وزارة الجمهوريـــة الجزائريـــة الديمقراطيـــة الشعبيـــة
وزارة التعليـــم العالـــي والبحـــث العلمـــي
جامعة الشهيد الشيخ العربي التبسي- تبســة
كليــة الحقــوق والعلـوم السياسيـــة
الشعبـــــة: الحقـــــوق
القسم: القانون الخاص

أطروحـــــة لنيـــل شهـــادة الدكتـوراه علـــوم
تخصـص: قانـــون جنائـــي
بعنـــــوان

مظاهـــر العـدوان الإجـرامي عبـر الإنترنـت ومـــدى تأثيـــره علـــى المجتمـــع

إعداد الطالبـــة :
هـــزيل آمـــال

تحـــت إشـــراف :
أ. د دلـــول الطاهـــر

لجنـــة المناقشـــة

أ.د ثابت دنيا زاد	أستاذ التعليم العالي	جامعة العربي التبسي تبســـة	رئيســـا
أ.د دلول الطاهر	أستاذ التعليم العالي	جامعة العربي التبسي تبســـة	مشرفا ومقررا
د. لامية شعبان	أستاذ محاضر – أ–	جامعة العربي التبسي تبســـة	عضوا مناقشا
د. ناصري سفيان	أستاذ محاضر – أ–	جامعة العربي بن مهيدي أم البواقي	عضوا مناقشا
د.شدادي محسن	أستاذ محاضر – أ–	جامعة محمد الشريف مساعدية سوق أهراس	عضوا مناقشا
د. مامن بسمة	أستاذ محاضر – أ–	جامعة لغرور عباس خنشلة	عضوا مناقشا

الموسم الجامعي 2024-2025

بسم الله الرحمن الرحيم

"بسم الله الرحمان الرحيم"

"و ما توفيقي إلا بالله عليه توكلت وإليه أنيب"

سورة هود الآية (88)

"بسم الله الرحمان الرحيم"

"وترى المجرمين يومئذ مقرنين في الأصفاد "

سورة إبراهيم الآية (49)

إهداء

اهدي هذا الجهد المتواضع إلى فرحتي في هذه الحياة

و نورها إلى من كان دعائها سر نجاحي أمي الحبيبة

حفظها الله ورعاها

إلى والدي الكريم حفظه الله

إلى زوجي العزيز حفظه الله

إ إلى إخوتي وأخواتي الأعزاء الذين طالما كانوا سندا

لي حفظهم الله ورعاهم

إلى أحلى هدية من الله وأغلى الناس رامي أديب حفظه

الله ورعاه

إلى أحبابي أبناء إخواني

إليكم جميع أهديها

شكر خاص

من هذا المقام أتوجه بأسمى عبارات الشكر والتقدير والعرفان والاحترام إلى الدكتور دلول الطاهر لما أولاه لي من شرف قبول مهمة مواصلة الإشراف على أطروحتي هذه. فله مني جزيل الشكر ووافر التقدير والاحترام، نسأل الله عز وجل أن يجازيه عنا خير الجزاء وأن يبارك له في وقته وفي عمله.

كما لا يفوتني أن أتقدم بأزكى آيات الشكر والتقدير والعرفان والاحترام إلى الأساتذة الأفاضل أعضاء لجنة المناقشة الذين تكرموا بقبول قراءة هذه الأطروحة والحكم عليها.

إهداء خاص

إلى روح المغفور له الدكتور سعادنة العيد الذي شاءت الأقدار أن يتوفاه الله عز وجل قبل أن يرى ثمرة إشرافه .

رحمه الله وطيب ثراه وأسكنه فسيح جناته

- قائمة الاختصارات

- باللغة العربية

ج : جزء

ج ر : الجريدة الرسمية

ص : صفحة

ق ع ج : قانون العقوبات الجزائري

ق.م.ج : القانون المدني الجزائري

ق.إ.م : قانون الإجراءات المدنية

ق إ ج : قانون الإجراءات الجزائية

- بالفرنسية

ART : Article

Edit : Edition

N° : Numéro

Op.cit : Opuce Citatum

P : PAGE

مقدمة

إن ظهور شبكة الإنترنت وشيوع استخدامها أدى إلي نقلة نوعية في الحياة الإنسانية لما كان لهذه الشبكة من فضل في ولادة عصر اللامحدودية العلمية، فالثورة الإلكترونية وثورة تقنية المعلومات والحكومة الإلكترونية، والنظام المعلوماتي، والتوقيع الإلكتروني، والحاسب الآلي، وشبكة الاتصالات المعلوماتية وشبكة الإنترنت، كلها مصطلحات تستخدم للدلالة على العصر الذي نعيش فيه، عصر المعلومات والتكنولوجيا اللامتناهية أو العصر الرقمي.

فمقارنة بما سبق أدى إنتشار تقنية المعلومات إلى تغيير مظاهر الحياة التقليدية والمادية وتحويلها إلى كل ما هو رقمي ومتطور، وأصبحت الاستعمالات المستمرة للحواسيب والهواتف النقالة المتصلة بشبكة الإنترنت أمرا شائعا داخل أغلب مجتمعات العالم المعاصر، وقد تغلغلت شبكة الاتصالات في كل جوانب الحياة لما تقدمه من تسهيلات في شتى المجالات، وأصبح يعتمد عليها اعتمادا كبيرا داخل الدولة للسيطرة على إدارة المرافق الحيوية فيها، بالإضافة إلى انتشارها بين أفراد أغلب المجتمعات عبر مختلف بلدان العالم باعتبارها وسيلة اتصال عالمية، إضافة إلى استعمالها لإدارة أعمالهم اليومية بفضل ما تقدمه من خدمات.

فمن الثابت أن شبكة الإنترنت تتميز بتقديم العديد من الخدمات لمستخدميها من اتصال ونقل للمعرفة بين الناس والحصول على معلومات، وإتمام المعاملات والحصول على البرامج، وتسهيل إجراء الدراسات، وجني الأموال، كما تتسم بأنها شبكة حرة بالرغم من عالميتها وعدم خضوعها لحدود معينة، بالإضافة لاستقلالها التام كونها لا تقع تحت سيطرة أي دولة أو حكومة أو منظمة. فطابع الحرية الذي يميزها هي أنها لا تخضع لأي جهة محددة، كما يمكن استخدامها في أي وقت أو مكان، وإذا ما توافرت الأدوات اللازمة والتي تمكن من ذلك، بالإضافة إلى أن استخدام شبكة الإنترنت يعمل على خلق عالم افتراضي ينقل مستخدميها إلى عالم إلكتروني يتم فيه تبادل المعلومات والبيانات والرسائل النصية

والصوتية والمرئية والكتابية وتسويق المنتجات، والتعرف على أخر الأخبار والمستجدات، وتعيين المواقع عن طريق" gps "، ومراجعة الحسابات المصرفية الشخصية ودفع الفواتير. وما يميز الشبكة المعلوماتية أيضا أنها شبكة عابرة للدول وغير مقيدة لا بحدود جغرافية أو حدود سياسية أو طبيعية، وتربط بين مستخدميها في جميع أنحاء العالم وتسهل علي هؤلاء وبكل يسر وسرعة كبيرة التنقل المعنوي في العالم الافتراضي بين المواقع والبرامج التي توفرها شبكة الإنترنت وبحرية تامة.

والجدير بالذكر أن أهم خاصية لشبكة الإنترنت هي انتشارها كوسيلة اتصال معلوماتية واستخدامها كبديل لوسائل الاتصال التقليدية الممثلة في الهواتف والرسائل النصية التي تستخدم خطوط الهاتف الباهظة التكلفة، وأهم ميزاتها أيضا انخفاض تكلفة الاستخدام مع إمكانية استعمالها في أي وقت وفي أي مكان توفرت فيه، وسهولة استخدامها من طرف جميع شرائح المجتمع باختلاف أجناسهم وفئاتهم العمرية ومهما كان مستوى ثقافتهم، أضف إلى هذا تعدد شبكات التواصل الاجتماعي الموجودة على الإنترنت. وهى خدمة إلكترونية توفرها شبكة الإنترنت مثل الفيسبوك واليوتيوب والأنستاجرام والسنبشات والتيكتوك، والتي أضحت من أهم الشبكات وأكثرها إثارة للاهتمام وجاذبية للملايين من مستخدمي الإنترنت، ومؤخراً أصبحت الأكثر شعبية والأكثر استخداماً، خاصة بين المراهقين والشباب الذين يعيشون تحررا من أفكار مجتمعهم التقليدية ومن القيود التي كان يفرضها عليهم الواقع الاجتماعي الذين يعيشون فيه، من خلال التواصل عبر شبكات التواصل الاجتماعي التي منحتهم الحرية للتعبير عن أنفسهم وخلقت لهم ثقافة خاصة، وآراء واتجاهات تؤثر في سلوكهم بجميع نواحيه.

لقد شكلت الإنترنت منذ ظهورها مساحة واسعة لحرية التعبير تجاوزت كل الحدود بين الدول. وبالرغم من الفوائد الكبيرة والجليلة للإنترنت إلا أنها أصبحت تستخدم كوسيلة اتصال للإساءة للغير، أو بهدف نشر المعلومات الغير مشروعة أو المسيئة أخلاقيا ودينيا،

ومما يزيد الوضع تعقيدا غياب هيئة رقابية مركزية عالمية مسؤولة عن مراقبة ما يحدث على الإنترنت وكل ما ينشر عبرها، مما دعا البعض إلى وصف الشبكة العنكبوتية بأنها منطقة بدون قانون، ويزداد الأمر صعوبة في تحديد المسؤول عن الفعل الغير مشروع، وفي أغلب الأحيان بسبب لجوء مستخدمي الإنترنت إلى الدخول إلى الشبكة بشخصية مجهولة أو باسم مستعار. كما أن كثرة المعلومات المتداولة وسرعة انتقالها عبر شبكة الإنترنت يقلل من معرفة محتوى المعلومات المنتشرة وإمكانية فرض الرقابة عليها. ونتيجة للاستعمال السيئ للإنترنت اكتشفت أساليب إجرامية عديدة مستحدثة جعلت من ارتكاب نوع معين من الجرائم أمرا في غاية السهولة.

وهكذا جاء التقدم العلمي مصحوبا بصورة مستحدثة لجرائم تستعين بتقنية المعلومات وأساليبها المتطورة، وأصبحنا أمام ظاهرة مستحدثة هي الجريمة عبر الإنترنت، وهي جريمة باتت من أعقد المشاكل التي تواجه العالم المعاصر نتيجة لانتشارها وتزايدها الواسع والمستمر وبمعدلات مخيفة ومفزعة مست كافة الدول والمجتمعات، وصارت تشكل تهديدا حقيقيا لما ينتج عنها من خسائر هائلة وأضرار على كافة المستويات الاقتصادية والاجتماعية والثقافية والأمنية.

لقد أثبتت بعض الدراسات في علم الإجرام عبر الإنترنت، أن هذه النوعية من الجرائم تتميز بكون مرتكبيها يمتلكون العديد من الصفات التقنية الخاصة التي تؤهلهم من استخدام شبكة المعلومات وتطويعها لصالحهم، حتى يتم تحقيق مشاريعهم الإجرامية التي تحتاج لمهارات وخبرات اكتسبت من خلال الدراسة والتخصص في مجال تقنية المعلومات ومن خلال التعامل المستمر معها، وعليه فإن مجرمي الإنترنت لم يكونوا من المتخصصين في مجال الرقمنة وإنما اكتسبوا الخبرات والمهارات اللازمة من خلال الممارسة كلا حسب نسبة الذكاء التي يمتلكها. وعليه أصبحت الإنترنت أداة جديدة غيرت من شكل الجريمة بصفة عامة.

لقد أطلق على الجرائم الواقعة عبر الإنترنت مصطلحات عديدة دون الاتفاق على تسمية موحدة تدل على هذا النوع من الجرائم المستحدثة وهذا نتيجة تزايدها وتنوعها المستمر وهذا بسبب التطور الدائم في مجال تقنية المعلومات، إضافة لأنها ترتبط مع غيرها من الجرائم المستحدثة، فبدأ بتسميتها بمصطلح جرائم الكمبيوتر أو الجريمة المرتبطة بالكمبيوتر وبعدها جرائم الكمبيوتـــــر والانترنـــت أو الجرائم السيبرانية، ثم جرائـــم الهاكرز، وجرائم الساحة الافتراضية.

ولكثرة الاختلافات في المصطلحات المستخدمة للإشارة إلي ظاهرة الإجرام الناشئ في بيئة الحاسب الآلي والإنترنت، قد اعتمدنا في هذه الدراسة مسمى العدوان الإجرامي عبر الإنترنت للدلالة عليها، ومن المهم جدا أن أنوه إلى أن سبب اختيار هذا المصطلح هو أنه أكثر تعبير يدل عن خطورة هذه الظاهرة وخطورة الآثار التي تترتب عليها سواء على الفرد أو على المجتمع. فهو عدو غير مرئي يتربص بالجميع.

لقد تباينت وتشعبت الصور الإجرامية لظاهرة الجريمة عبر الإنترنت، فبعدما كان الاستيلاء على الأموال يتم بالطرق التقليدية المعروفة، أصبحت هذه الأموال يعتدي عليها بواسطة اختراق الشبكات المعلوماتية وعن طريق إجراء تحويلات إلكترونية من بلد لبلد أخر بسهولة تامة وفي أوقات قياسية.

وبعد ما كانت خصوصية الأشخاص يعتدي عليها من خلال التصنت على المكالمات الهاتفية أو من خلال سرقة الصور الشخصية، أصبحت تنتهك من خلال قرصنة البريد الإلكتروني وقواعد البيانات الخاصة المخزنة على أجهزة الكمبيوتر الشخصية.

لقد تعددت مظاهر وتصنيفات جرائم الإنترنت بظهور أنماط مستحدثة من المجرمين، وبذلك صارت مشكلة عالمية تهدد كافة القطاعات، وتستهدف جميع أفراد المجتمعات في العالم بجميع فئاتهم وأعمارهم وبمختلف دياناتهم وثقافاتهم. هذا النوع من الإجرام بمختلف أشكاله له عواقب وخيمة تهدد أمن وسلامة المجتمع من جميع النواحي، فالجرائم المرتكبة

عبر الإنترنت أصبحت سببا من أسباب الفساد الأسري، وفساد الأخلاق والانحطاط الثقافي وزعزعة الأمن والاستقرار الوطني، إضافة إلى كل ما ينجم عنها من خسائر مالية سواء على مستوى الفرد أو الدولة. وبمعنى أخر أصبح الفرد لعبة وأداة للسرقة وللاحتيال وللتهديد والتشهير والابتزاز والتحقير والتحريض في يد مجرمين استطاعوا أن يجعلوا من الإنترنت تهديدا حقيقيا على الحقوق الاقتصادية والاجتماعية وحتى السياسية للأفراد.

لقد أصبحت هذه الجرائم تشكل هاجسا للكثير من الدول باعتبارها من أخطر الجرائم العابرة للحدود، ولأنها تتم وتنظم الكترونيا مما أضفى علبها سمة التعقيد وصعوبة السيطرة والملاحقة القانونية والإجرائية، لذلك وقف المجتمع الدولي على ضرورة الحد من مثل هذه الظواهر الإجرامية وذلك عن طريق ابتكار إجراءات ووسائل وأساليب فعالة لردع هذا الشكل من الانحرافات.

كل هذا جعل المشرع الجزائري ملزما بمتابعة هذه المستجدات والتعامل معها من خلال التدخل التشريعي لمكافحة الجريمة عبر الإنترنت ومن أجل الحفاظ على مصالح الفرد والمجتمع ، والقيام باستحداث آليات قانونية لتستجيب مع هذه التحولات، خاصة وأن التطور الذي عرفته تكنولوجيا المعلومات وتطبيقاتها المتعددة أدت إلى بروز مشاكل قانونية جديدة، يطلب حلها البحث في الأوضاع القانونية القائمة ومدى ملاءمتها لمواجهة هذه المشاكل، خاصة وأن القاضي الجزائي مقيد بمبدأ الشرعية، فمن غير الممكن تجريم أفعال لم ينص عليها القانون مهما كانت درجة خطورتها.

فالتطور التكنولوجي على الرغم من أثاره الإيجابية إلا أن لديه العديد من السلبيات التي تهدد استقرار وأمن المجتمع ليس في الجزائر فقط بل في العالم بأكمله، هذا النوع من الجرائم أصبح يتعدى حدود الدولة الواحدة، وبذلك خرج عن نطاق السيطرة، وفي ظل تطور

الجريمة عبر الإنترنت وتنوعها وخروجها عن النطاق العادي للجريمة التقليدية. وأصبحت جريمة تهدد الإنسان في وجوده.

وتعود أهمية هذه الدراسة إلى تعدد مظاهر الجريمة عبر الإنترنت وتعدد تصنيفاتها، وتنوع وتشعب طرق ووسائل ارتكابها واختلافها من شخص لأخر، وهي جرائم ليس من اليسر حصرها بسبب سرعة تطورها وظهور أشكال مختلفة لها من يوم لأخر.

كما تكمن أهمية موضوع هذا البحث في الرغبة في دراسة خطورة ظاهرة الإجرام عبر الإنترنت والتعمق في الأضرار الجسيمة المنجرة عنه. فمع انتشار واستعمال الشبكة المعلوماتية والإقبال الواسع لأغلب فئات المجتمع عليها واعتماد مصالحنا وإدارتنا المطلق على تكنولوجيا المعلومات، لاسيما وأن مؤخرا شهد العالم طفرة كبيرة ونمو في استعمال الهواتف المحمولة الحديثة التي ساهمت في تسجيل الكثير من الأشخاص في سجلات خدمات الشبكة. وبعد انتشار وتنوع خدمات الإنترنت وزيادة الطلب عليها أصبح الأفراد ينظرون إلى الخدمة على أنها من أساسيات الحياة اليومية ومن أهم متطلباتها، والاعتماد عليها لتسيير أمور العمل في كل المجالات واعتبارها أهم وسيلة للتواصل. ونتيجة للاستعمال المفرط للإنترنت واتساع دائرة الإعلام والاتصال الالكتروني عبر الشبكة، ساعد هذا مرتكبي الجرائم في تنفيذ جرائمهم واعتداءاتهم بكل سهولة وأريحية. لذلك يتوجب علينا تسليط الضوء على هذه الظاهرة مع إبراز الآثار المترتبة عنها، خصوصا في ظل غياب دراسات سابقة متعلقة بموضوع الآثار المترتبة عن الجرائم المرتكبة عبر شبكة الإنترنت. فكانت هذه الدراسة محاولة لتسليط الضوء على هذه الجرائم الخطيرة، وعلى أهم وأبرز الآثار المترتبة عنها والتي أصبحت تهدد حياتنا اليومية. لذا فإن إدراك ماهية هذه الظاهرة واستظهار أنواعها وآثارها يتخذ أهمية استثنائية لسلامة التعامل معها.

أما الهدف من الدراسة فيقف على أساسين هما :

– تسليط الضوء على الجريمة المرتكبة عبر الإنترنت وإبراز أهم أنواعها وحجمها وأساليبها وأسبابها باعتبارها نمطا إجراميا مستجدا بالنظر إلى التطور التكنولوجي المتوسع بشكل دائم ومستمر.

– الوقوف على إبراز أهم أنواع المخاطر والخسائر التي تترتب عنها من الناحية الاجتماعية والاقتصادية والأمنية على النطاق الواسع بشكل عام وعلى الجزائر بصفة خاصة. مع عرض فاعلية أساليب ووسائل مواجهتها وطنيا ودوليـــــــا.

إن دراسة موضوع الجرائم المرتكبة عبر الإنترنت والتعمق فيها واجهه صعوبة في الإلمام بالموضوع لتشعبه. بالإضافة إلى ندرة الأحكام والسوابق القضائية في هذا الميدان وصعوبة التحصل عليها. كذلك صعوبة الحصول على إحصائيات دقيقة، فمعظم الإحصائيات كانت متضاربة في ما بينها.

وانطلاقا مما سبق نطرح الإشكالية التالية:

ماهي الجرائم المرتكبة عبر الإنترنت وما مدى انعكاس آثارها على الفرد والمجتمع ؟ وما مدى مساهمة المشرع الجزائري في تعزيز سبل وآليات مواجهة الجريمة عبر الإنترنت؟

وللإجابة على هذه الإشكالية قد اعتمدنا المنهج الوصفي التحليلي من أجل تحليل المعلومات التي تتوافر عن مشكلة الدراسة، فمن خلاله يتم تحديد مفهوم الظاهرة الإجرامية بكل أنواعها وطبيعتها وأسبابها وآثارها، إضافة لوصف وتحليل النصوص القانونية التي تنظمها، للتعرف على أفضل الحلول لمواجهتها.

وعلى هذا الأساس تم قسيم هذه الدراسة على النحو الأتي:

الفصل التمهيدي: ماهية العدوان الإجرامي عبر الإنترنت

الباب الأول: مظاهر العدوان الإجرامي عبر الإنترنت

الباب الثاني: آثار العدوان الإجرامي عبر الإنترنت وآليات مكافحته

الفصل التمهيدي :
ماهية العدوان الإجرامي عبر الإنترنت

إن الثورة المعلوماتية وما تضمّنته من تكنولوجيا حديثة للاتصالات كان لها الأثر الكبير على حياة الأشخاص العامة والخاصة. ولقد استعملت وسائط متنوعة لتبادل المعلومات، وكانت شبكة الإنترنت الوسيلـة رقم واحد في هذه الوسائط بالاعتماد على الكمبيوتر، الذي يعد الدماغ المسيطر على أنشطة الأشخاص في جميع الأماكن والمجالات لدى كافة الدول.

ولقد تم الاعتماد على الكمبيوتر والإنترنت في شتى المجالات حيث استخدمت كوسيلة للاتصالات واستخدمت في التجارة والزراعة والتعليم والأمن وآليات الحرب وفي العديد من النواحي الأخرى، ورغم أن استعمالها قد جلب للبشريـة عدة منافع لكنها في المقابل ساهمت في انتشار الجريمة والعديد من الكوارث الاجتماعية التي تلحق ضرراً كبيراً بالمجتمع والدولة ذاتها.

ونتيجة لسلوك الشخص الذي قد يكون في بعض الأحيان عرضة للانحراف والعدوان وقد يسيء استخدام الموارد المتاحة له، ظهرت جرائم جديدة نسبة لحداثة الإنترنت، وذلك من قبل فئة أصطلح عليها وصف" مجرمـي الإنترنت"، وهم أفراد لا يقلون خطورة عن المجرمين التقليدين من المحتالين والقتلة والسارقين.

إن جرائم الإنترنت هي الجرائم المرتكبة بواسطة الحاسوب، فكل جرائم الإنترنت يشترط لارتكابها جهاز حاسوب متصل بالإنترنت، وعليه لا تعد كل جرائم الحاسوب جرائم إنترنت إلا إذا كانت الجهاز موصول بالشبكة، ويرى عددا كبيرا من الفقهاء من بينهم الفقيه الألماني Sieher Ulrich والأمريكي Parker اللذان يعتبران من الأوائل في دراسة هذه الظاهرة، أن الإنترنت جزء من النظام المعلوماتي المجسد في الكمبيوتر، ولتفادي الوقوع في اللبس يعد مصطلح جرائم الحاسوب والإنترنت هو الأكثر شيوعا لوصف هذه الجرائم، إضافة إلى هذا استخدم مصطلح جرائم الإنترنت في استراليا للفترة من 16 إلى 17 فيفري 1998[1] في مؤتمر جرائم الإنترنت، وهو مصطلح استخدم لتمييز جرائم الإنترنت عن الجرائم الأخرى التي يعرفها عالم المعلوماتية.

[1] – بحر عبد الرحمن محمد ، معوقات التحقيق في جرائم الإنترنت ، دراسة مسحية على ضباط الشرطة في دولة البحرين، رسالة ماجستير غير منشورة، أكاديمية نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية.2000

فالجرائم المرتكبة عبر الحاسوب والإنترنت أو العدوان الإجرامي عبر الإنترنت أو أيا كان الاسم الذي يطلق عليها فهي ظاهرة تتطور يوم بعد يوم مواكبة للتطور الإلكتروني، فهي جرائم ذكية تنشأ وتحدث في بيئة إلكترونية لا تعترف بالحدود الجغرافية، الأمر الذي ينجر عنه خسائر كبيرة على كافة الأصعدة الاجتماعية والاقتصادية والثقافية والأمنية، ولقد تأثرت المجتمعات العربية بشكل ملموس بمخاطر هذه الجرائم وبنمطها المستحدث مثلها مثل كافة المجتمعات عبر العالم، وبالمقارنة بالدول المتقدمة يمكن أن يكون الخطر المحتمل في البيئة العربية أكبر وأخطر باعتبار أن الوسائل التقنية والتشريعية لمواجهتها ليست بالمستوى المطلوب. وعليه فإن تحديد مفهوم جرائم الإنترنت والخصائص التي قد تتميز بها الجريمة ومرتكبيها من مجرمي الإنترنت وكذلك الإطار القانوني الذي يحكمها يعد من أهم أساسيات الموضوع، وقد حاولنا أن نتعرض لكل هذا بشيء من التفصيل من خلال هذا الفصل التمهيدي الذي قسمناه إلى مبحثين :

خصصنا المبحث الأول إلى **مفهوم العدوان الإجرامي عبر الإنترنت**

أما المبحث الثاني فخصصناه إلى: **الطبيعة الخاصة لجرائم الإنترنت**

المبحث الأول: مفهوم العدوان الإجرامي عبر الإنترنت

إن استفحال ظاهرة الجرائم المرتكبة عبر شبكة الإنترنت أصبحت في الآونة الأخيرة ظاهرة تنذر بخطر فتاك يهدد كافة المجتمعات المعاصرة بسبب حجم المخاطر وهول الخسائر الناجمة عنها، خاصة وأنها جرائم تنتهك الحق في المعلومات، وتهدد الأمن القومي، وتنتهك خصوصية الناس، وتعرض إبداع العقل البشري للخطر.

فالعدوان الإجرامي عبر الإنترنت هدفه الرئيسي المعلومات، ولا يمكن للمجرمين الوصول إلى المعلومات إلا من خلال بوابة واحدة، وهي نظام المعلومات (Système Informatique) الذي يشكل المتلقي الأساسي لها، والذي تم إنشاؤه خصيصا لغرض تداولها وفق أنظمة معالجة آلية محوسبة من خلال الاتصال بالشبكة، شبكة اتصالات (الإنترنت) ، وتركز هذه الخدمات على معالجة المعلومات بأفضل الطرق وأسرعها بهدف تسهيل المعاملات بين الأفراد داخل المجتمع ورفع الأداء المؤسساتي لأجهزة الدولة الحيوية، أضف إلي هذا تقديم خدمات للأشخاص ذات طابع إلكتروني كالبيع والشراء والدفع الإلكتروني، أو خدمات البريد الإلكتروني، أو تسهيل الاتصال بينهم عن طريق

مختلف شبكات التواصل الاجتماعي أو ما يجاورها من خدمات يشترط فيها تقديم معلومات شخصية سرية، الأمر الذي يجعل من هذه المعلومات مطلبا للعديد من هواة ومحترفي الجريمة عبر شبكة الإنترنت، هذه الأخيرة التي أصبحت تشكل عنصرا هاما في حياتنا اليومية، وحسب إحصائيات قامت بها مؤسسة "وي آر سوشيال" في بداية عام 2023 بلغ عدد سكان العالم 8.03 مليار نسمة، وعدد مستخدمي الهواتف النقالة 5.48 مليار شخص، أي ما يعادل 68% من سكان العالم، وبحسب بيانات شركة إريكسون للهواتف فإن في العالم حوالي 7 مليار هاتف مستخدم حاليا. أما عدد مستخدمي الإنترنت في العالم 5،18 مليار شخص وذلك ما يعادل 64،6% من إجمالي سكان العالم.[1] وحسب تقرير وكالة الاستشارات الدولية "داتا ريبورتال" في إحصائياتها السنوية حول الإنترنت وشبكات التواصل لعام 2023، بلغ عدد مستخدمي الإنترنت في الجزائر ما يقارب 32.09 مليون مستخدم في بداية عام 2023، أي بلغ معدل انتشار الإنترنت 70.9٪ من العدد الإجمالي للسكان بعد أن كان في حدود 27 مليون مستخدم عام 2022. ولا يزال هذا الرقم في تزايد مستمر[2].

لذلك يتعين علينا إدراك مفهوم جرائم الإنترنت من خلال التعريف بالإنترنت والتعريف بالجريمة المرتكبة عبرها وهذا ما سنتناوله في المطلب الأول، مع استظهار الخصائص التي تتسم بها والدوافع الكامنة وراءها والأدوات المستعملة لتحقيقها في المطلب الثاني.

المطلب الأول : مفهوم العدوان الإجرامي عبر الإنترنت

فالعدوان الإجرامي عبر الإنترنت[3] من الظواهر الحديثة التي أحاط التعريف بها الكثير من الغموض وقد كانت هناك محاولات عديدة لتعريفه وظل بعضها غير محدد بعلة أن هذه الجرائم ليست أكثر من جرائم تقليدية تُرتكب باستخدام تكنولوجيا المعلومات والكمبيوتر[4].

---

[1]– https://www.aljazeera.net/blogs/2023/5/7

اطلع عليه في 25 جوان 2023 على 17:25

[2] – أخر إحصائيات مستخدمي الانترنيت وشبكات التواصل بالجزائر على الموقع :

اطلع عليه في 22 جوان 2023 على الساعة 21:16

[3] – العدوان الإجرامي تعبيرا يبين مدى خطورة الظاهرة فالعدوان هو سلوك موجه لإيذاء الآخرين عمداً وهذا بالضبط ما تمثله الجرائم المرتكبة عبر الإنترنت فهي سلوكيات هدفها تعمد إيذاء الآخرين عبر الإنترنت وبشتى الطرق.

إن التشريعات التي تحاول تقنين هذا النوع من الإجرام وعدم اتفاقها على وضع تعريف محدد لها لاختلافها عن الجرائم الأخرى المرتكبة في العالم المادي، أدي بالفقه إلي محاولة الاجتهاد في وضع تعريف جامع مانع لها لسد الفراغ التشريعي[1]. وقبل تناول التعريف بالجريمة المرتكبة عبر الإنترنت لابد لنا من أن نعرف بشبكة الإنترنت الوسيلة المستعملة لتحقيقها مع إعطاء نبذة عن تطورها التاريخي.

الفرع الأول: مفهوم شبكة الإنترنت

إن استخدام الحوسبة والرقمية خلق بعض التفاعل والاندماج بين الأفراد باستخدام وسائل الاتصالات المختلفة مما أدى إلي خلق مساحة افتراضية تتلاقى فيها التعاملات المختلفة، الأمر الذي أسفر عن اكتشاف شبكة الإنترنت والتي تعتبر السبب الرئيسي في خلق المجتمع الافتراضي أو العالم الافتراضيCyberspace، والذي يعود الفضل في ربطه بالإنترنت إلي البروفيسور" جون بيري بارلو[2].

الفقرة الأولى : تعريف شبكة الإنترنت

عرفت تقنية الإنترنت بالعديد من التعريفات إذ يعرفها البعض على أنها " شبكة طرق المواصلات السريعة " أيضا تعرف على أنها" شبكة الشبكات".[3]

كثيرة هي التعابير التي تشير إلي الإنترنت والتي تعني لغويا الترابط بين الشبكات لأنها تتكون من شبكات مترابطة منتشرة في جميع أنحاء العالم[4]. ولقد عرفت الاتفاقية الأوروبية

تعددت التسميات الدالة على ظاهرة الجرائم عبر الإنترنت ومن الأمثلة على ذلك : الجرائم التي يساعد على ارتكابها الحاسب الآلي، الاحتيال الإلكتروني ، والبعض الأخر يستعمل عبارة التعسف في استعمال الحاسب الآلي أو إساءة استعمال الحاسب الآلي والإنترنت للدلالة على الظاهرة باعتبارها أوسع وأشمل إضافة إلى تسميات أخري، الجريمة المعلوماتية ، جرائم الحاسوب والإنترنت، إضافة إلي أسماء أخري استعملها الباحثون في العديد من الدراسات مثل جرائم شبكة الإنترنت أو جرائم الإنترنت أو العدوان الإجرامي عبر الإنترنت. كل هذه الأسماء تدل على ظاهرة واحدة وهي ظاهرة الجرائم المرتكبة عبر الإنترنت.

[4] –Michael L, Stevens–Identifying and Charging Computer Crimes I, The military , M L Rev ,1985, Vol 110 , p63

[1] – ربيع محمود الصغير، القصد الجنائي في الجرائم المتعلقة بالإنترنت والمعلوماتية ، مركز الدراسات العربية ، مصر، الطبعة الأولى ،2017 ، ص 90

[4]– ربيع محمود الصغير، المرجع نفسه ، ص 40

[3] – أسامة يوسف أبو حجاج ، دليلك الشخصي إلي عالم الإنترنت، نهضة مصر، القاهرة، 1998 ، ص 18

شبكة الإنترنت على أنها وصلة بين اثنين فأكثر من نظم الحاسوب والاتصال يمكن أن يكون أرضيا سلكي أو كابل أو لا سلكي مثل الراديو أو الأشعة تحت الحمراء أو الأقمار الصناعية، ويمكن للشبكة أن تكون ذات نطاق جغرافي محدد بمنطقة معينة (شبكة منطقة محلية) أو يمكن أن تقوم بتغطية منطقة كبيرة (شبكة لمنطقة ضخمة)، ومثل هذه الشبكات يمكن لها أن تتصل فيما بينها.

والإنترنت تتكون من عدد كبير من الشبكات المتصلة ببعضها وجميعها يستخدم ذات البروتكول ويوجد أنواع أخرى من الشبكات سواء كانت مرتبطة بالإنترنت أو لم تكن كذلك، وذات قابلية للاتصال ببيانات الحاسوب وبين نظمه المختلفة، ويمكن أن تتواصل نظم الحاسوب بالشبكة كنقطة طرفية أو كمعامل مساعد في الاتصالات أو الشبكات، وما هو ضروري هنا أنه يتم تبادل البيانات عبر الشبكة.[1]

والإنترنت هو اختصار للكلمة الانجليزية Network International والتي تعني الشبكة العالمية، ويشير مصطلح الإنترنت بهذا الاسم إلى مجموعة لا حصر لها من الأنظمة الإلكترونية الآلية المتصلة في جميع أنحاء العالم لتبادل البيانات والمعلومات المختلفة أشكالها، وهو الجزء الأكبر من شبكة الكمبيوتر العالمية الذي يربط أجهزة الكمبيوتر الشخصية والشبكات المحلية والشبكات العامة المنتشرة في أماكن مختلفة ومتنوعة في العالم.[2]

وشبكة الإنترنت توفر خدمات عديدة من أهمها :

أولا: البريد الالكتروني : يعد من أهم الخدمات المتوفرة عبر الإنترنـــت، إذ يستخدم لإرسال الرسائل واستقبالها ونقل الملفات بصورة سريعة لا تتعدى ثواني[3]. عندما يرسل شخص ما بريدًا إلكترونيًا، فإنه يستخدم برنامجًا يسمى البريد أو إمايل وبمجرد الانتهاء، يتم

---

[4]– أحمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية، الطبعة الأولى، 2006، ص26

[1] – ربيع محمود الصغير، المرجع السابق ، ص 46

[2] – منير وممدوح الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2006 ، ص7

[3] – صدام حسين ياسين العبيدي، جرائم الإنترنت وعقوبتها في الشريعة الإسلامية والقوانين الوضعية، المركز العربي للنشر، القاهرة، الطبعة الأولى، 2019، ص35

إرسال رسائل البريد الإلكتروني إلى مجموعة من أجهزة الكمبيوتر تسمى خوادم البريد الإلكتروني وأجهزة الكمبيوتر المركزية الأخرى قبل الوصول إلى هدفها أين يتم فتحها وقراءتها. [1] ولتمكين العملاء من الاتصال بشركة معينة يمكن استخدام البريد الالكتروني، ويمكن استخدامه أيضًا لإرسال البيانات والمستندات إلى العملاء، وإبلاغهم بآخر التحديثات للخدمات والمنتجات.

ثانيا: القوائـم البريديـــة : وتشمل قوائم العناوين البريدية لأشخاص يتميزون باهتماماتهم المشتركة. والفكرة هي أن يكون لدى المستخدم عدد كبير من الإيميلات التي يستطيع إرسال رسائل منتظمة لها يتحدث فيها عن منتجه أو عمله أو موقع أو حتى أي شيء تسوق له، بحيث يصبح هناك ثقة واضحة بينه وبين قائمة من ينتظرون رسائله، يتحدثون معه ويعرفون أنه خبير بهذا الموضوع الذي يهمهم.

ثالثا: خدمة المجموعة الإخبارية : من خلالها يمكن معرفة الأخبار السياسية والاقتصادية والطبية والرياضية وغيرها من الأخبار الأخرى، عن طريق الخدمة التي توفرها مواقع الصحف والمجلات والقنوات الإخبارية للمستخدمين من خلال الإطلاع على الأخبار، وتعد المجموعة الإخبارية من وسائل الاتصال المهمة التي توفرها شبكة الإنترنت، إلا أن بروتكولات هذه المجموعة لا تراسل المستخدمين إلا عند طلبهم الاشتراك في المجموعة الإخبارية وعند طلب الأخبار فلا يرسل له إلا العناوين لاختياره العنوان الذي يرغب فيه.[2]

رابعا: خدمة الاستعلام الشخصي : وهي الخدمة التي تمكن من معرفة العنوان البريدي لأي جهة تستخدم الإنترنت وكافة المسجلين فيها.

خامسا: خدمة المحادثات الشخصية : يقصد بها تبادل الحوار عبر الإنترنت. أي أنها خدمة تتيح التواصل مع كل الأشخاص والتحدث معهم عبر شبكة الإنترنت سواءً باستخدام المحادثة الكتابية عن طريق لوحة المفاتيح أو التحدث بالصوت عن طريق السماعات، أو حتى بالصوت والصورة معاً باستخدام الكاميرا (Cam)، حيث انتشرت مؤخراً بشكل كبير عدة مواقع للدردشة التي تستقطب عددا كبيرا من مستخدمي الإنترنت خاصة من فئة المراهقين.

---

[1] – منير و ممدوح الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، مرجع سابق، ص 11

[2] – جمال نادر تعلم الإنترنت بدون معلم ، دار الإسراء، عمان ، الطبعة الأولى ،2005 ، ص 28، 29

سادسا: خدمة الدردشة الجماعية Discussion group : من المستحب لدى الكثير التحاور والدردشة مع الأخريين عبر مجموعات أو منتديات المناقشة التي تعرف بأنها "عبارة عن المناقشات والمحاورات التي يمكن إجراؤها إلكترونيا عبر شبكة الإنترنت لتبادل الآراء ووجهات النظر وتساعد على قراءة المقالات الإخبارية والتعليق عليها." [1] لأن التحاور بين الأطراف فوريا، كما أن تكلفة الاتصال أقل تكلفة من المكالمات الهاتفية.

سابعا: خدمة تحويل أو نقل الملفات: هي خدمة تقوم بتنزيل الملفات من جهاز كمبيوتر إلى آخر على الإنترنت عبر (FTP)، وهو اختصار لبروتوكول نقل الملفات. وهناك أيضًا العديد من الأدوات التي تسمح بتنزيل أي قصاصة فنية للحصول على آخر تحديثات نظام التشغيل، وتعتبر هذه الأدوات سهلة وتسمح لأي شخص بتسجيل الدخول إلى الكمبيوتر الذي يحتوي على الملفات واستخدام أوامر البرامج النصية هذه لتحديد الملفات التي سيتم تحميلها، وتتوفر الآن العديد من برامج (FTP) المتطورة[2].

ثامنا: خدمة شبكة الاستعمالات الشاملة :Gopher يعمل على نقل المستندات والملفات والرسائل إلى القوائم البريدية وفهرسة المعلومات على الويب.

تاسعا: خدمة الاستعمالات واسعة النطاق:Wais وتعمل على البحث في المستندات أو الوثائق عن الكلمات الاستدلالية المحددة من طرف المستخدم ويتم تقديمها قي شكل قائمة تحدد المواقع المحتوية على المعلومات المطلوبة.

عاشرا: خدمة الدخول عن بعد: Telnetوهي خدمة تتيح باستعمال برامج وتطبيقات على الحاسوب عن بعد باستعمال بروتوكول "تالنت".

إحدى عشرة: الصفحة الإعلامية العالمية World Wide Web: فهو يجمع بين جميع مصادر الإنترنت المختلفة للعثور على كل ما في هذه الشبكات من أخبار باختلافها

---

[1] – زين العابدين عواد كاظم الكردي، جرائم الإرهاب المعلوماتي – دراسة مقارنة، منشورات الحلبي الحقوقية ، بيروت، الطبعة الأولى، 2018، ص 38، 39

[2] –HYPERLINK "https://www.commentcamarche.net/contents/519 –le protocole–ftp–file transferprotoco VU LE 2019 /05/12

وإحضارها بالنص والصوت والصور. والويب يعد فرعا من الإنترنت وهو نظام أكبر من أي نظام أخر لأنه يمكن الاستفادة منه لأغراض مختلفة [1].

الفقرة الثانية : لمحة تاريخية على الإنترنت

في الوقت الذي كانت فيه الحرب الباردة بين الاتحاد السوفياتي على أشدها، كانت الحاجة ملحة لدى الولايات المتحدة الأمريكية بتحقيق أكبر حماية ضد اعتداءات مرتقبة من الاتحاد السوفياتي، وكان الجهد الأمريكي العسكري منصبا حينها على إيجاد أفضل حماية ممكنة لإبقاء وإدامة الاتصالات حتى في أحوال الاعتداءات الخارجية خاصة بين الأنظمة والحواسيب[2]، وتنفيذا لهذا ظهرت للوجود ما يطلق عليه باسم ARRANET في 1969/01/02 وعندما قامت وزارة الدفاع الأمريكية بتشكيل فريق من العلماء للقيام بأعمال الكشف عن كيفية ربط شبكات الكمبيوتر فيما بينها ومنه أسست Alohnet وربطها بـ Arpanet وهي نماذج تمهيدية لربط مجموعات من الحواسيب مع بعضها البعض وكان الهدف من هذه التجارب هو تقسيم الرسالة لإرسالها إلى موقع محدد على الشبكة ثم إرسال الانقسامات بشكل مستقل عن بعضها البعض، حتى تصل لمكانها المرسل له، وكانت هذه القضية ذات أهمية كبيرة للولايات المتحدة في زمن الحرب، لأنه إذا تمكن العدو من تدمير خطوط اتصال معينة في منطقة ما، فيمكن للوحدات الأصغر الاستمرار بمواصلة السير بمفردها عبر أي خط حتى تحقق هدفها.

فبعد أن كانت الإنترنت مقتصرة على الأعمال العسكرية اتخذت صفة تجارية في بعض نشاطها أي أنها أصبحت تستخدم لأغراض تجارية [3]. وفي عام 1983 تم تقسيمها إلى شبكتين. بقيت الأولى بمصطلحها الأصلي" Arpane"، وكان غرضها الرئيسي عسكري، بينما الشبكة الثانية كانت تسمى" Milnet" وكانت مخصصة للأغراض المدنية، وفيما بعد تم التوصيل فيما بينهما وبدأت الإنترنت في التطور، وفي سنة 1986 تم ربط عدة شبكات بمركز كمبيوتر عملاق يسمى "NSFNET" وباتت النواة الأساسية لنمو وازدهار

---

[1] - حسين ياسين العبيدي، جرائم الإنترنت وعقوبتها في الشريعة الإسلامية والقوانين الوضعية ، مرجع سابق ، ص 36، 37

[2] - أسامة احمد المناعسة وجلال محمد الزغبي ، جرائم تقنية نظم المعلومات الالكترونية– دراسة مقارنة ، عمان ، الطبعة الثانية ، 2014، ص35

[2] – أسامة احمد المناعسة وجلال محمد الزغبي ، مرجع سابق ، ص 36

الإنترنت في أمريكا وبعدها دول العالم المختلفة وفي هذه المرحلة تم وضع بروتوكول الإنترنت والاتفاق على لغة موحدة لها[1] .

ومن عدة حواسيب مرتبطة بالشبكة عام 1985 توسعت الشبكة عام بعد عام إلي أن أصبحت تعد بالملايير في وقتنا الحالي، وحسب بعض الإحصائيات سيصل عدد مستخدمي الإنترنت عالمياً إلى 5 مليار مستخدم بحلول نهاية عام 2022.

دخلت الإنترنت رسميا إلى الجزائر سنة 1993 عبر مركز سيري للأبحاث العامة، وبعد خمس سنوات تقريبا صدر المرسوم رقم 265 لسنة 1998 الذي قام بالقضاء على احتكار الدولة لتقديم خدمات الإنترنت وإتاحة تقديم خدمات الإنترنت من طرف الشركات الخاصة بشرط أن يحمل المواطن للجنسية الجزائرية وأن يقدم المواطن الطلب إلى الوزير المختص مباشرة، وفي سنة 2000 تم السماح للمؤسسات الأجنبية بالخوض في هذا المجال وقد بلغ عدد المؤسسات الخاصة بين الأجانب والمقيمين في هذا المجال ثمانية عشر، وبحسب بيانات 2005 لوزير الاتصالات الجزائري ، فقد وصل عدد مشتركي الإنترنت إلى أكثر من تسعة ملايين مشترك في الجزائر وحوالي 5 ألاف مقهى إنترنت . وفي عام 2008 تم تخفيض سعر الاشتراك لدى اتصالات الجزائر مما زاد من عدد المشتركين، وبمرور السموات تطورت الإنترنت وازداد عدد مستخدميها في الجزائر بشكل كبير[2].

ومازالت عمليات تطوير شبكة الانترنت متواصلة، وازدياد التطور في الحواسيب والبرمجة الالكترونية وتطوير الأقمار الصناعية لتقديم تقنية جديدة للوصول إلى إنترنت أقوى. وحسب التوقعات قد يصل عدد الأجهزة الموصولة بالإنترنت إلى حوالي خمسون مليار جهاز عام 2025 ولتلبية العدد المتزايد من الأجهزة والخدمات ولتحمل التكاليف وتحسين الاستعمال تعمل الدول المتقدمة على تتطوير أجيال الاتصالات اللاسلكية من g1 g2 g3 g4 g5.

---

[3] – عبد القادر الفنتوخ ، الإنترنت للمستخدم العربي ، مكتبة العبيكان ، الرياض ، 2000 ، ص 21،24

[2] – الإنترنت في الجزائر الموقع https://www.marefa.org اطلع عليه في 2018/05/15 على الساعة 14:15

الفرع الثاني : تعريف العدوان الإجرامي عبر الإنترنت

قبل الخوض في تعريف العدوان الإجرامي عبر الإنترنت لابد من التطرق لتعريف الجريمة بحد ذاتها. وبصفة عامة ثمة عدة تعريفات للجريمة في مفهومها القانوني وتختلف معظمها في صياغتها ولكن ما تحتويه من أفكار يجمع بين كافة هذه التعريفات ولعل أهم ما ورد من تعريف لها هو تعريفها على أنها خرق ومخالفة للقانون الجنائي.[1] والمجرم هو الفرد الذي يؤدي سلوكا يخالف الأوامر الواردة في القانون الجنائي[2]. كما ورد لها تعريف قانوني صدر عن الاجتهاد القضائي الجزائري والذي عرف الجريمة على أنها" كلمة تطلق على كل فعل يعاقب عليه القانون جزائيا، سواء كان الفعل أو الامتناع مخالفة أو جنحة أو جناية".[3] وهذا التعريف يميز السلوك الإجرامي عن غيره من أنواع السلوك الأخرى بتجريم القانون له ومجازاة مرتكبه بعقوبة جزائية والفعل المجرم هو الذي نص عيه القانون .

تؤكد مختلف التعريفات للجريمة عدم وجود مدلول أو فكرة ثابتة للجريمة فتعبير الجريمة يختلف باختلاف وجهات النظر إليها، وهو ما ينطبق على العدوان الإجرامي عبر الانترنت أو الجريمة عبر الإنترنت الذي يمكن أن يطلق عليها الجريمة العالمية، والتي تستخدم فيها شبكة الإنترنت كوسيلة لارتكاب الجريمة. وهي جرائم اختلفت التعريفات الفقهية والقانونية لها. لذلك يتعين لنا الوقوف على أهم هذه التعريفات.

الفقرة الأولى : التعريف الفقهي للعدوان الإجرامي عبر الإنترنت

عادة ما يتفادى الفقهاء التسرع في تعريف الظواهر القانونية المستحدثة لما يميزها من عدم الاستقرار حتى لا يكون التعريف مغامرة غير موفقة. ومع ذلك حازت الجرائم المرتكبة عبر الإنترنت اهتماما كبيرا من جانب الفقه الجنائي لتعريفها واختلفت وتعددت التعريفاتّ إذ تم تعريفها بالنظر إلي مدى ارتباطها بالحاسب الآلي وارتباطها بموضوع الجريمة ذاتها وبالنظر إلى إحدى خصائصها وانقسمت إلي :

---

[1]– Don.C.Gibbons, Society crime and criminel law, Sweet and max well, London, 1982, p7

[2] – W.Elliott.and Selia Wells, Case Book on criminal law, Sweet and Max Well, London , 1982,p 47

[3] – جيلالي بغدادي ، الاجتهاد القضائي في المواد الجزائية ، الديوان الوطني للأشغال التربوية ، الجزء الأول، ص 296 ، قرار صادر في 1986/06/24 من الغرفة الجنائية الأولى في الطعن رقم 853-43

أولا: التعريفات التي تستند إلى وسيلة ارتكاب الجريمة.

إن جرائم الإنترنت عرفت على أنها جرائم حاسوب، وعرفت جرائم الحاسوب على" أنها كل عمل إجرامي غير قانوني يرتكب باستخدام الحاسوب كأداة أساسية، ودور الحاسوب في تلك الجرائم قد يكون هدفا للجريمة أو أداة لها". واعتمدت مجمل هذه التعريفات على وسيلة ارتكاب الجريمة حيث عرفت جريمة الإنترنت على أنها "كل عمل أو فعل غير مشروع تستخدم فيه شبكة الإنترنت كأداة لارتكاب الجريمة أو تسهيل ارتكابها" [1]. والجرائم المرتكبة عبر الإنترنت لا يتم ارتكابها إلا بواسطة الحاسب الآلي الذي يعتبر طرف أساسيا في ارتكاب هذا النوع من الجرائم ، إذ يعد الطرف الثاني لتنفيذ الاعتداء .

ولقد عرفت الجرائم المرتكبة عبر الإنترنت أبضا على أنها " الجرائم التي لا تعرف الحدود الجغرافية والتي يتم ارتكابهـــا بأداة هي الحاسب الآلي عن طريق شبكة الإنترنت وبواسطة شخص على دراية فائقــة "[2].

ومن بين التعاريف التي عرفت بها الجرائم المعلوماتية والتي يمكن أن نطبقها على الجريمة عبر الإنترنت هي التعريف على أنها " كل سلوك إجرامي يرتكب عن طريق مساعدة الحاسب الآلي"[1]. أيضا تعريفها بأنها " كل نشاط إجرامي يؤدي فيه نظام الحاسب الآلي دورا لإتمامه، على أن يكون هذا الدور على قدر من الأهمية ولا يختلف الأمر سواء أكان الحاسب الآلي أداة لإتمام النشاط الإجرامي أم كان محلا له".[2]

ومن خلال ما سبق فإن كل التعبيرات الدالة على هذه الظواهر الإجرامية كلها يربط بينها الحاسب الآلي الذي يكون إما هدف للجريمة أو وسيلة مساعدة لارتكاب الجريمة .

ومن هذا المنطلق يمكن تعريف العدوان الإجرامي عبر الإنترنت بأنها كل سلوك إجرامي يكون الحاسب الآلي وشبكة الإنترنت معا وسيلة لتحقيقه.

---

[1] – حسين محمد الغول ، جرائم شبكة الإنترنت والمسؤولية الناشئة عنها –دراسة مقارنة، مكتبة بدران الحقوقية ، صيدا، الطبعة الأولى، 2017، ص 50

[2] – منير و ممدوح الجنبيهي، جرائم الإنترنت والحاسب الآلي، مرجع سابق ، ص 13

[3] –Adrianrolden, computer crime and the law, c.I.J, 1991, vil ,15, p 399

[4]– نائلة عادل محمد فريد قورة ، جرائم الحاسب الآلي الاقتصادية ، دراسة نظرية مقارنة ، منشورات الحلبي الحقوقية ، الطبعة الأولى ، 2005 ، ص 32، 33

وقد تم انتقاد هذه التعريفات لأن تعريف الجريمة يجب أن يركز على السلوك الذي يشكلها، وليس فقط الوسائل التي ارتكبت بها.

ثانيا : التعريفات التي تستند إلى موضوع الجريمة

يربط البعض من الفقهاء تعريف الجرائم المرتكبة عبر الإنترنت بضرورة أن يكون العمل المرتكب غير مشروع ومخالف للقانون وأن يؤدي إلى إلحاق الضرر بالمجني عليه مع الأخذ بعين الاعتبار الإنترنت باعتبارها الوسيلة الأساسية لارتكاب الجرم وطبيعة كونها بعيدة عن ارتكاب العنف بطريقة مباشرة ومادية.

ومن بين هذه التعريفات تعريفها على أنها " كل سلوك غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات "[1]. وهذا التعريف يوسع من نطاق الجرائم عبر الانترنت ولا يربطها بنوع معين.

ومن التعريفات أيضا التي استندت إلي موضوع الجريمة أنها " كل سلوك هدفه الوصول إلى معلومات مخزنة داخل الكمبيوتر بغرض تغييرها أو نسخها".[2] وهذا التعريف يصف احدي الجرائم التي ترتكب بالدخول إلى شبكة الانترنت عن طريق الحاسب الآلي من خلال إرسال فيروسات عن طريق البريد الالكتروني وعند قراءتها يتمكن الفيروس من الوصول إلى مكان المعلومات و تدميرها أو العبث فيها.

وعرفت أيضا " بأنها عمل آو امتناع عن عمل يأتيه الإنسان إضرارا بمكونات الحاسب الآلي أو شبكات الاتصال به المحمية قانونا والمعاقب على هذا الفعل بموجب القانون".[3]

ونستنتج من هذا التعريف أن مكونات الحاسب الآلي لا يمكن أن تكون كلها محلا لجرائم المرتكبة عبر الإنترنت، كون الحاسب الآلي يتكون من مكونات مادية وهي أدوات الحاسب الآلي من شاشة وقرص صلب و كاميرا .... الخ من الأدوات التي يمكن الاعتداء عليها بدون الاتصال بشبكة الإنترنت وعن بعد، بل يمكن الاعتداء عليها بطريقة مباشرة

---

[1] – هدى حامد قشقوش ، جرائم الحاسب الالكتروني ، دار النهضة العربية القاهرة ، 1992، ص 20

[2] –Michael Alexander– Computer Crime K Ugly Secret For business– Computer World – vol 24–No– 11 March 21– 1990– P104

[3] – حسام الدين الاهواني و جميل عبد الباقي الصغير ، مقدمة في الحاسب الآلي ، دراسة علمية و نظرية، دار النهضة العربية ، القاهرة ،2000، ص 178

بتدميرها أو تفجيرها أو سرقتها. أما المكونات التي تصلح لأن تكون محلا للجرائم عبر الإنترنت فهي البيانات والمعلومات المخزنة داخل الحاسوب الآلي والتي يمكن الوصول إليها عن طريق الاتصال بشبكة الانترنت بقرصنتها وسرقتها أو تدميرها أو تحويلها أو نشرها أو الاعتداء عل صاحبها من خلالها.

ومن التعريفات الدقيقة لجرائم الإنترنت تعريفها على أنهـــــا : " جميع الأفعال المخالفة للقانون والشريعة، والتي ترتكب بواسطة الحاسب الآلي من خلال شبكة الانترنت، وهي تتطلب إلمام خاص بتقنيات الحاسب الآلي ونظم المعلومات، سواء لارتكابها أو للتحقيق فيها، أي أنها نشاط غير مشروع ناشئ في مكون أو أكثر من مكونات الإنترنت مثل مواقع الانترنت، وغرف المحادثة أو البريد الالكتروني"، ويدخل ضمن هذه الجرائم أي أفعال غير قانونية منها تقديم خدمات أو منتجات، قرصنة الكمبيوتر، الوصول إلى الملفات، التعدي على الملكية الفكرية، والابتزاز وغسل الأموال وسرقة الهوية إضافة إلى أي جريمة يمكن تصورها قد تقع عبر الإنترنت .[1]

ثالثا: التعريفات التي تستند لسمات شخصية مرتكب الجريمة

لقد استندت هذه التعريفات إلى شخصية الفاعل، واعتبرت صفة المعرفة بتقنية الحاسوب أساس لهذه التعاريف ومن أهمها تعريف وزارة العدل الأمريكية لجرائم الإنترنت سنة1989الذي جاء فيها:" أنها كل فعل غير مشروع يتطلب لارتكابه الماما وعلما بتقنيات الحاسب الآلي بقدر كبير".[2]

وكذلك عرفها Davidtompson بأنها: " جريمة يكون مطلوب لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب "[3].

لقد تعرضت هذه التعريفات للانتقاد لأن هناك بعض المجرمين ليس لديهم المعرفة اللازمة بالتكنولوجيا وقد يكون جهلهم هو السبب في ارتكاب هذه الجريمة، ويمكن أيضا أن يكون هناك العديد من المجرمين المساهمين فيها لا أحد منهم على دراية بتكنولوجيا

---

[1] – عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، دار الكتب والوثائق المصرية، الإسكندرية ، ص 38

[2] –Carl Benson , Andrew Jablan , Paul Kaplan And Mara Rosenthal , Computer Crimessss ,American C.L.R.N 1997 vol 34 , N2 , p 410

[3] – David Thompson , Current trends in Computer Crime , Computer Control Quar , trely , Vol 9 , N 1 ,1991 , P 2

المعلومات. ونظراً للتطور الذي شهدته التكنولوجيا وتبسيط الأساليب والأجهزة، لم يعد الأمر يتطلب مستوى عالياً من المعرفة، ولا يشترط لارتكابها معرفة أو خبرة الشخص الذي ارتكب الجريمة[1].

وأمام هذه الانتقادات ظهرت تعريفات جمعت بين عدة معايير، مثل تعريف جيون قريل بأنها: " أي عمل له في القانون أو أعراف قطاع الأعمال جزاء، ويضر بالأشخاص والأموال و يستخدم التقنية المتقدمة العالية لنظم المعلومات. [2]"

كما عرفها خبراء منظمة التعاون الاقتصادي والتنمية أنها" كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها.[3] "ووصفها Masse على أنها جرائم أموال.[4]

لقد تعرض معظم التعريفات السابقة للنقد على أساس أنها تستند إما على أساس وسيلة الجريمة وإما على أساس معيار موضوعي أو شخصيي أدى إلى تعريفات عامة ومطلقة لا تحدد جرائم الإنترنت بصورة دقيقـــــــة.

الفقرة الثانية : التعريف القانوني للعدوان الإجرامي عبر الإنترنت

عرفت الجرائم المرتكبة عبر الإنترنت من وجهة النظر القانوني على أنها الأفعال والأنشطة التي نص القانون على معاقبتها والتي تربط بين النشاط الإجرامي وتقنية المعلومات أي أنها كل فعل جنائي يشكل اعتداءا على برامج الكمبيوتر.[5]

كما عرفها مؤتمر الأمم المتحدة لمنع الجريمة المعلوماتية بأنها:" جريمة ترتكب داخل نظام كمبيوتر أو شبكة كمبيوتر. وتشمل هذه الجريمة بشكل أساسي جميع الجرائم التي

---

[1] – عرب يونس، جرائم الكمبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي،2002، ص4

[2] – هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة ، 1994،ص 32

[3] -myriamqueminer، yvescharpenel، la cybercriminalite،op،cit p08

[4] - محمود احمد عبابنة ، جرائم الحاسوب و أبعادها الدولية ، دار الثقافة للنشر والتوزيع ،عمان ، طبعة 2 ، 2009 ، ص 17 . وأنضر : محمد سامي الشوا، ثورة المعلمات وانعكاسها على قانون العقوبات ، دار النهضة العربية ، 1998 ، ص3

[5] – عبد الفتاح بيومي حجازي ، الدليل الجنائي و التزوير في الجرائم المعلوماتية و الانترنت، دار الكتب القانونية ، مصر سنة 2006 ، ص46

ترتكب في البيئة الإلكترونية."[1] وعرفت أيضا على أنها " جريمة تُرتكب إذا استخدم الشخص مهاراته في الكمبيوتر للقيام بسلوك غير قانوني."[2]

كما عرفت من حيث الأثر الذي يترتب على وقوع الجريمة والعقوبة أو التدبير الذي يفرضه القانون عليها كما يلي:" كل فعل ايجابي كان أم سلبي يكون النظام المعلوماتي أداته أو وسيلة لتنفيذه يشكل اعتداء على مصلحة يحميها القانون أو يعرضها للخطر، ويعاقب القانون على ارتكابه بعقوبة أو تدبير".[3]

أما في ما يخص التشريع الجزائري فلم يتطرق لتعريف جرائم الإنترنت، وبدلاً من ذلك، استخدمت مصطلح "انتهاك أنظمة معالجة البيانات الآلية" لوصف هذه الجريمة الجنائية واقتصرت على معاقبة أفعال محددة، تحت عنوان " الجرائم الماسة بنظام المعالجة الآلية للمعطيات" .[4]

أما من الناحية الشرعية فقد عرفت جرائم الإنترنت على أنها " جميع الأفعال المخالفة للشريعة الإسلامية والمرتبطة بواسطة الحاسب الآلي من خلال شبكة الإنترنت ويشمل ذلك الجرائم الجنسية والغير الأخلاقية،الجرائم المالية، جرائم الاختراقات، جرائم القرصنة، جرائم إنشاء مواقع المعادية."[5]

يتضح من خلال التعريفات المختلفة والمتعددة لجرائم الإنترنت أنه لا وجود لتعريف موحد ومحدد شامل مانع لها.

ومن ما سبق من تعريفات يمكن تعريف العدوان الإجرامي عبر الإنترنت على أنه كل سلوك أو فعل مخالف للقانون يرتكب عبر شبكة الإنترنت وبواسطة الخدمات التي تقدمها. والعدوان الإجرامي عبر الإنترنت ككل الجرائم التقليدية يتسم بخصائص متعددة يختلف بها عن الجرائم الأخرى، وهذه الخصائص أو السمات تم استخلاصها من خلال التعريفات المنوطة به.

---

[1] – مؤتمر فيينا في الفترة ما بين 10-17 أفريل 2000

[2] –محمد عادل ريان ، جرائم الحاسب الآلي و أمن البيانات، بيروت،2002، ص 03

[3] – زين العابدين عواد كاظم الكردي، جرائم الإرهاب المعلوماتي دراسة مقارنة ، المرجع سابق ، ص 52

[4] –القانون رقم 15/04 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات المؤرخ في 2004/11/10

[5] –صدام حسين ياسين العابدي ، مرجع سابق ، ص 40

المطلب الثاني : خصائص العدوان الإجرامي عبر الإنترنت

تستدعي السياسة الجنائية الحديثة محاولة حصر الخصائص المميزة لجرائم الحاســـب الآلي والإنترنت عن باقي الجرائم، والهدف هو خلق نصوص ملائمة لمحاربة الجرائم الجديدة التي تصاحب التطور التكنولوجي والمعرفي في عالمنا، بفضل تطور الحاسب الإلكتروني وتطور شبكة الإنترنت. وخصائص وسمات أي جريمة تنبع من خلال التعريف المعطى لها ومن خلال طبيعتها ووسيلة ارتكابها، والتعريف الذي أعطي لجرائم الإنترنت أظهر أن هذه الجريمة جاءت نتيجة التطور التقني الذي أدي إلي تشجيع المجرمين وسهل من عملهم وقلل من حجم الجهد المبذول مع الجريمة التقليدية.

وبالرغم من اختلاف الجريمة عبر الإنترنت عن الجريمة التقليدية إلا أنها تشترك معها في بعض الخصائص من حيث طرفي الجريمة والجاني والمجني عليه، فالجريمة مهما كان نوعها هي عمل غير قانوني .

أما عن الخصائص التي تنفرد بها جرائم الإنترنت هي الأسلوب والوسيلة، إضافة إلى أنها جريمة ذات حدود مفتوحة زمنيا ومكانيا صعبة الحصر والتعداد نظرا لازديادها المستمر وتنوع أساليبها مع ازدياد استعمال شبكة الإنترنت.

ومن خلال هذا المطلب سنحاول حصر الخصائص المميزة لجرائم الإنترنت عن الأنماط الأخرى من الأعمال الإجرامية، وسنحاول أيضا تحديد سمات مرتكبي جرائم الإنترنت مع استعراض طوائف مرتكبي هذا النمط المستحدث من الجرائم وأهم البواعث على ارتكابها.

الفرع الأول : سمات العدوان الإجرامي عبر الإنترنت

الفرع الثاني :المجرم في جرائم الإنترنت ودوافعه للجريمة

الفرع الأول : سمات العدوان الإجرامي عبر الإنترنت

الإنترنت هي هذه التكنولوجيا الحديثة التي أفادت بشكل كبير ذوي الميول الإجرامية وأحدثت تغيرا كبيرا في عالم الجريمة وساهمت في نقلها نقلة إلى ما وراء الحدود الجغرافية، وفي طمس آثارها لتبقي بعيدة عن القانون، حيث نجح مجرمي الإنترنت في تسخير التكنولوجيا الجديدة لخدمة أغراضهم الإجرامية، مستفيدين من أخطائها التقنية وأخطاء مستخدمي شبكة الإنترنت، وضعف الرقابة الأمنية والقانونية. وفي ما يأتي عدد لأهم السمات الخاصة بالجرائم المرتكبة عبر الإنترنت.

الفقرة الأولى : سمات الجريمة من الناحية الوصفية

تتميّز الجرائم المتعلقة بالإنترنت بعدّة خصائص من الناحية الوصفية أبرزها:

أولا : جريمة الإنترنت جريمة حاسوب:

جرائم الإنترنت عبارة عن سلوك إجرامي محلـــه ووسيلته شبكة الإنترنت وأداة ارتكابــه الحاسب الآلي أو أي وسيلة يمكن ربطها بالإنترنت، ومن المتعارف عليه أن شبكة الانترنت هي الخط الرابط بين كل الأهداف المحتملة لان تكون ضحية للجريمة، وعليه فهي جرائم يتطلب فيها اتصالا بالإنترنت واستخدما للحاسب الآلي، فهي جرائم كغيرها من الجرائم يستوجب لارتكابها وسيلة والتي تتمثل في الحاسب الآلي[1]. وتعرف الوسيلـــة التي يرتكب بها السلـــوك الإجرامي عامة بأنهـــــا " كل شيء أو آلة تدخل أو تتوسط بين الإرادة الإجرامية وارتكاب الجريمة "[2] ولقد كان يرى أغلب الفقهاء أن الحاسوب هو الوسيلة الوحيدة لارتكاب جرائم الإنترنت [3].

ومع التطور الذي تعرفه الأجهزة الإلكترونية أصبح ارتكاب هذا النوع من الجرائم يتم عن

---

[1]- جهاز الحاسوب PC أو كما يطلق عليه البعض الحاسب الآلي هو الأداة الرئيسية التي يستعملها المجرم المعلوماتي ليحقق غرضه غير المشروع .أنضر محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي ، دار الثقافة ، عمان، طبعة1، 2004، ص 143. وأنضر علاء الدين ، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني ، موسوعة دلتا كمبيوتر، مطابع المكتب العربي الحديث، القاهرة ، ص109

وينقسم الحاسب إلي أجهزة الكمبيوتر المحمولة أو أجهزة الكمبيوتر المكتبية ، نتبوك ، الكمبيوتر اللوح،كلها مكونة بنفس الطريقة:من الخارج تتكون من شاشة، لوحة مفاتيح، ماوس أو لوحة التتبع (لوحة اللمس) لأجهزة الكمبيوتر المحمولة : وحدة مركزية وقلب ودماغ الحاسوب ومن الداخل تتكون من المعالج .، معالج Intel ، معالج AMD ، معالج Intel Core ، المعالج الدقيق القرص الصلب الداخلي (قرص صلب SSD) ،اللوحة الأم (اللوحة الأم من Asus أو اللوحة الأم من Intel أو اللوحة الأم من المقبس أو اللوحة الأم من MSI) ،إمدادات الطاقة ،ذاكرة الوصول العشوائي ،بطاقة الرسومات وبطاقة الصوت وبطاقة الشبكة .أنضر

- SUPER PROF MAGASINE- https://www.superprof.fr/blog/l-interieur-d-un-personal-computer

[2]- عادل عازر ، النظرية العامة في ظروف الجريمة ، المطبعة العالمية ، القاهرة ، 1967، ص 4 ص5

[3]- منير و ممدوح محمد الجنبيهي ، المرجع سابق، ص 14

طريق أجهزة أخرى كالهاتف المحمول مثلا، فعن طريق الهاتف المحمول[1]يمكن الاتصال بشبكات الإنترنت ويكون الهاتف المحمول وسيلة لتنفيذ الجريمة أو من خلالها، ومع التطور الغير متناهي يمكن في السنوات المقبلة اختراع أجهزة أخرى فائقة التطور يمكنها الاتصال عبر الإنترنت ويمكن أن تكون هي الأخرى أداة لارتكاب جرائم الإنترنت.[2]

ومهما اختلفت الأجهزة التي يمكن لها الاتصال بالإنترنت يري البعض من الفقهاء أن الكمبيوتر قد يلعب ثلاثة أدوار في ميدان ارتكاب الجرائم فقد يكون أداة للجريمة، أو هدفا للجريمة أو بيئة للجريمة.

1: يكون الكمبيوتر أداة للجريمة في حالة استغلال الكمبيوتر للاتصال بشبكة الإنترنت والاستيلاء على الأموال بإجراء تحويلات غير مشروعة أو الاستيلاء على أرقام بطاقات الائتمان واستخدامها للاستيلاء على أموال الغير، أو استعمال أحد المواقع عبر الإنترنت للتشهير أو التحقير بالأشخاص ....إلخ من الجرائم .

2: في حالة الوصول غير المصرح به إلى نظام ما عبر الإنترنت لزرع فيروسات لتدمير البيانات والملفات المخزنة أو المنقولة بواسطة تلك الأنظمة يكون الهدف من الجريمة الكمبيوتر.[3] أو توجيه هجمات إلى معلومات الكمبيوتر لتدميرها أو سرقتها، وهذا ما يتم عادة عن طريق الاختراق، فعادة ما يكون الكمبيوتر مخزن للمعلومات الحساسة المتعلقة

---

[1]– الهاتف المحمول أو الهاتف النقال كما يطلق عليه هو أحد أشكال أدوات الاتصال و الذي يعتمد على الاتصال اللاسلكي عن طريق شبكة أبراج البث الموزعة ضمن مساحة معينة، وأصبحت الهواتف النقالة بديلا لأجهزة الحاسب الآلي حيث تحمل خصائصه ومكوناته ولكن على نحو مصغر ، بل تحتوي أحيانا على مزايا تفوق أجهزة الحاسب الآلي من حيث البرامج والتطبيقات الخاصة بالهواتف النقالة. وعلى غرار الحاسب إلي يتكون جهاز الهاتف المحمول من مكونات مادية ومكونات غير مرئية . المكونات المادية وتتمثل في بطارية الهاتف ولوحة الإدخال وهي اللوحة التي تحتوي على أرقام بمختلف اللغات والحروف الهجائية العربية أو أي لغة أخرى ومن خلالها يتم إدخال الأوامر إلي جهاز الهاتف النقال ومع التطور باتت الشاشات ذات لوحة الإدخال باللمس écran tactile. وليكون الهاتف النقال على اتصال بالشبكة يستوجب اتصاله من خلال شريحة أو بطاقة سيم sim. أنضر حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية دراسة مقارنة ،منشورات الحلبي الحقوقية ،بيروت،طبعة 1، 2014، ص 74وما بعدها.أنضر: **SERGE LEBLAL**– **P**ublié le 24 Mars 2015– https://www.lemondeinformatique.fr/actualites/lire-les-4-composants-phares-des-smartphones

[2]– محمد حماد مرهج الهيتي ، التكنولوجيا الحديثة والقانون الجنائي ، المرجع سابق ، ص 141

[3]– أمير فرج يوسف ، الجريمة الالكترونية المعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت ، مكتبة الوفاء القانونية ، الإسكندرية ، طبعة 1 ، 2011 ، ص92

بالجهات العسكرية أو الجهات القضائية وهذا ما يجعله هدفا من العديد من الجهات كالمنضمات الإرهابية مثلا، ولا تتوقف الجريمة هنا بل تتعدى لاختراق الأنظمة الحكومية، وذلك بالدخول مثلا إلي نظام الحجز في الفنادق لسرقة بطاقات الائتمان، أيضا قد يكون الكمبيوتر هدفا في أنشطة الاعتداء على الملكية الفكرية وسرقة الأسرار التجارية.

3: يكون الكمبيوتر بيئة للجريمة وذلك في حالة استخدامه للاتصال بتجار المخدرات مثلا لإجراء صفقات لترويج المادة المخدرة، أيضا يكون بيئة للجريمة عند استعماله لترويج الشبكات الإباحية وما شابهها من الأنشطة الغير أخلاقية الماسة بالآداب العامة.[1]

ثانيا: جريمة بدون حدود :

لقد أزالت الإنترنت جميع الحدود الجغرافية بين البلدان، حيث يمكننا الدردشة مع أشخاص ليس فقط من بلدان مختلفة، ولكن أيضًا من قارات مختلفة. لذلك أي جريمة ترتكب عبر الإنترنت من الممكن أن تتجاوز حدود الدولة التي ترتكب فيها، وتمتد عواقبها إلى جميع البلدان. وقد عرفت جرائم الإنترنت بأنها " الجرائم التي تتعدى كل الحدود الجغرافية. "[2] وعليه يمكن القول أن أهم مميزات الجرائم عبر الإنترنت أنها جرائم تخترق كل الحدود. فالإنترنت عالم منفتح اكتسبت طبيعة دولية وتخطت الحدود الجغرافية للدول.[3] ومع ظهور شبكات المعلومات، وبسبب السرعة التي تُرتكب بها الجريمة يمكن للعديد من البلدان المختلفة أن تتأثر بالجرائم السيبرانية في نفس الوقت، فمثلا جريمة تبيض الأموال وتحويلها عبر الإنترنت وسرقة البنوك وبطاقات الائتمان تتم من دون الحاجة إلى السطو الفعلي على البنك، وإنما تتطلب مهارة من المجرم في كيفية التحويل الالكتروني من خلال الضغط على زر لانجاز هذه العملية. أيضا بالإمكان ارتكاب جريمة من خلال حاسب ألي متصل بشبكة الإنترنت الموجود في بلد معين وتحقيق نتيجة هذا السلوك في بلد أخر.[4] فمثلا في مواقع البيع بين الدول عبر الإنترنت أين يقوم الزبائن بطلب سلعة معينة والدفع

---

[1]– أمير فرج يوسف ، المرجع نفسه ، ص 93

[2]– نائلة عادل محمد قورة ، المرجع السابق ، ص 52

[3]– خالد ممدوح ابراهيم ، الجرائم المعلوماتية ، دار الفكر الجامعي ، الإسكندرية ، طبعة 2، 2019، ص 76

[4] – حسين محمد الغول ، المرجع سابق، ص 69

بتحويل الأموال عبر الإنترنت وعادة ما تكون هذه المواقع للاحتيال والنصب لبيع بضائع وهمية لا يتم إرسالها.[1]

فالجرائم عبر الإنترنت ترتكب بغياب الفاعل على مسرح الجريمة وارتكابه للجريمة عن بعد، وهذا يعني أن المجرم الإلكتروني غير موجود فعليًا في مسرح الجريمة، وبالتالي هناك مسافة بين المجرم ومكان النتيجة، لذلك لا تنتهي هذه الجريمة داخل حدود دولة معينة، لكنها تمتد إلى حدود بلد آخر، الأمر الذي يجعل الكشف عنها أمرًا صعبًا. [2]

لقد أدت طبيعة الجريمة عبر الإنترنت باعتبارها جريمة عابرة للقارات إلى العديد من المشاكل المتعلقة بتحديد بلد الاختصاص والقانون المطبق والمشاكل المتعلقة بإجراءات تنفيذ القانون وغيرها من القضايا المتعلقة بالجريمة الدولية.

ثالثا :السهولة والمرونـــــــة في التنفيذ والاعتـــــداء :

أدى التطور التقني والتزايد المستمر لاستخدام شبكة الإنترنت، إلى تأقلم الجاني مع هذه الوسائل ذات الطابع التقني وإلي سهولة ارتكاب الجرائم عبر الإنترنت مما ترتب عليه سهولة تبادل الخبرات والأفكار بين الجناة حـــول العالم وإلى سهولة ومرونة التخطيـط والتنفيذ.[3] حيث لا تتطلب جرائم الإنترنت الكثير من الوقت والجهد، فبمجرد الضغط على الجهاز تنتقل ملايين الدولارات أو أي عملة كانت من مكان إلى مكان أخر بكل سهولة وهذا أيضا لا يعني أنها لا تتطلب أي تحضير أو الاستعانة بأجهزة وبرامج متخصصة.[4]

رابعا : الآثار الغير مرئية للجريمة واستتـــــارها

إن الطابع التقني للجريمة وقدرة المجرم على الاستفادة من شبكـــة الاتصال عـن بعد

---

[1] – Internet Crime Complaint Center– IC3– Internet Crime raport – 2007– p15

[2]– نائلة عادل محمد ، جرائم الحاسب الآلي الاقتصادية، مرجع سابق ، ص 52 , 53

[3]– عبد الله عبد الكريم عبد الله ، جرائم المعلوماتية و الانترنت (الجرائم الالكترونية) ،منشورات الحلبي الحقوقية ، عمان ، طبعة 1 ، 2007، ص 31

[4]– محمد رجب فتح الله ، الوسيط في الجرائم المعلوماتية ، دار الجامعة الجديدة للنشر ، إسكندرية ، طبعة 1، 2019، ص 71

لتنفيذها قد يترتب عنه صعوبة اكتشاف هوية منفذها، كونها جرائم ترتكب خلال ثـــــوان معدودة ولا تترك وراءها أي أثر[1]، كما أنه يجعل من الإبلاغ على هذا النوع من الجرائم من طرف المجني عليهم شبه منعدم لعدم الثقة بالقدرة على القبض على الجاني. والجدير بالذكر أيضا أن مجرم الإنترنت يختلف كليا عن مجرم الجريمة التقليدية سواء من ناحية العلم والمعرفة والاحتراف أو الهدف من الاعتداء، فمن المجرمين المستخدمين العاديين الذين يهدفون إلى التسبب في الضرر، والهواة الذين يهدفون إلى اكتساب مهارات معينة على حساب الآخرين، والمهنيين أو المحترفين الذين ينوون الاعتداء والتخريب والتدمير كالمنظمات الإرهابية[2]. فالجميع يرتكبون الجريمة مع عدم ترك أي اثر، فأكثر صور يكون هذا النوع من الجرائم مخفيًا ولا يلاحظه الضحية أو لا يعلم على الإطلاق بحدوثه وذلك من خلال إخفاء السلوك الذي يشكله من خلال التلاعب غير المرئي. وبالتالي عدم وجود أي اثر يمكن تتبعه لاقتفاء اثر الجاني واكتشاف الجريمة وإثباتها على الجاني .[3]

خامسا : جرائم ناعمة بلا عنف أو مقاومة

إن المجرمين المتربصين بضحايا الإنترنت لا يحتاجون لاستخدام العنف المباشر أو السلاح بل يحتاجون لقليل من المعرفة بتقنيات الحاسوب والإنترنت فقط، ففي الوقت الذي تتطلب فيه الجرائم التقليدية شكلاً من أشكال المجهود البدني الذي ينطوي على العنف والإصابة، مثل القتل أو الاعتداء أو القتل غير العمد، أو الضرب أو السرقة، فإن الجرائم عبر الإنترنت جرائم هادئة بطبيعتها soft crime لا تتطلب إلى العنف بل إلى القدرة على التعامل مع الكمبيوتر والإنترنت وذلك لارتكاب الأفعال الغير مشروعة من خلاله[4]. فبدون

---

[1]– محمد علي العريان ، الجرائم المعلوماتية ، دار الجامعة الجديدة للطباعة و النشر ، إسكندرية ، 2004 ، ص 53،63

[2]– David Wall – Cyber crimes and the Internet (crime and the internet) – Routldge Taylor and Francis group– 1st Edition 2001– p8

[3]– محمد حماد مرمج الهيتي ، التكنولوجيا الحديثة و القانون الجزائي ، المرجع سابق ، ص 166

[4]– عبد الرحيم سلطان العلماء ، جرائم الانترنت والاحتساب عليها ، المجلة العربية للدراسات الأمنية والتدريب ، ص 26

عناء وبمجرد الضغط عل الزر يبدأ الجاني في اصطياد ضحاياه، كمن يتلقى مثلا رسالة بريد الكترونية تحمل فيروسا فتاكا وبمجرد الاطلاع عليها تؤدي إلى إتلاف للمعلومـــــــات وسرقة الشفرات والأرقام السرية لبطاقات الائتمان[1]. لذلك عادة ما يطلق على إجـــــــرام الإنترنت بأنه إجرام الأذكياء بالمقارنة مع الإجرام التقليدي الذي يميل إلى العنف المادي.[2] وبالرغم من ذلك إن عددا معين من الجرائم عبر الإنترنت لا تحتاج لذكاء خارق لارتكابها كجريمة السب والتشهير مثلا.

الفقرة الثانية: سمات الجريمة من الناحية الإجرائية

تتميز الجريمة عبر الإنترنت بعدة سمات من الناحية الإجرائية من أهمها:

أولا: صعوبة اكتشاف الجريمة وصعوبة الوصول إلى الدليل

تتميز الجرائم عبر الإنترنت بصعوبة اكتشافها، وبالمقارنة بالجرائم التقليدية فإن حالات الكشف عن جرائم الإنترنت تعد ضئيلة، ويمكن أن تُعزى أسباب صعوبة اكتشاف الجرائم عبر الإنترنت إلى حقيقة أن هذه الجرائم لا تترك أي أثر خارجي مرئي. إضافة إلى أن المجرم يمكنه ارتكاب هذه الجريمة في مختلف الدول عبر العالم[3].

والمشكلة الأخرى هي أن إثبات جريمة الكمبيوتر أمر صعب، لأن المجرم الإلكتروني يمكنه في وقت قياسي حذف أو تغيير البيانات والمعلومات الموجودة على الكمبيوتر، لذلك تلعب الصدفة والحظ السيئ دورًا مهمًا في الكشف عنها، بدلاً من تقنيات التحقيق، ومعظم المجرمين الذين تم القبض عليهم، كما لاحظ أحد خبراء الجرائم الإلكترونية، تصرفوا بإهمال وكان استخدامهم لأنظمة الكمبيوتر خالي من أي مهارة.[4]

تحدث الجرائم المعلوماتية خارج الواقع المادي، حيث أن قاعدتها تعتمد على البيئة الحاسوبية والإنترنت، مما يجعل من إمكانية اكتشافها أمرا معقداً لدى سلطات الأمن وأجهزة

---

[1] – Michael Kunzenf Patrique wilson Computer Crime and Computer Fraud – Report to the montgmery county criminal Justice Coordinating Commission University of Mayrland Fepartment of Criminology and Criminal Justice Fall – 2004 – p 12.13

[2] – محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية ، 1998، ص 34

[3]– نهلا عبد القادر المومني ، الجرائم المعلوماتية، دار الثقافة، عمان ، طبعة1، 2008 ، ص 50، 51 ،53

[4]– محمد عبد الله أبو بكر سلامة ، جرائم الكمبيوتر والإنترنت ، المرجع سابق ، ص 95

التحقيق والملاحقة. فعبر الإنترنت تكون المعلومات نبضات إلكترونية مما يجعل من طمس الدليل أمرا سهلاً على الجاني[1]، وتكمن الصعوبة أيضا في إثبات الجريمة إلى تميز الجناة بالدهاء والذكاء والخبرة.[2]

لذلك بات من الضروري إقامة التعاون بين المؤسسات المتخصصة، ولا بد من عقد دورات تدريبية لوكلاء النيابة والشرطة والخبراء الفنيين، بهدف معرفة طبيعة عمل كل مؤسسة. للوصول إلى الأساليب القانونية الفعالة لمكافحة الجرائم عبر الإنترنت.[3]

ثانيا: نقص الخبرة الفنية لدى المحققين

إن نقص الخبرة الفنية لدى المحققين تشكل حاجزا أمام إثبات الجرائم المرتكبة عبر شبكة الإنترنت لأن هذا النوع من الجرائم يتطلب خبرات فنية كبيرة وملمة بكل طرق استخدام الحاسوب وشبكة الاتصالات وطرق التعامل معهما، ونتيجة لهذا النقص في الخبرة نجد جهات التحقيق لا تبذل قصارى جهدها في التحقيق في هذا النوع من الجرائم لكشف مرتكبيها واثبات الجرم عليهم، إضافة إلى هذا قد يكون المحقق ذاته هو السبب في إزالة الدليل بسبب سوء تعامله مع الأدلة بسبب نقص الخبرة والمعرفة الفنية التي تمكنه من استخراج الدليل بطريقة صحيحة والحفاظ عليه[4].

فالغرض من التحقيق هو ضبط الأدلة المادية، وجرائم الإنترنت ترتكب في بيئة غير تقليدية، لأنها تحدث خارج البنية المادية الفعلية، والأساس يقوم على بيئة الكمبيوتر والإنترنت، مما يزيد الأمور تعقيدا أمام الجهات الأمنية والتحقيقات والملاحقات القضائية، ففي بيئة الإنترنت البيانات والمعلومات تكون بمثابة نبضات إلكترونية من خلال نبضات معلوماتية، مما يجعل مسألة طمس الأدلة وإزالتها بشكل كامل من قبل الجاني بسيطة للغاية.[5]

---

[1] – خالد ممدوح إبراهيم ، الجرائم المعلوماتية ، المرجع سابق ، ص 43

[2] – محمد عبد الله أبو بكر سلامة ، المرجع السابق ، ص 99

[3] – نائلة عادل محمد فريد ، جرائم الحاسب الآلي الاقتصادية ، المرجع السابق ، ص 5

[4]– ممدوح عبد الحميد عبد المطلب ، البحث والتحقيق الجزائي الرقمي في جرائم الكمبيوتر والانترنت ، دار الكتب القانوني ،2006 ، ص 93

[5] – محمود رجب فتح الله ، الوسيط في الجرائم المعلوماتية ، المرجع السابق ، ص87

ثالثا: صعوبة المعاينة والتفتيش

جرائم الإنترنت تتم في الفضاء الافتراضي أي أنها تدخل في مجال المعالجة الآلية للمعلومات لأغراض معنوية وليست مادية، لذلك من الصعب جدًا ملاحقة هؤلاء المجرمين لعدم تركهم أي دليل خارجي مرئي للتحقيق فيه، مما يجعل من الصعب اكتشاف الجريمة ومعرفة الجاني، على عكس الجرائم التقليدية التي تترك آثارًا بشكل عام، مثل الأدلة المادية، وأقوال الشهود، وما إلى ذلك، وقد يتطلب موضوع البحث في بعض الأحيان تمديده ليشمل المتهم أو المشتبه فيهم .

فهذه الجرائم تقع في بيئة الكترونية ويستلزم التعامل معها استعانة الجاني بوسائل وأجهزة تقنية تتم في الغالب بالكمبيوتر وملحقاته الأساسية، وكذلك أجهزة الربط بالشبكات بغيرها، ولكن مع ذلك يمكن ارتكاب مثل هذه الجرائم أيضا من خلال وسائل تقنية أخرى كأجهزة الهاتف المحمول الجد متطورة، وغيرها من الأجهزة كالتقنيات التي يمكن أن تظهر إلى الوجود في أي لحظة، وهذه الخاصية بدورها تصعب من مهمة التفتيش والمعاينة لمحل هذه الجرائم والتحقيق فيها، هذا إذا مأخذنا بالاعتبار أن مجرمي الإنترنت غالبا ما يكونون على دراية واسعة بكيفية التحكم بهذه التقنيات بعكس جهات التفتيش والمعاينة.[1]

إن التفتيش وما شابهه يمكن أن يأتي على الجانب المنطقي للكمبيوتر، أي المعلومات والبيانات التي تتم معالجتها في الكمبيوتر، وهناك الكثير من الجدل حول ما إذا كان ينبغي أن تكون موضع تفتيش أم لا.

الفرع الثاني : المجرم في جرائم الإنترنت ودوافعه للجريمة

في ظل التطور التكنولوجي والاستخدام المتزايد لشبكة الإنترنت، التي تربط بين أنحاء العالم ظهرت طائفة جديدة من المجرمين الذين يطلق عليهم مجرمي الإنترنت، الذين تتوافر فيهم صفات وسمات خاصة بهم تميزهم عن المجرم الذي يقترف الجرائم التقليدية، فالأمر يختلف بالنسبة لجرائم الإنترنت كونها جرائم تقنية، وعادة ما يكون مرتكب الجريمة متخصصًا في تكنولوجيا المعلومات أو على الأقل شخصًا يتمتع بالحد الأدنى من مهارات الكمبيوتر للتعامل مع الإنترنت. ففي الجرائم المرتكبة عبر الانترنت ذات الطابع الاقتصادي

[1]– هبة هروال ، الجوانب الإجرائية لجرائم الإنترنت، دار الفكر الجامعي، الإسكندرية ،2013 ص 37

مثلا يتطلب في سرقة الأموال مهارة وقدرة تقنية فائقة من قبل مرتكبها وهذه المهارة لا يمتلكها كل الأشخاص ، كذلك جريمة التجسس أو القرصنة.

كذلك قد تختلف دوافع هذه الجرائم عن دوافع الجريمة التقليدية.

وعلى هذا الأساس سنتناول مجرم الإنترنت من حيث طبيعته وسماته وخصائصه في هذا الفرع، ثم طوائف المجرم عبر الإنترنت في الفرع الثاني، ونختم بالتعرض لدوافع وبواعث المجرم في هذا النوع من الجرائم.

الفقرة الأولى: السمات المميزة لمجرم الإنترنت

لقد مر مصطلح مجرم الإنترنت بأربعة أجيال حتى وصل إلى ما وصل إليه اليوم ولقد تشكل الجيل الأول من خلال مصطلح الهاكر أو الهكرة[1] في فترة الستينات من القرن العشرين ليتم إطلاقه على المبرمجين المبدعين من طلبة الحاسوب والاتصالات، وبصفة خاصة طلاب معهد ماساشوستس للتكنولوجيا في الولايات م أ[2]، لما اشتهر عنهم البراعة الكبيرة في مجال الحاسوب، ثم امتد ليطلق عليم مطوري الحاسوب وتقنية الاتصالات، ويعتبر هؤلاء الجيل الثاني لمصطلح Phreaker الذي يعني كل شخص لديه القدرة التقنية على اكتشاف نظام الهاتف ليحصل على خدمة اتصالات مجانية من منطلق التجربة والخبرة .

وفي الثمانينات أطلق هذا المصطلح على مخترقي الألعاب الإلكترونية عبر خدمات الشبكة الحاسوبية، ويمثلون الجيل الثالث أو جيل الحاسوب. وبعد التطور المستمر والكبير في هذا المجال وصل إلى ما عليه من مجرمين والذين يمثلون الجيل الرابع. والمصطلح المستعمل في وقتنا المعاصر هو المجرم التقني أي الذي سلك مسلك التقنية لارتكاب

---

[1] –الهكرة هم من وضع فكرة نظم التشغيل للحواسيب ، بالإضافة إلى أنهم قد يسيطروا على مكوناته المتعددة ، ففي عام 1969 وضع tompson kenneth نظاما لتشغيل UNIX والذي يعتبر حتى الآن من نظم التشغيل التي يمكنها استيعاب تطور حركة المعلومات ، وفي عام 1970 أطلق مصطلح Hacker على مجرم يستخدم تقنيات القراصنة لخرق القانون. ;وكان في الأصل يشير مصطلح "hacker" فقط إلى مبرمج تقني للغاية. واليوم غالبا ما يستخدم المصطلح مرادف مع المجرم. "المتسلل الإجرامي" و "التكسير" هما المرجعان الأكثر دقة لهذا الشخص. https://www.pcmag.com/encyclopedia/term/40473/criminal-hacker.

[2] – عمر محمد بن يونس، الجرائم الناشئة عن استخدام الإنترنت– الأحكام الموضوعية والجوانب الإجرائية ، دار النهضة العربية، القاهرة ، 2004، ص22

جرائمه، والذي يقوم بارتكاب جرائمه باستخدامه لتقنية الحاسوب والإنترنت والذي يطلق عليه أيضا مصطلح "مجرم الإنترنت " أو "الهاكر " [1].

ويعرف مجرم الإنترنت على أنه" الشخص الذي يملك المهارات لاكتشاف تفاصيل الأنظمة المبرمجة والاستحواذ على ما يهمه". ويعرف أيضا أنه" الشخص الذي يرغب ويهوي فهم استخدام الحيل التقنية لاكتشاف الأنظمة".[2]

هناك دراسات مختلفة تحدد مجرمي الإنترنت وشخصياتهم وخطورة جرائمهم وخصائصهم المتباينة، وهنا يمكننا طرح السؤال الأتي : هل هناك مثال معين لمجرمي الإنترنت؟

بطبيعة الحال لا توجد أمثلة محددة لهؤلاء المجرمين، ولكن هناك خصائص مشتركة بينهم، لذلك سوف نتناول المعايير التي تمييز مجرم الإنترنت عما قد يتشابه معه من أنواع المجرمين. ويمكن حصرها فيما يلي :

أولا : تخصص مجرم الإنترنت

إن مجرم الإنترنت غالبا ما تكون لديه القدرة الفائقة والمهارة الكبيرة في الدخول إلى الشبكة، وخرق التشفير وكلمات المرور، والتسلل إلى عالم الإنترنت والحصول على كل ثمين وقيِّم من بيانات ومعلومات موجودة على أجهزة الحاسوب عبر شبكة الإنترنت.

ولقد بينت العديد من الدراسات في هذا النوع من القضايا أن عددا معين من المجرمين متخصص في جرائم الإنترنت ولا يرتكب سواها ولا توجد لديهم أي صلة بالجرائم التقليدية الأخرى، وهذا يدل على أن المجرمين الذين يرتكبون جرائمهم عبر الإنترنت هم عادة مجرمون متخصصون في هذا النوع من الجرائم.[3]

ثانيا : مجرم الإنترنت مجرم غير عنيف:

يري بعض المختصين في دراسة الظاهرة الإجرامية أن المجرم عبر الإنترنت هو أحد هؤلاء المجرمين الذين لا يستخدمون العنف أبدًا لارتكاب جرائمهم لأنه يندرج تحت الجريمة التي تتطلب الحيلة فقط لأن هذه الجريمة لا تتطلب أي مستوى من العناء للقيام بها، أي

---

[1]– ربيع محمود الصغير ، القصد الجنائي في الجرائم المتعلقة بالإنترنت و المعلوماتية ، المرجع سابق ، ص117

[2] – امجد دخل الله ، القرصنة الإلكترونية ، مجلة المحامون ، العدد 4 ، سوريا، 2007 ، ص 25

[3]– عبد الفتاح بيومي حجازي ، الحماية الجنائية للتجارة الالكترونية ، دار الفكر الجامعي ، الإسكندرية ، الطبعة الثانية ، 2001 ، ص 97

أنها لا تحتاج للمجهود العضلي بل تحتاج للمجهود العقلي والمعرفة بعلم الحاسوب والإنترنت [1].

ثالثا : مجرم الانترنت مجرم محترف:

يتمتع مجرم الإنترنت بالمهارات والقدرات التقنية التي تسمح له باستخدام مهاراته في عمليات التسلل والسرقة والاحتيال وانتهاك حقوق الملكية الفكرية وغيرها من الجرائم مقابل ربح مادي. وبالإضافة إلى درجته المهنية العالية في ارتكاب جرائمه، حيث أنه ارتكب هذه الجرائم من خلال جهاز حاسوب متصل بالإنترنت، فالأمر يتطلب مستوى عالياً من الدقة والاحترافية في مجاله للتغلب على المعوقات التي وضعها الخبراء للحماية أنظمة الحاسوب كما هو الحال مع البنوك والمؤسسات العسكرية.[2]

رابعا: مجرم الإنترنت مجرم متعود بالإجرام

يتميز المجرم في الجرائم الواقعة عبر النت بالعودة إلى الجريمة لاستخدام مهاراته والتحكم في نظام الشبكة من خلال التلاعب بالحاسوب لتخزين البيانات والمعلومات والوصول إليها بطريقة غير مشروعة، فهو قد لا ينفذ جريمته بهدف إلحاق الضرر، ولكن غالبًا ما يعود مجرمو الإنترنت إلى ارتكاب جرائم أخرى في مجال الكمبيوتر بسبب إدراكهم لقدراتهم ومهاراتهم في التسلل، حيث يأملون في سد الثغرات التي أدت فيما سبق إلى تحديد هويتهم ومقاضاتهم في نهاية المطاف عدة مرات.[3]2AAZA

خامسا : مجرم الانترنت يتسم بالمهارة والمعرفة[4]

لتنفيذ الجريمة عبر الإنترنت يتطلب ذلك قدرا من المهارة يكتسبها المجرمون من خلال الدراسات المهنية في هذا المجال أو من خلال الاتصالات الاجتماعية مع أشخاص آخرين، ولكن قد لا يكون لدى المجرمين معرفة كبيرة مثبتة في الممارسة العملية، حيث لا يكتسب العديد من مجرمي الإنترنت المهارات اللازمة لارتكاب هذا النوع من الجرائم.

---

[1]– شيرين الياس دبابنة ،التأثير الاجتماعي والاقتصادي لجرائم الإنترنت في المجتمع الأردني ، رسالة لنيل شهادة الدكتوراه في علم الاجتماع ،كلية الدراسات العليا ، الجامعة الأردنية ، 2008

[2]– محمود رجب فتح الله ،الجرائم المعلوماتية، المرجع السابق ، ص 93

[3]– عبد الفتاح بيومي حجازي ، الحماية الجنائية للتجارة الإلكترونية ، المرجع السابق ص98

[4] –عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 42

ومن الخصائص المميزة لهؤلاء المجرمين المعرفة حيث أن المجرم يستطيع هنا أن يقوم بتخيل جريمته كاملة، وهذا عائد للمكان الذي تحدث فيه الجريمة وهو نظام الحاسب والإنترنت، فالفاعل يمكن له تطبيق جريمته من أنظمة مطابقة قبل التنفيذ.[1]

سادسا : مجرم الإنترنت مجرم ذكى

يمتلك هذا المجرم ذكاء يتيح له تعديل أنظمة الأمان وتطويرها ومنع تعقب أنشطته الإجرامية ومراقبتها داخل الشبكة أو الكمبيوتر.

فجرائم الإنترنت من الجرائم الذكية التي لا تحتاج لاستخدام القوة، بدلاً من ذلك فإن الذكاء هو المفتاح للمجرمين للعثور على الثغرات واقتحام البرامج المحمية، ووضع القنابل الزمنية أو يعمل على وضع فيروسات من شأنها إتلاف برامج الحاسوب وتدميرها أو تحويل مبالغ مالية لصالحه.[2]

سابعا : مجرم الإنترنت مجرم اجتماعي

من الصفات التي يتميز بها مجرم الإنترنت أيضا هو أنه اجتماعي بطبعه حيث أن هذا النوع من المجرمين يمارس عمله داخل الوسط الاجتماعي لذلك أفعاله الإجرامية قد تكون أحيانا لمجرد اللهو أي أن الدافع أحيانا قد لا يدل على وجود خطورة إجرامية كامنة في نفسه ، فقد يدفعه للقيام بجريمته مجرد رغبة كامنة في نفسه لإشباع رغبته في التحدي لقهر نظام معلوماتي معين أو من أجل التنافس مع الأصدقاء للوصول إلى معلومات معينة عبر الإنترنت، وكذلك قد يكون الدافع من وراء الجريمة النيل من شخص ما أو الثأر منه[3]. فمثلا قام أحد الخبراء الفرنسيين الذي يعمل في مجال نظم المعلومات ببعث قنبلة زمنية عبر الشبكة المعلوماتية الخاصة بالمؤسسة التي يعمل بها مما ترتب عليه إتلاف المعلومات المتعلقة بالمؤسسة بأجمعها، انتقاما لفصله منها .[4]

إن جريمة الكمبيوتر والإنترنت في السنوات الفارطة جريمة لا يصل إليها سوى المبرمج أو المستخدم المؤهل فنيا وتقنيا، ومع التطور المستمر وظهور الكمبيوتر الشخصي والهاتف

---

[1]– محمود رجب فتح الله ، الوسيط في الجرائم المعلوماتية ، المرجع السابق ، ص 93،94

[2]– محمود علي العريان، الجرائم المعلوماتية، المرجع السابق ، ص 62

[3]– زين العابدين عواد كاظم الكردي ، جرائم الإرهاب المعلوماتي دراسة مقارنة ، المرجع السابق ص 64

[4]– عبد الفتاح بيومي حجازي ، التجارة الالكترونية ، دار الفكر الجامعي ، الإسكندرية ، 2004 ، ص 42

النقّال أو الهاتف الخلوي الذي أصبح يعد أهم أشكال أدوات الاتصال التي وسعت نطاق وحجم المتعاملين مع الإنترنت ،أصبح من السهل التعامل مع الإنترنت[1].

وبالتالي يمكن القول أن الجرائم المرتكبة عبر الإنترنت بشكل عام تحتاج إلى قدر من المعرفة والدراية والذكاء والدهاء لارتكابها، إلى جانبها صفات خاصة تبعا للطبيعة المميزة لبعض جرائم الإنترنت والأغراض المراد تنفيذها [2]، ولكن في المقابل هناك عدة جرائم أصبحت لا تحتاج إلي قدر الذكاء والعلم اللذين كانت ترتبط بهم جريمة الإنترنت، وإنما تنفيذ الجريمة أصبح يستلزم القليل من المعرفة بتقنيات الحاسوب والإنترنت وكيفية التشغيل فقط لارتكابها، خاصة في بعض الجرائم التي لا تتطلب الذكاء الخارق.

الفقرة الثانية : الأنماط المختلفة لمجرم الإنترنت

يري البعض من الباحثون أن أفضل تصنيف في الوقت الحالي لمجرمي الإنترنت هو التصنيف الذي أساسه أغراض الاعتداء وليس الذي أساسه الطريقة الفنية التي يتم بها الاعتداء والوسائل المستخدمة فيه. وأفضل التقسيمات هي التي قسمت مجرمي الإنترنت إلى ثلاث فئات: المتسللون ، والكارهون والمحترفون ، وفصلت بين مجرمي الإنترنت الأحداث والبالغين.[3] وقد ذهب البعض الأخر إلي تقسيم مجرمي الإنترنت إلي المتسلل إلى الشبكة "الهاكر" ومخترقو الشبكات والمتسللين إلى النظـــم الخاصة بالاتصال الهاتفيPhreak ، ومخترقي الشبكات والنظم القليلين الخبرة Script Kiddies.[4]

وفي ظل هذه التقسيمات المتعددة والمتشابهة سنأخذ بالتقسيمات التي أخذت بعين الاعتبار كل الأشخاص القادرين على ارتكاب هذا النوع من الجرائم وذلك على أساس الربح المادي، أو تحقيق هدف شخصي، أو على أساس إثبات القدرات والتحدي، أو على أساس العمل لصالح منظمات أو جهات إرهابية أو العمل للصالح الذاتي. و لكن قبل التعرض

---

[1]– مدحت رمضان ، جرائم الاعتداء على الأشخاص و الانترنت ، دار النهضة ، القاهرة، 2000، ص 11

[2]–عرب يونس ، جرائم الكمبيوتر والانترنت ، المرجع السابق ، ص 266

[3] – David icove K Karl Serger ,Karl , williamVonstorch Computer Crime , O'Reilly and Associates , Inc K 1995 , p/70

[4] – https://www.neelwafurat.com/itempage.aspx?id=egb87928-5087895&search=books موسوعة الهاكرز ، تاريخ الاطلاع 12/8 /2018

لتصنيفات مجرم الإنترنت لابد من الإشارة إلي أن هذه التقسيمات لا تعني أن كل مجرم يدخل ضمن فئة محددة دون الفئات الأخرى التي سنذكرها لأنه يمكن أن يكون المجرم الواحد خليطا من مجموعة من الطوائف أو من طائفتين ... الخ.

أولا : التقسيم على أساس التحدي واثبات القدرات

1: المتسلل إلى شبكة الإنترنت "الهاكرز"

الهاكر هو شخص لديه مهارات يستخدم فيها أجهزة الكمبيوتر أو الشبكات أو غيرها من المعلومات لحل المشاكل التقنية. والهاكرز هو المتسلل ويدل في الواقع إلى شخص يستخدم مهاراته للوصول غير المصرح به إلى نظام أو شبكة لارتكاب جريمة معينة، وقد يقوم على سبيل المثال، بسرقة المعلومات بهدف إلحاق الأذى بالناس من خلال سرقة هويتهم أو بهدف الإتلاف أو بهدف إسقاط الأنظمة، وأحيانا ما يحتفظ بهذه الأنظمة كرهائن لطلب الفدية. ولقد كان مصطلح "المتسلل" تاريخيا مصطلحًا مثيرًا للخلاف، حيث يتم استخدامه في بعض الأحيان كمصطلح للإعجاب بالفرد الذي يتمتع بمهارات عالية بالإضافة إلى كونه مبدعًا في حل المشكلات التقنية. ولكن يتم استخدام هذا المصطلح بشكل شائع على الفرد الذي مهارته التقنية تستخدم لأغراض غير قانونية أو غير أخلاقية، إضافة إلى هذا قد يطلق علي هذا النوع من المجرمين مصطلح القراصنة للتعبير عنهم.[1]

فالهاكرز أيضا هو فرد ماهر في استخدام الكمبيوتر وفي التعامل مع الشبكات خاصة شبكة الإنترنت وهذه المهارات يستعملها للتغلب على مشكلة فنية، وهو خبير في اختراق أجهزة الكمبيوتر وبرامج الحماية بشكل قانوني بدافع الفضول، وهو في أغلب الأحيان شخص غير مؤذ، وهو شخص محب للتكنولوجيا وبالتعرف بتقنياتها الجديدة.[2]ويعرف على هذه الفئة بأنها فئة غير حاقدة أو تخريبية وإنما هدفها في اغلب الأوقات هو التحدي واثبات القدرات .[3]

---

[1]– https://searchsecurity. techtarget.com/definition/hacker, DEFINITION Hacker vu le 23/12 2018

[2]– Paul Taylor ,Hacktivisim in search of listethics , Crime and The Internet KEfited by David Wall k Routldge Taylor and Francid group ,1st Edition 2001, p56 .61

[3]– عرب يونس ، جرائم الكمبيوتر والإنترنت ، المرجع السابق ، ص268

أيضا هو شخص فضولي يفتخر بقدرته على خلق برامج جديدة وبمعرفته لكيفية عمل البرامج الالكترونية، فهو يستطيع نشر وإنشاء أجزاء صغيرة من الشفرة تسمى باتتشيز لإصلاح مشكل تعرض له و منعه من العمل بصورة صحيحة متداركا بذلك العلة التي أصابت البرنامج الذي يعمل عليه.

لقد استخدم مجتمع الأمن بشكل غير رسمي إشارات إلى لون القبعة كوسيلة للتعرف على أنواع مختلفة من المتسللين، أين تم تقسيمهم إلى ثلاثة أنواع: القبعة البيضاء والسوداء والرمادية.

يسعى أصحاب القبعة البيضاء المعروفون أيضًا باسم المتسللين الأخلاقيين إلى خدمة مصالح الناس، حيث يعمل العديد من قراصنة القبعة البيضاء من إجراء اختبارات الاختراق، ويتم توظيفهم لاختراق شبكات الشركات لإيجاد الثغرات الأمنية والتبليغ عنها.

أما متسلل القبعة السوداء فهو من يتعمد الوصول غير المصرح به إلى الشبكات والأنظمة بنية خبيثة سواء لمحاولة نشر فيروسات أو إتلاف معلومات بما في ذلك الحصول على سمعة سيئة. وعليه فإن قراصنة القبعة السوداء هم مجرمون ينتهكون القوانين للوصول إلى الأنظمة دون إذن، إضافة إلى هذا قد يشاركون في نشاط غير قانوني آخر كسرقة الهوية وهجمات الحرمان الموزعة من الخدمة.

أما متسلل القبعة الرمادية لا هم متسللين القبعة البيضاء ولا هم متسللين القبعة السوداء. ولكن دوافعهم قد تكون مماثلة لدوافع قراصنة القبعة البيضاء، إلا أن القبعات الرمادية أكثر احتمالا من قراصنة القبعة البيضاء للوصول إلى الأنظمة دون تصريح، في الوقت نفسه هم أكثر عرضة من المتسللين القبعة السوداء لتجنب إلحاق أضرار لا لزوم لها على الأنظمة التي تخترق، إلا أن قراصنة القبعة الرمادية قد يقومون بإصلاح الثغرات التي اكتشفوها من خلال أنشطتهم الخاصة غير المصرح بها بدلاً من استخدام معرفتهم لاستغلال الثغرات الأمنية من أجل الربح غير المشروع.[1]

ومن أمثلة الهاكر، الجزائري بن دلاج المبتسم الذي ألقي القبض عليه في مطار بانكوك بتايلاند أواخر عام 2013 بتهمة اقتحام أكثر من 217 بنكا عبر العالم. أُطلق عليه لقب

[1]–https://searchsecurity.techtarget.com/definition/hacker ، Types of hackers vu le 23/12/2018

"اللص المبتسم" لابتسامته أمام الشرطة وقت اعتقاله. وما زاد من شعبيته لدى العرب هو قرصنته لبعض المواقع الإسرائيلية وتقديم ما تحصل عليه من معلومات للمقاومة الفلسطينية.[1]

2: طائفة صغار السن Prankters

هم الأطفال المهووسين بالمعلوماتية وهم أشخاص دون سن الأهلية، دافعهم لاقتحام البرامج التحدي والتغلب على صعوبات وتقنيات الحاسوب، وقد يكون غرضهم أحيانا التسلية في اغلب الأحيان ونيتهم غالبا ما تكون بعيدة عن الإضرار بالآخرين.[2]

ثانيا: تصنيف المجرمين على أساس تحقيق الربح والانتقام

1: مخترقو الشبكات أو القراصنة المحترفون Cracker

بالنسبة للكثيرين في مجال التكنولوجيا، يتم تطبيق مصطلح "المتسلل" لأولئك الذين يستخدمون مهاراتهم دون نية خبيثة، ولكن مع مرور الوقت ظهر نوع أخر من الأشخاص الذين يستخدمون مهاراتهم بشكل ضار، لذلك تم اقتراح مصطلح المخترقين للقراصنة المجرمين، ويستعمل أيضا مصطلح المفرقع السيبراني للتعبير عن هذا النوع من المجرمين، وكلها مصطلحات تفيد كلمة كاكر **(Cracker)** والكاكر هم أولئك الذين يسعون للتعرف على العيوب في أنظمة الأمن والعمل على تحسينها، بما في ذلك خبراء الأمن المكلفون بتحديد العيوب في الأنظمة وإصلاح الثغرات الأمنية، ويقوم هؤلاء من ناحية أخرى باختراق أمن الكمبيوتر والشبكات لاستغلال هذه العيوب ذاتها لتحقيق مكاسب خاصة بهم.[3]

فالكاكر مثل الهاكر في الصفات ولكن جل اهتماماته منحصرة في سرقة البرامج ومواقع الإنترنت بوضع الفيروسات في المواقع التي يتم اختراقها بكسر حواجزها الأمنية بهدف

---

[1] – القصة الحقيقية لأحد أخطر الهاكرز الجزائري حمزة بن دلاج: العربي الجديد الموقع https://www.alarby.co.uk , vu le 15/9/2017

[2]– نائلة عادل قورة ، جرائم الحاسب الآلي الاقتصادية ، المرجع السابق ، ص 61

[3]–https://searchsecurity.techtarget.com/definition/hacker ، The Crackers vu le 23/12/2018

الوصول غير المشروع إلي الشبكة أو النظام المعلوماتي.[1] فهي فئة من الأشخاص تعكس اعتداءاتها عن ميولات إجرامية خطيرة، فهم فئة تتميز بالتخريب وحذف أو إضافة المعلومات أو الدخول إلي مزودات خدمة الإنترنت والتلاعب بمحتوياته أو الاستيلاء على أرقام بطاقات الائتمان لأغرض منفعية.[2] بالإضافة إلى العديد من الأعمال الغير مشروعة التي يقوم بها الكارز من أجل مصالحه الشخصية أو بقصد الانتقام.

2: الحاقدون

هم فئة من المجرمين الساخطين إما على شركائهم في العمل وإما على المؤسسات التي يعملون بها، وهدفهم من الأعمال الغير مشروعة ليس الربح المادي أو إثباتهم لقدراتهم وإنما التخريب وتحقيق الضرر، ويكون ذلك من خلال نشر البيانات أو مسحها بهدف الثأر والانتقام، واغلب نشاطاتهم الإجرامية تقوم على أساس استخدام الفيروسات الضارة لإتلاف أو التعطيل للنظم والمعطيات.[3]

ثالثا : المجرمين على أساس العمل لصالح المنظمات

1: المجرمون المحترفون Carer Criminal

المحترفون هم طائفة من الناس يعملون في مجال الجريمة المنظـمة عبر الحاســـــوب والإنترنت وهدفهم أعمالهم الغير مشروعة وتحقيق الربح المادي.[4] وهذا النوع من المجرمين يتمتعون بمهارات ومعرفة كبيرة بتقنية المعلومات ويعتبرون من اخطر مجرمي التقنية لخطورة الأعمال التي يقومون بها، ويصنف هؤلاء تبعا لنوع الجريمة المرتكبة والوسيلة

---

[1]– Patrick V Eecke, Jos Dumortier,Legal issue and the internet , Internet Européen Compared Law xv th International Congrès of comparative Law , Bristol , 26 Juil–1 aout 1998 , Bruxelles, 2000, p161

[2] – اهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان، دار الجامعة الجديدة ،الإسكندرية، 2007، ص 135

[3] –B Streling ,Thje Hacker Crackdown , Law and Electronic Fointer, London Viking , 1993 , p 35 36

[4] –Peter Graaposky , Russell Smith , Gillian Dempsey , Eliectronic Theft, , Unlawful acquisition in cyberspace , Cambridge university press , 1st publishd, 2001 , p198 ,199

المستخدمة في ذلك ، كالتجسس لحساب منافسين أو لصالح جماعات إرهابية أو لمصالح بعض الدول أو لمصالح سياسية.[1]

2: مجرمون المعتقدات والأفكار الخاصة

هم فئة من المجرمين تتغلب عليهم أفكار خاصة إما سياسية أو دينية وعادة ما يلجئون إلي الإجرام ضد الممتلكات من أجل لفت الانتباه إلى وجهات نضرهم ومطالبهم، ومن أهم الجرائم التي يقومون بها هؤلاء هي الاعتداء على أنظمة الحاسوب الدولية في ظل التطور التكنولوجي الحالي ومن أهم هذه الأعمال ما يخص الشؤون العسكرية كأنظمة المفاعل النووي أو أنظمة الخطط العسكرية وغيرها من الأنظمة السرية.[2]

رابعا : المجرمين القليلين الخبرة Script Kiddes

وهم طائفة من الأفراد الذين لا يتمتعون بمهارات ومعرفة كبيرة بتقنية المعلومات ويستخدمون ما توصـــل إليه الهاكر من المعلومات وبرامج لاستخدامها فـي الاختراق، ولكن لا يستطيعـــــون التوصل لاكتشاف الثغرات الموجودة في البرامج لعدم معرفتهم بها، فهم يقومون بتطبيق ما هو موجود فقط.[3]

وانطلاقا من ما سبق يمكن القول أن مرتكبي جرائم الإنترنت لا يصنفون ضمن خانة أو طبقة معينة أو فئة أو جنس معين فقد يكون بالغا أو حدثا، فقيرا أو غنيا، رجلا أو امرأة، بطال أو عاملا، طالب أو عالم. إضافة إلى هذا هدف أو غاية ارتكاب الجريمة تختلف من مجرم إلى أخر تبعا لرغباته وميوله، فقد تكون سياسية أو إرهابية أو مادية أو لمجرد إثبات المهارة، أو من أجل الانتقام، أو لتسخير قدراته التقنية لصالح عصابات لجني المنافع.

الفقرة الثالثة : الدوافع من ارتكاب جرائم الإنترنت

إن الدوافع والأسباب التي تدفـع بالجاني لارتكاب هذا النوع مـــن الجرائم هي الحـــب والرحمة والكراهية والانتقام وكســب المال، وكلها عوامل دافعة لإرادتـــه التي تحدد سلوكه الإجرامي وهي قوى نفسية توجه الرغبة في ارتكاب جرائم معينة لتحقيق أهداف محددة.

---

[1] – حسين طاهر داوود ، جرائم نظم المعلومات ، الرياض ، طبعة 1 ، 2000، ص75 و76

[2] – Michael Smith, International Review of the Red Cross: Humanitarian Dialogues in Law, Politics and Humanitarian Action, 2002, p. 88

[3] – حسن مظفر الرزو، الامن المعلوماتي: معالجة قانونية ، مجلة الامن والقانون ، اكادمية شرطة دبي ، عدد1 ، 2004 ، ص200

وبالتالي فإن الأسباب والدوافع التي تدفع المجرمين إلى ارتكاب أعمال غير مشروعة عبر الإنترنت تختلف عن الأسباب والدوافع التي تشجع المجرمين على ارتكاب الأعمال التقليدية الغير مشروعة[1]، وقد تكون أسباب ودوافع الجرائم عبر الإنترنت أساسا الرغبة أو الهواية في جمع المعلومات التي يمكن تخزينها على جهاز كمبيوتر وإرسالها عبر شبكات المعلومات العالمية، إضافة إلى الرغبة في إيذاء الآخرين. والرغبة في الربح السهل[2] الذي قد يؤدي إلى الهجمات على أجهزة الكمبيوتر وأنظمة المعلومات، بالإضافة إلى دوافع المجرم الشخصية لإظهار نفسه. وسنذكر بعض هذه الأسباب والدوافع فيما يلي:

أولا :الرغبة في جمع المعلومات وتعلمه

أولئك الذين يرتكبون هذه الجرائم يفعلون ذلك للحصول على معلومات جديدة. وقد أكد البروفيسور ليفي في كتابه عن أنظمة القرصنة أن أخلاقيات قراصنة الإنترنت تقف على مبدأين أساسيين.:

الأول: يمكنك معرفة كيفية سير العالم من خلال الدخول في أنظمة الكمبيوتر.

الثاني: "يجب أن يكون جمع المعلومات خاليًا من القيود."[3] ووفقا لوجهة نظرهم، يجب أن تكون جميع المعلومات المفيدة بشكل عام خالية من القيود، وبالتالي يجب أن تكون هناك حرية في نسخها وجعلها مناسبة للاستخدام الشخصي. وعادة ما يوضح المتسللين أن هدفهم الوحيد من الوصول إلى المعلومات هو اقتحام الشبكات الإلكترونية وأجهزة الكمبيوتر من أجل التعلم فقط. ويتشاركون المعلومات والخبرات، ويستخدمونها في أنشطة هادفة، حتى لو تم ذلك بطرق غير قانونية[4].

---

[1]–عبد الله حسين آل حجراف القحطاني ، تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية دراسة تطبيقية في هيئـــة التحقيق والادعاء العام بمدينة الرياض، رسالة ماجستير، الرياض، 2014 م، ص 32

[2] – Dorothee ay Dying ، قراصنة أنظمة الحاسب الآلي ، المؤتمر القومي الثالث عشر لأمن الحاسب الآلي ، سنة 2002 ، ترجمة ، أمنة علي يوسف ، ص 11

[3]– حسين بن سعيد الغافري ، جهود سلطنة عمان في مواجهة الجرائم المتعلقة بشبكة الانترنت، ص4 ، الموقع التالي http://hussain-alghafri.blogspot.com / اطلع عليه في 11/5 /2016

[4]– حسين بن سعيد الغافري ، المرجع السابق ص4 . وأنضر أيضا محمد على القرى ، السرية في العمليات المصرفية : مفهومها وضوابطها ، مقال منشور على الموقع: http// :www.elgari Article 67.htm –68k.com

ثانيا :الاستيلاء على المعلومات.

إن القيام بارتكاب الجريمة للوصول إلى المعلومات نفسها والاستحواذ عليها باستعمال الإنترنت والتصرف فيها إما تعديلها أو حذفها أو إلغائها بشكل دائم. وتختلف أسباب هذا السلوك من شخص لآخر، فمن الممكن أن يكون لأغراض تنافسية أو تحرش أو لتحقيق مكاسب مالية، وغالباً ما يكون هدفها الأساسي اقتصادياً أو سياسياً .

ثالثا :دافع التحدي والتفوق على الوسائل التقنية.

وقد يكون الهدف من ارتكاب هذا النوع من الجرائم هو الاستيلاء على النظام وإظهار قدرة المجرم وتفوقه على تعقيد وتطور الأدوات التكنولوجية الحديثة. وبعبارة أخرى بدافع التحدي واثبات القدرات، حيث يمضي الجاني كل وقته أمام أجهزته للتغلب على التشفير الأمنية واختراقه بغرض إثبات مهارته وقدراته ومن أجل تحدي كل التطورات في مجال تكنولوجيا التشفير[1].

رابعا: دافع إلحاق الأذى بالأشخاص والمنشئات

إن ارتكاب هذه الجرائم من خلال شبكة الكمبيوتر العالمية وتقنيات المعلومات عادة ما تكون بهدف أذى أشخاص أو جهات معينة. وغالبًا ما يتم توجيه مثل هذه الجرائم في شكل سب أو قذف أو تهديد أو ابتزاز، كما يحصل عادة في القضايا التي يقدم فيها الجاني بالسطو على البريد الإلكتروني لبعض الفتيات والحصول على صورهن الشخصية بطرق غير شرعية بغرض نشرها على شبكة الإنترنت عبر المواقع التي توفر هذه الخدمة، ويمكن أن تتم هذه الجرائم بطريقة غير مباشرة، حيث يمكن الحصول على المعلومات والبيانات المتعلقة ببعض المنظمات والأفراد ومن ثم استخدامها في جرائم مباشرة[2]. وكما يمكن أن يكون ذلك بواسطة نشر عبارات القذف والتشهير ضد شخص معين عن طريق موقع التواصل الاجتماعي مثلا الفيس بوك قصد المساس بشرفه واعتباره.

ويمكن أن يكون الدافع أيضًا لارتكاب الجريمة هو تعرض أحد الكيانات للخسارة والأضرار من جراء الهجمات على أنشطته. على سبيل المثال، أعلنت شركة

---

[1]– Dorothee ay Dying، قراصنة أنظمة الحاسب الآلي ، مرجع سابق ، ص 11

[2]–حسين بن سعيد الغافري ، جهود سلطنة عمان في مواجهة الجرائم المتعلقة بشبكة الانترنت، المرجع السابق، ص 4

Monster.com ، وهي شركة بريطانية ذات سمعة طيبة متخصصة في التوظيف عبر الإنترنت في المملكة المتحدة في 27 يناير 2009 أن قاعدة بياناتها قد تعرضت للهجوم من قبل متسلل وأن قاعدة البيانات بها نصف مليون مستخدم، بما في ذلك الأسماء والعناوين وأرقام الهواتف والبريد الإلكتروني، وأن هذه البيانات يتم استخدامها من قبل المتسللين لتزوير واستخدام بطاقات هوية المستخدمين.[1]

خامسا: دافع تحقيق الأرباح والمكاسب المالية

إن العديد من الجرائم السيبرانية ارتكبت بهدف مادي، مثل استخدام الإنترنت لدعم الأنشطة الإجرامية مثل الاتجار بالمخدرات والبشر. وقد ورد في بعض الأبحاث لمكافحة جرائم الإنترنت أن عصابات الإجرام المنظم استغلت التكنولوجيا الحديثة في تسيير شؤون التجارة الغير مشروعة بصفة عامة وخاصة من بينها جريمة التجارة في البشر. وقد لوحظ في بعض التحقيقات الخاصة بمكافحة الجرائم الإلكترونية قيام العصابات الإجرامية المنظمة باستغلال التكنولوجيا الحديثة لتسهيل المعاملات التجارية غير المشروعة بشكل عام، وجريمة الاتجار بالبشر بشكل خاص، هذه الأخيرة التي يصنفها الباحثون كتجارة إلكترونية إذا ما وقعت باستخدام الإنترنت، لأن التجارة عبر الإنترنت هي المعاملات التي تتم عبر شبكة الكمبيوتر العالمية المتمثلة في الإنترنت[2].

فالسعي وراء الربح المادي سواء السرقة أو غيرها من طرق تحقيق الربح هو الدافع وراء العديد من جرائم الانترنت[3]، فقد يقوم الجاني بتصميم مواقع وهمية لبيع بعض الأشياء ويقوم المستخدمين بالإقبال على هذا الموقع وشراء احتياجاتهم منه وتحويل الثمن إليه وبعده يتضح للمجني عليهم أنه موقع وهمي ولا توجد أية بضائع به .

