التالي:

أولاً: الأشخاص المعنويين (الجهات الحكومية والمؤسسات المالية):

تتركز الغالبية العظمى من جرائم نظم المعلومات على الأشخاص المعنويين، سواء العاميين أو الخاصين، وذلك لاعتمادهم الواسع والحيوي على الأنظمة المعلوماتية والبنية التحتية الرقمية في إدارة شؤونهم وتنفيذ معاملاتهم.

1- سعيداني نعيم، المرجع السابق ص 64.

2- غانم مرضي الشمري، المرجع السابق، ص 32.

وتُعدّ الجرائم الموجّهة ضد الأشخاص المعنويين العامين، ولاسيما المؤسسات العسكرية والأمنية والحكومية، الأشد خطورة لتداعياتها على الأمن القومي، ومن أبرز الأمثلة على ذلك عمليات الاختراق المنسقة التي نفذها قراصنة روس على مدى عام كامل ضد أنظمة المعلومات الحكومية والعسكرية الأمريكية، أفضت إلى سرقة بيانات حساسة واستغلالها لأغراض معادية، وكذلك حادثة تسريب الموظف السابق في وكالة الأمن القومي الأمريكي " إدوارد سنودن " عام 2013 لمعلومات سرية للغاية، شملت برنامج " PERSIM " للمراقبة والتجسس، مما عرّض الأمن القومي الأمريكي لخطر جسيم بعد نشر الصحفي لهذه المعلومات في صحيفتي " الغارديان و واشنطن بوست ".

أما الاشخاص المعنويين الخاصون وفي مقدمتهم البنوك والمؤسسات المالية وشركات التأمين والبورصات، فيشكلون الهدف الأول لمجرمي الجرائم المعلوماتية ذات الطابع المالي، نظرا لما تحتويه نظمهم من أرصدة وتدفقات مالية ضخمة، إذ يؤدي الاختراق والتلاعب إلى خسائر مادية ومالية مباشرة وفقدان للثقة في المؤسسة لدى المنفعين¹.

ثانياً: الاشخاص الطبيعيين (الأفراد).

بطبيعة الحال، لا تقتصر دائرة ضحايا جرائم نظم المعلومات على الأشخاص المعنويين (كالبنوك والمؤسسات الحكومية والجهات العسكرية) فحسب، بل تمتد لتشمل الأشخاص الطبيعيين، أي كل فرد يستخدم الحواسيب أو الأجهزة المتصلة بالشبكة المعلوماتية.

وتُشكّل الشبكة المعلوماتية بيئة خصبة للمجرمين لتوجيه اعتداءاتهم الإلكترونية ضد الأفراد، خاصة فيما يمسّ خصوصيتهم الفردية وحقوقهم الأساسية وبياناتهم الشخصية، وتُعدّ جرائم الإتلاف المعلوماتي عبر الفيروسات والبرمجيات الخبيثة من أوسع هذه الاعتداءات انتشاراً بحق الأشخاص الطبيعيين، حيث يُستخدم البريد الإلكتروني كإحدى البوابات الرئيسية التي يعتمد عليها القراصنة والمجرمين لاختراق الأجهزة الشخصية وإلحاق الضرر بها أو سرقة محتوياتها².

1- دلخار صلاح بوتاني، المرجع السابق، ص66.

2- سعيداني نعيم، المرجع السابق ص66.

ثالثاً: مقدمي الخدمة:

وهم الاشخاص الطبيعية أو المعنوية الذي يساعدون على الوصول إلى شبكة الانترنت فيمكن أن يكونوا وسطاء بين الزبون والعميل وما بين شبكة الانترنت والضحايا للجريمة المعلوماتية، و يتم هذا التوصيل بواسطة عقدين يتمثل الأول في عقد نقل المعلومات حيث يتولى الناقل بمقتضاه عملية الربط الفني بين شبكات الاتصال، في حين الثاني يكون من خلال متعهد الوصول الذي يوصل الزبون إلى الموقع الالكتروني المطلوب، ومقدمي الخدمة متعددين وهم:

1- متعهد الوصول: هو كل شخص طبيعي أو اعتباري يؤدي دوراً تقنياً محض يتمثل في

تمكين المشترك (الزبون) من الاتصال بشبكة الانترنت وشبكات الاتصال وذلك بموجب عقود اشتراك لتوصيل الزبون إلى المواقع التي يريدها، وهو أيضاً تلك المؤسسة التي تزود المستخدم بالوسائل الممكنة لدخول شبكة الانترنت وربط حاسبه الرئيسي بشبكة الاتصال، وبالتالي يقتصر دورهم على الجانب الفني البحث لعملية الربط والنقل دون أدنى مسؤولية أو علاقة بمحتوى المعلومات والبيانات التي يتم تبادلها أو تصل إلى المشترك¹.

2- متعهد الايواء: هو كل شخص طبيعي أو معنوي يقدم خدمات إيواء صفحات الانترنت

وينشئ المواقع عبر الانترنت واستغلالها، ويقدم خدمة تخزين المعطيات والتطبيقات والسجلات المعلوماتية على خوادمه²، ويمكن هذا المتعهد الجمهور من الاطلاع الدائم والمستمر على محتوى المواقع المستضافة عبر حساباته الخادمة (Servers) وذلك بجعل المعلومات المخزنة على الأجهزة المركزية متاحة لمستخدمي الشبكة المعلوماتية في أي وقت، ويعد متعهد الايواء - سواء كان شركة تجارية أ كياناً من أشخاص القانون العام -

1- حدة بوخالفه، المسؤولية الجزائية لمتعهد الدخول عبر الانترنت، مجلة الدراسات القانونية، العدد 01، المجلد

06، مخبر السيادة والعولمة جامعة يحي فارس المدية، الجزائر، سنة 2020، ص 2.

2- لقد عرّفت المشرع الجزائري متعهدو الايواء بأنهم " أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستخدميه"، للمزيد أنظر المادة 02 الفقرة "د" من القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالأعلام والاتصال ومكافحتها سالف الذكر.

مسؤولاً تقنياً فقط عن توفير البيئة التحتية اللازمة للاستضافة والتخزين، دون أن يكون له علاقة بمحتوى المعلومات المستضافة في الأصل¹.

3- متعهد الخدمات: (Service Provider / Content Provider): وهو الشخص

الطبيعي أو الاعتباري الذي يملك الموقع الإلكتروني أو المنصة الرقمية وينشر المحتوى المعلوماتي، ويُعد المسؤول قانوناً عن جميع المعلومات والبيانات التي يتم اتاحتها وبثها عبر موقعه إلى الشبكة المعلوماتية، ويتمتع هذا المتعهد بالسلطة الفعلية والمباشرة في اختيار المحتوى ومراقبته وتعديله وحذفه، مما يجعله الجهة الوحيدة القادرة والمكلفة بضبط ومراقبة المادة المعلوماتية المنشورة في نطاقه.

4- ناقل المعلومات (Data Carrier/Transit Provider): هو الشخص الطبيعي أو

الاعتباري - غالباً شركة اتصالات أو مزود بنية تحتية - الذي يتولى، بموجب عقد نقل بيانات، عملية الربط الفني وتوجيه حزم المعلومات (Packets) من جهاز المستخدم النهائي إلى الخادم الرئيسي لمتعهد الوصول، ثم إعادة توجيهها من هذا الخادم إلى الخوادم المرتبطة بالمواقع الإلكترونية المطلوبة أو إلى أجهزة المستخدمين الآخرين على الشبكة، وذلك دون أي تدخل أو سيطرة على محتوى البيانات المنقولة².

ختاماً من الملاحظ أن كل شخص لديه القدرة على أن يكون عرضه لجرائم نظم المعلومات، سواء كان شخصاً معنوياً أو شخصاً طبيعياً، وما يمكننا التأكد عليه أن معظم جرائم نظم المعلومات تحدث لسببين وهما الأموال والمعلومات، وبالتالي هنا يمكننا تحديد المجني عليه وهم أما البنوك و المصارف أو شركات المعلومات، ولكن يفضل أغلبيتهم أي المجني عليهم عدم الاعترافات بوقوعهم ضحايا جرائم نظم المعلومات مما يعطي حافز للمجرمين على مواصلة هجماتهم ضد الضحايا، وهذا الاحجام عن الاعتراف أو التبليغ يؤثر سلباً في السياسة التي يمكن أن توضع لمكافحة هذا النوع من الجرائم.

1- حدة بوخالفه، النظام القانوني لمتعهد الإيواء عبر الانترنت، مجلة المفكر، العدد 14، جامعة محمد خضير بسكرة الجزائر، بدون سنة نشر، ص 292.

2- سعيداني نعيم، المرجع السابق ص 67.

الفصل الثاني : النظام القانوني لجرائم نظم المعلومات.

يُعبّر النظام القانوني لجرائم نظم المعلومات عن مجموعة القوانين والتشريعات والآراء الفقهية والاتفاقيات الدولية المعمول بها في البلدان المختلفة والتي تنظم مجموعة واسعة من جرائم نظم المعلومات الممكنة في السياق الرقمي، والأعمال والسلوكيات غير المشروعة التي تتعلق بالاستخدام الغير قانوني للتقنيات الالكترونية والأنظمة المعلوماتية.

حيث يهدف إلى توفير الحماية للمستخدمين من الأفراد وبياناتهم الشخصية ومؤسسات الدولة من الاضرار التي تلحق بالمعلومات أو الشبكات المعلوماتية وأجهزة الحاسب الآلي، التي يقوم بها المجرمون أو المجموعات الإجرامية المنظمة ، كلاً حسب دوافعهم وأهدافهم التي تكون غالباً تتعلق بتحقيق عوائد مادية.

ولهذا عرجنا في دراستنا لهذا الفصل في المبحث الأول إلى تناول تقسيمات جرائم نظم المعلومات تبعا لعدة حالات منها التقسيم حسب دور نظم المعلومات والتقسيم بحسب دور الحاسب الآلي، إضافة إلى دراسة جرائم نظم المعلومات حسب الآراء الفقهية والوكالات المتخصصة، كتصنيف المجلس الأوروبي، واتفاقية بودابست لعام 2001، أما المبحث الثاني جرائم نظم المعلومات وارتباطها بالجريمة المنظمة، وطرحنا أهم الجرائم المنظمة المستحدثة.

المبحث الأول: تقسيمات جرائم نظم المعلومات.

يعتمد النهج السائد في تصنيف جرائم نظم المعلومات على تحديد موضوع الجريمة والنشاط الإجرامي غير المشروع الموجّه ضد هذه النظم، وهو وضع قائمة منهجية بأبرز صور تلك الأنشطة الإجرامية، وقد تبنت هذا المنهج معظم الجهات العلمية والفقهية والمنظمات الدولية المتخصصة، فاستندت إليه غالبية التشريعات الجنائية الوطنية عند سنّ قوانينها الخاصة بمكافحة الجرائم المعلوماتية، ويهدف التقسيم أساساً إلى تمييز مختلف أشكال السلوك الضار وغير القانوني المتعلق بالحواسيب والشبكات المعلوماتية، ودراسة كل فئة على حدة، بغية تجميع الأفعال المتشابهة في الطبيعة والخصائص ضمن وحدة تصنيفية مستقلة، وفصلها عن غيرها من الفئات، وتكتسب هذه العملية أهمية بالغة لأنها تمكّن الجهات المختصة من تقدير درجة الخطورة الجنائية لكل نوع بالإضافة إلى تحديد درجة الخطر الجنائي لمرتكبي جرائم نظم المعلومات،

وتحديد حجم الضرر الناتج عنه، وترتيب الأولويات لتكثيف الجهود الوقائية والردعية ضد الأشد خطراً منها، كأولوية أولى، كما تساعد في وضع استراتيجيات وطنية ملائمة لمواجهة الجرائم المحلية، وفي الوقت ذاته تحديد مستوى وشكل التعاون الدولي اللازم لكشف الجرائم العابرة للحدود وتعقب مرتكبيها¹.

وعليه قمنا بتقسيم هذا المبحث إلى مطالبين نتناول في الأول منها تقسيم جرائم نظم المعلومات حسب دورها، أما في المطلب الثاني فنتناول تقسيم جرائم نظم المعلومات حسب الآراء الفقهية و المؤسسات المتخصصة.

الفرع الاول: تقسيم جرائم نظم المعلومات تبعاً لدور الحاسب الآلي .

لقد تعددت الجهود الفقهية التي بذلت من أجل وضع تقسيم خاص لجرائم نظم المعلومات، حيث تلعب نظم المعلومات أدواراً ثلاثة في ميدان ارتكاب الجرائم، و دوراً رئيسياً في مجال اكتشافها.

أولاً: نظم المعلومات باعتبارها هدفاً للجريمة.

وهنا تكون أنظمة المعلومات هدفاً للجرائم، مثل الوصول غير المصرح به إلى النظام أو زراعة الفيروسات لتدمير أو تعديل البيانات والملفات المخزنة فيها، أو الاستيلاء على البيانات المخزنة أو المنقولة عبر النظم المعلوماتية، ومن أوضح الاشكال لاعتبار نظم المعلومات هدافاً للجريمة في مجال التصرفات غير المشروعة عندما تكون السرية والتكاملية والسلامة والقدرة على التوفير هي التي يتم الاعتداء عليها، مما يعني أن القرصنة - نشاط إجرامي - موجهة ضد المعلومات المخزنة في نظام أو خدمات المعلومات، بهدف المساس بالسرية أو سلامة المحتوى أو تعطيل القدرة والكفاءة للنظام في أداء عمله، ويستهدف هذا النموذج الإجرامي النظم المعلوماتية وخاصة المعلومات المخزنة فيها بغرض السيطرة على النظام دون سلطة أو حقوق، أو دون دفع المستخدم مقابل استخدامه، أو المساومة على سلامة المعلومات وتعطيل القدرة على

1- طارق أبراهيم الدسوقي عطيه، المرجع السابق، ص 214-215.

تقديم خدمات نظام المعلومات، وتضم معظم هذه الجرائم الدخول غير المصرح به إلى الأنظمة المستهدفة، والذي يتم وصفه في الوقت الحالي بأنشطة الهاكرز كناية عن فعل الاختراق¹.

و تتخذ السلوكيات بما في ذلك سرقة المعلومات أشكالاً عديدة، اعتماداً على الطبيعة التقنية للنظام الذي يتم مهاجمته و الوسائل التقنية المستخدمة لتحقيق الهجوم، فالنظام المعلوماتي هو مستودع ومخزن للمعلومات الحساسة، مثل الحالة الجنائية والوثائق المتعلقة بالجيش، وهي هدف لهجمات متعددة الأطراف، بما في ذلك جهات التحقيقات الجنائية، والمنظمات الإرهابية، وأجهزة الأمن والاستخبارات من جميع الأطراف، ولا تعتمد أنشطة القرصنة على المستندات والأنظمة الحكومية وغير الحكومية فقط، بل ويمكنها أن تمتد إلى بيانات النظام الخاص التي تحتوي على معلومات قيمة²، فعلى سبيل المثال يمكن الوصول إلى نظام حجز الفندق من قبل المتسللين المخترقين لسرقة أرقام بطاقات الائتمان، وتستهدف بعض أشكال هذا النمط - أي نظم المعلومات كهدف- الهجمات على الملكية الفكرية مثل سرقة الأسرار التجارية ونسخ المصنفات المحمية وإعادة إنتاجها، وخاصة برامج الحاسب الآلي والسجلات الطبية وأنظمة الهاتف وما إلى ذلك³.

ثانياً: نظم المعلومات باعتبارها أداة لارتكاب جرائم تقليدية.

تُستخدم نظم المعلومات في هذه الفئة كوسيلة أو أداة لتنفيذ جرائم تقليدية بأسلوب حديث، فيُصبح الحاسب الآلي والشبكة أداة الاعتداء بدلاً من كونه هدفاً، ومن أبرز صور ذلك: الاستيلاء على الأموال عن طريق التحويلات البنكية غير المشروعة، أو التزوير الإلكتروني للوثائق، أو سرقة أرقام بطاقات الائتمان وإعادة استخدامها في عمليات احتيال، أو حتى استخدام النظم المعلوماتية والتقنية لارتكاب جرائم قتل عن بُعد، كالتسلل إلى قواعد البيانات الطبية وتعديل الجرعات الدوائية أو التلاعب بأجهزة التنفس الصناعي وأجهزة دعم الحياة، أو العبث ببرامج التحكم في الطائرات أو السفن أو القطارات أو أنظمة المرور، مما يؤدي إلى حوادث مدمرة

1- طارق أبراهيم الدسوقي عطيه، المرجع السابق، ص 216-217.

2- أيمن عبدالله فكري، المرجع السابق، ص 118.

3- للمزيد أنظر في ذلك رصاع فتيحة، المرجع السابق، ص 70.

وخسائر في الأرواح.. وبهذا تتحول التكنولوجيا من وسيلة خدمية إلى سلاح فعلي يُستخدم لتحقيق غرض إجرامي تقليدي بكفاءة أعلى وتأثير أوسع¹.

ثالثاً: نظم المعلومات باعتبارها بيئة للجريمة.

في هذه الفئة تتحول نظم المعلومات إلى فضاء أو بيئة خصبة لارتكاب الجريمة وتسهيلها، فيستخدم الحاسب الآلي أو الشبكة كمخزن أو وسيط لتخزين ونشر المواد غير القانونية، مثل البرمجيات والأفلام والمصنفات المقرصنة، أو كقناة اتصال وتنسيق لأنشطة إجرامية تقليدية كترويج المخدرات، وتشغيل شبكات الدعارة والابتزاز الجنسي، وغسل الأموال².

وقد يجمع الحاسب الآلي في الواقعة الواحدة بين الأدوار الثلاثة معاً؛ فمثلاً قد يخترق أحد الهاكرز نظام مزود خدمة إنترنت (كشركة **America Online** سابقاً) دون تصريح (نظام معلومات كهدف)، ثم يستغل هذا الاختراق لتوزيع برامج مقرصنة مخزنة على جهازه (نظام معلومات كأداة لجريمة تقليدية)، وفي الوقت نفسه يكون جهازه بمثابة مخزن وبيئة للجريمة باحتفاظه بالملفات غير القانونية وتوزيعها على نطاق واسع، وبهذا تتداخل الأدوار الثلاثة (هدف - أداة - بيئة) في كثير من الجرائم المعلوماتية المعقدة³.

رابعاً: نظم المعلومات باعتبارها كاشفة للجريمة.

تُستخدم أنظمة المعلومات الآن كأداة أساسية وعلى نطاق واسع في التحقيقات الاستدلالية والجنائية لمعظم الجرائم، بالإضافة إلى اعتماد جهات إنفاذ القانون على الأنظمة التكنولوجية لإدارة عملها من خلال بناء قواعد بيانات داخل جهاز العدالة و دوائر التنفيذ القانوني.

وبما أن جرائم نظم المعلومات نفسها تتطور باستمرار بفضل التقنيات المتقدمة التي يستخدمها الجناة في نشاطهم غير المشروع، فإنه من الضروري استخدام نفس الوسائل الإجرامية المتقدمة للتحقيق فيها والكشف عنها من قبل جهاز إنفاذ القانون، لذلك تلعب أنظمة المعلومات نفسها دوراً محورياً في اكتشاف جرائم نظم المعلومات وتعقب مرتكبيها، وحتى التصدي لها و إبطال مفعولها، وخاصة هجمات الفيروسات وإنكار الخدمة وقراصنة البرامج، وغيرها من الأنماط

1- أيمن عبدالله فكري، المرجع السابق، ص 119.

2- للمزيد أنظر في ذلك بلال بن جامع، المرجع السابق ص 128.

3- أيمن عبدالله فكري، المرجع السابق، ص 119.

الإجرامية المعلوماتية، وبذلك تتحول التكنولوجيا من سلاح في يد الجاني إلى أقوى حليف لأجهزة العدالة في كشف الجريمة والحد منها.

ويتضح مما سبق عرضة أنه يمكن تقسيم جرائم نظم المعلومات حسب دور الحاسب الآلي في الجريمة فمن الممكن أن يكون دور الحاسب الآلي مساعدا في الجريمة وهنا يكون دورة ثانويا، ويمكن أن يكون دورة رئيسا عندما لا يمكن أن ترتكب الجريمة بدونه، وبهذا تكون جرائم نظم المعلومات حسب هذا التصنيف "هي كُلُّ نشاطٍ إجراميٍّ يُؤْذِي فِيهِ نِظَامُ الْحَاسِبِ دَوْرًا لِإِثْمَامِهِ عَلَى أَنْ يَكُونَ هَذَا الدَّوْرُ عَلَى قَدْرِ مِنْ الْأَهْمِيَّةِ ، وَلَا يَخْتَلِفُ الْأَمْرُ سِوَاءَ كَانَ الْحَاسِبُ الْآلِيَّ أَدَاةً لِإِثْمَامِ الْجَرِيمَةِ أَوْ مَحَلًّا لَهَا"¹.

المطلب الأول: تقسيم جرائم نظم المعلومات حسب دورها.

يمكن القول إن جرائم نظم المعلومات - رغم تنوع أشكالها وتصنيفاتها - تُختزل في أربع فئات رئيسية تحكمها عناصر مشتركة تتمثل في دور الحاسب الآلي في الجريمة، أو طبيعة المعلومات التي طالتها الجريمة، أو الأثر الناتج عنها على الأفراد وحقوقهم المالية والمعنوية، وعليه، يُمكن تقسيم جرائم نظم المعلومات، استناداً إلى تلك السمات المشتركة إلى أربعة تصنيفات رئيسية سيتم تناولها تفصيلاً في الفروع الأربعة التالية.

الفرع الثاني: تقسيم جرائم نظم المعلومات تبعاً لمحل الجريمة.

أولاً: جرائم نظم المعلومات الماسة بمعطيات الحاسوب.

يضم هذا التصنيف جميع الجرائم والأفعال التي تستهدف المعلومات والمعطيات الإلكترونية المخزنة والمسجلة على أجهزة الحواسيب وأنظمة المعلومات، وتتجلى بشكل أساسي في الاستخدام المباشر أو من خلال استخدام وسائل مختلفة لتدمير وتشويه البيانات والمعلومات الإلكترونية المسجلة على أنظمة المعلومات وبرامج الحاسب الآلي، باستخدام الوسائل التقنية المتقدمة كالفيروسات والبرامج المستخدمة للتدمير والاختراق.

كما يشمل التصنيف أيضاً الجرائم الواقعة على الأصول بما تمثله من قيم مالية ومادية للمعلومات، وهي جريمة تُعرف باسم "الغش المعلوماتي" أو جرائم الاتجار بالبيانات والمعطيات

1- طارق أبراهيم الدسوقي عطيه، المرجع السابق، ص219.

الآلية المسروقة من الحاسب الآلي أو نظم المعلومات وشبكات المعلومات المتعددة، وتعد هذه الفئة من جرائم الاعتداء المباشر على سلامة وتكامل وسرية المعلومات الرقمية كأصل مستقل ذي قيمة اقتصادية وقانونية¹.

ثانياً: جرائم نظم المعلومات الماسة بالمعطيات الشخصية.

يضم هذه النوع كافة الجرائم التي تستهدف البيانات والمعطيات الشخصية، وهي الجرائم ضد البيانات والمعلومات السرية أو المحمية والجرائم ضد البيانات الشخصية المتعلقة بالحياة الخاصة، ومجموعة من الأفعال التي يقوم بها مجرمو المعلومات، للحصول على المعلومات الشخصية والاستيلاء عليها واستغلالها في الأعمال التي تضر بمالك هذه المعلومات²، وتتخذ هذه الجرائم صوراً متعددة، منها التنصت الإلكتروني على المحادثات الخاصة عبر وسائل الاتصال المرتبطة بالحاسب، وتسجيلها، ونقلها، أو اختراق قواعد البيانات الشخصية، أو سرقة الهوية الرقمية، أو نشر معلومات خاصة دون موافقة صاحبها، وكلها أفعال تُشكّل انتهاكاً صارخاً للحياة الخاصة ولحقوق الخصوصية المكفولة قانوناً ودستورياً³.

ثالثاً: جرائم نظم المعلومات الماسة بحقوق الملكية الفكرية لبرامج الحاسب.

تتضمن هذه الفئة كل الأفعال غير المشروعة التي تنتهك حقوق الملكية الفكرية المتعلقة ببرامج وأنظمة الحاسوب في البيئة الرقمية، وأبرزها قرصنة البرمجيات، والنسخ غير المصرح به، والنقل، والتصنيع، وإعادة الإنتاج أو التوزيع للبرامج الإلكترونية دون إذن صاحب الحق، فضلاً عن التعدي على العلامات التجارية المسجلة وبراءات الاختراع المتعلقة بالتقنيات المعلوماتية دون ترخيص من المالك أو حامل الحق الأصلي⁴.

بالنظر إلى هذا التصنيف، نؤيد الرأي القائل إن الحدود الفاصلة بين فئات جرائم نظم المعلومات ليست صلبة ومحددة، بل تتسم بتداخل حقيقي وجوهري، ذلك أن الاعتداء على القيمة المادية أو المعنوية للبيانات والمعطيات المخزنة في الحاسب يُشكّل في الوقت ذاته مساساً بأمن

1- بلال بن جامع، المرجع السابق ص 131.

2- أيمن عبدالله فكري، المرجع السابق، ص 139.

3- غانم مرضي الشمري، المرجع السابق، ص 51.

4- بلال بن جامع، المرجع السابق ص 132.

هذه البيانات. غير أن الفارق الجوهرى يكمن في أن الهدف المباشر لهذه الفئة ينصبّ أساساً على قيمة المعلومات ذاتها أو ما تُمثّله من حقوق، بينما يتركز الاعتداء على حقوق الملكية الفكرية لبرامج الحاسوب على الحقوق المالية والأدبية للمؤلف أو الشركة المالكة، مع فارق أن محل الجريمة في هذا التصنيف هو البرنامج بحد ذاته، وأن الغرض الإجرامي الأساسي يتمثل في الاستعمال غير المشروع أو الحيازة غير القانونية لهذه البرمجيات دون سواها¹.

الفرع الثالث: تقسيم جرائم نظم المعلومات تبعاً لعلاقتها بالنظام الآلي.

يعتمد هذا التقسيم على البيئة التي تحدث فيها الجريمة و باعتبار نظم المعلومات هي البيئة الالكترونية التي يقع فيها هذا النوع من الجرائم المعلوماتية، فهذا يعني أن هذا التصنيف مقسم لنوعين إما جرائم ضد نظم المعلومات أو باستخدام هذه النظم المعلوماتية.

أولاً: الجرائم ضد نظم المعلومات.

في هذا النوع وجب التنبيه إلى أن الفقهاء والمتخصصين في جرائم نظم المعلومات يستخدمون تسميات متعددة ومتباينة لهذا النوع من الجرائم، فمنهم من أطلق عليها " جرائم التعدي على وظائف النظام المعلوماتي"، ومنهم من سماها " جرائم الاعتداء على أنظمة المعالجة الآلية للبيانات"، وغيرها من التوصيفات.

غير أنها تتميز جميعها عن الجرائم التقليدية بطبيعتها الهادئة والخفية، إذ لا تتطلب عنفاً جسدياً أو جهداً عضلياً، وإنما تكتفي بسلسلة من الأوامر والإجراءات التقنية عبر البرمجيات والأدوات الإلكترونية، بحيث يصدر الجاني تعليمات للحاسب الآلي تؤدي إلى اعتداء مباشر على أي من مكونات النظام المعلوماتي، سواء كانت مادية (الأجهزة والخوادم)، أو برمجية (نظم التشغيل والتطبيقات)، أو بيانية (المعلومات والسجلات والملفات المخزنة²، ويقسم هذا النوع من الجرائم على النحو التالي:

1- أنظر في ذلك أيمن عبدالله فكري، المرجع السابق، ص 139.

2- بلال بن جامع، المرجع السابق ص 132-133.

1- الجرائم الواقعة على المكونات المادية.

تميز هذه الفئة بتشابهها الكبير مع الجرائم التقليدية من حيث طبيعتها المادية واستخدام القوة الجسدية، إلا أنها تختلف عن الجرائم المعلوماتية النقية بكونها تستهدف الجانب المادي الملموس لأنظمة الحاسب والشبكات، وارتباطها بجرائم نظم المعلومات يقتصر على وقوع الاعتداء على الأجهزة والمكونات الفعلية التي تُشكّل البنية التحتية لتلك النظم، مثل سرقة الحواسيب أو الخوادم أو الأجهزة المتصلة بالشبكة، أو تخريب كابلات الألياف البصرية والتوصيلات الكهربائية، أو إتلاف الهوائيات وأجهزة الإرسال والاستقبال، أو تدمير الأقمار الصناعية أو المحطات الأرضية، وكلها أفعال تُرتكب بوسائل تقليدية لكنها تُصيب قلب البنية التحتية المادية لتنظم المعلومات وتعطل عملها¹.

2- الجرائم الواقعة على المكونات المنطقية لتنظم المعلومات.

تتجلى هذه الجرائم بشكل رئيسي في انتهاك المكونات غير الملموسة لأنظمة المعلومات، مثل البرامج والبيانات المخزنة على أجهزة الحاسب الآلي، وهناك نوعان أساسيان من الجرائم المرتكبة ضد برامج الحاسب الآلي، على حسب نوعية هذه البرنامج المستخدم، فإما أن تكون هجمات على البرامج التطبيقية أو على برامج تشغيل الحاسب الآلي، وبرنامج التشغيل هو البرنامج الذي يستطيع الحاسب من خلاله أداء وظيفة محددة، ويتم ارتكاب جريمة ضد برنامج التشغيل من خلال تزويد البرامج التطبيقية بمجموعة من التطبيقات الفرعية التي تسهل الوصول إلى نقاط الضعف في النظام والحصول على جميع البيانات والمعطيات الواردة في النظام المعلوماتي، أو الدخول في نظام المعلومات عن طريق شبكة الاتصالات والهاتف، أما النوع الثاني فهي الهجمات على البرامج التطبيقية التي تكون مكتوبة بأحد لغات الحاسوب، والتي تكون متاحة للاستعمال من قبل العملاء بغض النظر عن نوع الحاسب، ومقارنة ببرامج التشغيل فإن نسبة الاعتداء على البرامج التطبيقية أقل من برامج التشغيل، وتتم هذه الجريمة من خلال طرق

1- بلال بن جامع، نفس المرجع السابق ص 133.

فنية تمكن من التقاط المعلومات أو الدخول إلى الشبكات والتدخل في عمل البرامج التطبيقية للحصول على معلومات أو تعطيل معلومات إلكترونية¹.

ثانياً: الجرائم باستخدام نظم المعلومات.

هي الجرائم التي يقوم فيها المجرم المعلوماتي بعدد من الأفعال الإجرامية باستخدام النظم الآلية فيستخدم في ذلك الشبكات ويعتمد على التطبيقات المكونة للنظم الآلية من خلال إعطاء أوامر لتنفيذ إجراءات وتطبيقات لا توجد في النظام من أجل تحقيق منافع شخصية وغير مشروعة وهي تشمل ثلاثة أصناف:

1- الجرائم المرتبطة بالأموال الإلكترونية: وهي مجموعة الأفعال التي تستهدف الأموال وصورها الإلكترونية المخزنة أو المتداولة عبر الأنظمة الآلية وشبكات المعلومات، فيستفيد مجرم المعلوماتية من زيادة الرصيد المالي أو إلحاق الضرر بالموارد المالية، وتتجلى هذه الأفعال في صور متعددة أبرزها (جرائم الاحتيال في التجارة الإلكترونية، جرائم الغش بالأموال الإلكترونية، جرائم ضد حقوق المستهلك، جرائم التعدي على التحويل الإلكتروني للأموال، جرائم غسيل الأموال عبر الانترنت)².

2- الجرائم المرتبطة بالخصوصية: وتشمل القرصنة على البيانات الشخصية، انتحال الشخصية، جرائم السب والقذف عبر الانترنت، جرائم التعدي على الحياة الخاصة، الجرائم المخلة بالآداب العامة.

3- جرائم الدخول واستعمال النظام المعلوماتي: تعرف باسم " الاختراق " وتختلف دوافع هذه الاختراقات حسب الهدف من الاختراقات ومنها (اختراق الأمن الداخلي للمؤسسات، اختراق الأمن الشخصي للأفراد، اختراق الحماية الخاصة بالاتصالات وأمن البيانات، الاعتداء على

1- بلال بن جامع، المرجع السابق ص 134.

2- بلال بن جامع، نفس المرجع السابق ص 135.

عملية الحماية ، الاستعمال غير المصرح به للنظام المعلوماتي بقصد الاستطلاع أو الاستيلاء أو التعطيل¹.

4- جرائم الاعتداء على البريد الإلكتروني: ويشمل هذا النوع كل فعل إجرامي يستهدف البريد الإلكتروني كجريمة التعدي على البريد الإلكتروني، و جريمة تضخيم البريد الإلكتروني.

الفرع الرابع: تقسيم جرائم نظم المعلومات تبعاً لمساسها بالأشخاص والأموال.

يُعد هذا التصنيف أمريكي الأصل، وقد تبلور عام 1998 ضمن مشروع " القانون النموذجي لجرائم الكمبيوتر والانترنت" من قبل مجموعة الباحثين الاكاديميين تحت مسمى **"Model State Computer Crimer Code"** بهدف توحيد قوانين الولايات المتحدة المتعلقة بهذا الشأن، وفيه تم تقسيم جرائم الحاسوب والانترنت إلى خمس فئات (جرائم ضد الاشخاص وجرائم ضد الاموال وجرائم السرقة والاحتيال و التزوير والقمار وجرائم ضد الآداب وجرائم الاضرار بمصالح الدولة)².

أولاً: الجرائم الواقعة على الأشخاص.

يشمل الجزء الأول كل الجرائم الأفعال غير القانونية والممارسات التي تؤثر على الأشخاص والأموال، أو تهدد السلامة الجسدية والنفسية كالقتل بواسطة الحاسب الآلي، والتسبب في الوفاة، وجرائم الإهمال المرتبطة بالحاسب، والتحريض على الانتحار من خلال شبكة نظم المعلومات، والتحريض العمدي على القتل عبر الإنترنت، و الوصول إلى البيانات الشخصية والأنشطة المتعلقة بالفيروسات والمتمثلة في قنابل البريد الإلكتروني، ونقل معلومات مضللة أو كاذبة، وانتهاكات الشخصية لحرمة أجهزة الحاسب الآلي، أو الوصول غير المصرح به إلى الأنظمة الآلية³.

1- يعني الاستعمال غير المصرح به للنظام المعلوماتي أنه "كل افعـل إجرامي يهدف إلى سرقة وقت الحاسب الالي فهو بذلك كل استعمال غير شرعي للوظيفة التي يؤديها الحاسب الآلي خلال فترة دوام عمل الموظفين دو أن يكون مصرًا بذلك"، للمزيد أنظر في ذلك بلال بن جامع، المرجع السابق ص 143.

2- طارق أبراهيم الدسوقي عطيه، المرجع السابق، ص 234.

3- بلال بن جامع، المرجع السابق ص 146.

كما يشمل هذا النوع الجرائم الجنسية المرتكبة ضد الأشخاص وأبرزها تحريض القاصرين على الأنشطة الجنسية غير المشروعة، ومحاولات إغوائهم أو استدراجهم للقيام بأفعال جنسية غير مشروعة، واستخدام الشبكات للترويج للدعارة أو لنشر مواد إباحية، وعند التدقيق يتضح أن هذا النوع من الجرائم يتفق في جوهره مع استغلال الانترنت والحاسب الآلي كوسيلة فعالة للترويج للدعارة ونشر الأنشطة الجنسية غير المشروعة¹.

أولاً: الجرائم ضد الأموال (عدا السرقة).

ويتضمن الجزء الثاني من التصنيف الأمريكي كل الأفعال الإجرامية التي تلحق ضرر بالأموال والممتلكات الرقمية دون أن تشكل سرقة بالمفهوم التقليدي ومن أبرزها الدخول أو الوصول غير المصرح به إلى نظام أو شبكة الحاسب، وأعمال تدمير البيانات والمعطيات والأنظمة والممتلكات داخل نظام أو شبكة الحاسب، بما يعني تخريب الحاسب وانتهاك حقوق الملكية الفكرية و إنتاج برامج ضارة أو نشرها عبر أنظمة وشبكات المعلومات، أو انتحال أسماء العلامات التجارية أو استخدام اسم شخص آخر دون إذن المالك، أو إدخال بيانات كاذبة أو مزورة في أنظمة الحاسوب، أو إجراء تعديل غير مصرح به لأنظمة الحاسب، أو هجمات إنكار الخدمة أو تعطيل أو اعتراض العمل على أنظمة المعلومات، والحيارة غير المشروعة للمعلومات الإلكترونية².

ثانياً: جرائم السرقة والاحتيال والتزوير.

ويشمل الجزء الثالث من الجرائم الماسة بالأشخاص والأموال على جرائم الاحتيال³ والتلاعب بالمعطيات والنظم، واستخدام الحاسب للحصول على البطاقات المالية، واستخدام

1- غانم مرضي الشمري، المرجع السابق، ص 57.

2- بلال بن جامع، نفس المرجع السابق ص 147.

3- ونشير هنا إلى بعض التعريفات الفقهية لجريمة الاحتيال حيث عرفت على أنها "استخدام الجاني لطريقة احتيالية محددة وحمل المجني عليه بذلك على تسليم الجاني مالا منقولاً مملوكاً للغير"، أما الاحتيال الحاسوبي أو ما يسمى بالاحتيال المعلوماتي، فإن أصوله هي نتيجة التطورات التكنولوجية الحديثة التي أدت إلى ظهور نماذج إجرامية جديدة، والتي يعرفها البعض على أنها الاحتيال المرتكب باستخدام أجهزة الحاسوب وأنظمة الاتصالات لتحقيق مكاسب مادية، و أقرت هيئة للأمم المتحدة تعريفاً للاحتيال بأنه (إدراج أو حذف أو تعديل أو قمع البيانات أو برامج الكمبيوتر، أو التدخل الفعال في معالجة البيانات، مما يتسبب في خسارة اقتصادية أو فقد حيابة ملكية شخص بقصد الحصول على ربح اقتصادي غير مشروعة له أو لشخص آخر)، بينما اختارت

البطاقات هذه دون إذن من صاحبها، والاختلاس عبر الحاسب الآلي أو بواسطته، وسرقة معلومات الحواسيب الآلية، وقرصنة البرمجيات الآلية، وسرقة خدمات الحاسب الآلي أو ما يطلق عليه سرقة وقت الحاسب وسرقة ادوات التعريف والهوية عبر انتحال هذه الصفات أو المعلومات على الكمبيوتر، أما جرائم التزوير فهي تشمل كل الأعمال المرتبطة بتزوير البريد الإلكتروني وتزوير الوثائق والسجلات الإلكترونية وهوية الأفراد على الحواسيب ونظم المعلومات الآلية¹.

ثالثاً: جرائم المقامرة والجرائم ضد الاخلاق.

ويشمل النشاطات المرتبطة بالمقامرة على شبكة الانترنت وعدد من الأفعال المنافية للأداب والأخلاق العامة، حيث تم تحديدها في تملك وإدارة مشروع مقامرة على الانترنت، وتسهيل مشاريع القمار على الانترنت وتشجيع مشروع المقامرة على شبكة الانترنت واستخدام الانترنت لترويج للكحول ومواد الإدمان للقصر².

رابعاً: جرائم ضد الحكومة.

وتشمل كل أشكال الجرائم التي تؤدي إلى تعطيل الأعمال الحكومية وتطبيق القانون حيث جمعت هذه الفئة كل ما يترتب على الإخفاق في الإبلاغ عن جرائم الحاسب الآلي، والسلوكيات المؤدية إلى الحصول على معلومات سرية، والاعلام المضلل أو الخاطئ عن جرائم الحاسب الآلي، والعبث بالأدلة القضائية أو التأثير فيها والاعمال المرتبطة بتهديد السلامة العامة، وبث البيانات من مصادر مجهولة، كما تشمل الجرائم ضد الحكومة والإرهاب الإلكتروني والأنشطة التآرية الإلكترونية³.

مجموعة أخرى تعرف لجنة أوديت، وهي لجنة تدقيق للحسابات في المملكة المتحدة، تُعرّف الاحتيال على الحاسب الآلي بأنه (أي سلوك احتيالي أو خادع فيما يتعلق بجهاز الحاسب الآلي، يقصده شخص ما للحصول على ميزة أو مكاسب مالية)، للمزيد أنظر في ذلك، د غانم مرضي الشمري، المرجع السابق، ص58.

1- أيمن عبدالله فكري، المرجع السابق، ص 135.

2- طارق أبراهيم الدسوقي عطيه، المرجع السابق، ص237.

3- بلال بن جامع، المرجع السابق ص 147-148.

المطلب الثاني: تقسيم جرائم نظم المعلومات حسب الآراء الفقهية والوكالات المتخصصة.

في هذا الصدد قام العديد من الفقهاء والباحثين بمحاولات متنوعة اجتهدية لتقسيم جرائم نظم المعلومات، إضافة إلى تلك الجهود برزت جهود الوكالات والمنظمات المتخصصة ممثلة في منظمة التعاون الاقتصادي والتنمية والمجلس الأوروبي وكذلك التصنيفات التي جاءت بها الاتفاقية الدولية لمكافحة الجرائم المعلوماتية بودابست، ونبدأ بعرض هذا الاجتهادات بالتقسيم الفقهي لجرائم نظم المعلومات في الفرع الأول، ثم تصنيف الوكالات المتخصصة الدولية لجرائم نظم المعلومات في الفرع الثاني.

الفرع الأول : التقسيم الفقهي لجرائم نظم المعلومات.

شهد الفقه القانوني محاولات متعددة لتحليل وتقسيم جرائم نظم المعلومات، وذلك لما تتمتع به هذه الجرائم من خصائص فريدة تجعل ارتباطها بالحاسب الآلي عنصراً فارقاً يميزها عن غيرها من الجرائم التقليدية، وقد تباينت آراء الباحثين بشأن أسس تصنيف هذه الجرائم وتحديد الأفعال التي تندرج ضمن نطاقها، وفي هذا السياق، وهنا سنعرض التصنيفات التي وضعها كل من الفقيهين **Ulrich Sieber** و **Martin Vasik**.

أولاً: تقسيم الفقيه "Ulrich Sieber" لجرائم نظم المعلومات.

قسم الفقيه جرائم نظم المعلومات إلى ثلاثة طوائف رئيسية، تتعلق الطائفة الاولى بجرائم الحاسب الآلي الاقتصادية، والثانية بجرائم الحاسب الآلي التي تعتدي على الحياة الخاصة والثالثة طائفة الجرائم التي تهدد المصالح القومية أو السلامة الشخصية للأفراد.

1- جرائم الحاسب الآلي الاقتصادية:

النوع الاول من تقسيم الفقيه **"Ulrich Sieber"** وتشمل تمثل جرائم الحاسب الآلي الاقتصادية القسم الرئيسي لجرائم نظم المعلومات وقد أستبعد من نطاقها الأفعال التي تلحق الضرر بنظام الحاسب الآلي نتيجة الخطأ أو الإهمال، ويندرج ضمن هذا النوع من الجرائم مجموعة من الأفعال ذات الطابع الاقتصادي وهي:

- 1- الإحتيال المعلوماتي هو تلك الأفعال التي تقوم على التلاعب في نظم المعلومات للحصول بغير حق على أموال أو أصول أو خدمات.
- 2- التجسس المعلوماتي في نطاق قطاع الاعمال، وتقوم تلك الجرائم على اختراق النظام المعلوماتي من أجل الاستفادة بما يتم التوصل إليه من معلومات.
- 3- قرصنة برامج الحاسب الآلي.
- 4- الإتلاف المعلوماتي سواء تعلق بالمكونات المادية أو غير المادية للحاسب الآلي.
- 5- الدخول غير المصرح به لنظام الحاسب الآلي.
- 6- سرقة الخدمات أو الاستعمال غير المصرح به للنظام المعلوماتي.
- 7- الجرائم التقليدية في نطاق قطاع الاعمال والتي يساعد النظام المعلوماتي في ارتكابها، ويدخل في هذا النوع استخدام الحاسبات لإخفاء التلاعب الذي يتم من قبل القائمين على إدارة المؤسسات.

2- الجرائم المتصلة بانتهاك حرمة الحياة الخاصة.

في النوع الثاني من تقسيم الفقيه **Ulrich Sieber** أعتمد على معياراً موضوعياً يقوم على تحديد طبيعة الوسيلة المستخدمة في انتهاك الخصوصية لتصنيف صور التهديد المعلوماتي للحياة الخاصة، ويمكن وفق هذا المعيار التمييز بين أربعة أنماط رئيسية لهذا التهديد.

أ- استخدام بيانات شخصية غير صحيحة.

ويكون استخدام المعلومات الشخصية بنحو غير صحيح بأحد الطريقتين:

- تغيير البيانات الشخصية أو محوها عن طريق أشخاص غير مصرح لهم بذلك.

ويشمل هذا التلاعب الاعتداء على الحياة الخاصة لصاحب المعلومات وفي كثير من الاحيان يشمل أيضا على المساس بالحقوق المالية للمرخص لهم بتخزين هذه البيانات¹.

1- في هذا السياق، يُشار إلى قضية شركة TRW Company Credit Data الأمريكية، التي كانت تُقدّم خدمات تقارير حالة الجدارة الائتمانية أو القدرة، بحيث تقوم الشركة بجمع معلومات ائتمانية عن الأفراد وتُرَوّد عملاءها الذين يدفعون رسوم اشتراك للحصول على هذه التقارير، بهدف مساعدتهم على تجنّب المخاطر المرتبطة بالتعامل مع أشخاص ذوي سجل ائتماني سيئ أو ضعيف، إلا أن بعض موظفي الشركة قاموا بتلاعب غير مشروع في قواعد البيانات، حيث عمدوا إلى تعديل أو حذف المعلومات السلبية في ملفات ائتمانية لأكثر من

• جمع أو معالجة أو نشر معلومات شخصية غير صحيحة.

وهو الجمع المتعمد أو المعالجة أو النشر لمعلومات غير صحيحة من قبل الأشخاص المصرح لهم بنشر المعلومات، وقد يكون ذلك بصورة عمدية، ومع ذلك إن العديد من حالات جمع المعلومات الشخصية غير الصحية أو معالجتها أو نشرها تتم من خلال الإهمال، لا سيما فيما يتعلق بنظم تقارير الائتمان، وهذا ما تتخذ ضده الانظمة القانونية تدابير مدنية وإدارية¹.

ب- جمع وتخزين معلومات صحيحة على نحو غير مشروع.

لا يتم انتهاك الخصوصية وحق الأفراد في مجال النظم المعلوماتية عن طريق استخدام البيانات الشخصية فقط وإنما يكون كذلك في حالة جمع وتخزين بيانات شخصية غير صحيحة ولكن بطريقة غير مشروعة، ونجد صفة عدم المشروعية ممثلة في نقطتين الأولى وهي في الاساليب غير المشروعة للحصول على البيانات الشخصية كأستخدام الارتجاجات الصوتية على الجدران الاسمنتية وترجمتها بواسطة برامج خاصة، أو اعتراض الرسائل المتبادلة عبر البريد الإلكتروني، أو استخدام الأسلاك بطريقة خفية داخل الحاسب الآلي الذي تخزن فيه البيانات، أما النقطة الثانية التي يمكن أن تضيف صفة عدم المشروعية فتتمثل في مضمون المعلومات التي يتم جمعها أو تخزينها، ونعني هنا نوعية البيانات التي يمكن أن تجمع وتخزن بسبب مضمونها، أذ أن عدم وجود ضوابط قانونية يمكن أن يؤدي إلى جمع وتخزين ونقل كم هائل من المعلومات قد تتعلق بأدق الأمور الخاصة بالأفراد، وهو ما يمكن أن يتيح خلق صورة مفصلة لشخصهم بمجرد الاطلاع على معلوماتهم داخل نظام الحاسب الآلي².

ت- الإفشاء غير المشروع للمعلومات الشخصية وإساءة استخدامها.

عمل الفقيه "Ulrich Sieber" في هذا الخصوص على التفريق بين نوعين من البيانات الشخصية النوع الأول بيانات شخصية مشمولة بالحماية الجنائية التقليدية للأسرار وهي

100 شخص تقريباً، واستبدلوها ببيانات مزيفة تُظهر أن أصحاب هذه الملفات يتمتعون بسجل انتمائي جيد، وذلك مقابل منافع شخصية أو مالية، للمزيد أنظر، نائلة عادل قورة، المرجع السابق، ص 235-236.

1- نائلة عادل قورة، نفس المرجع السابق، ص 236.

2- نائلة عادل قورة، نفس المرجع السابق، ص 236، 237.

التي لا يثور أدنى شك في عدم مشروعية الإفشاء بها لطالما تسري عليها النصوص الجنائية التقليدية الخاصة بحماية الأسرار، ويظهر هذا أكثر وضوحاً في المجالات الخاصة كالطب والمحاماة والأعمال المصرفية على سبيل المثال، أما النوع الثاني فهو يتعلق بالبيانات الشخصية غير السرية والتي لا تتمتع بالحماية القانونية والتي يكون من الصعوبة تحديد نوعية ونسبة الضرر الذي يصيب المجتمع من جراء إفشاء هذه البيانات وعدم القدرة على تكييف هذا الفعل هل يدخل في إطار عدم المشروعية أم مباح، وتظهر هذه التصرفات في حالات تبادل البيانات الشخصية ما بين الجهات الحكومية لأغراض متعددة¹.

ث- مخالفة القواعد والإجراءات الشكلية التي تدخل في نطاق الحماية التشريعية لخصوصية المعلومات.

أنه لمن الضرورة أن تتمتع خصوصية المعلومات بالحماية القانونية حتى في الحالات التي أجبز فيها جمعها ومعالجتها ونشرها، هذا ما دفع العديد من النظم القانونية إلى العمل على وضع مجموعة من القواعد الشكلية لتنظيم جمع ونشر البيانات ذات الطبيعة الشخصية، وفي كثير من الدول يعتبر خرق هذه القواعد أو تجاهلها جرائم يعاقب عليها القانون².

3- الجرائم التي تهدد المصالح القومية أو السلامة الشخصية للأفراد.

نظراً للتوسع في تطبيق تكنولوجيا المعلومات في جميع مجالات الحياة، لا تقتصر جرائم المعلومات على الجرائم التي تؤثر على الجانب المالي أو الاعتداء على الحياة الخاصة، ولكنها توسعت أيضاً لتشمل أنواعاً أخرى من الجرائم³، فمن ناحية، قد تؤثر جرائم نظم المعلومات على

1- نائلة عادل قورة، نفس المرجع السابق، ص 237، 238.

2- ونشير في هذا الصدد إلى قضية الشركة الفرنسية "SKF" والتي قامت بتخزين بيانات تتعلق بالحياة الخاصة والاتجاهات السياسية وعضوية الاتحادات لموظفيها، حصلت عليها من الاستثمارات التي قام موظفيها بتقديمها عند التقدم للوظيفة دون إذن مسبق من اللجنة الوطنية للمعلومات والحريات "CNIL" طبقاً لأحكام القانون وهذا ما يعتبر مخالفة لنص المادة 42 من القانون الفرنسي رقم 78-17 الخاص بمعالجة المعلومات لسنة 1978 والمعدل في 11 مارس 1988 والتي تعاقب بالحبس من سنة إلى خمس سنوات وبغرامة لا تقل عن 20 ألف فرنك فرنسي ولا تزيد عن 02 مليون فرنك كل من قام بجمع وتخزين البيانات الشخصية بالمخالفة للقواعد الشكلية، مشار إليه أنظر في ذلك نائلة عادل قورة، نفس المرجع السابق، ص 238.

3- أيمن عبدالله فكري، المرجع السابق، ص 122.

المصلحة العليا للدولة، مثل الحصول على معلومات قد تتعلق بالأمن القومي، كما لو كانت متعلقة بالاستخبارات أو الدفاع، أو التلاعب الحاسوبي بنتائج الانتخابات، ومن ناحية أخرى، قد تمتد جريمة أنظمة المعلومات إلى السلامة الشخصية للأفراد ولعل أبرز مثال على ذلك هو التلاعب في أنظمة الحاسوب المتعلقة بالحركة الجوية تهديدًا للسلامة الشخصية، ومن الأمثلة على ذلك ما حدث في 18 يناير 1979 عندما تعرضت إحدى الطائرات في مطار جون كنيدي في نيويورك وعلى متنها السفير الروسي، تعرضت للتهديد بسبب تلاعب مراقبي الحركة الجوية بنظام الحاسب الآلي الخاص بالملاحه¹.

ثانياً: تقسيم "Martin Vasil" لجرائم نظم المعلومات.

عمد الاستاذ "Martin Vasil" إلى تقسيم جرائم نظم المعلومات إلى ثلاثة أنواع وتدرج تحت كل نوع مجموعة من الجرائم والأفعال غير المشروعة المرتبط بنظام الحاسب الآلي، حيث أنه أخذ في الاعتبار عند القيام بهذا التقسيم التعرف على أنماط السلوك المختلفة التي تدرج تحت مسمى الجريمة المعلوماتية وإلى أي مدى تتفق أو تختلف مع القواعد التي تحكم القانون الجنائي، ويمكننا إيجاز التقاسيم التي أوردها الفقيه "Martin Vasil" على النحو التالي:

1- الدخول والاستعمال غير المصرح بهما للنظام المعلوماتي.

ويشمل الأفعال التالية:

- "الدخول غير المصرح به إلى للنظام المعلوماتي.
- الدخول غير المصرح به للنظام المعلوماتي بنية ارتكاب جريمة معلوماتية أخرى.
- الاعتراض غير المشروع لنظام المعلوماتي
- الأفعال غير المشروعة المتصلة بالمعلومات الشخصية المعالجة آلياً.
- الاستعمال غير المصرح به للنظام المعلوماتي.

2- الاحتيال المعلوماتي وسرقة المعلومات.

ويشمل هذا النوع مجموعة من الأفعال التي تدرج تحته وهي:

- التلاعب في المعلومات المعالجة آلياً بقصد تحقيق ربح مادي غير مشروع.

1- نائلة عادل قورة، نفس المرجع السابق، ص 242، 243.

- تزوير المعلومات المعالجة آلياً بنية استخدامها في أغراض غير مشروعة.
- الحصول غير المشروع على المعلومات المعالجة آلياً.
- قرصنة البرامج المعلوماتية.

3- الجرائم التي يساعد الحاسب الآلي على ارتكابها.

ويشمل هذا النوع على مجموعة من الأفعال غير المشروعة وهي:

- التخريب أو الإتلاف سواء أنصب على المكونات المادية أو غير المادية للحاب الآلي.
- الاستعمال غير المشروع للحاسبات الآلية لإعاقة المستخدمين الشرعيين للنظام المعلوماتي عن الوصول إلى المعلومات التي يحتوى عليها.
- استخدام نظم المعلومات للاعتداء على سلامة وأمن الأفراد.
- التهديد بتدمير النظم المعلوماتية لابتزاز المجنى عليهم.
- الإقضاء غير المشروع للمعلومات المؤتمن عليها بمقتضى الوظيفة.
- صناعة وبيع المعدات والأدوات التي تساعد على ارتكاب الجريمة¹.

الفرع الثاني: تصنيف الوكالات المتخصصة الدولية لجرائم نظم المعلومات.

تُعد جرائم نظم المعلومات ذات بعد دولي بطبيعتها، مما تفرض الحاجة إلى وجود تعاون دولي فعال من أجل فهمها والتعامل معها، فقد أصبح ترابط شبكات الاتصال بين الدول في مختلف المجالات أصبح أمراً مألوفاً و واسع الانتشار، لذا أصبح التعاون الدولي أمراً حتمياً يفترض وجود فهم مشترك لهذه الظاهرة وللحلول المقترحة لها والتنسيق لمحاربتها والتقليل من أثارها المجتمعية المختلفة²، وفي هذا الإطار سنتناول بعض تصنيفات جرائم نظم المعلومات التي أقرتها الوكالات المتخصصة الدولية على النحو التالي:

1- أيمن عبدالله فكري، المرجع السابق، ص 122، 123..

2- نائلة عادل قورة، المرجع السابق، ص 246.

أولاً: تصنيف منظمة التعاون الاقتصادي والتنمية.

تُعد منظمة التعاون الاقتصادي والتنمية الأوروبية (CECD) أول منظمة دولية أهتمت بظاهرة جرائم نظم المعلومات والمخاطر التي تسببها والناجمة عنها، وقد تجلّى هذا الاهتمام مبكر من خلال التركيز على الخصوصية المعلوماتية، ما نتج عنه إصدار قواعد إرشادية وتوصيات توجيهية للدول الأعضاء لإدراجها في تشريعاتها الوطنية، وقد نصت هذه التوصيات على وجوب فرض عقوبات جنائية في حالة مخالفة تلك القواعد الإرشادية والتوصيات، وتعلقت هذه التوصيات بحماية البيانات ذات الطبيعة الشخصية وهي كالتالي:

- أ- "تحديد الغرض الذي يتم جمع البيانات من أجله.
- ب- مراعاة القواعد الشكلية الخاصة بالمحافظة على البيانات.
- ت- الانفتاح على الجميع ومعناه أن يكون كل ما يتعلق بالحياة الشخصية من سياسة عامة وتطوير وتخطيط معلنة للكافة لمعرفة.
- ث- المشاركة الفردية وضمان حق الأشخاص في الوصول والتعرف على البيانات الخاصة بهم وحقوقهم في الرد عليها أو التعديل فيها.
- ج- حدود الاستخدام ويعني ذلك أن لا تستخدم البيانات إلى في الغرض المحدد للجهة ولا يتم الخروج على ذلك إلا بموافقة الشخص.
- ح- المساءلة أو المحاسبة وهو مساءلة الشخص المنوط به التعامل مع البيانات ذات الطبيعة الشخصية عن مدى كفايتهم للقواعد والمبادئ السابقة في التعامل مع تلك البيانات"¹.

ومع تصاعد ظاهرة جرائم نظم المعلومات ازداد اهتمام منظمة التعاون الاقتصادي والتنمية بالجرائم المعلوماتية، ففي مطلع عام 1983 نظمت المنظمة سلسلة من الاجتماعات لمناقشة هذه الظاهرة المتفاقمة، وأسفرت هذه الاجتماعات إلى تشكيل فريق عمل مختص لدراسة الجريمة في الدول الأعضاء، وفي سنة 1986 أصدر الفريق تقريراً تحت مسمى "جرائم الحاسب الآلي Computer Crime" تضمن قائمة من الأفعال والتي ترتكب باستخدام الحواسيب وقد

1- أيمن عبدالله فكري، المرجع السابق، ص 125، 126.

شكلت هذه القائمة مرجعاً موحداً للدول الأعضاء تعتمد عليها عند صياغة أو تعديل نصوصها التشريعية الوطنية المتعلقة بمكافحة الجرائم المعلوماتية وتتمثل هذه الأفعال في:

أ- "إدخال أو تغيير أو محو المعلومات والمرتكبة عمدا بنية التحويل غير المشروع للأموال أو الممتلكات التي تمثلها هذه المعلومات.

ب- إدخال أو تغيير أو محو البيانات أو البرامج المعلوماتية والمرتكبة عمدا بنية التزوير والغش.

ت- إدخال أو تغيير أو مسح البيانات أو البرامج المعلوماتية أو القيام بأي فعل آخر من هذا النوع في النظام المعلوماتي عمدا بنية تعطيل الاتصال أو عمل النظام المعلوماتي.

ث- إنتهاك حقوق الملكية الفكرية أو سرقتها وذلك لبرنامج معلوماتي محمي بنية استغلاله تجارياً من أجل الحصول على عائد مادي.

ج- الدخول إلى النظام المعلوماتي عمداً وبدون تصريح من الشخص المسؤول عن النظام من خلال التعدي على تدابير الحماية بنية الضرر".

والملاحظ في هذا التصنيف أنه لم يستند إلى معيار واضح حيث تم اختزاله في نوعين من الجرائم وهي (الأفعال المرتكبة ضد البيانات والأنظمة المعلوماتية، وسرقة حقوق الملكية الفكرية)¹.

ثانياً: تصنيف المجلس الأوروبي لجرائم نظم المعلومات.

برز اهتمام المجلس الأوروبي بالمعلوماتية في مطلع السبعينات بالتزامن مع جهود منظمة التعاون الاقتصادية والتنمية، وركز في البداية اهتمامه على حماية البيانات الشخصية وحماية حقوق الأفراد في الخصوصية، وكان ذروة هذا الاهتمام في عام 1981 حيث تم توقيع الاتفاقية الخاصة بحماية الأفراد من إساءة استخدام البيانات المعالجة إلكترونياً (المعروفة باسم الاتفاقية رقم 108)، وتضمنت الاتفاقية عدد من المبادئ الأساسية التي تعتبر الحد الأدنى من

1- مفيدة مباركية، جرائم المعلوماتية في الفقه الإسلامي والتشريع الجنائي-دراسة تأصيلية مقارنة-، أطروحة لنيل شهادة الدكتوراه علوم في العلوم الإسلامية، كلية الشريعة والاقتصاد، جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة دولة الجزائر، السنة الجامعية 2021/2022، ص 25.

الضمانات والاحتياطات التي يجب أن تتضمنها تشريعات الدول الأطراف بهدف حماية الافراد من إساءة استخدام البيانات الشخصية المعالجة إلكترونياً، وتمثلت هذه المبادئ في:

- ضرورة الحصول على البيانات الشخصية من مصادر مشروعة.
- أن تكون البيانات صحيحة متفقة مع الغرض الذي جمعت من أجله.
- أن تراعي القواعد الشكلية اللازم اتباعها للحيلولة دون إساءة استخدام البيانات الشخصية¹.

والحقيقة أن هذه المبادئ لم تختلف عن سابقتها الصادرة عن منظمة التعاون الاقتصادي والتنمية لعام 1980 والمعلن عنها في شكل توصيات، وما الاختلاف إلا في عنصر الإلزام الذي تتميز به اتفاقية المجلس الأوروبي باعتبارها اتفاقية قانونية ملزمة للدول الأطراف².

وفيما يتعلق بالجريمة المعلوماتية على وجه الخصوص، ظهر الاهتمام بها لأول مرة في عام 1976 خلال الاجتماع الثاني عشر لمجلس أوروبا لرؤساء معهد العلوم الجنائية، والذي تطرق إليها بوصفها بأنها نتاج ثورة تكنولوجية واسعة النطاق، وأدى الاجتماع إلى تشكيل لجنة لدراسة الجرائم الاقتصادية بشكل عام، وبدورها عملت اللجنة إلى نشر التوصية رقم 12/81، والتي وافقت عليها لجنة الوزراء للمجلس الأوروبي في 25 يونيو 1981، ويقدم الاقتراح تعريفا عاما للجريمة الاقتصادية، بما في ذلك بعض جرائم الحاسب الآلي مثل سرقة المعلومات والتجسس المعلوماتي وجرائم التلاعب بالبيانات المعالجة إلكترونياً، وخلصت اللجنة في تقريرها إلى أن هذه الأفعال لا يمكن أن تشكل جريمة ما لم تتحقق الشروط التالية :

- أ- تسبب السلوك في ضرر جسيم، أو الخوف من حدوث مثل هذا الضرر.
- ب- أن يكون لدى الفاعل معرفة وفهم خاص بتكنولوجيا الحاسب الآلي.
- ت- وجود صلة وظيفية بين الجاني والفعل الإجرامي، أي المعالجة الإلكترونية للبيانات³.

1- نائلة عادل قورة، المرجع السابق، ص 250 و 251.

2- تم التوقيع على هذه الاتفاقية بتاريخ 28 فبراير 1981 من قبل الدول الاطراف فيها وهم (بلجيكا، الدنمارك، النمسا، فرنسا، ألمانيا الغربية سابقا، إيطاليا، اليونان، أيسلندا، النرويج، لوكسمبورج، إسبانيا البرتغال، السويد، المملكة المتحدة، تركيا)، ودخلت حيز النفاذ في 01 أكتوبر 1985.

3- أيمن عبدالله فكري، المرجع السابق، ص 127 و 128.

وبالنظر في الشروط السابقة وتعليقا عليها وعلى الحجج القائلة بوجوب استيفاء هذه الشروط من أجل تحقيق عدم شرعية الفعل، فإنه فيما يتعلق :

- بالشرط الأول فإن القول بأن الفعل يجب أن يسبب ضرراً جسيماً أو أن هناك خوفاً من التسبب في مثل هذا الضرر فإنه يتعارض مع الاتجاه الذي يجرم الوصول إلى نظام الحاسب الآلي ويعتبره بحد ذاته جريمة، سواء كان الوصول لغرض ارتكاب جريمة لاحقة أو إذا كان مجرد الوصول إلى المعلومات الواردة في هذا النظام وبغض النظر إذا كان الضرر قد حدث أو لا، وهذا بهدف حماية سرية المعلومات المعالجة إلكترونياً.
- أما الشرط الثاني فهو لا يخبرنا بمستوى معرفة تقنية المعلومات التي يجب أن يمتلكها الجاني، كما أنه يتعارض مع الواقع العملي، لأن مرتكبي جرائم المعلومات لا يمتلكون أحياناً هذا المستوى من المعرفة الحاسوبية، وهذا ويعد تضيقاً لا مبرر له للجريمة المعلوماتية.
- أما الشرط الثالث فالقول بضرورة وجود صلة وظيفية بين الفاعل والمعلومات محل الفعل الاجرامي سيجعل نطاق التجريم منحصرًا في حالات دون الأخرى، في حين انه في كثير من الحالات لا تربط بين الفاعل وهذه المعلومات صلة وظيفية، ومن الممكن أن يكون هذا الشرط صالحاً لظروف التشديد وليس شرطاً للتجريم¹.

أثيرت قضية الجرائم المعلوماتية مرة أخرى عندما أدرجتها اللجنة الأوروبية لمشاكل الجريمة في خطة عملها للفترة 1985-1986، حيث تشكلت لجنة من الخبراء لدراسة الموضوع أنهت عملها في مارس 1989 وقدمت تقريراً للجنة الأوروبية لمشاكل الجريمة في يونيو 1989 ولمجلس وزراء أوروبا في سبتمبر 1989 والذي تبناه في شكل التوصية رقم 09/89، حيث تضمنت بعض المبادئ التوجيهية للمشرعين الوطنيين، بهدف الوصول إلى سياسة تشريعية جنائية موحدة بشأن جرائم الحاسب الآلي، وقد ميزت الهيئة في تقريرها بين نوعين رئيسيين لجرائم الحاسوب، الأول تحت عنوان القائمة الأساسية والثاني تحت عنوان القائمة الاختيارية.

والفرق بين الفئتين هو إجماع اللجنة على خطورة أشكال معينة من جرائم المعلومات ومدى احتياجها للتدخل التشريعي، حيث اشتملت الفئة الأولى (الطائفة الأساسية) ثمانية جرائم أتفق

1- نائلة عادل قورة، المرجع السابق، ص 250 و 251.

على خطورتها وانتشارها، وهذه القائمة هي بمثابة تطور لتقسيم منظمة التعاون الاقتصادي والتنمية سالف الذكر، وهي:

- "الاحتيايل المعلوماتي.
- التزوير.
- إتلاف المعلومات والبيانات أو إتلاف برامج الحاسب الآلي.
- إعاقة نظام الحاسب الآلي عن أداء وظيفته.
- الدخول غير المصرح به إلى نظام الحاسب الآلي.
- الاعتراض غير المصرح به لنظام الحاسب الآلي.
- النسخ غير المشروع لبرامج الحاسب الآلي.
- النسخ غير المشروع للتصميمات الخاصة برقائ الحاسبات الآلية".

أما السلوك الذي يندرج في الفئة الثانية (الطائفة الاختيارية)، فيتميز بكونه لم يبدأ بالظهور إلا مؤخرًا، مع التنبيه إلى أن معدله سيرتفع في المستقبل، وعلى الرغم من ذلك، فإن تجريم هذه الأفعال لم يتوافق مع نفس توافق الطائفة الأولى، بل أن البعض رأي أن إدراج هذه الأفعال من شأنه توسيع دائرة جرائم الحاسب الآلي، ما حذا باللجنة لوضع هذه الأفعال ضمن الطائفة الاختيارية وتركت تقدير الحاجة في تجريمها إلى كل دولة على حده، وهذه الأفعال هي:

- "التعديل في البيانات المخزنة بالحاسب الآلي أو برامجه وذلك في الحالات التي لا يؤدي فيها التعديل إلى إتلاف لهذه البيانات والبرامج.
- التجسس المعلوماتي.
- الاستعمال غير المصرح به لنظام الحاسب الآلي.
- الاستعمال غير المصرح به لبرامج الحاسب الآلي التي تشملها الحماية القانونية"¹.

1- نائلة عادل قورة، نفس المرجع السابق، ص252 إلى 254.

ثالثاً: تقسيم منظمة الإنتربول الدولي لجرائم نظم المعلومات.

صنفت منظمة الإنتربول الدولي جرائم نظم المعلومات إلى طائفتين أساسيتين وهما الجرائم ذات التقنية العالية و الجرائم التي تساعد المعلوماتية في ارتكابها وتعزيزها.

1- الجرائم عالية التقنية.

جرائم التكنولوجيا العالية يُشار إلى هذه الفئة بالجرائم المتقدمة أو جرائم التكنولوجيا العالية لأنها تُرتكب ضد الكيانات المادية والبرمجية لأنظمة المعلومات بهدف المساس بسلامة أو موثوقية أو توافر البيانات وأنظمة المعلومات، وقد أحصت الأمانة العاملة للإنتربول أكثر من ثلاثين نوع من هذه الجرائم التي تستهدف البيانات والأنظمة المعلوماتية، حيث يمكن تقسيمها في 06 فئات¹:

- أ- الوصول والاعتراض غير المصرح به، وأهمها القرصنة، والاعتراض غير القانوني للبيانات، والاستعمال الخاص لوقت الحاسب الآلي، وما إلى ذلك.
- ب- تعديل البرمجيات أو البيانات وأهمها القنابل المنطقية وحضان طروادة والفيروسات.
- ت- الاحتيال في المعلومات وأحد أهم أشكال الاحتيال في المعلومات الغش المرتبط بالموزعات الآلية، والغش المعلوماتي المتعلق بالألعاب وقرصنة الهاتف.
- ث- النسخ غير القانوني ومن أهمها النسخ غير القانوني لطبوغرافيا أشباه الموصلات. والبرمجيات وألعاب الحاسوب.
- ج- تخريب المعلومات ويشمل التخريب المعلوماتي المادي والبرمجي.
- ح- جرائم أخرى².

2- الجرائم المدعومة بالمعلوماتية:

في هذا النوع من الجرائم، تعمل المعلوماتية كوسيلة وأداة لتسهيل الجريمة، هذه الجريمة والتي غالباً ما تعرف بالجريمة التقليدية، ولكن بسبب ارتباطها الوثيق بتقنية المعلومات تصنف

1- للمزيد أنظر في الموقع الإلكتروني الرسمي للإنتربول الدولي <https://www.interpol.int/ar/4/6>، أطلع

عليه بتاريخ 2022/9/15.

2- مفيدة مباركية، المرجع السابق، ص 28.

على أنها جرائم معلوماتية، مثل استغلال الأطفال، والجرائم المالية عبر الإنترنت، و جرائم الإرهاب.

بالإضافة إلى الابتزاز والاتجار بالمخدرات والفساد المصاحب وغسل الأموال والجرائم المتعلقة بتدفق المعلومات (مثل انتهاك حقوق النشر)، وانتهاك حرمة الحياة الخاصة وجرائم الصحافة والتشهير ونشر معلومات متطرفة ومواد إباحية، كما يمكن أن تضاف الجرائم المتعلقة باحترام الحريات والحقوق الفردية الأساسية، مثل المعاملات غير القانونية لقواعد البيانات ذات الطابع الشخصي والاستغلال الجنسي للقصر¹.

رابعاً: تقسيم اتفاقية بودابست لجرائم نظم المعلومات.

تعتبر اتفاقية بودابست² أول اتفاقية دولية لمكافحة جرائم نظم المعلومات، وهي نتاج لتعاون وعمل لجان قانونية وفنية من الدول الأعضاء رغم الاختلاف في نظمها القانونية، إلا أنه

1- مفيدة مباركية، نفس المرجع السابق، ص 28.

2- بناء على توصية اللجنة الأوروبية المتخصصة بمشاكل الإجرام CDPC، أقامت لجنة الوزراء هيئة جديدة تُعرف بـ «لجنة الخبراء المعنية بالجريمة في الفضاء الإلكتروني» وذلك استناداً إلى القرار رقم (97/583) المؤرخ في 4 نوفمبر 1997، بدأت هذه اللجنة - المعروفة اختصاراً بالرمز الإنجليزي - (PC-CY) نشاطها في أبريل 1997، وأخرطت في مناقشات حول مسودة معاهدة دولية حول الجريمة الإلكترونية، على أن تنتهي من مهامها بحلول 31 ديسمبر 1999، ونظراً لعدم قدرتها على استكمال المناقشات بشأن بعض النقاط الرئيسية في المشروع خلال تلك الفترة، فقد مدد نواب الوزراء ولايتها إلى غاية 31 ديسمبر 2000 بموجب القرار رقم 697/99، حيث أبدى وزراء العدل الأوروبيون دعمهم الصريح لعملية التفاوض في مناسبتين، الأولى بموجب القرار رقم (1) الذي تم اعتماده أثناء مؤتمرهم الحادي والعشرين (يونيو 1997)، حيث حثوا لجنة الوزراء على تعزيز الجهود الذي اضطلعت به اللجنة الأوروبية المعنية بمشاكل الإجرام في مجال الجريمة الإلكترونية، بهدف تقريب التشريعات الجنائية الوطنية من بعضها البعض، وتمكين الدول من استخدام وسائل تحقيق فعالة في لمواجهة هذه الانتهاكات.

كما شجّع المؤتمر الأطراف المتفاوضة على مواصلة مساعيها لإيجاد حلول مناسبة ومتوازنة تتيح لأكثر عدد ممكن من الدول الانضمام إلى المعاهدة، مع الاعتراف بالحاجة الملحة إلى نظام سريع وفعال للتعاون الدولي يراعي المتطلبات الخاصة لمكافحة الجريمة الإلكترونية، وخلال الفترة من 1997 حتى ديسمبر 2000، عقدت اللجنة 10 اجتماعات في جلسات عامة، و15 اجتماعاً لفريق الصياغة الذي كان مفتوحاً للعضوية.

وبعد انقضاء المدة الممددة، عُقدت ثلاث اجتماعات تحت رعاية اللجنة الأوروبية المعنية بمشاكل الإجرام، بهدف إكمال وضع اللامسات النهائية على مشروع المذكرة التوضيحية، ومراجعة مسودة الاتفاقية، بناء على توصيات الجمعية البرلمانية التي طلبت منها لجنة الوزراء في أكتوبر 2000 تقديم رأيها بشأن المسودة، وهو

وبالنظر إلى خطورة الموضوع وجسامة المخاطر المترتبة عليه في حالة عدم التكاتف في مواجهته تغاضت الدول عن ذلك الاختلاف، وذلك حتي تتمكن من تنظيم العمل والاستفادة من مجتمع المعلومات وثورة الاتصالات، فهذه الاتفاقية اسهمت في تقنين العديد من المجهودات الدولية التي بذلت في هذا المجال وهي المعاهدة الأوروبية بشأن حماية البيانات الشخصية، وكذلك استندت إلي الميثاق الدولي لحماية الحقوق المدنية والسياسية الصادر عن الامم المتحدة 1966، كما تأثرت بمعاهدة التعاون الدولي في مكافحة الجريمة المعلوماتية الصادر عن الأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية ودول الاتحاد الاوروبي ومجموعة وكذلك التوصيات الاوروبية رقم 10/85، والتوصية 20/88، والتوصية 9/89، والتوصية 13/95، وبالرغم من أن اتفاقية بودابست أوروبية المنشأ إلا أنها دولية النزعة، وذلك لأنها مفتوحة لإنضمام الدول الأخرى حتى يمكن أن تساهم في ضبط وتنظيم مجتمع المعلومات والاتصالات بشكل أفضل تعم فائدته على الجميع¹.

و أوردت اتفاقية بودابست أربع طوائف لجرائم نظم المعلومات، تضم كل طائفة مجموعة من الجرائم وهي كالتالي²:

- **الطائفة الأولى:** الجرائم التي تستهدف سلامة ومصادقية وموفرة البيانات والانظمة المعلوماتية وتشمل (الولوج غير المصرح به، الاعتراض غير المصرح به، الإضرار بسلامة البيانات، الإضرار بسلامة النظام، إساءة استخدام المعدات المعلوماتية "التجهيزات والبرمجيات).
- **الطائفة الثانية:** الجرائم المتصلة بالحاسوب وتشمل (التزوير المعلوماتي، الغش المعلوماتي).

الرأي الذي تم اعتمده في الجزء الثاني من دورتها العامة في أبريل 2001، و تم تقديم النسخة المعدلة والمكتملة من مسودة الاتفاقية المنقحة والنهائية، مع مذكرتها التفسيرية، للموافقة عليها إلى اللجنة الأوروبية المعنية بمشاكل الإجرام في دورتها العامة الخمسين المنعقدة في يونيو 2001، وبعد ذلك، عُرض نص مسودة الاتفاقية على لجنة الوزراء لاعتماده وفتح باب التوقيع عليها، للمميز أنظر التقرير التفسيري لاتفاقية الجريمة الالكترونية بودابست المعتمدة من لجنة وزراء مجلس اوروبا في الدورة التاسعة بعد المائة بتاريخ 8 نوفمبر 2001 والمفتوحة للتوقيع عليها في بودابست بتاريخ 23 نوفمبر 2001، ص 04.

1- أيمن عبدالله فكري، المرجع السابق، ص 129 و 130.

2- التقرير التفسيري لاتفاقية بودابست حول الجريمة الالكترونية، المرجع السابق، ص 05.

- **الطائفة الثالثة:** الجرائم المتصلة بالمحتوى وتتمثل في المخالفات المتعلقة بالاستغلال الجنسي للأطفال والأفعال الإباحية والأخلاقية.
- **الطائفة الرابعة:** الجرائم المرتبطة بالتعدي على الملكية الفكرية والحقوق المجاورة وحقوق المؤلف وقرصنة البرمجيات¹.

وما يمكن ملاحظة في تقسيم اتفاقية بودابست أنه لا يقوم على معيار صريح يمكننا من خلاله تمييز الجرائم فمثلا الطوائف الأولى والثالثة والرابعة هي جرائم تتعلق بموضوع الحماية القانونية، في حين أن الطائفة الثانية تشير إلى الوسيلة، كما والملاحظ أن الطائفة الأولى هي عبارة عن جرائم مستحدثة، في حين أن بقية الجرائم هي عبارة عن جرائم معروفة من حيث الجوهر، فكل من سرقة حقوق الملكية الفكرية والاستغلال الجنسي للأطفال والتزوير والغش هي معروفة سابقا في مختلف التشريعات العقابية منذ زمن، إلا أن الشيء المستحدث فيها هو وجود عنصر المعلوماتية في الركن المادي لكل جريمة منها².

وبالرجوع إلى التصنيفات السالفة الذكر يمكننا أن نفهم أنه من الصعب الاتفاق على معيار التصنيف لجرائم نظم المعلومات، بسبب طبيعتها المعقدة، وارتباطها بمجالات مختلفة، والأغراض المختلفة لمن يرتكبها، والأهم من ذلك التداخل والعلاقة بينها، فغالبا ما تكون جرائم القرصنة (الجرائم المتقدمة بمعنى الإنترنت) هي نتيجة ارتكاب إحدى الجرائم التقليدية.

بالإضافة إلى ذلك، ساهمت الاستخدامات العديدة للمعلوماتية في خلق جرائم جديدة لدرجة أننا نجد لها أشكال مماثلة في التشريعات العقابية التقليدية، مثل تزوير المستندات الإلكترونية، وانتهاك حقوق النشر المرتبطة بالبرامج الإلكترونية، و انتهاك حرمة الحياة الخاصة عبر خدمات التواصل الإلكترونية و إلى ذلك.

1- للمزيد أنظر الملحق رقم 02 المتعلق بشرح الأفعال التي تشكل جرائم تدخل في نطاق الجرائم المعلوماتية، والصادر عن مكتب الأمم المتحدة المعني بالمخدرات والجريمة، بعنوان دراسة شاملة عن الجريمة السيبرانية فبراير 2013.

2- مفيدة مباركية، المرجع السابق، ص 27.

لذلك يمكننا الاعتقاد أن التصنيف الأنسب هو مواءمة التصنيف الذي اقترحه المجلس الأوروبي والتصنيف الذي اقترحه الإنتربول، والذي يتم تحقيقه من خلال إعادة تخصيص بعض الجرائم الواردة في اتفاقية بودابست وفقاً للتصنيف الدولي لمنظمات الإنتربول، فيكون الناتج مجموعتين لأبرز جرائم المعلوماتية، **أولهما** مجموعة الجرائم الماسة بسرية وسلامة وإتاحة البيانات و الأنظمة المعلوماتية وهي (الجرائم المتقدمة أو عالية التقنية، بحسب الإنتربول)، **والثانية** الجرائم المرتكبة عبر البيانات والأنظمة المعلوماتية (الجرائم المدعومة بالمعلومات بحسب الإنتربول)، وبذلك تشمل **المجموعة الاولى** بحسب اتفاقية بودابست الجرائم كلا من (الدخول غير المشروع، الاعتراض غير المشروع، اتلاف البيانات، الإعاقة الخطيرة للنظام المعلوماتي، إساءة الاستخدام)، فيما تشمل **المجموعة الثانية** الجرائم الواردة في اتفاقية بودابست كلا من (التزوير المعلوماتي، الغش المعلوماتي، الاستغلال الجنسي للأطفال، التعدي على حقوق الملكية الفكرية)، وهذا التصنيف الذي سنعتمد عليه في دراستنا لجرائم نظم المعلومات.

المبحث الثاني: جرائم نظم المعلومات والجريمة المنظمة.

تجربنا دراسة جرائم نظم المعلومات على توضيح العلاقة بين هذه الجرائم والجريمة المنظمة التي جعلت منها موطناً وانتشرت في الفضاء الافتراضي، أين استغلت شبكة الانترنت العالمية والاتصالات العالمية في ارتكاب الجرائم المنظمة، هذا لأن الخصائص المميزة لجرائم نظم المعلومات تجعل من الفضاء الإلكتروني مسرحاً واسعاً ومريحاً للجريمة المنظمة، وعليه فقد قمنا بتقسيم هذا المبحث إلى مطلبين نتناول في المطلب الأول مفهوم الجريمة المنظمة موضحين تعريفها وخصائصها، أما المطلب الثاني فقد خصصناه لدراسة الجريمة المنظمة المستحدثة.

المطلب الاول: مفهوم الجريمة المنظمة:

بفضل شبكات الاتصال الدقيقة والمتطورة، تنقل كمية كبيرة جداً من المعلومات من مناطق تفصل بينها آلاف الكيلومترات باستخدام تقنيات لا تضمن لها الأمن الكامل، فقد يكون من الممكن التلاعب بهذه بالمعلومات العابرة للحدود، مما قد يتسبب في أضرار لبعض البلدان أو الأفراد أو الشركات بأضرار كبيرة، هذا لأن قدرة تقنيات المعلومات على تقصير المسافات وتحسين الاتصال بين أجزاء مختلفة من العالم، انعكست أيضاً في طبيعة الأعمال الإجرامية

التي يعتمد فيها المجرمون استخدام هذه التقنيات في انتهاكهم للقانون، وقد أدت هذه القدرة إلى أن مواقع متعددة في دول مختلفة يمكن أن تتأثر بجريمة واحدة وهي من جرائم الاعتداء على نظام المعلومات في نفس الوقت، لأن الجريمة يمكن أن يرتكبها أحد الجناة في بلد ما ضد ضحية في بلد آخر في وقت قصير جداً ، بحيث تؤدي إلى أضرار كبيرة و خطيرة جداً¹.

وحيث أن الشبكة العالمية للإنترنت ونظم المعلومات تسمح للمجرمين بالوصول إلى الضحايا والعملاء في أي مكان في العالم من خلال اتصال بالإنترنت، فيستفيد هؤلاء المجرمون من السهولة التي تتدفق بها المعلومات والاتصالات والأموال عبر الفضاء الإلكتروني، وبهذا يستخدمون الإنترنت لتبادل المعرفة والتواصل فيما بينهم دون أن يتم اكتشافهم، وبيع البيانات والسلع والخدمات التي استولوا عليها، إضافة إلى ذلك غسل الأموال المكتسبة بطريقة غير مشروعة، فضلاً عن تبادل الخبرات وتكتيكات الجريمة المنظمة المستحدثة والأدوات المستخدمة لارتكابها، وقد يعمل هؤلاء المجرمون بمفردهم أو في جماعات إجرامية منظمة².

تشير فكرة الجريمة المنظمة إلى الظاهرة الإجرامية التي ترتكبها جماعة إجرامية منظمة، وقد سميت هذه الجريمة بعبارات مختلفة بالإضافة إلى التعبير عن الجريمة المنظمة بتعبيرات عدة مثل المافيا والكارتل ومجموعة الأشرار، التي ترمز كلها إلى شيء غير قانوني فهذه المنظمات لها سلطة مركزية وتسلسل هرمي في وظائفها، حيث يخضع أعضاؤها لقواعد ملزمة ولديها هيئات تنفيذية تتميز بالولاء والطاعة لأوامر رؤسائها، والخطر هو حقيقة أن هذه المنظمات المنظمة يمكن لها أن تنفذ مهامها على الرغم من المؤسسات التي يقوم عليها حكم القانون³، ولإبراز ما سبق ذكره من تقنيات وعناصر للجريمة المنظمة كان لا بد من تقسيم هذا المطلب إلى فرعين نتناول في الفرع الأول تعريف الجريمة المنظمة، أما الفرع الثاني فنتناول فيه خصائص الجريمة المنظمة.

1- رشيدة بوبكر، المرجع السابق، ص 99 100.

2- راجع مكتب الأمم المتحدة المعني بالمخدرات والجريمة، عبر الموقع الإلكتروني ، تاريخ الاطلاع 2022/12/10 <https://www.unodc.org/e4j/en/index.html>.

3- محمد كريم علي، مكافحة الجريمة المنظمة في ظل المعاهدات الدولية، مركز الدراسات العربية للنشر والتوزيع، جمهورية مصر العربية، الطبعة الاولى 2020، ص 35.

الفرع الأول: تعريف الجريمة المنظمة.

ما يمكن ملاحظته أنه بما تشكله الجريمة المنظمة من الخطر الشديد على البلدان، لكونها دولية بطبيعتها، فهي غالباً ما تتجاوز حدود دولة إلى دولة أخرى، وترتبط بالاقتصاد والتجارة الدولية وسياسة الدولة، وتتخذ أشكالاً عديدة يتجاوز تأثيرها إقليم دولة مثل أخذ الرهائن والطائرات والقرصنة والإرهاب وغسيل الأموال وغيرها، ومع ما تمثله هذه الجريمة من خطر جسيم يهدد جميع المنظمات والمؤسسات الدولية والوطنية على جميع المستويات الدولية والإقليمية، إلا أنها لم تكن محلاً للاتفاق على تعريفها وتحديد مدلولها من قبل التشريع والفقهاء¹.

أولاً: التعريفات الدولية الجريمة المنظمة.

لعل أوضح تمييز بين الجريمة المنظمة والأشكال الأخرى للسلوك الإجرامي هو أنها منظمة بشكل عام، فلا تشمل الأعمال الإجرامية الفردية العشوائية وغير المخطط لها بدلاً من ذلك فإنها تركز حصرياً على الأعمال العقلانية المخطط لها التي تعكس جهود مجموعات الأفراد، حيث بُذلت جهود عديدة لاستنباط عناصر مشتركة لوصف الجريمة المنظمة وتعريفها بمزيد من التحديد، وعليه فإن قائمة الجرائم التي ترتكبها الجماعات الإجرامية المنظمة سوف تصبح غير موجودة أو قديمة بمعنى عفا عليها الزمن لأن التغيرات الاجتماعية والسياسية والتكنولوجية تؤدي إلى تغير فرص الجريمة في مواقع مختلفة، لذلك فإن وحدة التحليل في معظم التعاريف ليس الجرم بل الجاني، "جماعة إجرامية منظمة"، وهذا سيساعد في الفهم الأفضل لطبيعة هذه المجموعات وفي تطوير استجابات أكثر فاعلية لها².

1- سمر بشير خيرى، الجريمة المنظمة العابرة للحدود "الاتجار بالنساء والطفل نموذجاً"، منشورات الحلبي الحقوقية، بيروت لبنان، الطبعة الأولى 2017، ص 46، أنظر كذلك محمد كريم علي، المرجع السابق، ص 35.

2- راجع مكتب الأمم المتحدة المعني بالمخدرات والجريمة، عبر الموقع الإلكتروني، نفس المرجع السابق، <https://www.unodc.org/e4j/en/index.html>..

1- تعريف الجريمة المنظمة في اللغة.

كلمة جريمة تشير إلى الجريمة أو الجرم، أي الخطيئة والذنب، أما المنظمة فهي مشتقة من المنظم، والمنظم مستنبط من "منظم الحركة"، وعليه ، يمكن القول إن التعريف اللغوي يلقي الضوء بدقة على الخصائص التنظيمية التي تتمتع بها المنظمات الإجرامية، والتي تنتج عن رغبة الجماعات الإجرامية في تعظيم الاستفادة المرجوة من الأعمال الإجرامية باتباع وسائل التنظيم الإداري في التخطيط للعمل الإجرامي¹.

2- تعريف الجريمة المنظمة في الاصطلاح:

استُخدم مصطلح الجريمة المنظمة في الآونة الأخيرة، بعد التطور الذي عرفته الظاهرة الإجرامية، كبديل لكلمة "مافيا"، التي استُخدمت للإشارة إلى جماعة إجرامية متمركزة في بلد ما، إلا أن يوجد من يعتبر أن مصطلح الجريمة المنظمة مفهوم غير واضح حتى يحظى باتفاق دولي حوله، وهذا راجع لاختلاف نظرة المشرع في كل دولة حيث يصوره حسب واقعه السياسي والاقتصادي والاجتماعي، بينما يرى الآخرون فيه دلالة شعبية وليس دلالة قانونية، وبالرغم من قدم المصطلح إلا أنه ما زال يثير خلاف ويحيطه الغموض، حيث أصبح من الضروري الرجوع إلى التشريع الوطني لتحديد تعريفه خاصة بعد توسيع نطاقه وخروجه إلى مجال عبر وطني.

وعليه يمكن تعرف الجريمة المنظمة بأنها "عبارة عن بناء منظم يجمع مجموعة من الأشخاص، يؤدون نشاطهم بأسلوب منظم وبشكل مستمر، ويعملون في أنشطة إجرامية وغير مشروعة، بهدف تحقيق أكبر قدر ممكن من العوائد المالية والمادية"².

3- تعريف الاتحاد الأوروبي للجريمة المنظمة.

جاء تعريف الاتحاد الأوروبي للجريمة المنظمة عبر مجموعة مكافحة المخدرات والجريمة المنظمة بالاتحاد الأوروبي في سنة 1993 حيث عرفتها بأنها "جماعة مشكلة من أكثر من شخصين، تمارس مشروعاً إجرامياً ينطوي على ارتكاب جرائم جسيمة لمدة طويلة أو غير

1- محمد كريم علي، المرجع السابق، ص 41 42.

2- محمد كريم علي، نفس المرجع السابق، ص 43 44.

محددة، ويكون لكل عضو مهمة محددة في إطار التنظيم الإجرامي، وذلك بهدف الحصول على السطوة أو تحقيق الأرباح".

وحددت المجموعة السابق ذكرها مجموعة من المعايير أو الصفات التي تتميز بها الجريمة المنظمة وهي كالتالي:

1. التعاون بين أكثر من شخصين.
 2. تحديد المهام المسندة إلى كل من هؤلاء الأشخاص.
 3. استمرارية عمل الجماعة الاجرامية لمدة طويلة او غير محددة.
 4. أن تتضمن المجموعة شكلا من أشكال النظام والرقابة الداخلية.
 5. ان ترتكب جرائم جسيمة.
 6. أن تمارس نشاطاتها الإجرامية على المستوى الدولي.
 7. أن تستخدم وسائل التخويف والعنف.
 8. أن تستعمل التنظيمات التجارية أو ما يماثل ما هو متبع في قطاع الأعمال.
 9. أن تقوم بغسيل الأموال غير المشروعة.
 10. أن تمارس النفوذ على الأوساط السياسية، وعلى وسائل الإعلام والإدارة العامة والقضاء والاقتصاد.
 11. أن تهدف إلى تحقيق الربح الفاحش.
- وشددت مجموعة مكافحة المخدرات والجريمة المنظمة على ضرورة توافر ستة خصائص من الخصائص سابقة الذكر لا سيما النقاط 1-2-3-4-5-11 حتى توصف الجريمة بأنها جريمة منظمة¹.

4- تعريف الانتربول الدولي للجريمة المنظمة.

عرفت منظمة الانتربول الجريمة المنظمة في الندوة الدولية الأولى التي حضرها ممثلي 46 دولة والتي عقدت حول الإجرام المنظم بفرنسا في مايو 1988، وعرفت الجريمة المنظمة

1- محمود مدين، الانتربول الدولي وتسليم المجرمين، المصرية للنشر والتوزيع، جمهورية مصر العربية، الطبعة الثانية 2019، ص 37 38.

بأنها " أي جماعة تقوم بحكم تشكيلها بارتكاب أفعال غير مشروعة بصفة مستمرة وتهدف أساساً إلى تحقيق الربح دون التقيد بالحدود الوطنية"¹.

وكان هذا التعريف محلاً لنقد العديد من الدول، حيث ركز على بعض خصائص الجريمة المنظمة، وبصفة خاصة سعيها إلى تحقيق الربح، واستمرارية التشكيل، وممارسة النشاط عبر الحدود الوطنية، وتجاهل البعض الآخر منها، كالبناء التنظيمي المتدرج للجماعات الإجرامية واستخدام العنف، ولذلك أعادت وحدة الجريمة المنظمة للإنتربول تعريف الجريمة المنظمة بأنها، "جماعة من الأشخاص تتمتع بهيكل تنظيمي وتهدف إلى تحقيق الربح عن طريق ارتكاب أنشطة غير مشروعة، مستخدمة التخويف والرشوة"²، و الظاهر من النص أن التعريف الجديد أضاف إلى عناصر الجريمة المنظمة عنصري البناء أو الهيكل التنظيمي واستخدام العنف والرشوة أو الفساد كوسيلة غالبية للجماعات الإجرامية المنظمة، ولكنه تجاهل القواعد الداخلية التي تحكم أعضاء التنظيم الإجرامي والتي تهدف إلى ضمان ولاءهم وطاعتهم لأوامر رؤسائهم³.

5- تعريف الأمم المتحدة للجريمة المنظمة.

أدركت الأمم المتحدة أنه لا يوجد بلد واحد مهما كانت قوته يستطيع أن يحارب الجريمة المنظمة عبر الحدود وحدة بمعزل عن باقي الدول الأخرى، حيث أعطت الأمم المتحدة أولوية كبرى لمكافحة هذه الجريمة، ويظهر هذا على وجه الخصوص من عدد المؤتمرات الدولية حول من الجريمة ومعاملة المجرمين.

حيث جاء أول تعريف في المؤتمر الدولي الخامس لمكافحة الجريمة ومعاملة المذنبين الذي عقدته الأمم المتحدة في مدينة جنيف سنة 1975، وعرف الجريمة المنظمة بأنها " الجريمة التي تتضمن نشاطاً إجرامياً معقداً، يرتكب على نطاق واسع، وتتفذه مجموعات من

1- محمد حسن خمو المزوري، دور المنظمات الدولية في مكافحة الجريمة المنظمة عبر الوطنية، دار الكتب القانونية و دار شتات للنش والبرمجيات، طبعة 2017، ص 21.

2- محمد كريم علي، المرجع السابق، ص 59.

3- علاء زكي، الجماعات الإجرامية المنظمة في القانون الجنائي الدولي، دار الفكر والقانون، جمهورية مصر العربية، الطبعة الأولى 2018، ص 143.

الأشخاص على درجة كبيرة من التنظيم، بهدف تحقيق ثراء للمشاركين في هذا النشاط على حساب المجتمع وأفراده، وهي في الغالب ما ترتكب بأفعال مخالفة للقانون، منها جرائم ضد الأشخاص أو الأموال، وترتبط في معطاة الأحيان بالفساد السياسي"، وقد انتقد هذا التعريف لأنه لم يشير إلى المنظمة الإجرامية بشكل مباشر وإنما ركز على السلوك الإجرامي دون بيان العناصر الأساسية لقيام المنظمة الإجرامية، ومنها الاستمرارية في ممارسة النشاط الإجرامي والتخطيط لارتكاب الجريمة وأستخدم وسائل العنف¹.

أما في المؤتمر الثامن لمنع الجريمة ومعاملة المجرمين، الذي انعقد في هافانا "كوبا" في أغسطس عام 1990، فإنه جاء في تقرير الأمن العام للأمم المتحدة تحت عنوان " الجريمة المنظمة" أنه درجت العادة على استخدام مصطلح الجريمة المنظمة للإشارة إلى الأنشطة الإجرامية الواسعة النطاق المعقدة، التي تضطلع بها جمعيات ذات تنظيم قد يكون محكما وقد يكون لا يكون، وتهدف إلى إقامة تمويل أو استغلال أسواق غير مشروعة على حساب المجتمع حيث تتجاوز هذه الأنشطة الحدود الوطنية للدولة إلى دولة أخرى².

وما يلاحظ أن جهود الأمم المتحدة كانت دائماً تتواجه مع مشكلة تعريف الجريمة المنظمة حتى على مستوى المؤتمر العاشر المنعقد في أبريل لعام 2000 بفيينا، مع العلم أن اتفاقية فيينا المتعلقة بمكافحة الإتجار غير المشروع في المخدرات والمؤثرات العقلية تعبر بوضوح عن اهتمام الأمم المتحدة بمحاربة الجريمة المنظمة، خاصة وأن جرائم الإتجار الدولي في المخدرات تعد من أبرز صور الجريمة المنظمة العابرة للحدود الوطنية³.

تلى ذلك إصدار الأمم المتحدة اتفاقية مكافحة الجريمة المنظمة عبر الوطنية في عام 2000 والتي عرفت الجريمة المنظمة في مادتها الثانية وفق أربع معايير:

أ- " أنها جماعة محددة البنية، مكونة من ثلاثة أشخاص أو أكثر.

ب- موجودة لفترة من الزمن.

1- محمد حسن خمو المزوري، المرجع السابق، ص 20.

2- محمد كريم علي، المرجع السابق، ص 61، أنظر كذلك د. سمر بشير خيرى، المرجع السابق، ص 52.

3- علاء زكي، المرجع السابق، ص 146.

ت-تقوم بفعل مدبر بهدف ارتكاب واحدة أو أكثر من الجرائم الخطرة، أو الجرائم المقررة وفق لهذه الاتفاقية.

ث-الحصول بشكل مباشر أو غير مباشر على المنفعة المالية أو منفعة مادية أخرى¹.

ويقصد بتعبير {جريمة خطرة} سلوك يمثل جرماً يعاقب عليه بالحرمان التام من الحرية لمدة لا تقل عن أربع سنوات أو بعقوبة أشد، ويقصد بتعبير {جماعة محددة البنية} جماعة غير مشكلة عشوائياً لغرض الارتكاب الفوري لجرم ما، وإن يكون لأعضائها ادوار محددة مع استمرار عضويتهم فيها².

وما يتضح من التعاريف السابقة أن حجم الجماعة الإجرامية المنظمة من الممكن أن يكون صغيراً جداً، على الرغم من أن بعض الجماعات الإجرامية المنظمة ممكن أن تكون كبيرة، وليس من الضرورة أن تكون موجودة لفترة زمنية طويلة على الرغم من أن بعضها موجود فعلاً، والأهم من ذلك أن خطورة الجرائم التي ترتكبها هذه الجماعات وطبيعتها المدفوعة بالربح هي عناصر محددة لها³.

6-تعريف الدول العربية للجريمة المنظمة.

لم تكن الدول العربية بمنأى عن التطورات الحاصلة في المجتمع الدول حول تعرف الجريمة المنظمة⁴ وتناولت تعريفها في الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود

1- أنظر المادة الثانية من اتفاقية مكافحة الجريمة المنظمة عام 2000، المرجع السابق.

2- محمد كريم علي، المرجع السابق، ص 60 61، أنظر كذلك لدى، سمر بشير خيرى، المرجع السابق، ص 52 53.

3- للمزيد أنظر في ذلك، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، عبر الموقع الإلكتروني، المرجع السابق، <https://www.unodc.org/e4j/en/index.html>.

4- في هذا الشأن تشير الدكتورة نسرین عبد الحميد نبيه إلى العديد من التعريفات للجريمة المنظمة منها ما هو وضعي و أجرائي وقانوني، أم التعريف الوضعي فتصفه بأنه " تنظيم هرمي يقوم على التسلسل ويهدف لتحقيق الربح، وهي تقوم بأعمال جرمها القانون الدولي والمحلي وتقوم بأنشطتها عبر الحدود الدولية"، أم التعريف الإجرائي فتقول بأنه " بناء تنظيمي يتكون من مجموعة من الأشخاص المجرمين لهم ثقافة فرعية ينتمون لعدة دول ويعملون في نشاط أو أنشطة إجرامية عبر دولتين وأكثر بهدف تحقيق أكبر ربح مادي"، أما التعريف القانوني فتعرفها على انها " مشروع إجرامي قائم على أشخاص يحددون صفوفهم من أجل القيام بأنشطة إجرامية على أساس دائم ومستمر ويتسم هذا التنظيم بكونه ذات بناء هرمي (مستويات قيادية وأخرى للتنفيذ)، ويحكم هذا

الوطنية الصادرة في عام 2010 في الفقرة الثانية والثالثة من المادة الثانية بنصها "الجريمة المنظمة عبر الحدود الوطنية هي كل جريمة ذات طابع عابر للحدود الوطنية تضطلع بتنفيذها أو الاشتراك فيها أو التخطيط لها أو تمويلها أو الشروع فيها جماعة إجرامية منظمة على النحو الموصوف في الفقرة 03 من هذه المادة"، أما الجماعات الإجرامية فتم تعريفها في هذه الاتفاقية في الفقرة الثالثة من المادة المذكورة أعلاه على أنها "الجماعات الإجرامية المنظمة كل جماعة ذات بنية محددة مكونة لفترة من الزمن من ثلاثة أشخاص، أو أكثر، اتفق أفرادها على ارتكاب إحدى الجرائم المشمولة بهذه الاتفاقية من أجل الحصول على منفعة مادية مباشرة أو غير مباشرة"¹، إضافة إلى ذلك وصفت المادة الثالثة من الاتفاقية العربية لمكافحة الجريمة المنظمة الجريمة المنظمة التي يمكن أن تعتبر عابرة للحدود كقاعدة عامة².

ثانيا: التعريفات الفقهية للجريمة المنظمة.

يعرف بعض علماء القانون الجريمة المنظمة في تعريف بسيط بأنها " ممارسة مجموعة منظمة الأنشطة الإجرامية بغرض الحصول على مكاسب مادية"، ومع ذلك، فإن هذا التعريف واسع وغير محدد على الرغم من إيجازه، حيث يمكن أن يشمل تقريباً أي جريمة قد يتورط فيها عدد من الأفراد، ولكل منهم دور محدد، حتى يتمكن كل منهم من تحقيق أهدافه بطريقة متقدمة

الكيان نظم و لوائح تضبط إيقاع سير العمل داخله، ويستخدم في سبيل تحقيق أغراضه العنف والتهديد والابتزاز والرشوة في إفساد المسؤولين، أنظر في ذلك، نسرين عبد الحميد نبويه، الجريمة المنظمة عبر الوطنية، دار الفكر الجامعي، الاسكندرية جمهورية مصر العربية، طبعة 2015، ص 56 57.

1- المادة الثانية من الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، الصادرة بقرار عن مجلس الوزراء لجامعة الدول العربية رقم 184، المحررة في القاهرة بتاريخ 2010/12/21.

2- تنص المادة الثالثة من الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية على " نطاق تطبيق الاتفاقية، 1- تطبيق هذه الاتفاقية على ما يأتي: أ- الأفعال المجرمة بمقتضى هذه الاتفاقية. ب- أية جريمة أخرى منظمة عبر الحدود الوطنية معاقب عليها بعقوبة سالبة للحرية لمدة لا تقل عن ثلاث سنوات، وفقاً للقوانين الوطنية لكل دولة. 2- لأغراض الفقرة 1 من هذه المادة، تكون الجريمة عابرة للحدود الوطنية إذا ارتكبت : أ- في أكثر من دولة واحدة. ب- في دولة واحدة، وكان الإعداد أو التخطيط لها أو توجيهها أو تمويلها أو الإشراف عليها في دولة أو دول أخرى. ج- في دولة واحدة، من جماعة إجرامية منظمة تمارس أنشطة إجرامية في أكثر من دولة واحدة. د- في دولة واحدة، وترتبت عليها آثار شديدة في دولة أو دول أخرى".

يصعب على القانون أن يتصدى لها وهذا من خلال الوسائل المستخدمة لإخفاء اهدافه الإجرامية.

ويقدم آخرون تعريفا أكثر دقة، موضحين أنها " مجموعة- مهما كان عدد أعضائها- منظمة ومدروسة وقائمة على روابط سرية وتشتمل على هيكلية داخل الدولة أو خارج الدولة التي أساسها ارتكاب الجرائم الجسيمة المستخدمة لهذا الغرض والوسائل غير المشروعة التي تهدف إلى الحصول على مكاسب غير مشروعة والإضرار بالمصالح الاستراتيجية و الأمن العام لدولة أو لدول"، وكلمة الجريمة المنظمة هي ما يميزها عن الجرائم الأخرى، لأنها تعني بنية تنظيمية قائمة لتحقيق أهداف محددة حسب الأدوار المنوطة بأعضاء المنظمة، لما لها من خاصية الاستمرارية والتسلسل الهرمي ومستويات القيادة والتأمر.

كما قدم أساتذة علم الإجرام العديد من التعريفات للجريمة المنظمة، حيث يرى البروفيسور " **Cusson كوسون** " أن الجريمة المنظمة هي المقصود بها " التنظيم الإجرامي الذي يشكل شبكة مستقلة من مجموعة المجرمين القادرين على ارتكاب جرائم القتل، وتعتمد استدامة هذه الشبكة على ارتباط أعضائها بالسكان والدولة، و العلاقات التي تتنوع بين الحماية والترهيب والفساد " أما الأستاذ " **Gassin جاسين** " فيعتبر أن الجريمة المنظمة هي " تلك الجريمة التي تتميز بالتخطيط وارتكابها بالتنظيم الممنهج، والتي تمنح مرتكبيها وسائل العيش"¹.

أما الدكتور **شريف السيد كامل** فقد عرفها على أنها " فعل أو أفعال غير مشروعة تهدف غالبا للربح ترتكبها جماعة إجرامية باستخدام التهديد أو العنف أو الرشوة حيث تتصف هذه الجماعة الإجرامية بالاستمرارية والتنظيم الهيكلي المتدرج، حيث يعمل أعضاؤها وفق نظام داخلي يحدد دور كل منهم، كما يكفل ولأهم لأوامر رؤسائهم ويمتد نشاطها الإجرامي عبر عدة دول"².

1- طارق زين، الجريمة المنظمة العابرة للحدود الوطنية "التعاون الدولي وسبيل مكافحة" "التدابير الاحترازية"، المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية، بيروت لبنان، الطبعة الأولى 2017، ص 12.

2- محمود مدين، المرجع السابق، ص 41.

كما تعرفها **هدى حامد قشقوش** بأنها "مؤسسة إجرامية ذات تنظيم هيكلي متدرج تمارس نشاطات غير مشروعة بهدف تحقيق أرباح مالية، مستخدمة الطرائق المتاحة لتمويل مشروعها الإجرامي وتحقيق هذا الهدف وذلك في سرية تامة لتأمين وحماية أعضائها".

بناءً على التعريفات المذكورة أعلاه، نستنتج أنه لكي يتم اعتبار الجريمة منظمة ومتسقة مع الاتجاه السائد، يجب استيفاء العديد من الشروط، ففيما يتعلق بالسلوك الإجرامي المكون للجريمة، بحيث يجب أن يكون هذا السلوك على درجة من التعقيد والتشعب، وعلى درجة عالية من التنظيم والتخطيط الدقيق، وأن يكون تنفيذه قد أكتمل على نطاق واسع، وأن وسائل تنفيذه تشمل درجة من العنف، أو نوع من الخداع يتجاوز القاعدة في الجرائم العادية، وأنه من شأنه أن يولد خطراً عاماً على المستوى الاقتصادي أو الاجتماعي أو السياسي، ومن حيث الجناة تتكون المنظمات الإجرامية من مجموعة تتجاوز عددها المشترك في المساهمة الجنائية العادية، ويشترط أن يكون بين الجناة من أتخذ الإجرام حرفة يتكسب منها، وأن يكونوا على درجة من التنظيم وقدرة على التخطيط الدقيق، ويجب أن تتلاقى إرادة هؤلاء في ارتكاب الجريمة أو الجرائم محل التنظيم¹.

ومع ذلك فإن التعريف العام له حدود، لأن نشاط الجريمة المنظمة يختلف باختلاف البدان والمناطق وأنواع الجريمة وطبيعة تنظيمها، لذلك من المهم معرفة العناصر العامة للجريمة المنظمة ولكن هناك حاجة إلى مزيد من المعرفة لفهم كيفية ظهورها في مختلف المواقع والسياقات الإجرامية.

1- طارق زين، المرجع السابق، ص 16.

الفرع الثاني : خصائص الجريمة المنظمة.

بناء على التعريفات الفقهية والتعريفات التي تناولتها الاتفاقيات الدولية سابقة الذكر فإنه يمكن الوصول إلى أبرز خصائص الجريمة المنظمة على النحو التالي:

أولاً: التنظيم.

يعتبر التنظيم السمة الرئيسية للجريمة المنظمة عبر الوطنية ويهدف إلى تنظيم تجمع الأعضاء في هيكل وبيان كامل ومتكامل قادر على القيام بأنشطته الإجرامية، واتخاذ القرارات وتوجيه الأعضاء لتحقيق أهداف الجماعة الإجرامية، حيث يخضع الأعضاء إلى نظام سلطوي رئاسي، بحيث يكون الأعضاء تحت قيادة زعيم أو قائد أو لجنة عليا تكون مسؤولة عنهم.

كما يسمح التنظيم لأعضاء الجماعة الإجرامية بعلاقة قائمة على تدرج القوة حسب فاعلية تنظيمها، بحيث يتميز التنظيم الجماعي بتقسيم العمل بين أعضائه، وليس ضرورياً للهيكل التنظيمي اتخاذ شكل معين أو لمعرفة الاختصاص أو الأدوار لبقية الأعضاء، لذلك عادة ما تكون الهياكل التنظيمية سرية¹، كما لهذه التنظيم ميزتان رئيسيتان:

1- عدد الاعضاء إذ تشترك غالبية التشريعات في أن يكون عدد أعضاء المنظمة الإجرامية ثلاثة أشخاص فأكثر.

2- أن تتمتع المنظمة الإجرامية لهيكل تنظيمي هرمي، أي أن يكون هناك تدرج هرمي في الوظائف ابتداء بأعلى مسؤول وصولاً إلى أدنى مرؤوس وهذا يعني وجود سلطة مركزية للتنظيم تتولى الإدارة².

ثانياً: التخطيط.

أنه العامل الأكثر أهمية في الجريمة المنظمة، والذي يتطلب عدداً من محترفي المهن الإجرامية الذين يتمتعون بخبرة دولية ومعرفته وثقافته جنائية تسمح لهم بوضع خطط ناجحة، إذ يعتبر التخطيط من السمات الرئيسية للجريمة المنظمة، إذا لا بد من التخطيط المسبق للقيام بأية

1- سمر بشير خيري، المرجع السابق، ص 57 58.

2- محمد حسن خمو المزوري، المرجع السابق، ص 23 24.

عملية إجرامية تقوم المنظمة الإجرامية بارتكابها، وفي حالة توافر عنصر التخطيط فإن المنظمة الإجرامية بهذا تكفل لأعضائها الحماية فيما يرتكبونه من أنشطة إجرامية، حيث لا يُفترض أن تقوم هذه المنظمة أو المجموعة بأي نشاط إجرامي غير منسق أو غير مخطط بطريقة عملية لأن العمل ضد الجريمة لا يتوافق فقط مع المبادئ والقواعد التي تسمح بالتخطيط لها، بحيث يكفل النجاح للجريمة المنظمة، وبالتالي صعوبة اكتشاف هذه الجريمة أو القبض على فاعليها، وبالتالي فإن كل جريمة منظمة هي جريمة مخططة، ولكن كل جريمة مخططة لا يمكن عدها جريمة منظمة وذلك أن الجريمة المخططة قد تكون لغرض القتل لمرة واحدة عكس الجريمة المنظمة التي تكون مستمرة ويكون الهدف تحقيق الربح¹.

ثالثاً: الاستمرارية.

الجريمة المنظمة تتميز بطبيعة الاستمرارية والثبات، فهي تمتد مع مرور الوقت ولا تنتهي بانتهاء حياة العضو الرئيسي أو انتهاء عضوية أحد أعضائها لكنها تستمر، والقيادة تنتقل إلى شخص آخر لديه القدرة والسلطة والسيطرة على تسييرها، لذلك تستمد هذه التنظيمات الإجرامية صفة الاستمرارية من نشاطها وليس حياة أعضائها ورؤسائها لأن العبرة باستمرار التنظيم الإجرامي للجماعة وليس حياة الفرد داخلها، بحيث لا تتوقف أنشطتها الإجرامية نتيجة اكتشاف عملية أو إجراء من جانب الدولة أو عدة دول².

رابعاً: السرية.

أن أهم ركائز الجريمة المنظمة أنها تحافظ على سرية أنشطتها لنفسها، وتعني السرية التنفيذ الناجح لخططها، وعدم إجهاضها قبل تنفيذها من جهة، ومن جهة أخرى، حماية أعضائها وتأمين عملياتها دون مواجهة³، وفي هذا الشأن لقانون الصمت مكانه كبيرة داخل التنظيم الإجرامي، حيث يحترم جميع أعضائه السرية المطلقة، سواء في تكوين المنظمة الإجرامية أو

1- محمد كريم علي، المرجع السابق، ص 65 66.

2- نسرین عبد الحمید نبیه، المرجع السابق، ص 61، أنظر كذلك د. سمر بشیر خیری، المرجع السابق، ص 60.

3- علاء زکی، المرجع السابق، ص 232.

الأنشطة التي تقوم بها، وفي أعراف الجماعات الإجرامية المنظمة، وانتهاك السرية والكشف عن الحقيقة تعتبر مخالفة تعرض أعضائها للعقوبة القصوى وهي الإعدام، حيث تعاقب التنظيمات الإجرامية لخرق قواعد الصمت بقسوة شديدة، لأنها تؤدي إلى إحداث فجوة عميقة في الهيكل التنظيمي للتنظيم الإجرامي، و لذلك فإن العقوبات من الممكن أن لا تخص فقط العضو الذي انتهك التزامه وسريته ، بل تمتد أيضًا إلى عائلته¹.

خامساً: استخدام العنف.

إن من استراتيجية العمل الإجرامي المنظم استخدام العنف والتهديد والإرهاب إلى حد يصل إلى القتل والخطف والضرب والجرح المفضي إلى الموت، وهذا لترهيب الآخرين والضغط عليهم من أجل تحقيق الأهداف الإجرامية للجماعة والتهديد بنية منع الضحايا أو عائلاتهم من الإبلاغ عن الجرائم التي ارتكبتها هذه الجماعات ضدهم، بهدف عدم الدخول في مواجهة مع السلطات العامة².

ومن الممكن أن تستخدم الجماعات الإجرامية الرشوة والتهديدات والابتزاز لرشوة الموظفين العموميين، بما في ذلك مسؤولي الأمن والعدالة والمحققين والقضاة وحتى البرلمانين، من أجل الحصول على مزايا تمكنهم من تسهيل أنشطتهم الإجرامية والعمل في الأسواق المشروعة، وبهدف عرقلة خطة الدولة للتعامل مع هذه الجريمة، لذلك تلجأ إلى الفساد والرشوة، إما للعمل بشكل كامل على إفلات الجناة من العقاب أو التخفيف عنهم، أو لتمتعهم بمعاملة عقابية منفصلة ومتميزة.

وفي حالة عدم نجاح المنظمة الإجرامية في استخدام الرشوة أو التهديد لإخضاع السلطات العامة لها، فإنها تلجأ إلى استخدام العنف ضد السلطات بهدف إضعاف هيكل الشرطة والقضاء، بل و السلطة العامة كلها، وقد شهدت إيطاليا فترات اهتزت فيها السلطة العامة بسبب اعتداءات جسيمة كانت تحدث دائما في كل ازمة من أزمات المافيا، أو حيث تشعر أن مصالحها معرضة للخطر، ومن ذلك سلسلة الاغتيالات للقضاة ورجال السياسة الذين انتهجوا سياسة معادية للمافيا،

1- محمد كريم علي، نفس المرجع السابق، ص 70.

2- بن عمارة محمد، مفهوم الجريمة المنظمة دوليا ووطنياً، مقال منشور في مجلة البحوث في الحقوق والعلوم السياسية، كلية الحقوق والعلوم السياسية جامعة ابن خلدون تيارت الجزائر، العدد الرابع أكتوبر 2016، ص 7.

وهذا ما حدث عندما قامت جماعة المافيا في مدينة صقلية الإيطالية عام 1992 بعمل إرهابي وقتل القاضي {جيوفاي فالكون} وذلك باستعمال مادة متفجرة أدت أيضا إلى قتل زوجته وثلاث من أفراد حمايته، كذلك فإن تنظيم المافيا في روما قد استخدم نفس الوسيلة أي التفجير لقتل صحفيين كانوا مسؤولين عن أحد البرامج التلفزيونية أثار الرأي العام ضد المافيا وذلك في مايو عام 1993¹.

سادساً: تحقيق الربح.

يُعد السعي إلى تحقيق الربح الغاية الأساسية الذي تهدف المنظمة الإجرامية إلى تحقيقه من خلال ممارسة الأنشطة الإجرامية المختلفة، ويتحقق هذا الربح غالبا من خلال أنشطة تتخذ طابعاً تجارياً منظماً، تقوم على عرض سلع أو تقديم خدمات غير مشروعة، وتهدف من ورائها تحقيق الأرباح بغض النظر عن آثارها الخطيرة، أو ما تخلفه من أثار جسيمة على الأفراد والمجتمع، ويمكن أن يمتد الربح المالي إلى الأنشطة المشروعة في ظاهرها، حيث تستغل الأموال المتحصل عليها من الجرائم في استثمارات وأعمال قانونية بقصد إخفاء مصدرها غير المشروع فيما يعرف بغسيل الأموال، وتتسم أنشطة الجريمة المنظمة بالسعي إلى تحقيقي أرباح غير محدودة مستفيدة من استغلال مواطن الضعف البشري، ومن الممكن أن تتجاوز الغاية تحقيق الربح المالي أحيانا إلى تحقيق أهداف سياسية أو تعزيز النفوذ داخل الدولة².

1- محمد كريم علي، نفس المرجع السابق، ص 70 71.

2- نسرين عبد الحميد نبيه، المرجع السابق، ص 62.

المطلب الثاني: الجريمة المنظمة المستحدثة.

لا يقتصر الجانب السلبي لشبكات الاتصال وأنظمة المعلومات على الاحتيال والسرقة ونشر المواد الإباحية فحسب، بل يشمل أيضًا منظمات تهريب المخدرات والمنظمات الإجرامية والإرهابية التي تركز على استغلال المرافق والفرص التي توفرها شبكات الاتصال وأنظمة المعلومات أكثر مما تركز عليه في تعطيل عمل هذه الشبكات أو اختراقها، لأنها توفر أرباحاً جديدة ضخمة يمكن جنيها من خلال الأنشطة غير المشروعة باستخدام الشبكة الإلكترونية وأجهزة الكمبيوتر كأداة للجريمة¹.

في السنوات الأخيرة بدأت بعض الجماعات التي تتخذ من الجريمة المنظمة كعمل تجاري في إنشاء قاعدة أعمال في البلدان الضعيفة التي توفر لهم ملاذًا آمنًا يمكنهم من خلاله إجراء عملياتهم عبر الحدود، لذلك يوفر هذا الحال درجة إضافية من الحماية ضد تطبيق القانون وقد سمح للجماعات بتنفيذ أنشطتها، وهو ما يعد ميزة، فهذا يجعل النشاط الإجرامي عملاً سهلاً للغاية مقارنة بالواقع التقليدي للجريمة، حيث إن المنظمات الإجرامية ليست الوحدة الوحيدة في أسواق التجارة غير المشروعة، لكنها غالبًا ما تكون من بين أكبر المستثمرين نظرًا لتمتعهم بمنافسة أكبر توفرها قدرتهم على التهديد باستعمال العنف، ومهارتهم الكبيرة في اكتشاف واستغلال الفرص لتنفيذ مشاريع جديدة غير مشروعة².

لهذا سنتناول في هذا المطلب دراسة صور الجريمة المنظمة المستحدثة عبر وسائط النظم المعلوماتية والتي طورتها الجماعات الإجرامية المنظمة في الفرع الأول، أما الفرع الثاني فخصصناه لدراسة الإرهاب الإلكتروني.

1- عبدالله عبدالكريم عبدالله، جرائم المعلوماتية والانترنت (الجرائم الإلكترونية) دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والانترنت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا، منشورات الحلبي الحقوقية، بيروت لبنان، الطبعة الأولى 2007، 41.

2- عبدالله عبدالكريم عبدالله، نفس المرجع السابق ص 41 42.

الفرع الأول: صور الجريمة المنظمة المستحدثة.

من الجرائم المنظمة التي لاقت رواجاً على شبكات النظم المعلوماتية لسهولة ارتكابها عن طريق الشبكات والانترنت وصعوبة اكتشافها وتعقب مرتكبيها الاحتيال الالكتروني والاتجار بالبشر وغسل الاموال والاتجار بالمخدرات والاسلحة.

أولاً: الإحتيال الالكتروني.

يعني الاحتيال في اللغة الحذق وجودة النظر والقدرة على دقة التصرف، ويعرف فقهاً على أنه " كل تلاعب عمدي بالمعلومات أو البيانات تمثل قيمة مادية والمخزنة داخل نظام الحاسب الآلي، أو الإدخال غير المصرح به لمعلومات وبيانات صحيحة أو التلاعب في الأوامر والتعليمات أثناء عملية البرمجة أو استخدام أي وسيلة أخرى من شأنها التأثير في عمل الحاسب الآلي، بما يدفعه إلى تنفيذ عملياته استناداً إلى هذه الأوامر أو البيانات أو التعليمات، بقصد تحقيق منفعة أو ربح غير مشروع وإلحاق ضرر بالغير"، وفي تعريف آخر يعرف الاحتيال الإلكتروني على أنه " كل فعل أو سلوك متعمد من شخص طبيعي أو معنوي يستخدم فيه التقنية الإلكترونية بهدف كسب مادي غير مشروع على الأموال أو السندات وذلك عبر طرق احتيالية أو اتخاذ أسم كاذب أو صفة غير صحيحة"¹.

ويتمتع الاحتيال الالكتروني بالعديد من الخصائص التي تتقارب مع خائص جرائم نظم المعلومات نذكر منها على سبيل المثال:

3- يتخذ من الشبكة المعلوماتية والحاسب الآلي أداة أساسية لارتكاب جريمة الاحتيال الإلكتروني.

1- أما المشرع الجزائري فتناول جريمة الاحتيال في قانون العقوبات الجزائري ونص في المادة "372" على أنها (كل من توصل إلى أستلام أو تلقى اموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالفات أو إبراء من بالتزامات أو إلى الحصول على أي منها أو شرع ف ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبه أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500 إلى 20.000 دينار جزائري". للمزيد أنظر قانون العقوبات الجزائري.

- 4- لا تعترف جريمة الاحتيال الإلكتروني بالحدود الجغرافية.
- 5- يتميز مرتكب جريمة الاحتيال الإلكتروني بالخبرة الفائقة العلمية والعملية.
- 6- يهدف الاحتيال الإلكتروني إلى تحقيق الربح غير المشروع.
- 7- جريمة صعبة الاكتشاف والأثبات¹.

ويتم الاحتيال الإلكتروني بالعديد من الطرق فعلى سبيل المثال قد يتم بطريق القرصنة على أرقام بطاقات الدفع الإلكتروني حيث يمكن للمجموعات الإجرامية المنظمة الوصول لقواعد البيانات الخاصة ببطاقات الدفع الإلكتروني، وفي هذا السياق نجحت منظمة إجرامية تطلق على نفسها أسمها **"Shadow Crew"** في الحصول على أرقام بطاقات دفع لإلكتروني من قواعد البيانات وفي عام 2007 أُلقت السلطات التايلاندية القبض على ثلاثة رجال سريلانكيين وضبطت 5000 بطاقة أتمان وهمية بأسماء أشخاص من بريطانيا، وتبين أنهم تمكنوا من السحب بواسطة هذه البطاقات عدة مرات من أجهزة الصراف الآلي، إضافة إلى القرصنة فأن المزايدات الوهمية تعتبر من طرق الاحتيال الإلكتروني والسمسة في مختلف المجالات عن طريق الانترنت، والاحتيال باستخدام أساليب الاستثمار ويسمى هذا الأسلوب **"Pump-and-dump"**، بحيث يتم الإعلان المزيف عن الوضع المالي لمؤسسة اقتصادية كشركة ما من أجل رفع قيمة أسهمها في السوق المالي، تم بيعها بمجرد ارتفاع سعرها².

ثانياً، الاتجار الإلكتروني بالبشر.

أن الاتجار الإلكتروني بالبشر من أهم الجرائم المنظمة في الوقت الحالي وهي جريمة مستحدثة تتم بالاعتماد على الانترنت كأساس لنجاحها سواء في بدايتها أو حتى تمام عملية البيع وتنفيذها بوصول الانسان الذي تم بيعه أو جزء منه إلى المشتري، كما يمكن أن تتم عبر استغلال الأطفال في أعمال الدعارة والجنس، حيث في هذا الشأن أجرت الشرطة الألمانية تفتيش على مواطن يشتبه في ارتكابه جرائم تتعلق بدعارة الأطفال عبر الأنترنت، وأُتضح أن المشتبه به

1- صابرين جابر أحمد محمد، محمود بن علي بن سهيل المعشني، المواجهة الجنائية لجريمة الاحتيال الإلكتروني في التشريع العماني، مقال منشور في مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، المركز الجامعي أفلو، ولاية الأغواط الجزائر، المجلد السادس، العدد الأول مارس 2023، ص 175 176.

2- عبد الإله النوايسة، المرجع السابق، ص 156 157.

كان قد تبادل الصور الإباحية للأطفال عبر الأنترنت مع أشخاص في دول أخرى، وقد قاد هذا التحقيق لتنفيذ أوامر تفتيش في سبعة ولايات في أمريكا، وثلاثين أمر تفتيش في عشر بلدان أجنبية أخرى، بما في ذلك اليابان¹.

أما عن تعريف جريمة الاتجار بالبشر فقد عرفت العديد من الاتفاقيات منها ما جاء في المادة 3/أ من بروتوكول الاتجار بالبشر الصادر عن هيئة الأمم المتحدة على أنها " يُقصد بتعبير الاتجار بالأشخاص تجنيد أشخاص أو نقلهم أو تنقلهم أو إيوائهم أو استقبالهم بواسطة التهديد بالقوة أو استعمالها أو غير ذلك من أشكال القسر أو الاختطاف أو الاحتيال أو الخداع أو استغلال السلطة أو استغلال حالة استضعاف، أو بإعطاء أو تلقي مبالغ مالية أو مزايا لنيل موافقة شخص له سيطرة على شخص آخر لغرض الاستغلال، ويشمل الاستغلال، كحد أدنى، استغلال دعاية الغير أو سائر أشكال الاستغلال الجنسي، أو السخرة أو الخدمة قسراً، أو الاسترقاق أو الممارسات الشبيهة بالرق، أو الاستعباد أو نزع الأعضاء"².

إضافة إلى ذلك عرفت الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الوطنية لعام 2010 الاتجار بالأشخاص على أنها " أي تهديد بالقوة أو استعمالها أو غير ذلك من أشكال القسر أو الاختطاف أو الاحتيال أو الخداع أو إساءة استعمال السلطة أو استغلال حالة الضعف وذلك من أجل استخدام أو نقل أو إيواء أو استقبال أشخاص لغرض استغلالهم بشكل غير مشروع في ممارسة الدعارة " البغاء " أو سائر أشكال الاستغلال الجنسي أو السخرة أو الخدمة قسراً أو الاسترقاق أو الممارسات الشبيهة بالرق أو الاستعباد، ولا يُعتد برضاء الشخص ضحية الاتجار في كافة صور الاستغلال متى استُخدمت فيها الوسائل المبينة في هذه الفقرة"³.

1- عبد الإله النوايسة، المرجع السابق، ص 157.

2- المادة الثالثة من بروتوكول منع وقمع ومعاقبة الاتجار بالأشخاص، وبخاصة النساء و الأطفال، المكمل لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية الموضوع للتوقيع في عام 2002، الصادر عن الأمم المتحدة.

3- المادة الحادية عشر من الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الوطنية، الصادرة عن جامعة الدول العربية في عام 2010، في هذا الإطار لقد تناول قانون العقوبات الجزائري جريمة الاتجار بالبشر في المادة 303 مكرر 4 والتي نصت على " يُعاقب على الاتجار بالأشخاص، بالحبس من خمس (5) سنوات إلى خمس عشرة (15) سنة وبغرامة من 500.000 دج إلى 1.500.000 دج، إذا سهل ارتكابه حالة استضعاف الضحية

في حين تحتل جريمة الاتجار بالبشر المرتبة الثالثة عالميا من حيث مصدر العائدات المالية بعد تجارة تهريب المخدرات وتجارة الأسلحة، فهي من أكثر الجرائم المنظمة انتشارا في العالم، وعلى الصعيد العربي شهدت هذه الجريمة تزايدا ملحوظا وانتشار بشكل كبير في الدول العربية خلال الفترة الأخيرة، خاصة بعد أحداث الربيع العربي، حيث ساهمت حالة عدم الاستقرار والصراعات في تفاقم ظاهرة الهجرة غير الشرعية وزيادتها وخاصة باتجاه أوروبا، وفي هذا الإطار كشف تقرير الأمم المتحدة حول مكافحة جريمة الاتجار بالبشر لعام 2018 أن هذه الجريمة قد ازدادت في الدول العربية أكثر من أي وقت مضى¹.

أما الإتجار بالبشر عبر الانترنت فيمكن تعريفه على أنه " استغلال وسائل الإتصال الإلكتروني في تبادل المعلومات بشأن الصفقات غير المشروعة التي يكون محلها بيع أنسان حي أو استغلاله ، أو بيع جزء من جسده أو أحد مشتقات هذا الجسد "، إضافة إلى ذلك فإنه يمكن تعريفه على أنه " السلوك الإجرامي الذي يقوم من خلاله الجاني بإنشاء موقع الكتروني عبر الشبكة المعلوماتية من أجل تجنيد أشخاص أو نقلهم أو تنقلهم أو إيوائهم أو استقبالهم، بواسطة التهديد بالقوة أو استعملها أو غير ذلك من أشكال القسر أو الاختطاف أو الاحتيال أو الخداع أو إساءة استعمال السلطة، أو إساءة استغلال حالة استضعاف أو بإعطاء أو تلقي مبالغ مالية أو مزايا لنيل موافقة شخص له سيطرة على شخص آخر لغرض الاستغلال، ويشمل الاستغلال كحد أدنى استغلال دعاره الغير أو سائر أشكال الاستغلال الجنسي أو لسخرة أو لخدمة قسرا أو الاسترقاق أو الممارسات الشبيهة بالرق أو الاستعباد، أو نزع لأعضاء ".

الناجمة عن سببها أو مريضها أو عجزها البدني أو الذهني، متى كانت هذه الظروف ظاهرة أو معلومة لدى الفاعل"، وبناء على ما سبق من تعريفات لجرائم نظم المعلومات و وفقا للقانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاتصالات ومكافحتها، لأن أي جريمة يستخدم في ارتكابها وسائل الاتصال الإلكترونية فهي معاقب عليها وفقا للقانون 04-09 وبالتالي لأن جريمة الاتجار الإلكتروني بالبشر يوفر لها الركن الشرعي لأنها تقوم على استخدام وسائل اتصال إلكترونية أو منظومة معلوماتية، للمزيد أنظر المواد 303 مكرر 5 إلى المادة 303 مكرر 15 من قانون العقوبات الجزائري.

1- نبيلة كردي، الإتجار بالبشر عبر الانترنت، مقال منشور بمجلة أبحاث، مجلة علمية دورية متخصصة في الأبحاث السياسية والقانونية تصدر عن جامعة زيان عاشور الجلفة، الجزائر، المجلد السابع، العدد 02 لعام 2022، ص 524.

ومفاد ذلك أن العناصر الأساسية لظاهرة الاتجار الإلكتروني بالبشر تقوم بتوافر ثلاثة عناصر وهي:

1- **السلعة:** وهي في هذه الحالة الشخص سواء تم استغلاله بالكامل أو أن أحد أعضائه أو مشتقاته أو منتجاته المستخرجة منه، ويتم الحصول على الهدف من جريمة الاتجار الإلكتروني بالبشر عن طريق استدراج الأشخاص بطريق الخداع للحصول على فرصة عمل، أو من خلال إيهامهم بإبرام عقود الزواج، أو حتى بالحصول على حق اللجوء في بلدانهم، وبمجرد وصوله إلى الوجهة المحددة، يتم احتجازه ومعاملته على النحو الذي يريده.

2- **الوسيط (التاجر):** وهو المجموعة الإجرامية التي تقود العملية من بدايتها إلى نهايتها باستخدام مختلف الوسائل التكنولوجية المتاحة، حيث لا يتم هذا النوع من الجرائم في شكل الجرائم التقليدية، بل في شكل منظم يشبه إلى حد كبير عمل الشركات الدولية الشرعية، ولها مكتبها الرئيسي وموظفيها ومعداتنا وحراسها الأمنيون، وما إلى ذلك، ولديها أساليب عملها الخاصة واستراتيجيتها الخاصة على المدى الطويل وتسلسلها الهرمي، بل أنها تدخل في تحالفات استراتيجية مع منظمات إجرامية أخرى لتوسيع أنشطتها أو لتحقيق أرباح أكبر، حيث تمثل جريمة الاتجار بالبشر مصدر رئيسي للدخل لهذه الجماعات الإجرامية، وهو ما يجعلها تطور هذا النوع من الإجرام للوصول إلى أفضل الطرق لتحقيق أعلى الأرباح.

3- **السوق:** وهو المكان الذي يتم فيه عرض المنتجات المتاحة المذكورة أعلاه، ويتم ذلك من خلال استخدام الشبكات المعلوماتية وشبكة الانترنت، التي يتم عبرها عرض الأشخاص وتقديم مزاياهم وجذب أولئك الذين يرغبون في الحصول عليهم بأعلى سعر عن طريق تقديم عروض ومزايدات في حالات الطلب المتعدد على منتج متاح، حيث يعلب عنصر الطلب دوراً أساسياً في هذا النوع من الجرائم فكلما زاد الطلب ارتفعت في المقابل أرباح التنظيمات الإجرامية¹.

1- نبيلة كردي، المرجع السابق، ص 525.

ثالثاً: غسل الأموال أو تبييضها.

إن غسل الأموال هو أحد الأساليب التي تستخدمها المنظمات الإجرامية لإخفاء مصادر الأموال التي تكسبها من خلال أنشطتها الإجرامية، وبهذا تحاول اصباغ الشرعية على الأموال غير المشروعة التي حققتها من هذا النشاط المربح جداً، فالبعض حصر غسل الأموال في الأموال المحصلة من تجارة المواد المخدرة، إلا أن الأصح أنه يشمل كل عمليات غسل الأموال سواء كان أصلها من تجارة المخدرات أو الإتجار بالبشر والأسلحة أو أي أمر آخر غير مشروع¹.

إذ يشير غسل الأموال إلى العمليات التي يتم من خلالها إخفاء مصدر الدخل غير المشروع، فعلى الرغم من بساطة التعريف، إلا أنه يحتوي على جميع متطلبات غسل الأموال، وهي تفترض وجود أموال غير مشروعة، أي أن هذه الأموال تأتي من أنشطة إجرامية، وأن عمليات اقتصادية أو مالية تتم، وأن هذا يهدف إلى إعطاء الوضع القانوني لهذه الأموال².

وغالباً ما تمر عملية غسل الأموال بثلاث خطوات أساسية:

1- الإيداع:

تتمثل هذه الخطوة في التخلص من مبالغ نقدية كبيرة بإيداعها في مؤسسات مصرفية، أو في عدة حسابات، أو عن طريق التحويل المصرفي، أو بشراء أوراق مالية، أو عملات أجنبية، أو شراء معادن ثمينة، ويعبر عنها كذلك بالمرحلة التحضيرية أو التمهيديّة للغسل وهي الأكثر صعوبة بالنسبة للمجرمين العاديين أو التنظيمات الإجرامية، إذ يمكن أن تلفت الانتباه وتثير الشك حول مصدر الأموال فيتم اكتشافها³.

1- عبد العزيز بن غرم الله آل جار الله، جرائم الأنترنت وعقوبتها وفق نظام مكافحة الجرائم المعلوماتية السعودي دراسة مقارنة، دار الكتاب الجامعي للنشر والتوزيع، الرياض، المملكة العربية السعودية، الطبعة الأولى، 2017، ص 276.

2- عبد الإله النوايسة، المرجع السابق، ص 159.

3- علاء زكي، المرجع السابق، ص 192.

2- مرحلة التعتيم والتمويه:

خلال هذه المرحلة يتم تنفيذ العديد من المعاملات المتتالية بهدف إخفاء مصادر الأموال غير المشروعة، كإجراء عدة تحويلات من حساب بنكي إلى آخر، ويمكن تحويل الأموال المودعة في كل حساب منها إلى حسابات فرعية، وتهدف هذه المرحلة إلى وضع عقبات معقدة أمام السلطات لكشف مصادر الأموال غير المشروعة.

3- مرحلة الدمج:

في هذه المرحلة يتم تقنين الأموال المغسولة، بحيث تظهر الأموال المغسولة كعوائد نظيفة ناتجة عن استثمارها في أنشطة اقتصادية مشروعة مثل الفنادق والمشاريع السياحية والمطاعم¹، وبعد إدخال الأموال في دائرة التعامل الاقتصادي والمالي المشروع يتم مزج الدخول المتحصلة من هذه الأنشطة (المشروعة) بالأموال المتحصلة من الجريمة مما يجعل هذه الأموال الأخيرة تظهر وكأنها حصيلة عمل مشروع².

أما اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة لعام 2000 فقد تضمنت جريمة غسيل الأموال، بنصها في المادة السادسة منها على (تجريم غسيل عائدات الجرائم)، والزمّت الدول الأطراف على ضرورة تجريم أفعال غسيل الأموال غير المشروعة باعتبارها من الجرائم المنظمة والتي ترتكب في أكثر من إقليم دولي، حيث جاء في الفقرة الأولى من المادة سابقة الذكر النص على الأفعال التي تعتبر غسلا للأموال وهي على النحو التالي:

أ- تحويل الممتلكات أو نقلها، مع العلم بأنها عائدات جرائم، بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات أو مساعدة أي شخص ضالع في ارتكاب الجرم الأصلي الذي تأتت منه على الإفلات من العواقب القانونية لفعلته.

ب- إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو ملكيتها أو الحقوق المتعلقة بها، مع العلم بأنها عائدات جرائم.

1- عبد الإله النوايسة، المرجع السابق، ص 159.

2- علاء زكي، نفس المرجع السابق، ص 193.

ت- ورهنا بالمفاهيم الأساسية لنظامها القانوني اكتساب الممتلكات أو حيازتها أو استخدامها مع العلم، وقت تلقيها، بأنها عائدات جرائم¹.

وبالتأكيد أن غسيل الأموال لها آثار سلبية على الاقتصاد الوطني والدولي²، وبحسب تصريحات صندوق النقد الدولي، فإنه يغسل حول العالم حوالي 600 مليار دولار كل عام، وهو ما يمثل 2 إلى 5% من الناتج الإجمالي العالمي، كما لا شك أن هناك علاقة وثيقة بين الجريمة المنظمة وغسيل الأموال الإلكتروني، حيث استغلت المنظمات الإجرامية الثورة التكنولوجية لارتكاب جرائمها وغسل أموالها³.

وفي هذا الشأن تستعين المنظمات الإجرامية بالخبراء الاقتصاديين والفنيين للقيام بعمليات غسيل الأموال إلكترونياً، ما نتج عنه ظهور مصطلح "Cyber Laundering" الذي يشير إلى عمليات غسيل الأموال التي تتم عبر الإنترنت، وتعد من وسائل غسيل الأموال الإلكترونية بطاقات الدفع الإلكتروني، والبطاقات الذكية⁴، وبنوك الإنترنت، والنقود الإلكترونية المشفرة، والتحويلات الإلكترونية، والمحافظ الإلكترونية، وفي دراسة أجريت عام 2006 أفادت أن هناك 300 ألف موقع قمار على الإنترنت، 14% منها فقط مرخصة، وتنتج هذه الصناعة 15 مليار

1- المادة السادسة من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة لعام 2000، المرجع السابق، ص 2.
2- في هذا الشأن أشارت إحدى الدراسات الإحصائية أن تقديرات الأمم المتحدة لحجم جريمة غسيل الأموال على مستوى العالم في التسعينات تراوحت ما بين 350 - 500 مليار دولار وأن عمليات غسيل الأموال تشمل 70 بالمائة من حجم الدخل غير المشروعة للمنظمات الإجرامية على مستوى العالم، للمزيد أنظر عبد العزيز بن غرم الله آل جار الله، المرجع السابق، ص 277.

3- عبد الإله النوايسة، نفس المرجع السابق، ص 162.

4- تعد البطاقات الذكية من أهم اختراعات العصر الحديث في مجال الدفع بالبطاقات وهي بطاقة مصنوعة من البلاستيك تحتوي بداخلها على شريحة ذاكرة مزودة ببطاقة تخزين بيانات، توفر هذه البطاقة العديد من الخدمات بما في ذلك بيانات الشخص حامل البطاقة، مثل تاريخه الطبي ومعلومات حول حسابه المصرفي، ويمكن تعبئتها عبر جهاز الصراف الآلي من حسابه المصرفي، للمزيد أنظر، وهيبة عبد الرحيم، دراسة جريمة غسيل الأموال عبر القنوات الإلكترونية، مقال منشور مجلة الحقوق والعلوم الإنسانية دراسات اقتصادية، جامعة زيان عاشور الجلفة، الجزائر، العدد 01/19 أوت 2014، ص 44 وما بعدها.

دولار سنوياً، وتستغل هذه المواقع لارتكاب عمليات احتيال ضد العملاء والمنافسين من قبل المسؤولين عن الإدارة، حيث تعود أرباحها إلى المنظمات الإجرامية¹.

وعليه أن جريمة غسيل الأموال هي جريمة تابعة تفترض ابتداء سبق ارتكاب جريمة أولية نتج عنها أموال غير مشروعة، ثم تأتي مرحلة تالية وهي غسل تلك الأموال القذرة لتطهيرها، و لارتكاب إحدى صور السلوك الإجرامي المكون لجريمة غسيل الأموال يفترض وجود محل الجريمة، وهو المال الذي يتم غسله بعد تحصيله من مصدر غير مشروع²، عبر وسائط النظم المعلوماتية وشبكات الاتصال والأنترنت هذا أمر وارد في ظل نمو وازدهار التجارة الإلكترونية وذلك عن طريق تحويل الأموال أو توظيفها والتعامل مع البنوك عبر شبكات النظم المعلوماتية، مما يسمح بعمل العديد من التحويلات النقدية من حساب آخر ومن بنك لآخر بكل سهولة تحت غطاء التجارة الإلكترونية.

رابعاً: الإتجار بالمخدرات والأسلحة.

1- تجارة المخدرات.

تتصدر جرائم التجارة بالمواد المخدرة قائمة الأنشطة غير الشرعية التي تمارسها الجماعات الإجرامية، وذلك بسبب الأرباح العالية والسريعة التي تحققها، وفي التقرير السنوي لبرنامج الأمم المتحدة لمراقبة المخدرات عام 1997، تم تقدير حجم الموارد المالية التي تحققها جرائم التجارة بالمواد المخدرة بما يقرب من 400 مليار دولار سنوياً، وهي تمثل قيمة الصادرات العالمية بأكملها، وتشير تقارير أخرى إلى أن جماعات التنظيم الإجرامي المتعددة الجنسيات تستطيع أن تحقق أرباحاً تتراوح بين 450 و 750 مليار دولار سنوياً من جرائم التجارة بالمواد المخدرة.

وتزداد خطورة تجارة المخدرات بسبب استخدام عوائدها في تمويل جرائم أخرى، بما في ذلك الجرائم الإرهابية، وما لوحظ أن معظم هذه التجارة تنطلق من الجنوب، مثل أمريكا الجنوبية وجنوب شرق آسيا، إلى الشمال، مثل أمريكا الشمالية وأوروبا، ومن ناحية أخرى، يتزايد الطلب

1- عبد الإله النوايسة، نفس المرجع السابق، ص 162.

2- جعفر حسن جاسم الطائي، المرجع السابق، ص 207.

على الأسلحة في الجنوب، خاصة في مناطق جنوب أفريقيا التي تشهد نزاعات مسلحة، كما ولوحظ أيضًا وجود ارتباط مالي بين تجارة المخدرات وتهريب الأسلحة، إذ تستخدم الأموال التي يتحصل عليها من تجارة المخدرات في شراء الأسلحة¹.

وتعرف الاتفاقية الخاصة بالمؤثرات العقلية لعام 1971 الاتجار غير المشروع بالمخدرات على أنه "صنع المؤثرات العقلية أو الإتجار بها"، أما اتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع بالمخدرات والمؤثرات العقلية لعام 1988 فتعرفها في الفقرة الأولى والثانية من المادة الثالثة²، حيث يظهر أن مفهوم الإتجار غير المشروع يشمل إنتاج المخدرات أو صناعتها أو استخراجها أو تسليمها أو نقلها أو استيرادها وتصديرها أو زراعتها أو حيازتها أو تنظيم وإدارة كل أيا من هذه الأفعال، أو تحويل الأموال عنها أو إخفاء هذه الأموال وتمويه حقيقتها، وبالتالي فإن مصطلح الاتجار بالمواد المخدرة يشمل عدة أنشطة إجرامية تستهدف تحقيق الربح وتشمل عملية الانتاج الزراعي والتحويل الصناعي والتحويلي، وتهريب العقاقير المخدرة عبر الحدود والترويج والتوزيع³.

أما بالنسبة للمشرع الجزائري لم يتعرض لتعريف جريمة الاتجار غير المشروع بالمخدرات، حتى بعد مصادقته على اتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية لسنة 1988⁴، وعمل على مكافحتها، من خلال إصدار قانون يتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع استعمالها والاتجار غير المشروعين بهما⁵.

1- علاء زكي، المرجع السابق، ص 214 215.

2- يقصد بتعبير "الإتجار غير المشروع" الجرائم المنصوص عليها في الفقرتين 1 و 2 من المادة 3 من هذه الاتفاقية، والتي حملت عنوان الجرائم والجزاءات وجاء نصها على التالي: للمزيد أنظر باقي المواد من اتفاقية الأمم المتحدة لمكافحة الإتجار غير المشروع في المخدرات والمؤثرات العقلية، الموقعة في 20 ديسمبر 1988.

3- سمر بشير خيري، المرجع السابق، ص 64.

4- المرسوم الرئاسي رقم 95-41 المؤرخ في 28 يناير 1995، المتضمن المصادقة على اتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية، المؤرخة في 20 ديسمبر 1988 في فيينا، المرسوم صادر في الجريدة الرسمية عدد 7، بتاريخ 15 فبراير 1995.

5- قانون رقم 04-18 المؤرخ في 25 ديسمبر 2004، المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع استعمالها والاتجار غير المشروعين بهما، الجريدة الرسمية عدد 83، بتاريخ 26 ديسمبر 2004.

وفي نطاق التجارة الإلكترونية للمخدرات تعمل المجموعات الإجرامية على استغلال شبكة الإنترنت لترويج المخدرات، وفي هذا الشأن ذكر تقرير المخدرات العالمي لعام 2019 أن حجم مشتريات المخدرات عبر الشبكة الإلكترونية أخذ في الزيادة على المدي الطويل، بالرغم من انخفاضها في عام 2018، إلا أن شراء المخدرات عبر الانترنت لا يزال ظاهرة حديثة، وما يمكن أن يقال في هذا الامر أن تجارة المخدرات على شبكة الانترنت يمكن أن تدخل تغييرات في أنماط تعاطي المخدرات ومدى أنتشارها، فاستخدام الانترنت يمكن أن يخفف بعض الأخطار بالنسبة للمروجين والمتعاطين، ومع ذلك فلها مخاطر إلا أن مخاطرها تحدث خارج دائرة الاتصال بشبكات الانترنت، وقد اشار التقرير الصادر عن اليوروبول إلى تحقيق نجاح ملحوظ في تفكيك أسواق كبيرة للمخدرات عبر شبكة الانترنت، غير أن المجرمين يكتشفون وبسرعة وسائل بديلة للتحايل على انفاذ القانون، حيث يمكن لهم استخدام هويات متعددة من خلال استخدام ملفات تعريف متعددة عبر منصات مختلفة على الانترنت¹.

ومن الامثلة الحية على استخدام شبكة الانترنت لتجارة المخدرات موقع الحرير والذي كان اكبر موقع لتجارة المخدرات على شبكة الانترنت، وعلى حسب قول مكتب التحقيقات الفدرالي الامريكي فإن الموقع حقق منذ نشأته عمولات مالية تقدر بحوالي 80 مليار دولار، وتمكنت السلطات الأمريكية من اغلاق الموقع بعد التوصل إلى العديد من التجار مستخدمي الموقع في عدد من الدول كالولايات المتحدة الأمريكية وأستراليا وبريطانيا والسويد، وعلى الرغم من أغلاق الموقع إلا أن معاون صاحب الموقع الأصلي قام بإطلاق موقع طريق الحرير 2 بعد شهر من أغلاق الموقع الأول، وشمل الموقع الجديد قائمة بـ 500 نوع من المخدرات².

2- تجارة تهريب الأسلحة النارية.

تُستخدم الأسلحة النارية كسلعة للتجارة، وترمز إلى السلطة والقوة، وتُستخدم أيضًا كبديل عن الدفع بالبضائع غير الشرعية، مثل المخدرات، بالإضافة إلى ذلك، تؤدي التجارة بالأسلحة

1- رامي متولي القاضي، مكافحة الإجرام المنظم عبر شبكة الأنترنت المظلمة "دراسة تحليله في التشريع المصري"، مقال منشور في المجلة الجنائية القومية، المركز القومي للبحوث الاجتماعية والجنائية، القاهرة مصر، المجلد الرابع و الستون، العدد الثالث نوفمبر 2021، ص 78.

2- رامي متولي القاضي، المرجع السابق، ص 70.

النارية إلى زيادة التمرد والجماعات الإرهابية، مما يؤثر سلبيًا على الاستقرار الإقليمي في المناطق المتضررة، وتسهم التجارة غير الشرعية بالأسلحة النارية في تسليح الجماعات الإجرامية في المناطق الحضرية، وتزيد من العنف المرتبط بالعصابات في العديد من البلدان، وبشكل عام، يرتبط التجارة بالأسلحة النارية وإساءة استخدامها بشكل وثيق بالجماعات الإجرامية والشبكات المنظمات الإجرامية¹.

ويعتبر تهريب الأسلحة أيضًا جريمة رئيسية تستخدمها التنظيمات الإجرامية كمصدر ربح رئيسي، حيث شهدت أسواق الأسلحة السوداء تطورًا كبيرًا في السنوات الأخيرة، وترجع أسباب ازدهار هذا السوق إلى ضعف الرقابة في بعض الدول وعدم مراعاة قواعد السلوك الدولية لبيع السلاح، بالإضافة إلى النزاعات المسلحة في العديد من مناطق العالم، وعلى الرغم من عدم وجود إحصائيات دقيقة حول حجم الإتجار غير المشروع في السلاح، إلا أنه يتجاوز 500 مليون قطعة سلاح على مستوى العالم، و زادت خطورة هذه التجارة على المستوى الوطني والدولي عند قيام التنظيمات الإجرامية المنظمة بتهريب المواد النووية، وتم التأكد من ذلك عندما أعلن وزير الداخلية الألماني في أغسطس 1994 عن ضبط كميات مهربة من مادتي اليورانيوم والبلوتونيوم اللتين تستخدمان في صنع القنابل الذرية، وهنا يتخوف المجتمع الدولي من أنتشار تهريب تلك المواد و وقوعها في أيدي الجماعات الإجرامية الإرهابية².

وتعريف جريمة الاتجار غير المشروع بالأسلحة النارية، وفقا للاتفاقيات الدولية فقد عرفت المادة الثالثة من بروتوكول مكافحة صناعة الأسلحة النارية وأجزائها ومكوناتها والذخيرة والاتجار بها بصورة غير مشروعة لعام 2001، المكمل لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة 2000³، فيعرف السلاح الناري في نص المادة نفسها من البروتوكول

1- أنظر في ذلك لمكتب الامم المتحدة المعني بالمخدرات والجريمة، عبر الموقع الالكتروني التالي، <https://www.unodc.org/e4j/ar/secondary/firearms.html>، تاريخ الاطلاع 2022/12/14، ساعة الدخول 14:30 مساء.

2- علاء زكي، المرجع السابق، ص 218.

3- بروتوكول مكافحة صناعة الأسلحة النارية وأجزائها ومكوناتها والذخيرة والاتجار بها بصورة غير مشروعة لعام 2001، المكمل لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة 2000، المعتمد من ظرف الجمعية العامة للأمم المتحدة يوم 31 ماي 2001، رقم و رمز الوثيقة A/RES/55/255، أن الهدف

الفقرة (أ) على أنه " أي سلاح محمول ذي سبطانة يطلق أو مصمم أو يمكن تحويله بسهولة ليطلق طلقة أو رصاصة أو مقذوفا آخر بفعل مادة متفجرة أو هو مصمم، أو يمكن تحويله بسهولة، ليطلق طلقة أو رصاصة أو مقذوفا آخر بفعل مادة متفجرة، باستثناء الأسلحة النارية العتيقة أو نماذجها المقلدة "، ويقصد بتعبير "الاتجار غير المشروع" في الفقرة (هـ) من نفس المادة على أنها: " استيراد يقصد الأسلحة النارية وأجزائها ومكوناتها والذخيرة أو تصديرها أو اقتناؤها أو بيعها أو تسليمها أو تحريكها أو نقلها من إقليم دولة طرف أو عبره إلى إقليم دولة طرف أخرى إذا كان أي من الدول الأطراف المعنية لا يأذن بذلك وفقا لأحكام هذا البروتوكول، أو إذا كانت الأسلحة النارية غير موسومة بعلامات، منصوص عليها في نص المادة 8 من البروتوكول"¹.