والدافع المالي عادة ما يكون سببه معاناة الكثير من الشباب من المشاكل المالية والبطالة مما يؤدي بهم إلى إتباع أساليب غير قانونية، والتسلل لقواعد بيانات المؤسسات المالية والاستيلاء عليها، وارتكاب جرائم الاحتيال على شبكة الإنترنت باستخدام عدة

---

[1]– Cyber Criminal are adaptingthertactis to traget people wormien about ther finances and job security during the finzncialcrisis, experts have Warndt .http// : www.mxlogic.com .Vu le 15/06/2018

[2]–حسين بن سعيد الغافري ، جهود سلطنة عمان في مواجهة الجرائم المتعلقة بشبكة الانترنت، المرجع سابق، ص5

[3]– نائلة عادل قورة ، جرائم الحاسب الآلي ، المرجع السابق ، ص 590

أساليب، كبرامج التجسس، والبريد الالكتروني، ولقد أصبحت هذه الأدوات سهلة الاستخدام خاصة في ظل الانتشار الواسع للمنتديات التي تشرح شرحا مفصلا طرق الاختراق والتجسس، وهذا يضر بشكل خطير بتطبيقات التجارة الإلكترونية الحقيقية، خاصة في البلدان العربية التي تم حجبها من المواقع العالمية للمعاملات الإلكترونية نتيجة لانعدام الثقة والسياسات السليمة لمكافحة الجرائم المعلوماتية[1].

سادسا: دافع تهديد الأمني القومي والعسكري.

هناك العديد من الجرائم المرتكبة عبر الإنترنت أصبح هدفها الأساسي في وقتنا الحالي هدف سياسي ويتمثل في تهديد الأمن الدولي، ومن هنا وكما هو الحال في الدول المتقدمة إلكترونيا، نشأ ما يسمى بالتجسس عبر الإنترنت والإرهاب إضافة إلى حرب المعلومات.

المبحث الثاني: الطبيعة الخاصة لجرائم الإنترنت

جرائم الإنترنت ظاهرة إجرامية من نوع خاص وذات طبيعة قانونية خاصة تتعلق بالقانون الجزائي المعلوماتي، الأمر الذي يجعلها ذات صفة خاصة وهي اختصارها علي سلوك غير مشروع يقتصر على الاعتداءات الموجهة ضد المعلوماتية التي ترتكب عن طريق الدخول إلي الشبكة الدولية المعروفة بالإنترنت[2]. وجريمة الإنترنت "هي كل سلوك غير مشروع مرتبط بالحاسوب والإنترنت ويتسبب في إلحاق الخسائر المادية والمعنوية بالضحية ومن جهة أخرى مقابلة تؤدي إلى إمكانية حصول الجاني على مكاسب مادية ومعنوية أيضا ".[3]

إن جرائم الإنترنت قد تقع على المعلومات والبيانات والكيانات المنطقية كالبرامج التطبيقية وبرامج التشغيل، وبالتالي قد يكون هدفها الوحيد هو النظام المعلوماتي ومكوناته المعنوية، وبمعنى أخر تكون المعلومات هي موضوع الجريمة ومحلها في أن واحد، فالجريمة هنا هي كل سلوك يمس بالمعلومات المخزنة والمعالجة في نظام الكمبيوتر

---

[1]– صالح عطاالله ،الجرائم الالكترونية والمعلوماتية ، مجلة شمس المستقبل ، اطلع عليه في 2017 /3/24
http://newssparrow.blogspot.com/2013/01/blog-post_29.html

[2]– Vivant et autres – Informatique et droit pénal – les bien informatique objets de fraude Lamy informatique –1991– n3445–p151

[3]–Tiefemann fraude et autres délits D'affaires commis a l'aide ordinateurs électroniques RFPC–1984–N7–p61

والمتبادلة عبر شبكات الاتصال.[1] وعليه سنتناول الطبيعة القانونية الخاصة بجرائم الإنترنت من خلال دراستنا هذه من خلال تناول الوصف القانوني للوسائل التقنية لحماية شبكة الإنترنت كمطلب أول وبعده الوصف القانوني لجريمة الإنترنت في مطلب ثاني .

المطلب الأول: الوصف القانوني للوسائل التقنية لحماية الإنترنت

يشوب شبكة الإنترنت الكثير من العيوب في دفاعاتها، وهذا راجع لأخطاء البرمجة والعيوب في تصميم النظام الأمر الذي يؤدي إلي إمكانية الوصول إلى ما تحزنه من معلومات وبرامج وكل ما له علاقة بالدخول إلى الشبكة من قبل أي شخص دون سابق إنذار، كما إن الأخطاء في خادم الويب يسمح بدخول المستخدمين الغير المصرح لهم عن بعد إلى كل ما هو سري الأمر الذي يسمح بحدوث اختراقات.

وكما عرفت جرائم الإنترنت تطورا كبيرا في طرق ارتكابها، فإن التقنيين عبر العالم يعملون ليل نهار على تكوين برامج تعمل على حماية المستخدم وخصوصيته من الاختراقات ومن مختلف الجرائم من خلال وسائل الحماية المادية المتمثلة في البرامج المتمثلة في التشفير وتنقية المعلومات والبرامج التي تزداد تطورا يوما بعد يوم.

لذلك سنتناول من خلال هذا المطلب الحماية التقنية المشرعة قانونا من جرائم الإنترنت وذلك من خلال تقسيمه إلي فرعين: يتناول الفرع الأول التشفير والثاني نتناول فيه تنقية المعلومات والبرامج.

الفرع الأول: التشفير

لقد تم استخدام التشفير في فترات الحروب قبل الميلاد لحماية الرسائل من أيدي العدو خاصة الرسائل الحساسة، ولقد تم تطوير القياسية خوارزمية من طرف يوليوس قيصر والتي عرفت باسم تشفير قيصر، والتي كانت عبارة عن نص مشفر يستخدم لتأمين مراسلاته ثم تطورت إلى عدة أنواع [2] .

---

[1]– ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، رسالة مقدمة لنيل شهادة دكتوراه، كلية الحقوق والعلوم السياسية ، قسم الحقوق ، باتنة ، ص 26

[2]–Verton F 2001 technologyVendorsDetail Plans To Share Security Information Computerworld – http//www.computerworld.com/cwi/story/0-1199 – NAV47-STO56410-00 -html- vu le 2018-06-22

التشفير هو عملية تغيير البيانات من شكلها الأصلي بحيث لا يتمكن الآخرون من قراءة محتوياتها أو الوصول إليها، وتتم عملية التشفير باستخدام برامج خاصة مثل أداة فك التشفير أو كلمة المرور، لتصبح البيانات قابلةً للقراءة مرة أخرى[1]، ويعدّ التشفير معقّدًا للغاية مما يجعله صعب الاختراق، ولقد أثبتت برامج التشفير صمودها أمام محاولات كسر التشفير لا سيما مع انتشار الهاكرز وسرقة المعلومات الشخصية عبر العالم. ومن خلال دراستنا سنقوم بشرح التشفير من الناحية التقنية ثم نتعرض إلى الوصف القانوني للتشفير.

الفقرة الأولى : مفهوم التشفير

تمر الرسائل الإلكترونية والمعلومات عبر الإنترنت بالعديد من الخوادم في شكل صور متتابعة حتى تصل إلى المستهلك النهائي، والخوادم تقوم على عمل نسخة مؤقتة من محتواها، الشيء الذي يجعلها عرضة إلي التطفل واطلاع الغير على محتواها، لذلك بات من الضروري إيجاد حلول فنية تحمي الرسالة وتضمن سريتها، ومن هنا ظهرت تقنية التشفير كوسيلة لإخفاء رسالة البيانات وحمايتها.[2]

وطالما كانت صناعة التشفير حكرا على النواحي العسكرية والدبلوماسية خاصة في الولايات المتحدة وفرنسا وكانت تفرض عليه نظاما قانونيا صارما لتصديره للخارج، إلى أن بدأت بتحرير قطاع التشفير شيئا فشيئا إلى أن تزايدت قوة التشفير عبر أنحاء العالم[3]. وبالرغم من إيجابية التشفير على الصعيد العملي والاقتصادي والتجاري إلا أنه أصبح يستغل من طرف المجرمين لتمرير عملياتهم الإجرامية، ومن هنا سنتناول تعريف التشفير أولا وأنواعه ثانيا.

أولا : تعريف التشفير

يعرف التشفير بأنه" عملية تتضمن تحويل النص العادي إلى نص مشفر لمنع الوصول غير المصرح به إلى المعلومات، بالإضافة إلى عملية تحويل البيانات إلى معلومات

[1]– Encrypt، من موقع www.computerhope.com vu le 2018-4-5

[2] – فاروق حسين ،أمن الإنترنت ، دار الراتب الجامعي ، بيروت 1999، ص 91،93

[3]–Thoumyrel L– les enjeux de la cryptographie une analyse compare des des enjeux de la cryptographie au canada et etatas unis– www.juriscom.net vu le 22/05/2016

مجهولة مكتوبة في كود غير قابل للقراءة".[1] ومن المعهود أن شبكة الإنترنت أصبحت أكبر وسط للتواصل ونقل المعلومات، وعليه وجب تشفيرها للحفاظ عليها من المخربين والمخترقين. وتعمل المفاتيح على تشفير الرسالة، وتعتمد هذه المفاتيح على عمليات حسابية معقدة. [2] وفك التشفير هو عملية تحويل البيانات إلى شكلها الأصلي باستخدام مفاتيح فك التشفير المناسبة.[3]

وانطلاقا من تبني التشريعات لنظام التشفير كآلية تقنية ضرورية لحماية مختلف المعاملات اعتمد المشرع الجزائري، كأغلب القوانين الأخرى، التشفير كآلية لضمان أمن المعلومات ولتوفير الحماية التكنولوجية.

لذلك بالرجوع إلي القانون رقم 15-04[4]المتضمن القواعد العامة لتوقيع والتصديق الإلكتروني نجد أن المشرع ومن خلال الفصل الثاني أورد مصطلح التشفير، ففي المادة 2 الفقرة 3 منه المعنونة بـ : بيانات إنشاء التوقيع الالكتروني والتي عرفتها بأنها: رموز أو مفاتيح التشفير العمومية، والرموز المميزة أو المفاتيح الخاصة، يستخدمها الموقع لإنشاء توقيع إلكتروني. وبالرجوع للمادة فإن مفاتيح التشفير العامة أو الخاصة تستخدم لإنشاء التوقيع الإلكتروني.

كذلك الفقرة الخامسة من نفس المادة [5]، والتي جاءت تحت عنوان بيانات التحقق من التوقيع الإلكتروني لم تحمل أي تعريف لنظام التشفير لذلك يمكن القول بأن:

---

[1]- National Institute of Justice. Justnet- Justice Tecgnology Information Net – work .http//www.nlectc.org/assistance/justenet.html.vu le 15/10/2

[2] – David Thompson- Computer Crime and Security Survey- Information Management and Computer Security- 1998 ,p.78

[3]- Maher L ,Provingyour computer Security , www.certconf.org . Vu le 23/07/2016

[4]- القانون رقم 15-04 المؤرخ في 11 ربيع الثاني من عام 1436 الموافق لـ 1 فبراير سنة 2015 المتعلق بقواعد العامة للتوقيع والتصديق الالكتروني، جريدة الرسمية ، عدد 06 ، ص1

[5]- المادة 5/2 من القانون رقم 15- 04 "رموز أو مفاتيح التشفير العمومية أو أي بيانات أخرى مستعملة من اجل التحقق من التوقيع الالكتروني"

المشرع الجزائري لم يأت بتعريف واضح للتشفير بل اعتبره من بيانات إنشاء التوقيع الإلكتروني،[1] وهذا رجوعا لنص المادة 2 من الفصل الثاني الفقرة 3، أما في الفقرة الخامسة فهي خاصة باعتماد التشفير من بيانات التحقق من التوقيع.

وإذا دققنا في نص المادتين نجد وكأن المشرع فرق لنا بين نوعين من مفاتيح التشفير الخاصة التي ينشئ من خلالها التوقيع الالكتروني، كذلك مفاتيح التشفير العمومية التي تستعمل من أجل التحقق من هذا التوقيع. ولهذا يمكننا القول بأن على المشرع أن يضيف مادة إلى هذا الفصل لإعطاء تعريف للتشفير ذلك أنه لا يمكن أن يورد لنا نوعي هذا النظام ولم يعطي مفهوما له.

ثانيا :أنواع التشفير

يعتبر التشفير إحدى الوسائل التقنية الهامة في عصر تكنولوجيا المعلومات. وتصنف تقنيات التشفير إلى فئتين رئيسيتين فهناك تلك التي تستخدم المفتاح الخصوصي وتسمى تقنية التشفير المتماثل، وهناك التقنية التي تستخدم المفتاح العمومي وتسمى تقنية التشفير اللامتماثل.

1 – التشفير المتماثل

يستخدم التشفير المتماثل مفتاحًا سريًا واحدًا لتشفير البيانات وفك تشفيرها. وأساس هذا النوع من التشفير هو وظيفة المفتاح السري، ويمكن لأي شخص لديه المفتاح تنزيل وقراءة محتويات الرسائل أو الملفات، فعلى سبيل المثال، إذا أراد شخص ما إرسال رسالة سرية إلى طرف أخر، فهو بحاجة تأمين المفتاح لأنه إذا تلقى المفتاح أو عبارة المرور طرف ثالث يمكن له قراءة كل الرسائل المشفرة المرسلة بين الطرفين. ويمكن أن تحتوي كلمات المرور على رموز أو أحرف صغيرة أو كبيرة، ويقوم برنامج التشفير بعد ذلك بتحويل كلمة المرور إلى رقم ثنائي وإضافة أحرف إضافية لزيادة الطول،[2] وبالتالي فإن الأرقام الثنائية

[1]– التوقيع الالكتروني: هو إمضاء يوضع على محرر ويكون لو طابع منفرد يسمح بتحديد شخص الموقع وتمييزه عن غيره. انضر: حسام محمد نبيل الشنراقي ، الجرائم المعلوماتية، دراسة تطبيقية مقارنة عن جرائم الاعتداء على التوقيع الالكتروني، دار الكتب القانونية، دار النشر والبرمجيات، ، مصر، 2013 ، ص43

[2]– O’Brien – Managment Information Systems – J.a.5th ed. 2001– p 380

هي مفتاح التشفير. وعند تلقي رسالة مشفرة، يقوم المستلم بفك تشفير النص المشفر باستخدام نفس عبارة المرور، ويكرر البرنامج عبارة المرور لإنشاء مفتاح يحول نص الرسالة المشفرة مرة أخرى إلى شكله الأصلي والمفهوم. [1] والتشفير المتماثل يعتمد على معيار "دي"[2] ، وهذا النوع من التشفير عديم الفائدة كونه تشفير يشوبه العديد من الثغرات مما أدى إلى تراجُع استخدامه.

2 – التشفير الغير متماثل

وهو تشفير يسمى أيضا بالمفتاح العام Public Key، والذي يتم استخدام فيه نوعين من المفاتيح مفتاح العام ومفتاح خاص .[3] فالمفتاح الخاص معروف للمرسل فقط، والهدف منه تشفير الرسائل. وبالنسبة للمفتاح العام فهو مفتاح العديد من الأشخاص أو الأطراف. ويمكن للمفتاح العام فك تشفير الرسائل المشفرة بالمفتاح الخاص، لكن في المقابل لا يمكن استعمال المفتاح العام لفك تشفير الرسائل المشفرة بنفس المفتاح، والشخص الوحيد الذي يمكنه فك تشفير الرسائل المشفرة بالمفتاح العام هو مالك المفتاح الخاص.[4]

فالمفتاح العام يعتمد في تشفيره على نظام Rsa، هي خوارزمية تشفير المفتاح العام، وهي مناسبة لكل من التوقيع والتشفير. ولقد كان هذا أحد التطورات الرئيسية الأولى في التشفير باستخدام مفتاح عمومي يستخدم RSA وهو تشفير لا يمكن اختراقه طالما كان طول المفتاح طويل جدا[5].

---

[1] – Henry B Computer and Security – El Sevier Science –Ltd–p.26

[2] – إن معيار تشفير البيانات بالإنجليزية Data Encryption Standard :وهو بالإختصار DES وهي خوارزمية مفتاح متناظر ساد لفترة ماضية لتشفير البيانات الإلكترونية. وكان لها تأثير كبير في النهوض بأساليب التشفير الحديثة في العالم الأكاديمي. أنضر عبد الرحمن غسان زعرور، شرح خوارزمية التشفيرDES ، مكتبة النور ،حمص سوريا، 2008 ، ص 18

[3] – Straub.D , Carlson P and Jones E , Deterring Highly Motivated Computer Abusers , A Field Experiment In computer Security. In G. Gable and Caelli , IT Security , the Needs For International Cooperation Amsterdam, Elsevier Science Publishers , 1992, p 309.320

[4] –وسيم شفيق الحجار، الإثبات الالكتروني ، المنشورات الحقوقية، بيروت ، 2002، ص 191

[5]–Calderbank Michael, Le cryptosystème RSA: historique, algorithme, avantages , www.theses.fr,vu le 08–02–2015

وبالرغم أنRsa يعتبر النظام DES الأكثر أمنا إلا أنه يتصف بالبطء لأن التشفير وفكه يستوجب وقوعهما في نفس الوقت. ونظام RSA من الأنظمة الممكن اختراقها إذا ما توفرت الوسائل المساعدة على ذلك. ولهذا السبب طور التقنيون نظام PGP الذي يُعتبرُ أحسن نموذج متطور لنظام RSA ويتم استخدمه PGP مفتاحا يبلغ طوله مئة وثمانيـــــة وعشرون بت، مع استخدام البصمة الإلكترونية للرسالة.[1]

وفي إطار اتخاذ نظام التشفير من طرف كافة التشريعات كآلية تقنية ضرورية لحماية مختلف المعاملات فقد كان من الضروري أن تضع نصوصا من أجل إنجاح هذه العملية.

وهذا أيضا ما انتهجه المشرع الجزائري إذ تطرق إلى تعريف المفتاح العام من خلال المادة 2 الفقرة 9 مفتاح التشفير العمومي.[2]

والمشرع الجزائري قد فرق بين المفتاح الخاص والمفتاح العام المستخدمان في عملية التشفير فمن خلال التعريف السابق فالمفتاح العمومي يكون في متناول الجميع أي عكس المفتاح الخاص الذي يجب أن يكون سريا لا يعلمه إلا صاحبه.

أولا :الإطار القانوني للتشفير

إن استخدام التشفير كتقنية في نطاق المعلومات والبيانات يكون بواسطة جهات مختصة، ذلك أن مستوى من مستويات التشفير السابقة يحقق درجة من أمان عالية، ومع ذلك تقوم الجهات المختصة على تأمين معلوماتها وبياناتها باستخدام أكثر من مستوى للتشفير لضمان درجة أعلى من السرية ولكي يحدد هذا الهدف يجب أن تخضع البرامج والتقنيات المستخدمة في عملية التشفير إلى جهة معينة وهذا ما سنتطرق إليه من خلال دراستنا لنظام التشفير في القانون المقارن والتشريع الجزائري.

1: التشفير في القانون المقارن

أ – موقف المشرع الفرنسي

لقد مر القانون الفرنسي المتعلق بالتشفير بمرحلتين :

---

[1].clark R , Technology Criminel and Crime Science ,European Journal on Criminal Policy and Research ,10 p 55 .63

[2]– أنضر المادة 2، الفقرة 9 من القانون 04/15

المرحلة الأولى وهي مرحلة التحرير المشروط، إذ اعتبرت خدمة التشفير كأداة حرب، وتخضع لمبدأ المنع، مما أدى ببعض الفقهاء إلى نقد هذا الموقف، وهو ما أشار إليه الفقيه هويتما في كتابه الله خلق الإنترنت (le Dieu créa L'internet)[1].

وفي 29 ديسمبر 1990 صدر القانون الفرنسي المتعلق بتنظيم الاتصالات وظهر معه نظام جديد لا يخضع إلا لتصريح مسبق وكان استعمال هذه الوسائل لا يهدف إلا إلى استثبات المعلومة أو تأسيس سلامة الرسائل المحالة وبمقتضى هذا القانون يكون التشفير قد خرج من الإحاطة الكاملة للحكومة الفرنسية، وخفف القيود المفروضة على استخدام الأدوات التشفيرية، وقد سمح للمشاريع الخاصة باستعمال أدوات التشفير بعد اقتصاره على القطاعات العسكرية وعلى الحكومة، وخفف القانون القيود المفروضة على التشفير بسبب الحاجة إلى المعاملات المالية وإلى تقنيات ذات طبيعة معنوية لها قيمة اقتصادية معادلة للقيمة المالية كمعاملات البيانات الاسمية والشخصية الإلكترونية. [2]

وهذا القانون جاء نتيجة تطور المعاملات المعلوماتية وكان من الضروري تطوير التشريعات ذات الصلة خاصة تلك المتعلقة بضمان سرية تمرير أرقام بطاقات بنكية وبما يحيط بها من خطورة قرصنتها.

وفي عام 1996 ظهر القانون المتعلق بالاتصالات واعتمد تنظيما حديثا لا يوجب أي تصريح مسبق إذا كانت وسائل التشفير تمكن من تأمين الاستثبات وتمكن من تأمين سرية الرسائل. وبالرغم من هذا التطور في تحرير التشفير إلا أنه لم يسلم من الانتقاد واعتبر القانون الأكثر صرامة في العالم ككل.[3] ومن ثم قام المشرع الفرنسي بتحرير نظام التشفير ودعمه بالأمر عدد199 بتاريخ 17 مارس 1999 مواكبا عبره لتطور قدرات الحاسوب، فإذا تجاوزت حدود 40 بيتس وأقل من 128 بيتس، فإن التشفير لا يخضع لأية شكلية

---

[1]–Thierry Piette Coudol ,Andre Bertrand , Internet Et La Loi , Dalloz, 1997, p 141

[2]– A. Bensoussan ,Cryptologie et Signature Electronique , aspects juridique , Hermès Science , Publication , paris, 1999, p 29.30

[3]–FeralSchul ,cyberdroit, leFroit a L'epruve De L'internet , Dalloz, 3ed, 2002 , p 174 et p 175

وتصديره يتوقف على ترخيص مسبق، وخدمة التشفير تعتمد على الإعلام فقط أما إذا تجاوز فك التشفير سعة 128 بيتس فإنه يخضع في هذه الحالة إلى ترخيص مسبق.[1]

ومن خلال ذلك نص المشرع الفرنسي على تجريم الاعتداء على البيانات والمعلومات المشفرة وذلك في حالة استعمال وسائل تشفير غير مرخص بها، وإذا استورد أو ورد وسائل تشفير من دولة خارج دولة الاتحاد الأوروبي يعاقب بعقوبة الحبس والغرامة[2] .

وبعدها صدر القانون رقم 2001/616 معدلا قانون تنظيم الاتصالات في مادته رقم 28 الخاصة بالتشفير، حيث قضى على أن استعمال وسائل التشفير الغير متعلقة بتأمين سرية المعلومات هو حر، وكذلك تلك المختصة بالسرية إذا كانت تتم إدارة مفاتيح التشفير وفق الإجراءات المعينة وفق هيئة معتمدة رسميا، في حين أن التصدير يحتاج إلى ترخيص من الوزير المختص.[3]

وعليه فالمشرع الفرنسي جرم كل تدخل شخصي من شأنه المساس الإداري بنظام الحماية والإعلام، أي المساس بكل ما من شأنه نفي آثر الوسيلة التقنية، وحرمانها من القيام بوظيفتها في حماية المعلومة أو ما شابه. ويمكن القول أن التدخل الشخصي يشمل صورة التوصل إلى قراءة رمز الحماية أو فك الشيفرة الخاصة بالحماية، ولا يشترط في القانون الفرنسي تحقق خرق الوسيلة التقنية واقعا، فقد يتمثل التدخل الشخصي في محاولة المساس بالوسيلة التقنية خاصة بالنسبة لوسائل الحماية.[4]

ب – موقف المشرع الأمريكي

ترتبط عملية التشفير بمعلومات هامة وسرية، لذلك يجب أن تكون الأجهزة والبرامج معدة لقيام هذا النظام، وهناك جهات مختصة تحرص على هذه الأجهزة وهذه الجهات المشرفة

---

[1] – A Bensoussan , internet , Aspects Juridiques , 2nd Edition Revue Et Augmen . Tee, Hermes, 1998 ,p162

[2] – J Robert , les réponses juridiques ,Dossier internet et les libertes , les petites qfficges, n 224 du novzmbre 1999

[3] –A. Bensoussan , Yves le roux , Cryptologie et Signature Electronique , aspects juridique , Hermès Science , 1999, p 17 et 18

[4] –AntioneLatttreille et Thierry Maillard , op , cit , p217

يراعى فيها أن تكون جهات حكومية سيادية، تمتلك احتكار استيراد أدوات التشفير أو الترخيص باستيرادها وتشغيلها، والولايات المتحدة الأمريكية من أهم هذه الجهات.[1]

ولقد اعتمد التشفير في أمريكا عام 1996 نظاما خاصا عرف بنظام الغير موثوق به، وهو النظام الذي يتولى توريد وسائل التشفير عبر مشروع أطلق عليه اسم clipper chip وعلى الشخص الذي يقوم بعملية التوريد ضمان الثقة وأن يكون مسؤول عن عمليات التشفير من خلال اعتباره الوسيط بين الدولة المراقبة وبين المستخدم سواء على الصعيد الجماعي والمؤسساتي، وسواء كان شخص طبيعي أو شخص معنوي تمثل في الشركات.[2]

وفي عام 1999 اتخذت الإدارة الأمريكية خطوات جديدة نحو تحرير تصدير برامج التشفير، فأقرت كل من وزارات العدل والتجارة الدفاع قرارا يقضي بإعفاء التجار من إيداع طلبات الترخيص، وكل شخص حرفي أو عامل محترف أو تاجر يكتفي بطلب واحد لجميع الحرفيين والتجار، ويودع الطلب لدى الوكالة الوطنية للأمن Nsa ، وفيه جميع أسماء الحرفيين ومقراتهم .[3]فاستعمال وسائل التشفير حر داخل الولايات المتحدة الأمريكية، ولا يخضع لأية قيود في إقليمها، ولكنها صنفت على أنها معدات عسكرية وبالتالي تتطلب موافقة الدولة، وهذا وفقا للضوابط الواردة في إدارة لمعاملات United Arms International التي تراعى تصدير الأسلحة من الولايات و م أ.

ويشمل التصدير توصيل أو تقديم مثل هذه البرامج والمعلومات إلى مواطن أجنبي، حتى لو كان المواطن الأجنبي يقيم في الولايات المتحدة. وذلك بمقتضى النظام القانوني المعمول به .[4]

---

[1]– عبد الفتاح بيومي حجازي ، الحكومة الالكترونية و نظامها القانوني ، شركة الجلال للطباعة ، الإسكندرية ، 2004،ص 150

[2] –James Chu, Law Enforcement Information Tevhnology ,CrcPress, Usa, 2001 , p 135

[3] – Micheal Kuntz andpatrickWelson , Computer Crime and Computer Frauf , Report to The Montgomery County Criminal Justice Coordating Commission , Fall 2004, p 151.155

[4] –Micheal Kuntz andpatrick Welson , p 156.158

وانطلاقا مما سبق فبالرغم من ما تقدمه الثروة الرقمية للبشرية من تقدم والمتمثلة في العالم الافتراضي، إلا أن الخوض فيه من خلال شبكة الإنترنت أو عبر مختلف وسائل الاتصال الحديثة قد يؤدي إلى بعض الإشكالات وعدم الاستقرار، ما استوجب حماية قانونية وتدخلا تشريعيا للحفاظ على أمن المعلومات، لذ أوجدت بعض الجهات الحماية التقنية من خلال استخدام التشفير .

2 :التشفير في التشريع الجزائري

قام المشرع الجزائري باستحداث خدمة المصادقة الإلكترونية لأهميتها في مجال تقنية المعلومات، فهي تعمل على تأمين التعامل عبر الإنترنت، كما أنها تعمل على ضمان سلامة البيانات المنقولة عبر الإنترنت.

وقد جاء ذكر سلطة التصديق في مرسوم تنفيذي متعلق بخدمات الشبكات والموصلات السلكية واللاسلكية[1]. ويعرف التصديق الالكتروني كما يلي: " كل شخص مرخص له من طرف الدولة تسليم شهادات إلكترونية، وتقديم أي خدمات أخرى في مجال التوقيع الإلكتروني" .[2] وهذه الجهات تقدم خدمات أخرى في مجال التوقيع الإلكتروني، مثل حفظ المفاتيح المستعملة في التشفير وتسلمها، كما تؤدي خدمات فيما يخص تحديد عملية المتعاقدين، التحقق من مضمون التعامل وسلامته من الغش، كذلك البحث عن جدية المواقع التجارية. [3]

وبناء على ما سبق يحتاج التشفير إلى مجموعة من التجهيزات التي تستغل لضمان أمان المعلومات وحمايتها، هذه الأخيرة تخضع لرقابة من الدولة وإلى ترخيص مسبق من هيئة البريد والمواصلات.

---

[1]– المرسوم التنفيذي رقم 07–162 المؤرخ في 2007/5/30 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيه اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، الجريدة الرسمية، العدد 37 الصادر في 07 جويلية 2007

[2]– حابت آمال ، التوجه التشريعي بخصوص التوقيع والمصادقة الالكترونية بين قانون رقم 05–10 القانون 15–04 ، مؤتمر وطني حول الإطار القانوني للتوقيع والتصديق الالكتروني في الجزائر ، كلية الحقوق والعلوم السياسية وجامعة محمد الشريف مساعدية ، سوق اهراس 2016، ص 52

[3]– حابت آمال ، المرجع نفسه، ص 53

ولقد أصدر المشرع الجزائري المرسوم التنفيذي رقم09-410 [1] المحدد لقواعد الأمن المطبقة والمنصبة على التجهيزات الحساسة قصد وضع نظام قانوني لهذه التجهيزات والتي عرفها في المادة 2 من المرسوم بأنها: " كل العتاد الذي يمس استعماله غير المشروع بالأمن وبالنظام العام". ونجد أن المشرع نص عبر الملحق الأول في القسم الفرعي الثالث على التجهيزات والبرامج المعلوماتية. أما بالنسبة إلى اقتناء معدات وبرامج التشفير فالمشرع فرق بين حالتين على المستوي الوطني وعلى المستوى الأجنبي أو الخارجي[2]. وتنص المادة 13 من المرسوم تحت عنوان الفصل الثالث: إجراءات الاقتناء كالاستغلال والبيع والتركيب.

ومن خلال نص المادة فرق المشرع بين اقتناء التجهيزات الحساسة بما فيها برامج التشفير بالنسبة للشخص الطبيعي والمعنوي، فبالنسبة للشخص الطبيعي والذي يريد اقتناء هذه البرامج يحتاج للرخصة من الوالي وهذا بمكان ممارسة النشاط، أما بالنسبة للشخص المعنوي فلمكان تواجد الشركة، كما أنه يمكن اقتناء برامج التشفير من سوق أجنبية كما جاء في نص المادة 14، حيث يخضع شراء المعدات من الأسواق الخارجية لتأشيرة محددة على أساس الترخيص المحدد في المادتين 13 و17 من نفس المرسوم. بمعنى أن هذه البرامج تخضع لتأشيرة، كما أن المشرع اشترط أن تكون المعدات وبرامج التشفير مركبة وفي شكل قطع أو مدمجة ضمن نظام وهذا ما ذكره في الفقرة الأخيرة من نص المادة ويجب أيضًا تركيب المعدات التي تم الحصول عليها على شكل أجزاء ومدمجة داخل النظام المطابق للمعايير واللوائح المعمول بها .[3]

وعليه يصدر نظام الموافقة المسبقة من وزير الداخلية بعد أخذ إفادة من الجهة المؤهلة المسؤولة عن اعتماد أجهزة وبرامج التشفير المصنفة في الفقرة الثالثة من القسم أ.

---

[1]- المرسوم التنفيذي رقم 09-410 المؤرخ في 23 ذي الحجة عام 1430هـ الموافق لـ 10 ديسمبر 2009 يحدد قواعد الأمن على النشاطات المنصبة على التجهيزات الحساسة ، الجريدة الرسمية ، العدد73

[2]- غزالي نزيهة ، تامين وسائل الدفع بالية التصديق الالكتروني في الجزائر التوقيع ، مؤتمر وطني حول الإطار القانوني للتوقيع والتصديق الالكتروني في الجزائر ، كلية الحقوق والعلوم السياسية وجامعة محمد الشريف مساعدية ، سوق اهراس 2016 - وأنظر المرسوم التنفيذي رقم 09-410

[3]- المادة 13 و 14 من نفس المرسوم، ص 6

على ضوء ما سبق فالمشرع أدخل تقنيات التشفير ووسائله ضمن التجهيزات الحساسة، أما السلطة المؤهلة للمصادقة على التجهيزات كبرامج الترميز فهي تخضع لمصالح الوزارة المكلفة بالداخلية وفقا لنوع الاعتماد وهو ما نصت عليه المادة 7، أما أنواع الاعتمادات فتنقسم حسب النشاط إلى نوعين: "النوع الأول: النشاط المتعلق باستيراد وتصدير وإنتاج وبيع وتركيب وصيانة وإصلاح المعدات الحساسة. أما النوع الثاني: النشاط المرتبط فقط بتركيب التجهيزات الحساسة وصيانتها وتصليحها."[1] وباستقراء نص المادة 20 من نفس المرسوم نجد أن استخدام المعدات الحساسة المصنفة في الأقسام الفرعية من القسم أ يكون بترخيص من مصالح الوزارة المكلفة بتكنولوجيات الإعلام والاتصال وكذا وزارة الدفاع الوطني ووزارة الداخلية والسلطة المذكورة في الفقرة 2 من المادة 7 وكذا الوزارة المكلفة بالمصادقة على تجهيزات وبرامج الترميز.[2]

وعليه نستطيع القول أن تقنيات التشفير من منظور المشرع الجزائري منظمة بمجموعة من القوانين: القانون المتعلق بالتوثيق والتصديق الإلكترونيين وتحديدا لسلطة التصديق التي تقوم بدور الرقابة وحفظ مفاتيح التشفير والتأكد من هوية المتعاملين والموقعين، هذا من جهة، وكذا المرسوم التنفيذي السابق الذكر هو الذي يحدد لنا كيفية اقتناء واستخدام برامج التشفير وكذا بيان السلطة التي تمنح الترخيص لهذه البرامج.

الفرع الثاني : تنقية المعلومات والمواقع

مع الاستخدام المتزايد لشبكة الإنترنت ظهرت برامج تمنع المستخدم من الدخول إلى بعض المواقع أو الوصول لمعلومات قد تكون ذات طبيعة مخالفة للمبادئ والقيم والأخلاق، أو ذات صلة بالمصالح العليا للدولة وللأنظمة الخاصة بها، وهذه البرامج تقوم فكرتها على تصنيف وفهرسة المواقع المطلوب منع الدخول إليها. إضافة إلى هذا تقوم على تنقية

[1]– حماني سمير، التوثيق في المعاملات الإلكترونية دراسة مقارنة ، مذكرة لنيل شهادة الماجستير ، قسم الحقوق ، كلية الحقوق والعلوم السياسية، جامعة مولود معمري ، تيزي وزو، 2015 ، ص 68

[2]– المرسوم التنفيذي رقم 09–410 ص 6، 7

المعلومات بواسطة موزع خدمة الإنترنت، وتقوم أيضا على تنقية المواقع مما تحتويه من أوضاع ومواد محظورة ومخلة بالأمن والآداب العامة والأخلاق .[1]

إن تنقية المعلومات والمواقع التي تحتوي على كل ما يمكن أن يخطر ببال الإنسان من صور أو مشاهد تتضمن أدوات غير مشروعة وأوصاف غير مرغوب بها. ورغم أن هذه العملية بالغة الصعوبة. و مثلها مثل وسائل وبرامج الحماية الأخرى لشبكة الإنترنت قامت الدول الغربية على وضع أطر قانونية وتنظيمية لوسائل التنقية، لتضمـــــن نوعا وقدرا من الحماية لمستخدمي الشبكة وهذا ما سنعالجه من خلال الفقرات الآتية.

الفقرة الأولى : مفهوم تنقية المواقع والمعلومات

تعتبر تنقية المعلومات من الوسائل والأدوات التي تستخدم للحماية من المخاطـــر التي تعترض المستخدم والتي تمسه شخصيا، وذلك باستخدام البرامج التي تمنعه من الدخول إلى بعض المواقع التي لا يرغب بالدخول إليها والابتعاد عنها، وتتمثل في مجموعة من البرامج والوسائط التي تكون وظيفتها الأساسية منع الوصول إلى بعض المواقع والمعلومات المرتبطة بها، ويكون ذلك من خلال منع الوصول إلى هذه المواقع من خلال عنوانها الذي أنشأ الموقع على أساسه، إذ أنه كما للإنسان اسما له يعرف من خلاله، فإن لكل ويب أو بريد إلكتروني أو مجموعة إخبارية أو غرفة دردشة اسما أو عنوانا لو رمزا يتمكن المستخدم الوصول إليه من خلاله.[2]والمستخدم يستطيع أن ينشئ لنفسه قائمة المواقع الممنوع الدخول إليها ويقوم بفهرسة جدول بعدد من المواقع المضرة أخلاقيا واقتصاديا، وذلك من خلال العديد من البرامج المتوفرة في السوق التكنولوجية .[3]

يوجد العديد من برامج التنقية المعروفة كبرامج cyberpatrol و cybersister وغيرها من البرامج التي يمكن تنشيطها تبعا لنوعية برمجتها وتركيبها وإعدادها ولنوع المواقع أو المعلومات الغير مرغوب الوصول إليها أو المصنفة بها. وذلك كله مرتبط بنوع البرمجة

---

[1]– طوني ميشال عيسى، التنظيم القانوني بشبكة الانترنت" دراسة مقارنة في ضوء القوانين الوضعية و الاتفاقات الدولية ، طبعة 1 ، بيروت ، 2001 ، ص 228

[2]–Isabelle Wekstein , Droit Voisins Du Droit D'auteur Et Numérique , Litec , 2002 . p 80.82

[3]– Tournier .J , Internet Censure A Domicile , le Monde , Supplément MultiMedia , 1996, p 29.30

لمثل هذه الأنواع من البرامج. وتستخدم برامج التنقية لمنع الوصول إلي حاسب معين والاتصال بعنوان الموقع الراجع لهذا الحاسوب سواء كان عنوانا لبريد الكتروني أو عنوان لموقع ويب إلى غير ذلك من المواقع .[1]ويعتبر مثلا برنامج cyberpatrol حاليا المرشح الذكي لحماية الأطفال من الأخطار على الإنترنت، وهو معروف على نطاق واسع بتميزه في توفير ميزات مثل حظر المواد الإباحية، وإخفاء الألفاظ القبيحة وإدارة وقت الإنترنت.[2]

الفقرة الثانية : الأشخاص المستخدمين لتقنية تنقية المواقع والمعلومات

تعتبر شبكة الإنترنت سوق عالمية تلتقي فيه الدول والهيئات والمؤسسات والشركات الأفراد، ويحيط بها مستوى تنظيمي يتمثل في مجموعة من الهيئات والمراجع ومنها مؤسسة الإنترنت الأمريكية، موضوعها الترويج لعمليات الاتصال والارتباط فيما بين الشبكات والتي تضم العديد من اللجان ومنها مجلس هندسة الإنترنت، ومهمتها تطوير بروتوكولات الإنترنت ومراقبة الإرسال [3].

يتولى استخدام تقنية تنقية المعلومات والمواقع جهات عديدة ومختلفة أي أنه كل من له علاقة بالشبكة من عاملين مستخدمين، ويأتي في مقدمة مستخدمي هذه التقنية أساس البنية التحتية للأطراف المتعاملين بشبكة الإنترنت والتي تتكون من المستويات الآتية.

أولا : المستوى الأول :

الأطراف المتدخلين ضمن العملية التمويلية والتنظيمية والتشغيلية والتقنية، كالدول والسلطات الرسمية العامة، ومشغلي شبكات الاتصال العامة والخاصة، ناقلي البيانات الذين يتولون تأجير الخطوط الكيانية والتاجيرية وربط شبكات الاتصال المختلفة فيما بينها، هذه الشركات هي مالكة مواقع الميل الأخير التي توفر وصول الإنترنت للزبائن، ويستخدمون تقنيات مختلفة مثل DSL اللاسلكي أو الكابل أو المودام[4] .

[1] – https://www.cyberpatrol.com/ vu le 15/12/2018

[2] – https://www.hudsonvlle .org /libiraryInternetpolicy.html , vu le 28/02/2016

[3]–https://www.isok.org/pubpolpillar/docs/bp.interconnection .ar.pdf. vu le 02/03/2016

[4]–https://www.isok.org , vu le 02/03/2016

ثانيا: المستوى الثاني

وهم موردي خدمات الاتصال بالإنترنت بالمفهوم الواسع. وبمعنى أخر الذين يقدمون للمشتركين خدمة وصلهم بشبكة الإنترنت بموجب عقود اشتراك بالشبكـــة[1].

ثالثا: المستوى الثالث

يتمثل هؤلاء في ناشـــري الخدمات والمعلومات وسائر الخدمات ذات القيمـــة المضافـــة في شبكة الإنترنت. ويندرج ضمن هذه الفئة مثلا ، المصنعون والناشرون وبنوك وقواعد المعلومات والأخبار ووكالات الأنباء والصحافة ومراكز البيع عن بعد ...الخ. ويحتل هؤلاء موقعا رئيسا على شبكة الإنترنت كونهم مصدر التدفق المعلوماتي الأساسي في هذه الشبكـــــة.[2]

رابعا : المستوي الرابع

وهم المستخدمون العاديون لشبكة الإنترنت، وهؤلاء يعدون الأطراف الأكثر أهميـــــة في شبكة الإنترنت، والذين تتوزع أدوارهم بين مستهلك أي الذي يتحصل على المعلومة، وبين منتج أو مؤلف أو حتى مورد للبيانات والمعلومات [3].

الفقرة الثالثة : الوصف القانوني لتنقية المواقع

إن الهدف من استخدام برنامج تنقية المعلومات هو حماية الأفراد وحماية حياتهم الخاصة وحماية الأطفال وحماية العادات والتقاليد والأديان والحفاظ عليهم من الانجرار وراء العولمة والانفتاح الثقافي بكل سلبياته، وكذلك من أجل الحد من الجريمة المستحدثة وما تحتويها من أفكار هدامة. وكما هو معلوم ما هو مشروع في بلد غير مشروع في بلد أخر

---

[1] – Morgan Layanchy , La responsabiliteDelictuelle sur Internet En Driut suisse, Op. Cite .p 43.45

[2]– https://www.isok.org/pubpolpillar/docs/bp.interconnection .ar.pdf. vu le 04/03/2016

[3] – Morgan Layanchy, La responsabilité Delictuelle…,p45

والعكس صحيح وليست كل المواقع ينظر لها بنفس النظرة القانونية سواء في الدول الغربية أو العربية.

وانطلاقا من هذا الأساس عمدت غالبية الدول إلى العمل على تعديل قوانين الاتصالات لديها على الرغم من الصعوبات التقنية العالمية التي تواجه عملية تنقية المواقع والمعلومات وذلك من اجل إلزام موردي الخدمات بتقديم أساليب وبرامج التنقية للمشتركين لديها .

أولا :الإطار القانوني للتنقية في فرنسا .

إن المادة 15 من قانون 1996 المعدل لقانون 1986 الخاص بالاتصالات أوجبت كل شخص يعمل على تقديم خدمة الاتصال بواحدة من خدمات الاتصال السمعية والبصرية أن يقدم إلى المشتركين وسيلة تقنية في التنقية لبعض الخدمات .

لقد عدل هذا القانون أيضا سنة 2000 ونص في إحدى مواده على ضرورة قيام موردي خدمات الاتصال بإعلام المشتركين حول وسائل التنقية المتوفرة، وأن ما يتم عرضها عليهم مع طريقة الاستعمال وضرورة معرفتهم بواحدة من هذه التقنيات على الأقل.[1]

ولقد تعرض هذا القانون في ما بعد إلى غربلة من طرف المجلس الدستوري أدت هذه الغربلة إلى إلغاء العديد من مواده وأهمها الجزاءات التي كانت تطال مورد الخدمات في حال عدم إعلام المشترك عن خدمات وبرامج التنقية، والتزامه بموجب نتيجة الوصول المشترك إلى نتيجة بحصوله على خدمة برنامج تنقية. وهذا الإلغاء للعقوبة أدى إلى إفراغ قانون الاتصالات من مضمونه الجزائي ليصبح بمثابة توصية إلزامية لها، لأن تقديم وسائل وبرامج التنقية لم يعد خاضعا إلى أية عقوبة في حال عدم احترامه، وظل الأمر على حاله في التعديل الثاني 2000.[2]

لقد تعرض القانون الفرنـــسي للانتقاد من طرف مجلس الشيوخ والنواب الفرنسييـــن حول عدم تحديد الجهة المخولة بمراقبة أو تصنيف المواقع والمعلومات.[3]

---

[1]–la loi n 2000–719 du 1er aout morfiaient la loi n86 du 30 septembre 1986 relative a la liberté de communication , JO , N177 du aout 2000 , p 11093, www egifrance /gouv/fr , vu le 30 09 20016

[2]–Valerie Sadaillan ,Droit De l'internet, collection , AUI, p 135.136

[3]–V Sadaillan , Principe General Du Droit D La Responsabilité Et Responsabilité Des Acteurs De L'internet , op , cite , p34 36

ثانيا :الإطار القانون للتنقية في الولايات المتحدة الأمريكية

لقد تضمن قانون عام 1996 النصوص الخاصة بقانون آداب الاتصالات والذي اعتبر آنذاك مقيدا لحرية القصر في الاطلاع على المواد المخلة بالآداب العامة، وعاقب القانون كل من قام، بأية وسيلة من وسائل الاتصال، بعمل أو إنشاء أو تشجيع أو بث تعليقات أو طلبات أو اقتراحات أو صور فاحشة أو غير أخلاقية، مع العلم أن متلقيها لم يتم الثامنة عشرة من عمره.[1]

لقد تم تعديل وتحديث القانون الأمريكي للاتصالات ليلبي متطلبات التطور التكنولوجي اللاحق بوسائل الاتصالات عن بعد، لاسيما منه الوسائل السمعية والبصرية، وقد برز في جملة من التعديلات والأحكام التي تضمنه هذا التعديل وهي: حماية القاصرين من ما يتعلق بالبث الرقمي الحاصل عبر الشبكات بواسطة الكابل وإلزامية اعتماد أساليب تقنيـــة تدخل ضمن مفهوم التنقية، لمراقبة المواقع أو حجبتها ومنع القاصرين الوصول إليها [2].

وعليه فإن برامج التنقية هي برامج تمنع مستخدمي الكمبيوتر والإنترنت من الوصول إلى مواقع ويب معينة. ويتم استخدامها عادة لحظر المحتوى الذي يعتبر غير مناسب لمستخدمين محددين. وتستخدم على نطاق واسع في الدول الغربية في المكتبات العامة وأجهزة الكمبيوتر المدرسية. ويمكن استعمال برامج التنقية من قبل أي شخص لديه شبكة لاسلكية على سبيل المثال، ويمكن للوالدين استخدامها لتقييد الوصول إلى أطفالهم عن طريق الإنترنت[3].

---

[1]– Gay Kaymona , Droit De L'enfance Et De L adolescences , Litec , 2002 , p 373

[2]–Wiley D Parker ,Fighting Computer Crime , A New Framework for Protecting PuBlishing , NewYork , p 101,102

[3]– يعد عامل تنقية المواقع أو ما يطلق عليه برنامج تصفية الويب ، والذي يشار إليه عادة باسم "برنامج التحكم في المحتوى" ، جزءًا من البرامج المصممة لتقييد المواقع الإلكترونية التي يمكن للمستخدم زيارتها على جهاز الكمبيوتر الخاص به. يمكن أن تعمل هذه المرشحات إما باستخدام القائمة البيضاء أو القائمة السوداء: فالأول يسمح بالوصول فقط إلى المواقع التي يختارها على وجه التحديد أي شخص يقوم بإعداد المرشح ، ويقيد الأخير الوصول إلى المواقع غير المرغوب فيها على النحو الذي تحدده المعايير المثبتة في المرشح. تنظر هذه البرامج إلى عنوان URL الخاص بالموقع المرغوب فيه وتبحث من خلال محتوى الموقع عن الكلمات الرئيسية المحظورة ، ثم تقرر ما إذا كان سيتم حظر الاتصال أو السماح به. غالبًا ما يتم تثبيت المرشحات إما امتداد المستعرض أو كبرنامج مستقل على الكمبيوتر أو كجزء من حل أمان شامل. ومع ذلك ، يمكن تثبيتها أيضًا على جانب الشبكة ، إما بواسطة موفر خدمة إنترنت أو شركة ، لتقييد

المطلب الثاني: الوصف القانوني لجريمة الإنترنت

لقد تم تصميم شبكة الإنترنت أساسا لتكون وسيلة لنقل وتبادل المعلومات على نطـــــاق محدود ولكن وبعد تعميمها واستخدامها الواسع من طرف الأشخاص تحولت الإنترنـت إلى فضاء جديد لتبادل المعلومات بكافة أشكالها على النطاق العالمي. وأصبحت أيضا سوقـا عالمية باهرة لإتمام المعاملات والصفقات ذات طبيعة تجارية، وأيضا أداة مهمة في تسويق السلع والخدمات وترويجها عبر العالم [1].

ومادام في جريمة الإنترنت برامج ومعطيات الكمبيوتر وكل البيانات هي محل الجريمة،[2] أي أنها قد تستهدف الشيء المعلوماتي بكل مكوناته أو بما تمثله من أموال أو أسرار أو بيانات شخصية، ولأن كل هذه المعطيات هي موضوع الجريمة، ولأن المعلومة تعتبر الركيزة الأساسية في العديد من الجرائم عبر الإنترنت، نطرح هذا السؤال ما هو مدلول المعلومة وما هو مدلول كل ما له علاقة بالمعلومة من تقنية المعلوماتية والنظم المعلوماتية و الأمن المعلوماتي. وما هو الإطار القانوني لها ؟

وللإجابة على هذا السؤال وجب علينا تحديد ماهية المعلومة وبيان أنواعها أولا، وعرض الإطار القانوني لها ثانيا.

الوصول إلى الويب لعدة مستخدمين في وقت واحد. تتميز بعض محركات البحث أيضًا بمرشحات بدائية لإزالة الصفحات غير المرغوب فيها من نتائج البحث. ويحتوي برنامج فلترة الويب على قاعدتين رئيسيتين من العملاء: الآباء الذين يرغبون في منع أطفالهم من الوصول إلى المحتوى الذي يعتبرونه غير مرغوب فيه أو غير مناسب ، والشركات التي تريد منع الموظفين من الوصول إلى مواقع الويب التي لا تتعلق بوظائفهم. تُستخدم عوامل تصفية الويب أيضًا بشكل شائع كأداة لمنع البرامج الضارة ، حيث ستعمل عوامل التصفية على حظر الوصول إلى المواقع التي تستضيف برامج ضارة بشكل شائع ، مثل تلك المتعلقة بالإباحية أو المقامرة. يمكن للمرشحات الأكثر تقدمًا حظر المعلومات المرسلة عبر الإنترنت، لضمان عدم إصدار بيانات حساسة أنضر:

https://www.kaspersky.com/resource-center/definitions/web-filter , et

https://ncac.org/resource/internet-filters-2 , vu le 22 10 2016

[1]-Alfred Kagan ,The ElectonicIneormation Gap , Social Responsibilities Discussion Groupe Paper , Amsterdam 16 august 1998 international Federation of Libirary Asqociation and Institutions , http ://www.ifla.org / vu le 12 /11/2016

[2] -هدى حامد قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن ، مرجع سابق ، ص15

الفرع الأول : مفهوم المعلومة

إن المعلومة من الأشياء التي يمكن لكافة الأشخاص الاستفادة منها، ومن هنا جاءت فكرة حق الحصول على المعلومات، وهي عبارة عن مجموعة من الدلالات والبيانات والمؤشرات المفيدة لتحقيق نتائج محددة. فمثلا يمكن استعمالها من أجل اختراع جديد أو تسخيره من أجل أمر معين، لذلك لابد من حماية هذه المعلومة،[1]وعليه سنقسم هذا الفرع إلى تعريف المعلومة وبيان أنواعها وشروط حمايتها قانونيا، وتعريف المفاهيم الأخرى المرتبطة بالمعلومات، تقنية المعلوماتية، النظم المعلوماتية والأمن المعلوماتي.

الفقرة الأولى : المعلومة

لقد أصبحـــــت المعلومات وأدواتها مـــوردا ومفتاحا للشيفرة المعرفية التي تصف ظاهرة الجريمة عبر الإنتـــــرنت وأصبحت تشكـل تجسيدا لبداية الإجرام على الشبـكة العنكبوتية ومسرحا لها[2].

أولا: تعريف المعلومة

المعلومة هي" مجموعة الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون موضوعا للتبادل والاتصال أو التفسير أو تأويل أو المعالجة سواء بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتخزينها وجمعها ونقلها بوسائل وأشكال مختلفة ".[3]

وفي ما يخص مكافحة الجرائم المعلوماتية قد عرفها القانون الاتحادي رقم 2 لسنة 2006 بأنها" كل ما يمكن معالجته وتخزينه وإنشائه ونقله باستخدام تقنية المعلومات والاتصالات، وخاصة الحروف والأصوات والصور والعلامات والرموز والأرقام".[4]

---

[1]–امجد حسان، الفيروسات إرهابا يهدد أنظمة المعلومات ، مقال مقدم إلى ملتقي الإرهاب ،جامعة الحسين بن طلال ، عمان في 2008، ص 1

[2]– أحمد إبراهيم مصطفى سليمان ، الإرهاب والجريمة المنظمة ، مطبعة العشري ، القاهرة ، 2006 ، ص 31

[3]– W .Donparker , Fighting Computer Crime ,p27. نائلة عادل قورة، المرجع سابق ، ص 97 و

[4] – Axel Llefebvre , Etienne Montero , Informatique et Droit , Vers une Subversion De L'ordre Juridique , facults universitaires Notre Dame de Paix de Namur , Bruylant Bruxelles , 1999, p9

وما يجدر بنا ذكره هو تعريف المشرع الجزائري للمعطيات المعلوماتية الذي جاء في نص المادة 02 الفقرة "ج" من القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بأنها" كل عملية عرض للوقائع والمعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج التي تجعل من المنظومة المعلوماتية تؤدي وظيفتها". ويعتبر هذا التعريف عاما يبتعد عن الدقة، وعليه وجب إعطاء تعريف خاص للمعلومة من أجل التمييز بين مصطلح المعلومات والمصطلحات الأخرى.[1]

ثانيا: أنواع المعلومات.

للمعلومات عدة أنواع تتمثل في مايلي :

1- **المعلومات الاسمية** : تتضمن المعلومات المرتبطة بشخص معين كاسمه، موطنه، حالته الاجتماعية، وهي معلومات سرية لا يمكن الوصول إليها دون الإذن الشخصي.

2- **معلومات المصنفات الفكرية:** وهي معلومات تم حمايتها قانونيا ويضاف إليها المعلومات المتعلقة بالاختراعات والتسجيلات الفنية.

3- المعلومات المنشورة والمتاحة : وهي معلومات متاحة لجميع الأشخاص، كتقارير سوق الأوراق المالية وتقارير الطقس.[2]

ثالثا: شروط الحماية القانونية للمعلومات: من أجل أن تكون المعلومات خاضعة للحماية القانونية وجب توفرها على شروط معينة نذكرها كالآتي :

1- أن تكون المعلومة محددة ومبتكرة: من الواجب أن تتميز المعلومة بالتحديد. إضافة إلى هذا يجب أن تكون المعلومات أصلية ومبتكرة، أي أنها لم تكن موجودة من قبل. وغير

---

[1]- القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية رقم : 47 ، الصادرة بتاريخ : 16 أوت 2009- طالع الملحق رقم : 02.

[2]- عبد العال الدريبي، الجرائم الالكترونية، دراسة قانونية قضائية مقارنة مع احدث التشريعات العربية في مجال مكافحة الجرائم المعلوماتية والإنترنت، المركز القومي للإصدارات القانونية ، القاهرة، 2012 ، ص 45.

مدرجة في المعلومات العامة التي يمكن الوصول إليها بسهولة لأنها لا تتعلق بأشخاص معينين.[1]

2- سرية المعلومة : يجب أن تكون المعلومات سرية حتى يحميها القانون، ويجب أن تظل المعلومات سرية، إما بطبيعتها أو بالإرادة الشخصية، على سبيل المثال عن طريق تخصيص رقم سري خاص بها .[2]

الفقرة الثانية : تقنية المعلوماتية L'informatique

إن الانتشار الكبير للمعلومات من خلال اتساع دائرة الاهتمام بها، وإنشاء نظم تعمل على نطاق واسع وسريع، لتداول وتخزين المعلومات لضمان فعاليتها وهو ما يعرف بتقنية المعلوماتية. ويعود مصطلح المعلومات إلى الباحث الفرنسي ديرفوس الذي استعمله لأول مرة عام 1962 للتمييز بين أنظمة المعلومات الآلية وأنظمة معالجة المعلومات الأخرى.

وقد وضعت الأكاديمية الفرنسية تعريف للمعلوماتية حسب ما ورد في الجلسة المنعقدة في 02 أفريل 1967 بأنها " العلم التفاعلي العقلاني بواسطة آلات أوتوماتيكية مع المعلومات باعتبارها دعامة للمعارف الإنسانية وعماداً للاتصالات في ميادين التقنية والاقتصاد والاجتماع ".[3]

أما التعريف الأكثر دلالة على المعلوماتية، هو تعريفها بأنها" علم يعنى بالموضوعات والمعارف المتصلة بأصل المعلومات وتجميعها وتنظيمها، واختزانها واسترجاعها وتفسيرها وبثها وتحويلها واستخدامها، كما يتضمن البحث عن تمثيل المعلومات في النظم الطبيعية والصناعية والإدارية، واستخدام تقنيات الترميز في نقل الرسالة والتعبير عنها، إضافة إلى الاهتمام بالأساليب التي من خلالها يمكن معالجة المعلومات كنظم البرمجة والنظم المعلوماتية " وبطريقة ملخصة يطلق علي المعلوماتية " المعالجة الآلية للمعلومات "[4].

---

[1]- محمد علي العريان ، المرجع السابق ، ص 38.

[2]- عبد العال الديربي، المرجع السابق ، ص 45.

[3]- محمد علي العريان، الجرائم المعلوماتية ،مرجع سابق، ص 38.

[4] - تركي بن عبد الرحمان المويشير، بناء نموذج امني لمكافحة الجرائم المعلوماتية وقيـــاس فعاليته ، مرجع سابق ، ص 14.

الفقرة الثالثة : النظم المعلوماتية

أدى انتشار المعلومات وتركيزها إلى زيادة الحاجة إلى تغييرها ونقلها، مما أدى إلى انتشار تقنيات المعلومات التي كانت غايتها معالجة المعلومات تلقائيًا بفضل التقنيات المتوافرة. وكانت نتيجة للتقاطع بين علوم الحاسوب وعلوم الاتصالات، وهو ما تسبب في انتشارها بسرعة مذهلة في جميع دول العالم.[1]

تشكل نظم المعلومات أساس تكنولوجيا المعلومات. وبدونهم سيكون من المستحيل تحقيق هذا التقدم الحضاري. وبسبب التشابه في المصطلحات قد يكون من الصعب إنشاء تعريف محدد لنظم المعلومات، إلا أننا سنعرض مفهوم نظم المعلومات وتعريفها بما يتناسب مع موضوعنا، مبتعدين عن القيود المرتبطة بالتعريفات التي يقترحها علم نظم المعلومات.

لقد عرفت اتفاقية بودابست لمحاربة الجرائم المعلوماتية في المادة الأولى النظم المعلوماتية بأنها " كل آلة قادرة على تنفيذ برامج محددة للمعالجة التلقائية لبيانات الكمبيوتر، بمفردها أو مع مجموعة من العناصر ".[2]

أما المشرع الجزائري فقد قام بتعريفها على أنها " أي نظام منفصل أو مجموعة أنظمة مترابطة، يقوم واحد أو أكثر منها بمعالجة البيانات تلقائيا لتنفيذ برنامج معين".[3]

وبالرجوع للتعاريف السابقة يمكن اقتراح تعريف محدد لنظام المعلومات على أنه مجموعة من أجهزة الكمبيوتر الفردية أو المتصلة ببعضها من خلال شبكات اتصال داخلية أو خارجية تعمل تلقائيا وفق برامج صممت خصيصا لتحقيق المعالجة التلقائية للمعلومات. وتعتبر الحواسيب من أهم مكونات النظام المعلوماتي، بالإضافة إلى شبكة الإنترنت.

---

[1] – حسن طاهر داود ، جرائم نظم المعلومات ، جامعة نايف للعلوم الأمنية،الرياض، السعودية، طبعة 1 ، 2000، ص 18.

[2] – اتفاقية بودابست عن اجتماع المجلس الأوربي و ذلك بتاريخ :23 نوفمبر 2001 ، تحت رقم 185 و ذلك تحت وصف " اتفاقية بودابست لمكافحة الجريمة المعلوماتية" أنظر الملحق الاتفاقية رقم : 03 الموجهة. لوضع الأطر القانونية

[3] – الفقرة "ب" من المادة 02 من القانون 04-09 المتعلق بآليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها

تعد نظم المعلومات جوهر تكنولوجيا المعلومات بما توفره من أساليب وتقنيات متقدمة في معالجة المعلومات بفضل أجهزة الكمبيوتر وشبكات الاتصالات. ولهذه الأنظمة تأثير إيجابي بفوائدها التي يستحيل حصرها، واعتماد الحكومات والشعوب على هذه التكنولوجيا أدى إلى العمل على تطويرها وتحسين قدراتها بطريقة مستمرة. إلا أن النمو المتواصل لتكنولوجيا المعلومات وتأثيرها على أنماط الحياة قد خلق نمطاً من الهجمات الإلكترونية التي تستهدف هذه الأنظمة المعلوماتية بسبب ما تخزنه من معلومات شخصية ومالية وسرية... الخ. الأمر الذي أدى إلى ظهور الأمن المعلوماتي.

الفقرة الرابعة :الأمن المعلوماتي

تطور استخدام تكنولوجيا المعلومات وظهور أفكار جديدة مثل العقود الحكومية والإدارية والإلكترونية، وكذلك انتشار شبكات التواصل الاجتماعي على شبكة الإنترنت، والاعتماد الشبه كلي على الإنترنت في جميع المجالات جلب معه خطرا كبيرا يمس بالمعلومات الخاصة بمستخدمي الإنترنت، وعليه وجد الأمن المعلوماتي لحماية المعلومات من كافة أشكال الاعتداء عليها.

أولا: تعريف الأمن المعلوماتي .

يُعرّف أمن المعلومات بأنه "اتخاذ الاحتياطات والأنظمة التي تهدف إلى الحفاظ على المعلومات الموجودة في الكمبيوتر، وتجعلها في مأمن من الخلل أو الحوادث أو الجرائم المتعمدة".[1]وتهدف اغلب التعاريف إلى إبراز أسس الأمن المعلوماتي وهي :

1-المحافظة على المكونات المادية للحاسوب.

2- حماية المعلومات وسلامتها وسريتها والوصول إليها واستخدامها.

3-المحافظة على المعلومات من تخريبها، واستبدالها أو تحريفها، أو سوء تفسيرها وإلغائها أو الفشل في استخدامها أو سرقتها.

4- معالجة جميع انتهاكات الأمن والخصوصية والمعلومات الخاصة.

ويتمتع مجال الأمن المعلوماتي بالأهمية البالغة نظرا لازدياد أهمية وقيمة المعلومات، ودورها الحساس، بالنسبة للدول خصوصا تلك الأمنية والاقتصادية التي تلعب دورا

[1]- تركي بن عبد الرحمان ، المرجع السابق، ص 23.

استراتيجي هام، ولذلك فإن ارتبطت المعلومات بالسرية نظرا للأضرار التي قد تنجم عن فقدانها.[1]

ثانيا: غايات الأمن المعلوماتي .

تتمثل الغايات الأساسية لاعتماد إستراتيجيات الأمن المعلوماتي في أي منظومة معلوماتية في الحفاظ على المعلومة من حيث :

1-الإتاحة: أي إتاحة استخدامها بصورتها الأصلية أينما كانت وكيفما تطلب الأمر، ومنع تدمير المعلومات أو خلطها مع معلومات أخرى ملوثة.

2- التكامل: ويقصد به تكامل المحتوى، وبمعنى أخر المعلومات التي تتم معالجتها تلقائيا هي مجموعة لا تقبل التجزئة، وأمن تكنولوجيا المعلومات هو ما يضمن سلامة المعلومات في جميع أجزائها من بداية المعالجة إلى نهاية المعالجة، مما يضمن سلامة المعلومات من التلاعب بها.[2]

3- السرية : أي التأكد من الحفاظ على المعلومات المخزنة أو المنشورة على الموقع وعدم الاطلاع عليها أو استخدامها ما لم يتم التصريح بذلك، أو التأكد من أن الوصول إليها يكون لصالح المستخدمين المصرح لهم.[3]

الفرع الثاني : الإطار القانوني للمعلومات

يدور النقاش حول شرعية البرامج والمعلومات، وهل لها قيمة ذاتية، أم أن قيمتها تتمثل بكونها مجموعة جديدة من القيم التي يمكن الهجوم عليها بطريقة ما، وعليه يكون السؤال حول شرعية المعلومات؟ وهل لها قيمة في ذاتها.[4] وللإجابة على هذا السؤال فقد انقسم الفقه إلى اتجاهين:

الاتجاه الأول: فهو يرى أن المعلومات تتميز بطبيعة خاصة.

الاتجاه الثاني: يعتقد أن المعلومات ليست سوى مجموعة محدثة من القيم.

---

[1] – تركي عبد الرحمان ، المرجع السابق، ص 24.

[2] – سلمى مانع ، دور الأمن المعلوماتي في مكافحة الجرائم المعلوماتية، بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16و 17 نوفمبر 2015، كلية الحقوق ، جامعة بسكرة، الجزائر، ص 10.

[3] – تركي عبد الرحمان ، مرجع سابق، ص 52.

[4] – محمد علي العريان، المرجع السابق، ص 49.

أولا: المعلومات لها طبيعة قانونية من نوع خاص.

ينظر هذا الاتجاه إلى المعلومات على أنها ذات طبيعة خاصة، بناءً على حقيقة معترف بها وهي أن الأشياء الموصوفة بالقيم هي الأشياء التي تقبل امتلاكها. ويُنظر إليها أيضًا على أنها قيمة يمكن اكتسابها إلا في ضل حقوق الملكية الفكرية.

لقد تمت معالجة مشكلة الأخطاء في تفسير المعلومات أو معلومات الغير، لذلك يسعى الاتجاه إلى حماية هذه المعلومات في قضايا المنافسة غير المشروعة، وفقا لحكم المحكمة الجنائية الفرنسية:" الغرض من دعوى المنافسة غير قانونية هو ضمان حماية شخص لا يمكنه الاستفادة من حق استثنائي ".[1]

ثانيا: المعلومات مجموعة مستحدثة من القيم

يري هذا الرأي الحديث أن المعلومات مجموعة جديدة من القيم، الفضل في هذا راجع إلى الأستاذين" فيفو وكاتلا "ويرى كاتلا أن قابلية المعلومات للاستحواذ كقيمة واستقلالا عن دعايتها المادية، مستندا في ذلك على أن المعلومات تقوم حسب أسعار السوق الغير ممنوعة تجاريا بغض النظر عن قيمتها المادية فهي نتيجة لعمل مقدمها، وترتبط بأصلها بعلاقة قانونية تتمثل في علاقة ملكية. وهذا الرأي يؤسس حجتين تضفي على المعلومة وصف القيمة:

الأولى هو قيمة المعلومات الاقتصادية والثانية هي علاقة بناءة بين المؤلفين.

ولقد اعتمد الأستاذ فيفو على حجتين الأول: أن تكون فكرة الشيء أو القيمة لها شكل معنوي، وأن موضوع القانون قد ينتمي إلى قيمة معنوية ذات طابع اقتصادي وقد يستحق حماية القانون. والحجة الثانية هي أن كل شيء مملوك معنويا ومعترف به بموجب القانون، ومعترف به على أن له قيمة في هيئة براءات اختراع، أو تصاميم، أو نماذج، أو مجموعات أساسية، أو حقوق الطبع والنشر، فبدون قيمة المعلومات لا وجود للملكية المعنوية ، وعليه يرى أن قيمة المعلومات ليست شيئًا جديدًا ، لأنها موجودة بالفعل في مجموعة معينة.

[1] – محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على القانون الجزائي ، المرجع السابق. ص: 180.

ويـــــرى د محمد سامي الشوا بأن المعلومات لها قيمة في حد ذاتها من حيث جوهرها واستقلاليتها، إلى جانـــــب قيمتها الاقتصادية المثبتة، ممـــا يجعلها عرضة للحيازة غير المشروعة.[1]

في رأيي القول أن الأموال المعنوية المعلوماتية ليست أموالًا ولا يمكن سرقتها، سيتسبب في فقدان حماية القانون الجنائي ويفتح الفرص للمجرمين ومجرمي البرمجيات والبيانات.

ومما سبق يتضح لنا وجوب حماية المعلومات بأي شكل وردت عليه خاصة وأنها في انتشار متزايد، وبحاجة إلى مزيد من التخطيط وإلى استراتيجيات وتقنيات الأمن المعلوماتي ويرجع ذلك إلى تزايد عدد الجرائم المعلوماتية، وذلك من خلال التوسع في هذه التكنولوجيا والتعامل مع جوانب استخدامها اليومي في حياتنا. فبمجرد التهاون أو وجود فراغ في هذا المجال سيشكل وبدون شك منفذا لمحترفي الإجرام المعلوماتي مما يشكل تهديدا على المصالح الأساسية للدولة وخصوصا منها الدفاعية العسكرية والمالية والصحية، بالإضافة إلى الاهتمامات الشخصية للأفراد الذين ينمون باستمرار في المجال الرقمي، خصوصا وأن التكنولوجيا المعلوماتية أضحت مكتسبة في شكل هاتف نقال يصل إلى كل الأماكن.

ونتيجة للجوانب السلبية للاستخدام الغير القانوني لتكنولوجيا المعلومات ظهرت مظاهر مختلفة وتصنيفات متعددة للجرائم المرتكبة عبر الإنترنت وهذا ما سنتناوله في الباب الموالي .

[1]– محمد سامي الشوا، ثورة المعلومات وانعكاساتها على القانون الجزائي ، المرجع السابق ، ص 185

ملخص الفصل التمهيدي

أمام التطور العلمي الهائل والمستمر والتدفق الغزير للمعلومات نتيجة شيوع استخدام الشبكة المعلوماتية "الإنترنت" التي شملت كامل أنحاء العالم وربطت بين شعوبها وأصبحت الإنترنت وسيلة للتفاعل اليومي بين مختلف الطبقات والمجتمعات، وأمام اختلاف الأشخاص واختلاف المستويات التعليمية لمستخدمي الإنترنت، ظهرت ممارسات غير قانونية وأصبحت هذه الشبكة أداة لارتكابها. وظهرت معها نوع جديد من المجرمين الذين أطلق عليهم مجرمي المعلوماتية وهم أشخاص طوعوا شبكة الإنترنت لتصبح سلاحا لا يستهان به لممارسة فئة حديثة من الجرائم العابرة للحدود الوطنية تختلف عن الجرائم التقليدية الأخرى ، وأصبحنا أمام ظاهرة جديدة هي جرائم الإنترنت.

اختلفت الاجتهادات وتعددت التعريفات للجريمة عبر الإنترنت وظهرت صعوبة إيجاد تعريف جامع لها. ويرجع ذلك من ناحية إلى التطور السريع لتكنولوجيا المعلومات ومن ناحية أخرى إلى الدور الذي تلعبه هذه التكنولوجيا في الجريمة، ولقد انقسمت هذه التعريفات فمنها التي تستند إلى وسيلة ارتكاب الجريمة ومنها التي تستند إلى موضوع الجريمة ، ومنها التي تستند على سمات شخصية مرتكب الجريمة.

وبالرغم من تعدد التعريفات وتباينها إلا أنه لا وجود لتعريف موحد ومحدد وشامل لجرائم الإنترنت.

أما المشرع الجزائري، فلم يعرّف الجريمة السيبرانية، بل أخذ مصطلح " الإضرار أو المساس بأنظمة المعالجة الآلية للبيانات" للإشارة إليها.

ومن خلال دراستنا لجريمة الإنترنت يمكننا تعريفها على أنها كل سلوك أو فعل مخالف للقانون يرتكب عبر شبكة الإنترنت وبواسطة الخدمات والتطبيقات التي تقدمها.

والجريمة عبر الإنترنت هي نوع من الجرائم المعلوماتية، فليس كل جريمة معلوماتية هي جريمة إنترنت، لأن جرائم الإنترنت يشترط فيها الاتصال بشبكة الإنترنت عند ارتكابها.

تتمتع الجرائم عبر الإنترنت بطابع خاص يميزها عن باقي الجرائم، وذلك لارتباطها بتكنولوجيا المعلومات والكمبيوتر وبتقنياته العالية. فهي جرائم ألغت أي حدود جغرافية،

إضافة إلى تميزها بالسهولة والمرونـــة في التنفيذ والاعتـــداء بدون ترك آثار مرئية لذلك يصعب اكتشافها ويصعب الوصول إلى الدليل فيها، وهي أيضا جرائم ناعمة بلا عنف أو مقاومة و سريعة التنفيذ.

يتميز أغلب مجرمي الإنترنت بامتلاكهم الخبرة والقدرة الفائقة والمهارة والمعرفة الكبيرة في اختراق الشبكات، ولكن في المقابل هناك عدة جرائم أصبحت لا تحتاج إلي قدر من الذكاء والعلم، وإنما تستلزم القليل من المعرفة بتقنيات الحاسوب والإنترنت وكيفية التشغيل فقط لارتكابها، خاصة في بعض الجرائم التي لا تتطلب الذكاء الخارق كجرائم السب والقذف والتشهير وأيضا جرائم التهديد.

لقد صنف الباحثون مجرمي الإنترنت وأخذ هذا التصنيف بعين الاعتبار كل الأشخاص القادرين على ارتكاب هذا النوع من الجرائم وذلك على أساس الربح المادي، أو تحقيق هدف شخصي، أو على أساس إثبات القدرات والتحدي، أو على أساس العمل لصالح منظمات أو جهات إرهابية أو العمل للصالح الذاتي. ويمكن أن يكون المجرم الواحد مزيجا من عدة طوائف أو من طائفتين .

إن الدوافع والأسباب التي تدفع بالجاني لارتكاب هذا النوع من الجرائم هي العوامل المحركة لإرادته والتي توجه سلوكه الإجرامي كالمحبة والشفقة والبغضاء والانتقام وكسب المال، أو ابتغاء تحقيق غاية معينة، وتبعاً لذلك فإن الأسباب والدوافع التي تدفع الجناة لارتكاب الفعل الغير المشروع عبر الإنترنت تختلف عن الأسباب والعوامل التي تدفع بالمجرم لارتكاب الجرائم الكلاسيكية، وأهم دوافع الجريمة عبر الإنترنت الولع والرغبة في جمع المعلومات المخزنة في أجهزة الحاسوب والمنقولة عبر شبكة الإنترنت، ويمكن أن تكون الأسباب أيضًا الرغبة في إيذاء الآخرين أو الحاجة إلى الكسب والربح السهل ، مما قد يؤدي إلى انتهاك الأنظمة ونظم المعلومات، بالإضافة إلى دوافع الجاني الخاصة المتمثلة في التحدي وإبراز الذات.

الباب الأول:

مظاهر العدوان الإجرامي عبر الإنترنت

قدم الحاسوب والإنترنت الرقي للإنسانية في جميع الجوانب وعلى كافة الأصعدة، إلا أن هذا التقدم المذهل واكبه من جهة أخرى تطور الفكر والعقل البشري الإجرامي، الذي أفرز عن بروز أنواع متعددة للسلوك الإجرامي المرتكب عبر الحاسوب والإنترنت معا غزت كل العالم وباتت من أهم المخاطر التي تحدث على الإطلاق، وتهدد أمن وسلامة المستخدمين لشبكة الإنترنت .

وبما أن هذه الجرائم مرتبطة بتقدم تكنولوجيا المعلومات وتنمية المجتمع، فكلما زاد اعتماد المجتمع على أجهزة الكمبيوتر والإنترنت، كلما زاد ذلك من تأثيرها على زيادة معدل جرائم الإنترنت. وهذا ما أثبتته جائحة كورونا التي انتشرت سنة 2020 وتسببت في زيادة مذهلة في الجرائم عبر الإنترنت مست العالم بأسره، فمع انتشار الفيروس أصبح الاعتماد واسع النطاق على تقنيات التواصل الاجتماعي، وأصبح الاستخدام أوسع للخدمات المتوفرة عبر الإنترنت، الأمر الذي سهل على قراصنة المعلومات استغلال الأزمة الوبائية لشن هجماتهم وتنفيذ حيلهم .

وفي إحصائيات جاءت بها دراسات في منطقة الخليج تبين أن عدد الجرائم باستعمال الإنترنت زادت عن ذي قبل بنسبة 33 بالمئة خلال الأشهر الأولى من تفشي الوباء. وفي أوروبا أعلنت العديد من الدول أنها شهدت ارتفاع كبير في جرائم الإنترنت في الفترة التي انتشرت فيها جائحة كوفيد19 مثل ألمانيا وسويسرا بريطانيا. كما كشفت وكالة الشرطة الأوروبية يوروبول أن جائحة كورونا ساهمت بشكل كبير في زيادة عدد الجرائم المعلوماتية في كافة أنحاء أوروبا خاصة جرائم الاحتيال ونشر المواد الإباحية والترويج للمخدرات، كذلك ازدادت الهجمات السيبرانية التي تمس بالمستشفيات والشركات وإمدادات الطعام وكذا العديد من الوظائف الحيوية. كما أعلن مكتب التحقيق " إف بي أي أن الجرائم المعلوماتية تضاعف عدت مرات منذ بداية الوباء وحذر المواطنين من الوقوع ضحية لها.

أما الجزائر فهي الأخرى شهدت ازدهارا واسعا في الجريمة عبر الإنترنت خاصة جريمة الاحتيال وجريمة نشر الإشاعات الكاذبة بغرض المساس بأمن الدولة واستقرار الوطن نتيجة للاستعمال والإقبال الكبير على الإنترنت خاصة في فترة انتشار وباء كورنا . إضافة

إلى هذا شهد العالم في ظل هذه الجائحة بروز أنماط جديدة من الإرهاب والتطرف تعتمد على توظيف التقنيات الحديثة في بث خطابات الكراهية ، والترويج للأفكار الهدامة ، وذلك بهدف جذب أكبر عدد من المؤيدين لهذه الأفكار، وتقويض الثقة في الحكومات بشكل يؤدى إلى زعزعة أمن واستقرار البلد. مستغلين بذلك انشغال العالم بوقف انتشار العدوى وإيجاد عالج لهذا المرض "كوفيد 19".

لقد تعددت مظاهر العدوان الإجرامي عبر الانترنت وتعددت تصنيفاتها، وليس من اليسر علينا حصر هذا النوع من الجرائم بسبب تشعبها واختلاف أنواعها وسرعة تطورها، كما أن الفقه القانوني لم يستقر على معيار موحد لتصنيف هذا الجرائم وكان لكل تقسيم منها مبرراته، وفي ذلك قامت هذه الاتجاهات الفقهية إلى تصنيفها رجوعا إلى الوسيلة التي ارتكبت بها الجريمة، أو الدافع على الجريمة. إلا أن هذه التصنيفات قد صنفت جرائم الحاسوب وجرائم الحاسوب والإنترنت معا، ولم تقدم تصنيفا خاصا بجرائم شبكة الإنترنت، وبالتالي السبيل الأمثل لمعالجة هذا الاختلاف في التقسيمات الانطلاق لتقسيم الجرائم عبر الانترنت من الإطار الأوسع لارتكاب هذه الجرائم دون التضييق منها أو حسرها في معيار واحد، مما يستلزم علينا الأخذ بالتقسيم التقليدي للجريمة والذي تبناه الكثير من الباحثين كونه ملما بمختلف معايير التقسيم. وهذا التقسيم يضم كلا من طائفة الجرائم الواقعة على الأشخاص، والجرائم الواقعة على الأموال، إضافة إلى الجرائم الماسة بأمن الدول.

وعلى هذا الأساس سوف نعتمد على التقسيم السابق ذكره لتقسيم هذا الباب والذي سيكون كالآتي :

الفصل الأول: العدوان الإجرامي عبر الإنترنت الماس بالأشخاص

الفصل الثاني: العدوان الإجرامي عبر الإنترنت الماس بالذمة المالية

الفصل الثالث : العدوان الإجرامي عبر الإنترنت الماس بأمن الدول

الفصل الأول:

العدوان الإجرامي عبر الانترنت الماس بالأشخاص

بالرغم من ما للإنترنت من مزايا متعددة باعتبارها عالم واسع وشبكة عالمية بدون حدود وفرت للأشخاص كل ما يحتاجونه من معلومات في شتى المجالات، إلا أن تميزها هذا حولها إلى ساحة مفتوحة لممارسة جميع أنواع الجرائم الممكنة والمحتملة للتعدي على الغير، ومن بين هذه الجرائم نجد الجرائم الماسة بالأشخاص التي تنوعت وتعددت طرق ووسائل ارتكابها، وأصبحت تختلف من شخص لأخر.

تعتبر جرائم الاعتداء على الأشخاص عبر الإنترنت من أحد أكثر أنواع الجرائم العصرية ووقوعا وانتشارا، فهي جرائم يتم ارتكبتها عبر شبكة المعلومات العالمية وخدماتها المتاحة، إذ يساء استخدامها للمساس بحياة الغير والنيل من شرفهم أو كرامتهم أو اعتبارهم أو حياتهم أو أخلاقهم أو معتقداتهم أو ديانتهم. فهي تلك الجرائم التي أصبحت تهدد بالحقوق اللصيقة بالإنسان خاصة في ما مضي، وفي حين نما استخدام خدمات الإنترنت بشكل ملحوظ، فقد شهدت هذه الفترة بشكل خاص طفرة في استخدام الهواتف الذكية، مما ساعد عددًا كبيرًا من الأشخاص على التسجيل للحصول على الخدمة، وبعد انتشار خدمات الإنترنت وتنوعها وزيادة الطلب عليها، بدأ الناس ينظرون إلى هذه الخدمة باعتبارها إحدى ضروريات الحياة اليومية الأساسية، ويعتمدون عليها في جل المجالات.

ونتيجة للاستعمال المفرط للإنترنت واتساع دائرة الإعلام والاتصال الالكتروني عبر الشبكة، ساعد مرتكبو الجرائم في تنفيذ جرائمهم واعتداءاتهم ضد الأشخاص. والإشكالية المطروحة هنا ما هي الجرائم التي يمكن أن ترتكب عبر الإنترنت ويكون هدفها المساس بالأشخاص؟ وللإجابة على هذه الإشكالية ارتأينا تقسيم هذا الفصل إلى ثلاث مباحث وهما :

المبحث الأول : الجرائم الماسة بالسمعة والشرف عبر الإنترنت

المبحث الثاني: الجرائم الماسة بالأخلاق والآداب العامة المرتكبة عبر الإنترنت

المبحث الثالث : جرائم العنف عبر الإنترنت

المبحث الرابع: الاعتداء على حرمة الحياة الخاصة

المبحث الأول : الجرائم الماسة بالسمعة والشرف عبر الإنترنت

اهتمت التشريعات والقوانين الوضعية بالإنسان وسمعته وشرفه واعتباره لأنها من أسمى الحقوق الواجب حمايتها ولأنها أساس مقومات كل مجتمع، لذا حرست اغلب الدساتير والقوانين على حماية حق الإنسان والمساس به بأي أوجه من الوجوه، خاصة في الوقت الذي انتشر فيه استخدام شبكة الانترنت والاعتماد عليها للاعتداء على هذه الحقوق بكـــل سهولة وأريحية .

إن جرائم الاعتداء على السمعة والشرف أو جرائم النشر كما يطلق عليها البعض باتت أبرز الجرائم التي تقع عبر الإنترنت وتخلف أضرارا جسيمة تجاوزت تلك التي ترتكب بالطرق الكلاسيكية .

وجرائم النشر بصفة عامة هي تلك الجرائم الموجهة للأخريين بغير حق، والماسة بكرامتهم وشرفهم، ومن أهم هذه الجرائم جريمة القذف والسب والتشهير التي سنتناولها في هذا المبحث والذي سنقسمه إلى مطلبين: المطلب الأول سنتناول فيه صور الجرائم الماسة بالسمعة والشرف عبر الإنترنت، أما المطلب الثاني فسنتناول فيه أساليب ارتكاب الجرائم الماسة بالسمعة والشرف عبر الإنترنت.

المطلب الأول : صور الجرائم الماسة بالسمعة و الشرف عبر الإنترنت

إن جريمة القذف والسب وأيضا التشهير من الجرائم التقليدية التي تطال الأشخاص، وهي نوع من الجرائم التي تتم علانية سواء بالكتابة أو القول أو الفعل أمام الناس، ولقد أصبحت هذه الجريمة من الجرائم التقليدية في التسمية والحديثة في أسلوب ارتكابها. ومن أهم الجرائم التي قد تمس بالسمعة والشرف باستعمال الإنترنت جريمة القذف والسب وجريمة التشهير.

الفرع الأول: جريمة القذف عبر الإنترنت

قبل تناول جريمة القذف عبر الإنترنت لابد لنا من تعريف القذف في اللغة والاصطلاح القانوني، وبعدها نتناول تعريف جريمة القذف عبر الإنترنت مع عرض أركانها.

الفقرة الأولى : تعريف القذف في اللغة والاصطلاح القانوني

أولا : تعريف القذف لغة

قذف بالشيء يقذف قذفا فانقذف أي رمى، والتقاذف هو الترامي وقذفه به أي أصابـــــــه، وقذف المحصنة أي سبها [1].فالقذف إذن لغة تعني الرمي.

ثانيا : تعريف القذف في الاصطلاح القانوني

القذف قانونا هو" إسناد علني عمدي، أو إدعاء بواقعة محددة تستوجب احتقار من أسندت إليه".[2]

ولقد جاء في نص المادة 296 من ق ع ج تعريف القذف على أنه " يعد قذف كل ادعاء بواقعة قد تمس بشرف الأشخاص أو اعتبارهم أو الهيئة المدعى عليها به أو إنشاءها إليهم، وأيضا يعاقب على نشر هذا الادعاء أو ذلك الإسناد مباشرة أو بطريق إعادة النشر أيضا عن طريق التشكيك أو إذا قصد به شخص أو هيئة دون ذكر الأسماء ولكن كان من الممكن تحديدهما من عبارات الصياح أو الحديث أو الكتابة أو اللافتات أو التهديد أو المنشورات أو اللافتات أو الإعلانات موضوع الجريمة " [3].

---

[1]– ابن منظور أبو الفضل جمال الدين محمد بن مكرم ، لسان العرب ، دار صادر ، بيروت، 9: 276–277، حرف الفاء، فصل القاف ، مادة قذف

[2]– محمّد صبحي نجم ، شرح قانون العقوبات الجزائري القسم الخاص ، ديوان المطبوعات الجامعية، الجزائر، 2000، ص. 78

[3]– أمر رقم 66 –155، المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات ، عدد 48 صادر بـ08 جوان 1966 المعدل والمتمم بالقانون 06–23 المؤرخ في 20 ديسمبر 2006 ، عدد 84 الصادر ب 24 ديسمبر 2006 المعدل والمتمم .

الفقرة الثانية : تعريف القذف عبر الإنترنت

لقد عرف الباحثين القذف الالكتروني على أنه " جريمة معلوماتية، تستهدف بعض الأشخاص، من خلال ألفاظ تمس "الشرف" و"الكرامة"، ويتم ذلك عبر مختلف المواقع الإلكترونية كالمنتديات وشبكات التواصل الاجتماعـــــــي والصحف الإلكترونية والبريد الإلكتروني ...إلخ من المواقع المنتشرة عبر الإنترنت.[1]

وجريمة القذف عبر الإنترنت قد تتم بطريقة علنية عن طريق الكتابة وتكون هذه الكتابة مفهومة ومقروءة من قبل عدد من الناس وتعبر عن فكرة أو معنى معين للوصول إلى النتيجة المرجوة من الاعتداء. وقد تتم عن طريق القول بواسطة تسجيل مبعوث مثلا، ويتم ذلك بين شخصين الجاني والمجني عليه، وهذا النوع من القذف يعتبر من أنواع القذف غير العلني، إلا انه قد يلحق الأذى والضرر المعنوي للشخص الذي اسند إليه القول.[2]

الفقرة الثالثة : أركان القذف عبر الإنترنت

جريمة القذف كسائر الجرائم تشترط توافر الركن الشرعي، لا جريمة ولا عقوبة إلا بنص قانوني.[3] أي اكتساب السلوك الصفة غير الشرعية، وانطباقه على نص أو قاعدة قانونية (عقابية) تجرمه. إضافة إلى وجوب تحقق ركنيها المادي والمعنوي ويتكون الركن المادي لهذه الجريمة من النشاط الإجرامي ويتمثل في واقعة الإسناد والواقعة المحددة، ويتعين أن يكون الإسناد علنيا وبذلك نتعرض لعلانية الإسناد، ويتحقق الركن المعنوي بالقصد الجنائي.

أولا : الركن المادي

يتمثل الركن المادي في نشاط غير مشروع يقوم به المجرم وهذا بقيامه بإسناد واقعة إلى الغير تمس شرفه أو اعتباره بأي طريقة من طرق العلانية، وتعد جميع الوسائل الصالحة

---

[1]– نوال العيسي ، القذف الإلكتروني ، مجلة الرياض ، الاثنين 15 ذو القعدة 1433 هـ ، 1 أكتوبر 2012م ، العدد 161، ص 70

[2] – Kenneth R osenblat , High TechnologyCrime , Investigating Cases, London , K,S,K, Publication , 1995, p 67

[3]– أنضر المادة 1 من ق ع ج

للتعبير عن الأفكار والمعاني وسائلا تصلح لإسناد الواقعة إلى الغير.[1] وبالتالي يتحقق القذف أيا كانت الوسيلة المستخدمة في ذلك سواء بالوسائل التقليدية أو بالوسائل التكنولوجية الحديثة كالحاسوب والإنترنت، ويتحقق الركن المادي في جريمة القذف عامة بتحقق عدة عناصر سنذكرها في مايلي:

1- النشاط الإجرامي.

يتمثل النشاط الإجرامي في لصق واقعة معينة تمس بشرف أو اعتبار الضحية مهما كانت الطريقة كالقول أو الإشارة أو الكتابة أو أي وسيلة من وسائل العلنية، ولهذا السبب يوصف القذف بأنه جريمة تعبر أمام الغير عن ما يدور في ذهن الجاني تجاه المجني عليه. والقذف يتحقق شريطة أن يتم بأي وسيلة من وسائل الإعلان سواء كانت قديمة أو حديثة، وكذلك بكل الأساليب التقنية التي يمكن استخدامها للتعبير عن الرأي، وقد يحدث القذف عبر الإنترنت عن طريق إرسال رسائل يمكن لكل المتصلين عبر الشبكة مشاهدتها وقراءة ما فيها.[2] فقد تكون نصًا أو صورة أو رسمًا. المهم أنها تحقق النتيجة المرجوة منها فجريمة القذف تقوم عند الكشف عن الواقعة، وكل ما يحدث عند تداولها من خلال إذاعتها عبر شبكة الإنترنت [3].

2- موضوع النشاط الإجرامي (موضوع الإسناد والواقعة المحد)

والإسناد في جريمة القذف هو الحدث المعين الذي ينسبه المتهم إلى المجني عليه، مما يمس كرامته أو شرفه. [4]ولتوافر الواقعة موضوع الإسناد يستلزم توافر شرطان :

---

[1] – الموسي سالم رضوان ، جرائم القذف والسب عبر القنوات الفضائية ، منشورات الحلبي الحقوقية ، بيروت ، ط1 ، 2012،ص 23

[2]– ربيع محمود الصغير ، القصد الجنائي في الجرائم المتعلقة بالإنترنت والمعلوماتية: دراسة تطبيقية مقارنة، مركز الدراسات العربية للنشر والتوزيع، القاهرة، طبعة 1، 2017، ، ص 246

[3] – إبراهيم كمال إبراهيم محمد ، الضوابط الشرعية والقانونية لحماية حق الإنسان في اتصالاته . الشخصية ، بلا طبعة ، دار الكتب القانونية ، مصر ، 2010 ، ص 227 وما بعدها

[4]–خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية ، ط 1، دار الفكر الجامعي ، الإسكندرية ، 2010 ، ص 421

أ-**أن تكون واقعة معينة ومحددة** يشترط في الفعل المسند إلى الغير أن يكون معينا ومحددا وإلا أصبح سبا لا قذفا .

ب-أن يكون من شأنها المساس بشرف أو اعتبار الشخص المسند إليه الواقعة: يستوجب في القذف أن يكون الإسناد تحقير للشخص ومن شأنه المساس بشرفه واعتبـــاره. وفي جريمة القذف عبر الانترنت فان الواقعة تستوجب احتقار الشخص أمام أفراد مجتمعه، كأن يقوم الشخص بنشر أخبار على المجني عليه تفيد بأنه من الشاذين أو المثليين. [1]

3- صفة النشاط الإجرامي (العلانية):

يشترط لقيام جريمة القذف علانية الإسناد هي " اتصال الجمهور بمعنى مؤذ معين تم التعبير عنه بالقول أو الفعل أو بأية وسيلة أخرى من وسائل التعبير عن الرأي أو المعني."[2]

فعلانية الإسناد لا تتجاوز ثلاث طرق تتمثل في علانية القول أو الصياح، وعلانية الإيماء أو الفعل، أيضا علانية الكتابة أو الصورة[3]، وهنا يمكننا التساؤل عن علاقة العلانية بشبكة الإنترنت؟ وفي هذا السياق ومن خلال بعض التطبيقات القضائية التي تضمنت جريمة القذف باستخدام البريد الإلكتروني أو مختلف مواقع الدردشة الخاصة كفايبر أو مسنجر أو واتساب، أثير الجدل على مدى توافر العلانية بالنسبة للبريد الكتروني ومواقع الدردشة الخاصة.

لقد عالج المشرع الفرنسي هذا الأمر بنص خاص اعتبر فيه القذف بالبريد الإلكتروني قذف غير علني وعاقب عليه في أحكام المادة 2/222 ق ع، أما القانون المصري والعراقي فهما ينصان على جريمة القذف التي تحمل وجهين قذف علني وقذف غير علني، ولكن لم يعالجا القذف عبر البريد الالكتروني بالتحديد.[4] أما المواقع الأخرى التي يمكن من

---

[1]- ربيع محمود الصغير ، القصد الجنائي في الجرائم المتعلقة بالإنترنت ، المرجع السابق ، ص 248، 249

[2]- ربيع محمود الصغير ، المرجع نفسه ، ص 253

[3]- فوزية عبد الستار ، شرح قانون العقوبات القسم الخاص ، ط 4 ، دار النهضة العربية ، القاهرة ، 2012 ، ص 573

[4]- عدي جابر هادي ، الجناية الجزائية للبريد الالكتروني ، مجلة رسالة الحقوق ، جامعة القادسية ، العدد 3 ، ص201

- استقر الفقه والقضاء المصري على اعتبار وسائل التواصل الاجتماعي وسيلة من وسائل النشر التي يتحقق معـهـــا العلانية

خلالها اطلاع كافة الناس أو بعضهم على محتواها فيرون أنها تعتبر من وسائل النشر التي يتحقق معها العلانية.

أما المشرع الجزائري فيعتبر ركن العلانية أهم ركن، فإذا غاب تصبح الجريمة مخالفة ويعاقب عليها في الفقرة الثانية من المادة 463 ق ع بعنوان السّب غير العلني، وهكذا تتطلب قيام جنحة القذف توفر العلانية إما بالقول أو الفعل أو الكتابة أو الصّورة.[1]

ثانيا: الركن المعنوي لجريمة القذف

تعد جريمة القذف عبر الإنترنت من الجرائم التي لا تحدث بسبب الإهمال أو الخطأ وهي من الجرائم التي يقصد الجاني حدوثها ولابد من توفر نوعان من العلاقة ليكون الشخص مسؤولا عنها.

1-العلاقة المادية : ومفادها أن يكون هناك ثمة ارتباط مادي تقني بين الشخص والجريمة المرتكبة ويطلق علي هذا ارتباط الإسناد المادي والذي يتم بنسبة الأنشطة التقنية التي يقوم بها الجاني باستخدام الحاسوب وشبكة الإنترنت والتي يجرمها القانون باعتبارها سلوكيات مضرة بشخص المجني عليه، وهي أنشطة تدخل في نطاق جرائم الإنترنت.[2]

2-العلاقة النفسية أو المعنوية : العلاقة المعنوية تتوافر بصدور النشاط التقني الذي يجرمه القانون عن إرادة واعية آثمة، وعليه هذه العلاقة تسمح بإسناد الجريمة للشخص من الناحية المعنوية، وهذه العلاقة في جرائم النشر عبر الإنترنت تتخذ صورة القصد الجنائي، أي اتجاه إرادة الجاني نحو تحقيق العناصر المادية التقنية للجريمة، بعكس الجرائم التي ينص القانون على تحقيق النتيجة فيها والتي تكون بسبب الإهمال أو عدم مراعاة القوانين.

تعد جرائم النشر التي تتم عبر الإنترنت جرائم عمدية والأصل لقيامها هو القصد الجنائي العام، مثل ما هو الحال بالنسبة لجريمة القذف، ومن ثم فإنه بالإضافة إلى وجود القصد الجنائي للجاني، عليه أن يعلم أيضاً أن الوقائع التي ينسبها إلى المجني عليه تمس شرفه أو كرامته أو اعتباره.[3]

---

[1]- المادة 463 من قانون العقوبات الجزائري

[2] - ربيع محمود الصغير ، القصد الجنائي في الجرائم المتعلقة بالانترنت ، المرجع السابق ، ص 285

[3] - ربيع محمود الصغير ، المرجع نفسه، ص 286

والقصد الجنائي هو علم الجاني بأركان الجريمة وإرادة موجهة نحو قبولها أو تحقيق عناصرها، بالتالي يختلف القصد الجنائي عن الباعث التي يعني بها الأسباب الشخصية التي دفعت بالجاني لارتكاب جريمته، ويختلف أيضا عن الغاية التي تمثل الهدف من الجريمة، وإن كان لا يعتد بالباعث والغاية إلا أنه قد يؤخذ بها أحيانا لتشديد العقوبة مثلا.[1]

الفرع الثاني: جريمة السب عبر الإنترنت

أصبحت مواقع التواصل الاجتماعي خلال السنوات الأخيرة، منصات للشتائم والسب، وخاصة بعد انتشار وكثرة استخدام شبكة الإنترنت، التي ساعدت على استخدام فيس بوك، وتويتر وواتس آب ويوتيوب وغيرها من المواقع التي تستعمل كوسيلة يتم عبرها السب والشتم في حق أشخاص عاديين أو في حق رجال السياسة أو في حق المشاهير... الخ، خاصة وأن هذه الوسائل لا تخضع للرقابة بصفة كلية،[2] إضافة إلى هذا أغلب من يرتكب هذه الجرائم يختفي وراء أسماء وهمية. وقبل التطرق لتعريف جريمة السب عبر الإنترنت سنتناول تعريف السب في اللغة والاصطلاح القانوني ثم عرض الفرق بين القذف والسب، وبعد ذلك نتناول تعريف السب الواقع عبر الإنترنت والأركان التي تقوم عليها الجريمة.

الفقرة الأولى : تعريف السب في اللغة والاصطلاح القانوني

أولا : تعريف السب لغة

السب: هو الشتم وهو مصدر سبه يسبه سبا : أي شتمه ، والتساب هو التشاتم وتسابوا أي تشاتموا .[3]

ثانيا : تعريف السب في الاصطلاح القانوني

السب هو التعبير الذي يحط من قدر الإنسان نفسه أو يسيء إلى سمعتـــه لدى الآخرين [4]، ولقد عرف البعض جريمة السب على أنها "خدش شرف شخص ما أو سمعته عمدًا من خلال إسناد صفة معيبة أو لفظ جارح" [5].

---

[1]– عادل عزام سقف الحيط ، جرائم الذم و القدح والتحقير المرتكبة عبر الوسائط الالكترونية: دراسة قانونية مقارنة، دار الثقافة للنشر والتوزيع ،عمان ،طبعة 1، 2010، ص 74، 76

[2]– القذف عبر الوسائل الالكترونية ، على الموقع التالي : اطلع عليه 2017 /05/1

https://akhbarelyom.com/news

[3]– ابن منظور ، مرجع سابق ، 1: 455–456 ، حرف الباء فصل السين ، مادة سب

أمـا بالنسبة للمشرع الجزائري فقد عرفها في المادة 297 من قانون العقوبات كما يلي " يعد سبا كل تعبير مشين أو عبارة تتضمن تحقيرا أو قدحا لا ينطوي على إسناد واقعة ." فالسب إذن هو كل سلوك يتضمن بأي وجه من الوجوه خدشا للاعتبار والشرف ، الشرف هو القيم التي يمنحها الإنسان لنفسه وتشكل سمعته.[1]

ومن هنا تتضح العلاقة بين جريمة السب وجريمة القذف بشكل واضح و كلاً منهما يمثل اعتداءً على شرف الناس وسمعتهم، وذلك بأن ينسب إليه أمراً أو واقعة مخزية، ولكنهما يختلفان في الفعل الوارد في كل منهما. فالقذف لا يتم إلا من خلال إسناد حادثة معينة إلى الضحية ولو كانت صحيحة ستخلف حتما ازدراءه بين أهل بلده. أما السب فيحدث عن طريق إسناد صفة أو عيب إلى الضحية دون أن يعني ذلك إسناد واقعة معينة، فإذا قيل أن هذا اشخص سرق مال من شخص أخر فهذا يعد قذفا، أما إذا وصف بالسارق فقط دون إسناد واقعة محددة يعد سبا.[2]

الفقرة الثانية : تعريف السب عبر الإنترنت

لا يخرج معنى السب عبر الإنترنت عن السب التقليدي وإنما الخلاف يكون بوسيلة ارتكاب الجريمة فهذا يكون باللسان، والأخر يكون عن طريق الكلمة والصورة وما في ذلك باستخدام تقنية الحاسوب والإنترنت. فالسب عبر الإنترنت هو تعمد إهانة شرف شخص ما أو سمعته من خلال سلوك فظ أو لغة مسيئة أو مهينة له باستخدام أحد المواقع الإلكترونية كاستخدام وسائل التواصل الاجتماعي[3]. كما يستخدم في ذلك البريد الإلكتروني أين يتم إرسال رسائل للأشخاص المراد سبها ويكون إما بإرسالها للشخص وحده أو إرسالها إلى

---

[4]– شريف الطباخ, التعويض عن جرائم السب والقذف وجرائم النشر في ضوء القضاء والفقه ، دار الفكر الجامعي، الإسكندرية, 2007, ص 137

[5]– طارق سرور ، جرائم النشر والإعلام ، دار النهضة العربية ، القاهرة ، ط1، 2004، ص 553

[1]– حنان ريحان مبارك المضحكي ، الجرائم المعلوماتية ، مرجع سابق ، ص 317

[2]– أنور طلبة، قانون العقوبات في ضوء أحكام النقض ، مجلة القضاة ، طبعة نادي القضاة سنة 1980 ، ص 641.

[3]– عمار عباس الحسيني، جرائم الحاسوب والانترنت الجرائم المعلوماتية، منشورات زين الحقوقية، بيروت، ط1، 2017ص 389

عدة أشخاص لزيادة الأذى على من وقع عليه السب وانتشارها عبر أعداد كثيرة من الناس.[1]

لقد أصبحت مواقع التواصل الاجتماعي بأنواعها المختلفة ساحة يتم فيها تصفية الحسابات الشخصية بين الناس، فغالبا ما نرى الشتائم والسب والعديد من العبارات المسيئة منشورة ومتداولة بين الأشخاص وبمختلف فئاتهم العمرية، وبات الوضع اعتيادياً رغم تجريم هذه الأفعال لحماية الأشخاص وحقوقهم وحفظ أعراضهم، ومعاقبة مثل هذه الأفعال لم يمنع الناس من تجاوزاتهم تجاه الآخرين.

الفقرة الثالثة : أركان السب عبر الإنترنت

بالإضافة إلى الركن الشرعي لتحقق جريمة السب لابد من توافر الركن المادي والمعنوي.

أولا : الركن المادي :

الركن المادي لجريمة السب عبر الإنترنت يقوم على القيام بسلوك إجرامي يخدش شرف واعتبار المجني عليه أو بمعنى أخر صدور تعبير معين يسقط من قدر المجني عليه وينال من سمعته بأي طريقة من الطرق ويتحقق النشاط الذي يمس بالشرف ويخدشه وبإسناد عيب معين للمجني عليه دون تحديد واقعة معينة لأنها ستكون جريمة قذف وليس سبا، وعليه فجريمة السب تتحقق عندما ينسب الجاني للمجني عليه صفة تحقيرية للمجني عليه مثلا كقوله أن الضحية هو قاتل أو مرتشي أو سارق أو مزور أو خائن... الخ. وعليه يعتبر سبا كل صفة منبوذة ألصقت بالشخص مثل صفة سكير متشرد أو شاذ، يتحقق أيضا السب بتشبيه الشخص بالحيوان مثل القول على شخص أنه كلب أو حمار[2].

أما النشاط الإجرامي في جريمة السب قد يكون كتابيا أو قولا أو عن طريق مواقع شبكة الإنترنت، ولا تقوم جريمة السب إلا باللفظ المعيب المشين أو الجارح إلي شخص معين، ولا يعني ذلك ضرورة التعرف على الضحية من خلال إعطاء الاسم الكامل على سبيل المثال،

---

[1]– عبد الرحمان بن عبد الله السند ، الأحكام الفقهية للتعاملات الالكترونية الحاسب الآلي وشبكة المعلومات الإنترنت ، دار الوراق ، دار النيرين ، بيروت ، الرياض ، دمشق ، ط1 2004، ص313

[2] – صدام حسين ياسين العبيدي ، جرائم الانترنت و عقوبتها في الشريعة الإسلامية و القوانين الوضعية ، المرجع السابق ص ، 157 . و انظر :عادل عزام سقف الحيط ، جرائم الذم و القدح والتحقير ، المرجع السابق ، ص 83

ويكفي أن يعرف الأشخاص أو بعض الأشخاص من تعرض للإساءة بأي طريقة كانت. وإذا لم يكن الهدف هو الإهانة فلن تتحقق الجريمة. [1] وبموجب نص المادة 297 من قانون العقوبات نص المشرع الجزائري على أركان جريمة السب والتي تقوم على ثلاثة أركان وهي: التعبير المشين أو البذيء، العلانية والقصد الجنائي. ويقوم السّب أساسا على التعبير، ويشترط فيه أن يكون مشينا أو يتضمن ألفاظ بذيئة ماجنة وتحقيرية، فالسب يتوافر بكل ما يمكنه المساس بقيمة الشخص الذاتية وبكرامته في نظر الآخرين. ويجب على المحكمة أن تتضمن في حكمها ألفاظا جارحة وإلا كان حكمها باطلا لقصور الأسباب، ولا تقع الجريمة إذا كانت عبارات السب عامة مست بأشخاص وهميين، ولا يهم الوسيلة أو الطريقة التي يتم بها صياغة عبارات السب سواء كان صريحا أو ضمنيا.[2]

أما بالنسبة لركن العلانية لم يشر المشرّع الجزائري صراحة عليه في نص المادة 297 من قانون العقوبات عكس القانون الفرنسي والمصري الذي اشترط العلانية في الجنحة، فإنّ ما نصّت عليه المادة 463 من ق ع ج ومؤداها أن " كل من توجه لأحد الأشخاص بألفاظ سباب غير علنية ومن غير استفزاز يعاقب بغرامة من 30 إلى 100دج ويجوز أن يعاقب أيضا بالحبس لمدة ثلاثة أيام على الأكثر"، ويدل على أن عدم الإشارة إلى العلانية مجرد سهو وبالتالي انعدام العلنية يحول الجريمة من جنحة السّب إلى مخالفة السّب غير العلني المعاقب عليها بموجب الفقرة 2 من المادة 463 من ق ع ج.

ثانيا : الركن المعنوي

إن القصد الجنائي في جريمة السب عبر الإنترنت هي قصد عام وتتطلب توافر عنصري العلم والإرادة .

وعنصر العلم يتحقق بثبوت علم الجاني بمعنى الألفاظ التي صدرت منه، وإدراكه تماما بما تتضمنه هذه الألفاظ من خدش ومساس لشرف واعتبار المجني عليه وبما سيلحق به من أضرار جراء هذا السلوك الغير شرعي. أما عنصر الإرادة فيكون بتوجه إرادة الجاني

---

[1] – صدام حسين ياسين العبيدي ، المرجع السابق ، ص157

[2] – أحسن بوسقيعة، الوجيز في القانون الجنائي الخاص، ج 1، دار هومه للطباعة والنشر والتوزيع ، الجزائر،2008 ص 198

إلى إتيان فعل مادي غير مشروع يتمثل في القول أو الكتابة أو باستعمال أي وسيلة من وسائل الاتصال عبر الإنترنت أو عبر أيا من مختلف المواقع المنتشرة عبرها.[1]

الفرع الثالث : جريمة التشهير عبر الإنترنت

يرى الفقهاء أن المعنى الضيق لجرائم النشر يجب أن تشمل أكثر من الصحف والمجلات، لأن أجهزة الكمبيوتر والإنترنت تجعل هذه الجرائم تمتد ليدخل ضمنها الجرائم التي ترتكب عبر الوسائل الإلكترونية ومن أهمها شبكة المعلومات الدولية الإنترنت.

وبناء على ما سبق يمكن تعريف جرائم النشر على أنها كل جريمة ترتكب علناً من خلال الصحف التقليدية أو الإلكترونية. ومن أهم هذه الجرائم جريمة التشهير. وسنطرق من خلال هذا الفرع لمختلف التعريفات الخاصة بجريمة التشهير.

الفقرة الأولى : تعريف التشهير في اللغة والاصطلاح القانوني

أولا : تعريف التشهير لغة

التشهير مأخوذ من كلمة شهره، بمعنى أعلنه وأذاعه، وشهر به، أذاع عنه السوء، والشهرة ظهور الشيء وانتشاره، حتى يشهره الناس، والشهرة الفضيحة.[2]

ثانيا : تعريف التشهير في الاصطلاح القانوني

وضع القانونيين تعريفات عدة للتشهير أهمها" أنه إشاعة السوء عن إنسان بقصد الإضرار بسمعته والحط من قدره بذكر عيوبه وصفاته السيئة والتنقيص منه وذكر أخطاءه التي وقع فيها.[3] أيضا يمكن تعريفها على أنها "إلحاق فضيحة بفرد واحد أو مجموعة من الأشخاص ونشرها على الملأ، الأمر الذي يسبب لهم ضررا نفسيا ، ويجعلهم منبوذين من

---

[1]– صدام حسين ياسين العبيدي ، جرائم الانترنت و عقوبتها في الشريعة الإسلامية و القوانين الوضعية ، المرجع السابق ص 152 ،

[2]– ابن منظور ، المرجع السابق ، 4:431–432 حرف الراء ، فصل الشين ، مادة شهر

[3] – هروال هبة نبيلة، جرائم الانترنت "دراسة مقارنة" ، المرجع السابق ، ص 76

طرف المجتمع المحيط بهم، وكل هذا سببه السعي وراء الحصول على مصالح أو تحقيق أرباح مالية".[1]

الفقرة الثانية : تعريف التشهير عبر الإنترنت

عرف التشهير عبر الإنترنت بأنه:" استخدام الإنترنت لنشر مواضيع مضرة بسمعة وكرامة الغير، سواء كان ذلك عن طريق إحدى الصحف الالكترونية أو بواسطة البريد الإلكتروني أو من خلال النشر على لوحة الإعلانات الإلكترونية عبر الإنترنت، أو أية وسيلة أخرى متاحة على شبكات الإنترنت ".[2]

إن التشهير عبر الإنترنت أو كما يطلق عليه الفضح السيبيراني هو فضح أفعال تم فعلها في الخفاء ونقلها للعلانية عبر الفضاء السيبيراني، ويرى البعض أنه أداة تشجع التسلط عبر الإنترنت والمهاجمة والتنمر عبر الإنترنت، وغايته تدمير سمعة الأشخاص، وعادةً ما يتضمن التشهير عبر الإنترنت نشر معلومات سرية عبر الإنترنت باستخدام مستندات أو وثائق قد تكون مزورة أو مفبركة [3].

إن ارتكاب جريمة التشهير في تزايد مستمر خاصة في الوقت الذي انتشر فيه استخدام مواقع التواصل الاجتماعي المتوفرة عبر الإنترنت، وهي طريقة للإساءة للسمعة ويكون الغرض منها في أغلب الأحيان التنافس الوظيفي أو التنافس الحزبي أو التنافس الانتخابي أو التجاري أو للانتقام الشخصي أو لتشويه السمعة، وإن كان الدستور قد أتاح كشف قضايا الفساد وأعطي أيضا الحق في النقد، إلا أن حق النشر قد رسمه القانون وفق شروط محددة لا يجوز تجاوزها، ولا يسمح القانون بانتهاك حرمة خصوصية الناس إلا إذا كان لتحقيق المصلحة العامة، حيث أن النقد البناء هدفه كشف الحقيقة أما جريمة التشهير عبر الإنترنت سلوك غير قانوني، حيث أن النقد يتعلق بوقائع ثابتة ومعلومة للجمهور، أما

---

[1]– التشهير بالناس على الطريقة الإلكترونية ، اطلع عليه 2017/05/20
https://ar.islamway.net/article/35081/

[2] – عمر سامان فوزي ، المسؤولية المدنية للصحفي .دراسة مقارنة ، دار وائل للنشر والتوزيع ،عمان ،الأردن ، ط1 ،2007، ص242

[3]– https://ar.islamway.net/article/35081/ التشهير بالناس على الطريقة الإلكترونية ، اطلع عليه 2017/05/20

التشهير فهو يتعلق بأمور قد تكون غير معلومة للجمهور، وتتعلق بالحياة العامة أو الخاصة للمشهر به.[1]

الفقرة الثالثة : أركان التشهير عبر الإنترنت

كما هو الحال بالنسبة لجريمتي القذف والسب فإن لجريمة التشهير عبر الإنترنت ركنان مادي ومعنوي سنتناولهما تباعا كما يلي :

أولا :الركن المادي للتشهير

الركن المادي لجريمة التشهير يتحقق من خلال فعل التشهير وهو النشاط الإجرامي الغير مشروع، وينصب على موضوع معين وذلك بالتعبير عن فكرة أو معنى يراد به التشهير بشخص أمام العديد من الأشخاص بالقول أو عن طريق النشر بالصحف أو المجلات أو الإذاعة أو التلفزيون أو عبر وسائل الاتصال أو المواقع الالكترونية عبر الإنترنت .

ويشترط لقيام الجريمة توافر عنصر العلانية وذلك عبر الاعتداء على سمعة المجني عليه عن طريق أي وسيلة من وسائل العلانية، والعلانية تشمل كل الطرق التقليدية والطرق المستحدثة، من أهمها الطرق العلنية المستحدثة شبكة الإنترنت التي تعتبر علانيتها بدون حدود، إضافة إلى اعتبارها اخطر وسائل العلانية لاستخدامها من طرف المجرمين للتشهير بالأشخاص بكل سهولة [2]، وأصبحت من الجرائم المنتشرة بشكل كبير على مستوى العالم بأكمله. كما حدث في جويلية 2015، حيث قام عدد من الهاكرز باختراق البيانات الخاصة بمستخدمي موقع آشلي ماديسون، الذي يعد من أهم المواقع التجارية للمواعدة ويساعد الأشخاص على تسهيل خيانتهم لأزواجهم.

ويرى علماء النفس السريري أن الخيانة الزوجية تزيد من الضرر الذي يلحق بالشريك والأطفال إذا ما تم التعامل معها بطريقة علنية. وبأن وسائل التواصل الاجتماعي خلقت ثقافة عدوانية للإذلال العلني، حيث يمنح للأشخاص الحق في إلحاق الأذى النفسي يمن

---

[1] – الموسي سالم رضوان ، جرائم القذف والسب عبر القنوات الفضائية، المرجع السابق ، ص 112

[2] – يوسف صغير ، الجريمة المرتكبة عبر الانترنت ، رسالة ماجستير ، جامعة مولود معمري ، تيزي وزو ، كلية الحقوق والعلوم السياسية ، 2013

يعتقدون أنهم يستحقونه. وفي معظم الحالات تتجاوز العقوبة ما تستحقه الجريمة. وقد أضاف الخبير تشارلز جيه أورلاندو، الذي قام بإجراء أبحاث خاصة بالنساء اللاتي خنّ أزواجهن، واستنتج خوفهم من أن المواقع قد تتسبب في نشر رسائلهن الجنسية الصريحة وإلى إذلال أزواجهن وأطفالهن، إضافة إلى أن مثل هذه الأمور تثير القلق كون الأشخاص على الإنترنت يأخذون دور القاضي والجلاد في أغلب الأحيان. ولا يمكننا معاقبة الأشخاص على المواقع الافتراضية بوجود الملايين من المتفرجين[1].

ثانيا :الركن المعنوي للتشهير

تعد جريمة التشهير أيضا من الجرائم العمدية والتي تستلزم توافر عنصري العلم والإرادة، وعنصـــر العلم يتحقق بثبوت علم الجاني بما ستخلفه الواقعة التي أسندها للضحية ، وأن يتوفر لدى الجاني أيضا إرادة الإسناد لهذه الواقعة، إضافة إلى توافر عنصر العلانية بـــأي وسيلة من وسائل العلانية المنتشرة والمختلفة بما فيها شبكة الإنترنت .[2]

المطلب الثاني : صور وأساليب ارتكاب الجرائم الماسة بالسمعة والشرف عبر الإنترنت

بدأت ظاهرة جرائم السب والقذف والتشهير على الإنترنت تتوسع في الآونة الأخيرة، حيث أصبح من السهل على المستخدمين مهاجمة الآخرين من خلال وصفهم بألفاظ مسيئة ومهينة أمرا شائعا. ويتخذ الجناة في هذه الظاهرة عدة أساليب بعضهم يستخدم هويات مزورة لإخفاء هويتهم وتسهيل عملية الاعتداء على الآخرين، والبعض الآخر يختار الأساليب المباشرة، مثل التعليقات المهينة أو تشويه الصور الشخصية لأشخاص معينين. وما يزيد الطين بلة هو صعوبة السيطرة على هذا النوع من الجرائم، فهي تنتشر بسرعة كبيرة وتسبب الكثير من المشاكل والأضرار النفسية.

---

[1]–Ashley Madison Hack Could Have A Devastating Psychological Fallout,

http://www.huffingtonpost.com/entry/ashley-madison-hack-psychological-fallout_55d4afcee4b07addcb44f5d4 .2017/06/03 اطلع على الموقع

[2]– صدام حسين ياسين العبيدي ، جرائم الانترنت و عقوبتها في الشريعة الإسلامية و القوانين الوضعية ، المرجع السابق ص 176. وانظر :سعد حماد صالح القبائلي ، الجرائم الماسة بحق الإنسان في السمعة و الشرف والاعتبار عبر الإنترنيت، المؤتمر المغاربي الأول حول المعلوماتية والقانوني ، مدينة طرابلس– ليبيا ، أكتوبر 2009

وعليه تتنوع طرق وأساليب الجرائم الماسة بالسمعة والشرف عبر الإنترنت، وفي كل الحالات ترتكب هذه الجرائم من خلال عدة خدمات ومواقع متوفرة على النت وتتمثل في ما يلي:[1]

الفرع الأول: البريد الإلكتروني والمبادلات الإلكترونية:

الفقرة الأولى: البريد الإلكتروني

أصبح يشكل البريد الإلكتروني وسيلة اتصال أساسية في أغلب مجالات العمل، وأصبحت اليوم وسيلة للمراسلة بين مستخدمي الإنترنت كافة[2].

الفقرة الثانية: المبادلات الإلكترونية:

قد تحدث الجرائم الماسة بالسمعة ضمن المبادلات الإلكترونية التي تكون بين طرفين متصلين بالويب العالمية، وهي أكبر شبكة اتصالات على الإنترنت والأفضل بين جميع التقنيات لأنها منصة وسائط متعددة تجمع بين العديد من الخدمات المتاحة عبر الإنترنت. تُرتكب الجرائم الماسة بالسمعة والشرف عبر الإنترنت من خلال أي شيء مكتوب أو صوتي أو سمعي بصري يسيء إلى شرف الناس إما عن طريق إسناد أو ذكر حدث معين يبرر ازدراء الشخص المنسوب إليه، وهو في معظم الأحيان يكون بالشكل الكتابي، أو بنشرها على مواقع الويب في كتابات أو رسومات أو صور ساخرة، أو عبر البطاقات البريدية التي تسيء إلى الضحية[3].

الفرع الثاني: غرف المحادثات والدّردشة ومواقع التواصل الاجتماعي:

الفقرة الأولى: غرف المحادثات والدّردشة chat rooms

غرف المحادثات مساحات تسمح لروادها التواصل والتخاطب بشكل مباشر مع بعضهم البعض، وتعمل بطريقتين عامة وخاصة:

---

[1]–أحمد أمين أحمد الشوابكة، جرائم الحاسوب و الانترنت و الجريمة المعلوماتية، ط 1، دار الثقافة للنشر والتوزيع، الأردن،2009 ، ص 32.

[2]– عادل عزام سقف الحيط ، جرائم الذم و القدح والتحقير المرتكبة عبر الوسائط الالكترونية ، المرجع السابق، ص 202

[3]– عادل عزام سقف الحيط ، المرجع نفسه ص 199

بالنسبة للعامة تكون فيها المحادثة متاحة يلجا لها من يشاء من متصفحي الموقع، أما الخاصة فهي تقتصر على عضوين أو مجموعة خاصة ينشئها الأعضاء أنفسهم، ويستخدمون خادم الدردشة الجماعية مثل ما هو متوفر في خدمة مسنجر لإجراء محادثة خاصة، وعند مخاطبة مجموعة من الأعضاء في نفس مجموعة الدردشة يقوم المستخدم بإرسال الرسالة التي كتبها على لوحة المفاتيح ليتم عرضها. وهكذا قد تحدث جريمة التشهير عن طريق غرف الدردشة لإهانة شرف واحترام أي فرد، وهذا عن طريق إسناد أو تأكيد واقعة معينة نتيجتها ازدراء المتضررين[1].

الفقرة الثانية: مواقع التواصل الاجتماعي

يستغل الأشخاص الخدمات المتوفرة في المجال الافتراضي وخاصة في استعمالهم لمواقع التواصل الاجتماعي المتنوعة، فيتبادلون عبرها أفكارهم وأحاديثهم، ولكن في كثير من الأحيان ما تصبح هذه المواقع سبيلا للنيل من سمعة وكرامة الآخرين عن طريق السب والقذف والتشهير. نظرا لكون شبكات التواصل الاجتماعي توفر فرصة مخاطبة الأشخاص عن بعد وفي كثير من الأحيان خلف أسماء وشخصيات مستترة الأمر الذي يجعل المساس بشرف واعتبار الأشخاص أمرا في غاية اليسر والسهولة.

فقد أصبحت ظاهرة السب والشتم منتشرة بشكل كبير على مواقع التواصل الاجتماعي في الآونة الأخيرة. ولقد أصبحت فضاءا واسعا لضعاف النفوس وأداة لتحرير أنفسهم من صعوباتهم وضغوطهم النفسية، غير مهتمين بمن سيتضررون بالكلمات الجارحة وبالسب والشتم والتحقير. فلماذا أصبح الكثير من الكراهية تهيمن على مواقع الإنترنت، ولعل كل هذا وذاك يعود إلى الحرية المطلقة التي تشعر بها هذه الفئة خلف شاشاتها دون رقابة أو تنظيم، فضلا عن إيمانها بأن عالم الإنترنت يمنحها حرية التعبير غير المشروطة. فهم يمنحون أنفسهم الحق في قول ما يريدون دون أي مسؤولية أو تقدير لمشاعر الشخص الذي يتحدثون عليه.

[1]– عادل عزام سقف الحيط ، المرجع نفسه ، ص 203

المبحث الثاني:

الجرائم الماسة بالأخلاق والآداب العامة المرتكبة عبر الإنترنت

ليست كل الأفعال المخالفة للآداب العامة والأخلاق التي يجرمها التشريع يمكن ارتكابها عبر شبكة الإنترنت أو من خلالها، ولكن ما ترتكب عبرها تعد أخطرها وأشدها أثراً على كافة المجتمعات والمجتمعات الإسلامية بصفة خاصة، أهمها لعب القمار والجرائم الإباحية بالإضافة إلى الاستغلال الجنسي للأطفال، هذا الأخير الذي يعتبر صورة من صور الجرائم الجنسية المرتكبة عبر الإنترنت ولخطورته و كثرة انتشاره سيتم دراسته بقليل من التفصيل في مطلب خاص به.

وعليه سنتناول أكثر الجرائم المخلة بالأخلاق خطورة من خلال المطالب الثلاثة الآتية: الأول سنتناول فيه القمار عبر الإنترنت، والثاني سنتناول فيه الجرائم الجنسية والإباحية عبر الإنترنت، أما المطلب الأخير سنخصصه للاستغلال الجنسي للأطفال .

المطلب الأول : القمار عبر الإنترنت

من الظواهر التي لها الأثر البالغ سلبا على الأشخاص ألعاب القمار لاعتبارها ظاهرة سلوكية خطيرة مخالفة للآداب العامة ومخالفة لما جاءت به أحكام الشريعة الإسلامية، ولقد انتشرت هذه الظاهرة منذ القدم وكان دافعها الأساسي هو الرغبة الكبيرة داخل النفس الإنسانية لجني الأموال بسهولة وبدون أي عناء أو كد، ويجد الإنسان نفسه مدفوع بهذه الرغبة ليخوض تجربة القمار لجني الأموال وللفوز بالغنيمة.

وبفضل انتشار شبكة الإنترنت ظهر نوع جديد من القمار وهو القمار الإلكتروني يتم عبر الإنترنت والذي انتشر عبر العالم بطريقة مذهلة وبات يشكّل خطرا كبيرا خاصة على فئة الشباب، ومن الدوافع التي تكمن وراء تفضيل اللاعبون لممارسة القمار عبر الإنترنت، كونها متاحة بسهولة، إضافة إلي ذلك عدم وجود أية إشكاليات قانونية، ولأن مواقع القمار أون لاين تتيح اللعب للجميع مهما كانت جنسيتهم أو ديانتهم.

الفرع الأول : مفهوم القمار عبر الإنترنت

في هذا الفرع سنعرض أهم التعريفات التي أسندت للقمار

الفقرة الأولى :تعريف القمار لغة

القمار يعني طلب الغرَّة والمخادعة : تقمّرها : طلب خدعها، قال في لسان العرب: كأن القمار مأخوذ من الخداع[1]. ومن القمار : الرهان، ويقال: قامره فقمره : بمعنى غلبه في لعب القمار[2].

الفقرة الثانية :التعريف الفقهي والقانوني للقمار

القمار هو إجراء أو قرار محفوف بالمخاطر تتخذه على أمل الحصول على المال أو النجاح أو الميزة على الآخرين. ومن مرادفات القمار : خطر، فرصة، مغامرة، يانصيب الخ من مرادفات المقامرة، فإذا كنت مقامرًا بشيء ما، فإنك تتخذ إجراءً أو قرارًا محفوفًا بالمخاطر على أمل الحصول على المال أو النجاح أو التميز على الآخرين، والأشخاص الذين يقامرون عادة ما يفعلون ذلك بشكل متكرر إلى درجة قد تصل إلى الإدمان عليه[3].

ومن الناحية القانونية لقد عرف القمار على انه " كل لعب يحتمل الكسب والخسارة متوقفا على الحظ لا على عوامل يمكن تعيينها والسيطرة عليها مستقبلا."[4]

وبالرجوع إلى المشرع الجزائري لم يتناول تعريفا محددا لجريمة القمار وإنما جاءت أحكام المادة 165 ق ع ج نصت على القمار واليانصيب وبيوت التسليف وعلى الرهون وجاء في مضمونها عدم جواز فتح بغير ترخيص أي محل للألعاب الخاصة بالحظ.[5]

الفقرة الثالثة : تعريف القمار عبر الإنترنت

قبل ظهور التقنية المعلوماتية فإن لعب القمار كان يستلزم وجود لاعبين على طاولة واحدة و يتقدم كل لاعب للرهان على ما يرى أنه الفائز، ولكن وبعد انتشار العولمة وانتشار مواقع الانترنت عبر مختلف أنحاء العالم أصبح لعب القمار يتم من المنازل والمقاهي وأماكن العمل وكل مكان يتوفر فيه الحاسب الآلي والانترنت، لذلك برزت العديد من المواقع المتخصصة لتسويق لهذه الألعاب بل توجه العديد من المواقع لاستخدامها كغطاء

---

[1]– ابن منظور ، لسان العرب، ج5 ، المصدر السابق، ص 114

[2]– مختار الصحاح، ص 230، لسان العرب، ج5 ص 115

[3]–https://www.collinsdictionary.com/dictionary/english/gamble

[4]– حنان ريحان مبارك المضحكي ، الجرائم المعلوماتية ، المرجع السابق، ص 251

[5] – المادة 165 من قانون ع ج

لممارسة جرائم غسيل الأموال. ومن المواقع الالكترونية المتخصصة في القمار للعرب موقع www/onlinecasinosinarabic.com وكانت الغاية من وراء إنشاءها جذب المستخدمين العرب للتعامل معها، إضافة إلى مختلف مواقع القمار مفتوحة للاعبين عبر كافة أرجاء العالم، ولا يهم البلد الذي يعيشون فيه، حتى لو كانت نوادي القمار غير قانونية في بلد إقامتهم. والأغلبية الكبيرة لأندية القمار على الإنترنت توفر أيضا إمكانية مرور خاصة لجميع الألعاب التي اشتهرت بطريقة متعارف عليها بين اللاعبين العرب والأوروبيين وكذلك الآسيويين.

ولتلبية رغبات الزبائن عبر كافةّ أنحاء العالم، تسمح نوادي المقامرة عبر الإنترنت للاعبين بتحويل الأموال إلى عملتهم أو بنكهم. بالإضافة إلى ذلك قامت بعض نوادي المقامرة عبر الإنترنت بنشر مواقع مقامرة متعددة اللغات حتى تتضمن اللغة العربية لتسهيل اللعب على العرب.[1]

إن قواعد المقامرة الإلكترونية تشبه تماماً المقامرة العادية التي يلعبها الأفراد في الألعاب المتوفرة في الفنادق الكبيرة، وكذلك تتشابه أسماء الألعاب مثلاً البوكر والبلاك جاك والروليت، ويتم تشغيلها عن طريق محرك البحث المتوفر على "غوغل". ولقد غمرت الإنترنت العشرات من مواقع القمار حيث تروج لخدماتها بمميزات ورسوما جذابة، وإذا كان الباحث في الموقع مهتمًا ويريد المشاركة في التجربة، فسوف يطلب منه تقديم عنوان بريده الإلكتروني وكلمة المرور، لإنشاء حساب خاص به، وبعده تكون عملية اختيار لعبة الرهان، وشروط العملية الموضحة على الشاشة، وتحديد المبلغ المراد إيداعه [2].

وفي بعض الدراسات التي نشرت في بريطانيا أظهرت قلق المسؤولين نظراً للزيادة الهائلة في عدد المدمنين على المقامرة عبر الإنترنت، ولأن حجم الأموال المتداولة يعد بالمليارات. وقد حذرت مجلة "إندبندنت" من ارتفاع عدد المقامرين خاصة وأن مكاتب المراهنات تسعى بكل الطرق لإغواء مزيد من المقامرين، وقد أظهرت الإحصائيات أن حوالي مليون شخص

[1] – حنان ريحان مبارك المضحكي ، الجرائم المعلوماتية ، المرجع السابق، ص 252

[2] – القمار الالكتروني، https://alarab.co.uk

سنويا معرضين لخطر الإدمان على المقامرة عبر الإنترنت، في حين تضاعف عدد الأشخاص المدمنين فعلياً في السنوات الماضية إلى حوالي 500 ألف مدمن سنويا.[1]

وبالرجوع إلى ما سبق ذكره يمكن تعريف القمار عبر الانترنت بأنه كل لعب يتم عبر شبكة الإنترنت ويحتمل فيه الربح أو الخسارة المعتمدة على الحظ لا على عوامل يمكن التحكم فيها أو السيطرة عليها. أو يمكن تعريفه أيضا بأنها مجموعة رهانات وألعاب وممارسات يقوم بها اللاعب أو مجموعة من اللاعبين، عبر وسيلة الاتصال الالكتروني والمتمثلة في شبكة الانترنت، بحيث يقومون من خلالها باللعب أو المراهنة من أجل الكسب المالي معتمدين في ذلك على مبدأ الحظ والنصيب.

الفرع الثاني: أركان القمار عبر الإنترنت

القمار عبر الإنترنت كأي جريمة أخرى يشترط لقيامه توافر الركن المادي والمعـــــنوي.

الفقرة الأولى :الركن المادي

في الجريمة التقليدية يتحقـق الركن المادي بإعداد وتجهيز مكان لممارسة العاب القمـار فيه وتهيئة المحل أي أن المكان أصبح جائزا لاستقبال الجمهور فيه لممارسة ألعاب القمار، ولا تتجه التشريعات لتحديد العاب القمار على سبيل الحصر بل تكتفي للإشارة إليها بأنها العاب تحتمل الربح والخسارة على عوامل مرتبطة بالحظ أكثر من المهارة، ومحل القمار عادة ما يكون مالا أو شيء يمكن تقويمه بالمال.

أما في القمار عبر الإنترنت فيتوفر الركن المادي بإعداد موقعا الكترونيا أو بإنشاء غرف دردشة تقوم مقام المكان للممارسة القمار، من خلالها وعبرها يتم القمار، وعليه يتحقق الركن المادي بدخول المقامرون هذه المواقع أو الغرف المخصصة لذلك[2].

---

[1]– عمل البرلمان البريطاني على استصدار تشريع من شأنه أن يحد من ظاهرة إدمان القمار ، خاصة في ظل نمو الهائل لمواقع القمار وتمكنها من استقطاب زبائن جدد من الطبقة المتوسطة والنساء. ولأنهم يعتبرون إدمان القمار بأنه يضاهي في خطره الإدمان على تعاطي الكحول وقد أعرب بعض البرلمانيين عن قلقهم من أن القانون المقترح سيأتي بعد فوات الأوان لمحاربة القمار. www.aljazeera.net /2013/1/27

[2]– حنان ريحان مبارك المضحكي ، الجرائم المعلوماتية ، المرجع السابق، ص 253

الفقرة الثانية :الركن المعنوي

يتمثل الركن المعنوي في القصد الجنائي الذي يتحقق بتوافر العلم والإرادة بالسلوك ونية التوصل لنتيجته والمتمثلة في الحصول على كسب مادي من وراء الدخول للمواقع المخصصة للقمار عبر الانترنت وتتحقق النية أيضا حتى ولم يحصل المقامر علي مبالغ نتيجة مقامرته أو خسارته لأمواله .[1]

وبالرغم من انتشار ظاهرة القمار عبر الانترنت وانتشار الإدمان عليها، وباعتبارها كارثة حقيقية تهدد أغلب فئات المجتمع إلا انه لا توجد قوانين حقيقية تمنعه أو تعمل على تقيده أو تفرض الرقابة عليه، لذلك بات من الضروري وضع قوانين تنظيمية لممارسة القمار عبر الإنترنت، وضوابط تمنع من انتشاره أو تقلله على الأقل كتقيده لفئة معينة من الأشخاص فقط خاصة بالنسبة للدول الإسلامية .

المطلب الثاني: الجرائم الجنسية والإباحية عبر الإنترنت

تعد الاعتداءات الجنسية من أخطر الجرائم الموجهة ضد الأشخاص وتعود مدى خطورتها لكونها جرائم تمس بالسلامة الجسدية والحرية الجنسية، وهي في مجملها خروج عن النظم والمعايير الموضوعة من طرف المجتمع، إضافة إلى تنافيها مع مجمل التقاليد والديانات. وتشمل الجرائم الجنسية كل الأفعال والسلوكيات التي تهدف إلى الإشباع الجنسي بطرق غير شرعية.

ولقد ازدادت خطورة الجرائم الجنسية والإباحيـــــة في الوقت الحاضر نتيجة لدخول تقنية الإنترنت والحاسب الآلي الذي سهل حصول هذه الجرائم ووسع من انتشارها، كإنشاء مواقع إباحية أو نشر صور خليعة أو أفلام إباحية وترويجها أو إرسالها من أي مكان يتواجد فيه الجاني سواء المنزل أو مكتب العمل أو أي مكان أخر.

لذا سنتناول في هذا المطلب التعريف بالجرائم الجنسية والإباحية عبر الانترنت ومدى انتشارها، والأركان الواجب توافرها لتحقيقها .

[1]– حنان ريحان مبارك المضحكي ، المرجع نفسه ، ص254

الفرع الأول : تعريف الجرائم الجنسية والإباحية عبر الإنترنت

إن تعريف الجرائم الجنسية والإباحية عبر الإنترنت يقتضي أولا التعريف بمصطلحي الجنس والإباحية، وبعد ذلك نتطرق لتعريف الجريمة الجنسية والإباحية .

الفقرة الأولى : التعريف بمصطلحي الجنس والإباحية

قبل تعريف مصطلح الإباحية سنتطرق لتعريف الجنس أولا من الناحية اللغوية ثم من ناحية الاصطلاح.

أولا : تعريف الجنس لغة واصطلاحا

1-تعريف الجنس لغة

"جنسي مفرد اسم منسوب إلى جنس، تناسلي ، يغلب استعماله فيما يتعلق بالاتصال الشهواني و بعملية التوالد والأعضاء الجنسية ".[1]

2-تعريف الجنسية اصطلاحا :

الجنس هو نشاط جسدي فطري في معظمه، قد يرتبط بمشاعر أو التزامات نفسية أو معنوية تكون بين الطرفين، وفي بعض الثقافات قد يحدث أن يمارس الشخص الجنس مع فتاة لا يعلم حتى اسمها، أو تمارس فتاة الجنس مع شخص لا تعرفه من قبل وبعد انتهاء العلاقة قد لا تراه مرة أخرى، أيضا قد تتم ممارسة الجنس بمقابل مادي، وقد يحدث الجنس بالقوة أو بالإكراه أو بالاغتصاب[2].

ثانيا: تعريف الإباحية لغة واصطلاحا

1-تعريف الإباحية لغة

الإباحة عند أهل اللغة: تعبر عن عدة معان نذكر منها ما يتصل بمعناها الفقهي وذلك قولهم: " أحللت وأبحت الشيء، وأباح الشيء أي أطلقه له"[3].

---

[1] – أحمد مختار عمر، معجم اللغة العربية المعاصرة، عالم الكتب، القاهرة مجلد 1، طبعة 1، 2008

[2]– محمد طه ،الجنس و العلاقة الجنسية ، بحث منشور على الرابط التالي : أنظر الرابط التالي:
https://www.sehatok.com/psychology/2016/10/8/

[3]– إبن منضور ، لسان العرب. المرجع السابق، مادة أباح

2-تعريف الإباحية اصطلاحا

الإباحية لا تعني العلاقة الجنسية بين اثنين، بل تعني نشر هذه العلاقة الخاصة الحميمة أمام العامة. فالعلاقة بين اثنين هي مسألة شخصية ما دامت تتم بين جدران الغرفة سواء متزوجين أو غير متزوجين. وقد تصبح إباحية حتى لو توفر عنصر الزواج إذا قام هؤلاء بتسجيل علاقتهم الخاصة ونشرها أمام العامة، أو خروجها من غرف النوم إلى الحدائق والأماكن العامة هنا يتحقق فعل الإباحية. أيضا هناك نوع أخر من الإباحية وهي اللفظية عن طريق نقل القصص عن الأشخاص والكلام في أعراضهم.

الفقرة الثانية : تعريف الجريمة الجنسية عبر الإنترنت

الجريمة الجنسية هي كل التصرفات أو السلوكيات التي تهدف إلى الإشباع الجنسي بين الرجل والمرأة، أو بين شخصين من نفس الجنس، أو بين شخص من أي الجنسين وحيوان. وهذه الأفعال يحرمها الدين والقانون والعرف في العالم العربي وفي معظم أنحاء العالم. "[1]

ومن خلال التعريف القانوني للجريمة الجنسية التقليدية يمكن تعريف الجريمة الجنسية عبر الإنترنت بأنها كل الأفعال والسلوكيات الغير شرعية التي تتم عبر الإنترنت والهدف منها الإشباع الجنسي للأفراد بطرق افتراضية.

الفقرة الثالثة : التعريف بالجريمة الإباحية عبر الإنترنت

إن التعريف القريب من الجريمة الإباحية في وقتنا الحالي والذي ينطبق على الجريمة الإباحية عبر الإنترنت هو تعريفها بأنها" كل ما يحتوي على جنس فاضح وضمني من الصورة العارية الكاشفة للعورة إلى الفيلم الذي يعرض العلاقة الجنسية بجميع التفاصيل بين أطراف مختلفة، سواء كان أطفال أو بالغين، ويكون هدفها الأساسي إثارة الرغبة الجنسية لدى الجمهور، بغض النظر عن وسيلة تقديمها."[2]

ويمكن أن نعرفها أيضا استنادا إلى التعاريف السابقة للجريمة الجنسية، مع الأخذ بعين الاعتبار أن الوسيلة الالكترونية هي أداة الإيصال أو النشر أو تبادل أو تخزين أو ما يمثلها من أفعال تتصل بموضوع الجريمة عبر الإنترنت وهي الأفعال الإباحية. وعليه يمكن

---

[1]- علي الحوات، الجرائم الجنسية ، دار الحامد للنشر، عمان، 2014 ص 18

[2]- ميلود بن عبد العزيز، الجرائم اللإباحية وأثرها من منظور شرعي وقانوني، مجلة دراسة وأبحاث العدد 1، رقم 1، 2009/09/15، ص80

تعريف الجريمة الإباحية عبر الإنترنت بأنها كل فعل يتمثل في إرسال أو نشر إباحي أو يتمثل في معالجة أو حفظ أو طباعة أو ترويج أعمال تتصل بالدعارة والأعمال الإباحية التي تتم عن قصد عبر شبكة الإنترنت .

ولقد نص على الجرائم الجنسية مشروع الاتفاقية الأوروبية لجرائم الإنترنت والكمبيوتر 2000-2001 واعتبرها من الجرائم المتعلقة بالمحتوى وتشمل طائفة واحدة حسب ما جاءت به هذه الاتفاقية وهي الجرائم المتعلقة بالأفعال الإباحية والأخلاقية.[1]

بالإضافة إلى ذلك، تحاول هذه المواقع الإباحية دائمًا تبسيط طريقة الوصول إلى مواقعها، وطريقة الحصول على المحتوى والأفلام والصور الإباحية التي تقدمها للمرتدي عليها. واليوم يوجد الآلاف من مقاطع الفيديو الإباحية كلا حسب تخصصها. فمنها المتخصصة في الفيديوهات، ومنهم المتخصصة في التصوير، ومنهم المتخصصة في الدردشة chatting.[2]

الفرع الثاني : مدي انتشار الجرائم الجنسية و الإباحية عبر الإنترنت

أدت شبكة الإنترنت أدت إلى ظهور القرية العالمية الذي اعترف بها العديد من العلماء، وعلى الرغم من مزاياها. إلا أن هذه الشبكة قدمت وسيلة فعالة وجذابة لإنتاج وتوزيع الإباحية والجنسية.

لقد حدثت في الآونة الأخيرة ثورة جنسية جذرية استبدادية في جميع أنحاء العالم فاقت كل الحدود وكسرت كل المحظورات، مما جعل هذه القضية من أخطر الجرائم من حيث أثرها على الإنسان، وقد وصفها "جيمس ريستون" من مجلة يورك تايمز بأنها" تهديد قد ينتهي به الأمر أكبر من التهديد النووي "، وفي هذا الصدد ، تدل الإحصائيات إلى حدوث نمو مقلق في عام 2012 في عدد الأنشطة المتعلقة بالمواد الجنسية، إذ تقدر مبالغ صناعة الجنس العالمية برقم مذهل يقارب 57 مليار دولار، وهناك أكثر من 372 مليونًا من الصفحات على الإنترنت الذي تروج لمختلف المواد الجنسية ، وكذلك صناعة الجنس

[1]– U.Sieber , Legal aspects of computer – Related Crime in the information Society Legal Advisory Broad, European Commission ,Available AT M www.eurropa.eu .int /ispo/legal/encomcrime/siber.html vu le 122/07/1017

[2] – محمد الجنبيهي ، المرجع السابق، ص29- 30

عبر الإنترنت يبلغ دخلها أكثر من 2.5 مليار دولار كل عام. [1] ومن خلال البحث الذي أجراه موقع "ألاسكا" في عام 2013 ، والمتخصص في إحصائيات الإنترنت في كل دولة في العالم، فإن الجزائر هي خامس أكثر الدول اكتظاظًا بالسكان في العالم العربي في مشاهدة الأفلام الإباحية. وقبلها تأتي العراق وليبيا والأردن وفلسطين. وقد ازدادت انتشارا في السنوات الماضية وهو ما أدي إلى إنشاء مجموعات على فيسبوك من طرف عدد كبير من الشباب الجزائري بهدف اتخاذ إجراءات قانونية تسمح بحجب المواقع الإباحية التي تنتهك قيم وحقوق جيل بأكمله وسمحت للكثير من أفراد المجتمع على إدمانها. وأظهرت آخر إحصائيات موقع "ألاسكا" أن عدد تصفح المواقع الإباحية في البلاد العربية تعدى كل الحدود، بمعدل 55 مليون موقع إباحي و24 مليون بحث عن كلمة "جنس" شهريًا، وهي إحصائيات غير مسجلة من قبل أمريكا أو دول الاتحاد الأوروبي[2].

وفي الجزائر تُظهر البيانات أن 82 بالمائة من المستخدمين يتصفحون الصور والمواقع الجنسية، وخاصة المراهقين والشباب، لذلك غالبًا ما تكون مقاهي الإنترنت أماكن مشبوهة وغير خاضعة للرقابة وجعلت معظم الشباب يدمنون المواقع الإباحية [3]. ومع انتشار الهواتف الذكية أصبح الأمر غاية في السهولة.

وفي عام 2016 ، أضاف موقع "أليكسا" أن 8 دول عربية هي الأكثر شعبية لتصفح المواقع الإباحية ومقاطع الفيديو والبرامج الإباحية ، وجمهورية مصر هي الأولى بـ 350 ألف، ثم العراق ثم الجزائر بـ 270 ألفاً من حيث عدد الزائرين يومياً، يليهما المغرب وتونس، تليهما الأردن ولبنان وليبيا. ويبلغ إجمالي عدد المتصفحين العرب على المواقع

[1] – ميلود بن عبد العزيز ،لجرائم الإباحية وأثرها على المجتمع من منظور شرعي وقانوني، مقال منشور على الرابط التالي ، اطلع عليه في 2016/12/02 : https://www.asjp.cerist.dz/en/article/4419

[2] – موقع الشروق ،الجزائر الخامسة عربياً في تصفح المواقع الإباحية ،على الرابط التالي : اطلع عليه في 2016/12/02. https://www.echoroukonline.com

[3] – موقع الشروق ،الجزائر الخامسة عربياً في تصفح المواقع الإباحية ،على الرابط التالي : https://www.echoroukonline.com

الجنسية "الزرقاء" من هذه البلدان حوالي 2 مليون مشاهد يوميًا [1]. وكل هذه الأرقام قد تصبح أضعافا مع مرور الزمن.

وفي دراسة قام بها الدكتور مشعل بن عبد الله في دراسة له أن هناك إقبالا كبيرا في السنوات الأخيرة على المواقع الخاصة بالإباحية، وحسب إحصائيات شركة (بلاي بوي) المتخصصة في الإباحية أن ما يقارب4،7 مليون شخص يدخل مواقعهم في الأسبوع الواحد وبعض الصفحات يزورها 280.034 زائر يوميا، وهناك أكثر من 100 صفحة متشابهة يدخلها حوالي 20.000 زائر كل يوم، إلى غير ذلك من الأعداد الهائلة لمتصفحي المواقع الإباحية .[2]

ومن خلال هذه الأرقام أصبحت هذه المواقع تشكل خطرا كبيرا، ولا يقتصر هذا التأثير المدمر لهذه المواقع على مجتمعات دون غيرها، حيث قد نرى آثارها من خلال تزايد الشذوذ الجنسي، وزيادة جرائم التحرش والاغتصاب خاصة ضد الأطفال بسبب انتشار الشواذ من المشتهيين للأطفال(la pédophilie)، ولذلك ومع تزايد عدد مستخدمي الإنترنت في جميع أنحاء العالم، أصبح نشر مقاطع الفيديو والصور الجنسية على الإنترنت مصدر قلق عالمي.

فالجرائم الجنسية والإباحية تتم عن طريق المواقع الإباحية أو القوائم البريدية أو عن طريق غرف الدردشة. ويتم ذلك بتصفح المواقع الإباحية أو الاشتراك فيها أو الشراء منها. وبالرغم من وجود هذا النوع من المواقع التي تسعي إلي الربح المادي إلا أنه في المقابل أصبح الكثير من المواقع الإباحية في وقتنا الحالي مجانية. ويستطيع أي شخص أيا كان وبكل سهولة الدخول إليها ومشاهدة الصور أو الأفلام المعروضة من خلالها .

ولقد استفادت الواقع الإباحية من الانتشار الواسع عبر الإنترنت والمزايا الأخرى التي تتيحها حيث توفر الانترنت أحسن الطرق لنشر وتوزيع الصور والأفلام الإباحية المخزية

[1]– موقع اخبار اليوم ،المواقع الإباحية ومواقع التطرف تدمّر المجتمع ، نشر المقال بتاريخ يوم 07 – 05 – 2017 على الرابط التالي :https://www.djazairess.com/akhbarelyoum/212499

[2] – مشعل عبد الله ، المرجع السابق ، ص 6

علناً وبشكل فاضح ومشين. ويعرف انتشار الإباحية عبر العالم منذ استعمال الإنترنت ظهور وانتشار نوع معين من الإباحية و الذي يعرف بالإباحية المتشددة[1].

ولقد أصبح تشجيع الممارسات غير الأخلاقية والترويج لها، أهم الجرائم التي تقع عبر مواقع "الإنترنت"، وأصبحت من الجرائم الجنسية المرتكبة عبرها حيث استخدمها عدد من الأشخاص الذين يدعمون المثلية الجنسية والدعارة وتبادل الأزواج والزوجات، وتم القبض على العديد من مديري هذه المواقع ووجهت إليهم تهم ممارسة الرذيلة والفجور والتحريض على الفسق[2].

وتعتبر كل المواقع الإباحية والجنسية المنتشرة عبر الإنترنت وسائل للتحريض على الفسق والفجور والدعارة. وبالتالي أصبحت الإنترنت مكانًا للدعارة لا يمكن إهماله. حيث من خلالها يمكن الوصول بسهولة جدًا إلى مواقع المرافقة وهذا هو الاسم الذي يطلق على هذه الدعارة التي تمر عبر الشبكات الدولية الانترنت، حيث يتم عرض المرافقين ومعظمهم من النساء، كذلك الرجال والمتحولين جنسياً وتعرض التفاصيل عنهم: كاللغات المنطوقة، والقياسات، والفوائد ، وأماكن الاجتماعات والجداول الزمنية.

الفرع الثالث : أركان الجرائم الجنسية والإباحية عبر الإنترنت

إن هذه الجرائم كغيرها من الجرائم لها أركان من الواجب توافرها لتحقيقها. وهذا النوع من الجرائم شأنها شأن الجرائم الأخرى وجب توفير الركن الشرعي والمتمثل في المادة القانونية التي تجرمها وتعاقب مرتكبها، إضافة إلى الركن المادي والمعنوي. وما سنتناوله في هذه الدراسة هو الركن المادي والمعنوي للجريمة .

الفقرة الأولى: الركن المادي للجرائم الجنسية عبر الإنترنت

يتحقق الركن المادي للجرائم الجنسية عبر الإنترنت بتحقق الفعل الإجرامي وهو استخدام الإنترنت في إنتاج مواد إباحية غير مشروعة أو بيعها أو شراءها أو عرضها أو ترويجها أو توزيعها أو توفيرها أو نشرها. ويتمثل السلوك الإجرامي أيضا في إعداد وإنتاج

[1] – يتم تعريف المواد الإباحية القاسية أو المواد الإباحية المتشددة على أنها مواد إباحية تحتوي على صور مفصلة للأعضاء التناسلية أو أفعال جنسية علنية مفصلة وكاملة. حيث أن هناك المواد الإباحية الأقل وضوحا.

[2] – حنان ريحان مبارك المضحكي ، الجرائم المعلوماتية ، المرجع السابق ص 238

أو إرسال أو تهيئة أو تخزين مواد إباحية بهدف عرضها على الغير والاستغلال لها عن طريق الإنترنت مما يعد مساسا بالحرمة الجنسية للأفراد.[1]

الفقرة الثانية: الركن المعنوي للجرائم الجنسية عبر الإنترنت

إن الجرائم الجنسية والإباحية جرائم عمدية وجب فيها تحقق القصد الجنائي، المتمثل في اتجاه إرادة المجرم إلى ارتكاب الجريمة مع علمه بأركانها وعواقبها، ويجب على مرتكب الجريمة أن يعلم علم اليقين أن فعله سوف يترتب عليه جريمة جنائية. وإرادته يجب أن تكون حرة، فلا يكتمل القصد الجنائي للجاني إذا كانت إرادته معيبة، و بمعنى أخر صور هذه الجرائم قد تقوم لكن لا تترتب عليها المسؤولية الجنائية في حال لو ارتكبت هذه الجرائم في احد ظروف موانع المسؤولية الجنائية كالإكراه أو صغر السن أو السكر ...الخ .

يعتبر القصد الجنائي شرطا ضروريا لقيام المسؤولية الجنائية وأهميتها لا تقل عن الركن المادي. فإذا علم الفاعل بجميع عناصر الجريمة ووجه إرادته نحو إحداث النتيجة الجنائية ظلت المسؤولية قائمة. لكن يبقى توضيح ما إذا كان هناك نية إجرامية أم لا بحسب طبيعة الجريمة والأدلة المقدمة التي سيعتمد القاضي عليها في تكييفه للقضية[2].

المطلب الثالث : الاستغلال الجنسي للأطفال عبر الإنترنت

مع اتساع نطاق بيئة الانترنت، وتنوع الأنشطة والمهارات المتعلقة بها ودخول كافة فئات المجتمع في شتى مجالات تقنية نظم المعلومات، سعيا وراء الخدمات التي تقدمها هذه التقنية خصوصا تقنية الإنترنت واعتمادهم عليها، وفي ظل غياب الوعي وقلة المراقبة أصبح مستخدمي شبكة الإنترنت عرضة للاعتداءات الواقعة عبرها خاصة فئة القاصرين كونهم الشريحة الأكثر تعاملا مع الإنترنت.[3]

تعد فئة الأطفال موضوع اعتداءات متكررة عبر الإنترنت دون ردع حقيقي للمعتدين، ويؤخذ الاعتداء عليهم بصفة عامة مظهر الاستغلال الجنسي .

[1] – صدام حسين ياسين العبيدي ، المرجع السابق ، ص 79

[2] – صدام حسين ياسين العبيدي ، المرجع نفسه ، ص 79

[3] – أسامة احمد المناعسة ، المرجع السابق، 57

يعد الاستغلال الجنسي للأطفال[1] والذي يطلق عليه مصطلح "إباحية الأطفال" من الجرائم المرتكبة عبر الإنترنت والتي تمس بفئة القاصرين، ويعد من أهم وأبرز المجالات التجارية الأكثر انتشارا على الإنترنت.

وحسب التقرير الصادر عن " المركز القومي لأمريكي للأطفال المفقودين والمختطفين " تم تأكيد تزايد استغلال الأطفال في المواد الإباحية عبر شبكة الإنترنت على المستوي العالمي، وأشار أيضًا إلى أن غالبية مشاهدي البورنوغرافيا عبر الإنترنت هم من الأطفال الذين تتراوح أعمارهم بين 12 و18 عامًا. [2]

وفي نفس السياق أفادت هيئة مراقبة الإنترنت في الولايات المتحدة أنه في عام 2004 كان هناك 3433 موقعاً إلكترونياً إباحيا يتعامل مع القاصرين، وفي عام 2006 ارتفع هذا العدد إلى 10656 موقع، منها حوالي 54% في الولايات المتحدة الأمريكية.[3] ليرتفع هذا العدد في الآونة الأخيرة ليبلغ حدا فاق كل التصورات. ومن هذا المنطلق نطرح الإشكالية التالية ماذا نقصد بالاستغلال الجنسي للأطفال الذي يتم الإنترنت ؟ وماهي صور هذه الجريمة والوسائل المستعملة فيها؟ وللإجابة على هذه الإشكالية سنتناول في الفرع الأول: مفهوم بالاستغلال الجنسي للأطفال عبر الإنترنت، والفرع الثاني: صور الاستغلال الجنسي عبر الإنترنت، والفرع الثالث: وسائل الاستغلال الجنسي للأطفال عبر الإنترنت.

الفرع الأول :مفهوم الاستغلال الجنسي للأطفال عبر الإنترنت

مع توســـــع بيئة الإنترنت، بدأت فئات عمرية جديدة الاستفادة من خدماتها في المجال

---

[1] – الطفل لغة هو المولود حتى البلوغ , والجمع أطفال , ينظر : المعجم الوجيز , ص392 مجمع اللغة العربية , طبعة خاصة بوزارة التربية والتعليم ،2003

– أما قانونيا يعرف الطفل بأنه " هو الصغير الذي لم يبلغ سن الرشد الجنائي,أو هو كل من لم يتجاوز سنه ثمانية عشرة سنة ميلادية او هو الصغير منذ ولادته , سواء كان ذكراً أم أنثى إلى حين بلوغه سن الرشد الجنائي المحدد قانونا.

وبالرجوع إلى مفهوم الطفل في الفقه الإسلامي والقانون نجد أنه لا خلاف يذكر حول تحديد هذا المفهوم , فالطفل . سواء في الفقه الإسلامي أو القانون الجنائي . هو الصغير الذي لم يبلغ الثامنة عشرة من عمره : أنضر فوزية عبد الستار , المعاملة الجنائية للأطفال , دراسة مقارنة , دار النهضة العربية, 1998 ص3

[2] – البورنغرافيا أو الفن الإباحي، مقال للكاتب إي وايت، بحث منشور على الرابط التالي : – www.risalatalkaime.com/details.asp?id=٩٢٨/: إطلع عليه في 2017/02/10

[3] – علي كريمي , الشباب وتشريعات الإنترنت العربية جريمة الاستغلال الجنسي للأطفال نموذجا , بحث منشور على الرابط التالي : WWW.maroc.reunis.fr/comeld/index.php اطلع عليه في 2017/02/10

الواسع لتكنولوجيا نظم المعلومات، ومع غياب وعي الأهل وقلة المراقبة أصبح الأطفال موضوع اعتداءات متكررة، وأخذ بالاتساع بإتباع تقنية نظم المعلومات واستخداماتهم المختلفة لها، ويتم ذلك بكافة صور الاعتداءات الجنسية لاستغلالهم والحصول على المبتغى المرجو من ذلك. وقبل التطرق لتعريف الاستغلال الجنسي للأطفال عبر الإنترنت سنتطرق أولا لتعريف للاستغلال الجنسي التقليدي للأطفال. وثانيا لتعريف الاستغلال الجنسي للأطفال عبر الإنترنت.

الفقرة الأولى : تعريف لاستغلال الجنسي للأطفال

إن الاستغلال الجنسي للأطفال أو كما يطلق عليه بورنوغرافيا الأطفال هو مصطلح للدلالة على مشاركة القصر في أفلام أو مشاهد إباحية وجنسية[1]. وغالبا ما يظهر هؤلاء الأطفال عادةً بملابس قليلة أو معدومة تمامًا. ويعني المصطلح أيضًا أي تصوير لطفل يمارس نشاطًا جنسيًا صريحًا عبر أي وسيلة، أو أي تمثيل لأعضاءه الجنسية لإشباع الرغبة الجنسية. ويعتبر اعتداءا غير مباشر كل من يشاهد أو يحوز صوراً غير محتشمة للأطفال. ويستخدم مصطلح الاستغلال لوصف بغاء الأطفال واستخدامهم في الأنشطة الجنسية.[2]

ولقد اختلف الكثير من الفقهاء في تعريف الاستغلال الجنسي للأطفال، فهناك من يعتبره "كل تمثيل للأطفال في مواقف جنسية صريحة مهما كانت طبيعتها، سواء في الصور أو الرسومات أو الأصوات، سواء كانت حقيقية أو ملفقة، حتى لو تبين أن المشاركين فيها ليسوا أطفالاً ولكن تم اختيارهم وفقاً لمعايير خاصة بالأطفال بغرض الخداع.[3]

أما بشان اتفاقية مجلس أوربا لحماية الأطفال من الجرائم الجنسية لعام 2007، لم تستعمل تستخدم الاتفاقية مصطلح الاستغلال الجنسي، ولكنها تستخدم عدة مصطلحات

---

[1] – عادل عزام سقف الحيط ، المرجع السابق، ص 165

[2] – هاني جورجي , مناهضة الاستغلال الجنسي للأطفال والعنف الأسري , من إصدارات المجلس القومي للطفولة والأمومة , وحدة مناهضة الاتجار بالأطفال , بحث منشور على الرابط التالي:

Trafficking . Info/Upload/Files١٣٠٩٣٣٩٠٢٦٧١٦٢ .doc WWW.Child

[3] – الجرائم الجنسية المرتكبة ضد الأطفال , بحث منشور على الرابط التالي : تم الإطلاع عليه في 2017/02/13

com/biblio the que – collgue– docx WWW.emloffice

وخصصت معاني محددة لكل منها، وهذه المصطلحات هي: الاعتداء الجنسي، استغلال الأطفال في الدعارة، استغلال الأطفال في عروض إباحية، تحريض الطفل لهدف جنسي.[1]

ويعرف قانون المحكمة الجنائية الدولية الاستغلال الجنسي للأطفال باعتباره من صورة من صور الاتجار بالبشر بأنه " كل فعل جنسي تجاري يقع على أفراد يقل عمرهم عن 18 سنة تحت الإكراه أو الاحتيال أو غير ذلك. "

وقد يأخذ الاستغلال الجنسي للأطفال شكل الدعارة الجبرية أو القسرية، كما قد يأخذ شكل العروض الإباحية، ويقصد بدعارة الأطفال أو بغاء الأطفال كما ورد بالبروتوكول الاختياري بشأن بيع الأطفال وبغاء الأطفال واستغلالهم في العروض الإباحية بأنه " استخدام طفل لأغراض جنسية مقابل مكافأة أو أي شكل آخر من أشكال التعويض. " ويقصد بالعروض الإباحية أو المواد الإباحيـــة في ذات البروتوكول :" أي تصوير للأعضاء التناسلية للطفل لإشباع الرغبة الجنسية " .[2]

إن تصوير الأطفال في وضعيات إباحية هي عملية تجارية تتعلق بأجسادهم، حيث يتم التقاط صور معينة لطفل وهو عاري تمامًا أو في حالة مغرية وجذابة، ثم تظهر هذه الصور كجزء من إعلانات لأفلام إباحية. أو عبر مواقع تسوق للإباحية عبر الإنترنت،وفي كثير من الأحيان يتم حث الطفل على قبول هذه الخدمات أو العروض الإباحية، إما بالمال أو بالإكراه، وأحياناً بالتهديد، وأحيانا أخرى يتم تحت تأثير المخدرات[3]. والغرض من هذه العروض الإباحية المتعلقة بالأطفال هو تحقيق مكاسب مالية، حيث يقوم تجار الإباحية بالإعلان عنها لتلبية احتياجات المثليين جنسياً والشواذ خاصة الطبقة الثرية منهم، نضير مبالغ ضخمة.

---

[2] – البروتوكول الاختياري لاتفاقية حقوق الطفل وبغاء الأطفال واستخدامهم في العروض والمواد الإباحية , وقد صدر هذا البروتوكول عن الأمم المتحدة بعد اعتماد الجمعية العامـــــة في 25 ماي 2000 بموجب القرار رقم263/54 ودخل حيز التنفيذ في 18 /01/ 2002 . انظر الرابط التالي : http://www.umnedu/humanrts/arab. html اطلع عليه في 2017/06/22

[3] – محمد نور الدين سيد، جريمة بيع الأطفال والاتجار بهم , دراسة في قانون العقوبات المصري والإماراتي وقوانين مكافحة الاتجار بالبشر والاتفاقيات والبروتوكولات الدولية ، دار النهضة العربية ، 2012، ص 152

الفقرة الثانية : تعريف الاستغلال الجنسي للأطفال عبر الإنترنت

مع ظهور شبكات الإنترنت واتساع استخدامها أصبح الاستغلال الجنسي للأطفال في شكل العروض الإباحية أكثر اتساعا، وهي جرائم جنسية غير مباشرة، غرضها التحريض على ممارسة أنشطة جنسية ضد الأطفال بأي شكل من الأشكال. ويستخدم مرتكبو الجرائم الجنسية البريد الإلكتروني أو الرسائل الفورية أو غرف الدردشة لكسب ثقة أطفالهم ثم الترتيب لمقابلتهم شخصيًا. وبخلاف الأفعال الجنسية المباشرة، فإن الأفعال الاستغلالية لا تمس جسد الطفل بشكل مباشر، كالاغتصاب أو هتك العرض، لإشباع شهوة مرتكب الجريمة أو لرغبته في الانتقام. لكنهم يستخدمون الجسد من أجل الربح المادي[1].

ويقصد بالاستغلال الجنسي للأطفال عبر الانترنت " كافة الأنشطة غير المشروعة التي يقوم بها بعض الأشخاص الذين يستخدمون الإنترنت وشبكات التواصل الاجتماعي وتكنولوجيا هذه الشبكات في إغراء وخداع الأطفال الصغار بهدف ابتزازهم، سواء من خلال إنتاج مواد إباحية ذات طبيعة جنسية أو بتصويرهم والترويج لهم عبر الإنترنت. أو بمطالبتهم بممارسة الجنس معهم، إلى غير ذلك من أشكال الاستغلال، ثم تهديدهم بالتشهير بهم إذا لم تتم تلبية مطالبهم".[2]

ويعرف أيضا بأنه" تلك الصور أو الأفلام والمحادثات الحقيقية أو الإيحائية التي تجري بين شخص بالغ وطفل حول الجوانب الجنسية بقصد إغرائه أو خداعه لاستدراجه فعلياً إلى الفخ وممارسة الجنس معه، أو لتبادل هذه الصور والأفلام والاتجار بها عبر الانترنت. "[3]

وقد عرفت أيضا مؤسسة ICDL Arabia الاستغلال عبر الإنترنت على أنه " إساءة استخدام وسائل التواصل الاجتماعي مثل غرف الدردشة أو تقنيات المعلومات الأخرى

---

[1] – الجرائم الجنسية المرتكبة ضد الأطفال , بحث منشور على الرابط التالي : اطلع عليه في 2017/06/22
WWW.emloffice.com/biblio the que – collegue/201157/57. docx

[2]– إبراهيم إسماعيل عبده محمد ، الاستغلال الجنسي للأطفال عبر شبكات التواصل الاجتماعي ، جامعة الملك سعود ،الرياض، المملكة العربية السعودية ، مقال منشور في مجلة جيل العلوم الاجتماعية والإنسانية ، العدد 56 ، ص 243

[3]– السيد نجم، الاتجار في البشر والاستغلال الجنسي للأطفال، بحث في المؤتمر الدولي الثاني حول حماية المعلومات والخصوصية في قانون الإنترنت، القاهرة– يونيو 2008م، ص 6.

للاستفادة بشكل غير قانوني من معلومات الأفراد الشخصية للتلاعب بهم بغرض تحقيق مكاسب شخصية ".[1]

على الرغم من صغر سنهم، فإن الأطفال أكثر قدرة من البالغين على التحكم في تكنولوجيا الإنترنت، مما يسهل لهم الوصول إلى المواقع الإباحية عبر الشبكة، حتى ولو كانت هذه المواقع مغلقة، مما يجعلهم عرضة للاستغلال الجنسي الذي قد يتخذ أشكالًا عديدة، كجعلهم مثلا ضحايا للجناة الخطريــن والشواذ المنجذبين إلى الأطفال، الذين يغرون الأطفال من خلال الإنترنت، وقد يتم أيضا استمالهم عبر الإنترنت لتصوير أنفسهم بكاميرات الويب. هذه الظاهرة التي أصبحت أكثر انتشارا في الآونة الأخيرة والتي تعد من اخطر صور الإساءة الجنسية إلى الأطفال. وفي هذا الشأن أصدرت مؤسسة مراقبة الإنترنت تقريرها السنوي لعام 2017 الذي يرصد نشاط محاربة صور ومقاطع استغلال الأطفال جنسيا عبر الإنترنت.

ويؤكد التقرير أنه في عام 2017 ، يوجد موقع يحتوي على مواد إباحية للأطفال ويتم عرضها كل سبع دقائق. وقد استعرض نفس التقرير 132 ألف شكوى في عام 2017 حول 80 ألف صفحة من الصور ومقاطع الفيديو المتعددة لإساءة معاملة الأطفال.[2]

إضافة إلى هذا كشف نفس التقرير عن وجود مواقع يصل عددها إلى 78 ألف موقع في مجملها تحتوي على صورا تظهر استغلالا جنسيا للأطفال، أو تروج له، كذلك وجود 1729 مجموعة إخبارية هي الأخرى احتوت على صور استغلال جنسي للأطفال ضمن صفحاتها، وتضمن التقرير نسبة المحتوى الذي يقدم استغلالا جنسيا في الصفحات السابقة الذكر والتي تصل إلى 43 بالمئة ، ويظهر من خلالهم أطفالا بسن تتراوح بين 11 و15 عاما، و55 بالمئة من المحتوى يظهر أطفالا دون العاشرة، و2 بالمئة لأطفال دون سن العامين. ولقد ظهر من خلال التقرير أن 33 بالمئة من منها يعد استغلالا جنسيا للقصر، تضمنت اغتصابا وتعذيبا. وأظهر 21 بالمئة من المحتوى نشاطات جنسية غير مكتملة

[1] – مسعد عبد الرحمن زيدان، الاستغلال الجنسي للأطفال عبر الانترنت في ضوء أحكام القانون الدولي، كلية العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض،2016 ، ص 18.

[2] – حقائق عن استغلال الأطفال جنسيا، على الرابط التالي: اطلع عليه في 2017/06/22
https://www.alhurra.com

و46 في بالمئة من المحتوى كان غير لائق، لكنه ليس ضمن الفئتين المذكورتين، وأظهر 86 بالمئة من المحتوى استغلالا لإناث، مقابل 7 بالمئة للذكور.

وأشار نفس التقرير إلى أن 87 بالمئة من المواقع ذات محتوى استغلال الأطفال جنسيا، والتي تمكنت المؤسسة من تناولها صادرة من خمس دول هي هولندا والولايات المتحدة وكندا وفرنسا وروسيا.[1]

الفرع الثاني : صور الاستغلال الجنسي عبر الإنترنت

وراء كل صورة أو فيديو أو شاشة، هناك عدة أطفال ضحايا للاستغلال الجنسي. ومثل أشكال الاعتداء الجنسي الأخرى، يمكن أن تتسبب الإساءة عبر الإنترنت في إصابة الضحايا عاطفيًا وجسديًا مدى الحياة. ولكن على عكس الأشكال الأخرى لسوء المعاملة، يمكن أن يتعرض الطفل ضحية ملايين المرات في كل مرة يتم فيها مشاهدة صورة أو إرسالها أو تلقيها، ومن الصعب تحديد المخالفين والتحقيق معهم، لأنه غالبًا ما يحدث الاستغلال الجنسي عبر الإنترنت عبر عدة ولايات قضائية، وغالبًا ما يكون الضحايا والجناة في بلدان مختلفة، ولا يزال يتعين على بعض البلدان تحديث التشريعات التي تجرم مشاهدة أو حيازة مواد الاعتداء الجنسي على الأطفال عبر الإنترنت،[2] مهما كانت الصورة التي يحملها هذا الاعتداء.

وصور الاستغلال الجنسي للأطفال عبر شبكة الإنترنت كثيرة ومتنوعة ولا يوجد تحديد دقيق لها، لأن آراء المجتمعات في هذه الظاهرة تختلف من مجتمع إلى أخر ومن بلد إلى آخر، لأن القواعد التي تسري في المجتمع الغربي قد لا تسري على المجتمع العربي والإسلامي.

ومن أبرز صور الاستغلال الجنسي والتي يكون الطفل محلا لها هي تحريض القاصرين على الأعمال الجنسية، إنتاج صور فاضحة للأطفال، إعمال الدعارة والترويج لها، استغلال

---

[1] – حقائق عن استغلال الأطفال جنسيا ، الرابط التالي ، تقرير مؤسسة مراقبة الانترنت ، على الرابط: اطلع عليه في 2017/06/25

https://www.alhurra.com/a/internet-watch-foundation-annual-report/432910.html

[2] – Online child sexual exploitation ,https://www.ecpat.org/what-we-do/online-child-sexual-exploitation

الأطفال جنسيا.

الفقرة الأولى : تحريض القاصرين على الأعمال الجنسية

توجد الكثير من المواقع على شبكة الإنترنت متاحة لكافة الأشخاص متخصصة بالجنس، ويتم الدخول لها بالولوج لعنوان إلكتروني في دفتر العناوين، ويبدأ الموقع بإظهار النتائج مباشرة، والمشكلة هي أن معظم هذه المواقع مجانية وسهلة الوصول إليها. إضافة إلى هذا فتقنية الإنترنت تسمح للمواقع الإباحية الدخول إليها عبر مواقع أخرى وبمجرد استخدام الإنترنت يجد المستخدم نفسه عرضــة للصور ومناظر إباحية دون البحث عليها وعادة ما يكون المستخدم من الصغار سنا. وفي حالة دخول القاصر إلى المواقع الإباحية والجنسية، يجد نفسه ضحية سهلة لمروجي هذه التجارة، حيث تعرض عليهم هذه المواقع جوائز مغرية مقابل تحريضهم للقيام بأعمال جنسية معينة، سواء بصورة منفردة أو بصورة جماعية.[1]

الفقرة الثانية :أعمال الدعارة والترويج لها.

إن التحريض على الفسق " هي التأثير على نفس المخاطب وإقناعه بارتكاب فعل فاجر فلا يجد مفرا منه فيخضع لإرادة من حرضه ويتبعه."[2] وعليه فإن التحريض على الدعارة الموجه للأطفال والتي تتم عبر الإنترنت يمكن أن تتخذ الأشكال التالية:

– التشجيع من خلال المحادثات على ارتكاب الأفعال المنافية للأخلاق والتجاوزات، وغالباً ما يتم ذلك من خلال الحوار وغرف الدردشة.

– التحفيز من خلال وضع المواقع الترويجية على شبكة الإنترنت، فتقوم بتزويد الشخص بمعلومات عن الأطفال الممكن الاتصال بهم من أجل إشباع رغباتهم .

– التحريض بالرموز أو الرسوم التي قد تشكل دعوة واضحة أو تحريضاً على الفجور والابتذال، وكثرة التعرض للمواد الإباحية والمشاهدة غير اللائقة قد يترتب عليها زيادة الرغبة الشديدة إلى حد الإدمان مع وجود رغبة دائمة ومستمرة في التحفيز. [3]

---

[1] – أسامة احمد الناعسة و جلال محمد الزغبي ، جرائم تقنية المعلومات الالكترونية ، المرجع السابق، ص 262

[2] – ادوار غالي الذهبي، الجرائم الجنسية ،دار غريب للنشر ،القاهرة , طبعة 3، 2006، ص206

[3] – إبراهيم عيد نايل ، الحماية الجنائية لعرض الطفل من الاعتداء الجنسي , دراسة مقارنة بين قانون العقوبات الفرنسي والمصري , الطبعة الأولى , دار النهضة العربية 2001م ص41 .

– يتم التحريض على الفسق والدعارة من خلال صور أو أفلام مصورة تظهر الأطفال بحالات القيام بأعمال جنسية مختلفة سواء مع بعضهم أو مع بالغين وذلك بإرغام الطفل على الدخول إلى مواقع متخصصة.[1]

الفقرة الثالثة :عرض الصور والأفلام والمحادثات الجنسية

يتم استغلال الأطفال جنسيا بعرض المواد الإباحية عليهم لأغراض تربوية تعليمية، ثم محاولة التأثير على الطفل وإقناعه بأن ممارسة الجنس العلني أمر مرغوب ومقبول، ثم وإقناعه بأنه أمر شائع وبأنه ليس بمفرده في هذا المجال، وأن مثل هذا السلوك جيد، ومن ثم يسهل للطفل الدخول لتصفح المواد الإباحية وإزالة العوائق التي تمنعهم من المشاهدة، ثم دعوتهم للتحدث في مواضيع جنسية، ثم جعلهم يلتقطون مقاطع فيديو جنسيـــــة صريحة، لاستخدامها لجذب وإغراء المزيد من الضحايا.[2]

يعد الترويج للمواد الإباحية من أجل الإشباع الجنسي أو لتحقيق أرباحا تجارية أمرًا شائعًا على الإنترنت حيث يصور إساءة معاملة الأطفال، والأفعال الجنسية التي تشمل المواد الإباحية وأفلام أو صور لأطفال يتعرضون لعمليات تعذيب جنسي، والأعضاء الجنسية، وعمليات الاغتصاب، خاصة على الأطفال الذين تتراوح أعمارهم من4 إلى 6 سنوات. وفي بريطانيا تم الكشف عن شبكة توزع أفلاما مشينة خاصة بالأطفال. وتم العثور على جهاز الكمبيوتر الخاص بأحد أعضاء الشبكة يحتوي على مجموعة كبيرة من الصور الفاضحة للأطفال ما يقارب 150 قرصًا مضغوطًا، بالإضافة إلى عناوين العديد من الأشخاص الذين يحبون الأطفال أغلبهم في جنوب أفريقيا وهونج كونج وألمانيا. [3]

يظهر لنا تفاقم الاستغلال الغير مشروع للقاصرين عبر تقنية الإنترنت واعتبارها وسيلـة للاعتداء عليهم من خـــــلال توزيـــع الصـــور الفاضحة لهـــم، وبيع وتداول الصـــور

---

[1] – أسامة احمد الناعسة ، جلال محمد الزغبي ، جرائم تقنية المعلومات الالكترونية ، مرجع سابق، ص 265

[2] – أكمل يوسف السعيد , الحماية الجنائية للأطفال ضد الاستغلال الجنسي , رسالة دكتوراه , كلية الحقوق المنصورة ، مصر ,2012، ص 222

[3]– رشا خليل ، جرائم استغلال الأطفال عبر الإنترنت، جامعة ديالي, كلية القانون , مجلة الفتح، 2006م , العدد2، ص 33

والفيديوهات التي يظهرون من خلالها .[1]

الفرع الثالث: وسائل نشر صور الاستغلال الجنسي للأطفال عبر الإنترنت

تستعمل أغلب مجموعة الخدمات التي تعرضها شبكة الإنترنت في الاستغلال الجنسي للأطفال، ومن هذه الخدمات نذكر مايلي :

الفقرة الأولى: البريد الإلكتروني Email

يستعمل لإيصال رسائل أو صورا أو رسومات أو غيرها. فليس من الضروري الكشف عن عنوان البريد الإلكتروني لعرضه، ولكن من الممكن تقديم معلومات خاطئة والحصول على العنوان، ويمكن إخفاء هذا العنوان باستخدام وظيفة التشفير، ويوجد نوع من المجرمين القادرين على الدخول إلى البريد الالكتروني للأشخاص والاطلاع على محتوياته بكل سهولة عن طريق الاختراق، وبالتالي يمكن استغلال هذه الخدمة لإرسال الرسائل ذات المحتوي الجنسي المتعلقة بالاستغلال الجنسي للأطفال كصور الأطفال الفاضحة أو بورنوغرافيا الأطفال لأي عنوان إلكتروني[2].

الفقرة الثالثة : نوادي المناقشات :

يمكن تعريف نوادي المناقشة بأنها نظام دولي يوفر لمستخدمي الشبكة إمكانية المناقشة المباشرة، كما أنها بمثابة مساحة مفتوحة للأشخاص المنحرفين لتبادل الصور ومقاطع الفيديو والإعلانات المتعلقة باستغلال الأطفال في الممارسات الجنسية دون رقابة.

الفقرة الثالثة : مواقع الإنترنت

تتكون هذه الخدمة من معلومات وصور وغيرها. متاحة للمستخدمين بطريقة بسيطة، ويتم ذلك من خلال تخصيص حصص من الشبكة لمن يرغبون في إنشاء مواقع الويب، واليوم هناك شركات متخصصة في إنشاء مواقع الإنترنت، لذلك من الممكن إنشاء مواقع تتعلق بالاعتداء الجنسي على الأطفال والتي يمكن الوصول إليها بسهولة عبر الإنترنت.

إن سهولة الوصول إلى المواقع الإلكترونية والوصول إلى المواقع التي تستأجر صفحات يجعل الإنترنت أسهل وسيلة لانتشار جريمة الاستغلال الجنسي، بالإضافة إلى تواجد العديد

---

[1]– أسامة احمد الناعسة ، جلال محمد الزغبي ، جرائم تقنية المعلومات الالكترونية ، المرجع السابق ، ص 264

[2]– محمد محمد الالفي ، المسؤولية الجنائية عن الجرائم الأخلاقية عبر الانترنت ، المرجع السابق، ص133

من المواقع التي تشترط المقابل المالي للوصول إليها، وهي خاصة بالمشتركين بها، الأمر الذي يشكل حاجزا أمام الجهات الأمنية للوصول إليها أو مراقبتها، كما يشجع العنصر المادي على زيادة النشاط وعليه توسيع أعداد الأطفال المتأثرين جنسيا.[1]

الفقرة الرابعة :غرف المحادثة عبر شبكة الانترنت chat room

تعتبر خدمة غرف المحادثة عبر الإنترنت من أهم الخدمات التي تقدمها الشبكة نظرا للإقبال الكبير عليها خاصة من فئة الأطفال، لذلك تم استغلالها من طرف تجار الانحلال والجنس والإباحية وكذلك المنحرفين جنسيا (pédophile)[2] لاستدراج واستغلال ضحاياهم من الصغار. وباستخدام الإنترنت فان المحادثات يمكن أن تكون عميقة خاصة تلك ذات الطبيعة الجنسية وأن المحادثة قد تكون سمعية وبصرية في نفس الوقت، وبالتالي قد يتم عبرها استمالة الأطفال للحديث عن الجنس وتصوير أنفسهم وهم عراة و تحريضهم على أعمال مخلة بالحياة على المباشر باستعمال الكاميرا . وكل هذا يتم تسجيله للاستفادة منه أو استفادة أشخاص آخرين منه. وهذا ما يؤدي عادة إلي إدمان الصغار على الإباحية [3].

الفقرة الخامسة : المواقع الجنسية والإباحية

عبارة عن مجموعة من صفحات الويب المرتبطة المخزنة على خادم واحد. يمكن الوصول إليها باستخدام خدمة ويب وبرنامج كمبيوتر يسمى متصفح الإنترنت. ويمكن الاطلاع عليها على الأجهزة المحمولة باستخدام تقنية الإنترنت. وتتم استضافة مواقع الويب على ما يسمى بخوادم الويب.

ومن بين هذه المواقع هنالك المواقع المتخصصة في الإباحية والجنس التي تمنح المزيد من الناس إمكانية الوصول إلى شبكة الإنترنت العالمية ونمو وانتشار المواقع الإباحية

---

[1]–احمد لطفي السيد مرعي، إستراتجية مكافحة جرائم الاتجار بالبشر ، بحث منشور على الرابط التالي :
https://books.google.dz/books?id

[2] – بيدوفيلpédophile وهو الشاذ جنسيا بانجذابه للأطفال، هو عبارة عن عيب يتصف به الشخص البالغ والذي يحس بالجاذبية الجنسية المستمرة تجاه الأطفال ، وفي المجتمع الحديث ، يُعترف بهذا النوع من الجاذبية على أنه انحراف جنسي شديد الخطورة . أنضر الرابط التالي : اطلع عليه في 2017/06/30
ttps://www.larousse.fr/dictionnaires/francais/pédophilie/58976

[3] – الحمود وضاح محمود و نشأت مفضي ، جرائم الإنترنت ، دار المنار ،عمان، الأردن ، 2005 ص 109

بنشرها وعرضها عن طريق مواقع الويب.[1] هناك نوعان من المواقع الإباحية على الإنترنت تجارية ومجانية، وهذا النوع من المواقع يستغل من أجل الإيقاع بأكبر عدد من الضحايا خاصة الضحايا من صغار السن .[2]

الفقرة السادسة :المواقع الترفيهية على شبكة الإنترنت

وتتمثل هذه المواقع في مواقع الألعاب الالكترونية على شبكة الإنترنت، والتي تمثل مكانا جذابا للمنحرفين والشاذين جنسيا ولتجار الجنس، لما تقدمه هذه المواقع من إغراء، وبعد تنقية الضحايا من طرف تجار الجنس يتم الإيقاع بالأطفال واستدراجهم ومن ثم استغلالهم جنسيا بأفظع الطرق .[3]

ونتيجة لما سبق تعتبر جريمة الاعتداء على الأطفال عبر الإنترنت من أخطر الجرائم الجنسية الغير مباشرة، لأن الهدف منها هو استغلال الأطفال وتشجيعهم على ممارسة النشاط الجنسي بأي شكل من الأشكال عبر العالم الافتراضي، جاعلة من الطفل بضاعة تباع وتشترى، فضلا عن كونها وسيلة للثراء. ولقد أثبتت الإحصائيات أن هناك ½ من الأطفال أو المراهقين عبر العالم قد تعرض إلى مشهد اباحي ولو عن طريق الصدفة.

المبحث الثالث : جرائم العنف عبر الإنترنت

العنف عبر الإنترنت هو استخدام الرسائل وكاميرات الهواتف المحمولة ومسجلات الصوت بقصد انتهاك الخصوصية وإيذاء الآخرين. ويعرف إجرائيا بأنه: كل ضرر مادي أو معنوي يتم عبر الإنترنت ومواقع التواصل الاجتماعي من ابتزاز وتهديد بالصور ومقاطع الفيديو مسببا تأثيرات نفسية غير مرغوبة لدى المتلقي."[4] وقد يأخذ العنف عبر الإنترنت

---

[1]– تعريف المواقع الإباحية ، على الرابط التالي : اطلع عليه في 2017/97/16
https://ar.wikipedia.org/wiki/

[2]– عبد الفتاح بيومي حجازي ، الأحداث والإنترنت ، المرجع السابق ، ص 176

[3] – الحمود وضاح محمود و نشأت مفضي ، جرائم الإنترنت ، المرجع السابق ، ص 110 وما بعدها

[4]– محمدي فوزية وخدة فاطمة الزهراء ، تأثير العنف الالكتروني في مواقع التواصل الاجتماعي على العلاقات الاجتماعية لدى الشباب ، مقال نشر في مجلة جيل العلوم الإنسانية والاجتماعية العدد 40،جامعة ورقلة ، ص 47

صورا أخرى كالتحريض على الإيذاء والتحريض على القتل والانتحار وفي بعض الأحيان قد يأخذ صورة القتل الغير مباشر.

وفي دراستنا هذه سنسلط الضوء على أهم مظاهر العنف عبر الإنترنت وهي: جريمة الابتزاز (المطلب الأول) وجريمة القتل والتحريض على القتل والمساعدة على الانتحار (المطلب الثاني).

المطلب الأول : جريمة الابتزاز والملاحقة عبر الإنترنت

الابتزاز هو جريمة تستهدف أمن وسلامة الأفراد باستخدام شبكة الإنترنت، عن طريق قيام البعض باصطياد ضحاياهم وإكراههم على دفع مبالغ مالية أو أعمال غير قانونية لقاء عدم نشر محادثات شخصية أو معلومات سرية أو صور خاصة تحصل عليها الجاني من عدة طرق منها المشروعة ومنها الغير مشروعة عن طريق الاختراق مثلا. ولدراسة هذا النوع من الجرائم سيتم تسليط الضوء على تعريف جريمة الابتزاز عبر الإنترنت مع بيان صورها والوسائل التي يستعملها المبتزون للوصول إلي غاياتهم، وأخيرا الأركان الواجب توافرها لقيام هذه الجريمة .

الفرع الأول : مفهوم الابتزاز عبر الإنترنت

يتطلب تحديد الإشارة إلى مفهوم الابتزاز عبر الإنترنت في إطاره العام الإشارة إلى الابتزاز وفقا لمختلف التعاريف التي تضمنته كما سنوضحه في مايلي:

الفقرة الأولى: تعريف الابتزاز لغة

الابتزاز في اللغة يأتي من البَزُّ : أي السلب، وابتززت الشيء، استلبته، بَزَّهُ يبزه بَزّاً: غلبه وغصبه، وبز الشيء يبز بزا : انتزع ، وحكى عن الكنساني : لن يأخذه ابدا بزة مني اي قسرا ،ابْتَزَّهُ ثيابه : سلبه اياها.[1]

الفقرة الثانية: تعريف الابتزاز اصطلاحا

عرفه بعض الفقهاء على أنه محاولة الحصول على مزايا مادية أو معنوية من شخص طبيعي أو اعتباري باستخدام القوة أو التهديد بإفشاء سر الشخص المبتز.

[1] – ابن منضور ، معجم لسان العرب، المصدر السابق ، المجلد الثاني ، حرف الباء ، مادة بزز

وعرف أيضا بأنه "فرض أسلوب التهديد بالفعل، أو الترك للحصول على مكاسب من شخص، أو جهة ممنوعة شرعا، وعقلاً ." ويشير هذا التعريف إلى أن الغرض الأساسي من الابتزاز هو الحصول على منفعة، بغض النظر عما إذا كانت هذه المنفعة مادية أو معنوية، لأن الغرض يمكن أن يكون إلحاق الضرر وتشويه سمعة الشخص أمام الآخرين.[1]

الفقرة الثالثة: تعريف الابتزاز عبر الإنترنت

يعرف الابتزاز عبر الإنترنت أو كما يطلق عليه البعض الابتزاز الالكتروني أنه "الانتهاكات المرتكبة ضد الأفراد أو الجماعات نتيجة للجريمة وبقصد التسبب في الضرر المادي المباشر أو غير المباشر باستخدام شبكة الاتصالات الإنترنت وغرف الدردشة والبريد الالكتروني."[2]

ويعرف الابتزاز أيضا بالتهديد، والتهويل، ومن أمثلته تصوير فتاة في مواضع جنسية، وتهديدها بنشرها، أو بإفشاء أمور تخدش بشرفها، أو إلى من يهمه أمرها عبر منتديات الإنترنت، ومواقع التعارف، أو عبر رسائل الهواتف النقالة إذا لم تستجب إلى رغبات المعتدي المادية أو الجنسية، وقد يكون التهديد[3] كتابة، أو شفاهة، أو عن طريق الاتصال الصوتي عبر الإنترنت، أو بواسطة شخص ثالث، ويصاب المجني عليه بالخوف والفزع الذي يحمله على تنفيذ إرادة الجاني .[4]

ويمكن تعريفه أيضا على انه عملية تهديد للمجني عليهم بنشر الصور الشخصية أو مقاطع الفيديو أو الكشف عن معلومات سرية تم الحصول عليها مقابل مبالغ مالية ضخمة، ويمكن استخدام الابتزاز للكشف عن معلومات سرية حول الشركة أو صاحب العمل، ويمكن أيضا ابتزازهم من أجل الحصول على تنازلات أخلاقية من طرف الضحية لصالح

---

[1] – محمد بن شلهوب ، جريمة الابتزاز دراسة مقارنة، دار كنوز اشبيليا، الرياض، 2016 ، ص 09، 10

[2]– Hadler .D and Jaishankar ,K, Cyber crime and the Victimezation of Women , Rights and Regulations , Hershey , USA,IGA, Global , ISBN 978– 1– 60960 – 830. p 9

[3]– التهديد "هو كل فعل ، أو سلوك من شأنه أن يبعث الخوف في نفس المجني عليه بهدف الإضرار به ، أو بأي شخص آخر يهمه أمره، مما يحمل المجني عليه إلى أن ينفذ ما يريده الجاني" . عبد الوهاب المعمري ، جريمة الاختطاف الأحكام العامة والخاصة، والجرائم المرتبطة بها ، دار الكتب القانونية، القاهرة، 2010، ص351

[4] – عبد الوهاب المعمري، المرجع نفسه، ص352

الجاني. وعادة ما يحدث الابتزاز باستدراج المجني عليهم عبر مواقع الاتصال المستخدمة من طرف كل الفئات العمرية، ويتم اصطياد الضحايا عن طريق الفيسبوك أو سكايب أو واتس أب أو البريد الإلكتروني أو تويتر أو الإنستجرام أو فايبر أو مسنجر إلى غير ذلك من خدمات الاتصال المخولة عبر الإنترنت، والتي من خلالها يمكن الكشف عن المعلومات الشخصية أو السرية الخاصة بالضحية.

ومن البديهي أن يقوم الجاني بعد الاطلاع على أسرار الأفراد أو الجهات بعد استلامها من نفس الشخص الذي كشفها له أو بالاستيلاء عليها بطريقة غير شرعية، أن يستغل معرفته بهذه المعلومات أو الأسرار لابتزاز وتهديد من تمسه المعلومة، وفي حالة عدم الحصول على مبتغاه ينفذ تهديده [1].

ولقد أثبتت الدراسات أن معظـم ضحايا هذا النوع من الابتزاز هن النساء خاصة عندما يكون الابتزاز ذات طبيعة جنسية، وغالبا ما تنتهي الجريمة بنهاية مأساوية وهي انتحار الضحية. وحالات الانتحار بسبب جريمة الابتزاز الالكتروني أصبحت ظاهرة منتشرة عبر كافة أنحاء العالم بما فيهم الجزائر، وأصبحت تتزايد يوما بعد يوم بسبب تفشي هذه الجريمة التي دمرت مئات الضحايا إنسانياً واجتماعياً.

ومن حوادث الانتحار العديدة التي وقعت في الجزائر، إقدام فتاة مراهقة من قسنطينة سنة 2014 على الانتحار سنة 4 نتيجة سلوك غير مشروع قام به الجاني، حيث أنشأ صفحة باسمها على الفيسبوك ونشر صوراً لها بعد القيام بسرقتها من هاتفها الذكي. ولم يقتصر فعله على ذلك بل قام بتصوير محادثة غير أخلاقية ذات طبيعة جنسية بين حسابه والحساب المزيف الذي أنشأه، وكانت غايته تهديد وابتزاز الضحية (م.أ). ولأنها لم تستطيع تنفيذ مبتغاه وتصبح خليلته، نفذ تهديده، وبسبب الضغوطات النفسية والفضيحة لجأت إلى الانتحار [2].

---

[1] – حنان ريحان مبارك المضحاكي ، الجريمة المعلوماتية ، المرجع السابق ، ص 337. 338

[2] – جريدة التحرير الجزائرية ، انتحار شابة بسبب فضيحة على الفايسبوك ، مقال منشور على الرابط التالي: اطلع عليه في 2017/10/19

https://www.altahrironline.com/ara/articles/71489

وفي هذا الشأن أيضا واقعة أثارت ضجة في العالم الأوروبي في أواخر 2013، عند اقدام الطفل الاسكتلندي دانييل بيري البلغ من العمر 17 على الانتحار، وقد كشف التحقيق أنه انتحر بسبب ضغوط نفسية نتيجة الاحتيال الذي تعرض له من طرف شخص أوهمه عبر برنامج مكالمات فيديو (سكايب) بأنه فتاة، وجعله يقوم بتصوير فيديوهات وصور مخلة بالحياء. وهدد بنشرها على الإنترنت إذا لم بوافق على طلباته.[1]

وأصدرت وكالة حماية الطفل البريطانية تحذيرا من أن عددا كبيرا من الأطفال في بريطانيا يتعرضون للابتزاز والطلب منهم القيام بأعمال جنسية على الإنترنت. ويقوم الجناة بالتظاهر بأنهم أطفال، ويعملون جاهدين على حـــــث الأطفـــــال على القيام بنشاطـــا جنسية وتصوير أنفسهم وإرسالها.[2]

أضف إلى هذا إحصاء جاءت به السلطات الجزائرية يفيد انه قد تم "في عام 2017 2500 جريمة عبر الإنترنت تتعلق بالابتزاز والتشهير والتحرش الإلكتروني، وإن ارتفاع معدل الجرائم الإلكترونية ترتبط في الجزائر ارتباطًا وثيقًا بأرقام مستخدمي الإنترنت، الذين يتجاوزون ثلاثة وثلاثون مليون جزائري ، منهم 19 مليون مشارك بفيسبوك. وبحسبهم فإن هذه الأرقام تعني أن شبكات التواصل الاجتماعي " أصبحت بؤرة خصبة لجميع أنواع الجرائم ".[3]

الفرع الثاني : أنواع ووسائل الابتزاز الالكتروني

الفقرة الأولى: أنواع الابتزاز عبر الإنترنت: من أهم أنواع الابتزاز عبر الإنترنت مايلي:

---

[1] – الهروب من الابتزاز الجنسي الإلكتروني إلى الانتحار ، الإمارات اليوم ، مقال منشور على الرابط : اطلع عليه في 2017/10/22

https://www.emaratalyoum.com/local-section/accidents/2015-12-20-1.851407

[2] – ابتزاز مئات الأطفال في بريطانيا" عبر الإنترنت ،مركز مكافحة استغلال الأطفال وحمايتهم على الإنترنت في بريطانيا ، إحصائيات نشرت على الرابط الأتي : اطلع عليه في 2017/10/25

https://www.bbc.com/arabic/worldnews/2013/09/130920_cyber_blackmail_childeren

[3] – قانون الجزائر الجديد لمكافحة الجريمة الالكترونية، مقال منشور على الرابط الأتي : اطلع عليه في 2017/10/26

https://al-ain.com/article/algeria-law-electronic-crimes

أولا–الابتزاز المادي: وفيه يطلب المبتز من الضحية سواء كان ذكرا أم أنثى بأن تدفع مبالغ مالية أو تسريب معلومات سرية، مقابل عدم نشر معلومات سرية تخصها أو تخص عملها عبر مواقع بالإنترنت، أو محادثات صوتية، أو مرئية لها، أو رسائلها الكتابية على الشبكة العنكبوتية، أو صور أو فيديوهات خليعة تخصها وإرسالها إلى أحد أقاربها، أو عبر أجهزة الكمبيوتر الشخصية، أو مواقع التواصل الاجتماعي، أو أجهزة الاتصال الحديثة.[1]

ثانيا–الابتزاز الجنسي : يقوم فيه المبتز بطلب ممارسة الجنس مع الضحية أو مرافقته لينفرد به في مكان خاص، إما معه أو مع شخص آخر يختاره لممارسة الفاحشة معه بمقابل مادي أو مجاناً. وقد يكون الضحية في الابتزاز الجنسي إما ذكرا أو أنثي أو مراهقا أو طفلا، خاصة في ظل الانتشار الكبير للشذوذ الجنسي.[2]

بالإضافة إلى الابتزاز الجنسي والمادي قد يكون الهدف من الابتزاز الرغبة في الانتقام، والتشفي علي سبيل المثال الابتزاز الموجه لأحدى الفتيات بغرض تدميرها لتخليها عنه مثلا، وإقامتها علاقة أخرى مع غيره، إلى غير ذلك من الأسباب التي تدفع للانتقام المرضي.

الفقرة الثانية : وسائل الابتزاز عبر الإنترنت

من أهم الوسائل التي يتم بسببها الابتزاز ويستعملها المبتزون للوصول إلى مبتغاهم هي:

– الصور الشخصية إما أن تكون صورا عادية أو صور يكون فيه الأشخاص في أوضاع مثيرة تكشف عوراتهم.

– التسجيل الصوتي للمحادثات التي تجري بينهما والتي قد تفضح الفاحشة من الطرفين إما برضا أحدهما أو بإيعاز أو إكراه من الآخر.

– مقاطع الفيديو التي يظهر فيها المجني عليهم في أوضاع مخلة بالحياء، أو صور أو فيديوهات تظهرهم مع أشخاص مشبوهين.

– الرسائل الكتابية إما عن خلال البريد الإلكتروني، أو عبر وسائل الاتصال بالإنترنت أو مواقع التواصل الاجتماعي.

---

[1] – ممدوح رشيد مشرف الرشيد، الحماية الجنائية للمجني عليه من الابتزاز، المجلة العربية للدراسات الأمنية، مجلد (33)، الرياض، 2017م ، ص 20

[1]– ممدوح رشيد مشرف الرشيد، المرجع نفسه، ص 20

-الملفات السرية أو الأسرار الخاصة بالعمل، خاصة الملفات السرية أو الأسرار التي تخص عمل المجني عليه، والتي لا يرغب في معرفتها من طرف الغير.[1]

ومن الحوادث التي نشرت حول جريمة الابتزاز عبر الإنترنت، قيام أحد الأشخاص بإنشاء موقع إلكتروني لفتاة من إحدى الدول الخليجية ونشر صورها بدون ملابس، إضافة إلى صور لها وهي في وضعيات خليعة رفقة صديق لها، ولقد استطاع الحصول على هذه الصور باختراق الحساب الخاص بها وسرقتها منه وقام بابتزازها بهدف جنسي، ونتيجة رفضها هددها بنشر صورها في مواقع على الإنترنت، وبسبب إصرارها على الرفض قام نفذ تهديداته وقام بتوزيع كافة صورها على العديد من المواقع عبر الانترنت، الأمر الذي أدى بالفتاة إلى الانتحار لعدم تحملها العيش بعد فضيحتها أمام الجميع[2]. إضافة إلى هذا هناك العديد من الحوادث المشابهة لهذه الحادثة والتي تمت في مختلف أنحاء العالم وغالبا ما تنتهي بنفس النهاية المؤلمة.

الفرع الثالث: أركان جريمة الابتزاز عبر الإنترنت

يقوم الابتزاز عبر الإنترنت على ثلاثة أركان وهما الركن الشرعي وهو نص التجريم والعقاب، وهو النص الذي يستند إليه تجريم سلوك معين والعقاب عليه وما يعرف بمبدأ الشرعية. بالإضافة إلى وجوب توافر الركن المادي للجريمة والركن المعنوي .

أولا: الركن المادي لجريمة الابتزاز

يقصد به السلوك الخارجي الذي يجرمه القانون، وبمعنى أخر كل ما يندرج تحت جريمة الابتزاز عبر الإنترنت ويحمل طابعا ماديا ملموسا يكون شرطا لتحقق الركن المادي.[3]

وينقسم الركن المادي إلي ثلاثة عناصر هي :

-السلوك الإجرامي: وهو سلوك مادي يمثل مظهرًا خارجيًا لعمل إجرامي أو مجموعة من العناصر المادية التي تضر بمصلحة محمية قانونًا. ويقصد بالنشاط المادي ذلك التصرف الذي يصدر عن الجاني في ظروف معينة ابتغاء تحقيق غاية إجرامية، ولقيام جريمة الابتزاز يشترط أن يكون السلوك الإجرامي للمبتز هدفه الحصول على أمر ضد إرادة

---

[1] – الموقع الالكتروني https://www.maghress.com/search

[2] – الموقع الالكتروني نفسه

[3] – حنان ريحان مبارك المضحاكي ، الجريمة المعلوماتية ، المرجع السابق ، ص 338

الضحية، كطلب مال ليس من حقه، كذلك المطالبة بإقامة علاقة جنسية مع الضحية أو مع غيره، ويجب أن يكون الفاعل جاداً في تهديداته، بحيث يشعر المجني عليه بالخطر وبأنه سينفذ تهديده في حالة عدم الحصول على مطالبه، ويجب أن يكون التهديد صريحا أو ضمنيا يفهم منه التهديد، ولا يشترط في التهديد طرق معينة سواء كان عن طريق البريد الالكتروني أو غرف المحادثة الشخصية، فالعبرة ليست بالمطلوب عمله من الجاني ولكن العبرة بالإكراه والضغط والتخويف المقترن بالتهديد لإرغام الضحية على المثول لطلبات الجاني.

-النتيجة الجرمية: يقصد بالنتيجة الأثر المترتب على سلوك الغير مشروع، وفي جريمة الابتزاز لا تحدث النتيجة الجنائية إلا بعد أن يهدد المبتز الضحية بإفشاء سر من أسراره، والذي يعتبره شيئاً لا ينبغي لأحد أن يعرفه.

-العلاقة السببية : هي العلاقة بين السلوك المحظور والآثار التي يقرها القانون، ولقيام الركن المادي لا بد من أن تعزى نتائج الجريمة إلى الواقعة المحددة للجريمة، أي نتيجة الجريمة، أي أن النتيجة الجرمية تحدث بسبب الفعل الغير مشروع .

ثانيا: الركن المعنوي لجريمة الابتزاز

يشترط لقيام جريمة الابتزاز توافر القصد الجنائي، وعليه يجب أن يعلم المبتز أن ما يقوم به من الحصول على صور فاضحة أو أسرار غير مرغوب الاطلاع عليها وقيامه بتهديد الضحية بهذه المعلومات مقابل أي منفعة كانت هي جريمة معاقب عليها، وينبغي أن يعلم بأن فعله سيلحق الضرر بالمجني عليه. ولا يكفي علمه بالوقائع التي تشكل ماديات الجريمة بل يجب أن تتجه إرادة الفاعل إلى تحقيق نتيجتها، ومن البديهي أن لا يعتد القانون بهذه الإرادة ما لم يتمتع الفاعل بالإدراك وحرية الاختيار. ويجب أن يكون الهدف من التهديد والابتزاز الحصول على منفعة غير شرعية.[1]

وفي النهاية يمكننا القول أنه صحيح أن الضحية أو الشخص الواقع عليه الابتزاز يعاني من ضغوط نفسية كبيرة عند تهديده بفضحه أو بتسريب معلومات سرية تخصه ولا يستطيع أي شخص تخيل حجم الضغوطات والمعاناة ، إلا أنه يجب التفكير بطرق سليمة ومجدية

[1] – حنان ريحان مبارك المضحاكي ، الجريمة المعلوماتية ، المرجع السابق ، ص 338. 339

للتخلص من هذا المشكل، ونشير إلى أن التفكير في الانتحار عمليا لا يخلص الشخص من جريمة التهديد والابتزاز، بل يصعد الأمور حتى بعد إقدام الضحية على تنفيذ هذا الفعل، كون المشكلة لم تحل وقد تنتقل المعاناة إلى أهل الضحية .

المطلب الثاني: جريمة القتل والتحريض على القتل والمساعدة على الانتحار عبر الإنترنت

لقد تضاعفت جرائم الإنترنت بصورة كبيرة وفي مختلف دول العالم من خلال تسخيـــــر المجرمين لتقنية المعلومات والمعرفة المعلوماتية لممارسة سلبياتهم وأعمالهم المشينة على الشبكة حيث لا يتردد الكثير منهم عن سلوك طرق وأساليب قذرة للوصول إلى أهدافهم. ومن بين الجرائم التي طالتها أيدي مجرمي الإنترنت وطورت منها وجعلتها من الجرائم التي يتم ارتكابها عبر شبكة الإنترنت جرائم القتل العمد وكذلك جرائم التحريض على القتل أو الانتحار، هذه الجرائم التي انتشرت بطريقة مروعة في الآونة الأخيرة، خاصة جرائم التحريض على القتل والانتحار عبر الإنترنت التي باتت آثارها تظهر في مختلف أنحاء العالم. ومن خلال هذا المطلب سنقوم بدراسة هذه الجرائم، من خلال عرض مفهوم القتل عبر الإنترنت، وذلك عن طريق تعريف القتل لغة واصطلاحا ثم تعريفه عندما يتم عبر الانترنت مع بيان الأركان الأساسية للجريمة وهذا سيكون في الفرع الأول، أما في الفرع الثاني سنتطرق لدراسة مفهوم التحريض، وذلك عن طريق تعريف التحريض على القتل عبر الإنترنت، وبيان أنواعه، وأركانه، أما المطلب الثالث سنتطرق فيه لدراسة التحريض على الانتحار عبر الانترنت، خاصة وأنها جرائم تكاد تنعدم فيها الدراسة كونها جرائم مستحدثة.

الفرع الأول : جريمة القتل عبر الإنترنت

القتل العمد من أبرز جرائم الاعتداء الواقعة على الأشخاص وأخطرها كونه يستهدف إزهاق روح بشرية. وهي في مقدمة السلوكيات التي تسعى مختلف التشريعات الوضعية للحماية منها على مر السنين، وتظهر هذه الحماية من شدة العقوبة على الجاني المتعمد والمتمثلة في عقوبة الإعدام، وقد عاقبت الشريعة الإسلامية أيضا القاتل المتعمد بالقتل

عملا بقوله تعالى {وكتبنا عليهم فيها أن النفس بالنفس.. } المائدة الآية 45، وقوله تعالى :{ يا أيها الذين آمنوا كتب عليكم القصاص في القتلى } البقرة ، الآية 178.

ومع ازدهار الإنترنت وتطور تقنياتها، حدث تغير في شكل جرائم القتل، حيث أصبحت جريمة القتل قابلة للتحقيق بطريقة غير مباشرة عبر الإنترنت التي تزداد شرورها يومًا بعد يوم. ففي الوقت الذي كانت فيه جريمة القتل عبر الإنترنت من الجرائم التي كانت في كثير من الأذهان جريمة يستحيل وقوعها عبر الإنترنت بالرغم من تحذير منظمة الشرطة الأوروبية التي يطلق عليها "يوروبول" في سنة 2014 من جريمة القتل الأولى عبر الإنترنت واعتبرت حدوثها وشيكا، وهذا في ظل تزايد وتيرة الهجمات الإلكترونية وهجمات القرصنة، والاعتماد المتزايد من قبل الشركات التكنولوجية الكبرى على الإنترنت، حيث أن كل شيء تقريباً أصبح متصلاً بالإنترنت".[1] ولم تخطئ في تنبؤها. ففي عام 2016 أكدت السلطات المصرية على وقوع جريمة قتل عبر الإنترنت في أحد المستشفيات بالقاهرة. وفي سبتمبر 2020 بأحد المستشفيات بألمانيا توفيت امرأة لأنها لم تتلق العلاج. وكان هذا بسبب هجوم إلكتروني استهدف الشبكة الإلكترونية للمستشفى، مما أدى إلى شل أنظمتها جزئيًا. وكان الهدف من ذلك الحصول على فدية لإعادة الأنظمة إلى الحالة التي كانت عليها [2].

الفقرة الأولى : مفهوم القتل عبر الإنترنت

قبل تناولنا لتعريف جريمة القتل عبر الإنترنت لابد من تسليط الضوء أولا على تعريف القتل لغة واصطلاحا.

أولا :تعريف القتل لغة

قتل: مصدر قتل . 2 – إزهاق الروح ، إماتة . 3 – « القتل العمد » : "هو ما تعمده القاتل ضربا بالسلاح أو غيره" . 4 – « القتل الخطأ » : بدون قصد.[3]

---

[1]-منظمة الشرطة الأوروبية 'يوروبول' الموقع اطلع عليه في 2017/06/29
http://www.jo24.net/post.php?id=87740

[2] –هجوم الكتروني على مستشفى ألماني، الموقع اطلع عليه في 2021/05/23، http://www.youm7.com

[3] – جبران مسعود ، الرائد معجم لغوي عصري ، دار العلم للملاين ، مجلد واحد ، طبعة 7 ، 1992، مادة قتل

ثانيا : تعريف القتل من الناحية الفقهية والقانونية

إن أغلب الفقهاء من حنفية وشافعية يعرفون مصطلح القتل بأنه " كل فعل من العباد يؤثر في إزهاق الروح " أي كل فعل صادر من العباد ويكون أثره إزهاق روح بشرية .[1]

أما من الناحية القانونية فقد عرف القتل العمد بأنه "إهدار حق المجني عليه في إزهاق روحه عن قصد، مهما كانت الوسيلة، وفعل الاعتداء على الحياة هو الذي يتمثل في سلوك الجاني بإتيان فعل يؤدي بطبيعته إلى الوفاة مقترنا بنية القتل وتحقق وفاة المجني عليه بالفعل." [2] وقد عرفه المشرع الجزائري في نص المادة 254 ق ع "القتل إزهاق روح إنسان عمدا".

ثالثا : تعريف القتل عبر الإنترنت

يمكـن تعريف القتـل عبر الإنترنت بأنه، إزهاق روح إنسان قصدا باستعمال شبكة الإنترنت.

وفي هذا الصدد سنة 2016 تم إفصاح مدير مباحث الإنترنت بوزارة الداخلية المصرية عن حدوث جريمة قتل مع سبق الإصرار من خلال الإنترنت. وأن جريمة القتل المرتكبة عن طريق الإنترنت تمت بواسطة اقتحام الشبكات من طرف هاكرز، حيث قام بجريمة قتل عمدية، بعد قيامه بتغيير بعض بيانات المريض والأدوية التي كانت تعالجه، على الشاشة الخاصة بعلاجه والمتصلة بالشبكة، الأمر الذي تسبب في وفاته[3]. وبذلك تم القتل العمد بطريقة غير مباشرة باستخدام شبكة الإنترنت مباشرة.

وقد يتم القتل أيضا باستخدام شبكة الإنترنت التي تسهل على الجاني اختيار وجذب ضحاياه، تمامًا مثل الحالة الشهيرة في اليابان في 30 أكتوبر 2017 أين اكتشفت عدة

---

[1] – جلاب حنان ، السببية في جريمة القتل دراسة مقارنة بين الفقه الجنائي الإسلامي و قانون العقوبات الجزائري ،رسالة مقدمة لنيل الماجستير في الشريعة والقانون ، باتنة ، سنة 2004، ص 9

[2] – حسين فريجة ، شرح قانون العقوبات الجزائري جرائم الأشخاص والأموال ، ديوان المطبوعات الجامعية ، الجزائر ،طبعة 2 ، 2009 ، ص29 .

[3] – مباحث المعلومات: يمكن ارتكاب كل الجرائم عبر الإنترنت بما فيها القتل، الموقع اطلع عليه في 2017/06/29 https://www.youm7.com

جثث مقطوعة لرجال ونساء في غرفة بشقة في مدينة زاما بمحافظة كاناغاوا. ووجهت للمتهم شيراش إيتاكاهيرو تهمة السطو والاغتصاب والقتل باستخدام تويتر ووسائل التواصل الاجتماعي الأخرى لجذب الضحايا مستغلا مشاكلهم والضغط المحيط بهم[1].

وقد يتم القتل في بعض الحالات بسب الإنترنت، وبمعنى أخر هناك جرائم قتل تكون المواقع عبر الإنترنت طرفا فيها، ولقد نشرت مجلة مشهورة بالولايات م الأمريكية تقريرا في هذا الشأن تحدثت فيه عن جرائم بشعة كان لمواقع التواصل الاجتماعي الدور الأهم في وقوعها، وتتسبب البعض فيها إدمان المستخدم الشديد، وبعضها يعود إلى وقوع الضحايا في يد أشخاص لا يرجمون، وبعضها يتسبب قيه مرض الغيرة.[2]

ومع التطور التكنولوجي المذهل الذي يشهده عالمنا اليوم فمن البديهي تطور الجرائم التي تعتمد في ارتكابها على التكنولوجيا ولا نستطيع تخيل إلى أي مدي يمكنها أن تتطور، وإلى أي مدى ستصل .

الفقرة الثانية: أركان القتل عبر الإنترنت :

إن أركان القتل عبر الإنترنت هي بعينها أركان جريمة القتل التقليدية ولكن بإضافة الانترنت كوسيلة تتم عبرها الجريمة أو تسهل في ارتكابها. وعليه تتحقق جريمة القتل عبر الإنترنت أو عن طريق الإنترنت بتوافر الركن الشرعي المتمثل في المادة القانونية التي تجرم السلوك، أي أن وجود النص يكون قبل حدوث الفعل. وينص المبدأ على أنه لا يمكن معاقبة الشخص على فعل ارتكبه إلا إذا كان النص قد جعله مجرماً قبل ارتكاب الفعل، وأن يتم القتل على إنسان حي بالإضافة إلي وجوب توافر الركن المادي والركن المعنوي.

أولا: محل القتل

بصفة عامة، إن محل جريمة القتل العمد هو الحق الذي تمثله الحياة، وبالتالي فإن هدف الجريمة هو الشخص الحي. إذ يفترض في المجني عليه أن يكون إنسانا على قيد

---

[1] – جرائم الانترنت ، الموقع اطلع عليه في 2017/06/29
https://www.nippon.com/ar/features/c05701

[2] –جرائم تسببت فيها مواقع التواصل الاجتماعي، تقرير نشرته "عربي21"على الرابط الأتي :
https://www.alalamtv.net

الحياة وقت ارتكاب الجاني نشاطه الإجرامي، وحماية حياة الإنسان هي الهدف الأسمى للقانون. [1]

ثانيا: الركن المادي للقتل

هذا الركن يتطلب توافره في جميع صور القتل مهما كانت، والركن المادي يقوم على ثلاثة عناصر:

1-النشاط المادي : يشترط في جريمة القتل توفر نشاط إجرامي إرادي يصدر من الجاني، وغالبا ما يتخذ هذا النشاط شكلا ايجابيا وقد يتخذ صورة حركة عضلية بالضغط على زر جهاز الحاسوب لإتمام الجريمة مثلا، ومهما اختلف شكل النشاط الايجابي يضل النشاط الإجرامي واحد وهو إزهاق روح إنسان ، ولا يهم بعد ذلك الوسيلة المستعملة في ذلك .

2-النتيجة (إزهاق الروح)

وتكتمل جريمة القتل بموت المجني عليه، وقيام الجاني بفعل من شأنه أن يسبب الوفاة لا يكفي، بل يجب أن يؤدي هذا الفعل إلى وفاة المجني عليه. فالوفاة هي النتيجة الإجرامية التي قصدها الجاني بفعله الإجرامي.

3- توافر علاقة السببية بين الفعل المادي والنتيجة

يتعين لمساءلة الجاني ارتباط نشاط الجاني بحدوث النتيجة وهي الوفاة وهذا الارتباط ما يسمى بعلاقة السببية، ذلك أن الإنسان لا يسال عن النتيجة الإجرامية إلا إذا كانت ناتجة عن سلوكه، وإذا لم تكن علاقة مادية بين السلوك وحصول النتيجة الإجرامية فلا يمكن أن تسند إليه النتيجة بأي حال من الأحوال .

ونسبة لما سبق فانه لقيام جريمة القتل عبر الإنترنت يتعين على الجاني الاعتداء عبر الإنترنت أو باستعمال وسيلة من وسائل الاتصال المتوفرة عبر الإنترنت أو بواسطتها فعل يؤدي إلى إحداث الوفاة .

ثالثا: الركن المعنوي للقتل

تقتضي جريمة القتل عبر الانترنت توافر القصد الجنائي لدى الجاني.

[1]- JC Smith –B Hogan ,Criminel Law , Fifth Edition , Butter worths, London , 1983, p 272

1-القصد الجنائي العام

إن جريمة القتل عبر الإنترنت تنطوي على عنصرين وهما العلم والإرادة. بالنسبة للعلم يجب أن يكون مرتكب الجريمة على علم بأنه سلوكه سيؤدي بحياة الضحية، ويجب أن يكون على علم بأن سلوكه الإجرامي كان موجهًا إلى الضحية، وأنه في النهاية يجب أن يكون مرتكب الجريمة قد توقع أن الموت سينتج عن فعله. أما الإرادة فتتحقق بتوجيه إرادة الجاني لارتكاب سلوك الاعتداء عبر الإنترنت، وأيضا إلى أن تكون نتيجته إزهاق روح إنسان.

2-القصد الجنائي الخاص

يشترط توافر القصد الخاص لقيام جريمة القتل العمد، والمتمثل في نية قتل المجني عليه وإزهاق روحه.

وخلاصة القول ينبغي توافر جميـــــع الأركـــــان السابقـــة الذكر لقيام جريمة القتل عبر الإنترنت وانتفاء أي منها يؤدي إلى انتفاء الجريمة بأكملها.

الفرع الثاني : جريمة التحريض على القتل عبر الإنترنت

يعد التحريض من أخطر أشكال النشاط الإجرامي، حيث يكون المحرض في الغالب هو العقل المدبر لارتكابه، والعقل المدبر هو المسؤول الأول عن تنفيذها، وقد طالبت بعض القوانين استبعاد التحريض من نطاق المشاركة في الجريمة واستقلاله، واعتبار المحرض في حكم الفاعل الأصلي[1]. فالتحريض هو قيام شخص وهو المحرض بدفع أخر إلى ارتكاب الجريمة، إما بخلق أو زرع فكرة الجريمة في ذهنه. وهو سلوك يلعب دورًا في التأثير على الحالة النفسية لشخص آخر[2]. لذلك يرى معظم الفقهاء أن المحرض هو إنسان أخطر من الفاعل، فيستوي أن يوجه التحريض إلى شخص كان في الأصل خالي الذهن عن الجريمة، أو أن يوجه إلىَ شخـــص وجدت لديـــه أصـــلا فكرة الجريمة لكنها لم تتطور حتى يدفعه

[1] – عبد الحميد أحمد شهاب، "نظرية الفاعل المعنوي(دراسة مقارنة)"، مجلة الفتح، كلية القانون، جامعة ديالي، العدد 34، 2008 ،

[2] – محمد صبحي نجم، قانون العقوبات، القسم العام، النظرية العامة للجريمة، د ط، دار الثقافة للنشر و التوزيع، عمان، 2010 ، ص338

المحرض ويعقد العزم على ارتكابها.[1]

ومع ظهور وسائل الاتصال الحديثة خاصة شبكة الإنترنت أخذ التحريض على الجريمة منحنى أخر أخطر من ما كان عليه وأصبح المحرض يتخذ مختلف المواقع عبر الإنترنت لتنفيذ مخططاته، خاصة جرائم التحريض على العنف التي أصبحت تهدد كافة المجتمعات ومن أخطرها التحريض على القتل .

الفقرة الأولى : مفهوم التحريض على القتل عبر الإنترنت

يطلق على المحرض مصطلح محرك الشر، وهو الشخص الذي يعزز الرغبة في نفس شخص معين ويشجعها على ارتكاب الجريمة. مستخدما عدة وسائل للوصول لمبتغاه ومن بين هذه الوسائل الإنترنت التي أصبحت من أهم الوسائل المستغلة للتحريض على كل أنواع العنف ومن بينها القتل. وقبل التعرض لتعريف التحريض على القتل باستخدام الإنترنـــت بصفة مفصلة نتجه لتعريف التحريض بصفة عامة.

أولا : تعريف التحريض من الناحية اللغوية والفقهية والقانونية

1-تعريف التحريض من الناحية اللغوية

حرض:" التَّحْرِيض، التَّحْضِيض. قال الجوهري: التَّحْرِيضُ على القتال الإِحْماءُ والحث عليه". ويقال حارَضَ فلان على العمل وواكَبَ عليه وواظَبَ وواصَبَ عليه إِذا داوَمَ القتال ".[2]

2- :تعريف التحريض من الناحية الفقهية والقانونية

1-تعريف التحريض

لقد تعددت التعريفات لتحديد معنى التحريض على الجريمة، ولم يتفق الفقهاء على تحديد تعريف موحد، فمنهم من عرف التحريض على" أنه الدفع إلي الشر ". ومنهم من

[1] عبد الملك جندي ، الموسوعة الجنائية ، منشورات الحلبي الحقوقية، 2010 ، ص.705

[2] – إبن منظور ، مادة حرض، المرجع السابق ، ص 135

عرفه بأنه " خلق فكرة الجريمة لدى شخص تم تدعيمها كي تتحول إلى تصميم لارتكاب الجريمة ".[1]

أما التعريف القانوني فنجد البعض يعرفه بأنه "خلق فكرة الجريمة، وخلق التصميم عليها في نفس الجاني بأي وسيلة كانت"، ويتضح من هذا التعريف أن النشاط التحفيزي له طابع معنوي. وهذا التحفيز يدخل في دائرة الفكر والنية ليس في دائرة العمل والنتائج، لذلك إذا كان المحرض يناشد أفكار الفاعل فإنه يناشده قبل ارتكاب الفعل وليس بعده أو أثنائه، وهذا هو الذي يجعله منه فعل تحضيري لا فعل تنفيذي.[2]

وبالرجوع إلى المشرع الجزائري فإنه يعتبر المحرض على الجريمة فاعلا أصليا مخالفا بذلك أغلب التشريعات كالتشريع المصري الذي يعتبره شريكا. وإن التحريض بطبيعته يسبق دائما وقوع الجريمة، لأنه مجرد خلق فكرة أو زرعها في عقل الفاعل، وتثبيتها إذا لم تكن ثابتة أو غير حاسمة، وذلك دون أخذ بعين الاعتبار الوسيلة المستعملة لبلوغ هدفه وهذا ما جاءت به المادة 41 من ق ع ج[3].

ثانيا : تعريف التحريض على القتل عبر الإنترنت

من خلال التعريفات السابقة لجريمة التحريض يمكننا تعريف التحريض على القتل عبر الإنترنت بأنه قيام الجاني وهو المحرض، باستخدام واحدة من مختلف الخدمات التي تقدمها شبكة الإنترنت للاتصال عبرها بشخص أو عدة أشخاص ودفعهم إلى ارتكاب الجريمة، إما بخلق أو زرع فكرة الجريمة في ذهنه، فالمحرض يؤدي دوره بالتأثير على نفسية شخص أخر بزرعه لفكرة الجريمة في ذهنه وإقناعه بتنفيذها بكافة الوسائل المقنعة .

ويمكن أن يؤدي التحريض على القتل عبر الإنترنت إلى إنفاذ جريمة القتل واقعيا، مثلا من خلال مواقع التنظيمات الإرهابية التي تستهدف بحسب تصنيفها فئة معينة من المجتمع

---

[1]– نظام توفيق المجالي، شرح قانون العقوبات، القسم العام، ط 1 ، دار الثقافة للنشر و التوزيع، عمان، 2009 ، ص314.

[2]– جلال ثروت، نظم القسم العام في قانون العقوبات، دار العلوم للنشر والتوزيع، إسكندرية، 1999 ،ص345

[3] – محمد صبحي نجم، قانون العقوبات، القسم العام، النظرية العامة للجريمة ، مرجع سابق ،ص.337.

لقتلها. وقد انتشر هذا النوع من المواقع بين الجماعات الدينية التي أتاحت لها الإنترنت وبدون حدود نشر أفكارها ومعتقداتها.[1]

وعليه فجريمة التحريض عبر الإنترنت قد تكون بزرع بعض الأفكار المتطرفة التي قد تكون عنصرية أو سياسية أو اقتصادية أو دينية والهدف منها هو التلاعب بعقول الناس ونشر الصراعات والاستفادة من مشاكلهم لتحقيق مكاسب شخصية تتعارض مع مصالح المجتمع. وقد يكون التحريض صادرا عن شخص جاهل لكيفية استخدام التقنية المعلوماتية وبمساهمة شخص أخر خبير بتقنية المعلومات ترتكب الجريمة بناء على اتفاق بينهما، وباستجابة الشخص الذي وجه له التحريض عبر الوسائط الالكترونية قد ينتج الأثر الوخيم للجريمة.

الفقرة الثانية : أنواع التحريض

ينقسم التحريض من حيث من يوجه إليه، إلى تحريض خاص وفردي، وتحريض عام أي موجه إلى الجمهور.

أولا: التحريض الفردي :

التحريض في أصله يستهدف شخصا محددا،[2] ويجب أن يكون ذلك بطريقة مباشرة توجه إرادة فرد محدد إلى ارتكاب النشاط المكون للجريمة بنفسه، ويجب أن يركز على فعل غير قانوني محدد والمتمثل في القتل مثلا، بحيث يقوم المحرض بالاتصال بالفاعل والتأثير عليه للقيام بجريمته، وقد يتم التحريض الفردي بوسيلة القول، أو الكتابة، أو بواسطة رسالة أو عبر أية وسيلة متوفرة عبر الإنترنت تنتج أثرها فيخلق فكرة الجريمة لدى الغير، أو بالتشجيع عليها، وفي نفس الوقت يجب أن يكون التحريض واضحا، ومباشرا كما يجب أن تكون أيضا وسيلته واضحة، ومباشرة في دفع الغير للقيام بالسلوك الغير قانوني .[3]

---

[1] – وليد احمد ، جرائم ساهم الانترنت في انتشارها ، مقال منشور على الرابط الاتي :
/https://www.tech-wd.com/wd/2013/08/12/internet-crimes

[2] – محمود نجيب حسني، المساهمة الجنائية في التشريعات العربية، ط 2 ، دار النهضة العربية، القاهرة، 1998 ، ص.298

[3] – فخري عبد الرزاق الحديثي و خالد حميدي الزغبي، شرح قانون العقوبات القسم العام، دار الثقافة للنشر والتوزيع، عمان، ط 1 ، 2009 ، ص. 165

ثانيا: التحريض العام

يطلق عليه الإقناع الجماعي، ويشير إلى مجموعة من الأشخاص المجهولين الذين يجبرون الناس على القيام بشيء غير قانوني.[1] ويشترط أن يكون السلوك التحريضي علنيا، أي أن يتم إبلاغ حالة الحادثة المحددة والكشف عنها ونشرها بين الناس، وهذا هو شرط معاقبة مثل هذا السلوك التحريضي. [2]

فالتحريض العمومي هو أشد خطورة من التحريض الفردي، لأن العلانية تعد وسيلة سريعة الانتشار، وأشد انفعال بين الجمهور كما يعتبر أيضا الجمهور أسرع تأثرا على خلاف التحريض الفردي.[3] ولكي يعتبر التحريض العمومي تحريضا علنيا لابد من توافر مجموعة من الوسائل كالكتابة، والرسوم، والصور إذا وزعت، أو بيعت لأكثر من شخص، أو حركات في الطريق العمومي، أو حفل، أو مكان مفتوح أمام أعين الجمهور، يتحدثون فيه أو يصرخون بصوت عالٍ، وترديده في مكان عام مثل مواقع الإنترنت، وغيرها من وسائل الدعاية و النشر.[4]

إن خصوصية التحريض أنه كلام يستهدف العواطف والغرائز، وليس مناشدة للعقل، وكل تحريض جوهره هو الإيحاء، أي هي عملية نفسية هدفها إدخال فكرة إلى ذهن الشخص، لأن الفكرة متى استقرت مالت إلى التنفيذ بحكم طبيعة النفس إلى التحول إلى فعل أو تركه. [5]

الفقرة الثالثة :أركان جريمة التحريض على القتل

لكل جريمة أركانها الخاصة، وهي شروط حددها التشريع للعقاب، و إن هذه الأركان تختلف من جريمة إلى أخرى بحسب نوعها وطبيعتها، مثل ما هو الحال بالنسبة لجريمة

---

[1] – علي عبد القادر القهوجي، شرح قانون العقوبات القسم العام، دار العلوم للنشر والتوزيع ، إسكندرية، 1998 ،ص. 456.

[2] – أكرم ابراهيم نشأت، القواعد العامة في قانون العقوبات المقارن ، دار الجامعية للطباعة و النشر، بغداد، 1998، ص214

[3] – محمود نجيب حسني، المرجع السابق، ص 292 293.

[4] – فهد بن مبارك العرفج، التحريض على الجريمة في الفقه الإسلامي والنظام السعودي دراسة تأصيلية تطبيقية، تخصص لقانون الخاص و العلوم الجنائية، مذكرة ماجستير، جامعة نايف العربية للعلوم الامنية، 2006 ، ص 123.

[5] – فهد بن مبارك العرفج ، المرجع نفسه ، ص135

التحريض على الجريمة ومن بينها التحريض على القتل خاصة المرتكبة عبر الإنترنت التي تختلف عن الجرائم لأخرى نظرا للطبيعة الخاصة للتحريض، وحتى تقوم هذه الجريمة لا بد من توفر أركانها، وفي حالة انتفاء أي ركن من الأركان التي تقوم عليها فلا تقوم هذه الجريمة، و يتمثلّ الركنان الأساسيان لجريمة التحريض في الركن المادي، والركن المعنوي اللذان تنحصر فيهما الجريمة أما الركن الشرعي لجريمة التحريض هو خضوعه لنص التجريم. وسنخص بالدراسة الركن المادي والمعنوي لجريمة التحريض على القتل عبر الإنترنت مثلما تعودنا سابقا

أولا : الركن المادي

إن الركن المادي لجريمة التحريض على القتل في صورته التقليدية أو عندما يتم باستعمال شبكة الإنترنت، يتكون من عدة عناصر وجب توافرها لتحقيقه.

-**الفعل الإجرامي للمحرض:** ويتمثل في النشاط الذي يصدر عن المحرض، وهو كل عمل إيجابي ومهما كان نوعه، فالتحريض لا يقع بموقف سلبي إنما يستلزم خلق فكرة الجريمة، وإدخالها في ذهن كان خاليا منها ، فالمحرض هو صاحب فكرة الجريمة والرأس المدبر، فهو عقل الشخص الذي يرتكب الجريمة، والفاعل المباشر ما هو إلا أداة في يد المحرض، يحركها حسب رغبته، لأنه لو لم يكن التحفيز في التحريض فبالطبع لما كانت هناك جريمة. فالتحريض إذن هو من عمل المحرض، وليس من يوجه له التحريض من خلال التأثير على نفسيته عن طريق زرع الكراهية والعداوة فيه، ويصبح ذلك مبررا للجريمة.[1] ويمكن أن يكون التحريض بالكتابة، أو القول، أو الإيحاء، وغيرها من الوسائل فجميعها تملك نفس القيمة القانونية، وليس مهما إن كان التحريض فرديا موجها إلى الفرد، أم جماعيا متجها إلى الجمهور، فالمهم هو أن نشاطه يتجه إلى التحريض.[2]

-**النتيجة الإجرامية لنشاط المحرض:** النتيجة هي قيام الفاعل الأصلي بالجريمة فهي تعتبر كأثر للنشاط المادي المرتكب، وبالتالي فإن الشخص لا يسأل عن الجريمة إذا لم تكن

[1] – محمود نجيب حسني، المرجع السابق، ص .148

[2] – فخري عبد الرزاق الحديثي وخالد حميدي الزغبي، المرجع السابق، 163.

ناتجة عن النشاط الإجرامي، وهذا يتحقق بمجرد وقوع فعل الجريمة المحرض عليها. إذا المبدأ العام أن تترتب النتيجة على نشاط المحرض، و يتولد عن هذا تحقيق نتيجة جرميــة وهي موت الضحية، كما ترتبط هذه النتيجة بنشاط الجاني بالعلاقة السببية. [1]

-**علاقة السببية بين المحرض والجريمة المرتكبة** : فعلاقة السببية هي الرابطة بين الفعل المرتكب والنتيجة الحاصلة من هذا الفعل، بمعنى ارتباط الفعل بالنتيجة، وتحدد مسؤولية الجاني عن جريمته حسب طبيعة العلاقة بين أفعاله ونتائجها. ولذلك لا يسأل الفاعل عن نتائج جريمته إلا إذا كانت هناك علاقة سببية بين الجريمة ونتائجها. وهي صلة تربط بين الأفعال التي يقوم بها الفاعل وبين عواقبها، وإذا وجدت فالفاعل مسؤول عن عواقب أفعاله.[2]

ثانيا :الركن المعنوي للتحريض

يتطلب الركن المعنوي انصراف عناصره إلى إنشاء التصميم لارتكاب الجريمة، باعتبار أن التحريض هي جريمة عمدية لا تتحقق إلا بتوفر القصد الجنائي أي نية الإجرام، ولا يمكن تصور وقوعها عن طريق الخطأ أو الإهمال، وللقصد عنصران هما العلم والإرادة، فالعلم يكمن أن يكون المحرض عالما بأن الطريقة أو الوسيلة التي لجأ إليها للقيام بالتحريض من شأنها أن تأثر في نفس المحرض لارتكاب الجريمة التي تم التحريض عليها. أما الإرادة بمعنى أنها تكون إرادة المحرض قد اتجهت إلى خلق التصميم لدي المحرض لارتكاب الجريمة.[3]

الفرع الثالث : جريمة المساعدة على الانتحار عبر الإنترنت

لقد أصبحت ظاهرة التحريض على الانتحار ظاهرة منتشرة بشكل كبير ومتزايد حيث مست كل المجتمعات الغربية منها والعربية، ولقد أصبحت الإنترنت بيئة غنية بهذا النشاط الإجرامي وأضحى واقعا يهدد وبشكل مروع حياة الأفراد خاصة فئة المراهقين منهم، حيث

---

[1] – فخري عبد الرزاق الحديثي وخالد حميدي الزغبي، المرجع نفسه، ص 164

[2]-- فوزية عبد الستار، المساهمة الأصلية في الجريمة، تخصص القانون الخاص و العلوم الجنائية، رسالة دكتوراه، القاهرة، 1967 ،ص. 351

[3]– فوزية عبد الستار، المساهمة الأصلية في الجريمة، ، المرجع السابق ، ص. 351.

قام بعض الجناة باستغلال الصفحات الموجودة عبر الإنترنت واستتروا خلفها لمزاولة هذا النشاط الغير مشروع.

الفقرة الأولي : مفهوم الانتحار

يعد الانتحار قتلا للنفس، وهو رد فعل مأساوي على حياة مرهقة. وأبرز العوامل التـــي تزيد من خطر محاولة الانتحار الاضطرابات النفسية والعاطفية التي قد تصيب بعض الأشخاص خاصة إذا ما استغلها أطراف خارجية فقد تؤدي حتما إلى نتائج سلبية. والإنترنت وسيلة من الوسائل التي يستخدمها الجناة للاتصال بهذا النوع من الأشخاص للضغط عليهم ودفعهم لوضع حد لحياته بالوسائل التي تؤدي لتلك النتيجة. وقبل تناول تعريف هذه الجريمة عند ارتكابها باستخدام الانترنت. نتناول أولا تعريف الانتحار لغة واصطلاحا.

أولا : تعريف الانتحار من الناحية اللغوية والفقهية والقانونية

1-تعريف الانتحار من الناحية اللغوية

إنتحر، انتحارا . إنتحر : قتل نفسه. إنتحر القوم على الشيء : تخاصموا عليه . إنتحر هب العصا : ضربه بها.[1]

2- تعريف الانتحار من الناحية الفقهية والقانونية

يعرف العالم الاجتماعي الفرنسي إميل دور كايم الانتحار على أنه" الفعل المشير إلى المـــوت الذي يرجع بصورة مباشرة أو غير مباشرة، ولفعل ايجابي أو سلبي قام به الشخص المنتحر" وهناك تعريف بديل لهذا التعريف وجاء فيه بأن الانتحار يشير إلى ظروف قاتلة ناتجة عن أفعال إيجابية أو سلبية يقوم بها الشخص الانتحاري وهو يعلم أن ذلك سيؤدي إلى نتيجة.[2]

وقد فرق الفقيه هيفلاكس بين السلوك الإرادي الانتحاري إن صح التعبير، وبين أشكال الموت الجماعي وأهمها التضحية، فالانتحار بحسبه هو الموت الناتج عن فعل يأتيه

[1] – جبران مسعود ، الرائد معجم لغوي عصري ، دار العلم للملاين ، مجلد واحد ، طبعة 7 ، 1992، مادة انتحر

[2]– محمد على محمد ، رواه علم الاجتماع ، قراءة جديدة للذكر الاجتماعي العربي ، الهيئة المصرية العامة للمكاتب ، الإسكندرية ، 1976 ، ص120

الضحية لنفسه قصد قتلها وليس التضحية بها لشيء أخر فهو موت إرادي يقدم عليه القرد للتخلص من مشاكله وصعوباته.[1]

وحسب المشرع الجزائري المستمد من القانون الفرنسي الذي أباح الانتحار والشروع فيه هذا إذا كان الفعل صادر عن محض إرادة الشخص، بعيدا عن أية ضغوط أو تحريضا، وبالرجوع إلى النصوص القانونية في قانون العقوبات، فإنه لا يوجد أي نص يجرم الانتحار والمواد 254 وما بعدها تتعلق سوى بالقتل. وبالتالي فواقعة الانتحار لا تعد جريمة لانعدام النص القانوني، وفي المقابل يعاقب القانون الجزائري كل شخص ساعد الضحية على الانتحار حسب أحكام المادة 273 ق ع ج. [2]

ثانيا: تعريف المساعدة على الانتحار عبر الإنترنت

من خلال التعريفات السابقة لجريمة التحريض على الانتحار يمكننا تعريف الانتحار عبر الإنترنت على أنه خلق فكرة الانتحار أو خلق التصميم عليها في نفس الضحية مستخدما في ذلك الحاسوب والإنترنت لزرع فكرته أو تحقيق هدفه. فالتحريض على الانتحار عبر الإنترنت هو كل سلوك يتم باستغلال الخدمات المتوفرة عبر الإنترنت كغرف الدردشة أو عبر مواقع التواصل الاجتماعي ويراد به دفع الأفراد بدافع جرمي أو بدافع مرضي إلي إنهاء حياتهم بنفسهم عمداً مهدرين بذلك حقهم في الحياة، مستغلين في ذلك ضعف الأشخاص واليأس والاضطرابات النفسية التي يعانون منها.

الفقرة الثانية : انتشار المساعدة على الانتحار عبر الإنترنت

نتيجة لانتشار شبكة الإنترنت ظهرت بعض الألعاب والصفحات التي تحرض المراهقين على إيذاء أنفسهم بزعم الحصول على راحة نفسية أو حتى التخلص من الحياة، وعادة ما تنتهي بنهايات مأساوية، ومن تلك الوقائع صفحة على الفيسبوك بعنوان "كاتينج"، تم القبض على القائم عليها وهو مواطن مصري، تبين أنه يستغل الاضطراب النفسي للمراهقين ويحرضهم على الانتحار بقطع أيديهم أو تشويه وجوههم بجروح خطيرة.

---

[1] – محمد على محمد ، المرجع السابق ،121

[2] – إسحاق إبراهيم منصور ، شرح قانون العقوبات الجزائري ، جنائي خاص في الجرائم ضد الأشخاص والأخلاق وامن الدولة ، ديوان المطبوعات الجامعية ، الجزائر ، طبعة 2 ، 1988 ، ص20

وفي هذا الشأن أعلن قطاع نظم الاتصالات وتكنولوجيا المعلومات، بمصر أن القضايا المضبوطة خلال شهر أكتوبر سنة 2018 تمثلت في 324 قضية مختلفة في مجال متابعة أنشطة الفكر المتطرف والأفكار المحرضة عبر شبكة الإنترنت، وتمكنت الأجهزة الأمنية من السيطرة على 15 متخصصا في المنشورات التحريضية. وفى مجال مكافحة الجرائم الجنائية أعلنت الأجهزة الأمنية، أنه لوحظ أن بعض الفتيات المراهقات في محافظة الإسكندرية وبعض الأشخاص الذين يزورون أحد مراكز الشباب في نفس المحافظة أقدموا على إصابة أيديهم بشفرات حادة وقد أدت بحياة بعضهم. تقليداً لبعض الفيديوهات والصور الموجودة على موقع يوتيوب على الإنترنت العالمي والتي تدفع الأشخاص إلى الانتحار عن طريق (قطع الأوردة، والطعن)، مأخوذة من بعض أفلام الرعب الأجنبية. وتفاعلهم مع موقع التواصل الاجتماعي (فيسبوك) المسمى "التقطيع" الذي أنشأه أحد الطلاب في مصر. وتبين أن الموقع ساعد في نشر سلسلة صور لأيادي بعض الأشخاص وهم يتعرضون لإصابات في أيديهم وشفاههم بسكاكين حادة، لأنهم يعتقدون أن ذلك سيخفف الضغط عليهم لأنهم يعانون من مشاكل نفسية وصراعات أسرية، وقد تم القبض على مؤسس اللعبة والمحرض على الانتحار[1].

وصفحة كايتج ليست الوحيدة في هذا المجال بل سبقها العديد من ألعاب الموت عبر العالم، ومن أشهرها لعبة راح ضحيتها الكثير من المراهقين من كل أنحاء العالم من بينهم الجزائر وهي لعبة الحوت الأزرق التي ظهرت سنة 2016 .

وعليه أصبح التحريض على الانتحار لعبة يقوم بها عدمي الضمير والمجرمين، هذه الشريحة من الذئاب البشرية التي لا تستطيع العيش بدون توجيه الأذى للغير بأي وسلة كانت.

المبحث الرابع: الاعتداء على حرمة الحياة الخاصة

بالرغم من الحماية المسبقة من الدخول الغير مشروع لنظام المعلومات والبيانات الموجودة ضمن منظومة شبكة الإنترنت بما فيها البيانات الخاصة بالأفراد، إلا أن مجرمي الإنترنت وجدوا سبيل الدخول إليها وانتهاكها والاعتداء عليها بجميع الطرق.

[1] – الطريق إلى الموت بضغط زر، الموقع أطلع عليه في 2019/02/7، http://www.youm7.com

بتواجد الكم الهائل من البيانات والمعلومات الشخصية المتعلقة بحياة الناس ضمن شبكات الاتصالات المفتوحة، ومع سعة التخزين الضخمة لأجهزة الحاسب الآلي والسعة اللامتناهية لشبكة الربط المعلوماتي العالمي "الإنترنت "، ومع قدرة العقل البشري على اختراق نظم الاتصالات بطريقة أو أخرى للوصول إلى مكان وجود البيانات والمعلومات الخاصة بالحياة الخصوصية للأفراد، أصبحت هذه الأخيرة عرضة لمخاطر السلوك الإجرامي الذي يستهدفها بأشكال وصور مختلفة .

وهذا ما سندرسه من خلال هذا المبحث الذي قسمناه إلى ثلاث مطالب، تناولنا في الأول مفهوم الحق في الخصوصية عبر الإنترنت، ثم يأتي تصنيف الجرائم ضد الحق في الخصوصية عبر الإنترنت في المطلب الثاني، وبعده أركان الجريمة في المطلب الثالث.

المطلب الأول: مفهوم الحق في الخصوصية عبر الإنترنت

حق احترم خصوصية وسرية الأفراد من أي تدخل مهما كان نوعه حق كفله القانون. والهدف من هذه الحماية هي صيانة كرامة الإنسان واحترام آدميته. ومع انتشار استخدام شبكة الإنترنت صار هذا الحق أكثر عرضة للخطر من أي وقت مضى، خاصة مع تطور أساليب جديدة من خلال نظم المعلومات لارتكاب جريمة الاعتداء عبر شبكة الإنترنت على الحق في الحياة الخاصة.

تعتبر الدراسات القانونية المتعلقة بالخصوصية وحقوق الإنسان محدودة بشكل عام في ظل التقدم التكنولوجي، ويمكن القول أن مثل هذه الدراسات قد بدأت في أواخر الستينيات وأوائل السبعينيات، هذه هي الفترة التي تمت فيها مناقشة مفهوم خصوصية المعلومات لأول مرة، وأصبحت خصوصية المعلومات مفهومًا مستقلاً عن مفاهيم الخصوصية الأخرى.

ومصطلح الحق في الحياة الخاصة هو المصطلح الأكثر استعمالا للتعبير على هذا الحق في وقتنا الحالي بالرغم من وجود مصطلح أخر أقل شيوعا هو مصطلح الحق في الخصوصية.[1]

[1]–FRANCOIS RIGAUX, L'élaboration d'un « Right of Privacy » par la jurisprudence Américaine, Revue international de droit compare, Vol 32, N°4, October –December 1980 P 727

الفرع الأول: تعريف الحق في الخصوصية

أولا: تعريف الخصوصية لغة

خُصُوصيَّة مصدر خَصَّ، هذا الموضوع له خصوصيّة : له أهميَّة تميِّزه عن غيـــره. وهو ما يتعلّق بشخص بمفرده أو بمجموعة أو بأشياء محدّدة بدون سواها، مثلا سيارة خصوصيّة.[1]

ثانيا : تعريف الحق في الخصوصية من الناحية القانونية

لم يتفق الفقهاء أو رجال القانون على تعريف كامل وشامل للحق في الحياة الخاصة، نظرا لاختلاف المجتمعات والمعتقدات، وبالرغم من تعدد التعريفات على مستوى الفقه أو التشريع كلا يعرفها نسبة للمعيار الذي يراه مناسبا في منظوره. ففي مؤتمر رجال القانون المعتمد في العاصمة ستكهولم عام 67 قد عرف الحق في الخصوصية بناء على تعدد العناصر والصور التي تدخل في هذا الحق، وتم تعريفه على أنه" حق الشخص في أن يعيش بدون التدخل في حياته الأسرية والمنزلية، وفي كيانه العقلي أو البدني وأيضا حريته الأخلاقية أو العقلية وعدم الاعتداء على شرفه وسمعته، وجعله تحت الأضواء الكاذبة، وكذلك إذاعة حياته الخاصة واستعمال اسمه أو صوره، وبدون التجسس والتلصص عليه، والتدخل في مراسلاته، وسوء استخدام وسائل الاتصال الخاصة المكتوبة أو الشفوية، وإفشاء المعلومات المحصلة بحكم الثقة والمهنة."[2]

أما في ما يخص التشريعات العربية فقد عرف مؤتمر الإسكندرية الخاص بحرمة الحياة الخاصة :" بأنها حق الشخص في احترام كل ما تعلق بحرياته أو يعتبر من خصوصياته، مهما كان نوعها مادية كانت أو معنوية، على أن يتحدد ذلك بحسب المعيار الشخص العادي وفقا للقانون القائم في المجتمع وعاداته وتقاليده ووفقا لمبادئ الشريعة الإسلامية". [3]

---

[1]– احمد مختار عمر، معجم اللغة العربية المعاصرة ، عالم الكتب ، القاهرة ، مجلد 1، طبعة 1 ، 2008

[2] – محمد بشير الشافعي ، قانون حقوق الإنسان . مصادره وتطبيقاته الوطنية الدولية ، منشاة المعارف ، الإسكندرية ، ط، سنة 2007 ، ص 157

[3] – المادة الأولى من التوصيات الصادرة عن مؤتمر الحق في الحياة الخاصة المنعقد في الإسكندرية في الفترة من 4، 6 جويلية 1987

أما في ما يخص التشريع الجزائري فلم يتضمن تعريفا لهذا الحق بل اكتفى بحمايته من خلال المادة 29 من ق ع ج مع عده لبعض صور الحياة الخاصة كسرية المراسلات والاتصالات الخاصة بكل أنواعها وحرمة الشرف.[1]

وعليه يمكن تعريف الحق في الخصوصية على أنه الحق في عدم التدخـــــل في الحياة الشخصية للأفراد والشؤون الخاصة بهم وبعائلاتهم وهذا بأي وسيلة كانت.