وفيما يتعلق بالمشروع الجزائري فقد قدم مجموعة من النظم القانونية لمنع جرائم الإتجار في الأسلحة النارية غير الشرعية التي يهدف منها لحماية الجزائر من التأثيرات الخطيرة التي يمكن أن تحدثها عملية الإتجار بالأسلحة، حيث صدر الأمر رقم 97-06 في 21 / 01 /

من بروتوكول الأسلحة النارية كما هو مذكور في المادة الثانية هو تشجيع وتسهيل وتعزيز التعاون بين دول الأطراف لمنع ومحاربة وتخليص العالم من الصناعة والتداول غير الشرعي للأسلحة النارية ومكوناتها والذخيرة. يسعى جميع التزامات بروتوكول الأسلحة النارية إلى تحقيق هذا الهدف، ويدعم هذا النهج أهداف اتفاقية الجريمة المنظمة في منع الجريمة وتحقيق العدالة الجنائية بصفة عامة.

و تنص المادة رقم 4 بالوضوح في تحديد نطاق تطبيق البروتوكول، وذلك ليعكس نهج العدالة الجنائية، حيث يشمل منع تصنيع واتجار الأسلحة النارية غير المشروع وأجزائها ومكوناتها والذخيرة، بالإضافة إلى التحقيق وملاحقة مرتكبي الجرائم التي تم تحديدها في المادة رقم 5 من البروتوكول، حيث تكون تلك الجرائم على مستوى دولي وتنطوي على عصابات منظمة.

كما تحتوي المادة على تحذير مهم بشأن تطبيقها، وذلك لأنها لا تنطبق على المعاملات بين الدول، وتطبيقها قد يؤثر على حق دولة طرف في اتخاذ إجراء لصالح الأمن القومي وفقاً لميثاق الأمم المتحدة، فإن المعاملات بين الدول هي المعاملات التي تتم بصفة سيادية، وليس التجارية، كان هناك جدل خلال التفاوض على البروتوكول بشأن إدراج بعض التحويلات، وقالت بعض الدول إنها تمثل نفس خطورة التحويل إلى السوق السوداء، لذلك ينبغي أن يخضعوا للقيود الخاصة بالمبيعات التجارية، ومن ناحية أخرى، قدمت بعض الدول آراء مختلفة، مرجحة أن إدراج هذه التحويلات قد يوسع نطاق البروتوكول دون حاجة ويجعل المفاوضات تدخل في مناطق حساسة مرتبطة بمخاوف الأمن القومي.

1- المادة 3 الفقرة (أ) و (هـ)، من بروتوكول مكافحة صناعة الأسلحة النارية وأجزائها ومكوناتها والذخيرة والاتجار بها بصورة غير مشروعة لعام 2001، المرجع السابق.

1997 الذي يتعلق بنظام الأسلحة النارية والذخائر والعتاد الحربي، وقد أقرت الجزائر موافقتها على الاتفاقية الدولية لمكافحة الجريمة المنظمة، وتحديدًا البروتوكول الخاص بمكافحة الاتجار غير الشرعي في الأسلحة النارية، بموجب المرسوم الرئاسي 04-165 الذي تم إصداره في 08 يونيو 2004.

وتفيد التقديرات الدولية إلى أن تجارة الأسلحة عبر الإنترنت يمكن أن تصبح ميدانا وبيئة جاذبة لأعضاء الجماعات الإجرامية المنظمة والأفراد الذين يرغبون في شراء أسلحة نارية دون الكشف عن هويتهم أو لأغراض غير مشروعة، وفي ضوء دراسة أجرتها مؤسسة "RAND Europe" في عام 2017، تقدمت بها إلى الجمعية العامة للأمم المتحدة في عام 2018، لاحظت الحاجة الملحة للتعاون الدولي الجديد من أجل مكافحة بيع الأسلحة غير المشروعة التي أصبحت ممكنة من خلال حجب الهوية في الإنترنت والشبكة الخفية، ويبدو أن حجم مبيعات الأسلحة النارية عبر الشبكة الخفية أقل من حجم مبيعات غيرها من السلع غير المشروعة، ولكن تشير الدراسة إلى أن الأسلحة النارية هي الأكثر شيوعاً بنسبة 42% من جميع السلع المعروضة على الشبكة الخفية، تليها المنتجات الرقمية المتصلة بالأسلحة بنسبة 74%، والذخيرة بنسبة 22%¹.

1- رامي متولي القاضي، المرجع السابق، ص 78.

الفرع الثاني: جريمة الإرهاب الالكتروني.

يتشابه مفهوم الإرهاب والجماعات الإرهابية مع الجريمة المنظمة ويحصل كثيراً الخلط بينهما حيث يسعى كلاهما إلى إفشاء الرعب والخوف، كما أنهما يتفقان في أسلوب العمل والتنظيم، وقد يكون أعضاء المنظمات الإرهابية هم أساساً أعضاء في عصابات الجريمة المنظمة، حيث يسعون للاستفادة من خبراتهم الإجرامية في التخطيط والتنفيذ، إلا أنه مع هذا فإن مفهوم الجريمة المنظمة ذو مدلول واسع لأنها قد تمس بالسياسة في بعض صورها¹.

أولاً: تعريف الإرهاب.

تناولت العديد من الاتفاقيات والمعاهدات الدولية أشكال خاصة ومحددة من الإرهاب، ومنها اتفاقية طوكيو الخاصة بالجرائم والأفعال التي ترتكب على متن الطائرة 1963، واتفاقية لاهاي بشأن مكافحة الاستلاء غير المشروع على الطائرات الموقعة في 1970، واتفاقية مونتريال الخاصة بقمع الأعمال غير المشروعة ضد سلامة الطيران المدني في عام 1971، واتفاقية مكافحة العمليات الإرهابية بواسطة المتفجرات في عام 1997 التي نصت على أن " يرتكب جريمة كل شخص يقوم عمداً، وبصورة غير مشروعة على تسليم، أو وضع، أو تفجير، قذيفة قاتلة في مكان عام، أو إدارة رسمية أو منشآت عامة، أو وسيلة نقل، أو بنية تحتية،..."، إلى غيرها من الاتفاقيات التي تناولت موضوع الإرهاب² على المستوى الدولي.

كما عملت الدول العربية على تناول موضوع الارهاب الدولي في اتفاقياتها حيث دعا مجلس وزراء الداخلية العرب إلى ضرورة وضع استراتيجية أمنية عربية لمكافحة الإرهاب،

1- عبد العزيز بن غرام الله آل جار الله، المرجع السابق، ص 195.

2- عقد المجتمع الدولي العديد من الاتفاقيات الدولية الخاصة بالإرهاب منها ما تم أبرامه في عهد عصبة الأمم المتحدة نذكر على سبيل المثال اتفاقية قمع الاستيلاء غير المشروع على الطائرات، واتفاقية قمع العمال غير المشروعة الموجهة ضد سلامة الطيران المدني لعام 1971 واتفاقية المواد النووي وغيرها من الاتفاقيات، وكانت أول اتفاقية تتناول موضوع الإرهاب على المستوى الدولي في جنيف عام 1973 وسميت اتفاقية جنيف لمنع الإرهاب ومقاومته، وعرفت الأعمال الإرهابية على أنها "الوقائع الإجرامية الموجهة ضد دولة، وهدفها أو طبيعتها هو إثارة الرعب لدى شخصيات محددة في مجموعات أو في الجمهور، ودعت إلى إنشاء محكمة جنائية دولية تنظر في قضايا الإرهاب، إلا أن هذه الاتفاقية لم تصبح نافذة المفعول لعدم تصديقها إلا من دولة واحدة.

وصياغة اتفاقية عربية مشتركة لمكافحة التطرف، وفي أبريل 1998 أبرمت الاتفاقية العربية لمكافحة الإرهاب التي تتكون من ديباجة وأربعة أبواب و42 مادة¹.

وقد عرفته المادة الأولى من الاتفاقية العربية لمكافحة الإرهاب على أنه " كل فعل من أفعال العنف، أو التهديد به، أيا كانت بواعثه، أو أراضه، يعد تنفيذا لمشروع إجرامي فردي، أو جماعي أو بهدف إلقاء الرعب بين الناس، أو ترويعهم أو إيذائهم، أو تعريض حياتهم أو حريتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة، أو بأحد المرافق، أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها، أو تعريض أحد الموارد الوطنية للخطر)².

وتناول الفقه تعريف الإرهاب حيث يرى الدكتور " نبيل حلمي" بأنه " الاستخدام غير المشروع للعنف أو التهديد به بواسطة فرد أو مجموعة أو دولة ضد فرد أو مجموعة أو دولة، ينتج عنه رعب يعرض للخطر أرواحا بشرية أو يهدد حريات أساسية، يكون هدفه الضغط على الجماعة أو الدولة لتغيير سلوكها تجاه موضوع معين".

كما عرفه الدكتور "عبد العزيز سرحان" على أنه " كل اعتداء على الأرواح أو الممتلكات أو الأموال العامة والخاصة، يقع بالمخالفة لأحكام القانون الدولي بمصادرة المختلفة بما في ذلك المادة 83 من النظام الأساسي لمحكمة العدل الدولية، وبذلك يمكن النظر إليه على

1- إسرائ طارق جواد كاظم الجابري، جريمة الإرهاب الإلكتروني "دراسة مقارنة"، أطروحة ماجستير، كلية الحقوق قسم القانون العام، جامعة النهرين، جمهورية العراق، السنة الجامعة 2012، ص 23.

2- المادة الأولى من الاتفاقية العربية لمكافحة الإرهاب، الصادرة عن جامعة الدول العربية في 1998/04/22، والتي صادقت عليها الجزائر طبقا للمرسوم الرئاسي رقم 413/98 المؤرخ في 7 ديسمبر 1998، والمشور في الجريدة الرسمية رقم 1998/93، من دون شك ان ما قامت به الاتفاقية العربية لمكافحة الإرهاب من خلال تعريف ظاهرة الإرهاب نقلة نوعية وتحول من النقاش السياسي إلى القانوني والذي يعتبر في حد ذاته ضمانه لتحقيق تعاون وتنسيق أكثر ما بين الدول الأعضاء، ولكن بالرغم من هذا فغن تعريف الإرهاب جاء فضفاضا في تحديد عناصره حتى انه يفهم من التعريف بأن كل عنف هو من قبيل الإرهاب مما يفتح المجال أمام معاقبة أشخاص لارتكابهم أفعالا لا تعدو أن تكون سليمة وشرعية حتى أن منظمة العفو الدولية اتهمت المنظمة العربية بأن ما جاء في الاتفاقية لا يفي بمتطلبات الشرعية وفيه انتهاك للقانون الدولي الإنساني وحقوق الانسان، للمزيد أنظر في ذلك، لعراية عبد الحميد، فعالية التحالف الدولي في مكافحة الإرهاب، أطروحة لنيل شهادة الدكتوراه تخصص القانون الدولي الجنائي، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، السنة الجامعية 2019، ص 45.

أساس أنه جريمة دولية، أساسها مخالفة القانون الدولي، وهو يقع كذلك تحت طائلة العقاب طبقاً لقوانين سائر الدول".

إضافة إلى ذلك عرفة الدكتور "محمود شريف بسيوني" بأنه " استراتجية عنف محرم دولياً تحفزها بواعث عقائدية، وتتوخى أحداث عنف مرعبة داخل شريحة خاصة من مجتمع معين لتحقيق الوصول إلى السلطة، أو القيام بدعاية لمطلب، أو لمظلمة بغض النظر عما إذا كان مقترفو العنف يعملون من أجل أنفسهم أو نيابة عنهم، أو نيابة عن دولة من الدول"¹.

أما المشرع الأردني فقد قدم تعريفا للإرهاب في نص المادة 147 من قانون العقوبات الأردني المعدل بقانون 54 لسنة 2001، على أنه " استخدام العنف أو التهديد باستخدامه أيا كانت بواعثه و أغراضه يقع تنفيذاً لعمل فردي أو جماعي بهدف الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر إذا كان من شأن ذلك إيقاع الرعب بين الناس و ترويعهم أو تعريض حياتهم للخطر أو إلحاق الضرر بالبيئة أو المرافق أو الأملاك العامة والخاصة أو المرافق الدولية والبعثات الدبلوماسية أو باحتلال أي منها أو الاستيلاء عليها أو تعريض الموارد الوطنية للخطر أو تعطيل تطبيق الدستور والقوانين".

وتناول المشرع الجزائري تعريف الإرهاب في المرسوم التشريعي رقم 03/92 المؤرخ في 1992/09/30 وذلك بقوله أنه " أي مخالفة تستهدف أمن الدولة ووحدة الإقليم، واستقرار المؤسسات وسيرها العادي بواسطة عمل هدفة زرع الخوف في وسط السكان وخلق إنعدام الأمان والمساس بالأشخاص والممتلكات"، كما تناولت المادة 87 مكرر من قانون العقوبات الأمر رقم 95-11 المؤرخ في فبراير 1995 الأفعال التي تعتبر أعمالاً إرهابية أو تخريبية في مفهوم هذا الأمر².

1- توفيق مجاهد، جريمة الإرهاب الإلكتروني في ضوء أحكام الاتفاقية العربية لمكافحة تقنية المعلومات لعام 2010، مقال منشور بمجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، الجزائر، ديسمبر 2018، المجلد 09، العدد 03، ص 80

2- "يعتبر فعلاً إرهابياً أو تخريبياً في مفهوم هذا الأمر، كل فعل يستهدف أمن الدولة و الوحدة الوطنية والسلامة الترابية واستقرار المؤسسات وسيرها العادي عن طريق أي عمل غرضه ما يأتي: - بث الرعب في أوساط وخلق جو انعدام الأمن من خلال الاعتداء المعنوي والجسدي على الأشخاص أو تعريض حياتهم أو

وما يظهر من المادة السابقة أن المشرع الجزائري لم يعط تعريف للإرهاب بل عرفه بتوصيف بعض الأفعال بأنها أعمال إرهابية وتجريمها، شأنه في ذلك شأن الكثير من التشريعات قصد حماية وتحصين الدولة والوحدة الوطنية والسلامة الترابية واستقرار عمل المؤسسات ضد أي عمل إرهابي وهي بالفعل مجالات حيوية، سلامتها من سلامة أركان الدولة، مع ذلك فبعض التصرفات والأفعال لا بد أن تصدر من تنظيم إرهابي حتى يمكن اعتبارها عملا إرهابية، لأنها إن صدرت من قبل أناس عاديين وبشكل عفوي رغم خطورتها مثل قطع الطريق والاحتجاجات الشعبية، والتي لا يمكن أن ترتقي بأي حال من الأحوال لأن تشكل أعمالا إرهابية، كما أن المشرع الجزائري لم يلتفت للوسائل التي تستعملها الجماعات الإرهابية بل ركز على التأثير الذي تسببه من إدخال الرعب في النفوس وبالتالي يمكن القول أن الجانب البارز والذي يركز عليه المشرع الجزائري في تعريف الإرهاب هو الأثر النفسي الذي تخلفه الأعمال الإرهابية¹.

ثانيا: تعريف الإرهاب الإلكتروني.

تسلما منا بفكرة أن مفهوم الإرهاب كمصطلح تقليدي أصبح واضح إلى حد ما، فإن الإرهاب الإلكتروني يُعد من المفاهيم المستحدثة التي لاتزال تحيط بها درجة كبيرة من الغموض، لارتباطه الوثيق بتقنيات نظم المعلومات سواء من حيث وسيلة ارتكابه، أو ومن حيث دور الفاعل فيه وطبيعة سلوكه الإجرامي، فضلا عن ذلك فإن نتائجه تطول أمن المعلومات وتقنية أنظمة المعلومات، بالإضافة إلى ما يتسبب به من أضرار جسيمة واسعة النطاق وعظيمة الآثار.

أمنهم للخطر أو المس بممتلكاتهم، - عرقلة حركة المرور أو حرية التنقل في الطرق والتجمهر أو الاعتصام في الساحات العمومية، - الاعتداء على رموز الأمة والجمهورية ونش أو تدنيس القبور، - الاعتداء على وسائل المواصلات والنقل والملكيات العمومية والخاصة، - الاعتداء على المحيط أو إدخال مادة أو تسريبها في الجو أو في باطن الأرض أو إلقائها عليها أو في المياه بما فيها المياه الإقليمية من شأنها جعل صحة الإنسان أو الحيوان أو البيئة الطبيعية في خطر، - عرقلة عمل السلطات العمومية أو حرية ممارسة العبادة والحريات العامة وسير المؤسسات المساعدة للمرفق العام، - عرقلة سير المؤسسات العمومية أو الاعتداء على حياة أعوانها أو ممتلكاتهم أو عرقلة تطبيق القوانين والتنظيمات"، المادة 87 مكرر من قانون العقوبات الجزائري، المعدلة بالأمر رقم 95-11 المؤرخ في 25 فبراير 1995.

1- لعراية عبد الحميد، المرجع السابق، ص 53.

ويتميز الإرهاب الإلكتروني عن غيره من أنواع الإرهاب، باعتماده على أساليب عصرية متمثلة في استخدام وتوظيف الموارد المعلوماتية و الوسائل الإلكترونية التي أفرزتها حضارة التقنية في عصر المعلومات، حيث تصبح الأنظمة الإلكترونية والبنى التحتية المعلوماتية ذاتها أهدافاً رئيسية للأعمال الإرهابية، وبهذا تزداد خطورة الإرهاب الإلكتروني في الدول المتقدمة والتي تدار بنيتها التحتية بالحواسب الآلية والشبكات المعلوماتية، مما يجعلها هدفاً سهلاً للمال، فبدلاً من استخدام المتفجرات تستطيع الجماعات المنظمة والإرهابية، تدمير البنية التحتية وتحقيق آثار تدميرية تفوق مثيلاتها المستخدم فيها المتفجرات¹.

ويُعد الباحث " Barry Collin " من أوائل من استخدم مصطلح الإرهاب الإلكتروني خلال ثمانينات القرن الماضي، وذلك في دراسة خلص فيها إلى صعوبة وضع تعريف دقيق لظاهرة الإرهاب التكنولوجي سواء من حيث تحديد مفهومة أو الأساليب الملائمة لمواجهته، وكذلك تحديد دور الكمبيوتر والانترنت في العمل الإرهابي، وفي السياق ذاته نبهت الأكاديمية الأمريكية للعلوم في تقريرها المتعلق بأمن الكمبيوتر بالقول " نحن بصدد مخاطر متزايدة بسبب اعتماد الولايات المتحدة على أجهزة الكمبيوتر، مؤكدة أن الإرهابيين باتوا قادرين على إحداث دمار يفوق ما تحدثه الوسائل التقليدية، باستخدام لوحة المفاتيح بدلاً من المتفجرات، محذرة من احتمال وقوع ما وصفته بـ "بيرل هاربر إلكتروني جديد"².

وعلى المستوى الرسمي عرفت وزارة الدفاع الأمريكية الإرهاب الإلكتروني بأنه نشاط إجرامي يخطط له وينفذ باستخدام الحواسيب و وسائل الاتصال، وينتج عنه عنف أو تدمير أو نشر للخوف بين مستعملي الخدمات، بما يؤدي إلى حالة من الاضطراب وانعدام اليقين، وذلك بقصد التأثير على الحكومات أو السكان وحملهم على تبني مواقف أو توجهات سياسية أو اجتماعية معينة، كما وعرفته وكالة المخابرات المركزية الأمريكية على أنه "الإرهاب الإلكتروني

1- حسنين شفيق، الإعلام الجديد والجرائم الإلكترونية " التسريبات، التجسس الإلكتروني، الإرهاب"، دار فكر وفن للطباعة والنشر والتوزيع، مدينة السادس من أكتوبر، مصر، طبعة 2015، ص 20 21.

2- رافعي ربيع، الارهاب الدولي وعلاقته بالجريمة المنظمة (الارهاب الإلكتروني نموذجاً)، مقال منشور بمجلة القانون والعلوم السياسية، معهد الحقوق والعلوم السياسية، المركز الجامعي صالحي أحمد بالنعامة، الجزائر، المجلد رقم 07 العدد رقم 01 جانفي 2021، ص 73.

كل هجوم ذي دوافع سياسية يوجه ضد نظم معلومات الكمبيوتر أو برامجه أو البيانات والمعلومات المخزنة فيه، ويترتب عليه عنف يستهدف الأهداف المدنية، وترتكبه جماعات دون قومية أو عملاء سريين"¹.

إضافة إلى ذلك قدم مركز الدراسات الاستراتيجية والدولية تعريفا للإرهاب الإلكتروني على أنه " استخدام أدوات شبكات الحاسب الآلي لتعطيل البنية التحتية القومية مثل: المواصلات، عمليات الحكومة، الطاقة، تهريب الحكومة، تهريب وأكراه السكان المدنيين"².

وعرفة الدكتور "مارك بوليت" **Maek Pollitt** بأنه " هجوم عمدي تحركه دوافع سياسية ضد نظم المعلومات وبرامج الكمبيوتر والبيانات عن طريق مجموعات فرعية وطنية أو عميل سري يؤدي إلى العنف ضد أهداف غير حربية".

فيما عرفة الدكتور "أحمد فلاح العموش" بأنه " الإرهاب الناجم عن منتجات الحداثة الغربية موجه لتدمير تلك المنجزات الحضارية والثقافية بأساليب إجرامية متطورة ويستهدف المعلومات وأنظمة وبرامج الكمبيوتر والبيانات والتي ينتج عنها ارتكاب عنف ضد أهداف مدنية والتي تقوم بها مجموعات أو عملاء سريون"³.

ثالثا: عناصر الإرهاب الإلكتروني:

لا يمكن الحديث عن الإرهاب بالوسائل الإلكترونية إذا لم تحتوى الأفعال المجرمة فيه على عناصر الإرهاب، فحتى يتحقق الإرهاب يقتضي توافر العناصر التالية:

1- استخدام العنف أو التهديد باستخدامه، ويراد بالعنف العدوان على الأشخاص باستخدام الوسائل الإلكترونية، فالإرهابيون يعتمدون على استخدام وسائل الاتصال وشبكات المعلومات من أجل إرهاب الأشخاص وإلحاق الضرر فيهم وتهديدهم.

1- عادل صادق، استخدام الارهاب الإلكتروني في الصراع الدولي، دار الكتاب الحديث، القاهرة مصر، طبعة 2015، ص 106.

2- رافعي ربيع، المرجع السابق، ص 73.

3- ط د. توفيق مجاهد، المرجع السابق، ص 81.

- 2- أن يقع العنف أو التهديد تنفيذاً لعمل فردي أو جماعي، والمقصود بالعمل الفردي أو الجماعي النية المبيتة التي يتم وضعها وضع التنفيذ، بخطة مدبرة تتم ترجمتها من خلال جهود منسقة بقصد تحقيق الهدف المنشود، وعادة يكون العمل الفردي أو الجماعي في الجريمة الإرهابية مستند إلى الفكر الجيولوجي الذي يحرك سلوك القائمين به.
- 3- أن يكون العنف المُعد له سلفاً أو التهديد باستخدامه، من شأنه بثّ الخوف والفرع في أوساط السكان، أو تعريض سلامتهم وأمنهم للخطر، أو إحداث أضرار بالبيئة أو المرافق والمنشآت العامة أو الخاصة أو الدولية، أو الاستيلاء عليها أو المساس بالموارد الوطنية وتعريضها لأي خطر يهددها.
- 4- أن يكون الهدف من استعمال العنف المخطط له أو التهديد باستخدامه الإخلال بالنظام العام أو تعريض سلامة المجتمع للخطر، وزعزعة السكينة العامة لدى أفراد المجتمع¹.
- كما ويهدف الإرهاب الإلكتروني إلى تحقيق جملة من الأهداف غير المشروعة ويمكن ابراز بعضها كالتالي:

- 4- بثّ الخوف والهلع في نفوس الدول والشعوب.
- 5- المساس بالنظام العام والامن المعلوماتي وزعزعة حالة الطمأنينة العامة.
- 6- تعريض أمن المجتمع وسلامته للخطر.
- 7- إحداث أضرار بالبنى التحتية المعلوماتية أو تدميرها، والإضرار بوسائل الاتصالات وتقنية المعلومات.
- 8- الإضرار بالأموال والمنشآت العامة أو الخاصة.
- 9- تهديد السلطات العامة أو المنظمات الدولية أو ابتزازها أو الانتقام منها.
- 10- جمع الأموال أو الاستيلاء عليها بوسائل غير مشروعة².

1- مصطفى سعد حمد مخلف، جريمة الإرهاب عبر الوسائل الإلكترونية " دراسة مقارنة بين التشريعين الأردني والعراقي"، أطروحة ماجستير، كلية الحقوق قسم القانون العام، جامعة الشرق الأوسط، السنة الجامعة 2017، ص 33.

2- إسراء طارق جواد كاظم الجابري، المرجع السابق، ص 39.

وبناء على ما تم عرضه يتضح أن الإرهاب الإلكتروني يمثل امتدادًا حديثًا لظاهرة الإرهاب التقليدي، غير أنه يتسم بخطورة مضاعفة لاعتماده على النظم والشبكات المعلوماتية كوسيلة وهدف في آن واحد، مما يسمح للجماعات الإرهابية بتنفيذ أعمالها عن بُعد، وبأقل تكلفة، مع تحقيق آثار مدمرة تمس أمن الدول واستقرارها وبنيتها التحتية الحيوية، وقد تنوعت التعريفات الفقهية والدولية والوطنية للإرهاب الإلكتروني، إلا أنها التقت جميعًا حول عناصر أساسية تتمثل في العمدية، والدافع الإيديولوجي أو السياسي، واستخدام الوسائل الإلكترونية لبث الرعب وتهديد النظام العام وتعريض أمن المجتمع للخطر.

الباب الثاني:

جرائم النظم المعلوماتية و

الآليات الدولية لحمايتها.

بعد بيان ماهية جرائم نظم المعلوماتية وتصنيفاتها المختلفة والتصنيف المعتمد في هذه الدراسة، نأتي الآن إلى التفصيل جرائم النظم المعلوماتية، و ببيان مفهومها في ظل اتفاقية بودابست 2001، وعرض أبرز صورها وأساليب ارتكابها، ثم بيان موقف كل من التشريعات الجنائية الداخلية وكيفية مواجهتها ومعالجتها، وسنكتفي بدراسة الجرائم على حسب التشريعات الداخلية لكلاً من المملكة العربية السعودية، والأمارات العربية المتحدة، والجمهورية الجزائرية الديمقراطية الشعبية، والمملكة الاردنية الهاشمية، فيما سنكتفي بالتشريعات الدولية باتفاقية بودابست لعام 2001 و والاتفاقية العربية لمكافحة الجرائم الالكترونية .

ولهذا فقد قمنا بتقسيم هذا الباب إلى فصلين تناولنا في الفصل الاول الجرائم التي ترتكب ضد الانظمة المعلوماتية وهي التي يكون النظام المعلوماتي محلاً لها وتشمل حسب تصنيف اتفاقية بودابست 2001 جريمة الولوج غير المشروع والاعتراض غير المشروع والاتلاف المعلوماتي والاعاقة الخطيرة للنظام المعلوماتي وجريمة اساءة استخدام البيانات والانظمة المعلوماتية، فيما سنتناول في الفصل الثاني الجرائم التي ترتكب بواسطة النظم المعلوماتية وهي كذلك حسب تصنيف اتفاقية بودابست 2001 تشمل كلا من جريمة التزوير المعلوماتي وجريمة الغش المعلوماتي وجريمة اباحية الاطفال عبر الانظمة المعلوماتية وجريمة التعدي على الملكية الفكرية.

الفصل الأول: الجرائم المرتكبة ضد النظم لمعلوماتية.

أن ما يميز جرائم الصنف الأول هو أنها مستحدثة بصفة كاملة، مقارنة بجرائم الصنف الثاني، وهي أفعال تهدد سرية وإتاحة وسلامة البيانات والأنظمة المعلوماتية بالدرجة الأولى، ويمكن أن تقترب لذاتها، كما يمكن أن تقترب كمطية لارتكاب جرائم أخرى، والملاحظ في هذه الجرائم أيضا هو التداخل فيما بينها، بحيث تقترب جريمة بأخرى ويصعب الفصل أو التمييز بينها، سواء من حيث النشاط الجرمي أو المصلحة المستهدفة، الأمر الذي خلق اختلافا في تعامل التشريعات الجنائية معها، وسنتناول في هذا الفصل خمسة أنواع من الجرائم التي تستهدف نظم المعلومات وتشمل جريمة الولوج غير المشروع والاعتراض غير المشروع والاتلاف المعلوماتي والاعاقة الخطيرة للنظام المعلوماتي وجريمة اساءة استخدام البيانات والانظمة المعلوماتية، حيث سنحاول بيان مفهوم كل جريمة من الجرائم سابقة الذكر في ظل اتفاقية بودابست وعرض صورها الفنية والتقنية وكذلك بيان موقف كل من التشريعات الجنائية الداخلية سابقة الذكر منها.

المبحث الأول: جريمة الولوج غير المشروع.

جاء نص المادة الثانية من اتفاقية بودابست حول الجريمة المعلوماتية لعام 2001 خاليا من تعريف صريح لجريمة الولوج غير المشروع، وكذلك المذكرة التفسيرية للاتفاقية لم تعرف الولوج غير المشروع وذكرت على سبيل المثال لا الحصر أفعال القرصنة والسطو والولوج غير المشروع كأهم صور لجريمة الولوج غير المشروع، وبالاستناد إلى نص المادة الثانية¹، والمذكرة التفسيرية للاتفاقية فانه يمكن استنباط تعريف لجريمة الولوج غير المشروع بأنها "أي معالجة آليه للبيانات يقوم بها الشخص عمدا ودون وجه حق تمكنه من الاتصال الحسي مع النظام أو التحكم في نظام التشغيل تحكما كليا أو جزئيا سواء أكانت هذه المعالجة بسيطة أو معقدة"².

1- "تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق، النفاذ الكامل أو الجزئي إلى نظام كوميبيوتر، يجوز لطرف أن يستلزم أن تُرتكب الجريمة عن طريق مخالفة التدابير الأمنية، بنية الحصول على بيانات الكوميبيوتر أو بأي نية غير صادقة أخرى، أو في ارتباط بنظام كوميبيوتر متصل بنظام حاسوبي آخر"، للمزيد أنظر المادة الثانية من اتفاقية بودابست 2001، المرجع السابق.

2- د. مفيدة مباركية، المرجع السابق، ص 87.

كما يعرف فعل الدخول في إطار المعلوماتية بأنه " كافه الأفعال التي تسمح بالولوج إلى النظام المعلوماتي والإحاطة أو السيطرة على المعلومات التي يتكون منها أو الخدمات التي يقدمها"، أو هو إساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مرخص له باستخدامه والدخول إليه للوصول إلى المعلومات والبيانات المخزنة بداخله لاستخدامها في غرض ما، وقد عرف المشرع السعودي الدخول بدون تصريح في المادة الأولى من نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية بأنه "دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني أو نظام معلوماتي، أو شبكة حاسبات آليه غير مصرح لذلك الشخص بالدخول إليها"¹.

وتسعى الغالبية العظمى من التشريعات إلى تجريم الولوج غير المشروع²، ولكن تختلف هذه التشريعات فيما هو مطلوب لتجريم الوصول غير المشروع إلى أنظمة الحاسب الآلي، رغم أنها تتفق على أنه يجب أن يتم ذلك من خلال وسيلة منطقية واحدة تعتمد على استخدام الوسائل الإلكترونية للبحث عن المعلومات والوصول إليها، ومع ذلك، فإنه يجب تحديد مواصفات هذه الطريقة، والتي تأخذ شكل الدخول غير المصرح به أو اعتراض نظام الحاسب الآلي أو البقاء غير المشروع داخل النظام بعد عملية الدخول غير المشروعة، كما يجب تحديد محل الحماية سواء أكانت المعلومات أم النظام أو شبكة المعلومات، إضافة إلى ما يمكن أن ينتج عن الدخول من نتيجة معينة أو لا سواء تمثلت في الحصول على معلومات أو القيام بإتلاف المعلومات أو غيرها من الأفعال غير المشروعة³.

1- المادة الأولى من قانون نظام مكافحة جرائم المعلوماتية السعودي، المرجع السابق.

2- وهنا نشير أن التشريعات العربية عملت على تجريم الدخول بغير تصريح ولكن غالبيتها تستخدم كلمة "دخول" والبعض الآخر يستعمل كلمة "اختراق"، وعلى سبيل المثال استخدمت الكلمتان معا في المادة الأولى فقرة 20 من القانون العربي النموذجي الاسترشادي بشأن مكافحة الجرائم المعلوماتية، وكذلك المادة 394 مكرر من قانون العقوبات الجزائري المعدل، والمادة 02 من قانون مكافحة جرائم تقنية المعلومات الإماراتي الموحد رقم 2 لسنة 2006، وما يعاب على هذه التشريعات استخدامها الكلمتان للدلالة على نفس المعنى، حيث ان الدخول يستخدم عادة لدخول اماكن محمية أو غير محمية، في حين أن كلمة الاختراق تشير فقط إلى دخول الأماكن أو الأنظمة المعلوماتية المحمية ببرامج خاصة، للمزيد أنظر في ذلك، دلخار صلاح بوتاني، المرجع السابق، ص 191.

3- ايمن عبدالله فكري، المرجع السابق، ص 265.

وللوقوف على ثانيا هذه الجريمة سوف نقوم بتفصيل هذا المبحث إلى مطلبين نتناول في الأول تفصيل جريمة الولوج غير المشروع من حيث مفهومها واركائها وصورها، أما المطلب الثاني فقد خصصناه لكيفية معالجة جريمة الولوج غير المشروع على مستوى التشريع الجنائي الوطني ، والثالث معالجة الجريمة على المستوى الدولي.

المطلب الأول: تفصيل جريمة الولوج غير المشروع.

يمتد معنى الولوج في السياق المعلوماتي ليغطي كافة الأفعال والسلوكيات التي تسمح بالولوج إلى منظومة معلوماتية والتحكم في المعطيات والمعلومات التي تتكون منها، أو يمكن تعريفه والتعبير عنه بإساءة استخدام الحاسب الآلي ونظامه وبرمجياته من قبل شخص غير مرخص له باستخدامه أو الدخول إليه للوصول إلى المعلومات والبيانات المخزنة بداخله، وفعل الدخول المقصود هنا هو ذلك الفعل الذي ينطوي على نشاط ذهني يقوم الفاعل به وليس نشاطا ماديا محضا كاقترام أو دخول منزل أو حديقة¹، بل يقصد بالدخول هنا كظاهرة معنوية غير ملموسة تشبه تلك التي نعبر عنها بقولنا التغلغل في أفكار شخص أو قدراته الذهنية، أي الدخول إلى العمليات الذهنية التي يقوم بها النظام المعلوماتي، بالإضافة إلى ذلك لا يشمل هذا الدخول الوقائع الناشئة عن الصدفة المحضة، حيث لا يوجد فعل إيجابي مقصود لإتمام هذا الدخول والذي يستمد عدم مشروعيته من كونه غير مصرح به²، أي أن يكون الدخول بدون وجه حق لمن هم غير مصرح لهم الدخول إلى نظام الحاسب الآلي³.

1- هناك من يفضل استخدام مصطلح الاتصال بنظام المعالجة الآلية بدلا من مصطلح الدخول أو الولوج، هذا لا اعتبارهم أن الاتصال ليس له معنى مادي علا عكس مصطلح الدخول وأن "مصطلح الاتصال" لا يثير الإشكالات التي يثيرها مصطلح الدخول، وبالتالي يبتعد بالنص عن الغموض والخلاف في التفسير، للمزيد أنظر في ذلك، دلخار صلاح بوتاني، المرجع السابق، ص 192.

2- حسين محمد الغول، المرجع السابق، ص 450.

3- نشير إلى الأفعال التي تنطوي على الدخول إلى أحد أجزاء النظام الحاسوبي أو الدخول إلى النظام بأكمله، وذلك بدون تصريح أو مبرر لهذا الدخول، وفي هذا الحالة- على سبيل المثال - يقوم أحد الجناة بالتحايل على برنامج الحماية الخاص بالنظام الحاسوبي لأحد المصارف (على سبيل المثال) من الممكن أيضا أن تتمثل هذه الحالة، عند مواصلة أحد المستخدمين البقاء متصلا مع أحد الأنظمة الحاسوبية بعد انتهاء فترة الأذن الممنوح له/لها، مثل؛ قيام أحد الجناة بحجز سعة الخادم لفترة زمنية محددة، ولكن يستمر في الاستعمال بعد انتهاء الفترة الزمنية المسموح بها، هذا، وتتطلب بعض النهج الوطنية أن يكون تحايل الجاني منصبا على تدابير الحماية أو

وفي هذا السياق يرى الفقه الفرنسي أن مفهوم الدخول يحمل دلالة مزدوجة مادية ومعنوية، فالمدخلول المعنوي يُشبه الدخول إلى النظام المعلوماتي بمثابة الدخول إلى ذاكرة الإنسان، في حين تتجلى الدلالة المادية للدخول فانه يتمثل في أن الشخص يكون قد حاول الدخول أو الوصول الفعلي إلى النظام المعلوماتي، وبناء على التصور المعنوي للدخول، فإن الدخول يتحقق بأي صورة من صور الاعتداء، سواء كان ذلك مباشر أو بشكل غير مباشر، علما بأن الدخول بدون حق في حد ذاته حسب أنصار المدلول المعنوي يعد جريمة وقتية¹، وإن تخلفت عنها بعض الآثار التي تستمر حيزا من الزمن، ولم يحدد المشرع الفرنسي كيفية أو وسيلة الدخول إلى النظام أو اختراقه، وكذلك المشرع العربي في المادة 02 من القانون العربي النموذجي²، ولذلك يجوز الدخول إلى النظام بأي وسيلة تقنية، ومن ذلك انتهاك كلمة السر متى كان الجاني غير مخول في استخدامها، أو من خلال اللجوء إلى تطبيقات و برامج أو شيفرة خاصة، وتتحقق هذه الجريمة من قبل أي فرد بغض النظر عن صفته ومنصبه سواء كان يعمل في الأنظمة المعلوماتية أو لا علاقة له بالحاسب الآلي وشبكاته، وسواء أمتلك الكفاءة التقنية للاستفادة من النظام المعلوماتي أم لا، أذ يكفي ألا يكون من أولئك المخولون والذين لهم الحق في الدخول لهذا النظام³.

ويطلق البعض على هذه الجريمة مسمى جريمة الاختراق المعلوماتي وهي من أهم جرائم المساس بالأنظمة المعلوماتية باعتبار أن اغلب الجرائم لا يمكن ارتكابها إلا بعد الدخول إلى النظام، وبهذا تعتبر هذه الجريمة الحد الفاصل بين الجاني وبين ارتكابه لجريمة أخرى وهو ما

تقترن الأفعال بنية معينة، للمزيد انظر الملحق رقم 02 شرح الأفعال التي تشكل جرائم تدخل في نطاق الجرائم المعلوماتية.

1- L'infraction d'accès frauduleux à un système de traitement automatisé de données se caractérise par le simple fait de pénétrer, sans droit ni autorisation, dans tout ou partie d'un système informatique, indépendamment de la survenance d'un dommage. Le législateur a ainsi entendu protéger le système en tant que tel, en érigeant l'accès non autorisé en infraction autonome, qualifiée de délit formel, dès lors que l'atteinte à la sécurité du système est réalisée par le comportement même de l'auteur, Corinne Robaczewski, Atteinte aux systèmes de traitement automatisé de données, Jurisclasseur pénal code, N 4, LexisNexis, paris, 2013.

2- للمزيد أنظر المادة الثانية من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2011.

3- عبد الفتاح بيومي حجازي، المرجع السابق، ص 356.

جعل الكثير من التشريعات الغربية تجريم الولوج غير المشروع في قوانينها الداخلية¹، وترى في جريمة الولوج غير المشروع الأساس أما باقي الجرائم فما هي إلا نتاج لها وهذا بعد صراع فقهي جدلي حول إضفاء الصفة الجرمية لهذا الفعل من عدمه²، نتج عنه اتجاهين.

الاتجاه الأول: يرى بأنه لا توجد حاجة ضرورية لتجريم الدخول غير المصرح به أو البقاء في أنظمة المعلومات، وخاصة إذا لم يكن لدى الجاني نية إجرامية لارتكاب جرائم بعد الدخول أو البقاء غير المصرح به، وهم يبررون ذلك بأن السلوك ما هو إلا طريقة لإثبات القدرة التقنية والعقلية للشخص الذي نفذ الفعل، فالأمر بحد ذاته لا يشكل جريمة تستوجب معاقبة الفاعل، كما أنه لا يوجد أي ضرر ناتج عن هذا الاختراق من ورائه، ويصعب اكتشافه لأنه لا يترك أي أثر يدل على ذلك³.

الاتجاه الثاني: ويرى بضرورة الحاجة إلى تجريم مثل هذا السلوك حتى لو لم يكن المقصود ارتكاب جريمة في وقت لاحق، ويدعم وجهة نظره بأن الدخول غير المصرح به إلى أنظمة الحاسب الآلي يمكن أن يؤدي إلى خسائر كبيرة، ومن الممكن أن تكون هذه الخسائر

1- ومن التشريعات الغربية التي عملت على تجريم الدخول غير المشروع يمكننا الذكر على سبيل المثال المادة 323 من قانون العقوبات الفرنسي الجديد والمادة الأولى من القانون الانجليزي الخاص بإساءة استخدام الحاسبات الصادر في 1990، والفقرة الأولى من المادة 303 من قانون العقوبات الألماني، والفقرة الثالثة من المادة 370 من قانون العقوبات اليوناني، والمادة 21 من قانون العقوبات السويدي للمعلوماتية لعام 1973، والمواد 7 و 8 من قانون البرتغالي لجرائم المعلومات لعام 1991، والفقرة الأولى من المادة 138 من القانون الهولندي، والفقرة الثانية والرابعة من المادة 76 من قانون العقوبات الاسترالي، والمادة 342 من قانون العقوبات الكندي، والمادة 1030 الفقرة (5) من القانون الفدرالي الأمريكي لإساءة استخدام الحاسبات الآلية في الولايات المتحدة الأمريكية، والمادة 525 من قانون العقوبات التركي، والمادة الثامنة من قانون العقوبات الفنلندي، أنظر في ذلك، د. أيمن عبدالله فكري، المرجع السابق، ص 264.

2- معاشي سميرة، آليات مكافحة الجرائم المعلوماتية، أطروحة دكتوراه تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة محمد خضير بسكرة الجزائر، السنة الجامعية 2020، ص 83.

3- نائلة عادل محمد قورة، المرجع السابق، ص 318، د. نهال عبد القادر المومني، المرجع السابق، ص 157، د. رشيدة بوكر، المرجع السابق، ص 160.

نتيجة مجرد محاولة لمنع هذا الدخول حتى لو لم يتسبب فعليًا في تلف النظام والمعلومات التي يحتوي عليها¹.

إلا أن معظم الفقه يرى ضرورة تجريم فعل الولوج نفسه، لما يترتب عليه من مخاطر وعواقب، لأن الفعل خطوة ضرورية في ارتكاب الجرائم المتبقية الأخرى لنظم المعلومات، وأنه يمكن الوصول إلى معلومات قد تكون مهمة جدا من خلال هذا الفعل، كما هو الحال بالنسبة للمعلومات المتعلقة بأسرار الدولة أو الأسرار العسكرية والمهنية، فإن مجرد الوصول إلى النظام أو البقاء فيه والاطلاع على ما يحتوي عليه يعتبر انتهاكًا لسلامة النظام وسرية المعلومات، حتى لو لم تكن هناك جريمة لاحقة للدخول غير المصرح به، أو حتى لو كان الهدف من هذا السلوك إظهار القدرات الفنية والذهنية.

في حين أن ترك هؤلاء الأشخاص وأولئك الذين يرتكبون مثل هذه الأفعال دون عقاب يمكن أن يؤدي إلى مزيد من الهجمات على أنظمة المعلومات، ولهذا فقد اعترفت التشريعات بخصوصية الوصول غير المصرح به إلى الأنظمة المعلوماتية، وعالجتها من خلال النص على هذه الجريمة وتقنينها أما في قانون العقوبات أو في قوانين خاصة منفصلة، وهناك تشريعات ذهبت إلى أبعد من ذلك من خلال تجريم الدخول غير المصرح به، مع عقوبات أشد إذا أدى ذلك الدخول إلى ضرر لأجهزة تملك النظم المعلوماتية والمعلومات على حد سواء².

ويستفاد من ما تم تقديمه سابقا من النصوص القانونية و الآراء الفقهية حول جريمة الولوج غير المشروع أنها جريمة تقوم على أركان مثلها مثل باقي الجرائم والمتمثلة فيما يأتي:

أولاً: الركن المادي لجريمة الولوج غير المشروع.

تقوم هذه الجريمة بتحقيق فعل الولوج إلى النظام المعلوماتي دون رضا المسؤول عن هذا النظام عن طريق شخص غير مرخص له باستخدامه والدخول إليه، بهدف فتح باب يؤدي إلى

1- نهلال عبد القادر المومني، المرجع السابق، ص 157، د. رشيدة بوكري، المرجع السابق، ص 160، د.

ناثلة عادل محمد قورة، المرجع السابق، ص 317.

2- بوربابة صورية، قواعد الأمن المعلوماتي، أطروحة دكتوراه تخصص علوم قانونية، كلية الحقوق والعلوم السياسية، جامعة الجيلالي الياصب، سيدي بلعباس الجزائر، السنة الجامعية 2016، ص 64.

النظام المعلوماتي بمكوناته المنطقية، والاتصال بطريقة الغش مع النظام بغرض اختراقه كله أو في جزء منه، أو في البقاء في النظام دون وجه حق.

ويعدو الولوج غير المصرح به بأن يكون وصولاً مباشراً إلى المعلومات أو الأنظمة أو الاعتراض غير القانوني للاتصالات من أجل للوصول إلى النظام، أو قد يكون وصولاً غير مباشر من قبل الجاني إلى تلك المعلومات والنظام من خلال نظام آخر متصل بشبكة الاتصالات، والذي يتم تحقيقه من خلال اعتراض النظام الأول، لذلك من المهم ملاحظة أن الدخول غير المشروع إلى شبكة المعلومات لا يهدف دائماً إلى اعتراض الاتصالات في أنظمة الحاسب الآلي، فقد يكون الدخول للاستفادة من مزايا الشبكة دون دفع الرسوم اللازمة، من ناحية أخرى، قد يكون من الممكن اعتراض الاتصالات للوصول إلى المعلومات التي تنقلها دون الدخول إلى شبكة الاتصالات، وهنا نكون أمام الفعل المكون للركن المادي لجريمة الولوج غير المشروع¹.

فالركن المادي في جريمة الولوج غير المشروع يكتمل بحسب اتفاقية بودابست لعام 2001 وكحد أدنى بتحقيق عنصرين اثنين، الأول هو فعل الولوج إلى النظام المعلوماتي ولوجاً كلياً أو جزئياً، والثاني هو أن يكون هذا الولوج بغير وجه حق، ويكتمل كحد أقصى بتحقيق عنصرين آخرين، يمكن للمشرع الداخلي أن يشترطهما في نصوصه الداخلية، يتمثل العنصر الإضافي الأول في تمتع النظام محل الجريمة بالحماية الأمنية، فيما يتمثل العنصر الآخر في كون النظام محل الجريمة متصلاً عن بعد بنظام معلوماتي آخر.

1- المحل في جريمة الولوج غير المشروع.

بالنظر إلى التشريعات في مجال مكافحة جرائم نظم المعلومات، والتي تنطوي على جريمة الولوج غير المشروع، نجد أنها تميز بين ثلاث صور للمحل الذي يقع عليه الولوج غير

1- نائلة عادل قورة، نفس المرجع السابق، ص322.

المشروع الصورة الأولى هي المعلومات نفسها، والصورة الثانية وهي جهاز وأنظمة الحاسب الآلي غير المرتبط فيما بينها بشبكة اتصال، و الصورة الثالثة هي شبكة المعلومات¹.

أ- الاتجاه الأول الاتجاه الموسع.

محل الولوج غير المشروع وفق هذا الاتجاه يجمع بين الصور الثلاث التي أشرنا إليها أعلاه، أي المعلومات والأنظمة الحاسبات، وشبكات المعلومات، فهذا الاتجاه يوسع من محل الدخول غير المصرح به، لذلك أطلق عليه تسمية (الاتجاه الموسع)، وبالتالي فإن التجريم وفق هذا الاتجاه يطال حالات الدخول غير المباشر التي تتم من خلال عملية الاعتراض غير المشروع، ومن ثم الدخول إليها، إلى جانب الدخول إلى المعلومات وأنظمة الحاسبات الآلية التي تتم بصورة مباشرة، فجريمة الولوج غير المشروع _ الدخول بدون تصريح (الدخول غير المصرح به) كثيراً ما تقوم بفعلي الدخول والاعتراض معاً، لأن الدخول إلى المعلومات وأنظمة الحاسب الآلي قد يتحقق بصورة مباشرة عن طريق الحاسب الآلي الذي يتضمن المعلومات والنظام، وقد يتم بصورة غير مباشرة متى دخل الجاني إلى هذه المعلومات والأنظمة بالاستعانة بنظام آخر يتصل بالأول عن طريق شبكة الاتصالات بعد أن يتم اعتراض النظام الأول، وتبعا إلى هذا التوسع نصل إلى نتيجة مؤداها أن النقاط الإشارات الناجمة عن تبادل المعلومات عبر شبكة المعلومات يعد دخولا غير مصرح به إلى النظام المعلوماتي الذي يتضمن هذه المعلومات وفق هذا الاتجاه الموسع لمحل جريمة الدخول غير المصرح به².

1- دلخار صلاح بوتاني، المرجع السابق، ص 192.

2- تجدر الإشارة هنا إلى بعض التشريعات التي اخذت بالاتجاه الموسع لمحل الدخول غير المصرح به ويعد التشريع الجنائي الفرنسي مثالا على هذا الاتجاه إذ تجرم المادة 1/323 من قانون العقوبات الفرنسي لسنة 1992 والمعدل سنة 2002 فعل الدخول غير المصرح به او البقاء بدون تصريح داخل نظام المعالجة الآلية بالمعنى الواسع للكلمة، فهي تقتضي لقيام الجريمة الدخول إلى كل النظام أو إلى جزء منه، ولا تقوم الجريمة بالدخول إلى أي عنصر يحتوي على معلومات متى كان بمعزل عن نظام المعالجة الآلية للمعلومات،

د .دلخار صلاح بوتاني، المرجع السابق، ص 193، حسين محمد الغول، المرجع السابق، 450، نائلة عادل محمد فريد قورة، المرجع السابق، ص 322 و 333.

ب- الاتجاه الثاني الذي يستبعد شبكات المعلومات من نطاق التجريم.

هذا الاتجاه يقصى شبكات المعلومات من كونها محل لجريمة الدخول غير المشروع، ويركز على المعلومات وأنظمة الحاسبات مما يعنى استثناء هذه الشبكات من تجريم الوصول غير المصرح به، ويُعد تشريع المملكة المتحدة واحداً من أبرز النماذج لهذا الاتجاه، حيث تنص المادة الأولى من قانون إساءة استخدام أجهزة الحاسبات الآلية لعام 1990 على الدخول غير المصرح به إلى البرمجيات والمحتويات التي يضمها الجهاز الحاسوبي، كما تضمنت المادة 17 القانون ذاته مجموعة من التعريفات التي تساعد في شرح نصوصه، إلا أنها لم تشمل تحديداً واضحاً لمفهوم الحاسب الآلي أو البرمجيات أو البيانات التي تشكل موضوع جريمة الدخول غير المصرح به، كما أن المادة الأولى لم تحتوى على أي إشارة إلى شبكات المعلومات، ولكنها اقتصرت على البرامج والمعلومات التي يحتوى عليها الحاسب الآلي، أي المعلومات والبرامج الموجودة في وسائط التخزين الداخلي للحاسب الآلي، وينتج عن ذلك استبعاد المعلومات التي يتم نقلها عبر وسائل الاتصالات، وتثير المقالة السابقة بعض التساؤلات حول المقصود بعبارة "أي حاسب آخر" في إشارة إلى المحل الذي يقع عليه فعل الدخول غير المصرح به وظهر ذلك في أول تطبيق عملي لهذا القانون في عام 1991¹.

1- نشير هنا إلى القضية الأولى التي تعامل معها القضاء الانجليزي في عام 1991 وأثارت العديد من التساؤلات حول مصطلح "أي حاسب آخر" الوارد في المادة الأولى من هذا القانون، حيث تتلخص وقائع القضية في قيام أحد العاملين السابقين بأحد المتاجر بزيارة زميلة في العمل لقيامه بشراء بعض المستلزمات من المتجر الذي كان يعمل به، واثتاء انشغال زميلة قام المتهم بإدخال بعض التعليمات إلى نظام الحاسب الآلي يتم بمقتضاها خصم نسبة 70 بالمائة من قيمة البضائع التي كان يريد شراءها، وقدم المتهم إلى المحكمة بتهمة الدخول غير المصرح به إلى نظام الحاسب الآلي تطبيقاً للمادة الأولى من قانون إساءة استخدام الحاسبات الآلية لعام 1990.

إلا أن محكمة أول درجة برأت المتهم من التهمة المنسوبة إليه، وجاء في حكمها " أن العبارات الواردة في المادة الأولى سألغة الذكر تستدعي أن يقع الدخول إلى الحاسب الآلي عن طريق حاسب آلي آخر، وعليه المادة تتطلب أن يكون الدخول غير المصرح به إلى المعلومات والبرامج التي يحتوى عليها أي حاسب آلي وليس الحاسب الآلي الذي يستخدمه المتهم وإلا جاء نص المادة متضمناً تجريم الدخول إلى المعلومات والبرامج التي يحتوى عليها هذا الحاسب الآلي أو أي حاسب آخر"، إلا أن محكمة الاستئناف ألغت الحكم المتقدم، وجاء في حكمها انه " لا يجب تحميل عبارات النص أكثر مما تحتمل، حيث إن النص لم يحدد نطاق تطبيقه بوجوب ان يكون الدخول إلى الحاسب الآلي بواسطة حاسب آلي آخر، وإنما تقوم الجريمة بوجود حاسب آلي واحد وهو

ت-الاتجاه الثالث يجرم الدخول غير المصرح به إلى أنظمة الحاسبات الآلية عبر شبكات المعلومات.

يتمثل هذا الاتجاه في تجريم الدخول غير المصرح به إلى أنظمة الحاسبات الآلية من خلال شبكات المعلومات، ومن التشريعات التي تتبنى هذا الاتجاه القانون الجنائي السويسري المنح الذي قدمه المشرعون السويسريون في عام 1995، حيث تعاقب المادة 143 مكرر ق منه على الدخول غير المصرح به إلى نظام الحاسب الآلي، من خلال أجهزة نقل المعلومات، كما أوضحت المناقشات في الأعمال التحضيرية للقانون أن النص لم يكن يهدف إلى تجريم اعتراض وسائل الاتصال، بل الدخول غير المصرح به إلى الأنظمة الآلية عبر وسائل الاتصال، فهذا النص لا يعالج سوى حالات الدخول بدون تصريح من طرف أفراد من خارج المالكة للنظام، أما الحالات التي تشمل على وصول مباشر للأنظمة، والتي غالباً ما ينفذها موظفو المؤسسة التي تمتلك تلك الأنظمة، فإن النص لا ينطبق عليها ما لم يتم الوصول إلى النظام من خلال شبكة داخلية تتبع بالمؤسسة، بينما ينطبق على الوصول إلى النظام عن طريق التقاط الإشارات المنبعثة أثناء نقل المعلومات، ويتم ذلك باستخدام جهاز ينقل المعلومات¹.

من خلال استعراضنا لهذه الاتجاهات الثلاثة التي اعتمدتها نصوص تشريعية مختلفة لتجريم الدخول غير المشروع، نتبع الرأي الأول وهو الرأي الصحيح والذي يتبنى عدم التمييز بين المحال الثلاث للدخول بدون تصريح، بحيث يجب أن تطل عملية التجريم المحال الثلاث وجميع الأشخاص طالما أنهم يدخلون بدون إذن، وهذا ما تم تأكيده من خلال توصية منظمة التعاون الاقتصادي والتنمية للدول الأعضاء في تقريرها لعام 1986 بشأن جرائم المعلوماتية، بأن تشمل قوانين الدول الأعضاء في الشق الجنائي تجرم الدخول غير المصرح به إلى أنظمة المعلومات والاتصالات والاعتراض دون إذن الشخص المسؤول عن النظام.

المحل الذي ينصب عليه فعل الدخول"، للمزيد انظر في ذلك، د. نائلة عادل محمد فريد قورة، المرجع السابق، ص 326 و 327، أنظر كذلك مشار إليه لدى، د. حسين محمد الغول، المرجع السابق، ص 449.

1- دلخار صلاح بوتاني، المرجع السابق، ص 195.

2- مدى ضرورة خضوع النظام المعلوماتي للحماية الفنية.

يقصد بقواعد الحماية الفنية تلك التدابير التي تطبق للحد من التهديدات العرضية، مثل تلك الناتجة عن الكوارث الطبيعية كالزلازل والحرائق، أو التهديدات العمدية كالمخاطر التي تنشأ عن عملية الولوج والإتلاف غير المشروع التي تستهدف النظام المعلوماتي، ومن أبرز هذه الإجراءات و التدابير تقنيات التشفير واستخدام كلمة السر، ونظام الحماية ضد الاختراق.

إن المدى الذي يجب أن تتم فيه حماية أنظمة المعلومات من الناحية الفنية لضمان حمايتها الجنائية هو موضوع جدل واجتهادات ونزاعات قانونية، فبعض التشريعات تشترط لقيام جريمة الدخول غير المصرح به توفير تدابير الحماية والأمن، مثل التشريع الفيدرالي الأمريكي لعام 1984 ضد جرائم الحاسب الآلي، بينما يرى آخرون أنه غير الضروري توافر شرط الحماية الفنية والأمنية، مثل التشريع السويسري والفرنسي.

أما بالنسبة للمشرع الجزائري فهو لم يشير إطلاقاً إلى هذا الشرط من خلال تعديل قانون العقوبات لسنة 2004 وإنما جرم مجرد الدخول بغش إلى أنظمة المعالجة الآلية للمعطيات في المادة 394 مكرر، وهذا ما سلكته الاتفاقية العربية بشأن جرائم تقنية المعلومات سنة 2010 عندما نصت على هذا الفعل بموجب المادة 01/06¹ ولم تشر إلى شرط الحماية الفنية للنظام المخترق².

وهنا يثور التساؤل ومفاده هل يشترط لتجريم فعل الدخول بدون تصريح إلى النظام المعلوماتي أن يتوافر نظام حماية أمنية؟ بمعنى هل الحماية القانونية تشمل فقط الانظمة المحمية بأجهزة أمان أم تمتد إلى غيرها من الأنظمة؟، لقد نشأ جدل فقهي حاد بشأن مدى استحقاق النظم المعلوماتية غير المحمية بآليات أمنيّة محددة للحماية القانونية الجنائية ضد الدخول غير المصرح به، وقد برز عن هذا الخلاف اتجاهان:

1- تنص المادة 01/06 على "الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به"، للمزيد أنظر المادة 06 من الملحق رقم 01.

2- بورية صورية، المرجع السابق، ص 68.

أ- الاتجاه الأول الرأي المقيد للحماية الجنائية.

يرى مؤيدو هذا الاتجاه بأن النظام الأمني مطلوب، وهو شرط مفترض في جميع الجرائم المتعلقة بالمعلومات، ويشير أنصار هذا الاتجاه أيضًا إلى أنه من غير المعقول توفير الحماية الجنائية للمعلومات المهمة دون أي تدابير أمنية و حماية لازمة، وبالتالي يجب ألا يحمي القانون الجنائي الناس العاديين الذين يفشلون في اتخاذ الاحتياطات اللازمة والضرورية لتوفير الحماية للمعلومات، وبهذا يمكن النظر إلى وجود نظام أمني على أنه التزام مفروض على كل من يقوم بتشغيل نظام معلوماتي¹.

من المهم أن نلاحظ هنا أن المشرعين الفرنسيين جعلوا وجود نظام أمني التزامًا قانونيًا لقيام المسؤولية الجنائية في المادة 29 من قانون عام 1978 بشأن المعلوماتية والحريات، حيث تلزم هذه المادة كل شخص يعمل في نطاق الأتمتة تلتزمه باتخاذ الاحتياطات اللازمة للحفاظ عليها وحمايتها، ولا سيما لمنع تشويهها أو الحصول عليها من قبل أشخاص غير مصرح لهم بالاطلاع عليها.

علاوة على ذلك، ووفقًا لمؤيدي هذا الاتجاه، فإن وجود أنظمة أمنية وتسلسل الجناة عبرها باختراقها، يساعد في التحقق من سير الجريمة التي تحدث عند وجود نية إجرامية وقصد جنائي، حيث يترك هذا التسلسل آثارًا يدل عليه عادة، بل إن اختراق الأنظمة الأمنية يعد دليلًا على وجود القصد الجنائي لمرتكب الفعل².

ب-الاتجاه الثاني الرأي الموسع للحماية الجنائية.

على خلاف ما دعا إليه الرأي الأول، يعتقد أصحاب هذا الاتجاه أن الحماية القانونية والجنائية يجب أن تمتد إلى جميع أنظمة المعالجة المؤتمتة المحمية بأنظمة الأمان وغير المحمية، ويرون أن اقتصار نطاق الحماية الجنائية على الانظمة المحمية فنيا دون الأنظمة

1- بوربابة صورية، نفس المرجع السابق، ص 68.

2- دلخار صلاح بوتاني، المرجع السابق، ص 200، أنظر كذلك نهلا عبد القادر المومني، المرجع السابق، ص 159.

المفتوحة للجمهور مثل الدليل الإلكتروني، من شأنه أن يعمل على زيادة حالات الإفلات من العقاب.

انتقد أنصار هذا الاتجاه مؤيدي الاتجاه الأول، الذي يتطلب توافر أنظمة حماية أمنية لأنه يؤدي إلى تجاهل حالات الدخول إلى أنظمة المعلومات بسبب أخطاء البرمجة أو العيوب الإلكترونية، كما تسبب للمسؤولين عن تأمين النظام ببعض الصعوبات والمشاكل نظراً لأن أنظمة الحماية الأمنية مرتبطة بالجوانب التكنولوجية المتطورة بشكل مستمر، فقد لا تكون وسائل الأمن الحالية هي نفسها في المستقبل، ولا ينبغي اعتبارها بمثابة افتراض لتوافر النية الإجرامية¹، ويرى مؤيدو هذا الاتجاه بأن أنظمة الأمن لا ينبغي أن تكون شرطاً لتجريم الدخول غير المصرح به إلى أنظمة المعلومات، وإنما يمكن اعتبارها قرينة على تحقق القصد الجنائي².

وبالنسبة إلى موقف المشرع الجزائري من هذه المسألة، فبالنظر إلى نص المادة 394 مكرر³ يظهر من الواضح أن المشرع الجزائري قد سائر المشرع الفرنسي في موقفه من عدم اشتراط وجود نظام أمان لنظام المعالجة الآلية للمعطيات حتى تقوم جريمة الدخول غير المصرح به في نظام المعالجة الآلية للمعطيات، وبالتالي فنطاق الحماية القانونية يمتد ليشمل أيضاً الانظمة غير المحمية⁴.

ونحن نؤيد الاتجاه الثاني ونرى أن الحماية الفنية ليست شرطاً حتى تسبغ الحماية الجزائية على النظام، وما يمكن أن نستنتجه مما سبق أن جريمة الدخول غير المصرح به تقوم

1- دلخار صلاح بوتاني، نفس المرجع السابق، ص 201.

2- نهلا عبد القادر المؤمني، المرجع السابق، ص 160، أنظر كذلك، رشيدة بوكري، المرجع السابق، ص 172، مشار إليه لدى د. عبد الفتاح بيومي حجازي، المرجع السابق، ص 351.

3- تنص المادة 394 مكرر على (يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك)، للمزيد أنظر المادة 394 مكرر من قانون العقوبات الجزائري رقم 15/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 156/66 المؤرخ في 1966/06/08 المتضمن قانون العقوبات الجزائري، الجريدة الرسمية عدد 71 لسنة 2004 المعدل والمتمم.

4- معاشي سميرة، المرجع السابق، ص 88.

كجريمة حتى لو لم يكن مالك النظام أو صاحب السيطرة قد تحوط بوسائل حماية فنية لهذا النظام وإن كان من الصعب تصور عدم وجود الحماية الفنية في الوقت الحالي، وعليه فلا يعتد بعنصر الحماية الفنية لنظام المعالجة الآلية كشرط لقيام الجريمة.

3- السلوك الإجرامي .

يعتبر السلوك الإجرامي من أهم دعائم الركن المادي ويتخلفه فلا قيام لأي جريمة، فهو نقطة الالتقاء بين الجرائم التي تكتفي به لقيام الجريمة والجرائم التي تشترط تحقيق نتيجة إجرامية معينة لقيامها، سواء كانت الجريمة تامة أو غير تامة، ويتخذ السلوك الإجرامي في جريمة الدخول غير المصرح به صورتان وهما (سلوك إيجابي يتحقق بفعل الدخول، سلوك سلبي يتحقق بالامتناع ويتمثل بالبقاء داخل النظام)، وسنحاول توضيح الصورتين ضمن التفصيل التالي:

أ- مفهوم الدخول غير المصرح به.

يعتبر الدخول غير المصرح به وكما ذكرنا سابقاً مدخل الجرائم الماسة بنظم المعلومات ولهذا أغلب التشريعات¹ أعطته أهمية كبيرة عن طريق أسبقية التنظيم ولكونه كما ذكرنا باب الولوج إلى الجرائم المعلوماتية الأخرى.

ومصطلح الدخول غير المصرح به هو مصطلح شائع في أغلب التشريعات التي تعاقب على هذه الجريمة وتسمى جريمة الدخول غير القانوني أو الدخول غير المشروع، وتستخدم تشريعات أخرى مصطلح الدخول دون وجه حق، وقد عرفه التشريع الإنجليزي لسنة 1990 وفقاً للمادة 2/17 الدخول بأنه " الدخول إلى البيانات والبرامج الموجودة في جهاز الحاسب الآلي وذلك يجعله ينفذ أي وظيفة، ويمحو أو يغير في البيانات أو البرامج أو بنقل البيانات"، ومن التشريعات العربية التي عرفت الدخول نجد المادة 7/2 من نظام مكافحة جرائم المعلومات السعودي حيث عرفته المادة على أنه " دخول شخص بطريقة متعمدة إلى الحاسب

1- أنظر على سبيل المثال كلاً من المادة 1/323 من قانون العقوبات الفرنسي، المادة 394 مكرر من قانون العقوبات الجزائري، المادة 03 من قانون جرائم نظم المعلومات الأردني، المادة 1/06 من الاتفاقية العربية بشأن جرائم تقنية المعلومات.

الآلي أو موقع الكتروني أو نظام معلوماتي أو شبكة حاسبات آلية غير مصرح لذلك الشخص الدخول إليها"¹.

وحاول الفقه تعريف الدخول، حيث يعرفه بعضهم على أنه "عملية الدخول غير القانوني إلى نظام الحاسب الآلي من قبل أشخاص ودون إذن من الدولة لغرض التجسس والسرقة التخريب وما إلى ذلك من الأعمال غير المشروعة، مع الأخذ في الاعتبار أن لهؤلاء الأشخاص القدرة على نقل أو محو أو إضافة ملفات وبرامج كما لهم القدرة على التحكم في نظام التشغيل وإصدار الأوامر"، وفي تعريف آخر للفقه هو "إساءة استخدام الحاسب الآلي وأنظمتها من طرف شخص غير مرخص له للوصول إلى المعلومات والبيانات المخزنة فيه من أجل المشاهدة أو فقط لغرض الترفيه أو إرضاء الشعور بالنجاح في اختراق جهاز الحاسب الآلي"، أو هو "عملية الدخول غير المصرح به إلى أجهزة الغير وشبكاتهم الإلكترونية من خلال برامج متقدمة يستخدمها كل شخص لديه خبرة في استخدامها".

الملاحظ هنا أن التعريفات السابقة بشأن الدخول متقاربة من بعضها البعض، حيث حاولت قدر المستطاع احتواء هذا السلوك المستحدث المرتبط بالعالم الافتراضي، كما أنها - التعريفات - عملت على ربط الدخول بعبارة عدم التصريح فحسب، دون أن تقوم بتوضيح أو وضع تعريف جامع مانع لها، إضافة إلى ذلك حصرت التعريفات السابقة طرق الدخول إلى النظم المعلوماتية في ثغرات نظام الحماية الذي يدخل المنفذ عبره نتيجة خلل في نظام الأمن، وهذا غير صحيح إذا ما رجعنا إلى مسألة مدى اشتراط نظام الحماية الفنية لقيام جريمة الدخول غير المشروع والذي خرجنا بنتائج سلبية حوله أعلاه².

وفي هذا الصدد أوضحت المذكرة التفسيرية لاتفاقية بودابست أن الدخول غير المصرح به يتألف من الدخول الكامل أو الجزئي إلى نظام الحاسب الآلي³، و بأنه لا عقاب في حالة

1- أنظر المادة الثانية من نظام مكافحة جرائم المعلومات السعودي، المرجع السابق.

2- رشيدة بوبكر، المرجع السابق، ص 180.

3- أنظر المذكرة التفسيرية لاتفاقية بودابست، المرجع السابق، المادة 02 الفقرة 46 يتألف "من الدخول التام أو الجزئي إلى نظام الحاسب المعدات، والمكونات والبيانات المخزنة في النظام المثبت، والدلائل، وبيانات الحركة، والبيانات المرتبطة بالمحتوى، ومع ذلك، لا يشمل هذا المفهوم مجرد إرسال عن طريق البريد الإلكتروني

الدخول المصرح به من مالك النظام أو صاحب الحق وكذلك لا يكون هناك تجريم إذا كان الدخول إلى النظام مجاناً ومتاحاً للجمهور ويكون الولوج في هذه الحالة عملاً مشروعاً، ويقول آخر فإن الضابط أو المعيار الذي على ضوءه يمكن تحديد الدخول كان قد تم بطريقة غير مشروعة ومن تم يمكن تحديد كونه قد تم بصورة مشروعة هو انعدام حق الشخص في الدخول إلى هذا النظام سواء كان هذا الانعدام لكل النظام أو بعضه، وبالنظر إلى المادة الرابعة من اتفاقية بودابست نجد أنها أعطت الحرية للمشرع الداخلي في تجريمه للأفعال غير المشروعة وأكدت على واجب كل دولة طرف أن تجرم ما يلزم من الأفعال غير المشروعة إذا ما ارتكبت عمداً وحددتها على سبيل الحصر¹.

وعليه فإن الدخول بالمعنى المقصود في القانون يغطي جميع أشكال الاختراق غير المشروع للأنظمة المعلوماتية سواء كان هذا الاختراق تم من قبل شخص على الجهاز نفسه أو تم عن بعد، أو بواسطة شبكة الاتصالات، وينبغي على هذا أن جوهر مفهوم عدم مشروعية الدخول يرتبط بشكل أساسي بتحديد الأشخاص المخولين بالدخول بحق أو لهم صلاحية الوصول إلى نظام الحاسوب والنظام المعلوماتي، لذا يتمثل أساس عدم المشروعية للدخول غير المشروع في انعدام سلطة الفاعل (الجاني) في الدخول إلى هذا النظام مع علمه وإدراكه الكامل بذلك².

ب- البقاء داخل النظام بدون تصريح:

يقصد بفعل البقاء بدون تصريح داخل النظام التواجد داخل نظام المعالجة الآلية للحاسب الآلي ضد إرادة الشخص الذي له الحق في التحكم والسيطرة على هذا النظام، أذ يتمثل هذا الفعل في بقاء الجاني داخل النظام³، وتقوم جريمة البقاء بدخول سلمي فبالرغم من دخول الجاني

أو ملف إلى هذا النظام، كما ويشمل "النفاذ" الدخول إلى نظام حاسوب آخر مرتبط من خلال شبكات الاتصالات العامة، أو بنظام إلى نظام على الشبكة ذاتها، مثل الشبكة المحلية أو شبكة إنترنت داخل للمنشأة، أما آلية الاتصال فلا تُعد ذات أهمية جوهرية سواء بالاتصال عن بعد أو عبر وصلات لاسلكية أو من مسافة قريبة.

1- للمزيد انظر المادة الرابعة من اتفاقية بودابست 2001، المرجع السابق.

2- رشيدة بوبكر، المرجع السابق، ص 176.

3- دلخار صلاح بوتاني، المرجع السابق، ص 207.

عرضيا أو عن طريق الخطأ أو على الرغم من علمة بذلك، إلا أنه يرفض الخروج من النظام وتركه وبمعنى آخر يمتنع عن الخروج، لذلك فالنشاط الإجرامي يمثل في هذه الصورة سلوكا سلبيا من الجاني¹.

فالركن المادي لهذه الجريمة لا للدخول إلى النظام وهو الأمر المطلوب والذي تقوم به الجريمة السابقة "الدخول"، إنما الركن المادي لهذه الجريمة يتمثل في وجوب أن يقوم الجاني بسلوك إيجابي ينهي به الاتصال الذي تحقق عن طريق الخطأ، والتزامه برفض القيام بذلك يحقق صورة الفعل الإجرامي، وعليه يعكس الركن المادي عملية إيجابية يُطلب من الجاني إنجازها، ألا وهي قطع الاتصال، في حين يشكل امتناعه عن قطع الاتصال مع النظام بتحقيق السلوك الإجرامي المتطلب لقيام الجريمة، ومن هنا تنتمي هذه الجريمة إلى فئة الانتهاكات الإيجابية التي تتحقق من خلال التقصير أو الامتناع عن الفعل².

ويرى الفقه أن الامتناع عن ترك النظام الذي تم الدخول إليه ليس أساس التجريم، بل أن السلوك الإجرامي البقاء في النظام بعد الدخول فيه، علما أن هذا البقاء غير مصرح به ويشكل سلوكا إيجابيا، وذهب بعض الفقه إلى القول بأن جوهر البقاء هو جوهر الدخول نفسه، وكل ما ينطبق على الدخول ينطبق على البقاء، لكن الاختلاف يكمن في ما إذا كانت الجريمة تحدث في وقت واحد أو تستمر في الحدوث، لذلك يذهب رأي إلى أن جريمة الدخول وجريمة البقاء كلاهما من الجرائم المستمرة زمنياً، في المقابل ويرى آخر أن جريمة الدخول تتسم بالتسلسل في الأفعال وجريمة البقاء مستمرة، و رأي آخر يجد جريمة الدخول جريمة لحظية ذات عواقب ممتدة، وجريمة البقاء جريمة مستمرة بالأساس³.

وتتجلى أهمية تجريم البقاء داخل النظام المعلوماتي في الحالات التي لا يدخل فيه الدخول في حد ذاته في دائرة التجريم، كأن يقع الدخول مثلاً بطريق عرضية أو بالخطأ، ثم

1- عبد الفتاح بيومي حجازي، المرجع السابق، ص 359.

2- رشيدة بوبكر، المرجع السابق، ص 213.

3- عز الدين عثمانى، صور الركن المادي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر، الجزائر، المجلد 09 العدد 06 ديسمبر 2018، ص 614.

يستغل الجاني الفرصة بعد ذلك للحفاظ على بقاءه داخل النظام دون إذن أو تفويض، أو في حالات البقاء داخل النظام المعلوماتي خارج الفترة الزمنية المسموح بها من مالك النظام أو لأهداف غير الهدف المخصص، ومن ثم تبرز الحاجة الملحة لردع مثل هذه التجاوزات، وفي هذا السياق أكدت محكمة النقض الفرنسية بأن استمرار الجاني في استخدام الرقم السري الذي تتيح له بالدخول إلى قاعدة بيانات لمدة تتجاوز العامين، وهذه المدة غير مصرح بها، يشكل جريمة البقاء غير المشروع.

وفي هذا السياق لم يتطرق المشرع الجزائري إلى تحديد دلالة مصطلح البقاء بشكل محدد، إلا أنه يمكن الإشارة إلى أن صياغة المادة 394 مكرر من قانون العقوبات الجزائري أتسمت بالعمومية، حيث جرد المشرع الجزائري فعل البقاء غير المشروع دون أن يحدد حالاته، الأمر الذي يمكنه من احتواء حالات البقاء في الحالات التي يلجأ فيه الجاني إلى البقاء داخل النظام بعد ولوجه إليه عن طريق الخطأ أو الصدفة، أو حالات البقاء التي تتم بطريقة دخول قانونية ومشروعة إلى النظام المعلوماتي غير أنه يتجاوز الجاني لاحقاً حدود النطاق المرخص به من طرف صاحب النظام المعلوماتي ، سواء بتجاوز المدة المحددة أو الخروج عن الحدود المرخص بها¹.