وفي ضوء التطورات التقنية أصبحت الإنترنت قادرة على إيصال جميع البيانات والمعلومات الخاصة بالأفراد في شبكة واحدة تتداول وتعالج وتجمع وتفكك البيانات فيها بكل سهولة وسلاسة، وتستغرق هذه العمليات ثوانٍ للانتقال من بلد إلى آخر، ومن منظمة إلى أخرى، ومن مؤسسة عمل إلى أخري، ومن شخص إلى آخر، وباستخدام كل اللغات. لذلك قد أصبح الحق في خصوصية المعلومات معرّضا أكثر من ذي قبل للانتهاك من خلال مختلف المواقع الموجودة عبر الإنترنت، كمواقع الدردشة أو مواقع التواصل، التي صارت مودة هذا العصر وفضاء إلكترونيا واسعا، يقوم من خلاله الأشخاص بوضع كل المعلومات عن أنفسهم وحياتهم، وأيضا خصوصيتهم.

ولقد عرفت الخصوصية في المعلومات بأنها" قدرة الأفراد على التحكم بدورة المعلومات التي تتعلق بهم."[2]

ففي الحق في الحياة الخاصة عبر شبكة الإنترنت يمكن للمستخدم أن يقرر متى وكيف يمكنه الوصول إلى المستخدمين الآخرين وكذلك التعبير عن رأيه، وتشير الخصوصية عبر الإنترنت إلى ضرورة احترام خصوصية المستخدمين الذين يتصفحون تلك المواقع، سواء كانت تلك الخصوصية تتعلق بالحقائق أو المعلومات الموجودة على جهاز كمبيوتر الشخصي أو هاتف ذكي. أو حفظها من قبل مستخدمي وسائل التواصل الاجتماعي. واختراقها عن طريق الفيسبوك أو ما شابه، وسرقتها أو الاستيلاء عليها يعد انتهاكاً

[1] – المادة 29 من قانون العقوبات الجزائري

[2] – بوليين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، منشورات الحلبي الحقوقية، بيروت، 2009 ،ص 56

للخصوصية، وكذلك التجسس الإلكتروني وإفشاء الأسرار المرتبطة برسائل البريد الإلكتروني[1].

ومن هذا المنطلق فإنه وإن كانت البيانات الشخصية للفرد غالبا ما يقدمها الشخص بنفسه عبر خدمات الإنترنت، فإن تهديد الحرية الشخصية يقوم إذا تم إفشاء هذه البيانات دون إذن المعني ودون علمه أو إذا تم نشرها بطريقة خاطئة، وعليه فإن جمع المعلومات لا يعني أننا انتقلنا من السرية إلى النشر، كما أن الموافقة على الجمع والتخزين لا تعني حرية نقل تبادل المعلومات مع الجميع. خصوصا بعد انتشار مختلف التعاملات عبر الشبكة العنكبوتية مثل ما يسمى بالتجارة الإلكترونية، أين يمكن الآن إجراء التبادلات التجارية بما في ذلك البيع والشراء وإبرام العقود عبر الإنترنت، وطلبات الحصول على معلومات شخصية معينة تمكن من التعرف على الأفراد بشكل أفضل[2]. ويتم استخدام هذه البيانات لتحديد أرقام بطاقات الائتمان لإتمام عمليات الشراء، مما يجعل هذه البيانات الشخصية أكثر عرضة للاختراق أو الاحتيال أو السرقة من خلال ثغرات غير آمنة في الإنترنت. ومع ظهور التجارة الإلكترونية على شبكة الإنترنت، ظهرت هذه الدعوة لحماية المعلومات الشخصية، خاصة عندما يتم جمعها من خلال استخدام أساليب احتيالية ومخفية مثل تقنية الكوكيز وهي وسيلة للتعقب، ويمكنه تتبع الآثار التي يتركها المستخدم أثناء تصفح الإنترنت باستخدام ملفات نصية يتم إرسالها إلى القرص الصلب للخوادم المتصلة به على الإنترنت، ومن هناك يسمح للصفحات التي يزورها الحصول على معلومات شخصية.[3]

الفرع الثاني : الإنترنت وأثرها السلبي على الحق في خصوصية الأفراد

يشهد العصر الحديث تغلغلا مستمراً وتطورا كبيرا في الهجمات على المعلومات الشخصية لمستخدميه. ونظرًا لانتهاك خصوصية الأشخاص الذي أحدثته الثورة الرقمية في

---

[1]. تومي فضيلة ، إيديولوجيا الشبكات الاجتماعية وخصوصية المستخدم بين الانتهاك والاختراق ، مجلة العلوم الإنسانية والاجتماعية ، جامعة قصدي مرباح ، الجزائر ، العدد 30 ، سبتمبر 2017 ص 22

[2] – بوليين أنطونيوس، المرجع السابق، ص120

[3] – عبد الفتاح بيومي حجازي ، ، مكافحة جرائم المصارف الإلكترونية، ورقة عمل ضمن ندوة المصارف الالكترونية، تحت إشراف الجمعية المصرية لقانون الانترنت، بتاريخ 13 ماي 2007 ، ص138

الفضاء الإلكتروني، يسمي البعض العصر الذي نعيش فيه عصر الكشف والتعري، والذي يكشف من خلاله المستخدمون عن معلوماتهم الشخصية، سواء طوعًا أو تحت الإكراه.

فاستخدام وسائل تقنية المعلومات وشبكة الإنترنت صارت من أهم الضروريات في الحياة اليومية ولا يمكن لأي مجتمع أن يعيش بدونها، مما يزيد من مخاطرها التي تهدد خصوصية الحياة الخاصة مع إمكانية اختراق تقنيات المعلومات وانتهاكها عبرها[1]، ونظرًا لأن بساطة جمع وتخزين المعلومات وزيادة كميتها التي تم إنشاؤها بواسطة تقنيات معلومات اليوم المعاصرة تحد من قدرة الناس على التحكم في خصوصياتهم لوفرتها، وفي العصر الذي غزت فيه التطبيقات ومواقع الويب كل مكان، بات من السهل الوصول إلى المعلومات الشخصية وإساءة استخدامها بشكل غير قانوني.[2] بالإضافة إلى ذلك تزداد المراقبة والملاحقة للأفراد عبر الإنترنت التي تعرض خصوصيتهم للخطر من خلال الوصول إلى المعلومات المخزنة. [3]

لقد أدى انتشار الانتقالات الرقمية والمعلومات الشخصية عبر الإنترنت إلى ظهور جرائم تنال من حرمة الحياة الخاصة كالتجسس الالكتروني أو انتحال الشخصية، أو نشر الأسرار المهمة، حيث هناك إمكانية كبيرة لجمع المعلومات وتحويلها للمعالجة الإلكترونية، فضلا على ما توفره الإلكترونيات من رقابة وتحكمًا محكمًا من الناحية المرئيَّة والمقروءَة. [4] وفي بيئة الإنترنت يتم استخدام العديد من الوسائل التكنولوجية لتتبع بيانات العملاء كاستخدام

---

[1] . sophiepaillard, Les risques des technologies nouvelles de linformation Le Gazette du palais, 1997, p771.

[2] – Fred H cate–privacy in the information age–The Brooking institution, 1997,p15

[3]– Jean Frayssinet, Atteintes aux droits de la personne resultant des Fichiersou des traitementsinformatiques, juris, classeur penal, Articles 226–16 a 226–24,fasc, 1991,p221.

[4]– أندره لوك ، معالجة المعلومات القانونية في القرن الحادي والعشرين وتحدياتها، الجامعة اللبنانية ، مركز الأبحاث والدراسات في المعلومات القانونية ، منشورات صادر ، بيروت ، 2002 ، ص284

محركات البحث، فيمكن لمزود الخدمة التعرف على جميع مستخدمي الويب من خلال الوصول إلى جميع المواقع التي يزورها مستخدم الويب وكذا منتديات المناقشة التي يشارك فيها، وباختراقه من طرف مجرمي الإنترنت يمكن التوصل لكافة المعلومات الموجودة به.

فقد تضاعفت جرائم الاعتداء على البيانات الشخصية بأشكال مختلفة نظرا لانتشار استخدام شبكة الإنترنت، مم يؤكد أهمية الموازنة بين أهمية وفائدة تقنيات المعلومات، وبين منع ما سيصيب الأفراد من أضرار في حرمتهم الخصوصية من استخدام هذه الوسائل.[1]

المطلب الثاني : تصنيف الجرائم ضد الحق في الخصوصية عبر الإنترنت

لقد خلق من خلال الإنترنت سلسلة من الاعتداءات على الخصوصية سنحاول إبراز أهمها من خلال ما يأتي:

الفرع الأول : البوصلة والتصيد الاحتيالي عبر مواقع التواصل الاجتماعي.

الفقرة الأولى: البوصلة التقنية المعروفة بالكوكيز

العديد من مواقع الويب عند زيارتها يتم وضع ملف صغير على القرص الصلب لجهاز الكمبيوتر الخاص بالمستخدم، والذي يتصل بخادم موقع الويب الذي تمت زيارته على الإنترنت، والذي يرسل بعد ذلك الملف إلى القرص الصلب لجهاز الكمبيوتر الخاص بالمستخدم. وفي حالة تصفح هذا الأخير لأي موقع عبر الإنترنت، يقوم تخزين نسخ من هذه المعلومات، وقد يتعرض المستخدمون أثناء تصفحهم الويب وجمع البيانات الخاصة بهم لانتهاك خصوصيتهم، فباستخدام الكوكيز يمكن معرفة عنوان الإنترنت "أي بي" والمواقع التي يتم تصفحها ونوعية الجهاز ونوعية المعالج بالإضافة إلى بيانات المستخدم الإلزامية مثل الاسم والعنوان ورقم بطاقة الائتمان والبريد الإلكتروني وما إلى ذلك[2].

---

[1]– .ممدوح عبد الحميد عبد المطلب ، جرائم استخدام شبكة المعلومات العالمية ، الجريمة عبر الإنترنيت ، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنيت ، بيروت ، 2000 ، ص21

[2]– عثمان بكر عثمان ، المسئولية عن الاعتداء على البيانات الشخصية عبر شبكات مواقع التوصل الاجتماعي ، كلية الحقوق ، جامعة طنطا ، ص 1

الفقرة الثانية : التصيد الاحتيالي عبر مواقع التواصل الاجتماعي.

التصيد الاحتيالي هو أسلوب يستخدمه المتسللون لجمع المعلومات الشخصية من مستخدمي الإنترنت. وهو وسيلة شائعة لاختراق فيسبوك. وتُستخدم عمليات التصيد الاحتيالي عبر البريد الإلكتروني الشخصي للحصول على الأموال بشكل احتيالي، إضافة الاستيلاء على معلومات سرية، يتم إرسالها عادةً عبر البريد الإلكتروني مثل كلمة المرور ورقم بطاقة الائتمان والعديد من المعلومات الأخرى. حيث يقوم المتسللين باستخدام مواقع الويب ورسائل البريد الإلكتروني المزيفة الخاصة بمواقع البنوك أو العلامات التجارية، والطلب من مستخدمي الإنترنت بتزويدهم ببيانات أو معلومات شخصية مثل تفاصيل بطاقة الائتمان أو الحساب البنكي، واستغلالها في سرقة حسابات مصرفية أو غيرهـــا من الأمور التي تتطلب التحقق من الهوية.[1]

الفرع الثاني: جريمة انتحال شخصية مالك البيانات واستخدام بيانات مستخدم جديد على مواقع عبر الإنترنتَ

الفقرة الأولى: جريمة انتحال شخصية مالك البيانات

تتحقق هذه الجريمة بتعمد الجاني الولوج إلى نظام المعلومات أو عبر المواقع المتعددة عبر الانترنت وبعد اصطياد الضحية، يتم الاطلاع على محتوى النظام بغية انتحال صفة مالك النظام أو الموقـــــع الالكتروني، وقد يتم أيضا انتحاله لشخصيته والتعامل باسمه وهويته، من اجل تحقيق أهداف معينة.[2] وبمعني أخر تعتبر جريمة انتحال الشخصية أو سرقة هوية الشخص من جرائم الإنترنت التي تلعب برامج البيانات والمعلومات الحاسوبية دوراً أساسية فيها. وهو الفعل الذي يستخدم التكنولوجيا الإلكترونية بشكل مباشر أو غير مباشر كأدوات للجريمة المتمثلة في انتحال الشخصية، أي يعتمد الجاني على استغلال شخص آخر للاستفادة من سمعته أو ماله أو سلطته أو القيام بجميع المعاملات باسمه أو

[1] . محمد عبد الله المؤيد ، صور المسئولية التقصيرية الناشئة عن الاعتداء على بيانات الكمبيوتر والتعامل عبر الإنترنت وتسوية منازعاتها ، مجلة الدراسات الاجتماعية ، العدد الثامن والعشرون ، جانفي ، 712 ص، 20

[2] – أسامة احمد المناعسة وجلال محمد الزعبي، جرائم تقنية نظم المعلومات الالكترونية ، المرجع السابق ، ص 259

نيابة عنه أو لتشويه سمعته[1]. بالإضافة إلى العديد من الجرائم الأخرى التي ترتكب بسبب خصوصية المعلومات والبيانات المتعلقة بالأفراد.

الفقرة الثانية :استخدام البيانات الخاصة بمستخدم جديد على المواقع الموجودة عبر الإنترنتَ

يعانى مستخدمي المواقع المختلفة عبر الإنترنت من مجموعة المخاطر المرتبطة بإرسال طلبات التسجيل على وسائل التواصل الاجتماعي.

فمن المعروف، عندما يستخدم المستخدم شبكات التواصل الاجتماعي، فإنه يقدم طوعًا بعض المعلومات أو البيانات الشخصية من أجل الوصول لهذه الشبكات، حيث تشترط مواقع التواصل الاجتماعي على مستخدميها الإدلاء بمعلومات معينة تتعلق بحياته الشخصية، مثل الاسم وعنوان البريد الإلكتروني والجنس، وتاريخ الميلاد بالإضافة إلى معلومات شخصية أخرى متعلقة بالعمل من أجل العثور على الأصدقاء، ويُطلب من كل مستخدم أيضًا إكمال ملفه الشخصي من خلال تقديم المزيد من البيانات الخاصة مثل المعتقدات الدينية أو السياسية.[2] كل هذا يشكل العديد من المخاطر، مثل اختراق الحسابات، مشاركة الصور المحرجة، وصعوبة حذف أو إلغاء الحسابات إذا لم تكن المعلومات محمية بشكل كاف من خلال الإعدادات ويصبح الوصول إليها متاحا واستخدامها لأغراض غير مرغوب فيها وغير قانونية ممكنا، فالسمعة الرقمية تعتمد إلى حد

[1] – خالد محمد مصطفى ، المسئولية الجنائية لناشري الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل الاجتماعي ، مجلة رؤى استراتيجية ، مارس 2013

[2] –CORALIE DUMAS , LE DROIT DE LA PERSONNALITE ET LES RESEAUX SOCIAUX , MEMOIRE , FACULTE DE DROIT , UNIVERSITE DE MONTPELLIER , 2015 , P.14

أساسي على المستخدم لأنه هو الذي يقوم بنشر المحتوى والصور الخاصة به.[1]

ويعتبر الحق في الصورة من الجوانب الشخصية للأفراد التي تتمتع بالحماية، فيجوز له الاعتراض على نشر أو عرض أو استعمال صورته بأي طريقة من الطرق. ولا يشترط في هذا الجانب أن يقع ضرر على صاحب الصورة ليعد انتهاكا للخصوصية، أما في حالة وقوع ضرر فانه على الجاني تعويض الضحية على مدي الضرر وأثاره، ولا يحتاج الضحية أو أي شخص نشرت صورته بدون إذنه أو رضاه إلي إثبات سوء النية طالما تم نشر صورته.[2]

المطلب الثالث : أركان جريمة الاعتداء على الخصوصية

لتحقق جرائم الاعتداء على الخصوصية عبر الإنترنت ينبغي توافر جميع الأركان الأساسية المجتمعة حتى تقوم الجريمة وهي ثلاثة أركان.

الفرع الأول: الركن القانوني لجريمة الاعتداء على الخصوصية عبر الإنترنت

وكما ذكرناه سابقا يقصد بهذا الركن تجريم الفعل والمعاقبة عليه بموجب نص قانوني. ولمحاربة الإجرام الالكتروني استحدث المشرع الجزائري قانونا خاصا يهدف من خلاله محاربة الاعتداءات ضد المعلوماتية، حسب القانون رقم 15/04 المتضمن تعديل قانون العقوبات، وقد نصت المادة 303 مكرر من قانون العقوبات المعـــــدل بالقانـــــون رقم 06-23 المؤرخ في 2006 /12/20 على معاقبة كل من قام بالمساس بحرمة الحيـــاة الخاصة عمدا، مستخدما أي تقنية كانت بالحبس من 6 أشهر إلى 3 سنوات.[3]

---

[1] –Clemence Dani, Laura Garino, M. Gianni Giordano, Elisa Sicard , Reseaux Sociaux Et Protection Des Donnees Personnelles, Rapport Realise Sous La Direction De M. Le Professeur Jean Frayssinet Et M. Le Professeur Philippe Mouron, Universite De Aix Marseille , Faculte De Droit , 2014, Op,Cit , P.2

[2]– حنان ريحان مبارك المضحكي، الجرائم المعلوماتية ، المرجع السابق ، ص 327

[3] – القانون رقم 06-23 المؤرخ في 2006/12/20/ يتضمن تعديل قانون العقوبات الجزائري عدد84

الفرع الثاني : الركن المادي لجريمة الاعتداء على الخصوصية عبر الإنترنت

يتحقق الركن المادي لجريمة الاعتداء على الخصوصية عبر الإنترنت بمجرد القيام بالنشاط وبغض النظر عن تحقق النتيجة، فيكفي أن يقوم الجاني بفعل التصنت أو الاعتراض بغرض الاطلاع أو المشاهدة أو الحصول عليها بأي طريقة غير مشروعة.

الفرع الثالث : الركن المعنوي لجريمة الاعتداء على الخصوصية عبر الإنترنت

تعتبر جريمة التعدي على خصوصية الأفراد غبر الإنترنت من الجرائم العمدية التي تشترط توافر القصد الجنائي وهو اتجاه إرادة الفاعل إلى الاطلاع وجمع وتخزين المعلومات والبيانات الموجودة عبر الإنترنت من أجل تحقيق مصلحة معينة أو من أجل استخدامها لغير غرضها.[1]

ومما لا شك فيه أن انتشار الجرائم الماسة بالخصوصية التي يواجهها كثير من الناس بشكل متزايد سببه عدم الحيطة والحذر، لذلك ينبغي على متصفحي الإنترنت توخي الحذر عند الكشف عن معلوماتهم وبياناتهم الشخصية على مواقع الويب. فتدفق البيانات الشخصية للمستخدمين يمثل خطرا على هؤلاء الأشخاص مم يجعلهم عرضة لاستغلال بياناتهم.[2] وعليه يجب أن تأخذ أنظمة حماية المعلومات الشخصية عبر الإنترنت بعين الاعتبار طبيعة المخاطر التي قد يواجهها مستخدمي الإنترنت عند تصفحهم لها.

الفصل الثاني

العدوان الإجرامي عبر الإنترنت الماس بالذمة المالية

إن تطور آليات الاتصال وظهور المواقع الاليكترونية والإنترنت واستخدامها في جميع مجالات الحياة وزيادة مستخدميها بصفة مكثفة ساهم في ظهور عدة مفاهيم جديدة، خاصة في مجال التعاملات الالكترونية والذي جلب معه مفهوما حديثا للنقود والتي انتشرت مؤخرا بمصطلح النقود الإلكترونية، وهي موجودة بشكل شائع في أجهزة الصراف الآلي. ومع تطور هذه المفاهيم نمت وتطورت معها أشكال الجرائم ضدها، الأمر الذي ساعد زيادة

[1] – حنان ريحان مبارك المضحكي، الجرائم المعلوماتية ، المرجع السابق ، ص 335

[2]– Mallorie Wozny , Exploitation des données personnelles : raison commerciale, raison d'état et opportunités , mémoire , université de lyon , faculté de droit , 2017 , p.23

ارتقاء مستوى السرقة من سرقات تتم بالطرق التقليدية إلى سرقات تتم عبر الإنترنت وتستهدف المعلومات وقيمتها الاقتصادية كما ساهم في انتشار جرائم الاحتيال والنصب بصورة الكترونية، وذلك لسهولة الاعتداء عليها كونها تنصب على المعلومات باستخدام الحاسب الآلي وشبكة الإنترنت. لذلك اتجه القضاء إلى إثبات مدي شرعية وصف الجرائم التقليدية الواقعة على الأموال ذات الطابع المادي الملموس على القيم غير الملموسة التي أوجدتها تكنولوجيا المعلومات والإنترنت، خاصة وأن القانون الجزائري لم يكن على دراية بمفهوم الأموال الإلكترونية عند سنه لنصوصه التقليدية المتعلقة بجرائم الأموال وكانت الأشكال الرئيسية للهجمات على الأموال عبر الإنترنت تستند إلى جريمة السرقة التي تستهدف بطاقات الائتمان، وجريمة الاحتيال عن طريق بطاقات الدفع الالكتروني والاحتيال التجاري الالكتروني، إضافة إلي هذه الجرائم جريمـة المتاجرة بالمخدرات والمؤثرات العقلية عبر الإنترنت، وجريمة الاعتداء على الملكية الفكرية التي تندرج ضمن الجرائم المالية التي تتم عبر الإنترنت. ومن خلال هذا الفصل سنتناول جرائم الإنترنت الواقعة على الذمة المالية على النحو التالي:

المبحث الأول: جريمة السرقة عبر الإنترنت

المبحث الثاني: جريمة الاحتيال عبر الإنترنت

المبحث الثالث: جريمــة الاتجار بالمخدرات عبر الإنترنت

المبحث الرابع : جريمة الاعتداء على الملكية الفكرية

المبحث الأول: جريمة السرقة عبر الإنترنت

أصبحت الجرائم التقليدية تعتمد بشكل متزايد على التكنولوجيا الحديثة وباتت التكنولوجيا أساسا لكل جريمة خطيرة خاصة في ظل التطور والاستخدام الهائل لشبكة الانترنت، فمع هذا الاستخدام ظهرت جريمة السرقة المرتكبة عبر الانترنت سواء كانت متمثلة في سرقة بيانات شخصية وخاصة أو أرصدة بنكية أو حتى معلومات هامة، فلا فرد أو جماعة أو حتى دولة بمأمن من اللصوص الالكترونيين.

تعد شبكة الإنترنت أرض خصبة لارتكاب سرقة المعلومات الشخصية أو الأموال، وتعد شبكات التواصل الاجتماعي والبريد الالكتروني هي السبل الأكثر استخداما لارتكاب السرقة أين أصبح الحصول والحفاظ على المعلومات الشخصية من خلال خدمات الإنترنت أمر في غاية السهولة خاصة من طرف المخترقين والمتسللين. ولقد شهد العالم في السنوات الأخيرة تضاعفا في الهجمات المستهدفة لأموال الغير باستخدام الإنترنت، خاصة مع اعتماد المصارف والخدمات الإلكترونية، إذ يواجه عدد من كبرى المصارف العالمية عملية قرصنة وتسلل واسعة تنفذ كل يوم انطلاقا من آلاف الكمبيوترات المقرصنة في العديد من بلدان العالم. وسندرس في هذا المبحث جريمة السرقة عبر الإنترنت من خلال عرض مفهومها ومختلف صورها وأهم أركانها.

المطلب الأول: مفهوم جريمة السرقة عبر الإنترنت

السرقة المتعلقة بالإنترنت هي شكل من أشكال الجرائم المعلوماتية المتمثلة في الاستغلال الغير مشروع للإنترنت من طرف مستخدمي الشبكة، بحيث يقوم الجاني بأساليب ووسائل منظمة ومخطط لها باستخدام بعض المعلومات الإلكترونية أو التواصل مع بعض الأشخاص بهدف سرقتهم. وقبل التعرض لتعريف السرقة باستخدام الإنترنت بصفة مفصلة نتجه لتعريف السرقة بصفة عامة.

الفرع الأول: تعريف السرقة

قبل تناول التعريف الفقهي والقانوني للسرقة سنتناول أولا تعريف السرقة من الناحية اللغوية.

الفقرة الأولى تعريف السرقة من الناحية اللغوية

سَرَقَ منه الشيءَ يَسْرِقُ سَرَقاً وسَرِقاً وسَرَقَةً وسَرِقَةً وسَرْقاً واسْتَرَقَ هجاءَ مُسْتتِراً إلى
حِرْزٍ، فأَخَذَ مالاً لِغَيْرِه، وهي اخذ الشيء من الغير بطريقة خفية ومنها استرق السمع أي سمع متخفيا.[1]

[1]– ابن منظور، لسان العرب ، المرجع السابق ، مادة سرق

الفقرة الثانية :تعريف السرقة من الناحية الفقهية والقانونية

ذهبت الباحثة "مابل إليوت" إلى تعريف السرقة بأنها فعل يعبر عن مصلحة أشخاص يسعون فقط إلى إشباع رغباتهم الخاصة، والسرقة تعد خطر موجه ضد قيم الأمانة وحرمة ممتلكات الأفراد الخاصة.[1]

أما من الناحية القانونية قد عرفها المشرع الجزائري، من خلال نص المادة 350 ق ع بقوله " كل من اختلس شيئا مملوكا للغير يعد سارقا. فالسرقة إذا هي: اختلاس مال منقول مملوك للغير بنية التملك "[2].

الفرع الثاني : تعريف السرقة عبر الإنترنت

السرقة تبعا للقواعد العامة هي الاستيلاء على مال الغير المنقول خفية بغرض التملك أما جريمة السرقة عبر الإنترنت هو أي إجراء من شأنه الاستيلاء على البرامج أو المعلومات أو الحسابات المصرفية المملوكة للغير بواسطة الحاسوب أو أي جهاز يمكنه الارتباط بشبكة الإنترنت وذلك عن طريق إرسال برنامج يحمل فيروسات تقوم بنسخ البرامج والمعلومات والحصول عليها[3]، أو من خلال عمليات القرصنة الالكترونية التي يستغل فيها المجرمون شبكة الإنترنت للقيام باستخدام نقود الغير على نحو غير مرخص وذلك عن طريق سرقة الهوية والتصيد من خلال ما يعرف بعملية سرقة الحسابات[4]. وعادة ما يتعرض المستفيدون من الخدمات المصرفية أو الدفعات عبر شبكة الإنترنت لسرقة

---

[1]– إبراهيم أبو الغار، سرقة المساكن في المناطق الحضرية بمدينة القاهرة، المجلة الجنائية القومية، العدد الأول، المجلد12 ، القاهرة، 1978، ص6

[2] – حسين فريحة، شرح قانون العقوبات الجزائري، جرائم الاعتداء على الأشخاص والأموال، المرجع السابق، ص111

[3]–Peter Grabosky–Russell Smith–Gillian Dempsey – Electronic Theft Unlawful ac– quisition in Cyberspace . Cambridge University–2001– p45

[4] – سرقة الحسابات هي "دخول غير مرخص به استعمار غير مشروع لحسابات موجودة من خلال التصيد والاختراق "Hacking"

– Mark A. Fox Internet Banking ,E money And The internet Gift economy , First Monday , December 2005 , p 3

حساباتهم عن طريق الاختراق، أين يتلقى الضحية رسائل تصيد، الغرض منها الاستيلاء على حسابه المالي.[1]ويتم ذلك باستخدام المتسللون لرسائل الكترونية احتيالية ومواقع عبر الإنترنت لإغراء المستهلكين ودفعهم إلى إظهار معلوماتهم المالية والشخصية الخاصة بهم، وعن طريق موقع مخادع يبين الرسائل الالكترونية أنها رسائل مرسلة من المؤسسة المالية المتعامل معها، أين يطلب من الضحايا معلومات سرية تتعلق بحسابهم المالي كأرقام بطاقات الدفع أو الائتمان، الاسم واللقب، الكلمة السرية، مبلغ النقود الالكترونية ...الخ، أين تستخدم هذه المعلومات من طرف المتسللون للاستيلاء والحصول على المال المملوك للغير بطريقة تبدوا لهم في غاية السهولة .[2] أيضا يمكن إنشاء صفحة إنترنت مماثلة جدا لموقع بنك أو مؤسسة مالية، ومطالبة العملاء بإدخال البيانات أو تحديثها للحصول على البيانات المصرفية وسرقتها. إضافة إلى استخدام البريد الالكتروني ورسائله التي تأتي من مصادر مجهولة لطلب المشاركة في إطلاق الأموال من الخارج عن طريق الوعد بنسبة معينة من المبلغ، أو الرسائل التي تستهدف مستخدم البريد الإلكتروني وتوهمه بالفوز بجوائز معينة وتحثه على إرسال رقم حسابه الخاص، كلها طرق الهدف منها الحصول على المعلومات السرية بغية السرقة.

وفي هذا الشأن تعرض مستخدمو موقع " إيباي" عبر العالم سنة 214 إلي السرقة عبر الإنترنت، وتم اختراق وسرقة معلوماتهم الشخصية، وكان 30 مليونا منهم عملاء من منطقة الشرق الأوسط. وتعتبر المؤسسات المالية هي الأكثر عرضة للقرصنة الإلكترونية، وبسبب الاختراق يخسر العالم 1 تريليون دولار كل عام، ولقد تعرضت 30% من الشركات المالية على مستوى العالم للقرصنة السيبرانية، إضافة إلى تعرض 17% من الشركات غير المالية لنفس الاختراقات.[3]

[1] –Mark A. Fox Internet op cit ,p3

[2]– Mark A. Fox Internet, p 4

[3] – الاقتصاد والناس برنامج تلفزيوني بعنوان ،السرقة على الانترنت ، السبت بتاريخ 2014،/5/31على قناة الجزيرة العربية

المطلب الثاني: صور السرقة عبر الإنترنت

جاء في تقرير صدر عام 2014 أن السرقة عبر الإنترنت زادت بنسبة 12٪ في سنة 2014 واستمرت في الارتفاع، لكن أبرز ما جاء في هذا التقرير أنه تم الكشف عن خمس طرق للاعتداء على الأموال من خلالها يمكن للقراصنة ومجرمي الإنترنت سرقة أموال الضحايا. ويكشف هذا التقرير الذي نشرته جمعية تجار التجزئة البريطانيين أن العديد من طرق التسوق والدفع التي تعتبر آمنة توفر فرصا سهلة للمحتالين لمهاجمة البنوك وأخذ الأموال منها، مما يعني أن كل دافع للنقود من خلال وسائل الدفع الالكترونية قد يصبح ضحية للسارقين والمخادعين.

ويشير التقرير إلى أن الارتفاع الكبير في حجم التجارة الإلكترونية يرافقه زيادة مستمرة في جرائم السرقة. وبأن ما يقارب 72٪ من تجار التجزئة لا يتخذون الإجراءات المهمة واللازمة حماية بيانات عملائهم، ويعتمد أغلبهم على برامج لمحاربة الفيروسات القديمة والحماية القديمة، والتي تعد حماية غير كافية بطريقة دائمة، لأن السارقون والمخترقون في بحث مستمر عن طرق جديدة للنفاذ من هذه الوسائل.[1] وسوف نتطرق إلى أكثر الطرق التي يستغلها الهاكرز للاستيلاء على الأموال.

الفرع الأول : اختراق بطاقات الائتمان

توجد ثغرة أمنية تتيح اختراق بطاقات الائتمان[2]، ويستطيع المتسللون الحصول على معلومات سرية وحساسة في ثوانٍ معدودة. وتتمثل نقطة الضعف في أنظمة الدفع الالكتروني باستخدام الإنترنت في أنه لا يمكنها اكتشاف الطلبات المزيفة للدفع من مواقع الويب المختلفة، كذلك طلب يسهل على مجرمي الإنترنت سرقة البيانات وتجميعها إذا تم طلبها من طرف مواقع متعددة، ويستطيع المتسللون تخمين كافة تفاصيل بطاقات فيزا

---

[1]– se protéger de 5 piratages de données parmi les plus répandus,Frederic BERGÉ,https://bfmbusiness.bfmtv.com/hightech/comment-se-proteger-de-5-piratages-de-donnees-parmi-les-plus-repandus-1241613.html

[2] – بطاقة الائتمان بالإنجليزيّة " بطاقة خاصة يصدرها المصرف لعميله ،تمكنه من الحصول على السلع والخدمات من محلات و أماكن معين عند تقديمه لهذه البطاقة ويقوم بائع السلع أو الخدمات بتقديم الفاتورة الموقعة من العميل إلى المصرف (مصدر البطاقة) فيسدد قيمتها له .

وماستركارد إذا كانوا يمتلكون أول 6 أرقام من البطاقة، وعادةً ما تحتوي البطاقة الأولى على 16 رقمًا. وتعرض الأرقام الأولى معلومات حول البنك ونوع البطاقة المشتركة بين جميع البطاقات الصادرة عن نفس البنك ويستخدم المتسللون تقنية تسمى "هجوم التخمين الموزع"، هذا النظام مصمم لمنع اتخاذ الإجراءات الأمنية ضد العمليات الاحتيالية، ويعمل النظام من خلال جمع الكثير من المعلومات من مواقع الويب المختلفة، مثل عنوان حامل البطاقة والرمز البريدي وتاريخ انتهاء البطاقة. والنتيجة هي رمز CVV مكون من ثلاثة أرقام، والذي يعتبر خطوة التحقق النهائية عند استخدام البطاقة لعمليات الشراء عبر الإنترنت وتاريخ الانتهاء لا يزيد تخمينه عن ستين محاولة. ويستغرق الأمر أقل من ألف محاولة لاكتشاف رمز التحقق من البطاقة، والسبب الرئيسي هو الكشف عن معلومات البطاقة المخفية بسبب تكرار بعض تفاصيل البطاقة في نظام الدفع الإلكتروني الخاص بالموقع.[1]

الفرع الثاني : اختراق نقاط البيع

يرى خبراء الإنترنت أن الأنظمة والأجهزة عند استخدامها في نقاط البيع، يمكن أن تصبح أداة أو مصدرًا للقرصنة والسرقة، إذ يقوم الكثير باستهداف واختراق مواقع الشراء والبيع للمنتجات على الإنترنت، والكثير من هذه المواقع تقوم بتخزين معلومات خاصة بعملائها في قاعدة البيانات الخاصة بهم دون حمايتها مثل بطاقات الائتمان ثم تقوم بأخذهم ودخول إلى بطاقتهم .

وفي حال سرقة الرقم السري للبطاقات فإنه من الصعب جدًا على الشركات وتجار التجزئة معرفة أن البطاقة قد سُرقت، والمستخدم ما هو إلا محتال يجري عملية شراء من

[1]–IEEE Security and Privacy Magazine Journal uri icon. Overview; Identity; View All ... Computer Security Education and Research in Australia . 60–63. 2016

الحساب البنكي المملوك للغير، خاصة في الحالات التي يتم استخدامها من أجل الشراء عبر الإنترنت.[1]

الفرع الثالث: المواقع المزورة واستعمال طريقة Phishing أو سبام

الفقرة الأولى :المواقع المزورة

تعد مواقع الويب االمزيفة أسلوبًا مهمًا وشائعًا لسرقة الأموال عبر الإنترنت، والسبب أن المجرمين الذين يتبنون هذه الوسيلة لسهولتها في ارتكاب جرائمهم خاصة وأن هذا النوع من المجرمين يمتعون بدرجة عالية من الاحتراف والخبرة. وهي مشكلة قد يتعرض لها معظم الناس أثناء التسوق عبر الإنترنت. ووفقاً لهذه الطريقة، يقوم متسللي الإنترنت بإنشاء موقع ويب باسم معروف وبنفس الشكل، وعادة ما يتم إرسال الرابط إلى الضحية عبر البريد الإلكتروني، ويقوم بإدخال معلوماته، والتي تنتهي في المكان الخطأ بن أيدي السارقين. ومن أهم الأمثلة على مواقع قراصنة الإنترنت، المواقع التي تنتحل صفة البنك الالكتروني العالمي الذي يطلق عليه اسم "باي بال" ومواقع مثل «فيزا» أو «ماستر كارد»، التي تنتحل صفة مواقع عالمية أو لمواقع بنوك داخلية، حيث يتلقى المجني عليه بريدًا إلكترونيًا يطلب منه استخدام حسابه، ثم ينقر على الرابط ويحصل على عرض منتظم للصفحة حيث يقوم بإدخال تفاصيل معلوماته البنكية على الفور، أو البيانات الخاصة ببطاقته، لتصبح هذه المعلومات في حوزة الجاني لاستخدامها من أجل سرقة ما لديه من أموال.

الفقرة الثانية : السبام

السبام هو إرسال نفس الرسالة في معظم الأحيان لملايين الأفراد وإيهامهم بأنها رسالة هامة من البنك، وفي هذه الرسالة يطلب من الضحية إغلاق حسابه ما لم يفعله، وبعد ذلك يتم توجيه المجني عليه إلى صفحة مزورة تشبه كليا البنك الخاص ويطلب منه جميع تفاصيل بطاقته.[2]

---

[1]– Fraud Types, https://www.westernunion.com. et – How to Avoid Gift Card Scams,https://www.consumerreports.org/gift-cards/how-to-avoid-gift-card-scams/ vu le 24/12/2017

[2]– السبام: (Spam)يعرف على أنه بث أو إعلان أو إرسال رسائل بريد إلكتروني عن طريق الخدمات رسائل أو محتويات غير مطلوبة وغير ملتمسة، ويدخل ضمن ذلك المواد الإعلانية والترويجية، لبقية المستخدمين الذين يرفضون

الفرع الرابع : سرقة العملة الصعبة (البتكوين)

في الوقت الذي أصبحت فيه عملة «بيتكوين» [1] الأكثر انتشارا في الوقت الحالي، وأصبح تداولها على أوسع نطاق عبر الإنترنت، وتم الاعتراف بها كعملة افتراضية مقبولة من معظم الدول والسلطات، فقد تم تحويلها إلى أداة سطو ونهب أموال الضحايا، بالرغم أن غالبية الأشخاص يعتقدون أنهاالطريقة الأكثر أماناً للتداول والدفع عبر شبكة الإنترنت، غير أن تقنيو الأمن السبيراني يجزمون بأن سرقة البتكوين تحدث فقط عندما يتم تعرض الضحية لقرصنة يقوم من خلالها الجاني بانتهاك حاسوبه الشخصي وسرقة معلوماته، وبالتالي التحصل على أموال البتكوين الخاصة به.

ويرى جيمس لاين أحد الخبراء في شركة «سوفوز» أن الهاكرز باستطاعتهم فتح باب خلفي في حاسوب المجني عليه، عن طريق ملف اختراق يرسل عشوائيا لأي شخص مستهدف، وتتم حينها عملية تسلل وسرقة المعلومات المخزنة على جهاز الكمبيوتر، أو التجسس على المستخدم أثناء قيامه باستعمال الجهاز. وغالبا ما تفتقر أجهزة الحاسوب الخاصة بالأفراد للحماية مقارنة بالأجهزة التي يتم استخدامها في أنظمة الدفع المالية أو المصرفية. وهذا ما يجعل الأمور أسهل على المتسللين والمحتالين.[2]

يستطيع المتسللون سرقة آلاف وملايين الدولارات من خلال البنوك، وخداع موظفي البنوك للوصول إلى البريد الإلكتروني الخاص بالبنك أو عملائهم، والحصول على معلومات حساسة يمكنهم استخدامها ضدهم، وإرسال رسائل بريد إلكتروني إلى العملاء

أو لا يسمحون باستقبال مثل هذه الرسائل أو المحتويات. ، أنضر الموقع التالي الذي إطلع عليه في 2019/02/12: https://safeonline.najah.edu

[1]– البتكوين (Bitcoin):هي نظام دفع عالمي وعملة يمكن مقارنتها بالعملات الأخرى مثل الدولار أو اليورو، لكن مع فوارق أساسية، من أهمها أن هذه العملة هي عملة إلكترونية بشكل كامل تتداول عبر الإنترنت فقط من دون وجود ملموس لها. وهي أول عملة رقمية لامركزية ونظام يعمل دون مستودع أساسي أو مدير واحد، أي أنها تختلف عن العملات التقليدية بعدم وجود هيئة تنظيمية مركزية تقف خلفها.

[2]– FraudTypes, https://www.westernunion.com/us/en/fraudawareness/fraud-types.html. et – How to Avoid Gift Card Scams,https://www.consumerreports.org/gift-cards/how-to-avoid-gift-card-scams/ vu le 24/12/2019

نيابة عن بنوكهم، يزودهم بخادم بوت نت مشفر، الذي يقوم باختراق البنك كاملا لأن الخادم يحتوي على برنامج كشف يقوم في بعض الأحيان بسرقة معلومات غير مشفرة، مثل كلمات المرور وأرقام بطاقات الائتمان. أو في بعض الأحيان للحصول على عنوان الاتصال بالإنترنت إذا قام العميل بفتح حسابه، فسيتم إعلام الجاني الذي سيزود بجميع البيانات اللازمة ويكون الحساب تحت تصرفه[1].

المطلب الثالث : أركان السرقة عبر الإنترنت

إضافة إلى الركن الشرعي لابد من توافر الركن المادي والمعنوي لجريمة السرقة عبر الإنترنت.

الفرع الأول :الركن المادي للسرقة عبر الإنترنت

يشترط لقيام هذا الركن في جريمة السرقة عبر الإنترنت قيام الجاني بسلوك مادي وملموس لانتهاك نظام الحماية والاستيلاء على تلك المعلومات الموجودة في النظام الالكتروني[2]. ويعرف الركن المادي هنا بأنه " نزع الشيء من الضحية بغير علمه ورضاه ونقلها إلى حيازة الجاني، بمعنى أخر هي الحيازة الكاملة للشيء حيازة مادية ومعنوية، بدون رضاء المالك الأصلي أي حرمان صاحب الحيازة الشرعي منها"[3].

وتم تعريفه من طرف محكمه النقض المصرية بأنه " الاستيلاء على الشيء المسروق استيلاءا كليا أي نقل ملكية المالك الأصلي للشيء وجعله في حيازة السارق يتصرف فيه بحرية"[4]. ونسبة لما سبق ذكره يمكن تطبيق عقوبات جريمة السرقة التقليدية على جريمة السرقة المتعلقة بشبكة الإنترنت، لأن اختلاس الشيء المتمثل في المعلومات وتحويل الأموال يتحقق عن طريق النشاط المادي الذي يقوم به المجرمون الذين يستخدمون أجهزة

---

[1]- "برمجيات التشمم برنامج كمبيوتر يقوم بتحليل البيانات على شبكة اتصال لجمع المعلومات الاستخبارية ، مثل اكتشاف كلمات المرورالمهمة التي يتم نقلها عبر الإنترنت. يتم استخدام المتشممون بواسطة التسلل على الأنظمة المخترقة للتجسس على حركة مرور الشبكة وسرقة معلومات الوصول لمزيد من الأنظمة". انضر :

-Sniffer Program or PacketSniffe, Computer ,

Definition:https://www.yourdictionary.com/sniffer-program-or-packet-sniffer

[2]- بلال أمين زين الدين ،جرائم نظم المعالجة لألية للبيانات ، دار الفكر العربي ،سنه 2008 ، ص 271 .

[3]- احمد فتحي سرور ، الوسيط في قانون العقوبات ، القسم الخاص ، ط3 ، 1992 ، ص806.

[4]- نقض 1978/10/5 – مجموعه أحكام النقض – ص28 – رقم 24 – ص684 .

الكمبيوتر والإنترنت للاستيلاء على المعلومات المراد التحصل عليها بغرض للحصول على أرباح مادية، وبهذا تتحقق نتيجة حصوله عليها[1]، بانصراف إرادة الجاني للقيام بهذا السلوك المؤدي إلى النتيجة، وهذا يعكس الجانب الموضوعي [2].

ومن التعريفات السابقة يتضح أنه لا بد من توافر شرطين لحدوث السرقة.

الشرط الأول: فعل الحيازة، أي حيازة الشيء بغير رضاء مالكه، ثم يأخذه الجاني. وذلك بأخذ الأموال من حيازة المجني عليه وإدخالها في ملكيته. والشرط الأخر هو انعدام رضاء المجني عليه، تمامًا مثل المال على شكل معلومات مهمة يحتفظ بها صاحبها على جهاز الكمبيوتر الخاص به، فيقوم الجاني بالحصول عليها باستعمال الإنترنت ويحتفظ بها لنفسه، حيث قام الجاني بنقل المعلومات إليه مما يحقق معنى السرقة.

ويمكن ملاحظة أن هناك اتجاهين مختلفين في التكيف مع واقع السرقة، فهناك اتجاه إلى يرى إمكانية سرقة المعلومات وبالتالي يجب تجريم سرقة المعلومات، ووفقا لهذا الاتجاه يمكن للمعلومات أن تكون عرضة لجريمة السرقة. ويعتبر السلوك المادي لمرتكب الجريمة، والذي يتمثل في الاستيلاء على المعلومات بأي وسيلة تقنية رغماً عن إرادة مالكها أو حاملها القانوني جريمة سرقة إذا اكتملت بقية العناصر، وطالما أن المعلومات المسروقة سرية وغير متاحة للجميع، فإن الضرر سوف ينجم عن تلك السرقة، ويجب أن يكون نشاط مرتكب الجريمة نتيجة إرادة حرة لمحاولة السيطرة على تلك المعلومات وحيازتها. فمن استولى على وثائق سرية من مؤسسة ما وأراد نسخها ثم إعادتها فهو سارق[3].

أما الاتجاه الأخر فيرى أن سرقة المعلومات لا يمكنها أن تخضع للنصوص القانونية الخاصة بالسرقة التقليدية، مسببين رأيهم بأن المعلومات غير ملموسة لا يمكن امتلاكها.

---

[1] –The No Electronic Theft (NET) Act, enacted in 1997 by the U.S. Congress, amended titles 17 and 18, United States Code, to provide greater protection for copyright owners by amending criminal copyright infringement provisions, and for other purposes.

[2]– هدى حامد قشقوش ، الحماية الجنائية للتجارة الالكترونية عبر الإنترنت، المرجع السابق ، ص 61 وما بعدها.

[3]– السيد عتيق ، جرائم الإنترنت، دار النهضة العربية الطبعة 1، سنه 2000 ، ص103

وبالعودة إلى فعل الاستيلاء فإن الجريمة لا تتحقق إلا إذا تم الفعل دون موافقة الحائز الشرعي[1].

الفرع الثاني : الركن المعنوي للسرقة عبر الإنترنت

يشترط ارتكابها من شخص مدرك وقادر على تحمل تبعات أفعاله، كذلك يشترط لقيام هذه الجريمة القصد العام والخاص.

الفقرة الأولى :القصد العام في السرقة عبر الإنترنت

القصد العام هو إرادة الاعتداء على الأنظمة الإلكترونية ونسبة لما جاء في أحكام نص الفقرة الأولى من المادة 323 من ق ع الفرنسي المستحدث، فالقصد العام يتوجب فيه توافر علم الجاني بعناصر جريمة السرقة، ثم اتجاه إرادة الجاني لارتكاب النشاط المادي والتي ينجر عنه تحقيق النتيجة الإجرامية، بالإضافة إلى علمه بما يحتوي سلوكه من اعتداء على ممتلكات الغير، وعليه يظهر القصد الإجرامي من خلال سيطرة الجاني على أفعاله ونتائجها، وتكون الإرادة هي الأساس[2].

الفقرة الثانية : القصد الخاص

يشترط توافر نية تملك الشيء المسروق في السرقة الواقعة عبر الإنترنت والظهور بمظهر المالك له، ويكون ذلك باتجاه الإرادة لسرقة المعلومات والأموال وممارسة نشاطات المالك القانوني عليها، مع توافر نية الاحتفاظ بالشيء حتى يمكن اعتباره سارقاً.

ومادام القصد من الفعل هو امتلاك ما هو ملك للغير وإلحاق الضرر بهم سواء عن طريق الاستيلاء على بيانات أو معلومات أو أموال تخصهم وبتحقق النتيجة المتمثلة في الانتفاع بها من طرف الجاني بأي طريقة كانت تتحقق جريمة السرقة عبر الإنترنت .

وأخيرا ونسبة لما ذكر ففي ظل انتشار استخدام الإنترنت أصبحت الحياة الشخصية للإنسان غير آمنة كما كانت في الماضي، وأصبح الشخص مهددا بسرقة بياناته ومعلوماته الشخصية في كل وقت خاصة مع تطور الأساليب التي يستعملها القراصنة للاستيلاء عليها، معتمدين في ذلك على شبكة الإنترنت، أضف إلي ذلك التهديد المتربص بالأرصدة

---

[1]– محمود نجيب حسني ، شرح قانون العقوبات ،القسم الخاص ، دار النهضة العربية ، القاهرة، ط 6، 1989 ، ص 838.

[2] – محمود نجيب حسنى ، المرجع نفسه، 867

البنكية والحسابات الإلكترونية والحسابات المصرفية التي أصبحت أكثر عرضة للاختراق والسرقة، وغالبا ما يستفيد الهاكرز من الثغرات الأمنية الموجودة في أجهزة التشغيل لأجهزة الكمبيوتر، والتطبيقات العملية المنتشرة على الإنترنت والتي يتفاعل معها المستخدمون، وعليه من الضروري أن نفطن لطبيعة مخاطر الإنترنت المحيطة بنا، ومن الضروري تعلم كيفية مواجهتها.

المبحث الثاني : جريمة الاحتيال عبر الإنترنت

تعد جريمة الاحتيال من الجرائم التقليدية، وبانتشار الإنترنت وتعدد التطبيقات والمواقع التي توفرها تطورت أنماط وصور وأساليب ارتكابها، ويمارس المحتالون أساليب وطرق الخداع المختلفة، بالإضافة إلى القدرة على تكييف هذه الطرق والوسائل مع تطور التكنولوجيا الحديثة والتغيرات الاجتماعية والحضارية. وما يساعد الجناة في مهامهم أن ضحايا الاحتيال أنفسهم يوقعون بأنفسهم في فخ المحتالين بدافع الجشع وحب الثراء بطرق سهلة وسريعة، كما يقوم الجناة بتزيين أكاذيبهم بطريقة ذكية، مدعومة بمظهر لامع. يجعل الضحايا يتخلون عن أسرارهم وأموالهم طواعية دون إكراه أو ضغط من إرادتهم الحرة، وخاصة أولئك الأفراد الساذجون وذوي النوايا الحسنة.[1]

لقد خلق الإنترنت العديد من التحديات والتهديدات الجديدة، وأصبح الاحتيال عملاً مربحًا تبلغ قيمته مئات الملايين من الدولارات كل سنة.

ومن الجرائم التي عرفت ارتفاع كبيرا في معدلاتها أثناء فترة إنتشار وباء كورونا جريمة الاحتيال عبر الإنترنت. حيث أجمعت معظم دول العالم ومن بينها الجزائر على أنه ومنذ انتشار فيروس كورونا أخذت عمليات الاحتيال عبر الإنترنت في الازدياد من عمليات نصب واحتيال واستيلاء على معلومات وسلب أموال، ومواقع عنكبوتيه كاذبة ومحلات تجارية لا وجود لها وحسابات مصرفية مزيفة تحت شعار تبرعوا من أجل مواجهة كوفيد 19.

[1] – محمد الشناوي، جرائم النصب المستحدثة ، دار الكتب القانونية، القاهرة، 2008، ص 5

وسنحاول من خلال هذا المبحث الوقوف على مفهوم جريمة الاحتيال في شكلها المستحدث، مستأنسين برأي القانون في ذلك مع عرض أهم الوسائل المستعملة في هذه الجريمة ، ناهيك عن محاولة مناقشة الأركان التي تقوم عليها .

المطلب الأول: مفهوم الاحتيال عبر الإنترنت

قبل اللجوء إلى تعريف الاحتيال عبر شبكة الإنترنت وبغية إعطاء معنى أوضح لهذه الجريمة سنحاول أولا أن نعرج إلى تعريف جريمة الاحتيال لغة ثم من الناحية الفقهية والقانونية.

الفرع الأول: تعريف الاحتيال من الناحية اللغوية

يقصد بالاحتيال لغةً أي طلب الشيء بالحيل، أي بوسائل بارعة ابتغاء الوصول إلى المقصود.[1]

الفرع الثاني : تعريف الاحتيال من الناحية الفقهية والقانونية

قد حاول الفقهاء ورجال القانون وضع تعريف للاحتيال، فمنهم من عرفه بأنه: "استعمال الجاني طريقة من طرق التدليس المحددة في القانون، مما يؤدي بالمجني عليه إلى تسليم الجاني مالاً منقولا مملوك للغير". وعرف أيضا بأنه "الاستيلاء على مال منقول مملوك باستعمال وسائل احتيالية بنية تملكه." وهو "الاستيلاء على منقول مملوك للغير بناء على الاحتيال بنية تملكه." وهو "سلب مال الغير بطريق الحيلة".[2]

وقد عرف أيضا على أنه " توصل الجاني أو أي شخص آخر إلى الحصول على مال منقول للغير دون وجه حق، نتيجة استخدامه لأي وسيلة من وسائل الخداع التي نص عليها في القانون على سبيل الحصر والتي تؤدي بالضحية إلى الوقوع في الغلط الدافع إلى التسليم".[3]

وبالرجوع للمشرع الجزائري فهو لم يعرف جريمة الاحتيال في قانون العقوبات بل اكتفى

---

[1] – محمد أبو عزام، إجابة لكل سؤال، http://www.ejaaba.com/topic/106002011/11/26 تم الاطلاع عليه بتاريخ 2014/11/24

[2] – محمد الشناوي، المرجع السابق ، ص 19

[3] علي عدنان الفيل، الجرائم الالكترونية، تم الاقتباس عن الموقع الالكتروني ستار تايمز، شؤون قانونية، 2011/2/1، http://www.startimes.com/?t=27016443 تم الاطلاع عليه بتاريخ 2014/11/24

بتوضيح الأفعال المكونة والظروف المشددة لهذه الجريمة، من خلال المادة 372 ق ع ج.

الفرع الثالث : تعريف الاحتيال عبر الإنترنت

مكتب التحقيقات الفيدرالي الأمريكي يعرف الاحتيال عبر الإنترنت بأنه " يلعب أي مخطط إنترنت احتيالي دورًا رئيسيًا في عرض سلع أو خدمات غير موجودة و المطالبة بالدفع مقابل هذه الخدمات أو السلع عبر الإنترنت". وفيما يتعلق بوزارة العدل الأمريكية فقد عرفته على أنه "شكل من أشكال المخطط الاحتيالي لاستخدام محتوى الإنترنت، مثل: المحادثات ورسائل البريد الإلكتروني والمواقع الإلكترونية وغيرها لتقديم معاملات احتيالية أو الاحتيال على المؤسسات المالية".[1]

ويُعرّف الاحتيال الحاسوبي أو الاحتيال المعلوماتي بأنه "أي عمل احتيالي ينطوي على عملية احتيال إلكتروني بغرض الحصول على مكاسب أو مزايا مالية".[2]

والجدير بالذكر أن المشرع الجزائري لم يعرف ولم يجرم صراحة الاحتيال الالكتروني، على الرغم من التزايد الكبير في عمليات الاحتيال الواقعة على مستخدمي الإنترنت، واكتفى بالنصوص التقليدية والقوانين المجرمة للجريمة الماسة بالنظام المعلوماتي.

وقد وضعت أغلب القوانين الاحتيال الالكتروني ضمن القواعد العامة لجريمة الاحتيال الواردة في الباب المخصص له في قانون العقوبات، ولم ينشئوا نصًا خاصا بالاحتيال الالكتروني. ولكن من ناحية أخرى هناك قوانين جزائية وضعت نصوصا قانونية محددة لهذه الجريمة الحديثة، مثل القانون الاتحادي الإماراتي لمكافحة جرائم تقنية المعلومات وكذلك الولايات المتحدة. التي سنت قانونا ينص على معاقبة الاستخدام غير قانوني لأجهزة الكمبيوتر للقيام بأعمال غير مشروعة وارتكاب أعمال احتيالية للحصول على الأموال.[3]

كما اختلفت التشريعات في تسميتها لجريمة الاحتيال، فهناك من ذهب لتسميتها بجريمة النصب مثل ما هو الحال بالنسبة للقانون الجزائري والليبي والكويتي والبحريني والمغربي

---

[1]– محمد طارق الخن، المرجع السابق، ص 38

[2]– علي جبار الحسيناوي، جرائم الحاسوب والإنترنت، دار اليازوري للنشر والتوزيع، عمان، 2009، ص 72

[3]– علي عدنان الفيل، الجرائم الالكترونية، المرجع السابق، ص 2

والمصـــــــري، أما آخرون فاعتمدوا تسمية الاحتيال كالقانون والســوري الأردنـــي والعـــراقي.[1]

المطلب الثاني : وسائل الاحتيال عبر الإنترنت

يتم الاحتيال عبر الإنترنت باستعمال خدمات الإنترنت المختلفة مثل غرف المحادثة والبريد الإلكتروني أو عبر العديد من الخدمات التي توفرها الإنترنت، وعليه يتخذ الاحتيال صورا وأشكالا متنوعة بتنوع وتعدد خدمات الإنترنت، وغالبا ما يحرص المجرمون على إتباع كل التطورات في خدمات الإنترنت وتقنية المعلومات للاستفادة منه تطوير في عمليات الاحتيال التي يقومون بها واختراع حيل جديدة. ولقد شهد العالم ازدهار ليس له مثيل للاحتيال على الشبكة العنكبوتية في زمن كورونا. حيث انتشرت عمليات النصب والاستيلاء على المعلومات وسلب الأموال عبر رسائل بريد إلكتروني مزيفة، ومحلات تجارية غير واقعية، ومواقع تحث على التبرع من أجل محاربة فيروس كورونا، ولكن في الواقع كل التبرعات يجنيها ويستفيد منها محتالي الإنترنت.

وعليه يمكن القول بأن أساليب الاحتيال تتغير وتتجدد باستمرار مع كل تطور موازي في تقنية المعلومات. وسوف نعرض هنا لأهم هذه الأنواع على النحو التالي:

الفرع الأول :الاحتيال عبر البريد الالكتروني

قد برز استعمال البريد الإلكتروني لسهولته في الإرسال والاستقبال وقلة وتوفير الوقت وقلة المصاريف، هذه كلها ايجابيات أدت إلى تفاقم حجم الرسائل المزيفة والمزورة عبر الإنترنت إضافة إلى ارتكاب العديد من الجرائم المستهدفة للمال من خلال البريد الإلكتروني والخدمات التي يقدمها. وبحسب بعض الإحصائيات، فإن خسائر جريمة الاحتيال قد تصل إلى مئات الملايين، خاصة في الحالات التي يقوم فيها الضحية بتزويد شخص ما برقم حسابه البنكي عبر البريد الإلكتروني. ونجد أن مراكز عمل المحتالين منتشرة في البلدان التي لا تملك سيطرة تذكر على النشاط الحاسوبي، خاصة في أفريقيا.[2]

[1]– علي عدنان الفيل، المرجع السابق، ص 2

[2]– علي عدنان الفيل، المرجع نفسه، ص 5

يأتي الاحتيال عبر البريد الإلكتروني بعدة أشكال أهمها أداة تقوم بإرسال بريد إلكتروني إلى جميع صناديق البريد الإلكتروني لمستخدمي الإنترنت مع رسالة مبروك، لقد فزت بمليون دولار أمريكي، من شركة تختار الفائزين من الإنترنت بطريقة عشوائية. وفي الرسالة يرد بأنه تم العثور على مبلغ نقدي يصل إلى ملايين الدولارات الأمريكية في حساب مصرفي يملكه أحد زبائنهم الذي تعرض إلى حادث تحطم طائرة ومات مع كل أفراد عائلته، ومنذ تلك الفترة لم يتقدم أي شخص للمطالبة بالمبلغ المالي، ولم يتم دفع الحساب البنكي لأنه لم يتقدم أحد للمطالبة به، رغم أن الشركة أكدت عدم وجود وريث قانوني، فقررت إرسال المبلغ إلى أحد الفائزين المحظوظين باليانصيب وتم اختيارك. [1] لذلك نطلب منك تقديم رقم الهاتف ورقم الحساب البنكي واسم البنك، بالإضافة إلى اسم المستفيد ورقم الحساب عند وفاتك. فيقوم الضحية بموافاتهم بجميع المعلومات المطلوبة التي تخصه، ثم يقوم الجاني المرسل بالإجابة مؤكدا ربح المبلغ المالي مضيفا أنه لإتمام العملية يجب على المرسل إليه إرسال رقم هاتفه وعنوانه وصورة طبق الأصل من بطاقته الشخصية، وبعدها سيُطلب منه دفع رسوم البريد مسبقًا ورقم بطاقة الائتمان لإرسال الأموال بالدولار، وبعد ذلك تتوقف جميع الاتصالات منهم[2].

ومن أساليب الاحتيال الرسائل التي يطلق عليها الرسائل المتسلسلة chainletters التي تتم عبر البريد الالكتروني من خلال إرسال رسالة للآخرين تجمع أسماء عدد قليل من الأشخاص، واحداً تلو الآخر على شكل قائمة، ويطلب من متلقي الرسالة إرسال مبلغ من المال بالبريد العادي إلى عنوان الاسم الموجود في أعلى القائمة، بعد تجاوز الاسم الأول الذي أرسلت إليه الأموال، ويكتب اسمه في أسفل القائمة ويرسل رسالة للآخرين ليفعلوا الشيء نفسه. والغرض من ذلك هو التأكد من أن اسم الشخص المسجل يكون في أعلى القائمة في النهاية ، أي أنه يصبح في موقع الاسم الأول، حيث يتلقى مبالغ مالية كبيرة من عدد غير محدود من المساهمين في المسلسل. ويكتشف في نهاية الأمر أنه كان ضحية

[1]–Philippine National Police anti–cyber crime group, Common Types of internet fraudscams, p8

[2]– علي عدنان الفيل، الجرائم الالكترونية، المرجع السابق، ص 5

لعملية احتيال وأن جميع الأسماء يمكن أن تنتمي إلى شخص واحد حصل على كل الأموال.[1]

ومن أنواع الاحتيال باستخدام البريد الالكتروني، ما يعرف باحتيال العروسة الروسية. وتعرف بهذا الاسم لأن واضعي هذه الطريقة هم في الغالب رجال من روسيا، وأحد أكبر المحتالين في هذا المجال يبلغ من العمر 40 عامًا ويدعى روبرت ماك كوي والذي كان يصطاد ضحاياه من خلال الإعلانات الشخصية التي ينشرها على مواقع الويب ويلعب دور العاشقة التي تريد مقابلة حبيبها وتحتاج إلى 1800 دولار لشراء تذكرة الطائرة. وهكذا وبهذه الطريقة يتحصل على مبالغ مالية ضخمة.[2]

وفي زمن كورونا حذرت المنظمة الدولية للشرطة الجنائية (إنتربول) من غزو الخطر السيبراني. وقد صدر تقرير يحذر من مجرمي الإنترنت وهذا تحت عنوان "تهديدات الإنترنت المرتبطة بفيروس كورونا" ، حيث استغلت الجائحة لارتكاب مجموعة متنوعة من الجرائم. وأنه تم إعادة برامج خبيثة للعمل بعد اختفائها لفترة، إذ استغلت انتشار المرض واتخذت العديد من الأشكال الحديثة نتيجة للتطور المستمر في هذا المجال.[3]

الفرع الثاني: احتيال التسوق" التجارة الإلكترونية"

إذا تم استغلال الإنترنت بهدف التسوق فإنه من الطبيعي التعرض لجريمة الاحتيال. فأفضل وسيلة للاحتيال عبر الإنترنت هي تزوير مواقع التسوق كوضع إعلانات وهمية عن بضائع لا وجود لها، أو إنشاء مواقع مزيفة تحمل أسماء شركات معروفة، أو مركات معروفة. وعندما ينخدع المستهلك ويبدأ بالتواصل مع المحتال يقوم المحتال بخداعه والاستحواذ على تحويلاته المالية أو أرصدته المالية باستخدام بياناته الشخصية. ويبقى المجني عليه في انتظار البضاعة، أو قد تأتيه بضاعة قليلة الجودة، أو مغشوشة. ومن أبرز الأساليب التي يتم عبرها الاحتيال ما يلي:

---

[1] – محمد طارق الخن، المرجع السابق، ص 67

[2] – محمد طارق الخن، المرجع نفسه ، ص 68

[3] –الاحتيال الإلكتروني في كورونا https://www.independentarabia.com

أولا : المواقع المزيفة:

يلجأ عدد من المحتالين إلى إنشاء مواقع مزورة عن شركات مشهورة أو ماركات معروفة بغرض الاستيلاء على معلومات بطاقات الائتمان وأرقم الحسابات المصرفية الخاصة بالأشخاص. وعند قيام المجني عليه بالاتصال بالموقع للاقتناء ما يحتاجه يطلب منه الجاني أن يعطيه كل ما يخصه من معلومات لاستغلال البيانات في الاعتداء على أموال الضحية.

ثانيا : احتيال الإعلانات المبوبة:

يحدث هذا الاحتيال عبر الإنترنت عندما يتم وضع إعلانات كاذبة على مواقع إعلانية مشروعة. ويمكن أن تكون الإعلانات على عقارات للإيجار، أو حيوانات أليفة للبيع، أو سيارات للبيع أو لأجهزة كهرومنزلية مستعملة، وتكون بخسة الثمن في أغلب الأحيان[1]. وإذا تم الاتصال من أجل الشراء يتم دفع مقابل السلعة المراد الحصول عليها. ويتم اكتشاف عملية النصب عندما يكتشف الضحية أنه اشترى سلعة وهمية لم تصله أبدا.

ثالثا: احتيال الأدوية المزيفة:

يلجأ الكثير من الصيدليات إلى استخدام شبكة الانترنت لبيع أدوية غير صالحة وأنتجت بغير المواصفات الصحيحة للأدوية. إذ ينشر عبر المواقع المزيفة أسماء لأدوية وغرض استعمالها من أجل الترويج لها وبيعها، وباستخدام هذه الأدوية قد يتأثر المشتري وتزداد سوء صحته لأنها قد تكون ملوثة أو تحتوي على مكونات فاسدة. لذلك ينصح بالعودة للطبيب قبل شراء الأدوية التي تباع عبر شبكة الإنترنت.

لقد تلقت مصالح الأمن الجزائرية، تحذيرات من "الأنتربول"، بخصوص جماعة إجرامية منظمة كثفت أنشطتها في ظل تفشي فيروس كورونا وتستخدم أساليب حديثة في الخداع والاحتيال. كالترويج لأدوية وأقنعة واقية مزيفة ومغشوشة عبر الإنترنت.

وحذرت المنظمة برسالة أرسلتها لمصالح الأمن المشاركة فيها من التخطيطات التي يستخدمها المجرمون، حيث يقوم الجاني بالاتصال بالعديد من الأشخاص متظاهر بأنه

---

[1]–The Australien Compétition and Consumer Commission (ACCC)، The Little Black Book of Scams,p12

طبيب أو مسؤول في مستشفى، ويطلب المساعدة بجمع الإمدادات الطبية والتبرعات والأقنعة والقفازات وحتى المطهرات. ثم يقوم ببيعها عبر الإنترنت ويكسب الملايين من مثل هذه الأنشطة الاحتيالية .

كما بتم تقديم أمثلة أخرى عن الاحتيال والنصب كالادعاء بالإصابة بفيروس كورونا والحاجة الماسة إلى مبالغ مالية للعلاج الطبي، إذ يقوم المحتال بطلب التبرع بالمال من أجل مساعدته على تلقي العلاج المناسب، ثم يقوم بفتح حساب شخصي ويتم تحويل هذه الأموال إلى حسابه.[1]

رابعا : مستحضرات التجميل المزيفة:

بعض منتجات ومستحضرات الجمال والصحة المعروضة على الإنترنت هي منتجات مزيفة واحتيالية. وقد تؤدي بعض هذه المنتجات إلى الإصابة بالسرطان. وعلى سبيل المثال اكتشفت الدراسات والاختبارات الحكومية والصناعية عن وجود مكونات خطيرة جدا في المنتجات المزيفة الخاصة بالبشرة، إضافة إلى احتواءها على مكونات احتيالية مضرة كالزرنيخ والكاداميوم وكلها مواد مسرطنة، إضافة إلى الألومنيوم بكميات هائلة وخطيرة . الأمر الذي تسبب في إصابة العديد من النساء بمضاعفات مثل تقرح الجلد وحب الشباب والصدفية .

خامسا :الغش في المزادات عبر الإنترنت:

توجد على شبكة الإنترنت العديد من مواقع المزادات التي تبيع مختلف البضائع، والتي يمكن لها أن تكون عرضة لجرائم الاحتيال. وعمليات الاحتيال التي تحدث في المزادات عبر الإنترنت تتم بطرق كثيرة، بتغيير المنتج المعلن عنه مثلا، وقد لا يتم إرسال البضاعة إلى المستهلك أصلا [2]. إضافة إلى هذا يتم إيهام المستهلك بحصوله على فرصة جديدة لشراء بضاعة قد سبق ووضع عطاءات عليها لأن الفائز أعلن عن انسحابه في أخر

---

[1] –مجلة الشروق عدد 21ماي 2022م, الموافق ل 19 شوّال 1443هـ الموقع الإلكتروني :
https://www.echoroukonline.com

[2]–the Australian Competition and Consumer Commission (ACCC)، The Little Black Book of Scams ,p13

لحظة، ويطلب من المجني عليه الدفع بطريق أخر خارج وسيلة الدفع الخاصة بموقع المزاد، وفي هذه الحالة يفقد أمواله ولن يتمكن من اللجوء لموقع المزاد طلبا حل مشكلته.

سادسا : الاحتيال في بيع السيارات عبر الإنترنت:

بيع السيارات عبر الإنترنت وسيلة رائجة يتم النصب على الأفراد من خلالها، وتتم بنشر صور مزيفة للسيارات للبيع لا وجود لها في حيازة الجاني. ويتضمن الإعلان المزيف عادةً على صور مطابقة لنوع السيارة ورقم الهاتف لتمكين المستهلك من الاتصال بالبائع المحتال. ويحاول البائع المفترض أن يجعل عملية الاحتيال تبدو وكأنها تمت بطريقة قانونية من خلال طلب العون من شركة ذات صيت، وإيهام المشتري أن عملية البيع ستتم وفقا لبرنامج حماية المشتري، وبمجرد الانتهاء من المعاملة و حصول الجاني على مبلغ البيع، يتم تجاهل المجني عليه عبر كل وسائل الاتصال بما فيها رسائل البريد الإلكتروني، وأحيانا قد تصل به الجرأة بطلب أموال إضافية ، ولا يتم تسليم السيارة ولا يتمكن المشتري أبدًا من استرداد خسائره.

المطلب الثالث: أركان جريمة الاحتيال عبر الإنترنت

لقيام الاحتيال عبر الإنترنت لابد من توافر عدة أركان أهمها:

الفرع الأول: محل جريمة النصب في نطاق الاحتيال عبر الإنترنت

تتركز الإشكاليات التي يثيرها الفقه بخصوص تطبيق النموذج القانوني لجريمة الاحتيال، على الأفعال التي تتمثل في التلاعب في المعلومات والبيانات والبرامج بهدف الحصول على مال أو أي شيء آخر ذات قيمة. فيرى البعض أن الطبيعة المعلوماتية هي المستهدف الأول للاحتيال المعلوماتي، تتعلق الكثير من المعلومات المستخدمة لأغراض التلاعب والاحتيال بكشوف الحساب والأرصدة المصرفية وبطاقات الائتمان والبيانات والتقارير المالية. واستنادا إلى الخبرة السابقة، فإن الاحتيال الأكثر احتمالا يقع على المرتبات، وتقارير التكلفة والمصروفات.[1]

وقد ثار خلاف في الفقه بشأن اعتبار المعلومات محل لجريمة الاحتيال إلى اتجاهين،

[1]–عمر أبو الفتوح الحمامي، الحماية الجنائية للمعلومات ، دار النهضة العربية ، مصر ، 2010، ص 642

الأول: يرى صلاحية المعلومات لأن تكون محل لجريمة النصب أو الاحتيال، والاتجاه الثاني: يرى عدم صلاحية المعلومات لأن تكون محلاً للنصب أو الاحتيال. ولكن هناك إجماع فقهي حول صلاحية المكونات المادية للأنظمة المعلوماتية مثل الشرائط، شاشات العرض لوحات المفاتيح وخلافه لان تكون محل لجريمة الاحتيال، باعتبار أن هذه المكونات ما هي إلا مال منقول مملوك للغير، كذلك فإن المعلومات والبرامج صالحة لأن تكون محلاً لجريمة الاحتيال شريطة أن تكون مثبتة على دعامات مادية، حيث تكون الدعامة محلاً للجريمة نظراً لطبيعتها المادية[1].

لقد حددت مختلف التشريعات العربية والأجنبية أن يكون موضوع الاحتيال مالاً ماديا، وسواء كان هذا المال منقولاً أو غير منقول، وسواء كان هذا المال مملوكاً لشخص آخر، فإن سبب هذا الشرط هو أن الاحتيال جريمة تشمل التعدي على حقوق الملكية، ولا يصلح إلا الشيء الذي له صفة المال أن يكون محلا للملكية، ويشترط أن يكون المال ذا طبيعة مادية، أي أنه يمكن تسليمه وامتلاكه. ويتم استبعاد الأشياء المعنوية من مفهوم المال، كالأفكار والآراء والمخترعات الفنية، لكن هذه الأشياء تتحول إلى مال مادي إذا أفرغت في وعاء مادي، كالسند أو الكتاب أو النوتة الموسيقية أو براءة الاختراع، فالاستيلاء على هذه الأشياء بالخداع يتحقق فيه جريمة الاحتيال.[2] فعندما يكون للشيء صفة المال فإنه يكون عرضة لأن يكون محلا للاحتيال، سواء كانت قيمته كبيرة أو صغيرة مادية كانت أو معنوية. وبناءً على ذلك يمكن أن يكون تذكار عائلي موضوعًا للاحتيال كونه ذا قيمة معنوية. وكذلك جريمة الاحتيال عبر البريد الالكتروني لا تخرج عن هذا الأصل عندما يكون محل التسليم شيئاً له صفة المال المادي كالنقود أو العقارات.[3]

الفرع الثاني : الركن المادي للاحتيال عبر الإنترنت

الركن المادي في هذه الجريمة هو الحيلة التي يستخدمها المحتال بهدف الاستيلاء على مال منقول لنفسه أو لغيره، ولقيامها يشترط توافر عدة عناصر تتمثل في مايلي.[4]

---

[2] -عمر أبو الفتوح الحمامي،المرجع نفسه، ص 643

[3]- محمد طارق الخن، المرجع السابق، ص 135

[3] محمد طارق الخن، المرجع السابق ، ص137-138

[1]-علي عدنان الفيل، الجرائم الالكترونية، المرجع السابق، ص 4

الفقرة الأولى: السلوك الإجرامي (الطرق الاحتيالية)

أولا: اتخاذ اسم أو صفة كاذبة

إن الكذب مهما كانً مرتباً و يؤدي إلى تصديقه لا يكفي أن يكون وسيلة للاحتيال، إلا إذا اجتمع على أعمال مادية ومظاهر يلجأ لها المحتال، ويقوم بحبكها من أجل إيهام المجني عليه بصحتها، وبالرجوع إلىً محاكم النقض المختلفة نذكر على سبيل المثال أن محكمة الاستئناف الإيطالية ترى أنه لإثبات الاحتيال لا يكفي الكذب، ولكن يجب أن تكون الكذبة فعالة في حث الضحية على ارتكاب خطأ ما. وتتخذ القوانين في مصر وفرنسا نفس هذا المنهج.[1]

فوسائل الاحتيال غير محددة قانونيا، فكل ما يمكنه تضليل الضحية وخداعها يعد وسيلة من وسائل الاحتيال مثلا إقناع الناس بالقدرة على شفاءهم من أي علة، أو الإعلان عن قيام مشروع استثماري وهمي، أيضا التغيير في الاسم الحقيقي وفي الصفة يعتبر من الوسائل الاحتيالية ، فبمجرد تغيير الاسم باسم غير حقيقي، أو تغيير الصفة إلى طبيب أو عامل ببنك أو شرطي من شأنه خداع الضحية ووضعها في قبضة المحتالين وهذا ما نجده في القانون الفرنسي والقانون الجزائي العربي الموحد، أما القانون السوداني نجده مخالف لأغلب التشريعات الجزائية الأخرى ولم يوضح وبصورة دقيقة وسائل النصب والاحتيال على غرار بقية التشريعات، بل اكتفي بنص عام وفتح المجال للقضاة بأن يجتهدوا ويجدون طرق الاحتيال.[2]

ثانياً: الاحتيال بطريق التصرف في عقار أو مال منقول

يتم الاحتيال بهذه الطريقة بسلوك الجاني الذي ينطوي على ادعاء كاذب، ووقوع المجني عليه في الخطأ، وهذا الخطأ هو الذي اضطره إلى إعطائه ماله. ولكي يقع الاحتيال بهذه الوسائل لا بد من توفر شرطين: معاً هما: التصرف في الأموال المنقولة أو العقارات، وبشرط أن تكون مملوكة للغير، ولا يحق للجاني التصرف فيها.[3]

---

[2]– محمد هشام عبد الفتاح ، جريمة الاحتيال دراسة مقارنة،رسالة ماجستير، نابلس، فلسطين، 2008 ، ص 15

[2]– علي عدنان الفيل، الجرائم الالكترونية، المرجع السابق، ص 4

[2]– محمد هشام عبد الفتاح، المرجع السابق، ص، 50

الفقرة الثانية : النتيجة الجرمية (تسليم المال)

لم تكن هناك مشكلـــــــة في محل جريمة الاحتيال، قبل ظهور الإنترنت، فكل الأموال المنقولة التي تحمل طابعا ماديا تصلح لأن تكون محلاً للنصب والاحتيال.[1]

و بظهور الإنترنت، تم إثارة عدة مسائل منها مسألة المنافع والخدمات التي وفرتها شبكة الإنترنت وجعلت منها محلاً للنصب والاحتيال.

لقد اختلفن التشريعات الجزائية في ما بينها حول تحديد طبيعة المال الذي يمكن له أن يكون موضوع جريمة الاحتيال عبر الإنترنت :

الاتجاه الأول : يرى من الضروري أن يكون المال منقولاً مادياً لأن يكون محلا للاحتيال سواء كان هذا المنقول مادي يحمل قيمة مادية أو عبارة عن نقود، وعليه فإن المال المنقول المعنوي كالخدمات مثلا لا يمكنها أن تكون محلاً للاحتيال عبر مواقع الإنترنت، وهذا الاتجاه يشمل قطر ومصر وكذلك الإمارات والعراق .

الاتجاه الثاني : بعكس الاتجاه الأول فهو يري أنه من غير الضروري أن يكون المال منقولا ماديا حتى يصبح محلا للاحتيال عبر الإنترنت، بل أدخل المنافع والخدمات لتصبح محلاً لهذه الجرائم وبتعبير أخر يمكن أن يكون محلا للتسليم مالاً غير مادي، فقيام أحد الأشخاص بطلب استشارة محامي أو طبيب وبواسطة عبر الإنترنت وجعله يعتقد أن تكلفة الاستشارة تم دفعها ببطاقة الائتمان ولم يدفعها، فيعتبر مرتكباً جريمة احتيال عبر الإنترنت. كذلك الاستفادة من الكتب عبر مواقع الانترنت أو الاشتراك في إحدى الصحف الإلكترونية بطرق احتيالية حققت له بعض الفائدة. وهذا الاتجاه يساوي بين الخدمات والأموال، وبالتالي فإن الأموال المنقولة، سواء كانت مادية أو معنوية، تعد محلا لهذه الجرائم. وهذا الاتجاه يشمل فرنسا والسودان وكذلك اليمن.[2]

ووسيلة التسليم في جريمة الاحتيال عبر الإنترنت لا تكون تقليدية كما هو الحال بالنسبة لجريمة الاحتيال العادية. فالتسليم يتم بالنقود واستخدام البنك أو شركة تحويل الأموال أو بطاقة الائتمان أو الشيك. ولذلك من المستحيل تصور إرسال الأموال مباشرة باليد، أما إذا

---

[1]– علي عدنان الفيل، الجرائم الالكترونية، المرجع السابق، ص 7

[2]– علي عدنان الفيل، الجرائم الالكترونية، المرجع نفسه، ص 8

لم يتم إرسال الأموال، بالرغم من قيام فعل الاحتيال، مثل أن يدرك المجني عليه أن البريد الذي استلمه غير حقيقي، فهنا نواجه ما يسمى في جريمة الشروع في الاحتيال باستخدام الإنترنت، والشروع يكون محكوماً في الجرائم عبر الإنترنت بقواعد عامة وبالتالي يسأل الجاني عن جريمة الشروع. فالاحتيال هو كل فعل قوم به الجاني باستعمال الغش والخداع عبر شبكة الإنترنت وهذا ما نص عليه القانون المصري. ففي حالة القيام بفعل من أفعال الغش والخداع ولم ينجح لسبب خارج عن إرادة الجاني أي يقع المجني عليه في شرك القائم بالاحتيال ولم يقم بتسليم المال، فجريمة الاحتيال تعد ناقصة لانعدام النتيجة. كما أن قيام الجريمة لا تتأثر بإعادة المال لصاحبه لإحساسه بالندم، لأن هذا يعتبرّ ظرفاً مخففاً[1].

تعد جريمة الاحتيال عبر الإنترنت من الجرائم الواقعة على الأموال ومن البديهي أن يترتب على وقوعها حصول ضرر يلحق بالمجني عليه أو بغيره، و بالرغم من ذلك فإن العديد من التشريعات الجزائية المقارنة لم تتفق حول النص صراحة على وجوب تحقق الضرر. فالاتجاه الأول يستلزم وجوب تحقق الضرر، حيث أشار إلى ذلك ضمنياً من خلال عبارات النص القانوني من خلال عبارة الحصول على فائدة مادية من خلال الاستحواذ على مال الغير، فهذه عبارات تشير إلى حصول ضرر خلفه فعل الاحتيال. ويشمل هذا الاتجاه كلا من فنلندا وقطر والعراق والإمارات واليمن. أما الاتجاه الثاني هو أكثر وضوحاً من الاتجاه الأول، ذكر بكل وضوح السلوك الضار أو الخسارة غير قانونية.[2]

الفقرة الثالثة : علاقة السببية في جريمة الاحتيال

وحتى يتوافر الركن المادي للاحتيال، لا يكفي أن يمارس مرتكب الجريمة نشاطاً يشكل احتيالاً، ويؤدي إلى قيام الضحية بتسليم أمواله إلى الجاني تحت تأثير الخطأ. بل يجب أن تكون هناك علاقة سببية بين الفعل والتسليم. فبدون الخداع لا يوجد تسليم ويجب أن تؤدي عملية الاحتيال إلى وقوع الضحية في الخطأ، ويجب على الضحية ارتكاب نفس الخطأ الذي كان مرتكب الجريمة ينوي أن يرتكبه. أما إذا علم المجني عليه بخداع مرتكب الجريمة ولم يخطئ زالت علاقة السببية.[3] ولا يشترط أن يكون الخطأ هو السبب الوحيد لتسليم

---

[1]– علي عدنان الفيل، المرجع السابق ، ص 9

[2]– علي عدنان الفيل، الجرائم الالكترونية، ستار تايمز، المرجع السابق ، ص 9

[3]–محمد طارق الخن، المرجع السابق ، ص 174

أمواله، ولكن يكفي أن يكون أحد الأسباب التي دفعت الضحية إلى التسليم. وتستمد هذه القاعدة من نظرية تكافؤ الأسباب التي اعتمدتها بعض التشريعات العربية، وهذه القاعدة يترتب عليها، أن إهمال المجني عليه وعدم مبالاته في التحقق من الفعل الاحتيالي لا ينفي علاقة السببية الضرورية للاحتيال. فحسن نية الضحية وميله إلى ارتكاب الأخطاء لا ينفي هذه العلاقة. أما إذا ثبت أن الخطأ لم يؤثر على المجني عليه عند تسليمه أمواله، فقد انتفت علاقة السببية. كما لا توجد علاقة سببية بين الاحتيال والتسليم بسبب خطأ متعمد من مرتكبه، ولكن بسبب خطأ آخر ارتكبته الضحية دون تدخل المحتال. وبناء على ما سبق إذا أرسال شخص بريداً إلكترونياً إلى شخص آخر يدعي فيه أنه الوريث الوحيد لتاجر معروف ويطلب من المستلم مبلغاً من المال لتغطية تكاليف تسوية التركة على أن يقوم بتسليمه جزء منها، بحيث يرسل المجني عليه المبلغ المطلوب لا لأنه يفعل ذلك عن طريق الخطأ، ولكن من باب اللطف والإحسان. وفي هذه الحالة لا تقع جريمة الاحتيال عبر الإنترنت لانتفاء علاقة السببية بين الخطاء وفعل التسليم.[1]

الفرع الثالث :الركن المعنوي للاحتيال عبر الإنترنت

هذا النوع من الجرائم جرائم عمديه تستلزم توفر القصد الجنائي العام والخاص. ويرتكز القصد الجنائي العام على عناصره المتمثلة في العلم والإرادة، أما العلم فيقتصر على قيام المجرم بعمله وهو يعلم أن أفعاله وأقواله كاذبة وتزييف للحقيقة، وبالإضافة إلى العلم، يجب أن تكون لدى مرتكب الجريمة إرادة ارتكاب الفعل الإجرامي، وهو الاستيلاء على أموال شخص آخر، وأن يؤدي الاحتيال الذي يرتكبه إلى خداع المجني عليه ووقوعه في الخطأ، وإجباره على تسليم أمواله.

وهناك من يرى بأن القصد الجنائي الخاص في هذه الجريمة يعنى به القصد الجنائي العام ، لأنه يدخل ضمن القصد العام وعليه ليس من الضروري اشتراط وجوب توافر قصد جنائي خاص. وبالرغم من ما سبق يشترط تزامن القصد العام والخاص في جريمة الاحتيال المتعلقة بالشبكة المعلوماتية مع زمن الحصول على الأموال. وقيام القصد الجنائي العام

[1]– محمد طارق الخن، المرجع السابق، ص 175،176

والخاص يرجع إلى ما استخلصته محكمة الموضوع من وقائع الدعوى، ولا يؤخذ بالدافع وراء ارتكاب الجريمةً.[1]

وبالرجوع لجريمة النصب في القانون ومن خلال الاطلاع على نص المادة 372 نستنتج أن الاحتيال هو أن يستلم الشخص أموالاً أو منقولات سواء باستخدام أسماء زائفة أو أوصافًا زائفة أو وسائل احتيالية، وهذا بهدف خلق الوهم بوجود نشاط يشترط فيه توافر أربع عناصر:

1- ضرورة أن تكون وسيلة الاحتيال نصت عليها المادة 372 ق ع ج على سبيل الحصر.

2- يجب على الجاني أن يحصل على تسليم مبلغ من المال أو منقول أو أي قيمة يتم تحويلها بهذه الوسائل.

3 – ضرورة تسبب الاحتيال في ضرر مادي للمجني عليه

4- يجب توافر نية للغش.

المبحث الثالث: المتاجرة بالمخدرات عبر الإنترنت

مع انتشار استخدام الشبكة المعلوماتية التي أصبحت بيئة ممتازة للتلاقي وعرض وترويج المخدرات بين الناس، باتت تجارة المخدرات هاجس يهدد كافة دول بما فيها الجزائر. وباستخدام الإنترنت خلقت بيئة إيجابية لزيادة واستفحال نشاط عصابات المتاجرة بالمخدرات، ومما يزيد من تعقيد المشكلة العلاقة بين الاتجار بالمخدرات والجريمة المنظمة والإرهاب وغسل الأموال والفساد من ناحية، والمخاطر والآثار الوخيمة الناجمة عنها من ناحية أخرى.

فالنسبة لمروج المخدرات في الوسط المعلوماتي تمثل شبكة الإنترنت غطاء ممتاز له ووسيلة مثلى لارتكابه لهذه الجريمة، كون الإنترنت بيئة أوسع للتعامل مع شرائح مختلفة من الجمهور سواء من ناحية الكم أو النوع، إضافة لكونها تحول دون اكتشاف الجريمة على النحو الذي يتم به اكتشاف الترويج والمتاجرة بشكل تقليدي. أما بالنسبة للمتعاطي للمخدرات فتمثل له الوسيلة الأسرع للحصول على المادة المخدرة دون أن يكلف نفسه عناء

[1]- علي عدنان الفيل، الجرائم الالكترونية، المرجع السابق، ص 9

البحث.[1]وعليه سنقوم من خلال هذه المبحث تسليط الضوء على جريمة المتاجرة بالمخدرات عبر الإنترنت، وذلك بالتطرق لمفهومها والطرق التي تتم بها والأركان الواجب توافرها لقيامها.

المطلب الأول : مفهوم تجارة المخدرات عبر الإنترنت

تعد الإنترنت والمواقع والخدمات المنتشرة عبرها أحسن وسيلة يعتمد عليها مروجي المخدرات باستخدام ألغاز وشفرات وصور خاصة عبر حسابات وضعت بغرض بيع سمومهم والإيقاع بضحاياهم. وقبل التطرق لتعريف تجارة المخدرات عبر الإنترنت. لابد من تعريف تجارة المخدرات في شكلها التقليدي.

الفرع الأول : تعريف تجارة المخدرات

قبل التطرق لتعريف جريمة تجارة المخدرات سنتناول أولا تعريف المخدرات .

الفقرة الأولى : تعريف المخدرات لغة

يعود أصل كلمة المخدرات في اللغة العربية "إلى كلمة خدر أي ستر، واستخدمت كلمة المخدرات للدلالة على مواد تغيب العقل. أما في اللغة الفرنسية فتقابلها كلمة Drogue، وهي مادة تستخدم في أغراض طبية بمفردها أو بخلطها تعمل على تغيير حالة أو وظيفة الخلايا أو الأعضاء أو الكائن الحي.[2]

الفقرة الثانية: التعريف الفقهي والقانوني للمخدرات

وتعرفها منظمة الصحة العالمية بأنها التسمم الدوائي الناتج عن الاستخدام المتكرر للمادة المخدرة.[3]

---

[1] – حنان ريحان مبارك ، الجرائم المعلوماتية ، المرجع السابق ، ص 292

[2]– نبيل صقر، جرائم المخدرات في التشريع الجزائري، دار الهدى عين مليلة، الجزائر، ص 6

[3]– حسين بن شيخ آت ملويا، المخدرات والمؤثرات العقلية، دراسة قانونية تفسيرية، دار هومة للنشر، الجزائر 2010، ص7

كما عرفت على أنها " مواد كيميائية تتسبب في النعاس وفي النوم أو فقدان الوعي، مصحوبة بتسكين الألم، وهذه المادة بحكم طبيعتها الكيميائية تؤثر على نفسية الكائن الحي ووظائفه والجهاز العصبي المركزي، فتسبب تغيرات في الدماغ ووظائف تتعلق بتنشيط أو انقطاع مراكز المخ المختلفة التي تؤثر على الذاكرة والتفكير واللمس والبصر والشم والسمع والتذوق والإدراك والكلام." [1]

أما في التشريع الجزائي فقد عرفت المخدرات من خلال المادة 2 من القانون 04 -18 المؤرخ في 25 ديسمبر 2004 على أنها " كل مادة طبيعية كانت أم اصطناعية من المواد الواردة في الجدولين الأول والثاني من الاتفاقية الوحيدة للمخدرات لسنة 1961 بصناعتها المعدلة بموجب برتوكول 1972". وقد عرف المؤثرات العقلية على أنها " كل مادة طبيعية كانت أم اصطناعية أو كل منتوج طبيعي مدرج في الجدول الأول أو الثاني أو الثالث أو الرابع من اتفاقية المؤثرات العقلية لسنة 1971 ".[2]

وبالنسبة للاتفاقية العربية لمكافحة الاتجار بالمخدرات والمؤثرات العقلية لعام 1994 فقد عرفت المخدر في المادة 1/ 17 بأنه " جميع المواد الطبيعية أو المصنعة الواردة في الجزء الأول من الجدول الموحد ".

الفقرة الثانية : تعريف تجارة المخدرات

الاتجار بالمخدرات هي تجارة غير قانونية في معظم أنحاء العالم و تنطوي على زراعة وإنتاج وتوزيع وبيع المواد الخاضعة لقوانين مكافحة المخدرات. ولقد تضمنت اتفاقية الأمم

[1]– نصر الدين مروك، جريمة المخدرات في ضوء القوانين والاتفاقيات الدولية، دار هومة للنشر والتوزيع، الجزائر، 2007، ص 17.

[2]– قانون رقم 04 / 18 المؤرخ في 25 ديسمبر 2004 المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار الغير المشروعين بهما، 83 المؤرخة في 26 ديسمبر 2004.

المتحدة لمكافحة الاتجار غير المشروع بالمخدرات والمؤثرات العقلية 1988 القانون الدولي والتزامات الدول فيما يتعلق بالمتاجرة غير المشروعة، حسب ما نصت عليه المادة 3 منه.[1]

الفرع الثاني : تعريف جريمة الاتجار بالمخدرات عبر الإنترنت

جريمة المتاجرة بالمخدرات عبر الإنترنت هي "عبارة عن تعبير يشمل اجتماع التعامل بالمخدرات والمؤثرات العقلية بتكنولوجيا المعلومات والإنترنت وذلك باستخدام وسائلها". وهي استخدام للإنترنت لتسهيل التعامل بالمخدرات والمؤثرات العقلية مهما كان نوعها بنشرها أو الاتجار بها أو ترويجها أو تعاطيها.[2]

المطلب الثاني : طرق ترويج المخدرات عبر الإنترنت

ينتهج مجرمي الإنترنت عدة طرق للترويج المخدرات والمتاجرة بها عن طريق شبكة الإنترنت.

الفرع الأول: شبكة "الإنترنت المُظلِم"

استغل مروجي المخدرات شبكة "الإنترنت المُظلِم" والتي تسمّى أحياناً "الإنترنت الخفيّة" لاستخدامها في ترويج و بيع المواد المخدرة عن طريق شبكات التواصل الاجتماعي، وفي معظم الأحيان لجذب انتباه الضحايا إلى حساباتهم الإلكترونية ، يلجئون إلى الغرافيتي على جدران الشوارع، خاصة في الدول الغربية. ويستخدمون أجهزة حاسوب يطلق عليها "بوتس"، والتي يكون مالكوها مجهولين وقد تم التحكم فيها مسبقًا، للتواصل مع العملاء من خلالهم.

وقد تغيرت تقنيات االترويج بعد أن نفذت مواقع التواصل الاجتماعي طرق تشفير تسمح للمستخدمين بالبقاء مجهولين عن طريق تقنية لإخفاء المعلومات الشخصية .

إن الاستعمال المتزايد من طرف مروجي المخدرات لهذا التطبيقات الجديدة، وهذا ما تمت ملاحظته من طرف خبراء لديهم خبرة في مكافحة الجريمة المعلوماتية، مشيرين إلى أن هؤلاء المجرمين يستخدمون أساليب مبتكرة للتهرب من الشرطة، وقد صرح خبير في

---

[1]– تنص المادة 3 من اتفاقية الأمم المتحدة لمكافحة الاتجار غير المش روع بالمخدرات والمؤثرات العقلية لعام 1988 " أن يتخذ كل طرف ما يلزم من تدابير لتجريم الأفعال المدرجة في إطار قانونه الداخلي في حال ارتكابها عمدا.

[2] – هروال هبة نبيلة، جرائم الإنترنت دراسة مقارنة ، أطروحة دكتوراه، جامعة تلمسان ، 2013-2014،ص250

شبكة الإنترنت الخفيّة، أنه يمكن للمجرمين الدخول إلى خدمة "تلغرام" وكيفية استخدام أجهزة الكمبيوتر الخاضعة لتحكم "بوتس" للتواصل بين المروجين وعملائهم، وهي طريقة بسيطة وسهلة لتجنب العقاب. وقد قام نفس الخبير بنشر سلسلة صور تحمل اسم قنوات على الجدران القريبة من محطات العبور والشوارع الرئيسية، وعلى هذه القنوات تم نشر إعلانات تشرح كيفية الاتصال بتجار المخدرات، حتى يتمكن المستخدمون الجدد من رؤيتها.[1]

وهناك اختلاف كبير في طريقة ترويج المخدرات على الإنترنت والاعتماد على الأماكن المظلمة على سبيل المثال. أي يمكن لأي شخص استخدام البريد الالكتروني الذي ترك من طرف صاحبه للترويج للعناصره المحظورة، ويمكن للعملاء رؤيتها والقيام بالعملية باطمئنان. حيث تساعد هذه الطريقة في تجنب مخاطر الاجتماعات وتجنب أيضًا مخاطر التحكم في المنتج إذا تم تسليمه على سبيل المثال عن طريق البريد.

يقوم تجار المخدرات عبر الإنترنت بإخفاء المواد المخدرة في أماكن تظهر للعامة مثل الحدائق وبعد تأكيد الشراء، يتلقى العميل رسالة حول موقع الأدوية المخدرة. وأول من قام بالعمل بطريقة الأماكن الميتة" مجموعة إجرامية في أوكرانيا، وأطلق عليها عصابات الأمكنة الميتة. وبعدها انتشرت في روسيا وأوروبا.

ويقول ريك فورغسون، المنسق الخاص في وحدة الشرطة الأوروبية التابعة لليوروبـــــول، إن القدرة على استخـدام الرسائل المشفرة وإخفاء الهويات بين المتصلين، بالإضافة إلى نقاط الضعف في تقنيـــات التحقيق، هو ما يجعل تجار المخدرات ينجذبون لمثل هذه التطبيقات.[2]

---

[1]– انطوني كاثبرتسون ، مجرمو الإنترنت الخفي، مقال منشور على الموقع الأتي :

https://www.independentarabia.com/node/12881 ، تم الاطلاع عليه في 08/05/ 2019

[2]– انطوني كاثبرتسون ، مجرمو الإنترنت الخفي، مقال منشور على الموقع الأتي :

https://www.independentarabia.com/node/12881 ، تم الاطلاع عليه في 08/05/ 2019

الفرع الثاني : المخدرات الرقمية عبر الإنترنت .

لم تفلت الموسيقى من بلاء مجرمي الإنترنت، حيث أتاحت التكنولوجيا المتقدمة وسيلة جديدة تستخدم للإدمان والانتحار البطيء. فمنذ وقت ليس ببعيد كانت المخدرات الرقمية مصطلحا لا وجود له، وكانت الموسيقى تسمع في كل الأوقات ولم تؤذي أي شخص، ولكنها تحولت في عصرنا هذا إلى تجارة وإدمان عبر الإنترنت، على شكل ملفات صوتية ومقاطع الفيديو على الويب في البداية مجانية للاختبار حتى يتم الوصول إلى الهدف ويصبح المستمع ضحية وعندما يصل اهتزاز الموسيقى إلى المخ، تنقل الضحية إلى حالة عدم توازن وحالة اللاوعي. وهناك العديد من أشكال واستخدامات للمخدرات الرقمية واستخداماتها وتختلف أسماءها، تمامًا مثل المؤثرات العقلية الكيميائية، مثل"كريستال ميث" وغيرها من التي تدفع للهلوسة وآخري للاسترخاء وآخري للتركيز.

الفرع الثالث: إنشاء أو نشر مواقع خاصة على الشبكة العنكبوتية

قد تطورت وتغيرت أساليب الترويج للمخدرات، ومن هذه الأساليب الإجرامية إنشاء مواقع على الإنترنت هدفها تسويق المخدرات والمؤثرات العقلية أو الترويج لها أو تسهيل تداولها، وقد توزع من خلال تقنية المعلومات باستخدام الهواتف الذكية أو أجهزة الكمبيوتر أو الساعات الإلكترونية القادرة على الاتصال بالإنترنت، أو عن طريق مواقع التواصل مثل الواتساب أو الفايسبوك وغيرها من التطبيقات المختلفة، وغالبا ما يتم باستخدام الأسماء المستعارة للترويج للمخدرات أو من خلال المجموعات المغلقة أو السرية على وسائل التواصل الاجتماعي. وكافة المواقع التي يستخدمها تجار المخدرات تكون مشفرة لمنع وقوعها تحت سيطرة السلطات، تلك الجهة المخول لها متابعة مثل هذه الجرائم، مثل الشرطة المختصة بمكافحة المخدرات.[1]

إضافة إلى ما سبق تحتوي هذه المواقع على معلومات حول طرق الإنتاج أو التصنيع والتسويق والترويج واستخدام المواد المخدرة أو المؤثرات العقلية. فالفضاء الافتراضي مكان

[1] –Falgun Rathod: Handbook on Cyber Crime and Law in India Compiled, Falgun Rathod, India, 2014, P 52.

مفتوح يمكن للجميع الدخول إليه والوصول إلى المواقع التي يتم من خلالها عرض المخدرات أو يمكن أن تصل إليه من خلال التكنولوجيا الحديثة المتمثلة في وسائل التواصل الاجتماعي، أو عبر البريد الإلكتروني.[1]

المطلب الثالث: أركان جريمة الاتجار بالمخدرات عبر الإنترنت

سنتناول في هذا المطلب أركان هذه الجريمة حيث سنعرض في الفرع الأول الركن المادي لها، بينما سيتناول في الفرع الثاني الركن المعنوي.

الفرع الأول: الركن المادي في جريمة الاتجار بالمخدرات عبر الإنترنت

الركن المادي لهذه الجريمة يشمل السلوك والنتيجة وعلاقة السببية. فالجوهر القانوني لهذه الجريمة هو تجريم النشاط المفترض على الإنترنت من خلال إنشاء موقع على شبكة الإنترنت أو تكنولوجيا المعلومات بهدف الاتجار بالمخدرات أو الترويج لها أو تسهيل تداولها، أو تشفير أي موقع عبر الإنترنت يستخدمه مروجو المخدرات بغرض حمايتهم من الوقوع تحت سيطرة أجهزة الأمن، أو توفير جهاز كمبيوتر مزود بلوازم فك الشفرة والتي يتم إرسالها إلى أحد الأطراف لتوزيع المواد المخدرة، كما يعرض على الموقع الإلكتروني معلومات مفصلة عن كيفية إنتاج المواد المخدرة أو المؤثرات العقلية، إضافة إلى طرق تصنيعها وتسويقها وتوزيعها وطرق تناولها من خلال شبكة الإنترنت. وتجدر الإشارة هنا إلى أن السلوك الذي يشكل الركن المادي يجب أن يكون سلوكا إيجابيا مع احتمال استمراره، لأنه قد يتم وضع إعلانات إلكترونية مشفرة من طرف تجار المخدرات وبالتالي يستمر عرض هذه الإعلانات لمدة طويلة، وبالتالي تستمر الجريمة طالما استمر السلوك المادي.

[1] –Drugs in the mail: how can it be stopped? hearing before the Subcommittee on Criminal Justice, Drug Policy, and Human Resources of the Committee on Government Reform, House of Representatives, One Hundred Sixth Congress, second session, May 26, 2000, P35.

الفرع الثاني: الركن المعنوي في جريمة الاتجار بالمخدرات عبر الإنترنت

يتكون هذا الركن من الفعل الإجرامي للمجرم، وأساس هذا الفعل هي الإرادة الإجرامية الرابطة بين الجاني والنشاط المرتكب، وأن يتم هذا النشاط بإرادته المنفردة. وتجدر الإشارة هنا إلى أن القاعدة العامة لجرائم الاتجار بالمخدرات تشير إلى أن ركنها المعنوي لا يرتكز فقط على القصد الجنائي العام، بل يجب توافر القصد الجنائي الخاص.

فبالرغم من أن جريمة الاتجار بالمخدرات عبر الإنترنت تعد من أخطر الجرائم في العصر الحديث، لأنها جريمة تشكل تهديدا لصحة الإنسان وأمنه، إلا أنه لا يزال هناك فراغ قانوني في محاربة هذه الجريمة خاصة في ما يتعلق بالمخدرات الرقمية.

المبحث الرابع : الاعتداء على الملكية الفكرية

لطالما كانت جرائم حقوق الطبع والنشر مشكلة حقيقية في عالم المنتجات المادية، ولكن مع ارتفاع استخدامات الإنترنت، أصبح الاعتداء على الملكية الفكرية عبر الإنترنت يشكل تهديدًا كبيرا للاقتصاد. فالاعتداء على الحقوق الفكرية والصناعات الإبداعية وحدها تعد قيمتها بالملايير.

فأساس الحقوق الفكرية هو العقل البشري، الذي يتجلى في صورة أفكار، إذا تمت إدارتها بطريقة محددة، فإنها تخلق حقوقًا مهمة جدًا لأصحابها في النظام والقانون الدولي ذي الصلة.

وانتهاك الملكية الفكرية هو نشاط من شأنه الاعتداء على هذا الحق دون إذن، وقد عرف البعض هذا الاعتداء بأنه" كل اعتداء يمس ابتكارا جديدا سواء كان أدبيا أو فنيا أو علميا". ولقد اتسعت مجالات الاعتداء على حقوق الملكية الفكرية والأدبية لتشمل أشكال التعبير المبتكرة التي أظهرها التطور التكنولوجي، فشملت كلا من تشغيل نظم المعلومات وقاعدة بيانات الحاسوب الالكترونية بعد أن كانت محمية باعتبارها داخلة ضمن حقوق الملكية الصناعية وأصبحت تعتبر الآن من المصنفات التي تدخل ضمن حقوق الملكية الأدبية والفكرية حسب اتفاقية تربس سنة 1994 الخاصة بالجوانب المتصلة بالتجارة وبالملكية الفكرية .

فبعد أن أصبحت الإنترنت تحتوي في أن واحد على مجموعة جد متنوعة من الأعمال والمؤلفات الفكرية تتراوح بين النصوص والتسجيلات الصوتية والموسيقية والصور الثابتة والمحترمة والأعمال البيانية والرسومية من جهة وبين برامج الحاسوب الآلي و قواعد وبنوك البيانات من جهة أخرى، والأفلام والأعمال السمعية والبصرية ومواقع الويب وبرامج المتصفحة ومحركات البحث وغيرها، باتت الإنترنت فضاء تقع عبره جرائم تنتهك حقوق الملكية الفكرية بصور متعددة، ولعل من أهمها وأبرزها " جريمة التقليد وجريمة القرصنة " سواء في مجال الملكية الصناعية (البراءات، العلامات، الرسوم كذلك النماذج الصناعية) أو ما يخص الملكية الأدبية والفنية.[1]

ونظرا للأثر السلبي لهذه الجرائم، ليس فقط على الفرد وإنما عن الكيانات الاجتماعية وأنظمتها الاقتصادية. سنتناول في هذا المبحث مفهوم جريمتي التقليد والقرصنة لاعتبارهما أهم الاعتداءات التي تقع على الملكية الفكرية باستخدام الإنترنت في المطلب الأول، وفي المطلب الثاني سنعرض فيه صور أخري لجرائم الاعتداء على الملكية الفكرية عبر الإنترنت، أما المطلب الثالث سنتناول فيه أركان جريمة الاعتداء على الملكية الفكرية عبر الإنترنت .

المطلب الأول : مفهوم جريمتي التقليد والقرصنة الفكرية عبر شبكة الإنترنت :

قبل تعريف جريمتي التقليد والقرصنة عبر الإنترنت، يقتضي تحديد معنى التقليد والقرصنة بدقة وذلك بتعريفهما اصطلاحا لإزالة التداخل بينهما.

الفرع الأول :مفهوم جريمة التقليد عبر الإنترنت

الفقرة الأولى : تعريف التقليد من الناحية الفقهية

التقليد هو صنع شي مشابه للشيء الأصلي بطريقة يكون فيها التشابه مخادعا للناس، ويقوم التقليد من خلال أوجه الشبه بين ما هو مقلد و وما هو حقيقي، فجريمة التقليد تشمل عدة صور وأنواع من وأهمها التقليد وهو اعتداء على المصنفات الفكرية والإبداعية من خلال النقل، وهذا ما يطلق عليه بتقليد الملكية الأدبية وكذلك الفنية، كما قد ينطوي هذا الأمر أيضًا على التعدي على حقوق أصحاب العلامات التجارية والصناعية والمخترعين

[1] – حسين محمد الغول ،جرائم شبكة الإنترنت، المرجع السابق ،ص184

من خلال تقليد العلامة التجارية أو التصميم الأصلي، أي إنشاء علامة تجارية أو تصميم أو نموذج مماثل مزيف مشابه في الشكل و الأسلوب. ما يؤدي إلى تضليل الغير المضلل.

وقد اختلف الفقهاء في تعريف التقليد بسبب تنوع موضوعاته وتعقيدها. وقد عرفه البعض أنه "إنشاء شيء جديد أقل قيمة من القديم وأشبه به، بقصد الاستفادة منه.[1]

الفقرة الثانية: تعريف التقليد عبر الإنترنت

إن ما يميز التقليد في ضل التطور التكنولوجي عن جريمة التقليد في جرائم الاعتداء التقليدية هو وقوعه في بيئة الإنترنت. وأيا كانت الوسيلة التي يتم بها الاعتداء فهي انتهاك للحقوق والشخصية الفكرية، وهو سلوك تم تجريمه من طرف كل القوانين على اختلافها .

ولقد عرفت منظمة الويبوا التقليد عبر الإنترنت أو ما يسمى بالنسخ المعلوماتي بأنـــه استنساخ للمصنفات المنشورة أو الفوتوغرافية بطريقة مناسبة من أجل توزيعها على الجمهور بدون أي ترخيص." وبعبارة أخرى هو كل اعتداء بشكل مباشر أو غير مباشر عبر شبكة الإنترنت على مصنفات وابتكارات الغير الواجبة الحماية .

وقد يتم التقليد عبر شبكات الإنترنت عن طريق إزالة أو تعطيل بسوء النية الحماية التقنية التي يستعملها صاحب الحقوق كالتشفير أو غير ذلك بغرض الاعتداء وتقليد المادة المؤلفة أو المبتكرة. إضافة إلى هذا تعد جريمة الاعتداء على الملكية الفكرية عبر الإنترنت كل تقليد لمصنف أو برنامج إذاعي أو تسجيل صوتي أو أي ابتكار يحميه القانون وتم نشره عبر أجهزة الحاسب الآلي وشبكات الإنترنت بدون إذن صاحبها.[2]

ويوجد نوعان من التقليد على شبكة الإنترنت: النوع الأول هو التقليد الإلكتروني المقترف بالكامل على الشبكة، والذي يستهدف الابتكارات اللامادية أو الأنظمة المعلوماتية، أما النوع الثاني، فهو التقليد المقترف بواسطة الشبكة والذي يستهدف المنتجات والبضائع على أنواعها.

---

[1] –claude colombet , propriete litteraire et droit voisins,9eme edition,dalloz,delta, 1999,p194

[2] – حسين محمد الغول ، المرجع السابق، ص 480 .484 . 485

الفرع الثاني : مفهوم جريمة القرصنة الفكرية عبر الإنترنت

قبل تعريف القرصنة الفكرية عبر الإنترنت يتوجب علينا تعريف القرصنة الفكرية من الناحية الفقهية.

الفقرة الأولى : تعريف القرصنة من الناحية الفقهية piratage

القرصنة ظاهرة أطلق عليها هذا المصطلح نظراً لخطورتها وعواقبها السلبية على الإبداع والملكية الفكرية، ويطلق على الشخص الذي يمارس القرصنة في مجال الفكر أيضاً اسم "القرصان". وهو كائن طفيلي يعيش على إبداع الآخرين ومواهبهم واستثماراتهم ويسرق ثمار جهودهم مجانا."

فمفهوم القرصنة يشمل قرصنة المصنفات الأدبية أو الفنية وكذلك المنتجات الصناعيــة والتجارية، ويتضمن أيضًا الوصول غير المصرح به إلى أنظمة كمبيوتر معينة، بما فــي ذلك التزوير والتزييف والانتحال والغش المعلوماتي. وما يهمنا نحن هو القرصنة الفكرية. [1]

الفقرة الثانية: تعريف جريمة القرصنة الفكرية عبر الإنترنت

القرصنة هي سرقة أو توزيع دون تفويض أو ترخيص لمادة تتمتع بحقوق النشر والتأليف أو الاختراع، والقرصنة تتم عبر الإنترنت عن طريق الاستيلاء على تصميم كمبيوتر أو برنامج يتمتع بحق النشر والتأليف ونسخها دون تفويض ،ويتم ذلك مثلا عن طريق تحميلها من جهاز الكمبيوتر باستعمال الإنترنت وإجراء نسخة منها.[2]

ومع ظهور ما يسمى بالتجارة الالكترونية والمواقع الالكترونية المتواجدة عبر الإنترنت لعرض المنتجات والخدمات، ظهر أيضا ما يسمى بالعنوان الالكتروني،[3] الذي يعتبر

---

[1] – Richard Milchir M , Marques et noms de Dmaine de quelques Problemes Actuels , lamydrois commercial n 135 juillet , 2000 bulletin d actualite , p2

[2] – – حسين محمد الغول ، المرجع السابق، ص 188

[3] – تعرف العنوان الالكتروني "بأنه مجرد تحيل او نقل مجموعة من الأرقام في صورة حروف تشكل مصطلحا يتماشى واسم المشروع " و نتقسم العناوين الالكترونية الى عناوين الكترونية دولية ا عامة لا تنتمي الى دولة معينة ومن أمثلتها تلك التي تنتهي بالمقطعorg net " com ، وعناوين الكترونية وطنية تنتهي بحرفين من حروف كل دولة من أمثلتها ، الفرنسية fr والمصرية eg . انضر شريف محمد غنام ، حماية العلامات التجارية عبر الانترنت في علاقتها بالعنوان الالكتروني ، ص4

الوسيلة الأساسية للوصول إلي هذه المواقع عبر الفضاء الكبير للإنترنت. إذ حرصت المشاريع المتواجدة عبر العديد من المواقع اختيار عناوين الكترونية تحمل اسمها أو علامتها التجارية حتى يتم تمييز الموقع الخاص بها عن المواقع الأخرى من الشركات المنافسة ، وعليه أصبح العنوان الالكتروني هدفا للأشخاص الذين يقومون بتسجيل عناوين الكترونية دون أن يمتلكون أي حق أو مصلحة مشروعة لذلك. وهذا السلوك الحديث يشكل نوعا من القرصنة والسطو على حقوق الآخرين باستعمال شبكة الإنترنت، ولعل أهم جرائم القرصنة التي تمس بالملكية الفكرية هي قرصنة العناوين الالكترونية.

ويقصد بالقرصنة أو السطو على العناوين الالكترونية عبر الإنترنت هو أن يقوم شخص ليس لديه أي حقوق على العلامة التجارية ويقوم بتسجيلها على صورة عنوان الكتروني على الإنترنت بهدف الإضرار بالمالك الأصلي لهذه العلامة أو بهدف بيع العنوان الالكتروني للمالك مرة أخرى أو بيعه لأحد منافسيه مقابل استفادة مادية[1].

ولقد تزايدت القرصنة بالنسبة للعناوين الالكترونية خاصة الدولية منها كونها مجال خصب لجذب الأشخاص والمشاريع، مما يساعد على الاعتداء على العلامات التجارية. [2]

ومن أوائل الأحكام القضائية التي صدرت في هذا الشأن الحكم الصادر من محكمة مدينة نانتار الفرنسية عام 2000 إذ جاء في الحكم أن عملية بيع عناوين الكترونية مقلدة لماركات تجارية مشهورة تعد جريمة قرصنة واستوجبت العقاب عليها "[3]

ووفقا لتقرير اللجنة الأمريكية المستقلة لدراسة القرصنة الفكرية، قدرت خسارة الولاية المتحدة الأمريكية جراء هذه الجريمة ما يقارب حوالي 600 مليار دولار سنويا، إضافة إلى هذا لا تزال الملكية الفكرية في الولايات المتحدة تشكل تهديدا خطيرا للاقتصاد الأمريكي وتقدر الخسائر الناجمة عن هذه القرصنة بأكثر من 250 مليار دولار في شكل تزوير

– Richard Milchir M , Marques et noms de Dmaine de quelques Problemes Actuels , lamydrois commercial n 135 juillet , 2000 bulletin d actualite , p2

[1]– Lamy ,Droit de l informatique et des Reseaux /op cit , n 2308 , p 1331

[2]– j Larreu , Protection duneMarqueeRonommee Contre le Cyberpiratage , Expertises, aout, Septembre 1999, p 260

[3]– حسين محمد الغول، المرجع السابق ، ص 512

منتجات وبرامج حاسوب منسوخة وأسرار تجارية مسروقة قد تكلف ما يصل إلى 600 مليار دولار، وهذا بحسب تقرير اللجنة لعام2018 . وذكرت نفس اللجنة أن الصين مازالت هي أكبر مصدر للقرصنة الفكرية في العالم لسياسته الصناعية التي تمنح الأولوية لاكتساب وتطوير الابتكارات العلمية والتكنولوجية. وعلى الرغم من أن الكونجرس الأمريكي وإدارته قد أنشئوا آليات سياسية للسيطرة على القرصنة الملكية، إلا أن العديد من هذه الآليات بعيدة المنال ولا تزال القرصنة أكبر مهدد للاقتصاد.[1]

ونظرًا للتطورات الحالية في تكنولوجيا " الذكاء الاصطناعي"، باتت حقوق الملكية الفكرية التي تولدها الآلات دون تدخل بشري حقيقة واقعة للخبراء القانونيين والهيئات التشريعية والقضاء في الحكومات حول العالم، وهو ما دفع إلى طرح سؤال : مَن يملك حقوق الملكية الفكرية التي لم يصنعها البشر؟

قد استضافت المنظمة الدولية للملكية الفكرية حلقة نقاش حول القضايا الأخلاقية المحيطة بالآلات الذكية والتدابير التنظيمية للتعامل معها وللإجابة على هذا التساؤل.

إن الابتكارات في تكنولوجيا الويب والذكاء الاصطناعي والواقع الافتراضي وتطبيقات المحادثة والبيانات الضخمة والتكنولوجيا ثلاثية الأبعاد قد غير الطريقة التي يعيش بها الناس وقد أثر على الصناعات التقليدية القائمة، والنظام القانوني الحالي غير مجهز بالتشريعات اللازمة للتعامل مع هذه التغييرات حتى الآن. وأشار آخرون إلى أن التغييرات التي نتجت عن هذه التقنيات واسعة النطاق وهائلة، لكنها تفتقر إلى الأطر القانونية والتنظيمية، وقد صرحوا بأن أنه على الرغم من أنه من المستحيل أن تؤدي الثورة الصناعية الرابعة إلى إنشاء ملكية فكرية جديدة، إلا أنه ستكون هناك تغييرات كبيرة في طريقة إدارة الملكية الفكرية[2].

---

[1] – القرصنة الفكرية : مقال منشور على الرابط الأتي:
https://m.annabaa.org/arabic/economicreports/10059 أطلع عليه في 2018/03/05

[2] – القرصنة الفكرية : مقال منشور على الرابط الاتي : أطلع عليه في 2018/03/05.
https://m.annabaa.org/arabic/economicreports/10059

المطلب الثاني : أنواع أخرى من التعدي وانتهاك حق الملكية الفكرية في شبكة الإنترنت والصعوبات التي تواجه صاحب حق المؤلف على الشبكة

في هذا المطلب سنتناول أنواع أخرى من التعدي وانتهاك حق الملكية الفكرية في شبكة الإنترنت، وبعدها سنتطرق إلى الصعوبات التي يواجهها صاحب حقوق الطبع والنشر على الإنترنت.

الفرع الأول: أنواع أخرى من التعدي وانتهاك حق الملكية الفكرية في شبكة الإنترنت

يمكن التطرق إلى أنواع التعدي في النقاط التالية :

أولا–التحايل الذي يعزز وييسر الوصول إلى العمل المحمي. والتعدي يدخل ضمنه القرصنة والاختراق المباشر والتخريب لدور النشر الرقمية والمواقع الالكترونية، ولأعمال المؤلفين الأصلية، وهو ما ينجر عنه انتهاك للحقوق الأدبية والمالية للمؤلف، في صورة تحميل أو نسخ ...الخ.

ثانيا– إنشاء وتعزيز برامج للتحايل على المعايير الفنية لحماية الأعمال المحمية بحقوق النشر: وهو بيع وتطوير وتبادل الأدوات والبرامج المضادة، التي تعمل على تسهيل الوصول إلى عمل محمي وقرصنة حقوق النشر في شبكة تم حمايتها وفقا للمعايير التقنية.

ثالثا– الاستعمال السيئ : ويتضمن ذلك ما يقوم به المستخدمين من جميع الفئات حيث غالبًا ما يتم عرض الكتب والملفات المحمية وتنزيلها وتثبيتها على الحواسيب ومشاركتها مع الأصدقاء حتى لو كانت القصد من ذلك هو مشاركة المعلومات للأغراض معرفية فإنه يتسبب في ضرر مادي ومعنوي للمؤلف، وتنتهك حقوقه المحمية قانونًا ، ويتم التشجع على مثل هذه الأعمال غير القانونية.

ومن بين أشكال الاعتداءات عبر الإنترنت نذكر:

– نشر المصنف دون إذن المؤلف:

وهو نشر مصنف أصلي أو جزء منه سابق الوجود بطريقة مباشرة في دور النشر عبر الإنترنت. وهذا ما واجهه القضاء الفرنسي في قضية دامت لسنوات، وهي قضية أحد الشركات الكندية والتي تحمل إسم "ميكروفور"والتي كانت تنشئ قاعدة بيانات إخبارية بما في ذلك الأخبار الفرنسية، الأمر الذي يمكن للقارئ من قراءة المقالات المنشورة في الجرائد

الفرنسية والتي تدخل ضمنها لوموند. وأنتجت هذه الشركة مؤشرا شهريا وأخر سنوي يصدر نهاية السنة. وأطلقت عليه اسم أخبار فرنسا، ويتكون من قسمين الأول تحليلي مع كلمات منفصلة تشير إلى محتوى المقال، والثاني تاريخي يجمع المعلومات الببليوغرافية لكل مقال مع تحديد المجلة التي نشرتها إضافة إلى ملخصا موجزا يشرح القصة أو الحدث، والإشكال ظهر في الوقت الذي أرسلت فيه الشركة رسالة إلى المكتبة الوطنية بفرنسا تطلب منها المشاركة في هذا الفهرس، واعتبرت جريدة لوموند أن هذا العمل تعديا على حقوقها بصفتها مالك حقوق النشر لجميع مقالاتها المنشورة في مجلتها. [1]

– النسخ الالكتروني :

في قضية المغني جاك برال قضت المحكمة في هذه الدعوى التي كانت فيها التهمة ببث ونشر مصنف على مواقع النت دون ترخيص .

وتتمثل وقائع القضية في أن طالبين من طلاب المدرسة العليا للاتصالات بفرنسا قد قاما ببث أغاني لـ Jaques Brel على موقعهما الشخصي عبر شبكة الإنترنت ونتيجة لذلك مُنِح مستخدمو الإنترنت الفرصة لنسخ العمل المحمي بحقوق الطبع والنشر دون إذن المؤلف، وقضت المحكمة بإدانة الجاني بتهمة نشر العمل المحمي بحقوق الطبع والنشر رقميًا عبر الإنترنت بدون موافقة صاحب البلاغ [2].

وحسب اتفاقية الويبو، المعتمدة عام 1996، التي تحمل عنوان البيانات المتفق عليه بشأن المادة 4/1 ووفقاً لأحكام المادة 9 من اتفاقية برن، فإن حق الاستنساخ" ينطبق بالكامل في البيئة الرقمية خاصة الانتفاع بالمصنفات في شكل رقمي". ومن المفترض أن تخزين المصنف الرقمي على وسيط إلكتروني يعد نسخا.

– قرصنة المواقع العالمية :

موقع الويب قد يصبح جديرا بالحماية طبقاً للقانون باعتباره من مصنفا أدبيا أو لما يحتويه من تسجيلات صوتية. إضافة إلى هذا ما يحتويه الموقع من عدد كبير للحقوق

[1] – أنواع التعدي على حقوق المؤلف، مقال منشور على الموقع التالي: https://riadrobinho/blogspot.com

[2] – النشر العلمي الالكتروني في الجزائر ، مقال منشور على الموقع التالي: https://journals/ju.edu.jo

المجاورة وحقوق المؤلف من نصوص مكتوبة تعد مؤلفات أدبية، ورسومات أو تصميمات تعد هي الأخرى مصنفات فنية، وكذلك إذا كان الموقع يحتوي على ملفات موسيقية. حيث كثيرا ما تتعرض كل هذه الأعمال للقرصنة والتخريب من قبل الهاكر.

أيضا يعد توزيع الأغاني ونشرها عبر شبكة الإنترنت دون إذن اعتداء على مصنف محمي .

وهنا يمكننا أن نتذكر قيام الشركة المعروفة باسم "نابستر". والتي تمتلك موقعًا على شبكة الإنترنت بتوزيع تطبيق يسهل العثور على ملفات موسيقى MP3 على الإنترنت. أتاحت هذه الشركة تقديم برامج كمبيوتر تسمح لمستخدمي الإنترنت بنسخ برامجهم الموسيقية.

وقد تمكن ما يقدر بنحو 300000 شخص حول العالم من تنزيل أغاني فرقة شهيرة مجانًا من خلال نابستر، ولكن تمت مقاضاتهم لاحقًا.[1]

- قرصنة الكتب :

نشرت جريدة الشرق الأوسط في لندن مقالاً بعنوان "قرصنة الكتب والبث المباشر للقراءة الإلكترونية وألبومات الموسيقى ، مشكلة تؤثر على ناشرين على الإنترنت". وتتزايد قرصنة الكتب مع زيادة شعبية القراءة الإلكترونية التي تقدم تنزيلات مخفضة التكلفة للكتب الإلكترونية. وأصبح بعض الكتب متوافرة حتى قبل نشرها بطريقة رسمية، وقد أنشأت رابطة الناشرين البريطانيين صفحة حيث يمكن للمؤلفين الإبلاغ عن مواقع الويب غير القانونية. وتلقى موقع الشركة على الويب 831 إشعارًا بالانتهاك ، و 2194 إشعارًا بإلغاء الموقع، وما يقرب من 32000 أمر إغلاق عام 2011.[2]

- الرقمنة دون علم المؤلف :

تمثل رقمنة المصنف بغرض نشره على الإنترنت تهديد حقيقيا ماس بحقوق المؤلف الأدبية، لأنها لا تقدم تمثيلا صادقا للعمل الأصلي لأنه يتطلب الترتيب والمعالجة والتعديل التي قد تمس بصورة المصنف الأصلية.

---

[1] – القضاء يوقف نشاط نابستر، مقال منشور على الموقع التالي: https:/www.al-jazirah.com

[2] – أنواع التعدي على حقوق المؤلف في بيئة الانترنت على الرابط التالي :http://riadrobinho.blogspot.com

- استغلال مزايا التفاعلية وانتهاك الحقوق عبر الانترنت:

إن الخطر الرئيسي الذي يتعرض له المصنف في بيئة الإنترنت يعود إلى ما يسمى بالتفاعل، وهو أحد أهم خصائص الترقيم، وهو على سبيل المثال يتعارض مع كرامة العمل الذي ينتهك الحقوق الأدبية، أو تحويل مسرحية إلى فيلم روائي طويل أو العكس، أو تحويل رواية إلى مسرحية. علاوة على ذلك فإن الخلط بين الأعمال الفنية والأدبية يطرح مشكلة ملكية المصنف أو العمل الناتج عن الاختلاط أو التفاعل بين العديد من المبدعين.[1]

الفرع الثاني : الصعوبات المواجهة لأصحاب حقوق التأليف والنشر على الإنترنت

- وجود انتهاكات عديدة على الحقوق الموجودة عبر الإنترنت من خلال نشرها أو نسخها الالكتروني بدون إذن مالكها .

- اختلاف السلطات التي تتعامل مع حالات انتهاك حق المؤلف والحقوق المجاورة.

- كثرة النصوص القانونية المتعلقة بحالات العمل الغير شرعي والاختلافات بينها بالنظر إلى الدول التي حدث فيها هذا العمل من خلال الاستغلال أو النشر أو إعادة النشر بدون إذن أو ترخيص من أصحاب حقوق التأليف والنشر أو أصحاب الحقوق المجاورة.

- تعدد الاعتداءات، كأعمال النشر والنسخ والتوزيع بدون إذن من صاحب الحق على أجهزة الكترونية متفرقة لأشخاص أجانب على بعضهم البعض لا يجمعهم سوى استخدامهم للإنترنت.

- إذا أراد مالكو حقوق الطبع والنشر مقاضاة منتهكي حقوق النشر، فعليهم مقاضاة أشخاص في بلدان مختلفة، وهنا يكون بصدد مواجهة مشاكل تعدد القوانين المعمول بها، بالإضافة إلى مشكلة الاختصاص وارتفاع تكاليف التقاضي مما يمنع صاحب الحق من المطالبة بحقه.

المطلب الثالث : أركان جريمتي التقليد والقرصنة الفكرية عبر الإنترنت

لقد فرضت التقنيات التكنولوجية نفسها على حقوق المؤلف بما توفره من وسائل إلكترونية تسمح ببروز أشكال جديدة للتعبير، غير أن ما حدث هو العكس حيث تنامت

[1] – أنواع التعدي على حقوق المؤلف في بيئة الانترنت انظر الموقع نفسه

وتنوعت الاعتداءات الحاصلة على هذه الحقوق وهو ما يعرف بجرائم الاعتداء على الملكية الفكرية عبر الانترنت أو العالم الافتراضي، وبالرجوع إلى المشرع الجزائري فإنه لم يحدد أركان هذه الجرائم بل ترك ذلك للقواعد العامة إلا أن ما يميزها هو وقوعها في بيئة الإنترنت.

الفرع الأول: الركن المادي

إن الركن المادي لجريمتي القرصنة والتقليد باستخدام الإنترنت يتوافر بالتثبيت المادي لبرامج الحاسب الآلي ونسخه بأي طريقة باستخدام شبكة الإنترنت التي تتيح نقلها المباشر أو غير المباشر للجمهور، ويتم ذلك من خلال التصوير أو التسجيل أو التحميل أو التثبيت على اسطوانات أو بأي طريقة أخرى. وعملية التثبيت هي جوهر الركن المادي للجريمة، حيث أن الجاني يقوم بالاستيلاء على البرامج باستخدام الإنترنت وتثبيتها سواء في ذاكرة الحاسب الآلي أو بطاقات ذاكرة وإعادة توزيعها أو بثها واستغلالها سواء بمقابل أو غير مقابل، ولمصطلح القرصنة مفهوم أوسع بحيث يشمل عدة جرائم منها التقليد وسرقة البرامج والنسخ المباشر للبرامج والاعتداء على العناوين الالكترونية.

فاصطناع علامة تجارية أو نموذجا صناعيا أو رسما أو اختراعا مطابق للأصل يشكل تقليدا، ويعاقب المشرع عملية الإنتاج بغض النظر عن عملية الاستهلاك. وفي مجال الملكية الأدبية والفنية، يعتبر مقلدا كل من ابتكر أو عرض أو نقل مصنفاً فكرياً غير مشروع، وهذا الاعتداء يمس بحق المؤلف وصاحب الحقوق المجاورة في عرض مصنفاته، وذلك عن طريق الكشف غير المشروع والترجمة بدون رخصة والمساس بسلامة المنصف أو الأداء ونشر المصنف بدون علم صاحبه وذلك طبقا للمادة 251 من الأمر 03 -05 المتعلق بحق المؤلف والحقوق المجاورة الصادر بتاريخ 2003/07/19.

الفرع الثاني: الركن المعنوي

بالإضافة إلى توافر العناصر المسيئة للمصنف المحمي، يجب أن تكون هناك نية لارتكاب الجريمة، وعلى اعتبار جريمة التقليد عبر الإنترنت من الجرائم العمدية يشترط لتحققها أن يكون الناسخ أو المقلد قد ارتكب فعلاً غير مشروع على المصنف محمي قانونا، مع علمه بذلك، فضلاً عن اتجاه إرادته ضد الجهة التي يستهدفها، وإضافة إلى القصد

الجنائي العام لابد من توافر القصد الخاص وهو قصد استغلال البرنامج أو المصنف الذي تم الاعتداء عليه بقصد الاستفادة من بيعه أو عرضه أو غير ذلك من أنواع الاستغلال[1].

وفي الأخير تتنوع وسائل استغلال عناصر الملكية الفكرية بتنوع هذه العناصر، فالملكية الفكرية تتشكل من عنصرين رئيسين هما حق المؤلف والحقوق المتصلة به أو المجاورة له أولا، وحقوق الملكية الصناعية ثانيا.

أولا: وسائل استغلال حق المؤلف والحقوق المتصلة به رقميا: حتى نستطيع تحديد هذه الوسائل على وجه التحديد، فإنه يلزمنا معرفة ما هي العناصر أو المصنفات التي تدخل تحت مفهوم حق المؤلف والحقوق المتصلة به، كالمصنفات الأدبية من روايات وقصائد ومسرحيات، والمصنفات المرجعية كالصحف والأفلام والمقطوعات الموسيقية وتصميمات الرقص وقواعد البيانات وبرامج الكمبيوتر والأعمال الفنية مثل اللوحات والمنحوتات والرسومات، كذلك المصنفات الهندسية كالخرائط والرسوم الفنية، الموجودة جميعها على الصورة الرقمية سواء على أجهزة الكمبيوتر أو المنشورة عبر شبكة الانترنت .

أما الحقوق المجاورة أو المتصلة بحق المؤلف فتتشكل من حقوق فناني الأداء كالممثلين والموسيقيين، وحقوق منتجي التسجيلات الصوتية والحقوق الإذاعية في برامجها ودور النشر في منشوراتها، والموجودة أيضا بالصورة الرقمية أو الالكترونية. لذا فإن عملية النشر الالكتروني لأي من هذه العناصر أو المصنفات دون إذن صاحب الحق فيها أو ادعاء الحق بها يعد أحد أساليب استغلال الملكية الفكرية، كما أن نسخ هذه العناصر والتعديل عليها سواء من جهاز كمبيوتر إلى آخر أو من قرص مدمج إلى جهاز كمبيوتر أو أي قرص مدمج آخر أو تنزيل أية مصنفات رقمية من خلال الانترنت لأي جهاز كمبيوتر أو قرص مدمج أو أية وسيلة رقمية أخرى، أو طباعة هذه المصنفات جميعا دون إذن صاحب الحق فيها، يعد أحد أهم وسائل استغلال الملكية الفكرية بصورة غير قانونية. كما تعد عملية إعادة توزيع هذه المصنفات الرقمية سواء عبر الانترنت أو بأية وسيلة أخرى رقمية أو غير رقمية لأشخاص آخرين أو جهات أخرى انتهاكا لحقوق الملكية الفكرية لهذه المصنفات الرقمية المحمية .

[1]–حنان ريحان، المرجع السابق، ص 188

ثانيا: وسائل استغلال الملكية الصناعية: إن الملكية الصناعية تتضمن براءات الاختراع، والعلامات التجارية والنماذج الصناعية والأسماء التجارية وأسماء المواقع الالكترونية وعناوينها. بالتالي فإن القيام بنشر أي من عناصر الملكية الفكرية المذكورة بصورة رقمية أو نسخها أو تقليدها أو استخدامها دون إذن من صاحبها أو ادعاء الحق بها أو استخدام اسم أو عنوان موقع الكتروني مطابق لاسم أو عنوان محمي أو استخدام اسم أو عنوان مشابه جدا لاسم أو عنوان الكتروني محمي بصورة تثير اللبس كل هذه تعد صورا ووسائل لاستغلال غير قانوني لعناصر الملكية الصناعية .

الفصل الثالث

العدوان الإجرامي عبر الإنترنت الماس بأمن الدول

تشكل الجرائم التي تمس بأمن الدولة مجموعة الجرائم الماسة بشكل مباشر بأراضي الدولة وبسيادتها وسلامة مواطنيها، أو تنال من نظام الحكم فيها.

فبظهور شبكة الإنترنت التي تعد من أحدث إنجازات هذا العصر، ازداد وجه الجرائم الماسة بأمن الدول قبحاً وخطورة وانتشارا عما كان عليه في الماضي، وتسبب في سقوط وانهيار عدة دول بمكوناتها الاجتماعية والسياسية والاقتصادية، وإعاقة تطورها وجعلتها تغرق في فتنٍ وابتلاءات عمياء يصعب الخروج منها.

ولخطورة وبشاعة هذا النوع من الجرائم، ولأن سلامة وهيبة الدولة مرتبطة بسلامة أفراد المجتمع حرصت كافة القوانين الوضعية على تجريم مختلف صور الجرائم المخلة بأمن الدولة سواء في صوره التقليدية أو المستحدثة.

ونظرا لتعدد الجرائم في هذا الباب اخترنا الجرائم الماسة بأمن الدول عبر الإنترنت الأكثر خطورة والأكثر شيوعا، ولتوضيحها بصورة وافية سأقسم هدا الفصل إلى ثلاثة مباحث كما يأتي:

المبحث الأول: جريمة الإرهاب عبر الإنترنت

المبحث الثاني: جريمة غسيل الأموال عبر الإنترنت

المبحث الثالث : جريمة التجسس باستخدام الإنترنت

المبحث الأول: جريمة الإرهاب عبر الإنترنت

يعد الإرهاب ظاهرة إجرامية خطيرة ومدمرة، وتتجلى خطورة الإرهاب من خلال الأفكار والمعتقدات الهدامة للإرهابيين وفي اعتقادهم بأن أفكارهم دائما هي الصائبة وأن باقي الأفكار ضالة وغير صحيحة، أضف إلي هذا زعمهم امتلاك مشروع دولة متكامل من كافة النواحي، وفي سبيل تحقيق هذه الدولة نجدهم يسعون جاهدين لنشر أفكارهم ومعتقداتهم حتى ولو تطلب الأمر ارتكاب أعمال إجرامية وحشية مادامت تؤدي إلى تحقيق بناء دولتهم المنشودة، ولقد تسببت الأعمال الإرهابية عبر العالم في حجم كبير من الدمار والخراب وعملت على نشر حالة من الخوف والذعر بين الناس فضلا عما خلفته من خسائر بشرية ومادية هائلة.[1] وأحسن مثال ما شهدته الجزائر من معاناة من هذه الظاهرة مع بداية التسعينات أين ظهر خلالها الإرهاب بشكل واضح وعرض مصالح الدولة الكبرى للخطر، وسقط بسببه الآلاف من الضحايا والشهداء.

وباكتشاف شبكة الإنترنت سارعت الجماعات الإرهابية إلى استخدام التقنيات الحديثة والخدمات المتوفرة عبرها، مما أدي إلى ظهور نوع جديد من الإرهاب على الساحة، ويعتبر من أصعب أنواع الإرهاب لما يحمله من مخاطر تجاوزت أضرار قنبلة على جانب الطريق أو طرد مفخخ في منطقة مزدحمة. وهذا النوع من الإرهاب يطلق عليه الإرهاب السيبراني أو الالكتروني.

لقد ظهر مصطلح الإرهاب الشبكي أو الرقمي عندما اعتمدت الجماعات الإرهابية ممارسة إرهابها عبر الإنترنت و صار هذا النوع من الإرهاب هو السائد، حيث يمارس من خلال شبكة الإنترنت العديد من صور الإرهاب ، إذ قام بإنشاء عدة مواقع على الإنترنت من طرف جماعات إرهابية لممارسة أنشطتهم المختلفة عبرها، كإقناع الشباب عبر الإنترنت بفكرهم المتطرف وأفكارهم الإرهابية الهدامة وغسل عقولهم لتجنيدهم وحثهم على الالتحاق بصفوفها سواء كانوا ذكورا أو إناثا، أيضا من أجل التحريض على القتل أو

---

[1] كريم مزعل شبي، مفهوم الإرهاب دراسة في القانون الدولي و الداخلي ، مجلة أهل البيت ، كربلاء ، العدد 2، 2005 ص30

العنف، وإتلاف الممتلكات والأموال العامة، ولتعليم صناعة القنابل والمتفجرات اليدوية أو كيفية تفجيرها ...الخ.[1]

وتمثل الهجمات الإلكترونية من أكثر التهديدات انتشارا في الوقت الحديث [2]. ولقد تضاعف عدد تلك الهجمات واختلفت أشكالها بالمقارنة مع الأعوام الفارطة.

ولأن جرائم الإرهاب من أخطر الجرائم المرتكبة عبر الإنترنت في وقتنا الحاضر لكونها جرائم تهدد حياة الناس وسلامة أوطانهم في آن واحد، سنتناول دراستها من خلال تقسيم هدا المبحث إلى مطلب أول نتناول فيه مفهوم الإرهاب عبر الإنترنت، والمطلب الثاني : خصائص وأهداف الإرهاب عبر الإنترنت والمطلب الثالث: وسائل وأنواع الإرهاب عبر الإنترنت والمطلب الرابع : أركان الإرهاب عبر الإنترنت.

المطلب الأول : مفهوم الإرهاب عبر الإنترنت

قبل تعريف الإرهاب عبر الانترنت لابد من التطرق إلى تعريف الإرهاب عموما.

الفرع الأول :التعريف اللغوي والفقهي والقانوني للإرهاب

الفقرة الأولى: التعريف اللغوي

أَرْهَبَ فهو فعل يحمل عدة معاني نذكر منها : أرهبَ يُرهب، إرهابًا، وأرهب فلانًا : خوَّفه وأفزعه. ومصطلح إرهاب يعني مجموع أعمال العنف التي تقوم بها منظّمة أو أفراد قصد الإخلال بأمن الدَّولة. [3]

الفقرة الثانية : التعريف الفقهي والقانوني للإرهاب

عرف الفقيه wardlaw الإرهاب على أنه "استخدام القوة أو التهديد من قبل شخص أو مجموعة تعمل مع أو ضد السلطة القائمة، عندما يكون الغرض من هذا العمل هو خلق مخاوف جدية بين مجموعة مسؤولة عن الأسباب المباشرة للإرهاب، وإجبار تلك المجموعة على الالتزام بالمطالب السياسية لمرتكبي أعمال إرهابية"[4].

---

[1] – المري بهاء، جرائم المحمول والإنترنت ، منشاة المعارف ، الإسكندرية ، سنة 2017، ص 24

[2] – – الموقع الإلكتروني : https://www.un.org/ar/un75/new-era-conflict-and-violence

[3]– معجم المعاني الجامع الإلكتروني على العنوان الإلكتروني (http://www.almaany.com/ar/dict/ar-ar)

أما من الناحية القانونية لقد عرف الإرهاب من طرف هيئة الأمم المتحدة بأنه "أعمال العنف التي تمارسها الدول ضد شعوب بأكملها للسيطرة عليها أو التدخل في شؤونها الداخلية باستخدام القوة المسلحة، وهو سلسلة من أعمال الانتقام أو الدفاع الوقائي التي تمارسها دولة ما ضد سيادة دولة أخرى. وإن دفع الجماعات الإرهابية إلى أراضي الدولة يهدف إلى بث الرعب والذعر بين المواطنين وإشعال النظام السياسي، وكلها أمور يجب أن تدخل في نطاق تعريف الإرهاب لجسامتها و خطورتها.[1]

الفرع الثاني : تعريف الإرهاب عبر الإنترنت

يعرفه بعض الفقهاء على أنه " كل نشاط يقوم به شخص بمفرده أو مجموعة منظمة تنفيذا لمشروع إرهابي باستخدام مختلف الوسائل المتوفرة عبر الإنترنت من شأنها توقيع ضرر أو تعريض مصلحة يحميها القانون ." [2]

أما من المنظور الإسلامي فقد عرف الإرهاب عبر الإنترنت على أنه " الترويع الحسي أو المعنوي المقصود للأمن باستخدام الوسائل الالكترونية الحديثة بغرض تحقيق أهداف تتنافى ومقاصد الدين الإسلامي ."[3] ومن هذا المنظور يشمل الإرهاب عبر الانترنت كل ترهيب أو تخويف عن قصد يلحق بالضحية ضررا ماديا أو معنويا سواء صدر من فرد أو جماعة أو دولة، وذلك لتحقيق أهداف غير شرعية كتضليل الناس عن حقيقة الدين الإسلامي، وسفك الدماء وانتهاك الأعراض وإتلاف الأموال سواء الخاصة أو العامـــة إلى غير ذلك من أعمال تخريب وفساد شملت العالم بأكمله .[4]

---

[4] – عبد القادر زهير النفوري، المفهوم القانوني لجرائم الإرهاب الداخلي والدولي، ط1 ،منشورات الحلبي الحقوقية للنشر، سورية، سنة 2008 ،ص20.

[1] هيثم فاتح شهاب، جريمة الإرهاب وسبل مكافحتها في التشريعات الجزائية المقارنة، ط1 ، دار الثقافة للنشر والتوزيع، الأردن ، 2010. ص38 –37

[2]– زين العابدين عواد ، جرائم الإرهاب المعلوماتي دراسة مقارنة ،المرجع السابق ، ص 85

[3]– أحمد مداح ، الجريمة الالكترونية في الفقه الجنائي الإسلامي ، أطروحة دكتوراه جامعة الحاج لخضر باتنة كلية العلوم الإنسانية والعلوم الإنسانية –قسم العلوم الإسلامية ، السنة الجامعية 2014–2015 ، ص 411

[4]– أحمد مداح ، المرجع السابق ، ص 411

وبالتالي فإن الغرض من الإرهاب السيبراني هو استخدام القوة وأشكال مختلفة من العنف ضد الأشخاص أو الممتلكات العامة من أجل ترهيب الأفراد والحكومات لتحقيق أهداف سياسية أو اجتماعية أو شخصية، إضافة إلى عدة أهداف أهمها:

1- الرغبة في الشهرة والظهور للعلن، فهناك بعض الأشخاص يرون أن وجودهم ليس له أي هدف فيصاب بحالة من السخط على الناس، فيتجه إلى العدوان والتخريب والتدمير لإثبات وجوده .

2- الرغبة في تحقيق أهداف أو رغبات معينة أو الوصول إلى منصب مرغوب فيه، فيلجأ إلى المواقع المتخصصة في تجنيد الإرهابيين لتحقيق غرضه.

3 عدم وجود دور للإنسان في الأسرة والمجتمع. والشعور بالفشل الاكتئاب يؤدي إلى الانحراف واكتساب الخصائص السلبية، والشعور بعدم الانتماء للوطن، كل هذه الأمور تجعل منه فريسة سهلة للتنظيمات الإرهابية.

7- الافتقاد للرقابة الأسرية والذاتية، الأمر الذي مهد الطريق أمام الجماعات الإرهابية لترويج خطاباتهم التكفيرية، وما ساهم في رواج خطاباتهم المنتشرة عبر الإنترنت هو أنه في كل أحاديثهم تبين عملهم وفقا لمبادئ يمكن للجميع إتباعها والاتفاق عليها، أهمها نصرة المظلوم ومحاربة الفساد والفاسدين.[1] إن الوجود النشط للإرهابيين عبر الإنترنت متقطع ومراوغ ويتخذ أشكال متنوعة، فقد يظهر موقع إرهابي وسرعان ما يختفي ويظهر بشكل جديد وعنوان جديد في فترة وجيزة، فالمنظمات الإرهابية عبر مواقعها الإلكترونية لا تستهدف مؤيديها وممولها فقط بل تستهدف أيضا وسائل الإعلام والرأي العام والمجتمعات التي ترهبهم وتخيفهم، وتهدف هذه الحملات إلى شن حرب نفسية ضد الدول المعادية، خاصة بنشر فيديوهات وصور بشعة لإعدام رهائن وسجناء، بينما يدعون في الوقت نفسه أنهم يقومون بعمل نبيل وأنهم يدافعون على قضايا مصيرية، ويشكون المعاملة السيئة من طرف الآخرين. [2]

---

[1]-حسن علي كاظم ، لتطرف والإرهاب الفكري عبر الإنترنت ومواقع التواصل، مجلة رابطة أمناء الشام ، العدد750، 2014

[2] - ايهاب شوقى، الارهاب الالكترونى وجرائمه، شبكة الأخبار العربية أطلع عليه في 2015/12/07

ومن هم المواقع العربية التي استغلت لأهداف إرهابية ما يأتي :

- موقع النداء: وهو موقع تنظيم القاعدة الرسمي عقب هجمات 11 سبتمبر في الولايات المتحدة، والذي يتم عبره نشر البيانات الإعلامية الخاصة بالتنظيم.

- صوت الجهاد: ويصدرها تنظيم القاعدة وتتضمن حوارات القادة فيما بينهم وأهم البيانات التي يصدرونها.

- موقع البتار: تصدر هي الأخرى عن تنظيم القاعدة، وهي عبارة عن مجلة عسكرية إليكترونية مختصة بالمعلومات العسكرية والتجنيد[1].

المطلب الثاني :أسباب جرائم الإرهاب عبر الإنترنت

تعددت الأسباب التي دفعت بالأشخاص إلى ارتكاب جرائم إرهابية منها أسباب سياسية وأسباب إيديولوجية وأسباب اقتصادية واجتماعية وحتى أسباب شخصية إلى غير ذلك من الأسباب والتي يمكن إيجاز أهمها من خلال ما يلي:

الفرع الأول: الأسباب السياسة والأيديولوجية

الفقرة الأولى: الأسباب السياسية

إن للإرهاب عبر الإنترنت علاقة وطيدة بالأوضاع السياسية داخل الدولة خاصة إذا كانت حكام هذه الدولة من الطغاة الذين يريدون البقاء على عروشهم متسلطين، وفي سبيل ذلك يلجئون إلى استعمال العنف للحفاظ على حكمهم وفي المقابل يرد الشعب بنفس أعمال العنف، وعليه يعد الاعتداء على حقوق الأفراد دافعا من دوافع ظهور الإرهاب المعلوماتي باعتباره وسيلة لاسترجاع الحقوق والحريات المفقودة .[2]

---

http://www.anntv.tv.news

[1] – ايهاب شوقى، الارهاب الالكترونى وجرائمه، شبكة الأخبار العربية أطلع عليه في 2015/12/07 http://www.anntv.tv.news

[2] حسنين المحمدي بادي ، حقوق الإنسان بين مطرقة الإرهاب وسندان الغرب ، دار الفكر الجامعي ، الاسكندرية ، 2004، ص64

الفقرة الثانية :الأسباب الإيديولوجية

إن اختلاف الأيديولوجيات لدى الكيانات السياسية سواء في السلطة أو خارجها قد يؤدي إلى صراع بينهم، حيث يعمل كل كيان على فرض أفكاره على الساحة السياسية بأساليب مختلفة بما في ذلك مختلف الجرائم الإرهابية باستعمال شبكة الانترنت خاصة إذا كان هذا الكيان خارج السلطة وممنوعا من الدخول إلى الحياة السياسية، وعليه ينشأ الصراع بين مؤيدي الأيديولوجيات المتنوعة، ويسعى كل صاحب أيديولوجية الوصول إلى السلطة بكل الطرق الممكنة لتطبيقها. فالإيديولوجيات المتباينة تعد أهم أسباب الإرهاب المعلوماتي خاصة إذا كان هم أصحابها الوحيد هو الاستيلاء على السلطة دون وضع الحلول الواقعية الملموسة لمشكلات الدولة، فذلك حتما سيؤدي إلى استفحال الجرائم الإرهابية أكثر وأكثر.[1]

الفرع الثاني : الأسباب الاجتماعية والاقتصادية

الفقرة الثانية : الأسباب الاجتماعية

إن السلوك الإرهابي سلوك ناتج عن تفاعل عدة عوامل، وتعد العوامل الاجتماعية من أهم هذه العوامل، فالعوامل الاجتماعية كثيرة ومتنوعة، و لعل أهم عامل للتأثير على الفرد هي البيئة المحيطة به والمتمثلة في الأسرة المدرسة والعمل، فكما قد يكون لها التأثير الإيجابي على الفرد قد يكون لها التأثير السلبي، خاصة إذا كانت البيئة التي يعيش فيها غير صالحة.

فغياب القيم الاجتماعية يؤدى إلى نجاح التنظيمات الإرهابية في تجنيد الأفراد، من خلال إدخال القيم الاجتماعية التي تتنافى مع قيم كافة المجتمعات، ولكنها تتوافق مع المعتقدات والقيم الخاصة بالمنظمة، وتجعل الفرد يتأثر بها ويؤمن بها لدرجة أنه يمكنه التضحية بروحه للحفاظ على هذه القيم والمعتقدات.[2]

---

[1]– عصام عبد الفتاح ، الجريمة الإرهابية ، دار الجامعة الجديدة، الإسكندرية، 2008 ،ص32

[2] – مجدي الداغر، دور الإعلام الجديد فى تشكيل معارف واتجاهات الشباب الجامعي نحو ظاهرة الإرهاب على شبكة الإنترنت: دراسة ميدانية، مجلة الآداب والعلوم الاجتماعية، العدد 36، الكويت، 2016، ص88:89.

الفقرة الأولى : الأسباب الاقتصادية

إن جرائم الإرهاب عبر الإنترنت كمثلها من الجرائم ما هي إلا إفرازات لتدهور الأوضاع خاصة الاقتصادية منها، ولقد ثبت أن الظاهرة الإجرامية مرتبطة ارتباطا كبيرا بالنظام الاقتصادي، والتأثيرات السلبية للأنظمة الاقتصادية يمكن أن تنعكس بالسلب على السلوك الإنساني بما فيه السلوك الإجرامي. فتردي الأوضاع الاقتصادية وتردي الحالة المعيشية يولد انتشار ظواهر سيئة كالفقر والبطالة المؤدية بدورها إلى انتشار الكره الحقد بين الأفراد وهذا ما قد يدفعهم في اغلب الأحيان إلي ارتكاب أفعال غير مشروعة بما في ذلك إتباع الطريق الإرهابي .[1]

المطلب الثاني : وسائل الإرهاب عبر الإنترنت

تعتمد الجماعات الإرهابية على الإنترنت للدعاية والتشجيع على العنف ولترويج خطاباتهم المتطرفة وللتجنيد والتدريب والتحريض على الأعمال الإرهابية، أضف إلى ذلك تقوم الجماعات الإرهابية عبر الإنترنت بتمويل أعضاءها عن طريق خدمات الدفع.

كما يستخدمون كافة الأدوات المتوفرة في المجال الإلكتروني مثل البريد الإلكتروني ووسائل الاتصال المختلفة والمواقع الإلكترونية ومواقع التواصل الاجتماعي وغرف الدردشة، للقيام ببعض الأنشطة الإرهابية كالاتصال والتدريب ونشر المعلومات والتهديدات التي تحتوي على الترهيب والتخويف. كما يستخدمون العديد من وسائل التدمير والتفجير في المجال الإلكتروني، مثل وزرع الفيروسات والقنابل الإلكترونية وأحصنة طروادة وغيرها. وفي هذا المطلب سنعرض أهم الوسائل المتاحة عبر الإنترنت والمستخدمة من طرف المنظمات الإرهابية

الفرع الأول : شبكات التواصل الاجتماعي

مع الزيادة الفائقة في استخدام وسائل التواصل الاجتماعي من طرف جميع فئات وطبقات المجتمع، استغلت المنظمات الإرهابية هذا الاستخدام للترويج لأفكارها الهدامة، وعليه بات من المهم التركيز على دور المواقع الإرهابية في تجنيد الشباب والشابات

[1]– عصام عبد الفتاح ،المرجع نفسه، ص 27

واستدراجهم لتنفيذ مبتغاهم[1]. حيث استخدمت الجماعات الإرهابية الخدمات المتوفرة عبر شبكة الإنترنت خاصة تويتر وفايسبوك كوسيلة لنشر أفكارهم التكفيرية واستقطاب الشباب والشابات للحاق بصفوفهم، والقتال إلى جانبهم[2].

ومن أهم المنظمات الإرهابية تنظيم الدولة الإسلامية داعش المعروف عالميا، والذي قام بتنظيم صفوفه ميدانيا وعسكريا، بالإضافة إلى شنه لحرب عبر مواقعه الإعلامية، باستخدامه لأفضل الوسائل التكنولوجية[3]. فهو لم يتوانى عن استخدام الإنترنت والخدمات المتوفرة عبرها لنشر أفكاره وتجنيد المزيد من الأشخاص في صفوفه. ومن أهمها الفيسبوك واليوتيوب وتويتر والواتساب والانستغرام التي تم اتخاذها من أجل تحقيق الأهداف وتجنيد الأعضاء، وما يؤكد تطور استغلال شبكات التواصل الاجتماعي الحديثة لداعش، هي تصريحات أدلى بها وزير داخلية اسبانيا خورخي فرناندیز مؤكدا بأن 80% من الإرهابيين يتم تجنيدهم من خلال وسائل التواصل الاجتماعي، بينما يتم تجنيد 20% بالطرق العادية.[4] .

الفرع الثاني : البريد الالكتروني

يعد البريد الإلكتروني (E-mail) من أسهل وأسرع الطرق التي يتم بها التواصل، لذلك أصبحت أهم سلاح في أيدي المنظمات الإرهابية، حيث يتم من خلاله تبادل المعلومات في ما بينهم ،إضافة إلى استعماله كوسيلة لجذب وتكثير المتعاطفين لتجنيدهم[5].

---

[1]– وداد حمدى، استغلال مواقع التواصل الاجتماعي من قبل التنظيمات الإرهابية، متاح على http://ajo-ar.org :، تقرير المرصد العربى للصحافة، تاريخ النشر 7 أبريل 2017 .

[2] – غادة البطريق، تعرض الشباب العربي للمواقع الإلكترونية المتطرفة فكريا وعلاقته بإدراكهم للمنطق الدعائي للتنظيمات الإرهابية : دراسة ميدانية في إطار نظرية تأثير الشخص الثالث، مجلة بحوث العلاقات العامة الشرق الأوسط، الجمعية المصرية للعلاقات العامة، القاهرة، ديسمبر 2016، ص177

[3] – رضا ابن مقلة، الإعلام الإلكترونى المتطرف وسبل مواجهته: تنظيم داعش نموذجا، مجلة الحكمة للدراسات الإسلامية، مؤسسة كنوز الحكمة للنشر والتوزيع، الجزائر، 2015، ص 154.

[4] – مرصد الأزهر، استخدام داعش لوسائل التواصل الاجتماعي، تاريخ النشر: 2015/12/4، متاح على : http://www.azhar.eg/observer/replies

[5] – صدام حسين ياسين العبيدي ، المرجع السابق ، ص 219

الفرع الثالث : إنشاء مواقع إرهابية على الإنترنت

ينشئ الإرهابيون مواقع لأنفسهم على شبكة الويب العالمية للحصول على المعلومات ونشر أفكارهم والدفاع عن مبادئهم وتعاليمهم وأساليبهم التي تسهل أنشطتهم الإرهابية. وقد تم إنشاء مواقع لتعليم كيفية اختراق الويب وتعطيله، وكيفية اختراق البريد الإلكتروني، وكيفية الوصول إلى المواقع المحجوبة، وكذلك كيفية نشر الفيروسات إلى غير ذلك من الأعمال الإرهابية.

إن الإنترنت سهلت من تبادل الآراء والأفكار والمعلومات فيما بين العصابات والمنظمات الإرهابية، فمن الممكن التقاء العديد من الأشخاص في أماكن مختلفة في نفس الوقت، فمن السهل والممكن إنشاء مواقع إلكترونية واستخدام غرف الدردشة عبر الإنترنت لتحقيق أهداف إرهابية، إضافة لذلك نجد بعض التنظيمات الإرهابية تنشأ الآلاف من المواقع الإلكترونية لضمان التوزيع على نطاق أوسع، حتى لو كان هناك إمكانية الوصول إلى بعضها ويتم حظرها أو تدميرها، ويظل الوصول إلى المواقع الأخرى متاحًا[1].

المطلب الرابع : أركان الإرهاب عبر الإنترنت

إضافة إلى الركن المفترض يجب توافر الركن المادي والمعنوي لقيام جريمة الإرهاب عبر الانترنت مثلها مثل كافة الجرائم الأخرى.

الفرع الأول: الركن المادي للإرهاب عبر الإنترنت

إن السلوك الإجرامي في الإرهاب عبر الإنترنت يتمثل في إنشاء مواقع على الإنترنت أو باستخدام أي وسيلة من الوسائل التي توفرها هذه التقنية تحت أسماء تمويهية لتسهيل الاتصال وترويج الأفكار الإرهابية أو لتمويلها، أو من أجل أي سلوك يوصف بأنه عمل إرهابي. وعليه فإن الركن المادي في هذا النوع من الجرائم يتوافر بتحقق إمكانية إيقاع الفعل باستخدام تقنية الإنترنت.[2]

[1] – صدام حسين ياسين العبيدي ، المرجع نفسه، ص 220

[2] – أسامة احمد المناعسة و جلال محمد الزغبي ، جرائم تقنية المعلومات الالكترونية ، مرجع سابق ، ص 323

الفرع الثاني : الركن المعنوي للإرهاب عبر الإنترنت

يعد الإرهاب عبر الإنترنت من الجرائم التي يتطلب لقيامها توافر القصد العام، إذ يجب على الفاعل أن يعلم أن سلوكه الذي يقوم به باستخدام الإنترنت يعد سلوكا إجراميا يعاقب عليه القانون، وفي نفس الوقت يجب أن تتجه إرادته نحو ارتكاب الفعل المكون للجريمة مع تحقق هذه النتيجة.

المبحث الثاني: جريمة غسيل الأموال عبر الإنترنت

تعد جريمة غسيل الأموال من الجرائم الحديثة، وغالبا ما ترتبط بالجريمة المنظمة وهي أيضا تدخل ضمن الجرائم الماسة بسلامة الدول، وقد تطورت أشكالها وتضاعفت في ظل التطور التكنولوجي الكبير، حيث أتقن بعض المجرمون استخدام تكنولوجيا المعلومات وأجهزة الكمبيوتر والإنترنت لتنفيذ جرائم مالية معقدة.

غسيل الأموال السيبراني هو نوع من السلوك والأنشطة الإجرامية التي تعيد إدخال الأموال السوداء الناتجة عن الأنشطة غير المشروعة إلى الاقتصاد العالمي باستخدام الإنترنت ومختلف خدماته، وبالتالي تدر عوائد مالية ضخمة على أصحابها، ونظرًا لانفتاح وترابط الأسواق العالمية، والاقتصاد المتداخل، والتشابك المالي المتزايد بين مناطق العالم، يمكن ارتكاب أنشطة مثل صفقات الأسلحة وتجارة الرقيق والبغاء على الإنترنت، بالإضافة إلى تجارة المخدرات التي تعد من أبرز الأموال المبيّضة عالميا.

وعليه سنتعرض في هذا المبحث لمفهوم جريمة غسل الأموال في المطلب الأول، وخصائصها المميزة، والمراحل اللازمة لإعدادها، والوسائل المتبعة في ممارستها.

المطلب الأول : مفهوم غسيل الأموال عبر الإنترنت

يعتبر مصطلح غسيل الأموال من المصطلحات الحديثة في الدراسات والأبحـــــــاث القانونية. ولذلك هناك اختلاف في الرأي من وجهة نظر القانون والاقتصاد حول معنى هذا المصطلح. خاصة مع ظهور شبكة الإنترنت واعتماد مرتكبي الجريمة عليها، ولهذا سنحاول من خلال هذا المطلب أن نجلي الغموض ونزيل الإبهام على مفهوم جريمة غسيل الأموال عبر الإنترنت.

الفرع الأول : تعريف غسيل الأموال

قبل التطرق لتعريف غسيل أموال من الناحية الفقهية والقانونية نتطرق أولا لتعريفه من الناحية اللغوية.

الفقرة الأولى : تعريف غسيل الأموال من الناحية اللغوية

غسل الشيء غسلا: أزال عنه الوسخ ونظفه بالماء. ويقال:غسل: طهره من إثمه.[1] أما المال هو كل ما يمتلكه الفرد أو الجماعة من متاع أو عروض وتجارة[2].

الفقرة الثانية :التعريف الفقهي والقانوني لغسيل الأموال

تنوعت وتعددت التعاريف المتعلقة بجريمة تبييض الأموال أهمها تعريفها بأنها " نقل أو الأموال التي يتم الحصول عليها بطرق غير قانونية إلى أشكال أخرى لتغطية مصادرها والتجهيل بها للاحتفاظ بالأموال".[3]

أما تعريف غسيل الأموال من المنظور القانوني قد عرفها القانون التنظيمي الإداري الأوروبي المشترك لسنة 1991 في مادته الأولى على أنه " نقل الأموال أو التصرف فيها مع العلم أنها متحصل عليها من جريمة بقصد إخفاء أو تغيير مصدر الأموال أو مساعدة شخص متورط في ارتكاب جريمة تساعده على التهرب من القانون من خلال هذا الفعل "[4].

أما المشرع الجزائري فلم يعرف جريمة غسيل الأموال في نصوصه التشريعية والتنظيمية، بل اقتصر الأمر على وصف الأنشطة التي تشكل جريمة غسل الأموال ووسائل مكافحتها. ويمكننا تعريف غسيل الأموال بموجب المادة 2 من قانون غسل الأموال والمادة 389 من قانون العقوبات بأنها تحويل أو نقل الممتلكات مع العلم أنها ناشئة نتيجة جريمة معينة، وذلك بغرض إخفاء المصدر غير القانوني لهذه الممتلكات أو لغرض مساعدة أي شخص شارك في ارتكاب الجريمة الرئيسية (مصدر الأموال القذرة) لتجنب

---

[1]–المعجم الوسيط، الجزء الثاني، ص 892

[2] – أبو محمد عبد الله بن أحمد ابن قدامة المقدسي، المغني، ج 01 ، تحقيق: رائد بن صبري بن أبي علفة، بيروت: بيت الأفكار الدولية، 2004 ، ص 218

[3] – سيد أحمد عبد الخالق، الآثار الاقتصادية والاجتماعية لغسيل الأموال، القاهرة: دار النهضة العربية، 1997 ، ص 03

[4] – محمود محمد سعيفان تحليل و تقييم دور البنوك في مكافحة عمليات غسيل الأموال ، دار الثقافة للنشر والتوزيع ، عمان طبعة 1 ، 2008 ، ص 28

العواقب القانونية الناتجة عن الفعل الذي قام به. وكذلك هو تمويه وإخفاء حقيقة طبيعة المال الحقيقي أو مصدره أو موقعه أو حركته أو ملكيته القانونية مع العلم بأن الممتلكات تم الحصول عليها عن طريق جريمة معينة، بما في ذلك أخذ البضائع أو الاحتفاظ بها أو استخدامها مع العلم التام بأنها ناتجة عن أنشطة إجرامية[1].

الفرع الثاني: تعريف جريمة غسيل الأموال عبر الإنترنت

من خلال تسهيل الاتصال بين الأفراد والجماعات، أصبحت الإنترنت ملاذاً آمناً لغاسلي الأموال المتمرسين عبر الإنترنت، حيث تمكن القائمين بغسيل الأموال من الوصول إلى الفضاء الإلكتروني، وشكلت ما يعرف بأصحاب الأموال القذرة الذين صاروا يعتمدون عليه اعتماد شبه كلي لغسيل أموالهم، وهذا ما سبب إشكالية خطيرة تواجه الاقتصاد العالمي. فزوال الحواجز الاقتصادية والاتصال بين الدول، ساعد بشكل كبير في إيجاد طرق جديدة ومتعددة لغسل الأموال من خلال استخدام شبكات الإنترنت، سواء عبر بنوك الإنترنت الافتراضية أو البطاقات الممغنطة بمختلف أنواعها سواء كانت للسحب أو الائتمان أو الشيكات أو باستخدام الشيك الالكتروني أو التحويلات النقدية عبر الهواتف المحمولة سواء داخل الدولة أو خارجها[2]، ولقد وصف أحد الباحثين حركة الأموال عبر الشبكة "أنها سريعة، ومغفلة التوقيع، ولا توقفها الحدود الجغرافية".

ويعد غسل الأموال عبر الإنترنت تجمع إجرامي مشترك من المتخصصين في التمويل والمصارف والتكنولوجيا، إضافة إلى جهود خبراء الاستثمار المالي وجهود غيرهم من المجرمين، ولهذا تتطلب هذه الجريمة دراية كافية ومعرفة لمرتكبيها، ويتطلب أيضا العمل والتعاون عبر الحدود الجغرافية، ولذلك يلاحظ صعوبة الوقوف على الحجم الحقيقي للأموال التي يجري غسلها عبر وسائل الاتصال الحديثة، ولكن هناك اتفاق عالمي على أنها مبالغ ضخمة جدا قد تصل إلى نحو 500 بليون في العالم .[3]

---

[1] – القانون الجزائري الصادر بمقتضى الأمر 66/ 156 المؤرخ في 8يونيو 1966 ، المعدل و المتمم بقانون 15/2004 المؤرخ في 2004/11/10

[2] – عبد الفتاح بيومي حجازي ، جريمة غسل الأموال عبر شبكة الإنترنت "دراسة متعمقة عن جريمة غسل الأموال عبر الوسائط الإلكترونية في التشريعات المقارنة " ، المصدر القومي للإصدارات القانونية ، طبعة 1، 2009، ص 21

[3] – محمود رجب فتح الله، الوسيط ، مرجع سابق ، ص 380

المطلب الثاني: مراحل وأساليب غسل الأموال عبر الإنترنت

إن جريمة غسل الأموال تتم في مناطق مختلفة، وتتضمن مراحل مختلفة وتنطوي على أساليب متنوعة من التهريب والنقل من مكان إلى آخر ومن دولة إلى أخرى. لتكون بعيدًة عن شكوك ومراقبة السلطات.

الفرع الأول : مراحل غسل الأموال عبر الإنترنت

تمر جريمة غسل الأموال بعدة مراحل سنتطرق لها على النحو الأتي:

الفقرة الأولى: مرحلة الإيداع

وهي المرحلة الأولى التي تأتي بعد اقتناء الأموال الغير مشروعة وهي مرحلة يعرف فيها المال ركودا تاما، أي يتم ركنه في مكان بعيد لوقت معين بغرض نسيان مصدره، ويقوم الجاني في هذه الفترة بفتح حسابات بنكية باسم حقيقي أو مزيف إضافة إلى شراء أسهم من شركة أو مؤسسة مالية خاصة على الأسهم التي لا تشير إلى أصلها، وتترك الأموال تنتظر الوقت المناسب للانتقال إلى الخطوة التالية للهروب من إمكانية المراقبة أو التحكم.

الفقرة الثانية: مرحلة التكديس

وفيها يظهر المال الغير مشروع، وتأتي المرحلة الموالية والمتمثلة في مرحلة التبييض الابتدائية وتتم باستثمار الأموال في مشاريع حقيقة مثل المشاريع العقارية كبناء قرى وفنادق سياحية أو بإدخالها في شركات مزيفة في البلد التي لا تفرض قيوداً على حركة رؤوس الأموال، لذا يصعب إيجاد مصادر للتمويل. وهدف هذه المرحلة هو تمويه الجهات الرقابية المختصة عن مصدر الأموال القذرة، وأسلوب التضليل يمكن أن يتم أيضا من خلال خدمات مصرفية معقدة وتحويل الأموال إلكترونياً عن بعد أو من بنك إلى آخر.

الفقرة الثالثة : مرحلة الاندماج

وتتميز هذه العملية بانفتاح نشاطها، لأن الأموال المتأتية من مصادر غير مشروعة تندمج بشكل كامل في الاقتصاد القانوني، مما يجعل من الصعب فصلها وتمييزها عن العائدات المالية القانونية.

وغالبًا ما يصعب اكتشاف هذه الخطوة إلا من خلال المراقبة أو التحقيق السري أو المعلومات السرية، ومن أمثلة تقنيات الدمج التراخيص الزائفة أو الوهمية أو معاملات الشراء والتصدير التي تنتهي في مستندات الإيداع المصرفي، وبشراء العقارات، والأنشطة الاستثمارية مثل الفنادق والمنتجعات والتأمين.[1]

الفرع الثاني : أساليب غسل الأموال عبر الإنترنت

إن استخدام الإنترنت لتطهير المال المتحصل عليه بطريقة غير شرعية يتم من خلال الاستعانة بما يلي:

أولا : تقنية الدفع الالكتروني

توقع المختصون بأن التعامل بالاعتماد المستندي الالكتروني سيؤدي حتما للوقوع في الغش.[2] إلا أن الواقع أثبت عكس ذلك، حيث أصبحت معاملات خطابات الاعتماد الإلكترونية من أخطر الأدوات التي يمكن أن يستخدمها المجرمون لغسل أموالهم.[3]

يقوم الاعتماد المستندي على التعامل بالمستندات ذات الطبيعة الالكترونية، وينتقل المال من بنك فاتح الاعتماد إلى المستفيد عبر نظام الاعتماد المستندي الالكتروني بطريقة الكترونية، وهذا باعتماد أحد أنظمة النقل الالكتروني للأموال السابقة الذكر.

---

[1] – مراد رشدي، غسل الأموال عبر الوسائل الإلكترونية،المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية منظم المؤتمر : أكاديمية شرطة دبي – مركز البحوث والدراسات تاريخ الإنعقاد : 26 /2003/4: دبي ،الأمارات العربية المتحدة

[2]–la Chambre de commerce internationale sur le guide du eRUU :" That is not to say that fraud can be eliminated from credit transactions simply by the use of electronic presentation, but only that the possibilities for fraud become more limited. " voire : RAKOTONANAHARY Salohy Miadana, op. cit.,p 20.

[3]– عبد الفتاح بيومي حجازي، جريمة غسل الموال بين الوسائط الالكترونية ونصوص التشريع، دار الكتب القانونية، مصر، 2007، ص 107

ومن هنا باتت عملية التحويل الإلكتروني للأموال وسيلة مثالية لغاسلي الأموال لغسل أموالهم، بسبب السرعة التي تستطيع بها هذه التقنية الحديثة أداء عملها.[1] وفي هذه الحالة قد يكون المصدر الذي تم منه الدفع بأموال متحصل عليها بطريقة غير قانونية من جهة فاتح الاعتماد، والذي يرغب في تبييض هذه الأموال القذرة. حيث يقوم بإيداع مبالغ كبيرة من الأموال غير مشروعة ببنكه الخاص، ويتم فتح هذه الاعتمادات الإلكترونية وتحويلها إلى الحساب البنكي للمستفيد من الاعتماد المستندي، وبدون الإفصاح عن مصدر هذه الأموال، لأن البنك الخاص بالعميل لن يقوم بالاستعلام عن مصدر هذه الأموال ولن يقوم بنك المستفيد بالتحقق من مصدر الأموال.[2]

من عواقب ارتكاب جرائم الأموال باستخدام عملية التحويلات المالية الالكترونية، أن هذه التحويلات المفاجئة للأموال وبمبالغ ضخمة خارج الحدود من شأنها التأثير على أوضاع وثقة البنوك والأسواق المالية، وبالتالي استقرار نظامها المالي والمصرفي. [3]

ولكن هناك نظام آخر يسمى نظام تبادل البيانات المالية الإلكتروني، والذي يعتمد على التبادل الإلكتروني لجميع المعلومات المتعلقة بالمعاملات مثل النقد والفواتير والتحويل بين الحسابات، وهذا يعني أن المعاملات الإلكترونية لا تقتصر على النقد، بل تركز على المعلومات المتعلقة بالمعاملة. وبسبب تكلفته الباهظة لا يستخدمه سوى الشركات الكبرى، لتوفيره الأمان أكثر من الأنظمة الأخرى.[4]

---

[1] – بقبق ليلى اسمهان، لعمليات البنكية غير المشروعة وأثرها على الاقتصاد (عمليات تبييض الأموال) ، الملتقى الوطني حول الاقتصاد غير الرسمي في الجزائر: الآثار وسبل الترويض (المداخل القياسية)، معهد العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، المركز الجامعي د. مولاي الطاهر، ولاية سعيدة، الجزائر، ص 13.

[2] – عبد الفتاح بيومي حجازي، المرجع السابق، ص 108، 109

[3] – سليمان ضيف الله الزبن، التحويل الالكتروني للأموال ومسؤولية البنوك القانونية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2012 ، ص68

[4]– مصطفى كمال طه، الأوراق التجارية ووسائل الدفع الالكترونية الحديثة، دار الفكر الجامعي، الاسكندرية، مصر، 2007، ص 329.

ثانيا : بنوك الإنترنت (Internet Banking)

يستطيع أي فرد استخدام الإنترنت لإنشاء بنك افتراضي أو شركات مزيفة في الدول التي تغض الطرف عن العمليات التي يتم من خلالها غسيل الأموال، وتدور النقود الإلكترونية في هذا الفضاء الافتراضي الذي يتم فيه التعامل بالأموال الالكترونية التي تنتقل بسهولة من مكان إلى آخر عبر شبكة الإنترنت، وبعيدًا عن رقابة السلطات المختصة في العمليات المصرفية، وتعد الخدمات المصرفية عبر الإنترنت طريقة سهلة ومثالية لغسل الأموال خاصة وأن البنوك عبر الإنترنت ليست أكثر من كيانات افتراضية بسبب غيابها المادي، ولا تخضع للقوانين واللوائح المرتبطة بالبنوك التجارية التقليدية، ووجودها خارج القانون يمنح البنك المركزي سلطة مراقبة البنوك وتنظيم أنشطتها والحق في ملاحقتها في حالة خرقها للقانون[1]

ثالثا: التحويل الالكتروني

بسبب الثغرات الموجودة في النظام الالكتروني، يلجأ القائمون على غسيل الأموال إلى التحويلات الإلكترونية للأموال، بما في ذلك الودائع المجهولة في البنوك الأجنبية[2].

ففي هذه الحالة يقوم الجناة بإيداع أموالهم في بنوك ثم القيام بتحويلها إلى شركات وهمية . ولا يعرف البنك المحول نفسه الغرض من تحويل الأموال، لأن البنك المصرح هو الوحيد الذي يملك صلاحية التحري في أهداف العميل من هذا التحويل[3]. وبالتالي نجد أن تحويلات البنوك الأجنبية غالبا ما لا تحمل اسم العميل المنشئ وتذكر فقط مايلي:" إن عميلنا يرغب في تحويل .....إلي عميلكم " وعليه فإن نظم التحويل البرقي أو الالكتروني

---

[1]–بركات ،إبراهيم محمد "أهمية الإفصاح عن مخاطر المعاملات المالية المتعلقة بغسل الأموال في البنوك التجارية ": دراسة تحليلية في ضوء نظرية المسؤولية الاجتماعية، بحث مقدم للمؤتمر العلمي السنوي السابع إدارة المخاطر واقتصاد المعرفة المحور السابع : إدارة المخاطر والمحاسبة، جامعة الزيتونة الأردنية ،عمان ، الأردن 2007،ص 35

[2]– جلال وفاء محمدين ، دور البنوك في مكافحة غسيل الأموال ، دار الجامعة الجديدة للنشر ، الإسكندرية ، 2001، ص 27

[3] – عبد الفتاح بيومي حجازي ، جرائم غسيل الأموال بين الوسائط الالكترونية و نصوص التشريع ، دراسة مقارنة ، القاهرة ،2010، ص 65

للأموال هي ثلاثة نظم : نظام الفيدواير، نظام غرفة المقاصة، نظام الاتصالات السلكية واللاسلكية .[1] ويعد النظام الأول والثاني من الآليات الفعلية لتسوية وإتمام التحويلات، أما النظام الأخير فإنه يحرر جهاز مراسلة يستغل للإخطار عن الحركة الفعلية للأموال. ويستخدم نظام فيدواير للتحويلات البرقية المحلية وهو نظام فوري لا يقبل الرجوع فيه، في حين أن نظام غرفة المقاصة يستخدم في التحويلات البرقية الدولية وهو عبارة عن عملية تسوى في نهاية اليوم.[2]

رابعا: التجارة الإلكترونية:

في الآونة الأخيرة وبسبب تطور تقنيات المعلومات والاتصالات انتشرت ظاهرة التجارة الإلكترونية باستخدام الإنترنت وبشكل كبير، حيث لم يعد وجود الأطراف المتعاقدة في المواجهة ضروريا، كذلك ليست هناك الحاجة لتنفيذ الالتزام في المكان نفسه، وقد تم إطلاق قانون موحد شامل للتجارة الإلكترونية في 16 ديسمبر 1996 من قبل لجنة الأمم المتحدة للقانون التجاري الدولي.

وتعد التجارة الالكترونية إحدى الطرق التي يتم غسل الأموال عبرها ولا يتعلق الأمر بشراء سلع للاستهلاك فحسب بل يتعلق الأمر بإجراء معاملات مالية كبيرة مع شركات كبيرة ثم إعادة طرحها في الأسواق، ومن أمثلة هذه الصفقات، الصفقات المتعلقة بالعقارات أو السيارات أو الأحجار الكريمة والمعادن الثمينة[3].

---

[1] –Duncan FalFord ,Antimaney Laundering regulations : A,Bueden on Financial institutions, p 665

–فيدواير :هو مصطلح يشير إلى نظام شبكيّ لتسوية أموال البنك المركزي، حيث تستخدم البنوك الاحتياطية الفيدرالية هذه الشبكة لتسوية المدفوعات النهائية بالدولار الأمريكي بشكل إلكتروني بين المؤسسات الأعضاء.

– نظام المقاصة بين البنوك أو غرفة المقاصة (CHIPS) هو مركز مقاصة خاص بالولايات المتحدة للمعاملات ذات القيمة الكبيرة.

–SWIFTهي شبكة مملوكة من قبل البنوك المستخدمة للبورصات العالمية بين البنوك (أكثر من 7000 مؤسسة متصلة بها في 192 دولة).

[2]– جلال وفاء ، دور البنوك في مكافحة غسيل الأموال ، المرجع السابق ، ص 28

[3] – عبد الفتاح بيومي حجازي، جريمة غسل الموال بين الوسائط الالكترونية ونصوص التشريع، المرجع السابق ، 98

خامسا :النقود الالكترونية

تعد النقود الالكترونية وسيلة مثالية يلجا لها غاسلي الأموال باعتبارها نوعا حديثا من التكنولوجيا الالكترونية والتي لا يتم التعامل فيها بالأوراق ويسمح بتحويل الأرصدة النقدية من شخص إلى آخر في جميع أنحاء العالم عبر الإنترنت، وذلك دون الحاجة إلى المرور عبر المصارف، واهم ميزة في النقود الالكترونية أنها بسيطة وزهيدة في تكلفة تداولها إضافة إلى كونها سهلة الاستخدام، لأنها تعفى من إجراءات البنكية التقليدية، كما أنها تسرع عمليات الدفع والتحويل من خلال الإيداع بالرقـــم السري. [1]

وهناك طريقة حديثة تسمى بـ الكارت الذكي (Smart Card)، وهي تقنية نشأت في إنجلترا وتم استخدامها في الولايات المتحدة. وتتميز بخاصية الاحتفاظ بملايين من النقود المخزنة على قرص، ويمكن بسهولة نقل هذه القيمة إلكترونيًا على كارت آخر يستخدم آلة معدة لهذا الغرض ودون تدخل البنوك، و بهذا تجنب البطاقة الذكية التفتيش أو الرقابة من قبل أي جهة أمنية، وتعتبر وسيلة فعالة لمجرمـــي غسل الأموال للقيام بعملياتهم الإجرامية. [2]

إضافة إلى الكارد الذكي هناك حافظة الأموال الالكترونية، وهي بطاقة الدفع السابق، أين تحتفظ بالدفعات الأولى والمتعددة الاستعمالات، وهي لا تستخدم للدفع مقابل خدمة محددة بذاتها كما في بطاقة الهاتف، وذلك لأن الحافظة تشكل احتياطيا ماليا يتم تخزينه في معالج بطاقة الائتمان.

ويتم استخدام حافظة النقود الالكترونية في تبييض الأموال من خلال إيداع الأموال الغير المشروعة المراد غسلها إلكترونيًا، ومن ثم يقوم البنك المودع لديه هذه الأموال بطريقة قانونية بإصدار حوافظ مالية أو نقدية في صورة هواتف تليفون أو غيرها من صور هذه النقود الالكترونية وبعد إنفاقها يتم غسل الأموال كما أراد الجناة .[3]

---

[1] – حمدي عبد العظيم ، غسيل الأموال جريمة العصر البيضاء ، القاهرة ، 2000، ص 40

[2]– عبد الفتاح حجازي ، جرائم غسل الأموال ، مرجع سابق ، ص78

[3] – عدنان ابراهيم سرحان ، الوفاء (الدفع الالكتروني)، بحث مقدم إلى مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون المنعقد بتاريخ 2006/12/10 جامعة البحرين.

سادسا : الشيك الإلكتروني والبورصة عبر الإنترنت

قد أتاحت التقنية الحديثة في تنويع طرق تبييض الأموال إذ بات من السهل القيام بالعديد من العمليات المصرفية والتحويلات المالية في وقت قياسي الأمر الذي يصعب مراقبة حركتها، كما سهلت المواقع التي يطلق عليها مصطلح "الإنترنت العميق" في حركة الأموال القذرة وفي تبييضها، ومن الأساليب التقنية المتطورة الذي شاع استخدامها في عمليات غسيل الأموال ظهور "الشيك الإلكتروني"، الذي يتم تداوله فقط باستخدام الوسائل الالكترونية .[1]

ومن الوسائل الالكترونية الأخرى التي يلجا لها مجرمي غسيل الأموال، البورصة وسوق الأوراق المالية التي تعتبر من الاستثمارات الهامة لهؤلاء الجناة، نظرا لتداول رأس المال بسهولة وسرعة تامة خاصة باستخدام شبكة الإنترنت، حيث يقوم الجاني بشراء مجموعة كبيرة من الأسهم والسندات بأموال ذات مصدر غير مشروع أو المضاربة في البورصة على سلعة أو معدن نفيس ثم يقوم ببيعها ثم يقوم بشرائها حتى يتم تبييضها بسهولة عبر شبكة الإنترنت من خلال التعامل على مواقع البورصة التي تملك مواقع على الإنترنت.[2]

سابعا : نوادي القمار الافتراضية، وتقنية موندكس في غسيل الأموال عبر الإنترنت

نوادي القمار الافتراضية هي عبارة عن مواقع تقوم بتصميم وتوفير كل أشكال القمار وألعابه، وهي نوادي افتراضية وتعتبر أسلوب من أساليب عملية غسيل أموال لصعوبة تتبع أماكن وجودها الحقيقي وخروجها من الاختصاص الإقليمي للدول، حيث لا توجد حدود جغرافية لها، أين يلجأ الراغبين في تبييض أموالهم إلى نوادي القمار الافتراضية للحصول على قسائم اللعب مقابل مال نقدي، وبعدها تستبدل القسيمة بشيكات مسحوبة من مصارف فتصبح أموال ناتجة عن ربح من اللعبة.

---

[1] – موسي عيسى العامري، الشيك الذكي، بحث مقدم إلى مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون ، المنعقد بتاريخ 2006/12/10 جامعة البحرين.

[2]– عبد الفتاح حجازي، الحكومة الالكترونية بين الواقع والطموح ، دار الفكر الجامعي، القاهرة ، 2008، ص 431

أما تقنية المندكس هي تقنية مستخدمة في العالم السيبراني تتيح للمستخدمين بتحويل المال القذر عبر المودم أو عبر الإنترنت، مما يوفر تشفيرًا آمنًا لعمليات غسيل الأموال دون ترك آثار يمكن من خلالها التعرف على المجرمين.

وتتميز تقنية موندكس في غسيل الأموال بالابتعاد عن البنوك العامة أو الخدمات المصرفية العادية وعبور للحدود الإقليمية بكل سهولة، وتعد تقنية المونداكس من أهم الطرق التي تستخدم في الجريمة المنظمة، ويتم من خلالها تحويل الأموال القذرة وتشفير التحويلات عبر الإنترنت مما يجعل من المستحيل تحديد محتويات العملية التي منها جاءت الأموال المحولة. وعليه فإن جرائم غسل الأموال هي عملية مبارزة بين أجهزة الوقاية والجناة أصحاب العقلية الابتكارية، فبالتطور المستمر والدائم في تقنية المعلومات تتطور معه وسائل إخفاء مصادر الأموال، وتزداد معه طرق المكافحة.[1]

المطلب الثاني: أركان جريمة غسل الأموال عبر الإنترنت

تقوم جريمة غسل الأموال عبر الإنترنت على عدة أركان أساسية تتمثل في ما يلي :

الفرع الأول: وجود المال غير المشروع كشرط أساسي لقيام الجريمة

تنطوي جريمة غسيل الأموال على فعل يستهدف تحويل مال ما من صفته غير الشرعية إلى صفة شرعية، أي إيجاد سبب وذريعة قانونية تبرر وجود المال. وهو ما يعرف بتحـول العوائد الجرمية إلى أصول يصعب تعقب مصدرها الغير قانوني.[2]

وعليه يشترط في قيام جريمة غسيل الأموال عبر الإنترنت أن تكون الأموال المراد غسلها ناتجة عن ارتكاب جريمة من الجرائم، أو كما يصفها البعض بالأموال القذرة الفاقدة للمشروعية، بمعنى أن المال لا يكون محلا لجريمة غسيل الأموال ما لم يكن نتاج عمل إجرامي، يشكل في حد ذاته جريمة يعاقب عليها القانون، وهذا ما يجعل من جريمة غسل الأموال جريمتين في جريمة واحدة .

---

[1] – مصطفى الطاهر، المواجهة التشريعية لظاهرة غسيل الأموال المتحصلة من جرائم المخدرات، مطابع الشرطة للطباعة والنشر، القاهرة، 2002 ص 89

[2]– أسامة احمد المناعسة ، جلال محمد الزعبي ،جرائم تقنية المعلومات الالكترونية، مرجع سابق ، ص 180

الفرع الثاني : الركن المادي لجريمة غسل الأموال عبر الإنترنت

إن الركن المادي لهذه الجريمة يتمثل في الأفعال التي تهدف إلى تحويل الأموال أو التلاعب في قيمتها أو تبادلها أو تحويلها أو السيطرة على حركتها، أو أي عمل يهدف إلى إخفاء مصدرها أو تمويهه، مع العلم أن الحصول عليها كان نتيجة لنشاط غير قانوني.[1] وتختلف هذه السلوكيات المادية بحسب دور مرتكبيها في القيام بغسل الأموال. كما أنها تتنوع بين السلوك الإيجابي، ويعني القيام بنشاط معين، والسلوك السلبي ويعني الامتناع عن القيام بنشاط معين[2].

الفرع الثالث : الركن المعنوي لجريمة غسل الأموال عبر الإنترنت

باعتبارها من الجرائم العمدية يشترط في قيام جريمة غسيل الأموال عبر الإنترنت توافر الركن المعنوي والمتمثل في القصد الجنائي المتكون من عنصرين: الأول العلم، والثاني عنصر الإرادة.

أولاً: العلم :

يتوجب على مرتكب جريمة غسيل الأموال عبر الإنترنت أن يعلم بأن الأموال التي سيتم غسلها مصدرها أعمال غير مشروعة قانونيا، أما في حالة ما كان الجاني جاهلا للمصدر الغير شرعي للأموال وأعتقد بحسن نية أنها نظيفه، لا يقوم القصد الجنائي لانعدام شرط من شروطه والمتمثل في عنصر العلم، ويشترط أيضا في جريمة غسيل الأموال علم الجاني أن ما يقوم به عبر شبكة الإنترنت من عمليات من شأنها تنظيف الأموال الغير مشروعة وإدخالها في دائرة المال المشروع[3].

ثانيا: الإرادة

---

[1]– أسامة احمد المناعسة ، جلال محمد الزعبي ،المرجع نفسه، ص 183

[2]– حنان ريحان مبارك ، الجرائم المعلوماتية ، المرجع السابق ، ص 387

[3]– محمد عبد الله سلامة، الكيان القانوني لغسيل الأموال: الجريمة، المسؤولية الجنائية، المكافحة، ، المكتب العربي الحديث، الإسكندرية، طبعة 1 ، 2007، ص91

يشترط توافر عنصر الإرادة لدي الجاني والمتمثلة في انصراف إرادته في تحقيق النتيجة الإجرامية وهي غسيل المال غير المشروع باستعمال أي وسيلة متوفرة عبر الإنترنت من شأنها إظهار الأموال على أنها مشروعة ومستمدة من أنشطة مشروعة.

المبحث الثالث : التجسس عبر الإنترنت

مع نهاية القرن العشرين حدث تغير كبير في مفهوم وأدوات وأساليب التجسس في ظل التطور التكنولوجي المعلوماتي، الذي أدى إلى ظهور شبكات الحاسبات المتصلة مع بعضها البعض، والذي تطور ليصل إلى شبكة الإنترنت، وأصبحت كل المعلومات السياسية والاقتصادية والعسكرية من الممكن الوصول إليها بكل سهولة، فالتطور الالكتروني وثورة المعلومات والإنترنت التي قربت المسافات وأسقطت الحدود، قد خلقت فضاءً جديداً لعالم الجواسيس يتحركون فيه دون عناء وقيود ومراقبة من أجل الحصول على المعلومات، وباتت حرب المعلومات يتم خوضها والانتصار فيها بقدر ما يُتَحَصَل عليه من معلومات عن الخصم سواء كان فرداً أو شركة أو مجتمعاً أو دولة.

وبذلك ظهر نوع آخر من أنواع التجسس هو "التجسس الالكتروني" أو ما يعرف بالتجسس المعلوماتي، والذي يتمثل في القدرة على اختراق المواقع الالكترونية، أو التسلل إلى أجهزة الكومبيوتر واعتراض الإشارات وجمع المعلومات المرسلة من أجهزة الكومبيوتر عبر الإنترنت ومن ثم سرقتها منه.

ولبيان ماهية التجسس سنعرض مفهوم التجسس الالكتروني في المطلب الأول، ثم نعرض الصور السائدة للتجسس الالكتروني في المطلب الثاني، ويليهم أركان جريمة التجسس الالكتروني في المطلب الثالث.

المطلب الأول : مفهوم التجسس عبر الانترنت

مفهوم التجسس عبر الإنترنت يقتضي معرفة التعريف العام للتجسس.

الفرع الأول : تعريف التجسس

قبل التطرق لتعريف التجسس من الناحية الفقهية والقانونية نتطرق أولا لتعريفه من الناحية اللغوية.

الفقرة الأولى :تعريف التجسس في اللغة

التجسس من الجس، والجس هو اللمس باليد، وموضعه المجسَّة، وجَّس الشخص بعينه: أحَدَّ النظر إليه ليستبينه ويستثبته. وجَّس الخبر: بحث عنه وتفحصه.[1]

الفقرة الثانية :التعريف الفقهي والقانوني للتجسس

لم يرد في كتب الفقه تعريفاً فقهيا محدداً ومتفقاً عليه للتجسس، وربما بسبب ظهور معناه ووضوحه لم يجعل الفقهاء للتجسس يبحثون عن معنى زائد على المعنى اللغوي.

أما من الناحية القانونية فلا نجد تعريف موحد للتجسس، وانقسم رجال القانون في ذلك إلى فريقين، اتجه الفريق الأول إلى التضييق من مدلول التجسس، بأن قصره على أنشطة جمع المعلومات العسكرية لصالح العدو من خلال التكتيكات الخادعة والدعاية الخبيثة.[2] أما الفريق الآخر وسع في تعريف التجسس وفي رأيهم هو كل فعل يخدم مصالح الدولة الأجنبية.

فنجد إن الفقيه "جارو" عرف التجسس بأنه:" قيام الأجنبي بجمع الوثائق والمعلومات السرية المتعلقة بالوضع الاقتصادي والسياسي والموارد العسكرية والتنظيم الدفاعي والهجومي للدولة، وذلك بهدف تسليم تلك المعلومات والوثائق إلى الدول الأجنبية سواء كان ذلك بمقابل أو مجانا". ويعد التجسس في نظر أغلب فقهاء القانون الدولي عملاً يتعارض مع قواعد القانون الدولي لأنه يمثل انتهاكا وتهديداً للسلامة الإقليمية للدول وسيادتها واستقلالها وأمنها.[3]

الفرع الثاني : تعريف التجسس الالكتروني

لا يختلف التجسس عبر الإنترنت عن التجسس الكلاسيكي إلا في الأداة المستعملة في التجسس والمتمثلة في شبكة الإنترنت التي سهلت على الجاسوس المعلوماتي أو الالكتروني التجسس بعيد عن أعين الرقابة، وقد تنوعت تعريفات القانونيين للتجسس الالكتروني، بين تعريف يشمل الأفراد والدول، وبين من يحسره فقط في حدود الدولة وأسرارها بدون الأفراد،

---

[1]– ابن منظور، لسان العرب، المجلد السادس، ص 38

[2] – حافظ، مجدي محمود ،الحماية الجنائية لأسرار الدولة ، الهيئة المصرية العامة للكتاب، الإسكندرية ،1990 ، ص222

[3]– لحرش عبد الرحمن ،التجسس والحصانة الدبلوماسية، مجلة الحقوق، جامعة الكويت، العدد الرابع، 2003 ،ص 182.

ولقد عرفه الفريق الأول بأنه " الاطلاع على معلومات خاصة بالغير محفوظة على جهاز الكتروني متصل بشبكة الإنترنت وليس مسموحا لغير المخولين الاطلاع عليها".[1]

أما الفريق الثاني بأنه "استخدام وسائل تقنية المعلومات الحديثة للدخول بشكل غير مسموح به إلى أنظمة المعلومات الالكترونية الخاصة بالحكومات والتصنت عليها بهدف الحصول على ما لديها من معلومات مهمة تتعلق بنظامها وأسرارها، وتشمل جميع المعلومات الأمنية والعسكرية والاقتصادية والسياسية والاجتماعية والعلمية."[2]

ويرى بعض الباحثين انه لا يمكن حسر جرائم التجسس عبر الإنترنت في حيز الدولة وجماعاتها فقط، بل لابد أن يشملها التجسس على الأفراد أيضا، خاصة وان التجسس على الأفراد يشكل أهمية كبيرة للجهة المتجسسة نتيجة للأسرار المهمة والحساسة المحتفظ بها من طرفهم، خاصة وأن المعلومات الشخصية للأفراد تعد أهم ما يتم الاستيلاء عليه عبر الإنترنت بغية الابتزاز أو التهديد أو السرقة أو بغية الاستقطاب والتجنيد من طرف مختلف التنظيمات الإرهابية[3].

إن التجسس عبر الإنترنت يوفر عملية التصنت وتصوير المجني عليهم من خلال استهداف واختراق حواسيبهم أو هواتفهم النقالة، ويتم وضع الكاميرا أو الميكروفون قيد التشغيل بدون علمهم. إضافة إلى الحصول على كل البيانات الخاصة بهم، ويسهل التجسس أيضا الدخول للملفات الخاصة بالعدو وسرقتها ومن ثم تهديده، وبسبب الخوف من كشف أسراره قد يصبح من السهل تجنيده.

تعتمد الولايات المتحدة، مثل العديد من البلدان الأخرى، على خدمات التجسس للحفاظ على أراضيها آمنة في عهد الرقمنة، وتعتبر برامج التجسس الخاصة بالولايات م أ من أخطر البرامج، الأمر الذي خلق نوعا من الخوف والقلق لدى معظم دول العالم خاصة وأن

---

[1] – ابوغليون عطوة مسلم، الجرائم الالكترونية بين الشريعة الإسلامية والقوانين الوضعية، رسالة ماجستير في القضاء الشرعي من كل الدراسات العليا بالجامعة الأردنية ،عام 2009 ،ص64

[2] – علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة"دراسة مقارنة " مكتبة زين الحقوقية والأدبية ، بيروت ،ط 1، ص 569

[3] – على بن سالم العدوي، مكافحة التجسس الإلكتروني في القانون العماني مقارنة بالشريعة الإسلامية والقانون الجنائي الدولي، المؤتمر الدولي الأول ، كلية العلوم الشرعية، تحديات الواقع وآفاق المستقبل، ديسمبر 2018 م

الواقع أثبت أن هذه البرامج قد استهدفت حتى الدول الحلفاء للولايات م أ. وهذا ما تسبب في حدوث عدة أزمات سياسية ودبلوماسية، مما دفع بأغلبية الحكومات كذلك الشركات إلى اعتماد أساليب جديدة في حماية نفسها ومواطنيها من عمليات التجسس الواقعة ضدها[1].

المطلب الثاني : أهداف ووسائل التجسس عبر الإنترنت

يعتمد المتجسسون من أجل تحقيق أهدافهم على العديد من الوسائل في سبيل الحصول على المعلومات. وسنعرض هذه الأهداف والوسائل في ما يأتي:

الفرع الأول : أهداف التجسس عبر الإنترنت

تتنوع أهداف التجسس عبر الإنترنت حسب المعلومات التي يستهدفها المتجسسون، إما معلومات ذو طبيعة اقتصادية أو عسكرية أو أمنية أو سياسية.

الفقرة الأولى : المعلومات الاقتصادية

إن سرقة المعلومات الاقتصادية أصبح الشغل الشاغل للكثير من أجهزة المخابرات لـــدى بعض الدول، إضافة إلى بعض المنظمات الإرهابية وعصابات المافيا للأهميـــة العظمـــى للاقتصاد في نمو الدول وتقدمها .

فالاقتصاد يعد من العوامل الرئيسية في حفظ استقرار الدولة وسيادتها، لذا تسعى أغلب الدول جاهدة للإبقاء على معلوماتها الاقتصادية رهينة الكتمان، وتضع من الوسائل ما يحفظ من انتقالها إلى جهات أخرى، لذلك نجد أن نسبة التجسس الاقتصادي عبر الإنترنت من قبل الجهات المستفادة يستهدف دائما موارد الدول وحجم إنتاجها واحتياطاتها ومكان تواجدها ومكان قوتها الاقتصادية ومكان تواجد الثغرات الاقتصادية لديها، ومحاولة الوصول إلي مواطن الضعف المتواجد في هياكلها الاقتصادية.[2]

الفقرة الثانية : المعلومات السياسية

يعد التجسس السياسي من أهم أنواع التجسس عبر الإنترنت لكونه يستهدف المعلومات المتعلقة بالحركة السياسية في الدولة من نشاط سياسي داخلي أو خارجي، بالإضافة إلى

---

[1] –https://www.francetvinfo.fr/monde/espionnage-d-internet/Espionnage américain

[2] – ممدوح الشيخ ، التجسس التكنولوجي سرقة الأسرار الاقتصادية و التقنية ، مكتبة بيروت ، سلطنة عمان ، 2007، ص 133،135

رصد التحركات والنشاطات المتعلقة بالقادة والرؤساء ومختلف الأحزاب السياسية في الدولة من اجل التكهن بالخطوات المستقبلية التي ستنتهجها الدولة. كما يهدف هذا النوع من التجسس إلى معرفة ثقافة وقيم المجتمع وكذلك عوامل الوحدة والتفرقة لديه، أيضا معرفة الشخصيات الفعالة فيه، وذلك من اجل محاولة استنباط مواطن القوة والضعف السياسي في الدولة، الأمر الذي تنتهجه اغلب الدول الكبرى من اجل إيجاد الطريقة لفرض السيطرة على الدول سياسيا، وذلك عن طريق اختراق اغلب أجهزة الكمبيوتر في العالم، وهذا ما جاء به "خابر يزيوكالف" و"تيري بيستيه" في كتابهما " عين واشنطن" أين كشفوا من خلال كتابهما عن قيام جهاز المخابرات الأمريكية وجهاز الموساد الإسرائيلي في قرصنة المعلومات المسجلة في اغلب الأجهزة الالكترونية المتواجدة عبر العالم والتجسس عليها، وذلك من خلال نصب كمين لأنظمة المعلومات التي تنقل نسخة من المعلومات المخزنة على هذه الأجهزة عبر برنامج معلوماتي تبيعه أمريكا لمعارضي وأعداء إسرائيل. ومن طرف إسرائيل لأعداء أمريكا وخصومها. ويذكر الكتاب أيضًا وجود ما يسمى بمركز المعلومات العالمي، حيث يتم تخزين جميع المعلومات التي يجمعها البرنامج المذكور أعلاه، كما كشف ذلك عن وجود شبكة عالمية ضخمة تسمى "أشلون" تديرها وكالة المخابرات المركزية الأمريكية إلى جانب عدة أجهزة بريطانية وكندية وأسترالية ونيوزيلندية، مهمتها رصد الرسائل بكل أنواعها ومنها الرسائل الالكترونية وتقوم بتحليلها والاستفادة بالمعلومات المهمة فيها.[1]

الفقرة الثالثة : المعلومات العسكرية

تعد المعلومات العسكرية والأمنية من أهم المعلومات الخاضعة للتجسس لكونها تتعلق بالأمن القومي للدول، فابرز ما يستهدفه التجسس الالكتروني هو كل ما يخص الجيوش وأسلحتها ومعداتها الحربية وذخائرها، وكذا التجهيزات والمواقع العسكرية، كما يستهدف الخطط الحربية وأسرار الدفاع، ومراكز أجهزة الاتصالات وأماكن تمركز القوة العسكرية ومكان القوة والضعف فيها، والبرامج العسكرية والنووية وأماكن تواجدها خاصة من طرف الدول الكبرى فيما بينها. وإذا كان التجسس العسكري ينشط وقت الحرب فانه لا يقل نشاطا وقت السلم وذلك تحسبا للحرب أو الاستعداد لها.

[1] – المناعسة أسامة واحمد الزغبي، المرجع السابق، ص 302

إن برامج القرصنة العسكرية والتجسس الإلكتروني هي منتجات شركات لها علاقات بأجهزة الاستخبارات العالمية، مثل كل الفيروسات التي تم إنشاؤها بغرض التدمير الإلكتروني، فهي أيضًا منتجات نفس الأجهزة.[1]

وتعتبر "إسرائيل" الأولى عبر العالم في عمليات التجسس الإلكتروني وتمتلك 27 شركة متخصصة في هذا المجال، وتمتلك ثمانية ألاف ومئتين وحدة في التجسس الإلكتروني، وفي حال إحالة أحد أعضاء هذه الوحدة على المعاش، يتم تدريب أشخاص آخرين يتم جلبهم من شركات إسرائيلية مختصة في هذا المجال.[2]

إن التجسس العسكري لا يقتصر على الدول في ما بينها فقط، إذ تتبعه أيضا بعض المنظمات والجماعات الإرهابية مستخدمة المعلومات العسكرية المتحصل عليها من التجسس في زعزعة استقرار الدول، أو بابتزازها لتفرض سيطرتها ووجودها عبر العالم، خاصة في كل ما يتعلق بالسلاح النووي الذي تسعى بكل الطرق الوصول إليه.

الفرع الثاني: وسائــل التجسس عبر الانترنــت

تتنوع الوسائل والتقنيات المستخدمة لأغراض التجسس ومن أهمها:

أولا: الفيروسات

حصان طروادة هو الاسم الرسمي لبرامج التجسس الذي تستخدمه أجهزة الأمن وتمكنها من اختراق الأجهزة التي يمكن ربطها بالإنترنت. ويختفي هذا الفيروس داخل تطبيقات الحاسوب أو الهاتف الذكي أو داخل مقاطع فيديو أو ملفات نصية أو صور فوتوغرافية. وباستقبال المستخدم لهذه الملفات ينصب الفيروس نفسه في الحاسوب دون أثر لذلك، ومن خلال ذلك يمكن للجاني فرض سيطرته على جهاز الضحية[3]. بمجرد تثبيت حصان

---

[1] – لوادي حسنين المحمدي ، إرهاب الإنترنت الخطر القادم ، دار الفكر الجامعي ، الإسكندرية ، طبعة 1، 2006، ص55

2 – كيف غيرت التكنولوجيا أساليب التجسس؟ على الموقع التالي:

https://www.noonpost.com/content/36070 تم الاطلاع عليه في 2020/06/17

[3] – الحسيني عمار عباس، جرائم الحاسوب والإنترنت"الجرائم المعلوماتية" ، منشورات زين الحقوقية، بيروت ، ط2، 2019 ، ص334

طروادة على جهاز الكمبيوتر، يتم فتح الباب الخلفي، حتى يتمكن المرسل مراقبة كل ما يفعله مالك الحاسوب أو الهاتف الذكي، ونسخ الملفات والبحث على القرص الصلب بطريقة سرية خاصة وأن الأجهزة الذكية المتقدمة كلها مزودة بميكروفونات وكاميرات، فضلا عن إمكانية الاستماع إلى المكالمات الهاتفية والمحادثات عبر برامج الاتصال المتعددة مثل Skype. وقد تم مؤخرا إطلاق إصدار جديد من برنامج حصان طروادة والذي يعد استخدامه قانونيًا حيث تمت برمجته للسماح باستخدامه فقط بالطرق المعتمدة للمراقبة الإلكترونية[1].

ثانيا: تقنيات إنترنت الأشياء

تعد إسرائيل أكبر وحدة خبيرة في التجسس عبر الإنترنت، وتعد الوحدة المسؤولة عن الحرب الإلكترونية في إسرائيل. وتكشف هذه الممارسة عن تطور ازدياد استخدام الأجهزة الاستخبارية للإنترنت وهو ما يعرف بالتجسس الالكتروني "السيبار الذكي"، والذي يعتمد على استعمال الفضاء السيبيراني في تنفيذ مهامه الاستخبارية، إلى جانب استخدامه من طرف المنظمات الإرهابية، وقد أثبتت الدراسات أن إسرائيل والولايات المتحدة الأمريكية يبحثان عن تقنيات يمكن من خلالها اختراق أنظمة السيارات والحافلات لتوسيع مجال التجسس.[2]

ثالثا: القرصنة عبر الملاك الباكي

Weeping Angel هي تقنية مراقبة تُستخدم لإصابة أجهزة التلفزيون الذكية والهواتف الذكية وحتى السيارات الذكية، وتحويلها إلى أجهزة تنصت حتى عند إيقاف تشغيلها. وتقوم بتسجيل كل ما يتم حدوثه في المنزل أو الغرف ليتم إرساله عبر الإنترنت إلى الخادم الخاص بالمرسل.

رابعا: البريد الالكتروني

يستعمل البريد الالكتروني في عمليات التجسس على دول وهيئات ومنظمات وأفراد. وعمليات التجسس تتم في حالات المنافسة بين الحكومات أو المؤسسات أو الشركات أو

---

[1] – الحسيني عمار عباس،جرائم الحاسوب والإنترنت ، المرجع السابق ، ص334

[2] – أساليب التجسس الإلكتروني المتقدمة. على الموقع:https://futureuae.com/ar/Mainpage/Item/2631

الأفراد، ومن أهداف التجسس باستخدام البريد الالكتروني إمكانية التعرف على مشاريع الشركات المنافسة، فهذا قد يمكنها من الاطلاع علي من يسبقهم في صفقة أو مشروع معين. وعليه فان المراسلات الكترونية لا تتمتع بسرية حقيقية، وإنما يمكن في أي لحظة أن يتعرض الشخص للقرصنة أو يكون ضحية لعمليات تجسس تتم من خلال الشبكة العنكبوتية. ولقد تبين أخيراً أن خدمة البريد الالكتروني الأوسع انتشاراً في العالم بأكمله هي الأخرى عرضة للاختراق والتجسس، وأن طرفاً ثالثاً غير المستخدم والشركة المالكة للخدمة يمكنه الدخول والوصول إلى الرسائل.[1]

خامسا: مواقع التواصل الاجتماعي

تعد مواقع التواصل الاجتماعي وسيلة للتجسس باستعمـــــال الإنترنت وذلك باختراق مواقع الضحايا المراد التجسس عليها. وفي هذا الشأن أقام تطبيق واتس اب دعوى قضائية ضد شركة إسرائيلية خلال شهر نوفمبر 2019، متهما إياها بمساعدة وكالات تجسس حكومية على هكترة ما يقرب من 1400 هاتف ذكي عبر العالم مستهدفين بهذا الاختراق معارضين سياسيين ديبلوماسيين ومسؤولين حكوميين وصحفيين. وفي سنة 2018 تم اختراق تطبيق واتساب بطريقة كبيرة من خلال برامج ضارة. فبمجرد فتح التطبيق، يصبح المتسللون قادرين على تنزيل كمية مفخخة من برامج التجسس ويمكن للمخترقين الوصول إلى الجهاز عن طريق مكالمة يتم تعليقها مباشرة. هذا هو ما يُعرف باسم تكنولوجيا Zero Click . وأصدرت واتساب برامج تصحيحات سريعة لإصلاح هذه المشكلة لمستخدميها الذي يفوق مليارين شخص، لكن دون التوصل لمن يقف وراء الهجوم[2] .

المطلب الثالث : أركـان التجسس عبر الإنترنـــت

من المعروف أن أي جريمة من الجرائم لها ركنان، مادي ومعنوي، ويشتمل الركن المادي في جريمة التجسس عن طريق الإنترنت في غالب الحالات على الوسائل التي

---

[1] - – التجسس الرقمي، على وسائل التواصل الاجتماعي على الموقع التالي:
https://www.europarabct.com

[2] – التجسس الرقمي، على وسائل التواصل الاجتماعي على الموقع التالي:
https://www.europarabct.com

يستخدمها المجرم في سبيل تحقيق جريمته، والمجالات التي يستهدفها من ذلك، أما الركن المعنوي فيشتمل على عنصري العلم والإرادة .

الفرع الأول : الركـــــن المـــادي للتجسس عبر الإنترنــت

الركن المادي في جريمة التجسس عبر الإنترنت هو النشاط الإجرامي الذي يقوم به الجاني لجمع معلومات مهمة وحساسة بشكل غير قانوني باستخدام الوسائل المتوفرة عبر شبكة الانترنت بهدف تحقيق النتيجة المرجوة المتمثلة في استخدام هذه المعلومات لأغراض شخصية أو مالية أو لأغراض إرهابية ضد الدول أو المؤسسات أو الأفراد، فهذا النوع من السلوك يقف على الوسائل التي يتبعها المجرمون للحصول على الأسرار والمعلومات.

الفرع الثاني : الركـــــن المعنـــوي للتجسس عبر الإنترنت

تعتبر جريمة التجسس باستعمال الإنترنت من الجرائم العمدية التي تتطلب علم الجاني بأنه يقوم بفعل مخالف للقانون بدخوله في نظام الكتروني بطريقة غير مشروعة والوصول إلى المعلومات السرية ذات الصلة بالاقتصاد أو الأمن أو الدفاع أو السياسة، فالمجرم يعلم انه يعتدي على حق حماه القانون ويعاقب على إتيانه، والمتمثل في الاطلاع والاستحواذ على معلومات سرية وغير متاحة بغير حق، وتكون إرادته متجهة إلى إحداث النتيجة الجرمية المقصودة بالدخول إلى النظام الالكتروني باستعمال الإنترنت، كما تتطلب هذه الجريمة قصدا خاصا يتمثل في القصد الجاني ونيته في الإطلاع على معلومات سرية لا يجوز له الاطلاع عليها.[1]

ملخص الباب الأول

لقد تنوعت وتشعبت الصور الإجرامية عبر الإنترنت، وأصبحت ظاهرة تهدد العالم بأسره، وليس من اليسر حصر هذا النوع من الجرائم بسبب تشعبها واختلاف أنواعها وسرعة تطورها، مما استلزم علينا الأخذ بالتقسيم التقليدي للجريمة والذي تبناه الكثير من الباحثين كونه ملما بمختلف معايير التقسيم. وهذا التقسيم يضم كلا من طائفة الجرائم الواقعة على الأشخاص، والجرائم الواقعة على الأموال، إضافة إلى الجرائم الماسة بأمن الدول.

[1] - الحسيني عمار عباس، المرجع السابق 334

تعتبر جرائم الاعتداء على الأشخاص عبر الإنترنت من أحد أكثر أنواع الجرائم العصرية ووقوعا وانتشارا، فهي جرائم يتم ارتكبتها عبر شبكة المعلومات العالمية وخدماتها المتاحة، إذ يساء استخدامها للمساس بحياة الغير والنيل من شرفهم أو كرامتهم أو اعتبارهم أو حياتهم أو أخلاقهم أو معتقداتهم أو ديانتهم. فهي تلك الجرائم التي أصبحت تهدد بالحقوق اللصيقة بالإنسان خاصة في الفترة الأخيرة التي زاد فيها استخدام مواقع شبكة الإنترنت بشكل ملحوظ، خاصة أنه خلال هذه الفترة كان هناك زيادة حادة في استخدام الهواتف الذكية، مما ساهم في إدراج عدد كبير من الأشخاص في سجلات الخدمة. وبعد انتشار وتنوع خدمات الإنترنت وزيادة الطلب عليها أصبح الأفراد ينظرون إليها على أساس أنها من متطلبات الحياة اليومية.

ونتيجة للاستعمال المفرط للإنترنت واتساع دائرة الإعلام والاتصال الالكتروني عبر الشبكة، ساعد مرتكبو الجرائم في تنفيذ جرائمهم واعتداءاتهم ضد الأشخاص، وتأتي في مقدمتها الجرائم الماسة بالسمعة والشرف عبر الإنترنت والمتمثلة في جريمة السب والقذف والتشهير، وبعدها تأتي الجرائم الماسة بالأخلاق والآداب العامة المرتكبة عبر الإنترنت والمتمثلة في انتشار نوادي القمار عبر الإنترنت والجرائم الإباحية والجنسية واستغلال الأطفال جنسيا هذه الأخيرة التي تعتبر من أخطر الجرائم التي يمكنها أن تمس بالطفل. فقد أدى ظهور شبكة الإنترنت إلي توفير الوسائل الأكثر فعالية لإنشاء محتوى إباحي وجنسي، وأصبح العالم اليوم يعيش ثورة جنسية فاقت كل الحدود وتجاوزت كافة القيود، ولقد أشارت الإحصائيات إلى وجود ما يفوق 400 مليون صفحة مروجة للمواد الجنسية عبر الإنترنت، وأن أكثر مستخدميها يقل عمرهم عن 18 سنة. الأمر الذي يجعل من الجرائم الجنسية أشد الجرائم خطرا وأثرا على جل المجتمعات خاصة الإسلامية.

أما جرائم العنف فتتمثل في جريمة انتهاك حرمة حياتهم الخاصة، إضافة إلى الجرائم التي سهلت التكنولوجيا القيام بها وهي جرائم القتل والتحريض على القتل والانتحار باستخدام الإنترنت، وجريمة القتل كانت في كثير من الأذهان جريمة يستحيل وقوعها عبر الإنترنت لذلك لم يقم أيا من الباحثين بتصنيفها ضمن الجرائم الواقعة عبر الإنترنت .

أما الجرائم الواقعة على الأموال فبتطور الإنترنت واستخدامها في جميع مجالات الحياة وزيادة مستخدميها بصفة مكثفة ساهم في ظهور عدة مفاهيم جديدة، خاصة في مجال التعاملات الالكترونية والتي بدورها أدخلت معها مفهوما حديثا للأموال وهو ما يطلق عليه تسمية الأموال الالكترونية، وهذا النوع يظهر أساسا في عمليات السحب والإيداع من أجهزة الصراف الآلي. ومن خلال هذه التطورات تحولت جريمة السرقة من سرقة تقليدية إلى سرقات تستهدف المعلومات وقيمتها الاقتصادية كما ساهم في انتشار جرائم الاحتيال والنصب عبر الإنترنت التي تعد من أكثر الجرائم انتشارا خاصة في الفترة التي انتشر فيها وباء كورونا ووصلت إلى أرقام قياسية، وذلك لسهولة ارتكابها عبر شبكة الإنترنت. وتبعا لما سبق عمد القضاء إلى تصنيف الجرائم الواقعة على الأموال الغير ملموسة الناتجة عن المعلوماتية في حيز الجرائم الواقعة على الأموال المادية والملموسة، خاصة وأن المشرع الجزائري عند صياغته للنصوص التقليدية الخاصة بجرائم الأموال لم تكن لمفاهيم الأموال الالكترونية وجود. وأبرز الجرائم الواقعة على الأموال باستخدام الإنترنت والتي يشهدها العالم في وقتنا الحديث هي جريمة السرقة خاصة سرقة بطاقات الوفاء والدخول إلى مواقع البنوك وحسابات العملاء، أما صور التحويلات الالكترونية غير المشروعة للأموال فتجسدت في جريمة الاحتيال عن طريق بطاقات الدفع الالكتروني والاحتيال التجاري الالكتروني، إضافة إلي هذه الجرائم جريمة الاتجار غير المشروع بالمخدرات والمؤثرات العقلية عبر الإنترنت التي طالت كل الفئات، وجريمة الاعتداء على الملكية الفكرية التي تندرج ضمن الجرائم المالية التي تتم عبر الإنترنت.

وفي ضل الأزمة الصحية التي مست العالم بانتشار فيروس كوفيد 19 الذي كان من نتائجه انفتاح كل العالم على الإنترنت لكونها أصبحت الوسيلة الوحيدة للاتصال بالعالم الخارجي، عرفت الجريمة عبر الإنترنت تفشيا وارتفاع كبير في معدلاتها لم يسبق له نظير، خاصة الجرائم المستهدفة للأموال والأمن الوطني مثل جريمة الاحتيال عبر الإنترنت والسرقة والتزوير والقرصنة وزيادة كبيرة في ترويج المخدرات، ولقد شهدت أغلب الدول المصابة بالفيروس موجة من جرائم الاحتيال والنصب التي لم يسبق لها نظير ووصلت الخسائر التي خلفتها هذه الجرائم إلى مليارات الدولارات.

أما الجرائم الماسة بأمن الدولة هي الجرائم التي تهدد أمن سيادة الدولة وأراضيها واقتصادها وسلامة مواطنيها، وغالبا ما تعرض مؤسساتها للخطر، ومن أهدفها أيضا زعزعة كيان الدولة في المحيط الدولي، أو تجزئة أراضيها أو شل دفاعها والإساءة إلى علاقاتها أو تغير علاقاتها، ومن أهم هذه الجرائم جريمة الإرهاب عبر الإنترنت وجريمة غسيل الأموال عبر الإنترنت وجريمة التجسس باستخدام الإنترنت.

ومع ظهور الإنترنت، التي تعد من أحدث تطورات هذا العصر وأبرز وسيلة اتصال وبوابة مفتوحة على العالم. ازداد وجه الجرائم الماسة بأمن الدول قبحاً وخطورة وانتشارا عما كان عليه في الماضي، وتسبب في سقوط وانهيار عدة دول من جميع النواحي الاجتماعية والسياسية والاقتصادية، وإعاقة تطورها وجعلتها تغرق في فتنٍ وابتلاءات عمياء يصعب الخروج منها. والإرهاب أسرع من قام باستخدام هذه التقنية الحديثة، و من خلاله ظهر نوع حديث من الإرهاب، وهو من أسوأ أنواع الإرهاب في خطورته وأضراره الضخمة، ألا وهو الإرهاب الإلكتروني Cyber Terrorism، حيث يمارس من خلال شبكة الإنترنت العديد من صور الإرهاب، إذ قام بإنشاء عدة مواقع على الإنترنت من طرف جماعات إرهابية لممارسة أنشطتهم المختلفة عبرها، كإقناع الشباب عبر الإنترنت بفكرهم المتطرف وأفكارهم الإرهابية الهدامة وغسل عقولهم لتجنيدهم وحثهم على الالتحاق بصفوفهم سواء كانوا ذكورا أو إناثا، أيضا من اجل التحريض على القتل أو العنف، وإتلاف الممتلكات والأموال العامة، ولتعليم صناعة القنابل والمتفجرات اليدوية أو كيفية تفجيرها.

ومن الجرائم التي تمس بأمن الدولة جريمة التجسس التي تغيرت أساليبها في ظل التطور التكنولوجي المعلوماتي، وأصبحت كل المعلومات السياسية والاقتصادية والعسكرية من الممكن الوصول إليها بكل سهولة، فالتطور الالكتروني وثورة المعلومات والإنترنت التي قربت المسافات وأسقطت الحدود، الأمر الذي خلق فضاءً جديداً لعالم الجواسيس يتحركون فيه دون عناء وقيود ومراقبة من أجل الحصول على المعلومات، وباتت حرب المعلومات يتم خوضها والانتصار فيها بقدر ما يُتَحَصَل عليه من معلومات عن الخصم سواء كان فرداً أو شركة أو مجتمعاً أو دولة. فبظهور التجسس الالكتروني" أو ما يعرف بالتجسس باستعمال الإنترنت، والذي يتمثل في القدرة على اختراق المواقع الالكترونية، أو عن طريق التسلل إلى أجهزة

الكومبيوتر، أو اعتراض المعلومات المرسلة من الحاسوب باستخدام الإنترنت وسرقتها، وإن الضرر الناجم عن التجسس على أنظمة المعلومات التي تحكم جميع المرافق المعتمدة على استخدام أجهزة الكمبيوتر والإنترنت يعطل المجتمع بأسره، وبالتالي يضر بالأفراد والشركات والدول بأكملها، والخسائر التي تلحق نتيجة للتجسس هي أشد بكثير مما قد يتصوره الإنسان.

ومن الجرائم الاقتصادية الماسة بأمن وسلامة الدول جريمة غسل الأموال، هذه الجريمة التي تعد من الجرائم المستحدثة والتي يتم ربطها غالبا بالجريمة المنظمة، وفي ظل التطور الهائل في المجال الالكتروني تطورت واختلفت صورها، خاصة استخدام الإنترنت الذي يتقنه بعض المجرمين لتنفيذ مجموعة واسعة من الجرائم المالية المتطورة.

وجريمة غسيل الأموال هناك من صنفها على أنها جرائم مالية وهناك من صنفها على أنها جرائم تهدد استقرار وأمن الدول مثلها مثل الإرهاب.

ويعتبر غسيل الأموال عبر الإنترنت جريمة ولدت عائدات مالية ضخمة من الأموال القذرة التي يتم إعادتها إلى الاقتصاد العالمي عبر الإنترنت من خلال الأموال الإلكترونية، وغيرها من الأنشطة المالية والتجارية، ففي ظل الانفتاح العالمي وترابط الأسواق وتداخل الاقتصاد وزيادة الترابط المالي بين جهات مختلفة عبر العالم أصبحت تجارة القمار والاتجار بالأسلحة والدعارة والرقيق تتم باستخدام تقنيات شبكة الإنترنت، ويتم تنظيمها إلكترونيا بشكل يدر أرباحا طائلة ويولد أموالا يضطر أصحابها في أغلب الأحيان إلى غسلها وإدخالها في الدورة الاقتصادية العالمية بعيدا عن أي شكل من أشكال الرقابة وأجهزة المتابعة.

وفي صدد الحديث عن الجرائم الماسة بأمن الدولة شهدت الجزائر في فترة تفشي فيروس كورنا استغلال بعض الأشخاص انتشار المرض ونشروا بعض الأخبار المضللة عبر مختلف شبكات التواصل الاجتماعي والتي كان الهدف من وراءها تخويف الأفراد وبث الإحساس بعدم الأمان لديهم، الأمر الذي كان له التأثير الكبير على بعض التصرفات التي قام بها العديد من أفرد المجتمع كإقبالهم على تكديس المواد الغذائية لخوفهم من نفاذها في السوق، مما أدى السلطات العليا للتحذير من مثل هذه الأعمال التي من شأنها المساس

بسلامة المواطن وأمنه لافتين انتباههم بأن القانون سيعاقب كل شخص قام بنشر خبر أو شائعات على أي موقع إلكتروني بقصد المساس بأمن الدولة أو الإضرار بأي من مؤسساتها. إضافة إلى هذا تم تحريم الشائعات في وقت الأزمات من طرف المجلس العلمي للإفتاء. إضافة إلى هذا سجلت المصالح المعنية حسب الأرقام التي أدلت بها جريدة الشروق قرابة 8 آلاف جريمة إلكترونية خلال سنة 2020، وهي أرقام قياسية مقارنة بالسنوات الماضية.

على الرغم من أن أزمة كورونا " كوفيد 19 " فرضت تحديات كثيرة على الدول من أجل التعامل مع العدوى وفقا لآليات الوقاية والعلاج المفروضة، إلا أن ذلك لم يمنع التنظيمات المتطرفة عن القيام بأعمالهم الإرهابية عبر الإنترنت، حيث شهد عدد من الدول ممارسة أعمال إرهابية و هجمات إلكترونية شكلت تهديدا على أمنهم واستقرارهم، إذ قامت العديد من التنظيمات المتطرفة في استخدام الإنترنت من أجل بث خطابات الكراهية ونشر الآراء المتطرفة. إذ تشير المعطيات إلى أن الجماعات الإرهابية استغلت مزايا الإنترنت كعنصر حيوي لدعم وتحقيق أهدافها الهدامة.

الباب الثاني :

أثر العدوان الإجرامي عبر الإنترنت وآليات مكافحته

لقد وفرت التطورات الحديثة في التكنولوجيا مجموعة متنوعة من الآليات التي أتاحت المجال أمام العديد من المجرمين لارتكاب جرائم بتكاليف وبمخاطر أقل. وبالتالي فإن الجرائم التقليدية أصبحت ترتكب إلكترونياً على نطاق أوسع دون أي رادع حقيقي لها. مما أدى إلى ارتفاع معدلات الجرائم بصورة كبيرة، مخلفة وراءها العديد من المخاطر والأضرار.

إن الانشغال بمخاطر جرائم شبكة المعلومات، والآثار الخطيرة التي تترتب عنها خاصة وأنها عقبة أمام تنمية الإنسان على جميع المستويات، أدى بالعديد من الدول إلى سن قوانين مختلفة بشأن هذه الجرائم، وتم إبرام العديد من الاتفاقيات الدولية والإقليمية للتصدي لتزايدها، وربما أهمها اتفاقية بودابست الموقعة في 2001/11/23 تحت رعاية مجلس أوروبا.

لقد أصبحت مسألة الآليات القانونية لمكافحة الجرائم عبر الإنترنت موضوع اهتمام أغلب المشرعين، مما وسع نطاق التعاون بين رجال القانون والمتخصصين في مجال التكنولوجيا الرقمية على الصعيد الوطني والمجتمع الدولي بغية سن قوانين تكافح مرتكبي هذه الظاهرة الإجرامية.

ولهذا خصصنا هذا الباب لدراسة الآثار المترتبة على الجرائم المرتكبة عبر الإنترنت، مع إبراز آليات التصدي لهذه الظاهرة مع معرفة مدى كفاية النصوص القانونية الحالية لمنع هذه الجرائم، والحاجة الماسة لخلق أحكام قانونية جديدة لمحاربتها. ولقد تم التطرق لذلك من خلال الفصلين التاليين :

الفصل الأول : الآثار المترتبة على العدوان الإجرامي عبر الإنترنت

الفصل الثاني: آليات مكافحة الجريمة عبر الانترنت على المستوى الوطني والدولي

الفصل الأول :

الآثار المترتبة على العدوان الإجرامي عبر الإنترنت

لقد ساهمت العولمة والمعلوماتية وعدة عوامل منها الاقتصادية والصناعية والتجارية والأخلاقية والاجتماعية والسياسية إلى بروز جرائم الإنترنت وانتشارها في أغلب أنحاء العالم، وهو ما اتبعه تنامي المخاطر الناجمة عنها كما ونوعا، بشكل أصبح يهدد كافة فئات المجتمع، وأصبح الجميع عرضة لجرائم متعددة كالتشهير والابتزاز والتحرش والإغواء الجنسي وسرقة البيانات الشخصية، والاحتيال والتجسس وغيرهم من الجرائم الخطيرة.

لقد ترتب على الجرائم الإلكترونية انعدام أو قلّة الثقة والأمان تجاه استخدام الأجهزة الإلكترونية المتصلة بالإنترنت، بسبب ما ترتبط به من جرائم ومخاطر وخيمة. فالجرائم عبر الإنترنت تعد وباء ينهش ويفتك بالمجتمعات وبالعلاقات الإنسانية، وبأمن وسلامة المجتمع، ويعد سبب رئيسي في تأخير عجلة التقدم والتنمية التي يعيشها العالم مؤخرًا بسبب الخسائر الاقتصادية الناتجة عنها، فوفقا لما ذكر في تقرير جاءت به مجلة الجرائم الإلكترونية في أواخر سنة 2021، أن الجرائم الالكترونية بأنواعها المختلفة قد كلفت الاقتصاد العالمي أكثر من 6 تريليون دولار عام 2021 ويتوقع أن تصل تكلفة هذه الجرائم على الاقتصاد العالمي نحو 10,5 تريليون دولار سنويا بحلول 2025.[1]

إن للجريمة عبر الإنترنت لها تأثير بالغ على كافة المجالات والمستويات، حيث لم تقف عند المجال الاقتصادي بل تعدته لتمس بالمجتمع من الناحية الاجتماعية، من خلال الجرائم الأخلاقية، وجرائم الإساءة بسمعة الأفراد وإظهارهم بصورة غير لائقة أمام المجتمع المحيط بهم، إضافة إلى حالات الانتحار التي تسببت فيها جرائم التهديد والابتزاز خاصة التي تقع على الإناث من خلال الإنترنت، ذلك أن إحصائيات الحالات الاجتماعية للمجني عليهن في جرائم الابتزاز والتهديد المعلوماتي تصل إلى أرقام مخيفة تتصدرها الفتيات العازبات ومن ثم تأتي النساء المتزوجات ثم المطلقات ثم الأرامل. ناهيك عن المخاطر التي تهدد بأمن وسيادة الدول، بسبب جرائم القرصنة والتجسس وجرائم الإرهاب المتواصلة

[1] – تحذيرات من ارتفاع تكلفة الجرائم الإلكترونية لـ10.5 تريليون دولار: على الموقع التالي
https://www.independentarabia.com/node/34619

التي تعرض الجهات والأجهزة الحكومية للخطر، الأمر الذي يؤدي حتما إلى زعزعة الأمن والاستقرار، وبذلك تتحمل الدول المستهدفة خسائر كبيرة.

وبما أن التكنولوجيا أصبحت تتحكم في وسائل الإعلام وفي الوسائل الترفيهية هذا سيؤدي حتما إلى نشأة جيل جانح لا يهتم لا بالقوانين ولا بالأخلاق ولا بجوهر الإنسانية.

وتعتبر مواقع شبكات التواصل الاجتماعي هي الأكثر شيوعاً على شبكة الإنترنت نظراً لما يميزها عن المواقع الأخرى، مما شجع متصفحي الإنترنت حول العالم على الانخراط فيها واستخدامها بشكل أكبر على الرغم من الانتقادات اللاذعة التي تتعرض لها. ومن هذه الانتقادات تأثيرها السلبي على الأسرة والمشاكل التي تحدث بداخلها، فهناك من يرى أنها وسيلة مهمة للتقدم والتماسك بين المجتمعات. ولدمج الأفكار ووجهات النظر مع الآخرين ودراسة ثقافات الأمم المختلفة. إضافة لدورها الفعال والمتميز كوسيلة اتصال ناجعة، الأمر الذي جعل منها أرضية خصبة وسهلة لارتكاب الجرائم عبرها.

وعليه سيتم تقسيم هذا الفصل إلى مبحثين:

المبحث الأول : مدى تأثير شبكات التواصل الاجتماعي على المجتمع

المبحث الثاني: الآثار المترتبة عن الجرائم المرتكبة عبر الإنترنت

المبحث الأول

مدى تأثير شبكات التواصل الاجتماعي على المجتمع

لقد ساهمت شبكات التواصل الاجتماعي الموجودة على الإنترنت في إنشاء المجموعات الافتراضية وتطويرها كجزء من عملية نقل العلاقات الاجتماعية بين أعضاء المجتمع من الحياة الواقعية إلى العالم الافتراضي، فهي أدوات مفيدة لتبادل المعلومات والخبرات والمحادثات، فضلا عما تضمه هذه النظم الاجتماعية من عدد كبير للأعضاء ذوي الاهتمامات المشتركة.

وبالرغم مزاياها المتعددة، إلا أنه تم استخدامها من قبل المجرمين والجماعات الإرهابية لتنفيذ أهدافهم المدمرة ضد المجتمع، وبالتالي التأثير على العقل ومواءمته مع اتجاه فكري أو إيديولوجي معين، إضافة إلى هذا استغلالها لتعزيز ثقافة العولمة في دول العالم الثالث. مما يستوجب في هذه الدراسة التعرف على أهم شبكات التواصل الاجتماعي، والوقوف على أهم الآثار المترتبة على استخدامها سواء على الأفراد أو على المجتمع بأكمله. وسنتناول ذلك في مطلبين كما يلي:

المطلب الأول : مفهوم مواقع التواصل الاجتماعي

المطلب الثاني : أساليب استخدام مواقع التواصل الاجتماعي

المطلب الأول : مفهوم مواقع التواصل الاجتماعي

تعددت مواقع التواصل الاجتماعي وتنوعت خدماتها لتحقيق مختلف الإشباعات لمستخدميها، وتجاوز الأمر اعتبارها وسيلة من وسائل الاتصال والتفاعل مع الآخرين في أوقات الفراغ وأصبح إدمانًا لا يمكن الاستغناء عنه، وقبل التطرق لأنواع مواقع التواصل الاجتماعي، سنتناول أولا مختلف التعاريف التي تضمنته.

الفرع الأول : تعريف مواقع التواصل الاجتماعي

لقد تناول العديد من فقهاء تكنولوجيا المعلومات مفهوم الشبكات الاجتماعية المرتبطة بتكنولوجيا المعلومات.

وقد تم تعريفها على أنها مواقع الويب التي توفر لمستخدميها مجموعة من الخدمات بخيارات متعددة، مثل الدردشة الفورية ومشاركتها مع أشخاص آخرين "[1].

كما أنها عبارة عن أجهزة ومواقع تسمح للمستخدمين بمشاركة المعلومات حول العالم. وتُستخدم لإزالة المسافة الافتراضية بين الأعضاء ولجمع المعلومات ونشرها ومشاركتها. ومصطلح وسائل التواصل الاجتماعي أطلق عليها لأنها ببساطة منبر للحوارات على الشبكة الالكترونية، فهي أكثر منها طرق تقليدية للتواصل فيما بين الأشخاص.

وقد عرفها قاموس odlis على أنها منصة إلكترونية على شبكة الإنترنت مصممة للمستخدمين لإنشاء صفحات خاصة أو التواصل مع أشخاص آخرين، بهدف والتعاون والترابط والتبادل المعلوماتي، ويمكن للمستخدمين المسجلين فقط الوصول إلى صفحات الأطراف المشاركة، بما في ذلك مجموعات محددة من الأصدقاء أو مستخدمي هذه التطبيقات منها Facebook و Twitter....[2].[3]

ومن التعريفات السابقة يمكننا معرفة أم ما يميز الشبكات الاجتماعية.

- **تبادل الأفكار**. تشجع وسائل التواصل الاجتماعي مشاركة أصحاب المصلحة وردود الفعل مما يسد الفجوة بين وسائل الإعلام والمجتمع.
- **الانفتاح على العالم:** فمعظم وسائل الإعلام عبر مواقع التواصل تفتح مجال المشاركة أو الإنشاء أو التعديل على الصفات، وتشجع التعليق والمشاركة والتصويت، وفي الغالب لا تقيد الوصول إلى المحتوى واستخدامه.
- **المحادثة والتفاعل:** حيث تتميز وسائل التواصل الاجتماعي ووسائل الإعلام الاجتماعية بأنها محادثة ثنائية الاتجاه .

---

[1] – عبد الأمير الفيصل، دراسات في الإعلام الالكتروني، دار الكتاب الجامعي للنشر و التوزيع، الإمارات ،2014 ، ص 6

[2] – مجدوب عبد المؤمن، سفيان، دور شبكات التواصل الاجتماعي في عملية التحول السياسي بتونس 2011-2014 ، المجلة الجزائرية للأمن والتنمية، العدد13 ، 2018، ص273-291

[3] – مركز المحتسب للاستشارات، دور مواقع التواصل الاجتماعي في الاحتساب توتير نموذجا، دار المحتسب للنشر والتوزيع، الرياض، ط1 ، 1438 هـ، ص 16.

- **ترابط المجتمعات:** تتيح الشبكات الاجتماعية للأشخاص بالتواصل بإنشاء صفحاتهم الخاصة في وقت قياسي. وفي جميع أنحاء العالم ترتبط هذه المجتمعات من خلال نفس الاهتمامات والتوجهات. وبهذا يصبح العالم قرية صغيرة ذات روابط قوية
- **شبكة مترابطة في ما بينها:** ترتبط مواقع التواصل الاجتماعي ببعضها البعض وترتبط بمواقع ويب أخرى من خلال الروابط التي توفرها ميزات هذه المواقع.
- **الحضور الغير مادي والمتخفي:** توفر هذه الشبكات إمكانية التواصل دون الحاجة للقاء، وتسمح بترك رسالة نصية أو صورة أو معلومات.[1]
- تشمل وسائل التواصل الاجتماعي نظامًا دوليًا يتجاوز الحدود الإقليمية والوطنية، وهو عالم تقني يعتمد على العناوين الشخصية والتعليمات الخاصة بنقل المعلومات بالوسائل الإلكترونية.

الفرع الثاني :أنواع شبكات التواصل الاجتماعي ومواقع التواصل الاجتماعي

الفقرة الأولى : أنواع الشبكات الاجتماعية

تم تقسيم مواقع التواصل الاجتماعي حسب الغرض من إنشائها أو حسب الخدمات المقدمة إلى ما يلي:

أ –الشبكات الفردية ، وهي شبكات مملوكة للأفراد وتتيح لهم الالتقاء وتكوين صداقات، مثل Facebook أو Instagram.

ب –شبكات ثقافية :تروج للإبداع الفني وتعمل على جمع الأفراد ذات الثقافة المشتركة.

ج –الشبكة المهنية: خاصة بالاهتمامات والصلات بين الأشخاص ذوي الأدوار المتشابهة لخلق بيئة أفضل من الجانب التدريبي والتعليمي .

كما تم تقسيمها أيضاً وفقاً للخدمات أساليب التواصل إلى ما يلي:

أ –شبكات توفر الكتابة للاتصال بالمستخدمين الآخرين.

ب –شبكات الصوت.

ج –شبكات توفر الاتصال المباشر مع الآخرين بالصوت والصورة[2].

[1] – حنون نزهة، استخدام مواقع التواصل الاجتماعي وانعكاساتها على قيم المواطنة لدى الشباب الجزائري دراسة ميدانية على عينة من مستخدمي مواقع التواصل الاجتماعي، مجلة العلوم الإنسانية، العدد الثامن، 2017 ، ص67–80

أيضا تم تقسيمها إلى:

أ –**شبكات خاصة داخلية** Internal Social Networking : هي تتألف من شركة مغلقة أو عدد من الأشخاص يمثلون مجموعة من الأشخاص أو منظمة أو مجتمع، من خلال مشاركة الأفكار والملفات والنقد المباشر وما شابه ذلك، ولا يتم التلاعب برغبات الناس في الدخول والتفاعل مع الموقع والتحكم فيه.

ب –**شبكات عامة خارجية** .Extern at Social Networking : هذه الشبكات مفتوحة لجميع مستخدمي الإنترنت وهي مصممة لجذب الأفراد للمشاركة فيها مثل الفيسبوك وتويتر وغيرها.

الفقرة الثانية : مواقع شبكات التواصل الاجتماعي:

تتميز هذه المواقع بالإقبال الكبير عليها من جميع أنحاء العالم لأنها تجذب انتباه الكثير من الشباب من جميع أنحاء العالم، بما في ذلك العالم العربي والجزائر خاصة.

1–موقع فيس بوك: (Facebook)

يعتبر موقع فيسبوك أحد أهم مواقع التواصل الاجتماعي الافتراضية على شبكة الإنترنت، وهو مصمم ليتيح للمستخدمين التفاعل مع الأصدقاء، حيث يقوم كل منهم بعمل بروفايل شخصي خاص به، يقوم من خلاله بتحميل الصور والرسائل وتكوين مجموعات لها نفس الميول والاهتمامات والرغبات، وقد انطلق الفيس بوك كنتاج غير متوقع من موقع فيس ماتش الذي ابتكره مارك زوكربيرج " في 28 أكتوبر 2003 م، عندما كان طالباً في السنة الثانية بجامعة هارفارد الأمريكية، وهو موقع يقوم بنشر صور لعدد من الأفراد ثم يتم اختيار الشخص الأكثر جاذبية، ثم أطلق زوكربيرج فيس بوك بعد إضافة الكثير من التعديلات على موقع فيس ماتش، وسرعان ما انتشر الموقع بين طلبة الجامعات والمدارس الأمريكية الثانوية واستمر الموقع قاصرا على الطلبة لمدة عامين حتى قرر زوكربيرج فتح أبواب موقعه على الإنترنت لكل من أراد استخدامه، وأدى ذلك إلى نمو مستخدمي الموقع الذي ارتفع إلى 12 مليون مستخدم في ديسمبر 2006، ليصل إلى أكثر من 60 مليون

---

[2] – السلطان مسفر مبارك الصاعدي، الشبكات الاجتماعية خطر أم فرصة، بحث مقدم لشبكة الألوكة، المسابقة الثانية (فرع الدراسات والأبحاث)، المملكة العربية السعودية، 2010 ، ص 10

عضو عام 2007[1]. ولقد سجل مع بداية عام 2021 قرابة 2.8 مليار مستخدم حول العالم. وبهذا احتلت شبكة فايسبوك المرتبة الأولى عالميا.[2]

2-موقع يوتيوب: (You Tube) -

تم تأسيس موقع اليوتيوب عام 2005 من قبل موظفين من الولايات المتحدة الأمريكية يعملون بشركة يطلق عليها اسم pal pay وهم "شاد هارلي" و"جاود كريم" و"ستيف تشن". ويتيح هذا الموقع مشاهدة عدة مقاطع من الأفلام السينمائية والتلفزيونية وفيديوهات موسيقية. وفي عام 2006 تم شراءها من طرف جوجل مقابل 65 مليار دولار. ويعد موقع يوتيوب من مواقع الجيل الثاني، وفي عام 2006 أصبح الشبكة الاجتماعية الأولى حسب التصويت الذي قامت به مجلة التايمز الأمريكية. حيث حصل هذا الموقع على شعبية كبيرة بين كافة الفئات العمرية، وبالرغم من أنه موقع لا وجود فيه لإعلانات تجارية تحقق أرباح مالية، لكن الشهرة التي اكتسبها الموقع عادت بمكاسب قيمة للأشخاص الذين عملوا على تأسيسه وكذلك على الأشخاص الذين يستخدمونه لنشر فيديوهاتهم، فهو أصبح أكبر المستضيفين لأفلام الفيديو سواء على المستوى الشخصي أو عبر شركات المتخصصة في الإنتاج، وأصبح اسم YouTube اسمًا مألوفًا عند الإشارة إلى أسماء شركات التكنولوجيا البارزة حول العالم. وعبر شبكة الانترنت، إضافة إلى أنه بات جزءًا من حياة ملايين الأشخاص من جميع الأعمار وبمختلف الاهتمامات. ويستخدم الموقع لغات متعددة يصل مجملها حوالي 51 لغة أهمها :اللغة إنجليزية، والروسية ،العربية، الفرنسية، البولونية، الإيطالية، البرتغالية، الإسبانية، الألمانية، الهولندية، الإيطالية ، الصينية، اليابنية ....[3]

إن موقع YouTube يحتوي على قاعدة جماهيرية كبيرة للبالغين والأطفال على حد سواء، والشباب هم بلا شك الفئة الأكثر استخدامًا له، مما يعني وجود الكثير من الأفلام والفيديوهات على الموقـــــع. الأمر الذي يستدعي الانتباه للأطفال لأنه ليس كل ما

---

[1] – أحمد يوسف فرغلي ، دور التقنيات الحديثة في تحول الشباب الجامعي العربي من قراءة الصحافة المطبوعة إلى الإلكترونية ، رسالة ماجستير غير منشورة ، الجامعة الهولندية، ، 2012 ، ص 100

[2] –فيس بوك يحتل الصدارة ، على الموقع التالي : https://alghad.com/

[3] – مروة عصام صلاح، الإعلام الإلكتروني، الأسس وآفاق المستقبل، دار الإعصار العلمي للنشر و التوزيع، الأردن، ط1، 2015، ص.204.

يعرض عبر اليوتوب مناسبا للأطفال، لهذا السبب يقدم الموقع وسائل رقابة يمكن للوالدين استخدامها للتحكم في ما يراه أطفالهم.[1]

يتم مشاهدة ما يعرض على YouTube عن طرق تنزيل تطبيق YouTube، ثم إدخال اسم البحث في مربع البحث المعروض على صفحة YouTube لإيجاد الأفلام أو المقاطع المرغوب مشاهدتها، ثم تشغيل زر المشاهدة. ويمكن أيضًا تصفية نتائج البحث لمقاطع فيديو على YouTube حسب التاريخ أو عدد المشاهدات أو نوع الفيديو للعثور على مقاطع الفيديو المراد مشاهدتها أو مشاركتها مع الأصدقاء على الشبكات الاجتماعية .[2]

ويبلغ عدد مستخدمي يوتيوب حوالي 2.3 مليار مستخدم نشط شهرياً وذلك وفقاً لإحصائيات 2022 ومن المتوقع أن تحقق منصة يوتيوب المزيد من النمو خلال نهاية هذا العام.[3]

3- موقع الإنستغرام: (Instagram)

يُعتبر الإنستغرام شبكة اجتماعية تتيح للأفراد تبادل الصور والفيديوهات القصيرة، وقد ظهر في 10 يونيو 2010 م، على يد مؤسسيه كيفن سيستروم ((Kevin Systrom) ومايك كاريجر Mike Krieger ، خريجا جامعة ستانفورد الأمريكية، وفى البداية كـــــان الإنستغرام لا يعمل إلا على هواتف آيفون فقط، وبدأ 80 شخص باستخدامه، وبعد10 أيام على إطلاقه بلغ عدد مستخدميه 10 آلاف مستخدم، وفى ديسمبر 2010 م، أعلن مؤسس الإنستغرام عن ربطه بالدعم الكامل على شبكة Foursquare ، حيث وصل عدد مستخدميه إلى مليون مستخدم، وكان الهدف من ذلك تمكين المستخدمين من وضع صور ذات جودة عالية ومشاركتها على مختلف شبكات التواصل الاجتماعي الأخرى، وتم إتاحته للمستخدمين من خلال 25 لغة مختلفة حول العالم، وفى عام2011 ، بلغ عدد مستخدمي الإنستغرام مليون وسبعمائة ألف مستخدم يتشاركون أكثر من 300 صورة يومياً، وحصلت

---

[1] – What is YouTube?", edu.gcfglobal.org, Retrieved Retrieved .