4- عدم التصريح بالدخول.

لكي يعتبر الدخول إلى النظام المعلوماتي سلوكاً غير مشروع ، يجب أن يكون قد تم بدون تصريح أو أساس قانوني يمنح الشخص السلطة والصلاحيات في الدخول إلى النظام، ومن هنا لابد من تحديد الشخص أو الكيان المخولة بمنح تصريح الدخول، وكذلك حالات انعدام التصريح، وهو ما سنتناوله في النقاط التالية.

أ- صاحب الحق في منح التصريح.

1- بطحي نسيم، جريمة الدخول أو البقاء غير المشروع إلي النظام المعلوماتي، مقال منشور بمجلة الفقه والقانون السياسي، مخبر الدراسات القانونية جامعة تيارت، الجزائر، المجلد 01 العدد 01 2019، ص 78.

يطلق عليه في الفقه الفرنسي لقب "صاحب السلطة أو التحكم في النظام"، ويعرف وفق ما ورد في المادة الثانية من الاتفاقية المتعلقة بحماية الافراد في مواجهة نظم المعلومات المعتمدة من طرف المجلس الاوروبي 1981، أنه " كل شخص طبيعي أو معنوي، أو كل سلطة عامة أو كل مؤسسة أو جهاز يملكون السلطة في التصرف بنظام الحاسب الآلي الخاص بهم، وتقرير مضمونة أو محتواه، وكيفية تنظيمه والهدف منه"¹.

والحقيقة إن تحديد صاحب الحق في منح التصريح بالدخول أمر في غاية الأهمية، أذ عن طريقة يتم تنظيم وإدارة النظام وعليه يتوقف قيام الجريمة كونه صاحب الحق في الصريح بالدخول من عدمه، وتحديد الشخص أو الجهة المسؤولة عن النظام التي تسمح بتحديد الأشخاص الذين ينطبق عليهم وصف الدخول بدون تصريح إلى النظام المعلوماتي، فمن يملك حق الدخول إلى النظام هو إما المسؤول أو صاحب السلطة عليه أو من ترخص له بهذا الدخول، وكل ما عدا هؤلاء يعتبر دخولهم غير مصرح به².

ب- حالات عدم التصريح بالدخول.

إن أساس عدم التصريح بالدخول هو انعدام سلطة الفاعل في الدخول إلى النظام المعلوماتي مع علمه بذلك، ويتحقق وصف الدخول غير المصرح به إلى النظام في حالتين هما:

- الحالة الأولى عدم وجود تصريح بالدخول إطلاقاً.

تتجسد هذه الحالة عندما لا يكون للشخص الذي يدخل للنظام أية علاقة به، كونه ليس من الموظفين لدى المؤسسة التي يتبعها النظام أو أنه من الموظفين لدى هذه المؤسسة ولكن طبيعة عمله لا تمنحه الحق في الدخول إلى النظام، بمعنى أن هذا الشخص في كلتا الحالتين لا يملك ترخيصاً بالدخول إلى النظام، بغض النظر عما إذا كان الترخيص يتوقف على دفع

1- أنظر المادة الثانية من الاتفاقية الخاصة بحماية الأفراد في مواجهة نظم المعالجة الآلية للمعلومات ذات الطابع الشخصي المعتمدة من قبل المجلس الأوروبي في 28 يناير 1981.

2- دلخار صلاح بوتاني، نفس المرجع السابق، ص 203.

مبلغ من المال أو على اكتساب عضوية جهة معينة، أو كان الدخول إلى النظام ممنوعاً على الإطلاق¹.

- الحالة الثانية تجاوز تصريح موجود.

تتمثل هذه الحالة في أن من يقوم بالدخول إلى النظام المعلوماتي يملك تصريحاً بذلك لكنه لا يمثل للقيود المنصوص عليها في التصريح، حيث يتجاوز القدر المسموح له بالدخول إليه، وتثير هذه الحالة إشكالات قانونية كبيرة، ففي معظم الحالات يكون الجاني موظفاً للجهة التي دخل نظامها ولكنه تجاوز الحد المسموح له به، بالإضافة إلى مشكلة صعوبة تحديد ما إذا كان العامل قد تجاوز الرخصة الممنوحة له، الأمر الذي يتطلب تفصيلاً دقيقاً لقدرات واختصاصات كل عامل وما إذا كان قد تجاوز تلك القدرات عمداً أو عن طريق الإهمال أو الخطأ والصدفة.

وهذا هو السبب في أن التشريعات في بعض البلدان تجرم الدخول غير المصرح به من قبل موظفي المؤسسات التي يتبعون لها ويعلنون صراحة وعبر تعليمات واضحة داخل المؤسسة تحدد بوضوح من لديه حق الدخول إلى النظام ومن لا يمكنه ذلك.

إضافة إلى ذلك يمكن أن يكون تجاوز التصريح من غير العاملين في المؤسسة التي تعرضت أنظمتها للدخول المتجاوز للتصريح، أي من الآخرين المسموح لهم بالدخول إلى أنظمة معلومات المؤسسة ولكنهم يتجاوزون حدود هذا الإذن، وهذا الفعل يحدث عادة في نطاق مستخدمي شبكة المعلومات العالمية (الانترنت)، فإن الرأي الراجح يذهب إلى أن الدخول هنا يعد بدون تصريح، وقد تعرض القضاء الأمريكي إلى هذه الحالة التي يسميها الفقه و القضاء الأمريكي (معيّار اختبار تأدية الوظيفة) في واحدة من أهم قضايا الجرائم المعلوماتية

1- من التطبيقات القضائية لهذه الحالة قضية ولاية كنساس الأمريكية ضد المواطن "Allen" الذي قام بالدخول بدون تصريح إلى النظام المعلوماتي لشبكة الاتصال الخاصة بشركة الهاتف الجنوبية الغربية وإجراء مكالمات بعيدة المدى مجاناً، وقضية ولاية واشنطن ضد المدعو "Joseph Riley" الذي قام بالدخول بدون تصريح إلى نظام الاتصال الهاتفي لشركة تيلكو وإجراء مكالمات هاتفية مجانية بدون دفع الاشتراك من خلال تخمين كلمات المرور، أنظر في ذلك. د دلخار صلاح بوتاني، المرجع السابق، ص 204.

وهي قضية دودو الإنترنت¹، وما يتضح أن فكرة الدخول غير المشروع تعرف بدلالة المكان بأنها " التسلل إلى داخل النظام المعلوماتي، أم الدخول غير المشروع من حيث الزمان فإنه يتمثل في تجاوز حدود التصريح أو الترخيص داخل النظام والممنوح لفترة زمنية محددة عن طريق تجاوز هذه الفترة الزمنية"².

وخلاصة القول ووفقا لما سبق دراسته يمكننا الخروج بالنقاط التالية:

ت- أن الاختلاف في المفهوم التشريعي للدخول ينعكس على التجريم للدخول غير المصرح به، فالتشريعات التي لم تعرف الدخول تزيد كثيرا عن التشريعات التي عرفته، وبالنظر لواقعنا فإنه المنهج التشريعي الأصح، لأن تجريم الدخول غير المصرح به للنظام المعلوماتي يرتبط بأمور تقنية متطورة ومتغيرة، فتعريف الدخول قد يحد من التجريم لعجز التعريف عن مواكبة واستيعاب المستجدات التكنولوجية.

ث- تعتبر جريمة الدخول إلى نظام معلومات جريمة شكلية، تتحقق بمجرد الدخول إلى نظام معلومات، ولا يتطلب استكمال الركن المادي الدخول إلى المعلومات والبيانات الواردة في النظام أو التسبب في ضرر لمالك هذه البيانات، لأن الغرض من تجريم الدخول غير المصرح به هو حماية سلامة النظام نفسه، وليس سلامة البيانات التي تتم معالجتها، وعليه فإن الفقه يشبه فعل الدخول غير المصرح به إلى النظام المعلوماتي كجريمة نسخ مفتاح المنزل و الدخول دون حق إليه بالرغم من عدم التسبب في ضرر³.

ج- أنه فيما يتعلق بضرورة الحماية الأمنية لنظام المعلومات واختراقها كشرط لجريمة الدخول غير المشروع ، نعتقد أن هذا إجراء شكلي وليس له علاقة بالنموذج القانوني المعمول به، فشكل الدخول غير المصرح به بهذه المتطلبات تؤدي إلى منطق تمييزي في بسط الحماية الجنائية للنظم المعلوماتية، حيث توفر الحماية الجنائية للأنظمة المعلوماتية المحمية بإجراءات أمنية ولا توفرها للأنظمة المعلوماتية غير المحمية بإجراءات أمنية وهذا لا يستقيم مع المنطق القانوني.

1- دلخار صلاح بوتاني، نفس المرجع السابق، ص 204 - 206.

2- عبد الفتاح بيومي حجازي، المرجع السابق، ص 362.

3- بطحي نسيم، المرجع السابق، ص 78.

ثانيا: الركن المعنوي لجريمة الولوج غير المشروع.

الركن المعنوي ويسميه البعض الركن الأدبي للجريمة وهو الإرادة الأثمة التي يقترن بها الفعل سواء اتخذ صوة القصد الجنائي ام صورة الخطاء، أذ أن الجريمة لا تكتمل بوجود الركن المادي ما لم يكن هذا العمل المادي مظهراً لإرادة إنسانية، وتتمثل الإرادة الأثمة في الجرائم العمدية "بالقصد الجنائي"، كما تتمثل في الجرائم غير العمدية بالخطاء، وهو اذا ما كانت النتيجة الحاصلة غير ما أراده الجاني¹.

ومن المتفق عليه أن للركن المعنوي أهمية كبيرة في تحقق الجريمة وكذلك هو الحال بالنسبة لجريمة الولوج غير المشروع إلى النظام المعلوماتي، فالأفعال التي تقوم بها هذه الجريمة يقوم بها كل يوم مستخدمو الأنظمة المعلوماتية، ومن بين هذه الأفعال فإنه لا يمكن تجريم سوى تلك التي يتحقق بشأنها القصد الجنائي، فالركن المعنوي لجريمة الولوج غير المشروع إلى النظام المعلوماتي في الغالبية العظمى من التشريعات التي تناولتها يتخذ صورة القصد الجنائي باعتبارها من الجرائم العمدية²، مع أنها ليست بحاجة إلى ذلك على اعتبار الأصل في الجريمة أنها عمدية والاستثناء التجريم عن طريق الخطاء الذي يكون بحاجة إلى النص عليه بشكل صريح، وما يظهر من حرص المشرعين على النص على أن هذه الجريمة قصدية إلا من باب التأكيد على أن هذه الجريمة لا تقع بصورة الخطاء غير المقصود³، فلا بد أن تكون إرادة الجاني موجهة نحو الفعل الإجرامي، وعليه أن يعلم بأن نشاطه غير مشروع، وأنه يعتدي على صاحب الحق في المعطيات محل الاعتداء ومع ذلك تتجه إرادته إلى ذلك الفعل رغما عن إرادة صاحب الحق في المعطيات والبيانات أو الشخص الذي يتحكم في النظام المعلوماتي⁴.

1- عبد العزيز بن غرم الله آل جار الله، جرائم الأنترنت وعقوبتها وفق نظام مكافحة الجرائم المعلوماتية السعودي دراسة مقارنة، دار الكتاب الجامعي للنشر والتوزيع، الرياض، المملكة العربية السعودية، الطبعة الأولى، 2017، ص 93 94.

2- نائلة عادل محمد فريد قورة، المرجع السابق، ص 364.

3- عبد الإله النوايسة، المرجع السابق، ص 225.

4- عبد الفتاح بيومي حجازي، المرجع السابق، ص 391.

وسوف نتناول هنا عناصر القصد الجنائي المطلوب تحققها في جريمة الولوج غير المشروع إلى النظام المعلوماتي.

1- القصد الجنائي العام لجريمة الولوج غير المشروع.

عبرت النصوص القانونية التي تناولت جريمة الولوج غير المشروع عن القصد الجنائي العام المتطلب لهذه الجريمة بالرغم من الاختلاف في العبارات المستخدمة، وتناولت القصد الجنائي على أنه " النية الجرمية في ارتكاب الجريمة على النحو الذي عرفها به النص القانوني"، ويعتمد تحقق القصد الجنائي العام في هذه الجريمة على توافر عنصري " العلم والإرادة"¹.

أ- العلم:

فالعلم هو ذلك المنصب على جميع عناصر الجريمة ومادياتها، أي أن يعلم الجاني بكل الوقائع التي تعد من عناصر الجريمة وذات الأهمية القانونية في تكوين الجريمة، فالجاني حتى تنطبق عليه المبادئ العامة للركن المعنوي للجريمة ملزم بالإحاطة بكل واقعة قانونية تدخل في تكوين الجريمة ومحيط أحاطه كاملة بالركن المادي للجريمة، ويعلم أن فعله أي موضوع الجريمة ينصب على النظام المعلوماتي بما يتضمنه من معلومات وبرامج وليس على شيء آخر، وأنه ليس له الحق في الدخول أو البقاء في النظام المعلوماتي وخطورة ذلك على المصلحة التي يحميها القانون أي العلم بحقيقة الفعل وخطورته².

فإذا كان الجاني يعتقد وكان اعتقاده مبني على أسباب معقولة أنه يقوم على سبيل المثال بإجراء بعض العمليات الحسابية باستخدام الحاسب الآلي دون أن يتجه علماً أنه يقوم بالدخول والبقاء غير المشروع في نظام معلوماتي³، ورغم أن هذا الافتراض قليل الحدوث واقعياً حيث أن المجرمين في هذا المجال غالباً ما تتوافر لديهم الخبرة التكنولوجية العالية، إلا أنه في حال حدوثه فنحن أما حالة عدم توفر القصد الجنائي لدى الجاني وبالتالي ينتفي عنه

1- حسين محمد الغول، المرجع السابق ص 458.

2- رشيدة بوبكر، المرجع السابق، ص 236.

3- دلخار صلاح بوتاني، المرجع السابق، ص 211.

القصد الجرمي¹، كما ينتفي عنه القصد الجرمي في حالة اعتقاده أنه له تصريح بالدخول أو البقاء أو أن الموقع مفتوح للجمهور وكذلك هو الأمر عند الدخول بالصدفة أو السهو أو الخطاء، وينبغي على الجاني أن يخرج فوراً من النظام عند علمه بأن دخوله غير مصرح به، فإذا امتنع عن ذلك وقع تحت طائلة العقاب لقيام القصد الجنائي لديه منذ اللحظة التي تحقق فيها العلم².

ب- الإرادة:

يعتبر توافر العلم بكافة العناصر التي تشكل الجريمة لدى الجاني غير كاف لقيام القصد الجنائي، بل يجب توافر الإرادة والتي تعرف بأنها الحالة الذهنية والنفسية التي يكتسبها الجاني وقت قيامه بالجريمة، ويمكن تصور هذه الحالة باتخاذ قرار تنفيذ الجريمة واعطاء الأوامر للجسم لإتيان السلوك الاجرامي المكون للجريمة بما يحقق النتيجة المطلوبة³.

وبما أن جريمة الدخول غير المشروع هي من الجرائم الشكلية التي لا تستوجب قصداً جنائياً خاصاً مثل قصد إلحاق الضرر، حيث أن الركن المادي لهذه الجريمة يتحقق تلقائياً بمجرد وقوع فعل الدخول أو البقاء غير المشروع أو الإضافة أو الحذف أو التعديل، وتندرج هذه الجريمة ضمن فئة جرائم الخطر وليست من جرائم الضرر بحيث أن المشرع يستشعر الخطورة النابعة من سلوك الجاني ذاته، فمجرد تعريض البيانات لخطر الاستغلال الاحتمالي يكفي لوصف السلوك بالغير مشروع⁴، ولا ينتظر حصول نتيجة معينة حتى يتم معاقبة الجاني، وفي حال ترتب عن هذه الأفعال نتائج إجرامية معينة يعتبر ذلك ظرفاً مشدداً للعقوبة⁵، وبهذا

1- عبد الإله النوايسة، المرجع السابق، ص 225.

2- رشيدة بوبكر، نفس المرجع السابق، ص 236.

3- رشيدة بوبكر، نفس المرجع السابق، ص 236.

4- « La cybercriminalité identitaire s'inscrit dans une logique de criminalité de danger plutôt que de résultat, dès lors que l'atteinte réside avant tout dans la mise en péril de l'intégrité des systèmes d'information et de la fiabilité de l'identité numérique. L'infraction est ainsi constituée indépendamment de la réalisation d'un préjudice matériel effectif, la simple exposition des données personnelles à un risque d'exploitation frauduleuse suffisant à caractériser le comportement incriminé », Christophe Naudin, *Cybercriminalité identitaire*, Cahiers de la sécurité, n°6, INHES, 2008.

5- للمزيد أنظر في ذلك المادة الثانية من اتفاقية بودابست بشأن مكافحة الجريمة المعلوماتية عام 2001، المرجع السابق.

لا يعتد بالباعث في قيام جريمة الدخول أو البقاء ويبقى القصد الجنائي قائماً بحق الجاني حتى لو كان الباعث على الدخول هو الفضول أو السعي إلى تحقيق الربح المادي أو أثبات القدرة أو الانتصار على النظام، فإن ذلك لا يحول دون القول بتوافر أركان الجريمة في حق هذا الشخص بدخوله للنظام المعلوماتي دون وجه حق أو سند قانوني¹.

2- القصد الجنائي الخاص لجريمة الولوج غير المشروع.

تعد نية الجاني في تحقيق غاية معينة من وراء ارتكاب الجريمة هي جوهر القصد الجنائي الخاص أي توافر باعث معين لدي الجاني، ويلتقي القصد الجنائي الخاص مع القصد الجنائي العام في جميع عناصره ويزيد عنه في تحديد الإرادة الجرمية لدي الجاني إما بباعث معين قد يدفعه إلى الجريمة وإما بنتيجة محددة يريدها الجاني، ولإظهار الفرق بين العام والخاص فإن القصد العام يقوم على العلم والإرادة كما يقوم القصد الخاص على العلم والإرادة، غير انه يمتاز عنه بأن العلم والإرادة فيه لا يقتصران على أركان الجريمة وعناصرها، وانما يمتدان بالإضافة إلى ذلك إلى وقائع ليست في ذاتها من أركان الجريمة، وإذا تطلب القانون في جريمة توافر القصد الخاص فمعنى ذلك أنه يتطلب أولاً انصراف العلم والإرادة إلى أركان الجريمة، وبذلك يتوافر القصد العام ثم يتطلب بعد ذلك انصراف العلم والإرادة إلى وقائع لا تعد طبقاً للقانون من أركان الجريمة، وبهذا الاتجاه الخاص للعلم والإرادة يقوم القصد الخاص².

واشترطت بعض التشريعات التي جرمت جريمة الولوج غير المشروع وجود قصد جنائي خاص إلى جانب القصد العام، مما قد يترتب على توافر هذا الشرط تشديد العقوبة، ومن التشريعات التي نحت هذا المنحنى قانون إساءة استخدام الحاسوب البريطاني لعام 1990، حيث جرمت المادة 1/2 فعل الدخول غير المشروع إلى النظام المعلوماتي بنية ارتكاب جريمة أخرى، ولا يشترط ارتكاب الجريمة الأخرى التي تم دخول النظام المعلوماتي من أجلها، حيث تشدد القانون الانجليزي حيال مرتكبي هذه الجريمة، وسأل الفاعل عن الجريمة سواء ارتكبت الجريمة الأخرى وقت الدخول أو في وقت آخر، كما أن الفاعل يُسأل عن الجريمة حتى لو

1- عبد الفتاح بيومي حجازي، المرجع السابق، ص 391 392.

2- محمد ممدوح بدير، المرجع السابق، ص 103.

تبين أن ارتكاب الجريمة الأخرى أصبح مستحيلاً¹، وكذلك الحال بالنسبة للقانون النرويجي فقد تشدد في عقوبة جريمة الدخول غير المصرح به إذا ارتكبت بغرض الحصول على مكسب غير مشروع لأي شخص.

أما على المستوى الفقهي فقد ثار خلاف بين الفقهاء حول ضرورة توافر القصد الجنائي الخاص في جريمة الولوج غير المشروع، فذهب بعض من الفقهاء الفرنسيين يتزعمهم الفقيه **"Raymond Gassin"** إلى ضرورة توافر القصد الجنائي الخاص في جريمة الدخول غير المشروع والذي يتمثل بالغش حسبهم، ولو كان غرض المشرع الاكتفاء بالقصد العلم كان استعمل عبارة عمداً، ويرون أن الدخول والبقاء غير المشروع يتحققان عندما يكونان بدون رضا صاحب النظام، معتمدين على قرار محكمة باريس الذي اصدرته في 5 أفريل 1994 المتعلق بالدخول والبقاء غير المصرح بهما في النظام المعلوماتي حينما قضت بأن الدخول والبقاء يكون بدون حق مع معرفة السبب، وعليه يخلص هذا الرأي إلى أن الغش يكون عند معرفة الشخص بغياب حق الدخول أو البقاء في النظام المعلوماتي².

أما الرأي الثاني ويتزعمه الفقيه **"Jean Devese"** والذي يرى أن المشرع الفرنسي لم يشترط نية خاصة " فعبارة بدون حق مع معرفة السبب " التي جاءت في حكم محكمة باريس تنصرف في مدلولها على أن الفعل يجب أن لا يكون نتيجة خطأ بسيط، وإنما لا بد أن يكون إتيانه على علم بصفته غير المشروعة، وأن الركن المعنوي يتحقق بتوافر القصد الجنائي العام، وما عبارة عن طريق الغش الواردة في المادة 1/323 من قانون العقوبات الفرنسي إلا وصف يندرج ضمن ماديات الجريمة³.

وخلاصة القول مما تقدم أنه يمكن الاكتفاء بالقصد الجنائي العام لقيام جريمة الولوج غير المشروع دون اشتراط وجود القصد الجنائي الخاص متمثلاً في نية الاضرار أو غيرها من البواعث، لأن اشتراط وجود قصد جنائي خاص يتعارض مع الركن المادي لجريمة الولوج غير

1- عبد الإله النوايسة، المرجع السابق، ص 228.

2- بطحي نسيمية، المرجع السابق، ص 80.

3- رشيدة بوبكر، المرجع السابق، ص 238.

المشروع على اعتبار أنها من الجرائم الشكلية التي لا تستلزم تحقق نتيجة إجرامية كما ذكرنا سابقا.

المطلب الثاني: معالجة جريمة الولوج غير المشروع في التشريع الجنائي.

تتعامل التشريعات الجنائية مع جريمة الولوج غير المشروع بشكل جدي وتفرض عقوبات قانونية على مرتكبيها، وقد تختلف هذه العقوبات من بلد إلى آخر وفقاً للتشريعات المحلية، ولكن عادةً ما تشمل العقوبات المحتملة غرامات مالية وفترات سجن محددة.

ويُعتبر التشريع الجنائي في العديد من البلدان مرجعاً قانونياً هاماً لمعالجة جريمة الولوج غير المشروع، حيث يتضمن التشريع العناصر الأساسية التي تحدد ما يعتبر ولوجاً غير مشروعاً والعقوبات المتوقعة عند ارتكاب هذه الجريمة، وعليه سنوضح كيف عالجت التشريعات الوطنية جريمة الدخول غير المشروع في قوانينها الداخلية.

أولاً: التشريع الجزائري.

لقد أدرك المشرع الجزائري الخطر البالغ الذي ينطوي عن فعل الولوج غير المشروع، من حيث مقدمته لأفعال إجرامية أخرى فأورد جرائم الاعتداء على المنظومة المعلوماتية بمقتضى القانون 04-15 المؤرخ في 10 نوفمبر 2004 في القسم السابع مكرر الذي يحمل عنوان " المساس بأنظمة المعالجة الآلية للمعطيات"، وقد حرص على تجريم فعل الدخول غير المصرح به بحد ذاته لأنه يشكل جريمة، إذ أن مجرد الدخول إلى النظام سواء كان مدفوعاً برغبة الوصول إلى المعلومات والبيانات أو لمجرد الفضول والتسلية هو مخالفة قانونية تشكل تعدياً غير مشروع على النظام المعلوماتي، وجاءت المادة 349 مكرر من قانون العقوبات الجزائري بالنص على عقوبة الحبس من ثلاث أشهر إلى سنة وبغرامة مالية من 50.000 دينار جزائري إلى 100.000 دينار جزائري لكل من يقوم بالدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو حتى مجرد محاولة ذلك¹، كما وشدد العقوبة إذا أسفرت عن هذه الأفعال المذكورة تخريب لنظام تشغيل المنظومة المعلوماتية، لتصبح العقوبة

1- المادة 349 مكرر من قانون العقوبات الجزائري.

السجنية من ستة أشهر إلى عامين ومن 50000 ألف دينار جزائري إلى 150000 دينار جزائري.

والملاحظ من خلال المادة أن المشرع الجزائري قد جرم فعل الدخول والبقاء في النظام المعلوماتي سواء ادي هذا التواجد إلى نتائج معينة أم لم يؤدي أو أي شكل من أشكال الضرر، فإذا حصل الفعل المكون للجريمة وهو الدخول أو البقاء غير المصرح بهما تكتمل الجريمة، وهنا نكون أمام تصنيف الحالة من ضمن الجرائم الشكلية، ولكن الملاحظ أيضا أن المشرع قد أخرج جريمة الدخول والبقاء غير المشروع من طابعها الشكلي إلى طابعها المادي، ويكون ذلك إذا اقترن فعل الجاني بنتيجة مادية محدث نتائج ضارة بالنظام المعلوماتي، وهنا شدد المشرع العقوبة على الجاني في حالة ما إذا إدي هذا الدخول أو البقاء إلى تخريب ومحو أو تعديل لمعطيات هذا النظام¹.

والملاحظ كذلك تأكيد المشرع الجزائري على صورة السلوك لجريمة الولوج غير المشروع بأنه الدخول والبقاء غير المصرح بهما حيث تضمنتهما المادة معا وفي نص واحد، كما يتضح من نص المادة أن المشرع ساير التشريع الغربي في عدم افتراض وجود الحماية الفنية لنظام المعالجة الآلية كشرط لقيام جريمة الولوج غير المشروع، كما أن المشرع الجزائري لم يشترط وجود صفة معينة في الشخص الذي يقوم بعملية الولوج لينطبق عليه وصف جانبا²، كما أن المشرع الجزائري لم يلتفت خلال التجريم و تقدير الجزاء لطبيعة البيانات والأنظمة المستهدفة وبالتالي يكون قد أخضعها لعموم المادة 349 مكرر³.

وبالنظر إلى الركن المعنوي لجريمة الولوج غير المشروع في القانون الجزائري فقد أكدت عليه المادة 349 مكرر من قانون العقوبات الجزائري، مقرة بعمدية جريمة الولوج غير المشروع بنصها " كل من يدخل أو يبقى عن طريق الغش..."، حيث تقوم هذه الجريمة بتوافر القصد الجنائي العام بعنصرية العلم والارادة، ولا تتطلب قصداً جنائياً خاصاً، فيكفي علم الجاني بأن

1- معاشي سميرة، المرجع السابق، ص 102.

2- معاشي سميرة، نفس المرجع السابق، ص 84-91.

3- مفيدة مباركية، المرجع السابق، ص 98.

دخوله للنظام المعلوماتي غير مشروع ولا يستند فيه إلى حق قانوني أو سلطة مستمدة من القانون تمنحه هذا الحق¹.

أما بالنسبة للعقوبة فقد قرر المشرع الجزائري تعديلاً على القسم الرابع مكرر من قانون العقوبات المتضمن المساس بنظم المعالجة الآلية، وذلك بموجب القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، ومس به تشديد عقوبة الغرامة دون المساس بالنصوص التجريمية الواردة في هذا القسم " القسم السابع مكرر من القانون 04-15"، حيث قررت المادة 349 مكرر في فقرتها الأولى عقوبتان أصليتان على مرتكب جريمة الدخول والبقاء غير المشروع، أما الفقرة الثانية فقد شددت العقوبة على هذه الجريمة إذا نجم عنها نتائج معينة، " بقولها تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة"²، وهذا ما يعني ضرورة وجود نتائج معينة يترتب على حدوثها تشديد للعقوبة³، أما العقوبات فقي كالتالي:

• العقوبات الأصلية لجريمة الدخول والبقاء غير المشروع.

ح- العقوبة الأصلية للجريمة في حالتها البسيطة: وتكون هنا في حالة حصول الدخول والبقاء غير المشروع دون إعاقة أو إفساد للنظام أو تعديل أو إزالة للمعلومات، وتكون العقوبة:

أ- الحبس من ثلاثة أشهر إلى سنة وغرامة مالية من 50.000 دينار جزائري إلى 150.000 دينار جزائري.

ب- الغرامة المضاعفة إلى خمس مرات عما هو مقرر للشخص الطبيعي من 250.000 دينار جزائري إلى 100.0000 دينار جزائري في حالة ارتكاب الجريمة من شخص معنوي، وهذا ما أشارت إليه المادة 349 مكرر 4⁴ من قانون العقوبات الجزائري.

1- بعقيقي عبير، مكافحة الجريمة المعلوماتية في التشريعين الجزائري و الإماراتي دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد خضير بسكرة، الجزائر، العام الدراسي 2017-2018، ص 141.

2- أنظر الفقرة الثانية من المادة 349 مكرر من قانون العقوبات الجزائري.

3- رشيدة بوبكر، المرجع السابق، ص 231.

4- تنص المادة 349 مكرر 4 على " يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الأقصى المقرر للشخص الطبيعي".

خ- العقوبة الاصلية للجريمة في حالة التشدد: لقد تشدد المشرع الجزائري في عقوبة جريمة الدخول غير المشروع إذا نجم عن البقاء والدخول نتيجة إجرامية كتغيير لمعطيات النظام او حذف للمعلومات، وهنا ترتفع العقوبة لحدّها الأقصى لتكون كالتالي:

أ- الحبس من 06 أشهر إلى عامين وغرامة مالية من خمسون ألف دينار جزائري إلى مائة وخمسون ألف دينار جزائري.

ب- إذا إدي الدخول والبقاء غير المصرح بهما إلى تخريب النظام فالعقوبة تكون الحبس من أشهر إلى عامين والغرامة من خمسون ألف دينار جزائري إلى ثلاث مائة ألف دينار جزائري.

ت- الحبس من 06 أشهر إلى ثلاث سنوات وبغرامة من خمسمائة ألف دينار جزائري إلى اثنين مليون دينار جزائري في حالة ادخال معطيات للنظام أو ازالة معطيات عن طريق الغش، حسب نص المادة 394 مكرر¹.

ث- بالنسبة للشخص الاعتباري تكون العقوبة الغرامة التي تساوي مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي حسب نص المادة 349 مكرر 4 سابقة الذكر.

• العقوبات التكميلية لجريمة الدخول والبقاء غير المشروع.

د- المصادرة: يظهر من خلال نص المادة 349 مكرر 6 من قانون العقوبات الجزائري أن مصادرة الأجهزة التي يستخدمها الجاني في عملية الدخول غير المشروع تكون وجوبية، أذ تكون محل مصادرة كل وسيلة تستجد مهما كان نوعها أو طبيعتها مخصصة لهذا النوع من الجرائم استخدمت لارتكاب الجريمة، وهنا وجب التنبيه على أن هذه العقوبة لا بد لها أن لا تخل بحقوق الغير حسن النية، كمالك الحاسوب الذي استخدمه الجاني لتخريب نظام المعالجة الآلية للمجني عليه.

ذ- الغلق: ونصت عليه المادة 349 مكرر 6 من قانون العقوبات الجزائري حيث قررت عقوبة الغلق في حالة ارتكاب جريمة الدخول والبقاء غير المشروع لمحل وقوع الجريمة ومكان الاستغلال¹.

1- أنظر نص المادة 349 مكرر 1 من قانون العقوبات الجزائري، المرجع السابق.

وخلاصة القول يبين القانون الجزائري حرص المشرع على حماية الأنظمة المعلوماتية من الولوج غير المشروع، باعتباره جريمة قائمة بذاتها سواء ترتب عنها ضرر أم لا، مع تشديد العقوبة عند إحداث أضرار فعلية للبيانات أو النظام. ويقوم الركن المعنوي على القصد الجنائي العام، حيث يكفي علم الجاني بعدم مشروعية الدخول واتجاه إرادته لارتكاب الفعل، وتعكس العقوبات الأصلية والمشددة والتكميلية توجه المشرع نحو ردع المخالفين وضمان سلامة النظم المعلوماتية، مع مراعاة شمولية التجريم لجميع الأنظمة والبيانات دون اشتراط حماية تقنية أو صفة خاصة للفاعل.

ثانيا: التشريع السعودي.

سعى التشريع السعودي من خلال نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية رقم 17 لسنة 2007 إلى التصدي لجريمة الدخول غير المشروع بنصوص قانونية، بما في ذلك المادة الثالثة في فقرتيها الثانية والثالثة والتي حددت عقوبة الحبس مدة لا تزيد عن سنة وبغرامة لا تزيد عن 500.000 ألف ريال، أو بإحدى هاتين العقوبتين كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

- 1- التصنت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي- دون مسوغ نظامي صحيح - أو التقاطه أو اعتراضه.
- 2- الدخول غير المشروع لتهديد شخص أو ابتزازه، لحملة على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعا.
- 3- الدخول غير المشروع إلى موقع إلكتروني لتغيير تصاميم هذا الموقع، أو إتلافه أو تعديله أو شغل عنوانه...².

1- تنص المادة 349 مكرر6 من قانون العقوبات الجزائري على " مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع اغلاق الموقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم على أغلاق المحل أو مكان استغلال إذا كانت الجريمة قد ارتكبت بعلم مالئها".

2- أنظر المادة الثالثة من نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية.

كما أن المادة الخامسة أضافة عقوبة السجن مدة لا تتجاوز عن الأربع سنوات، والغرامة لا تزيد عن ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين، لكل شخص يرتكب أيا من الجرائم المعلوماتية الآتية- الدخول غير المشروع لإلغاء بيانات خاصة، أو إتلافها، أو تدميرها أو تسريبها، أو محوها، أو تعديلها، أو إعادة تسريبها ونشرها، - إيقاف الشبكة المعلوماتية عن العمل أو إرباكها وتعطيلها أو تدمير ومسح البرامج، أو البيانات الموجودة، إعاقاة الوصول إلى الخدمة أو تشويشها، أو تعطيلها بأي وسيلة كانت.¹، كما أن الفقرة الثانية من المادة السابعة تنص على فرض عقوبة السجن مدة لا تزيد عن عشرة سنوات وبغرامة لا تتعدى خمسة ملايين ريال أو إحدى العقوبتين، لكل شخص يرتكب أيا من الجرائم المعلوماتية الآتية: 2- الدخول غير المشروع إلى موقع إلكتروني أو منظومة معلوماتية بشكل مباشر، أو عبر الشبكة المعلوماتية، أو من خلال أحد أجهزة الحاسب الآلي بهدف الاستحواذ على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني².

والملاحظ من هذه النصوص أنها تجرم الدخول غير المشروع الذي يتم كمقدمة لارتكاب جرائم أخرى أو بنية ارتكاب جرائم أخرى كتهديد شخص أو ابتزازه أو حذف بيانات أو الحصول على معلومات تمس الأمن الداخلي للدولة أو الاقتصاد واقتصرت معاقبتها للدخول المجرد على الدخول غير المشروع إلى موقع إلكتروني والذي عرفته في المادة الأولى فقرة 9 من هذا النظام على أنه " مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد"، وهو ما يعاب على المشرع السعودي.

فالدخول غير المشروع قد لا يكون بنية ارتكاب جريمة أخرى وإنما لمجرد قهر النظام مثلاً، كم إن المشرع قد نص على جريمة الدخول غير المشروع في عدة مواد بينما كان بإمكانه جمعها في مادة واحدة تفادياً للتكرار وسيراً على نهج أغلب المشرعين، كما أنه لم يتطرق إلى فعل أو جريمة البقاء غير المشروع الذي قد يتحقق نتيجة دخول مشروع أو خطأ أو سهو وهو ما يعد نقصاً تشريعياً المشرع مدعو إلى تلافيه، وإن كان المشرع السعودي قد أخذ بالمفهوم

1- المادة الخامسة من نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية.

2- أنظر المادة السابعة من نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية.

الواسع لمحل الدخول الذي يشمل الحاسبات الآلية والمعلومات وشبكات المعلومات وهو ما يحدد عليه¹.

و لكن ما يظهر من نص المشرع السعودي في الفقرة 2 من المادة 7 والتي تنص "الدخول غير المشروع إلى موقع إلكتروني أو نظام معلوماتي مباشرة أو عن طريق الشبكة المعلوماتية، أو إحدى أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني"، أنه اشترط تحقق نتيجة معينة وهو الحصول على معلومات تمس الأمن الداخلي أو الخارجي للدولة، ما يعني ضرورة وجود قصد جنائي خاص بجانب القصد الجنائي العام، وهو قصد الجاني من الدخول غير المشروع للحصول على معلومات تخص الأمن الداخلي أو الخارجي للدولة²، وما نؤيده الاكتفاء بالقصد الجرمي العام بعنصرية العلم والإرادة في تجريم الدخول غير المشروع، حيث متى توافر القصد الجرمي لا مكان للباعث على ارتكاب الجريمة سواء كان الباعث سياسي أو تجاري أو غيره.

أما بالنسبة للعقوبات التكميلية فقد أجاز المشرع السعودي للمحكمة صلاحية إصدار أحكام بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب الجريمة، إلى جانب الأصول المالية المتحصلة منها، كما يتيح للمحكمة الحكم بإغلاق مؤقت أو دائم للموقع الإلكتروني أو جهة تقديم الخدمة في حال ثبت كونها المنشأ الرئيسي لارتكاب الجريمة، وكانت الجريمة ارتكبت بعلم مالكة وهذه الأحكام يجوز فرضها في كل الجرائم المعلوماتية المنصوص عليها في النظام السعودي ومنها الالتقاط أو الاعتراض أو التجسس المعلوماتي وغيرها من الجرائم³.

ثالثاً: التشريع الإماراتي.

لقد تناول المشرع الإماراتي جريمة الولوج غير المشروع في قانون مكافحة تقنية المعلومات لعام 2006 وعبر عنه بمصطلح الوصول العمدي بغير وجه حق إلى النظام، وتناوله بالتجريم

1- دلخار صلاح بوتاني، المرجع السابق، ص 217-218.

2- ضرغام جابر عطوش آل مواش، المرجع السابق، ص 166-180-184.

3- ضرغام جابر عطوش آل مواش، نفس المرجع، ص 192.

في نص كلا المادتين الثانية والرابعة عشر، حيث تنص المادة الثانية من هذا القانون على " إنه كل فعل عمدي توصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي سواء بداخل الموقع أو النظام أو بتجاوز مدخل مصرح به، يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين، فإذا ترتب على الفعل إلغاء أو حذف أو تدمير أو إفشاء أو اتلاف أو تغيير أو إعادة نشر بيانات أو معلومات فيعاقب بالحبس مدة لا تقل عن ستة أشهر وبالغرامة المالية أو بإحدى هاتين العقوبتين..."¹.

والملاحظ أن المشرع الإماراتي جعل من نص المادة الثانية عاماً في التجريم بحيث يشمل كافة الأنظمة المعلوماتية بما فيها المواقع الالكترونية سواء كانت متصلة بالأنظمة والشبكات أو منفصلة، أو كانت تتمتع بالحماية الفنية أم لا، بحيث جعل من الجريمة شكلية لا يلتفت فيها لتحقيق الضرر أو نتيجة معينة، بالإضافة إلى أنها عمدية يكفي لتحقيقها إثبات القصد الجنائي العام دون النظر إلى القصد الجنائي الخاص.

أما المادة الرابعة عشر من نفس القانون سابق الذكر أعلاه فقد نصت على أن " كل من دخل بدون وجه حق موقعاً للشبكة المعلوماتية لتغيير تصاميم هذا الموقع أو إلغائه أو اتلافه أو تعديله أو شغل عنوانه يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين"، وهنا لا يشترط المشرع تحقق النتيجة فعليا بل يكفي أثبات قصد الفاعل في التوصل إليها وإن لم تتحقق النتيجة ما يبقى الجريمة دائماً شكلية².

تلى ذلك إصدار المشرع الإمارات المرسوم بالقانون رقم 05 لعام 2012 لمكافحة جرائم تقنية المعلومات حيث نص في المادة الرابعة منه على أن " يعاقب بالسجن المؤقت والغرامة التي لا تقل عن 250 ألف درهم ولا تتجاوز مليون وخمسمائة ألف درهم، كل من دخل بدون تصريح

1- أنظر المادة الثانية من قانون مكافحة جرائم تقنية المعلومات الاماراتي 2006، وللمزيد انظر في ذلك، عبدالله عبدالكريم عبدالله، جرائم المعلوماتية والانترنت (الجرائم الالكترونية) دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والانترنت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا، منشورات الحلبي الحقوقية، بيروت لبنان، الطبعة الأولى 2007، ص 66 و 67.

2- مفيدة مباركية، المرجع السابق، ص 98، وما وجب التنبيه له أن هذا لقانون السابق الذكر رقم 2006/2 قد تم إلغائه بموجب المرسوم رقم 05 الصادر بعام 2012، وما ذكره الباحث إلا في سبيل إثراء البحث.

إلى موقع إلكتروني أو نظام معلوماتي إلكتروني أو شبكة معلوماتية، أو وسيلة تقنية معلومات سواء كان بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية، وتكون العقوبة السجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تتجاوز مليون درهم، إذا تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر¹.

وبهذا يكون المشرع الإماراتي قد عاقب على الدخول غير المشروع وشدد في العقوبة في حال ما إذا ترتب على الدخول دون وجه حق نشر للبيانات والمعلومات السرية الخاصة بالحكومة والمؤسسات أو الشركات المالية والتجارية والاقتصادية، وتكون العقوبة كما ذكر سابقاً في نص المادة 04 من مرسوم قانون مكافحة جرائم تقنية المعلومات بالحبس مدة لا تقل عن خمس سنوات والغرامة المالية التي قد تصل إلى مليونين درهم إماراتي².

وحديثاً تناول المشرع الإماراتي جريمة الولوج غير المشروع في القانون الجديد لسنة 2021 في المادة الثانية منه تحت عنوان الاختراق الإلكتروني والتي نصت على " 1_ يعاقب بالحبس والغرامة التي لا تقل عن 100,000 مائة ألف درهم ولا تزيد على 300,000 ثلاثمائة ألف درهم، أو بإحدى هاتين العقوبتين، كل من اخترق موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات.

2_ وتكون العقوبة الحبس مدة لا تقل عن 6 ستة أشهر والغرامة التي لا تقل عن 150,000 مائة وخمسون ألف درهم ولا تزيد على 500,000 خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أو الحصول على أي بيانات أو معلومات أو خسارة سريتها.

1- ضرغام جابر عطوش آل مواش، المرجع السابق، ص 167.

2- ضرغام جابر عطوش آل مواش، المرجع السابق، ص 178-180.

3_ وتكون العقوبة الحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن 200,000 مائتي ألف درهم ولا تزيد على 500,000 خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات لتحقيق غرض غير مشروع"¹.

وما يلاحظ على نص المادة الثانية أعلاه أنها حددت المحل في جريمة الولوج غير المشروع بالنسبة للمشرع الإماراتي حيث حددها الموقع الإلكتروني أو النظام المعلوماتي الإلكتروني أو شبكة المعلومات أو وسيلة تقنية معلومات، و اعتبرت ان فعل الاختراق الإلكتروني كافي لقيام الركن المادي لجريمة الولوج غير المشروع ودلالاتنا على ذلك عبارة كل من اخترق وهنا يتضح لنا قصد الدخول بدون تصريح من قبل الجاني إلى النظام المعلوماتي أو الشبكة المعلوماتي.

إلا أنه لم يتطرق لصور الركن المعنوي في جريمة الدخول أو البقاء غير المشروع للنظام المعلوماتي في صورتها المجردة الواردة في المادة الثانية ،وذلك بخلاف ما كان عليه الحال في القانون الاتحادي رقم 02 لسنة 2006 الملغي، والذي عالج الركن المعنوي صراحة، إذ أستهل المشرع الفقرة الأولى من المادة الثانية بعبارة " كل فعل عمدي يتوصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو ..."، ويستفاد من ذلك أن المشرع في القانون الملغي كان أكثر دقة ، حيث قرر عمدية فعل الدخول الغير مشروع إلى النظام المعلوماتي، يعاقب فيها الجاني إذا دخل متعمدا إلى النظام المعلوماتي بشكل غير مشروع، ومع ذلك فإن المادة 43 من قانون العقوبات الاتحادي الاماراتي لعام 2012 لم تميز في العقوبة بين الجريمة العمدية والجريمة غير العمدية².

أما في القانون الجديد لسنة 2021 فيعتبر المشرع الإماراتي جريمة الولوج غير المشروع من الجرائم العمدية التي يتطلب لقيام الركن المعنوي فيها توافر القصد الجنائي العام فقط، ودليل

1- المادة الثانية من قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي لسنة 2021.

2- إبراهيم محمد القاسمي، جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية - وفقا للمرسوم بقانون اتحادي رقم 05 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات وتعديلاته، أطروحة ماجستير في القانون العام، قسم القانون العام كلية القانون، جامعة الامارات العربية المتحدة، الإمارات العربية المتحدة، السنة الدراسية 2018، ص 36 و 39.

ذلك عبارة (كل من أخترق) الوارد ذكرها في الفقرة الأولى من المادة الثانية للدلالة على عمدية جريمة الاختراق الإلكتروني.

أما المادة الثالثة من القانون الجديد لسنة 2021 فتناولت معالجة جريمة الولوج غير المشروع الواقعة على الأنظمة المعلوماتية الخاصة بمؤسسات الدولة حيث نصت على "1_ يعاقب بالسجن المؤقت والغرامة التي لا تقل عن 200,000 مائتي ألف درهم ولا تزيد على 500.000 خمسمائة ألف درهم، كل من اخترق موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات عائدة لمؤسسات الدولة .

2_ وتكون العقوبة السجن مدة لا تقل عن 5 خمس سنوات والغرامة التي لا تقل عن 250.000 مائتين وخمسين ألف درهم ولا تزيد على 1500.000 مليون وخمسمائة ألف درهم، إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات أو خسارة سريتها أو وقعت الجريمة نتيجة لهجمة إلكترونية.

3_ وتكون العقوبة السجن مدة لا تقل عن 7 سنوات والغرامة التي لا تقل عن 250.000 مائتين وخمسين ألف درهم ولا تزيد على 1500.000 مليون وخمسمائة ألف درهم، إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات الخاصة بتلك الجهات المنصوص عليها بالفقرة الأولى من هذه المادة"¹.

ويستفاد من نص المادة الثالثة أن المشرع الإماراتي قد أتجه إلى تشديد السياسة العقابية جريمة الاختراق المعلوماتي متى أنصبت على البيانات والمعلومات العائدة ملكيتها لمؤسسات الدولة، إذ قرر عقوبات سالبة للحرية ومالية مشددة تعكس خطورة المساس بالأنظمة المعلوماتية الحكومية، و أوجب عقوبة السجن مدة لا تقل عن خمس سنوات، وغرامة مالية لا تقل عن مائتين وخمسون ألف درهم ولا تتجاوز مليون وخمسمائة ألف درهم، وذلك متى ترتب على الولوج غير المشروع حدوث ضرر أو تدمير أو إيقاف عن العمل لموقع إلكتروني أو نظام معلوماتي،

1- المادة الثالثة من قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي لسنة 2021.

أو كان هذا الضرر ناتجاً عن هجمة إلكترونية، كما شدد المشرع العقوبة أكثر، فقرر مدة السجن لا تقل عن سبع سنوات، إلى جانب غرامة لا تقل عن مائتين وخمسون ألف درهم ولا تزيد على مليون وخمسمائة ألف درهم، إذا كان الولوج غير المشروع موجهاً بقصد الاستيلاء على بيانات ومعلومات خاصة بالمؤسسات الحكومية التابعة للدولة وذات الطابع السيادي.

أما بالنسبة للعقوبات التكميلية فقد ألزم التشريع الإماراتي المحكمة وجعل من إلزامه وجوباً أن تصدر المحكمة حكم يقضي بأبعاد الأجنبي خارج البلاد في حال الحكم عليه بالحبس وفق أحكام المرسوم سابق الذكر، بعد أن يتم تنفيذ العقوبة المحكوم بها، وإلزام المشرع المحكمة في جميع الأحوال بإصدار حكم يقضي بمصادرة الأجهزة أو البرامج أو الوسائل التي استُخدمت في ارتكاب الجريمة¹، أو الأموال المتحصلة منها، فضلاً عن محو المعلومات أو البيانات أو إعدامها، كما خول التشريع للمحكمة الحكم بإغلاق المحل أو الموقع الذي ترتكب فيه أيّاً من هذه الجرائم، سواء غلقاً كلياً أو للمدة التي تحددها المحكمة².

رابعاً: التشريع الأردني.

قام المشرع الأردني بالنص على هذا السلوك من خلال تجريمه لفعل الدخول غير المصرح به إلى نظام معلوماتي وهذا بقانون مؤقت رقم 30 لسنة 2010 متعلق بجرائم أنظمة المعلومات في المادة الثالثة منه، ونص على عقوبة الدخول غير المصرح به وحدد عقوبته في صورته البسيطة دون المشددة من خلال المادة الثالثة والتي جاءت بالنص " أ- كل من يدخل قصداً موقعاً إلكترونياً أو نظام معلوماتي بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح، يعاقب بالحبس مدة لا تقل عن أسبوع ولا تزيد عن ثلاثة أشهر أو بغرامة مالية لا تقل عن 100 دينار ولا تزيد عن 200 مائتي دينار أو بكليتا العقوبتين"³، والملاحظ هنا أنه المشرع الأردني لم يحدد أو ينص على عقوبة البقاء غير المشروع، وفرض عقوبة على الدخول غير المشروع المجرد بالحبس مدة لا تقل عن أسبوع ولا تزيد عن ثلاثة أشهر أو بغرامة مالية لا تقل

1- للمزيد راجع نص المواد من 56 حتى 60 من قانون مكافحة الشائعات والجرائم المعلوماتية الإماراتي لسنة 2021.

2- ضرغام جابر عطوش آل مواش، المرجع السابق، ص 194.

3- المادة الثالثة من قانون جرائم أنظمة المعلومات الأردني لسنة 2010.

عن 100 دينار ولا تزيد عن 200 دينار أو بـكـلتـا هاتين العقوبتين، وهو بذلك أعطى سلطة تقديره للقاضي في الحكم بالعقوبتين معا أو بإحدهما وكذا الحدين الأقصى والأدنى على حسب ظروف كل قضية، وهي عقوبة غير رادعة مقارنة بحجم العقوبات المقررة في التشريع الجزائري والسعودي.

أما عقوبة الدخول غير المصرح به في صورتها المشددة لم ينص عليها المشرع الأردني بالصيغة التي نص عليها المشرع الجزائري، وإنما جاء في الفقرة الثانية من المادة الثالثة أنه إذا كان الدخول بهدف إلغاء أو حذف، بما يعنى إذا كان القصد من الدخول وقوع أفعال أخرى مثل إتلاف أو انتحال صفة إلى غير ذلك، فالقصد هنا متوفر منذ البداية وليس مترتب عن نتيجة جرمية، وترتب عنه أضرار تشدد العقوبة، إضافة إلى ذلك يعاقب المشرع الأردني على الدخول غير المصرح به إلى موقع إلكتروني أو نظام معلومات بأي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة للاقتصاد الوطني، فأن العقوبة تتضاعف بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن 500 دينار ولا تزيد عن 50.000 دينار¹.

كما جرم المشرع الأردني الدخول غير المشروع في المادة الثالثة من قانون الجرائم الإلكترونية رقم 27 لسنة 2015 وجاء نص المادة " يعاقب كل من دخل قصداً إلى الشبكة المعلوماتية، أو نظام معلومات بأي وسيلة..."، وهذا يعني أن الدخول غير المشروع يجب أن يكون محلة شبكة معلومات أو نظام معلومات، وهو ما ورد تعريفه في المادة الثانية من نفس القانون بنصها " نظام المعلومات مجموعة من البرامج والأدوات المعدة لإنشاء البيانات أو المعلومات إلكترونياً، أو إرسالها، أو تسليمها أو معالجتها أو تخزينها، أو إدارتها، ويقصد بالشبكة المعلوماتية ارتباط بين أكثر من نظام معلومات لإتاحة البيانات والمعلومات والحصول عليها"²، وما يمكن ملاحظة على المشرع الأردني أنه جرم الدخول غير المشروع المجرد، كما أنه لم

1- بوربابة سورية، نفس المرجع السابق، ص 184-185.

2- المادة الثالثة من قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015، منشور على الصفحة رقم 6531 من الجريدة الرسمية عدد 5343 بتاريخ 01/06/2015.

يشترط وجوب توافر الحماية الفنية للنظام المعلوماتي حتى تكفل له الحماية الجزائية وجاء خاليا من هذا الشرط¹.

المطلب الثالث: معالجة جريمة الولوج غير المشروع في التشريع الدولي.

وسوف نتناول معالجة جريمة الولوج غير المشروع عبر إطرارات قانونية دولية واتفاقيات دولية، الهدف منها تعزيز التعاون الدولي لمكافحة جريمة الولوج غير المشروع وحماية نظم المعلومات والتي سنوجزها في النقطتين الاتيتين وهما اتفاقية بودابست والاتفاقية العربية لمكافحة الجرائم المعلوماتية:

أولاً: جريمة الولوج غير المشروع في اتفاقية بودابست:

لقد تناولت اتفاقية بودابست² جريمة الولوج غير المشروع في المادة الثانية منها حيث نصت على أنه "يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية، وفقاً لقانونه الداخلي، الولوج العمدي لكل جزء من

1- عبد الإله النوايسة، المرجع السابق، ص 207-208.

2- لم تكن هذا الاتفاقية نتيجة مصادفة بين دوله الأعضاء، بل سبقتها مراحل أولية واجتماعات عدة بين هذه الدول لرسم الخطوط الرئيسية التي يمكن من خلالها الوصول إلى صورة واضحة لمكافحة هذه الجرائم بجوانبها الموضوعية و الإجرائية، وفي عام 1999، اجتمع وزراء العدل والداخلية لدول مجموعة الثماني في موسكو وطلبوا من ممثلهم تطوير خيارات وحلول عملية تسمح بالكشف عن الاتصالات الإلكترونية الدولية ومراقبتها في إطار التحقيقات الجنائية، وخلال اجتماعهم في أوكيناوا اليابان عام 2000 وضع الخبراء أول مقترحاتهم التي لاقت بدورها قبولا لدى مسؤولي الدول الثمانية، وفي عام 2001 طلب وزير العدل والداخلية للخبراء الثمانية البارزين من الاجتماع الذي عقد في ميلانو، وضع توصيات بشأن مراقبة المجرمين على شبكة المعلومات، مع مراعاة احترام الحقوق الأساسية مثل حماية المعلومات الشخصية والحريات الفردية، وقد جعل وقوع أحداث سبتمبر 2001 هذا العمل أكثر إلحاحاً وأسرع، لأن الإرهابيين يمكنهم استخدام المواقع الإلكترونية والرسائل الإلكترونية وغيرها من وسائل الاتصال التقنية المتقدمة لتنفيذ خططهم ونشر المعلومات ونقلها في القارات المختلفة حتى يتم اكتشافها. يصبح صعباً أو مستحيلاً، وتعتبر هذه الاتفاقية أول اتفاقية دولية في مجال مكافحة الجرائم الإلكترونية والحاسوبية، حيث يعتبر هدفها الأساسي خلق انسجام بين القوانين الجنائية الداخلية للدول ووضع قانون جنائي إجرائي يتيح التحقيق والملاحقة القضائية للمخالفات وخلق تعاون دولي فعال لمحاربة مثل هذه الجرائم، للمزيد أنظر في ذلك، نادر عبد الكريم الغزواني، الحماية الجنائية من جرائم الانترنت دراسة مقارنة، بدون دار نشر، تونس، 2017، ص 154 155 وما يليهما.

جهاز الحاسب بدون حق، كما يمكن له أن يشترط أن ترتكب الجريمة من خلال إنتهاك إجراءات الأمن، بنية الحصول على بيانات الحاسب أو أية نية إجرامية أخرى، أو أن ترتكب الجريمة في حاسب آلي يكون متصلاً عن بعد بحسب آخر¹.

في ضوء المادة أعلاه، من الواضح أن اتفاقية بودابست قد اعتبرت أن جريمة الوصول غير المشروع هي الجريمة الأصلية التي تتطوي على تهديد وانتهاك لأمن سرية وسلامة وتوافر نظم المعلومات والبيانات، لأن هناك حاجة إلى حماية كافية لمصالح المنظمات، خاصة لموظفي الإدارة حتى يتمكنوا من الإدارة والاستثمار ويتحكمون في أنظمتهم دون تدخل أو إعاقة من أي نوع، وبالتالي فإن مجرد الدخول غير المصرح به أو القرصنة أو السرقة لنظام المعلومات يعتبر عملاً غير قانوني في حد ذاته كمبدأ عام².

وفقاً لذلك، فإن الطريقة الأكثر فعالية لمنع الوصول غير المصرح به هي، بالطبع ، تقديم وتطوير تدابير أمنية فعالة، والتي تشمل استجابة شاملة للتهديد باستخدام تدابير القانون الجنائي لمنع الوصول غير المصرح به وتوفير حماية إضافية للنظام والبيانات الموجودة بحد ذاتها في مرحلة مبكرة ضد المخاطر المذكورة أعلاه.

وفي هذا الصدد، تجدر الإشارة إلى أن العديد من القوانين الوطنية تحتوي بالفعل على أحكام بشأن جرائم الدخول والدخول غير القانونيين، لكن نطاقها وعناصرها المكونة تختلف اختلافاً كبيراً في هيكلها، والنهج الواسع للتجريم المشار إليه في الفقرة الأولى من المادة الثانية من اتفاقية بودابست المذكورة أعلاه تعتبر مشكلة، ولكن المعارضة تنشأ من الحالات التي لا تنجم فيها المخاطر عن مجرد الدخول غير القانوني، أو التي تؤدي فيها أعمال القرصنة والاختراق والدخول إلى الكشف عن نقاط الضعف في الأنظمة، مما دفع مجموعة من الدول إلى تبني النهج الضيق الذي يفرض شروط مؤهلة إضافية³، وهو النهج الذي تم اعتماده في التوصية رقم "89" 9 واقترحه الفريق العامل لمنظمة التعاون الاقتصادي والتنمية في عام 1985¹.

1- أنظر الملحق رقم 01 المادة الثانية من اتفاقية بودابست 2001 .

2- طارق أبراهيم الدسوقي عطيه، المرجع السابق، ص 303.

3- بالنسبة للتشريع الذي يفرض شروطاً أمنية على جريمة الدخول غير المشروع، فنستشهد على سبيل المثال، بالقانون النرويجي والهولندي والسويسري، لكن هذه التشريعات اختلفت في تعريف هذه الشروط، فمنهم من

والملاحظ أيضا أن الاتفاقية قد اعطت للأطراف أمكانية اتباع نهج واسع وتجريم الدخول والاختراق ببساطة وفقاً للجملة الأولى من المادة الثانية، هذه، لتشمل، كليا أو جزئيا، العناصر المؤهلة المدرجة في الجملة الثانية: خرق الضمانات والتدابير الأمنية، والنية الشخصية للحصول على بيانات الكمبيوتر أو أي نية أخرى غير شريفة تبرر المسؤولية الجنائية أو تتطلب ارتكاب جريمة ذات صلة بنظام الكمبيوتر متصل عن بعد بنظام كمبيوتر آخر، وهنا يسمح هذا الخيار الأخير للأطراف باستبعاد الحالة التي ينفذ فيها الشخص الدخول مادياً إلى جهاز كمبيوتر مستقل دون استخدام أي نظام كمبيوتر آخر، كما و أجازت للأطراف الحد من هذا الخرق من خلال تقييد هذه الجريمة بالدخول غير المشروع إلى أنظمة الحاسوب الشبكية بما في ذلك الشبكات العمومية والشبكات الخاصة الداخلية والخارجية "إنترنت، إكسترنات".

حيث تشير المذكرة التفسيرية، في توضيحها لمصطلح الوصول غير المشروع، أن مناط التجريم يقتضي أن يتم فعل الوصول بدون وجه حق، مما يعني انتفاء المسؤولية الجنائية في الحالات التي يكون فيها الدخول مصرحاً به من قبل مالك النظام أو من يملك جزءاً منه أو يتمتع بحق عليه، كما هو الشأن في حالات الاختبار أو الحماية المأذون بها للنظام محل الدخول،

اعتبرها خرق الحماية المحيطة بهذه البيانات، في حين رأت بعض التشريعات أن البيانات التي يتم الوصول إليها يجب أن تكون مشمولة بحماية مثل هذه الإجراءات الأمنية، بغض النظر عما إذا كان هناك انتهاك فعلي لهذه الإجراءات أم لا، للمزيد أنظر في ذلك، د نائلة عادل قورة، المرجع السابق، ص 356 و 357.

1- أنظر التقرير التفسيري لاتفاقية بودابست " التقرير التفسيري لاتفاقية الجريمة الالكترونية، المعتمد من قبل مجلس أوروبا في تاريخ 2001/11/8 في المؤتمر الدولي حول الجريمة الالكترونية، وبالإضافة إلى النصوص السابقة فقد تم معالجة جريمة الولوج غير المشروع في العديد من الاتفاقيات والمؤتمرات الدولية ومنها، اتفاقية الاتحاد الافريقي 2012 بشأن إنشاء إطار قانوني للمساعدة في الامن السيبراني في أفريقيا في المواد 15 و 16، اتفاقية السوق المشتركة لشرق وجنوب افريقيا 2011 مشروع القانون النموذجي بشأن الامن السيبراني في المواد 18 و 19، و كومنولث اتحاد الدول المستقلة 2001 اتفاقية بشأن التعاون في مكافحة الجرائم المتعلقة بالمعلومات الحاسوبية في المواد 5 و 7، والبروتوكول الاختياري لاتفاقية بودابست 2001 المادة 2، والجماعة الاقتصادية لدول غرب افريقيا 2009 مشوع توجيهي بشأن مكافحة الجريمة السيبرانية داخل دول غرب أفريقيا في المواد 2 و 3، ومجلس اوربا 2005 القرار افطاري للمجلس 2005/222/JHA بشأن الهجمات ضد نظم المعلومات في المادة 2 فقرة 1، والاتحاد الاوروبي من خلال المشروع النهائي التوجيهي للجنة التنفيذية 2010/073 بالبرلمان الاوروبي ومجلس اوربا بشأن الهجمات ضد نظم المعلومات وإلغاء القرار الإطاري للمجلس 2005/222/JHA في المادة 03، والاتحاد الدولي للاتصالات الجماعة الكاريبية 2010 بشأن الجريمة السيبرانية CTU/CQRICO/ITU في المواد 4 و 5.

وعلى ذات النهج لا تقوم الجريمة إذا كان الوصول إلى النظام متاحاً ومجانياً لعامة الجمهور إذ يغدو الوصول في هذه الحالة حقاً مشروعاً¹.

وعلى كل حال فإن الجرائم الناتجة عن فعل الدخول غير المشروع للنظم المعلوماتية متشعبة وكثيرة ومنها ما قد يسبب ضرراً كبيراً ومنها ما قد يتوقف على الاطلاع على البيانات والمعلومات فقط، ويعود أمر تكييف هذه الجرائم لمشريعي الدول الاطراف في الاتفاقية ولهم السلطة التقديرية في تكييف فعل الدخول غير المشروع و فرض العقوبة على الجاني حسب ما تقرضه حاجتهم لحماية أمنهم الداخلي و الوطني.

ثانياً: جريمة الولوج غير المشروع في الاتفاقية العربية.

تناولت الاتفاقية العربية لمكافحة الجرائم المعلوماتية جريمة الولوج غير المشروع وطالبت بتشديد عقوبتها في المادة السادسة منها، حيث فصلتها إلى جريمتين وهما جريمة الدخول أو الاتصال غير المشروع وجريمة البقاء والاستمرار في الاتصال، وجاء نص المادة كالتالي "جريمة الدخول غير المشروع:

- ر- الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.
- ز- تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال، أ- محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين، ب- الحصول على معلومات حكومية سرية"².

أما القانون العربي النموذجي لمكافحة جرائم المعلوماتية فقد واجه جريمة الدخول بدون تصريح وذلك في المادة الثالثة منه وعرفها على أنها " كل من دخل عمدا وبغير وجه حق موقعا أو نظاما معلوماتيا يعاقب بالحبس ... والغرامة أو بإحدى هاتين العقوبتين.

1- أيمن عبدالله فكري، المرجع السابق، ص 289.

2- المادة السادسة من الاتفاقية العربية لمكافحة الجرائم المعلوماتية.

فإذا كان الدخول بقصد إلغاء أو حذف أو تدمير أو أفشاء أو اتلاف أو تغيير أو بإعادة نشر بيانات أو معلومات شخصيه يكون الحد الأدنى لعقوبة الحبس ... و لعقوبة الغرامة ...¹.

وما يلاحظ على المادة الثالثة أنها حددت محل جريمة الولوج غير المشروع "الموقع الالكتروني أو النظام المعلوماتي" بشكل عام، وأكدت على تشديد العقوبة متى ما كانت غاية الفعل العمد إلى إلغاء البيانات أو تعريضها للإتلاف، أو استغلال الولوج غير المشروع من أجل استغلال معلومات شخصية بهدف تحقيق منفعة ذاتية².

كما ورد تعريف الاختراق في المادة الأولى منه على أنه " الدخول غير المصرح به أو غير المشروع لنظام المعالجة الآلية للبيانات، وذلك عن طريق انتهاك الإجراءات الأمنية"، وهذا ما يعنى ضرورة تأمين النظام المعلوماتي الذي تم اختراقه، إلا أن صياغة المادة الثانية من نفس القانون لم توجي بضرورة تمتع النظام بالحماية الأمنية حتى تقوم الجريمة في حق الجاني.

وفي نفس السياق يلاحظ أن المشرع يعاقب على الدخول المجرد إلى النظام المعلوماتي، ذلك ان مجرد الدخول إلى النظام تقوم به الجريمة حتى لو لم يترتب على دخوله ضرر أو يتحقق له من وراء الدخول فائدة طالما أن الدخول غير مشروع³.

1- المادة الثالثة من القانون العربي النموذجي لمكافحة جرائم المعلوماتية.

2- بعقيقي عبير، المرجع السابق، ص292.

3- عبد الفتاح بيومي حجازي، المرجع السابق، ص 356.

المبحث الثاني: جريمة الاعتراض غير المشروع.

بما أن تبادل المعلومات والبيانات عبر الوسائل الإلكترونية وشبكات الاتصال أصبح أمراً مشاعاً جداً في وقتنا هذا واعتماد غالبية الدول على شبكات الاتصال والأنترنت في إدارة جميع قطاعات الدولة المختلفة، فإنه من الطبيعي أن نلاحظ ازدياداً مقابلاً في السلوكيات غير المشروعة التي تهدف إلى اعتراض واختراق النظم المعلوماتية أو الاستحواذ عليها و أو إعاقة سيرها.

والاعتراض يمكن تعريفه على أنه "رصد الاشارات الكهرومغناطيسية في الانظمة المعلوماتية وتحليلها بهدف استرجاع المعلومات المفهومة او المقروءة منها"، كما يشمل التنصت أو نقل البيانات التي تتم داخل جهاز الحاسب أو عبر جهازين عن بعد عبر الشبكات المعلوماتية المختلفة¹.

وفي هذا الشأن لم تقدم المادة الثالثة من اتفاقية بودابست 2001 ولا المذكرة التفسيرية لها تعريفاً خاصاً ودقيقاً لجريمة الاعتراض غير المشروع، وهنا نؤيد التعريف الذي تبنته الدكتوراة مفيدة مباركية وعرفت الاعتراض غير المشروع من خلاله على أنه " كل معالجة آليه للبيانات يقوم بها الشخص عمدا دون حق، من أجل الاطلاع على بيانات مرسله عبر وسائل اتصال أو الحيلولة دون وصولها سليمة إلى وجهتها الصحيحة أو إرسال بيانات غير صحيحة، سواء تمت هذه المعالجة في منشأ الرسالة أو في مرفئها أو أثناء تدفقها عبر قناة الاتصال"².

ويقصد بهذه الجريمة كل فعل ينطوي على اعتراض يتم بدون وجه حق لأي معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها³، ويكون الاعتراض لخط سير البيانات بشكل متعمد أو قطع بث أو استقبال بيانات،

1- ضرغام جابر عطوش آل مواش، المرجع السابق، ص 202.

2- مفيدة مباركية، المرجع السابق، ص 110.

3- في هذا الشأن نشير إلى تعريف القانون الجمهوري الأمريكي رقم 10175 والمعروف ايضا بقانون منع الجرائم الالكترونية حيث ورد تعريف جريمة الاعتراض غير المشروع في القاعدة الثانية منه تحت عنوان الافعال والعقوبات التي يعاقب عليها (الجرائم الالكترونية)، كالتالي " الاعتراض غير القانوني - الاعتراض الذي يتم بوسائل تقنية وبدون حق، لأي نقل غير عام لبيانات الكمبيوتر إلى نظام كمبيوتر أو منه أو داخله، بما في ذلك

وذلك باستخدام وسائل تقنية توجه لنظام الحاسب الآلي أو عدة نظم أو شبكة اتصالات¹، وبهذا يكون الاعتراض غير قانوني ومتعمد وبدون حق بواسطة وسائل تكنولوجيا للبيانات المرسله أو الاشعاعات الكهرومغناطيسية المنبعثة من أو إلى نظام الحاسوب².

وهنا يختلف الدخول غير المصرح به إلى نظام المعلوماتية عن اعتراض هذا النظام من حيث طبيعة السلوك الإجرامي في كل منهما، فالدخول إلى النظام يفترض قيام الجاني بتشغيله أو الدخول إلى ما يحتوي عليه من معلومات، أما في حالة اعتراض النظام فإن عملية تشغيله تكون قد بدأت بالفعل بواسطة شخص آخر غير الجاني، ويقتصر دور هذا الأخير على النقاط أو اعتراض عملية الاتصال الجارية بغرض الوصول إلى المعلومات التي تتضمنها عملية الإتصال.

أفضت هذه التناقضات بين جريمة الدخول إلى نظام المعلوماتية وبين جريمة اعتراضه إلى الاتجاه نحو التفرد بنص خاص يجرم كل منهما، وهذا ما أوصى به المجلس الأوروبي بضرورة إدراج قاعدة خاصة تعالج فعل اعتراض أنظمة المعلوماتية، يُجرم بمقتضاها كل اعتراض لاتصال يتم من أو إلى داخل الأنظمة المعلوماتية عبر شبكات الاتصالات، ونتيجة لذلك سارت

الانبعاثات الكهرومغناطيسية من نظام كمبيوتر يحمل بيانات الكمبيوتر هذه: بشرط، مع ذلك، أن لا يجوز للمسؤول أو الموظف أو وكيل مزود الخدمة، الذي تُستخدم مرافقه في نقل الاتصالات، أن يعترض تلك الاتصالات أو يكشف عنها أو يستخدمها في سياق العمل العادي، أثناء الانخراط في أي نشاط ضروري لتقديم الخدمة أو لحماية حقوق أو ملكية مقدم الخدمة، باستثناء أنه لا يجوز للأخير استخدام مراقبة الخدمة أو المراقبة العشوائية إلا لأغراض فحص الجودة الميكانيكية أو مراقبة الخدمة"، للمزيد أنظر في ذلك Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012" عبر رابط الموقع الإلكتروني المرفق https://cybercrime.doj.gov.ph/irr/?_cf_chl_tk=NaPB0jAlvbxnJr6NExFagoKcOGExLvbEbF6bUBexQnM-1714424894-0.0.1.1-1493 تاريخ الاطلاع 2024/04/30 الساعة 15:22 مساءً.

- 1- حاتم أحمد محمد بطيخ، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات-دراسة تحليلية مقارنة، مطبوعة صادرة عن جامعة عين شمس، القاهرة مصر، بدون سنة طبع، ص 46 47.
- 2- عبدالله عبد الكريم عبدالله، المرجع السابق، ص 132.

العديد من الدول على هذا النهج ، فأقرت نصوصاً قانونية مستقلة و واضحة تجرم سلوك الاعتراض بصورة محددة ومفصلة¹.

إضافة إلى ذلك يظهر الاختلاف في فكرة الحماية المقررة والبيانات في الجريمتين، فمثلاً أن الهدف من تجريم الولوج غير المشروع إلى الأنظمة المعلوماتية هو حماية البيانات المخزنة داخل الأنظمة المعلوماتية، أما تجريم اعتراض البيانات فإنه يهدف إلى حمايتها أثناء تبادلها ونقلها عبر الأنظمة المعلوماتية الموصولة فيما بينها، والتي غالباً ما تكون موصولة بالإنترنت².

وللوقوف على تفاصيل هذه الجريمة سوف نقوم بتفصيل هذا المبحث إلى ثلاث مطالب نتناول في الأول تفصيل جريمة الاعتراض غير المشروع من حيث مفهومها و أركانها، أما المطلب الثاني فقد خصصناه لكيفية معالجة جريمة الاعتراض غير المشروع على مستوى التشريع الجنائي الوطني والثالث خصصناه لمعالجة الجريمة على المستوى الدولي.

المطلب: تفصيل جريمة الاعتراض غير المشروع.

يتضح الهدف من تجريم الاعتراض غير المشروع هو حماية الحق في احترام نقل البيانات وحماية خصوصيتها³ بغض النظر عن وسائل نقل البيانات سواء كان عن طريق الهاتف أو الفاكس أو البريد الإلكتروني أو نقل الملفات، وإن هذه الجريمة تعد انتهاكاً لهذا الحق، وبهذا فإن جريمة الاعتراض غير المشروع تقوم على مجموعة الأفعال⁴ والسلوكيات الإجرامية غير المشروعة، وكغيرها من الجرائم تقوم على مجموعة من الأركان سنوضحها فيما يلي:

1- عباوي نجاة، الإشكالات القانونية في تجريم الاعتداء على أنظمة المعلومات، مقال منشور بمجلة دفاتر السياسة والقانون، الصادرة عن جامعة قاصدي مرباح، ورقلة الجزائر، العدد 16 المنشور في جانفي 2017، ص 285 286.

2- مفيدة مباركية، المرجع السابق، ص 109.

3- وهنا نرى أن الاعتراض غير المشروع يعد انتهاكاً لحقوق الخصوصية للأفراد والتي يترتب على انتهاكها قيام المسؤولية الجنائية والمدنية، ولهذا يجب أن يكون الأفراد والمنظمات على دراية بالقوانين التي تحكم الاتصالات الإلكترونية والتأكد من حصولهم على الترخيص المناسب قبل مراقبة أو تسجيل أي اتصالات، مع الأخذ بعين الاعتبار الحقوق الفردية المتعلقة بالخصوصية الشخصية.

4- " وهنا نشير إلى الأفعال التي تنطوي على الوصول إلى البيانات الحاسوبية بدون تصريح أو مبرر لذلك، ويتضمن ذلك الحصول على بيانات أثناء إحدى عمليات الإرسال التي لا يقصد بها أن تكون علانية، فضلاً عن

أولاً: الركن المادي لجريمة الاعتراض غير المشروع.

يظهر الركن المادي في جريمة الاعتراض غير المشروع بتوافر عنصرين اثنين الاول يتعلق بالجاني وبأحقيقته في اعتراض المعلومات، والعنصر الثاني يتعلق باستخدام الوسائل الفنية بفعل الاعتراض، ومن وهنا يمكن لنا تحديد الافعال التي تشكل الركن المادي لجريمة الاعتراض غير المشروع وهي كالتالي:

1-اعتراض البيانات باستخدام الوسائل الفنية.

وهو يأخذ أكثر من حالة ويتم بأكثر من طريقة ولغايات متعددة، ونعني هنا أن يتم الاعتراض باستخدام وسائل فنية تتعلق بالتنصت ومراقبة المحتوى والاتصالات بطريقة مباشرة كالدخول غير المشروع للنظام المعلوماتي، أو بطريقة أخرى غير مباشرة مثل استخدام أجهزة للمراقبة والتنصت الالكتروني و تسجيل البيانات، بالإضافة إلى أنه يمكن ان يشمل الأجهزة الفنية المرتبطة بخطوط النقل والاتصالات، مثل أجهزة تسجيل الاتصالات اللاسلكية¹، كما يمكن أن تشمل استخدام البرمجيات وكلمات المرور والرموز، وغالبا لا تخرج الافعال عن الالتقاط أو التنصت أو الاعتراض.