[2] –Elise Moreau (10-2-2020), "What Is YouTube? How Do I Use It?" ،www.lifewire.com, Retrieved 19-7-2020. Edited

[3] – عدد مستخدمي يوتوب على الموقع https://abuomar.ae/2022/03/14

الشركة على تمويل قدره 7 مليون دولار أمريكي من مجموعة مستثمرين من ضمنهم جاك دورسى (Jack Dorsey) مؤسس تويتر.[1]

ويصل حوالي 2 مليار مستخدم لتطبيق انستاغرام شهرياً وهذا حسب إحصائيات 2022، والهند تأتي في المرتبة الأولى استخداماً لإنستغرام حيث يوجد بها أكثر مستخدمي Instagram نشاطًا بحوالي 253 مليون مستخدم ، وبعدها تأتي الولايات المتحدة بحوالي 155 مليون مستخدم، و قي الصين لا يزال الموقع محظورًا.[2]

4- تطبيق واتس آب: (What App)

وهو تطبيق للتراسل والمحادثات الفورية متعدد المنصات يستخدم على منصات أجهزة الآيفون والأندرويد والويندوز، ويتيح لمستخدمه التواصل الفوري بالرسائل والصور والفيديوهات والتسجيلات الصوتية، دون حد أقصى، ولكن بشرط الاتصال بشبكة الإنترنت، وهو تطبيق يتم استخدامه بكثافة كبيرة كبديل للهاتف. ولقد تم تأسيس شركة واتس آب في ديسمبر 2009 من قِبل بريان أكتون (Brian Acton) ، وجان كوم (Jan Com) وكلاهما من قدامى المبرمجين فى شركة ياهو Yahoo ، ويوجد مقر الشركة في سانتا كلارا بولاية كاليفورنيا الأمريكية. وتم تصميمه لتبادل الرسائل والدردشة دون مقابل. ويرجع تسميته بهذا الاسم نسبة إلى العبارة الأمريكية الشهيرة Whats Up ومعناها " كيف الحال "، ويعمل البرنامج فقط على الهواتف المحمولة المتصلة بشبكة الإنترنت وقد أصبح شائعًا جدًا وجذب ملايين المستخدمين عبر مختلف بلدان العالم، حتى أنه تفوق على تويتر. ويبلغ عدد الرسائل المتداولة عليه حوالي 18 مليار رسالة يومياً .

5 -تويتر twitter

هي شبكة اجتماعية توفر خدمات تتيح للمستخدمين نشر تحديثات الحالة الخاصة بهم على صفحتهم الأساسية أو عبر ملف تعريف المستخدم، مع الحصول على الإجابات والتحديثات.

---

[1] – Margaret Rouse, "Instagram" ،searchcio.techtarget.com, Retrieved 16-10-2020. Edited.

[2] – عدد مستخدمي الإنستغرام، https://abuomar.ae/2021/03/01

ولدت خدمة تويتر المصغرة في أوائل عام 2006. وتأخذ اسمها من كلمة Twitter ، وتعني تغريدة، والطائر هو رمزها، وهي خدمة صغيرة تسمح بإرسال نصوص قصيرة لا تزيد عن 140 حرفًا لكل رسالة، يمكن لأي شخص لديه حساب تويتر مشاركة هذه التغريدات مع أصدقائه، التي ستظهر على صفحتهم الشخصية أو في حال زيارتهم لصفحة المستخدم الذي أرسل الرسالة.

ويوفر Twitter لمستخدميه الكثير من االخدمات، أهمها السماح للأصدقاء بمعرفة ما يفعلونه طوال الوقت، وهو أيضًا أسرع طريقة لطرح أسئلة على الأصدقاء والحصول على الردود الفورية، وإتاحة إمكانية إرسال أخبار مهمة وسريعة من حولك. كما يوفر خدمة متابعة الأحداث المهمة من جميع أنحاء العالم، ويمكن للمستخدمين متابعة أخبار أصدقاؤهم ومعارفهم ورؤية ما يفعلونه، كما يعرف الموقع على أنه: " خدمة تتيح للأصدقاء وأفراد الأسرة والزملاء التواصل والبقاء على اتصال مع بعضهم البعض "[1].

6- موقع فليكر

يُعد موقع Flicker نموذجًا لأحد أهم استخدامات الصحافة العامة المتخصصة في نشر صور الأحداث المهمة، وقد ساعد موقع فيلكر في مناسبات متعددة في أن يحل محل منافذ الأخبار، على سبيل المثال خلال فترة هجمات مترو أنفاق لندن، وخلال فترات حدوث التسونامي عبر العالم. فهو موقع يتم من خلاله تخزين الصور وتنظيمها ومشاركتها. وهو جمعية عبر الإنترنت تجمع الهواة في التصوير الفوتوغرافي. والموقع ليس فقط موقعًا مشهورًا لمشاركة الصور الشخصية، ولكن يستخدمه المدونون أيضًا لإعادة استعمال ما يوجد عليه من صور. ويشتهر الموقع بابتكاراته المتمثلة في قدرة الزوار على إضافة تعليقاتهم.[2]

---

[1] – فؤاد شعبان وعبيدة صبطي، تاريخ الاتصال وتكنولوجياته، دار الخلدونية للنشر والتوزيع، الجزائر، 2011 ، ص 180

[2] – سلطان مصف مبارك الصاعدي، الشبكات الاجتماعية خطر أم فرصة، المملكة العربية على الموقع: http://www.conference.ncwegypt.

7. موقع الويكي . Wiki

كلمة "ويكي" تعني: بسرعة، ومن الناحية التقنية هو نوع بسيط من قواعد البيانـــات يتم تشغيله على الإنترنت، وقد تم إنشاءه أول مرة من طرف كل من وارد كننغهام وبوليوف سنة 1995 مما أنشأ مجتمعًا مفتوحًا وتعاونيًا حيث يمكن لأي شخص إضافة محتوى و تطويره وتحريره. وقد تم إنشاء العديد من برامج ويكي منذ ذلك الحين، وتعتمد العديد من مواقع الويب عليها للمساعدة في تبسيط وتطوير المحتوى.[1]

8- موقع ماي سبيسMySpace

هي أكبر شبكة اجتماعية للأصدقاء على الإنترنت، وهو موقع يمنحهم زوايا خاصة تمكنهم من خلالها تقديم حياتهم وصورهم وموسيقاهم وأفلامهم ومدوناتهم عبر الصفحة، ولدى MySpace محرك بحث خاص ونظام مراسلة داخلي، ويمكن لجميع الأشخاص عبر مختلف دول العالم التواصل بشكل احترافي، وإنشاء ملفات تعريف إلكترونية عن حياتهم، وكذلك الانضمام إلى مجتمع خاص، وجدولة الاجتماعات، وتعزيز الأعمال التجارية، ومشاركة الاهتمامات، والعثور على الأصدقاء القدامى وزملاء الدراسة، أيضًا يوفر الموقع لمستعمليه مساحة للخصوصية والتكامل الثقافي، ومن خلاله يتفاعل عدد قياسي من الأفراد مع وسائل الإعلام ويعبرون عن أراءهم.[2]

المطلب الثاني : آثار شبكات التواصل الاجتماعي

صنعت وسائل التواصل الاجتماعي ثورة في الاتصال والتواصل حيث تجمع بين العدد الكبير للمستخدمين الذين يشاركون كميات هائلة من البيانات والمعلومات في نفس الوقت، مما يسمح بمشاركة المعلومات والأفكار بطريقة غير مسبوقة، الأمر الذي أدى إلى زيادة أعداد المشتركين فيها بصورة كبيرة جداً خاصة من فئة المراهقين والشباب، وهناك مجموعة من العوامل التي ساعدت على انتشار الشبكات الاجتماعية من أبرزها ظهور العزلة

---

[1] – أماني جمال مجاهد: الشبكات الاجتماعية في خدمات مكتبية متطورة، مجلة مركز دراسات المعلومات، القاهرة، ماي، العدد 08 ، جامعة المنوفية ،2011 ص37

[2] – محمد منصور، تأثير شبكات التواصل الاجتماعي على جمهور المتلقين، رسالة ماجستير، جامعة القاهرة، 2012 ، ص 84.

الاجتماعية في الأوساط الأسرية والاجتماعية بسبب نمط الحياة المعاصرة. وبسبب عدم التواصل في وسط الأسرة نفسها، لأن معظم أفراد الأسرة بعيدون عن المنزل، مما يولد نقصًا في التواصل، الأمر الذي ينتج عنها غياب ونيس في الواقع. ويتم اللجوء لشبكات التواصل الاجتماعي للبحث عنه. فضلا عن شبح البطالة الذي دفع بالكثيرين إلى الإنترنت لتضييع أوقاتهم.

لقد أصبحت مواقع التواصل الاجتماعي مطلبا رئيسيا للعديد من الناس. وبالتالي كان لاستخدامه العديد من الفوائد والايجابيات والعديد من السلبيات. حيث سجلت لهذه الشبكات جملة من الآثار الايجابية والسلبية على المستخدمين نبرزها فيما يلي:

الفرع الأول: إيجابيات شبكات التواصل الاجتماعي

جلبت تقنيات وسائل التواصل الاجتماعي جانبًا إيجابيًا في حياة المجتمع بأسـره، حيث أدخلـت تحـولات مست بجميع المجالات الاجتماعية والاقتصاديـة والسياسية والثقافيـة، ومن أهمها:

أولا: لا نهائية المعلومات

يوفر الإنترنت ثروة من المعلومات حول جميع المجالات مع سهولة الوصل إليها. وفي السنوات الأخيرة أنتج العقل البشري معرفة أكثر مما كان عليه في زمن ماضي، وهذا من خلال ما يتم التعبير عنه يوميًا في مجموعات متنوعة من العلاقات عبر الإنترنت.

ثانيا: وسيلة اتصال عالمية

في الوقت الحالي أصبحت الشبكات الاجتماعية بديلا لوسائل الاتصال الأخرى من هاتف وفاكس وغيرها، واستحدثت أنماط جديدة من التفاعل الاجتماعي والاتصال بالآخرين دون مقابل كبير ودون التقيد بالموقع الجغرافي أو كلفة الانتقال أو قلة الوقت اللازم للمقابلة.[1]

ثالثا: سهولة الاستخدام

تم تصميم شبكات التواصل الاجتماعي لتكون سهلة مع اختلاف أعمـار مستخدميهـا

[1] – ماجد الزبيدي ، الإنترنت والتدريب في علوم المعلومات والمكتبات : رسالة مكتبية ، المجلد 3 ، العدد الأول والثاني ،2004، ص 6

ومستوياتهم الاجتماعية والاقتصادية، حيث استخدامه يتطلب جزءا من المهارة والمعرفة في أسس الكمبيوتر، كما أنها تمتاز ببساطتها في التصميم وسهولة الدردشة الصوتية والنصية والمرئية،[1] مما يجعلها أحسن وسيلة للتواصل بين الأشخاص خاصة الذين تفرقهم مسافات طويلة.

لقد أصبحت شبكات التواصل الاجتماعي بديلاً لوسائل الاتصال التقليدية، حيث ازداد الاعتماد عليها مؤخرا كوسيلة اتصال وتواصل عبر مختلف أنحاء العالم وذلك لانخفاض تكلفتها مقارنة بوسائل الاتصال التقليدية ، إضافة إلى سهول استخدامها، الأمر دفع بملايين الشباب حول العالم إلى الاعتماد عليها في الحصول على المعلومات والتواصل ومشاركة الآراء مع الآخرين.

رابعا : الاعتماد على شبكات التواصل الاجتماعي كوسيلة إعلام

لقد وفرت الشبكات الاجتماعية لمستخدميها متابعة محطات الراديو ومشاهدة جميع القنوات التلفزيونية واستقبال الأحداث العالمية الحية، ومتابعة كل ما له علاقة بالسياسة والثقافة والعلوم والرياضة. ويمكن استخدامها لإنشاء صفحات خاصة لنشر ومشاركة الأحداث مع مستخدمين آخرين.[2]

خامسا: تخطي كافة الحدود

تغلبت الشبكات الاجتماعية على جميع الحواجز الجغرافية التي وقفت عائقا أمام انتشار الأفكار واختلاط الناس ومشاركة الخبرة والمعلومات.

سادسا: تخطي الزمان

يتم نقل المعلومات عبر شبكات التواصل الاجتماعي بسرعة كبيرة جدا تجعل من حق كل مستخدم الحصول على المعلومة في نفس الوقت وفي أي مكان في العالم بدون وجود فارق زمني كبير بين انتقال المعلومة من المُرسل إلى المُستقبل .

---

[1] – فتحي شمس الدين، شبكات التواصل الاجتماعي والتحول الديمقراطي في مصر ، القاهرة ، دار النهضة العربية ،2013، ص 64

[2]– ماجد الزبيدي ، المرجع السابق، ص 7

وفي عصر الإنترنت بإمكان المستخدم من خلال شبكــات التواصل الاجتماعي التغيير من دور المتلقي إلى دور الناشر أو المرسل.

سابعا: تنوع وتوفر التطبيقات

التطبيقات والخدمات التي تقدمها شبكات التواصل الاجتماعي متنوعة وفى شتى المجالات وتغطي كل اهتمامات المستخدمين لها.

ثامنا : المجانية

كثير من العلامات التجارية التي تعمل في مجال تقديم خدمات الإنترنت بدأت في تخفيض تكلفتها حتى تمكن الجميع من خدمة الإنترنت. أي أن كل فرد غني كان أو فقير بمقدوره أن يستخدم الشبكات الاجتماعية المتوفرة على الإنترنت.[1]

تاسعا: إمكانية إظهار المشاعر الإنسانية

كان من أهم سلبيات الإنترنت أنه لا يوجد فرصة كبيرة لإظهار المشاعر الإنسانية من خلال المحادثات التقليدية التي كانت تتم من خلالها، لأن الإيماءات والإشارات البشرية كان من الصعب أن تتضمن في تلك المحادثات، وأتاح ظهور شبكات التواصل الاجتماعي المشاركة العاطفية، وتقدم بعض شبكات التواصل الاجتماعي الأشكال التي تعبر عن الحالة المزاجية التي يعيشها المستخدم، بأن يضع تعبير على شكل كرتوني "إموج" بأنه سعيد أو حزين أو متعب أو مسافر أو يأكل، والأشخاص بشكل عام تتاح لهم إمكانية مشاركة العواطف من خلال التعبير عن الحالات الانفعالية والمزاجية التي يمرون بها، وهو الأمر الذي وفرته شبكات التواصل الاجتماعي وسهلته لمستخدميها.[2]

وبالرغم من إيجابية هذا التطبيق إلا أن الاعتماد عليه بشكل كلي قد يشكل خطرا في المستقبل على اللغة المنطوقة والمكتوبة، ويُضعف استخدام الأشخاص لها في محادثاتهم عبر شبكات التواصل الاجتماعي لأنهم وجدوا البديل الأسهل للتعبير عن مشاعرهم وأفكارهم، مما يهدد السلامة اللغوية للأفراد.

---

[1] – محمد السيد حلاوة ، رجاء على عبد العاطي ،العلاقات الاجتماعية للشباب بين دردشة الإنترنت والفيس بوك ، دار المعرفة الجامعية، الإسكندرية 2011، ص 59

[2]– فتحي شمس الدين ، شبكات التواصل الاجتماعي والتحول الديمقراطي في مصر ،المرجع السابق، ص 66

إضافة لأهم المزايا التي ذكرناها يمكننا ذكر إيجابيات أخرى لشبكات التواصل الاجتماعي:

– نشر التعليم وجمع المعلومات: يتبادل من خلالها الطلاب والباحثون الخبرات والمهارات ويناقشون القضايا الاجتماعية. فهي وسيلة لاكتساب الخبرة والقدرة والكفاءة.

– علاقة المواطن بالحكومة: تتواصل العديد من الدوائر والهيئات والمؤسسات الحكومية مع الجمهور " على كافة المستويات من خلال الإعلام الذي يعتبر أسهل وسيلة للتواصل بين الهيئات الحكومية والجمهور.

– فرصة لتعزيز الذاتي : أي شخص ليس لديه القدرة على إنشاء شخصية مستقلة وكيان فريد خاص به في المجتمع، يمكنه ذلك من خلال استخدام مواقع التواصل الاجتماعي وملء البيانات الشخصية وإنشاء موقع خاص به.

– الانفتاح على الآخرين وبناء العلاقات الاجتماعية: التواصل مع الآخرين هو سمة فردية بغض النظر عن لون البشرة والمظهر. فمواقع التواصل الاجتماعي تمكن مستخدميها من التواصل مع الآخرين وإنشاء صداقات ومشاركتهم بالأفكار والتواصل في الشؤون العامة.

– التغلب على الشعور بالوحدة: من السمات الرئيسية لمواقع التواصل الاجتماعي أنها ببساطة تتمتع بحرية توسيع صفحاتها وإضافة محتوى يعبر عن آرائك وميولاتك التي قد تتعارض مع الآخرين، وهي فضاء مفتوح يسهل حرية التعبير، مما يجعل الشبكات الاجتماعية وسيلة مهمة للتعبير عن المواقف والآراء الفردية حول القضايا ذات الأهمية الكبيرة.

– وسيلة للدعاية والإعلان: وهي وسيلة تسمح بالإعلان المجاني المسموح به وهي وسيلة يستغلها كل من يشتغلون في الدعاية التجارية بغاية التوسع والانتشار السريع.

– تعزيز الحوار بين الحضارات: إذ تعمل على ربط الثقافات والحضارات المختلفة فيما بينها.

– وسيلة للشراء واقتناء الحاجيات عن طريق التجارة عبر الإنترنت.

– وسيلة للعمل في البيت دون الحاجة للتنقل لمكان العمل خاصة للأشخاص الذين يعتمدون في عملهم على الإنترنت.

الفرع الثاني: سلبيات شبكات التواصل الاجتماعي

تعددت مزايا شبكات التواصل الاجتماعي وما تتمتع به من إمكانات ومردودات توفرها للمستخدم، وباعتبار شبكات الاجتماعية فهي سلاح ذو حدين حيث نجد العديد من العيوب والآثار السلبية الناتجة عن استعمالها والتي مست كافة المستويات الاجتماعية والثقافية والسياسية والاقتصادية.

أولا: الفساد الأسري والتفكك الأسري

وقد خصصت العديد من الدراسات المختلفة لتحليل ظاهرة الفساد الأسري وأسبابه. وقد أشارت هذه الدراسات إلى العديد من التسهيلات التي تقدمها تقنيات وسائل التواصل الاجتماعي والتي ساعدت على انتشار الفساد من خلال:

- اختلاط القيم الأخلاقية.
- تفشي المحتويات المتدنية عير الإنترنت ذات التأثير على الأخلاقيات.
- عدم الرقابة على استخدام أجهزة تكنولوجيا المعلومات.

إن ما وفرته مواقع التواصل الاجتماعي أدى إلى تغييرات جذرية في العلاقات داخل الأسرة الواحدة إذ أصبح الأفراد يعيشون بمعزل داخل أسرهم ويقضون وقتا كبيرا أمام المواقع الاجتماعية، الأمـــر الذي خلق لديهم عدم الرغبة في الحديث والحوار مع أفراد أسرتهم، وأصبحت جل اهتماماتهم بالعالم الافتراضي، وتحويل علاقاتهم الافتراضية إلى علاقات حقيقية.

ثانيا: نشر الأفكار والمعتقدات المتطرفة والهدامة

تُستخدم شبكات التواصل الاجتماعي لنشر المعتقدات والأفكار المتطرفة سواء الدينية أو السياسية أو العنصرية مما يجعل الكثير من الأشخاص خاصة فئة الشباب فريسة سهلة لكل تلك الأفكار المنافية للدين والأخلاق والعادات والتقاليد المجتمعية الأصيلة والقيم الوطنية والانتماء إلى المجتمع، مما ينعكس على المجتمع بالسلب بانتشار التعصب والتطرف والانهيار الأخلاقي والديني.

ولقد قامت بعض التنظيمات الإرهابية المتطرفة من إنشاء صفحات متعددة على شبكات التواصل الاجتماعي مثل الفيس بوك لاستقطاب الشباب للانضمام إلى التنظيم وتجنيدهم

للقيام بعمليات انتحارية وإرهابية، وقد نجح بالفعل في تجنيد العديد من الشباب بما فيهم الجزائريون، ولم تستطع أي من الحكومات العربية أو الغربية من وضع أي قيود رقابية على استخدام الشباب لشبكات التواصل الاجتماعي لحمايتهم من مخاطر السقوط في أفخاخ الجماعات الإرهابية.

ثالثا: التشويه بالدين الإسلامي

تستخدم بعض المنظمات المشبوهة شبكة الإنترنت لإنشاء صفحات على شبكات التواصل الاجتماعي تهاجم الدين الإسلامي وتشوه القران الكريم وتؤلف سور قرآنية لزعزعة العقيدة لدى المسلمين، ورغم ما تثيره هذه المحاولات من غضب واستياء في نفوس المسلمين، إلا أنها تمثل إنذار ينبهنا إلى ضرورة إعداد الداعية الإسلامي المناسب القادر على التعامل مع تقنيات القرن الجديد، والذي يتمتع بفهم جيد للإسلام، ويتحدث لغة أجنبية بطلاقة، ويستخدم تكنولوجيا الحاسبات الرقمية للدخول على هذه المواقع والرد المناسب على ما تبثه من أكاذيب ودعاوى مضللة.[1]

رابعا: إنتشار الإباحية الإلكترونية والفساد الأخلاقي

تعتبر شبكات التواصل الاجتماعي من أبرز الوسائل في فعاليتها وجاذبيتها لنشر الإباحية بكل وسائل عرضها من صور وفيديوهات على مرأى الجميع، ويكمن خطرها في إمكانية حصول الأطفال والمراهقين على هذه المواد، وتعرضهم لها رغم وجود الكثير من المحاولات من الآباء لمنع وصولهم لهذه المواقع التي قد تبث الصور الإباحية في صورة رسائل بريدية عشوائية تقتحم على المستخدم خصوصيته، ولا تعترف بأي حدود جغرافية أو دولية وعلى الرغم من أن الغربيين يغضون الطرف أحيانًا عن المواد الإباحية للبالغين بدعوى الحرية فذلك لا ينطبق على الأطفال، خاصة مع انتشار" دعارة الأطفال " عبر شبكات التواصل الاجتماعي، ونشر صور إباحية لأطفال صغار، فهي مواقـــــــع لا يوجد

[1] – شريف درويش اللبان ، تكنولوجيا الاتصال : المخاطر والتحديات والتأثيرات الاجتماعية ، الدار المصرية اللبنانية ، القاهرة ،2000 ، ص 126

عليها أي رقابة قانونية تستطيع أن تمنع نشر هذه الصور.[1]

خامسا: خلق الشعور بالعزلة والتوحد.

أثبت عدد كبير من الباحثين أن كثرة استخدام الإنترنت يؤدي إلى عزلة الأفراد عن بعضهم البعض وهو ما يمكن أن يؤثر سلباً على علاقة الأفراد فيما بينهم، إضافة إلى خلقه شعوراً بالوحدة والعزلة والغربة، حيث أن تواصل الأشخاص إفتراضيا باستخدام شبكات التواصل يقضي على الوقت الحقيقي الذي يقضونه سويا وهذا ما يشهده الواقع المعاش، إلى جانب تعطيل الحياة الاجتماعية نتيجة استبدال الوقت الاجتماعي الذي كان يُقضى مع الأسرة والأصدقاء بالوقت الذي يُقضى على الشبكات الاجتماعية، فقد أصبحنا نضحك أمام شاشات الموبايل أكثر بكثير مما نضحكه في وجوه بعضنا البعض.

سادسا: انتشار إدمان الإنترنت

لقد بينت الدراسة التي قامت بها يونج Young أن الإفراط في استخدام الإنترنت وشبكات التواصل الاجتماعي يؤدى إلى الإدمان الإلكتروني الذي يتورط فيه الأطفال والمراهقون والشباب أكثر من غيرهم، وذلك لتعويض نواحي القصور والإحباطات في حياتهم مثل التعثر الدراسي والتفكك الأسري وعدم الرعاية الوالدية أو افتقار القدرة على تكوين صداقات أو الخروج من علاقات عاطفية فاشلة، مما يؤدى إلى طول المدة التي يقضونها على الشبكات الاجتماعية والتي قد تصل إلى أكثر من40 ساعة أسبوعيا، ويكون لها تأثير سلبي على الأفراد حيث تؤدي إلى فقدان القدرة في السيطرة على الرغبة في استخدام تلك الشبكات، والشعور بالغضب عند محاولة الوالدين قطع الخط، إلى جانب العودة لاستخدامه ثانية رغم ضياع أوقات ثمينة، وتصف يونج (Young) الإدمان الإلكتروني بأنه استخدام شبكات التواصل الاجتماعي والإنترنت لأكثر من 38 ساعة أسبوعيا أي بواقع 7 ساعات يومياً.[2]

---

[1] – محمد السيد حلاوة ، رجاء على عبد العاطي ،العلاقات الاجتماعية للشباب بين دردشة الإنترنت والفيس بوك، المرجع السابق ، ص 65

[2] - محمد السيد حلاوة ، رجاء على عبد العاطي ،العلاقات الاجتماعية للشباب بين دردشة الإنترنت والفيس بوك، المرجع السابق، ص 64،65

وقد أكدت بعض الدراسات والبحوث التي أجريت حديثا على أن الإدمان على الانترنت أصبح واقعاً ومرض خطير يعاني منه الكثير من الأشخاص عبر العالم، حيث عمل الأطباء النفسيون على البحث في هذا المرض وفي كل ما يتعلق بالمخاوف المتعلقة بالاستخدام المكثف والمفرط للإنترنت، وتم التأكيد على أنه شكل من أشكال الإدمان الحقيقي تتشابه خصائصه وأعراضه السريرية وآثاره الجسدية والنفسية مع حالات إدمان المخدرات والكحول.

سابعا: انتشار الجرائم عبر الإنترنت

لقد ترتب على الاستخدام المتزايد لمواقع التواصل الاجتماعي نشوء عدة مخاطر، أهمها مخاطر الاحتيال أو سرقة الهوية. إضافة إلى ذلك مساهمتها في ترويج المخدرات، ونشر الرذيلة عن طريق المواقع الإباحية، واعتبارها فضاء يتم من خلاله ممارسة جريمة التهديد والابتزاز، والسب والقذف والتشهير، والاحتيال، والاعتداء على الخصوصية إلى غير ذلك من الجرائم .

ثامنا: انعدام السرية والثقة

عدم كفاية توفير أمن المعلومات المنتشرة على الإنترنت، مع إمكانية اختراقها من طرف مجرمي الإنترنت، فضلا عن إمكانية اختراق الحكومات لخصوصية الأفراد وتصفح منشوراتهم ومراقبتها.

تاسعا: التزوير الإلكتروني

نتيجة للتقدم التكنولوجي الهائل في أجهزة الكمبيوتر والطابعات الملونة وبرامج مسح الصور ومعالجتها، اتسع مجال التزوير والتلاعب بصور الأشخاص والقيام بتزييفها بأوضاع مخلة بالآداب بحيث تكاد الصور المزيفة أن تتطابق مع الأصلية، ثم ابتزاز أصحابها وطلب الأموال منهم، كما يتم تزييف توقيعات الأفراد على الشيكات والمستندات والعقود والاستيلاء على أموالهم و ممتلكاتهم .

عاشرا: المخاطر الصحية والنفسية

لقد أثبتت الدراسة العلمية التي قام بها الطبيب البريطاني تشارلز وايت Charles Whiteعام 2014 م، أن طول الفترة التي يمضيها الفرد في استخدام الكمبيوتر للعمل

باستخدام شبكة الإنترنت وشبكات التواصل الاجتماعي تتسبب في ظهور أعراض الصداع وضعف الإبصار والآلام في العنق والكتفين والظهر واليدين والرسغين، خاصة لدى الأطفال الذين لا تزال هياكلهم العظمية في مرحلة التكوين.

بالإضافة إلى ذلك يمكن لمستخدم الشبكة الاجتماعية إخفاء اسمه وعمره وصورته وسلوكه عند استخدام الخدمة عبر الإنترنت. لذلك فإن بعض الأشخاص الذين يشعرون بالوحدة وعدم الأمان في حياتهم الحقيقية يستغلون المواقع لمشاركة أسرارهم ورغباتهم الخفية ومشاعرهم المكبوتة مع الأخرين، ولكن حين يصطدمون بحقيقة أن المجتمع الافتراضي على الإنترنت لا يستطيع تحقيق الحب والاهتمام اللذان يحققهما المجتمع الحقيقي، يتعرض هؤلاء لخيبة أمل وشعور بالألم ويصابون بأمراض نفسية قد تؤدى بهم إلى إنهاء حياتهم[1] .

إحدى عشرة: مخاطر مواقع التواصل الاجتماعي على الأطفال

تمثل مواقع التواصل الاجتماعي أكبر المخاطر على الأفراد، وتتضاعف هذه الخطورة في حال ما تعلقت بالأطفال بسبب ضعفهم وقلة خبراتهم وتمييزهم لصح والخطأ، ومن مخاطر شبكات التواصل الاجتماعي على الأطفال نذكر ما يلي:

– تعرضهم للإساءة والمضايقات والتنمّر، هذا الأخير الذي يتسبب في انتحار العشرات من المراهقين سنويا خاصة في الدول الغربية التي تعلن عن هذه الحالات.

– الدخول إلى مواقع غير لائقة وغير أخلاقية ومواد إباحية، عن قصد أو عن غير قصد.

– نشر مقاطع فيديو وتسجيلات غير لائقة من قبل صغار السن لجهلهم بما قد يضر بهم.

– تسبب وسائل التواصل الاجتماعية بمشاكل مختلفة للأطفال المستخدمين لها ومن أهم هذه المشاكل التوحد والعصبية .

– ومن أهم المخاطر التي لحقت بالأطفال بواسطة الإنترنت إنتشار بعض الألعاب الإلكترونية في السنوات الأخيرة تروج للتعذيب والتشويه الجسدي، فهي ألعاب تلحق بمن يمارسها وفي مقدمتهم الأطفال أضرارا جسيمة تصل بهم لحد إنهاء حياتهم من خلال

[1] – محمد السيد حلاوة ، رجاء على عبد العاطي ،العلاقات الاجتماعية للشباب بين دردشة الإنترنت والفيس بوك، المرجع السابق ص 67 .

تعليمات افتراضية تؤثر بهم. وقد أودت بحياة كثير من الشباب والمراهقين عبر العالم ولقد أطلق عليها اسم ألعاب الموت ، ومن المثير للاهتمام أن إحدى قواعد هذه الألعاب هي أنها من طرف شخص بمفرده، كما لو كان مجبرًا على الموت دون أن ينقذه أحد. وعلى رأس القائمة لعبة الحوت الأزرق التي ظهرت عام 2015، والتي تسبّبت في العديد من حالات الانتحار تفوق 137 شخص عبر العالم من بينهم عدة حالات في الجزائر. حيث تجبر لاعبيها على المشاهدة المستمرة لأفلام الرعب مدة 24 ساعة، ثم مطالبتهم بتقطيع أجسادهم بأدوات حادة، والطلب منهم الاستفاقة من النوم على فترات عشوائية أثناء الليل والتقاط صور لأنفسهم، أيضًا حثهم على إزالة أجزاء صغيرة من جسمهم وفي كل مرة يأخذ الطفل جزءًا صغيرًا ويلتقط صورة. وتبدأ مرحلة جديدة يحظى فيها بالإعجاب ويعتبرون أنفسهم أبطالًا ويقتل اللاعب نفسه على الفور عندما تصل اللعبة إلى اليوم الخمسين. فلعبة الحوت الأزرق تقوم بغسل دماغ الأفراد المعرضين للخطر لمدة 50 يومًا وبالقيام بأشياء مرعبة، وفي النهاية يتم أمرهم بإنهاء حياتهم. ولقد استمرت مخاطر اللعبة لغاية القبض على مخترعها الروسي فيليب بوديكين 21 عام.[1]

وهناك أيضًا لعبة "بوكيمون" التي تتسبب في جنون وهوس الضحية الذي ينتهي بها المطاف إلى الإنتحار. أما بالنسبة للعبة الجنية النارية فيتم من خلالها خداع الأطفال بتحويلهم إلى مخلوقات نارية وخارقة، وحثهم إلى البقاء بمفردهم في غرفهم والقيام بحرق أنفسهم لتحويلهم إلى "Fire Fairies". وكانت الجنية من أكثر الألعاب المغرية للأطفال. أما لعبة "مريم" المخيفة، والتي تعتمد على بنت اسمها "مريم" فقدت أهلها ومنزلها، وتقدم لها يد المساعد للعودة إليه وتقوم الضحية بالقيام بما يطلب منها لمساعدتها[2].

اثنا عشرة: شبكات التواصل الاجتماعي والإرهاب

حرص الإرهاب المعاصر في ظل ثورة المعلومات، أن تُذاع أعماله الإرهابية على شاشات التليفزيون والإنترنت وأن تملأ مواقع التواصل الاجتماعي، وهذا بهدف تصعيد

---

[1] -– ألعاب الموت: كيف تحمي طفلك منها ، مقال منشور على الرابط التالي:
https://www.alaraby.co.uk تم الإطلاع عليه في 20 نوفمبر 2018 على الساعة 22:34

[2] – ألعاب الموت: الموقع نفسه

الرعب لدى الأفراد، وتضخيم الأحداث لزيادة معدلات المشاهدة، حيث أن الإرهاب إذا لم يحظى بتغطية إعلامية تأثيره يقل في المجتمع. إضافة إلى أن استخدام شبكات التواصل الاجتماعي هدفه منها التواصل وتمرير خطابات التجنيد وطلب التمويل.

ثلاثة عشرة: الغزو الثقافي للدول

تركز الدول القوية على نشر ثقافتها داخل الدول الأخرى مما أدى إلى ضعف الثقافة المحلية والقيم الأصيلة لكثير من دول العالم، من خلال فرض ثقافات حديثة على حساب تدمير ثقافات أصلية لشعوب محددة من خلال استغلال شبكة الإنترنت ودعوة الصفوة من مثقفي الدول الضعيفة لزيارة الدولة الأقوى لاستقطابهم إليها، ويعتقد البعض أن ظاهرة المعرفة والثقافة العابرة للحدود هي ظاهرة أمريكية، لأن الولايات المتحدة تتفوق في هذا المجال بشكل واضح. فشبكات التواصل الاجتماعي تعد أحد وسائل نشر ثقافات الدول الغربية خاصة لدى فئة الشباب المنبهرين بالتقدم الغربي.

أربعة عشرة: نشر الأخبار الكاذبة والشائعات[1]

أصبحت مواقع التواصل الاجتماعي فضاء يستغله المجرمين لنشر الأخبار الكاذبة ونشر الشائعات، وإنتشار ظاهرة الشائعات الإلكترونية لم تعد مجرد أخبار كاذبة أو معلومات خاطئة يلقيها شخص معين بل أصبحت جريمة يقف خلفها مؤسسات متخصصة احترفت نشر المعلومات الزائفة بهدف زعزعة أمن واستقرار الدول.

المبحث الثاني

آثار العدوان الإجرامي عبر الإنترنت

تشكل ظاهرة العدوان الإجرامي عبر الإنترنت أحد أكبر التحديات في عالم اليوم. وقد أصبحت ظاهرة عالمية تشير إلي الخلل القائم في الأنظمة التربوية والاجتماعية والاقتصادية في أغلب المجتمعات. ومن المثير للقلق أن الإحصاءات الرسمية تشير إلى ارتفاع معدلات الجريمة وضحاياها، خاصة بين الشباب الذين هم مستقبل أي بلد وأساس التنمية والأمن الوطني.

[1] _ فتحي شمس الدين ، المرجع السابق ، ص 7

لقد أصبحت الجريمة عبر الإنترنت مشكلة عالمية، وتعدت آثارها السلبية على الجانب الاجتماعي والاقتصادي لتمس بالجانب الأخلاقي والسياسي الذي يهدد أمن الدول ومستقبل البشرية.

المطلب الأول :آثار جرائم الإنترنت من الناحية الاجتماعية

أهم التأثيرات السلبية التي تترتب على ارتكاب الجرائم عبر الإنترنت من الناحية الاجتماعية، تلك التي تمس بالشخص وعرضه وتأتي في مقدمتها جرائم التهديد والابتزاز والجرائم الجنسية وجرائم ترويج المخدرات وجريمة غسيل الأموال وظاهرة الإرهاب الإلكتروني.

الفرع الأول : تأثير جرائم التهديد والابتزاز والجرائم الجنسية على المجتمع

تزايدت الجرائم عبر الإنترنت خاصة جرائم التهديد والابتزاز والجرائم الجنسية وتزايدها المستمر أصبح يشكل خطرا كبيرا على كافة المجتمعات لما تخلفه هذه الجرائم من سلبيات.

الفقرة الأولى : تأثير جرائم التهديد والابتزاز: من أخطر الجرائم المرتكبة عبر الإنترنت جرائم التهديد والابتزاز خاصة التي تقع على الإناث من خلال الإنترنت، ذلك أن إحصائيات الحالات الاجتماعية للمجني عليهن في جرائم الابتزاز والتهديد المعلوماتي تصل إلى أرقام مخيفة، وتتصدرها الفتيات العازبات من ثم تأتي النساء المتزوجات ثم المطلقات ثم الأرامل، وغالبا ما يكون نهاية هذه الجرائم مأساويا خاصة في الدول العربية وذلك بانتحار المجني عليها وفي بعض الأحيان قتل الضحية من قبل ذويها للخلاص من العار نتيجة لمقاطع فيديو أو صور تعود للمجني عليها استطاع الجاني الحصول عليها عبر وسائل مختلفة مستغلا سذاجة المجني عليها أحيانا، أو مستعملا لوسائل القرصنة على الإنترنت عبر سحب ملفات شخصية وبثها عبر مواقع التواصل الاجتماعي المختلفة.

إن الابتزاز الالكتروني له تأثير كبير وواسع على شتى جوانب الحياة مادياً واجتماعياً ونفسياً، وسنلخص أهم هذه الأضرار التي قد يتسبب بها كالآتي:

–الابتزاز غالبا ما يؤدي للسرقة التي قد تؤدي بدورها إلى القتل وارتكاب جرائم أخرى في بعض الأحيان.

– ارتفاع نسب الانتحار، وترجع معدلات الانتحار المرتفعة إلى الخوف من العواقب الوخيمة التي قد تتعرض لها الضحية إذا لم تمتثل للطلبات المبتز بسبب ما يملكه هذا الأخير من محتوي إبتزازي. وهذا ما حدث في مصر مطلع عام 2022 ، حيث انتحرت فتاة مصرية اسمها بسنت بعد أن قام شاب بتثبيت صور لها وقام بتعديلها ثم نشرها على مواقع التواصل الاجتماعي لابتزازها، حيث لم تتحمل الفتاة انتشار تلك الصور بين سكان قريتها.[1] ولقد تكررت مثل هذه الحادثة عدة مرات وعبر مختلف الدول العربية بما فيها الجزائر.

– التفكك الأسري: هناك الكثير من جرائم الابتزاز التي أضرت بالعلاقات الاجتماعية وأثرت بشكل خطير على الأسر. ففي كثير من الأحيان بسبب الفضائح ، يطلق الأزواج زوجاتهم، سواء أكانوا مذنبين أم لا، نتيجة سوء التواصل الذي يؤدي إلى عملية الابتزاز الإلكتروني.

– يمكن إنشاء المحتوى الفاضح من خلال البرامج الإلكترونية المتقدمة، مما يتسبب في اضطراب العلاقات الاجتماعية وتشويه السمعة، وكثير من الناس لا يدركون مفهوم هذه التقنيات، وعندما يرون محتوى الابتزاز الخاص بأحد أقربائهم، فإنهم يسارعون إلى الاعتقاد بأنه حقيقي، الأمر الذي ينتج عنه عواقب اجتماعية سلبية خطيرة للغاية ، أهمها الإحساس بعدم الأمن .

–الوقوع في الخيانة بجميع أشكالها، الخيانة الزوجية، خيانة الأمانة ...إلخ.

الفقرة الثانية: تأثير الجرائم الجنسية

من أكثر الآثار السلبية المدمرة للمجتمع تسببت فيه الجرائم الجنسية والإباحية عبر الإنترنت، ولقد أشارت إحصائيات قامت بها شركات التكنولوجيا العالمية، أنه توجد 45

[1] – انتحار فتاة مصرية" ابتزاز وصور مفبركة" مقال منشور على الموقع التالي: https//www.bbc.com تم الإطلاع عليه 2022/07/09

مليون صورة ومقطع فيديو في شبكة الإنترنت متعلق باستغلال الأطفال جنسيا، خلال العام 2018.

ونشرت صحيفة "نيويورك تايمز" الأمريكية، بحثا يُظهر أن مشاهد استغلال الأطفال جنسيا، ارتفعت ضعفين في الإنترنت، مقارنة بالأعوام السابقة. وأن المشاهد وجد بها صور لأطفال في سن الثالثة والرابعة تم استغلالهم جنسيا، وآخرون تعرضوا للتعذيب.[1]

وتشير إحصائيات حديثة في هذا المجال أيضا إلى أن 100 ألف موقع إباحي ينشر صور وفيديوهات لأطفال يتم استغلالهم جنسيا بكل الطرق المشينة. وفي كل أسبوع يتم نشر 20 ألف صورة جديدة لإساءة معاملة الأطفال جنسيا على الإنترنت، وأحيانًا لا يتجاوز عمرهم عامين. وتشير نفس الإحصائيات إلى أن تسعة من كل عشرة أطفال تتراوح أعمارهم بين 8 و16 عامًا شاهدو صورًا إباحية أثناء تصفح الإنترنت، وعدد كبير من الأهل يجهلون مشاهدة أطفالهم لمواقع جنسية. ونظراً لارتفاع معدلات الأمية المعلوماتية بين البالغين، وخاصة في الدول العربية، فإن نسبة هؤلاء الآباء تزداد كثيرا.[2]

وفي ظل تطور تقنيات الإنترنت الرهيب والمتزايد، وازدياد عدد الأجهزة المتصلة عبر إنترنت ابتداء من أجهزة الهاتف الذكية إلى أجهزة المطبخ الذكية والمساعدات المنزلية الافتراضية إلى أجهزة الأمن المنزلية باستعمال كاميرا للمراقبة، إلى أجهزة التليفزيون الذكية المزودين بكاميرا، وحتى الأجهزة القابلة للارتداء Devices Wearable كساعة اليد الذكية وغيرها التي تم انتشارها في جميع نواحي الحياة، أصبح الشخص المستخدم لكل هذه الأجهزة مهددا في حريته أو حياته أو ماله بصفة مستمرة. وفي هذا الشأن تم في الولايات المتحدة الأمريكية اتصال بعض الهاكرز بأطفال عن طريق كاميرات المراقبة الموضوعة في غرف نومهم والمتصلة عبر شبكة الانترنت بهواتف آباءهم لمراقبة أبناءهم، حيث قام هؤلاء بالاتصال بهم والحديث معهم وتحريضهم على فعل أشياء مخلة بالحياء، وهذا على أساس أنهم (**الأب نوال**) وإذا لم يتبعوا ما يقولون يحرمون من هدايا عيد الميلاد، وتم ذلك

[1] – الاستغلال الجنسي للأطفال ، إحصائيات منشورة على الرابط التالي: https://www.aa.com.tr/ar
اطلع عليه في 2020/07/10

[2] – استغلال الأطفال عبر الانترنت ، بحث منشور على الرابط :https://forums.graaam.com/524784.html

عن طريق كاميرات من نوع CAMERA RING AMAZON التي تم التشكيك في نوعيتها، ولكن المشكل لا يكمن في مدى صلاحية أو حداثة أو نوعية الجهاز، ولكن المشكل يكمن في إمكانية اختراق كافة الأجهزة الالكترونية المتصلة بشبكة الانترنت من طرف الهاكرز إذا أرادوا ذلك مهما كانت نوعية الجهاز [1].

إضافة إلي هذا فإن الجرائم الجنسية عبر الانترنت التي تطال الأطفال يمكن أن تشوه الرغبة الجنسية الفطرية والطبيعية لدى الطفل، ويقوده إلى أعماق الانحراف والشذوذ الذي انتشر بطريقة مروعة في وقتنا الحالي ونتيجة له انتشار التحول الجنسي "المتحولين الجنسيين" وكذلك انتشار الزواج المثلي، زيادة على هذا قد يصبح الضحية لهذا النوع من الجرائم عاجزا عن الزواج وعن ممارسة الجنس الطبيعي مستقبلا، بالإضافة إلى وصمة العار التي سترافقه بقية حياته.

فالانتشار الكبير للمواقع الإباحية تعد سببـا من أسباب الفسـاد الأسري، وفساد الأخلاق والانحطاط الثقافي وتراجع القيم الأخلاقية التي تحث على الرذيلة والانحلال الخلقي والتي تجد طرق الوصول إليها أمر غاية في السهولة وتتسبب في تدمير عقول الشباب والمراهقيـن، [2]وأصبح الإدمان عليها ظاهرة متفشية في العالم بأسره بما في ذلك الجزائر. والإدمان على المواقع الإباحية قد يتسبب في الكثير من المخاطر الماسة بالفرد والمجتمع.

– **المخاطر المُترتبة على الأطفال:** من الخطورة الكبيرة بالنسبة للأطفال دون سن 14 عامًا مشاهدة المواد الإباحية، وقد ثبت من خلال بعض الدراسات الخاصة بالأطفال تأثر هؤلاء بشكل كبير بمشاهدة هذه المواد خاصة في هذا العمر، وقد لوحظ أن هناك تغيرات كبيرة ودائمة في نشاط وسلوك أجزاء من دماغ الأطفال الذين يشاهدون المواد الإباحية. ويزيد خطر هذه الأفلام عند إحداثها لتحولات لا نهاية لها في دماغ الطفل الذي يشاهدها، مما يؤدي إلى تغيير في سلوكه وأفكاره وآرائه عندما يعتاد على فكرة أن الجنس شيء طبيعي وضروري في المستقبل وأنه أمر لا تحكمه أي قيود. ومن خلال ما نشره الدكتور فيكتور

[1] –حادثة تم بثها في اخبار 7.45 لقناة M6 الفرنسية ، تم البث يوم 2019 /12/13

[2] – الآثار السلبية لشبكة الإنترنت https://www.annajah.net article–23110 ، تم الاطلاع عليه في 05 فيفري 2020، على الساعة 16:12.

كلاين فإن التعود على مشاهدة الأفلام الجنسية تشجع على السلوك والأفعال الشاذة لدى مشاهديها، لأنها تزيد من احتمالية ارتكاب جريمة أخلاقية، مثل الاغتصاب والتحرش والاعتداء الجنسي وإساءة معاملة الأطفال.[1]

وقد أظهرت بعض الدراسات أنه ومع تقدم العمر وتكرار الاستخدام تدريجيا تبدأ ظاهرة التعود، مما يؤدي إلى استكشاف موضوعات جنسية أخرى، حتى تلك ذات الطبيعة العنيفة. والتي يتم فيها الإكراه وسوء المعاملة، إذ نجد أكثر من 5/4 من محتويات المواد الإباحية علاقات جنسية قسرية وعنيفة لفظيًا وجسديًا. وتحتوي معظم المواقع أيضًا على محتوى غير قانوني (اغتصاب، مواد إباحية للأطفال، إلخ). وأثبتت هذه الدراسات أن استهلاك المؤثرات العقلية أو الكحول مرتبط بشكل كبير باستخدام المواد الإباحية على الإنترنت وبممارسة الجنس عبر الرسائل النصية، وتعمل المؤثرات العقلية على الشعور بالتثبيط من خلال إبرازه، وتعمل على تخفيف الشعور بالعواطف مثل الخزي أو الذنب. كما أبرزت أيضا ارتباط ظاهرة استخدام المواد الإباحية على الإنترنت أو إرسال الرسائل الجنسية باستهلاك المواد أو الكحول، وبالتالي خلق تكييف بين المؤثرات العقلية والمواد الإباحية .[2]

ويعتقد بعض المراهقين أن المواقع الجنسية دليلًا للممارسات الجيدة وأنه مصدر للتعلم الصحيح، ويتم الانقياد وراء هذه المواقع لدرجة أنها تستطيع التحكم فيهم من خلال تأجيج الإثارة وتخطي الخيال، وينتهي الأمر بإغراق المراهقين الأكثر هشاشة في الفاحشة، وغالبًا ما يؤدي بهم تدريجيًا إلى إدمان الإباحية ويصبحون معرضون لفقدان الحس باللذة الجنسية بمرور الزمن وللإصابة بمختلف الأمراض الجنسية أو العقلية أو العصبية .[3]

---

[1] – المشاهدة الجنسية تتلف الدماغ : موقع عبد الدائم الكحيل :http//www .kaheel 7.com تم الإطلاع عليه في 2017/09/27

[2] – Pornographie en ligne : des risques préoccupants pour les adolescents

https://www.lagazettedescommunes.com ،vu le 25 /12/2022 a 21:35

[3] –Barbara Smaniotto، Réflexions autour de l’impact de la pornographie… sur la sexualité adolescente، Revue de l'enfance et de l'adolescence 2017/1 (n° 95), p5

- المخاطر المُترتبة على الفرد:

من أهم مخاطر الإباحية على الأفراد المشاكل التي تتسبب فيها بين الزوج وزوجته. لأن المدمن يعيش في جو خيالي بعيد عن الواقع، ويصبح الجنس بالنسبة له عملية افتراضية تؤثر على علاقته بالطرف الأخر وتحولها إلى علاقة جنسية بحتة خالية من الأحاسيس. الأمر الذي يؤدي إلي افتقاد الشعور بالسعادة تدريجيا، وكنتيجة حتمية تؤدي إلى فشل المدمن في علاقته الزوجية.[1] فضلا عن هذا يمكن أن تؤدي المواد الإباحية والإدمان إلى قيام المدمن بأفعال جنسية غريبة وغير طبيعية، مما يؤدي في النهاية إلى إصابته بأمراض ناجمة بشكل رئيسي عن العلاقات والسلوكيات المحرمة.[2]

إضافة إلى هذا قد تتسبب الأفلام الإباحية في مشاكل في الحياة الزوجية بسبب عدم رضا أحد الأطراف، مهما وصل الشريك إلى أقصى إمكاناته لإرضائه، إلا أن المدمن يرى أن الشريك لا يستطيع إرضائه كما تفعله تلك الجرائم[3]. ولأن المدمنين على المواد الإباحية لا يمكنهم تجربة العاطفة الطبيعية التي تأتي من النشاط الجنسي التلقائي. فإن رغبتهم في تطبيق ما تم مشاهدته في الأفلام الإباحية سيحرجهم أمام أزواجهم، لأن ما يتم مشاهدته غير واقعي سيجعلهم ينطوون على أنفسهم ويعيشون في عالم خيالي.

وبحسب دراسة أجراها علماء في معهد ماكس بلانك في برلين، وهو معهد اختص في التنمية البشرية، خلصوا فيها إلى أن هناك فرقًا بين الرجال المدمنين على المواد الإباحية مُقارنة بالرجال الذين لا يُشاهدونها وهذا الاختلاف يتمثل في تلف القشرة الدماغية، وكذلك تقلص جزء من الدماغ الذي يعمل على التشجيع والتحفيز الدماغي ويطلق عليه مصطلح striatum.[4]

---

[1] – المشاهدة الجنسية تتلف الدماغ :الموقع السابق

[2] –إدمان المواد الإباحية تدمير للفرد والمجتمع : مقال منشور على الموقع: http//www .afrigatenews.net تم الإطلاع عليه في 2017/09/27

[3] – إدمان الزوج للمواقع الإباحية: مقال منشور على الموقع التالي : http//www .aljazeera.net تم الاطلاع عليه في 2022/06/28

[4] – إدمان المواد الإباحية تدمير للفرد والمجتمع، الموقع السابق.

ومن بين آثاره ميل الشباب إلى استهلاك المنشطات الجنسية بشكل كبير للتوفيق بين الواقع وما يشاهدونه في الأفلام الإباحية، وهذه المنشطات قد لا ترقى إلى مستوى المهمة، الأمر الذي يؤدي إلى إدمانها للوصول إلى الاكتفاء الجنسي المرغوب فيه.[1]

ومن آثارها أيضا خلق نوع من العقد النفسية خاصة بين فئة المراهقين وعدم رضاهم بأشكال أجسادهم الأمر الذي أدى إلى انتشار عمليات التجميل الجسدية خاصة في البلدان المتقدمة وذلك من أجل تعديل ما قد يرونه غير طبيعي متأثرين بأبطال الأفلام الإباحية.

-المخاطر المُترتبة على المجتمع :

فوفقا لدراسة علمية نشرت في مجلة جراحة الأعصاب عام 2011، أدت المواد الإباحية إلى انتشار السلوكيات غير الطبيعية، بما في ذلك القسوة والعنف تجاه المرأة. والسلوكيات الغير عادية تجاه الأطفال، مثل الاعتداء عليهم جنسيًا في الحياة الواقعية.[2] كذلك تسببت في الانحراف وكثرة الجرائم الجنسية التقليدية داخل المجتمع وانتشار الرذيلة والفسق.

الفرع الثاني : تأثير جرائم الترويج والمتاجرة بالمخدرات عبر الإنترنت على المجتمع

تعتبر ظاهرة ترويج المخدرات عبر الإنترنت من أخطر التحديات الاجتماعية، حيث أصبحت حيازة المخدرات وتعاطيها وإدمانها ظاهرة اجتماعية عالمية، مما يدل على الخلل القائم في النظم التعليمية والاجتماعية في العديد من المجتمعات. والمهم أن الإحصائيات الحكومية تظهر أن عدد مدمني المخدرات في تزايد عند الجميع. كما تظهر الأبحاث العلمية التي أجريت في الدول العربية أو في العديد من دول العالم أن المخدرات هي السبب الرئيسي لجرائم مثل السرقة والقتل والتهريب وغيرها من الجرائم. فضلا عن خطورتها التي تكمن في آثارها المدمرة على القدرة الإنتاجية وعلى الصحة الجسدية والعقلية، ولا تقتصر أضرارها على المدمن فقط، بل تمتد إلى الأسرة والمجتمع ككل.

---

[1] – كريم احمد ،أضرار مشاهدة الأفلام الإباحية: مقال منشور على الموقع التالي :http//www .almawdoo3.com تم الاطلاع عليه في 2022/06/28

[2] – إدمان المواد الإباحية تدمير للفرد والمجتمع، الموقع السابق.

الفقرة الأولى: الآثار الاجتماعية للمخدرات علي الفرد

من أهم هذه الآثار نذكر ما يلي :

– عدم التوافق الاجتماعي: بسبب تعاطي المخدرات أو الإدمان لا يستطيع الفرد إقامة علاقات اجتماعية طبيعية مع أسرته أو مع أفراد مجتمعه. وهذا سيؤدي به إلى العزلة الاجتماعية الأمر الذي يزيد من ضغطه النفسي ومن قلقه وبالتالي يزيد من إدمانه للهروب من الواقع .

– عدم قدرة الفرد على القيام بأدواره الاجتماعية: كنتيجة طبيعية لعدم التكيف الاجتماعي للمدمن والعزلة الاجتماعية والانحراف السلوكي، يفشل الفرد في الوفاء بالتزاماته الاجتماعية مثل مسؤوليات الأب أو الابن أو الزوج أو العامل. وهذا الفشل سيؤدي به في معظم الأحيان إلى الجريمة والانحراف الاجتماعي .

– الأضرار الجسمية : أظهرت العديد من الدراسات الطبية والاجتماعية والنفسية أن المخدرات تؤثر على جميع أجهزة الجسم، مما يؤدي إلى توقف تلك الأجهزة وتعطل عملها، مما يجعل الإنسان في كثير من الأحيان عرضة لخطر المرض والوفاة. وتشمل هذه المخاطر توقف وظائف الجزء العلوي من الدماغ، وأمراض الجهاز الهضمي والجهاز التنفسي، والعقم، وفشل الجنين عند النساء الحوامل اللاتي يتعاطين المخدرات، وضعف الجسم، ونقص المناعة، والشلل والإيدز، وغيرها الكثير.[1]

الفقرة الثانية: الآثار الاجتماعية للمخدرات علي الأسرة

أهم الآثار سنبرزها في النقاط التالية:

– التفكك الأسري : يؤدي إدمان أحد أفراد الأسرة للمخدرات إلى حدوث خلـــل في التوازن

[1] – أضرار المخدرات على جسم الإنسان : مقال منشور على الموقع التالي :http//www .hopeeg.com تم الاطلاع عليه في 2022/09/28

داخل الأسرة خاصة إذا كان المدمن رب تلك الأسرة، حيث تصبح الأولوية للمـــدمن هي تغذية إدمانه بالدرجة الأولى وعلى حساب كل شيء حتى أسرته.

– إن تفكك الأسرة وفقدان السيطرة على أفرادها يؤثر بشكل كبير على مكانتها الاجتماعية والاقتصادية في المجتمع ويغير أيضاً نظرة الأسرة في المجتمع، ونتيجة لذلك تصبح الأسرة غير قادرة على القيام بالوظائف الاجتماعية المتوقعة منها، ويصعب معها تلبية احتياجات الحياة.

– أثر المدمن علي أفراد الأسرة : إذا كان هناك مدمن مخدرات في الأسرة، خاصة إذا كان رب الأسرة، وباعتباره النموذج يمكن أن يؤدي إلى انحراف الأبناء، وبالتالي تفاقم المشاكل داخل الأسرة ، الأمر الذي سيؤدي في النهاية إلى دمارها وانهيارها.

الفقرة الثالثة: الآثار الاجتماعية للمخدرات علي المجتمع

يمكن تحديد تأثير المخدرات على المجتمع من خلال النقاط التالية:

– يمثل متعاطي المخدرات والمدمنين شريحة مهمة من المجتمع تعتمد عليهم في التنمية الاجتماعية. وإذا تم الإخلال بهذا المصدر المهم للموارد البشرية، فإنه سيؤثر بالتأكيد على عملية تنمية المجتمع. وبذلك أصبح من الواضح أن المخدرات لها تأثير سلبي على الإنتاج الوطني وبرامج التنمية الاقتصادية والاجتماعية نتيجة تراجع الكفاءة الإنتاجية للمجتمع بسبب تراجع إنتاجية مدمني المخدرات ومتعاطيها.

– ونظراً لحجم الأموال التي تنفقها الدولة على التعليم والإعداد المهني لهؤلاء الأشخاص، فإن تعاطي المخدرات يمثل إهداراً لموارد الدولة. فإن انتشار المخدرات في المجتمع يتطلب عبئا ماليا كبيرا على الدولة، وذلك من خلال زيادة الإنفاق على المجالات غير الإنتاجية، مثل تكلفة علاج مرضى المخدرات ورعاية المدمنين، وإنشاء مستشفيات متخصصة لتقديم العلاج والأدوية، فضلا عن التكاليف الموجهة لملاحقة تجار ومهربي المخدرات من قبل أجهزة محاربة المخدرات مثل الجمارك ووزارة العدل ووزارة الصحة ورجال الضبطية.

– التفكك الاجتماعي : الأسرة هي أساس المجتمع وجينته الأول، وعدم استقرار الأسرة وتفككها لا يؤثر على الفرد بمفرده، بل تأثيرها يمتد إلى المجتمع بأكمله.

– إن استهلاك المخدرات والكحوليات أحد الأسباب الأساسية في زيادة عدد حوادث الطرق، مما يعني ارتفاع التكاليف المالية وخسارة كبيرة على المستوى الاجتماعي والاقتصادي.

– إنتشار الجريمة والسلوك الغير أخلاقي من الآثار الناجمة عن تعاطي وإدمان المخدرات، حيث عدد كبير من الجرائم يلعب تعاطي المخدرات والإدمان فيها دورا هاما. ومن أمثلة ذلك السرقة والسطو والاحتيال والقتل للحصول على المال لشراء المخدرات بسبب تأثير المهلوسات والمخدرات على العقل والسلوك الإنساني.

وبما أن الإدمان يخلق لدي الشخص عدم التوازن في موقفه وتفكيره ويتحكم في مشاعره وعواطفه، ويؤثر أيضا على ميوله الأخلاقية، الأمر الذي يؤدي به حتما إلى سرقة المقربين منه ضاربا عرض الحائط جميع الأعراف الاجتماعية، والقوانين السائدة في مجتمعه. وبالتالي السعي لتلبية رغباته بالطرق الشرعية والغير شرعية وحتى لو اضطر لاستخدام العنف.

الفرع الثالث : تأثير جريمة غسيل الأموال عبر الإنترنت على المجتمع

تترك جريمة غسيل الأموال باستعمال الإنترنت أثار سلبية على المستوى الاجتماعي للفرد ومن خلاله على المجتمع ومن مخاطر جريمة غسل الأموال تزايد مشاكل التضخم والركود والبطالة، وهي مشاكل تؤثر سلباً على حياة الطبقة الوسطى، مما قد يؤدي إلى تآكلها.

تجدر الإشارة إلى أن العمل الإجرامي المتمثل في غسل الأموال يصاحبه تضخم وانخفاض في قيمة العملة المحلية، وشل اقتصاد البلاد ونمو الطبقة الوسطى والفقيرة، مما يعني انخفاض الدخل الفردي وانخفاض القدرة الشرائية، مما يزيد من أعباء الأفراد. ما قد يؤدي بهم إلى السقوط فريسة سهلة للانحراف.

الفرع الرابع : تأثير الإرهاب الإلكتروني من الناحية الاجتماعية

يؤثر الإرهاب بطريقة مباشرة على الحقوق الاجتماعية، عن طريق اعتداءاته على المنشآت الصناعية الأمر الذي يؤدي إلى تدني الاقتصادي نتيجة للعزلة الاجتماعية، وقلة فرص عمل وارتفاع نسبة البطالة.

كما يستهدف التطرف العنيف طبقات المجتمع المهمشة، واستغلال قلة علمهم لتغليطهم بالمفاهيم الدينية المتطرفة وتحريضهم على العنف والأعمال التخريبية. إضافة إلى القيود المفروضة على الحريات الدينية من طرف المنظمات المتطرفة الأمر الذي يؤدي إلى خلق تشنجات في العلاقات المؤدية في أغلب الأحيان إلى خلق الكراهية بين أفراد المجتمع المعتنقة لديانات مختلفة، وهذا يؤدي إلى عزل المجتمع الذي تنطلق منه هذه الأشكال من التطرف عن باقي المجتمعات.

كما له الأثر السلبي المتمثل في خلق الخوف والشعور بانعدام الأمن داخل المجتمعات، كذلك خلق نوع من الكره للجنسيات الأجنبية والديانات الأخرى وعدم تقبلهم، كذلك نشر الأفكار المتطرفة والممارسات العنيفة ضد المرأة.

المطلب الثاني : تأثير جرائم الإنترنت من الناحية الاقتصادية

مع الطبيعة العالمية لجرائم الإنترنت فإنها تؤثر على الاقتصاد في عمومه وكافة قطاعاته. وتأثيرها يتجاوز بكثير الأثر الاقتصادي للجريمة التقليدية، حيث أظهرت دراسات نشـــرت في 9 /06/ 2014 إلى أن جرائم الإنترنت ينتج عنها حولي نحو 445 مليار دولار خسائر اقتصادية عالمية كل عام[1]، وتتسبب بخسارة لحقت بقطاع الأعمال قدرت بحوالي 160 مليار دولار نتيجة سرقة حقوق الملكية الفكرية، وأضاف تقرير مركز الدراسات الإستراتيجية والدولية أن الجريمة المعلوماتية تعود بالضرر على التجارة والابتكار، وأن إجمالي خسائر أمريكا والصين واليابان وألمانيا بلغ 200 مليار دولار سنويا،

[1] – الجرائم الإلكترونية https://www.mcit.gov.sa، تم الاطلاع عليه في 26 مارس 2021 على الساعة 19:07

أما الخسائر التي تتعلق بالمعلومات الشخصية فقد بلغت 150مليار دولار. وذكر أن الجريمة الإلكترونية تقلل من وتيرة الابتكار العالمي بتقليل معدل العائد للمبدعين والمستثمرين.[1]

وفي نهاية 2019 حدث هجوم إلكتروني على شركة سولار ويندز الأميركية وسرقت بيانات ثمانية عشر ألف عميل من بينهم وزارات في أميركا، هذا الهجوم لم يكتشف إلا في أواخر عام 2020 .

وبحسب شركة سيبار سيكوريتي فونتورز فإنه ومن الممكن أن تصل خسائر الجرائم السيبرانية العالمية إلى 10.5 تريليون دولار بحلول عام 2025، إذ من المتوقع أن تنمو هذه الخسائر العالمية بنسبة 15% سنويا على مدى السنوات الخمس المقبلة، لتصل إلى 10.5 تريليون دولار في عام 2025، في حين كانت 3 تريليون دولار عام 2015.

وتشمل المبالغ المذكورة أعلاه تلف وتدمير البيانات، سرقة الأموال، قلة الإنتاجية، وسرقة الملكية الفكرية، وسرقة المعلومات الشخصية والمالية، الابتزاز، والاحتيال، غسل الأموال وتعطيل العمليات التجارية ...الخ[2].

ومن تأثيرات جرائم الإنترنت على مستوى الفرد، تلك التي تؤثر على الجانب المادي لديه، كسرقة بطاقة الائتمان الخاصة به أو تعرضه للابتزاز والتهديد أو لعمليات احتيال ونصب أو تحويل أو نقل حسابه المصرفي للجاني أو نقل ملكيته للأسهم أو زيادة الفواتير بتحويل فواتير المجرم للضحية.

أيضا في ضل الأزمة الصحية التي مست العالم بانتشار فيروس كوفيد 19 الذي كان من نتائجه انفتاح كل العالم على الإنترنت لكونها أصبحت الوسيلة الوحيدة للاتصال بالعالم

---

[1] – تقرير جرائم الإنترنت https://www.alittihad.ae/article/13882/2018، تم الاطلاع عليه في 22 فيفري 2020 على الساعة 10:55

[2] – مقال منشور على الرابط التالي :https://www.alarabiya.net/aswaq/special-storie، تم الإطلاع عليه في 15 نوفمبر 2021 على الساعة 14:32

الخارجي، عرفت الجريمة عبر الإنترنت تفشيا وارتفاع كبير في معدلاتها، خاصة الجرائم المستهدفة للأموال والأمن الوطني مثل جريمة الاحتيال عبر الإنترنت والسرقة والتزوير والقرصنة، ولقد شهدت بعض الدول المصابة بالفيروس موجة من جرائم الاحتيال والنصب من بينها الجزائر، وفي هذا الشأن أبدت الشرطة الفرنسية قلقها من خلال تقرير لها أوضحت فيه مخاوفها من انتشار لمواقع مبيعات زائفة عبر الإنترنت، وكذا شعورها بالقلق الكبير إزاء ظهور برامج لسرقة البيانات الشخصية للأفراد قصد سرقة حساباتهم وتهديد أمنهم، ولقد جاء في نفس التقرير أنه وفي الأسبوع الأول من الحجر الصحي تلقت منصة فاروس الفرنسية التي تديرها الشرطة القضائية مئة شكوى، أغلبها يتعلق بالنصب عبر الإنترنت، ويتوقع الكثير أن هذا العدد قابل للارتفاع أكثر فأكثر في ضل الإقبال الكبير على الإنترنت الذي سيكون له حتما آثارا وخيمة .[1]

إضافة إلي ما سبق شهدت بعض الدول المتقدمة في الوقت الذي انتشرت فيه جائحة كورونا، تفشي ظاهرة تعرف بالهجوم السيبيراني خاصة علي المستشفيات أدت إلى عرقلة السير الحسن لها الأمر الذي تسبب في التأخر بالاعتناء ببعض الحالات المصابة بالفيروس ما أدي إلي وفاتهم.

إن جميع الأفعال الإجرامية المرتكبة عبر الإنترنت لها آثار اقتصادية تتسع حسب جسامة الفعل وخطورته، وتأتي جريمة غسل الأموال والترويج للمخدرات في طليعة الجرائم الاقتصادية المؤثرة على اقتصاد الدول إضافة إلى العديد من الجرائم الأخرى.

الفرع الأول : تأثير جرائم الاختراق وقرصنة البيانات

تنجم عن جرائم الاختراق وقرصنة البيانات حجم كبير من الأضرار التي تؤثر على اقتصاديات الدول وهي جرائم مست كافة دول العالم .

[1] -https://www.20minutes.fr/societe/2743143-20200318. Vu le 16 septembre 2020 à 05.:21

ففي عام 2019 تم الإبلاغ عن أكثر من 3800 حالة اختراق للبيانات، مما أدى إلى تعرض أكثر من 4 مليار قاعدة بيانات للاختراق خاصة الخاصة بالأشخاص، وقد حققت وزارة الصحة الأمريكية في أكثر من 550 مليون حالة من اختراق المعلومات الشخصية الناجمة عن السرقة أو القرصنة أو الوصول إلى المعلومات الغير مصرح بها، وتشمل هذه الحالات 35 مليون فرد وغالبا ما تكون هذه الاختراقات من الداخل ومن الخارج.[1] ومن الأمثلة الحديثة على خرق البيانات خرق 100 مليون قرص لمؤسسة "كابيتال وان" عام 2019 من طرف مهندس من نفس الشركة .[2]

ووفقًا لتقرير الجرائم الإلكترونية الصادر عن مركز شكاوى جرائم الإنترنت التابع لمكتب التحقيقات الفيدرالي FBI ، شهدت الولايات المتحدة الأمريكية زيادة غير مسبوقة في الهجمات الإلكترونية والأنشطة الإلكترونية الغير مشروعة في عام 2021. من أهمها اختراق البريد الإلكتروني والذي أدى إلى خسائر معدلة بقيمة 2.4 مليار دولار للشركات والأفراد . ويمثل هذا الرقم زيادة كبيرة عن رقم 1.8 مليار دولار الذي تم الإبلاغ عنه في عام 2020. وبالنسبة للجمهور الأمريكي ، يعد هذا أيضًا رقمًا قياسيًا جديدًا للخسائر المالية من الهجمات المخترقة للبريد الإلكتروني. وشكلت هذه الهجمات ما يقرب من 35 ٪ من جميع الخسائر المالية المتعلقة بجرائم الإنترنت التي تم الإبلاغ عنها العام الماضي، بزيادة 28 ٪ عن عام 2020، وقدم ضحايا الجرائم الإلكترونية عددًا قياسيًا من الشكاوى إلى FBI وتتجاوز الخسائر المحتملة بسبب هذا النوع من الجرائم 6.9 مليار دولار. وبينما زاد عدد الشكاوى المقدمة بنسبة 7٪ فقط مقارنة بعام 2020 ، وقفز إجمالي الخسائر المنسوبة لحوادث الجرائم الإلكترونية بنسبة 64٪ في عام 2021 ، بحيث كانت 4.2 مليار دولار في عام 2020.[3]

---

[1] –Zhanna Malekos Smith ،Eugenia Lostri ،James A. Lewis .(DECEMBER 2020) .The Hidden Costs of Cybercrime .McAfee, San Jose.p 24

[2] –ما هو خرق البيانات (Data Breach) وكيف يمكنك حماية نفسك؟ على الموقع التالي:https://www.annajah.net

[3] – Rapport IC3 du FBI : les pertes financières dues à la fraude par email atteignent un niveau record en 2021 ،https://www.proofpoint.com ، vu le 07/09/2022

وفي الجزائر أدان الخبير في المعلوماتية "عثمان عبد اللوش" القرصنة الإلكترونية وأشار إلى انتشارها الكبير وارتكابها بشكل يومي، حيث إن كل شخص يملك حسابا وأي مؤسسة لديها موقع إلكتروني مهدد بأن يكون ضحية للقرصنة، كون هذه الجرائم أصبحت سهلة في ظل غياب الثقافة الرقمية، أو ما يسمى بالأمية الرقمية، خاصة وأن الكثير يجهل التعامل مع الأجهزة الإلكترونية.

فقد سجلت المصلحة المركزية لمكافحة الجرائم المعلوماتية التابعة للأمن الوطني قرصنة 200 موقع خاص بالمؤسسات الوطنية الخاصة والعامة بالإضافة إلى البنوك عام 2015، حيث لم تسلك المؤسسات العمومية والخاصة من الحروب التي يشنها القراصنة على مواقعها المتنوعة، حيث سجلت الجهات المختصة قرصنة ما يصل إلى 200 موقع لمؤسسات عمومية وخاصة. فالهجمات على مثل هذه المؤسسات من قبل المتسللين ليست نتاج دوافع ترفيهية ولكنها جرائم تركز على المال وعلى الانتقام.[1]

الفرع الثاني : تأثير جرائم الاحتيال والسرقة عبر الإنترنت

يتكبد الأفراد والمؤسسات مبالغ ضخمة وخسائر كبيرة من جراء جرائم الاحتيال والسرقة عبر الإنترنت. ومن بين أكبر السرقات حول العالم سرقة المنصة التي تتخذ من طوكيو مقراً لها، والتي شهدت تداول 70% من جميع عملات بتكوين حول العالم والتي كانت هدفاً مثالياً للمخترقين، الذين استخدموا أوردر بووك الذي يسرد معلومات حول عدد العملات المتداولة، وقاموا بسرقة 850 ألف عملة بتكوين. وعلى الرغم من استرجاع 200 ألف عملة في ما بعد ذلك إلا أنه لم يتم محاكمة الجناة، هذا وكانت قيمة المسروقات 23 مليار دولار والذي يعتبر من حيث الخسائر أكبر اختراق.

أيضا تعرضت أكبر شركات الدفع في أميركا لأحد أخطر التسريبات الأمنية في التاريخ وتعرض النظام السيبراني لهذه الشركة لاختراق لمعلومات بطاقات الائتمان لعشرات الملايين من العملاء لديها، وتم القبض على منفذ الاختراق وتمت محاكمته وعوقب بـ 20 سنة سجن. وبالرغم من القبض عليه لم يتغير مقدار الخسائر التي مست بالشركة والتي

[2] – القانون الجزائري.. لا يُدين الهاكر، مقال منشور على الرابط التالي :https://africanews.dz اطلع عليه 23 /2022/05 على الساعة 20:50

وصلت لحوالي 140 مليون دولار مبالغ تعويضات و26 مليون دولار دفعت كرسوم قانونية[1].

إضافة إلى جريمة السرقة عبر الإنترنت يقع عشرات الآلاف من الناس ضحية للنصب والاحتيال، والشعور الرئيسي لهؤلاء جراء هذه الجريمة هو الإحباط والخيانة أو الاغتصاب. والحقيقة أن النصب تجارة مربحة لمرتكبيها. ومن أهم أنواع الاحتيال المربح الاحتيال الرومانسي أو الودي الذي كلف خاصة النساء مبالغ باهظة. ففي أمريكا مثلا كلف الأميركيين نحو 350 مليون دولار في عام 2021. ويُعرِّف مكتب التحقيقات الفيدرالي "عملية احتيال الرومانسي" على أنها جريمة يرتكبها مجرم يقدم ادعاءات كاذبة وغير صحيحة على الإنترنت لإيقاع بضحيته، ثم يبدأ في إرباك وإغراء الضحية لكسب ثقتها وإقامة علاقة رومانسية معها للاستيلاء على ما تملكه من أموال[2]. وهذا النوع من الاحتيال أصبح منتشرا بشكل كبير في مختلف بلدان العالم بما فيهم الجزائر.

وقد كشف تقرير أصدره المركز الوطني لبريطانيا للإبلاغ عن جرائم الاحتيال باستخدام الإنترنت، عن تلقي حوالي 8863 شكوى كلها تتعلق بعمليات احتيال إلكتروني كانت ضحيتها نساء تعرضوا لخسائر كبيرة بسبب علاقاتهم الافتراضية عبر الانترنت، وهذه الجرائم وقعت بين سنة 2020 وسنة 2021. وقد بلغ عدد الشكاوي لسنة 2021 وحده حوالي 901 شكوى، وتسببت عمليات الاحتيال العاطفي هذه بسرقة حوالي 100 مليون جنيه استرليني[3].

---

[1]– 5 جرائم سيبرانية تسببت في خسائر مالية وأمنية كبيرة، مقال منشور على الرابط التالي:
https://www.cnbcarabia.com

[2] – محمد سناجلة ، خسائر بملايين الدولارات للباحثين عن الحب في الإنترنت، مقال منشور على الرابط التالي :
https://www.aljazeera.net

[3]– الاحتيال الرومانسي الذي يقع فيه البريطانيون، مقال منشور على الرابط التالي :
https://www.trtarabi.com/explainers

أيضًا من أهم أنواع الاحتيال الخطيرة الاحتيال في التجارة الإلكترونية إذ يتعرض الضحايا للاحتيال من طرف أصحاب مواقع إلكترونية غير معتمدة، أو صفحات على منصات التواصل الاجتماعي بعد قيامهم بالترويج لسلع سواء مغشوشة أو غير مطابقة للصور المنشورة. وتتم عمليات "الاحتيال" بعدم تلقي السلع التي دفع ثمنها، أو بتلقي سلعا غير مطابقة لما تم الاتفاق عليه مسبقا.

ولقد وجدت دراسة أجراها مركز الولايات المتحدة للدراسات الإستراتيجية والدولية حديثا أثبتت أن خسائر الجرائم الإلكترونية في جميع أنحاء العالم بلغت قيمتها 445 مليار دولار، وكانت الولايات المتحدة وأوروبا في المقدمة، وأثبتت الدراسة أيضا أن تأثير الجريمة السيبرانية تجاوز الخسائر المالية، حيث تنفق الشركات والحكومات كميات كبيرة من الوقت والمال على تدابير الأمن السيبراني وعليه فإن للاحتيال عبر الإنترنت آثار مالية وشخصية كبيرة على العملاء، بما في ذلك الخسائر المالية وانتهاكات المعلومات الشخصية، حيث تتسبب جرائم الإنترنت في خسائر بمليارات الدولارات في جميع أنحاء العالم[1].

الفرع الثالث : تأثير الجرائم المتعلقة بانتهاك الملكية الفكرية على الجانب الاقتصادي

يشكل الاعتداء على حق الملكية الفكرية من أخطر الجرائم المنتشرة في وقتنا الحالي خاصة في ضل التطور وظهور التكنولوجيات الحديثة، وأهم الاعتداءات وأخطرها هي جريمة التقليد والقرصنة بالنظر لأثارها السلبية على الجانب الاقتصادي. ونسبة لإحصائيات عالمية هناك ما يقرب من 40 مليار دولار خسارة سنوية في جميع أنحاء العالم بسبب انتهاك حقوق الملكية الفكرية عبر الإنترنت.

ولقد نشر مكتب الاتحاد الأوروبي للملكية الفكرية ومنظمة التعاون الاقتصادي والتنمية بداية سنة 2023 دراسة حول تأثير انتهاكات حقوق الملكية الفكرية على الشركات الصغيرة والمتوسطة.

[1]– 445 مليار دولار...الاحتيال عبر الإنترنت: ظاهرة متفاقمة ولا حلول حقيقيّة مقال منشور بتاريخ 2023/04/26 على الموقع التالي :https://madar.news اطلع عليه 2023/04/29 على الساعة 11:38

حيث أظهر التقرير المتعلق بمخاطر التجارة غير المشروعة في السلع المقلدة للمؤسسات الصغيرة والمتوسطة الحجم أن الشركات الصغيرة والمتوسطة التي تُنتهك ملكيتها الفكرية أقل عرضة بنسبة 34٪ للبقاء على قيد الحياة. فالخطر كبير بشكل خاص بالنسبة للشركات الصغيرة والمتوسطة المستقلة التي تقع ضحية التعدي على براءات الاختراع والتي ليست جزءًا من مجموعة كبيرة .

إن البراءات هي حقوق الملكية الفكرية التي تحمي الابتكارات بشكل مباشر. وبالتالي فإن الهجمات على براءات الاختراع تشكل خطورة خاصة على الاقتصاد بشكل عام والشركات الصغيرة والمتوسطة على وجه الخصوص، ووفقًا لأحدث SME Scoreboard، وقع 15٪ من الشركات الصغيرة والمتوسطة التي لديها حقوق ملكية فكرية مسجلة ضحايا لانتهاكات حقوق الملكية الفكرية. هذه النسبة أعلى بالنسبة للشركات الصغيرة والمتوسطة التي أدخلت ابتكارات (19.4٪ في حالة الشركات الصغيرة والمتوسطة التي أدخلت ابتكارات على مستوى العالم). وبالتالي فإن التعديات على حقوق الملكية الفكرية هي مشكلة خاصة للشركات الصغيرة التي تبتكر وتخلق فرص العمل والنمو.[1]

الفرع الرابع: تأثير غسيل الأموال من الناحية الاقتصادية

لجريمة غسل الأموال تأثير سلبي على الاستثمارات في كل من البلدان التي تنشأ منها الأموال غير المشروعة والبلدان التي تتدفق إليها. ومن أهم هذه الآثار.

أولا- تأثير خروج الأموال غير المشروعة على الاستثمار:

إن خروج الأموال يتسبب في زيادة الطلب على العملة بسبب تحويل الأموال غير المشروعة إلى عملة حرة لتهريبها إلى الخارج، مما يؤدي إلى نقص الأموال المتاحة للاستثمار. وللحصول على السيولة يلجأ المستثمرين أصحاب الأموال غير الشرعية إلى رشوة العاملين في البنوك أو في أي مؤسسة نقدية عامة كانت أو خاصة، وتخسر البلدان

[1] – Les atteintes à la propriété intellectuelle constituent une menace majeure pour les PME de l'UE LE MONDE DU DROIT 1 FÉVRIER 2023 https://www.lemondedudroit.fr

جزءاً كبيراً من عملاتها الأجنبية التي كان من الممكن استخدامها في الاستثمار الحقيقي الذي من شأنه أن يعزز التنمية.[1]

ومن الجدير بالذكر أن إخراج الأموال التي تم الحصول عليها عن طريق الجريمة، أيا كان نوعها، له تأثير أكبر بكثير من إخراج الأموال التي تم الحصول عليها عن طريق الأنشطة المشروعة. لأن هذه الأخيرة استخدمت لخدمة الاقتصاد الوطني وتلبية احتياجات عددا كبيرا من الأشخاص. أما الأموال التي تأتي بشكل غير قانوني فهي من مصادر تضر بالمجتمع في المقام الأول. مثل السرقة والقمار وتجارة المخدرات، فضلا عن أنها تمنع الجمهور من استثمار رأس ماله في الأشياء الجيدة.[2]

ثانيا: تأثير دخول الأموال غير المشروعة على الاستثمار

للأموال غير المشروعة تأثير سلبي على الاستثمار في البلدان التي يتم غسلها فيها، وذلك من النواحي الآتية:

– ترتبط الأموال القذرة بعدم الاستقرار، حيث تنتقل من مكان إلى آخر مع التغيير في أشكالها للاحتفاظ بها. ومن أبرز هذه الأشكال الودائع والسندات والأسهم والعقارات. وهذا يجعلها عديمة الفائدة للاستثمار الاقتصادي الوطني. [3]

– يتم ضخ الأموال الغير نظيفة بشكل روتيني في المشاريع الحرة في البلد المقصد، مما يفقد ثقة الأشخاص المشاركين في هذه المشاريع، الأمر الذي يكون له عواقب سلبية.

– من نتائج دخول الأموال غير المشروعة فقدان الثقة في المؤسسات المالية. ولو تمكَّن غاسل الأموال من السيطرة على المؤسسات المالية سيشكل ذلك حتما خطرا كبيرا، إذ يؤدي

---

[1] – محمد عبد السلام سلام، جرائم غسل الأموال إلكترونياً في ظلّ النظام العالمي الجديد للتجارة الحرّة ، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، وغرفة تجارة وصناعة دبي، 10 . 12 مايو2003

[2] – سيد شوربجي عبد المولى، عمليات غسل الأموال وانعكاساتها على المتغيرات الاقتصادية والاجتماعية، المجلة العربية للدراسات الأمنية والتدريب، العدد345 :28 ، الرياض،1420

[3] – فؤاد مرسي، الرأسمالية تجدد نفسها، سلسلة عالم المعرفة، الكويت، 1990 ، ص126

ذلك إلى إلحاق الضرر بالتنمية لفقدان هذا النوع من المؤسسات تعاملها برأس المال المشروع.[1]

ثالثا: تأثير غسيل الأموال على المدَّخرات الوطنية

يؤثر غسيل الأموال على المدخرات الوطنية لبلد ما من خلال خروج رؤوس الأموال إلى الخارج دون إعادتها إلى الوطن، ويتم تحويل مدخرات البلاد إلى البنوك الأجنبية بدلاً من استثمارها محليا. ويتم تعويض هذا العجز بزيادة الضرائب على المواطنين والاعتماد على القروض من الخارج، وبالتالي زيادة الديون.

رابعا: تأثير غسيل الأموال على الأجهزة المصرفية والمؤسّسات المالية

غالباً ما تتم عمليات غسل الأموال داخل البنوك والمؤسسات المالية، الأمر الذي يعود بالسلب عليها وعلى اقتصادها الوطني.[2]

الفرع الخامس: تأثير جرائم الترويج والمتاجرة بالمخدرات عبر الإنترنت من الناحية الاقتصادية

تلعب معدلات الاستثمار المرتفعة دوراً مهماً في تحقيق النمو الاقتصادي. لكن إذا قام جزء كبير من المجتمع بإنفاق الأموال على شراء المخدرات بدلا من توفيرها، فإن ذلك سيؤثر على نمو الاقتصاد الوطني. علاوة على ذلك، تهدد جرائم المخدرات الاستقرار المالي للبلاد بزعزعة ثقة المستثمرين، خاصة المستثمرين الأجانب، ودفعهم للبحث عن أسواق أخرى أمنة، وهذا ما يؤثر سلباً على عملية التنمية الاقتصادية المحلية.

المطلب الثالث: تأثير جرائم الإنترنت من الناحية الأمنية

[1] – عصام محمد، مكافحة غسيل الأموال بين التجريم والتعاون الدول، المركز القومي للدراسات القضائية،1996 ،ص 5

[2] – فؤاد شاكر، التوجهات الإستراتيجية لمكافحة تبييض الأموال من قبل المصارف العربية ،تبييض الأموال، اتحاد المصارف العربية، عمان،2002 ، ص 11

إن الجرائم عبر الإنترنت مثل القرصنة والتجسس وجرائم الإرهاب المتواصلة قد تعرض الجهات والأجهزة الحكومية للخطر، الأمر الذي يؤدي حتما إلى زعزعة الأمن والاستقرار، وبذلك تتحمل الدول المستهدفة خسائر كبيرة.

الفرع الأول : تأثير الجماعات الإرهابية

استغلت الكثير من الجماعات المتطرفة شبكة الإنترنت من أجل نشر معتقداتها وأفكارها داخل المجتمعات، ونجحت في عدة ممارسات مست بأمن الدول المعتدى عليهم وسلامة أفرادها.

حيث استغلت الإمكانيات المتاحة عبر الإنترنت وتمكنت من التخطيط وتمرير التوجيهات الإجرامية وتنفيذ العمليات التي كان لها الوقع الكبير على الدول المجني عليها، إذ توصلت في بعض الأحيان إلى إبادة قري بأكملها وزعزعة بلدان كثيرة في أمنها.

الفرع الثاني: المساس بالنظام والأمن العموميين:

لقد وفرت الإنترنت مجالا واسعا للتأثير على ممارسات ومعتقدات وديانات الملايين من الأشخاص، مما يجعلهم عرضة لانتشار الأفكار والأمراض والصراع الديني، وانتشار جميع أنواع العنف.

ومن الجرائم المرتكبة عبر الإنترنت التي قد تتسبب في زعزعة الاستقرار السياسي انتشار المخدرات وما تؤدي إليه من مضاعفات كانتشار جرائم القتل والسرقة والتزوير والاحتيال والنصب والانحرافات الأخرى، الأمر الذي يضعف من الهيمنة السياسية للبلاد. كما أن ازدياد عدد المتعاطين والمدمنين للمخدرات من شأنه أن يمكن العدو من تسخير البعض منهم لغرض الجوسسة والقيام بالأعمال الإرهابية والتخريبية. ومن الأمثلة على ذلك ما تقوم به المخابرات الإسرائيلية (الموساد) في نشر الماريجوانا والأفيون والهيروين في عدد من البلدان والدول العربية منها مصر وفلسطين ولبنان والعراق، وتم نشر عدد من العملاء في البلاد. وعليه ينبغي أن لا نغفل الأبعاد السياسية لمشكلة المخدرات، وأن المخدرات في العصر الراهن أصبحت تستخدم كسلاح من أسلحة الحرب ضد الشعوب المستهدفة.

ومن الجرائم التي تهدف إلي المساس بالنظام والأمن العموميين الشائعات ونشر وترويج الأخبار الكاذبة عبر مختلف المواقع الالكترونية، حيث أصبحت الإشاعات خاصة

الإشاعات الالكترونية مؤثرة على مجتمعنا، وذلك أمر له انعكاساته السلبية على كافة النواحي، فالإشاعات يكون غرضها دائما زعزعة المجتمع وبالتالي المساس بأمنه واستقراره ، فالإشاعات الالكترونية خاصة الكاذبة منها تعد من اخطر الجرائم التي إذا تفشت في دولة ما اضطربت أحوالها وضعفت الثقة بين أبناءها. ونتيجة لانعدام وجود آليات دقيقة للتحقق من مصدر الأخبار والمعلومات على شبكات التواصل الاجتماعي، ارتفع عدد الشائعات وانتشر بصورة كبيرة، ويلاحظ في كثير من الأحيان أن متصفحيها يعتقدون أن هذه المعلومات دائماً صحيحة ويمكن الأخذ بها دون التأكد من صحتها وصحة مصدرها، مما يخلق شائعات في المجتمع ليس لها أساس من الصحة.

إن ظاهرة انتشار الشائعات الإلكترونية لم تعد مجرد أخبار كاذبة أو معلومات خاطئة يلقيها شخص معين، بل أصبحت جريمة يقف خلفها مؤسسات متخصصة احترفت التلاعب بالمعلومات بهدف زعزعة أمن واستقرار الدول، وتختلف طبيعة وغرض ومحتوى الشائعات. فالبعض لها غرض اقتصاديٌ والأخرى سياسي، مثل خلق عداوة بين الرؤساء السياسيين، وأحيانا قد تتعلق بقضايا صحية مثل التهويل حول انتشار بعض الأمراض والغرض منها بث الخوف والرعب بين أفراد المجتمع ...الخ من أنواع الإشاعات الكاذبة.

وفي هذا الصدد استغل بعض الأشخاص انتشار مرض كورونا في الجزائر لنشر بعض الأخبار المضللة عبر مختلف شبكات التواصل الاجتماعي والتي كان الهدف من وراءها تخويف وتهويل الأفراد وبث الإحساس بعدم الأمان لديهم، الأمر الذي كان له التأثير الكبير على بعض التصرفات التي قام بها العديد من افرد المجتمع كإقبالهم على تكديس المواد الغذائية لخوفهم من نفاذها في السوق. مما أدى السلطات العليا للتحذير من مثل هذه الأعمال التي من شانها المساس بسلامة المواطن وأمنه، لافتين انتباههم بان القانون يعاقب كل شخص قام بنشر معلومات أو خبر أو شائعات على أي شبكة معلوماتية أو أي موقع الكتروني بقصد المساس بأمن الدولة أو الأضرار بأي من مؤسساتها أو من شانها التشكيك في مجهودات الدولة وإثارة القلق والاضطراب لدى أفراد مجتمعها. إضافة إلى القرار الذي أصدرته لجنة الفتوى التابعة لوزارة الشؤون الدينية بتحريم مثل هذه الأفعال (الشائعات وقت الأزمات) واعتبارها من الكبائر لما تلحقه من أضرار على الفرد والمجتمع.

ولقد تم تجريم نشر وترويج أنباء كاذبة بأي وسيلة كانت بهدف المساس بالنظام والأمن العموميين من خلال التعديلات التي مست قانون العقوبات الجزائري وتم المصادقة عليها من طرف البرلمان في أفريل 2020.[1] وأدخل القانون رقم 20-06 المؤرخ في 28 أفريل 2020 المادة 196 مكرر في قانون العقوبات والتي نصت على معاقبة الجاني بالحبس من سنة إلى ثلاث سنوات ومبلغ 100.000 دينار ج إلى 300.000 دج غرامة مالية.

الفصل الثاني:

آليات مكافحة الجريمة عبر الإنترنت على المستوى الوطني والدولي

لم يكن التطور الكبير للإنترنت مصحوبًا بقواعد قانونية واضحة، ما أثار مخاوف عديدة بشأن الجرائم الواقعة عبر الإنترنت.

وقد جذب التهديد المتنامي للجرائم المرتكبة باستخدام الانترنت والمخاطر التي تخلفها على اهتمام معظم دول العالم. ولا تزال الجهود المبذولة لمكافحـــــة هذا النوع من الجرائـم قائمة بشكلٍ مكثف وجديّ خاصة في الدول الغربية، وبالمقارنة بهم لا تزال القوانين الوطنية متخلفة في هذا الموضوع، ولا تغطي مجموعة كبيرة من الجرائم السيبرانية .

إن النقص في الحماية القانونية يجبر الأفراد والشركات والحكومات على استخدام تدابير ووسائل محدودة لحماية مصالحهم وأنفسهم من الاختراقات الواقعة عبر الإنترنت إليها.

والتساؤل المطروح هنا يكون على مدى كفاية النصوص القانونية المتواجدة حاليا لمنع الجريمة عبر الإنترنت وردع مرتكبيها ومدى الحاجة إلى خلق نصوص قانونية جديدة للحد من هذه الظاهرة؟

لقد أصبح موضوع الآليات القانونية لمحاربة الجريمة عبر الإنترنت هاجسا يؤرق رجال القانون بصفة خاصة، لذلك أصبح من المستعجل أن تتسع دائرة التعاون مع رجال العلم المتخصصين في تكنولوجيا المعلومات ورجال القانون داخل الدولة، وعلى المستوى الدولي

[1]- القانون رقم 20-06 المؤرخ في 28 أفريل 2020 المعدل والمتمم للأمر رقم 66-156 المؤرخ في 08 يونيو 1966 والمتضمن لقانون العقوبات الجزائري،الجريدة الرسمية الصادرة في 29 افريل 2020،عدد25

أيضا بغية سن قوانين تكافح مرتكبي تلك الجرائم. وسنتناول في هذا الفصل مكافحة الجريمة عبر الإنترنت على المستوى الوطني، وعلى المستوى الدولي من خلال:

المبحث الأول: مكافحة الجريمة عبر الإنترنت على المستوى الوطني

المبحث الثاني: مكافحة الجريمة عبر الإنترنت على المستوى الدولي

المبحث الأول: مكافحة الجريمة عبر الإنترنت على المستوى الوطني

تسعى كافة الدّول والحكومات بشكلٍ جديّ وبكل الطرق القانونية للحدّ من الجَرائم عبر الإنترنت وآثارها، وفي إطار الجهود الدولية والإقليمية المتعلقة بسياسة مكافحة الجرائم المعلوماتية، عمل المشرع الجزائري على مسايرة المسار التشريعي لأجل البقاء على اتصال بأحدث الحلول التشريعية الخاصة بهذا النوع من الجرائم ، خاصة وأن الجزائر وفي السنوات الأخيرة تعرف تعميما لخدمة الربط بشبكة الانترنت، ودعم كبيرا للجهات الحكومية بتقنيات المعلوماتية، وهذا ما أدى إلى ارتفاع ملحوظ في معدلات الجرائم عبر الإنترنت، وهو ما دفع المشرع الجزائري إلى التدخل من أجل وضع خطط قانونية وعملية لتنفيذ سياسة وقائية ورادعة ضد الجرائم السيبرانية. وتجدر الإشارة على أن المشرع الجزائري قد وضع النصوص التي تعاقب على بعض الأفعال التي تشكل جرائم معلوماتية وكان ذلك سنة 2001، المادة 144 مكرر، ومكرر 1 ، ومكرر 2 ، والمادة 146 من قانون العقوبات ثم جاء القانون رقم 15/04 المؤرخ في 2004/11/10 الذي أورد فيه قسما خاصا تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، القسم السابع مكرر من قانون العقوبات ويشمل سبعة مواد من المادة 394 مكرر إلى المادة 394مكرر 7.

ولم يكتف المشرع الجزائري بذلك بل فرض حماية جنائية على الحياة الخاصة للأفراد من خلال القانون 23/06 المؤرخ في 2006/12/20 والذي مس المادة 303 وأقره بالمادة 303 مكرر إلى 303 مكرر 03، وهذا تصديا للاستخدام السيئ لوسائل التكنولوجيا الحديثة .[1]

[1] – مولود ديدان، قانون العقوبات، دار بلقيس للنشر، الدار البيضاء، الجزائر، 2012 ،ص 120.

إضافة إلي هذا أحكام الدستور الجزائري سنة 1996 الذي كفل حرمة الحياة الخاصة بالمواطنين من خلال ضمان سرية المراسلات والاتصالات الخاصة بجميع أشكالها. أيضا القانون رقم 18-07 الخاص بتحديد قواعد حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي في إطار احترام الحياة الخاصة للأفراد.

وعموما فإن الجرائم المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري تشمل جريمة الدخول عن طريق الغش إلى النظام الآلي، وجريمة البقاء غير المصرح به في النظام المعلوماتي وأخيرا جريمة إتلاف نظام المعالجة الآلية للمعطيات.

غير أن هذا الجهد لم يكن كافيا لتفعيل سياسة مكافحة الجرائم المعلوماتية وهذا بسبب تعارض أحكام قانون العقوبات وقانون الإجراءات الجزائية وخصوصا مسائل الاختصاص النوعي والإقليمي التي وقفت عائقا في وجه تطبيق النصوص العقابية، مما استدعى تدخل المشرع الجزائري بموجب القانون 06-22 المؤرخ في 2006/12/20 المعدل والمتمم لأحكام قانون الإجراءات الجزائية الجزائري، والذي تناول تعديل وتحديث نصوص المواد 45 إلى 47 منه والتي تحدد قواعد الاختصاص النوعي والمحلي ومواعيد إجراء التفتيش بشأن الجرائم المعلوماتية، ومس أيضا التعديل قانون العقوبات بموجب القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص الواردة في هذا القسم من القانون 04-15.

ولقد صدر بتاريخ 2009/08/05 تحت رقم 09-04 القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الذي يعتبر نموذجا قانونيا خاصا بمكافحة الجرائم المعلوماتية على اعتبار أنه قانون يتضمن نصوصا خاصة، وقد تضمن الأحكام العامة الخاصة بالعمل بهذا القانون، كأهدافه والمتمثلة أساسا في وضع قواعد خاصة بالوقاية من الجرائم المعلوماتية إضافة إلى تحديد قائمة المصطلحات المفتاحية، وتحديد مجال تطبيق أحكامه وتضمن بيان مفهوم المراقبة الإلكترونية وحدد القواعد الإجرائية لعمليات التفتيش الإلكترونية، وكيفية حجز الأدلة الإلكترونية وجملة الالتزامات الملقاة على عاتق مقدمي خدمات الإنترنت في مجال مساعدة السلطات بشأن

التحقيقات الجنائية في مادة الجرائم المعلوماتية، وحدد مهام الهيئة الوطنية للوقاية من الجرائم المعلوماتية وحدد قواعد اختصاص القاضي في مجال التعاون الدولي في مسائل البحث والتحقيق في الجرائم المعلوماتية. ومن خلال المادة 13 من القانون 04/09 نص المشرع على إنشاء الهيئة الوطنية المكلفة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، وقد صدر التنظيم بصدور المرسوم الرئاسي رقم 172/19 بتاريخ 2019/07/06 المتضمن تحديد تشكيلة الهيئة الوطنية المكلفة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفية سيرها.

وفي أبريل 2020، وافق البرلمان على تعديلات في قانون العقوبات الجزائري، لا سيما تلك التي تجرم نشر لأخبار المزيفة والكاذبة بغرض الإضرار بالنظام العام والأمن العام.

وواصل المشرع الجزائري جهوده في إطار مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، حيث قام بوضع باب سادس ضمن القواعد الإجرائية العامة ويحتوي استحداث قطب جزائي وطني من اختصاصه مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال التي تدخل ضمنها جرائم الإنترنت بموجب الأمر 21-11 المؤرخ في 25 أوت 2021 المتمم للأمر 66-156 المتعلق بقانون الإجراءات الجزائية تعزيزا وتكريسا لفكرة التخصص القضائي في مكافحة الجرائم الخطيرة .

وفي هذا المبحث سنتناول كل ذلك بالتفصيل من خلال مطلبين يتناول المطلب الأول مكافحة الجريمة علي الإنترنت بكافة أنواعها بموجب القانون الجزائري، وسنتناول في المطلب الثاني القواعد الإجرائية للجريمة عبر الإنترنت في التشريع الجزائري.

المطلب الأول : مكافحة الجريمة عبر الإنترنت في التشريع الجزائري

لابد من الاعتراف أن الإسهام في اقتراح حلول للإشكالات التي يطرحها موضوع الجريمة عبر الإنترنت مهمة تعترضها صعوبة منهجية كبرى مصدرها اتساع وتنوع هذه الجرائم، لذلك سوف نتعرض في هذا المطلب إلى موقف المشرع الجزائري من أهم الجرائم التي تقع عبر الإنترنت.

الفرع الأول : موقف المشرع الجزائري من الجريمة الواقعة على النظام المعلوماتي

من أجل سد الفراغ الذي عرفه التشريع الجزائري في مجال الجرائم المعلوماتية لقد جاء القانون رقم 15/04 الصادر في 10 نوفمبر 2004 ، المتضمن قانون العقوبات بتجريم كل أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات، وقد ورد النص على هذه الجرائم في القسم السابع مكرر من قانون العقوبات، تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وذلك في المواد 394 مكرر إلى 394 مكرر 07 .

أولا: جريمة الدخول عن طريق الغش إلى النظام الآلي:

تضمن قانون العقوبات الجزائري هذه الصورة من الجرائم حيث تنص المادة 394 مكرر " يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة مالية من 50.000دج إلى 100.000دج كل من **يدخل** أو يبقى باستعمال الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، تضاعف العقوبة إذا ترتب عن ذلك تغيير أو حذف لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج"[1] ومن خلال نص المادة 394 مكرر من ق ع ج تقوم جريمة الدخول إلى نظام المعالجة الآلية للمعطيات، على الركن المادي وهو الدخول غير المشروع إلى النظام. والركن المعنوي المتمثل في القصد الجنائي .

1-الركن المادي: يتكون الركن المادي في هذه الجريمة من النشاط الإجرامي بشكل أساسي والمتمثل في فعل الانتهاك الذي يكون له نتيجة إيجابية وليس سلبية، لأنه لا يمكن تحقيق الجريمة بالأنشطة السلبية.

وما يميز هذا النوع من الجرائم أنه ليس ما يسمى بجريمة ذوي الصفة، مثل الاختلاس أو الرشوة، بل يتم ارتكابها من طرف أي شخص مهما كانت صفته، بغض النظر عن إمكانياته، سواء يعمل في مجال الأنظمة ويفهم كيفية عمل النظام أو لا يفهمه. وسواء كان يستطيع أن يستفيد من الدخول أو لا.[2]

---

[1] – أنظر المادة 394 مكرر من قانون ع ج

[2] – نائلة عادل محمد فريد قورة ، جرائم الحاسب الآلي ، الاقتصادية ، المنشورات الحلبي الحقوقية ، ط 1 ، 2005 ، ص 323

وتجدر الإشارة أيضًا إلى أن معنى كلمة "تسجيل الدخول" التي تشير إلى جميع الإجراءات التي تسمح بالوصول إلى نظام المعلومات أو للتحكم في البيانات والمعلومات التي يتكون منها، وعملية الدخول إلى النظام لا يعتبر بحد ذاته سلوكا غير مشروع ، وإنما يتخذ هذا الوصف انطلاقا من كونه قد تم بطريقة غير شرعية، وبمعنى أدق لقيام هذه الجريمة يجب أن يتحقق اتصال فعلي من قبل الجاني بالبرنامج وعلى هذا الأساس يفضل استخدام لفظ الاتصال بالنظام الآلي.

2-الركن المعنوي: لا تقوم هذه الجريمة في التشريع الجزائري، إلا بتوافر القصد الجنائي، ويقصد به اتجاه إرادة الجاني إلى القيام بفعل من الأفعال التي يجرمها القانون، وجريمة الدخول إلى نظام الآلي تعد من الجرائم العمدية، بحيث يتخذ الركن المعنوي فيها صورة القصد الجنائي المتكون من علم وإرادة، وذلك بأن تتجه إرادة الجاني إلى الدخول مع علمه أن ليس له الحق في الدخول إلى النظام، وبالتالي لا يتحقق الركن المعنوي إذا كان دخول الجاني مسموحا به، أو وقع في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول في نطاق هذا الحق كأن يجهل بوجود خطر للدخول، أو كان يعتقد أنه مسموح له بالدخول . وعليه إذا كانت النية الإجرامية موجودة بعنصريها، المعرفة والإرادة، فإنها لا تتأثر بدافع الدخول أو البقاء، بحيث تظل النية قائمة حتى لو كان الدافع هو التطفل أو هزيمة النظام أو إثبات المهارة. ومن خلال نص المادة 394 مكرر من قانون العقوبات الجزائري، يلاحظ أن القصد الجنائي لا يكفي وحده، ويجب توافر قصد جنائي خاص والمتمثل قي الغش. وبهذا نكون بصدد جريمة الدخول غير المشروع للنظام الآلي.

ثانيا: جريمة البقاء غير المصرح به في النظام المعلوماتي:

تناول المشرع الجزائري هذه الصورة من الجرائم في المادة 394 مكرر من قانون العقوبات ج، والتي جاء في نصها ".. أو **يبقى** باستخدام الغش في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات "[1]

وعلى ضوء هذا النص يمكن تعريف البقاء الاحتيالي في نظام المعلوماتية بأنه البقاء في نظام معالجة البيانات الآلي ضد إرادة أولئك الذين لديهم الحق في تشغيل النظام، وفعل البقاء الغير القانوني يتحقق بمجرد دخول شخص ما إلى النظام بموافقة ولكنه يتجاوز الفترة التي يُسمح له بالبقاء فيها، أو يكون ذلك التحول خطأ أو سهوا في نظام آخر ولم ينسحب فورا ولا يقطع وجوده، أو يقوم بطبع نسخة من المعلومات في حين سمح له بالرؤية فقط هنا تقوم جريمة البقاء غير المشروع في نظام المعالجة الآلية للمعطيات. بتوفر جميع أركانها.

1-الركن المادي:

يتم تحقيق ذلك ببساطة عن طريق البقاء في الداخل، حيث يتم قياس البقاء غير القانوني بمقدار الوقت الذي يستخدم فيه المجرم النظام وعليه فإن تكملة تلك الجريمة تكون بإكمال فعل البقاء لفترة من الوقت بخلاف ما يتعلق بالدخول غير القانوني .[2]

2-الركن المعنوي:

تعد جريمة البقاء الغير قانوني في النظام من الجرائم العمدية التي تتطلب تحقيق القصد الجنائي العام بعنصريه العلم والإرادة، حيث يحتاج الجاني إلى معرفة أنه يتنقل في نظام معلومات بطريقة غير قانونية. فضلا عن ذلك وفي الوقت نفسه، يجب أن تتجه إرادة الجاني إلى البقاء داخل النظام وعدم قطع الاتصال به. وتدخل هذه الجريمة ضمن الجرائم الشكلية التي لا ينص التشريع فيها على نتيجة محددة، وتعد كذلك من الجرائم المستمرة التي تتطلب من الجاني مواصلة التدخل.[3]

---

[1] – المادة 394 مكرر من قانون العقوبات ج

[2] –أمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، دار هومه الجزائر ، ط 2 ، 2007 ، ص 110.

[3] –أمال قارة ، المرجع السابق ، ص 124.

ومن خلال نص المادة 394 مكرر الفقرة الثانية يلاحظ أن المشرع الجزائري قد شدد في عقوبة كلا من جريمة الدخول وجريمة البقاء في النظام المعلوماتي، حيث ضاعف من العقوبة إذا ترتب عن الدخول والبقاء حذف أو تغيير لمعطيات المنظومة الآلية، وبالمثل تكون العقوبة مشددة في حالة تعطيل تشغيل النظام. كما تضاعف العقوبة إذا استهدفت الجريمة منظمات أو مؤسسات خاضعة للدفاع الوطني أو للقانون العام. وهذا ما نصت عليه المادة 394 مكرر 3 من قانون العقوبات الجزائري.

ويجتمع معا الدخول والبقاء الغير مشروع عندما لا يكون للمجرم الحق في الوصول إلى النظام ويقوم بتسجيل الدخول ضد إرادة من لهم الحق في السيطرة عليه، مع البقاء لفترة معينة داخل النظام.[1]

ثالثا: جريمة إزالة أو تعديل معطيات في نظام المعالجة آلية بطرق تدليسية:

عالج المشرع الجزائري هذا النمط من الجرائم من خلال نص المادة 394 مكرر 1 من قانون العقوبات والتي تنص على أنه" يعاقب بالحبس من ستة أشهر إلى 3 سنوات وبغرامة مالية من 5000.00 دج إلى 20.000.00 دج كل من أدخل باستخدام الغش معطيات داخل نظام المعالجة الآلية أو عدل أو أزال بطريق الغش المعطيات التي يتضمنها."[2]

اعتبر المشرع الجزائري الإزالة أو التعديل الاحتيالي للبيانات الواردة في النظام عملاً إجرامياً.

ويقصد بإزالة المعطيات سواء جزئيا أو كليا إما محوها أو تخريبها أو إتلافها من أجل منع النظام القيام بمهامه أو تعطيل النظام المعلوماتي، والطرق متعددة مثل نشر الفيروسات فيتعلق الأمر بتعديل البيانات ، فهذا يعني إما إدخال معلومات مزيفة أو تزويرها داخل النظام.

وبالإضافة إلى ذلك نصت المادة 394 مكرر 2 قانون العقوبات الجزائري[3] على الاعتداءات العمدية بنصها " يعاقب بالحبس من شهرين 02 إلى ثلاثة سنوات وبغرامة من

---

[1] – أمال قارة، المرجع نفسه ، ص118

[2] – المادة 394 مكرر 1 من قانون العقوبات من القانون04-15

[3] – المادة 394 مكرر 2 من قانون العقوبات

1000000 إلى 5000000 دج كل من يقوم عمدا أو باستخدام الغش بما يلي : تصميم أو تجميع أو بحث أو توفير أو الاتجار أو نشر في معطيات مخزنة أو معالجة أو مرسلة باستخدام منظومة معلوماتية...." أي أنها قامت بتجريم الأفعال التالية :

* بحث أو تصميم أو جمع أو التجارة أو توفير أو نشر البيانات المخزنة أو المعالجة أو المنقولة باستخدام نظام معلومات قد تُرتكب فيه واحدة من هذه الجرائم المذكورة أعلاه.

* إفشاء أو حيازة أو استخدام أو نشر بيانات تم الحصول عليها من أي من جرائم الغش المعلوماتي لأي غرض من الأغراض[1].

تعد هذه الجرائم من أكثر الجرائم وقوعا في العالم الافتراضي ويرى المشرع الجزائري أن عملية إنشاء برنامج مخصص لارتكاب أعمال تزوير المعلومات أو إنشاء برامج معيبة تقنيًا من الجرائم المعاقب عليها، ولا سيما البرامج المبرمجة لممارسة أعمال الاحتيال أو جمع بيانات ومسحها لغرض الاستخدام أو النشر أو الاتجار وذلك بخلق ثغرات فيه عن طريق الإنترنت، على أساس أن جريمة النشر والإفشاء تشكل خطورة على الحياة الخاصة.

رابعا: قانون الحماية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال رقم09-04.

يلم هذا القانون بين القواعد الإجرائية والقواعد الوقائية التي تكمل قانون الإجراءات الجنائية التي تتيح الكشف المبكر للهجمات المحتملة والتدخل الفوري لتحديد المسؤولين عنه، وقد جرم الأفعال المخالفة للقانون وينطبق هذا بشكل عام على الاتصالات التي تنتهك القانون، وبالتالي ينطبق على جميع التقنيات الجديدة والقديمة، التي تدخل ضمنها شبكة الإنترنت وجميع التقنيات التي قد تظهر في ما بعد.

ويحدد القانون الحالات التي يتاح فيها بالمراقبة الإلكترونية، خاصة في حالة وجود مؤشرات على هجوم محتمل على نظام معلومات أو فعل مصنف كجريمة تخريب أو جريمة إرهابية أو جريمة ضد الأمن القومي. ويحدد الفصل الأول من القانون الغرض منه، فضلا عن تحديده لمفهوم التكنولوجيا.

[1] –مولود ديدان ، قانون العقوبات ، المرجع السابق ، ص 121.

ويتناول الفصل الثاني مبادئ محددة لمراقبة الاتصالات الإلكترونية، أما الفصل الثالث فجاءت فيه المبادئ والقواعد الإجرائية للتحقيق والتفتيش والقبض على الجناة في مجال تكنولوجيا المعلومات والاتصالات.

ويخصص الفصل الرابع لتعريف واجبات المتعاملين في مجال الاتصالات الالكترونية ، أما الفصل الخامس فهو يحدد إنشاء هيئة وطنية لمنع ومكافحة الجرائم المتعلقة بتكنولوجيا الاتصالات. والفصل السادس فهو مخصص للتعاون القضائي الدولي فيما يتعلق بجرائم تكنولوجيا المعلومات والاتصالات.[1]

الفرع الثاني : موقف المشرع الجزائري من الجرائم عبر الإنترنت الماسة بالأشخاص

الفقرة الأولى: الجرائم الماسة بالسمعة والشرف عبر الإنترنت

تعرض المشرع الجزائري للجرائم الماسة بسمعة وشرف الأشخاص في القسم الخامس من الباب الثاني الذي يحمل عنوان الجنايات والجنح ضد الأفراد في المواد 296 –299 قانون عقوبات جزائري. أين تم تعريف القذف في المادة 296 ق ع. وعرف السب في المادة 297 ق ع، ولقد اشترط المشرع الجزائري في هاتين الجريمتين وجوب توافر صفة العلانية والتي تستخلص من الوسائل أو الطرق المستعملة المنصوص عليها في المادة 296 من قانون العقوبات ج وهي نفسها بالنسبة لجريمة السب.[2]

و من خلال أحكام المادة 296 من ق ع ج نستنتج أن المشرع الجزائري فرق بين ثلاث طوائف تقوم بهم العلانية وهما:

- العلانية بطرق القول أو الصياح أو ترديده، والتي تتحقق إذا حصل الجهر والإفصاح بالكلام بطريقة تسمح بسماعها من الغير، أي تكون في مكان عمومي مليء بالأشخاص، وهذا ما يمكن تطبيقه على جريمة السب أو القذف عبر الإنترنت باعتبارها فظاء مليء بالمشاركين ويقدم العديد من الخدمات ويعتمد أساسا على تبادل الصوت والصورة وعليه يتحقق فيه العلانية .

[1] – فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، كلية الحقوق جامعة محمد خيضر – بسكرة ، مجلة الحقوق والحريات، العدد الثاني،،2015، ص18

[2] هروال هبة نبيلة ، جرائم الإنترنت (دراسة مقارنة)، المرجع السابق، ص 94

- العلانية بالكتابة أو المنشورات أو اللافتات أو الإعلانات[1] : مواقع شبكة الإنترنت تعتمد في أغلبها على الكتابة والمنشورات وبذلك يتحقق عنصر العلانية .
- العلانية بوسائل أخرى : نصت المادة 1/144مكرر و144 مكرر 2 والمادة 146ق ع على العلانية بوسائل أخرى. ومن خلال هذه المواد يمكن أن تكون هذه الوسائل أي آلية لبث الصوت أو الصورة أو أي وسيلة إلكترونية أو معلوماتية أو أي وسيلة إعلامية أخرى.[2]

حدد المشرع الجزائري عقوبة لكل من جريمتي السب والقذف وتختلف هذه العقوبة حسب تصنيف الأشخاص الموجهة لهم .

أما بالنسبة لعقوبة القذف الموجهة إلى الأفراد العاديين فهي طبقا لأحكام المادة 298 ق ع "الحبس من شهرين إلى ستة أشهر وبغرامة مالية من 25.000 دج إلى 50.000 دج" أو بإحدى هاتين العقوبتين، ويضح صفح الضحية حدا للمتابعة الجزائية" وطبقا لأحكام المادة 299 عقوبة السب تتمثل في الحبس من شهر إلى ثلاثة أشهر وبغرامة مالية من10.000 دج إلى 25.000 دج أو بإحدى هاتين العقوبتين. ويضح صفح الضحية حدا للمتابعة الجزائية".

أما بالنسبة لعقوبة القذف أو السب الموجه إلى أشخاص ينتمون إلى مجموعات عرقية أو ينتمون إلى دين معين من أجل التحريض على الكراهية بين الأشخاص، تتمثل حسب أحكام المادة 298 فقرة 2 في " الحبس من شهر إلي سنة أو بغرامة مالية من 10000دج إلى 100000دج أو بإحدى هاتين العقوبتين ".[3]

أما بالنسبة للقذف أو السب الموجه لمؤسسة أو هيئة ذات طابع عام فالعقوبة كالأتي:

- جريمة القذف أو السب الموجه لشخص رئيس الجمهورية يعاقب الجاني حسب أحكـــام المادة 144 مكرر" بغرامة مالية من 100.000دج إلى 500.000دج " ويشدد العقاب في حالة العود.

---

[1] – المادة 296 من ق ع ج

[2] – هروال هبة نبيلة ، جرائم الإنترنت (دراسة مقارنة)، المرجع السابق، ص 95

[3] – المادة 298 فقرة 1و2 من قانون العقوبات

- جريمة القذف أو السب الموجه لهيئات أو مؤسسات عمومية، تطبق على الجانـــي أحكام المادة 144 مكرر.
- جريمة القذف والسب الموجهتان ضد رموز الدين وحسب المادة 144 مكرر 2 ق ع " هي الحبس من 3 إلى 5 سنوات وبغرامة من 50000 دج إلى 100000 دج" .[1]

الفقرة الثانية : الجرائم الماسة بالأخلاق والآداب العامة المرتكبة عبر الإنترنت

يندرج ضمن الجرائم الماسة بالأخلاق والآداب العامة الجرائم الجنسية والإباحية عبر الإنترنت وجريمة الاستغلال الجنسي للأطفال

أولا : الجرائم الجنسية والإباحية عبر الإنترنت

لقد جرمت كل القوانين العربية ومعظم القوانين في بلاد العالم الجرائم الجنسية وجريمة التحريض على ممارستها، كما هو الحال بالنسبة للقانون الجزائري ولكنه التزم الصمت حيال هذه الجرائم عند ارتكابها عبر الإنترنت. وهنا يمكننا أن نتساءل هل النصوص التي جرم المشرع الجزائري من خلالها الإخلال بالأخلاق بصورتها التقليدية تكتسب من المرونة ما يسمح بتطبيقها أو لا على الأفعال المخلة بالأخلاق التي استخدمت فيها الإنترنت كوسيلة للقيام بها؟.

لقد جرم المشرع الجزائري الإخلال بالأخلاق بصورتها التقليدية من خلال نص المادة 333 مكرر من قانون العقوبات الجزائري حيث نصت على أنه: " يعاقب بالحبس من شهرين إلى سنتين وبغرامة من 500 إلى 2.000 دج كل من صنع أو حاز أو استورد أو سعى في استيراد من أجل التجارة أو وزع أو أجر أو لصق أو قام معرضا أو عرض أو شرع في العرض للجمهور أو باع أو شرع في البيع أو وزع أو شرع في التوزيع كل مطبوع أو محرر أو رسم أو إعلان أو صور أو لوحات زيتية أو صور فوتوغرافية أو أصل الصورة أو قالبها أو أنتج أي شيء مخل بالحياء"[2].

[1] – المادة 144 مكرر و المادة 144 مكرر فقرة 1و2 من قانون العقوبات.

[2] – المادة 333 مكرر من قانون العقوبات الجزائري

كما نصت المادة 347 على أنه:" يعاقب بالحبس من 6 أشهر إلى سنتين وبغرامة من 1000إلى 20.000 دج كل من قام علنا بإغراء الأفراد من أي من الجنسين بقصد تحريضهم على الفسق وذلك بالإشارة والأقوال أو الكتابة أو بأية وسيلة أخرى" .[1]"

من خلال المواد السابقة الذكر من قانون العقوبات الجزائري، نجد أن المشرع حـــرص على تجريم أي فعل خليع يؤدي إلى إفساد الأخلاق. وعليه فإذا كانت مقاهي الإنترنت من الأماكن العامة التي يرتادها جمهور الناس فإن عرضت مواد إباحية خليعة داخله على شاشات الكمبيوتر الموجودة فيها تتحقق به الجريمة طبقا لنص المادة 333 مكرر السابقة الذكر، وكل من يصنع تلك الأشياء الخليعة ويقوم بتحميلها وعرضها على صفحات الانترنت أو يسمح بعرض تلك الأشياء المخلة بالحياء في محله تقع عليه المسؤولية الجنائية.

ومن الأمور المشددة في الجرائم الجنسية أمرين:

العلانية أثناء ممارسة الفعل والعلانية في التحريض على الممارس، ومثال ذلك ما هو منصوص عليه في قانون ع ج من تجريم لتلك الأفعال من خلال المواد 343، 342، 333مكرر، والمادة347 ق ع. ولأن شبكة الإنترنت شبكة مقصودة من الكثير من الأشخاص ومن كافة الجنسيات على مستوى العالم، الأمر الذي يجعلها تحمل نفس خصائص الأماكن العامة التي توفر صفة العلانية، بمعنى أن كل من يقوم بفعل على شبكة الإنترنت فبإمكان أي من مرتادي الشبكة الإطلاع عليه.

كذلك المواقع الإباحية المنتشرة على شبكة الإنترنت هي مواقع تحرض على الفسق والدعارة لا بالإشارة القول فقط، وإنما أكثر من ذلك، فهي تحرض على ذلك بالصور وأفلام الجنس، وهو الفعل الذي تم النص على المعاقبة عليه في المادة 347 من قانون العقوبات الجزائري.

أما عن المحادثات الجنسية من خلال ما يعرف بغرف المحادثات (chating) فتندرج تحت إتيان الأفعال الإباحية الفاضحة التي تتم علانية والتي تم النص على تجريمها طبقا للمادة 333 من قانون العقوبات الجزائري[2].

[1] – المادة 347 من قانون العقوبات الجزائري

ثانيا: الاستغلال الجنسي للأطفال عبر الإنترنت:

وفقًا لتقرير صادر عن المركز الدولي للأطفال بعنوان: تشريع نموذجي "استغلال الأطفال في المواد الإباحية" وحسب المراجعة العالمية "لعام 2016" ، تشهد البلدان في جميع أنحاء العالم تقدمًا فيما يتعلق بقوانين مكافحة الإباحية واستغلال الأطفال عبر الإنترنت، والتي تم تحديدها ب86 بلد وهو عدد كبير مقارنة بالسنوات الماضية.

والجزائر هي واحدة من الدول التي تتضمن قوانينها حماية ضد المواد الإباحية على الإنترنت واستغلال الأطفال وفقًا لنفس التقرير، مستثنية الأحكام القانونية التي تطلب من مزودي خدمة الإنترنت إبلاغ السلطات الأمنية.[1]

وبتفحص القانون الجنائي الجزائري وقانون حماية القاصرين، نجد أنه ليس لديهم قوانين واضحة تحدد أو تجرم الاستغلال الجنسي للأطفال عبر الإنترنت بما يتوافق مع طبيعة تكنولوجيا المعلومات، وفيما يخص استغلال الطفل في المواد الإباحية نجد نص المادة 333 مكرر1 من قانون العقوبات أضيفت بالقانون رقم 14-01 المؤرخ في 2014/02/04 والتي نصت على معاقبة كل من يقوم بأفعال ذات طبيعة جنسية على قاصر بأي وسيلة كانت .

إن كل هذه القوانين غير كفيلة بمواجهة الاستغلال الجنسي للأطفال، لا سيما في مواجهة الاستخدام المكثف وغير الملائم للإنترنت، الأمر الذي يحتاج سن قوانين تمكن من إحاطة هذه التكنولوجيا وتحديد جميع مظاهر هذا النوع من الإجرام، بسبب الانتشار الكبير للاعتداء الجنسي على الأطفال باستخدام الإنترنت واحتواء مواقعها على أفلام لأطفال يتعرضون للإيذاء الجنسي بأبشع الطرق وأكثرها رعبًا، وقد حظرت معظم دول العالم هذه الأفعال وأخذت هذا النوع من الجرائم على محمل الجد.

والجدير بالذكر أن باقي النصوص التقليدية الخاصة بالجرائم الإباحية غير مكيفة لمواجهة الاستغلال الجنسي للأطفال عبر الإنترنت مثل نص المادة 342 من قانون العقوبات التي نصت على جريمة تحريض الطفل على أعمال الدعارة، وهذا يعني أن يستفز

---

[2] – المادة 347 والمادة 333 من قانون العقوبات

[1] – جريمة الاستغلال الجنسي للأطفال عبر الإنترنت، على الموقع التالي:https//academia-arabia.com

الطفل في أي سلوك يؤثر على نفسيته أو يؤدي به إلى مثل هذا السلوك أو يدعمه أو يساعده على القيام بذلك، ويتمثل هذا السلوك في تقديم جسده للاستجابة لرغبات وشهوات الجاني الجنسية بغض النظر عما إذا كان الطفل ذكرا أو أنثى، ولقد جعل من سن الطفل ظرفا لتشديد العقوبة فإذا كانت العقوبة المقررة لجنحة التحريض على الدعارة من سنتين إلى خمس سنوات وغرامة من 500 دج إلى20.000دج حسب المادة 343 ق ع ج، فإن الجزاء المقرر للأفعال المنصوص عليها في المادة 342 على طفل لم يكتمل 16سنة الحبس من 5 إلى10 سنوات وغرامة مالية تتراوح بين 500 دج إلى 25.000دج[1].

ومع ذلك لا يزال هذا القانون غير متسق مع إغراء الطفل بقصد الاستغلال الجنسي أو ممارسة المواد الإباحية عبر الإنترنت .

أما النص الذي يتماشى مع حماية الطفل من جريمة استغلاله عبر الإنترنت هو نص المادة 140 من القانون 15-12 المتعلق بحماية الطفل، هذا ليس بسبب تجريم الابتزاز وانتهاك خصوصية الطفل على الإنترنت على وجه التحديد، ولكن لأنه يجرم عمومًا نشر صور أو نصوص بأي طريقة تنتهك خصوصية الطفل، وكل من يقوم بمثل هذه الأفعال يواجه عقوبة بالسجن من سنة إلى ثلاث سنوات وغرامة تتراوح بين 150 ألف و 300 ألف دج. ومع ذلك لا تزال هذه الأحكام غير رادعة بشكل كافي وليست بجسامة هذه الجرائم.

من خلال ما سبق يتضح جليا قصور التشريع الجزائري وأحكامه القانونية المحاربة لاستغلال الأطفال والاعتداء الجنسي بشكل عام، وتتجاهل التطور السريع للجوانب التكنولوجية للتواصل البشري، بالإضافة إلى التخلي عن العديد من الأفعال التي يتوجب إدراجها في النصوص التي تتعلق بحماية الطفل والمجتمع.

لهذا على المشرع الجزائري أن يعنى بتعديل هذه النصوص بحيث تشمل على تجريم المساس بالأخلاق والآداب العامة عبر الإنترنت بما يتفق ومبدأ المشروعية الجنائية، أو يقوم بإصدار قانون خاص بهذه الجرائم.

[1] – المادة 342 قانون ع والمادة 343 ق ع ج

الفقرة الثالثة: موقف المشرع الجزائري من جرائم العنف عبر الإنترنت

أولا : جريمة الابتزاز عبر الإنترنت

لم تنل جريمة الابتزاز والتهديد عبر الإنترنت بصفة عامة حضها في قانون العقوبات، ولازالت تخضع للقواعد التقليدية الخاصة بجريمة التهديد وفقا للمواد 284 إلى 287 من قانون العقوبات الجزائري، فقد عاقبت المادة 284 كل" من هدد بارتكاب جرائم القتل أو...أو أي اعتداء أخر على الأشخاص مما يعاقب عليها بالإعدام أو السجن المؤبد بمحرر موقع أو غير موقع أو بصور أو رموز أو شعارات يعاقب بالحبس من سنتين إلى عشر سنوات و بغرامة من 500 إلى 5.000 دج إذا كان التهديد مصحوبا بأمر بإيداع مبلغ النقود في مكان معين أو بتنفيذ أي شرط أخر" [1].

وقد يكون التهديد كتابة أو شفاهة، فالمادة 287 من قانون العقوبات الجزائري تتضمن في فحواها بأنه : يعاقب بالحبس من ثلاثة أشهر إلى سنة، وبغرامة من 500 إلى 1.000 دج، إذا كان بأمر أو كان التهديد بالقتل أو العنف[2].

وموضوع التهديد والابتزاز عبر الإنترنت بالرغم من اعتباره من الجرائم الشائعة في الوقت الحالي إلا أنها لا تزال من الموضوعات الحديثة، والتي لم تنل نص تشريعي خاص بها، وهذا دليل على قصور قواعد القانون الجنائي في مواجهة تهديد حياة الأشخاص عبر الوسائط الإلكتًرونية.

ثانيا : جريمة الاعتداء على الحياة الخاصة عبر الإنترنت في التشريع الجزائري

اهتم الدستور الجزائري بحماية الحياة الخاصة، فنص في المادة 39 على حماية الحق في الحياة الخاصة، وتعتبر هذه المادة الأساس الدستوري لحماية الحق في حرمة الحياة الخاصة فلا يجوز الاعتداء على هذه القاعدة الدستورية الهامة سواء من المعاهدات والاتفاقيات التي تبرمها الجزائر أو القوانين العضوية والعادية أو القوانين التنظيمية واللائحية، كما أنه إلى جانب الحماية الدستورية نجد نوعين من الحماية يتمثلان في : الحماية المدنية والحماية الجزائية من خلال قانون العقوبات والقانون المدني، حيث أقر

[1] – المادة 284 ق ع ج

[2] – المادة 287 ق ع ج

المشرع من خلال نص المادة 47 وما يليها من القانون المدني الجزائري الحماية المدنية للمساس بالحقوق الملازمة لشخصية الأفراد، أي أن لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف الاعتداء مع التعويض عما لحقه من ضرر، ويكون لمن وقع عليه الاعتداء الحق في طلب وقفه دون حاجة لإثبات الضرر.

أما الحماية الجزائية فقد أورد المشرع الجزائي قواعد التجريم للمساس بالحق في الخصوصية لأول مرة سنة 2006 بموجب إتمام قانون العقوبات بعد مضي عشر سنوات على صدور دستور 1996 الذي تضمن الحماية الدستورية للحياة الخاصة من خلال التعديل الذي جاء في القانون رقم 06-23 المتعلق بقانون العقوبات في المواد 303 مكرر إلى المادة 303 مكرر2 ، وتضمن نص المادة الأساسي المتمثل في نص المادة 303 مكرر على " يعاقب بالحبس من 6 أشهر إلى 3 سنوات وبغرامة مالية من 50000 دج إلى300000دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك:

1-بالتقاط أو نقل مكالمات تسجيل أو أحاديث خاصة أو سرية بغير إذن صاحبها أو بغير رضاه.

2-بتسجيل أو التقاط أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو بغير رضاه، وفي هذه المادة يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها بالعقوبات المقررة للجريمة التامة، وصفح الضحية يضع حدا للمتابعة الجزائية.[1]

كما تطرق المشرع الجزائري في العديد من القوانين الخاصة إلى حماية الحق في الخصوصية نذكر منها على سبيل المثال قانون المحاماة والقانون الأساسي للوظيفة العامة والقانون العضوي المتعلق بالإعلام. وأجاز المشرع اختراق الحق في الخصوصية حماية للمصلحة العامة في إطار التحقيق في بعض الجرائم الخطيرة متى اقتضت ضروريات التحري في الجريمة الملتبس بها أو التحقيق الابتدائي، طبقا للأحكام الواردة في قانون الإجراءات الجزائية بموجب المواد 65 مكرر 5 إلى 65 مكرر 10 والمواد من 65 مكرر 10 إلى 65 مكرر 18 .

[1] – المادة 303 مكرر من القانون 23/06 .

ولمواكبة التطورات والجرائم التي تمس خصوصية الأفراد أصدر المشرع الجزائري حديثا القانون رقم 18-07 المؤرخ في 10 يونيو2018 والذي هدف من خلاله إلى تحديد قواعد حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي وذلك في إطار احترام الحياة الخاصة للأفراد. ويقصد بالمعطيات ذات الطابع الشخصي وفقا لأحكام هذا القانون "كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعريف بصفة مباشرة أو غير مباشرة، لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الثقافية أو الاجتماعي. كما تجدر الإشارة إلي أن مخالفة أحكام هذا القانون تعرض المخالف للأحكام الجزائية التالية

-خرق الحياة الخاصة عند معالجة المعطيات: أوجب المشرع أن تتم معالجة المعطيات ذات الطابع الشخصي مهما كان مصدرها أو شكلها في إطار حماية الحياة الخاصة للأفراد وكل خرق لهذا الواجب يعاقب الجاني ب بالحبس من سنتين إلي خمس 5 سنوات، وبغرامة من 200000دج إلي500000دج .

-معالجة المعطيات الشخصية رغم اعتراض الشخص المعني: حسب نص المادة 7 من القانون رقم 18-07 يجب معالجة المعطيات ذات الطابع الشخصي بالموافقة الصريحة للشخص المعني، فإذا تمت معالجة هذه المعطيات رغم اعتراضها يعاقب الجاني بالحبس من سنة إلي ثالث سنوات وبغرامة من 100000دج على 300000دج.

-طبقا للمادة 12 من القانون رقم 18/07 يجب إخضاع كل عملية معالجة معطيات شخصية لتصريح مسبق من السلطة المختصة، وفي حالة القيام بالمعالجة دون الحصول على هذا التصريح يعاقب المسؤول بالحبس من سنتين إلى خمس سنوات وبغرامة من 200000دينار إلى 500000دينار.

- الاستعمال غير الشرعي للمعطيات الشخصية: المعلومات والبيانات الإسمية التي يتم تجميعها وتخزينها ومعالجتها في جهاز الحاسوب يتعين أن يكون لها هدف محدد وواضح ومعين سلفا، ولابد من التزام الجهة القائمة على النظام المعلوماتي بالهدف أو الغاية التي من أجلها قامت بتجميع المعلومات ومعالجتها إلكترونيا، فلا يجوز وصول هذه المعلومات

إلي شخص آخر أو جهة أخرى تجع معلومات لغاية مغايرة لأن هذا من شأنه إلحاق الضرر بالشخص لذا تدخل المشرع الجزائري وعاقبه بالحبس من ستة أشهر إلى سنة وبغرامة من 60000دج غلي 100000دينار، أو بإحدى هاتين العقوبتين فقط، كل من قام بإنجاز أو استعمال معالجة معطيات غير تلك المصرح بها أو المرخص لها.

– جمع المعطيات الشخصية بطريقة غير شرعية: يعاقب من سنة إلى ثالث سنوات وبغرامة من 100000 دينار إلى 300000دينار كل من قام بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة طبقا لنص المادة 59 من هذا القانون، فهذا الفعل فيه انتهاك للحياة الخاصة للأفراد يتمثل في جمع معلومات صحيحة عنهم لكن على نحو غير مشروع وغير قانوني .

ويستمد هذا الجمع صفته غير المشروعة إما للأساليب غير المشروعة المستخدمة للحصول على هذه البيانات أو المعلومات كمراقبة الرسائل المتبادلة واعتراضها عن طريق البريد الإلكتروني أو بتوصيل أسالك خفية إلى الحاسوب الذي تختزن فيه البيانات، أو من حيث طبيعة مضمونها فتمثل صفة عدم المشروعية في أن البيانات غير صالحة للجميع بسبب مضمونها، كأن تتعلق بالمعتقدات الدينية والسياسية والانتماءات الحزبية والأصل العرقي للأفراد، فلابد أن تكون بعيدة عن عمليات التجميع في الحواسيب، لأن مضمون هذه البيانات يدخل في نطاق الحياة الخاصة للأفراد .

–الولوج غير الشرعي للمعطيات الشخصية: يعاقب بالحبس من 6 أشهر إلى سنتين وبغرامة من 60000 دينار إلى 200000 دينار أو بإحدى العقوبتين فقط، كل من عرقل عمل السلطة الوطنية:

* بالاعتراض على إجراء عملية التحقق في عين المكان .

*رفض تزويد أعضائها أو الأعوان الذي وضعوا تحت تصرفها بالمعلومات والوثائق الضرورية لتنفيذ المهمة الموكلة لهم أو إخفاء أو إزالة الوثائق أو المعلومات المذكورة .

*عن طريق إرسال معلومات غير مطابقة لمحتوى التسجيلات وقت تقديم الطلب أو عدم تقديمها بشكل مباشر وواضح .

إفشاء المعطيات الشخصية: يعاقب الشخص الذي يقوم بإفشاء معلومات محمية بموجب المادة 301 من قانون 25 العقوبات الخاصة بإفشاء الأسرار المهمة.

–الاحتفاظ بالمعطيات الشخصية أكثر من المدة القانونية: يعاقب بغرامة من 200000دج إلى 500000 دينار المسؤول عن المعالجة الذي يحتفظ بالمعطيات ذات الطابع الشخصي بعد المدة المنصوص عليها في التشريع الساري المعمول أو تلك الواردة في التصريح أو الترخيص، وهذا وفقا لمقتضيات المادة 65 من هذا القانون.

– نقل المعطيات الشخصية إلى دولة أجنبية: يعاقب من سنة إلى 5 سنوات، وبغرامة من 500000 دينار إلى 1000000دج كل من ينقل معلومات ذات طابع شخص ي نحو دولة أجنبية .

الفرع الثالث : موقف المشرع الجزائري من الجرائم عبر الإنترنت الماسة بالذمة المالية

يدخل ضمن الجرائم الماسة بالذمة المالية عبر الإنترنت جريمة السرقة وجريمة النصب والاحتيال، وجريمة المتاجرة بالمخدرات، إضافة إلى جريمة الاعتداء على الملكية الفكرية، ومن خلال هذا الفرع سنسلط الضوء على القوانين العقابية التي وضعها المشرع الجزائري للتصدي لكل هذه الجرائم.

الفقرة الأولى: جريمة السرقة عبر الإنترنت.

لم يأخذ المشرع الجزائري على عكس التشريعات الغربية موقفا واضحا يجرم جريمة السرقة الواقعة عبر الإنترنت باعتبارها جريمة واقعة على معلومات ومعطيات ذات طبيعة معنوية، بل اكتفى بتطبيق القوانين العقابية التقليدية الخاصة بجريمة السرقة، والتي نص عليها في القسم الأول من الفصل الثالث والذي جاء بعنوان السرقات وابتزاز الأموال من المادة 350 إلى المادة 369 من قانون العقوبات، ومن خلال التعريف الذي جاء في المادة 350 من ق ع ج للسرقة نلاحظ أن كلمة الشيء المملوك للغير جاء غير محدد ولم يوصف بالشيء المادي أو المعنوي وعدم تحديد طبيعة الشيء محل السرقة هو الذي دفع المشرع لإمكانية تجريم سرقة الغاز أو الكهرباء بالرغم من كونها ليست ذات طبيعة مادية، وعليه يمكن اعتبار المعلومات من الأشياء القابلة للتملك والحيازة ولا يمكن أن تنقل إلا بموافقة حائزها عن طريق كلمة السر، وعليه يمكن أن تكون محلا للسرقة بالاستيلاء عليها

من طرف أي شخص تمكن من الحصول عليها بأي وسيلة كانت بالرغم من طبيعتها غير المادية، ولا يمثل هذا خروجا عن مبدأ الشرعية لأن صفة الشيء محل الجريمة لم تحدد، ولأنها أشياء معنوية يمكن وصفها بالأموال[1]، ويمكن أن يطبق نص المادة 350 على كل شخص اختلس معلومات أو بطاقات ائتمان أو أفكار باستعمال الإنترنت. "ويعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 100.000دج إلى 500.000دج".[2]

الفقرة الثانية: جريمة الاحتيال عبر الإنترنت

تعتبر جريمة الاحتيال والنصب عبر الإنترنت من الجرائم الجديدة على الشارع الجزائري، وانتشرت بسبب الاستخدام المتواصل للإنترنت ووسائل التواصل الاجتماعي التي توفرها، وبسبب إمكانية التواصل على الإنترنت مع إمكانية إخفاء الهوية الحقيقة. إذ يقوم الجاني بالاحتيال والإدعاء أنه شخص آخر ذو صفة أخرى وله قدرة مميزة تمكنه من ارتكاب الاحتيال من خلال الصفحات والإعلانات المنتشرة عبرة الإنترنت أو مواقع التجارة الإلكترونية .

ولقدت شهدت الجزائر مثلها مثل الكثير من دول العالم استفحال واسع واحتيالات بالجملة خلال فترة تفشي فيروس كورونا من خلال البيع الإلكتروني.

إن الاحتيال عبر الإنترنت من الجرائم المتعددة التي ترتكز في تنفيذها على الشبكة العنكبوتية، ولقد صمت المشرع الجزائري مثله مثل معظم التشريعات العربية عن مواجهته، وأكتفي بتطبيق النصوص التقليدية عليها[3]، وهذا من خلال المواد 375/372 من ق ع ج في القسم الثاني من الفصل الثالث تحت عنوان النصب وإصدار شيك بدون رصيد، وبالرغم من عدم اعتراف المشرع الجزائري بجريمة النصب والاحتيال عبر الإنترنت، إلا أنه

---

[1] – أمال قارة ، المرجع السابق ، ص 29

[2] – المادة 350 من القانون رقم 06-23 المتضمن قانون العقوبات.

[3] – من التشريعات العربية التي قامت بسن قوانين خاصة بتجريم الاحتيال الإلكتروني نجد التشريع الامراتي، أين نص صراحة في المادة 10 من التشريع الإماراتي الإتحادي رقم 2006/02 على تجريم النصب باستعمال إحدى وسائل تقنية المعلومات أو الشبكة العنكبوتية . كما قام بتجريم الاحتيال الإلكتروني المشرع السعودي من خلال نظام مكافحة جرائم المعلوماتية السعودي من خلال المادة 4 فقرة 1.كذلك قام كلا من المشرع السوداني والأردني بتجريم النصب عبر الإنترنت بنص صريح خاص به.

لا يوجد ما يمنع وقوع البيانات الوهمية المنشورة عبر الشبكة العنكبوتية تحت طائلة نصوص المواد 375/372 ق ع.

تنص المادة 372 قانون العقوبات على أن " كل من توصل إلى استلام أو تلقى أموال أو منقولات أو تصرفات أو سندات أو وعود أو مخالصات أو أوراق مالية أو إبراء من التزامات أو الحصول على أي منها أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع أي شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500 إلى 20.000 دينار".[1]

وفي جميع الحالات يجوز أن يحكم علاوة على هذا بالحرمان من جميع الحقوق أو من بعضها الواردة في المادة 14 وبالمنع من الإقامة لمدة سنة على الأقل وخمس سنوات على الأكثر.

وتنص المادة 373 ق ع :على أنه " تطبق الإعفاءات و قيود مباشرة الدعوى العمومية المنصوص عليها في المادتين 368 و 369 ق ع على جنحة النصب التي نصت عليها أحكام المادة 372 ".

وفي هذا الشأن أدانت محكمة الجنح بالدار البيضاء بالجزائر العاصمة في بداية عام 2022 عدة متهمين في قضية مست الرأي العام وتخص طلبة عبر مواقع التواصل الاجتماعي تعرضوا لجريمة الاحتيال وتبين تورط عدة مؤثرين مشهورين على الإنترنت، وهذه الواقعة أحدثت ضجة كبيرة وجدل كبيرا حيال ممارسة النشاطات التجارية عبر الإنترنت، واستعمال المؤثرين الذين يحضون بمتابعة الآلاف من الأشخاص للترويج لسلعهم وخدماتهم.

ولقد تم تحريك القضية بعد اكتشاف العدد الكبير من الطلاب تعرضهم للاحتيال من قبل شركة وهمية أوهمتهم عبر الإنترنت بإمكانية التسجيل ومزاولة الدراسة خارج الوطن وساعد

[1] – المادة 372 قانون العقوبات

في ذلك الترويج لها من طرف بعض المؤثرين المعروفين في الأوساط الإلكترونية منهم نوميديا لازول وستانلي وغيرهم، وتم متابعتهم بأحكام المادة 372 ق ع .[1]

وحسب تقرير أمني في سنة 2020 قد تم إحصاء أكثر من ثمانية ألاف جريمة الكترونية في الجزائر.[2]

الفقرة الثالثة : جريمــة الاتجار بالمخدرات عبر الإنترنت

تصدي المشرع الجزائري لجريمة المخدرات مثله مثل كافة المشرعين عبر العالم وذلك من خلال الأمر رقم 75-9 المؤرخ في 1975/04/17 والذي يتضمن قمع الاتجار والاستهلاك المحظورين للمواد السامة والمخدرات وبعدها جاء القانون رقم 04-08 المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين بها، حيث نص في الفصلين الأولين على الأحكام العامة والتدابير الوقائية. أما الفصل الثالث فقد نص على الأحكام الجزائية والردعية وهذا من خلال المواد 12إلى 31.

لقد خرج المشرع الجزائري في القانون رقم 04-18 المتعلق بالوقاية من المخدات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين بها عن القواعد العامة المنصوص عليها في المادة 05 من قانون العقوبات التي جعلت العقوبات الأصلية في مادة الجنح عقوبة الحبس من شهرين إلى خمس أعوام، وطبق قاعدة يقرر فيها القانون حدود أخرى إذ جعل بعض الجنح عقوبتها مشددة قد تصل إلى 20 سنة حبس.

وعليه يعاقب على الاستهلاك أو الحيازة للمخدرات أو المؤثرات العقلية من أجل الاستهلاك الشخصي " بالحبس من شهرين إلى سنتين و بغرامة من 5000 دج إلى 50.000 دج أو بإحدى هاتين العقوبتين طبقا لأحكام المادة 12 من قانون المخدرات".

ويعاقب على جنحة وتسليم وعرض المخدرات أو المؤثرات العقلية بهدف الاستعمال الشخصي"بالحبس من سنتين إلى عشر سنوات وبغرامة من 100.000دج إلى 500.000

---

[1] - الجزائر :عام حبس لمؤثرين في قضية احتيال. مقال منشور على الموقع التالي :https//www.alarabya.net

[2] – نوارة باشوش، الإجرام الإلكتروني أرقام مرعبة https://www.echoroukonline.com

دج "، وتُضاعف العقوبة القصوى وتصبح عقوبة من سنتين إلى عشرين سنة في حالة عرض أو تسليم مواد مخدرة أو مؤثرات عقلية إلى قاصر أو معوق أو أي شخص أثناء فترة التعليم أو في مصحة أو مركز الاجتماعي أو مستوصف للعلاج من تعاطي المخدرات، طبقا لأحكام المادة 13 .

و يعاقب على جنحة عرقلة الأعوان المكلفين بمعاينة جرائم المخدرات " بالحبس من سنتين إلى خمس سنوات وبغرامة من 100.000 دج إلى 200.000 " طبقا لأحكام المـادة 14.

كما يعاقب على تسهيل للغير الاستعمال الغير مشروع للمواد المخدرة أو المؤثرات العقلية سواء أكان ذلك بمقابل أو غير مقابل ومهما كانت الوسيلة المستعملة لتحقيق الغرض بالحبس من خمس سنوات إلى خمسة عشر سنة وبغرامة من500.000 إلى 1.000.000 طبقا لأحكام المادة15. وحسب هذه المادة يمكن الوسيلة المستعملة هي الإنترنت لتسهيل الاستعمال الغير مشروع للمخدرات، وعليه يمكن القول بتطبيق هذه المادة على هذه الجريمة عند ارتكابها عبر الإنترنت.

ويعاقب قانون العقوبات أيضا على جنحة " إنتاج المواد المخدرة أو المؤثرات العقلية أو صنعها أو حيازتها أو سمسرتها أو شحنها أو نقلها عن طريق العبور أو عرضها للبيع أو الحصول عليها أو شرائها قصد البيع أو التسليم التوزيع و التخزين أو التحضير أو الاستخراج طبقا لأحكام المادة 17.

ويعاقب أيضا على جنحة التحريض والتشجيع والحث على ارتكاب جنح المخدرات طبقا لأحكام المادة 22. ويعاقب على الشروع في مثل هذه الجرائم بالعقوبات ذاتها المقررة للجريمة التامة.

وتعاقب المادة 17 فقرة 02 على جميع جنايات المخدرات بالسجن المؤبد وهي : جناية القيام بطريقة غير مشروعة بإنتاج أو صناعة أو حيازة أو عرض أو بيع أو عرض للبيع أو حصول وشراء قصد البيع والتخزين واستخراج.... والتي تتم بواسطة جماعة إجرامية منظمة.

وتنص المادة 18 على جناية تسيير أو تنظيم أو تمويل الأنشطة المنصوص عليها في المادة 17 . وتنص المادة 19 على جناية تصدير أو استيراد مخدرات أو مؤثرات عقلية بطريقة غير مشروعة .

أما المادة 20 فتنص على جناية زراعة النباتات المخدرة. أما جناية صناعة أو نقل أو توزيع سلائف أو تجهيزات أو معدات بهدف استعمالها في زراعة المواد المخدرة أو إنتاجها أو صناعتها بطريقة غير مشروعة أو مع علمه أنها ستستعمل لهذا الغرض نصت عليها المادة 21 . كما يعاقب الشريك في كل الجرائم بنفس عقوبة الفاعل الأصلي .

وفي سياق ما تم عرضه نلاحظ أن قانون العقوبات يشوبه نقص وفراغ تشريعي يخص منع استخدام الإنترنت للترويج للمخدرات والاتجار بها، وهذا الفراغ التشريعي سيؤدي حتما إلى زيادة استفحال هذه الجرائم داخل التراب الوطني.

وبالرغم من كل ما سبق يمكننا القول أنه من الممكن تطبيق المواد 15و17 والمادة 20 من القانون رقم 04-18 لقمع جريمة المتاجرة والترويج للمخدرات الواقعة عبر الإنترنت.

أما بالنسبة للمخدرات الرقمية فهي تعاني من فراغ تشريعي عالمي لا يقتصر على الجزائر فقط.

الفقرة الرابعة : جريمة الاعتداء على الملكية الفكرية عبر الإنترنت

يعتبر موضوع الملكية الفكرية من أكثر المواضيع التي اهتم بها رجال القانون كونه يدخل ضمن دائرة حماية الحقوق الشخصية، فهذه الحقوق من المنافع التي تعد في رأي التشريع من الأموال. وقد قام المشرع بمواجهة الجريمة الإلكترونية من خلال قانون الملكية الأدبية والفنية الصادر بموجب الأمر رقم 05/03 المؤرخ في 19جويلية 2003[1] المتعلق بحقوق المؤلف وبحقوقه المجاورة، حيث وسع قائمة المؤلفات المحمية، وذلك بإدماج برامج المعلوماتية ضمن المصنفات الأصلية والتي عبر عنها بمصنفات قواعد البيانات وبرامج المعلوماتية، كما شدد العقوبات على المساس بحقوق المؤلفين خاصة المصنفات الرقمية التي تشملها الحماية.

[1] – الأمر 05/03 المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية، عدد 44 ، صادرة بتاريخ 2003/07/23

وتتمثل الحماية المقررة للملكية الفكرية في التشريع الجزائري أساسا في إجراءات وقائية تحفظية وأخرى تدابير جزائية .

أولا: الإجراءات التحفظية:

وهي تدابير استعجاليه تهدف إلى المحافظة على حقوق صاحبها باجتناب اعتداء وشيك الوقوع، والحفاظ على الأدلة ذات الصلة بما يتعلق بالتعدي على صاحب الحق، وهذه الإجراءات تعتبر إجراءات سريعة وفعالة .

1- محضر الحصر ووقف العرض : لصاحب الحق أن يستصدر أمرا من المحكمة بإيقاع الحجز التحفظي على المنتج الأصلي أو نسخه، ويقوم بإجراء وصف تفصيلي للشيء المقلد الذي تم نشره أو أعيد عرضه خلافا لأحكام القانون، وكذا إجراء وصف للآلات الإلكترونية والأدوات المستخدمة في التقليد.

2- الحجز التحفظي : يعتبر الحجز من الوسائل الهامة التي تكفل الحماية لصاحب الحق، لأن بقاء المصنف في حيازة المعتدي قد يؤدي إلى تلفه، لأن إجراءات الدعوى قد تطول وقد ينتشر الشيء المقلد في الأسواق وعبر الشبكة العنكبوتية. والحجز الذي يلجأ إليه صاحب حق الملكية الفكرية فهو المصنف سواء أكان مؤلفا أو علامة أو رسما. ويتمثل في استصدار أمر بوقف نشر وعرض وتداول الشيء محل الاعتداء ووضعه تحت يد القضاء عن طريق الحجز ولا يقتصر الحجز على الشيء الأصلي، بل يشمل أيضا نسخا منه، وصورا عنه.

ثانيا : الحماية الجزائية

تناول المشرع الجزائري جريمة الاعتداء على الملكية الفكرية والأدبية من خلال الأمر 05/03 المتعلق بحق المؤلف والحقوق المجاورة، وذلك بعد اعتباره لبرامج الحاسوب على أنها من المصنفات المحمية في المادة 4 فقرة 1، إذ يشكل أي اعتداء على الحق المالي أو الأدبي لمؤلف البرنامج فعلا من أفعال التقليد، ونص على هذه الجريمة من خلال الفصل الثاني من نفس الأمر في المادة 151إلى غاية المادة 160.

أما عن الأفعال التي اعتبرها المشرع الجزائري مشكلة لجنحة التقليد فهي كالأتي:

-الأفعال التي تمس بالحق المالي للمؤلف، وتضم كلا من استنساخ مصنف بأي طريقة من الطرق في شكل نسخ مقلدة، وكذا إبلاغ المصنف للجمهور عن طريق الأداء العلني أو السمعي أو البصري أو عن طريق أي منظومة معالجة معلوماتية .

-الأفعال التي تنتهك حقوق الطبع والنشر، بما في ذلك الأفعال التي تضر بسلامة العمل والأداء الفني. إضافة إلى الكشف الغير قانوني عن عمل أو أداء فني.

-الأفعال المشابهة لجنحة التقليد : وتضم استراد النسخ المقلدة وتصديرها سواء بالنقل المادي أو المعنوي باستعمال شبكة الإنترنت. وتضم أيضا بيع نسخ مقلدة أو تأجيرها أو عرضها، إضافة إلى جنحة المشاركة في المساس بحق المؤلف.

***العقوبات المقررة للاعتداء على الملكية الفكرية:** إن العقوبات منها ما هو أصلي يتم الحكم به بمجرد توافر أركان جنحة التقليد وتتمثل في الحبس أو الغرامة أو كليهما، ومنها ما هو تكميلي.

العقوبات الأصلية : بالنسبة للملكية الأدبية والفنية، فلقد حدد الأمر رقم 03 -05 مبلغ الغرامة من 500.000دج إلى 1000.000دج والحبس مدة 6 أشهر إلى ثلاثة سنوات طبقا للمادة 153 من الأمر 03 -05 . وبالنسبة للملكية الصناعية فالأمر 03-06 المتعلق بالعلامات حدد الغرامة بـ 500.000دج إلى 10.000.000 دج والحبس من 6 أشهر إلى سنتين، وبالنسبة للبراءات فالأمر 03 -07 حدد الغرامة 500.000 دج إلى 10.000.000دج والحبس من ستة أشهر إلى سنتين.

كما شدد المشرع العقوبة الأصلية في حالة العود إلى ضعف العقوبة المقدرة في المادة 154 المشار إليها سابقا.

العقوبات التكميلية :

المصادرة وهي تضمن تدابير عينية وقائية تنص على الشيء المقلد لإخراجه من دائرة التعامل ونص عليها المشرع الجزائري في المواد 157 من الأمر 03-05 ، والمادة 2/32 من الأمر 03 -06.

أيضا الإتلاف والغلق ونشر الحكم للسلطة المختصة بأن تأمر بالتصرف في السلع المقلدة وذلك بالتخلص من المواد والمعدات المستعملة في عملية التقليد.

الفرع الرابع : موقف المشرع الجزائري من الجرائم عبر الإنترنت الماسة بأمن الدول

نتناول في هذا الفرع جريمة الإرهاب الإلكتروني والتجسس الإلكتروني وجريمة غسيـــل الأموال عبر الإنترنت باعتبارهم من الجرائم التي تمس بشكل مباشر بسيادة الدولة وأرضيها ومواطنيها وتعرض مؤسستها ومكانتها المالية للخطر.

الفقرة الأولى : الإرهاب الالكتروني

أمام ثورة تكنولوجيا المعلومات وما نتج عنها من تعاظم لمخاطر الإرهاب واتساع نطاقه ومجالاته إلى درجة أن أصبح ظاهرة عالمية تهدد كل المجتمع الدولي، لذلك كان المشرع الجزائري ملزما بمواكبة التطور التشريعي في هذا المجال، وهذا من خلال تجريمه لظاهرة الإرهاب الالكتروني، وكان هذا بمصادقته على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 2010/12/21 بموجب المرسوم الرئاسي رقم 14- 252 المؤرخ في 2014/12/08[1] ، والتي أشارت فيه المادة 15 إلى الجرائم المتعلقة بالإرهاب والمرتكبة عبر تقنية المعلومات. إضافة إلى تتميمه لقانون العقوبات بالقانون رقم 16-02 المؤرخ في 2016/06/19 وذلك بإضافة المادتين 87 مكرر 11 والمادة 87 مكرر 12 .

وقد جاء في المادة 87 مكرر 11 على أنه " يعاقب بالسجن المؤقت من خمس إلى عشر سنوات وبغرامة من 100.000الى 500.000دج كل جزائري أو أجنبي مقيم بالجزائر، بطريقة شرعية، يسافر أو يحاول السفر إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو تدابير أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي التدريب عليها". كما يعاقب بنفس العقوبة كل شخص يكتتز أو يجمع المال بشكل مباشر بأي شكل من الأشكال مع العلم أنه سيتم استخدامه للسفر إلى بلد آخر بغرض ارتكاب الأفعال المذكورة في الفقرة الأولى من نفس المادة. أو يمول أو يرتب عمدا لسفر الأشخاص إلى بلد آخر أو التسهيل للسفر بهدف ارتكاب جرائم إرهابية أو التخطيط لها أو التحضير

[1] – الجريدة الرسمية عدد 57 الصادرة بتاريخ 2014/09/28، المرسوم الرئاسي رقم 14-252 المؤرخ يتاريخ 2014/09/08 المتضمن المصادقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات .

لها أو المشاركة فيها أو التدريب عليها. ولقد عاقبت هذه المادة بنفس العقوبات كل من يستخدم تكنولوجيات الإعلام والاتصال لارتكاب الأفعال المذكورة في هذه المادة.

كما عاقبت المادة 87 مكرر 12 ق ع كل من يستخدم تكنولوجيات الإعلام والاتصال لتجنيد أشخاص لصالح أي جماعة أو جمعية أو كيان أو مجموعة منظمة أو كيان إرهابي بهدف دعم أنشطته أو أعماله ونشر أفكاره وتنظيم شؤونهم بشكل مباشر أو غير مباشر.

في الوقت الذي أصبحت فيه التنظيمات الإرهابية تساير الدول في استعمالها للإنترنت وبصورة جد فعالة من أجل تحقيق أهدافها التدميرية العابرة لحدود، وبالرغم من المخاطر غير المحدودة التي يمكن أن يخلفها الإرهاب الالكتروني، إلا أن الجهود لم تصل إلى المستوي المطلوب، وبحاجة إلى بذل المزيد من الجهود في سبيل التصدي لهذا النوع من الجرائم التي أصبحت شبحا يهدد أمننا في كل وقت.

الفقرة الثانية : التجسس عبر الإنترنت

أدى التطور المذهل والمتسارع والمتلاحق لتكنولوجيا المعلوماتية وشبكات المعلومات إلى ظهور نمط جديد من التجسس، وقد ساهمت شبكات الاتصال المتعددة في عولمة هذه الجريمة وأصبحت ترتكب بوسائل تكنولوجية غاية في الدقة والإتقان. الأمر الذي دفع بالمشرعين في مختلف الدول إلى وضع قواعد قانونية تحمي من الأخطار التي يسببها هذا النوع من الجرائم والسؤال المطروح في هذا الصدد هل المشرع الجزائري جرم التجسس المرتكب عبر الإنترنت؟ في واقع الأمر جرم المشرع الجزائري جريمة التجسس في المادة 64 من قانون العقوبات ويعاقب مرتكبها بعقوبة الإعدام باعتبارها من الجرائم الماسة بأمن الدول، دون الإشارة منه لهذه الجريمة عند وقوعها عبر الإنترنت. ولقد حاول استدراك هذا الفراغ القانوني من خلال تجريمه للأفعال التي ترتكب بواسطة استخدام تكنولوجيا المعلومات أول مرة بالقانون رقم 15/04 المعدل والمتمم لقانون العقوبات ووضعها تحت مصطلح جرائم المساس بمنظمة المعالجة الآلية للمعطيات، وذلك من خلال المواد من 394 مكرر إلى 394 مكرر 7 دون إشارة منه للتجسس الالكتروني، وجاءت هذه الجرائم في ثالث صور كما ذكرناه سابقا. وبالرجوع لهذه الصور من الجرائم المستحدثة التي حددها المشرع الجزائري في القانون رقم 15/04 يمكننا القول بأن عدم

تحديده لكافة الجرائم المستحدثة سوف يؤدي إلى إفلات الكثير من الجرائم من العقاب لأن الجرائم التي يرتكبونها لا تدخل في نطاق أي صورة من الصور المحددة قانونا ومن بينها جريمة التجسس باستعمال الإنترنت.

وبالرجوع لنص المادة 394 مكرر3 نجد أن المشرع شدد العقاب على المجرم إذا كانٌ يستهدف بجرٌمه الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بالعقوبات الأشد، وعليه فإنه إذا ارتكبت جريمة من جرائم المساس بأمن الدولة بما فيها التجسس بواسطة استعمال أنظمة المعالجة الآلية للمعطيات فإنه تطبق عليها عقوبتها، لأن العقوبات التقليدية لهذا النوع من الجرائم أشد من العقوبات المنصوص عليها في المواد 394 مكرر إلى 394 مكرر2[1] .

ومن أجل التصدي أكثر للجرائم الواقعة باستعمال الحاسوب وشبكة الاتصالات، ولأن القانون رقم 15/04 كان مقتصرا على ثلاثة صور من الجرائم الإلكترونية، تم إصدار القانون رقم 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. أين نصت الفقرة أ من المادة 02 على أن" الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، هي جرائم المساس بمنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وكل جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية ".

وعليه فإن كل جريمة محددة في قانون العقوبات أو في أحد القوانين المكملة له إن ارتكبت بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية، فإنه تطبق عليها العقوبة المحددة في القانون، بمعنى أن العقوبة التي حددها المشرع للجرائم في قانون العقوبات تطبق سواء ارتكبت بوسيلة الكترونية أو بطريقة تقليدية[2].

[1] – إلهام بن خليفة، جمال غريسي ، التجسس الالكتروني كجريمة ماسة بأمن الدولة في التشريع الجزائري ، مجلة دفاتر السياسة والقانون المجلد: 11 ، العدد: 01، 2022 ، ص155

[2] – إلهام بن خليفة، جمال غريسي، المرجع نفسه، ص156

فعقوبة الإعدام تطبق على الجاسوس سواء ارتكب جريمة التجسس بطريقة تقليدية كما هي محددة في المادة 64 أو ارتكبها باستعمال شبكة الاتصالات.

الفقرة الثالثة: جريمة غسيل الأموال عبر الإنترنت

يعد غسيل الأموال من أهم المشاكل التي تؤرق معظم دول العالم وذلك للحجم الهائل في الأموال المتأتية عن تلك العمليات والآثار السلبية التي تنشأ عنها مم يجعل مهمة مكافحة غسيل الأموال مهمة صعبة وشاقة خاصة بعد التطور التقني الذي أفرز عن ظهور جرائم جديدة خاصة جريمة غسيل الأموال عبر الإنترنت وانتشار العصابات المنظمة التي تتبع سياسة التخطيط الدقيق في عملياتها. وللتصدي لجريمة غسيل الأموال قامت الجزائر بالمصادقة على كافة الاتفاقيات المتعلقة بمكافحتها، أولها المصادقة بموجب المرسوم رقم 45/95 المؤرخ في 28 يناير 1995على اتفاقية الأمم المتحدة لمكافحة المتاجرة غير المشروعة بالمخدرات والمؤثرات العقلية المنعقدة بفينا، أيضا اتفاقية محاربة الإرهاب لسنة 1995، فضلا عن مصادقتها لاتفاقية الجريمة المنظمة عام 2000 بموجب المرسوم الرئاسي رقم 02-55 المؤرخ في 2002/02/25 إضافة إلى سنه لعدة قوانين من أهمها:

- " القانون رقم 11/02 المؤرخ في 2002/12/24 المتضمن قانون المالية لسنة 2003".
- " القانون رقم 05-01 المؤرخ في 6 فيفيري 2005 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتها".
- "القانون المتعلق بالوقاية من الفساد ومكافحته رقم 06-01 المؤرخ في 20 فيفري 2006".
- " القانون رقم 06-22 المؤرخ في 20ديسمبر 2006 المعدل والمتمم لأمر رقم 66-155 المتضمن لقانون الإجراءات الجزائية" .
- " الأمر رقم 66-156 المؤرخ في 08 يونيو 1966 ،المتضمن قانون العقوبات الجزائري المعدل والمتمم بموجب القانون 04-15 لسنة 2004، المؤرخ في 10-11-2004 الصادر بالجريدة الرسمية رقم71 ، لسنة 2004 " . والذي بموجبه تم تجريم غسيل الأموال من خلال المواد 389 مكرر إلى 389 مكرر 7 ق ع.

– "القانون رقم 06–23 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لأمر رقم 66–156 المتضمن لقانون العقوبات، الصادر بالجريدة الرسمية رقم 84 " .

وطبقا لنص المادة 389 مكرر قانون عقوبات، وهي ذاتها المادة 02 من الأمر 05–01 السالف الذكر، وهي مأخوذة حرفيا من المادة 6 من الاتفاقية الأممية لمكافحة الجريمة المنظمة، نجد أربعة أشكال إذا توافر إحداه قامت جريمة تبييض الأموال. [1]

وقد نص المشرع الجزائري على عقوبات للأشخاص الطبيعية وعقوبات للأشخاص المعنوية.

أما عن الأشخاص الطبيعية فيعاقب كل من قام بتبييض الأموال" بالحبس من خمس إلى عشر سنوات وبغرامة من مليون دج إلى ثلاث ملايين دج"، ويعاقب على المحاولة في ارتكاب جريمة تبييض الأموال بالعقوبات المقررة للجريمة التامة[2].

أما عن الأشخاص المعنوية فيعاقب الشخص المعنوي الذي يرتكب جريمة تبييض الأموال طبقا لنص المادتين 389مكرر 1 و 389 مكرر 2 .

وبموجب القانون رقم 06–22 المؤرخ في 2006/12/20 المعدل والمتمم للأمر رقم 66–155 المتضمن قانون العقوبات، وعملا بأحكام المادة 37 المعدلة عن طريق التنظيم أصبح يجوز تمديد الاختصاص المحلي لوكيل الجمهورية لمتابعة الأشخاص الطبيعية القائمين بجريمة غسيل الأموال إلى دائرة اختصاص محاكم أخرى.

واعتبارا لما سبق تعد جريمة غسيل الأموال في صورتها التقليدية من الجرائم الحديثة العهد، وعليه فإن جريمة غسيل الأموال عبر شبكة الإنترنت كظاهرة إجرامية مستحدثة لا تزال غائبة عن المنظومة القانونية الجزائرية بشكل مستقل، وإنما تندرج ضمن جريمة غسيل الأموال بشكلها التقليدي. وما نلاحظه هو عجز النصوص التقليدية عن مجابهة الصور المستحدثة لهذه الجريمة .

---

[1] – الأمر رقم 66–156 المؤرخ في 08 يونيو 1966 ،المتضمن قانون العقوبات الجزائري المعدل والمتمم بموجب القانون 04–15 لسنة 2004، الصادر بالجريدة الرسمية رقم 71 المؤرخ في 2004 –11–10

[2] – المادة 389 مكرر 1 ،2 ،3 من قانون العقوبات الجزائري

المطلب الثاني: القواعد الإجرائية للجريمة عبر الإنترنت

تتسم الجريمة عبر الإنترنت بطبيعة خاصة هذا لأنها تتخذ من العالم الافتراضي ملجأ لها بحيث لا تكاد تترك أثرا ملموسا في العالم الخارجي عكس الجرائم التقليدية. إضافة إلى أنها جرائم تتسم بالطابع الدولي الذي لا يعترف بالحدود الجغرافية ولا بالحدود الإقليمية للدول، لأن شبكة الإنترنت جعلت معظم الدول في حالة اتصال دائم ومستمر. ونظرا لما تتميز به هذه الجرائم من خصوصيات تجعل من اكتشافها أمرا غاية في الصعوبة، وأمام هذه الإشكاليات والمسائل يتبادر إلى ذهننا تساؤلين أساسين حول معرفة تحديد المحكمة المختصة إقليميا في الجرائم الواقعة عبر الإنترنت، ومعرفة المشاكل التي تواجهها في مراحل الاستدلال والتحقيق فيها .

الفرع الأول: الاختصاص القضائي في الجرائم السيبرانية

هو مباشرة سلطة التحقيق والمتابعة والحكم في الجريمة بناءا للقواعد التي رسمها القانون والحدود التي وضعها المشرع لتتبعها السلطات أثناء ممارسة مهامها.

الفقرة الأولى :القانون الواجب التطبيق

لقد اعتمد كلا من مجلس وزراء العدل للدول العربيـــــة فـــي 2003/10/08 بالقرار رقم 495 ومجلس وزراء الداخلية للدول العربية في سنة21 في 2004 على القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والإنترنت، أين نص على ما يلي " تسري أحكام التشريع الجنائي للدولة على الجريمة المعلوماتية إذا ارتكبت كلها أو جزء منها داخل حدودها وفقا لمبدأ الإقليمية، كما تختص المحاكم فيها بنظر الدعوى المترتبة على تلك الجرائم، وعلى الدول العربية عقد اتفاقات لتبني المعيار الأول في حالة تنازع الاختصاص بين الدول".[1]

ولقد نص قانون العقوبات في مادته 3 على أنه تسري أحكام قانون ع ج داخل إقليم الجزائر، كما يطبق على الجرائم التي ترتكب في الخارج إذا كانت تدخل في اختصاص المحاكم الجزائرية طبقا لأحكام قانون إ ج .

[1] – عبدالفتاح بيومي حجازي، مبادئ الإجراءات الجزائيّة فَي جرائمالكومبيوتر والإنترنت، مرجع سابق، ص 49

وكأغلب التشريعات كرس المشرع الجزائري مبدأ إقليمية النص الجنائي، والذي تنص أحكامه على أن كل جريمة مهما كانت جنسية مرتكبها ارتكبت داخل الإقليم تطبق عليها القانون الوطني للدولة [1]. إلا أن هذا المبدأ يخضع لعدة استثناءات، إذ يمتد تطبيق القانون الجزائري على الجرائم المرتكبة خارج الإقليم الوطني في الحالات التي نصت عليها المادة 582 والمادة 588 من ق إ ج وهي :

– الجرائم المرتكبة من طرف جزائريين، على أن يكون الفعل مجرما في كلا من التشريعين وأن لا يكون صدر حكم نهائي عليه في نفس الجريمة من محكمة أجنبية .

–الجرائم الماسة بالمصالح الأساسية لدولة، إذ يطبق القانون الجزائري بغض النظر عن جنسية مرتكب الجريمة ومكان ارتكابها.[2]

الفقرة الثانية: الاختصاص المحلي

هو سلطة المحاكم في المنازعات والدعاوى بحسب المقر أو الموقع أو المكان وما يعبر عنه بدائرة اختصاص المحكمة.

ولقد عالج المشرع الجزائري الاختصاص المحلي للجهات القضائية، ويتم ذلك بتحديد كل سلطة قضائية منطقتها الجغرافية التي لا يجوز لها الانحراف عنها، والاعتماد على عناصر تعمل على ربط اختصاص السلطات القضائية حسب القضية الجنائية. والمنطقة الجغرافية هي مكان وقوع الجريمة أو مكان القبض علي الجاني أو المكان الذي يوجد به مقر سكنه، لكن إذا كانت الجريمة المعلوماتية فهي جرائم عابرة للإقليم، وغالبا ما يكون الجاني في بلد والمجني عليه في بلد أخر، كما قد يكون الضرر الحاصل في بلد ثالث في الوقت نفسه.

لهذا قام المشرع الجزائري بإجراء بعض التعديلات التي مست قانون الإجراءات الجزائية وخصت الاختصاص المحلي في الجريمة عبر الإنترنت بموجب القانون 22/06 المؤرخ

---

[1] – عبدالله سلّميان، شرح قانون العقوبات الجزائري، القسمالعام" الجريمة" ، الجزء 1 ، ديوان المطبوعات الجامعّية، الجزائر،ص115

[2] – سعيداني نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير في العلوم القانونية ، كلية الحقوق والعلوم السياسية ، جامعة الحاج لخضر باتنة 2012–2013 ، ص98

في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم155/66 الموافق لـ1966/06/08 ، لهذا سنتطرق لتلك القواعد على النحو التالي:

أولا: الاختصاص المحلي للنيابة العامة

وفقا للمادة 37 ق إ ج ج فإن الاختصاص المحلي للنيابة العامة يكون على أساس المكان التي وقعت به الجريمة أو مكان سكن المشتبه فيه أو الذي ساهم في الجريمة، لذلك لا ينبغي أن يمتد اختصاص وكيل الجمهورية خارج المكان الذي ارتكبت فيه الجريمة، أو مكان إقامة أحد الأشخاص المشتبه في تورطهم في الجريمة، أو مكان احتجاز هؤلاء الأشخاص، حتى لو كان في بلد آخر أو لسبب أخر. لكن بما أن الجريمة عبر الإنترنت هي جريمة قد ترتكب في مكان معين وتمتد آثارها إلى مكان أخر، لذلك أجاز المشرع الجزائري بموجب المادة 37 فقرة2 ق إ ج توسيع الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى لكنه ترك كيفية تنفيذه إلى التنظيم الذي سيحدد المحاكم المختصة.[1] ووفقا للمادة40 مكرر1 من ق إ ج ج فإن ضابط الشرطة القضائية ملزما بإخطار وكيل الجمهورية في المحكمة التي وقعت فيها الجريمة مع إرسال نسختين من أعمال التحقيق. إضافة إلى إرسال النسخة الثانية دون تأخير إلى النائب العام بمجلس القضاء الذي تتبعه المحكمة المختصة.[2]

ثانيا :اختصاص قاضي التحقيق ومحاكم الجنح

1: الاختصاص المحلي لقاضي التحقيق

أجاز المشرع الجزائري تمديد اختصاص قاضي التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وبالتالي فإن المشرع أجاز تمديد الاختصاص المحلي لقاضي

---

[1] – تنص المادة 2/37 من قانون الإجراءات الجزائية الجزائري على ما يلي:" يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف"

[2] – المادة 40مكرر من قانون الإجراءات ج

التحقيق في الجرائم الواقعة عبر الإنترنت إلى دائرة اختصاص محاكم أخرى وترك تحديد كيفية تطبيق الإجراءات للتنظيم الذي سيصدر فيما بعد.[1]

2: اختصاص المحاكم المحلي.

طبقا للمادة329 من قانون الإجراءات الجزائية الجزائري يتحدد الاختصاص المحلي لمحاكم الجنح بمكان وقوع الجريمة، أو بمحل إقامة احد الأشخاص المتهمين، غير أن المشرع في التعديل الصادر بموجب القانون 14/04 أضاف فقرة أخرى حيث أجاز في حالة ارتكاب جريمة من الجرائم الماسة بأنظمة المعالجة الآلية توسيع اختصاص محاكم الجنح، ولكنه ترك ذلك للتنظيم الذي سيصدر لاحقا والذي يحدد تلك المحاكم التي يمتد إليها الاختصاص، وقرر في المادة 40 مكرر تطبيق القواعد المتعلقة بالدعوى العمومية والتحقيق والمحاكم أمام الجهات القضائية التي تم توسيع اختصاصها المحلي طبقا للمواد329،40،37 من قانون الإجراءات الجزائية [2]. والحقيقة أن مشكلة الاختصاص القضائي في الجريمة المعلوماتية تعد من المشكلات العويصة التي تعرقل الحصول على الدليل، ذلك أن هذه الجريمة قد ترتكب في مكان معين، وتنتج أثارها في مكان أخر.[3]

الفرع الثاني: الاستدلال والتحقيق.

إن الجريمة المرتكبة عبر الإنترنت تعتبر كأي جريمة أخرى، تبدأ بمرحلة الاستدلال ثم التحقيق.

الفقرة الأولى: التحري والاستدلال في جرائم الإنترنت

إن مرحلة الاستدلال هي من اختصاص ضباط الشرطة القضائية، وما يهمنا في هذه الدراسة هو دور الضبطية القضائية ومجال اختصاصها فيما يتعلق بالجريمة السيبرانية. وسنقسم طرق التحري والاستدلال إلى طريقتين تقليدية وحديثة .

أولا: الطرق التقليدية لـجمع الـدليل : تتمثل هذه الإجراءات في المعاينة والتفتيش والضبط

---

[1] – أمال قارة، المرجع السابق، ص 57

[2] – محمد الأمين البشري، التحديات الأمنية المصاحبة لوسائل الاتصال الجديدة، دراسة وصفية تأصيلية للظاهرة الإجرامية على شبكة الانترنت، الدليل الالكتروني للقانون العربي، ص372

[3] – محمد الأمين البشري ، المرجع نفسه، ص 373

1-**المعـاينة** : يقصد بها الانتقال إلى مسرح الجريمة والمحافظة عليه من أجل البحث وأخذ عينة من الآثار المتروكة من طرف مرتكب الجريمة، وضبط كل ما يلزم لكشف الحقيقة، والمعاينة في الجريمة عبر الإنترنت تختلف عنها في الجريمة التقليدية، وهذا راجع إلى سهولة طمس المعالم والآثار في البيئة الافتراضية.[1]

وينبغي التعامل في مسرح الجريمة عبر الإنترنت على إمكانية توافر مسرحان:

-المسرح التقليدي : يقع خارج البيئة الإلكترونية لأنه يتكون من المكونات المادية للمكان الذي وقعت فيه الجريمة، وهو أقرب إلى مسرح الجريمة التقليدية، ويترك فيها الجاني عدة أثار كالبصمات وبعض متعلقاته الشخصية أو وسائط تخزين رقمية.

-المسرح الافتراضي : يقع داخل البيئة الالكترونية، لأنه يتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الإنترنت وفي ذاكرة الأقراص الصلبة الموجودة بداخله. [2]

ونظرا لاختلاف مسرح الجريمة عن غيره من الجرائم الأخرى فينبغي التعامل الخاص مع هذه الجريمة، وذلك بإتباع عدة قواعد فنية قبل الانتقال لمسرح الجريمة الإلكترونية، والمتمثل في ضرورة وجود معلومات مسبقة عن مكان الجريمة من حيث عدد الأجهزة المطلوب معاينتها، ووجود خريطة تبين الموقع الذي سيتم معاينته وتفاصيل المبنى أو الطابق موضوع البلاغ، وعدد الأجهزة والخزائن والملفات، ويحدد ذلك من خلال مصادر سرية لجهات الأمن، أيضا تحديد الأجهزة المحتمل تورطها في الجريمة المعلوماتية حتى يتم تحديد كيفية التعاون معها فنيا قبل المعاينة، كذلك تأمين الأجهزة والمعدات التي سيتم الاستعانة بها في عملية المعاينة سواء كانت أجهزة أو برامج، إضافة إلى هذا إعداد الفريق المتخصص الذي يتولى المعاينة من الخبراء ورجال الضبط والأمن، وتحديد البيانات والمهام والاختصاصات المطلوبة من كل عضو في فريق المعاينة على حدي، وذلك حتى

---

[1] – عفيفي كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف كالمصنفات الفنية، دار الثقافة للطباعة والنشر، القاهرة، ص 338

[2] – عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن ، دار الجامعة الجديدة ، كلية الحقوق جامعة الإسكندرية ، 2006 ، ص 84

لا تتداخل الاختصاصات، وإعداد خطة المعاينة الموضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على الوجه الأكمل[1].

2-التفتيش

إن التفتيش في المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه في القواعد الإجرائية العامة من حيث الشروط الشكلية والوضعية.

يكون التفتيش بالنسبة للشخص المتهم في مكان إقامته بغرض ضبط أشياء متعلقة بالجريمة في منزله، وهو من اختصاص النيابة العامة كأصل عام والضبطية كاستثناء، ويشمل التفتيش المكونات المادية للحاسب اللي التي قد تكون في مسكن المتهم أو مكان عمله.

ومن خلال المواد 44 الى47 من قانون الإجراءات ج بين المشرع إجراءات التفتيش مثل الحصول على إذن مكتوب، وأن يكون التفتيش نهارا من الساعة الخامسة صباحا إلى الثامنة مساءا. كما يشمل التفتيش في المجال الالكتروني العناصر غير المادية للحاسب الآلي .[2]

يعتبر التفتيش إجراء من إجراءات البحث والتحقيق وغرضه البحث عن الأدلة لإثبات وقوع جريمة ما في مكان معين، حيث أنه ونظرا لخطورته تشترط أغلب التشريعات الحصول على رخصة للتفتيش من الجهة المختصة.

إن الالتزام بقواعد التفتيش في الجرائم المرتكبة عبر الإنترنت يثير إشكالات كبيرة خاصة وأن نظم المعالجة الآلية تتكون من مكونات مادية وأخرى غير مادية ترتبط بغيرها عبر شبكات الاتصال المتطورة والمعقدة، كما أن التفتيش في هذا النوع من الجرائم يحتاج إلى تقنيات ومهارات خاصة ودراية وتحكم في الأجهزة وكيفية إخفاء المعلومات فيها، سواء

---

[1] – عائشة بن قارة مصطفى ، المرجع السابق ، ص 85 ، 86 ، 87

[2] – المادة 47 الفقرة 04 من القانون الإجراءات الجزائرية الجزائري" إذا تعلق الأمر بجريمة ماسة بأنظمة المعالجة الآلية للمعطيات يمكن للقاضي التحقيق أن يقوم بأي عملية تفتيش أو حجر ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني ، أو يأمر ضباط الشرطة القضائية القيام بذلك. "

تعلق الأمر بتفتيش المكونات المادية للحاسوب أو تفتيش الشبكات المعلوماتية المتصلة بالحاسوب عن بعد، إضافة إلى مختلف وسائل الاتصال كالهواتف النقالة وغيرها.[1]

لقد أباح المشرع الجزائري في إطار قانون الإجراءات الجزائية، للسلطات القضائية ولضباط الشرطة القضائية الدخول بغرض التفتيش. وقد أجاز للسلطات المكلفة بالتفتيش اللجوء إلى أي شخص خبير بعمل المنظومة المعلوماتية بهدف مساعدتها وتزويدها بكل المعلومات الضرورية لانحاز المهمة الخاصة بها حسب الفقرة الأخيرة من المادة الخامسة من القانون04/09 .

إضافة إلى هذا أجاز المشرع الجزائري للسلطة المكلفة بالتفتيش في أي منظومة معلوماتية، وحفظ البيانات المخزنة، والكشف عن وقائع الجريمة والجناة الذين قاموا بها.

وبالتالي فإن المشرع الجزائري أعطى للسلطة المختصة بالتحري والتحقيق في الجرائم عبر الإنترنت وسائل تسمح لهم بالتدخل بشكل مقبول لتقديم الأدلة اللازمة لإدانة المتهمين.

3- التوقيف للنظر : وهو إجراء من إجراءات الاستدلال ويمس مباشرة بحرية الفرد المكفولة من طرف القانون وقد أجازها المشرع الجزائري في حالتين :

-أن تكون الجرائم الملتبس بها طبقا للمادة 51 من قانون الإجراءات الجزائية.

-أن يكون التوقيف إذا دعت لذلك مقتضيات التحقيق الابتدائي طبقا للمادة 65 من نفس القانون.

ويشترط في التوقيف للنظر أن يقوم به ضابط الشرطة القضائية ويتم إخطار وكيل الجمهورية فورا مع إبداء الأسباب، مع تحرير محضر سماع للموقوف يتضمن مدة استجوابه، ويجب أن لا تتجاوز مدة التوقيف للنظر 48 ساعة، ويمكن التمديد بإذن من وكيل الجمهورية حتى خمس مرات حسب نوع الجريمة المرتكبة، وفي الجريمة الماسة بالمعالجة الآلية للمعلومات يتم التمديد مرة فقط[2] حسب المادة 51 ق إ ج ج.

---

[1] - أحمد فتحي سرور، المرجع السابق ،ص135

[2] - بدري فيصل ، مكافحة الجريمة المعلوماتية في القانون الداخلي، أطروحة لنيل شهادة الدكتوراه ، جامعة الجزائر" يوسف بن خدة" كلية الحقوق 2017-2018، ص 210

ثانيا: طرق الاستدلال الحديثة

بعد تطور هذه الجرائم، وضع المشرع الجزائري نصوصا جديدة لمكافحة جرائم المعلومات. تضمنت قواعد وإجراءات وجب توفرها للقيام بالتحقيق القضائي والتحري عن الجريمة .

1-مراقبة وتجميع الاتصالات الإلكترونية

تمت حماية البيانات الشخصية من خلال الدستور الجزائري، وهذا في إطار القواعد العامة المختصة بالحماية القانونية للحياة الخاصة للأفراد، وهذا يعني في الأساس حماية بياناتهم الشخصية من الجريمة المعلوماتية، بحيث اعترف المشرع الدستوري الجزائري بها في المادة 77 التي نصت على أن لكل شخص الحق في ممارسة جميع حرياته مع احترام الحقوق التي يحميها الدستور، وأهمها الحق في الاحترام والكرامة والحياة الخاصة.

كما أيدت ذلك المادة 46 من دستور سنة 1996 التي نصت على عدم جواز الاعتداء على الخصوصية الشخصية، وحاول المشرع مواكبة التطور الذي يشهده العالم في مجال حماية البيانات الشخصية وقام بتعديل الدستور، من خلال إضافة فقرتين للمادة أعلاه والتي أتاحت المساس بأي حق من الحقوق إذا كان ذلك من خلال أمر معلل من السلطة القضائية[1].

علما أن جل الدساتير العربية اكتفت بالحماية الدستورية للمراسلات بكافة أنواعها، فقط الدستور الجزائري وحده الذي تطرق لحرمة البيانات الخاصة من المعالجة الإلكترونية[2].

كما جاء القانون 04/09 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في مادته الرابعة، بالحالات التي تسمح بتطبيق مراقبة الاتصالات الإلكترونية، وهي كالأتي:

---

[1] – القانون رقم 16 – 01 المؤرخ في 6 مارس 2016 المتضمن التعديل الدستوري، الجريدة الرسمية العدد 14 ، الصادرة في 07 مارس 2016.

[2]– لوكال مريم، الحماية القانونية للبيانات ذات الطابع الشخصي في العالم الرقمي ، بالملتقى الوطني الموسوم بـ: الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المنعقد بالمركز الجامعي غليزان يومي 7 و8 فبراير 2017، ص 6.

– الحماية من الأعمال التي تتصل بالإرهاب أو التخريب أو الجرائم الموجهة ضد الأمن.
– إذا كانت هناك معلومات حول إمكانية الهجوم على نظام تكنولوجيا المعلومات بطريقة تهدد كافة المؤسسات المهمة في الدولة.
– لاحتياجات التحري والتحقيق، من غير الاعتماد على المراقبة الإلكترونية يكون من الصعب الوصول إلى الجاني.
– إذا تطلب الأمر المساعدة القضائية الدولية.

من خلال نص المادة أعلاه يظهر لنا، أن المشرع الجزائري قد حاول الاستفادة من التطور التكنولوجي والايجابيات التي تميزه، وهذا باستعماله للمراقبة الإلكترونية ووضع المشتبهين تحت مراقبتها، وهي على عكس المراقبة التقليدية فعالة ومربحة للوقت والمال، وعليه فإن وضع الشخص تحت المراقبة الإلكترونية سواء ما تعلق باتصالاته الهاتفية أو نشاطاته عبر الإنترنت، من شأنه انتهاك حرمة البيانات ذات الطابع الشخصي له، ولكنه وللتأكد من قيمة المعلومة كدليل إثبات أو نفي، يستدعي قراءتها، للوصول لأمرين إما أنها معلومة ضرورية لاستكمال التحقيقات، أو أنها معلومات شخصية لا دخل لها بالقضية[1].

* وتضيف المادة 2/4 من القانون 04/09 إلى عدم جواز المراقبة إلا بإذن كتابي من السلطات المختصة.

وفي حالة الجرائم الإرهابية أو التخريبية أو التي تستهدف أمن الدولة، فإن النائب العام بالمجلس القضائي الجزائري لديه سلطة تفويض ضباط الشرطة القضائية لمدة أربعة أشهر قابلة للتجديد على أساس تقرير يتبين فيه نوع الحلول التقنية المستخدمة والأهداف التي توجهها[2].

كما تنص المادة 41 من المرسوم الرئاسي رقم 261/15 المؤرخ في 08 أكتوبر 2015، الذي يحدد هيكل وتنظيم عمل الهيئة الوطنية لمنع ومكافحة الجرائم المتعلقة بتكنولوجيا

[1] – لوكال مريم، المرجع السابق، ص 09

[2] – المادة 65 مكرر 7 من قانون الإجراءات الجزائية.

المعلومات والاتصالات[1]، على أن تعمل في مجال مراقبة الاتصالات الإلكترونية تحت مراقبة قاض مختص.

كما يخضع الموظفون الذين يمكنهم الاطلاع على معلومات سرية إلى أداء اليمين أمام المجلس القضائي قبل تنصيبهم، وهم ملزمون بالسر المهني من خلال المادتين 27 و28 من المرسوم الرئاسي 261/15.

إن وضع مثل هذه الآلية، التي تنتهك حريات الفرد، تحت سيطرة سلطة قضائية مستقلة هو ضمان صحيح، حيث يسعى القاضي إلـى تحقيق التوازن بين الحاجة إلى التحقيق وواجب حماية المشتبه بهم، فليس كل متهم مجرم، وهذا ما يطلق عليه بضمانات الإجراءات القانونية العادلة.

* تعيين حدود تقنية المراقبة الإلكترونية واستخدام المعلومات التي تم الحصول عليها. وتهدف الأساليب التقنية للمراقبة الإلكترونية إلى جمع وتسجيل المعلومات المتعلقة بالحالات المذكورة أعلاه، مثل الأعمال الإرهابية.

وفيما يتعلق بالأساليب الفنية التي يمكن استخدامها فيما يتعلق بالمراقبة الإلكترونية: فتكون باعتراض المراسلات الإلكترونية والتقاط الصور، والتسجيل الصوتي، والبحث والتفتيش في أنظمة المعلومات ومصادرتها حسب المادة 5 و7 من القانون 04/09، إلا أن السؤال الأهم هو ما مصير المعلومات المتحصل عليها؟

أجابت المادة 09 من القانون 04/09 المتعلقة بحدود استعمال المعطيات المتحصل عليها عن طريق الحجز، بأنه لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية، وما تشير إليه هذه المادة هو أن الاستعمال المشروع للبيانات الشخصية المتحصل عليها من المراقبة الإلكترونية يتحدد بضرورات التحقيقات، وهو ما يستدعي تجريم كل استعمال لها خارج هذا الإطار.

[1] – الجريدة الرسمية العدد 53 ، الصادرة في 08 أكتوبر 2015.

* فرض عقوبات على جريمة إفشاء المعلومات الشخصية من خلال المراقبة الإلكترونية. مع ضرورة تمتع الموظفين المسؤولين عن إجراءات المراقبة الإلكترونية بإمكانية الوصول إلى المعلومات ذات الصلة بالجرائم والبيانات الشخصية الأخرى، وكلاهما يخضع للسرية. ولهذا السبب تم تجريم أي فعل تقوم به هذه السلطات لاستخدام وظائف المراقبة لأغراض شخصية، أي حصر المراقبة الإلكترونية في عدم انتهاك حرمة الحياة الشخصية للأفراد لأي سبب كان. أو الكشف عن المستندات نتيجة التفتيش أو المشاهدة من قبل شخص غير مؤهل مهنيًا لرؤيتها، وبدون إذن كتابي من المتهم أو أصحاب الحقوق أو المستلم أو الموقّع لهذه الوثيقة، إلا وفقًا لمتطلبات التحقيق[1] .

2- التسرب:

اعتبر المشرع الجزائري إجراء التسرب بموجب المادة 65 مكرر 11 آلية للبحث والتحقيق في الجريمة العابرة للحدود بأشكالها المختلفة، على غرار التشريعات الأجنبية التي كانت رائدة في هذا المجال. وقد حاولت الجزائر مواكبة الاتفاقيات الدولية الداعية إلى تطوير آليات جديدة تتكيف مع متطلبات الجرائم المستحدثة التي تدخل ضمنها جرائم الإنترنت، بما في ذلك اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام 2000 ، التي صادقت عليها الجزائر.

والتسرب هو تقنية جديدة أدخلها المشرع في تعديل عام 2006 لقانون الإجراءات الجزائية عندما تقتضي الجرائم المدرجة في المادة (65 مكرر 5) التحقيق فيها، ويجوز لوكيل الجمهورية، تحت وصايته وحسب مقتضيات القضية، السماح ببدء عملية التسرب في ظل شروط خاصة، بشرط أن يتلقى الشخص المسؤول عن الإعفاء تفويضًا من وكيل الجمهورية ، تاركًا العملية تحت سيطرة ومراقبة هذا الأخير.

ويتاح للجهة المختصة أن تأذن تحت رقابتها حسب الحالة بمباشرة عملية التسرب ضمن شروط محددة[2] ويشترط حصول الضابط المكلف بالتسرب على الإذن من وكيل الجمهورية

---

[1] – المادة 46 من الأمر رقم 15 – 02 المؤرخ في 23 جويلية 2015 يعدل ويتمم الأمر رقم 66 – 155 المؤرخ في 8 جويلية 1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 40 ، الصادرة في 23 جويلية 2015.

[2] – المادة (65 مكرر 11) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

المختص، ويجب أن تتم العملية تحت أشرافه ومراقبته، والشروع في هذا الإجراء من قبل قاضي التحقيق يكون بإبلاغ وكيل الجمهورية أولا، ولكي لا يقع تحت طائلة البطلان يتوجب إعطاء إذن كتابي لضابط الشرطة القضائية ثم الذي يتولى إجراءات التسرب، مع وجوب تضمنه على كل ما يتعلق بعملية التسرب وبشرط تدوين هويته فيه وهوية ضابط وأعوان الشرطة المأذون لهم بالعملية. [1]

عندما يدفع المسؤول عن عملية التسرب المشتبه فيهم إلى الاعتقاد بأنه مجرم أو شريك يحدث التسرب. [2] وهو قيام الشخص المخول له التحقيق في الجريمة، التسلل إلى جماعة إجرامية ومراقبة الشخص المشتبه فيه، وجعله يعتقد أنه شريكه. فمن أجل تنفيذ القانون يتم السماح للمتسرب باستخدام هوية مزورة للتصرف، وعند الاقتضاء ارتكاب أفعال إجرامية معينة دون تحمل مسؤولية جنائية.[3]، وذلك بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، بإخفاء الهوية الحقيقية[4].

وفي الوقت نفسه، يجوز لموظفي أو مساعدي هيئة التحقيق الجنائي، التي يُسمح لها بالتحكم في التسرب، أداء بعض الإعمال المسموح بها بموجب المادة 65 مكرر 14 من الأمر رقم 155/66" [5].

و يحظر على المتسرب الكشف عن هويته في أي مرحلة من مراحل العملية لأي سبب، حيث أن الكشف عن هويته الحقيقية من شأنه أن يقضي حتمًا على خطة القبض على المشتبه بهم، ويعرض للخطر الشخص الذي تم الكشف عن هويته، وهو ما أكده "المشرع بموجب المادة (65 مكرر 16) .

---

[1] – محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الطبعة الثانية، الجزائر، 2009، ص 115.

[2] – المادة 65 مكرر12 الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

[3] – عيساوي نبيلة، المرجع السابق، ص 02

[4] – عبد الرحمن خلفي، ، محاضرات في قانون الإجراءات الجزائية، دار الهدى عين مليلة، الجزائر، 2010، ص 74-75

[5] – المادة 65 مكرر 14 من الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

ويتم معاقبة الأشخاص الذي قاموا بالكشـــف عن هوية ضباط أو موظفين في الشرطة القضائية، ويـؤدي الكشف عن الهوية إلى أعمال عنف أو إلحاق ضرر بأحـد هؤلاء الأشخاص أو أزواجهم أو أطفالهم أو أصولهم، وقد يتسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص.[1]

3- اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

يسمح القانون الجنائي الجزائري للشرطة القضائية بطريقة سرية اعتراض التسجيلات الصوتية والرسائل وتسجيلات الفيديو للكشف عن الجرائم المعلوماتية وأنشطتها الخاصة، على الرغم من أنها تمس بالحق في الخصوصية[2].

وتستخدم أدوات التصوير في المحلات والأماكن العامة لتصوير ومراقبة المشتبه فيهم، ولتسجيل المحادثات ويتم تسجيل الأصوات، من خلال مراقبة الهواتف، ويمكن تركيب ميكروفونات حساسة يمكنها جمع الأصوات وتسجيلها على أجهزة خاصة.

من المهم التأكيد على أن مثل هذه الإجراءات يمكن أن تعرض الحق في الخصوصية للخطر، خاصة عندما نعلم أن خصوصية المراسلات هي حق دستوري، وبالرغم من ذلك نصت المادة 03 من القانون رقم 04/09 المؤرخ 5 أغسطس 2009 على الوقاية من الجرائم المتصلة بالإعلام والاتصال. و أجازت مراقبة الاتصالات الإلكترونية، وجمع وتسجيل محتوياتها في الوقت المناسب والدخول لنظام المعلومات ومصادرة وتخزين كل ما يهم إجراءات التحقيق إذا اقتضت الضرورة لذلك[3].

فضلا عن هذا فإن جميع المتهمين أبرياء حتى تثبت إدانتهم. لذلك هل يُسمح إدانة المتهم بناءا لرسائل صوتية أو تسجيلات صوتية أو صور فوتوغرافية في الأماكن الخاصة أو العامة. وخاصة أن تلك الأساليب قد تمس حتى بمن حوله من عائلته وأصدقائه.

---

[1] – بدري فيصل، مكافحة الجريمة المعلوماتية ، أطروحة لنيل شهادة الدكتوراه، جامعة الجزائر كلية الحقوق، 2017،2018

[2] – خلفي عبد الرحمن، المرجع السابق، ص 72- 73.

[3] – المادة 03 من القانون رقم 04/09 المؤرخ في 5 أوت 2009

في حين يختلف مفهوم اعتراض المكالمات الهاتفية الذي يكون دون موافقة الشخص المعني ومفهوم وضع خط الهاتف تحت المراقبة، الذي يتم بموافقة أو طلب الشخص المعني بعد موافقة السلطات المختصة.

تعتبر عملية اعتراض المراسلات والتسجيلات الصوتية والتصوير أشكالاً مهمة من إجراءات التحقيق في وقتنا الحالي، التي أجاز بها المشرع لقضاة التحقيق لضبط المسؤولين عن جرائم المعلومات.

إضافة إلى هذا تعد وسيلة فعالة لما يمكن استخلاصه منها كدليل ضد من أجريت عليه تحقيقات جادة وأثبتت مشاركته في ارتكاب هذه الجريمة، بعد ما صعب ذلك بالوسائل العادية للبحث.

الفقرة الثانية : التحقيق

إن مقتضيات تطبيق مبدأ الشرعية تقتضي إرساء مجموعة قواعد إجرائية تخضع لها السلطة القضائية وأعوانها، حتى يستطيع رجال الضبط القضائي ممارسة إجراءات خاصة تتوافق وطبيعة الجرائم المعلوماتية التي لا يمكن بأي حال من الأحوال البحث والتحري فيها بالأساليب التقليدية.[1]

لقد منح القانون 09-04 دورا ايجابيا لمقدمي الخدمات من خلال مساعدة السلطات العمومية في مواجهة الجرائم المعلوماتية وكشف مرتكبيها حيث تنص المادة 3 منه على مراقبة الاتصالات الإلكترونية وجمع محتواها وتسجيله في الوقت المناسب، ووضع تدابير تقنية لتنفيذ إجراءات التفتيش في نظام المعلومات. ولقد جاءت أحكام المادة 4 من القانون بحالات يسمح فيها للسلطات الأمنية بممارسة الرقابة على المراسلات والاتصالات الإلكترونية، منها الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب والجرائم التي تمس بأمن الدولة، أيضا عندما تكون هناك أنباء عن هجوم محتمل على نظام معلومات يهدد الوكالات الحكومية أو الأمن القومي أو النظام العام، ولأجل ما تقتضيه تداعيات

[1] – عز الدين عثمان ، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية – مخبر المؤسسات الدستورية والنظم السياسية ،العدد الرابع ،جانفي 2018، ص49

التحقيق، عندما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية، وفي إطار تلبية طلبات تبادل المساعدة القضائية الدولية، يمكن للسلطات القضائية، وكذلك ضباط الشرطة القضائية لأغراض التحقيق حتى عن بعد، الاتصال والوصول إلى أنظمة الكمبيوتر، وكذلك مراجعة المعلومات المخزنة فيها، مع إمكانية إشراك السلطات الأجنبية المختصة في المساعدة، وتلقي البيانات ذات الصلة في نظام المعلومات الموجود في الخارج، ويسمح القانون للمحققين بتسجيل البيانات المعنية إذا تم إثبات فائدة المعلومات المخزنة في الكشف عن جريمة، لأن الملاحقة عبر الحدود تستوجب قيام هذا الإجراء في إقليم بلد أخر.[1]

ومن المعروف أن هناك جهازًا قضائيًا للشرطة يشرف على التحقيق والملاحقة القضائية للجرائم المختلفة، وهو هيئة تقوم بالتحقيق في الجرائم وجمع المعلومات عنها. غير أن ذلك لا يمنع أن يكون هناك استثناء على ذلك، وهو قيام جهات خاصة بحكم خبرتها في مجالات عديدة وتعاملها المستمر مع التكنولوجيا أو الجرائم المتصلة بالتكنولوجيا، وهي كفيلة لاكتشاف الجرائم الواقعة عبر الحدود، ويكون ذلك عبر التعاون مع رجال الضبطية القضائية من أجل الحصول على أقصى قدر من الفعالية في التحقيق في الجرائم وتحديد مرتكبيها.

ومن أجل إدخال مشغلي الإنترنت والخطوط الأرضية في مكافحة الجريمة المعلوماتية، ينص القانون 04-09 وجوب تقديم المساعدة الفورية للسلطات المعنية المختصة في جمع وتسجيل البيانات المتعلقة بما تحتويه الاتصالات مع الالتزام بتخزين البيانات.

وتتضمن هذه المساعدة البيانات التي تحدد زبائن الخدمة، وكل المعلومات المتعلقة بتاريخ ووقت ومدة الاتصالات، بالإضافة إلى البيانات المتعلقة بالخدمات الأخرى المستخدمة، بما في ذلك معلومات لتحديد المستلم وعناوين مواقع الويب التي تمت زيارتها [2]. كما يوجد أحكام عقابية تمنع أي تهرب من الالتزامات وهو القانون 09-04

[1] – موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، مقال مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 2009، ص02.

[2]– عز الدين عثمان ، المرجع السابق، ص50

الذي يسلّط هذا الأخير على الأشخاص الطبيعيين الذين يعرقلون سير التحريات القضائية "عقوبة السجن من 5 إلى 6 سنوات وغرامة مالية تتراوح ما بين 50.000 دج إلى 500.000 دج" [1].

إن الجريمة عبر الانترنت ترتكب في بيئة علمية لذلك فإن التحقيق فيها يتطلب كفاءات ومؤهلات علمية كتقنية عالية في مجال الرقمية، مما يضع جهات التحقيق في حالة عجز شبه كلي وهذا راجع إلى نقص خبرتهم وكفاءتهم في هذا المجال، هذا ما يحتم على المسؤولين عن التحقيق اللجوء إلى انتداب خبراء في ميدان التكنولوجيا، وهو إجراء يقوم به قاضي التحقيق، وله كل السلطة والحرية في اختيار الخبير طبقا لأحكام المادة 147 ق إج ج ويشترط أن يكون اختياره من بين الخبراء المعتمدين في الجدول طبقا لنص المادة 144 ق إ ج ج.

الفرع الثاني: الإثبات في الجريمة عبر الإنترنت

إن التحقيق والأدلة موضوعان مترابطان، ولم يتخذ المشرع الجزائري أي إجراء يتبنى أفعال الاعتداء على المعلومـــــات إلا من خلال التعديل الذي جاء به قانون العقوبات 04-15، إذ من الصعب إثبات هذه الجرائم الخطيرة، لذا فإن الأدلة الرقمية اعتبــرت أداة قوية ودليل مهم وفعال.

الفقرة الأولى: تعريف الدليل الرقمي :

عرف الدليل الرقمي أو الدليل الالكتروني بأنه " كل البيانات التي يمكن إعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسوب من انجاز مهمة ما". كما عرف على أنه "جميع البيانات الرقمية التي يمكن أن تثبت بأن هناك جريمة قد ارتكبت، أو توجد عالقة بين الجريمة والجاني أو عالقة بين الجريمة والمتضرر منها. والبيانات الرقمية هي مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة، الرسومات، خرائط الصوت أو الصورة " [2].

---

[1]- المادة 11 من القانون رقم 09-04 ،المؤرخ في 05 /09/ 2009 ،المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

[2] – حنان رّيحان مبارك ، الجرائمالمعلوماتية، المرجع السابق، ص 345، 355

وبالرجوع للمشرع الجزائري نجد أنه لم يعرف الدليل الإلكتروني سواء في القانون 09-04 السالف الذكر.

الفقرة الثانية : مميزات الدليل الإلكتروني: يتميز هذا الدليل بـ :

– أنه دليل علمي يتشكل من معطيات الكترونية غير ملموسة يتم استخلاصها من طبيعة تقنية المعلومات.

– إمكانية نسخ الدليل الرقمي بحيث يمكن نسخ نسخة مطابقة الأصل وهذه الميزة لا تتوفر في الأدلة التقليدية.

–الدليل الرقمي متنوع ومتطور ويمكن أن يكون وثيقة معدة بنظام المعالجة الآلية للكلمات بأي نظام، كما يمكن أن يكون صورة ثابتة أو متحركة أو معدة بنظام التسجيل السمعي، أو أن تكون مخزنة في نظام البريد الإلكتروني.

– صعوبة التخلص من الدليل التقني والرقمي : وهي أهم خصائص الدليل الرقمي،حيث يمكن استرجاعها بعد محوها وإصلاحها، وذلك باستخدام أدوات وبرمجيات ذات طبيعة رقمية متطورة.

الفقرة الثالثة: أهمية الدليل الرقمي في مجال الإثبات في الجزائر

إن الدليل الإلكتروني من أبرز الوسائل للكشف على الجريمة المرتكبة عبر الإنترنت.

أولا–حجية الدليل الإلكتروني: يقصد بحجية الدليل الإلكتروني قوته الاستدلالية في إبراز الحقيقة وتتوقف القيمة القانونية التي يتمتع بها الدليل التقني على مسألتين مهمتين هما : مشروعية هذا الدليل، والمصداقية التي يتمتع بها .

1– مشروعية الدليل الرقمي: يتسع ويضيق قبول الدليل الرقمي تبعا للمبادئ التي تقوم عليها أنظمة الإثبات السائدة، وفي هذا الصدد نجد المشرع الجزائري وكغيره من المشرعين أصدر نصوص تحفز القاضي على قبول أو عدم قبول أي دليل بما في ذلك الدليل التقني كما أن حرية الإثبات في المسائل الجزائية من المبادئ المستقرة في نظرية الإثبات، وبذلك أقر المشرع الجزائري بحرية الإثبات في المادة212 من قانون الإجراءات الجزائية.

ومن بين مبررات الأخذ بمبدأ حرية الإثبات ظهور الأدلة العلمية الحديثة التي كشف عنها العلم الحديث في إتيان الجريمة ونسبها إلى المهتم، كبصمة الصوت والبصمة الوراثية.

ويتجلى الدور الايجابي للقاضي الجزائري في الجرائم الإلكترونية في عنصرين هامين هما :

- توفر الدليل من خلال البحث عن الدليل باستعمال السلطات المخولة له قانونا، حيث يستطع أن يأمر القائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراق النظام والولوج إليه، من خلال الإفصاح عن كلمات المرور والشفرات الخاصة بتشغيل البرنامج.
- سلطة الأمر بتفتيش نظم الحاسوب بجميع مكوناته بحثا عن الدليل الرقمي.

2- مصداقية الدليل الرقمي:

زاد ظهور الدليل التقني من دور الإثبات العلمي، والذي كان دور الخبراء فعال فيـــــه وهذا بالنظر إلى الجرائم المرتكبة عبر الإنترنت، والخبرة التقنية مهمة في توليد الأدلة التقنية وتلعب دورًا في السعي وراء المصداقية في مجال معالجة آلية المعلومات.

ثانيا – الضوابط المتعلقة بالدليل الرقمي : تتمثل أهم الضوابط المستمدة من الدليل الرقمي في سلطة القاضي الجزائي في تقديره لهذا الدليل، وهي تستمد من ضرورة الإقناع بالأدلة الرقمية الصحيحة، وضرورة مناقشته لها في الجلسة مع وجود أصل الدليل في أوراق الدعوى المعروضة في المحكمة.

نستنتج من ما سبق أن المشرع الجزائري قام بإدخال قانون إجرائي خاص بالجريمة عبر الإنترنت المتمثل في القانون رقم09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. كما استحدث آليات التحري الخاصة مثل التسرب الإلكتروني، المراقبة الإلكترونية، إلا أن الإشكالات التي تواجه سلطات البحث والتحقيق مازالت متعددة، أهمها القيمة القانونية للأدلة الإلكترونية و قبول القضاة بها.

المبحث الثاني :
مكافحة الجريمة عبر الانترنت على المستوى الدولي

بالنظر لخطورة هذه الجريمة وصعوبة الكشف عنها وغياب الدليل المادي الذي يدين مرتكبها، فإنها أصبحت تطغى على ساحة الإجرام وبشكل كبير لذلك تنوعت الجهود الدولية لمكافحتها، حيث تم اتخاذ العديد من الآليات والإجراءات للحد منها إلا أن هذه الجهود تبقى غير كافية مقارنة بالتقدم التكنولوجي الذي يشهده العالم على مستوى المعلوماتية والاستعمال اللامتناهي للإنترنت. وسنتطرق إلى إبراز هذه الجهود مع عرض صور التعاون الدولي للقضاء على هذا النوع من الجرائم العابر للحدود.

المطلب الأول : الجهود الدولية والإقليمية لمكافحة الجريمة عبر الإنترنت

إن مكافحة الجرائم المتعلقة بالإنترنت لا يتحقق إلا بتكاتف الجهود الدولة فيما بينها وكذلك الجهود الإقليمية.

الفرع الأول: الجهود الدولية

إذا كان التعاون الدولي آلية فعالة لمكافحة الجرائم السيبرانية، فإن هذا التعاون يتطلب تخفيف الاختلافات بين الأنظمة الجنائية الوطنية لأن الاختلافات بين هذه الأنظمة ستدفع مجرمي الإنترنت إلى البحث عن أنظمة أكثر تسامحا. ولذلك تم إبرام العديد من الاتفاقيات الدولية التي تتطلب التعاون الدولي لمكافحة الجرائم السيبرانية، لأن عدم التعاون يزيد من المسافة بين الأنظمة الجزائية، مما يساهم في زيادة هذا النوع من الجرائم.

الفقرة الأولى : جهود الأمم المتحدة لمكافحة الإجرام عبر الإنترنت

إدراكا من الدول بمدى انتشار الجريمة المعلوماتية بوصفها جريمة عابرة للحدود لقد بذلت الأمم المتحدة جهوداً كبيرة في سبيل العمل على مكافحة الإجرام المعلوماتي بصفة عامة، وذلك لما تسببه هذه الجرائم من أضرار بالغة وخسائر فادحة في كل المجالات، ولأن هذا النوع من الجرائم يتطلب لمكافحته استجابة دولية في ضوء الإساءة في استخدام الكمبيوتر والجرائم المتعلقة به.

صدر قانون جرائم الكمبيوتر عن الأمم المتحدة في هافانا عام 1990 في دورتها الثامنة حول منع الجريمة والمعاقبة عليها. وأضاف أنه ولمواجهة الجرائم المستحدثة يتطلب من الدول الأعضاء اتخاذ عدد مهم من الإجراءات[1] تتلخص فيما يلي:

– اتخاذ تدابر الأمن والوقاية مع مراعاة خصوصية الأفراد واحترام حقوق الإنسان.

– إصلاح القوانين الجنائية وكذا الغرض منها، والتي يدخل ضمنها تطبيق القوانين الجنائية القائمة، من التحقيق المناسب والأخذ بالأدلة، والعمل بالتعديلات حسب الاقتضاء.

– توعية الجمهور والقضاة والهيئات المشاركة بهذه الجرائم بهدف محاربتها.

–التعاون مع المنظمات المهتمة بهذا الموضوع، ووضع وتدريس الآداب المتخذة في استخدام الحاسوب في المناهج التعليمية

–حماية مصالح الدولة وحقوق ضحايا جرائم الحاسوب.

لكن تزايد الجريمة المعلوماتية بما فيها جرائم الإنترنت وما تثيره من مشاكل أدى منظمة الأمم المتحدة إلى عقد الاتفاقية الخاصة بمكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية في ديسمبر 2000 ، رقم 55/63 الجلسة العامة، أين أكدت على الحاجة إلى تعزيز التنسيق والتعاون بين الدول في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، بالإضافة إلى ما يمكن أن تقوم به المنظمات الإقليمية الأخرى.[2]

كما عقدت الأمم المتحدة المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية بالبرازيل أيام 12 إلى 19 أفريل 2010 ، حيث ناقشت فيه الدول الأعضاء التعمق في مختلف التطورات الأخرى في استخدام التكنولوجيا من طرف المجرمين والسلطات المختصة في مكافحة الجريمة، حيث تبقى منظمة الأمم المتحدة الإطار الأمثل لمكافحة الإجرام عبر الإنترنت حيث وضعت مجموعة من القواعد لمواجهة هذا النوع من الجرائم أهمها:

* القواعد الموضوعية : تتضمن هذه القواعد النص على قائمة الحد الأدنى للأفعال الواجب تجريمها واعتبارها من قبيل الإجرام عبر الإنترنت[3] وتحديثها دورياً و المتضمنة ما يلي :

---

[1] – عبد الفتاح مراد، المرجع السابق، ص 237

[2] – عبد الفتاح مراد، المرجع السابق، ص 237

[3] – عبد الفتاح مراد، المرجع نفسه ، ص 242

– جريمة الاحتيال أو الغش المرتبط بالكمبيوتر: و يشمل ذلك الإدخال والإتلاف والمحـو لمعطيـــات الكمبيوتر أو اتخاذ أي إجراء يؤثر على المعالجة الآلية للبيانات ويؤدي إلى فقدان الحيازة أو الخسارة أو فقدان ملكية شخص من أجل تزويد الفاعل بمزايا ومنافع اقتصادية لنفسه وللآخرين.

– جريمة التزوير التي تطال برامج الكمبيوتر أو التزوير المعلوماتي : يتضمن ذلك إدخال أو حذف أو تغيير البيانات أو البرامج أو أي إجراء يؤثر على المسار الطبيعي للاتصال الذي يتم تنفيذه بمساعدة الكمبيوتر.

– جريمة تخريب الكمبيوتر وإلحاق الضرر به: تشمل الوصول أو إتلاف أو التلاعب أو أي عمل آخر يهدف إلى إتلاف عمل على جهاز كمبيوتر أو أي نظام على الشبكة.

– جريمة الوصول غير المصرح به: هي الوصول التعسفي إلى نظام أو مجموعة أنظمة بانتهاك الإجراءات الأمنية.

– جريمة الاعتراض الغير مشروع: تشير إلى استخدام تقنية الاتصالات للتصنت على أنظمة الكمبيوتر أو شبكات الاتصال.

* القواعد الإجرائية : تتضمن بعض الأسس الواجب مراعاتها وهي كالأتي :

– تحديد إلزامي للأطراف التي تقوم بالرصد والرقابة في بيئة تكنولوجيا المعلومات، ولا سيما مراقبة الأمور ذات الصلة والتحكم في الكمبيوتر.

– يجب أن يكون هناك تعاون كاف وفعال بين الطرفين من أجل الحصول على المعلومات التي يمكن استخدامها لأغراض قانونية لردع هذه الجرائم.

–يسمح هذا للهيئات الحكومية باعتراض الاتصالات في بيئة المعلومات باستخدام الأدلة المتاحة.

– إجراء بعض التغييرات التشريعية، إذا لزم الأمر، وفقًا لطبيعة الجريمة الإلكترونية في التشريعات الوطنية والمعايير القائمة في مجال الأدلة الإلكترونية فيما يتعلق بمصداقية الأدلة والمشاكل التي يمكن أن تسببها عند استخدامها.

– يجب النظر في جميع القضايا المتعلقة ببيئة تكنولوجيا المعلومات، بما في ذلك التجسس، وانتهاك الخصوصية، وخطر الخسارة الاقتصادية، وتكلفة استعادة قاعدة البيانات إلى حالتها السابقة. قبل التحقيق أو التفتيش.[1]

ومن جهة ثانية، أصدرت منظمة الأمم المتحدة عددا كبيرا من القرارات مست العديد من المجالات التي لها صلة وطيدة بأمن الفضاء الإلكتروني وعلى سبيل المثال نذكر:

– القرار الصادر في 16/2/2007 الخاص بمكافحة الاستغلال الجنسي للأطفال قرار المجلس الاقتصادي والاجتماعي 07/20 بتاريخ 26 يوليو 2007 بعنوان التعاون الدولي من أجل منع وتحري ومقاضاة ومعاقبة جرائم الاحتيال الاقتصادي والجرائم المتصلة بالهوية.

– قرار المجلس الاقتصادي والاجتماعي 2004/26 بتاريخ 21 /07/ 2004 بعنوان التعاون الدولي لمنع التحقيق والمقاضاة والمعاقبة على الاحتيال، وإساءة استعمال الهوية وتزييفها والجرائم ذات الصلة.

– الفقرة 18 من إعلان فيينا بشأن الجريمة والعدالة : « مواجهة تحديات القرن الحادي والعشرين، التي أقرتها الجمعية العامة في القرار 55/59 المؤرخ 4 ديسمبر 2000 والفقرة 36المرفقة بقرار الجمعية العامة 56/261 المؤرخ 31 كانون الثاني/يناير 2002 .

–الفقرتان 15 و 16 من إعلان بانكوك بشأن أوجه التآزر والتعاون :التحالفات الإستراتيجية في مجال منع الجريمة وتحقيق العدالة الجنائية، الذي أقرّه قرار الجمعية العامة 60/177 بتاريخ 16 ديسمبر 2005.

–توصيات مؤتمر ورشة العمل على التدابير الرامية إلى مكافحة الجريمة المتصلة بأجهزة الكمبيوتر، الذي عقد في بانكوك في 22 أبريل 2005 كجزء من مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية .الفقرة 2 من قرار الجمعية العامة 60/177 التي دعت الحكومات لتنفيذ جميع التوصيات التي اعتمدها المؤتمر الحادي عشر.

–قرار لجنة مكافحة المخدرات 43/8 في 15 مارس 2000 عبر الإنترنت.

[1] – عبد الله عبد الكريم عبد الله ، المرجع السابق ، ص 114

– قرار المجلس الاقتصادي والاجتماعي 2004/42 بشأن بيع المخدرات المشروعة الخاضعة للمراقبة الدولية إلى الأفراد عن طريق الإنترنت.

– مختلف توصيات الهيئات الفرعية التابعة للجنة مكافحة المخدرات واللجنة الفرعية المعنية بالاتجار غير المشروع بالمخدرات والمسائل المتعلقة بالمشرقين الأدنى والأوسط.

– التوجيهات والتوصيات المقدمة من طرف الهيئة الدولية لمراقبة المخدرات، إذ قامت سنة 2005 بنشر توجيهـــات للحد مـــن بيع المواد غير المشروعة خاصـــة ما يتعلق بالمستحضرات الصيدلانية عبر الإنترنت[1].

في قراراتها المختلفة التي تشبه في كثير من الأحيان قرارات الاتحاد الدولي للاتصالات، تحث الجمعية العامة الدول الأعضاء على مراعاة عمل لجنة منع الجريمة عند تطوير القوانين الوطنيـــة والسياسات العامة لمكافحة إساءة استخدام تكنولوجيا المعلومات. ولجنة العدالة الجنائية وغيرها من المنظمات الدولية والإقليمية.

الفقرة الثانية : .مجموعة الدول الثماني G8 :

اعتمد وزراء العـــدل والشؤون الداخلية في دول مجموعة الثماني، في اجتماعات مختلفة، سياسة لمكافحة الأشكال المختلفة للجرائم الإلكترونية على أساس المبادئ التالية:

– عدم توفير منافذ آمنة لمهاجمي تكنولوجيا المعلومات، والتعاون مع جميع البلدان المتضررة من الجريمة الإلكترونية وردعها في أي مكان وقعت به الجريمة.

– تدريب الموظّفين المكلفين بتنفيذ القوانين، وتجهيزهم بالمعدات الضرورية للتعامل مع الجرائم ذات التقنية العالية.

إضافة إلـــى ما سبـــق، تـــم حث دول مجموعـــة الثمانـــي على مواصلة عملها حتى يتم إيجاد حلول دولية ناجعة، بإبرام اتفاقيات دولية لمكافحة جرائم التكنولوجيا الفائقة والبناء على عمل المنظمات الدولية المختلفة والدراسات العديدة التـــي أعدتهـــا مجموعة الثمانية بما في ذلك: المبادئ وخطة العمل بشأن التقنيـــات المتقدمة والجرائم الإلكترونية عام 1997 وقواعد الوصول خارج الحدود الإقليمية إلى المعلومات المخزنة على جهاز

[1]– عبد الله عبد الكريم عبد الله ، المرجع السابق ، ص116

كمبيوتـــــر، وتوصيات 1999 بشأن مراقبـة شبكات الاتصـالات خارج التراب الوطني في التحقيقات الإرهابية 2002، إضافة إلى مبادئ الوصول إلى البيانات الرئيسية لحماية الأمن العــام، وإعلان مجموعة الثمانيـــة الخاص بإقـرار أنظمــة أمــن المعلومات.

وحين انعقاد قمة مجموعة الدول الثمانية التي ضمت وزراء العدل والداخلية في واشنطن 2004/11/10 تم إصدار بيان جاء فيه ما يلي"مواصلة تعزيز القوانين المحلية لبناء القدرات العالمية لمكافحة الاستخدامات الإرهابية والإجرامية للإنترنت، وعلى الدول أن تواصل في تحسين القوانين التي تجرم إساءة استخدام الشبكات الحاسوبية والتي تسمح بسرعة التعاون في التحقيقات المتصلة بالإنترنت، ومع دخول اتفاقية مجلس أوربا للجريمة الالكترونية حيز التنفيذ في 2004/7/1، وكان البيان يحث الدول الأعضاء في الاتفاقية أن يتخذوا خطوات لتشجيع اعتماد المعايير القانونية التي تتضمنها على قاعدة واسعة.[1]

لقد صدر بيان عن اجتماع مجموعة دول الثمانية عام 2005 وتم من خلاله النص على وجوب استجابة الجهات المختصة للتهديدات والمخاطر التي تشكلها الجريمة عبر الإنترنت.[2]

وفي اجتماع بموسكو عام 2006 لوزراء العدل والداخلية لدول مجموعة الثمانية G 8، نوقشت الجريمة السيبرانية وقضايا الفضاء الإلكتروني " Cyberspace" وصدر بيان موسكو الذي ينص على "...أنه من الضروري اتخاذ مجموعة من التدابير لمنع الأعمال الإجرامية المحتملة، بما في ذلك مجال الاتصالات السلكية واللاسلكية والعمل ضد بيع البيانات الخاصة والمعلومات المزيفة وتطبيقات الفيروسات وبرامج الكمبيوتر الضارة الأخرى، وسيوجه خبراءنا لتعميم مناهج موحدة لمكافحة الجريمة الإلكترونية، وسوف نحتاج للقواعد القانونية الدولية لهذا العمل، وسوف نطبق كل ذلك لمنع الإرهابيين من استخدام مواقع الكمبيوتر والإنترنت لتوظيف الإرهابيين الجدد، وتوظيف الجهات الفاعلة غير القانونية الأخرى"[3].

---

[1] – مركز معلومات G8–على الموقع الالكتروني html.G8/net.CybercimeLaw.www://html

[2] – مركز معلومات G8– الموقع السابق نفسه .

[3] – الموقع الإلكتروني : Center Information 8–G

وسنة 2006 أصدرت قمة مجموع الدول الثمانية في سانت بترسبغ بشأن مكافحة الجرائم الإرهابية نص وتضمن ما يلي: نؤكد من جديد التزامنا بالتعاون لمكافحة التهديد الإرهاب والتصدي بفاعليه لحملات إساءة استخدام الفضاء الإلكتروني لأغراض إرهابية بما في ذلك التحريض على ارتكاب أعمال إرهابية، وعلى التواصل مع الإرهابيين وصنع الخطط الإرهابية وتجنيد وتهريب الإرهابيين.[1]

وفي اجتماع انعقد في 23-25 ماي بميونيخ ألمانيا عام 2007 جمع كل وزراء العدل والشؤون الداخلية لدول مجموعة الثمانية في ميونخ وتم الإجماع فيه على: العمل من خلال الأطر القانونية الوطنية بشأن استخدام الإنترنت لأغراض إرهابية[2]. وأتت قمة مجمع الثمانية عام 2009 المنعقدة في ايطاليا في نفس الوقت والتقى وزراء العدل والداخلية في روما 28-30 مايو 2009 وتم إصدار بيان تضمن جرائم الإنترنت والأمن السيبراني وإشارة تقرير صدر عن مجموعة روما ليون قدم لمفوضية الأمم المتحدة مانع الإجرامية والعدالة الجنائية، وأشار البيان إلى أن التقدم التكنولوجي أسفر عن" إساءة استعمال الشبكات الاجتماعية وخدمات التشفير وخدمات النطاقات، وأن الهجمات الإجرامية الجديدة المتطورة الأخرى على أنظمة المعلومات تشكل تحديات إضافية تواجه إنفاذ القانون".

وفي قمة الدول الثمانية التي انعقدت في دوفيل بفرنسا 2011 في 26 ماي 2011 تضمن الجزء الثاني من الاجتماع، دراسة الإعلان بقضايا الإنترنت وأكد على أن شبكة الإعلان أصبحت ضرورية في كافة أنحاء العالم لتجمعاتنا واقتصادياتها وهي مصدر فريد للمعلومات والتعليم للمواطنين ولتعزيز الحرية والديمقراطية وحقوق الإنسان، كما أن شبكة الإنترنت أصبحت أداة أساسية لتسيير التجارة ولتطوير العلاقات مع المستهلك، كما

---

[1] – الموقع الإلكتروني السابق نفسه.

[2] – أنظر الموقع السابق لمفوضية الأمم المتحدة لمنع إجرامية والعدالة الجنائية

: Criminel and Prevention Crime on Commission UN Justice

أنها بالنسبة للحكومات أداة للإدارة أكثر كفاءة وتعد الشبكة محركا رئيسيا للاقتصاد العالمي والنمو والابتكار والانفتاح والشفافية[1].

إن دول مجموعـــة الثمانية مقتنعة بأن الحمايـــــة الفعالة ضد جرائم التكنولوجيا العالية تتطلب الاتصال الداخلي والدولـــي والتنسيق والتعاون بين جميع المعنيين من القطاع الخاص والمؤسسات العلمية والدولــة، ولذلك تعهدت دول مجموعة الثمانية بتدريب جميع موظفي إنفـاذ القانـون وتزويدهـم بالمعدات اللازمة لمكافحة الجرائم الواقعة عبر الإنترنت. والتزمت بمساعدة جميع الدول الأعضاء في إنشاء مراكز اتصال على مدار الساعة طوال أيام الأسبوع.

إن وجود جرائم تستند إلى التكنولوجيا المتطورة يشكل تحديات كبيرة على القضاء، ومعظم الوقت يكون من الصعب على المحققين المدربين تدريباً عالياً العمل بسرعة كبيرة لحماية البيانـــات الإلكترونية وتحديد المتهمين بانتهاك القانون. وعليه فإن الشبكة التي تقترحها دول الثمانية مهمة لأنها ستسمح لهم بالاستجابة بسرعة فائقة لطلبات السلطات الرسمية أو مستخدمي الإنترنت.

ونلخص توصيات مجموع الثمانية المتعلقة بالجرائم المعلوماتية في ما يلي:

– ضرورة تجريم كل الانتهاكات التي تمس بحقوق الغير عبر الإنترنت مع وجوب فرض عقوبات جزائية مناسبة، إضافة إلى معالجة المشاكل المتعلقة بالتحقيقات القضائية بالتدريب الفعال لمنع الجريمة، وإقامة تعاون دولي في ما يتعلّق بمكافحة هذه الانتهاكات.

يجب على كافة الدول اتخاذ تدابير رادعة لمنع جرائم التكنولوجيا المتقدمة ، ومنها:

- العمل مع الصناعة لضمـــان أمن شبكـات الكمبيوتر وأنظمـــــة الاتصالات وإيجاد الآليات المناسبة للهجمات على مواقع الويب.
- اعتماد وتنفيذ قوانين وتدابير أخرى لضمان الحماية الكافية لحقوق الملكية الفكرية من التقليد والقرصنة.

[1] –G8 information Centre – Deauville Déclarations

• تحديد المشاكـــــل المحتملة والتعامل معها في المستقبل والتي قد تنشأ من التطورات في تكنولوجيا المعلومات.

• توعية الجمهور بجرائم التكنولوجيا العالية والجرائم المتعلقة بالإنترنت.

• ضرورة عمـــل الدول باستمرار علـــى اكتســاب التقنيات المناسبة وتطوير المعارف والمهارات بشكـــل مستمــر في مجــال التحقيق، من أجل القبض على المجرمين الذين يستخدمون تكنولوجيا المعلومات لارتكــاب جرائمهم، وينبغـــــي على الدول أن تشجع المزيد من التحقيقات لزيادة فعالية تقنيات تطبيق القانون.

• ضرورة تحسين الاتصال بين مسؤولي تطبيق القانون في مختلف بلدان العال ، بما فـــي ذلك تبادل الخبرات في التعامل مع هذا النوع من المشاكل.

• يجب على الدولة أن تحقق توازنًا جيدًا بين حماية الحق في الخصوصية، أمام الخطر الذي تشكله التقنيات الناشئة، وتعزيز قدرة إنفاذ القانون لحماية القيم الاجتماعية والأمن العام.

• ينبغي للدول أن تشجع على تطوير القوانين وتنفيذ التدابير اللازمة لحماية الأطفال بشكل مناسب من جميع مظاهر الاستغلال الجنسي عبر الإنترنت.

• يجب أن تعمل البلدان معًا لتطوير التقنيات بشكل مستمر للمساعدة في إنفاذ القانون ومحاربة كل أشكال الجرائم الجنسية عبر الإنترنت والتي تستهدف الأطفال.

وفي النهاية ينبغي للبلدان أن تشجع تطوير الاستراتيجيات المناسبة للتوعية العامة في هذا الصدد، والتعاون في التقييم المستمر لبرامج المكافحة. والأساليب القانونية المتبعة.[1]

الفقرة الثالثة: جهود المنظمات الدوليـة في جمال مكافحة الإجرام السيبراني

لقد تم اتخاذ العديد من المبادرات من قبل العديد من المنظمات كالإتحاد الأوروبي الذي أنشأ أجهزة تساعد على محاربة الجرائم السيبرانية، من بينها جهاز اليوروبول والمركز الأوروبي لمكافحة الجريمة المعلوماتية والذي أفتتح في جانفي2013 ، مؤسسة الإنترنت للأسماء والأرقام المخصصة، والمنظمة الدولية لتوحيد المقاييس واللجنة الكهروتقنية الدولية،

[1] - O'Connell, Cyber-Crime hits $ 100 Billion in 2007, ITU News related to ITU Corporate Strategy, 17.10.2007, available at: http://www.ibls.com

وفرق بين عمل هندسة الإنترنت ومنتدى الاستجابة للأحداث ومجموعات الأمن بآسيا والمحيط الهادي، ومنظمة الدول الأمريكية وجامعة الدول العربية ودول جنوب شرق آسيا، ومنظمة التعاون الاقتصادي إضافة إلى الاتحاد الإفريقي. وأهم هذه المنظمات منظمة التعاون الاقتصادي والتنمية والتي تهدف إلى تحقيق أعلى مستويات النمو الاقتصادي وتناغم التطور الاقتصادي مع التنمية الاجتماعية، وبدأت هذه المنظمة بالاهتمام بالجريمة السيبرانية منذ عام 1978، حيث وضعت مجموعة من الأدلة وقواعد إرشادية تتصل بتقنية المعلومات، ويعد الدليل المتعلق بحماية الخصوصية وقواعد نقل البيانات من أول الأدلة التي تم تبنيها من قبل مجلس المنظمة في عام 1980 مع التوصية للأعضاء بالالتزام بها، وأصدرت بعدها تقريرا بعنوان الجرائم المرتبطة بالحاسوب وتحليل السياسة القانونية الجنائية، حيث استعرض التقرير السياسة الجنائية القائمة والمقترحات الخاصة في عدد من الدول الأعضاء، وتضمن التقرير الحد الأدنى من أفعال سوء استخدام الحاسوب والتي على الدول تجريمها وتشمل هذه الأفعال[1]:

-الاستخدام أو الدخول إلى نظام ومصادر الحاسب على نحو غير مصرح به.

-الإفشاء غير مصرح به للمعلومات المعالجة آلياً والنسخ والإتلاف أو التخريب، ما يحتويه من برامج وبيانات غير مشروعة بغرض التوصل لمصادر الحاسب وتعطيل أو إتلاف برامجه أو البيانات المخزنة فيه.

وفي عام 1992 وضعت المنظمة توصيات وإرشادات خاصة بأنظمة المعلومات وأوصت بضرورة أن تعطي التشريعات الجنائية للدول الأعضاء مبادئ عامة[2] تتمثل في:

- حدود التجميع: فرض قيود على تجميع البيانات .

-نوعية البيانات: حيث تنص على أن تتعلق البيانات بالغاية والغرض الذي سوف تستخدم من أجله .

---

[1] - غازي عبد الرحمان هيان الرشيد، الحماية القانونية من جرائم المعلوماتية "الإنترنت" ، مذكرة دكتوراه، جامعة السالمية، لبنان، 2004 ، ص92

[2] - علي جبار الحسناوي ، جرائم الحاسوب و الإنترنت ، دار اليازوي العلمية للنشر والتوزيع ، 11 عمان ، 2009 ، ص 154

– تحديد الغرض: يكون الهدف من استخدام المعلومات الشخصية محدودًا ومحددًا مسبقًا.
–حدود الاستخدام: يقتضي الالتزام بعدم إفشاء البيانات الشخصية ونشرها لغير المصرح لهم بذلك .
–الوقاية الأمنية : ضرورة اتخاذ تدابير وإجراءات أمنية ملائمة وحازمة في إحاطة البيانات.
– الانفتاح: يجب الكشف عن السياسة العامة للتطوير التطبيقات المتعلقة بالبيانات الشخصية.
–المشاركة الفردية: حق الأشخاص المعنية في الوصول والتعرف على البيانات التي خصتهم فضلا عن رقابة مدى صحتها .
–المسائلة والمحاسبة : التي تقتضي حماسية الأشخاص والجهات المرخص لهم الوصول والاطلاع على البيانات والتعامل معها، في حالة تجاوز أي من الإجراءات التي تكفل حماية البيانات ذات الصفة الخاصة. [1]

الفرع الثاني: الجهود الإقليمية

أهم الجهود الإقليمية في مواجهة الجريمة المتعلقة بالإنترنت هي التي قام بها المجلس الأوروبي الذي برز كعنصر فعال في مكافحة هذه الجرائم المستحدثة.

الفقرة الأولى : اتفاقية بودابست

تعد اتفاقية أوروبية بمثابة دعوة موجهه إلى دول العالم للتفاعل مع الجرائم المستحدثة والتي جاءت نتيجة عدة محاولات حتى ظهرت بشكلها في 20 أفريل 2000 أين تقدمت اللجنة الأوروبية بمشروع اتفاقية جرائم الكمبيوتر وتقنية المعلومات وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء من وقت إصدار مشروعها الأول وحتى إعداد مسودتها النهائية التي أقرت لاحقا في بودابست 2001. وتعرف باتفاقية بودابست" أو اتفاقية الجرائم الإلكترونية " وكان قد طرح مشروع الاتفاقية للعامة، ووزع على مختلف الجهات وأطلق ضمن مواقع عديدة أوروبية وأمريكية على شبكة الإنترنت لجهة التباحث وإبداء الرأي،

[1] – علي جبار الحسناوي، المرجع السابق، ص154

وتعكس الاتفاقية الجهد الواسع والمميز للاتحاد الأوروبي ولجان الخبراء فيهما المنصبة على مسائل جرائم الكمبيوتر وأغراضها منذ أ كثر من عدة سنوات.[1]

ومن الدوافع التي أدت إلى إبرام الاتفاقية هو الحاجة إلى اتخاذ تدابير تشريعية لمكافحة جرائم الحاسوب والإنترنت للقضاء عليها وعلى مخاطرها المدمرة على كافة المستويات، خاصة في الوقت الذي انتشرت فيه شبكات المعلومات وفي الوقت الذي تزايد فيه نمو أنظمة الحواسيب ونقل وتدفق المعلومات بسرعة فائقة، إضافة إلى التشديد على أهمية مكافحة كافة الأنشطة التي تستهدف أمن المعلومات ونظم الكمبيوتر[2]. هذه التدابير التشريعية والتنظيمية لضمان ملاحقة مرتكبي هذه الجرائم وكشفها، وتوفر قواعد ملائمة للتحري والتحقيق والضبط والتفتيش والمحاكمة مع التركيز على أهمية التعاون المحلي والإقليمي والدولي مع ضرورة التنسيق بين الحاجة إلى دعم تطبيق القانون والحاجة إلى احترام الحقوق الشخصية، وبما أن هذا الاتفاق خاص بالجهود الدولية والإقليمية، فقد سلط الضوء أيضًا على ما بذل من جهود لمكافحة الجرائم الإلكترونية من قبل الأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية والإتحاد الأوروبي ومجموعة الدول الصناعية. وبالنتيجة فإن مشروع الاتفاقية قد ركزت على عناصر أساسية.[3] تكمن في التدابير التشريعية الموضوعية أي نصوص التجريم والتدابير التشريعية والإجرائية، وتدابير التعاون الدولي والإقليمي في مجال مكافحة الجرائم.

إن اتفاقية بودابست قامت بتحديد قائمة جرائم الكمبيوتر والإنترنت وأنماطها وطوائفها وكانت أول تقدم فيها إطارا للتقسيم، إذ حتى الآن وبالرغم من الجهود التشريعية والتدابير الإقليمية والدولية لم تتوفر رؤية شاملة أو إطار واضح يحدد قائمة هذا النوع من الجرائم، وبالرجوع إلى المعيار الذي اعتمدته، نجده بالأساس يقوم على فكرة دور الكمبيوتر بالجريمة.

---

[1] – يونس عرب ، قراءة في الإتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية، ملتقى تجربة سلطنة عمان، تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية ، 2– 4 افريل 2006 ، مسقط، ص15

[2] – عبد الله عبد الكريم عبد الله ، المرجع السابق ، ص126

[3] – يونس عرب ، المرجع السابق، ص16

ولقد جاءت المادة الأولى من الاتفاقية في الفصل الثاني الذي جاء تحت عنوان الإجراءات المتعين اتخاذها على المستوى الوطني، 3 أقسام : القسم الأول، ويتضمن المواد من 2–13 ويعالج النصوص الموضوعية لجرائم الكمبيوتر، والقسم الثاني ويتضمن المواد من14 إلى 21 وتتعلق بالقواعد الإجرائية، والقسم الثالث ويحتوي على المادة 22 وتتعلق بالاختصاص. أما الفصل الثالث من الاتفاقية والذي جاء تحت عنوان التعاون الدولي، وجاء بقسمين، الأول تحت عنوان المبادئ العامة ويضم المواد من 23إلى 28 أما الثاني وجاءت به النصوص الخاصة من المادة 29إلى 35 ،أما الأحكام الختامية فتضمنها الفصل الخامس من خلال المواد من 36 – 48 .

ولقد أكدت الاتفاقية في مقدمتها على الحاجة الملحة إلى اتخاذ تدابير تشريعية لمكافحة جرائم الكمبيوتر والأنشطة التي تستهدف العناصر الثلاثة لأمن المعلومات ونظم الكمبيوتر وهي السرية وسلامة المحتوى وتوفر المعلومات والنظم، كما أن المقدمة نجدها تلخص أهداف الاتفاقية وهي كالأتي:[1]

– بذل مجهود لتحقيق التوحيد في الإجراءات التشريعية بين الدول الأوروبية المشاركة في الاتفاقية وغير الأوروبية.

– أهمية التعاون الإقليمي والدولي في مكافحة الإرهاب.

– أهمية التعاون الإقليمي والدولي في مكافحة جرائم الحاسوب والجرائم الإلكترونية والجهود المبذولة لتبني قوانين وأنظمة تحارب الجرائم الإلكترونية.

–ضرورة فعالية خطط العمل لمكافحة الأنشطة التي تستهدف سرية وسلامة وتوفر المعلومات وأنظمة الكمبيوتر وشبكات الكمبيوتر وأنشطة إساءة استخدام الكمبيوتر والشبكات، وتحديد الإطار الأساسي لهذا النشاط والإطار الإجرائي للتحقيق والملاحقة القضائية في الجرائم الإلكترونية محليًا ودوليًا.

يضم الفصل الأول مادة واحدة المادة الأولى وهي التعريفات.[2] ولعلى أن هذه المادة من أهم المواد في ميدان اتفاقيات تقنية المعلومات بسبب الاختلاف الكبير بشأن تعريف

[1] – المجلس الأوروبي ، المذكرة التفسيرية لاتفاقية بودابست 2001 ، النسخة المترجمة بالعربية، 2014/05/12

[2] – الهلالي عبد الإله، المرجع السابق، ص 30 وما بعدها

اصطلاحات الكمبيوتر تبعا لزاوية الرؤيا وهدف استخدام التعريف، إلى جانب التباين بشأن المعايير والمقاييس التقنية، ولعلى لهذه المادة أهمية استثنائية لجهة توحيد التعريفات بعدما ظهر التناقض والتباين في تشريعات جرائم الكمبيوتر التي جرى سنها في أوروبا وأمريكا واستراليا وعدد من دول شرق آسيا، كما عرفت نظام الكمبيوتر، وعرفت هذه المادة معطيات الكمبيوتر تعريفاً واسعا يشمل الحقائق والمعلومات والمفاهيم بشكل مناسب لعمليات المعالجة في نظام الكمبيوتر.

ويتضمن الفصل الثاني من الاتفاقية، بعنوان "المعايير الواجب اتباعها على المستوى الوطني" ثلاثة أقسام. الأول يتعلق بالتدابير الموضوعية، أي القانون الجنائي الموضوعي، الذي يهتم بالسلوكيات التي يجب اعتبارها جريمة جنائية، والثاني يتعلق بالتدابير الإجرائية، ويتناول التدابير المتخذة لإجراء تحقيقات أكثر فعالية فيما يتعلق بجرائم الحاسوب، ويجب التأكيد على أن هذه التدابير الإجرائية يمكن استخدامها مع أي جرائم جنائية تتعلق بنظام الحاسوب، والثالث يتعلق بالاختصاص القضائي، ومع هذا الفصل قدمت الاتفاقية الإطار القانوني للإجراءات التشريعية الموضوعية والإجرائية الواجب اتخاذها لمواجهة الجريمة.[1]

لقد تم تخصيص الفصل الثالث لجرائم الإنترنت للتعاون الدولي ودعوة الأطراف على التعاون في تطبيق المعايير الدولية في المسائل الجنائية، وفي حالة عدم وجود وثائق دولية ملزمه. إيجاد قواعد خاصة بالمعلومات المقدمة والمساعدات القانونية المتبادلة.

أما الفصل الرابع تناول الأحكام الختامية، ويهتم هذا الفصل خاصة بالدول غير الأوروبية كما ينص على الطرق التي يتم بها الانضمام إلى الاتفاقية من طرف الدول غير الأعضاء .

أما القانون الجنائي الموضوعي يعد موضوع القسم الأول من هذه الاتفاقية ويعد دليلا إرشاديا لتحسن أو إصلاح وسائل منع وقمع الإجرام المعلوماتي، بتحديد أدنى القواعد العامة التي تسمح باتخاذ بعض التصرفات القانونية اتجاه هذه الجرائم ويسهل مكافحتها

[1] – طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية، ص297

على المستوى الوطني والدولي، ويحدد قائمة تسمح بتجريم بعض الأفعال والتصرفات غير المشروعة التي ترتكب على بيئة معلوماتية.[1]

ولقد تناولت المواد من 2 إلى 10 الجرائم الواردة في هذه الاتفاقية:

-جرائم ضد سرية وسلامة توافر البيانات والنظم المعلوماتية : كان الهدف من تناول هذه الجرائم هو محاربة سرية وسلامة وإتاحة أو تهيئة البيانات ونظم الحاسب للعمل أو التشغيل، وبالتالي يخرج من نطاق التجريم الأنشطة المشروعة والعادية والمرتبطة بتصميم الشبكات وكذلك الممارسات الاستثمارية أو التجارية المشروعة والعادية، وقد تناولتها المواد من 2 إلى 6.[2]

- الولوج غير القانوني "المادة 02" والذي يعد الجريمة الرئيسية التي تهدد سرية وأمن وسلامة المعلومات وتوفرها، وعلى ذلك مجرد التدخل غير المصرح به بمعنى القرصنة أو الدخول غير المشروع في النظام يعتبر تصرفاً غير مشروع .

-الاعتراض غير القانوني "المادة 3" وتهدف هذه المادة لحماية الحق في احترام نقل البيانات، وأن هذه الجريمة تمثل انتهاكاً للحق في احترام الاتصالات مثل التصنت والتسجيل التقليدي للمحادثات والمراسلات بين الأشخاص.

-"المادة 4" اعتراض على سلامة البيانات والغرض منها هو منح البيانات وبرامج الكمبيوتر نفس الحماية التي تهدف إليها ضد الضرر المتعمد الناجم عن الأشياء المادية التي تتسبب في تلف الوحدات المادية والمنطقية التي يتكون منها الكمبيوتر. ومحو البيانات والبرامج[3].

إلى غير ذلك من المواد التي تناولت الجريمة عبر الإنترنت من معظم الزوايا.

الفقرة الثانية : توصيات المجلس الأوروبي:

أدى التطور السريع في مجال تكنولوجيا الكمبيوتر والإنترنت وشعور الدول الأوروبية بأهمية إعادة النظر في الإجراءات الجزائية في هذا المجال إلى إصدار المجلس الأوروبي للتوصية رقم 95/13 في 11/9/1995 في شأن مشاكل الإجراءات الجزائية

---

[1] – طارق إبراهيم الدسوقي عطية، المرجع السابق ، ص 302

[2] – هلالي عبد الإله أحمد، المرجع السابق، ص68

[3] – المجلس الأوروبي، المرجع السابق، ص21

المتعلقة بتكنولوجيا المعلومات، وحث الدول الأعضاء بمراجعة قوانين الإجراءات الجزائية الوطنية لكي تتلاءم مع التطور في هذا المجال، ومن أهم ما ورد بتوصية المجلس الأوروبي ما يلي:

– تبيين ما حدده القانون من إجراءات التفتيش على الحاسبات الآلية، ومصادرة المعلومات الواردة فيها، ومراقبة المعلومات المنقولة.

– تسمح الإجراءات الجنائية الوطنية لسلطات التفتيش بمصادرة برامج الكمبيوتر والمعلومات الموجودة في الأجهزة في نفس الظروف مثل إجراءات التفتيش العادية ويجب أن تبلغ الشخص المسؤول عن الجهاز بأنه قد تم فحص النظام. وذكر أنه تم القبض عليهم، والسماح بالطعن في قرارات التوقيف والتفتيش وفق الإجراءات المعتادة.

– السماح للسلطات التنفيذية أثناء عملية التفتيش وفي ضوء الإجراءات الأمنية المعمول بها بتوسيع نطاق التفتيش ليشمل أنظمة الكمبيوتر الأخرى الخاضعة لولايتها القضائية والمرتبطة بالنظام ، لحذف واستعادة المعلومات الخاصة بها عند الضرورة.

– تطبق إجراءات المراقبة والتسجيل في مجال التحقيق الجنائي في حالة الضرورة في مجال تكنولوجيا المعلومات، ويتعين توفير السرية والاحترام للمعلومات التي يفرض القانون لها حماية خاصة.

– يجب إلزام العاملين بالمؤسسات الحكومية والخاصة التي توفر خدمات الاتصال بالتعاون مع سلطة التحقيق لإجراء المراقبة والتسجيل.

– أن يوضح قانون الإجراءات الجزائية أن الإجراءات الخاصة بالوثائق التقليدية تنطبق في شأن المعلومات الموجودة بأجهزة الكمبيوتر.