وهنا نوضح أنه من الممكن أن يكون النظام المعلوماتي المخترق والذي تم عليه الاعتراض هو نفس النظام دون حاجة لنظام اخر يستقبل المعلومات، ومثال ذلك تدفق المعلومات من وحدة المعالجة المركزية إلى الشاشة أو الطابعة بين نظامين للكمبيوتر ينتميان إلى نفس الشخص بين جهاز او جهازين متصلان ببعضهما البعض أو عبر الانبعاثات

الاطلاع على البيانات الحاسوبية(مثل نسخ البيانات) بدون تصريح، وتتمثل هذه الحالة، على سبيل المثال، إذا قام أحد الجناة بالوصول بشكل غير قانوني إلى إحدى قواعد البيانات الحاسوبية، تسجيل عمليات الإرسال بدون حق داخل إحدى شبكات الاتصال اللاسلكي، أو يقوم أحد الجناة، والذي يعمل لدى إحدى الشركات المعنية، بنسخ الملفات وأخذها بدون تصريح، وتتطلب بعض النهج الوطنية أن تكون البيانات ذات الصلة محمية ضد الدخول غير المصرح به، أيضا، تتضمن بعض النهج الوطنية اعتراض الانبعاثات الكهرومغناطيسية التي لا يجوز تصنيفها كبيانات حاسوبية، وغالبا ما قد تتطوي أغراض التجسس الصناعي أو التجاري على فعل النفاذ غير المشروع أو اعتراض البيانات الحاسوبية أو حيازة البيانات الحاسوبية"، للمزيد أنظر في ذلك الملحق رقم 02، الخاص بشرح الافعال بالمذكرة التفسيرية لاتفاقية بودابست 2001..

1- مفيدة مباركية، المرجع السابق، ص 112 113.

الكهرومغناطيسية، وعليه يمكن تضمين الجرائم المرتبطة بالانبعاثات الكهرومغناطيسية ضمن جرائم الاعتراض غير المشروع¹.

2-اعتراض البيانات بدون حق.

لكي تتعدد المسؤولية الجنائية عن فعل الاعتراض غير المشروع، يشترط أن يتم هذا الاعتراض بدون وجه حق وبصورة عمدية، ويكون ذلك في حالة غياب سبب قانوني ومشروع يبرر الاعتراض أو يضيف عليه المشروعية.

وما يمكننا ملاحظته هنا أن هناك شرط لوجود الجريمة، موجود في كلا المعيارين المتعلقين بتكوين الجريمة يحتمل اباحية الجريمة وهو شرط الحق، فعندما يكون الجاني قد فعل بغير حق فعل الاعتراض فنحن أمام جريمة، أما الاعتراض فقد يكون مشروعاً إذا كان للطرف الذي يقوم باعتراض البيانات الحق في الاستفادة من البيانات المرسلّة، أو إذا كانوا يتصرفون تحت تصرف أو تفويض من المشاركين أو متلقي الإرسال، بغض النظر عما إذا كانت البيانات مخصصة لهم للاستخدام الخاص أو للاستخدام العام، أو إذا كان الإشراف بسبب نص قانوني محدد مصرح به لمصلحة الأمن القومي أو من أجل السماح للسلطات كشف بعض الجرائم التي ارتكبت.

ثانياً: الركن المعنوي لجريمة الاعتراض غير المشروع.

ليتحقق الركن المعنوي لهذه الجريمة يكفي تحقق القصد الجرمي العام وهو علم الجاني واتجاه إرادة ليعترض أو يتتصت على المكالمات والاحاديث الشخصية وتسجيلها ونقلها عبر النظام المعلوماتي، أو لبيانات ليس من حقه الاطلاع عليها، وهي من الجرائم الشكلية التي يكفي لوقوعها تحقيق فعل الاعتراض دون النظر إلى ما قد ينتج عن هذا الاعتراض من ضرر².

1- للمزيد أنظر في ذلك المذكرة التفسيرية لاتفاقية بودابست لعام 2001، المرجع السابق، المادة الثالثة الفقرة 55، ص10.

2- " تشترط عادة الصكوك متعددة الأطراف أن تتوافر نية الفعل المتعمد عند ارتكاب جريمة الاعتراض غير المشروع، فعلى سبيل المثال؛ تقتضي اتفاقية مجلس أوروبا بشأن الجريمة الإلكترونية أنه بإمكانية الدول الأطراف أن تحد من الأفعال التي تشكل جريمة الاعتراض القانوني في الحالات التي ارتكبت فيها، والمقتربة بتوافر نية

اما اذا كان مكرها من قبل غيره بوسائل الاكراه المادي أو المعنوي فلا قيام للركن المعنوي وبالتالي لا قيام للجريمة ، بمعنى أن جريمة الاعتراض لا تقوم حتى وان توافر الركن المعنوي في حالتين وهما عدم توافر القصد الجرمي أولا و إذا كانت التتصت والاعتراض تنفيذا للقانون¹.

المطلب الثاني: معالجة جريمة الاعتراض غير المشروع في التشريع الجنائي.

ونتناول في هذا المطلب معالجة التشريعات الجنائية الداخلية لجريمة الاعتراض غير المشروع والعقوبات المقررة لها وهي كالتالي:

أولاً: التشريع الجزائري:

أعتبر المشرع الجزائري الاعتداء على الاتصالات وعلى ما هو مرسل عن طريق الشبكة المعلوماتية أو النظام المعلوماتي بأي طريقة تقنية اعتداء خطير على حرمة الحياة الخاصة وقديستها، وبالتحديد حرية الاتصال والمراسلات، هذه الحرية التي كفلها الدستور الجزائري في المادة 39 منه في فقرتها الثانية حيث جاء فيها " سرية المراسلات والاتصالات بكل أشكالها مضمونه".

وما يلاحظ أن المشرع الجزائري قد جرم فعل الاعتراض غير المشروع من خلال تشريعات خاصة ومثال ذلك قانون البريد والمواصلات السلكية واللاسلكية رقم 03/2000 المعدل والمتمم حيث جاء في المادة 127 منه ما يلي:

احتماليه لدى الجاني، وقد أظهر استعراض التشريعات الوطنية أن هناك دولا قليلة تشترط نية إضافية، بينما ترى دول أخرى أن نية ارتكاب جريمة الاعتراض غير القانونية تصاحبها نية ارتكاب جرائم أخرى دون الفصل بين النيتين، فعلى سبيل المثال، تجرم إحدى دول أوروبا الشرقية الاعتراض غير القانوني للبيانات الحاسوبية فقط إذا كان الهدف ارتكاب جرائم حاسوبية محددة، إلى جانب ذلك، تعتبر بعض الدول وجود نية إضافية بمثابة شرط مشدد للعقوبة وفي هذا الصدد، تعتبر دولتان من دول أوروبا الغربية أن الاعتراض غير المشروع بقصد تحقيق مكاسب مالية بمثابة ظرف لتشديد العقوبات"، للمزيد أنظر في ذلك، دراسة شاملة عن الجريمة السيبرانية، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، فيينا، شباط فبراير 2013، ص 125.

1- ضرغام جابر عطوش آل مواش، المرجع السابق، ص 215 216.

" تطبق العقوبات المنصوص عليها في المادة 137 من قانون العقوبات على كل شخص مرخص له بتقديم خدمة البريد السريع الدولي أو كل عون يعمل لديه والذي في إطار ممارسة مهامه، يفتح أو يحول أو يخرب البريد أو ينتهك سرية المراسلات أو يساعد في ارتكاب هذه الأفعال.

تسري نفس العقوبات على كل شخص مرخص له بتقديم خدمة مواصلات سلكية ولاسلكية وكل عامل لدى متعاملي الشبكات المعلوماتية للمواصلات السلكية واللاسلكية والذي في إطار ممارسة مهامه وزيادة على الحالات المقررة قانونا، ينتهك وبأية طريقة كانت سرية المراسلات الصادرة أو المرسلة أو المستقبلية عن طريق المواصلات السلكية واللاسلكية أو الذي أمر أو ساعد في ارتكاب هذه الأفعال.

يعاقب بالحبس من شهرين إلى سنة وبغرامة مالية من 50.000 دج إلى 1.000.000 دج أو بإحدى هاتين العقوبتين، كل شخص غير الاشخاص المذكورين في الفقرتين السابقتين، ارتكب أحد الأفعال المعاقب عليها بموجب هاتين الفقرتين...¹.

وبهذا حاول المشرع الجزائري الإحاطة بكل المعطيات لحماية البيانات والمعلومات المعالجة آليا أو المرسلة عبر النظام المعلوماتي أو وسائل التقنية العالية أو قطع سيرها أو اعتراضها سواء في قوانين خاصة أو قانون البريد والمواصلات والاتصالات².

إلا أن المشرع الجزائري لم يشر صراحة على جريمة الاعتراض غير المشروع ولكنه استدرك الأمر كونه قد حمى الاتصالات والمراسلات من الاعتداء بأية تقنية كانت في نص المادة 303 من قانون العقوبات الجزائري.

و واصل المشرع الجزائري تطوير قواعده القانونية المتعلقة بالجرائم المعلوماتية ليستحدث بذلك تعديلا في القانون رقم 22/06 يتعلق بالفصل الرابع من قانون الاجراءات الجزائية تحت عنوان " في اعتراض المراسلات وتسجيل الأصوات والنقاط الصور"، وشمل ستة

1- المادة 127 من قانون رقم 03/2000 الذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، المنشور بالجريدة الرسمية عدد 48، الصفحة 03، المؤرخ في 05 أغسطس 2000.

2- بوربابة صورية، المرجع السابق، ص 117.

مواد من المادة 65 مكرر حتى المادة 65 مكرر 10 تناول خلالها مسألة السرية وضمانات استخدام وسائل الاتصال، وجاء في نصت المادة 65 مكرر 5 المقصود بالاعتراض بقولها " ... اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية وهاته المراسلات عبارة عن بيانات قابلة للإنتاج والتوزيع والتخزين والاستقبال والعرض".

وفي نفس السياق تناول المشرع الجزائري الاعتراض غير المشروع عند أذخالة تعديلا على قانون العقوبات 23/06 بشأن حرمة الحياة الشخصية، وشمل التعديل على أهم الافعال التي يجرمها هذا القانون وهي كالتالي:

أ- **فض واتلاف الرسائل والمراسلات:** ونصت عليه المادة 303¹ من قانون العقوبات والملاحظ عليها أن المشرع قد وسع من التجريم في هذه المادة ولم يقتصرها على الشق الورقي فقط بحيث شملت كافة الرسائل والمراسلات دون تقييد لشكلها، ما يعني بالمفهوم العام اشتمالها لرسائل البريد الإلكتروني والرسائل المرسله عبر مختلف تكنولوجيات الاعلام والاتصال، وحدد لها عقوبة معتدلة بالحبس من شهر إلى سنة أو بغرامة مالية من 25.000 دج إلى 100.000 دج أو بأحدة هاتين العقوبتين.

ب- **التقاط وتسجيل البيانات الشخصية:** ونصت عليه المادة 303 مكرر² من قانون العقوبات، والتجريم هنا يقع بغض النظر عن الوسيلة أو التقنية المستخدمة في ارتكاب

1- المادة 303 من قانون العقوبات الجزائري " كل من يفض أو يتلف رسائل أو مراسلات موجهة إلى الغير وذلك بسوء نية وفي غير الحالات المنصوص عليها في المادة 137 * يعاقب بالحبس من شهر إلى سنة وبغرامة من 25000 ألف دج إلى 100.000 ألف دج أو بإحدى هاتين العقوبتين".

- تنص المادة 137 من قانون العقوبات على " كل موظف أو عون من أعوان الدولة أو مستخدم أو مندوب عن مصلحة للبريد يقوم بفض أو اختلاس أو اتلاف رسائل مسلمة إلى البريد أو يسهل فضاها أو اختلاسها أو اتلافها يعاقب بالحبس مدة من 03 ثلاثة أشهر إلى 05 خمس سنوات، وبغرامة مالية من 30.000 ألف دج إلى 50.000 ألف دج...".

2- المادة 303 مكرر من قانون العقوبات الجزائري المعدل والمتمم، حيث نصت على الاعتداء على حرمة الحياة الخاصة والتي جاءت "يعاقب بالحبس من 06 ستة أشهر إلى 3 سنوات وبغرامة من 50.000 دج إلى 300.000 دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت: بالتقاط أو تسجيل أو

الفعل سواء عبر النظام المعلوماتي أو عبر وسائل الاتصال كأجهزة الهاتف المحمولة، وبذلك فهو حمى الاتصالات والمراسلات من الاعتداء بأية تقنية كانت¹.

وفي إطار التجريم نشير إلى أنه لا يمكننا تجريم فعل الاعتراض غير المشروع في قانون العقوبات الجزائري من خلال نص المادة 394 مكرر الخاصة بتجريم الدخول أو البقاء إلى نظام المعالجة الآلية للبيانات، حيث أن النصوص المتعلقة بالدخول والبقاء غير المصرح به لا تنطبق على جريمة الاعتراض غير المشروع، وبهذا فإن قانون العقوبات الجزائري في نصوصه الخاصة بتجريم المساس بأنظمة المعالجة الآلية للمعطيات لم يتضمن نصا قانونيا يجرم فعلي الالتقاط أو الاعتراض للمعطيات أثناء انتقالها من طرف إلى آخر.

ولكن المشرع أعطى مفهوما موسعا لفعل الدخول عن طريق الغش إلى نظام المعالجة الآلية ليمتد ليشمل الالتقاط غير المشروع والاعتراض غير المشروع للمعلومات أثناء انتقالها باعتبار أنها في النهاية تمثل انتهاكا لاتصال معلوماتي بين النظم المختلفة أثناء عملها وهذا واضح في نص المادة 394 مكرر².

وحديثا أصدر المشرع القانون الجزائري القانون رقم 18-04 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، حيث تناول في الباب الرابع منه بعنوان الأحكام الجزائية ومنها جريمة الاعتراض غير المشروع في المادة 164 والتي جاءت بالنص على " يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة مالية من 500.000 دج إلى 1000.000 دج كل شخص ينتهك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الإلكترونية أو يفشي مضمونها أو ينشره أو يستعمله دون ترخيص من المرسل أو المرسل إليه أو يخبر بوجودها"³.

نقل مكالمات أو احاديث خاصة أو سرية بغير إذن صاحبها أو رضاه، بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه..."

1- مفيدة مباركية، المرجع السابق، ص 119.

2- رشيدة بوكري، المرجع السابق، ص 210.

3- المادة 164 من القانون رقم 18-04 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الصادر بالجريدة الرسمية الجزائرية، صفحة رقم 03 عدد 27، بتاريخ 13 مايو 2018.

ثانياً: التشريع السعودي:

لقد جرم التشريع السعودي فعل الاعتراض غير المشروع من خلال نص الفقرة " 01 من المادة الثالثة " من نظام مكافحة جرائم المعلوماتية السعودي والتي نصت على (يعاقب بالسجن مدة لا تزيد على سنة وبغرامة مالية لا تزيد عن خمسمائة ألف ريال أو بإحدى هاتين العقوبتين، كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي دون مسوغ نظامي صحي- أو التقاطه أو اعتراضه...¹.

كما تناولت المادة السادسة من نظام مكافحة جرائم المعلوماتية السعودي التشديد على هذه النوعية من الجرائم إذا كان الفاعل قد تجاوز فعله الجرمي مجرد الفعل إلى إنتاج ما من شأنه انتهاك حرمة الحياة الخاصة أو إعدادة أو إرساله أو تخزينه عن طريق الشبكة أو الحاسب، وقرر المشرع السعودي للجاني عقوبة عن هذه الأفعال تم ذكرها في المادة السادسة تتمثل في الحبس مدة لا تتجاوز خمس سنوات أو غرامة مالية لا تتجاوز ثلاثة ملايين ريال سعودي².

وبالنظر إلى المادتين سالفتين الذكر نجد أنها تتضمن العديد من الجرائم ولكن ما يهمنا هو توضيح المتعلق بالاعتراض غير المشروع حيث:

أ- اعتبر المشرع السعودي جريمة التنصت من الجرائم المعلوماتية إذا ارتكبت باستخدام الحاسب الآلي أو الشبكة المعلوماتية، وبالتالي نجد أن المشرع السعودي قد فرق بين ارتكاب جريمة التنصت باستخدام الوسائل التقنية وبين ارتكابها وفق الطرق التقليدية.

ب- أن الركن المادي لهذه الجريمة حسب المشرع السعودي هو ارتكاب فعل التنصت والاعتراض غير المشروع بإساءة استخدام الشبكة المعلوماتية بما يهدف للمساس بالحياة الخاصة، وتحقق هذا الركن بسلوك الجاني لهذا الفعل وحدث نتيجة وهو تضرر خصوصيات الآخرين.

1- المادة الثالثة من نظام مكافحة جرائم المعلوماتية السعودي، المرجع السابق.

2- عبد العزيز بن غرام الله آل جار الله، المرجع السابق، ص 146.

ت-أن الركن المعنوي لهذه الجريمة هو وجود قصد المساس بالحياة الخاصة ويتحقق ذلك بتوافر العلم لدى الجاني بأنه يقوم بفعله بقصد الاضرار بخصوصية الآخرين وبكامل إرادته واختياره.

ثالثا: التشريع الاماراتي:

تناول المشرع الإماراتي جريمة الاعتراض غير المشروع في العديد من القوانين¹ كان أولها القانون الاتحادي رقم 2006/02 والذي تم إلغاؤه وحل محله المرسوم رقم 05 الصادر بعام 2012، والذي تناول جريمة الاعتراض غير المشروع في المادة 15 منه بنصها "يعاقب بالحبس والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من التقط أو اعترض عمدا وبدون تصريح أي اتصال عن طريق أي شبكة معلوماتية ، فإذا أفشى أي شخص المعلومات التي حصل عليها عن طريق استلام أو اعتراض الاتصالات بغير وجه حق فإنه يعاقب بالحبس مدة لا تقل عن سنة واحدة"².

كما تناول القانون الجديد لسنة 2021 جريمة الاعتراض غير المشروع في نص المادة الثانية عشر بعنوان الاعتراض غير المشروع وإفشاء المعلومات حيث نصت المادة على "1- يعاقب بالحبس والغرامة التي لا تقل عن 150.000 مائة وخمسين ألف درهم ولا تزيد على 500.000 خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، كل من أعاق أو اعترض الوصول إلى شبكة معلوماتية أو موقع إلكتروني أو نظام معلومات إلكتروني أو أي اتصال أو معلومات أو بيانات إلكترونية.

1- لقد تناول المشرع الإماراتي جريمة الاعتراض غير المشروع من خلال نص المادة الثامنة من القانون الاتحادي الملغي رقم 2006/02 المتعلق بمكافحة جرائم تقنية المعلومات، والتي جاء فيها " كل من تنصت أو التقط أو اعترض عمدا، دون وجه حق ما هو مرسل عن طريق الشبكة المعلوماتية أو احدى وسائل تقنية المعلومات، يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين "، وما يمكن ملاحظته من خلا النص اعلاه انه حصر الركن المادي في أفعال التنصت والالتقاط والاعتراض، وان التجريم يتعلق فقط بالمعلومات المرسلة فقط ام تلك التي يتم التقاطها وهي لا تزال مخزنة في النظام المعلوماتي فليست مشمولة بحماية هذا النص".

2- المادة الخامسة عشر من المرسوم بقانون اتحادي رقم 05 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات الاماراتي، المرجع السابق.

2-إذا أفشى الجاني أو سرب المعلومات أو البيانات أو مضمون الاتصال الذي حصل عليه عن طريق الاعتراض كانت العقوبة الحبس مدة لا تقل عن سنة والغرامة التي لا تزيد على 1000.000 مليون درهم.

2-وتكون العقوبة السجن المؤقت إذا كان فعل الاعتراض قد وقع على اتصال أو معلومات أو بيانات لإحدى مؤسسات الدولة¹.

والملاحظ من نص المادة أعلاه أن المشرع الإماراتي قد حدد السلوك المجرم المكون للركن المادي في جريمة الاعتراض غير المشروع بعبارات واضحة وصريحة والمتمثلة في الاعاقا أو الاعتراض المنصب على الشبكة المعلوماتية أو الموقع الإلكتروني أو البيانات الإلكترونية، أما من حيث القصد الجنائي فقد اعتبرها المشرع الإماراتي من الجرائم العمدية التي يتطلب قيام الركن المادي فيها توفر القصد الجنائي العام من علم الجاني بعدم شرعية الفعل الذي يقوم به واتجاه أرادة للقيام بهذا الفعل.

كما ويلاحظ تشدد المشرع الإماراتي في العقوبة المقررة لجريمة الاعتراض غير المشروع اذا اقترنت الجريمة بقيام الجاني بإفشاء المعلومات أو البيانات التي حصل عليها من عملية الاعتراض غير المشروع، محددًا له عقوبة الحبس مدة لا تقل عن سنة وغرامة مالية لا تزيد عن مليون درهم إماراتي، كما تشدد في حالة كان فعل الاعتراض غير المشروع يستهدف الاتصالات والبيانات التابعة لإحدى المؤسسات الحكومية، ووضع لها عقوبة من حد واحد وهو السجن المؤقت.

رابعاً: التشريع الأردني:

تناول المشرع الأردني جريمة الاعتراض غير المشروع في قانون الجرائم الإلكترونية لسنة 2015 في المادة الخامسة منه والتي نصت على " يعاقب كل من قام قصداً بالتقاط أو باعتراض أو بالتتصت أو اعاق أو حور أو شطب محتويات على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنة

1- المادة 12 من قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي لسنة 2021.

وبغرامة لا تقل عن 200 مائتي دينار ولا تزيد على 1000 ألف دينار¹، وما يمكن ملاحظته هنا أن المشرع الاردني بهذا النص قد قام بتعديل المادة الخامسة من قانون جرائم أنظمة المعلومات لسنة 2010 والتي كانت تنص على " كل من قام قصداً دون سبب مشروع بالنقاط أو اعتراض أو التتصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد عن سنة أو بغرامة لا تقل عن 200 دينار ولا تزيد عن 1000 دينار أو بكلا هاتين العقوبتين"، ويظهر تشدد المشرع في عقوبة الحبس في القانون الجديد حيث رفع الحد الأدنى لعقوبة الحبس من مدة من شهر في القانون القديم إلى ما لا يقل عن ثلاثة أشهر في القانون الجديد².

وحديثاً أصدر المشرع الاردني قانون الجرائم الإلكترونية الجديد رقم 17 لسنة 2023 ليُلغي بموجبه قانون الجرائم الإلكترونية رقم 27 لسنة 2015³، والذي تناول جريمة الاعتراض غير المشروع في المادة السابعة منها بنصها على:

"أ- يعاقب كل من قام قصداً ودون وجه حق باعتراض خط سير البيانات او النقاط محتوها أو اعاق أو حور أو شطب أو قام بتسجيل ذلك المحتوى سواء المرسل عن طريق الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات أو البيانات المتبادلة داخل النظام أو الشبكة

1- المادة الخامسة من قانون الجرائم الإلكترونية الاردني رقم 27 لسنة 2015، المرجع السابق.

2- يلاحظ أن المشرع الاردني قد تناول الاعتراض غير المشروع سابقاً في قانون الاتصالات لسنة 1995 في المادة 76 منه والتي جاء فيها " كل من أعترض، أو أعاق، أو حور، أو شطب محتويات رسالة بواسطة شبكات الاتصالات، أو شجع غيره على القيام بهذا العمل يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد عن ستة أشهر أو بغرامة لا تزيد على 200 دينار أو بكلا العقوبتين".

3- وبالإطلاع على الهيكل العام للقانون الجديد والقديم يتبين لنا وجود اختلاف ظاهرياً بينها، بحيث يكمن هذا الاختلاف في عدد المواد التي يتضمنها كلا منهما ففي القانون القديم لسنة 2015 كان يشمل على 18 مادة، بينما القانون الجديد في 2023 يحتوي على 41 مادة أي يفارق 23 مادة زيادة لصالح القانون الجديد، ويتناول القانون الجديد بالتجريم بعض الجرائم التي لم يكن يجرمها في القانون السابق، وهو امر مقبول في مثل هذه القوانين كونها تنظم جرائم مستحدثة وهذه الجرائم تتسم بالتطور يوماً بعد يوم، كما تناول القانون الجديد التعريف لذات المصطلحات التي تناولها القانون القديم في المادة الثانية منه وأضاف عليها متعرف لمصطلحات تقنية المعلومات و خط سير بيانات الحركة و منصة التواصل الاجتماعي و مزودو الخدمة، وبهذا يلاحظ ويتضح من ذلك أن القانون الجديد قد توسع في المصطلحات القانونية بما يخدم مواجهة الجرائم الإلكترونية المستحدثة.

ذاتها بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن 1500 ألف وخمسمائة دينار ولا تزيد عن 6000 ستة الاف دينار.

ب- يعاقب الفاعل بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن 3000 ثلاثة الاف دينار ولا تزيد على 6000 ستة الاف دينار إذا أفضى أو سرب أو أستخدم ما حصل عليه عن طريق الاعتراض.

ج- إذا كان الاعتراض قد وقع على معلومات أو بيانات أو أي اتصال لجهة رسمية تكون العقوبة الاشغال المؤقتة مدة لا تقل عن خمس سنوات وغرامة لا تقل عن 15000 خمسة عشر ألف دينار ولا تزيد عن 45000 خمسة واربعون ألف دينار¹.

والملاحظ من نص المادة تشدد المشرع الأردني في العقوبة المقررة لجريمة الاعتراض غير المشروع عما ذكره في القانون القديم لعام 2015 حيث رفع عقوبة الحبس من ثلاثة أشهر إلى ستة أشهر والغرامة المالية إلى 1500 ألف وخمسمائة دينار حداً الأدنى و 6000 ستة آلاف دينار حداً الأقصى في الوضع الطبيعي للعقوبة، كما قرن المشرع الأردني الجريمة بظروف تشديد للعقوبة في حالة قيام الجاني باعتراض المعلومات المتعلقة بالجهات الرسمية ليصل الحد الأدنى من عقوبة الحبس إلى خمس سنوات مع الشغل المؤقت بالإضافة إلى الغرامة المالية التي قد تصل إلى 45 ألف دينار أردني.

وبناء على ما سبق يمكن القول أن الاعتراض غير المشروع يختلف تماماً عن الدخول غير المصرح به لكون الاعتراض غير المشروع لا يتضمن تدخلاً في نظام معين ينتمي للحاسوب، ولكنه يمثل نوعاً من التلصص على الرسائل والمعلومات المرسلة بين جهازين داخل النظام المعلوماتي، وبهذا لا يعتبر من قبيل الجرائم التي يعاقب عليها باعتبارها تدخلاً غير مصرح به، بل جريمة منفردة وله عقوبة خاصة به.

أما عن فعلي الالتقاط والاعتراض فإنه يمكن التفرقة بينهما في الفعل الاجرامي كما يمكن أن يكونا مقترنين ببعض، ففعل الاعتراض قد يمثل الفعل السابق للالتقاط، أو يهدف إلى

1- المادة السابعة من قانون الجرائم الإلكترونية الأردني الجديد رقم 17 لسنة 2023، المنشور بالجريدة الرسمية عدد 5874 رقم 3579 والصادر بتاريخ 13/08/2023.

ارتكاب فعل آخر، فعن طريق الاعتراض من الممكن ان يقوم المعترض بالتقاط المعلومات أو يعمل على اتلافها.

المطلب الثالث: معالجة جريمة الاعتراض غير المشروع في التشريع الدولي.

وسنتناول في هذا المطلب معالجة الاتفاقيات الدولية لجريمة الاعتراض غير المشروع عبر اتفاقيتين وهما اتفاقية بودابست 2001 والاتفاقية العربية لمكافحة الجرائم المعلوماتية:

أولاً: جريمة الاعتراض غير المشروع في اتفاقية بودابست.

تتناول المادة الثالثة من اتفاقية بودابست بشأن الجرائم الإلكترونية لعام 2001 تجريم الاعتراض غير المشروع للاتصالات والتي تدخل ضمن جرائم المساس بسرية وسلامة البيانات والنظم المعلوماتية، وتلعب هذه المادة دوراً حاسماً في مكافحة الجرائم الإلكترونية من خلال إنشاء إطار للدول الموقعة لتجريم ومحاكمة الأفراد أو الجماعات المتورطة في جريمة الاعتراض غير المشروع للاتصالات الإلكترونية والنظم المعلوماتية، وتؤكد هذه المادة على أن الهدف من تجريم الاعتراض غير المشروع هو حماية الحق في احترام نقل البيانات داخل الانظمة المعلوماتية، فالاعتراض غير المشروع يمثل انتهاكاً للحق في احترام الاتصالات¹.

حيث نصت المادة على " يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية، وفقاً لقانونه الداخلي، واقعة الاعتراض العمدي وبدون حق، من خلال وسائل فنية للإرسال غير العلني، لبيانات الحاسب في مكان الوصول، في المنشأ، أو في داخل النظام المعلوماتي، بما في ذلك الانبعاثات الكهرومغناطيسية من جهاز حاسب يحمل هذه البيانات، كما يمكن لأي طرف أن يستوجب أن ترتكب الجريمة بنية إجرامية (بقصد الغش) أو أن ترتكب الجريمة في حاسب آلي يكون متصلاً عن بعد بحاسب آخر"².

1- مفيدة مباركية، المرجع السابق، ص 110.

2- المادة الثالثة من اتفاقية بودابست بشأن مكافحة الجرائم الإلكترونية لعام 2001، وبالإضافة إلى النصوص السابقة فقد تم معالجة جريمة الاعتراض غير المشروع في العديد من الاتفاقيات والمؤتمرات الدولية ومنها، اتفاقية الاتحاد الافريقي 2012 بشأن إنشاء إطار قانوني للمساعدة في الامن السيبراني في أفريقيا في المادة 23،

وتعليقا على المادة نجد انها تشمل النقاط الرئيسية التالية:

ث- **التجريم:** تطلب المادة من الدول الموقعة اعتماد تدابير تشريعية لتأسيس اعتراض الاتصالات دون الحصول على إذن مناسب باعتباره جريمة جنائية، ومن خلال تجريم مثل هذه الأفعال، تهدف الدول إلى ردع الأفراد أو الجماعات عن الانخراط في أنشطة اعتراض غير مشروعة.

ج- **العقوبات:** تنص المادة الثالثة على أنه يجب على الدول الموقعة فرض عقوبات مناسبة على الاعتراض غير القانوني، والتي قد تشمل السجن أو الغرامات أو كليهما، بحيث تعمل هذه العقوبات بمثابة رادع وتساعد على ضمان مواجهة أولئك الذين تثبت إدانتهم بالاعتراض غير المشروع.

والملاحظ أن المادة الثالثة لم تميز بين نوعية البيانات باعتبارها محل للجريمة، ما اذا كانت بيانات شخصية أو اقتصادية أو سياسية أو مصنفة فكرية وانما شملتها جميعا بالحماية، كما أنها لم تميز بين أهميتها وقيمتها، إلا أنها ميزت بين نوعين من البيانات باعتبارهم محل لجريمة الاعتراض غير المشروع وهما البيانات المتدفقة عبر وسائل الارسل غير العلنية، والثانية الانبعاثات الكهرومغناطيسية التي تصدر من جهاز الحاسب الآلي.

كما أن المادة نصت في شطرها الاخير على امكانية أن تشترط الدول في نصوصها الداخلية لقيام الركن المعنوي للجريمة توافر القصد الجنائي الخاص لاكتمال الجريمة عندما أقرنت ارتكابها بنية إجرامية (بقصد الغش).

اتفاقية السوق المشتركة لشرق وجنوب افريقيا 2011 مشروع القانون النموذجي بشأن الامن السيبراني في المواد 19 و 20، وكومنولث اتحاد الدول المستقلة 2001 اتفاقية بشأن التعاون في مكافحة الجرائم المتعلقة بالمعلومات الحاسوبية في المواد 5 و 8، وكومنولث اتحاد الدول المستقلة 2001 اتفاقية بشأن التعاون في مكافحة الجرائم المتعلقة بالمعلومات الحاسوبية في المادة 1/3 فقرة أ، و البروتوكول الاختياري لاتفاقية بودابست 2001 المواد 2 و 3، و الجماعة الاقتصادية لدول غرب افريقيا 2009 مشوع توجيهي بشأن مكافحة الجريمة السيبرانية داخل دول غرب أفريقيا في المادة 6، و الاتحاد الاوروبي من خلال المشروع النهائي التوجيهي للجنة التنفيذية 2010/073 بالبرلمان الاوروبي ومجلس اوربا بشأن الهجمات ضد نظم المعلومات وإلغاء القرار الإطاري للمجلس 2005/222/JHA في المادة 6، والاتحاد الدولي للاتصالات الجماعة الكاريبية 2010 بشأن الجريمة السيبرانية CTU/CQRICO;ITU في المواد 6 و 8.

وبشكل عام، توفر المادة الثالثة من اتفاقية بودابست بشأن الجرائم الإلكترونية إطاراً شاملاً لمعالجة قضية الاعتراض غير المشروع للاتصالات على المستوى الدولي، ومن خلال وضع معايير مشتركة وتعزيز التعاون بين الدول الموقعة، تساهم هذه المادة من الاتفاقية سابقة الذكر في الجهود العالمية لمكافحة الجرائم الإلكترونية وحماية حقوق الخصوصية للأفراد في العصر الرقمي.

ثانياً: جريمة الاعتراض غير المشروع في الاتفاقية العربية.

جاءت الاتفاقية العربية بهدف تقديم إطار قانوني لمكافحة جرائم التكنولوجيا والمعلومات في العالم العربي وفي محاولة لحصر جرائم المعلوماتية تناولت الاتفاقية العربية تجريم جريمة الاعتراض غير المشروع، أذ اعتبرت واحدة من الأنشطة المحظورة والمعاقب عليها في الاتفاقية العربية ونصت عليها في المادة السابعة، تحت عنوان جريمة الاعتراض غير المشروع، وجاء نصها على التالي " الاعتراض المعتمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات"، كما تناولت الاتفاقية في المادة الثانية الفقرة الثامنة تعريف الالتقاط على أنه " الالتقاط مشاهدة البيانات أو المعلومات أو الحصول عليها"¹.

المبحث الثالث: جريمة الاتلاف المعلوماتي.

يُعرف الإتلاف في اللغة بأنه مصدر الفعل "التلف" بمعنى الهلاك، ويقال رجل متلاف أي كثير الإضرار الإتلاف لماله، أما اصطلاحاً فيقصد به كل فعل من شأنه لإحداث تأثير في مادة الشيء يؤدي إلى زوال أو التقليل من قيمته الاقتصادية ، وذلك بالانقاص من كفاءته للاستعمال المعد له، وعليه فجوهر الاتلاف يتمثل في افقاد المال المتلف منفعته وتجريده من صلاحيته للاستعمال في الغرض الذي أعد من أجله.

فالأتلاف هو تعييب الشيء على نحو يفقده قيمته الكلية أو الجزئية، وذلك إذا كان الفعل قد أفقد الشيء قيمته كلها أو جزء منها فقد تحقق الاعتداء الذي يجرمه القانون، فهو بذلك أفناء

1- أنظر المادة السابعة والمادة الثانية الفقرة 8 من الاتفاقية العربية لمكافحة الجرائم المعلوماتية، المرجع السابق.

لمادة الشيء أو أحداث تغييرات عليها كلية أو جزئية بحيث تصبح غير صالحة للوظيفة والغرض التي أعدت من أجله وبالتالي تفقد قيمتها لدى المالك¹.

ويقع فعل الاتلاف في نطاق المعلوماتية من خلال الاعتداء على الوظائف الطبيعية للحاسب الآلي أو النظام المعلوماتي ذاته، سواء عبر الاعتداء على مكوناته المادية أو على المكونات المعنوية لهذا النظام المتمثلة في المعلومات والبرامج والبيانات المخزنة في النظام المعلوماتي، دون أن يؤدي الإتلاف بالضرورة إلى إلحاق ضرر بأي عنصر مادي من مكونات النظام المعلوماتي.

ففي الحالة الاولى يخضع الاتلاف الذي يقع على المكونات المادية للنظام المعلوماتي كالأشاشات والاشرطة والاسطوانات والكابلات وغيرها إلى النصوص التقليدية الخاصة بجريمة الإتلاف في قانون العقوبات الذي يوفر لها الحماية و يجرم فعل الاتلاف الذي يؤدي إلى إلحاق ضرر بالمال المنقول المملوك للغير، أما في الحالة الثانية المتعلقة بوقوع الاتلاف على المعلومات أي المكونات غير المادية المخزنة في جهاز الحاسوب أو المتبادلة عبر الشبكات المحلية والعالمية، فإنها تخضع لقوانين خاصة بمجال المعلوماتية توفر لها الحماية بحيث تحدد الفعل الاجرامي وتضع له العقوبة².

وبناءً على ذلك يُعرف الاتلاف المعلوماتي على أنه كل فعل يؤدي إلى (محو المعلومات أو البرامج كلياً أو تدميرها بوسائل إلكترونية، أو تشويهها على نحو يفقدها صلاحيتها للاستعمال أو يقلل من قيمتها الوظيفية)، وينصب هذا النوع من الأتلاف على المكونات المعنوية للنظام المعلوماتي أي المعلومات والبيانات والبرامج، دون أن يمتد بالضرورة إلى المكونات المادية، كما أن السلوك الاجرامي المكون لجريمة الاتلاف المعلوماتي لا يؤدي إلى إعاقة أو تعطيل سير النظام المعلوماتي دائماً، الأمر الذي يقتضي من الناحية العلمية والقانونية التمييز بين الإتلاف المعلوماتي من جهة، وبين تعطيل النظام وفساده من جهة أخرى، ومعاملتها على أنهما سلوكين منفصلين لكل منهما أركانه وأحكامه الخاصة من موجبات الاعتبارات

1- عبدالفتاح بيومي حجازي، المرجع السابق، ص 525.

2- نهلا عبد القادر المومني، المرجع السابق، ص 123 124.

العلمية، فقد يكون هناك اتلاف معلوماتي ينصب على برامج أو معلومات موجودة داخل نظام معلوماتي كحالة محو بعض الملفات المخزنة داخل النظام دون أن يؤدي ذلك إلى تعطيل للنظام المعلوماتي، ولذلك فإن أغلب التشريعات ميزت بين جريمتي الاتلاف المعلوماتي وتعطيل أو أفساد النظام المعلوماتي.¹

وتعتبر جريمة التخريب أو الاتلاف للمعطيات والبيانات من أشد أنواع الجرائم إلحاقاً للأذى، ذلك أن الجاني قد تأصلت فيه نوازع الشر لدرجة أوصلته إلى الرغبة في التدمير والتخريب لما يمكن أن يساوي مبالغ طائلة ومجهودات كبيرة.²

وبناء على ما سبق سوف نقسم هد المبحث إلى ثلاثة مطالب: المطلب الأول نتناول فيه تفصيل جريمة الإلتلاف المعلوماتي بما يشمل أركانها، والمطلب الثاني نبين فيه موقف القوانين العقابية الوطنية، أما المطلب الثالث فقد خصصناه للمعالجة الدولية لجريمة الإلتلاف المعلوماتي.

المطلب الأول: تفصيل جريمة الإلتلاف المعلوماتي.

يمكن تعريف جريمة الإلتلاف المعلوماتي على أنها " كل معالجة آلية للبيانات تستهدف البيانات الرقمية عمدا ودون حق لإفراغها من المعلومة أفرغا كلياً أو جزئياً وسواء تم ذلك بصفة دائمة أو مؤقتة"، وهذا التعريف يشمل كل أنواع المعلومات بما فيها أنظمة تشغيل النظام المعلوماتي، وجميع القطع البرمجية لمسؤولة عن عمل النظام، وعبرة المعالجة الآلية للبيانات الوارد ذكرها في التعريف تشمل جميع الأفعال المنصوص عليها في المادة الرابعة من اتفاقية بودابست 2001.

1- دلخار صلاح بوتاني، المرجع السابق، ص 254.

2- عبد العزيز بن غرام الله آل جارالله، المرجع السابق، ص 220، يقصد بالتخريب توقف الشيء تماماً عن أن يؤدي منفعة حتى ولو لم تقنئ مادته سواء كان هذا التوقف كلياً أو جزئياً، ويرى بعضهم بأن التخريب والإلتلاف مترادفان ويدلان على جعل الشيء غير صالح للاستعمال في الغرض المخصص له، ويرى جانب من الفقه بأن التفرقة بينهما هي تفرقه في كمية التدمير، ففي الإلتلاف يكون الشيء لا يزال قابل للإصلاح وأن صلاحيته للاستعمال أنقصت، أما في التخريب فيعني أن الشيء لم يعد قابل للإصلاح، ويقصد بعدم الصلاحية للاستعمال جعل الشيء لا يقوم بوظيفته المرصود لها على النحو الأكمل والتعطيل هو توقف الشيء عن القيام بوظيفته فترة مؤقتة ويكفي أي من هذه الأفعال حتي تقع الجريمة، أنظر في ذلك الدكتور أيمن عبدالله فكري، المرجع السابق، ص 181.

و محل جريمة الإتلاف المعلوماتي هو المعلومات والبيانات الرقمية بمختلف أنواعها سواء كانت داخل النظام المعلوماتي أو مخزنة على دعامة مادية خارجية، أو برامج أو أنظمة التشغيل المسؤولة عن عمل النظام المعلوماتي، فجميعها يمكن أن تشكل محلاً لجريمة الإتلاف المعلوماتي المنصوص عليها في الاتفاقية الدولية سابقة الذكر¹.

وعليه فإن جريمة الإتلاف المعلوماتي وكغيرها من الجرائم تقوم على مجموعة من الأركان سنوضحها فيما يلي:

أولاً: الركن المادي لجريمة الإتلاف المعلوماتي.

يتخذ الركن المادي في جريمة الاتلاف المعلوماتي العديد من الصور يمكن حصرها في ثلاث أفعال أساسية على الأقل تتمثل في " الإدخال والمحو والتعديل" في حالة الاعتداء على المعلومات داخل النظام المعلوماتي، أو في حالة الاعتداء على نظم المعالجة الآلية للمعلومات، حيث يتحقق النشاط الجرمي على الأقل بإتيان احد هذه الأفعال الاجرامية التالية:

1- فعل الادخال: يعرف فعل الادخال على أنه " تغذية النظام بالمعلومات المراد معالجتها، أو بتعليمات لازمة لعملية المعالجة"، ويقصد بذلك ادخال معلومات وبيانات لنظام المعالجة الآلية للمعلومات لم تكن موجودة من قبل بهدف إتلاف المعلومات المخزنة بالنظام أو الإضرار ببرامج النظام كونها معلومات دخيلة عليه، وتشمل هذه الفئة الوسائل التي أصبحت معروفة لمستخدمي النظام المعلوماتي مثل " الفيروسات والقنابل المنطقية والزمنية" همشهم².

1- مفيدة مباركية، المرجع السابق، ص 135.

2- بوربابة صورية، المرجع السابق، ص 102، " وفي هذا الشأن يعرف الفيروس على أنه برنامج مكون من عدة أجزاء مكتوب بإحدى لغات البرمجة بطريقة خاصة تسمح له بالتحكم في البرامج الأخرى وهو قادر على تكرار نفسه، ويحتاج إلى برنامج وسيط يكون العائل له أو أن يجد مساحة تنفيذية على النظام، والفيروسات بشكل عام خطيرة جدا وتهدد الاجهزة والشبكات بالتلف، ومن الامثلة انواع الفيروسات نجد فيروسات الجزء التشغيلي(newzeland)، والفيروسات المتطفلة كفيروس (cascade)، والفيروسات المصاحبة للبرامج، وفيروس حصان طروادة والذي غالبا ما يلحق بملفات التجسس بحيث يتخفى في وصلات الملفات الداخلية.

أما القنابل المنطقية والزمنية فهي مجموعة من التعليمات تنفذ عملاً مؤدياً عن توفر شروط معينة، وقد تكون تلك الشروط توفر يوم معين أو ساعة معينة أو غير ذلك، ومثال ذلك ما قام به أحد المبرمين العرب بوضع تعليمات معينة ضمن برامج الشركة بحيث يتم محو جميع ملفات الشركة عندما يتم حذف اسمه من ملف

وبناء على ذلك يُعد فعل الإدخال عملية تعتمد على إضافة معطيات دخيلة وغريبة على النظام، من شأنها الإضرار بالمعطيات الأصلية من خلال المساس بسلامة المعلومات وقيمتها الموجودة بداخله، وذلك بصرف النظر عن مدى صحة المعطيات المضافة من عدمه، طالما أن إدخالها من شأنه التشويش على المعلومات المخزنة أو الإخلال بوظيفتها¹.

2- فعل المحو: وهو محو الأشياء ويكون بنفسها تماما من الدعامة حيث تخزن، وبالتالي جعلها غير موجودة تماما ككيان معنوي وهو يعادل تدمير الأشياء المادية وجعلها في حالة لا يمكن التعرف عليها، ويعرفه الاستاذ (J. P. Buffelan) على أنه " اقتطاع خصائص مسجلة على دعامة ممغنطة عن طريق محوها أو عن طريق طمسها- بمعنى ضغط خصائص أخرى فوقها- تلمس الخصائص القديمة".

وفي ذات الشأن فقد ميز المجلس الأوروبي في تقريره المرقم "89"9 بخصوص جرائم المعلوماتية بين نوعين من انواع التدمير الذي يلحق بالمعلومات وهما محو المعلومات أي ازالته تماما، وبين فعل إخفاء المعلومات حيث يمكن الوصول إليها دون أن يؤدي ذلك إلى لإزالتها تماما، إلى أن هناك من يرى أن فعل الإخفاء طالما لا يؤدي إلى إزالة المعلومات بصورة نهائية لا يعدو أن يكون إلا تعديلا للمعلومات لا تدميرا لها².

3- فعل التعديل: ويقصد بالتعديل تغيير المعطيات أو المعلومات الموجودة داخل النظام المعلوماتي واستبدالها بمعطيات أخرى³، أو التلاعب بمعلومات و برامج بإمدادها بمعطيات مغايرة عن تلك التي صمم البرنامج لأجلها⁴.

والتعديل بهذا المعنى قد يتم باستبدال المعلومات أو عن طريق التلاعب في البرنامج وذلك بإمداده بمعلومات مغايرة تؤدي إلى نتائج مغايرة عن تلك التي صمم البرنامج لأجلها،

المرتبات"، للمزيد أنظر في ذلك د عبد العزيز بن جار الله آل غرام الله، المرجع السابق، ص 221 و 222 وما بعدها، وللمزيد أكثر أنظر د نهلا عبد القادر المومني، المرجع السابق، الصفحات 125 حتى 134.

1- بشأن عبد النور، الجوانب الموضوعية لمعالجة الجريمة المعلوماتية، أطروحة لنيل شهادة الدكتوراه في الحقوق، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 01، الجزائر، السنة الجامعية 2017-2018، ص338.

2- دلخار صلاح بوتاني، المرجع السابق، ص 259 260.

3- حسين محمد الغول، المرجع السابق، ص 466.

4- بوربابة صورية، المرجع السابق، ص 104

ذلك أن كثير من البرامج يتم إعدادها واختيارها تمر ببعض التعديلات لتصويب أخطاء اكتشفت بعد العمل بها، وهو ما يتيح إدخال تغييرات من شأنها ان تساعد الجاني في إتمام جريمته وإخفائها، كما قد يتم التعديل عن طريق البرامج الخبيثة¹.

ويختلف فعل التعديل عن فعل الإدخال في كون التعديل يتضمن التغيير في البيانات المخزنة في النظام، أما الإدخال فقد يتم بإدخال بيانات إلى نظام خال من البيانات، وقد يتم إدخال بيانات إلى البيانات الموجودة في النظام، كما يختلف فعل التعديل عن فعل الإزالة في كون الأول يتضمن تغييرا في البيانات الموجودة أصلا في النظام، أما الثاني فيتضمن إزالة ومحو البيانات الموجودة².

والجدير بالذكر أن الأفعال المكونة للركن المادي في جريمة الإتلاف المعلوماتي لا يشترط اجتماعها في جريمة واحدة بل يكفي توفر فعل واحد من الأفعال سابقة الذكر لقيام النشاط الاجرامي، كما وتعد جريمة الإتلاف المعلوماتي من الجرائم المادية التي لا يكفي فيها ان تهدد سلامة المعلومات بخطر الإزالة أو التعديل أو الإدخال، وإنما لا بد من وقوع ضرر فعلي على هذه المعلومات ألا وهو تغيير حالتها من خلال الأفعال الممثلة للنشاط الجرمي في هذه الجريمة.

ثانيا: الركن المعنوي لجريمة الإتلاف المعلوماتي.

تعتبر جريمة الإتلاف المعلوماتي من الجرائم العمدية التي تتحقق بتوافر القصد الجنائي العام لدى من يرتكبها، وبالتالي توافر القصد بشقية العلم و الإرادة، فيلزم أن يعلم الجاني أن المال المعلوماتي الذي يقع عليه فعله مملوك للغير، وأن من شأن فعله التأثير في مادة الشيء أو في قيمته بشكل يجعله غير صالح للإستعمال، وأن ما يقوم به بمعزل عن رضاء وإذن صاحب الحق في المال أو مالك النظام وضد أرائته³.

1- رشيدة بوكري، المرجع السابق، ص256.

2- فايز محمد راجع غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني ، أطروحة لنيل شهادة الدكتوراه في الحقوق، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 01، الجزائر، السنة الجامعة 2009-2010، ص 215.

3- أيمن عبدالله فكري، المرجع السابق، ص 182.

وعليه اذا اعتقد الجاني أن المال المعلوماتي محل جريمة التلاف مملوك له فإن القصد الجنائي ينتفي لديه لعدم العلم كمن يعتقد ملكيته لنظام معلوماتي أو حاسب آلي تم يثبت ملكيتها للغير، كما يشترط توافر إرادة لدى الجاني تهدف إلى تحقيق نتيجة عن فعله وذلك بإحداث إتلاف بشكل يؤدي إلى توافر ضرر ناتج عن فعله، لذلك إذا حدث لإتلاف غير مقصود كما لو حدث شيء عارض وتسبب في إتلاف جزء من معلومات النظام فإن الفاعل يسأل عن الخطأ نتيجة إهماله وتقصيره¹.

فإذا توافر الركن المعنوي بعنصرية السابقين العلم و الإرادة إلى جانب الركن المادي وقعت الجريمة وإستحق مرتكبها العقوبة المنصوص عليها قانوناً.

أما القصد الجنائي الخاص فقد اشترطت بعض التشريعات على ضرورة توافره بجانب القصد الجنائي العام لقيام جريمة الإتلاف المعلوماتي، وذلك بأن تتجه إرادة الجاني إلى تحقيق غاية محددة وقصد خاص، كقصد الإضرار بالغير أو قصد تحقيق منفعة وريح مادي غير مشروع للجاني أو للغير، غير أن هذا الاتجاه لم يسلم من الانتقاد ولا سيما فيما يتعلق باشتراط تحقيق الربح المادي، إذ أن الأخذ به سوف يؤدي إلى استبعاد الحالات التي لا تتجه فيها نية الجاني إلى تحقيق ربح مادي غير مشروع، بالرغم من أهمية المعلومات التي قد يتم إتلافها وجسامة الضرر المترتب عليها كما في حالة إتلاف معلومات علمية أو طبية، أما فيما يتعلق بالقصد الخاص المتمثل بالإضرار بالغير، فيرى المنتقدون ضرورة تفسيره تفسيراً واسعاً بحيث لا يقتصر على مجرد الخسائر أو الأضرار المادية التي قد تصيب المجني عليه بل يمتد لشمول كافة مصالحه المشروعة².

1- محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنت " الجريمة المعلوماتية"، مكتبة دار الثقافة للنشر و التوزيع، عمان الأردن، الطبعة الأولى 2004، ص 221.

2- دلخار صلاح بوتاني، المرجع السابق، ص 265.

المطلب الثاني: معالجة جريمة الإلتلاف المعلوماتي في التشريع الجنائي.

سنحاول هنا توضيح موقف القوانين العقابية الوطنية من جريمة الإلتلاف المعلوماتي وكيف حاولت حماية المعلومات والتصدي لهذه الجريمة أما من خلال نصوص قانونية جديدة أو التعديلات على القوانين العقابية التقليدية.

أولا: التشريع الجزائري:

تناول المشرع الجزائري جريمة الإلتلاف المعلوماتي من خلال نص المادة **394 مكرر 1** من قانون العقوبات والخاصة بجريمة التلاعب والإلتلاف المعلوماتي، حيث نصت على " يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها ¹، وبالنظر إلى المادة فإن الإطار العام لها لم يميز بين نوعية المعلومات ولعل مسعى المشرع من عدم التفريق هدفه حماية المعلومات بكافة أنواعها.

وما يلاحظ من نص المادة أن المشرع لم يشترط أن تكون جريمة الإلتلاف المعلوماتي قد حدثت بعد الولوج غير المشروع للنظام المعلوماتي، وبالتالي فإن جريمة الإلتلاف المعلوماتي تقوم متى قصدها الجاني بغض النظر عن كيفية الدخول سواء كان دخول غير مشروع أو مشروع، وأن كان يثير في الحالة الأولى مسألة التعدد المادي للجريمة فتطبق العقوبة الأشد وفقا للمواد **33 و 38** من قانون العقوبات الجزائري.

و انطلاقا من نص المادة المذكورة أعلاه يتضح أن الركن المادي لجريمة الإلتلاف المعلوماتي تتم بالسلوك الإجرامي الذي يرتكبه الجاني والذي يتخذ أحد الصور التالية " الإدخال أو التعديل أو الإزالة " ، -الإزالة- الذي ذكره المشرع الجزائري بدلا لمصطلح المحو، وعليه فإن ارتكاب فعل واحد من هذه الأفعال كافي لقيام الركن المادي لجريمة الإلتلاف المعلوماتي حيث أن الأفعال وردت في نص المادة على سبيل الحصر، أي لا يدخل ضمن دائرة التجريم أي فعل

1- المادة 394 مكرر 1 من قانون العقوبات الجزائري المعدل والمتمم.

آخر غيرها مهما كانت علاقته بالنظام المعلوماتي¹، إضافة إلى ذلك لا يتم العقاب عليها إلا إذا ارتكبت بدون إذن، وبالتالي بمفهوم المخالفة لا جريمة ولا عقوبة إذا كان إتيان هاته السلوكيات مصرح به من مالك النظام أو مالك جزء منه².

وعن محل الجريمة فبالنظر إلى الأفعال السابقة نجد أن محل جريمة الإتلاف المعلوماتي في التشريع الجنائي الجزائري هو المعلومات التي يحتويها النظام، وهذا يعني أن النشاط الجرمي في جريمة الإتلاف المعلوماتي إنما يقع فقط على المعلومات التي تتم معالجتها آليا، والمعلومات الموجودة داخل النظام المعلوماتي وتشكل جزء منه وهذا واضح في نص المادة **394 مكرر 1** بقولها "... بطريقة الغش المعطيات التي يتضمنها..."، أو المعلومات المعالجة التي انفصلت عن النظام تم أعيد إدخالها فيه³، ويستوي بذلك ان يكون محل الجريمة معلومات مخزنة في أشربة أو أقراص أو معالجة آليا أو مرسلّة عن طريق منظومة أو شبكة معلوماتية، أما المعلوماتي التي لم تدخل إلى النظام أو لم يتم معالجتها آليا، فهي خارج نطاق الحماية المقررة في المادة **394 مكرر 1** من قانون العقوبات الجزائري⁴.

أما النتيجة الإجرامية فيرى المشرع الجزائري أن جرائم الاعتداء على نظم المعلومات المعالجة آليا من قبيل الجرائم الخطرة، حيث يستشعر المشرع خطورة الجاني من السلوك المجرد الذي يقوم به حتى لو لم يترتب على ذلك حصول ضرر مادي ليتم عقابه، أي أن المشرع لم يشترط لوقوع جريمة الإتلاف المعلوماتي أن يترتب على النشاط الجرمي نتيجة مادية ملموسة وضارة على الحق الذي يحميه القانون، وإنما اكتفى فيها لقيام الجريمة العدوان المحتمل أو التهديد بالخطر في سرية المعلومات وسلامتها⁵.

كما اعتبرها المشرع الجزائري من الجرائم العمدية والتي يكفي لقيام ركنها المعنوي توافر القصد الجنائي العام من علم و إرادة، أي يعلم بعملية إدخال أو محو أو تعديل غير مصرح به

1- بشأن عبد النور، المرجع السابق، ص 340.

2- رشيدة بوكري، المرجع السابق، ص 247 إلى 250.

3- رشيدة بوكري، نفس المرجع السابق، ص 262.

4- دلخار صلاح بوتاني، المرجع السابق، ص 274 .

5- رشيدة بوكري، نفس المرجع السابق، ص 268.

لمعلومات النظام المعلوماتي و أن من شأن أفعالة هذه أن تؤدي إلى تغيير حالة المعلومات، كما أن أرائته تتجهن إلى ارتكاب هذا الفعل وإلى تحقيق هذه النتيجة، ولم يظهر من خلال نص المادة **394 مكرر 1** أن المشرع الجزائري تطلب وجود نية خاصة أو قصد خاص لقيام الركن المعنوي أن لفظ الغش الذي أستخدمه المشرع انما للدلة على أن هذه الجريمة عمدية، وبذلك يستفاد أن القصد الجنائي العام كافي لقيام الجريمة¹.

وتشدد المشرع الجزائري في عقوبة الإلتلاف غير المشروع في حال اقترانها بجريمة الولوج غير المشروع وحدد لها عقوبة حسب نص المادة **394 مكرر** اذا نتج عن هذا الولوج وقوع جريمة الأتلاف بأفعالها المتمثلة بالمحو أو الإدخال أو التعديل، كما نصت المادة **394 مكرر 1** على عقوبة جريمة الإلتلاف المعلوماتي والتي تراوحت ما بالحبس ما بيت 06 أشهر إلى ثلاثة سنوات وغرامة مالية من **500.000** دج إلى **2.000.000** دج بحق كل من قام بإدخال معطيات أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها النظام المعلوماتي.

ثانيا: التشريع السعودي.

جاء موقف المشرع السعودي مسائرا للاتجاه الحديث الذي يقضي بضرورة إيجاد نص خاص للعقاب على جريمة الإلتلاف المعلوماتي وعدم ترك المسألة للقواعد العامة التقليدية، حيث تناول جريمة الإلتلاف المعلوماتي في الفقرة الثانية من المادة الخامسة من نظام مكافحة الجرائم المعلوماتية السعودي لسنة 2007 والتي نصت على "يعاقب... إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو اتلافها، أو تعديلها"²، ولقد تضمنت المادة العديد من الجرائم التي اعتبرها المشرع السعودي جرائم معلوماتية اذا ارتكبت بواسطة الحاسب الآلي أو الشبكة المعلوماتية، وما يهمنا هو توضيح الخاصة بالأتلاف منها:

1- رشيدة بوكر، نفس المرجع السابق، ص 269 270.

2- الفقرة الثانية من المادة الخامسة من نظام مكافحة الجرائم المعلوماتية السعودي رقم 17 لسنة 2007.

ح- أعتبر المشرع السعودي أن الركن المادي لجريمة الاتلاف المعلوماتي له عدة صور وهي (تغيير تصاميم موقع أو اتلافه أو شغل عنوانه أو تعديله، أو إلغاء بيانات خاصة أو حذفها أو تعديلها، أو اتلافها أو تدمير أو مسح البرامج أو تعديلها)، بأي وسيلة كانت ويتحقق هذا الركن بسلوك الجاني لأي من هذه الأفعال وما تفضي إليه من تخريب أو اتلاف أو تغيير، وحدوث نتيجة وظهور ذلك فعلياً على الشبكة المعلوماتية أو جهاز الحاسب الآلي.

خ- أعتبر المشرع السعودي أن الركن المعنوي لجريمة الإتلاف المعلوماتي يتمثل بالقصد الجنائي العام، أي نية ارتكاب أيا من أفعال التخريب والإتلاف ويتحقق هذا الركن بتوافر العلم لدى الجاني بأنه يقوم بأعمال تخريب قصدا وليس سهواً أو بسبب خطأ مادي، ويكفي توافر نيته الجرمية لتجريم هذا الفعل حال صدوره منه وهو بكامل إرادته¹.

وعاقب المشرع السعودي على جريمة الإتلاف المعلوماتي في المادة الخامسة سابقة الذكر بعقوبة السجن لمدة لا تزيد عن أربع سنوات، أو بغرامة مالية لا تتجاوز ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين، ويلاحظ من استقراء العقوبات المقررة والمنصوص عليها في المواد الثالثة والرابعة والخامسة من نظام مكافحة جرائم المعلوماتية، أن المشرع قد أنتهج سياسة قائمة على التدرج في التشديد ، تبعاً لجسامة الفعل الإجرامي وخطورته، وبناء على ذلك تتراوح العقوبة المقررة لجرائم الاتلاف تتراوح بعدها الأعلى المذكور أعلاه، وحدها الأدنى هو السجن مدة لا تزيد عن ثلاث سنوات أو غرامة مالية لا تتجاوز مليوني ريال أو بإحدى هاتين العقوبتين.

ثالثاً: التشريع الإماراتي.

بالنظر إلى قانون العقوبات الإماراتي الملغي إذ كان لا بد من التعرّيج عليه لأثره البحث نجد أن المشرع تناول جريمة الإتلاف المعلوماتي من خلال الفقرة الثانية من نص المادة الثانية من القانون رقم 2006/02 والتي جاءت بالنص " فإذا ترتب عن الفعل إلغاء أو حذف أو تدمير أو افشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات..."، وما يتضح لنا أن المشرع الإماراتي قد جعل محل جريمة الاتلاف هو الاعتداء على المعلومات داخل النظام

1- عبدالعزيز بن غرام الله آل جار الله، المرجع السابق، ص 229.

المعلوماتي أيا كان أسلوب احتوائها (حاسب آلي أو دعامة أو وسيط أو غيرها، كما أضاف فعل الالغاء أو الحذف، وهو ما يرادف فعل المحو والإتلاف لتطابقهما في النتيجة)¹.

أضافة إلى ما سبق عالج المشرع الإماراتي جريمة الإتلاف المعلوماتي بنصوص مستقلة في حالة اقترانهم بجرائم أخرى مثل جريمة الإعاقة الخطيرة لعمل النظام وتدمير البيانات الطبية وهذا في نصوص المواد السادسة والسابعة من نفس القانون والتي جاءت بالنص " كل من أدخل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، ما من شأنه إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تعديل البرامج او البيانات أو المعلومات فيها يعاقب بالسجن المؤقت وبالغرامة التي لا تقل عن خمسين ألف درهم أو بإحدى هاتين العقوبتين"²، أما المادة السابعة فقد عالجت حالة خاصة للإتلاف المعلوماتي وهو ذلك المنصب على الفحوصات والكشوفات الطبية، حيث جاءت بالنص " يعاقب بالسجن المؤقت أو الحبس كل من عدل أو أتلّف الفحوص الطبية أو التشخيص الطبي، أو العلاج الطبي، أو الرعاية الطبية، أو سهل للغير فعل ذلك، أو مكنه منه، باستعمال الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات"³.

كما تناول المشرع تجريم جريمة الإتلاف المعلوماتي في القانون رقم 05 لسنة 2012 في المواد 02 و 04 و 05 و 07⁴ وحدد الأفعال التي تمثل السلوك الإجرامي لجريمة الاتلاف المعلوماتي ب الإدخال والمحو والتعديل، ولم يشترط اجتماعها في جريمة واحدة وإنما يكفي توافر أحدها لوقوع الجريمة، ومن خلال تحديد السلوك الإجرامي يتضح أن الجريمة في التشريع الاماراتي لا تقع إلى على المعطيات أي على البيانات والمعلومات المعالجة آلياً، والموجودة داخل النظام المعلوماتي، وبذلك يكون المشرع الإماراتي قد استبعد من دائرة التجريم المعلومات والبيانات التي لم تعالج بعد أو لم تدخل إلى نظام المعالجة الآلية، وكذلك المعلومات الموجودة

1- دلخار صلاح بوتاني، المرجع السابق، ص 272.

2- المادة السادسة من قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم 2006/02.

3- المادة السابعة من نفس القانون.

4- للمزيد أنظر المواد الثانية والرابعة والخامسة والسابعة من قانون مكافحة جرائم تقنية المعلومات الاماراتي رقم 05 لسنة 2012، المرجع السابق.

خارج النظام المعلوماتي سواء على دعامة خارجية أو على قرص مضغوط حيث أنها أصبحت خارج النظام المعلوماتي¹.

وفي القانون الجديد لسنة 2021 تناول المشرع الاماراتي جريمة الإلتلاف المعلوماتي في المادة السادسة والسابعة حيث خصص المادة السادسة للاعتداء على المعلومات والبيانات الشخصية ونصت على " 1- يعاقب بالحبس مدة لا تقل عن 6 سنة أشهر والغرامة التي لا تقل عن 20.000 عشرين ألف درهم ولا تزيد على 100.000 مائة ألف درهم، أو بإحدى هاتين العقوبتين، كل من حصل أو استحوذ أو عدل أو أتلّف أو أفشى أو سرب أو ألغى أو حذف أو نسخ أو نشر أو أعاد نشر بغير تصريح بيانات أو معلومات شخصية إلكترونية، باستخدام تقنية المعلومات أو وسيلة تقنية معلومات .

2- فإذا كانت البيانات أو المعلومات المشار إليها في البند 1 من هذه المادة، تتعلق بفحوصات أو تشخيص أو علاج أو رعاية أو سجلات طبية أو حسابات مصرفية أو بيانات ومعلومات وسائل الدفع الإلكترونية عد ذلك ظرفاً مشدداً.

3- ويعاقب بالحبس والغرامة، أو بإحدى هاتين العقوبتين، كل من تلقى أي من البيانات والمعلومات المشار إليها بالبندين 1 ، 2 من هذه المادة، واحتفظ بها أو خزنها أو قبل التعامل بها أو استخدامها رغم علمه بعدم مشروعية الحصول عليها"².

أما المادة السابعة فقد خصصها المشرع الاماراتي للاعتداء على البيانات والمعلومات الحكومية حيث نصت على " 1- يعاقب بالسجن المؤقت مدة لا تقل عن 7 سبع سنوات والغرامة التي لا تقل عن 500.000 خمسمائة ألف درهم ولا تزيد على 3.000.000 ثلاثة ملايين درهم كل من حصل أو استحوذ أو عدل أو أتلّف أو أفشى أو سرب أو ألغى أو حذف أو نسخ أو نشر أو أعاد نشر بغير تصريح بيانات أو معلومات حكومية سرية.

2- وتكون العقوبة السجن المؤقت مدة لا تقل عن 10 سنوات والغرامة التي لا تقل عن 500.000 خمسمائة ألف درهم ولا تزيد على 5.000.000 خمسة ملايين درهم إذا ترتب على الأفعال المنصوص عليها بالبند 1 من هذه المادة أضراراً للدولة، أو إذا ترتب عليها فقدان

1- بعقيبي عبير، المرجع السليق، ص 160.

2- المادة السادسة من قانون مكافحة الشائعات والجرائم الالكترونية الاماراتي لسنة 2021.

سرية عمل الأنظمة والبرمجيات الإلكترونية الخاصة بالمنشآت العسكرية والأمنية وما يتعلق بالاتصال ونقل المعلومات السرية.

3- ويعاقب بالسجن المؤقت كل من تلقى أي من البيانات والمعلومات المشار إليها بالبند 1 من هذه المادة، واحتفظ بها أو خزنها أو قبل التعامل بها أو استخدامها رغم علمه بعدم مشروعية الحصول عليها"¹.

أعتبر المشرع الإماراتي جريمة الإلتلاف المعلوماتي من قبيل الجرائم العمدية التي تتطلب قصدا جنائيا عاما بعنصرية العلم والإرادة، أي العلم بالنشاط الإجرامي الذي يقوم به الجاني ليس له الحق للقيام به، واتجاه إرادته إلى تحقيق نتيجة فعل الإدخال أو المحو أو التعديل، ولم يشترط المشرع الإماراتي توافر القصد الجنائي الخاص لقيام الجريمة وإنما اكتفى بالقصد العام أي قيام الجريمة بمجرد القيام بالسلوك الإجرامي.

وأقر المشرع الإماراتي عقوبة لجريمة الإلتلاف المعلوماتي نصت عليها الفقرة الثانية من المادة الثانية سابقة الذكر أعلاه بالحبس مدة لا تقل عن 6 أشهر والغرامة التي لا تقل عن 150.000 درهم ولا تتجاوز 750.000 درهم أو إحدى هاتين العقوبتين.

والملاحظ أن المشرع الإماراتي قد تشدد في العقوبة وأعتبر توافر بعض الشروط ظرفا مشدد ومثال ذلك إذا كانت البيانات والمعلومات المتلفة شخصية، أو إذا تعلق الأمر بصفة الجاني كونه موظف، أو كانت الملفات المتلفة طبية أو حسابات مصرفية، وحدد لها عقوبة الحبس مدة لا تقل عن سنة وغرامة مالية لا تقل عن 250.000 درهم ولا تتجاوز 1000.000 درهم أو إحدى هاتين العقوبتين، كما تشدد في العقوبة في نص المادة الرابعة الفقرة الثانية² وحدد لها عقوبة السجن المؤقت أو الغرامة المالية التي لا تزيد عن مليون

1- المادة السابعة من قانون مكافحة الشائعات والجرائم الإلكترونية الاماراتي لسنة 2021.

2- المادة الرابعة من قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم 5 لسنة 2012 وتنص " يعاقب بالسجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تتجاوز مليون وخمسمائة ألف درهم كل من دخل بدون تصريح إلى موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواء كان الدخول، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية".

وخمسمائة ألف درهم إذا تعلق الأمر بأتلاف البيانات الحكومية والمعلومات السرية الخاصة بمنشأة مالية أو تجارية أو اقتصادية.

كما تشدد في عقوبة الإتلاف المعلوماتي إذا كانت الجريمة تستهدف الاعتداء على البيانات والمعلومات الحكومية، وحدد عقوبة للإتلاف الحبس لمدة لا تقل عن 7 سنوات وغرامة مالية لا تقل عن 500.000 ألف درهم، ولا تتجاوز 3000.000 درهم، كما ضاعف من العقوبة إذا كانت الجريمة تستهدف البيانات والمعلومات الحكومية بالحبس مدة لا تقل عن 10 سنوات والغرامة التي لا تقل عن 500.000 درهم ولا تزيد عن 3000.000 درهم، وهذا في حالة اقتران السلوك الإجرامي بمصلحة حماية أمن الدولة.

رابعاً: التشريع الأردني:

كغيره من التشريعات السابقة جرم المشرع الأردني جريمة الإتلاف المعلوماتي في قانون الجرائم الإلكترونية حيث تنص المادة الرابعة على " يعاقب كل من ادخل أو نشر أو استخدم قصدا برنامجا عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ أو التقاط أو تمكين الآخرين من الاطلاع على بيانات أو معلومات أو إعاقة أو تشويش أو إيقاف أو تعطيل عمل نظام معلومات أو الوصول إليه أو تغيير موقع الكتروني أو الغائه أو اتلافه أو تعديل محتوياته أو اشغاله أو انتحال صفته أو انتحال شخصية مالكه دون تصريح أو بما يجاوز أو يخالف التصريح يعاقب بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنة وبغرامة لا تقل عن 200 مائتي دينار ولا تزيد على 1000 ألف دينار¹، وبالنظر إلى المادة أعلاه نجد أن المشرع الأردني قد استخدم مصطلحات عدة في وصفة للسلوك الإجرامي الذي يمثل جريمة الإتلاف المعلوماتي، ولعل ذلك يرجع إلى رغبة المشرع الأردني في توفير أكبر حماية ممكنة للمعلومات والبيانات والمواقع الإلكترونية.

وتكون العقوبة السجن مدة لا تقل عن خمس 5 سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز 2 مليون درهم ، إذا تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر .

1- المادة الرابعة من قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015.

إضافة إلى ما سبق تناول المشرع الأردني جريمة الإتلاف المعلوماتي في القانون رقم 17 لسنة 2023 في المادة الثالثة منه والتي نصت على تجريم الأفعال مقترنه بفعل الدخول غير المشروع وجاء نص المادة كالتالي "... إذا كان الدخول أو الوصول المنصوص عليه في الفقرة ' أ ' من هذه المادة لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو نشر أو إعادة نشر أو لإتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو خسارة سريتها و تشفير أو إيقاف أو تعطيل عمل الشبكة المعلوماتية أو نظام معلومات أو تقنية معلومات أو أي جزء منها، فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد عن سنة وبغرامة مالية لا تقل عن 600 دينار ولا تزيد عن 3000 دينار، وتكون العقوبة الحبس مدة لا تقل عن سنة ولا تزيد عن ثلاث سنوات، وغرامة مالية لا تقل عن 3000 دينار ولا تزيد عن 15000 دينار إذا تمكن من تحقيق نتيجة"¹.

أما المادة السادسة فقد نصت صراحة على الأفعال الإجرامية التي تمثل جريمة الاتلاف المعلوماتي وجاء نصها " يعاقب كل من أدخل أو نشر أستخدم قصداً برنامجاً أو امر برمجياً عن طريق الشبكة المعلوماتية او وسيلة تقنية معلومات أو باستخدام نظام معلومات لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو أتلاف أو حجب أو تشفير أو تعديل أو تغيير أو نقل أو نسخ أو التقاط أو تمكين الآخرين من الاطلاع على بيانات أو معلومات أو إعاقه أو تشويش أو وقف أو تعطيل عمل نظام المعلومات أو الوصول إليه أو تغيير موقع إلكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو أشغاله دون تصريح أو بما يجاوز أو يخالف ذلك التصريح أو انتحال صفته أو انتحال شخصية ماله بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن 2500 دينار ولا تزيد عن 10000 دينار"².

من خلال ما نص عليه المشرع الأردني في الفقرة "ج" من نفس المادة فيتضح أنه يقصد به قيام الركن المعنوي لجريمة الاتلاف المعلوماتي حيث اعتبرها من الجرائم العمدية أي يكفي لقيامها القصد الجنائي العام، إلا أنه استلزم القصد الجنائي الخاص في نفس المادة في الفقرة "ج" والمتمثل في تحقيق الغاية التي تم الدخول من أجلها حيث نصت الفقرة "ج" من المادة

1- المادة الثالثة من قانون مكافحة الجرائم الإلكترونية الأردني رقم 17 لسنة 2023.

2- المادة السادسة من قانون مكافحة الجرائم الإلكترونية الأردني رقم 17 لسنة 2023.

الثالثة على " يعاقب كل من دخل أو وصل قصدا موقع إلكتروني لتغيير أو إلغائه أو اتلافه أو تعديل محتوياته أو إشغاله أو تشفيره وإيقافه أو تعطيله أو انتحال صفته أو انتحال شخصية مالكه بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن 600 دينار ولا تزيد عن 3000 دينار"، وبذلك فقد تطلب المشرع توافر القصد الجنائي الخاص والذي كان سببا في تشديد العقوبة، فجعل من توافر الغاية المتمثلة في تحقيق نتيجة في حالة الدخول غير المشروع باعث خاص يستوجب تشديد العقوبة.

المطلب الثالث: معالجة جريمة الإلتلاف المعلوماتي في التشريع الدولي.

وسنتناول في هذا المطلب معالجة جريمة الإلتلاف المعلوماتي في اتفاقية بودابست لسنة 2001 والاتفاقية العربية لمكافحة الجرائم المعلوماتية لسنة 2010.

أولاً: جريمة الإلتلاف المعلوماتي في اتفاقية بودابست.

تتناول المادة الرابعة من اتفاقية بودابست بشأن الجرائم الإلكترونية لعام 2001 تجريم الإلتلاف المعلوماتي وتصلت على " - يجب على كل عضو أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية لتجريم، تبعا لتشريعته الداخلي، إذا حدث ذلك عمداً، ودون حق، أي أضرار، أو محو، أو تعطيل، أو إلتلاف، أو طمس لبيانات الحاسب.

د- يمكن لأي طرف ان يحتفظ بحق اشتراط أن يكون السلوك المنصوص عليه في الفقرة الأولى يؤدي إلى أضرار جسيمة"¹.

وتشير المذكرة التفسيرية إلى أن الهدف من تقرير هذا النص هو أن تكون البيانات وبرامج الحاسب الآلي مكفولة بحماية مماثلة لتلك التي تتمتع بها الأشياء المادية ضد الأضرار التي تحدث عمداً، والمصلحة المحمية هنا هي سلامة بيانات أو برامج النظام المخزنة وحسن تشغيلها واستخدامها.

وقد ورد في الفقرة الأولى من المادة الرابعة مصطلح الأضرار ومصطلح التعديل، وهي من الأعمال المترابكة التي تتصل على وجه الخصوص بالإلتلاف السلبي لسلامة أو محتوى

1- المادة الرابعة من اتفاقية بودابست لسنة 2001.

البيانات والبرامج، كما ورد مصطلح محو البيانات وهذا المصطلح يعادل تدمير الأشياء المادية، فهو يهدمها ويجعلها في حالة لا يمكن التعرف عليها، وقصدت بإتلاف بيانات الكمبيوتر أي عمل يمنع أو ينهي توافر البيانات للشخص الذي لديه حق النفاذ إل النظام أو لوسيلة حفظ البيانات التي تم تخزين البيانات عليها، وعنت بمصطلح " التغيير " تعديل البيانات القائمة وبالتالي فإن إدخال رموز خبيثة ، مقل الفيروسات وأحصنة طروادة مشمولة في هذه الفقرة¹.

كما أوضحت المادة أن تلك التصرفات لا يمكن المعاقبة عليها إلا إذا كانت قد ارتكبت بدون حق، عكس الأنشطة العادية المتمثلة في تصميم الشبكات أو تطبيقات شائعة للتشغيل أو الممارسات التجارية، أو التي تعد لمحاولات اختراق أو حماية أمن نظام معلوماتي والمصرح بها من قبل المالك أو مشغل النظام².