المطلب الثاني : التعاون الدولي في مواجهة الجريمة عبر الإنترنت

إن أي دولة مهما كانت قوية ومتينة، لا يمكنها الاستغناء عن الدخول في علاقات تعاون متبادل مع الدول الأخرى. خاصة وأن جهودها الداخلية في المكافحة أو الملاحقة للجرائم لم تعد كافية لمنع الجريمة أو تقليص حجمها، خاصة الجرائم العابرة للحدود التي تفاقم حجمها على المستويات الوطنية والإقليمية والعالمية بسب التقدم التكنولوجي كالإرهاب، وغسيل الأموال، مما يؤدي إلى توزيع أركانها على عدة دول، كما أن أدلة

إثباتها يسهل طمثها ومحوها، مما يجعل هناك صعوبة قائمة ضد القوانين الوطنية التقليدية في مواجهة هذا النوع من الجرائم، هذا ما جعل المجتمع الدولي يتجه نحو إنشاء أجهزة تعاونية تعمل على مستويات حكومية أو غير حكومية من أجل ضمان التنسيق والمتابعة فيما يتخذ من تدابير دولية وداخلية لوضع الالتزام الدولي بالتعاون موضع التنفيذ الإيجابي.

ومن أبرز مظاهر التعاون ما يلي:

الفرع الأول : التعاون القضائي

تعد جرائم الإنترنت من الجرائم العابرة للحدود كما ذكرناه أنفا ولتقديم مرتكبيها للمحاكمة وتوقيع العقاب عليهم يستلزم القيام بأعمال إجرائية خارج حدود الدولة حيث ارتكبت الجريمة، مثل معاينة موقع الإنترنت في الخارج، أو ضبط الأقراص الصلبة التي توجد عليها معلومات غير مشروعة أو صور إباحية، أو للبحث فيما يتعلق بالاتصالات عن بعد، أو من أجل الحصول على المعلومات التي قد تساعد في التحقيق في الجرائم المعلوماتية. كل هذا لا يمكن تحقيقه بدون تعاون قضائي بين الدول.

ويتخذ التعاون القضائي الدولي في هذا المجال عدة صور أهمها المساعدة القضائية والتعاون الأمني.

الفقرة الأولى : المساعدة القضائية

لقد اضطرت الدول إلى التنسيق من أجل تبادل المساعدة القضائية للقضاء على الجريمة المعلوماتية بصفة عامة ومتابعة مجرميها، ولتوفير حماية وردع أفضل، وهذه المساعدة عادة ما تكون بموجب اتفاقيات دولية ثنائية أو متعددة الأطراف بين السلطات المركزية للدول، تتمثل غالبا في وزارة العدل من أجل تعزيز التعاون القضائي، ومن أجل معرفة كيف يتم ذلك، سيتم التطرق إلى تعريف المساعدة القضائية ومصادر المساعدة القضائية وبعده تأتي مظاهر المساعدة القضائية .

أولا: تعريفها

تعد المساعدة القضائية إحدى الوسائل الإجرائية الهامة للتعاون الدولي على مكافحة الجريمة، وهي عملية قضائية غرضها تسهيل ممارسة الاختصاص القضائي في بلد أخر

وهذا لضمان الملاحقة القضائية السريعة والفعالة وفرض العقوبة، وهو أمر ضروري تقتضيه المصلحة المشتركة للدول لمكافحة الإجرام.[1]

فالمساعدة القضائية المتبادلة هي الإطار الإجرائي للتعاون القضائي الدولي، هي كل إجراء تقوم به السلطة المختصة في إحدى الدول بناء على طلب السلطة المختصة في دولة أجنبية، وذلك لقيام الأدلة المطلوبة خارج إقليم الدولة، أو في حوزة سلطات أجنبية أخرى. والهدف منها هو تعاون الأطراف في التحقيقات والملاحقات والإجراءات القضائية المتعلقة بالجرائم التي تشملها الاتفاقية، وذلك من أجل الحصول على الأدلة أو الأقوال من الأشخاص، أو تبليغ المستندات القضائية، أو تنفيذ عمليات التفتيش والضبط وتجميد الأموال ومعاينة الأشياء والمواقع وتقديم المعلومات والأدلة التي يقوم بها الخبراء، وتقديم أصول المستندات والسجلات المتعلقة بالقضايا المشمولة بالاتفاقية بما فيها السجلات الحكومية أو المصرفية أو المالية أو سجلات الشركات أو الأعمال،[2] ومن أجل هذا جاءت توصيات مؤتمرات الأمم المتحدة تحث على تقديم المساعدات القضائية وكل الخدمات التي تسعى إلى قمع الجريمة المعلوماتية بكل أنواعها.

ثانيا : مصادر المساعدة القضائية

يعتبر التشريع الوطني والاتفاقيات الدولية من أهم و أبرز مصادر المساعدة القضائية، أين تعتمد الدول بشأن المساعدة القضائية المتبادلة في المسائل الجنائية أحكام معاهدة الأمم المتحدة النموذجية ذات الصلة والمعتمدة بموجب القرار 117/45 الذي تم تأريخه 14 /12/ 1990 والتي ورد فيها أحكام المساعدة المتبادلة، سواء في التحقيقات أو إجراءات المحاكمة والمساعدة في أخذ شهادة الشهود أو بيانات الأشخاص .

يكون تقديم المعاونة في التحريات بتبليغ الوثائق القضائية، وتنفيذ عمليات التفتيش والحجز وفحص الأشياء والوثائق، كما تتضمن هذه المساعدة اعتقال الأشخاص وتسليمهم،

---

[1] – حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، مقال منشور على موقع المنشاوي للدراسات والبحوث: www.manchawi.com

[2] –أحمد عبد الحليم شاكر، دور الإنابة القضائية الدولية في مكافحة الجريمة، بحث منشور بمجلة الفكر الشرطي، المجلد 18 ،العدد 4 ،2007م، ص 153.

وتقوم السلطة المطالبة بتنفيذ أحكام جنائية صادرة عن الدولة الطالبة بالقدر الذي تسمح به قوانين الدولة المطالبة والبروتوكول الاختياري الملحق بهذه المعاهدة، كما يتعين على كل دولة تعيين سلطات تتولى تقديم الطلبات أو تلقيها وتبليغ الطرف الأخر، و تعالج المواد 4،5،6 شروط التسليم وإجراءاته وعدم الاحتجاج بالسرية المصرفية ومحتويات الطلب، والغرض من ذلك قبول المساعدة فورا حسب ما ينص قانون الدولة المطالبة ، ولا يجوز أن تستخدم الدولة الطالبة أو تحول معلومات أو بيانات تقدمها الدولة المطالبة إلى إجراءات غير تلك المسببة في الطلب وعليها حفظ سرية الطلب ومحتوياته[1] .

ثالثا : مظاهر المساعدة القضائية

نظرا لتطور أساليب ارتكاب الجريمة واستفادتها من التطور التكنولوجي، أصبحت المكافحة في المجال القضائي تقتضي تبني وسائل أخرى لمكافحة مثل هذه الجرائم وتكون أكثر فعالية، ومن أهم هذه الوسائل الإنابة القضائية الدولية وتبادل المعلومات ونقل الإجراءات.

1-الإنابة القضائية الدولية

تعتبر الإنابة القضائية من الوسائل الجديدة للتعاون الدولي. ولقد عرفها البعض على أنها طلب من السلطة القضائية المنيبة إلى السلطة المنابة قضائية أم دبلوماسية، أساسه التبادل باتخاذ إجراء من إجراءات التحقيق أو جمع الأدلة في الخارج وكذا أي إجراء قضائي آخر يلزم اتخاذه للفصل في المسألة المثارة، أو المحتمل إثارتها في المستقبل أمام القاضي المنيب، الذي ليس في مقدوره القيام به في نطاق دائرة اختصاصه.[2]

لقد أبرمت الدول عدة اتفاقيات على مختلف الأصعدة بغرض تنظيم أحكام التعاون القضائي بينها ولتبادل التعاون بين السلطات القضائية، كما حاولت التخفيف من شدة القاعدة التي تقضي بأن تنفيذ الإنابة طبقا لقانون الدولة المطلوب إليها يعد نزولا عن مبدأ الإقليمية، فأجازت للقاضي في الدولة المطلوب إليها المساعدة تنفيذ الإنابة القضائية وفقا للإجراءات الواجبة الإتباع في قانون الدولة الطالبة، وذلك في الحالات التي لا يوجد فيها

[1]- حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، المرجع السابق

[2] – حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، المرجع السابق

تعارض مع المبادئ الأساسية في الإجراءات الجنائية في دولته، وهذه الوسيلة الجديدة تسهل استعمال الأدلة التي تم الحصول عليها عن طريق الإنابة القضائية أمام محاكم الدولة الطالبة، وهو ما لا يمكن تحقيقه في كثير من الأحوال عند تطبيق قانون الدولة المطلوب إليها .

إن الهدف من الإنابة هو تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على مشكلة السيادة الإقليمية التي تقف عقبة أمام الدول الأجنبية وتمنعهم من ممارسة بعض الأعمال القضائية بأقاليم دول أخرى، كسماع الشهود أو إجراء التفتيش وغيرها ومن الصور الحديثة للتعاون القضائي ما يسمى بنظام قضاة الاتصال، وذلك عن طريق الاتصال المباشر بين السلطات القضائية المختصة في الدول المعنية بدلا عن الطريق الدبلوماسي، لضمان سرعة إنجاز الإنابات القضائية وطلبات المساعدة القضائية بصفة عامة، وقد نصت على هذا النظام الاتفاقية الدولية للإتحاد الأوروبي في 29 مايو 2000 حيث يفترض هذا النظام وجود اتفاقيات ثنائية بين الدول.[1]

ويكون تنظيم الإنابة القضائية عن طريق الاتفاق بين الدول عن طريق إبرام معاهدات دولية جماعية وثنائية كما أن هناك من الدول من تنص في قانونها الوطني عن بعض قواعد هذه الإنابة القضائية.

2- تبادل المعلومات :

يتم تبادل المعلومات والوثائق التي تطلبها سلطة قضائية أجنبية بصدد جريمة من الجرائم عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم، كما أن هناك مظهر آخر من مظاهر تبادل المعلومات وهو ما يتعلق بالسوابق القضائية للجناة من خلالها تتعرف الجهة القضائية بدقة على الماضي الجنائي للفرد المحال إليها، فهي التي تساعد في تطبيق الأحكام الخاصة بالعود ووقف تنفيذ العقوبة وعدم الأهلية.[2]

[1] – جميل عبد الباقي الصغير، الجوانب الإجرائية، المرجع السابق ص86

[2] – عيسى سليم داود، المرجع السابق، ص 136

وقد قررت بتبادل المعلومات الاتفاقية الأوروبية حول الجريمة الافتراضية في المادة 23 والتي نصت صراحة على وجوب توافر التعاون الدولي بين الدول الأطراف وتعميقه وتقليل العوائق، بما يوفر أكبر قدر من السهولة والسرعة لتبادل المعلومات والأدلة بين الأطراف. كما نصت المادة الأولى من اتفاقية التعاون القضائي لمنعقدة بالرياض على هذا التبادل بقولها "تتبادل وزارت العدل لدى الأطراف المتعاقدة بصفة منتظمة نصوص التشريعات النافذة والمطبوعات والنشرات والبحوث القانونية والقضائية والمجلات التي تنشر فيها الأحكام القضائية، كما تتبادل المعلومات المختلفة بالتنظيم القضائي.[1]

3- نقل الإجراءات:

إن نقل الإجراءات هو قيام الدولة بناء على اتفاق باتخاذ إجراءات جنائية بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة، وذلك إذا توافرت الشروط التالية:

أ- أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب منها .

ب- يجوز الطرف المتعاقد أن يطلب من أي طرف آخر أن يتخذ الإجراءات الجزائية في أي حالة من الحالات الآتية :

* إذا تعرض المتهم أو سيخضع لعقوبة تحد من حريته في الدولة الطالبة .

* إذا كان قانون الدولة التي يتم فيها تقديم الطلب لنفس الجريمة ينص على الإجراء الواجب إتباعه.

* أن يؤدي الإجراء المطلوب إلى اكتشاف الحقيقة، كدليل على جريمة في البلد المطلوب منه.

*إذا كان تنفيذ الحكم في الدولة المطلوب إليها يحقق إعادة التأهيل الاجتماعي للشخص المحكوم عليه.

[1] – http://www.arableagueonline.org

* إذا تعذر حضور المتهم الجلسة في البلد الطالب وضمان حضوره للجلسة في البلد المطلوب إليه.

ج- ويجوز للدولة المطلوب إليها أن ترفض نقل الإجراءات في الحالات الآتية:

* إذا كان طلب نقل الإجراءات ليس له ما يبرره، بأن تكون الأسباب التي ذكرتها الدولة الطالبة لا تدعو لاتخاذ مثل هذه الإجراءات .

*إذا ثبت أن الباعث من وراء طلب نقل الإجراءات اعتبارات عنصرية أو دينية أو سياسية .

*إذا كانت الدولة المطلوب إليها قد طبقت قانونها على الجريمة قبل استلامها من الدولة الطالبة وكان الإجراء الذي سبق اتخاذه مطابقا للقانون[1] .

*إذا كانت الإجراءات التي تطلبها الدولة الطالبة مخالفة لواجبات ملتزمة بها الدولة المطلوب إليها .

*إذا كانت الإجراءات المطلوبة مخالفة للمبادئ الأساسية للنظام القانوني في الدولة المطلوب إليها[2] .

وهناك من يرى أن تطبيق الآليات التقليدية للاتفاقيات يثير بعض الإشكاليات، مثل وجود معوقات خاصة بالجرائم المرتكبة عبر الإنترنت. وعلى الرغم من وجود هذه العقبات على المستوى المحلي أو الوطني، إلا أنها تثار أيضًا على شبكة الإنترنت. ومن بين هذه العقبات، تتبع الاتصالات الإلكترونية عن طريق سلطات التحقيق الدولي وإقامة الدليل على الجرائم التي ترتكب في مجال الإنترنت، وذلك بالنظر إلى الاختلافات التي توجد بين التشريعات المختلفة فيما يتعلق بشروط قبول الأدلة وتنفيذ بعض الإجراءات مثل التفتيش عبر الحدود ووقف بث الرسائل ذات المحتوى غير المشروع.[3]

---

[1]- سالم الأوجلي، المرجع السابق، ص 427 ،428

[2] - سالم الأوجلي، المرجع نفسه، ص 428

[3] - جميل عبد الباقي الصغير، المرجع السابق، ص 80

رابعا: موقف المشرع الجزائري من المساعدة القضائية:

قد ساير المشرع الجزائري الركب المعلوماتي في هدا المجال بأن تبنى نصوص تشريعية حديثة جسد من خلالها اغلب الأحكام الواردة في الاتفاقية الدولية للإجرام الالكتروني، وقد تطرق القانون إلى المساعدة القضائية المتبادلة كعنصر مهم في مواجهة الإجرام الالكتروني، ومن بين النقاط التي تظهر ذلك نجد القواعد الخاصة بالوقاية من الجرائم ذات الصلة بتكنولوجيا الإعلام والاتصال ومكافحتها طبقا لأحكام القانون 04/09 .

وتظهر مجالات التعاون القضائي الدولي في مجال مراقبة الاتصالات الالكترونية، ونص المشرع على الحالات التي تسمح باللجوء إلى المراقبة الالكترونية، ومن بينها إطار تنفيذ طلبات المساعدة القضائية المتبادل ، كذلك في إطار تفتيش المنظومة المعلوماتية فقد أشار المشرع للمساعدة القضائية المتبادلة وهدا في حالة ما إذا كانت المعطيات المبحوث عنها يمكن الدخول إليها انطلاقا من منظومة معلوماتية تقع خارج الإقليم الوطني ويكون الحصول عليها بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

كما كرس القانون مبدأ التعاون والمساعدة القضائية في حالة ما إذا كان مرتكبها أجنبيا وتستهدف مؤسسات الدولة، واسند مهام الرقابة على هده الجرائم للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بمقتضى المادة الثالثة عشر التي حددت مسؤولياتها، من بينها تبادل المعلومات مع نظيراتها في الخارج، بقصد جمع كل ما له صلة لتحديد وتعقب المجرمين المتورطين في جرائم التقنية.

الفقرة الثانية : التعاون الأمني الدولي

إن كل دولة لا تستطيع بمجهوداتها المنفردة أن تقضي على الجريمة خاصة الجريمة العابرة للحدود كما أثبته الواقع خاصة مع التطورات الكبيرة التي تحدث في جميع أنحاء العالم ، لذلك هناك حاجة ماسة لوجود كيان دولي يقوم بهذه المهمة ولأجهزة الشرطة في الدول كافة التعاون من خلال هذا الكيان، خاصة حول تبادل المعلومات بحيث يمكن ملاحقة المجرمين ومعاقبتهم. ومن الجهود المبذولة في هذا المجال جهود المنظمة الدولية للشرطة الجنائية الإنتربول وكان من أهم أهدافها تأكيد وتشجيع التعاون بين أجهزة الشرطة

في الدول الأطراف المتعاقدة وعلى نحو فعال في مكافحة الجريمة، وتجميع البيانات والمعلومات المتعلقةّ بالمجرم والجريمة، وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنضمة لها.[1] أضف إلى ذلك التعاون بين الدول الأعضاء في ضبط المجرمين بمساعدة أجهزة الشرطة بواسطة المعلومات المتوفرة والخاصة بالنسبة للجرائم المستحدثة مثل جرائم الإنترنت.

ولقد لعبت منظمة الإنتربول دورا هاما في اكتشاف العديد من الجرائم عبر الإنترنت ومثال على ذلك دورها في ما يتعلق بالجرائم المتعلقة بالإنترنت في ما حصل في اندونيسيا، حيث أتاحت عملية سيبرانية نسّقها الإنتربول لكشف برمجية خبيثة تستهدف مواقع للتجارة الإلكترونية وتحديد عدة مواقع ملوثة وأدت إلى توقيف ثلاثة أشخاص يستخدمون برمجية تنتمي إلى فئة برمجيات يطلق عليه ب JavaScript-sniffer في اندونيسيا وتستهدف مواقع التجارة الإلكترونية وعند تلويث الموقع، يتم سرقة تفاصيل البطاقات المصرفية الخاصة بالزبائن بواسطة البرمجية، ويتم كذلك سرقة البيانات الشخصية من أسماء وعناوين وأرقام الهاتف، ويتم إرسال المعلومات المتحصل عليها إلى خواديم قيادة وتحكّم يستخدمها مجرمي المجال السيبري.

كذلك توفرت للإنتربول بيانات عن البرمجية وحجمها ونطاقها عبر شراكته مع شركة الأمن السيبري "إي بي قروب"، وساعد ذلك في كشف مئات مواقع التجارة الإلكترونية الملوثة عبر العالم. ووفرت شركة الأمن السيبيري خبرتها في مجال الأدلة الجنائية في البيئة الرقمية، وهذا ما ساعد على معرفة المشتبه بهم والقبض عليهم. وقد قام الإنتربول بتوزيع تقارير على البلدان المعنية تخص الأنشطة السيبرية لتيسير تحقيقاتها الوطنية ولتطوير قدرات مكافحة الجريمة السيبرية خاصة في منطقة" جنوب شرق أسيا "الأمر الذي سمح بكشف خواديم C2 وعدد كبير من المواقع الملوثة على الشبكة في الكثير من البلدان من نفس المنطقة.

[1] -Malcom Anderson ،Policing the world : Interpol the Politics of International Police Co-Operation ، Clarendon press.Oxford,1989,p 168-185

وتبعا لما سبق وفر مكتب رابطة أمم جنوب أسيا مساعدة تقنية بناءا على طلب الشرطة الوطنية في إندونيسيا، وتم من خلالها إلى توقيف عدد من المشتبه فيهم في تشغيل خواديم C2.

ومن خلال التحقيق اكتشف المشتبه بهم وكذا شراءهم لسلع الكترونية ومنتجات فخمة باستخدامهم للبيانات المصرفية المسروقة وقيامهم ببيع المشتريات لتحقيق الأرباح. وقد سرح مدير مكافحة الجريمة السيبرانية: " أن الشركات الفعالة بين قطاع الأمن في مجال المعلومات والشرطة ذات الأهمية الكبيرة لتتمكن أجهزة تطبيق القانون في العالم كله من الحصول واقتناء المعلومات التي تحتاج إليها لمواجهة مشاكل التهديدات السيبرانية في العالم المعاصر". وأضاف أيضا أن هذه العملية الناجحة تدل على قدرة أجهزة إنفاذ القانون على التكيف واستخدام التكنولوجيا الجديدة لدعم التحقيقات والتوصل في أخر الأمر إلى القضاء على الجرائم المعلوماتية عالميا". إضافة إلى ما سبق تم تعطيل خواديم C2 من طرف الأمن في سنغافورة. والتحقيقات بقت جارية في بلدان منطقة جنوب آسيا، في حين استمرت الإنتربول على مساعدة الشرطة لمعرفة مكان باقي الخواديم وكشف كافة مواقع الإنترنت الملوثة ومعرفة المجرمين.[1]

ولقد أنشأ المجلس الأوروبي في لكسمبورج عام 1991 شرطة أوروبية لتكون الرابط بين أجهزة الشرطة الوطنية ،في الدول المنظمة والملاحقة للجرائم العابرة للحدود والجرائم عبر الإنترنت.[2]

أما عن التعاون العربي نجد أن مجلس وزراء الداخلية العرب أنشأ المكتب العربي للشرطة الجنائية بهدف تنمية التعاون بين أجهزة الشرطة وتأمينها بين الدول الأعضاء لمكافحة الجريمة خاصة العابرة لحدود وملاحقة المشتبه فيهم في ضل القوانين والأنظمة المعمول بها في كل دولة. إضافة إلى هذا من أجل التعاون وتطوير الأساليب في مجال دعم أجهزة الشرطة في الدول الأعضاء.

---

[1] – أنظر الموقع الإلكتروني : https//www.interpol.net 2020 اطلع عليه في 2021/09/22

– 2c هي شركة للخدمات تعمل في مجالين تكامل حلول مركز الاتصال وتطوير البرمجيات .

[2] – جميل عبد الباقي الصغير – الجوانب الإجرائية المتعلقة بالإنترنت، دار النهضة العربية، ط 2001، ص 79

ومن أهم وأبرز صور التعاون الأمني في مجال مكافحة جرائم الإنترنت هي تبادل المعاونة لمواجهة الكوارث والأزمات والمواقف الحرجة، خاصة وأن أجهزة العدالة الجزائية ليست بنفس المستوي والجاهزية في جميع الدول وإنما هناك تفاوت فيما بينها، حيث نجد أن بعض الدول متقدمة تقنيا وتكنولوجيا ولها خبرة كبيرة تشريعيا وفنيا في مواجهة الجرائم المعلوماتية من بينها الجرائم عبر الإنترنت، والبعض الأخر يفتقد لذلك.[1]

ومن صور التعاون الأمني أيضا القيام ببعض العمليات المشتركة في تعقب مجرمي المعلوماتية بما فيها جرائم الشبكة العنكبوتية، بهدف تعقب الأدلة الرقمية وضبطها والقيام بعملية التفتيش العابر للحدود لمكونات الحاسب الآلي والأنظمة المعلوماتية وشبكات الاتصال،[2] وللتحري وجمع الأدلة لإدانة مرتكبي الجريمة المعلوماتية بصفة عامة.

الفرع الثاني : تسليم المجرمين والتدريب على مواجهة الجريمة المرتكبة عبر الإنترنت

سنتناول في هذا الفرع شكلين من أشكال التعاون الدولي في مجال مكافحة الجريمة عبر الإنترنـت، الأول تسليم المجرمين، والثاني التدريب على تقنية المعلومات كالبرمجة وتصميم النظم وتحليلها وإدارة الشبكات وعمليات الحاسب الآلي.

الفقرة الأولى: تسليم المجرمين

يعد تسليم المجرمين شكل من أشكال التعاون الدولي في مجال مكافحة الإجرام السيبراني، والذي تناولته ونظمته عدة قوانين وطنية واتفاقيات دولية، كما أنه من أكبر جوانب التعاون الدولي إثارة للجدل نظرا لمساسه الشديد بالحرية الشخصية، مما أوجب العناية الشديدة بتنظيمه منعا للخلاف والتعارض واحتراما لكل مصلحة قانونية جديرة بالحماية. وهو إجراء غرضه مكافحة الجريمة السيبرانية وحماية المجتمعات من الماسين بأمنها واستقرارها على المستوى الدولي والمحلي، وحتى لا يفلت هؤلاء المجرمون من العقاب.[3]

---

[1] – محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الإلكترونية، المجلة الأكاديمية للبحث القانوني، المجلد14، العدد 02 –20 ص54

[2] – محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الإلكترونية، المرجع نفسه، ص54

[3] – جميل عبد الباقي الصغير، الجوانب الإجرائية، المرجع السابق ، ص 88

وفي هذا الفرع سوف نقوم بالحديث عن مفهوم هذا النظام، وشروطه وإجراءاته بوجه عام، ثم نتبعه بالحديث عن نظام تسليم المتهمين في مجال الجرائم السيبرانية وذلك على النحو التالي:

أولا: تعريف تسليم المتهمين :

إن إجراء تسليم المتهمين يقوم من ناحية على وجود علاقة بين دولتين، تقوم الدولة الأولى بالمطالبة بأن يسلم إليها مرتكب الجريمة لتتخذ بحقه الإجراءات اللازمة، والدولة الثانية التي وجه إليها طلب التسليم، وعليها التقرير إما بالاستجابة إذا كان الطلب متوافقا مع تشريع نافذ المفعول فيها أو معاهدة أو اتفاق بين البلدين، وإما الرفض لعدم وجود ذلك التشريع أو تلك الاتفاقية. ومن ناحية أخرى نجده يشمل نوعين من الأشخاص، النوع الأول هم المتهمين الذين تسند إليهم تهمة ارتكاب جرائم إلا أنه لم يصدر بحقهم أية أحكام قضائية بعد، والنوع الثاني هم المحكوم عليهم الذين صدر بحقهم حكم قضائي بالإدانة إلا أنه لم ينفذ بعد نتيجة فرارهم إلى دولة أخرى. وعليه فإن التسليم ثلاثة أنواع تسليم إداري وتسليم قضائي وتسليم مختلط.

ولقد نص المشرع الجزائري على إجراء التسليم في المادة 694 إلى المادة 719 من قانون إج في بابه الأول " تسليم المجرمين".

ثانيا : شروط نظام تسليم المتهمين

حتى يتم العمل بنظام تسليم المتهمين، هناك شروط لابد من توافرها، وهذه الشروط تكمن أهميتها في كونها تفصل حدود العلاقة بين الدول الأطراف في عملية التسليم وتضع الأحكام العامة التي على أساسها سيتم التسليم من عدمه.[1] وإذا توافرت هذه الشروط يتم البت في قرار التسليم. وتتمثل هذه الشروط فيما يلي:

1 –شرط ازدواج التجريم : ويقصد بهذا الشرط أن يكون الفعل المطلوب التسليم من أجله مجرما في تشريع الدولتين الطالبة والمطلوب إليها التسليم، والمطلوب هنا أن يكون الفعل مجرما أيا كانت الصورة التشريعية المعاقب عليها، فالعبرة بالوصف أو

[1] – هلالي عبد الله أحمد، ، اتفاقية بودابست لمكافحة جرائم . المعلوماتية، دار النهضة العربية، القاهرة، 2011 ،ص 308

التكييف القانوني الذي يطلق على الفعل عند تقرير توافر هذه الشروط والمعاقبة عليه، فقد تختلف تشريعات الدول في التكييف القانوني الذي توصف به الجريمة، فعلى سبيل المثال لو كان الفعل معاقبا عليه في تشريع الدولة الطالبة تحت مسمى جريمة منظمة، بينما كان الفعل نفسه معاقبا عليه تحت مسمى غسيل الأموال في الدولة المطلوب منها التسليم، فان ذلك لا يمنع من توافر شرط ثنائية التجريم أو ازدواجيته[1] .

ويبرر اشتراط ازدواجية الجرم أن الدولة طالبة التسليم وراء الطلب تسعى إلى مقاضاة من ارتكب السلوك الإجرامي أو تنفيذ العقوبة المفروضة عليه، وهذا يؤكد أن السلوك يعاقب عليه التشريع ، إذ إنه إذا لم يكن مجرما فلا يتصور وجود دعوى جنائية أو ملاحقة جزائية ضد شخص المتهم كما لا يمكن تصور قيام حكم جزائي يقضي بالعقوبة عليه، ولا يجوز مطالبة الدولة المطلوب منها التسليم بإيقاع عقوبة على ارتكاب سلوك ما هو في الأصل غير مجرم وفقا لقانونها .

ولقد ذهب أغلب الفقه إلى أن شرط ازدواج التجريم قد يكون عقبة في مجال تسليم المجرمين، ففي التشريعات الجنائية الوطنية نجد أن الجرائم المعلوماتية غير معاقب عليها في معظم الدول هذا من جهة ومن جهة أخرى انه من الصعب تحديد ما إذا كانت النصوص التقليدية في تشريعات الدولة المطلوب إليها التسليم يمكن أن تطبق على جرائم الإنترنت. بالإضافة إلى أن الدول قد تفسر بتوسع شرط ازدواج التجريم، الأمر الذي يترتب معه إعاقة تطبيق الاتفاقيات الدولية في مجال تسليم المتهمين ويحول ذلك دون جمع الأدلة ومحاكمة مرتكبي جرائم الإنترنت.[2] ويتطلب ذلك توافر التنسيق أو التوحيد الإلزامي بين مختلف التشريعات فيما يتعلق بتعريف جرائم المعلومات وجرائم الإنترنت، أو على الأقل عدم اشتراط التجريم المزدوج. كما يتضح من الاتفاقية القائمة بين

[1] – عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية ، دار النهضة العربية، القاهرة،2015 ، ص 88

[2] – طارق إبراهيم الدسوقي، الحماية القانونية لأمن الدولة من جهة الداخل والخارج، دار الجامعة الجديدة للنشر ،2010، ص 58

كندا والولايات المتحدة الأمريكية بشأن المساعدة القانونية المتبادلة، التي لم يشترط فيها ازدواجية التجريم لقيام هذا التعاون، وجرائم الإنترنت مدرجة في هذه الاتفاقية.[1]

2- شروط تسليم الأفراد :

إنه لا يجوز تسليم الرعايا، وقد نصت على ذلك معظم التشريعات الوطنية والاتفاقيات الدولية فإذا ما قام شخص من رعايا الدولة بارتكاب جريمة فلا يجوز تسليمه ، كذلك لا يجوز تسليم من تم منحهم حق اللجوء السياسي[2]، إذ أن هناك إجماعا دوليا على استبعاد الجرائم السياسية من نطاق التسليم سواء على الاتفاقيات الدولية أم التشريعات الوطنية، ولن يتم الخروج عنه في وقتنا الحالي. كذلك لا يجوز تسليم الشخص الذي قد سبقت محاكمته عن الجريمة المطلوب تسليمه من أجلها وبرء منها أو عوقب عنها، أيضا لا يجوز التسليم متى كان قيد التحقيق والمحاكمة عن ارتكابه فعلا ما هو ذاته المطلوب تسليمه من أجله. ويعد هذا الشرط من الضمانات الأساسية عند محاكمة الشخص المطلوب تسليمه، ويهدف إلى توفير اكبر قدر ممكن من الحماية القضائية للشخص المطلوب تسليمه إلى الدولة الطالبة وذلك حتى لا يواجه الشخص عقوبة مزدوجة، وهو شرط تقبله معظم القوانين والمعاهدات والاتفاقيات[3].

3- شروط الجريمة المطلوب التسليم لارتكابها :

هناك عدة أساليب تتخذها العديد من الدول لتحديد طبيعة الجرائم التي يجوز فيها التسليم وذلك على النحو التالي:

- **أسلوب الحصر أو نهج القائمة:** ويعتمد هذا الأسلوب على إدراج مجموعة من الجرائم على سبيل الحصر على سبيل المثال، النصب، السرقة، غسيل الأموال.... وتدرج هذه الجرائم في قائمة تلحق بالقانون أو الاتفاقية لتكون هذه الجرائم دون غيرها من الجرائم الأخرى هي التي يتم التسليم من أجلها، ويعد هذا الأسلوب من أقل الأساليب

---

[1] - جميل عبد الباقي الصغير، المرجع السابق، ص 92

[2] -Gilbert (Geoff) , Aspects of extradition law,london, kluwer, academic, 1991, p 95

[3] - حسين بن سعيد الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، المرجع السابق.

انتشارا بين دول العالم، إذ إنه يؤدي إلى إفلات بعض المجرمين من العقاب متى كانت الجريمة المرتكبة من قبلهم غير واردة في القائمة.

- **أسلوب جسامة الجريمة أو الحد الأدنى للعقوبة:** وهو الأسلوب الأكثر استخداما في تحديد الجرائم التي يجوز التسليم فيها،[1] وهو أن تحدد الدول في تشريعاتها الداخلية أو في الاتفاقيات أو المعاهدات الثنائية أو متعددة الأطراف الحد الأدنى للعقوبة المقررة للجرائم التي يمكن أن يتم التسليم من أجلها.

- **النظام المختلط** : وهو أسلوب من الأساليب الشائعة في تحديد الجرائم التي يجوز التسليم من أجلها، وهو أسلوب يضمن درجة معينة من جسامة الجريمة المعاقب عليها في البلدين لكي يتم التسليم وفقا لها، أيضا يضمن خضوع جرائم متعددة تمثل خطرا على الدول الأطراف للتسليم دون النظر إلى درجة جسامتها أو العقوبة المقررة لها.[2]

ثالثا: إجراءات نظام تسليم المتهمين

إجراءات تسليم المتهمين هي تلك القواعد ذات الطبيعة الإجرائية التي تتخذها الدول الأطراف في عملية التسليم وفقا لقوانينها الوطنية وتعهداتها، والغرض من ذلك إتمام عملية التسليم بهدف التوفيق بين المحافظة على حقوق الإنسان وحريته، وبين تأمين الصالح العام الناشئ عن ضروريات التعاون الدولي في مكافحة الجريمة بحيث لا يمكن لأي مجرم أن يفلت من العقاب.[3]

1- إجراءات الدولة طالبة التسليم :

حيث تبدأ الدولة طالبة التسليم إجراءاتها بالطلب ورغبتها في استلام الشخص المطلوب تسليمه، فلا يمكن تحريك طلب التسليم إلا بناء على طلب يقدم من الدولة الطالبة إلى الدولة المطلوب منها التسليم.[4]

---

[1]- يوسف حسن يوسف، الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، القاهرة، ط1، 2011 ، ص 167

[2]- يوسف حسن يوسف، المرجع السابق، ص 167

[3] - أمير فرج يوسف،الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت، مكتبة الوفاء القانونية، ط 2 ، 2011 ص 459

[4] - يوسف حسن يوسف، المرجع السابق، ص 169

2- إجراءات الدولة المطلوب منها التسليم:

إن الإجراءات التي تقوم بها الدولة في حالة إذا ما طلب منها تسليم أحد الأشخاص تنقسم إلى عدة مراحل :

-المرحلة الأولى: تتم بتلقي الطلب واتخاذ إجراءات التحري وجمع الاستدلالات والتحقيق والقبض على الشخص المطلوب.

- المرحلة الثانية: وفيها يتم استجواب المقبوض عليه وحبسه احتياطيا أو إطلاق سراحه بكفالة أو بدونها أو منعه من السفر إلى أن يتم الفصل في الطلب الوارد بتسليمه.

-المرحلة الثالثة: تتمثل في فحص الطلب من قبل المحكمة المختصة والبت فيه بالقبول أو الرفض، وعليها التحقق أولا من توافر الشروط الشكلية الواجب إتباعها من قبل الدولة طالبة التسليم كوجود ملف التسليم واحتوائه على جميع الوثائق المطلوبة والواجب إرفاقها مصدقة من الجهات المختصة في الدولة الطالبة، أيضا يجب التأكد من توافر الشروط الموضوعية كشرط ازدواج التجريم أو عدم انقضاء الدعوى العمومية أو العقوبة، كذلك التأكد من عدم وجود أي مانع من موانع التسليم المنصوص عليها. [1]

ومن بين الاتفاقيات الدولية في شأن تسليم المتهمين اتفاقية اليونان بشأن تسليم المتهمين لسنة 1986 والاتفاقية المبرمجة في المجر سنة 1988 والخاصة بالمساعدة القضائية وتسليم المتهمين ونقل المحكوم عليهم، واتفاقية التعاون القضائي في المواد الجنائية ونقل المحكوم عليهم أو المحبوسين وتسليم المتهمين في بولندا سنة 1992 . [2]

إن هذه الاتفاقيات يمكن تطبيقها في مجال جرائم الإنترنت، ويمكن للدول الأعضاء أن تطلب تسليم مجرم من الدولة العضو في الاتفاقية وذلك لمحاكمته أو تنفيذ عقوبة ضده في إحدى الجرائم المرتكبة عبر شبكة الإنترنت.

[1] - أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية، المرجع السابق، ص 4 61 ،462

[2] - عبد الرؤوف المهدي، المرجع السابق، ص 85 ،86

رابعا: نظام تسليم المتهمين في مجال الجرائم السيبرانية

كما سبق ذكره لم تعد الحدود الجغرافية بين الدول تشكل عائقا أمام ارتكاب الجرائم عبر الإنترنت، كما أن النشاط الإجرامي لم يعد مقتصرا على إقليم معين بل يمتد أثره ليشمل أكثر من دولة، فقد يقوم المجرم بالتحضير للجريمة في دولة معينة ويقوم بالتنفيذ في دولة أخرى، ويمتد اثر تلك الجريمة إلى دول أخرى ويقوم بالهرب إلى دولة لم يمسها هذا الأثر. فالمجرم يستطيع التنقل من دولة لدولة أخرى، ومن الممكن أن يرتكب هذا المجرم الهارب جرائم أخرى في بلدان متعددة، مما يجعله مجرما دوليا[1]. ولأن أجهزة الدول تعمل من أجل تنفيذ القانون، وتسعى إلى ملاحقة المجرمين، ولا يمكن لها أن تتجاوز كل دولة حدودها أو تعبر حدود دولة أخرى لممارسة الإجراءات الجزائية على الفارين من العقوبة طبقا لمبدأ السيادة الإقليمية. كان لزاما عليها أن تلجأ الدول لحل هذا الأشكال عن طريق وضع نظام لتسليم المجرمين يسهل على سلطات الدولة المعتدى عليها إنفاذ القانون والقبض العلى المجرمين وإرجاعهم إلى البلد التي نفذوا فيه الجريمة ومحاكمتهم وفق أحكام القانون. لذلك حرصت معظم الدول على سن التشريعات الخاصة بتسليم المجرمين، إضافة إلى هذا عقد اتفاقيات إقليمية ودولية بشأن تسليم المتهمين. ومن أبرز الاتفاقيات التي عالجت جرائم القرصنة هي اتفاقية بودابست بشأن مكافحة الجرائم المعلوماتية، والتي تم توضيحها في ما سبق. وعليه كان من الواجب على الدول تقوية إجراءات التسليم من خلال التطبيق الفعالً لقاعدة التسليم أو المحاكمة، وبالتالي فرض التزامات على الدولة التي يتواجد على إقليمها المتهم، إضافة إلى البحث والتحري عن هوية المجرم ومكان تواجده، ثم القبض عليه وأدانته طبقا لقانونها الداخلي، كذلك يجب على دول العالم الالتزام بتنظيم القانون الدولي والتوفيق بين ضروريات التعاون القضائي الدولي ومقتضيات السيادة للحماية من جرائم الإنترنت[2] .

[1] – عيسى سليم داود ، جرائم القرصنة الإلكترونية، رسالة ماجستير، جامعة الإسكندرية، 2017 ، ص 146

[2] – فريد ناشف، آليات التعاون الدولي في مكافحة الجرائم الالكترونية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 8 . العدد 1، 2022، ص 443

وعليه يعد نظام تسليم المتهمين خاصة في الجرائم السيبرانية هو الحل الأمثل والأساسي لمكافحة الهجوم السيبراني وما يترتب عن تلك الجريمة من خسائر للمؤسسات العامة والخاصة، فما الفائدة من تحديد مرتكب الجريمة وتحديد مكانه دون القدرة على محاكمته ومعاقبته عما اقترفه من جرائم. فالتسليم يعد وسيلة أساسية للحد من جرائم الإنترنت.

الفقرة الثانية : التدريب على مواجهة الجريمة المرتكبة عبر الإنترنت

التعاون الدولي في مجال التدريب على الحد من الهجوم السيبراني، هو نشاط علمي مخطط يهدف إلى تنمية القدرات والمهارات وتغيير سلوكيات الأفراد، وتزويدهم بالمعلومات الضرورية لتمكينهم من أداء فعال ومثمر يؤدي لبلوغ الهدف. كما عرف التدريب في المجال الأمني بأنه إعداد رجال الأمن أو سلطات إنفاذ القانون وتدريبهم على مواجهة الجرائم وذلك لتزويدهم بالخبرات والمهارات الكافية لمكافحة الجريمة [1].

وتتمثل أهمية التدريب في أنه يعد الوسيلة الفعلية والتطبيقية الناجحة والمؤثرة التي تكفل الاستفادة من مهارات وتجارب الأخريين من خلال أشخاص أكفاء مؤهلين وقادرين على نقل هذه التجارب وتلك المهارات بوسائل سهلة ميسرة، كما أنه يعد من ناحية أخرى الوسيلة الملائمة والفعالة لوضع المعارف العلمية موضع التطبيق والتعرف على الأخطاء والسلبيات التي يمكن أن تكشف التطبيق العملي للقوانين والأنظمة واللوائح، ووضع الحلول الكفيلة بتجنبها [2]. وعليه يلعب التدريب دور هام جدا وفعال في مجال مكافحة الجرائم عبر الإنترنت .

فقد اثبت الواقع العملي أن هناك جرائم متعلقة بشبكة الإنترنت قد ارتكبت على مرأى ومسمع من رجال الشرطة بل قام رجال الشرطة بتقديم يد المساعدة للجناة نتيجة لقلة خبرتهم، وكان هذا عند قيام إدارة الشرطة الأمريكية بأمر الشركة المخترقة التوقف عن استخدام أجهزتها الآلية حتى يتاح لهم تعقب واكتشاف حركة الجاني ومراقبته، ونتيجة لذلك

---

[1] – عيسى سليم داود، المرجع السابق، 148

[2] – محمد السيد عرفة، تدريب رجال العدالة و أثره على تحقيق العدالة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2005 ، ص 2

تم إتلاف الملفات والبرامج المقدمة. وذلك عندما طلبت إحدى دوائر الشرطة بالولايات المتحدة الأمريكية من شركة تعرضت للقرصنة أن تتوقف عن تشغيل جهازها الآلي لتتمكن من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة ونتيجة لهذا تم إتلاف البرامج والملفات المسلمة. فإن ظهور هذه الأنماط الجديدة من الجرائم أدى إلى تشكيل عبء ثقيل على عاتق جميع أجهزة العدالة الجنائية سواء رجال الضبط القضائي أو رجال التحقيق أو المحاكم على مختلف درجاتها. خاصة وأن متطلبات العدالة تقتضي أن تتحمل الأجهزة الأمنية الحكومية كامل المسؤولية تجاه اكتشاف كافة الجرائم المرتبطة بالإنترنت للقبض على المجرمين.[1]

وعليه كان من الضروري أن تكون تلك الأجهزة على مختلف أنواعها على درجة كبيرة من الكفاءة والمعرفة والقدرة على كشف غموض تلك الجرائم والتعرف على مرتكبيها. وهذا لن يتحقق إلا بالتدريب، فكفاءة رجال العدالة لمواجهة هذه الظواهر المستحدثة وقدرتهم في التصدي لها يجب أن ترتكز على كيفية تطوير العملية التدريبية، ومن هذا المنطلق كانت الدعوى إلى وجوب تأهيل وتدريب القائمين على هذه الأجهزة. [2]حيث إنه لا يوجد دولة تستطيع مواجهة هذه الأنماط المستحدثة بمفردها دون وجود تعاون وتنسيق مع الدول الأخرى، لذلك كان لازما أن يتم التنسيق والتعاون الدولي في مجال التدريب، ولا يقصد بالتدريب هنا التدريب التقليدي وإنما من الضروري إكسابهم خبرة فنية في مجال الجريمة المعلوماتية. وهذه الخبرة الفنية لا تتأتى دون تدريب تخصصي يراعى فيه العناصر الشخصية للمتدرب من حيث قدرته العلمية والذهنية والنفسية لتلقي التدريب.[3]

وبالرغم من الحاجة إلى تعاون دولي وجهود مشتركة لتفعيله، إلا أنه لا يزال هناك الكثير من الصعوبات والعقبات التي يتعين حلها، وعلى وجه الخصوص:

---

[1] – فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، ط 2016 ، ص 603

[2] –هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة ، ماي 2000 ، المجلد الثاني الطبعة الثالثة، ص 430

[3] –هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، المرجع السابق ،ص 496

–عدم وجود اتفاق عام بين الدول على مفهوم الجرائم المعلوماتية فقد ما تجرمه دولة قد تبيحه دولة أخرى.

– غياب التوافق بين الدول فيما يتعلق بقوانين الإجراءات الجنائية الخاصة بالتحقيق في الجريمة المعلوماتية.

– نقص صارخ في الكفاءة لدى الشرطة والنيابة والقضاء.

– تتسم إجراءات المساعدة المتبادلة بالبطء والتعقيد، وهو ما لا يتوافق مع سرعة تطور الإنترنت وما يرتكبها عبرها من جرائم، وهو ما ينعكس في ملاحقة الجرائم ذات الصلة.

ملخص الباب الثاني

لقد تناولنا في هذا الباب مختلف الآثار المترتبة على العدوان الإجرامي عبر الإنترنت، وآليات مكافحته على المستوى الوطني والدولي.

إن انتشار هذا النوع من الجرائم أدى إلى حدوث خلل عام قد يهدد كافة جوانب الحياة الاقتصادية والاجتماعية والسياسية. فمع تزايد نسبة جرائم غسيل الأموال وجرائم المخدرات عبر الإنترنت وجرائم السرقة والنصب على البنوك والمصارف، لا شك أنها تسببت في خسائر مادية كبيرة وخطيرة أكثر مما تسببه الجرائم التقليدية، ليس فقط على مستوى الفرد فقط بل تتعداه إلى مستوى المنظمات والجهات والمؤسسات وهذا بالطبع يؤثر بشكل سلبي على الاقتصاد في عمومه وكافة قطاعاته، وقد أشارت إحصائيات حول الخسائر الاقتصادية العالمية الناجمة عن جرائم الإنترنت والتي تقدر بالمليارات. والتي تزداد يوم بعد يوم. ناهيك عن المخاطر التي تهدد بأمن وسيادة الدول، بسبب جرائم القرصنة والتجسس وجرائم الإرهاب المتواصلة التي تعرض الجهات والأجهزة الحكومية للخطر، الأمر الذي يؤدي حتما إلى زعزعة الأمن والاستقرار، وبذلك تتحمل الدول المستهدفة خسائر كبيرة.

أما الجرائم الأخلاقية، وجرائم الإساءة بسمعة الأفراد وإظهارهم بصورة غير لائقة أمام المجتمع المحيط بهم، وجرائم انتحال الشخصية وجرائم التهديد والابتزاز خاصة التي تقع على الإناث من خلال الإنترنت، قد أثبتت إحصائيات الحالات الاجتماعية للمجني عليهم الأثر البالغ الخطورة لمثل هذه الجرائم من انتحار وتفكك أسري وضياع للشباب وانتشار للرذيلة بكافة أنواعها.

إن معظم دول العالم والحكومات سعت بكل الطرق القانونيـة المتاحة للحد من الجَرائم الواقعة عبر الإنترنت وآثارها، وعمل المشرع الجزائري على مسايرة المسار التشريعي لأجل البقاء على اتصال بأحدث الحلول التشريعية الخاصة بهذا النوع من الجرائم، خاصة وأن الجزائـر وفي السنوات الأخيرة تعرف تعميما لخدمة الربط بشبكة الإنترنت، ودعم كبيرا للجهات الحكومية بتقنيات المعلوماتية، وهو ما تولد عنه ارتفاع محسوس فـي معدلات

الجريمة عبر الإنترنت، وهذا ما دفع بالمشرع الجزائري إلى التدخل من أجل رسم الخطط القانونية والعملية لتنفيذ سياسة وقائية وردعية ضد الجرائم المعلوماتية، وتجدر الإشارة على أن المشرع الجزائري، قد حاول وضع النصوص التي تعاقب على الأفعال التي تشكل جرائم معلوماتية وكان البداية سنة 2001، المادة 144 مكرر، ومكرر 1 ، ومكرر 2 ، والمادة 146 من قانون العقوبات ثم جاء القانون رقم 15/04 المؤرخ في 2004/11/10 الذي أورد فيه قسما خاصا تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، القسم السابع مكرر من قانون العقوبات ويشمل سبعـــة المادة 394 مكرر إلى المادة 394مكرر 7. ولم يكتف المشرع الجزائري بذلك بل فرض حماية جنائية على الحياة الخاصة للأفراد من خلال القانون 23/06 المؤرخ في 2006/12/20 والذي مس المادة 303 وإقراره بالمادة 303 مكرر إلى 303 مكرر 03، وهذا تصديا للاستخدام السيئ لوسائل التكنولوجيا الحديثة.

إضافة إلي هذا أحكام الدستور الجزائري سنة 1996 الذي كفل في ما سبق حرمة الحياة الخاصة للمواطن من خلال ضمان سرية المراسلات و الاتصالات الخاصة بكل أشكالها، والقانون رقم 18-07 المؤرخ في 10 يونيو2018 الخاص بتحديد قواعد حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي وذلك في إطار احترام الحياة الخاصة للأفراد.

وعموما فإن الجرائم المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري تشمل جريمة الدخول عن طريق الغش إلى النظام الآلي، وجريمة البقاء غير المصرح به في النظام المعلوماتي وأخيرا جريمة إتلاف نظام المعالجة الآلية للمعطيات.

وبالرغم من الجهد في هذا المجال إلا أنه لم يكن كافيا لتفعيل سياسة مكافحة الجرائم المعلوماتية بسبب تعارض أحكام قانون العقوبات وقانون الإجراءات الجزائية وخصوصا مسائل الاختصاص النوعي والإقليمي التي وقفت عائقا في وجه تطبيق النصوص العقابية، مما استدعى تدخل المشرع الجزائري بموجب القانون 06-22 المؤرخ في 2006/12/20 المعدل والمتمم لأحكام قانون الإجراءات الجزائية الجزائري، والذي تناول تعديل وتحديث

نصوص المواد من 45 إلى 47 منه والتي تحدد قواعد الاختصاص النوعي والمحلي ومواعيد إجراء التفتيش بشأن الجرائم المعلوماتية، ومس أيضا التعديل قانون العقوبات بموجب القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص الواردة في هذا القسم من القانون 04-15. وربما يرجع سبب هذا التعديل إلى ازدياد خطورة وانتشار هذا النوع المستحدث من الإجرام باعتباره جريمة تؤثر على الاقتصاد الوطني وعلى المجتمع بالدرجة الأولى.

ولقد صدر بتاريخ 2009/08/05 تحت رقم 09-04 القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الذي يعتبر نموذجا قانونيا خاصا بمكافحة الجرائم المعلوماتية على اعتبار أنه قانون يتضمن نصوصا خاصة، وقد تضمنت الأحكام العامة الخاصة بالعمل بهذا القانون، كأهدافه والمتمثلة أساسا في وضع قواعد خاصة بالوقاية من الجرائم المعلوماتية إضافة إلى تحديد قائمة المصطلحات المفتاحية وتحديد مجال تطبيق أحكامه، وتضمن بيان مفهوم المراقبة الإلكترونية وحدد القواعد الإجرائية لعمليات التفتيش الإلكترونية وكيفية حجز الأدلة الإلكترونية وجملة الالتزامات الملقاة على عاتق مقدمي خدمات الإنترنت في مجال مساعدة السلطات بشأن التحقيقات الجنائية في مادة الجرائم المعلوماتية، وحدد مهام الهيئة الوطنية للوقاية من الجرائم المعلوماتية وحدد قواعد اختصاص القاضي في مجال التعاون الدولي في مسائل البحث والتحقيق في الجرائم المعلوماتية.

إضافة إلى صدور المرسوم الرئاسي رقم 172/19 بتاريخ 2019/07/06 المتضمن تحديد تشكيلة الهيئة الوطنية المكلفة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. وتنظيمها وكيفية سيرها.

وبعدها جاءت مصادقة البرلمان في أفريل 2020 على تعديلات في قانون العقوبات الجزائري، خاصة التي تجرم نشر وترويج أنباء كاذبة باستعمال أي وسيلة بما في ذلك الإنترنت بهدف المساس بالنظام والأمن العموميين.

وواصل المشرع الجزائري جهوده في إطار مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، حيث قام بوضع باب سادس ضمن القواعد الإجرائية العامة يتضمن استحداث قطب جزائي وطني متخصص لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بموجب الأمر 21-11 المؤرخ في 25 أوت 2021 المتمم للأمر 66-156 المتعلق بقانون الإجراءات الجزائية تعزيزا وتكريسا لفكرة التخصص القضائي في مكافحة الجرائم الخطيرة.

وبالرغم من محاولة المشرع الجزائري مواجهة هذا النوع من الجرائم إلا أنه مازالت العديد من الجرائم الواقعة عبر الإنترنت تخضع للقوانين التقليدية ولم يخصها المشرع بقانون قائم بذاته.

وما يعاب على المشرع الجزائري أيضا أنه بالرغم من وضعه لبعض النصوص العقابية الخاصة بالجريمة المعلوماتية إلا أنها تبقى دائما كمادة خام غير قابلة للتطبيق، ذلك أنها تحتاج إلى نصوص إجرائية خاصة تلازمها نظرا لما تمتاز به هذه الجريمة من خصوصية تختلف عن باقي الجرائم، خاصة وأن هذه الجرائم تمتاز بتخطيها لحدود الدول مما أفرز جملة من التحديات القانونية على الصعيد الإجرائي تجسدت في الصعوبات التي تكتنف إثبات هذه الجرائم وقبول الدليل بشأنها باعتبارها لا تترك أثرا ماديا ملموسا، فضلا عن العقبات التي تواجه الأجهزة القضائية والأمنية في سبيل مباشرة بعض الإجراءات عبر الحدود كالمعاينة والتفتيش والضبط في البيئة الافتراضية، إضافة إلى مشكلة تنازع الاختصاص باعتبار أثارها المتجاوزة للحدود، الأمر الذي يحتاج إلى تعاون دولي شامل، وهو الأمر الذي لا يزال محل اهتمام على الصعيدين الوطني والدولي.

وفي إطار الجهود الدولية والإقليمية والتعاون الدولي لمحاربة ظاهرة الجريمة الواقعة عبر الإنترنت باعتبارها جرائم عابرة للحدود ويستدعي مواجهتها وجود كيان دولي يسعى إلى اتخاذ كافة التدابير والإجراءات الضرورية للحد من انتشارها، هناك العديد من الهيئات والمنظمات والمجالس الدولية التي قامت بوضع الإطار القانوني لحماية النظام المعلوماتي

بشكل عام، على رأسها هيئة الأمم المتحدة والمجلس الأوروبي ومجموعة الدول الثمانية...الخ.

وعلى المستوى الإقليمي فقد أصدر مجلس الاتحاد الأوروبي في 23 نوفمبر 2001 اتفاقية بودابست والمتعلقة بمكافحة الجرائم المعلوماتية، والتي تعد من أهم الاتفاقيات التي تعمل على التعاون الدولي في مجال مكافحة الجرائم المعلوماتية. وعليه فإن أهم المبادئ القانونية الدولية المستخدمة في العالم المعاصر لمحاربة هذه الجرائم هو مبدأ التعاون الدولي خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة .

الخاتمة

وفي نهاية هذه الرسالة التي حاولنا فيها دراسة جرائم الإنترنت والمظاهر التي قد تتخذها والآثار الوخيمة المترتبة عنها والآليات المتبعة لمكافحتها على الصعيدين الوطني والدولي. قد توصلنا إلى جملة من النتائج تتمثل في مايلي:

– إن الواقع الذي لا يمكن إنكاره أننا أصبحنا اليوم نعيش عصر تكنولوجيا المعلومات والاتصالات التي باتت هي الأساس الذي يعتمد عليه في معظم المجالات، ولدى جميع المؤسسات، سواء كانت مؤسسات عامة تملكها حكومات الدول أو مؤسسات خاصة يمتلكها الأفراد، فتقنية المعلومات وشبكات الاتصالات هي الأداة الأساسية المستخدمة في إدارة شؤون الدول وتقديم الخدمات وتسهيلها، إضافة إلى الزيادة المتسارعة جدا في أعداد المستخدمين لهذه التكنولوجيا لدرجة أن العالم الافتراضي الذي يعيشه أغلب سكان العالم أصبح جزءا لا يتجزأ من حياتهم اليومية.

– الانتشار الواسع لمواقع التواصل الاجتماعي خلال السنوات الأخيرة وتعدد وتنوع خدماتها لتحقيق مختلف الإشباعات لمستخدميها، وتجاوز الأمر كونه وسيلة للتواصل مع الآخرين في وقت الفراغ، وتحول إلى إدمان حقيقي لا يمكن الاستغناء عنه.

– التطور السريع والمستمر في مجال تقنية المعلومات والاتصالات وشبكة الإنترنت في العالم كله أدى إلى ظهور أنماط جديدة من الجرائم جاءت عن طريق الاستغلال السيّئ للتكنولوجيا، وهي الجرائم المتعلقة بالحاسب الآلي والإنترنت، والتي تتم عن طريق هجمات واختراقات وتسلل داخل النظم المعلوماتية بغرض إما تدمير تلك النظم أو الحصول على معلومات سرية سواء عسكرية أو اقتصادية، أو بقصد إلحاق الضرر بالآخرين، أو من أجل الحصول على منفعة مادية أو معنوية.

–إن جرائم الإنترنت من أكثر الجرائم التي عرفها العالم خطورة ومن ما يزيد من خطورتها سهولة استخدام هذه التقنيات الحديثة إذ يقوم مستخدمها بعمله الإجرامي وهو متواجد في أي مكان، منزله أو مكتبه أو حتى في الشارع، وهذا ما تتميز به الجريمة عبر الإنترنت عن الجريمة التقليدية، كما أنها جرائم عابرة لحدود الدول، مما يجعل تأثيرها كبير جدا بالمقارنة مع الجرائم التقليدية.

– تعددت التسميات التي أطلقت على الجريمة عبر الإنترنت " الجريمة السيبرانية، "الجريمة المتعلقة بالإنترنت"، "جرائم التقنية العالية"." جرائم العالم الإفتراضي"، العدوان الإجرامي باستعمال الإنترنت.

– العدوان الإجرامي عبر الإنترنت من الظواهر الحديثة التي أحاط التعريف بها الكثير من الغموض حيث تعددت الجهود الرامية إلى وضع تعريف محدد لها، وبالرغم من ذلك لم يوضع لها تعريف محدد نتيجة للتطور المستمر في مجال تكنولوجيا المعلومات وشبكة الإنترنت.

- يمكن تعريف العدوان الإجرامي عبر الإنترنت على أنه كل سلوك أو فعل مخالف للقانون يرتكب عبر شبكة الإنترنت وبواسطة الخدمات التي تقدمها.

– تختلف الجرائم المرتكبة عبر الإنترنت عن الجرائم التقليدية من حيث طبيعة وخصائص هذه الجرائم، ومن هذه الخصائص تميزها بأنها جرائم عابرة للحدود وتتسم بالنعومة في ارتكابها وبكون الحاسوب أداة لارتكابها، وترتكب في عالم افتراضي وتنعدم للآثار التقليدية، إضافة إلى ما يميز مرتكبيها من مهارة ومعرفة وذكاء، خاصة الجرائم التي تتطلب مهارة وذكاء معين، ويطلق علي مرتكبيها "مجرمي الإنترنت" أو "مجرمي المعلوماتية".

– اختلاف الجريمة الإلكترونية عن الجريمة عبر الإنترنت، حيث من الممكن ارتكاب جريمة إلكترونية دون الاتصال بشبكة الإنترنت، وذلك باستعمال الحاسوب فقط كتعمد إدخال جهاز USB أو قرص مليء الفيروسات داخل الكمبيوتر من أجل تدمير وتخريب المعلومات المتواجدة به. أما جرائم الإنترنت يشترط لارتكابها الاتصال بشبكة الإنترنت.

– تنامي ظاهرة الجريمة عبر الإنترنت، وازدياد حجم النشاط الإجرامي بشكل مفزع في السنوات الأخيرة.

–تعددت محاولات تصنيف جرائم الإنترنت، إلا أن هذه التصنيفات قد صنفت جرائم الحاسوب وجرائم الحاسوب والإنترنت معا، ولم تقدم تصنيفا خاصا بجرائم شبكة الإنترنت.

– تم اعتماد السبيل الأمثل لمعالجة الاختلاف في التقسيمات من الإطار الأوسع لارتكاب هذه الجرائم دون التضييق منها أو حسرها في معيار واحد، والأخذ بالتقسيم التقليدي للجريمة والذي تبناه الكثير من الباحثين.

– بعد ما أصبحت التكنولوجيا الآن تتدخل في كل شي أصبح من السهل القيام بجرائم القتل والتحريض على القتل من خلالها. وجريمة القتل من الجرائم التي كانت في كثير من الأذهان جريمة يستحيل وقوعها عبر الإنترنت.

– حصد الإنترنت أرواح الآلاف من المراهقين حول العالم بسبب ألعاب الموت التي تحرضهم على الانتحار، وكان من أشهر هذه اللعب الحوت الأزرق.

– تعد جرائم السب والقذف والتشهير والابتزاز الواقعة عبر الإنترنت من الجرائم الأكثر انتشارا خاصة بعد ظهور الإنترنت، إضافة إلى أنها من الجرائم التي تترك أثر بالغ الخطورة في أنفس المجني عليهم، وغايتها هي للنيل من شرف الغير أو كرامتهم أو اعتبارهم واحتقارهم، ناهيك عن تسببها في حصد أرواح الكثير من الأشخاص بانتحارهم هروبا من العار خاصة فئة النساء والمراهقين .

– أصبحت شبكة الإنترنت في وقتنا الحالي من الوسائل الأكثر ترويجا للجرائم الماسة بالأخلاق والآداب العامة كتسهيل إدارة مشاريع القمار على الإنترنت، واستخدام شبكات الإنترنت لترويج للدعارة، بنشرهم للإباحية الجنسية بشتى الوسائل من صور وفيديوهات وحوارات، تعد أخطر هذه الجرائم جريمة استغلال الأطفال جنسيا.

–الجرائم الجنسية عبر الإنترنت التي تطال الأطفال قد تؤدي إلى تشويه الدافع الجنسي الفطري والطبيعي لدى الطفل، والانحراف به نحو حضيض الشذوذ الذي انتشر بطريقة مروعة في وقتنا الحالي ونتيجة له انتشار المتحولين والزواج المثلي.

– الجرائم المرتكبة عبر الإنترنت سببا من أسباب الفساد والتفكك الأسري، وفساد الأخلاق والانحطاط الثقافي وتراجع القيم الأخلاقية، وسببا في إدمان المواقع الإباحية.

– أضحت الإنترنت قناة اتصال ممتازة ومجالاً رحباً للتعامل غير المشروع لمستهلكي المخدرات والمؤثرات العقلية بشكل أكثر أمناً للمروج والمدمن أو المعتمد على المخدرات والمؤثرات العقلية، وأصبحت فضاء لترويج نوع جديد من المخدرات والتي يطلق عليها المخدرات الرقمية.

– إن انتشار الجريمة عبر الشبكة العنكبوتية قد أدي إلى تأثيرات سلبية تهدد المجتمع بأكمله في اقتصاده وسيادته وأمنه الوطني.

-إن الجـرائم عبـر الإنترنـت مثـل الاحتيـال وغسـيل الأمـوال والقرصـنة والتجسـس وجـرائم الإرهاب المتواصلة قد تعرض الاقتصاد والأجهزة الحكومية للخطر، الأمر الذي يؤدي حتما إلى تهديد الأمن الاجتماعي والاقتصادي وتزعزع استقرار المجتمعات، وبذلك تتحمل الدول المستهدفة خسائر كبيرة.

- تكبد الجرائم السيبرانية الاقتصاد العالمي مبالغ ضخمة سنويا.

- إن الأموال لم تعد تلك العملات المعدنية والورقية التي عرفناها منذ زمن بعيد، فقد أصبحت الأموال عبارة عن قيمة مالية مخزنة في بطاقات تقرأها الآلة تارة، و تخزن على القرص الصلب للحاسب تارة أخرى، أما طرق الاعتداء فلم تعد بالاختلاس الذي يتمثل في إنهاء مادي لحيازة المجني علية سواء تم ذلك بوسائل احتيالية أو خلسة دون رضائه، بل أصبح الاعتداء يتم بطرق مستحدثة مثل الاختراق وفك الشفرات المختلفة للوصول إلى أرقام بطاقات الصرف والائتمان، أو عن طريق إعداد برامج خاصة لتنفيذ عملية الاختلاس أي أن إنهاء الحيازة تتم عبر الإنترنت، وهي عملية تتم بعيدا عن موقع الجريمة.

- لقد سهلت شبكة الإنترنت من فرص التأثير على معتقدات وتقاليد مجتمعات بأكملها، مما يجعلها عرضة للهزيمة الفكرية والأمراض والصراعات الطائفية، الأمر الذي يسهل من انتشار كل أنواع الفوضى.

- أصبحت الإنترنت وسيلة تستغلها المنظمات الإرهابية لبثّ أفكارهم المسمومة وترويجها ولتجنيد أفراد جدد وتمويلهم .

- من الجرائم التي تهدف إلى المساس بالنظام والأمن العموميين الشائعات ونشر وترويج الأخبار الكاذبة عبر الإنترنت، فالإشاعات يكون غرضها زعزعة المجتمع وزعزعة أمنه واستقراره. فانتشار الإشاعات الإلكترونية لم تعد مجرد أخبار كاذبة أو معلومات خاطئة يلقيها شخص معين، بل أصبحت جريمة يقف خلفها مؤسسات متخصصة احترفت التلاعب بالمعلومات بهدف زعزعة أمن واستقرار الدولة.

- في ضل الأزمة الصحية التي مست العالم بانتشار فيروس كوفيد 19 الذي كان من نتائجه انفتاح كل العالم على الإنترنت لكونها أصبحت الوسيلة الوحيدة للاتصال بالعالم الخارجي، عرفت الجريمة عبر الإنترنت تفشيا وارتفاع كبير في معدلاتها، خاصة الجرائم المستهدفة للأموال والأمن الوطني مثل جريمة الاحتيال عبر الإنترنت والسرقة والتزوير

والقرصنة، ولقد شهدت بعض الدول المصابة بالفيروس موجة من جرائم الاحتيال والنصب من بينها الجزائر، إضافة إلى إنتشار الشائعات ونشر وترويج الأخبار الكاذبة عبر مواقع التواصل الاجتماعي، والتي كان غرضها زعزعة المجتمع وزعزعة أمنه واستقراره. وهذا ما هو إلا دليل على أنه كلما ارتفع عدد مستخدمي الإنترنت يرتفع معه عدد الجرائم المرتكبة عبرها.

– كشفت الجرائم المرتكبة عبر الإنترنت القصور التشريعي العالمي للنصوص القانونية وإثارتها لخلاف حول من يدعو إلى تعديل القوانين التقليدية لتشمل الجرائم المعلوماتية، وحول من ينادي لضرورة تكريس تشريعات خاصة بهذه الجرائم.

– توجه العديد من الدول والحكومات للاهتمام بظاهرة الجريمة عبر الإنترنت خاصة الغربية منها، ويتجلى ذلك من خلال التحديثات المتتالية للنصوص العقابية والإجرائية.

– لم تبقى الجزائر بمعزل عن بقية الدول، حيث حاولت العمل على تطوير منظومتها القانونية بشكل يساير التطور في مجال تقنية المعلومات، إذ قام المشرع الجزائري بضمان حماية برامج الحاسب الآلي وإنفاذ قوانين الملكية الفكرية بموجب الأمر 03-05 الصادر في 2003/07/19 والمتعلق بحقوق المؤلف والحقوق المجاورة. فضلا عن تداركه ولو نسبيا للفراغ القانوني في مجال الجرائم المعلوماتية وذلك باستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون04-15 المؤرخ في 2004/11/10 المعدل والمتمم للأمر 66-156 المؤرخ في 1966/06/08 المتضمن قانون العقوبات، ويشمل المواد394 إلى 394 مكرر7 والذي تم خلاله إقرار واستحداث قسم خاص معنون بقسم جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

- صدور عدة قوانين خاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. من خلال القانون رقم 09-04 المؤرخ في 2009/08/05 ، ثم تلاه صدور المرسوم الرئاسي رقم 172/19 بتاريخ 2019/07/06 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. حيث تم إرساء قواعد جديدة تتضمن تحكما جيدا في أساليب مكافحة هذا النوع من الجرائم.

– تمت مصادقة البرلمان في أفريل 2020 على تعديلات في قانون العقوبات الجزائري، خاصة التي تجرم نشر وترويج أنباء كاذبة بهدف المساس بالنظام والأمن العموميين، المادة 196 من القانون رقم 20–06 المؤرخ في 28 أفريل 2020 المعدل والمتمم للأمر رقم 66–156 المؤرخ في 08 يونيو 1966 والمتضمن لقانون ع ج، الجريدة الرسمية الصادرة في 29 افريل 2020 عدد25.

– وضع باب سادس ضمن القواعد الإجرائية العامة يتضمن استحداث قطب جزائي وطني متخصص لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بموجب الأمر 21–11 المؤرخ في 25 أوت 2021 المتمم للأمر 66–156 المتعلق بقانون الإجراءات الجزائية .

– من خلال هذه الدراسة ظهر قصورا واضحا في التشريع الجزائري من الناحية الموضوعية والإجرائية في مواجهة ظاهرة الجريمة الواقعة عبر الإنترنت، حيث لا يزال العديد من هذه الجرائم خاضعا للنصوص التقليدية، ومن هذه الجرائم نذكر الجرائم الماسة بالشرف والجرائم المخلة بالآداب وجريمة السرقة والاحتيال، وهذا ما يترتب عليه الاعتداء على مبدأ الشرعية من جهة أو إفلات الكثير من الجناة من العقاب.

– بالرغم من محاولة المشرع الجزائري لمواجهة هذه الجريمة إلا أنه لم يخصها بقانون قائم بذاته. وبمعنى أخر لا تشكل الإنترنت موضوع لتشريع مستقل في الجزائر.

– يرى العديد من المختصين الجزائريين أن سبب انتشار هذا النوع من الجرائم الحديثة العهد في الجزائر راجعا إلى وجود فراغ قانوني لمعالجتها.

– الدولة لا تستطيع بجهودها المنفردة القضاء على الجريمة المعلوماتية خاصة مع التطور المذهل في تكنولوجيا المعلومات، على أساس أنها أصبحت عابرة للحدود الوطنية تتطلب عملا منسقا ومتماسكا على كل الأصعدة. وقد أصبح التعاون الدولي ضرورة ملحة. فأجهزة تنفيذ القانون لا تستطيع تجاوز حدودها الإقليمية لممارسة الأعمال القضائية على المجرمين الفارين من حدودها إلى أقاليم دول أخرى ذات سيادة، لذلك لابد من التعاون بين الدول لاتخاذ الإجراءات القضائية فوق أقاليمها.

– التعاون الدولي لمواجهة الجرائم المعلوماتية يتم بالدخول في اتفاقيات ومعاهدات تجرم صور هذه الجرائم كلها وتبين كذلك الاختصاص المكاني وكيفية تسليم مجرمي المعلوماتية،

كما يمكن أن تنص هذه الاتفاقيات على تبادل الخبرات والمعلومات في المسائل المتعلقة بالجرائم المعلوماتية.

– تنوع واختلاف النظم القانونية والإجرائية من دولة إلى أخرى من حيث طرق التحري والتحقيق ومدى قانونية ومشروعية الإجراءات الجنائية من دولة إلى أخرى، فما يعتبر إجراء مشروع في دولة قد يعتبر غير مشروع في دولة أخرى. فمشكلة الاختصاص القضائي قد يحد من التعاون الدولي، حيث إن اختلاف التشريعات والنظم القانونية ينتج عنه تنازع في الاختصاص القضائي بين الدول مما يعوق التعاون الدولي.

– إن آلية تنفيذ المساعدات القضائية الدولية آلية تتم عن طريق دبلوماسي يتميز بالبطء والتعقيد الذي يتعارض مع طبيعة الجريمة السيبرانية والإنترنت التي تتميز بالسرعة.

وعلى ضوء هذه النتائـــــج توصلنا إلى مجموعة من التوصيـــات :

– العمل على إعطاء تعريف دقيق للجرائم المرتكبة عبر الإنترنت.

– اعتماد تصنيف دقيق جامع لكل الجرائم المرتكبة عبر الإنترنت.

– على المشرع الجزائري الالتزام بسن قانون جديد مستقل لمواجهة ظاهرة الإجرام المعلوماتي، ويتضمن كافة الآليات الموضوعية والإجرائية المتعلقة بجميع الجرائم الواقعة عبر الإنترنت، والهدف من ذلك تأمين حماية فعالة للحياة الشخصية من كافة نواحيها.

– أهمية الحد من ضرر الجريمة عبر الإنترنت من خلال عقوبات متناسبة ورادعة وتعويضات كافية لجبر الضرر. وتشديد العقوبة إذا كان الضحية قاصرا.

– على الدولة أن تعمل على تبني جهازاً خاصاً للخبرة الجنائية للجريمة المعلوماتية، يتكون أعضاؤه من فريق متخصص فنياً في التقنية المعلوماتية، وأن يتم إعادة النظر في القواعد الموجودة، لأن إثبات الجريمة المعلوماتية يتطلب المزيد من القواعد الجديدة الخاصة للتعامل مع الأدلة في هذه الجرائم، لأن البحث عنها يتم داخل نظام اليكتروني معقد.

– ضرورة عقد ندوات علمية ومؤتمرات حول الجرائم المعلوماتية والقانون، من أجل رفع مستوى الكفاءة المعلوماتية في القطاع الوظيفي للدولة، ولإنشاء دورات تدريبية مستمرة للقضاة ورجال النيابة العامة ولرجال الشرطة، لرفع مستوى الكفاءة لديهم في استخدام التقنية المعلوماتية. وإجراء مسابقات وطنية لاقتناء كوادر من الفنيين والتقنيين الذين يمتلكون الخبرة والمهارة العالية في المجال السيبراني "الهاكر" والاستفادة منهم في مجال الجريمة المعلوماتية.

– ضرورة التعاون الدولي لمكافحة الجرائم عبر الإنترنت من خلال إنشاء وحدات متخصصة على المستوى الدولي والعربي، تهتم بالتنسيق بين الدول في مجال متابعة ومعاقبة مرتكبي هذه الجرائم .

– إنشاء لجنة وطنية على غرار اللجنة الوطنية للمعلومات والحريات في فرنسا تتولى دراسة ظاهرة الإجرام المعلوماتي بكافة جوانبه. وتعمل على صياغة التعديلات التشريعية اللازمة، ونشر التوعية اللازمة لمستخدمي النظام المعلوماتي بفوائد ومخاطر التعامل عبر الشبكة العالمية.

– على الدول العربية عقد اتفاقيات دولية وإقليمية وعربية مكثفة للتعاون على مكافحة الجرائم عبر الإنترنت على المستوى التشريعي، ومن أجل تعاون أجهزة الشرطة في ما بينها لتبادل المهارات والتقنيات اللازمة لاكتشاف وملاحقة ومتابعة المتهمين بارتكاب الجريمة عبر الإنترنت.

– الاستفادة من تجارب وخبرات الدول المتطورة في مجال مكافحة الجرائم عبر الإنترنت والعمل على استعمال الآليات الوقائية الإجرائية قبل وقوع الجريمة، خاصة عندما يتعلق الأمر ببعض الجرائم عبر الإنترنت التي تهدد أمن الدولة مثل الإرهاب الإلكتروني أو التجسس الإلكتروني .

– تفعيل دور المجتمع المدني خاصة الجمعيات للقيام بدورها في توعية ووقاية الشباب من الوقوع في الممارسات الخاطئة عبر شبكة الإنترنت.

– ضرورة نشر الوعي الرقمي بين المستخدمين داخل المؤسسات التعليمية، وكيفية تفادي التعدي على بياناتهم الشخصية وتعريفهم بحجم الخطورة التي ترصدهم في حالة عدم اتخاذ الاحتياطات اللازمة.

– ضرورة نشر الوعي بين صفوف المواطنين خاصة المراهقين منهم والشباب، وتحذيرهم من المخاطر النفسية والاجتماعية، الناجمة عن الاستعمال الغير آمن للإنترنت، وتكثيف التوعية عن الآثار السلبية الصحية المترتبة عن الممارسات الجنسية الشاذة.

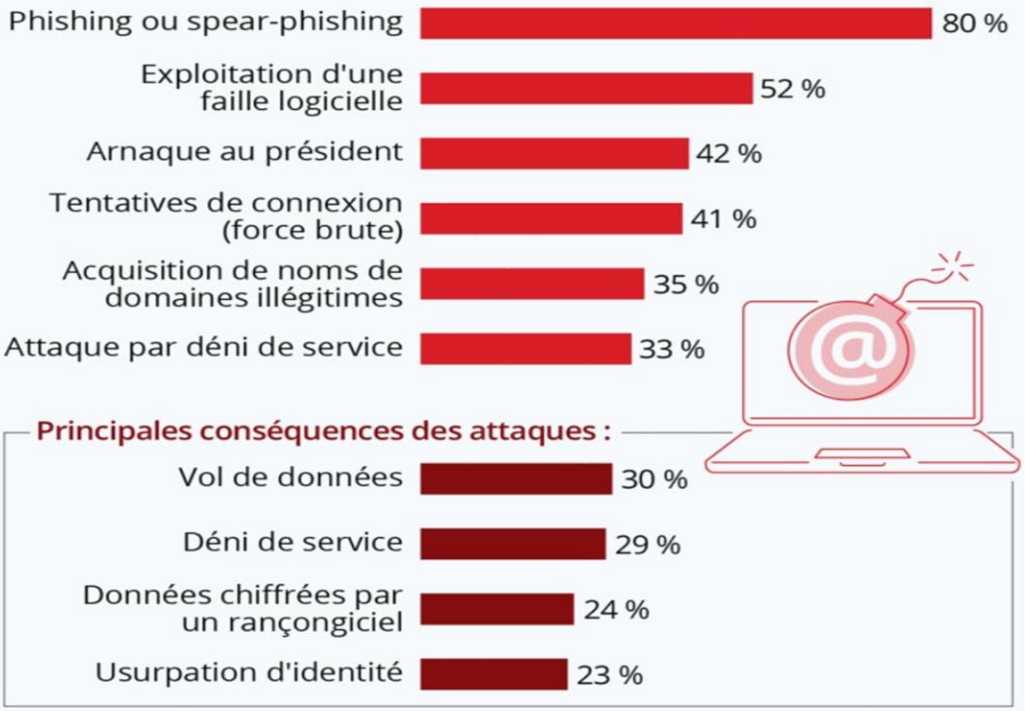
– نشر الإحصائيات والأرقام المتعلقة بالجرائم المعلوماتية لتحفيز المزيد من الحذر من الاستخدام الخاطئ لوسائل التواصل الاجتماعي.

– تكثيف الحملات الإعلامية الخاصة بموضوع الجريمة عبر الإنترنت، وبث برامج توعية موجهة للأسرة. وتحذير الأب والأم من مخاطـــر الحاســـــوب والإنتـرنت على أطفالهم. فنتيجة لقلة وعيهم وعدم تميزهم بين الصح والخطأ، فإن الخطر الذي يواجهه الأطفال يزداد يوما بعد يوم.

الملاحق

Les cyberattaques les plus courantes contre les entreprises

Types d'attaques les plus courants constatés par les entreprises françaises en 2020 *

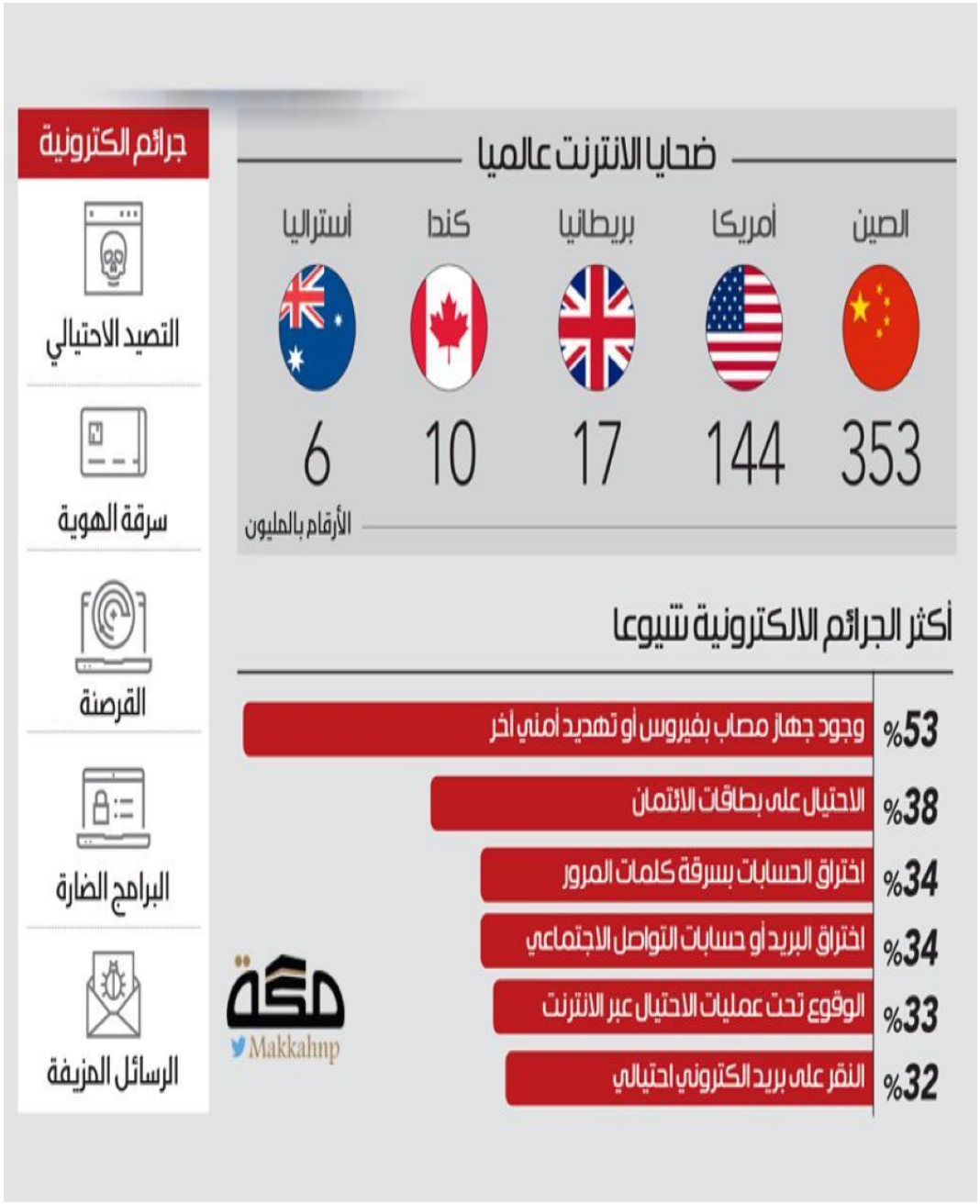


* Plusieurs réponses possibles, sélection des plus fréquentes. Les entreprises ciblées ayant répondu à l'enquête ont subi en moyenne 3,6 attaques et 2,3 conséquences.

Sources : CESIN, OpinionWay

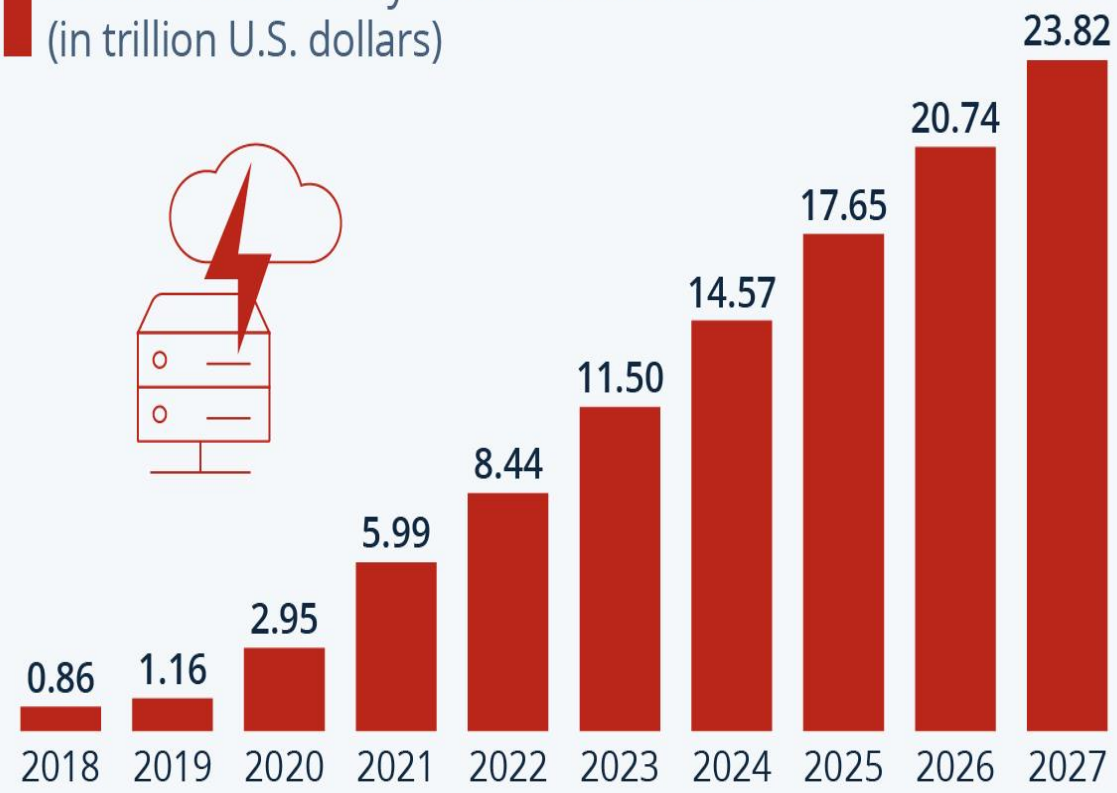

تقديرات خسائر الجرائم الإلكترونية سنوياً حتى عام 2028
التكلفة التقديرية للجرائم الإلكترونية في جميع أنحاء العالم (تريليون دولار أميركي)
تريليون دولار أميركي
25
20
15
10
5
0
22.82
20.74
17.65
14.57
11.50
8.44
5.99
2.95
1.16
0.86
2027
2026
2025
2024
2023
2022
2021
2020
2019
2018


تقديرات خسائر الجرائم الإلكترونية سنوياً حتى عام 2028
22.82
20.74
17.65
14.57
11.50
8.44
5.99
2.95
1.16
0.86
2027
2026
2025
2024
2023
2022
2021
2020
2019
2018


جرائم الكترونية
التصيد الاحتيالي
سرقة الهوية
القرصنة
البرامج الضارة
الرسائل المزيفة
ضحايا الانترنت عالميا
الصين
أمريكا
بريطانيا
كندا
أستراليا
353
144
17
10
6
الأرقام بالمليون
أكثر الجرائم الالكترونية شيوعا
53% وجود جهاز مصاب بفيروس أو تهديد أمني آخر
38% الاحتيال على بطاقات الائتمان
34% اختراق الحسابات بسرقة كلمات المرور
34% اختراق البريد أو حسابات التواصل الاجتماعي
33% الوقوع تحت عمليات الاحتيال عبر الانترنت
32% النقر على بريد الكتروني احتيالي
مكة
Makkahnp

Cybercrime Expected To Skyrocket in the Coming Years

Estimated cost of cybercrime worldwide
(in trillion U.S. dollars)



As of November 2022. Data shown is using current exchange rates.

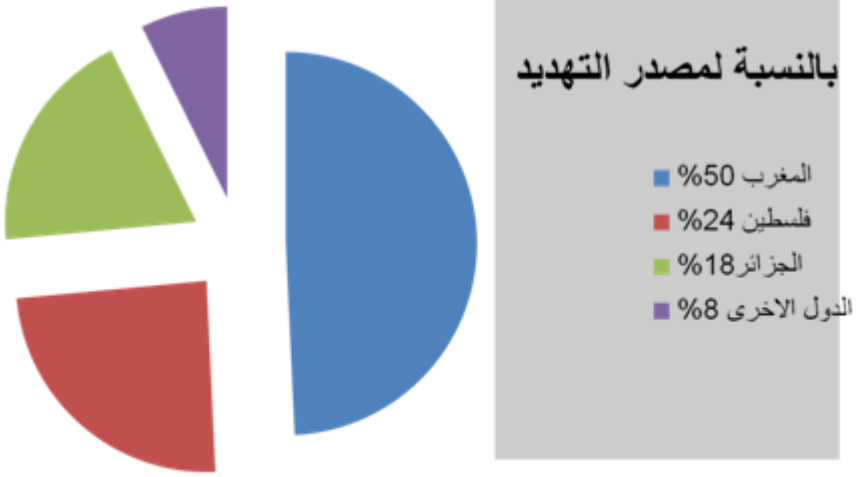
Sources: Statista Technology Market Outlook,
National Cyber Security Organizations, FBI, IMF

التقرير العام
للجريمة الالكترونية

بالعالم العربي مابين سنة

2014 و 2018

إحصائيات

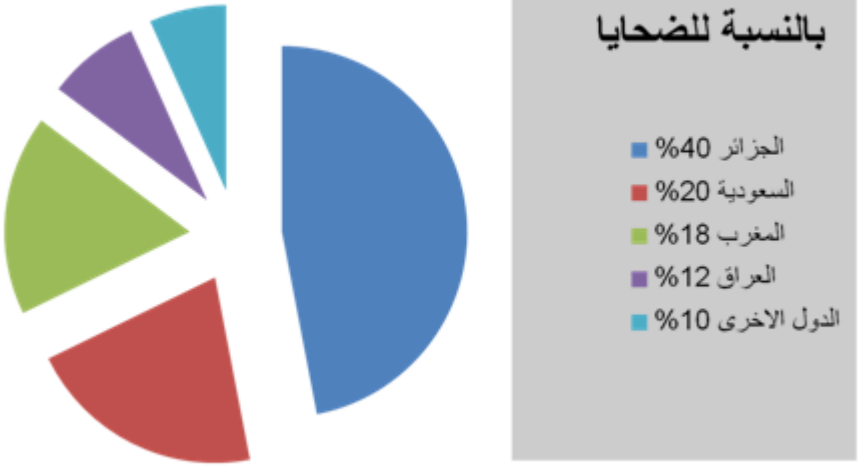


التقرير العام
للجريمة الالكترونية

بالعالم العربي مابين سنة

2014 و 2018

إحصائيات



نسخة عادية

الجمهورية الجزائرية الديمقراطية الشعبية

باسم الشعب الجزائري

حكم

21/01748
22/00274
22/03/09

بالجلسة العلنية المنعقدة بمقر محكمة **ششار**
بتاريخ: **التاسع من شهر مارس سنة ألفين و إثنان وعشرون**
النظر في قضايا الجنح
برئاسة السيد (ة): [redacted] رئيسا
وبمساعدة السيد(ة): [redacted] أمين ضبط
وبحضور السيد(ة): [redacted] و كيل الجمهورية

صدر الحكم الجزائي الأتي بيانه بين الأطراف التالية
السيد وكيل الجمهورية_ مدعيا باسم الحق العام.
من جهة

و /

1): [redacted] ضحية حاضر
من مواليد: [redacted] بـ: ششار
إبن: [redacted] و [redacted] متزوج -ة
الساكن : حي [redacted]

بمساعدة الأستاذ(ة): [redacted]

2): [redacted] ضحية حاضر
من مواليد: [redacted] بـ: [redacted]
إبن: [redacted] متزوج -ة
الساكن : [redacted]

بمساعدة الأستاذ(ة): **كواشي فاروق**

من جهة ثانية

ضد /

1): [redacted] متهم حاضر
من مواليد: [redacted] بـ: خنشلة
إبن: [redacted] و [redacted]
الساكن : [redacted] الرشيد ششار

من جهة اخرى

بيان وقائع الدعوى

حيث أن المنهم [redacted] متابع هذا على انه منذ مدة لم يدركها التقادم القانوني بعد بدائرة الاختصاص الإقليمي لمحكمة ششار مجلس قضاء خنشلة لارتكابه جنحة القذف الفعل

المنصوص و المعاقب عليهما بالمادة 298 من قانون العقوبات
- أحيل المتهم على محكمة الجنح وفقا لإجراءات الاستدعاء المباشر الصادر عن وكيل الجمهورية عملا بنص المواد 333 و 335 من قانون الإجراءات الجزائية لتتم محاكمته طبقا للقانون
تتلخص الوقائع في انه بتاريخ 19/08/2020 تقدم المدعو [redacted] بشكوى امام وكيل الجمهورية مفادها تعرضه للقذف عبر مواقع التواصل الاجتماعي بصفحة ششار [redacted] متهما اياه بات تاريخه وسخ وانه لص وابن خامج رغم انه شهيد ضحى على تحرير هذا البلد وعمل بكل اخلاص وتفاني ببلدية ششار لمدة 45 كمتصرف اداري ولم يرتكب اي خطأ. وبفتح تحقيق تم سماع الشاكي اكد ما جاء به في شكواه وباستكمال اجراءات التحقيق لمعرفة هوية صاحب الصفحة تبين انه تم الولوج الى الصفحة بالرقم الهاتفي الثابت والمسجل باسم [redacted].
حيث ان المتهم حضر لجلسة المحاكمة وصرح بعد التأكد من هويته ومواجهته بالتهمة المنسوبة اليه انه ينكر ما نسب اليه وان صفحة ششار [redacted] ليست ملك له.
حيث أن الضحية [redacted] حضر جلسة المحاكمة وصرح انه تعرض للقذف بصفحة ششار [redacted] وان المتهم لا يعرفه وليست له أي علاقة به مؤكدا ما جاء به من تصريحات امام الضبطية القضائية
حيث ان الضحية [redacted] تغيب عن جلسة المحاكمة.
حيث ان دفاع الضحيتين الاستاذ [redacted] رافع بثبوت الوقائع والاركان ملتمسا تعويض قدره 50 مليون سنتيم لكل واحد منهما.
حيث أن وكيل الجمهورية إلتمس 06 اشهر حبس نافذ و100.000دج غرامة نافذة
- حيث أن الكلمة الأخيرة أعطيت للمتهم طبقا لنص المادة353 فقرة03 من قانون الإجراءات الجزائية وكانت البراءة.
حيث وضعت القضية للنظر لجلسة 09/03/2022 للنطق بالحكم الاتي بيانه

وعليه فإن المحكمة

بعد الإطلاع على المواد 335-368- من قانون الإجراءات الجزائية
بعد الإطلاع على محاضر الضبطية القضائية
بعد النظر قانونا.
في الدعوى العمومية:
حيث أن المادة 296 من قانون العقوبات عرفت جنحة القذف على أنها كل ادعاء بواقعة من شأنها المساس بشرف أو اعتبار الأشخاص أو الهيئات المدعى عليها بها أو اسنادها إليهم أو إلى تلك الهيئة و يعاقب على نشر هذا الإدعاء أو ذلك الإسناد مباشرة أو بطريقة إعادة النشر حتى ولو تم ذلك على وجه التشكيك أو إذا قصد به شخص أو هيئة دون ذكر الاسم و لكن كان من الممكن تحديدهما من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الإعلانات موضوع الجريمة
حيث و الحال كذلك فإن أركان جريمة القذف هي الإدعاء بواقعة شائنة أو إسنادها للغير على أن يكون ذلك علنيا و بقصد من الفاعل.
حيث ثبت للمحكمة من خلال أوراق الملف، اين تبين ان العبارات التي تمت كتابتها من قبل المتهم والتي تمس شرف واعتبار الضحيتين قد كانت ضمن منشورات بموقع التواصل الاجتماعي بالصفحة المسماة ششار [redacted] وانه بعد التحقيق الالكتروني تبين انها باسم المتهم وتتسم بالعلنية لكونها موجهة للعامة وعليه فإن ركن العلنية مما يجعل من جنحة القذف قائمة في مواجهة المتهم طبقا لنص المادة 296 من قانون العقوبات ويتعين معه ادانة المتهم ومعاقبته وفقا للقانون.
عن الدعوى المدنية:
حيث أن الضحيتين أعلنا تأسيسهما كطرفين مدنيين بالجلسة عن طريق دفاعهما ملتمسين تعويض قدره 500.000 دج لكل واحد منهما عن الأضرار اللاحقة بهما.

1 / في الشكل: حيث أن تأسيس الضحية كطرفين مدنيين جاء طبقا للاوضاع و الشروط المنوه عنها قانونا بالمواد 02،03،239،241 من قانون الإجراءات الجزائية، مما يتعين قبوله شكلا.
2/ في الموضوع:
حيث أن طلب الطرفين المدنيين الراميين إلى تعويضهما مؤسس قانونا طبقا لنص المادة 124 من القانون المدني بنظر الضرر الحاصل بفعل المحكوم عليه من جراء واقعة القذف الذي أدى إلى إحداث أضرار في نفس الضحيتين ، مما يتعين الاستجابة لهما، إلا أن المبلغ المطالب به هو مبلغ مبالغ فيه مما يتعين على المحكمة رده إلى حده المعقول والمتناسب مع الضرر اللاحق بالضحيتين.
- حيث أن المصاريف القضائية تقع على عاتق المتهم المدان طبقا لأحكام المادة 367 من قانون الإجراءات الجزائية والمقدرة ب800دج وكذا مصاريف التبليغ عن طريق المحضر القضائي والمقدرة 3000دج دج وفقا لكشف المصاريف المرفق بالملف.

ولهـذه الأسـباب

حكمت المحكمة حال فصلها في قضايا الجنح علنيا ابتدائيا حضوريا وجاهيا للمتهم وحضوري للضحيتين:
في الدعوى العمومية: ادانة المتهم [redacted] بجنحة القذف الفعل المنصوص والمعاقب عليه بالمادة 298 من قانون العقوبات وعقابا له الحكم عليه ب04 اشهر حبس نافذ وخمسين ألف دينار جزائري (50.000 دج) غرامة نافذة.
في الدعوى المدنية:
في الشكل: قبول تأسيس الضحيتين [redacted] كطرفين مدنيين.
في الموضوع: الزام المتهم المدان بأن يدفع للطرفين المدنيين لكل واحد منهما مبلغ 100.000دج (مائة الف دج) تعويضا لهما.
مع تحميل المتهم المدان بالمصاريف القضائية المقدرة بـ 800 دج (ثمانمائة دج) ومبلغ 3000 دج (ثلاثة الاف دج) مصاريف التبليغ مع تحديد مدة الاكراه البدني بحدها الاقصى.
بذا صدر الحكم وأفصح به جهارا بالجلسة العلانية بالتاريخ المذكور أعلاه ووقع أصل الحكم من طرفنا نحن الرئيس وأمين الضبط

الرئيس (ة)

أمين الضبط

قائمة المصادر والمراجع

المصادر والمراجع باللغة العربية

المصـــــادر

*** المعاجم والقواميس:**

– ابن منظور أبو الفضل جمال الدين محمد بن مكرم ، لسان العرب ، دار صادر ، بيروت

– أحمد مختار عمر، معجم اللغة العربية المعاصرة، عالم الكتب، القاهرة مجلد 1، طبعة 1، 2008

– جبران مسعود، الرائد معجم لغوي عصري، دار العلم للملاين ، مجلد واحد، طبعة 7، 1992

– المعجم الوجيز، ص392 مجمع اللغة العربية، طبعة خاصة بوزارة التربية والتعليم، 2003

*** الدساتير**

– دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 1966 المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية رقم 76 المؤرخة في 8/ 12/ 1996

*** الاتفاقيات**

– اتفاقية بوداباست لمكافحة الجرائم المعلوماتية ، المنبثقة عن اجتماع المجلس الأوروبي ببوداباست، المجر، تحت رقم 185 ، بتاريخ 21 نوفمبر 2001

***القوانين**

– القانون رقم 03-2000 المؤرخ في 2000/08/05 المحدد للقواعد المتعلقة بالبريد والمواصلات السلكية واللاسلكية في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية رقم 48 ، الصادرة بتاريخ2000/08/06

– القانون رقم 15/04 المؤرخ في 2004/11/10 المعدل والمتمم للأمر 66-156 المؤرخ في 1966/06/08 المتضمن لقانون العقوبات الجزائري

– القانون رقم 04 / 18 المؤرخ في 25 ديسمبر 2004 المتعلق بالوقاية من المخدرات والتجارة بها، المؤرخة في 26 ديسمبر 2004

– القانون رقم 09–04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنشور في الجريدة الرسمية للجمهورية الجزائرية رقم 47 الصادرة بتاريخ 16 أوت 2009.

– القانون رقم 15–04 المؤرخ في 11 ربيع الثاني من عام 1436 الموافق لـ 1 فبراير سنة 2015 المتعلق بقواعد العامة للتوقيع والتصديق الالكتروني، جريدة الرسمية ، عدد 06.

– القانون رقم 16 – 01 المؤرخ في 6 مارس 2016 المتضمن التعديل الدستوري، الجريدة الرسمية العدد 14 ، الصادرة في 07 مارس 2016

– القانون رقم 20–06 المؤرخ في 28 أفريل 2020 المعدل والمتمم للأمر رقم 66–156 المؤرخ في 08 يونيو 1966 والمتضمن لقانون العقوبات الجزائري، الجريدة الرسمية الصادرة في 29 افريل 2020، عدد25.

*** الأوامر**

– الأمر 66/ 156 المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات الجزائري المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية العدد رقم 49 الصادرة في 11جوان 1966

– الأمر 05/03 المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية، عدد 44 ، صادرة بتاريخ 2003/07/23

– الأمر 21–11 المؤرخ في 25 أوت 2021 المتمم للأمر 66–156 1المتعلق بقانون الإجراءات الجزائية .

*** المراسيم التشريعية**

–المرسوم التنفيذي رقم 09–410 المؤرخ في 23 ذي الحجة عام 1430هـ الموافق لـ 10 ديسمبر 2009 يحدد قواعد الأمن على النشاطات المنصبة على التجهيزات الحساسة ، الجريدة الرسمية، العدد73

*** المراسيم الرئاسية**

– المرسوم الرئاسي رقم 15–261 المؤرخ في 08 أكتوبر 2015 والمتضمن تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام

والاتصال ومكافحتها، المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية رقم 53 الصادر بتاريخ 2015/10/08

المراجع

1: الكتب:

أ: المراجع العامة:

- إبراهيم كمال إبراهيم ، الضوابط الشرعية والقانونية لحماية حق الإنسان في اتصالاته الشخصية، بلا طبعة ، دار الكتب القانونية ، مصر ، 2010
- إبراهيم نشأت، القواعد العامة في قانون العقوبات المقارن، د ط، دار الجامعية للطباعة و النشر، بغداد، د س ن.
- إبراهيم عيد نابل ، الحماية الجنائية لعرض الطفل من الاعتداء الجنسي ، دراسة مقارنة بين قانون العقوبات الفرنسي والمصري، دار النهضة العربية، طبعة 1، 2001
- أحسن بوسقيعة، الوجيز في القانون الجنائي الخاص، ج 1، دار هومه للطباعة والنشر والتوزيع ،الجزائر، 2008
- أحمد فتحي سرور ، الوسيط في قانون العقوبات، القسم الخاص، طبعة 3 ، سنه 1992
- أحمد مختار عمر، معجم اللغة العربية المعاصرة، عالم الكتب، القاهرة، مجلد 1، طبعة 1 ، 2008
- أحمد إبراهيم مصطفى سليمان ، الإرهاب والجريمة المنظمة ، مطبعة العشري ، القاهرة ، 2006
- ادوار غالي الذهبي، الجرائم الجنسية ، دار غريب للنشر ،القاهرة , طبعة 3، 2006
- أكرم ابراهيم نشأت، القواعد العامة في قانون العقوبات المقارن ، دار الجامعية للطباعة و النشر، بغداد، 1998

- أندريه لوك ، معالجة المعلومات القانونية في القرن الحادي والعشرين وتحدياتها، الجامعة اللبنانية، مركز الأبحاث والدراسات في المعلومات القانونية ، منشورات صادر ، بيروت ، 2002
- إسحاق إبراهيم منصور ، شرح قانون العقوبات الجزائري ، جنائي خاص في الجرائم ضد الأشخاص والأخلاق وامن الدولة، ديوان المطبوعات الجامعية، الجزائر ، طبعة 2 ، 1988
- جبران مسعود ، الرائد معجم لغوي عصري ، دار العلم للملاين ، مجلد واحد ، طبعة 7 ، 1992
- –جلال وفاء محمدين ، دور البنوك في مكافحة غسيل الأموال ، دار الجامعة الجديدة للنشر، الإسكندرية ، 2001
- جلال ثروت، نظم القسم العام في قانون العقوبات، دار العلوم للنشر والتوزيع، إسكندرية، 1999
- جمال نادر، تعلم الإنترنت بدون معلم ، دار الإسراء، عمان ، الطبعة الأولى، 2005
- جيلالي بغدادي ، الاجتهاد القضائي في المواد الجزائية ، الديوان الوطني للأشغال التربوية ، الجزء الأول. د س ن
- حافظ، مجدي محمود ،الحماية الجنائية لأسرار الدولة ، الهيئة المصرية العامة للكتاب، الإسكندرية، 1999
- حسام الدين الاهواني و جميل عبد الباقي الصغير ، مقدمة في الحاسب الآلي ، دراسة علمية ونظرية، دار النهضة العربية ، القاهرة ، 2000
- حسنين المحمدي بادي ، حقوق الإنسان بين مطرقة الإرهاب وسندان الغرب ، دار الفكر الجامعي، الاسكنديرية ، 2004

- حسين بن شيخ آت ملويا، المخدرات والمؤثرات العقلية، دراسة قانونية تفسيرية، دار هومة للنشر، الجزائر 2010
- حسين فريجة ، شرح قانون العقوبات الجزائري جرائم الأشخاص والأموال ، ديوان المطبوعات الجامعية ، الجزائر ،طبعة 2 ، 2009
- حمدي عبد العظيم ، غسيل الأموال جريمة العصر البيضاء ، القاهرة ، 2000
- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية ، دار الفكر الجامعي ، الإسكندرية، طبعة 1، 2010
- سليمان ضيف الله الزبن، التحويل الالكتروني للأموال ومسؤولية البنوك القانونية، طبعة 1، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2012
- سليمان عبد المنعم سليمان، الجوانب الإشكالية في النظام القانوني لتسليم المجرمين، دار المطبوعات الجامعية، 2015
- سمير فايز إسماعيل ، تبيض الأموال دراسة مقارنة ، منشورات زين الحقوقية ، بيروت ، 2010
- سيد أحمد عبد الخالق، الآثار الاقتصادية والاجتماعية لغسيل الأموال، القاهرة: دار النهضة العربية، 1997
- شريف الطباخ, التعويض عن جرائم السب والقذف وجرائم النشر في ضوء القضاء والفقه، دار الفكر الجامعي، الإسكندرية, 2007
- شريف درويش اللبان ، تكنولوجيا الاتصال : المخاطر والتحديات والتأثيرات الاجتماعية ، الدار المصرية اللبنانية ، القاهرة ،2000
- صالح خليل الصقور ، الإعلام و التنشئة الاجتماعية ، دار أسامة للنشر والتوزيع ، الأردن، 2012.
- طارق إبراهيم الدسوقي، الحماية القانونية لأمن الدولة من جهة الداخل والخارج، دار الجامعة الجديدة للنشر ،2010

- طوني ميشال عيسى، التنظيم القانوني لشبكة الانترنت" دراسة مقارنة ، طبعة 1 ، بيروت ، 2001
- عادل عازر ، النظرية العامة في ظروف الجريمة ، المطبعة العالمية ، القاهرة ، 1967
- عبد الأمير الفيصل، دراسات في الإعلام الالكتروني، دار الكتاب الجامعي للنشر والتوزيع، الإمارات ،2014
- عبد الرحمن خلفي، ، محاضرات في قانون الإجراءات الجزائية، دار الهدى عين مليلة، الجزائر، 2010
- عبد الرحمن غسان زعرور، شرح خوارزمية التشفيرDES ، مكتبة النور ،حمص سوريا، 2008
- عبد القادر الفنتوخ ، الإنترنت للمستخدم العربي ، مكتبة العبيكان ، الرياض ، 2000
- عبد القادر زهير النفوري، المفهوم القانوني لجرائم الإرهاب الداخلي والدولي، طبعة 1 ، منشورات الحلبي الحقوقية للنشر، سورية، 2008
- عبد الفتاح بيومي حجازي ، الحكومة الالكترونية ونظامها القانوني ، شركة الجلال للطباعة، الإسكندرية ، 2004
- عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، 2015
- عبد الملك جندي ، الموسوعة الجنائية ، منشورات الحلبي الحقوقية، 2010
- عبد الوهاب المعمري ، جريمة الاختطاف الأحكام العامة والخاصة، والجرائم المرتبطة بها ، دار الكتب القانونية، القاهرة، 2010
- عصام عبد الفتاح ، الجريمة الإرهابية ، دار الجامعة الجديدة، الإسكندرية، 2008
- علي الحوات، الجرائم الجنسية ، دار الحامد للنشر، عمان، 2014

- علي عبد القادر القهوجي، شرح قانون العقوبات القسم العام، دار العلوم للنشر والتوزيع، إسكندرية، 1998
- عمر سامان فوزي ، المسؤولية المدنية للصحفي .دراسة مقارنة ، دار وائل للنشر والتوزيع ،عمان ،الأردن ، طبعة 1 ،2007
- فاروق حسين ، أمن الإنترنت ، دار الراتب الجامعي ، بيروت 1999
- فتحي شمس الدين، شبكات التواصل الاجتماعي والتحول الديمقراطي في مصر ، القاهرة ، دار النهضة العربية ،2013
- فخري عبد الرزاق الحديثي و خالد حميدي الزغبي، شرح قانون العقوبات القسم العام، دار الثقافة للنشر والتوزيع، عمان، طبعة 1 ، 2009
- فؤاد شعبان وعبيدة صبطي، تاريخ الاتصال وتكنولوجياته، دار الخلدونية للنشر والتوزيع، الجزائر، 2011
- فوزية عبد الستار ، شرح قانون العقوبات القسم الخاص ، طبعة 4 ، دار النهضة العربية، القاهرة، 2012
- فوزية عبد الستار , المعاملة الجنائية للأطفال , دراسة مقارنة , دار النهضة العربية, 1998
- لحرش عبد الرحمن، التجسس والحصانة الدبلوماسية، مجلة الحقوق، جامعة الكويت، العدد الرابع، 2003
- ماجد الزبيدي ، الإنترنت والتدريب في علوم المعلومات والمكتبات : رسالة مكتبية، المجلد 3 ، العدد الأول والثاني ،2004
- محمد السيد حلاوة ، رجاء على عبد العاطي ،العلاقات الاجتماعية للشباب بين دردشة الإنترنت والفيس بوك ، دار المعرفة الجامعية، الإسكندرية، 2011
- محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، طبعة 2، الجزائر، 2009

- محمد الأمين البشري، التحديات الأمنية المصاحبة لوسائل الاتصال الجديدة، دراسة وصفية تأصيلية للظاهرة الإجرامية على شبكة الانترنت، الدليل الالكتروني للقانون العربي
- محمد عبد الله سلامة، الكيان القانوني لغسيل الأموال: الجريمة، المسؤولية الجنائية، المكافحة، ، المكتب العربي الحديث، الإسكندرية، طبعة 1 ، 2007
- محمد السيد عرفة، تدريب رجال العدالة و أثره على تحقيق العدالة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2005
- محمّد صبحي نجم ، شرح قانون العقوبات الجزائري القسم الخاص ، ديوان المطبوعات الجامعية، الجزائر، 2000
- محمد نور الدين سيد، جريمة بيع الأطفال والاتجار بهم , دراسة في قانون العقوبات المصري والإماراتي وقوانين مكافحة الاتجار بالبشر والاتفاقيات والبروتوكولات الدولية ، دار النهضة العربية ، 2012
- محمد بن شلهوب ، جريمة الابتزاز دراسة مقارنة، دار كنوز اشبيليا، الرياض، 2016.
- محمد صبحي نجم، قانون العقوبات، القسم العام، النظرية العامة للجريمة، د ط، دار الثقافة للنشر والتوزيع، عمان، 2010
- محمد على محمد ، رواه علم الاجتماع ، قراءة جديدة للذكر الاجتماعي العربي ، الهيئة المصرية العامة للمكاتب ، الإسكندرية ، 1976
- محمد بشير الشافعي ، قانون حقوق الإنسان . مصادره وتطبيقاته الوطنية الدولية ، منشاة المعارف، الإسكندرية ، طبعة 4 ، سنة 2007
- محمود نجيب حسني، المساهمة الجنائية في التشريعات العربية، ط 2 ، دار النهضة العربية، القاهرة، 1998

- محمود محمد سعيفان تحليل و تقييم دور البنوك في مكافحة عمليات غسيل الأموال ، دار الثقافة للنشر و التوزيع ، عمان، طبعة 1 ، 2008
- محمود نجيب حسني ، شرح قانون العقوبات ،القسم الخاص ، دار النهضة العربية ، القاهرة، طبعة 6، 1989.
- مركز المحتسب للاستشارات، دور مواقع التواصل الاجتماعي في الاحتساب توتير نموذجا، دار المحتسب للنشر والتوزيع، الرياض، طبعة 1 ، 1438 هـ
- مصطفى الطاهر، المواجهة التشريعية لظاهرة غسيل الأموال المتحصلة من جرائم المخدرات، مطابع الشرطة للطباعة والنشر، القاهرة، 2002
- مصطفى كمال طه، الأوراق التجارية ووسائل الدفع الالكترونية الحديثة، دار الفكر الجامعي، الاسكندرية، مصر، 2007
- ممدوح خليل البحر ، الجرائم الواقعة على الأشخاص في قانون العقوبات الإماراتي ، طبعة 1 دار إثراء للنشر والتوزيع ، الأردن ، 2009
- مولود ديدان، قانون العقوبات، دار بلقيس للنشر، الدار البيضاء، الجزائر، 2012
- نبيل صقر، جرائم المخدرات في التشريع الجزائري، دار الهدى عين مليلة، الجزائر، 2006
- نصر الدين مروك، جريمة المخدرات في ضوء القوانين والاتفاقيات الدولية، دار هومة للنشر والتوزيع، الجزائر، 2007
- نظام توفيق المجالي، شرح قانون العقوبات، القسم العام، طبعة 1 ،دار الثقافة للنشر و التوزيع، عمان، 2009
- هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة ، 1994
- هيثم فاتح شهاب، جريمة الإرهاب وسبل مكافحتها في التشريعات الجزائية المقارنة، طبعة 1، دار الثقافة للنشر والتوزيع، الأردن ، 2010

- وسيم شفيق الحجار، الإثبات الالكتروني ، المنشورات الحقوقية، بيروت ، 2002
- **ب: المراجع المتخصصة**
- أحمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية، طبعة 1، 2006
- أحمد إبراهيم مصطفى سليمان ، الإرهاب والجريمة المنظمة ، مطبعة العشري ، القاهرة ، 2006
- أسامة يوسف أبو حجاج ، دليلك الشخصي إلي عالم الإنترنت، نهضة مصر، القاهرة، 1998
- أسامة احمد المناعسة وجلال محمد الزغبي ، جرائم تقنية نظم المعلومات الالكترونية، دراسة مقارنة، عمان ، طبعة 2، 2014
- الحسيني عمار عباس، جرائم الحاسوب والإنترنت"الجرائم المعلوماتية" ، منشورات زين الحقوقية، بيروت ، ط2، 2019
- الحمود وضاح ومحمود و نشأت مفضي، جرائم الإنترنت، دار المنار، عمان، الأردن، _2005
- السيد عتيق ، جرائم الإنترنت، دار النهضة العربية طبعة 1، سنه 2000
- المري بهاء ، جرائم المحمول والإنترنت ، منشاة المعارف ، الإسكندرية ، سنة 2017
- الموسي سالم رضوان ، جرائم القذف والسب عبر القنوات الفضائية ، منشورات الحلبي الحقوقية، بيروت ، طبعة1 ، 2012
- أمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، دار هومه الجزائر ، طبعة 2 ، 2007
- أمير فرج يوسف،الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت، مكتبة الوفاء القانونية، طبعة 2 ، 2011

- بلال أمين زين الدين ،جرائم نظم المعالجة لأليه للبيانات ، دار الفكر العربي ،سنه 2008
- بولين أنطونيوس أيوب ،الحماية القانونية للحياة الشخصية في مجال المعلوماتية ، دارسة مقارنة، الطبعة الأولى، منشوارت الحلبي الحقوقية، بيروت ، لبنان، 2009
- جميل عبد الباقي الصغير– الجوانب إلإجرائية المتعلقة بالإنترنت، دار النهضة العربية، 2001
- حسام محمد نبيل الشنراقي ، الجرائم المعلوماتية، دراسة تطبيقية مقارنة عن جرائم الاعتداء على التوقيع الالكتروني، دار الكتب القانونية، دار النشر والبرمجيات، ، مصر، 2013
- حسن طاهر داود، جرائم نظم المعلومات، جامعة نايف للعلوم الأمنية، الرياض، السعودية، طبعة 1، 2000
- حسين طاهر داوود ، جرائم نظم المعلومات ، الرياض ، طبعة 1 ، 2000
- حسين محمد الغول ، جرائم شبكة الإنترنت والمسؤولية الناشئة عنها –دراسة مقارنة، مكتبة بدران الحقوقية ، صيدا، طبعة 1، 2017
- حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية دراسة مقارنة ،منشورات الحلبي الحقوقية، بيروت،طبعة 1، 2014
- خالد ممدوح ابراهيم ، الجرائم المعلوماتية ، دار الفكر الجامعي ، الإسكندرية ، طبعة 2، 2019
- رافي جوبتا، هوج بروكس، وسائل التواصل الاجتماعي و تأثيرها على المجتمع، (ترجمة عاصم سيد عبد الفتاح)، المجموعة العربية للتدريب والنشر ، 2017
- ربيع محمود الصغير ، القصد الجنائي في الجرائم المتعلقة بالإنترنت والمعلوماتية، دراسة تطبيقية مقارنة، مركز الدراسات العربية للنشر والتوزيع، القاهرة، طبعة 1، 2017

- زين العابدين عواد كاظم الكردي، جرائم الإرهاب المعلوماتي ، دراسة مقارنة، منشورات الحلبي الحقوقية ، بيروت، طبعة 1، 2018
- صدام حسين ياسين العبيدي، جرائم الإنترنت وعقوبتها في الشريعة الإسلامية والقوانين الوضعية، المركز العربي للنشر، القاهرة، طبعة 1، 2019
- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية، 2009
- طارق سرور ، جرائم النشر والإعلام ، دار النهضة العربية ، القاهرة ، طبعة 1، 2004
- عادل عزام سقف الحيط، جرائم الذم و لقدح والتحقير المرتكبة عبر الوسائط الالكترونية، دراسة قانونية مقارنة، دار الثقافة للنشر والتوزيع ،عمان ،طبعة 1، 2010
- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن ، دار الجامعة الجديدة ، كلية الحقوق جامعة الإسكندرية ، 2006
- عبد الرحمان بن عبد الله السند، الأحكام الفقهية للتعاملات الالكترونية الحاسب الآلي وشبكة المعلومات الإنترنت ، دار الوراق، بيروت ، الرياض ، دمشق ، طبعة 1 ، 2004
- عبد الفتاح بيومي حجازي ، *جريمة* غسل الأموال عبر شبكة الإنترنت "دراسة متعمقة *عن جريمة* غسل الأموال عبر *الوسائط* الإلكترونية في التشريعات المقارنة " ، المصدر القومي للإصدارات القانونية ، طبعة 1، 2009.
- عبد الفتاح بيومي حجازي ، جرائم غسيل الأموال بين الوسائط الالكترونية و نصوص التشريع ، دراسة مقارنة ، القاهرة ،2010
- عبد الفتاح بيومي حجازي ، التجارة الالكترونية، دار الفكر الجامعي، الإسكندرية ، 2004

- عبد الفتاح بيومي حجازي ، الحماية الجنائية للتجارة الالكترونية ، دار الفكر الجامعي ، الإسكندرية، طبعة 2 ، 2001
- عبد الفتاح بيومي حجازي ، الدليل الجنائي والتزوير في الجرائم المعلوماتية والانترنت، دار الكتب القانونية ، مصر ، 2006
- عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، دار الكتب والوثائق المصرية، الإسكندرية
- عبد الله عبد الكريم عبد الله ، جرائم المعلوماتية والإنترنت دراسة مقارنة ، طبعة 1 ، منشورات الحلبي الحقوقية ، 2007
- عبد العال الدريبي، الجرائم الالكترونية، دراسة قانونية قضائية مقارنة مع احدث التشريعات العربية في مجال مكافحة الجرائم المعلوماتية والإنترنت، المركز القومي للإصدارات القانونية ، القاهرة، 2012
- عبد الفتاح حجازي ، الحكومة الالكترونية بين الواقع والطموح ، دار الفكر الجامعي، القاهرة ، 2008
- عفيفي كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف كالمصنفات الفنية، دار الثقافة للطباعة والنشر، القاهرة،2007
- عصام محمد، مكافحة غسيل الأموال بين التجريم والتعاون الدول، المركز القومي للدراسات القضائية،1996
- علي جبار الحسناوي ، جرائم الحاسوب و الإنترنت ، دار اليازوي العلمية للنشر والتوزيع ، عمان، 2009
- علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة"دراسة مقارنة " مكتبة زين الحقوقية والأدبية ، بيروت، ط 1، 2013
- عمار عباس الحسيني، جرائم الحاسوب والانترنت الجرائم المعلوماتية، منشورات زين الحقوقية، بيروت، ط1، 2017

- عمر محمد بن يونس، الجرائم الناشئة عن استخدام الإنترنت، الأحكام الموضوعية والجوانب الإجرائية، دار النهضة العربية، القاهرة ، 2004
- عمر أبو الفتوح الحمامي، الحماية الجنائية للمعلومات ، دار النهضة العربية ، مصر ، 2010
- عيسى سليم داود ، جرائم القرصنة الإلكترونية، رسالة ماجستير، جامعة الإسكندرية، 2017
- فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، ط 2016
- فؤاد مرسي، الرأسمالية تجدد نفسها، سلسلة عالم المعرفة، الكويت،1990
- فؤاد شاكر، التوجهات الإستراتيجية لمكافحة تبييض الأموال من قبل المصارف العربية ،تبييض الأموال، اتحاد المصارف العربية، عمان،2002
- لوادي حسنين المحمدي ، إرهاب الإنترنت الخطر القادم ، دار الفكر الجامعي ، الإسكندرية ، طبعة 1، 2006
- محمد الشناوي، جرائم النصب المستحدثة ، دار الكتب القانونية، القاهرة، 2008
- محمد أمين أحمد الشوابكة، جرائم الحاسوب و الانترنت و الجريمة المعلوماتية، طبعة 1، دار الثقافة للنشر والتوزيع، الأردن،2009
- محمد سامي الشوا، ثورة المعلمات وانعكاسها على قانون العقوبات ، دار النهضة العربية ، 1998
- محمد عادل ريان ، جرائم الحاسوب الآلي وأمن البيانات، بيروت، لبنان،2002
- محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي ، دار الثقافة ، عمان، طبعة1، 2004.
- محمد رجب فتح الله ، الوسيط في الجرائم المعلوماتية ، دار الجامعة الجديدة للنشر ، إسكندرية ، طبعة 1، 2019

- محمد طارق الخن، جريمة الاحتيال عبر الإنترنت، منشورات الحلبي الحقوقية، مصر،طبعة 1، 2011
- محمد علي العريان ، الجرائم المعلوماتية ، دار الجامعة الجديدة للطباعة والنشر، إسكندرية ، 2004
- محمود احمد عبابنة ، جرائم الحاسوب و أبعادها الدولية ، دار الثقافة للنشر والتوزيع ، عمان ، طبعة 2 ، 2009
- مدحت رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة، القاهرة، 2000
- مسعد عبد الرحمن زيدان، الاستغلال الجنسي للأطفال عبر الانترنت في ضوء أحكام القانون الدولي، كلية العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2016
- ممدوح الشيخ ، التجسس التكنولوجي سرقة الأسرار الاقتصادية والتقنية، مكتبة بيروت، سلطنة عمان ، 2007
- ممدوح عبد الحميد عبد المطلب ، البحث والتحقيق الجزائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانوني ،2006
- منير وممدوح الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2006
- نائلة عادل محمد فريد قورة ، جرائم الحاسب الآلي الاقتصادية ، دراسة نظرية مقارنة ، منشورات الحلبي الحقوقية ، طبعة 1 