ولم تحدد الاتفاقية نوع معين من المعلومات والبيانات التي يحميها النص القانوني أذ كل الأنواع من المعلومات تكون محمية بالنص القانوني سواء تلك المؤمنة منها أو غير المؤمنة وذلك لأن القصد هو حماية سلامة وإتاحة المعلومات للجميع أثناء تعاملاتهم المعلوماتية، ويمكن

1- للمزيد أنظر في ذلك المذكرة التفسيرية لاتفاقية بودابست لعام 2001، المرجع السابق، المادة الرابعة الفقرة 61، ص11، كما تم معالجة جريمة الإتلاف المعلوماتي في العديد من الاتفاقيات والمؤتمرات الدولية ومنها، اتفاقية الاتحاد الافريقي 2012 بشأن إنشاء إطار قانوني للمساعدة في الامن السيبراني في أفريقيا في المواد 19-20-24، اتفاقية السوق المشتركة لشرق وجنوب افريقيا 2011 مشروع القانون النموذجي بشأن الامن السيبراني في المواد 20-22 فقرة أ، و كومنولث اتحاد الدول المستقلة 2001 اتفاقية بشأن التعاون في مكافحة الجرائم المتعلقة بالمعلومات الحاسوبية في المادة 3 فقرة ج، والبروتوكول الاختياري لاتفاقية بودابست 2001 المادة 4، والجماعة الاقتصادية لدول غرب افريقيا 2009 مشوع توجيهي بشأن مكافحة الجريمة السيبرانية داخل دول غرب أفريقيا في المواد 5 و7، الاتحاد الأوروبي 2005 القرار الإطاري للمجلس 2005/222/JHA بشأن الهجمات ضد نظم المعلومات في المادة 4، والاتحاد الأوروبي من خلال المشروع النهائي التوجيهي للجنة التنفيذية 2010/073 بالبرلمان الأوروبي ومجلس أوروبا بشأن الهجمات ضد نظم المعلومات وإلغاء القرار الإطاري للمجلس 2005/222/JHA في المادة 5، و الاتحاد الأوروبي 2001 في القرار الإطاري للمجلس الأوروبي 2001/413/JHA لمكافحة الاحتيال والتزوير و وسائط الدفع غير النقدية في المادة 3، والاتحاد الدولي للإتصالات الجماعة الكاريبية 2010 بشأن الجريمة السيبرانية CTU/CQRICO/ITU في المادة 7.

2- د طارق أبراهيم الدسوقي عطية، المرجع السابق، ص 309 310 311، و د دلخار صلاح بوتاني، المرجع السابق، ص 281 282.

للدول الأعضاء اشتراط درجة من الجسامة في فعل الائتلاف المعلوماتي بما يؤثر على المصلحة المبتغاة من هذا النص¹.

وسمحت الاتفاقية في الفقرة الثانية من المادة الرابعة للدول الأطراف بالتحفظ بشأن الجرم من حيث أنها قد تقتضي أن يؤدي إلى ضرر جسيم في أشاره للقصد الجنائي الخاص، وتركت للتشريع المحلي الحرية في تفسير ما يشكل ضرر جسيما، مع ضرورة أشعار الامين العام لمجلس أوروبا بتفسيرها اذا ما تم استخدام هذا التحفظ.

ثانيا: جريمة الإئتلاف المعلوماتي في الاتفاقية العربية.

تناولت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات جريمة الإئتلاف المعلوماتي في المادة الثامنة بعنوان "الاعتداء على سلامة البيانات" وتتص على " - تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا وبدون وجه حق، - للطرف أن يستلزم لتجريم الأفعال المنصوص عليها في الفقرة (1) من هذه المادة، أن تتسبب بضرر جسيم"².

والملاحظ أن المادة الثامنة أضافت فعليين يدخلان في باب المساس بسلامة البيانات وهما الحجب والتدمير، والليذان يقابلهما في اتفاقية بودابست في المادة الرابعة مصطلحي الإئتلاف والطمس وهما مصطلحان مترادفان يؤديان نفس المعني.

ومن حيث العقوبة تشدد المشرع العربي في عقوبة جريمة الإئتلاف في الفقرة الثانية من المادة السادسة والتي تنص على " تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة ولأجهزة والأنظمة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين".

1- أيمن عبدالله فكري، المرجع السابق، ص 297.

2- المادة الثامنة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

المبحث الرابع: جريمة الإعاقة الخطيرة للنظام المعلوماتي.

تشمل جريمة إعاقة النظام المعلوماتي الاعتداء على النظام وتدميره من خلال إعاقة سير عمل النظام أو ما يسبب تأخير عمله وعدم استقراره، أو ما يسبب جعله غير صالح للخدمة أما كالشلل التام أو المؤقت في عمله، فهي تتعلق بالتخريب المتعمد لنظام المعلومات أو أي من أدواته أو تعطيله، وتعد من الجرائم العمدية نظرا لما تحدثه من آثار خطيرة على أمن المجتمع والاقتصاد في الدولة فقد يؤدي توقيف نظام معين عن العمل إلى التسبب في كارثة بيئية أو صحية تنعكس أثارها السلبية على المجتمع ككل.

وفي شأن التعريف يوجد العديد من التعريفات لجريمة إعاقة النظام المعلوماتي والتي غالبيتها تؤكد على نتيجة هذه الجريمة المتمثلة في إمتناع النظام عن إداء وظائفه بصورة تامة أو جزئية، أو حدوث تغيير في حالة عمل النظام، وفي هذا الشأن فإننا ندعم تعريف جريمة الإعاقة الخطيرة للنظام المعلوماتي الذي قدمته الدكتورة مفيدة مباركية وعرفت من خلاله جريمة إعاقة النظام بأنها " كل معالجة آلية للبيانات تتم عمدا ودون حق، تمنع النظام المعلوماتي من أداء وظيفته المخول له أدائها ابتداء بكل سلاسة وفاعلية"¹، ولإيضاح والتفسير قمنا بتفصيل هذا المبحث كسابقه لثلاث مطالب نتناول في الأول منه تفضيل جريمة الإعاقة الخطيرة للنظام المعلوماتي، وفي الفرع الثاني المعالجة القانونية للجريمة في التشريعات الوطنية، أما الثالث فخصصناه للمعالجة الدولية لجريمة إعاقة النظام المعلوماتي.

1- مفيدة مباركية، المرجع السابق، ص 150.

المطلب الأول: تفصيل جريمة إعاقة النظام المعلوماتي.

ومن خلال التعريف السابق يظهر لنا محل جريمة إعاقة النظام المعلوماتي والمتمثل في التعدي على سلامة نظام المعلومات سواء نظام التشغيل أو البرامج التشغيلية التي تؤدي مهام أساسية في عمل النظام المعلوماتي، وغيرها من البرامج المسؤولة عن عمل النظام بصورة حسنة، فالغاية من تجريم الاعتداء عليها هو حماية النظام من التخريب والتعطيل العمدي متى كان أثره إعاقة سير التشغيل المعتدل¹.

أولاً: الركن المادي لجريمة أعاقه النظام:

يتمثل الركن المادي في هذه الجريمة بالنشاط الإجرامي الذي يؤدي إلى إعاقة النظام المعلوماتي وما ينتج عنه من عدم القدرة على الوصول إلى الخدمة، فلا إعاقة تمثل كل عمل من شأنه إرباك النظام وتعطيله وتخريب الأجهزة والشبكات.

1- فعل التعطيل أو الإعاقة:

يعني العطل في اللغة الخلو أو البقاء بلا عمل، وفي الاصطلاح فيقصد به فعل يتسبب في توقف أو تباطؤ أو إرباك عمل النظام المعلوماتي، ومعنى ذلك منع النظام المعلوماتي من العمل بصفة جزئية أو كليه أو منع أحد البرامج الموجودة داخله²، وبالتالي تعطيل سير وظائف النظام عن العمل، وعليه فأن التعطيل يكون موجهاً إلى برامج تشغيل النظام كالبرامج التشغيلية والتطبيقية التي يستند عليها النظام للقيام بعمله، وليس على المعلومات بالمعنى الضيق³.

ويمكن القيام بالتعطيل عبر العديد من الوسائل منها المادية والمعنوية، فالمادية تتمثل في وقوع النشاط الإجرامي على الأجهزة المادية للنظام عن طريق تخريبها أو كسرها أو سكب سائل عليها، وغيره من الأفعال التي من شأنها منع العاملين في النظام من العمل، إلا أن أياً من الصور المادية لا يمكن اعتبارها جريمة أعاقه خطيرة لعمل الأنظمة المعلوماتية، حتى وأن افضت هذه الأفعال على المساس بالمصلحة المحمية المتمثلة بسلامة عمل الأنظمة المعلوماتية،

1- عادل حماد عثمان حماد، حماية المعلومات في التشريع الجنائي السوداني (دراسة مقارنة)، جامعة نايف

العربية للعلوم الامنية الرياض، المملكة العربية السعودية، الطبعة الأولى 2013، ص 336.

2- بوربابة صورية، المرجع السابق، ص 98.

3- دلخار صلاح بوتاني، المرجع السابق، ص 230.

لأنها أفعال تتم بعيدا عن المعالجة الآلية للمعلومات¹، أما المعنوية فتكون عند وقوع النشاط الإجرامي على الكيانات المنطقية للنظام مثل البرامج وهذا بإدخال برامج فيروسيه تؤدي إلى توقيف النظام عن العمل بشكل دائم أو بصفة مؤقتة، بالإضافة إلى استخدام القنابل المعلوماتية الزمنية أو المنطقية².

2- فعل الإفساد:

يعني الإفساد لغةً الخلل أو التلف، وإصطلاحا واسقاطا على هذه الجريمة يقصد به "ممارسة أي فعل على النظام المعلوماتي من شأنه أن يعدل في وظيفته دون أن يعوقه عن أداء هذه الوظيفة"، أو هو تشويه أداء النظام المعلوماتي لعمله وجعله غير صالح للاستعمال، وهو بذلك يجعل النظام المعلوماتي في حالة يعطي نتائج غير تلك المراد الحصول عليها³، فالنظام المعلوماتي في حالة الإفساد لا يتوقف كليا وإنما لا يعمل بحالته الطبيعية، وهذا ما يقصد الجاني عندما يقوم بإخال ما من شأنه أن يتسبب في خلل للنظام المعلوماتي، وتختلف الطرق التي يمكن عبرها تحقيق فعل الإفساد في النظام المعلوماتي مثل استخدام القنبلة المعلوماتية والتي تتكاثر داخل النظام وتجعله غير صالح للاستعمال، و استخدام برنامج يحمل فيروساً يقوم بتغيير غير ملموس في البرامج والمعلومات الموجودة في النظام.

وفي ذات السياق وبالنظر إلى فعلي التعطيل والإفساد فإنه يصعب التمييز بينهما من حيث الوسائل التي يتحققان بها وهما كثيرا ما يتطابقا في المجال العملي، إلا أنه يجب التمييز بينهما وذلك تقديرا لمبدأ تقرير العقوبة، حيث أن الضرر الناتج عن التعطيل أكبر من الضرر الناتج عن الإفساد ذلك أن التعطيل يؤدي إلى توقف النظام بشكل كامل عن العمل عكس الإفساد الذي يبقى فيه النظام يؤدي وظيفته ولكن بشكل غير كامل وغير دقيق، مما يستدعي أن تكون عقوبة التعطيل أشد من عقوبة الإفساد⁴.

1- مفيدة مباركية، المرجع السابق، ص 153.

2- دلخار صلاح بوتاني، نفس المرجع ، ص 230.

3- بوربابة سورية، نفس المرجع، ص 98.

4- دلخار صلاح بوتاني، نفس المرجع ، ص 233.

وبناء على ما سبق فإن أفعال جريمة الإعاقة الخطيرة للنظام المعلوماتي لا تشكل جريمة إلا إذا أفضت إلى أعاققة النظام المعلوماتي عن أداء مهامه و وظائفه المفترضة، ويتعين أن تكون هذه الإعاقة ناتجة عن إتيان أحد الأفعال المذكورة أعلاه على سبيل المثال وهذا بأثبات العلاقة السببية بين السلوك والنتيجة.

ثانيا: الركن المعنوي لجريمة أعاققة النظام.

تعتبر جريمة أعاققة وإفساد النظام من الجرائم العمدية التي يلزم لقيامها القصد الجنائي العام بعنصريه العلم والإرادة، وقد تتطلب بعض التشريعات إضافة إلى القصد العان ضرورة توافر القصد الجنائي الخاص المتمثل في إحداث الضرر لمالك النظام او المستفيد منه، كون الفاعل يعلم مسبقاً أن فعل الإعاقة او الإفساد للنظام المعلوماتي لا شك يترتب عليه أحداث ضرر للغير¹.

المطلب الثاني: معالجة جريمة إعاقة النظام المعلوماتي في التشريع الجنائي.

عمدت بعض التشريعات إلى أفراد نص خاص بجريمة اعاققة النظام المعلوماتي على اعتبار انها جريمة مستقلة ومن باب حرصها على حماية مصلحة المستخدمين وحسن سير الأنظمة المعلوماتية، إلا أن هناك بعض التشريعات اعتبرتھا بالنظر إلى الأفعال التي يشملها التجريم تتصل مع جريمتي الإتلاف المعلوماتي والدخول غير المشروع، حيث يؤدي أتلاف المعلومات أو تعديل البرامج إلى الأضرار بحسن سير النظام المعلوماتي أو تعطيله او أعاقته، وسنقدم من خلال دراسة التشريعات المعتمدة في البحث صورة أكثر وضوحا للطبيعة القانونية لهذه الجريمة.

أولاً: التشريع الجزائري.

تناول المشرع الجزائري جريمة إعاقة النظام المعلوماتي في المادة 394 مكرر حيث نصت الفقرة الثالثة منها على " إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال

1- فايز محمد راجع غلاب، المرجع السابق، ص 246.

المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150.000 دج¹.

وما نلاحظه من نص المادة أن المشرع الجزائري لم يضع نص خاص لجريمة إعاقة أو إفساد النظام المعلوماتي وأكتفى بالفقرة الثالثة من المادة 394 مكرر بنتيجة تعطيل النظام كظرف مشدد لجريمة الدخول والبقاء عن طريق الغش، كما يلاحظ أن المشرع الجزائري يعالج صورة واحدة من صور الإعاقة للنظام المعلوماتي وهي المتعلقة بتخريب وتعطيل نظام التشغيل دون التطرق للصورة الثانية المتعلقة بإفساد النظام مع بقاءه سليماً يؤدي عملة.

ولعل ذلك يرجع إلى التشابه الكبير بين جريمة إعاقة النظام المعلوماتي وجريمة إتلاف المعلومات والمعطيات السابق ذكرها، حيث يصعب التمييز بينهم بسبب النتيجة التي تؤديها جريمة إتلاف المعطيات في الأخير وهي أعاقلة النظام و إفساده².

وبناء على موقف المشرع الجزائري من جريمة إعاقة النظام كظرف مشدد لجريمة الدخول غير المشروع فإنه لا يمكن العقاب على جريمة إعاقة النظام إلا بعد ارتكاب جريمة الدخول غير المشروع للمنظومة المعلوماتية، وعليه وباعتبار جريمة الدخول غير المشروع جريمة عمدية فإنه وتباعاً تعد جريمة تخريب و إعاقة النظام عمدية، لذلك لا يشترط المشرع عند عقابه على جريمة إعاقة النظام إظهار العمدية في فعل التعطيل وإنما يكفي إثبات العلاقة السببية بين جريمة الدخول غير المشروع وجريمة تعطيل النظام³.

ثانياً: التشريع السعودي.

تناول المشرع السعودي جريمة إعاقة وتعطيل النظام المعلوماتي بنص المادة الخامسة من قانون مكافحة جرائم المعلوماتية حيث جاء في فقرتيها الثانية والثالثة "... إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها أو تدميرها، أو مسح البرامج أو البيانات الموجودة أو

1- المادة 394 مكرر من قانون العقوبات الجزائري المعدل والمتمم.

2- معاشي سميرة، المرجع السابق، ص 115.

3- بعقيبي عبير، المرجع السابق، ص 145.

المستخدمة فيها أو حذفها أو تسريبها أو اتلافها أو تعديلها،... إعاقة الوصول إلى الخدمة، أو تشويهها، أو تعطيلها، بأي وسيلة كانت"¹.

والظاهر من نص المادة أعلاه أن المشرع السعودي لم يشترط توافر عنصر المعالجة الآلية في إكمال الركن المادي لجريمة إعاقة النظام المعلوماتي وهذا ما يفهم من قوله "بأي وسيلة كانت"، وعليه فأنها يمكن أن ترتكب بأي وسيلة مادية أخرى، كما أنه أقتصر التجريم على الشبكة المعلوماتية، ومعنى ذلك أن جرائم الإعاقة الخطيرة الواقعة على الأنظمة المعلوماتية المعزولة عن غيرها من الأنظمة عبر الشبكة لا يشملها التجريم الوارد في هذا النص².

إلا أنه يشترط أن تتحقق نتيجة معينة على السلوك الإيجابي الذي يصدر من الجاني، وهي إما تعطيل النظام أو تدمير ومسح البيانات الموجودة فيه، وهذا كله بغض النظر عن الوسيلة المستخدمة في إتيان السلوك الإجرامي، سواء تم ذلك عبر أذخار برامج خبيثة للنظام أو عبر تضخيم البريد الإلكتروني³.

ويعاقب المشرع السعودي على جريمة الإعاقة الخطيرة للنظام المعلوماتي بعقوبة السجن التي لا تتجاوز مدته أربع سنوات وبغرامة مالية لا تزيد عن ثلاثة ملايين ريال أو بإحدى العقوبتين.

ثالثا التشريع الإماراتي.

تناول المشرع الإماراتي جريمة الإعاقة الخطيرة للنظام المعلوماتي في القانون الاتحادي لسنة رقم 5 لسنة 2012 الملغي في المادتين الثامنة والعاشرة منه والتي جاء نصهما كالتالي " يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تتجاوز ثلاثمائة ألف درهم أو إحدى هاتين العقوبتين كل من أعاق أو عطل الوصول إلى الشبكة المعلوماتية أو موقع إلكتروني أو نظام معلوماتي إلكتروني"⁴.

1- المادة الخامسة من نظام مكافحة الجرائم المعلوماتية السعودي.

2- مباركية مفيدة، المرجع السابق، ص 158.

3- دلخار صلاح بوتاني، المرجع السابق، ص 248.

4- المادة الثامنة من قانون مكافحة جرائم تقنية المعلومات الإماراتي.

أما المادة العاشرة فنصت " يعاقب بالحبس مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تتجاوز ثلاثة ملايين درهم أو بإحدى هاتين العقوبتين كل من أدخل عمدا وبدون تصريح برنامج معلوماتي إلى شبكة المعلومات أو نظام معلوماتي إلكتروني أو إحدى وسائل تقنية المعلومات، وأدى ذلك إلى إيقافها عن العمل أو تعطيلها أو تدميرها أو مسح أو حذف أو إتلاف أو تغيير البرامج أو النظام أو الموقع الإلكتروني أو البيانات أو المعلومات.

وتكون العقوبة السجن والغرامة التي لا تتجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين إذا لم تحقق النتيجة، وتكون العقوبة الحبس أو الغرامة أو إحدى هاتين العقوبتين عن أي فعل عمدي يقصد به اختراق البريد الإلكتروني بالرسائل وإيقافه عن العمل أو تعطيل أو إتلاف محتوياته¹.

وفي القانون الجديد لسنة 2021 نصت المادة الرابعة على جريمة إعاقة النظام المعلوماتي تحت عنوان الإضرار بأنظمة المعلومات ونصت على "1- يعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن 500.000 خمسمائة ألف درهم ولا تزيد على 3.000.000 ثلاثة ملايين درهم، أو بإحدى هاتين العقوبتين، كل من تسبب عمداً في الإضرار أو تدمير أو إيقاف أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات.

2- تكون العقوبة السجن المؤقت والغرامة التي لا تقل 500.000 خمسمائة ألف درهم ولا تزيد على 3.000.000 ثلاثة ملايين درهم، إذا كان الإضرار قد لحق جهة مصرفية أو إعلامية أو صحية أو علمية، أو إذا كان الغرض من ذلك تحقيق أمر غير مشروع أو وقعت الجريمة نتيجة لهجمة إلكترونية².

بالنظر إلى المواد أعلاه نجد أن المشرع الإماراتي قد حدد صوراً عديدة للسلوك الإجرامي المكون للركن المادي لجريمة إعاقة النظام المعلوماتي ومنها " إعاقة أو تعطيل الوصول إلى خدمات الحاسب الآلي والموقع الإلكتروني وغيرها..."، حيث لم يشترط المشرع وسيلة معينة

1- المادة العاشرة من نفس القانون.

2- المادة الرابعة من قانون مكافحة الشائعات والجرائم الإلكترونية الاماراتي لسنة 2021.

لحدوث الإعاقة فمن الممكن وقوعها بطريقة مادية أو معنوية، فالمادية تتمثل في السلوكيات التي تقع على أجهزة الحاسب الآلي وشبكات الاتصالات مثل افعال العنف والتخريب وقطع شبكات الاتصال، أما الطريقة المعنوية فقد تكون إذا وقعت على الكيانات المنطقية للنظام والبرامج والمعطيات، ونتيجة لذلك تكون جريمة إعاقة وإفساد النظام بإيقافه عن العمل أو تعطيله أو تدمير البرامج أو النظام، ويستوي في ذلك ان يكون التوقف دائماً أو مؤقتاً كما يمكن أن تكون الإعاقة كلياً أو جزئياً¹.

أما من حيث قيام الركن المعنوي لجريمة الإعاقة في التشريع الإماراتي فقد اعتبرها المشرع من قبيل الجرائم العمدية والتي تقوم على توافر القصد الجنائي العام فيها بعنصريه العلم و الإرادة وهذا ما أبرزته المادة العاشرة من القانون الملغي بنصها " كل من أدخل عمداً..." الواردة في مقدمة المادة، وبذلك تستوجب العقوبة التي حددها المشرع في المادة الثامنة والعاشرة ففي الأولى وهي حالة إعاقة وتعطيل الوصول إلى الشبكة المعلوماتية تكون العقوبة المفروضة الحبس أو الغرامة المالية التي لا تقل عن مائة ألف درهم ولا تتجاوز ثلاثمائة ألف درهم أو إحدى هاتين العقوبتين.

أما في الحالة الثانية والمتمثلة في إدخال برنامج معلوماتي إلى النظام يؤدي إلى إيقافه أو تعطيله، فقرر المشرع تشديد العقوبة متى تحققت النتيجة الإجرامية، إذ قرر لها عقوبة السجن مدة لا تقل عن خمسة سنوات وغرامة مالية التي لا تقل عن خمسمائة ألف درهم ولا تتجاوز ثلاثة ملايين درهم، أو إحدى هاتين العقوبتين، وإذا لم تتحقق النتيجة تكون العقوبة السجن والغرامة التي لا تتجاوز خمسمائة ألف درهم أو إحدى هاتين العقوبتين².

ما يلاحظ على القانون الجديد لسنة 2021 أن المشرع الإماراتي قد تشدد في عقوبة جريمة أعاق النظام المعلوماتي في حال أستهذفت الإعاقة مؤسسات الدولة والمرافق الحيوية، حيث نص على ذلك في المادة الخامسة من قانون مكافحة الشائعات والجرائم الالكترونية لسنة 2021 بالاتي "يعاقب بالسجن المؤقت والغرامة التي لا تقل عن 500.000 خمسمائة ألف

1- بعقبي عبير، المرجع السابق، ص 152 153.

2- أنظر المادة العاشرة من قانون مكافحة جرائم تقنية المعلومات الإماراتي.

درهم ولا تزيد على 3.000.000 ثلاثة ملايين درهم، كل من تسبب عمداً في الإضرار أو تدمير أو إيقاف أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، عائدة لمؤسسات الدولة أو أحد المرافق الحيوية، فإذا وقعت الجريمة نتيجة لهجمة إلكترونية أعتبر ذلك ظرفاً مشدداً¹.

رابعاً: التشريع الأردني.

تناول المشرع الأردني جريمة إعاقة النظام المعلوماتي في المادة السادسة من القانون الجديد رقم 17 لسنة 2023 والتي نصت على " يعاقب كل من أدخل أو نشر أو استخدم قصداً برنامجاً أو أمراً برمجياً عن طريق الشبكة المعلوماتية أو وسيلة تقنية معلومات أو باستخدام نظام معلومات لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تشفير أو تعديل أو تغيير أو نقل أو نسخ أو إلتقاط أو تمكين الآخرين من الاطلاع على بيانات أو معلومات أو إعاقة أو تشويش أو وقف أو تعطيل عمل نظام المعلومات أو الوصول إليه أو تغيير موقع إلكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله دون تصريح أو بما يجاوز أو يخالف ذلك التصريح أو انتحال صفته أو انتحال شخصية مالكه بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن 2500 ألفان وخمسمائة دينار ولا تزيد عن 10000 عشرة آلاف دينار"².

والملاحظ من نص المادة أعلاه أن المشرع الأردني قد توسع في تحديد الأفعال التي تشكل الركن المادي لجريمة إعاقة وتعطيل النظام المعلوماتي بحيث عدد صوراً عديدة اعتبرها من السلوكيات المجرمة والتي يعد توافرها أو توافر أحداها مقيماً للجريمة بشرط أن يتم ذلك عبر الشبكة المعلوماتية أو النظام المعلوماتي، كما حدد بعضاً من السلوكيات التي تستهدف البرنامج أي يكون محلاً للجرم بحيث يكون البرنامج محل الاعتداء بالإدخال أو النشر أو بالاستعمال أو بزرعة الفيروسات أو القنابل المنطقية والزمنية.

1- المادة الخامسة من قانون مكافحة الشائعات والجرائم الإلكترونية الاماراتي لسنة 2021، المرجع السابق

2- المادة السادسة من قانون الجرائم الإلكترونية الاردني رقم 17 لسنة 2023، المرجع السابق

أما من حيث النتيجة فلم يشترط المشرع الأردني حدوث نتيجة حيث أعتبر جريمة أعاقاة النظام المعلوماتي من الجرائم الشكلية التي تقع بمجرد القيام بالفعل دون الحصول على نتيجة أو بمعنى آخر يستوى حدوث أو عدم حدوث نتيجة فيها¹.

كما ويعتبر المشرع الأردني جريمة أعاقاة النظام المعلوماتي من الجرائم العمدية التي يكفي فيها لقيام الركن المعنوي توافر عنصرية العلم والإرادة، وعبر عن ذلك صراحة في نص المادة السادسة، فالجاني يجب أن يكون عالماً بقيامة بالنشاط المجرم كالإدخال أو النشر أو الاستخدام أو الاعاقاة أو التشويش أو التعطيل، وأن تتم هذه الأفعال عن طريق الشبكة المعلوماتية، إضافة إلى اتجاه أرائه للقيام بالسلوك المكون للجريمة.

ومن حيث العقوبة فإن الملاحظ تشدد المشرع الأردني في عقوبة جريمة إعاقاة وتعطيل النظام مقارنة بالعقوبة التي كانت مقررة في المادة الرابعة من القانون الملغي رقم 27 لسنة 2015، حيث نصت المادة السادسة من القانون الجديد على عقوبة أعلى تتمثل في الحبس الذي لا تقل مدته عن ستة أشهر وبغرامة لا تقل عن 2500 ألفان وخمسمائة دينار ولا تزيد عن 10000 عشرة آلاف دينار².

المطلب الثالث: معالجة جريمة أعاقاة النظام المعلوماتي في التشريع الدولي.

وسنحاول هذا المطلب معالجة جريمة أعاقاة النظام المعلوماتي حسب ما جاءت به اتفاقية بودابست لسنة 2001 والاتفاقية العربية لمكافحة الجرائم المعلوماتية لسنة 2010.

أولاً: جريمة اعاقاة النظام في اتفاقية بودابست.

نصت المادة الخامسة من اتفاقية بودابست على الجرائم التي تستهدف سلامة النظام المعلوماتي، حيث خص المشرع الدولي الإلتلاف والإعاقاة الواقعة على وظيفة النظام المعلوماتي بنص مستقل وهذا للتأكيد على تجريم الإعاقاة الواقع على عمل النظام وبالدرجة الأولى جريمة إعاقاة النظام حيث جاء نصها كالتالي (تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير ترى أنها ضرورية لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير

1- عبد الإله النوايسة، المرجع السابق، ص 264.

2- راجع المادة السادسة من قانون الجرائم الالكترونية الاردني رقم 17 لسنة 2023.

حق: الإعاقة الخطيرة لاشتغال نظام الحاسب عن طريق إدخال بيانات حاسوبية، إرسالها، إتلافها، حذفها، إفسادها، تغييرها أو تدميرها¹.

وبالنظر إلى تفسير المادة أعلاه يظهر الهدف منها وهو تجريم العرقلة والاعتداء المتعمد على أنظمة الحاسب الآلي بما في ذلك الاتصالات السلكية واللاسلكية، وهذا من خلال استخدام معلومات وبيانات الحاسب الآلي أو التأثير عليها، كما وتظهر المصلحة المحمية من خلال نص المادة وهي حماية مصلحة سلامة عمل النظام ومشغلي ومستخدمي أنظمة المعلومات والحاسب الآلي بحيث يكونوا قادرين على تشغيلها بشكل سليم وبدون إعاقة.

ويشير مصطلح العرقلة الوارد في المادة أعلاه إلى الإجراءات التي تعترض التشغيل السليم للنظام المعلوماتي متمثلة في عمليات إدخال بيانات للنظام أو نقلها أو إتلافها أو حذفها أو تغييرها أو تدميرها، والتي يباشرها الجاني بدون وجه حق، أما ما يكون من أفعال حماية النظام المعلوماتي أو إعادة تشكيل النظام أو أعمال ولوج غير مشروع ولكن بترخيص من قبل المالك، فلا تشملها هذه المادة بالتجريم حتى وأن تسببت في عرقلة جسيمة للنظام المعلوماتي².

1- المادة الخامسة من اتفاقية بودابست لسنة 2001.

2- للمزيد أنظر في ذلك المذكرة التفسيرية لاتفاقية بودابست لعام 2001، المرجع السابق، المادة الخامسة الفقرة 68، ص12، كما تم معالجة جريمة التدخل والإعاقة غير القانونية في النظام الحاسوبي في اتفاقية الاتحاد الأفريقي 2012 بشأن إنشاء إطار قانوني للمساعدة في الأمن السيبراني في أفريقيا في المواد 18 و 19، اتفاقية السوق المشتركة لشرق وجنوب أفريقيا 2011 مشروع القانون النموذجي بشأن الأمن السيبراني في المادة 22 فقرة أ، و كومنولث اتحاد الدول المستقلة 2001 اتفاقية بشأن التعاون في مكافحة الجرائم المتعلقة بالمعلومات الحاسوبية في المادة 3 فقرة ج، والبروتوكول الاختياري لاتفاقية بودابست 2001 المادة 5، والجماعة الاقتصادية لدول غرب أفريقيا 2009 مشروع توجيهي بشأن مكافحة الجريمة السيبرانية داخل دول غرب أفريقيا في المادة 5، الاتحاد الأوروبي 2005 القرار الإطاري للمجلس 2005/222/JHA بشأن الهجمات ضد نظم المعلومات في المادة 3، والاتحاد الأوروبي من خلال المشروع النهائي التوجيهي للجنة التنفيذية 2010/073 بالبرلمان الأوروبي ومجلس أوروبا بشأن الهجمات ضد نظم المعلومات وإلغاء القرار الإطاري للمجلس 2005/222/JHA في المادة 4، و الاتحاد الأوروبي 2001 في القرار الإطاري للمجلس الأوروبي 2001/413/JHA لمكافحة الاحتيال والتزوير و وسائل الدفع غير النقدية في المادة 3، والاتحاد الدولي للاتصالات الجماعة الكاريبية 2010 بشأن الجريمة السيبرانية CTU/CQRICO/ITU في المادة 9.

وأشارت المادة إلى عمدية جريمة أعاق النظام المعلوماتي بمعنى أن تكون لدى الجاني نية العرقلة الجسيمة للنظام، ووفقاً للاتفاقية تكون العرقلة جسيمة عندما تكون البيانات المرسلة أو المدخلة من الحجم أو التواتر ما يحدث ضرراً جسيماً لقدرة المالك أو المشغل على استخدام النظام بصورة سليمة وطبيعية¹.

كما أعطت المادة الحرية للأطراف في تحديد متى وفي أي الأحوال يعد النظام معاقاً جزئياً أو كلياً، بشكل مؤقت أو دائم حتى يمكن معرفة ما إذا كانت الإعاقة تستوجب جزاءً إدارياً أم جزاءً جنائياً بمقتضى قانونهم الداخلي².

ثانياً: جريمة أعاق النظام في الاتفاقية العربية.

تناول المشرع العربي جريمة أعاق النظام المعلوماتي في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وهذا في المادة الثامنة بعنوان الاعتداء على سلامة البيانات والتي نصت على "1- تدمير أو محو أو أعاق أو تعديل أو حجب بيانات تقنية المعلومات قصداً وبدون وجه حق، 2- للطرف أن يستلزم التجريم الأفعال المنصوص عليها في الفقرة (1) من هذه المادة، ان تتسبب بضرر جسيم"³.

والملاحظ على المادة الثامنة من الاتفاقية أنها ذكرت جريمة إعاق النظام المعلوماتي ولم تذكر جريمة الإفساد، كما أنها في الفقرة الثانية اعطت الحرية للدول للأطراف في تحديد الافعال والسلوكيات الإجرامية الجسيمة ومستوى الضرر الذي تتسبب به ومن خلاله يمكن قياس مستوى الجسامة، كما تناول القانون العربي النموذجي جريمة الاعاق الخطيرة للنظام المعلوماتي وجريمة تعطيل وافساد النظام في المادة السابعة منع والتي تنص على " كل ما إعاق أو شوش أو عطل عمداً أو بأي وسيلة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات يعاقب بالحبس ... والغرامة... أو بإحدى هاتين العقوبتين"⁴.

1- أيمن عبدالله فكري، المرجع السابق، ص 299.

2- طارق أبراهيم الدسوقي عطية، المرجع السابق، ص 318.

3- المادة الثامنة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، المرجع السابق.

4- المادة السابعة من القانون العربي النموذجي لمكافحة جرائم تقنية المعلومات.

إن هذه المادة جاءت أكثر وضوحاً من المادة الثامنة من الاتفاقية العربية من حيث التجريم فحددت الأفعال التي تشكل جريمة أعاقا وإفساد النظام المعلوماتي كما حددت الوسيلة التي تتم عبرها أي الشبكة المعلوماتية، إضافة إلى ذلك أكدت على عمدية جريمة تعطيل وإفساد النظام¹.

الفصل الثاني: الجرائم المرتكبة عبر النظم المعلوماتية.

أن ما يميز جرائم الصنف الثاني هو أنها جرائم معروفة قبل ظهور البيانات والأنظمة المعلوماتية، مقارنة بجرائم الصنف الأول والتي هي أفعال مستحدثة تهدد سرية وسلامة الأنظمة المعلوماتية بالدرجة الأولى، والملاحظ في على هذا النوع من الجرائم أنها لا تستهدف البيانات والمعلومات بالدرجة الأولى وإنما تهدد مصالح أخرى ولكنها تتخذ من الانظمة المعلوماتية وسيلة لإرتكابها والتي بدونها لن نكون أما هذا النوع من الجرائم، وسنتناول في هذا الفصل أربعة أنواع من الجرائم التي ترتكب عبر الأنظمة المعلوماتية وتشمل، جريمة التزوير المعلوماتي، وجريمة الغش المعلوماتي، وجريمة إباحية الأطفال عبر الأنظمة المعلوماتية، جريمة الاعتداء على الملكية الفكرية.

المبحث الأول: جريمة التزوير المعلوماتي.

هذه الجريمة ليست مستحدثة كغيرها من الجرائم التي تناولناها في المبحث الأول، بل تعد امتداداً طبيعياً لجريمة التزوير التقليدية، فهي بالنظر إلى موضوعها تهدد الثقة في المعاملات عبر الأنظمة المعلوماتية شأنها في ذلك شأن جريمة التزوير الواقعة على المحررات التقليدية.

ويعرف التزوير في اللغة بأنه تزوين الكذب، وفي الاصطلاح يعني به إصلاح الكلام وتهيينته وتزويقه، والتزوير بالمدلول العام هو تغيير الحقيقة بغض النظر عن وسيلته أو موضوعه، وتزوير المحرر المعلوماتي² هو تغيير للحقيقة الأصلية فيه بطريقة من طرق التغيير كالتوقيع أو الحذف أو الإضافة أو التعديل بما يترتب عليه ضرر للغير¹.

1- دلخار صلاح بوتاني، المرجع السابق، ص 250.

2- وفي هذا الصدد لا بد من تعريف المحرر المعلوماتي، حيث يعرف على أنه " كل جسم منفصل أو يمكن أن يتم فصله عن نظام المعالجة الآلية للمعلومات، وقد سجلت عليه معلومات معينة سواء أكان معداً للاستخدام

أما فقهاء فيعرف التزوير بأنه " تغيير للحقيقة بقصد تزوير مستند أو وثيقة بما يحقق الضرر بالغير سواء كان هذا التغيير بطريقة معنوية أو مادية"، وبالتالي فهو ينصب على وثيقة من أجل تغيير محتواها ومعناها بما يخدم مصلحة المزور ويرتب ضرر للغير أو للمصلحة العامة.

فالتزوير المعلوماتي يعتبر من أخطر صور الغش المرتبط بالمعلوماتية وهذا بسبب حلول النظام المعلوماتي محل الوثائق والمحركات في تسجيل التصرفات والاعمال القانونية التي ترتب حقوق وتنشأ التزامات للجميع، وبالتالي انتقال الثقة من إطار المحركات التقليدية فقط لتشمل المحركات المعلوماتية².

وعليه يمكن تعريف التزوير المعلوماتي على أنه " أي تغيير في مخرجات الحاسب الآلي سواء كانت مخرجات مكتوبة أو كانت مرسومة ومكتوبة ومحفوظة داخل النظام ولها أثر قانوني معين بإثبات حق أو التزام، بغض النظر عن اللغة التي كتبت بها"، فهو إذا تلاعب بمنتجات نظام المعالجة الآلية للنظام أو بمصلح أصح التلاعب بالمستند المعلوماتي سواء بخصائصه أو ما يحتوي عليه من معلومات بقصد استخدامه والاستفادة منه زورا³.

وبهذا يمكن أن يتخذ التزوير المعلوماتي إحدى الصورتين، وتتمثل الأولى في التلاعب في معلومات داخل النظام المعلوماتي والحاسب الآلي ويكون ذلك بتغيير الحقيقة في هذه المعلومات والتلاعب بها وتعديلها، والثانية إدخال معلومات غير صحيحة لصناعة مستند غير صحيح، وفي كلتا الحالتين يتم استخدام تكنولوجيا المعلومات لإكمال التزوير⁴.

وفي هذا الشأن وجب علينا تمييز جريمة التزوير المعلوماتي عن جريمة التزوير التقليدي وجريمة التلاعب غير المصرح به:

بواسطة نظام المعالجة الآلية للمعلومات أم مشتق من هذا النوع"، للمزيد أنظر في ذلك د أيمن عبدالله فكري، المرجع السابق، ص 331.

1- عادل حماد عثمان حماد، المرجع السابق، ص 149.

2- أيمن عبدالله فكري، المرجع السابق، ص 314..

3- مباركية مفيدة، المرجع السابق، ص 135، 136.

4- عادل حماد عثمان حماد، المرجع السابق، ص 150.

• **التزوير المعلوماتي والتزوير التقليدي:** يتشابهان بأن لهما نفس الكيان المادي والمعنوي، ويختلفان من حيث دخول التقنية الحديثة في التزوير المعلوماتي وإلزام الفاعل بهذه التكنولوجيا، على عكس التزوير التقليدي الذي يكون بشكل تقليدي.

• **التزوير المعلوماتي وجريمة التلاعب غير المصرح به:** يشابهان في محل الاعتداء حيث تصع على المعلومات والبيانات التي يتضمنها النظام المعلوماتي والمحرر المعلوماتي بالتلاعب بالإدخال أو المحو أو تغيير الحقيقة، ويختلفان أولاً من حيث مصدر المحل حيث أن المعطيات في جريمة التلاعب هي جزء من النظام وهي وحدة واحدة لا تتجزأ، أما المعلومات في التزوير المعلوماتي فهي مخرجات النظام، وثانياً من حيث أثر الاعتداء، فالأثر في جريمة التلاعب هو إتلاف النظام وعدم تمكنه من القيام بمهامه بشكل طبيعي، أما الأثر في التزوير لا يتلف المحرر وإنما يبقى على حالة مع تغيير الحقيقة، أما من ناحية الضرر ففي التلاعب لا تستوجب تحققه عكس التزوير المعلوماتي، كما أن المصلحة المراد حمايتها في جريمة التلاعب هي مصلحة صاحب النظام، أما في التزوير المعلوماتي فالمصلحة المراد حمايتها هي الثقة العامة¹.

وتبعاً لما فصلناه أعلاه فإن حماية صحة المعلومات بشكل عام ترتبط بفكرة التحول من الوثائق التقليدية إلى الدعامات المعلوماتية التي تحتوي على معلومات كانت موجودة في الوثائق التقليدية، مما أثار تساؤلات حول إمكانية حماية هذه المعلومات الموجودة في الدعامات، والتي تكمن أهميتها في كونها موضوع جريمة التزوير المعلوماتي، وكونها أصبحت مشابهة أو حتى أفضل، من المحررات الورقية المستخدمة، بحيث أصبحت مرتبطة بمجموعة مهمة من الأنظمة الإدارية والتجارية والمالية والتي بدورها تمثل فكرة الحكومة الإلكترونية التي تقدم خدماتها للأفراد والمؤسسات العامة والخاصة من خلال المحرر المعلوماتي².

1- عادل مستاري، روائية زليخة، جريمة التزوير الإلكتروني، مقال منشور بمجلة العلوم الإنسانية، الصادرة عن كلية الحقوق والعلوم السياسية، جامعة محمد خضير بسكرة، الجزائر، العدد 46، صادر في مارس 2017، ص 299 و 300.

2- أيمن عبدالله فكري، المرجع السابق، ص 309.

- وعليه فالسؤال الذي يطرح هو كيفية ضمان الحماية من التزوير المعلوماتي من خلال القانون الجنائي أو التشريعات الجنائية الدولية، وهل الحماية التقليدية من جرائم التزوير التقليدي كافية لتطبيقها، أم أنها تتطلب حماية خاصة؟.

المطلب الأول: تفصيل جريمة التزوير المعلوماتي.

وسنتناول في هذا المطلب تفصيل ماديات جريمة التزوير المعلوماتي شأنها شأن باقي الجرائم بما يشمل ركنيها المادي المتمثل في تغيير الحقيقة والركن المعنوي المتمثل بالقصد الجنائي .

أولاً: الركن المادي لجريمة التزوير المعلوماتي:

يتحقق الركن المادي في جريمة التزوير المعلوماتي بتوافر نشاط الجاني بتغيير الحقيقة في المحرر المعلوماتي وباستخدام تكنولوجيا المعلومات بما يسبب ضرر للغير.

1- تغيير الحقيقة: يعد تغيير الحقيقة الركن الجوهرى والاساس الذي تقوم عليه جريمة التزوير المعلوماتي، إذ يترتب على عدم توافره زوال هذه الجريمة تمام، والمقصود بتغيير الحقيقة عرض أمر معين وإظهاره في صورة غير التي يجب أن يظهر عليها وبشكل مخالف للحالة الواقعية التي ينبغي أن يكون عليها لو لم يتدخل نشاط الجاني في تغييرها، أو هي إنشاء حقيقة مخالفة بالتغيير إذ يمكن أن يكون تغيير الحقيقة كلياً أو جزئياً، سواء بنشاط إيجابي مثل التغيير أو نشاط سلبي مثل الترك لبيانات جوهرية ما يترتب عليه مساس بالمراكز القانونية للغير¹.

ويتم فعل التغيير في جريمة التزوير المعلوماتية بأي معالجة آليه للبيانات من أجل التلاعب في محتوى المحرر المعلوماتي ويكون بإتيان أحد الأفعال التالية على سبيل الحصر " الإدخال، الإتلاف، المحو، الطمس"، بما يكون أو يخلق أو يعدل بيانات مسجلة أو محفوظة

1- ط. د خليفى فتيحة، د. مهداوي محمد صالح، التزوير المعلوماتي في البيئة الرقمية، مقال منشور في مجلة الدراسات القانونية، مخبر السيادة والعولمة، جامعة يحيى فارس المدية، الجزائر، المجلد 08، العدد 02، جوان 2022، ص 266.

في دعائم النظام المعلوماتي، وعليه فإن جريمة التزوير المعلوماتي تقع على البيانات والمعلومات بغض النظر عن لغتها أو شكلها أو الحالة التي وجدت عليها¹.

2- تحقق الضرر: إلى جانب تغيير الحقيقة يجب تحقق الضرر للمجني عليه، فإذا انتفى تحقق الضرر تنتفي الجريمة باعتبار أن تغيير الحقيقة لم يترتب عليه أي ضرر يصيب الغير، أو أي إخلال بمصلحة يحياها القانون، فتوافر الضرر ضروري لاكتمال الركن المادي لجريمة التزوير المعلوماتي، وهذا الضرر قد يكون ماديا كخسارة مادية للمجني عليه، أو معنوية أدبية كفقدان الثقة في المعاملات في المجتمع بشكل عام².

3- العلاقة السببية: ولتوافر الركن المعنوي في جريمة التزوير المعلوماتي لا بد من ارتباط ذلك بالعلاقة السببية ما بين الفعل الإجرامي وهو تغيير الحقيقة، وبين الضرر الذي ينجم عنها، فلا يكفي لقيام الجريمة وقوع الفعل الإجرامي وتحقيق النتيجة الإجرامية، بل لا بد أن يكون هذا الفعل هو الذي أدى بذاته إلى تحقق النتيجة، وأن سلوك من قام بالتزوير المعلوماتي هو الذي سبب الضرر المادي أو المعنوي لصاحب الحق، إذ أن السببية تقوم بمجرد اقتران الفعل الإجرامي مع النتيجة، حتى لو كان هناك عامل آخر من الممكن أن يحقق نفس النتيجة بعد حين.

ثانيا: الركن المعنوي لجريمة التزوير المعلوماتي.

تعتبر جريمة التزوير المعلوماتي من الجرائم العمدية والتي يتطلب لقيامها توافر الركن المعنوي بقصد الجنائي العام أي اتجاره إرادة الجاني لارتكاب هذه الجريمة مع العلم بوقائع وماديات الجريمة وسلوكه الإجرامي من تغيير للحقيقة بمختلف الطرق في محرر معلوماتي بما يترتب عليه ضرر، و إتجاه إرادته الغير معيبة للقيام بتغيير الحقيقة في محرر معلوماتي.

1- بوربابة صورية، المرجع السابق، ص 139.

2- ط د وفاء صدراتي، آليات الحماية القانونية للتوقيع الإلكتروني من جرائم التزوير الإلكتروني في التشريع الجزائري، مقال منشور بمجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر بالوادي، الجزائر، المجلد 11، العدد 01، أفريل 2020، ص 591.

كما يجب توافر القصد الجنائي الخاص في هذه الجريمة والذي يتمثل بنية الغش في استعمال المحرر المزور فيما زور من أجله، وإلحاق الضرر بالغير¹.

المطلب الثاني: معالجة جريمة التزوير المعلوماتي في التشريع الجنائي.

نحاول أن نعالج في هذا المطلب الحماية الموضوعية من التزوير المعلوماتي التي وفرتها التشريعات الجنائية موضوع الدراسة من خلال قوانينها العامة أو الخاصة وهذا في محاولة منا للإجابة على السؤال المطروح أعلاه في رأس المبحث.

أولاً: التشريع الجزائري.

اعترف المشرع الجزائري للمحرر المعلوماتي بالحماية الجنائية من خلال شموليته بالحماية المقررة للبيانات والأنظمة المعلوماتية ضد أي تعديل أو حذف سواء كانت مقرونة بنية التزوير أم لا، حيث جرم المشرع هذه الأفعال في القسم السابع مكرر من قانون العقوبات الجزائري بعنوان المساس بأنظمة المعالجة الآلية للبيانات²، حيث اعتبر أن التزوير المعلوماتي من ضمن الجرائم الوارد ذكرها في المادة 394 مكرر 1 والتي جاء فيها " ... كل من ادخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

أما فيما يتعلق بجريمة التزوير المعلوماتي بتفاصيلها الدقيقة فلم يتناولها المشرع الجزائري ضمن القسم السابع مكرر من قانون العقوبات الجزائري، ولم يضع لها تعريفاً محدداً ولا يحدد

1- عادل مستاري، روائية زوليخة، المرجع السابق، ص 302.

تتعدد طرق التزوير فمنها الطرق المادية والمعنوية، فالتزوير بالطريقة المادية يشمل على العديد من السلوكيات نذكر منها (وضع توقيع مزور أو وضع ختم مزور على مخرجات الحاسب الآلي، أو اصطناع محرر، أو حذف أو إضافة أو تغيير مضمون المحرر)، أما الطرق المعنوية فتشمل (تغيير إقرارات وای الشأن، و جعل واقعة مزورة في صورة واقعة صحيحة)، للمزيد أنظر عبدالله بلقاسم، الطبيعة الخاصة لجريمة التزوير في المحررات الالكترونية، مقال منشور بمجلة الدراسات القانونية المقارنة، مخبر القانون الخاص المقارن، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي الشلف الجزائر، المجلد 06، العدد 02، ديسمبر 2020، ص 989 990.

2- د مباركية مفيدة، المرجع السابق، ص 191 192.

أركانها، حيث أنها ما زالت تخضع للقواعد العامة لجريمة التزوير التقليدية في المواد 214 حتى 229 من قانون العقوبات.

إلا أن المشرع الجزائري عالج جريمة التزوير المعلوماتي في بعض القوانين الخاصة كالقانون رقم 04-15 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين المؤرخ في 01 فبراير 2015، والذي نص على مجموعة من الأحكام التي تحول دون وقوع تزوير في المحرر الإلكتروني كما جرم بعض الأفعال التي تعيب قيمته القانونية و وظيفته في الأثبات، بالإضافة إلى ذلك تم تناول التزوير المعلوماتي في القانون رقم 05-18 الخاص بالتجارة الإلكترونية، حيث تناول جريمة التزوير المعلوماتي و وضع بعض التدابير الوقائية ضد محاولات التزوير المحتملة على محررات التجارة الإلكترونية والحيلولة دون وقوع التزوير، كما نص على التزوير المعلوماتي في القانون رقم 03-14 المتعلق بسندات و وثائق السفر، أذ نص في الفقرة الثانية من المادة 17 منه على تجريم التزوير الذي يذال البيانات المخزنة في النظام البيرومتر الإلكتروني.

لكن في هذا الصدد، يجب على المشرع الجزائري مواكبة التطورات التي تشهدها جريمة تزوير المعلومات، باعتبار الوثيقة المعلوماتية (المحرر المعلوماتي) إحدى نتائج عملية المعالجة الآلية للبيانات، لذلك لا بد من تخصيص مواد خاصة لجريمة التزوير المعلوماتي، وتحديد العقوبة لها، وحماية البيانات منها، إضافة إلى ضرورة توافق القوانين الجنائية الوطنية مع الاتفاقيات الدولية التي وقعتها الجزائر، والتي تجرم هذا النوع من الأفعال، مثل اتفاقية بودابست في المادة السابعة والاتفاقية العربية في المادة العاشرة.

ثانيا: التشريع السعودي.

بالنظر إلى التشريع السعودي الخاص بجرائم المعلوماتية لسنة 2007 نجد أنه جاء خاليا من أي نص يجرم التزوير في المحررات المعلوماتية، أذ لم ينص النظام على هذا المسمى صراحة، وهذا على عكس ما جاء في المرسوم الملكي الملغي رقم 53 حيث نصت في المادة 14 منه على " كل من زور الصور الضوئية أو المستندات المعالجة آليا أو البيانات المخزنة

في ذاكرة الحاسب الآلي أو على شريط ممغنط أو أسطوانة أو غيرها من وسائط، أو استعمالها وهو عالم بتزويرها، يعاقب بالعقوبات الواردة في هذا النظام"¹.

ولكن المشرع السعودي شمل جريمة التزوير المعلوماتي ضمن الجرائم المنصوص عليها في المادة الرابعة والخامسة من نظام مكافحة الجرائم المعلوماتية لسنة 2007 حيث نصت المادة الرابعة على "يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

1- الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ أسم كاذب، أو انتحال صفة غير صحيحة"².

وعليه يتضح أن المشرع السعودي قد فرق بين الجرائم المعلوماتية الواردة في نص المادة الرابعة وبين ما يماثلها من الجرائم المرتكبة بالطرق التقليدية، فلا يصوغ لأحد أن يكيف الجرائم المرتبطة بالحاسب الآلي بنفس تكيف ما يماثلها من الجرائم التقليدية.

وحدد المشرع السعودي الركن المادي في جريمة التزوير المعلوماتي باتخاذ الجاني السلوك الإجرامي المتمثل في (الاستيلاء على المحرر، تعديل أو تغيير ما يحتويه، انتحال صفه غير صحيحة)، ويتحقق هذا الركن بسلوك الجاني للأفعال الموضحة سابقاً مع تحقيق النتيجة وهي الضرر الذي ينجم عن فعل التزوير.

أما الركن المعنوي في جريمة التزوير المعلوماتي فيستوجب أن يتوفر القصد الجنائي العام من علم بأن فعله غير مشروع وأنه يعتدي على حق ليس من حقه غير مملوك له، و إتياره إرادة الجاني للقيام بفعل التزوير مع تحقق الضرر ضد المجني عليه أو المنفعة لشخص الجاني³.

1- دلخار صلاح بوتاني، المرجع السابق، ص 178.

2- المادة الرابعة من نظام مكافحة الجرائم المعلوماتية السعودي.

3- عبدالعزيز بن غرام الله آل جار الله، المرجع السابق، ص 187.

ومن حيث العقوبة على جريمة التزوير المعلوماتي فقد قرر المشرع السعودي لها عقوبة تنحصر بين حداها الأعلى وهو السجن مدة لا تزيد عن أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال سعودي أو إحدى هاتين العقوبتين، وبين حداها الأدنى وهو السجن مدة لا تزيد عن ثلاثة سنوات وبغرامة لا تزيد عن مليوني ريال سعودي أو بإحدى هاتين العقوبتين.

ثالثاً: التشريع الإماراتي:

كان التشريع الإماراتي سابقاً في مكافحة جريمة التزوير المعلوماتي وفي هذا الشأن كانت إمارة دبي قد أصدرت قانون رقم 02 لسنة 2002 تحت مسمى قانون المعاملات والتجارة الإلكترونية وقد تناولت فيه تجريم التزوير المعلوماتي في المادتين 29 و 30 وتعلقتا المادتين بمعالجة حالة التزوير خلال إنشاء المحرر المعلوماتي، وحددت لها عقوبة بالحبس أو غرامة لا تتجاوز 250.000 ألف درهم إماراتي أو بإحدى هاتين العقوبتين، أما المادة 32 من نفس القانون فقد أكدت على معاقبة من يرتكب جريمة باستخدام وسيلة إلكترونية، وبما أن جريمة التزوير بالتعريفات السابقة تدخل في سياق الجرائم المترتبة باستخدام وسيلة إلكترونية وبالتالي تدخل في نطاق تطبيق هذه المادة، وحددت لها المادة عقوبة الحبس لمدة أقصاها سنة وبغرامة لا تتجاوز 100.000 ألف درهم أو بإحدى هاتين العقوبتين¹.

وتلى ذلك تناول المشرع الإماراتي جريمة التزوير المعلوماتي في قانون مكافحة جرائم تقنية المعلومات رقم 2 لسنة 2006 الملغي، وتناولها في المادة الرابعة منها بشأن تزوير المستندات الخاصة بالحكومة الاتحادية أو غيرها من الهيئات المحلية، حيث ذكر في نص المادة الرابعة وصف التزوير عبر النظام المعلوماتي.

ليستمر المشرع الإماراتي في تطوير قواعد القانونية تماشياً مع التطور المستمر في الجانب التكنولوجي، وفي هذا الشأن قدم تعريفاً للمستند الإلكتروني في المادة الأولى من نفس القانون السابق ذكره²، كما تناول التعريف أيضاً في المادة الأولى من قانون مكافحة جرائم تقنية المعلومات رقم 5 لسنة 2012 والتي نصت "المستند الإلكتروني: سجل أو بيان معلوماتي يتم

1- مباركية مفيدة، المرجع السابق، ص 194.

2- للمزيد حول التعريف أنظر المادة الأولى من القانون رقم 2 لسنة 2006 الإماراتي الملغي.

إنشاءه أو تخزينه أو استخراجيه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة إلكترونية على وسيط"، والملاحظ على التعريف في قانون سنة 2012 أنه جاء بنفس المصطلحات في القانونيين إلا أنه أقتصر على تعريف المستند الإلكتروني دون التطرق إلى حالته أذا تلف أو تم استرجاعه.

أما القانون الجديد بشأن مكافحة الشائعات والجرائم الالكترونية لسنة 2021، فقد أبقى على نفس التعريف للمستند الإلكتروني في القانون السابق الملغي لسنة 2012، كما تناول جريمة التزوير المعلوماتي في المادة 14 تحت عنوان تزوير المستند الإلكتروني والتي نصت على: "1- يعاقب بالسجن المؤقت والغرامة التي لا تقل عن 150.000 مائة وخمسون ألف درهم ولا تزيد على 750.000 سبعمائة وخمسون ألف درهم كل من زور مستنداً إلكترونياً من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية أو المحلية. 2- وتكون العقوبة الحبس والغرامة لا تقل عن 100.000 مائة ألف درهم ولا تزيد على 300.000 ثلاثمائة ألف درهم، أو بإحدى هاتين العقوبتين، إذا وقع التزوير في مستندات جهة غير تلك المنصوص عليها في البند 1 من هذه المادة. 3- ويعاقب بذات العقوبة المقررة لجريمة التزوير، بحسب الأحوال، من استعمل المستند الإلكتروني المزور مع علمه بتزويره"¹.

و فرضت المادة 14 عقوبة الحبس والغرامة التي لا تقل عن 100.000 ألف درهم ولا تزيد عن 3.00.000 ألف درهم بحق الجاني أذا وقع التزوير في مستندات عامة لا تخص الحكومة أو مؤسساتها المحلية، أو بإحدى هاتين العقوبتين، والملاحظ على المادة المذكورة أعلاه وكعادة المشرع الإماراتي في القانون الجديد أنها تشددت في العقوبة في حال استهدفت جريمة التزوير المعلوماتي المستندات الإلكترونية الخاصة بالحكومة الاتحادية أو إحدى مؤسساتها المحلية، وحددت لها عقوبة السجن المؤقت والغرامة التي لا تقل عن 150.000 ألف درهم ولا تزيد عن 750.000 ألف درهم .

1- المادة الرابعة عشر من قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي لسنة 2021.

رابعاً: التشريع الأردني.

تناول التشريع الأردني تعريف جريمة التزوير في قانون العقوبات المعدل لسنة 2022 في المادة 260 وما يليها على أنه " هو تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطوط أو بيانات نظام معلومات رسمي يحتج بها نجم أو يمكن أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي".

إلا أنه لم يضع تعريفاً للتزوير الإلكتروني كما أنه لم يضيف أي تعديل لأي من القوانين ليبين مفهومها، وفي هذا الإطار أجتهد جانب من الفقه وقدم تعريف لها على أنها " نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كأداة أو هدف لتحقيق الفعل الإجرامي المقصود، بحيث يقع التزوير على الحاسب الآلي ومخرجاته.

أما المادة 265 المعدلة في سنة 2022 فنصت على عقوبة الأشخاص الذين يرتكبون تزويراً في الوثائق الرسمية للدولة وجاء ذكر بيانات نظام المعلومات باعتبارها محل لجريمة التزوير حيث نصت المادة على " يعاقب سائر الأشخاص الذين يرتكبون تزويراً في الأوراق الرسمية أو في أي بيانات نظام معلومات رسمي بإحدى الوسائل المذكورة في المواد السابقة بالأشغال المؤقتة أو الاعتقال في الحالات التي لا ينص فيها القانون على خلاف ذلك"¹.

وقد تناول القانون رقم 27 لسنة 2015 الملغي بعض المفردات والكلمات التي تحمل في مضمونها معنى التزوير المعلوماتي مثل (تغيير، تعديل) وهذا في المواد الثالثة والرابعة والخامسة عشر، إلا أن الأخذ بها على أنها تدل على جريمة التزوير المعلوماتي لما تحمله المعاني من توافق مع معنى جريمة التزوير وهو تغيير الحقيقة، يعد مخالفة للقواعد الأساسية في النص الجزائي الذي يشترط أن يكون النص الجزائي مفهوماً واضحاً ولا يقبل التأويل وذلك بناء على قاعدة " عدم جواز القياس في المسائل الجزائية".

1- المادة 265 من قانون العقوبات الأردني.

أما قانون الجرائم الإلكترونية الأردني الجديد رقم 17 لسنة 2023¹ فيرى الباحث أنه جاء بالنص فيه على جريمة التزوير المعلوماتي محتشماً إذ لم يرد تفصيل دقيق عن الجريمة وإنما ذكرها المشرع الأردني من خلال العقوبة وهذا في نص المادة الثامنة الفقرة أ والتي عاقبت على جريمة التزوير والتعامل بالمزور حيث حددت عقوبة لمرتكب جريمة التزوير المعلوماتي بالحبس مدة لا تقل عن سنة ولا تزيد عن ثلاث سنوات وبغرامة مالية لا تقل عن 2500 دينار

1- بالاطلاع على موقف مكتب الأمم المتحدة لحقوق الإنسان من القانون الأردني الجديد للجرائم الإلكترونية، يتبين أنه عبّر عن مخاوف جدية إزاء هذا التشريع، فقد صرّحت ليز ثروسيل، المتحدثة باسم المكتب، بأن القانون الجديد يفرض قيوداً واسعة ويُجرّم أنشطة يمارسها الأفراد والمنظمات عبر الإنترنت، كما يقرّ عقوبات على نشر محتوى قد يُعد مسيئاً لموظفي إنفاذ القانون، وأضافت أن من شأن هذه الأحكام أن تؤدي إلى إسكات الأصوات الناقدة وتقويض مبدأ المساءلة العامة، فضلاً عن تمكين السلطات من إزالة المحتوى أو حجبهِ دون رقابة قضائية كافية، كما وأشارت المتحدثة إلى أن من بين الجرائم الإلكترونية التي وُصفت في التشريع بأنها فضفاضة ومبهمّة: التحريض على الفجور أو إغواء الغير، والمساس بالآداب العامة، و«اغتيال الشخصية»، وإثارة الفتنة أو النعرات، والنيل من الوحدة الوطنية، وازدراء الأديان، كما أوضحت أن القانون يقرّ عقوبات سالبة للحرية تتراوح بين أسبوع وثلاث سنوات، إلى جانب غرامات مالية تتراوح بين 423 دولاراً و105 آلاف دولار، تبعاً لطبيعة المخالفة.

وبناءً على ذلك، أعرب المكتب عن تزايد قلقه إزاء هذا القانون، في ظل ما وصفه بتنامي مظاهر التهريب والمضايقة واعتقال الناشطين، وتضييق الفضاء المدني في الأردن، ولفتت إلى أن قانون الجرائم الإلكترونية السابق لسنة 2015، الذي حلّ هذا التشريع محلّه، قد استُخدم لاعتقال عدد من نشطاء حقوق الإنسان والصحفيين بتهم من قبيل «التشهير». واستشهدت المتحدثة في هذا السياق بقضية الصحفي الساخر أحمد حسن الزعبي، الذي صدر بحقه حكم بالسجن لمدة عام في 9 آب/أغسطس، استناداً إلى القانون الحالي، بسبب منشور على موقع فيسبوك انتقد فيه طريقة تعامل السلطات مع إضراب سائقي الشاحنات.

ورغم إقرار المتحدثة بحاجة الدول إلى اتخاذ تدابير فعّالة لمكافحة الجرائم السيبرانية، شددت في المقابل على ضرورة أن تستند استراتيجيات مكافحة هذه الجرائم إلى القانون الدولي لحقوق الإنسان، وأن تكون النصوص واضحة ومحددة، وألا تُبنى الجرائم على مضمون التعبير عبر الإنترنت.

وفي هذا الإطار، دعا مكتب الأمم المتحدة لحقوق الإنسان السلطات الأردنية إلى إعادة النظر في هذا التشريع بما يضمن توافقه مع الالتزامات الدولية، ولا سيما العهد الدولي الخاص بالحقوق المدنية والسياسية الذي صادق عليه الأردن، كما حثّها على الاستفادة من الخبرات المتاحة، بما في ذلك خبراء تكنولوجيا المعلومات والقانون ومنظمات المجتمع المدني ذات الصلة، إضافة إلى مكتب حقوق الإنسان التابع للأمم المتحدة، من أجل تطوير تشريعات تواجه التهديدات الإلكترونية مع الحفاظ على حقوق الإنسان الأساسية، للمزيد من المعلومات أنظر في ذلك الموقع الإلكتروني لمكتب الأمم المتحدة لحقوق الإنسان عبر شبكة الانترنت في الرابط <https://news.un.org/ar/story/2023/08/1122817>، منشور في أوت 2023، تاريخ الاطلاع

2024/10/08 الساعة 19:52.

أردني ولا تزيد عن 10000 دينار أردني لكل من قبل التعامل بالبطاقات المزورة أو المقلدة أو المنسوخة أو غيرها من وسائل الدفع الإلكتروني أو بيانات وسائل الدفع الإلكتروني المستوى عليها بطريقة غير مشروعة مع علمة بعدم مشروعيتها¹.

المطلب الثالث: معالجة جريمة التزوير المعلوماتي في التشريع الدولي.

ونقدم هذا المطلب معالجة جريمة التزوير المعلوماتي حسب ما جاءت به اتفاقية بودابست لسنة 2001 والاتفاقية العربية لمكافحة الجرائم المعلوماتية لسنة 2010.

أولاً: جريمة التزوير المعلوماتي في اتفاقية بودابست.

تناولت اتفاقية بودابست لسنة 2001 جريمة التزوير في المادة السابعة منها حيث نصت على "تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبغير حق: إدخال، تغيير، حذف أو إتلاف بيانات كمبيوتر، بشكل يجعل بيانات غير أصلية تبدو بقصد اعتبارها أو استخدامها لأغراض قانونية، بغض النظر عما إذا كانت تلك البيانات قابلة للقراءة والفهم بشكل مباشر أم لا، ويجوز للدولة الطرف أن تشترط وجود نية الاحتيال، أو نية غير صادقة مشابهة، سابقة لإلحاق المسؤولية الجنائية"².

وتهدف هذه المادة إلى إنشاء جريمة توازي جريمة التزوير التقليدية (التزوير الملموس)، من أجل سد الثغرات في القوانين الوطنية المتعلقة بجريمة التزوير المعلوماتي والتي لا تنطبق

1- أنظر المادة الثامنة من القانون رقم 17 لسنة 2023 الأردني، المرجع السابق.

2- المادة السابعة من اتفاقية بودابست لسنة 2001، بالإضافة إلى ذلك نصت على جريمة التزوير المعلوماتي في العديد من الاتفاقيات والبروتوكولات الدولية منها (اتفاقية الاتحاد الأفريقي لسنة 2012 مشروع اتفاقية بشأن إطار قانوني للمساعدة في الأمن السيبراني في أفريقيا في المواد 24 و 25، والسوق المشتركة لشرق وجنوب أفريقيا "الكوميسا" مشروع القانون النموذجي بشأن الأمن السيبراني في المادة 02، ومجلس أوروبا اتفاقية بشأن الجريمة السيبرانية والبروتوكول الإضافي للاتفاقية بشأن الجريمة السيبرانية 2001 في المادة 03، والاتحاد الأوروبي القرار الإطاري للمجلس JHA/222/2005 بشأن الهجمات ضد نظم المعلومات في المادة 13، والاتحاد الدولي للاتصالات "الاتحاد الكاريبي للاتصالات" 2010 النصوص التشريعية النموذجية بشأن الجريمة السيبرانية والجريمة الإلكترونية في المادة 11).

عليها القوانين التقليدية، حيث من الممكن أن يكون التلاعب بالمعلومات والبيانات المخزنة إلكترونياً له نفس العواقب الخطيرة التي تترتب على أعمال التزوير التقليدي، وبالتالي تظهر هنا المصلحة القانونية المحمية في أمن وموثوقية البيانات الإلكترونية التي قد تكون لها عواقب على العلاقات القانونية.

وبهذا حددت المادة الأعمال التي تشكل جريمة تزوير معلوماتي عند وقوعها على الوثائق أو البيانات بغض النظر أن كانت هذه الوثائق والبيانات ذات طبيعة عامة أو خاصة ما دام أنها تستند إلى الخداع كأساس للتجريم، ومن هذه الأعمال (الإدخال - التغييرات الجزئية أو الكلية، الحذف كإزالة بعض البيانات من وسيلة التخزين، الإتلاف وإخفاء البيانات)، أما الفقرة الأخيرة من المادة فتركت المجال مفتوح أمام التشريعات الوطنية في إمكانية إضافة شرط نية الاحتيال أو أي نية مشابهة قبل إلحاق المسؤولية الجنائية¹.

ثانياً: جريمة التزوير المعلوماتي في الاتفاقية العربية.

خصّت المادة 10 من الاتفاقية العربية لمكافحة الجرائم الإلكترونية جريمة التزوير المعلوماتي بتجريم واضح، باعتبارها من أخطر الجرائم التي تمسّ مصداقية الوثائق المعلوماتية وسلامة البيانات والمعاملات الرقمية، وتنصّ المادة على تجريم كل من يُدخل عمداً بيانات غير صحيحة، أو يعدّل أو يغيّر أو يمحو أو يتلف بيانات صحيحة، أو يعيد إنتاجها أو نسخها أو استخدامها بصورة غير مشروعة، متى كان ذلك من شأنه تغيير الحقيقة في محرر أو سجل أو وثيقة إلكترونية، وبقصد استخدامها لتحقيق منفعة غير مشروعة أو الإضرار بالغير².

وتقوم جريمة التزوير المعلوماتي في هذه المادة على ثلاثة عناصر رئيسية تتمثل بسلوك مادي يتمثل في كل فعل يغيّر في خصائص البيانات والمعلومات من خلال الإدخال أو التعديل أو المحو أو الإتلاف أو النسخ غير المشروع، وهو ما يجعل النص شاملاً لمختلف صور التحريف المعلوماتي، ونتيجة محتملة قوامها المساس بالحقيقة الرقمية عبر إنشاء محرر أو وثيقة إلكترونية مزيفة أو التلاعب بمحتوى قاعدة بيانات أو نظام معلوماتي، قصد جنائي

1- التقرير التفسيري لاتفاقية بودابست حول الجريمة الإلكترونية، المرجع السابق، ص 14.

2- المادة العاشرة من الاتفاقية العربية لمكافحة الجرائم الإلكترونية، المرجع السابق،

خاص يتمثل في نية الاستعمال أو الإضرار أو تحقيق منفعة غير مشروعة، وهو ما يميز التزوير المعلوماتي عن الأخطاء التقنية أو التعديلات غير العمدية.

وتبرز أهمية المادة 10 في أنها تبنت مفهوماً موسعاً للتزوير المعلوماتي مقارنة بالتزوير التقليدي، إذ لم تحصر الجريمة في الوثيقة الرسمية أو التجارية فقط، بل شملت كل أنواع البيانات والمخرجات الرقمية، بما في ذلك السجلات الإلكترونية الحكومية والخاصة، والبرمجيات، وقواعد البيانات، كما أن المادة تقرر التزام الدول العربية الأطراف باتخاذ التدابير التشريعية اللازمة لتجريم هذه الأفعال، بما يساهم في توحيد الحد الأدنى من الحماية الجنائية للوثائق الإلكترونية على المستوى العربي، لا سيما في ظل استخدام التزوير المعلوماتي في أنشطة الاحتيال الإلكتروني، والاختراق، والتلاعب بالأنظمة المالية والمصرفية.

ويمكن القول أن المادة 10 قدّمت معياراً واسعاً ومرناً في التجريم، يعكس إدراك واضعي الاتفاقية لطبيعة التزوير السiberاني وتطوره السريع، وذلك بهدف تعزيز الثقة في البيئة الرقمية وحماية سلامة المعاملات الإلكترونية.

المبحث الثاني: جريمة إباحية الاطفال المعلوماتية.

تشكل إباحية الأطفال عبر الشبكات المعلوماتية إحدى أخطر الظواهر الإجرامية في العصر الرقمي، ذلك أن التطور الهائل في التكنولوجيا وتوسع استخدام الشبكة العنكبوتية وفرا لجناة أدوات سهلة وسرية لإنتاج وتخزين ونشر وتوزيع المواد الإباحية التي تستغل الأطفال جنسياً، حيث أصبح الفضاء الإلكتروني ساحة رئيسية لهذه الجرائم المنظمة والمستترة، ولا يمكن أغفال الترابط الوثيق بين الجريمة المعلوماتية والاستغلال الجنسي للأطفال¹.

وإذ يعتبر الاستغلال الجنسي من أبشع الجرائم التي تُرتكب في حق الإنسان، سواء كان الضحية شخصاً بالغاً أو طفلاً، وهو من الأفعال المنافية للأخلاق والقيم الإنسانية التي تُمقتها وتُجرّمها جميع الثقافات والأديان والتشريعات، ومع ذلك، فإن هذه الجريمة تشهد ازدياداً مطرداً

1- زيدان بن جمعة بن عبيد الفارسي، الاستغلال الجنسي للأحداث عبر وسائل التواصل الاجتماعي وفق التشريع العُماني، رسالة ماجستير تخصص القانون العام، كلية الحقوق، جامعة الشرقية، سلطنة عُمان، سنة 2025 ص 54.

في معدلات انتشارها يوماً بعد يوم، خاصة مع التطور الهائل الحاصل في مجال تكنولوجيا المعلومات والاتصالات والنظم المعلوماتية التي سهّلت ارتكابها وتوسعت في قنوات تنفيذها.

وفي هذا الشأن عرفت اتفاقية بودابست لسنة 2001 جريمة استغلال الاطفال إباحيا عبر النظم المعلوماتية بأنه " كل تصوير بصري لقاصر يشترك في نشاط جنسي صريح، أو لشخص حقيقي يبدو كطفل يشترك في السلوك، أو صورة حقيقية تمثل قاصراً وهو يمارس سلوكاً جنسياً"¹.

وفي نفس السياق عنيت بعض الصكوك الدولية بتعريف إباحية الاطفال نذكر منها تعريف البروتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الاطفال واستغلال الاطفال في البغاء وفي المواد الاباحية الوارد في نص المادة (2 فقره ج) بأنها " يُقصد باستغلال الأطفال في المواد الإباحية تصوير أي طفل، بأي وسيلة كانت، يمارس ممارسة حقيقية أو بالمحاكاة أنشطة جنسية صريحة أو أي تصوير للأعضاء الجنسية للطفل لإشباع الرغبة الجنسية أساساً"²، ويغطي هذا التعريف الجرائم المرتبطة بالمحتوى الاباحي من انتاجه أو توزيعه غير المشروع فضلاً عن السلوك غير اللائق الذي يسئ إلى شرف الطفل، والذي بدأت بالظهور حديثاً عبر النظم المعلوماتية.

وهو تعريف بات يشكل مرجعاً أساسياً في التشريعات الوطنية والاقليمية والدولية اللاحقة بما في ذلك اتفاقية مجلس أوروبا للحماية من الاستغلال والاعتداء الجنسي على الاطفال (اتفاقية لانزاروتي)³.

1- المادة التاسعة من اتفاقية بودابست 2001.

2- المادة الثانية من البروتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الاطفال واستغلال الاطفال في البغاء وفي المواد الاباحية، الصادر بموجب قرار الجمعية العامة للأمم المتحدة رقم A/RES/54/263 في الدورة الرابعة والخمسون بتاريخ 25 مايو 2000.

³ تُعد اتفاقية مجلس أوروبا للحماية من الاستغلال الجنسي والاعتداء الجنسي على الأطفال المعروفة اختصاراً بـ اتفاقية لانزاروتي أول معاهدة دولية ملزمة تُكرّس نفسها بالكامل والحصري لمكافحة كافة أشكال العنف الجنسي الموجّه ضد الأطفال دون سن الثامنة عشرة. اعتُمدت الاتفاقية في مدينة لانزاروتي بإسبانيا يوم 25 أكتوبر 2007، ودخلت حيز النفاذ في 1 يوليو 2010، وهي مفتوحة للتوقيع والتصديق أو الانضمام من قبل جميع دول العالم - وليس أعضاء مجلس أوروبا فقط - وقد انضمت إليها حتى الآن أكثر من 50 دولة، تشمل

وإذ يمكننا في هذا السياق تعريف الاستغلال الجنسي للأطفال عبر الشبكات المعلوماتية على النحو التالي، " كل سلوك جنسي يصدر عن شخص بالغ ويُوجه إلى طفل باستخدام النظم والشبكات المعلوماتية، سواء تمثل ذلك في:

- إجبار الطفل أو حمله أو تشجيعه على القيام بأفعال ذات طابع جنسي.
- أو التوسط في مثل هذه الأفعال.
- أو الاستفادة منها.
- أو استغلالها عن طريق الإنتاج أو التوزيع أو النشر أو العرض أو الحيازة، وذلك بقصد تحقيق إشباع جنسي للجاني أو لغيره، أو الحصول على منفعة مادية أو أي مزايا أخرى"¹.

وتتنمو هذه الجريمة بشكل متسارع بالرغم من الجهود المبذولة لمكافحتها، حيث تحولت إلى تجارة عالمية إذ يتم استغلال هذه الأفعال باعتبارها محتوى عبر المواقع الإلكترونية التي توفرها شبكات الانترنت العالمية، ويتدفق مئات الآلاف من المتصفحين والباحثين يوميا عن صور الاطفال المستغلين جنسيا، وهو ما ساهمت التكنولوجيا الحديثة في تسهيل وصولهم إلى هذه المواد، وقد انعكس ذلك سلبا على ارتفاع مستوى هذه الجريمة².

وبناء على ما سبق من تعريفات سوف نقسم هــ المبحث إلى ثلاثة مطالب نتناول في الأول تفصيل جريمة إباحية الاطفال وبيان أركانها، والثاني نبين فيه موقف القوانين العقابية والتشريع الجنائي الوطني ، والثالث لمعالجة الجريمة إباحية الاطفال على المستوى الدولي.

الاتفاقية كل صور الاعتداء والاستغلال الجنسي ضد الأطفال، سواء وقعت داخل الأسرة أو خارجها أو عبر الفضاء الإلكتروني.

1- فريدة بوتعني وآخرون، الطفل والجريمة المعلوماتية "جريمة الاستغلال الجنسي للأطفال عبر الانترنت"، مقال منشور بمجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد العاشر، العدد الثاني، لسنة 2021، ص256.

2- عبد الإله النوايسة، المرجع السابق، ص 307 وما بعدها.

المطلب الاول: تفصيل جريمة إباحية الأطفال.

بالنظر إلى ما قدمناه من تعريفات عن جريمة إباحية الأطفال سنحاول أن نفصل في هذا الفرع محل الجريمة والذي يتمثل بالسلوك الإجرامي المكون لهذه الجريمة الخطيرة (الركن المادي)، ونية والجاني واتجاه إرادته (الركن المعنوي).

أولاً: الركن المادي لجريمة اباحية الاطفال:

يتحقق الركن المادي لجريمة إباحية الأطفال بمجرد قيام الجاني بإتيان أي من السلوكيات التالية عبر الأنظمة المعلوماتية، سواء بقصد الاستغلال أو الترويج أو حتى بدون قصد مباشر للتوزيع:

- إنتاج أو تصوير أو صنع المواد الإباحية التي تتضمن أطفالاً عبر نظام معلوماتي.
- نشرها أو توزيعها أو بثها أو عرضها أو جعلها متاحة للغير عبر النظام المعلوماتي.
- الترويج لها أو تسهيل الوصول إليها عبر النظام المعلوماتي.
- حيازة أو تخزين المادة الإباحية داخل النظام معلوماتي أو جهاز إلكتروني، دون الحاجة إلى إثبات نية التداول.

وتكون هذه الجريمة بمجرد قيام الجاني بتصوير أطفال - حقيقيين أو افتراضيين - في أوضاع جنسية مخلة، ثم عرض هذه الصور عبر الإنترنت، أو إرسالها إلى الغير عبر الشبكات والوسائل الإلكترونية، ويُعتبر الطفل " افتراضياً " في حالة الصور الزائفة كالمونتاج، حيث يتم تجميع أجزاء من صور متعددة لإنتاج صورة واحدة تبدو واقعية، مما يُشكل في كل الأحوال اعتداءً على الطفولة وحق الشخص في الملكية على صورته الشخصية¹.

أما إذا كانت هذه المواد موجهة عمداً إلى أطفال آخرين بهدف إفسادهم أو تحريضهم على ممارسات جنسية أو فسق، فإن الركن المادي يتحقق أيضاً لجريمة منفصلة هي " تحريض قاصر على الفسق أو الدعارة "، وهنا يبرز التداخل الواضح بين الجريمتين من حيث السلوك المادي،

1- بن تركية نصيرة، الحماية القانونية للأطفال من الاستغلال الجنسي عبر الانترنت، مقال منشور عبر الانترنت في الموقع الإلكتروني التالي، [https://e-biblio.univ-](https://e-biblio.univ-mosta.dz/server/api/core/bitstreams/816d536e-2bc2-482e-a636-de5d97ad9b57/content)

[mosta.dz/server/api/core/bitstreams/816d536e-2bc2-482e-a636-de5d97ad9b57/content](https://e-biblio.univ-mosta.dz/server/api/core/bitstreams/816d536e-2bc2-482e-a636-de5d97ad9b57/content)، تاريخ الاطلاع 2025/08/12، الساعة 17:22، ص 05.

وبهذا يتسع نطاق الركن المادي ليشمل كل فعل يتعلق باستغلال الأطفال في المواد الإباحية، سواء كان الجاني بالغًا يستهدف بالغين آخرين أو يستهدف الأطفال أنفسهم، ففي كلا الحالتين يُشكلان ركن مادي لجريمة إباحية الاطفال¹.

ثانيا: الركن المعنوي لجريمة إباحية الاطفال:

يُشكّل الركن المعنوي في جريمة إباحية الأطفال أساسًا يقوم على مبدأ العمدية، حيث يكفي توافر القصد الجنائي العام؛ أي علم الجاني وإدراكه الكامل بأن الأفعال التي يرتكبها - سواء كانت إنتاجًا أو توزيعًا أو حيازة مواد إباحية تتعلق بالأطفال - غير مشروعة، مع توجيه إرادته صراحةً نحو تنفيذها، وفي هذا السياق، لا يُقبل الدفع بجهل المجرم المعلوماتي أو عدم معرفته بسن الضحية، إذ يُفترض عليه علمًا مطلقًا بذلك السن وفقًا لقواعد القانون الجنائي الدولي والوطني².

1- بشأن عبد النور، المرجع السابق، ص 290.

2- بشأن عبد النور، نفس المرجع السابق، ص 290.

المطلب الثاني: معالجة جريمة إباحية الاطفال في التشريع الجنائي.

ونتناول في هذا الفرع المعالجة الموضوعية لجريمة اباحية الاطفال في التشريعات الوطنية محل الدراسة ومنا نصت عليه من مواد تكافح فيها الجريمة المستحدثة وتحمي من خلالها الأطفال المستغلين جنسيا.

أولا: التشريع الجزائري.

1- الحماية المقررة للطفل وفق قانون حماية الطفل لعام 2015.

وتناول المشرع الجزائري هذه الجريمة في الباب الخامس من هذا القانون والذي جاء تحت عنوان (الاحكام الجزائية العقوبات المقررة لجريمة استغلال الاطفال جنسيا عبر الانترنت)، في المادتين 141 و 143.

فالمادة 141 خصصت حماية خاصة للطفل من هذا النوع من الجرائم أذ نصت على (دون الإخلال بالعقوبات الأشد يعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة من 150.000 دج إلى 300.000 دج كل من يستغل الطفل عبر وسائل الاتصال مهما كان شكلها في مسائل منافية للأداب العامة والنظام العام)¹.

أما المادة 143 تناولت الجرائم الاخرى المتعلقة بالاستغلال الجنسي للأطفال بنصها (يعاقب على الجرائم الاخرى الواقعة على الطفل ولا سيما الاستغلال الجنسي للطفل واستعماله في البغاء وفي الاعمال الاباحية والاتجار به والتسول به أو تعريضه للتسول واختطاف الطفل طبقا للتشريع الساري المفعول ولا سيما قانون العقوبات)².

ويتضح من نص المادتين أن المشرع افرد عقوبة خاصة لمرتكبي جريمة إباحية الاطفال عبر الانترنت وكل من يستغلهم جنسيا وهي الحبس من 03 إلى 05 سنوات أو الغرامة المالية التي لا تقل عن 150 ألف دينار جزائري وتصل إلى 300 ألف، كما يظهر أن المشرع تشدد

1- المادة 141 من قانون حماية الطفل الجزائري رقم 15-12 مؤرخ في 15 يوليو 2015 المتعلق بحماية الطفل، المنشور بالجريدة الرسمية عدد 39، والصادر بتاريخ 19 يوليو 2015.

2- المادة 143 من قانون حماية الطفل الجزائري، المرجع السابق.

بالعقوبة عندما أحالنا ضمنا في نص المادة 141 أعلاه إلى ما جاء من عقوبة في المادة 333 من قانون العقوبات الجزائري وهذا بنصه (دون الاخلال بالعقوبات الاشد) أذ يستنتج ان هناك عقوبة أشد لهذا النوع من الجرائم منصوص عليها في المادة 333 سالفه الذكر¹.

2- الحماية المقررة للطفل وفق قانون العقوبات الجزائري.

تناول المشرع الجزائري جريمة اباحية واستغلال الاطفال جنسيا في المادة 333 مكرر من قانون العقوبات في الفصل الثاني منه "الجنايات والجرح ضد الاسرة والآداب العامة" في القسم السادس بعنوان " انتهاك الآداب" اذ نصت المادة على (يعاقب كل من صنع أ حاز أو استورد أو سعى استيراد من أجل التجارة او وزع أو أجر أو لصق أو أقام معرضاً أو شرع في العرض للجمهور أو باع أو شرع في البيع أو وزع أو شرع في التوزيع، كل مطبوع أو محرر أو رسم أو اعلان أو صورة أو لوحة زيتية أو صورة فوتوغرافية أو أصل الصورة أو قالبها، أو انتج أي شيء مغل بالحياء بالحبس من شهرين أو سنتين وبغرامة من 20.000 دج إلى 100.000 دج)².

كما قدم المشرع الجزائري المادة 333 مكرر 1 وهذا في القانون رقم 01/14 الصادر في 04 فبراير 2014 والمعدل للأمر رقم 66-155 المتضمن قانون العقوبات، والتي نصت على (يعاقب بالحبس من 05 سنوات إلى 10 سنوات وبغرامة مالية من 500.000 ألف إلى 10.000.000 دج، كل من صور قاصرا لم يكمل 18 سنة بأي وسيلة كانت وهو يمارس أنشطة جنسية بصفة مبينة، حقيقية أو غير حقيقية، أو صور الأعضاء الجنسية للقاصر لأغراض جنسية أساسا، أو قام بإنتاج أو توزيع أو نشر أو ترويج أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية متعلقة بالقصر)³.

وفق هذين المادتين يتحقق الركن المادي بقيام الجاني بعدد من السلوكيات أو أحدها المبينة أعلاه مثل (النشر الانتاج التوزيع التصوير الاستيراد التصدير ...) والتي يكون محلها

1- بن تركية نصيرة، المرجع السابق، ص 07.

2- المادة 333 مكرر من قانون العقوبات الجزائري، المرجع السابق.

3- المادة 333 مكرر 1 من قانون العقوبات الجزائري، نفس المرجع السابق.

طفل، والظاهر أن المشرع الجزائري تشدد في العقوبة التي وضعها لهذه الجريمة في نص المادة 333 مكرر 1 والتي وصلت إلى عقوبة الحبس بمدة من 05 إلى 10 سنوات وغرامة مالية من 500 ألف دينار جزائري إلى مليون دينار جزائري، بغض النظر عن الوسيلة المستخدمة للاستغلال الجنسي للأطفال سواء كانت باستخدام الوسائل التكنولوجية كالحواسيب أو الهواتف أو غيرها، إلا أن نص المادة يمتد اختصاصها تلقائياً إلى هذا النوع من الجرائم المستحدثة عبر النظم المعلوماتية.

أما الركن المعنوي فاعتبرها المشرع الجزائري من الجرائم العمدية التي يكفي لتحقيقها توافر القصد الجنائي العام من توافر للإرادة باتجاه ارادة الجاني الواعية نحو ارتكاب الفعل، والعلم بأن ما يقوم به من فعل موجه ضد الطفل.

وما يلاحظ من خلال المواد المذكورة اعلاه والتي تضمنها المشرع الجزائري في قوانينه سواء العقوبات أو القوانين الخاصة المتعلقة بحماية الطفل، أن المشرع حاول قدر الامكان توفير حماية خاصة للطفل من جميع اشكال الاستغلال الجنسي بغض النظر عن الوسيلة المستخدمة سواء كانت تقليدية أو عبر استخدام النظم المعلوماتية، وما التشدد في العقوبة الوارد في المواد إلا لردع المجرمين وتثنيهم عن الجرائم التي تستهدف الاطفال.

ثانيا: التشريع السعودي.

تناولت الماد السادسة من نظام مكافحة الجرائم المعلوماتية السعودي عدد من الجرائم التي من شأنها المساس بالآداب العامة والقيم الدينية، بالإضافة إلى ذلك الجرائم المتعلقة بنشر أو تخزين أو أعداد أو انشاء المواد والبيانات الإباحية والأنشطة المخلة بالحياء، وجاء نص المادة كالتالي:

"يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين

ريال، أو بإحدى هاتين العقوبتين كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

ذ- إنتاج 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.

ر- إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للإتجار في الجنس البشري، أو تسهيل التعامل به.

ز- إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية، أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها.

س- إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للإتجار بالمخدرات، أو المؤثرات العقلية، أو ترويجها، أو طرق تعاطيها، أو تسهيل التعامل بها"¹.

والملاحظ أن هذه المادة (السادسة من نظام مكافحة جرائم المعلوماتية السعودي) جاءت عامة في تجريم الجرائم الإباحية عبر الأنظمة أو الشبكات المعلوماتية، دون أن يقصرها المشرع السعودي على الأطفال فحسب، بل شملتهم بغض النظر عن سن الضحية، واعتبر المشرع هذه الأفعال جرائم معلوماتية إذا ارتكبت باستخدام تقنيات المعلومات أو أنظمة الحاسب الآلي، وبهذا يفرق بينها وبين الجرائم التقليدية المماثلة.

ومع ذلك، فقد تشدد المشرع السعودي في المادة الثامنة من النظام نفسه على رفع الحد الأدنى للعقوبة إذا اقترنت الجريمة بحالة تغيير القاصر أو استغلاله في هذا النوع من الجرائم، حيث جاء نصها كالتالي (لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى إذا اقترنت الجريمة بأي من الحالات الآتية: ... 3- التغيير بالقُصْر ومن في حكمهم، واستغلالهم)².

ويشمل الركن المادي لهذه الجريمة ارتكاب أي من الأفعال التالية: إنتاج مواد تمس بالنظام العام أو القيم الدينية أو الآداب العامة، أو إعدادها أو إرسالها أو تخزينها؛ أو إنشاء مواقع للإتجار بالبشر أو تسهيل التعامل بها؛ أو إنشاء مواد وبيانات إباحية أو نشرها أو ترويجها، ويعتبر هذا الركن متحققا بسلوك الجاني لهذه الأفعال وحدث نتيجة تتمثل بظهور وتوافر المواد والمحتوى على الشبكة المعلوماتية، حتى لو لم يتضرر أحد فعلياً.

1- المادة السادسة من نظام مكافحة الجرائم المعلوماتية السعودي، المرجع السابق.

2- المادة الثامنة من نظام مكافحة الجرائم المعلوماتية السعودي، المرجع السابق.

أما الركن المعنوي لهذه الجريمة فيتمثل في وجود القصد لدى الجاني بالمس بالقيم الدينية أو النظام العام أو الآداب العامة، ويتحقق ذلك بتوافر العلم لديه بأن فعله للأفعال المنصوص عليها أعلاه يعد انتهاك لهذه المحرمات وهو يقوم به بكامل إرادته واختياره¹.

ثالثاً: التشريع الاماراتي.

تناول المشرع الاماراتي جريمة اباحية الاطفال عبر النظم المعلوماتية في المرسوم بقانون اتحادي 34 لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية، وهذا في المادة 35 منه والتي جاءت بعنوان (استخدام الأطفال في إعداد مواد إباحية) إذ نصت على " يعاقب بالحبس مدة لا تقل عن 02 سنتين والغرامة التي لا تقل عن 250 مائتين وخمسين ألف درهم ولا تزيد على مليون درهم، أو بإحدى هاتين العقوبتين، كل من قام بتحريض أو إغواء أو بمساعدة طفل على بث أو إعداد أو إرسال مواد إباحية باستخدام شبكة معلوماتية أو إحدى وسائل تقنية المعلومات، وتكون العقوبة السجن المؤقت والغرامة التي لا تزيد على مليون درهم إذا كانت المواد الإباحية المعدة أو المرسله موضوعها هذا الطفل، ولا يسأل جزائياً الطفل الضحية عما يرتكبه من أفعال نتيجة التحريض والإغواء"².

وتُعد المادة 35 من هذا القانون نصاً متخصصاً في حماية الأطفال من الاستغلال الجنسي عبر الوسائل الإلكترونية، وتركز بشكل أساسي على تجريم التحريض أو الإغواء أو المساعدة التي يقدمها البالغ للطفل ليشترك بنفسه في إعداد أو بث أو إرسال مواد إباحية باستخدام شبكة معلوماتية أو وسائل تقنية المعلومات.

ش- وحددت المادة في الفقرة الأولى منها عقوبة الحبس بمدة لا تقل عن سنتين وغرامة من 250 ألف إلى مليون درهم أماراتي، وهي عقوبة مشددة مقارنة بجرائم إباحية أخرى في القانون الإماراتي لتعكس بذلك خطورة استغلال الاطفال جنسياً.

1- عبدالعزيز بن غرام الله آل جارالله، المرجع السابق، ص 173.

2- المادة 35 من قانون مكافحة الشائعات والجرائم الإلكترونية الاماراتي، المرجع السابق.

ص- تشددت المادة بالفقرة الثانية في عقوبتها حال كان الطفل الضحية موضوع المواد الإباحية المنشورة أو المعدة للنشر، بعقوبة تصل إلى السن المؤقت 15 سنة والغرامة التي لا تزيد عن مليون درهم أمارتي.

ض- وجاءت الفقرة الثالثة منها بالنص صراحة على عدم مساءلة الطفل جزائياً عن الأفعال الناتجة عن التحريض أو الإغواء، وهذا النص متقدم ويتوافق مع المبادئ الدولية التي تعتبر الطفل ضحية لا جانباً في مثل هذه الحالات، مما يشجع على الإبلاغ ويحمي الطفل من الملاحقة الثانوية، ويُعزز من سياسة حماية الضحايا في التشريع الإماراتي.

أما المادة 36 من نفس القانون والتي جاءت بعنوان (حيازة مواد إباحية للأطفال) فقد ركزت على تجريم حيازة المواد الإباحية المتعلقة بالأطفال عبر وسائل النظم المعلوماتية، بما يساهم في مكافحة انتشار هذه المواد ويحد من الطلب عليها، وبالتالي يقلل من الجرائم المرتبطة بها مثل الإنتاج والتوزيع، حيث نصت على "يعاقب بالحبس مدة لا تقل عن (6) ستة أشهر والغرامة التي لا تقل عن (150,000) مائة وخمسين ألف درهم ولا تزيد على (1,000,000) مليون درهم كل من حاز عمداً مواد إباحية للأطفال باستخدام نظام معلومات إلكتروني، أو شبكة معلوماتية، أو موقع إلكتروني، أو إحدى وسائل تقنية المعلومات"¹.

الركن المادي: في المادة 35 يتمثل في اتيان الفاعل البالغ أي من السلوكيات التي تعد من أفعال التحريض والتي تثير الطفل أو تدفعه نحو القيام بالفعل، أو التي تجذبه بطريقة تجعله يقبل القيام بهذا الفعل، أو تقديم المساعدة له لبث أو اعداد أو إرسال مواد إباحية، اما المادة 36 فيتمثل الركن المادي في قيام الجاني بحيازة وامتلاك وتخزين مواد إباحية موضوعها الطفل وتشمل أي محتوى سمعي أو بصري مخزنة عبر إحدى وسائل النظم المعلوماتية.

الركن المعنوي: يتطلب قيام الركن المعنوي في هذه الجريمة توافر القصد الجنائي العام (العمد)، أي أن يكون الفاعل مدركاً لطبيعة فعله ويريده، مع علمه بأن الضحية طفل وبأن المواد التي ينشرها أو يعرضها للطفل مواد إباحية، ولا يشترط قصد خاص حيث أن الجريمة عمدية بطبيعتها.

1- المادة 36 من قانون مكافحة الشائعات والجرائم الالكترونية الاماراتي، المرجع السابق.

رابعاً: التشريع الأردني.

تناول المشرع الأردني جريمة إباحية الاطفال عبر النظم المعلوماتية بالتجريم في قانون الجرائم الالكترونية رقم 17 لسنة 2023 في المادة 13 فقرة ب1 منه حيث نصت المادة على (...يعاقب على الأفعال المنصوص عليها في البند (1) من الفقرة (أ) من هذه المادة بالحبس مدة لا تقل عن سنة وبغرامة ال تقل عن 6000 ستة آلاف دينار ولا تزيد على 30000 ثلاثين ألف دينار إذا كان هذا المحتوى صوراً أو تسجيلات أو رسومات أو غيرها مثيرة جنسياً لأعضاء جنسية أو أفعال جنسية حقيقية أو افتراضية أو بالمحاكاة لحدث لا يتجاوز الثامنة عشرة من عمره أو كان المحتوى يتعلق بشخص مصاب بمرض نفسي أو بإعاقة عقلية)¹.

وتعليقاً على ما سبق تُعد هذه الفقرة جزءاً من المادة 13 التي تهدف إلى مكافحة الجرائم الإلكترونية المتعلقة بالمحتوى الإباحي، مع تركيز خاص على حماية الفئات الضعيفة مثل الأطفال والأشخاص ذوي الإعاقات النفسية أو العقلية، وتأتي هذه المادة كظرف مشدد للأفعال المذكورة في الفقرة 1/أ مثل (الإرسال، النشر، الاعداد، الانتاج، الترويج لأنشطة إباحية عبر شبكات المعلومات)، أذ ترفع العقوبة إلى الحبس بما لا يقل عن سنة وغرامة مالية قد يصل حدها الأقصى ثلاثون ألف دينار أردني إذا كان المحتوى يتعلق بصور أو تسجيلات مثيرة جنسياً او افعال جنسية حقيقة او افتراضية متعلقة بالقصر، ومن خلال النص يمكننا تحديد أركان جريمة إباحية الاطفال في القانون الاردني.

الركن المادي: لقيام الركن المادي لجريمة إباحية الاطفال في التشريع الاردني يشترط المشرع قيام الجاني بالأفعال المحصورة في المادة 13 على سبيل الحصر فقد عددها (الإرسال النشر الانتاج الاعداد المعالجة الحفظ العرض الطباعة الشراء البيع النقل أو الترويج....) لمحتوى إباحي، والذي يشمل صوراً أو رسوماً أو تسجيلات أو غيرها مثيرة جنسياً لأعضاء أو أفعال حقيقية أو افتراضية، لقصر دون سن 18 سنة، أو لشخص مصاب بمرض نفسي أو إعاقة عقلية، عبر استخدام شبكة معلوماتية أو نظام معلوماتي أو موقع إلكتروني، ولم يشترط وقوع ضرر على المجني عليه أذ يكفي الفعل نفسه لاكتمال الجريمة (كجريمة شكلية).

1- المادة 13 من قانون الجرائم الالكترونية رقم 17 لسنة 2023 الأردني، المرجع السابق.

الركن المعنوي : يتطلب لقيام الركن المعنوي في جريمة إباحية الاطفال في التشريع الاردني توافر القصد الجنائي العام (العمد)، أي أن يكون الفاعل مدركاً لطبيعة المحتوى (أنه إباحي متعلق بقاصر أو ذي إعاقة) ويريد ارتكابه، مع علمه بأن فعله غير مشروع.

أما الفقرة الثانية من المادة 13 فقد جاءت بالنص على عقوبة مرتكب الأفعال المنصوص عليها في البند (3) من الفقرة (أ) من هذه المادة بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن 9000 تسعة آلاف دينار ولا تزيد على 30000 ثلاثين ألف دينار إذا كان المحتوى صوراً أو تسجيلات أو رسومات أو غيرها مثيرة جنسياً لأعضاء جنسية أو أفعال جنسية حقيقية أو افتراضية أو بالمحاكاة لحدث لا يتجاوز الثامنة عشرة من عمره أو مصمماً لإغرائه أو كانت الغاية منه توجيهه أو تحريضه على ارتكاب جريمة أو بقصد استغلاله أو كان هذا المحتوى يتعلق بشخص مصاب بمرض نفسي أو بإعاقة عقلية).

وتمثل هذه المادة ظرفاً مشدداً آخر ضمن المادة 13 التي تجرم الأنشطة الإباحية عبر النظم المعلوماتية والتقنية، حيث ركزت على حماية القصر و ذوي الإعاقات النفسية من الاستغلال الجنسي الرقمي وهذ بوضعها عقوبة أشد من الفقرة الأولى من نفس المادة بعقوبة حبس تصل إلى سنتين وغرامة مالية تبدأ بحدها الأدنى من تسعة آلاف دينار أردني وتصل بحدها الأعلى إلى ثلاثون ألف دينار أردني، وهذا على الأفعال التي تعتبر من قبيل استغلال الأطفال في الأعمال الإباحية وتحديثهم على الانخراط في الدعارة والفجور أو تحضرهم على جريمة من هذا القبيل أو تسهيل مثل هذه الأنشطة، عبر شبكات النظم المعلوماتية والمواقع الإلكترونية .

كما عاقبت المادة 13 فقرة ج بالحبس مدة لا تقل عن 06 أشهر وبغرامة لا تقل عن ثلاثة آلاف دينار لا تزيد على ستة آلاف دينار كل من حاز داخل نظام المعلومات أو دعامة لتخزين البيانات صوراً أو تسجيلات أو رسومات أو غيرها مثيرة جنسياً لأعضاء جنسية أو أفعال جنسية حقيقية أو افتراضية أو بالمحاكاة لحدث لا يتجاوز 18 سنة.

أما المادة 14 فقرة ب فنصت على عقوبة كل من يستخدم الشبكة المعلوماتية والنظم المعلوماتية أو تقنية لإنشاء موقع إلكتروني وهذا تجسيدا للغايات المنصوص عليها في الفقرة أ

من هذه المادة إي لاستغلال من لم يكمل الثامنة عشرة من العمر أو من هو مصاب بمرض نفسي أو بإعاقة عقلية في الدعارة، بالحبس وبالأشغال المؤقتة كما فرضت عليه غرامة لا تقل عن خمسة عشر ألف دينار ولا تزيد على عن خمسة وأربعين ألف دينار)¹.

وفي نفس السياق تناول المشرع الاردني جريمة إباحية الاطفال عبر النظم المعلوماتية في قانون حقوق الطفل الأردني رقم 17 لسنة 2022 في المواد 21 و 22 و حظر تعريض الطفل للعنف أو البغاء أو الاستغلال في المواد الاباحية أو أي شكل من أشكال الاساءة الجنسية، و أوكل للجهات المختصة الوقائية والتربوية مهمة توفير الحماية اللازمة للطفل من هذا النوع من الجرائم الالكترونية².

1- أنظر المادة 14 من قانون الجرائم الالكترونية رقم 17 لسنة 2023 الأردني، المرجع السابق

2- أنظر المواد 21 و 23 من قانون حقوق الطفل الاردني رقم 17 لسنة 2022 الصادر بتاريخ 2022/10/12 والمنشور بالجريدة الرسمية رقم 5820 وساري المفعول بتاريخ 2023/01/10.

المطلب الثالث: معالجة جريمة إباحية الاطفال في التشريع الدولي.

أولاً: معالجة إباحية الاطفال في اتفاقية بودابست.

تناولت اتفاقية بودابست في المادة التاسعة جريمة إباحية الأطفال عبر النظم المعلوماتية¹، بهدف تعزيز حماية الأطفال من الاستغلال الجنسي من خلال تجريم استخدام تكنولوجيا المعلومات في هذا المجال وتحديث التشريعات الجزائية بفعالية أكبر، وتتماشى هذه المادة مع التوجه العالمي لحظر المواد الإباحية الطفولية²، كما عزز ذلك تبني البروتوكول الاختياري لاتفاقية الأمم المتحدة لحقوق الطفل المتعلق ببيع الأطفال ودعارتهم والمواد الإباحية.

وتجرم المادة التاسعة من اتفاقية بودابست جميع جوانب الإنتاج والحيازة والتوزيع الإلكتروني للمواد الإباحية التي تتضمن صور أطفال، رغم أن معظم الدول كانت تجرم بالفعل الإنتاج

1- المادة التاسعة من اتفاقية بودابست لسنة 2001 : (الجرائم ذات الصلة بمواد إباحية عن الأطفال 1. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم السلوكيات التالية في قانونها الوطني، إذا ما ارتكبت عمداً وبغير حق أ. إنتاج مواد إباحية عن الأطفال بغرض توزيعها عبر نظام الكمبيوتر؛ ب. عرض مواد إباحية عن الأطفال أو إتاحتها عبر نظام الكمبيوتر؛ ج. توزيع مواد إباحية عن الأطفال أو نقلها عبر نظام الكمبيوتر؛ د. الحصول على مواد إباحية عن الأطفال عبر نظام الكمبيوتر لصالح الشخص ذاته أو لفائدة الغير؛ هـ. حيازة مواد إباحية عن الأطفال داخل نظام الكمبيوتر أو على دعامة لتخزين بيانات الكمبيوتر. 2 لغرض الفقرة 1 أعلاه، تشمل عبارة " مواد إباحية عن الأطفال " المواد الإباحية التي تعرض بشكل مرئي: أ. قاصر وهو يمارس سلوكاً جنسياً واضحاً؛ ب. شخص يبدو قاصراً وهو يمارس سلوكاً جنسياً واضحاً؛ ج. صور واقعية تظهر قاصراً وهو يمارس سلوكاً جنسياً واضحاً).

2- بالإضافة إلى ما سبق ذكره نص على جريمة إباحية الاطفال واستعمال النظم المعلوماتية في انتاج أو توزيع أو حيازة مواد إباحية للأطفال، في العديد من الاتفاقيات والبروتوكولات الدولية منها اتفاقية الاتحاد الافريقي لسنة 2012 مشروع اتفاقية بشأن إطار قانوني للمساعدة في الأمن السيبراني في افريقيا في المواد 29 30 31 32، الكومنولث 2002 مشروع قانون الحاسوب والجرائم ذات الصلة بالحاسوب في المادة 10، ومجلس أوروبا اتفاقية بشأن الجريمة السيبرانية والبروتوكول الإضافي للاتفاقية بشأن الجريمة السيبرانية 2001 في المادة 09، مجلس أوروبا اتفاقية لانزوات المادة 20، الجماعة الاقتصادية لدول غرب أفريقيا 2009 في المواد 14 15 16 17، الاتحاد الأوروبي ومجلس أوروبا بشأن مكافحة الاعتداء جنسي والاستغلال الجنسي للأطفال عام 2011 في المادة 05، والاتحاد الدولي للإتصالات "الاتحاد الكاريبي للاتصالات" 2010 النصوص التشريعية النموذجية بشأن الجريمة السيبرانية والجريمة الالكترونية في المادة 13، الامم المتحدة البروتوكول الاختياري الملحق باتفاقية حقوق الطفل بشأن بيع الاطفال واستغلالهم في المواد الاباحية لسنة 2000 في المادة 03.

والتوزيع المادي التقليدي لإباحية الاطفال، إلا إن انتشار الإنترنت كوسيلة أساسية لتداول هذه المواد استدعى وضع نصوص دولية خاصة لمكافحة هذا النوع الجديد من جرائم استغلال الأطفال جنسياً¹.

وشملت المادة في فقرتها الاولى (أ) تجرم إنتاج المواد الإباحية الطفولية بقصد توزيعها عبر نظام معلوماتي، معتمدة بذلك على أن قاعدة مكافحة الخطر تبدأ من منع الإنتاج أصلاً، ففي هذه الفقرة حددت المادة معايير الحد الأدنى التي تعتبر الأفعال وفقها أعمال إباحية وتشمل أية مواد تظهر بشكل مرئي قيام القاصر بتصرفات جنسية أو ظهور أي شخص باتصال أو تصرف جنسي مع قاصر وكذلك الصور الواقعية التي تمثل أو تظهر قاصراً يتدخل بتصرف جنسي².

أما الفقرة الثانية (ب) فهي تُجرّم عرض المواد الإباحية الطفولية أو إتاحتها عبر نظام حاسوبي، ويشمل ذلك دعوة الآخرين أو التماسهم للحصول على هذه المواد-مع افتراض قدرة العارض على توفيرها فعلياً، نشر المواد على الإنترنت ليتمكن الغير من الوصول إليها، مثل إنشاء مواقع إباحية خاصة بالأطفال، و وضحت الفقرة الثالثة أن المقصود بالقاصر يحدد وفقاً للقوانين الوطنية للدول الأعضاء على أن يشمل في جميع الأحوال الأطفال دون سن 18 سنة.

الركن المادي حددت المادة التاسعة مجموعة من الأفعال والسلوكيات التي بتوافرها يتكون الركن المادي لجريمة إباحية الاطفال عبر النظم المعلوماتية وشملت إنتاج مواد إباحية بغرض نشرها أو تقديم و إتاحة مادة إباحية لطفل عبر النظام المعلوماتي، أو نقل المادة أو تزويد الغير بها عبر النظام المعلوماتي، أو حيازتها أو تخزينها.

الركن المعنوي بالنسبة للركن المعنوي لهذه الجريمة، تفرض المادة التاسعة تجريم مجموعة من الأفعال غير المشروعة المتعلقة بالمواد الإباحية الطفولية، مشابهاً لما جاء في الجرائم

1- التقرير التفسيري لاتفاقية بودابست حول الجريمة الالكترونية، المرجع السابق، ص15.

2- قطاف سليمان، بوقرين عبدالحليم، الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري، مقال منشور بالمجلة الأكاديمية للبحوث القانونية والسياسية، صارة عن كلية الحقوق والعلوم السياسية، جامعة عمار ثلجي، الاغواط، الجزائر، المجلد السادس، العدد الاول، تاريخ النشر 2022/03/31، ص243.

السابقة، شريطة ارتكابها عمداً، وبموجب هذا المعيار، لا تنشأ المسؤولية الجنائية إلا بتوافر النية لدى الشخص في تقديم أو إتاحة أو نشر أو نقل أو إنتاج أو حيازة مثل هذه المواد.

كما تسمح المادة للأطراف بتبني معيار أكثر دقة، بالنسبة لمقدمي الخدمات حيث يُعتمد على معيار العلم والسيطرة على المعلومات المنقولة أو المخزنة لقيام المسؤولية، أما إذا كان دور مقدم الخدمة يقتصر على كونه وسيطاً تقنياً لنقل هذه المواد عبر موقع إلكتروني، دون توافر القصد الجنائي المطلوب وفق التشريع الداخلي للدولة المنتمي لها، فلا تقوم مسؤوليته الجنائية ولا يُلزم بمراقبة المحتوى لتجنب هذه المسؤولية¹.

وتعد المادة التاسعة خطوة متقدمة في مكافحة جرائم إباحية الأطفال عبر الأنظمة المعلوماتية، إذ تجرم بشكل شامل الإنتاج، العرض، التوزيع، الاقتناء، والحيازة لهذه المواد سواء كانت حقيقية أو افتراضية، مما يوفر بيئة معززة لحماية الأطفال من الاستغلال الجنسي الرقمي ويشجع على التوحيد التشريعي والتعاون الدولي لمواجهة هذه التهديدات العابرة للحدود.

ثانياً: معالجة جريمة إباحية الاطفال في الاتفاقية العربية.

تناولت المادة الثانية عشرة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات جريمة إباحية الاطفال حيث جاءت المادة بثلاث فقرات حددت في الأولى الافعال المجرمة وفي الثانية ظروف التشديد العقوبة وفي الثالثة توسعت من نطاق التجريم وجاء النص كما يلي: (جَرِيْمَةُ الْإِبَاحِيَّةِ 1- إِنْتَاجُ أَوْ عَرْضُ أَوْ تَوْزِيْعُ أَوْ تَوْفِيْرُ أَوْ نُشْرُ أَوْ شِرَاءُ أَوْ بَيْعُ أَوْ اسْتِيْرَادُ مَوَادِّ إِبَاحِيَّةٍ أَوْ مُخَلَّاتٍ بِالْحَيَاءِ بِوَسْطَةِ تَقْنِيَّةِ الْمَعْلُومَاتِ. 2- شَدُّدُ الْعُقُوبَةِ عَلَى الْجَرَائِمِ الْمُتَعَلِّقَةِ بِإِبَاحِيَّةِ الْأَطْفَالِ وَ الْقَصْرِ. 3- يَشْمَلُ التَّشْدِيْدُ الْوَاردُ فِي الْفِقْرَةِ (2) مِنْ هَذِهِ الْمَادَّةِ، حِيَازَةَ مَوَادِّ إِبَاحِيَّةِ الْأَطْفَالِ وَالْقَصْرِ أَوْ مَوَادِّ مُخَلَّاتٍ بِالْحَيَاءِ لِلْأَطْفَالِ وَالْقَصْرِ عَلَى تَقْنِيَّةِ الْمَعْلُومَاتِ أَوْ وَسْطِ تَخْزِيْنِ تِلْكَ التَّقْنِيَّاتِ)².

1- مفيدة مباركية، المرجع السابق، ص 235.

2- المادة الثانية عشر من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المرجع السابق.

وتتطرق المادة الثانية عشر أعلاه إلى جريمة إباحية الأطفال، وتنصت في فقرتها الأولى والثالثة على تجريم أفعال إنتاج أو عرض أو توزيع أو إتاحة أو نشر أو شراء أو بيع أو استيراد مواد إباحية أو مخلة بالحياء باستخدام تقنية المعلومات، أما الفقرة الثانية من المادة فتتعلق بظروف تشديد العقوبة في الحالات المتعلقة بالقصر، سواء تعلّق الأمر بإنتاج أو تداول هذه المواد أو حتى حيازتها عبر تقنيات المعلومات أو وسائط تخزينها.

الركن المادي: يتحقق الركن المادي لجريمة إباحية الاطفال عبر النظم المعلوماتية في المادة الثانية عشر من خلال ارتكاب سلوك إيجابي يتم فيه استخدام تقنيات المعلومات والنظم المعلوماتية في إنتاج المواد الإباحية أو عرضها ونشرها و توزيعها أو أتاحتها ونقلها عبر النظم المعلوماتية أو حيازتها وتخزينها على وسائط رقمية، ويكفي لتحقيق هذا الركن ارتكاب أي فعل من الأفعال السابقة متى كان من شأنه تمكين الغير للوصول إلى المحتوى الإباحي أو التعبير بالقاصر للقيام بهذه الأفعال، دون اشتراط تحقق نتيجة معينة مما يجعل الجريمة من جرائم الخطر لا من جرائم الضرر.

الركن المعنوي: يقوم الركن المعنوي في هذه الجريمة على توافر القصد الجنائي "العمد" أي علم الجاني بطبيعة المحتوى الإباحي المتعلق بالقصر الذي يقوم بنشرة أو إنتاجه أو توزيعه، واتجاه أرائته إلى إيصاله للغير باستخدام تقنية المعلومات والنظم المعلوماتية.

وعلى الرغم من الأهمية الكبيرة للمادة 12 باعتبارها أطارا قانونيا مهماً لمكافحة جرائم النظم المعلوماتية ذات المحتوى الإباحي لا سيما التي تستهدف الأطفال، إلا أنها يؤخذ عليها أن المشرع العربي لم يضع تعريفاً دقيقاً لمصطلح " المواد المخلة بالحياء"، وهو ما يثير إشكالية قانونية وتباين في التطبيق بين الدول، ويسمح بتفسير واسع قد يمتد ليشمل أشكالاً متعددة من المحتوى الرقمي قد تمس حرية التعبير مثل الأعمال الأدبية والفنية وغيرها من أنشطة النشر الإلكتروني¹.

1- محمد الطاهر، تعليق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، مقال منشور على الموقع الإلكتروني لمؤسسة حرية الفكر والتعبير، منظمة حقوقية مستقلة، جمهورية مصر العربية، عبر الرابط

المبحث الثالث: جريمة التعدي على الملكية الفكرية المعلوماتية.

يرتكز النظام القانوني لحماية حقوق الملكية الفكرية، سواء في شقها الأدبي والفني أو في مجال الملكية الصناعية، على ضمان الحقوق المقررة لأصحاب المصنفات والابتكارات، وتُمنح هذه الحماية متى توافرت في المصنفات صفة الأصالة بالنسبة لحقوق المؤلف، ومتى اتسمت الابتكارات بالجِدَّة والطابع الابتكاري وقابليتها للتطبيق الصناعي، مع ضرورة استكمال المتطلبات الشكلية التي يحددها القانون فيما يتعلق ببراءات الاختراع والرسوم والنماذج الصناعية، ومن المؤكد أن مظلة الحماية القانونية لا تقتصر على الوسائل التقليدية فقط، بل تمتد لتشمل استخدام المصنفات والابتكارات عبر النظم المعلوماتية المتنوعة ووسائل النشر الإلكتروني، إذ يُحظر أي استغلال أو استعمال لهذه المصنفات على نحو يمس بالحقوق المقررة لأصحابها ما لم يصدر بذلك إذن أو ترخيص صريح ومسبق منهم، وإلا اعتُبر هذا السلوك تعدياً على حقوق الملكية الفكرية يستوجب المساءلة القانونية¹.

وتعرف الملكية الفكرية على أنها كل ما ينتجه ويبدعه العقل والذهن الانساني وتشمل الافكار والابتكارات التي تتجسد في أشكال ملموسة أو قابلة للحماية القانونية، مثل الابداعات الفكرية والاختراعات والعلامات والرسوم والنماذج، وتتمثل أهم خصائص هذه الحقوق في منح صاحبها الحق المعنوي الذي يتجلى في جانبين:

ط-الاول يتعلق بالسلطة المعنوية أو ما يعرف بحق الاستئثار الذي يمكن صاحب الحق الفكري من نسب أبداعه الفكري أو اختراعه إليه كامتداد لشخصيته، مما يحمي الهوية الأدبية أو الفنية أو العلمية للمبدع ويمنع انتحال أو نسب غير مشروع مع امكانية فرض عقوبات جنائية او مدنية على المخالفين.

ظ- الثاني يتعلق بالسلطة المادية أو ما يسمى بحق الاستثمار، الذي يتيح لصاحب الحق الفكري أو الأدبي الاستفادة المالية من مصنّفه من خلال بيعه، أو منح التراخيص للغير للاستفادة

، <https://afteegypt.org/research/research-papers/2015/03/11/9770-afteegypt.html> ،

تاريخ الاطلاع 2025/08/28 الساعة 13:20.

1- بوربابة سورية، المرجع السابق، ص167.

منه بشروط محددة ولمدة معينة، مع ضمان تعويضات عن أي انتهاك للأطر الزمنية المتفق عليها¹.

المطلب الاول: تفصيل جريمة التعدي على الملكية الفكرية المعلوماتية.

ويقصد بحماية الملكية الفكرية الحماية القانونية لجميع عناصر الابتكار سواء تمثلت في حقوق المؤلف أو الحقوق المجاورة لحقوق المؤلف أو الاسماء التجارية أو العلامات التجارية أو براءات الاختراع أو الرسوم والنماذج الصناعية أو تصميم الدوائر المتكاملة أو الاصناف النباتية الجديدة، وهذا وفقا للأحكام القانونية والوطنية المنظمة لهذه الحقوق، بما في ذلك اتفاقيات منظمة التجارة العالمية "تربس 1994 و اتفاقية برن لحماية المصنفات الادبية والفنية.

ويمكن اعتبار الجرائم المتعلقة بانتهاك حقوق الملكية الفكرية عبر أنظمة الحاسب الآلي والتكنولوجيات الحديثة ضمن فئة جرائم نظم المعلومات وذلك للاعتبارات التالية.

أ- أن حقوق الملكية الفكرية قد تكون ممثلة في صورة مادية، كبرامج الحاسوب، أو الاقراص المدمجة، كما يمكن أن تكون في هيئة حزم معلوماتية أو ملفات إلكترونية موضوعة على موقع إلكتروني، فلا فرق جوهري بينها إلا في طريقة عرضها أو الوسيلة الحاملة لها، مما يجعل الانتهاكات المعلوماتية معادلة للانتهاكات التقليدية لحقوق الملكية الفكرية.

ب- أن هناك تشابها كبيرا بين الالتزامات القانونية الواردة على هذه الحقوق سواء كانت في صورة مادية، كأسطوانات الليزر أو صورة معنوية كالملفات الإلكترونية وذلك من حيث (عدم جواز نسبتها إلى غير صاحبها، عدم جواز بيع النسخ المقلدة، عدم جواز التعديل غير المشروع على البرنامج، ولا اتلافه ولا تعطيله).

ت- باستثناء حالات تجريم نسخ البرامج بسبب كونها مادية، فإن الاحكام والقواعد القانونية المطبقة على البرامج بصفتها معلومات معنوية تنطبق على الحالتين، ولا فرق بينهما من هذه الناحية¹.

1- لواعر فاطمة، الملكية الفكرية في البيئة الرقمية، مقال منشور بمجلة الحوكمة والقانون الاقتصادي، كلية الحقوق والعلوم السياسية، جامعة باتنة 1 الجزائر، المجلد الثالث، العدد الثاني جويلية 2023، ص 9.

وتُعرّف جرائم انتهاك الملكية الفكرية وحقوق المؤلف والعلامات التجارية المرتكبة عبر أنظمة الحواسيب بأنها الأفعال غير المشروعة التي تنصب على المصنفات الرقمية² وبرامج الحاسوب وبياناتها والتصاميم والدوائر المتكاملة المنشورة عبر النظم المعلوماتية، وعناوين ومواقع الانترنت، وتشمل الأفعال نسخ أو استنساخ أو تقليد أو توزيع أو نقل أو استخدام المواد المخزنة في البيانات الحاسوبية أو البيانات الحاسوبية المولدة، مما يشكل انتهاكاً مباشراً للحماية القانونية المقررة بموجب قوانين حقوق الملكية الفكرية المحلية، بما في ذلك حقوق التأليف والنشر أو العلامات التجارية، وفقاً للاتفاقيات الدولية ذات الصلة مثل اتفاقية برن لحماية المصنفات الأدبية والفنية واتفاقية تريبس التابعة لمنظمة التجارة العالمية، ويتمثل هذا الانتهاك، على سبيل المثال لا الحصر، في حالة قيام الجاني بتوزيع أو مشاركة أغنية أو مصنف موسيقي محمي بحقوق التأليف والنشر، من خلال أنظمة تبادل الملفات أو المنصات الرقمية، دون الحصول على ترخيص صريح أو إذن مسبق من المؤلف أو صاحب الحق، مما يعرضه للمسؤولية الجنائية والمدنية، بما في ذلك التعويض عن الضرر المادي والمعنوي الناتج عن مثل هذه الأفعال³.

وكغيرها من الجرائم تتكون جريمة التعدي على الملكية الفكرية المعلوماتية من أركان أساسية سنحاول تفصيلها كالتالي:

الركن المادي لجريمة التعدي على الملكية الفكرية المعلوماتية يتمثل في عدد من السلوكيات والأفعال وهو سلوك إيجابي أو سلبي يشكل انتهاك لحقوق الملكية الفكرية مثل: ث-النسخ غير المشروع: إعادة إنتاج المصنف الرقمي دون إذن أو تصريح من صاحب الحق الأدبي مثل نسخ برامج الحاسوب وملفات الموسيقى.

1- عبد العزيز بن غرام الله آل جاراالله، المرجع السابق، ص 394 و 295.

2- يعرف المصنف الرقمي على أنه "كل مصنف أبداعي عقلي ينتمي إلى بيئة تقنية المعلومات" فبرامج الحاسوب مصنف رقمي كذلك قاعدة البيانات وطبوغرافيا الدوائر المتكاملة باعتبارها نتائج تطور علم الحاسوب، بخلاف أسماء وعناوين الانترنت والبريد الالكتروني التي تعتبر من المصنفات التي ارتبط ظهورها بشبكة الانترنت، أنظر في ذلك د ربيعي حشين، المرجع السابق، ص 83.

3- أنظر ملحق شرح الأفعال، المرجع السابق ص 366.

ج- التوزيع أو النشر: مشاركة أو رفع الملفات والمصنفات الرقمية والاعمال الفكرية عبر المواقع الالكترونية من أجل إتاحتها للجمهور.

ح- العرض أو التوفير: جعل المصنف متاحا للجمهور عبر النظم المعلوماتية أو عبر التطبيقات بدون ترخيص دون إذن صاحب الحق مع تغيير أو حذف لإدارة حقوق الملكية الفكرية.

خ- البيع أو الترويج والاستيراد الرقمي: وذلك بعرض نسخ مقلدة للبيع عبر مواقع إلكترونية أو الاعلان عنها، ونقل المصنفات المقلدة عبر الحدود الرقمية للنظم المعلوماتية¹.

وتعتبر هذه الأفعال إيجابية في الغالب، لكنها قد تشمل امتناعا في حالات نادرة مثل عدم ازالة محتوى مقلد رغم العلم به من طرف مقدمي الخدمات، ويجب أن يتم الانتهاك عبر استخدام النظم المعلوماتية والوسائل الرقمية، وهذا ما يميز الجريمة عن الانتهاكات التقليدية كطباعة كتاب مقلد، وتشمل الوسائل أنظمة الحواسيب والاجهزة الذكية والشبكات المعلوماتية و وسائل التخزين الرقمية والتي بدونها قد يصنف الفعل كانتهاك تقليدي وليس جرائم نظم معلوماتية.

الركن المعنوي يتطلب قيام الركن المعنوي لجريمة التعدي على الملكية الفكرية المعلوماتية توافر القصد ال عام أي أن يكون الجاني عالما بأن العل غير المشروع (علمه بأن المصنف الرقمي محمي وأن السلوك الذي يؤديه مخالف للقانون)، ومع ذلك يرتكب فعله بإرادة حرة، وفي بعض التشريعات يشترط توافر قصد جنائي خاص يتمثل باستفادة الجاني من منفعة مالية أو إلحاق ضرر بصاحب الحق خاصة في الجرائم التجارية الكبيرة "القرصنة".

وتعتبر هذه الجريمة جريمة شكلية في معظم التشريعات، أي أنها تكتمل بمجرد وقوع الفعل غير المشروع دون الحاجة إلى إثبات ضرر مادي فعلي مثل خسارة مالية لصاحب الحق ومع ذلك قد يؤخذ الضرر بعين الاعتبار كظرف مشدد للعقوبة أو في الدعوى المدنية المصاحبة (التعويضات).

1- عبد العزيز بن غرام الله آل جارالله، المرجع السابق، ص 289 و 299.

المطلب الثاني: معالجة جريمة التعدي على الملكية الفكرية المعلوماتية في التشريع الجنائي.

أولاً: التشريع الجزائري.

سعى المشرع الجزائري إلى مواجهة الجرائم المعلوماتية، خاصة تلك المتعلقة بانتهاك حقوق الملكية الفكرية، من خلال قانون حماية الملكية الادبية والفنية المتعلق بحقوق المؤلف والحقوق المجاورة الصادر بموجب الامر رقم 05/03 المنشور بتاريخ 2003/07/23¹، حيث أوسع نطاق قائمة المصنفات المحمية قانوناً من خلال إدراج برامج المعلوماتية ضمن المصنفات الاصلية، وأعرب عنها صراحة بمصنفات رقمية وتشمل قواعد البيانات وبرامج الحاسب الآلي وبرامج المعلوماتية، مع تشديد العقوبات الجزائية والمدنية على أي مساس بحقوق المؤلفين، لاسيما فيما يتعلق بالمصنفات الرقمية التي شملتها الحماية آليات الحماية القانونية²، وجاء هذا بما يتوافق مع اتفاقية برن لحماية المصنفات الأدبية والفنية واتفاقية ترسيم المتعلقة بالجوانب التجارية لحقوق الملكية الفكرية.

ولكي تحظى المصنفات الرقمية التي نص عليها المشرع الجزائري في المادة الرابعة من الأمر المذكور أعلاه (برامج الحاسب الآلي وقواعد البيانات والدوائر المتكاملة) بالحماية القانونية لحقوق الملكية الفكرية أوجب المشرع أن يتوافر بها عدة شروط وهي كالتالي:

د- الابتكار: يبرز شرط الابتكار بوضوح في نصوص المادتين 04 و 05³ من الأمر سابق ذكره المتعلق بحماية الملكية الفكرية والادبية، حيث اعتبرها المشرع الجزائري المصنفات الرقمية بمثابة مصنفات ذات ابتكار ذهني، مما يشترط فيها توافر عنصر الابتكار كشرط أساسي لحمايتها قانوناً، ويقصد بالابتكار هنا مفهوم الاصلية، أي أن يتميز المصنف

1- أمر رقم 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة المؤرخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003، المنشور بالجريدة الرسمية الجزائرية عدد 44 بتاريخ 23 يوليو 2003.

2- قطاف سليمان، بوقرين عبد الحليم، المرجع السابق، ص 350.

3- تهدف المادتين 04 و 05 إلى سرد أمثلة غير حصرية للمصنفات المحمية، مما يتيح للقضاء توسيع النطاق ليشمل أشكالاً جديدة من الإبداع مع تطور التكنولوجيا، مثل البرمجيات الرقمية أو المحتويات الإلكترونية، كما توسع هذه المادة نطاق الحماية ليشمل الإبداعات الرقمية، مما يساعد في مكافحة الجرائم الإلكترونية، للمزيد أنظر المادتين 04 و 05 من الامر 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة.

بطابع أصيل في إنتاجه أو في التعبير عنه، يعكس شخصية صاحبة في مضمون وجوهر الفكرة التي اتبعتها لعرض فكرته.

د- الإيداع أو التسجيل: يقصد به الإجراء القانوني الذي يلزم صاحب المصنف بإيداع نسخة من مصنفه لدى الجهة المختصة التي يحددها القانون، سواء كانت إحدى السلطات الحكومية أو إحدى المكتبات أو المؤسسات العامة المعينة لهذا الغرض، وذلك وفقاً للأحكام المنظمة لحقوق الملكية الفكرية في التشريع الجزائري، وقد اشترط المشرع الجزائري في الفقرة الثانية من المادة الثالثة¹ من الأمر رقم 05/03 الخاص بحقوق المؤلف والحقوق المجاورة، إيداع المصنف مهما كان نوعه أو نمط تعبيره أو وجهته، وسواء كان مثبتاً أو غير مثبت على أي دعامة تسمح بإبلاغه إلى الجمهور، مع ضمان أن يُشكل هذا الإيداع دليلاً أولياً على ملكية المصنف وتاريخ إنشائه، دون أن يُعد شرطاً جوهرياً للحماية القانونية المبينة على أساس ملكية المصنف².

يُلاحظ أن المشرع الجزائري لم يميز بين المصنفات التقليدية والمصنفات المعلوماتية (الرقمية) في توفير الحماية القانونية المقررة لها، وفقاً للأحكام المنصوص عليها في المواد السابقة من الأمر 05/03، كما أقر المشرع حماية جنائية لحقوق الملكية الفكرية من خلال دعوى التقليد، إلا أنه أكتفى بتحديد الأفعال التي تدرج ضمن هذه الجنحة دون تقديم تعريف خاص لجريمة التقليد، حيث يتحقق السلوك الإجرامي (الركن المادي) بوقوع أحد الأفعال التي تمس الحقوق الاستثنائية للمؤلف³، وفقاً لنص المادة 151 من الأمر المذكور، وتتمثل هذه الأفعال في:

ر- الكشف غير المشروع عن المصنف، مما يشكل انتهاكاً لحقوق السرية والنشر الحصري لصاحب الحق.

ز- المساس بسلامة المصنف، بما في ذلك أي تعديل أو تحريف غير مصرح به يؤثر على جوهر أو مضمونة

1- المادة الثالثة من الأمر 05/03 (تمنح الحماية مهما يكن نوع المصنف ونمط تعبيره ودرجة استحقاقه ووجهته، بمجرد إيداع المصنف سواء أكان المصنف مثبتاً أم لا بأية دعامة تسمح بإبلاغه إلى الجمهور).

2- بوريابة صورية، المرجع السابق، ص 164 و 165.

3- مفيدة مباركية، المرجع السابق، ص 275.

- س- الاستيراد أو التصدير لنسخ مقلدة من المصنف، بغض النظر عن مكان الفعل.
- ش- بيع نسخ مقلدة من لمصنف.
- ص- تأجير نسخ مقلدة من المصنف¹.
- ض- نشر المصنف المحمي عبر أجهزة الحاسب الآلي أو الشبكة المعلوماتية، دون الحصول على ترخيص مسبق من صاحب الحق، وفقا لأحكام المادة 152 من الأمر أعلاه.

وينصب محل الجريمة على كل مصنف أو ابتكار يتمتع بالحماية القانونية، سواء تعلق الأمر بمصنفات أدبية أو فنية في صورتها الرقمية، أو ببرامج الحاسوب وقواعد البيانات، أو بحقوق الملكية الصناعية كبراءات الاختراع والعلامات التجارية متى تم استغلالها عبر الوسائط أو النظم المعلوماتية، وتتمثل النتيجة الإجرامية في الإضرار بالمصالح الأدبية أو المالية لصاحب الحق، أو تعريضها للخطر، ويكفي في بعض الصور تحقق الخطر دون اشتراط وقوع ضرر فعلي، باعتبار أن هذه الجرائم تُصنف ضمن جرائم الخطر التي يكفي فيها المشرع بمجرد قيام الاحتمال الجدي للإضرار بالحق محل الحماية.

الركن المعنوي: يقوم الركن المعنوي لجريمة التعدي على الملكية الفكرية المعلوماتية في التشريع الجزائري بتوافر القصد الجنائي العام لدى الجاني باعتباره عنصرا أساسيا لقيام المسؤولية الجنائية حيث تعتبر هذه الجريمة من الجرائم العمدية، ويتحقق القصد العام بتوافر عنصره العلم والارادة، والعلم المقصود يقع على العلم بالوقائع لا العلم بالقانون فيكون الفاعل عالما بموضوع الحق المعتدى وأن المصنف أو الابتكار الذي يعدله أو ينسخه أو يستغله عبر وسائط النظم المعلوماتية، إنما هو محلاً يتمتع بالحماية وهو يفعل هذا الاعتداء بدون إذن أو ترخيص من صاحب الحق على المصنف، أما الارادة فتظهر في عزم الفاعل واتجاه تلك الإرادة الحرة إلى القيام بفعل من أفعال الاعتداء السالفة الذكر، ويتجسد ذلك في تعمد الجاني نسخ المصنف أو إتاحتها أو تداوله إلكترونياً، مع علمه بعدم مشروعية هذا السلوك².

1- أنظر المادة 151 من الامر 05/03 ، المرجع السابق.

2- بشأن عبدالنور، المرجع السابق، ص 255.

أما العقوبات المقررة لمرتكبي جرائم انتهاك الملكية الفكرية المعلوماتية، فقد نصت عليها المادة 153 من الأمر رقم 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة، حيث حددت عقوبة الحبس لمدة تتراوح بين ستة أشهر وثلاث سنوات، إضافة إلى غرامة مالية تتراوح بين خمسمائة ألف دينار جزائري ومليون دينار جزائري، مع تشديد العقوبة في حالة العود وفق المادة 156 من نفس الأمر، مع إمكانية فرض عقوبات إضافية مثل مصادرة الأدوات المستخدمة في الجريمة أو تعويض الضرر المدني لصاحب الحق، وفقاً لأحكام القانون الجنائي والمدني الجزائري¹.

ويتبين من خلال أحكام الأمر رقم 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة أن المشرع الجزائري أولى لحماية الملكية الفكرية بما فيها المصنفات الرقمية، أهمية واضحة، حيث وسّع نطاق الحماية ليشمل برامج الحاسب الآلي وقواعد البيانات والدوائر المتكاملة، دون تمييز بين المصنفات التقليدية والمعلوماتية، كما اشترط توافر عنصر الابتكار كركيزة أساسية للحماية، مع تنظيم الإيداع كوسيلة إثبات قانونية دون اعتباره شرطاً جوهرياً لقيام الحق.

وعلى الصعيد الجنائي، جرم المشرع الجزائري مختلف صور الاعتداء على الحقوق الأدبية والمالية للمؤلف، بما في ذلك الاستغلال غير المشروع للمصنفات عبر الوسائط المعلوماتية، مع اشتراط القصد الجنائي العام لقيام المسؤولية الجزائية، كما قرر عقوبات سالبة للحرية وعقوبات مالية مع تشديدها في حالة العود، إلى جانب العقوبات التكميلية، بما يعكس توجهه نحو توفير حماية جنائية فعالة للملكية الفكرية في البيئة الرقمية.

ثانياً: التشريع السعودي.

أبدت المملكة العربية السعودية اهتماماً مبكراً بحماية حقوق الملكية الفكرية، حيث بادرت إلى سن الأنظمة اللازمة لهذا الغرض منذ فترة مبكرة، ومن ذلك إصدار نظام مكافحة الغش التجاري لعام 1404هـ الموافق 1983م، تلاه إصدار نظام براءات الاختراع في عام 1409هـ الموافق 1989م، أما فيما يتعلق بحماية برامج الحاسب الآلي، فقد كانت المملكة سباقة على

1- أنظر المواد 153 و 156 و 157، من الامر 05/03، المرجع السابق.

المستوى العربي بتسجيلها كمصنفات أدبية محمية بموجب نص المادة 20 من نظام المطبوعات والنشر الصادر عام 1402هـ الموافق 1983م، كما صدر نظام حماية حقوق المؤلف بالمرسوم الملكي رقم م/11 لعام 1410هـ الموافق 1989م، حيث نص المشرع السعودي صراحةً على حماية حقوق أصحاب البرامج، إضافة إلى نظام حقوق المؤلف الصادر بالمرسوم الملكي رقم 41 لعام 1424هـ الموافق 2003م، والذي تم تعديله لاحقاً لتعزيز الحماية وفقاً لأفضل الممارسات الدولية¹.

وحدد النظام تعريف الأعمال المحمية في مادته الثانية، إذ يضمن هذا النظام حماية الإبداعات الأصلية في مجالات الأدب والفنون والعلوم، مهما اختلفت أنواع هذه الإبداعات أو أساليب التعبير عنها أو مستويات أهميتها أو أهداف من إنشائها، بعد ذلك، سرد هذه الأعمال الإبداعية الأساسية، مع الإشارة الصريحة إلى برمجيات الحاسب الآلي ضمن البند الحادي عشر منها، كما أشار النظام في مادته الثانية أن هذا التشريع يمتد أيضاً لحماية الإبداعات المشتقة، بما في ذلك قواعد البيانات، سواء اتخذت شكلاً قابلاً للقراءة الآلية أو أي نمط آخر مبتكر من حيث محتواها، وفيما يتعلق بالجزاءات المطبقة على من يخالف هذه الحماية.

ويتمثل الركن المادي لجريمة الاعتداء على حقوق الملكية الفكرية المعلوماتية في النظام السعودي في ارتكاب أحد الأفعال المادية غير المشروعة التي حددها المنظم صراحة، والتي تنطوي على مساس مباشر أو غير مباشر بحقوق المؤلف أو صاحب الحق في البيئة الرقمية أو المعلوماتية.

وقد تولّى المنظم السعودي في المادة (21) من نظام حماية حقوق المؤلف حصر أبرز صور السلوك الإجرامي التي تُعد انتهاكاً وتعدياً على حقوق التأليف والنشر التي يكفلها النظام، وهو ما يحقق قدرًا عاليًا من الوضوح والتحديد في بيان الركن المادي للجريمة²:

1- عبدالعزيز بن غرام الله آل جارالله، المرجع السابق، ص 303.

2- سعد بن ناصر آل غرام- عبد الرحمن جابر علوان، دور نظام الملكية الفكرية في الحد من جرائم الاحتيال الفكري والمادي على حقوق المؤلفين في المملكة العربية السعودية، مقال منشور في مجلة العلوم القانونية

- ث- إزالة أي معلومة كتابية وإلكترونية قد تتسبب في إسقاط حقوق أصحاب المصنف.
- ج- إزالة وفك أي معلومة احترازية إلكترونية تضمن استخدام النسخ الأصلية للمصنف، مثل التشفير، أو المعلومات المدونة بالليزر، أو غيره.
- ح- الاستخدام التجاري للمصنفات الفكرية بطرق التحايل التي لا تسمح بها الجهة صاحبة الحق، مثل استخدام البرمجيات المنسوخة، أو النقاط البرامج الإذاعية المشفرة بطرق غير نظامية.
- خ- تصنيع أو استيراد أدوات لغرض البيع أو التأجير لأي وسيلة من شأنها تسهيل استقبال أو استغلال مصنفات بطرق غير الطرق التي تحددها الجهة صاحبة الحقوق.
- د- نسخ أو تصوير أجزاء من كتاب أو مجموعة كتب أو أجزاء من أي مصنف بعوض أو بدون عوض دون الحصول على الموافقات الخطية من أصحاب الحق والجهات المعنية في الوزارة، باستثناء حالات النسخ المشروعة المبينة في المادة الخامسة عشرة من هذا النظام¹.

ويتضح مما سبق أن الركن المادي لجريمة الاعتداء على حقوق الملكية الفكرية المعلوماتية في النظام السعودي يقوم على سلوك إيجابي محدد يتمثل في إحدى الصور التي عدتها المادة (21)، ويكفي تحقق أي منها لقيام الجريمة متى وقع الاعتداء على مصنف محمي نظاماً، كما يعكس هذا التنظيم توجه المنظم السعودي نحو تشديد الحماية الجنائية للمصنفات الرقمية، ومواكبة التطور التقني، بالإضافة إلى التصدي لمختلف صور التعدي المعلوماتي، سواء المباشرة أو غير المباشرة.

أما الركن المعنوي في جريمة الاعتداء على حقوق الملكية الفكرية المعلوماتية في النظام السعودي فيقوم على القصد الجنائي العام، باعتبارها من الجرائم العمدية التي لا يتصور وقوعها بطريق الخطأ أو الإهمال، وذلك لطبيعة الأفعال التي عدتها المادة (21) من نظام حماية حقوق المؤلف، والتي تفترض جميعها تدخلاً إرادياً واعياً من الجاني، ويتحقق بتوافر عنصرين أساسيين هما العلم والإرادة، إذ يفترض المشرع السعودي علم الجاني بأن المصنف محل الفعل الاجرامي

والسياسية، صادرة عن كلية الحقوق والعلوم السياسية، جامعة حمة الاخضر الوادي، الجزائر، المجلد 16، العدد 02، سبتمبر 2025، ص 104.

1- للمزيد أنظر المادة 21 من نظام حقوق المؤلف السعودي الصادر بالمرسوم الملكي رقم 41 لعام 1424هـ الموافق لسنة 2003م.

محمي بموجب نظام حماية حقوق المؤلف، وأن الأفعال التي يقدم عليها كإزالة المعلومات أو فك التشفير أو النسخ، هي عمل غير مشروع وتتم دون ترخيص أو موافقة نظامية من صاحب الحق، ومع ذلك تتجه إرادة إلى ارتكاب الفعل، ولا يشترط هنا اتجاه إرادة الجاني إلى إحداث ضرر معين حسب النظام السعودي بل يكفي أن تنصرف إرادته إلى تحقيق الفعل المجرم مع علما بعدم مشروعيته.

أما من حيث العقوبة فقد فرض النظام مجموعة متنوعة من العقوبات الأساسية والفرعية والتكميلية، على الجاني وذلك ضمن أحكام المادة 22 وهي كالتالي:

يعاقب كل من خالف حكماً من أحكام هذا النظام بعقوبة أو أكثر من العقوبات الآتية:

أ- الإنذار.

ب- عقوبة مالية لا تزيد عن 250 ألف ريال.

ت- أغلاق المنشأة المتعدية أو التي ساهمت في الاعتداء على حق المؤلف مدة لا تتجاوز شهرين.

ث- مصادرة جميع نسخ المصنف وكذا المواد المخصصة أو المستخدمة في ارتكاب التعدي على حق المؤلف.

ج- السجن مدة لا تتجاوز الستة أشهر.

إضافة إلى ذلك تم تضمين عقوبات أخرى منها جواز إلزام الجاني التعويض لصاحب الحق، والتعويض عن التشهير و وقف نسخ المصنف المخالف، وذلك في بنود المواد (3- 4 - 5 - 6 - 7) من نظام حقوق المؤلف الصادر في عام 2003¹.

ثالثاً: التشريع الإماراتي.

أولت الإمارات العربية المتحدة اهتماماً بالغاً بحماية الملكية الفكرية، سواء التقليدية أو الإلكترونية، من خلال إصدار مرسوم بقانون اتحادي رقم 38 لسنة 2021 بشأن حقوق المؤلف والحقوق المجاورة، والذي جاء ليضع الإطار القانوني الواقي من الاعتداء على حقوق المؤلفين والمبدعين، ويعكس هذا القانون حرص المشرع الإماراتي على ضمان التوازن بين حرية الإبداع

1- المادة 22 من نظام حقوق المؤلف السعودي، المرجع السابق.

وحق المؤلف في استغلال أعماله قانونيًا، وحماية المجتمع من الانتهاكات التي تمس النظام الاقتصادي والثقافي والفكري.

ويعكس القانون موقف المشرع الإماراتي الحازم من جريمة التعدي على الملكية الفكرية، من خلال فرض عقوبات رادعة وضمان حماية قانونية شاملة لجميع المصنفات، سواء كانت تقليدية أو رقمية، وذلك عبر المواد (39) و(40) التي تحدد الأفعال المحظورة والعقوبات المقررة.

وفقاً لهذا القانون، يُعرف المصنف بأنه كل إنتاج مبتكر في مجال الآداب أو الفنون أو العلوم، بغض النظر عن نوعه، أو طريقة التعبير عنه، أو أهميته، أو الغرض من إنشائه، ويشمل هذا التعريف جميع أشكال الإبداع التي يمكن حمايتها قانونيًا، مما يضمن حقوق المؤلف في التحكم في استخدام أعماله والاستفادة منها، ويُعد الأساس القانوني لحماية الإبداعات الفكرية من الاستغلال غير المشروع.

وجاء النص على المصنفات المشمولة بالحماية في المادة الثانية من المرسوم المذكور اعلاه بشأن حقوق المؤلف والحقوق المجاورة، إذ يتمتع مؤلفو المصنفات وأصحاب الحقوق المجاورة بالحماية القانونية إذا وقع الاعتداء على حقوقهم، وتشمل الحماية بشكل خاص المصنفات الوارد ذكرها في المادة ومنها، المصنفات المكتوبة مثل الكتب والكتيبات والمقالات وغيرها، إضافة إلى المصنفات الرقمية مثل التطبيقات الذكية، وبرامج الحاسب الآلي وتطبيقاتها، وقواعد البيانات، وأي مصنفات مماثلة يحددها الوزير بقرار رسمي، ويُعد هذا التحديد أساساً لحماية حقوق المؤلفين وضمان عدم الاستغلال غير المشروع لمصنفاتهم، سواء كانت تقليدية أو رقمية¹.

ومن نص مواد القانون المذكور اعلاه يمكننا استخلاص أركان جريمة الاعتداء على الملكية الفكرية المعلوماتية في التشريع الإماراتي وهي كالتالي:

1- المادة الثانية من قانون حقوق المؤلف والحقوق المجاورة الإماراتي، المؤرخ في 20 سبتمبر 2021 والصادر بمرسوم اتحادي رقم 38 لسنة 2021 والمعمول به بتاريخ 02 يناير 2022.

الركن المادي وهو الفعل المادي الذي يُعد انتهاكاً لحقوق الملكية الفكرية المعلوماتية ويشمل استغلال المصنفات أو البرامج أو تعطيل أنظمة الحماية دون إذن شرعي و وفق المادة 40 يمكن تلخيصه كالآتي:

1. فعل التصنيع أو الاستيراد بدون وجه حق:
 - ح- نسخ مقلدة للمصنفات أو البرامج أو التطبيقات أو قواعد البيانات.
 - خ- أجهزة أو أدوات مصممة للتحايل على الحماية التقنية التي يستخدمها المؤلف أو صاحب الحق المجاور.
2. فعل التعطيل أو التعيب بدون وجه حق:
 - د- أي حماية تقنية أو نظام إدارة حقوق إلكترونية تم تعطيله أو العبث به.
3. فعل تحميل أو تخزين برامج الحاسب الآلي أو تطبيقاته أو قواعد البيانات بدون ترخيص من المؤلف أو صاحب الحق أو خلفه.

أما الركن المعنوي للجريمة فيقوم على القصد الجنائي العام باعتبارها من الجرائم العمدية التي لا يتصور وقوعها بطريق الخطأ أو الإهمال، والمبنية على نية ارتكاب الجاني لهذه الأفعال دون حق أو ترخيص مع علمه بعدم مشروعيتها ومخالفتها للقانون وعلمه بطبيعة المصنف والضرر الذي سوف يلحق بالمؤلف، إلا أن نيته واضحة ومباشرة وتتجه إلى تحقيق غرض غير مشروع وهو والرغبة في استغلال المصنفات أو البرامج أو تعطيل أنظمة الحماية.

أما من حيث العقوبة فقد نصت المادة 39 من قانون حقوق المؤلف والحقوق المجاورة، بمعاقبة كل من ينتهك حقوق المؤلف أو الحقوق المجاورة بدون إذن كتابي من المؤلف أو صاحب الحق أو خلفه، بالعقوبات الآتية:

- الحبس لمدة لا تقل عن شهرين، والغرامة المالية التي تتراوح بين 10,000 و 100,000 درهم، أو بإحدى هاتين العقوبتين، وذلك إذا قام المعتدي بأي من الأفعال التالية:
 - الاعتداء على الحقوق الأدبية أو المالية للمؤلف أو صاحب الحق المجاور، بما في ذلك وضع المصنف أو الأداء أو التسجيل الصوتي أو البرامج الإذاعية أو برامج الحاسوب المحمية في متناول الجمهور عبر أجهزة الحاسب أو شبكات الإنترنت أو شبكات

- المعلومات أو شبكات الاتصالات أو أي وسائل أخرى؛ أو البيع أو التأجير أو الطرح للتداول بالمصنف أو التسجيل أو البرنامج المحمي.
- في حالة العود، أي تكرار الجريمة، تكون العقوبة الحبس لمدة لا تقل عن ستة أشهر، والغرامة المالية بين 100,000 و 500,000 درهم، مع ملاحظة أن العقوبة تتضاعف بتعدد المصنفات أو البرامج أو التسجيلات محل الجريمة¹.

أما المادة (40) من نفس القانون فنصت مع عدم الإخلال بأي عقوبة أشد ينص عليها أي قانون آخر، يُعاقب بالحبس لمدة لا تقل عن ستة أشهر، والغرامة التي تتراوح بين 100,000 و 700,000 درهم، أو بإحدى هاتين العقوبتين، كل من ارتكب أيًا من الأفعال التالية: أولاً، التصنيع أو الاستيراد دون وجه حق بغرض البيع أو التأجير أو التداول لأي مصنف أو نسخ مقلدة، أو أجهزة وأدوات مصممة للتحايل على الحماية أو التقنية التي يستخدمها المؤلف أو صاحب الحق المجاور لتنظيم أو إدارة الحقوق أو المحافظة على جودة النسخ؛ ثانياً، التعطيل أو التعيب دون وجه حق لأي حماية تقنية أو معلومات إلكترونية تهدف لتنظيم وإدارة الحقوق المقررة؛ ثالثاً، تحميل أو تخزين برامج الحاسب الآلي أو تطبيقاته أو قواعد البيانات دون ترخيص من المؤلف أو صاحب الحق أو خلفه².

بالإضافة إلى المادة (41) التي عاقبت كل شخص يستخدم برنامج حاسب آلي أو تطبيقاته أو التطبيقات الذكية أو قواعد البيانات دون الحصول على ترخيص مسبق من المؤلف أو من يخلفه يُعاقب بغرامة مالية تتراوح بين 30,000 و 100,000 درهم عن كل برنامج أو تطبيق أو قاعدة بيانات، كما تنص المادة على تشديد العقوبة في حالة التكرار، حيث تصل الغرامة المالية إلى حد أدنى 100,000 درهم ولا تزيد عن 1,000,000 درهم.

ومن خلال المواد السابقة يظهر لنا حرص المشرع الإماراتي على حماية المصنفات الرقمية من الاستخدام غير المصرح به، سواء كان ذلك في برامج الحاسب أو التطبيقات الذكية أو قواعد البيانات، مؤكدة على الجانب المالي والاقتصادي للحقوق الرقمية وضرورة الحصول

1- المادة 39 من قانون حقوق المؤلف والحقوق المجاورة الاماراتي، المرجع السابق.

2- المادة 40 من قانون حقوق المؤلف والحقوق المجاورة الاماراتي، نفس المرجع السابق.

على تراخيص مسبقة لضمان احترام حقوق المؤلفين، كما تعكس هذه العقوبة الجدية القانونية في الردع ومنع التكرار، بما يعزز حماية الملكية الفكرية في البيئة الرقمية ويضمن التوازن بين حقوق المبدعين والمستهلكين.

رابعاً: التشريع الأردني.

أبدت المملكة الأردنية الهاشمية اهتماماً بحماية الملكية الفكرية منذ سنّها قانون حماية حق المؤلف والحقوق المجاورة رقم (22) لسنة 1992، المعدّل بالقانون رقم (23) لسنة 2014، حيث يهدف القانون إلى حماية المصنفات الأدبية والفنية والعلمية، بما يشمل الإبداعات الرقمية الحديثة، ويعكس التشريع الأردني حرص المشرع على توفير بيئة قانونية متوازنة تحمي حقوق المؤلفين والمبدعين، وتمكّنهم من استغلال أعمالهم بشكل قانوني، بينما يحافظ على مصالح المجتمع في الوصول المشروع للمعلومات والمعرفة.

وعرف المشرع الأردني المصنف في المادة الثانية منه على أنه " كل أبداع أدبي أو فني أو علمي والمحمي وفقاً لأحكام المادة 3 من هذا القانون"¹، حيث ينص القانون صراحة في المادة الثالثة منه فقرة ب رقم 8 على حماية المصنفات التي يكون مظهر التعبير عنها بالكتابة أو الصوت أو السم أو التصوير أو الحركة، وتشمل بوجه خاص ثمانية أنواع كان من بينها المصنفات الرقمية مثل برامج الحاسوب سواء أكانت بلغة المصدر أو بلغة الآلة، مؤكداً على أن حماية المصنفات الرقمية تعكس إدراكاً متقدماً لتحديات البيئة الرقمية والجرائم المعلوماتية².

ويقوم الركن المادي لجريمة التعدي على الملكية الفكرية المعلوماتية في التشريع الأردني على ارتكاب أفعال محددة تعد انتهاكاً لحقوق المؤلف، بما في ذلك البرامج الرقمية، ويشمل ذلك:

ذ- النسخ أو التحريف أو التعديل غير المشروع للمصنفات الرقمية أو التقليديّة دون إذن صاحب الحق.

1- المادة الثانية من قانون حماية حق المؤلف والحقوق المجاورة الاردني، رقم 22 لسنة 1992، المعدل بقانون حماية حق المؤلف رقم 23 لسنة 2014، والمنشور بالجريدة الرسمية عدد 5289 بتاريخ 2014/01/06.

2- أنظر المادة الثالثة من قانون حماية حق المؤلف الأردني لسنة 2014، المرجع السابق.

- ر- بيع أو تأجير أو توزيع نسخ مقلدة من المصنفات المحمية.
- ز- التحايل على وسائل الحماية التقنية المصاحبة للمصنفات الرقمية، مثل التشفير أو حماية النسخ الأصلية ، وتحميل أو تخزين البرامج أو قواعد البيانات دون موافقة صاحب الحق أو الترخيص النظامي.

يُعتبر تحقق أي من هذه الأفعال كافيًا لتكوين الركن المادي للجريمة، سواء أكانت الأفعال مباشرة أو عبر وسيط تقني.

أما الركن المعنوي فيشترط القانون الأردني لقيام المسؤولية الجنائية القصد الجنائي العام، باعتبار جريمة التعدي على حقوق الملكية الفكرية من الجرائم العمدية، فمعرفة الجاني بأن المصنف محل الفعل محمي قانونيًا، وأن أفعاله تتضمن انتهاكًا لحقوق صاحب الحق، واتجاه أرادته نحو ارتكاب الفعل المجرم بقصد استغلال المصنف أو التأثير على حقوق المؤلف دون ترخيص، أساسيين لتأسيس الركن المعنوي لجريمة التعدي على حقوق الملكية الفكرية المعلوماتية.

وأما من حيث العقوبات فقد حدد القانون الأردني عقوبات للجرائم المتعلقة بالتعدي على حقوق المؤلف، تشمل:

- أ- العقوبات الجنائية الأساسية: تشمل الحبس والغرامات المالية وفقًا لنوع الفعل وخطورته.
- ب- العقوبات التكميلية: مثل مصادرة النسخ المخالفة أو الأدوات المستخدمة في الجريمة، وإلزام الجاني بالتعويض المدني لصاحب الحق.
- ت- كما تشدد المشرع في حالة العود.

وخلاصة القول أن التشريع الأساسي لحماية الملكية الفكرية في الأردن يبقى قانون حقوق المؤلف رقم (23) لسنة 2014 الذي يحتوي على نصوص صريحة حول حماية المصنفات، بما في ذلك برامج الحاسوب، وتجريم الاعتداء عليها أما قانون 17 لسنة 2023 للجرائم الإلكترونية فلم يعالج جريمة التعدي على الملكية الفكرية المعلوماتية بصورة مستقلة، وإنما يركز على الجرائم الرقمية التقنية العامة، ويمكن أن يتقاطع مع حقوق الملكية الفكرية فقط عند استعمال الوسائط التقنية في ارتكاب مخالفات منصوص عليها في قوانين أخرى .

المطلب الثالث: معالجة جريمة التعدي على الملكية الفكرية المعلوماتية في التشريع الدولي.

ونهدف من خلال هذا المطلب معالجة جريمة التعدي على الملكية الفكرية المعلوماتية من خلال نصوص المواد التي تناولتها والواردة في اتفاقية بودابست لسنة 2001 والاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

أولاً: معالجة التعدي على الملكية الفكرية في اتفاقية بودابست.

جرّمت الاتفاقية التعدي على حقوق الملكية الفكرية المتصلة بالمصنفات المعلوماتية، مع سرد أفعال الاعتداء كانتهاكات للملكية الفكرية وحقوق المؤلف والحقوق المجاورة، وعبرت الاتفاقية عنها بتعبير انتهاكات الملكية الفكرية والحقوق المجاورة، وتضمنتها المادة العاشرة منها¹.

1- المادة العاشرة من اتفاقية بودابست 2001 (الجرائم المتعلقة بانتهاكات حقوق النشر والتأليف والحقوق ذات الصلة 1. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني: انتهاك حقوق النشر والتأليف، وفقاً لتعريفها بموجب القانون الخاص بتلك الدولة الطرف، وتبعاً لالتزاماتها بموجب وثيقة باريس المؤرخة في 24 يوليو/تموز 1971 والمنقحة لاتفاقية برن لحماية المصنفات الأدبية والفنية، والاتفاق الخاص بجوانب حقوق الملكية الفكرية المتصلة بالتجارة، ومعاهدة حقوق المؤلف للمنظمة العالمية للملكية الفكرية باستثناء أي حقوق معنوية مخولة بموجب هذه الاتفاقيات، عندما تُرتكب هذه الأفعال عمداً على نطاق تجاري وبواسطة نظام الكمبيوتر. 2. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني: انتهاك الحقوق ذات الصلة، وفقاً لتعريفها بموجب القانون الخاص بتلك الدولة الطرف، وتبعاً لالتزاماتها بموجب الاتفاقية الدولية لحماية الفنانين الأدبيين ومنتجي الاسطوانات وهيئات البث الإذاعي (اتفاقية روما)، والاتفاق الخاص بجوانب حقوق الملكية الفكرية المتصلة بالتجارة، ومعاهدة الويبو بشأن الأداء والتسجيلات الصوتية، باستثناء أي حقوق معنوية مخولة بموجب هذه الاتفاقيات، عندما تُرتكب هذه الأفعال عمداً على نطاق تجاري وبواسطة نظام الكمبيوتر. 3. يجوز للدولة

وأشارت المذكرة التفسيرية لاتفاقية أن الانتهاكات لحقوق الملكية الفكرية، وبشكل خاص تلك المتعلقة بحقوق التأليف والنشر، أحد أبرز الانتهاكات الجنائية الشائعة عبر شبكة الإنترنت، مما يولد مخاوف جدية لدى أصحاب هذه الحقوق ولدى المتخصصين في تشغيل أنظمة الحواسيب، ويُعد استنساخ الإبداعات المحمية وتوزيعها عبر الإنترنت دون إذن صاحب الحق أمراً متكرراً ومنتشر الوقوع، وتشمل هذه الإبداعات المحمية الأعمال الأدبية والتصويرية والموسيقية والسمعية البصرية، إلى جانب غيرها من الإنتاجات الفكرية، ومن المرجح أن سهولة إجراء النسخ غير المصرح به بفضل التقنيات الرقمية الحديثة، إلى جانب المدى الواسع لعمليات الاستنساخ والنشر ضمن إطار الشبكات الإلكترونية، هما العاملان الرئيسيان اللذان دفعا إلى دمج أحكام عقابية ضمن التشريعات الجنائية¹، مع تعزيز آليات التعاون الدولي في هذا النطاق في عديد من الاتفاقيات الدولية².

وتشمل المصنفات الخاضعة للحماية، وفقاً لأحكام المادة العاشرة المذكورة أعلاه، تلك الإبداعات التي تتوفر فيها الشروط التالية:

- أن تكون إبداعات فكرية أصيلة، مما يستبعد من نطاق الحماية أي انتهاكات تتعلق ببراءات الاختراع أو العلامات التجارية.
- أن تندرج ضمن فئة الإبداعات الفكرية المحددة في الاتفاقيات الدولية المشار إليها في الفقرة الأولى من المادة، وتشمل اتفاقية باريس 1971 واتفاقية برن لحماية الأعمال الأدبية والفنية المؤرخة في 9 سبتمبر 1886، واتفاقية الجوانب التجارية لحقوق الملكية الفكرية (TRIPS)

الطرف الاحتفاظ بالحق في عدم فرض المسؤولية الجنائية بموجب الفقرتين 1 و2 من هذه المادة في ظروف محدودة شريطة توافر سبل فعالة أخرى للانتصاف، وأن يتقيد هذا التحفظ بالتزامات الدولية للدولة الطرف المنصوص عليها في الصكوك الدولية المشار إليها في الفقرتين 1 و2 من هذه المادة.

1- للمزيد أنظر التقرير التفسيري لاتفاقية بودابست، المرجع السابق، ص 17.

2- بالإضافة إلى ما سبق ذكره نُص على جريمة التعدي على الملكية الفكرية وحقوق المؤلف في العديد من الاتفاقيات والبروتوكولات الدولية منها اتفاقية (كومنولث اتحاد الدول المستقلة في المادة 1 و3، القانون النموذجي العربي بشأن مكافحة الجريمة السيبرانية في المادة 14، المعاهدة الدولية للتعاون بشأن براءات الاختراع الويبو 1970، معاهدة قانون العلامات التجارية وايو 1994 ، اتفاقية التدابير المتعلقة بأثر التجارة على حقوق الملكية الفكرية تريبس 1994).

المؤرخة في 15 أبريل 1994، واتفاقية روما الدولية لحماية المؤدين والمنتجين للتسجيلات الصوتية ومنظمات البث المؤرخة في 26 أكتوبر 1961، إلى جانب معاهدة المنظمة العالمية للملكية الفكرية المتعلقة بحقوق الأداء والتسجيلات الصوتية المؤرخة في 20 ديسمبر 1996.

- بالإضافة إلى ذلك، يجب أن تكون هذه الإبداعات إلكترونية الطابع، أي تلك التي يتم تخزين محتواها على وسائط رقمية، ويجري نشرها وتداولها عبر الإنترنت أو غيرها من الأنظمة المعلوماتية، ويستفاد هذا الشرط من السياق العام للاتفاقية، التي تركز على الجرائم المعلوماتية، ومن الشروط المتعلقة بارتكاب الفعل عمداً وعلى نطاق تجاري وباستخدام نظام معلوماتي¹.

أما فيما يتعلق بالركن المادي المكون لجريمة التعدي على الملكية الفكرية المعلوماتية فلم تفرض أحكام المادة العاشرة المذكورة أعلاه عقوبات جنائية مباشرة على سلوكيات محددة، واكتفت بدعوة الدول الأعضاء إلى تعزيز آليات الحماية لحقوق المؤلف والحقوق المتفرعة عنه، في إطار الشبكات والمنظومات المعلوماتية، ويُعزى هذا النهج إلى اعتبارات منطقية، تتمثل في صعوبة تحديد الانتهاكات المحتملة لحقوق الملكية الفكرية عبر الوسائط الرقمية بشكل حصري، حيث تتشابه في ذلك مع غيرها من التحديات الناشئة عن تكنولوجيا الإنترنت والمفاهيم المتعلقة بها، كما يرجع ذلك إلى التنوع الملحوظ في التشريعات الوطنية المتعلقة بحماية الملكية الفكرية التقليدية، والتي تختلف في تصنيف الأفعال المكونة للعنصر المادي في جرائم الاعتداء على هذه الحقوق، وبالتالي، تجنب المشرع الدولي تحديد التصرفات الإجرامية المحددة في سياق تقنيات الاتصال الحديثة.

فيما يتعلق بالركن المعنوي للجرائم التعدي على الملكية الفكرية المعلوماتية، يشترط لقيام المسؤولية الجنائية أن تُرتكب هذه الجرائم عمداً أي توافر القصد الجنائي العام، وخلاف ما جرى عليه العمل في باقي النصوص السابقة ذات الطبيعة الموضوعية في هذه الاتفاقية، فقد استُخدم في هذا السياق مصطلح عمداً بدلاً من مصطلح قصداً وذلك في الفقرتين الأولى

1- مفيدة مباركية، المرجع السابق، ص 267.

والثانية من النص، انسجماً مع المصطلحات الواردة في اتفاقية تريبس التي اعتمدت مصطلح قصداً في المادة المتعلقة بالالتزام بتجريم انتهاكات حقوق المؤلف، وذلك لعدم تعارض المصطلحات القانونية المستخدمة أو خروج الاتفاقية عن المفاهيم المعتمدة في الصكوك الدولية المرجعية في مجال حماية حقوق الملكية الفكرية¹.

ثانياً: معالجة التعدي على الملكية الفكرية في الاتفاقية العربية.

بالنظر إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، نجد أنها نصت في المادة 17 على الجرائم التي تطل حقوق الملكية الفكرية وجاءت المادة تحت عنوان "الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة"، ونصت على "انتهاك حق المؤلف كما هو معروف حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي، وانتهاك الحقوق المجاورة لحق المؤلف ذات الصلة كما هي معرفة حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي"².

وتعقيباً على النص أعلاه نجد أن المادة 17 من الاتفاقية جاءت منقوصة من حيث جوهرها المتعلق بمعالجة جرائم التعدي على الملكية الفكرية المعلوماتية، حيث أنها اشتملت على حكماً عاماً يحيل إلى التشريعات الداخلية للدول الأعضاء تجريم المساس بحقوق المؤلف والحقوق المجاورة، شريطة ارتكاب الفعل المجرم عمداً ولأغراض غير الاستخدام الشخصي، وبالتالي، لم تقدم هذه المادة أي تطوير تشريعي مبتكر في شأن المعلوماتية، بل إنها لم تشير حتى إلى الاتفاقيات الدولية الأخرى التي قد تكون الدول طرفاً فيها، كما هو الحال في المادة 10 من اتفاقية بودابست، علاوة على ذلك، لم تتناول قضية تصنيف البرمجيات المعلوماتية أو برامج الحواسيب الآلية ضمن الإبداعات الخاضعة لحماية الملكية الفكرية.

1- مفيدة مباركية، المرجع السابق، ص 269.

2- المادة 17 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010، المرجع السابق.

خاتمة

لقد تناولت هذه الأطروحة موضوع حماية النظم المعلوماتية وفق الاتفاقيات الدولية والتشريعات الوطنية بوصفه أحد أهم التحديات القانونية في العصر الرقمي، خاصة مع التطور المتسارع للتقنيات وازدياد تعقيد الجرائم المعلوماتية واتساع نطاقها العابر للحدود، وقد تمحورت إشكالية الدراسة حول التساؤل: إلى أي حد تُسهم الاتفاقيات الدولية والتشريعات الوطنية في حماية النظم المعلوماتية، وما مدى كفايتها وفعاليتها في مواجهة التحديات المتجددة للأمن المعلوماتي؟ ومن خلال التحليل المعمق للنصوص الدولية والتشريعات الوطنية، ودراسة الإشكالات التطبيقية، أمكن الوصول إلى عدد من النتائج المهمة.

1- إن ما يميّز جرائم نظم المعلومات هو الطبيعة الخاصة لمحل الجريمة، إذ يتعلق الأمر غالباً بـ مال معنوي يقوم أساساً على النظام المعلوماتي ومكوناته غير المادية، وهي عناصر لم تستطع النصوص القانونية التقليدية مواكبتها أو توفير الحماية الكافية لها، وقد أدى هذا القصور إلى تدخل المشرعين لإفرادها بنصوص خاصة، سواء ضمن قانون العقوبات أو في قوانين مستقلة، بهدف حماية هذه الكيانات الرقمية وصون سلامتها من مختلف أشكال الاعتداء.

2- أن جرائم النظم المعلوماتية هي تلك الجريمة التي يكتمل ركنها المادي فقط من خلال القيام بعملية معالجة آلية للبيانات، سواء كانت هذه المعالجة بسيطة أو معقدة، وبناءً على ذلك، فإن الأفعال المادية التي تتم دون أي معالجة آلية للبيانات لا تُصنف كجريمة معلوماتية، حتى لو أسفرت عن نتائج مشابهة لتلك المترتبة على الأفعال المنفذة عبر المعالجة الآلية.

3- إن جرائم النظم المعلوماتية لا تستلزم بالضرورة مهارات تقنية عالية أو وسائل معقدة كما قد يُعتقد، إذ يمكن ارتكابها من خلال عمليات بسيطة ومشروعة الاستخدام في الأصل، فمجرد تنفيذ أوامر اعتيادية يُتيحها نظام التشغيل للمستخدم، مثل حذف البيانات أو نسخها أو إرسالها أو التعديل عليها، قد يُفضي إلى أضرار بالغة الخطورة، كتعطيل النظام بشكل جسيم، أو إتلاف جزء من البيانات، أو تسريبها وسرقتها، وغيرها من الممارسات التي من شأنها الإضرار الجسيم بالنظم المعلوماتية.

4- أن جريمة الإرهاب الإلكتروني أصبحت من أخطر التهديدات المعاصرة للأمن الوطني والدولي، الأمر الذي يفرض على التشريعات الجنائية تطوير نصوصها باستمرار، وتوحيد

المفاهيم القانونية، وتعزيز التعاون الدولي، إلى جانب إقرار سياسات وقائية وتقنية فعالة، لمواجهة هذا النمط المستحدث من الجرائم التي تتجاوز الحدود التقليدية للدول.

5- أن الجرائم المعلوماتية تنقسم إلى نوعين: النوع الأول يشمل الجرائم التي تمسّ سرية البيانات والمعلومات، وسلامتها، وإتاحتها، وهي جرائم مستحدثة بصورة جذرية، ترتبط بشكل مباشر بالمعلومات الرقمية وبالأنظمة المعلوماتية ذاتها، وتستهدف جوهر البيئة الرقمية ومقوماتها الأساسية، أما الصنف الثاني، فيتضمن الجرائم التي لها نظائر أو ما يقابلها في التشريعات التقليدية، غير أنها لا تُعدّ جرائم تقليدية بالمعنى الدقيق، لأن ركنها المادي يتحقق عبر نظم المعالجة الآلية للبيانات، بحيث تشكّل الأنظمة المعلوماتية البيئة التي يقع فيها الفعل الإجرامي أو الوسيلة التي تساهم في تنفيذه.

6- تمتاز الجرائم الماسة بسرية البيانات وسلامتها وإتاحتها، بدرجة كبيرة من التداخل والارتباط فيما بينها، سواء من حيث المصلحة القانونية محلّ الحماية، أو من حيث التقنيات والأساليب المستخدمة في ارتكابها، مما يجعل من الصعب، من الناحية القانونية، الفصل بين هذه الجرائم بصورة مطلقة، كما أنه غالباً ما يكون من غير الممكن، من الناحية التقنية، ارتكاب إحداها بمعزل عن الأخرى؛ فالدخول غير المشروع قد يسبقه أو يعقبه فعل الإلتاف، أو الاعتراض، أو النسخ، وغيرها من الأفعال المرتبطة، وقد أدى هذا التداخل إلى اختلاف واضح في التشريعات الداخلية بشأن كيفية تصنيف هذه الجرائم ومعالجتها وتجريمها.

7- أن الظاهرة الإجرامية المعلوماتية تشهد تنامياً ملحوظاً واتساعاً كبيراً في حجم أنشطتها، حيث انتقلت من مجرد أفعال تهدف إلى قرصنة المعلومات إلى نشاط إجرامي منظم يتسم بالاحترافية، ويغلب عليه الطابع الربحي باعتباره الدافع الرئيس لمجرمي المعلوماتية ومحركاً لسلوكهم، إلى جانب أهداف أخرى فرضها الواقع المعاصر، مثل الإرهاب الإلكتروني والجريمة المنظمة، وفي هذا السياق، أصبحت الجماعات الإجرامية والإرهابية تستغل النظم المعلوماتية والشبكات لتمويل نشاطها، ونشر أفكارها، وتنفيذ عملياتها، مستثمرةً البيئة الرقمية في بثّ الخوف وزرع الرعب بين الشعوب والأنظمة.

8- أن المشرّع الجزائري لتعريف الجرائم المرتبطة بنظم المعلومات، وأطلق عليها تسمية "الجرائم المتصلة بالإعلام والاتصال"، وذلك وفق ما نصّت عليه المادة 2 من القانون

04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وقد اعتبر المشرع هذه الجرائم بأنها تشمل، من جهة، الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات كما هي محددة في قانون العقوبات، ومن جهة أخرى كل جريمة تُرتكب أو يُسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية، وبهذا التعريف، يكون المشرع قد تبنى مفهوماً واسعاً يشمل كل الاعتداءات المباشرة على الأنظمة المعلوماتية، إضافة إلى الجرائم التقليدية التي تُستغل فيها الوسائط الإلكترونية كوسيلة لاقتوافها.

9- تبين أن الاتفاقيات الدولية—وفي مقدمتها اتفاقية بودابست للجريمة الإلكترونية—قد شكّلت خطوة محورية نحو بناء إطار قانوني دولي يكفل توحيد المفاهيم وتجريم الأفعال المعلوماتية وتسهيل التعاون القضائي بين الدول، إلا أن تأثيرها العملي ظل محدوداً بسبب عدم انضمام عدد كبير من الدول إليها، وبسبب التفاوت في تطبيق أحكامها، إضافة إلى غياب آليات رقابية قوية تُلزم الدول بتنفيذ التزاماتها، كما أن هذه الاتفاقيات لم تعد قادرة بالكامل على تغطية الجرائم المستحدثة المتصلة بالذكاء الاصطناعي، والعملات الافتراضية، والهجمات على البنى التحتية الحيوية، ما يجعل الحاجة إلى تطويرها ضرورة ملحة.

10- كشفت الدراسة أن التشريعات الوطنية تمثل ركيزة مهمة لحماية النظم المعلوماتية، حيث اتجهت معظم الدول إلى سن قوانين خاصة بالجريمة المعلوماتية، إلا أن هذه التشريعات تعاني في كثير من الأحيان من قصور في التجريم، وغموض في المفاهيم القانونية، وضعف في التمييز بين الأفعال التقليدية والمعلوماتية، فضلاً عن غياب الإجراءات الواضحة المتعلقة بضبط الأدلة الرقمية، وعدم مواكبة النصوص للتطور التقني المتسارع، كما أن التباين الواضح في التشريعات بين الدول يخلق مجالاً واسعاً للهروب القانوني ويحدّ من فعالية التعاون الدولي.

11- بينت الدراسة أن المشرع الجزائري ركز على تجريم الدخول غير المشروع إلى الأنظمة المعلوماتية كجريمة قائمة بذاتها، مع تشديد العقوبات عند حدوث أضرار فعلية، واعتمد القصد الجنائي العام كأساس للمسؤولية.

12- أظهرت الدراسة أن التحديات التطبيقية تشكل عائقًا كبيرًا أمام حماية النظم المعلوماتية؛ فصعوبة تتبع الجناة، وتعقيد الأدلة الرقمية، ونقص القدرات التقنية لدى جهات إنفاذ القانون، وضعف التنسيق بين المؤسسات الوطنية، كلها عوامل تُقلص من فعالية الجهود القانونية رغم وجود التشريعات، كما أنّ آليات التعاون الدولي لا تزال أبطأ بكثير مما تطلبه السرعة الكبيرة التي تُرتكب بها الجرائم المعلوماتية.

13- أنه فيما يخص جريمة إباحية الأطفال المعلوماتية أكد التشريع الدولي والوطني على حماية الأطفال من الاستغلال الجنسي عبر الشبكات الرقمية، مع تجريم الإنتاج والنشر والتوزيع والحيازة، والاعتماد على القصد الجنائي العام لقيام المسؤولية.

14- خلصت الدراسة إلى أن القواعد القانونية لا تكفي وحدها لتوفير الحماية القانونية للأطفال ضد مخاطر الاستغلال الجنسي عبر شبكة الانترنت فلا بد من اللجوء إلى الوسائل الفنية التي تمكن من منع وصول المضمون الإباحي إلى الطفل باستخدام برامج تمنع وصول الطفل له.

وبناءً على هذه النتائج، تُظهر الإشكالية أنّ الاتفاقيات الدولية والتشريعات الوطنية تُسهم فعلاً في حماية النظم المعلوماتية وتضع أساساً قانونياً ضرورياً لمواجهة الجرائم المعلوماتية، إلا أنّ فعاليتها ليست مكتملة، وكفايتها لا تزال بحاجة إلى تعزيز جوهري، سواء من خلال التعديل التشريعي أو بناء القدرات أو تطوير آليات التعاون الدولي.

التوصيات:

انطلاقاً من التحليل السابق، تقترح هذه الأطروحة مجموعة من التوصيات الهادفة إلى تعزيز الإطار القانوني لحماية النظم المعلوماتية:

1. تطوير الاتفاقيات الدولية القائمة وإعداد اتفاقية شاملة تراعي المستجدات التقنية، وتواكب الجرائم الناشئة المرتبطة بالذكاء الاصطناعي والعملات الرقمية والهجمات على البنى التحتية الحيوية.

2. تشجيع الدول على الانضمام إلى الاتفاقيات الدولية، خصوصاً اتفاقية بودابست، لتعزيز الانسجام التشريعي وتسهيل التعاون القضائي.

3. تحديث التشريعات الوطنية بما يضمن دقة التجريم ووضوح تعريفات الأفعال المعلوماتية، ووضع قواعد صريحة للأدلة الرقمية.
4. تعزيز القدرات المؤسسية عبر إنشاء وحدات متخصصة في التحقيق والادعاء والفصل في الجرائم المعلوماتية، وتزويدها بالخبرة التقنية والقانونية اللازمة.
5. تقوية آليات التعاون الدولي من خلال تبسيط إجراءات تبادل المعلومات، وتسريع آليات المساعدة القضائية، واعتماد منصات مشتركة للتنسيق السيبراني.
6. تعزيز التشريعات الوطنية لمكافحة الإرهاب الإلكتروني وتوحيد مفاهيمه القانونية، مع تطوير آليات الرقابة التقنية وإنشاء وحدات متخصصة للتحقيق في الجرائم الإلكترونية، وفرض عقوبات رادعة تتناسب مع خطورة الجريمة، ودعم البحث العلمي والتقني لتقديم حلول مبتكرة لحماية النظم المعلوماتية والبنى التحتية الحيوية من الاستغلال الإرهابي.
7. إطلاق برامج وطنية للتوعية القانونية تتعلق بالاستخدام الآمن للتكنولوجيا، بهدف الحد من فرص ارتكاب الجرائم المعلوماتية.
8. تشجيع البحث العلمي في مجال القانون المعلوماتي وتطوير أدوات تحليلية تساعد في استشراف المخاطر الرقمية المستقبلية.

وختاماً تخلص هذه الأطروحة إلى أن حماية النظم المعلوماتية لم تعد مجرد خيار قانوني بل أصبحت ضرورة استراتيجية عالمية، تتطلب تكاملاً بين الجهد الدولي والوطني، ومواكبة مستمرة للتطور التقني، وإرادة سياسية وتشريعية قادرة على بناء نظام قانوني مرن وفعال، ومع استمرار تطور الجريمة المعلوماتية واتساع نطاقها، تظل الحاجة قائمة إلى المزيد من الدراسات المتخصصة التي تسعى إلى تطوير المنظومة القانونية وضمان أمن الفضاء الرقمي في مواجهة تهديداته المتجددة.

الملاحق

الأفعال التي تشكل جرائم تدخل في نطاق الجرائم المعلوماتية، والصادر عن مكتب ملحق شرح الأمم المتحدة المعني بالمخدرات والجريمة، بعنوان دراسة شاملة عن الجريمة السيبرانية فبراير 2013.

تشير إلى الأفعال التي تنطوي على الدخول إلى أحد أجزاء النظام الحاسوبي أو الدخول إلى النظام بأكمله، وذلك بدون تصريح أو مبرر لهذا الدخول، وفي هذا الحالة - على سبيل المثال - يقوم أحد الجناة بالتحايل على برنامج الحماية الخاص بالنظام الحاسوبي لأحد المصارف (على سبيل المثال) من الممكن أيضا أن تتمثل هذه الحالة، عند مواصلة أحد المستخدمين البقاء متصلا مع أحد الأنظمة الحاسوبية بعد انتهاء فترة الأذن الممنوح له/لها، مثل؛ قيام أحد الجناة بحجز سعة الخادم لفترة زمنية محددة، ولكن يستمر في الاستعمال بعد انتهاء الفترة الزمنية المسموح بها. هذا، وتتطلب بعض النهج الوطنية أن يكون تحايل الجاني منصبا على تدابير الحماية أو تقتزن الأفعال بنية معينة.	النفاذ غير المشروع إلى نظام حاسوبي.
تشير إلى الأفعال التي تنطوي على الوصول إلى البيانات الحاسوبية بدون تصريح أو مبرر لذلك؛ ويتضمن ذلك الحصول على بيانات أثناء إحدى عمليات الإرسال التي لا يقصد بها أن تكون علانية، فضلا عن الاطلاع على البيانات الحاسوبية (مثل نسخ البيانات) بدون تصريح . وتتمثل هذه الحالة، على سبيل المثال، إذا قام أحد الجناة بالوصول بشكل غير قانوني إلى إحدى قواعد البيانات الحاسوبية، تسجيل عمليات الإرسال بدون حق داخل إحدى شبكات الاتصال اللاسلكي، أو يقوم أحد الجناة، والذي يعمل لدى إحدى الشركات المعنية، بنسخ الملفات و أخذها بدون تصريح، وتتطلب بعض النهج الوطنية أن تكون البيانات ذات الصلة محمية ضد الدخول غير المصرح به. أيضا، تتضمن بعض النهج الوطنية اعتراض الانبعاثات الكهرومغناطيسية التي لا يجوز تصنيفها كبيانات حاسوبية، وغالبا ما قد	النفاذ غير المشروع إلى بيانات حاسوبية أو اعتراض هذه البيانات أو الاطلاع عليها.

تتطوي أغراض التجسس الصناعي أو التجاري على فعل النفاذ غير المشروع أو اعتراض البيانات الحاسوبية أو حيازة البيانات الحاسوبية.	
تشير إلى الأفعال التي تعيق أداء أحد الأنظمة الحاسوبية، فضلا عن الأفعال التي تتطوي على ضرر يلحق بالبيانات الحاسوبية أو حذفها أو تالفها أو تغييرها أو طمسها، وذلك بدون تصريح أو مبرر، وتتمثل هذه الحالة، على سبيل المثال، إذا قام أحد الجناة بإحالة عدد كبير من الطلبات إلى أحد أنظمة الحاسوب والذي من شأنه أن يتسبب في عدم قدرة النظام الحاسوبي على الاستجابة للطلبات المشروعة (وهذا ما يعرف بهجمات الحرمان من الخدمة)، أو حذف ملفات برامج الحاسوب اللازمة لعملية تشغيل أحد خوادم الإنترنت، أو تغيير أحد السجلات في قاعدة بيانات أحد الحواسيب، وتغطي بعض النهج الوطنية فقط الأفعال ذات الصلة بالبيانات، بيد أن النهج الأخرى تتناول أيضا التلاعب في أجهزة الحاسوب، وقد تسبب "القرصنة" في أنظمة الحاسوب المرتبطة بالبنية التحتية للمنشآت الحيوية مثل شبكات المياه أو إمدادات الكهرباء في التدخل غير المشروع في البيانات أو إتلاف النظام.	التدخل غير المشروع في البيانات أو النظم.
تشير إلى الأفعال التي تتطوي على تطوير أو توزيع أجهزة أو برمجيات والتي يمكن استخدامها في ارتكاب الجرائم ذات الصلة بالحاسوب أو الإنترنت، وتتجسد هذه الحالة، على سبيل المثال، عندما يقوم أحد الجناة بتطوير أحد أدوات البرمجيات لتشغيل هجمات الحرمان من الخدمة بشكل آلي ومن أجل تجنب التدخل في الاستخدام المشروع لهذه الأدوات (مثل من قبل خبراء الأمن)، وتتطلب بعض النهج الوطنية أن تكون الأداة صممت خصيصا لأغراض غير قانونية، أو تقترن أفعال أحد الجناة بهدف استعمال الأداة لارتكاب أحد الجرائم.	إنتاج أو توزيع أو حيازة أدوات لإساءة استعمال الحواسيب.
تشير إلى الأعمال التي تتطوي على استخدام أحد النظم الحاسوبية	

لمعالجة المعلومات الشخصية أو نشرها أو الوصول إليها مما يشكل انتهاكا لأحكام حماية البيانات، وتتمثل هذه الحالة، على سبيل المثال، إذا كان أحد الجناة يعمل في أعمال التجارة الإلكترونية وقام بالكشف عن المعلومات الشخصية من قاعدة بيانات عملية التي يتعين عليه الإبقاء على سريتها.	انتهاك تدابير حماية الخصوصية أو البيانات.
تشير إلى الأفعال التي تنطوي على التدخل أو النفاذ غير المشروع لأحد الأنظمة أو البيانات الحاسوبية بهدف الحصول على المال بشكل فيه خداع أو تدليس، أو بهدف تحقيق منافع مالية أخرى، أو للتهرب من دفع إحدى الديون، فضلا عن الأفعال التي تنطوي على التدخل في نظام حاسوبي أو بيانات حاسوبية بشكل ينجم عنه توليد بيانات حاسوبية زائفة . وتتمثل هذه الحالة، على سبيل المثال، إذا قام أحد الجناة بتعديل البرمجيات المستخدمة من قبل أحد المصارف لإعادة توجيه تحويل مبلغ مالي إلى حسابه الشخصي، أو إذا قام أحد الجناة بتعديل إحدى رسائل البريد الإلكتروني الصحيحة الواردة من إحدى المؤسسات المالية بهدف الاحتيال بشكل أساسي. ويشير أيضا إرسال العديد من هذه الرسائل في مسعى من الجاني للحصول على معلومات شخصية أو للاحتيال إلى "التصيد الاحتيالي". أما فيما يتعلق باستخدام الحاسوب في التزوير، فإن بعض الاتجاهات الوطنية تتطلب أن تكون البيانات الحاسوبية الأصلية تتعلق بوثائق بهدف إنشاء ارتباطات قانونية ملزمة. بيد أن الاتجاهات الأخرى تتطلب أن يكون هدف أحد الجناة اعتبار النسخة المعدلة بمثابة التزامات قانونية أو أن تكون لها حجية التزامات قانونية.	استعمال الحاسوب في أعمال الاحتيال أو التزوير.
تشير إلى الأعمال التي تنطوي على إرسال أو حيازة أو استعمال تعريف شخص آخر مخزن في البيانات الحاسوبية، بدون حق، وذلك بهدف	

ارتكاب أي نشاط إجرامي غير مشروع أو المساعدة في ارتكابه أو التحريض على ارتكابه، وتتمثل هذه الحالة، على سبيل المثال، إذا قام أحد الجناة، بدون حق، بالحصول على معلومات رخصة قيادة من أحد الأنظمة الحاسوبية وقام إما ببيع هذه البيانات أو استخدامها لإخفاء هويته الحقيقية عند ارتكابه إحدى الجرائم، وتتطلب بعض الاتجاهات الوطنية أن يقتصر تطبيق هذه الأحكام على أدوات التعريف المحددة.	جرائم الهوية المرتكبة بواسطة الحواسيب.
تشير إلى الأفعال التي تنطوي على نسخ المواد المخزنة في البيانات الحاسوبية أو بيانات حاسوبية مولدة مما يشكل انتهاكا للحماية المفروضة لحقوق التأليف والنشر أو العلامات التجارية، وتتجسد هذه الحالة، على سبيل المثال، إذا قام أحد الجناة بتوزيع أحد الأغاني المحمية بموجب حق التأليف، وذلك من خلال نظام تبادل الملفات دون ترخيص من المؤلف صاحب المصنف.	جرائم حقوق المؤلف والعلامات التجارية المرتكبة بواسطة الحواسيب.
تشير إلى الأفعال التي تنطوي على استعمال أحد النظم الحاسوبية في إرسال رسائل إلى عدد كبير من المتلقين بدون تصريح أو طلب، ومن أجل تجنب التدخل في الأعمال الاعتيادية لمراسلات العمل، تتطلب بعض النهج الوطنية أن يكون أحد الجناة قام بعنونة هذه الرسالة بمعلومات كاذبة.	إرسال أو التحكم بإرسال الرسائل الطفيلية.

تشير إلى الأفعال التي تنطوي على استخدام أحد نظم الحاسوب في إزعاج أحد الأفراد، أو التحرش به، أو تهديده، أو تعقبه أو التسبب في خوفه أو ترويعه، وتتمثل هذه الحالة، على سبيل المثال، إذا قام أحد الجناة بإرسال رسائل مهينة أو تهديدية أو قبيحة، أو صور (أيضا يشار إلى "التصيد")، أو استعمال أحد نظم الحاسوب في تتبع أو تعقب، أو خلافا لذلك التدخل المادي أو المعنوي في مصلحة أي فرد، وتستبعد أيضا من هذه الفئة الأفعال التي تشكل قذفا فقط.	الأعمال المرتكبة بواسطة الحواسيب والتي تتسبب في ضرر شخصي.
تشير إلى الأفعال التي تنطوي على استعمال أحد نظم الحاسوب في توزيع مواد عنصرية أو تعرض على كراهية الأجانب أو إتاحة هذه المواد، أو استعمال أحد نظم الحاسوب في تهديد أو إهانة أحد الأفراد أو مجموعة من الأشخاص لأسباب عنصرية أو تحمل كراهية للأجانب. وتعني المواد العنصرية أو مواد كراهية الأجانب أي مواد مكتوبة أو صور أو أفكار أو نظريات تدعو أو تشجع أو تحض على التمييز أو الكراهية أو العنف ضد أي فرد أو مجموعة أشخاص على أساس العرق أو اللون أو النسب أو الأصل القومي أو العرقي، وكذلك الدين إذا ما استخدم كذريعة لتأجيج أي من هذه العوامل.	الأفعال المرتكبة بواسطة الحاسوب وتنطوي على عنصرية أو كراهية الأجانب.
تشير إلى الأفعال التي تنطوي على استخدام أحد نظم الحاسوب في إنتاج أو إنشاء أو توزيع أو الوصول أو رؤية أو تلقي أو تخزين أو حيازة أي مواد تمثيلية، بأي وسيلة كانت، لشخص حقيقي أو من وحي الخيال يقل عمره عن 08 سنة، أو يبدو أنه أقل من 08 سنة، مارس نشاطا جنسيا صريحا سواء حقيقيا أو بال محاكاة أو أي تصوير الأعضاء الجنسية لطفل لإشباع الرغبة الجنسية بشكل أساسي، وتتمثل هذه الحالة، على سبيل المثال، إذا قام أحد الجناة بتحميل صورة رقمية تبين الاعتداء الجنسي على أحد الأطفال.	إنتاج أو توزيع أو حيازة المواد الإباحية المتعلقة بالأطفال بواسطة الحواسيب.

تشير إلى الأعمال التي تنطوي على استعمال أحد نظم الحاسوب للعرض على أحد الأطفال الذين لم يبلغوا سن الموافقة على اللقاء الجنسي، لغرض ارتكاب إحدى الجرائم الجنسية ذات الصلة، وتتمثل هذه الحالة، على سبيل المثال، إذا قام أحد الجناة بالمحادثة النصية عبر الإنترنت مع أحد الأطفال مدعياً أنه طفل أيضاً، ويعرض على الطفل اللقاء، وذلك مع توافر نية الاعتداء على الطفل، ويمكن أن يطلق على هذا الفعل أيضاً "الاستمالة" وتقتصر بعض الاتجاهات الوطنية الجريمة على الإغواء الذي يتبعه أي فعل مادي يؤدي إلى لقاء.	الأفعال ذات الصلة بالحاسوب بغرض إغواء أو استمالة الأطفال لأغراض جنسية.
تشير إلى الأفعال التي تنطوي على استخدام نظام حاسوبي في دعم جرائم الإرهاب، ويشتمل ذلك على استعمال أحد الأنظمة الحاسوبية في إرسال إحدى الرسائل إلى الجمهور بقصد التحريض على ارتكاب إحدى الجرائم الإرهابية، سواء كان بشكل مباشر أو غير مباشر، حيث يمثل إتيان هذا السلوك خطورة ارتكاب جريمة أو أكثر من الجرائم الإرهابية (استخدام الحاسوب في التحريض على الإرهاب)، وهذا يتضمن أيضاً استخدام نظام حاسوبي في تقديم الدعم المالي أو جمعه بهدف استعماله - مع وجود الإدراك باستعماله، سواء بشكل كلي أو جزئي - في ارتكاب عمل إرهابي أو إحدى الجرائم الإرهابية (استخدام الحاسوب في الدعم المالي للعمليات الإرهابية)، أيضاً يتضمن استخدام أحد أنظمة الحاسوب في التخطيط أو الإعداد أو التنظيم لارتكاب عمل إرهابي أو إحدى الجرائم الإرهابية (استعمال الحاسوب في التخطيط لارتكاب جرائم إرهابية)، ويقصد بالجريمة الإرهابية أي فعل مجرم طبقاً للصوصك القانونية العالمية المعنية بمكافحة الإرهاب، أو يراد به التسبب في وفاة أحد المدنيين أو إلحاق إصابة جسيمة به، أو أي شخص آخر لا يشارك بدور نشط في الأعمال العدائية من حالة النزاع المسلح، وتعتبر أيضاً جريمة إرهابية، متى كان الغرض من الفعل - في سياق طبيعته - ترويع السكان أو إجبار إحدى الحكومات أو إحدى المنظمات الدولية لأداء عمل أو الامتناع عن أداء عمل.	أعمال دعم الجرائم الإرهابية بواسطة الحواسيب.

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

أولاً: المصادر:

أ- المصادر الدينية:

- القرآن الكريم، برواية ورش عن نافع.

ب- المصادر القانونية:

الاتفاقيات الدولية :

1. اتفاقية الأمم المتحدة لمكافحة الإتجار غير المشروع في المخدرات والمؤثرات العقلية، الموقعة في 20 ديسمبر 1988.
2. اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة الصادرة بموجب قرار الجمعية العامة للأمم المتحدة 55/25 المؤرخ في 15/نوفمبر/2000 والتي بدأ نفاذها بتاريخ 29/سبتمبر/2003.
3. الاتفاقية العربية لمكافحة الإرهاب، الصادرة عن جامعة الدول العربية في 1998/04/22، والتي صادقت عليها الجزائر طبقاً للمرسوم الرئاسي رقم 413/98 المؤرخ في 7 ديسمبر 1998، والمشور في الجريدة الرسمية رقم 1998/93،
4. الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، الصادرة بقرار عن مجلس الوزراء لجامعة الدول العربية رقم 184، المحررة في القاهرة بتاريخ 2010/12/21.
5. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة في القاهرة والموقع عليها بتاريخ 2010/012/21.
6. اتفاقية المجلس الأوروبي، المتعلقة بحماية الأشخاص الذاتيين تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي، والموقعة في ستراسبورغ، بتاريخ 1981/01/28
7. اتفاقية بودابست بشأن مكافحة الجريمة المعلوماتية، الصادرة عن مجلس أوروبا تحت رقم 185، بتاريخ 2001/11/23.
8. القانون العربي النموذجي لمكافحة جرائم المعلوماتية.

المواثيق والبروتوكولات الدولية:

1. الاعلان العالمي بشأن المبادئ الأساسية لتوفير العدالة لضحايا الجريمة وإساءة استعمال السلطة والصادر عن الجمعية العامة للأمم المتحدة بموجب القرار رقم 40/34 والصادر بتاريخ 1985/11/29.
2. بروتوكول مكافحة صناعة الأسلحة النارية وأجزائها ومكوناتها والذخيرة والاتجار بها بصورة غير مشروعة لعام 2001، المكمل لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة 2000، المعتمد من ظرف الجمعية العامة للأمم المتحدة يوم 31 ماي 2001، رقم و رمز الوثيقة A/RES/55/255.
3. بروتوكول منع وقمع ومعاقبة الاتجار بالأشخاص، وبخاصة النساء و الأطفال، المكمل لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية الموضوع للتوقيع في عام 2002، الصادر عن الأمم المتحدة.

التقارير:

1. التقرير التفسيري لاتفاقية الجريمة الالكترونية بودابست المعتمدة من لجنة وزراء مجلس أوروبا في الدورة التاسعة بعد المائة بتاريخ 8 نوفمبر 2001 والمفتوحة للتوقيع عليها في بودابست بتاريخ 23 نوفمبر 2001.
2. دراسة شاملة عن الجريمة السيبرانية، مكتب الامم المتحدة المعني بالمخدرات والجريمة، فيينا، شباط فبراير 2013.

القوانين والمراسيم الوطنية:

التشريع الجزائري:

1. قانون رقم 03/2000 المؤرخ في 05/08/2000 والذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، المنشور بالجريدة الرسمية للجمهورية الجزائرية، الصفحة 03، عدد 48، بتاريخ 06 أغسطس 2000.
2. أمر رقم 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة المؤرخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003، المنشور بالجريدة الرسمية الجزائرية عدد 44 بتاريخ 23 يوليو 2003.

3. قانون العقوبات الجزائري رقم 15/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 156/66 المؤرخ في 1966/06/08 المتضمن قانون العقوبات الجزائري، الجريدة الرسمية عدد 71 لسنة 2004 المعدل والمتمم.
 4. قانون رقم 04-18 المؤرخ في 25 ديسمبر 2004، المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع استعمالها والاتجار غير المشروعين بهما، الجريدة الرسمية للجمهورية الجزائرية، عدد 83، بتاريخ 26 ديسمبر 2004.
 5. قانون رقم 04-09 والمؤرخ في 2009/08/05 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والمنشور بالجريدة الرسمية للجمهورية الجزائرية، عدد 47، بتاريخ 16 أوت 2009.
 6. قانون حماية الطفل الجزائري رقم 15-12 مؤرخ في 15 يوليو 2015 المتعلق بحماية الطفل، المنشور بالجريدة الرسمية عدد 39، والصادر بتاريخ 19 يوليو 2015.
 7. قانون رقم 04-18 المؤرخ في 2018/05/10 والذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الصادر بالجريدة الرسمية للجمهورية الجزائرية، صفحة رقم 03 عدد 27، بتاريخ 13 مايو 2018.
- التشريع الأردني :**

1. قانون المعاملات الاردني رقم 85 لسنة 2001، المنشور بالجريدة الرسمية على الصفحة 6010 عدد رقم 4524 بتاريخ 2001/12/3.
2. قانون جرائم أنظمة المعلومات الاردني لسنة 2010.
3. قانون حماية حق المؤلف والحقوق المجاورة الاردني، رقم 22 لسنة 1992، المعدل بقانون حماية حق المؤلف رقم 23 لسنة 2014، والمنشور بالجريدة الرسمية عدد 5289 بتاريخ 2014/01/06.
4. قانون الجرائم الإلكترونية الاردني رقم 27 لسنة 2015، منشور بالجريدة الرسمية عدد 5343 صفحة رقم 6531 بتاريخ 2015/06/01.
5. قانون حقوق الطفل الاردني رقم 17 لسنة 2022 الصادر بتاريخ 2022/10/12 والمنشور بالجريدة الرسمية عدد رقم 5820 وساري المفعول بتاريخ 2023/01/10.

6. قانون الجرائم الإلكترونية الاردني الجديد رقم 17 لسنة 2023، منشور بالجريدة الرسمية عدد 5874 رقم 3579 والصادر بتاريخ 2023/08/13.

التشريع الاماراتي:

1. المرسوم بقانون اتحادي رقم 05 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات الاماراتي، منشور بالجريدة الرسمية للأمارات العربية المتحدة، عدد 540 بتاريخ 2012/08/26.

2. قانون حقوق المؤلف والحقوق المجاورة الإماراتي، المؤرخ في 20 سبتمبر 2021 والصادر بمرسوم اتحادي رقم 38 لسنة 2021 والمعمول به بتاريخ 02 يناير 2022.

3. قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي لسنة 2021، المؤرخ في 20 سبتمبر 2021 والصادر بمرسوم بقانون اتحادي رقم 34 لسنة 2021.

التشريع السعودي:

1. نظام حقوق المؤلف السعودي الصادر بالمرسوم الملكي رقم 41 لعام 1424هـ الموافق لسنة 2003م.

2. نظام مكافحة جرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم 17 بتاريخ 2007/03/23، والمنشور بجريدة ام القرى بتاريخ 2007/03/26.

ث- قانون رقم 82 لسنة 2002 المؤرخ في 2002/06/03، بشأن حماية حقوق الملكية الفكرية المصري، المنشور بالجريدة الرسمية لجمهورية مصر العربية، عدد 22، بتاريخ 2002/06/03.

ج- القانون رقم 69 لسنة 2008 المؤرخ في 2008/05/17 بشأن المعاملات الالكترونية في سلطنة عُمان، المنشور بالجريدة الرسمية لسلطنة عُمان، عدد 864، بتاريخ 2008/06/01.

ثانيا: المراجع باللغة العربية.

أ- الكتب:

الكتب العامة:

1. سمر بشير خيرى، الجريمة المنظمة العابرة للحدود "الاتجار بالنساء والطفل نموذجا"، منشورات الحلبي الحقوقية، بيروت لبنان، الطبعة الأولى 2017.
2. طارق زين، الجريمة المنظمة العابرة للحدود الوطنية "التعاون الدولي وسبيل مكافحة" "التدابير الاحترازية"، المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية، بيروت لبنان، الطبعة الأولى 2017.
3. علاء زكي، الجماعات الإجرامية المنظمة في القانون الجنائي الدولي، دار الفكر والقانون، جمهورية مصر العربية، الطبعة الأولى 2018.
4. محمد حسن خمو المزوري، دور المنظمات الدولية في مكافحة الجريمة المنظمة عبر الوطنية، دار الكتب القانونية و دار شتات للنشر والبرمجيات، جمهورية مصر العربية و الامارات العربية المتحدة، طبعة 2017.
5. محمد كريم علي، مكافحة الجريمة المنظمة في ظل المعاهدات الدولية، مركز الدراسات العربية للنشر والتوزيع، جمهورية مصر العربية، الطبعة الاولى 2020.
6. محمود مدين، الانتربول الدولي وتسليم المجرمين، المصرية للنشر والتوزيع، جمهورية مصر العربية، الطبعة الثانية 2019.
7. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، بيروت لبنان، الطبعة الاولى 2005.
8. نسرین عبد الحمید نبیه، الجريمة المنظمة عبر الوطنية، دار الفكر الجامعي، الاسكندرية جمهورية مصر العربية، طبعة 2015.

الكتب المتخصصة:

1. أيمن عبدالله فكري، جرائم نظم المعلومات دراسة مقارنة، دار الجامعة الجديدة، الاسكندرية، جمهورية مصر العربية، طبعة 2007.
2. جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة، دار البداية ناشرون وموزعون، عمان الاردن، الطبعة الاولى 2007.

3. حسنين شفيق، الإعلام الجديد والجرائم الإلكترونية " التسريبات، التجسس الإلكتروني، الإرهاب"، دار فكر وفن للطباعة والنشر والتوزيع، مدينة السادس من أكتوبر، جمهورية مصر العربية، طبعة 2015.
4. حسين محمد الغول، جرائم شبكة الانترنت والمسؤولية الجزائية الناشئة عنها - دراسة مقارنة، مكتبة بدران الحقوقية، بيروت لبنان، الطبعة الاولى 2017.
5. خالد دواوي، الجريمة المعلوماتية، دار الاصدار العلمي للنشر والتوزيع، عمان الاردن، الطبعة الاولى 2018.
6. خالد ممدوح أبراهيم، أمن الجريمة الالكترونية، منشورات الدار الجامعية، الإسكندرية جمهورية مصر العربية، طبعة 2008.
7. دلخار صلاح بوتاني، الحماية الجنائية الموضوعية للمعلوماتية، دار الفكر الجامعي، الاسكندرية، جمهورية مصر العربية، الطبعة الاولى 2016.
8. ذيب بن عايض القحطاني، أمن المعلومات، مدينة الملك عبد العزيز للعلوم والتقنية، منشورات الشركة العربية السعودية الرياض، المملكة العربية السعودية، طبعة 2015.
9. رشدي محمد على محمد عيده، الحماية الجنائية الموضوعية للمعلومات عبر شبكة الانترنت، دراسة مقارنة، منشورات دار النهضة العربية، القاهرة جمهورية مصر العربية، طبعة 2013.
10. رشيدة بوكري، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، بيروت، لبنان، الطبعة الأولى 2012.
11. ضرغام جابر عطوش آل مواش، جريمة التجسس المعلوماتي-دراسة مقارنة-، المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع، القاهرة ، جمهورية مصر العربية، الطبعة الأولى 2017.
12. ضياء مصطفى عثمان، السرقة الالكترونية، دراسة مقارنة، دار النفائس للنشر والتوزيع، الاردن، الطبعة الاولى 2011.
13. طارق ابراهيم الدسوقي عطيه، الأمن المعلوماتي النظام القانوني لحماية المعلوماتية، دار الجامعة الجديدة للنشر الاسكندرية، جمهورية مصر العربية، طبعة 2009.

14. عادل حماد عثمان حماد، حماية المعلومات في التشريع الجنائية السوداني (دراسة مقارنة)، منشورات جامعة نايف العربية للعلوم الامنية الرياض، المملكة العربية السعودية، الطبعة الأولى 2013.
15. عادل صادق، استخدام الارهاب الإلكتروني في الصراع الدولي، دار الكتاب الحديث، القاهرة جمهورية مصر العربية، طبعة 2015.
16. عبد الإله النوايسة، جرائم تكنولوجيا المعلومات شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، دار وائل للنشر والتوزيع، عمان الاردن، الطبعة الأولى 2018.
17. عبد العزيز بن غرم الله آل جار الله، جرائم الأنترنت وعقوبتها وفق نظام مكافحة الجرائم المعلوماتية السعودي دراسة مقارنة، دار الكتاب الجامعي للنشر والتوزيع، الرياض، المملكة العربية السعودية، الطبعة الأولى 2017.
18. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي- دراسة قانونية متعمقة في القانون المعلوماتي - ، دار الكتب القانونية المحلة الكبرى، القاهرة ، جمهورية مصر العربية، طبعة 2007.
19. عبدالعال الديربي أ. محمد صادق أسماعيل، الحاسوب والانترنت، الجرائم الإلكترونية دراسة قانونية قضائية مقارنة مع احدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والانترنت، المركز القومي للإصدارات القانونية، القاهرة، جمهورية مصر العربية، الطبعة الاولى 2012.
20. عبدالله عبدالكريم عبدالله، جرائم المعلوماتية والانترنت (الجرائم الإلكترونية) دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والانترنت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا، منشورات الحلبي الحقوقية، بيروت لبنان، الطبعة الأولى 2007.
21. محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنت "الجريمة المعلوماتية"، مكتبة دار الثقافة للنشر و التوزيع، عمان الأردن، الطبعة الأولى 2004.

22. محمد عطية علي محمد الرزازي، الحماية القانونية لقواعد البيانات في القانون المصري والتشريعات المقارنة، دار الجامعة الجديدة، جمهورية مصر العربية، طبعة 2013.

23. محمد ممدوح بدير، مكافحة الجريمة المعلوماتية عبر شبكات الانترنت والاستدلال كوسيلة لإثبات الجريمة المرتكبة عبر الانترنت، مركز الدراسات العربية، القاهرة جمهورية مصر العربية، الطبعة الاولى 2019.

24. نادر عبد الكريم الغزواني، الحماية الجنائية من جرائم الانترنت دراسة مقارنة، دار نشر نور، تونس، طبعة 2017.

ب- الأطروحات والرسائل:

الأطروحات:

1. إبراهيم محمد القاسمي، جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية - وفقا للمرسوم بقانون اتحادي رقم 05 لسنة 2012 في شان مكافحة جرائم تقنية المعلومات وتعديلاته، أطروحة ماجستير في القانون العام، قسم القانون العام كلية القانون، جامعة الامارات العربية المتحدة، الإمارات العربية المتحدة، السنة الدراسية 2018.

2. إسراء طارق جواد كاظم الجابري، جريمة الإرهاب الإلكتروني "دراسة مقارنة"، مذكرة لنيل شهادة الماجستير في القانون العام، كلية الحقوق، جامعة النهرين، جمهورية العراق، السنة الجامعية 2012.

3. بشان عبد النور، الجوانب الموضوعية لمعالجة الجريمة المعلوماتية، أطروحة لنيل شهادة الدكتوراه في الحقوق، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 01، الجزائر، السنة الجامعية 2018.

4. بعقيقي عبير، مكافحة الجريمة المعلوماتية في التشريعين الجزائري و الإماراتي دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد خضير بسكرة، الجزائر، العام الدراسي 2018.

5. بلال بن جامع، الجرائم المعلوماتية على شبكة الانترنت دراسة حالة جامعة عبد الحميد مهري قسنطينة2، أطروحة لنيل شهادة الدكتوراه علوم في علم المكتبات والتوثيق، معهد علم المكتبات والتوثيق، جامعة قسنطينة2، الجزائر، السنة الجامعية 2017.
6. بوربابة صورية، قواعد الأمن المعلوماتي، أطروحة دكتوراه تخصص علوم قانونية، كلية الحقوق والعلوم السياسية، جامعة الجيلالي الياصب، سيدي بلعباس، الجزائر، السنة الجامعية 2016.
7. درار نسيم، الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الالكتروني -دراسة مقارنة، أطروحة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة ابو يكر بلقايد، تلمسان الجزائر، السنة الجامعية 2016.
8. رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة ابي بكر بلقايد، الجزائر، السنة الجامعية 2018.
9. ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة لنيل شهادة الدكتوراه في الحقوق، قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية ، جامعة باتنة 1، الجزائر، السنة الجامعية 2016.
10. فايز محمد راجع غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة لنيل شهادة الدكتوراه في الحقوق، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 01، الجزائر، السنة الجامعية 2010.
11. لعراية عبد الحميد، فعالية التحالف الدولي في مكافحة الإرهاب، أطروحة لنيل شهادة الدكتوراه تخصص القانون الدولي الجنائي، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، السنة الجامعية 2019.
12. معاشي سميرة، آليات مكافحة الجرائم المعلوماتية، أطروحة لنيل شهادة الدكتوراه تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة محمد خضير بسكرة، الجزائر، السنة الجامعية 2020.
13. مفيدة مباركية، جرائم المعلوماتية في الفقه الإسلامي والتشريع الجنائي-دراسة تأصيلية مقارنة-، أطروحة لنيل شهادة الدكتوراه علوم في العلوم الإسلامية، كلية الشريعة والاقتصاد،

جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، الجزائر، السنة الجامعية 2022/2021.

الرسائل الماجستير:

1. رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الانترنت، مذكرة لنيل شهادة الماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة ابي بكر بلقايد، الجزائر، السنة الجامعية 2012.

2. زيدان بن جمعة بن عبيد الفارسي، الاستغلال الجنسي للأحداث عبر وسائل التواصل الاجتماعي وفق التشريع العُماني، رسالة ماجستير تخصص القانون العام، كلية الحقوق، جامعة الشرقية، سلطنة عُمان، سنة 2025.

3. سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، الجزائر، السنة الجامعية 2013.

4. مصطفى سعد حمد مخلف، جريمة الإرهاب عبر الوسائل الإلكترونية " دراسة مقارنة بين التشريعين الأردني والعراقي"، أطروحة لنيل شهادة الماجستير، كلية الحقوق قسم القانون العام، جامعة الشرق الأوسط، الأردن، السنة الجامعية 2017.

ج-المقالات العلمية :

1. بطحي نسيم، جريمة الدخول أو البقاء غير المشروع إلي النظام المعلوماتي، مقال منشور بمجلة الفقه والقانون السياسي، مخبر الدراسات القانونية جامعة تيارت، الجزائر، المجلد 01 العدد 01 2019.

2. بن عمارة محمد، مفهوم الجريمة المنظمة دوليا ووطنياً، مقال منشور بمجلة البحوث في الحقوق والعلوم السياسية، كلية الحقوق والعلوم السياسية جامعة أبن خلدون تيارت الجزائر، العدد الرابع أكتوبر 2016.

3. توفيق مجاهد، جريمة الإرهاب الإلكتروني في ضوء أحكام الاتفاقية العربية لمكافحة تقنية المعلومات لعام 2010، مقال منشور بمجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، الجزائر، المجلد 09، العدد 03، ديسمبر 2018.

4. حدة بوخالفة، المسؤولية الجزائية لمتعهد الدخول عبر الانترنت، مقال منشور بمجلة الدراسات القانونية، مخبر السيادة والعولمة جامعة يحي فارس المدية، الجزائر، العدد 01، المجلد 06، سنة 2020.
5. حدة بوخالفة، النظام القانوني لمتعهد الإيواء عبر الانترنت، مقال منشور بمجلة المفكر، جامعة محمد خضير بسكرة الجزائر، العدد 14، بدون سنة نشر.
6. خليفي فتيحة، د. مهداوي محمد صالح، التزوير المعلوماتي في البيئة الرقمية، مقال منشور بمجلة الدراسات القانونية، مخبر السيادة والعولمة، جامعة يحيى فارس المدية، الجزائر، المجلد 08، العدد 02، جوان 2022.
7. رافعي ربيع، الارهاب الدولي وعلاقته بالجريمة المنظمة (الارهاب الإلكتروني نموذجاً)، مقال منشور بمجلة القانون والعلوم السياسية، معهد الحقوق والعلوم السياسية، المركز الجامعي صالحى أحمد بالنعامة، الجزائر، المجلد رقم 07 العدد رقم 01 جانفي 2021.
8. رامي متولي القاضي، مكافحة الإجرام المنظم عبر شبكة الأنترنت المظلمة "دراسة تحليلية في التشريع المصري"، مقال منشور بالمجلة الجنائية القومية، المركز القومي للبحوث الاجتماعية والجنائية، القاهرة جمهورية مصر العربية، المجلد 64 ، العدد 03 نوفمبر 2021.
9. سعد بن ناصر آل غرام- عبد الرحمن جابر علوان، دور نظام الملكية الفكرية في الحد من جرائم الاحتيال الفكري والمادي على حقوق المؤلفين في المملكة العربية السعودية، مقال منشور في مجلة العلوم القانونية والسياسية، صادرة عن كلية الحقوق والعلوم السياسية، جامعة حمة الاخضر الوادي، الجزائر، المجلد 16، العدد 02، سبتمبر 2025.
10. شعبان سمير، الجريمة الإلكترونية مقارنة تحليلية لتحديد مفهوم الجريمة والمجرم، مقال منشور بمجلة دراسات وأبحاث، جامعة زيان عاشور الجلفة، الجزائر، العدد الأول، سنة 2009.
11. صابرين جابر أحمد محمد، أ. محمود بن علي بن سهيل المعشني، المواجهة الجنائية لجريمة الاحتيال الإلكتروني في التشريع العماني، مقال منشور بمجلة الباحث الاكاديمي في العلوم القانونية والسياسية، المركز الجامعي أفلو، الأغواط الجزائر، المجلد 06، العدد الأول مارس 2023.

12. عادل مستاري، أرواحنة زوليخة، جريمة التزوير الإلكتروني، مقال منشور بمجلة العلوم الإنسانية، كلية الحقوق والعلوم السياسية، جامعة محمد خضير بسكرة، الجزائر، العدد 46، مارس 2017.
13. عباوي نجاه، الإشكالات القانونية في تجريم الاعتداء على أنظمة المعلومات، مقال منشور بمجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقلة الجزائر، العدد 16، جانفي 2017.
14. عز الدين عثمانى، صور الركن المادي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، مقال منشور بمجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر، الجزائر، المجلد 09 العدد 6 ، ديسمبر 2018.
15. فريدة بوتعني وآخرون، الطفل والجريمة المعلوماتية "جريمة الاستغلال الجنسي للأطفال عبر الانترنت"، مقال منشور بمجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد العاشر، العدد الثاني، لسنة 2021.
16. قطاف سليمان، بوقرين عبدالحليم، الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري، مقال منشور بالمجلة الأكاديمية للبحوث القانونية والسياسية، صارة عن كلية الحقوق والعلوم السياسية، جامعة عمار ثلجي، الاغواط، الجزائر، المجلد السادس، العدد الاول، مارس 2022.
17. لواعر فاطمة، الملكية الفكرية في البيئة الرقمية، مقال منشور بمجلة الحوكمة والقانون الاقتصادي، كلية الحقوق والعلوم السياسية، جامعة باتنة 1 الجزائر، المجلد الثالث، العدد الثاني جويلية 2023.
18. نبيلة كردي، الإتجار بالبشر عبر الانترنت، مقال منشور بمجلة أبحاث متخصصة في الابحاث السياسية والقانونية، جامعة زيان عاشور الجلفة، الجزائر، المجلد السابع، العدد 02 لعام 2022.
19. وفاء صدراتي، آليات الحماية القانونية للتوقيع الالكتروني من جرائم التزوير الإلكتروني في التشريع الجزائري، مقال منشور بمجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر بالوادي، الجزائر، المجلد 11، العدد 01، أبريل 2020.

20. وهيبة عبد الرحيم، دراسة جريمة غسيل الأموال عبر القنوات الإلكترونية، مقال منشور بمجلة الحقوق والعلوم الإنسانية دراسات اقتصادية، جامعة زيان عاشور الجلفة، الجزائر، العدد 19 / 01 أوت 2014.

خ-الأبحاث العلمية:

1. حاتم أحمد محمد بطيخ، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات- دراسة تحليلية مقارنة، مطبوعة صادرة عن جامعة عين شمس، القاهرة مصر، بدون سنة طبع.

د- المقالات والأبحاث الإلكترونية:

1. بن تركية نصيرة، الحماية القانونية للأطفال من الاستغلال الجنسي عبر الانترنت، مقال منشور عبر الانترنت في الموقع الالكتروني التالي، <https://e-biblio.univ-mosta.dz/server/api/core/bitstreams/816d536e-2bc2-482e-a636-de5d97ad9b57/content>

2. محمد الطاهر، تعليق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، مقال منشور على الموقع الالكتروني لمؤسسة حرية الفكر والتعبير، منظمة حقوقية مستقلة، جمهورية مصر العربية، عبر الرابط <https://afteegypt.org/research/research-#papers/2015/03/11/9770-afteegypt.html>

3. الموقع الالكتروني لمكتب الأمم المتحدة لحقوق الانسان عبر شبكة الانترنت في الرابط <https://news.un.org/ar/story/2023/08/1122817>،

4. الموقع الإلكتروني الخاص بالمكتب الأمم المتحدة المعني بالمخدرات والجريمة <https://www.unodc.org/e4j/ar/tip-and-som/module-6/key-issues/international-legal-framework.html>

5. الموقع الإلكتروني الخاص بمكتب الامم المتحدة المعني بالمخدرات والجريمة <https://www.unodc.org/e4j/en/index.html>

6. الموقع الرسمي للإنتربول: www.interpol.int

ذ. المراجع الأجنبية:

1. Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the “Cybercrime Prevention Act of 2012” عبر الموقع الإلكتروني المرفق https://cybercrime.doj.gov.ph/irr/?_cf_chl tk=NaPB0jAlvbxnJr6NExFagoKcOGExLvEbF6bUBexQnM-1714424894-0.0.1.1-1493.
2. Corinne Robaczewski, Atteinte aux systèmes de traitement automatisé de données, Jurisclasseur pénal code, N 4, LexisNexis, paris, 2013.
3. Revue Cahiers de la sécurité – « La Criminalité numérique », Numéro 6, INHES, France, Octobre–Décembre 2008.
4. El-Guindy, Mohamed N. 21st Century Cyber Threats and the Middle East Dilemma. Lulu.com, June 19, 2011.
5. Minimum Security Requirements for Federal Information and Information Systems.Federal Information Processing Standards Publication (FIPS PUB) No. 200, U.S. Department of Commerce, Gaithersburg, MD, March 2006.

الفهرس

المحتويات	رقم الصفحة
الآيه	ب
الإهداء	ج
الشكر والعرفان	د
مقدمة	01
الإشكالية	08
الباب الأول:	13
الإطار المفاهيمي للنظم المعلوماتية.	
الفصل الأول:	15
النظم المعلوماتية بالمفهوم العلمي والتقني.	
المبحث الأول:	16
المدلول العلمي للنظم المعلوماتية.	
المطلب الأول: التعريف اللغوي والإصطلاحي للمعلومات.	16
الفرع الأول: تعريف المعلومات في اللغة.	16
الفرع الثاني: تعريف المعلومات في التشريع.	20
المطلب الثاني: تمييز المعلومات وخصائصها.	24
الفرع الأول: تمييز المعلومات عن شبيهاتها من المصطلحات.	24
الفرع الثاني: المعلومات أنواعها وخصائصها.	29
المطلب الثالث: الطبيعة القانونية للمعلومات.	36
الفرع الأول: المعلومات لها طبيعة من نوع خاص.	36
الفرع الثاني: المعلومات ذات قيمة اقتصادية.	39
المبحث الثاني:	41
الدلول التقني والجنائي للنظم المعلوماتية.	
المطلب الأول: مفهوم النظم المعلوماتية.	41
الفرع الأول: تعريف النظم المعلوماتية.	42
الفرع الثاني: المكونات المادية للنظم المعلوماتية.	46
المطلب الثاني: النظم المعلوماتية جنائيا.	56
الفرع الأول: تعريف جرائم نظم المعلومات.	56
الفرع الثاني: خصائص جرائم نظم المعلومات.	66

72	المطلب الثالث: سمات ودوافع مرتكبي جرائم نظم المعلومات.
72	الفرع الأول: سمات مجرمي نظم المعلومات.
79	الفرع الثاني: دوافع إرتكاب جرائم نظم المعلومات.
82	الفرع الثالث: الضحية في جرائم نظم المعلومات).
88	الفصل الثاني: النظام القانوني لجرائم نظم المعلومات.
88	المبحث الأول: تقسيمات جرائم نظم المعلومات.
89	المطلب الأول: تقسيم جرائم نظم المعلومات حسب دورها.
89	الفرع الأول: تقسيم جرائم نظم المعلومات تبعاً لدور الحاسب الآلي.
92	الفرع الثاني: تقسيم جرائم نظم المعلومات تبعاً لمحل الجريمة.
94	الفرع الثالث: تقسيم جرائم نظم المعلومات تبعاً لعلاقتها بالنظام الآلي.
97	الفرع الرابع: تقسيم جرائم نظم المعلومات تبعاً لمساسها بالأشخاص والاموال.
100	المطلب الثاني: تقسيم جرائم نظم المعلومات حسب الآراء الفقهية والوكالات المتخصصة.
100	الفرع الأول: التقسيم الفقهي لجرائم نظم المعلومات.
105	الفرع الثاني: تصنيف الوكالات المتخصصة الدولية لجرائم نظم المعلومات.
115	المبحث الثاني: جرائم نظم المعلومات والجريمة المنظمة.
115	المطلب الأول: مفهوم الجريمة المنظمة.
117	الفرع الأول تعريف الجريمة المنظمة.
126	الفرع الثاني: خصائص الجريمة المنظمة.
130	المطلب الثاني: الجريمة المنظمة المستحدثة.
131	الفرع الأول: صور الجريمة المنظمة المستحدثة.
145	الفرع الثاني: جريمة الإرهاب الإلكتروني.
152	الباب الثاني: جرائم النظم المعلوماتية والآليات الدولية لحمايتها.
154	الفصل الأول: الجرائم المرتكبة ضد النظم المعلوماتية.

154	المبحث الأول: جريمة الولوج غير المشروع.
156	المطلب الأول: تفصيل جريمة الولوج غير المشروع.
180	المطلب الثاني: معالجة جريمة الولوج غير المشروع في التشريع الجنائي.
193	المطلب الثالث: معالجة جريمة الولوج غير المشروع في التشريع الدولي.
198	المبحث الثاني: جريمة الاعتراض غير المشروع.
200	المطلب الأول: تفصيل جريمة الاعتراض غير المشروع .
203	المطلب الثاني: معالجة جريمة الاعتراض غير المشروع في التشريع الجنائي
212	المطلب الثالث: معالجة جريمة الاعتراض غير المشروع في التشريع الدولي.
214	المبحث الثالث: جريمة الاتلاف المعلوماتي.
216	المطلب الأول: تفصيل جريمة الاتلاف المعلوماتي.
221	المطلب الثاني: معالجة جريمة التلاف المعلوماتي في التشريع الجنائي.
230	المطلب الثالث: معالجة جريمة الاتلاف المعلوماتي في التشريع الدولي.
233	المبحث الرابع: جريمة الاعاقة الخطيرة للنظام المعلوماتي.
234	المطلب الأول: تفصيل جريمة إعاقة النظام المعلوماتي.
236	المطلب الثاني: معالجة جريمة إعاقة النظام المعلوماتي في التشريع الجنائي.
242	المطلب الثالث: معالجة جريمة إعاقة النظام المعلوماتي في التشريع الدولي.
245	الفصل الثاني: الجرائم المرتكبة عبر النظم المعلوماتية.
245	المبحث الأول: جريمة التزوير المعلوماتي.
248	المطلب الاول: تفصيل جريمة التزوير المعلوماتي.
250	المطلب الثاني: معالجة جريمة التزوير المعلوماتي في التشريع الجنائي.
257	المطلب الثالث: معالجة جريمة التزوير المعلوماتي في التشريع الدولي.
259	المبحث الثاني: جريمة إباحية الاطفال المعلوماتية.

262	المطلب الاول: تفصيل جريمة إباحية الاطفال.
264	المطلب الثاني: معالجة جريمة إباحية الاطفال في التشريع الجنائي.
273	المطلب الثالث: معالجة جريمة إباحية الاطفال في التشريع الدولي.
277	المبحث الثالث: جريمة الاعتداء على الملكية الفكرية المعلوماتية.
278	المطلب الاول: تفصيل جريمة التعدي على الملكية الفكرية المعلوماتية.
281	المطلب الثاني: معالجة جريمة التعدي على الملكية الفكرية المعلوماتية في التشريع الجنائي.
293	المطلب الثالث: معالجة جريمة التعدي على الملكية الفكرية المعلوماتية في التشريع الدولي.
297	خاتمة
303	قائمة الملاحق
310	قائمة المصادر والمراجع
325	الفهرس
330	الملخص

تهدف هذه الأطروحة إلى تحليل الإطار القانوني لحماية النظم المعلوماتية من خلال مقارنة تجمع بين الاتفاقيات الدولية والتشريعات الوطنية، وذلك في ظلّ التنامي المتسارع للتهديدات السيبرانية واتساع نطاق الجرائم المعلوماتية التي باتت تمسّ الأمن القومي للدول واستقرارها الاقتصادي وسلامة بنيتها الرقمية الحيوية، وتنطلق الدراسة من إشكالية رئيسة مفادها: إلى أي حد تُسهم الاتفاقيات الدولية والتشريعات الوطنية في حماية النظم المعلوماتية، وما مدى كفايتها وفعاليتها في مواجهة التحديات المتجدّدة للأمن المعلوماتي؟

وقد اعتمدت الدراسة المنهج القانوني التحليلي والمقارن من خلال فحص معمّق لاتفاقية بودابست والاتفاقية العربية لمكافحة الجرائم الالكترونية والمعايير الدولية ذات الصلة، إلى جانب تحليل مجموعة من التشريعات الوطنية ذات الخلفيات القانونية المختلفة كالجزائر والسعودية والاردن والامارات وكشفت النتائج أن الإطار الدولي، رغم أهميته، لا يزال يعاني من محدودية الانتشار وضعف الالتزام، وأنه يحتاج إلى تطوير جوهري يأخذ بعين الاعتبار المخاطر المستحدثة المرتبطة بالمعلومات والهجمات الموجهة إلى البنى التحتية الحيوية، كما أظهرت الدراسة أن التشريعات الوطنية، في معظمها، تركّز على التجريم دون أن توفر منظومة متكاملة للوقاية وإدارة الحوادث، فضلاً عن وجود قصور مؤسسي يتمثل في ضعف التنسيق بين الجهات المعنية ونقص الخبرات التقنية والقضائية المتخصصة.

Summary:

This dissertation aims to analyze the legal framework for protecting information systems through an approach that combines international conventions and national legislations, in light of the rapidly growing cyber threats and the expanding scope of cybercrimes that have come to undermine national security, economic stability, and the integrity of vital digital infrastructures. The study is grounded in a central research question: *To what extent do international conventions and national legislations contribute to the protection of information systems, and how sufficient and effective are they in addressing the evolving challenges of information security?*

The study adopts both the analytical legal method and the comparative method, conducting an in-depth examination of the Budapest Convention, the Arab Convention on Combating Cybercrime, and other relevant international standards, in addition to analyzing a set of national legislations with diverse legal backgrounds, such as those of Algeria, Saudi Arabia, Jordan, and the United Arab Emirates.

The findings reveal that the international framework, despite its importance, still suffers from limited adoption and weak compliance, and requires substantial development that takes into account emerging risks related to data, information, and targeted attacks on critical infrastructures. The study also shows that most national legislations focus primarily on criminalization without providing an integrated system for prevention and incident management. Furthermore, the research highlights an institutional deficiency manifested in weak coordination among competent authorities and a shortage of specialized technical and judicial expertise.

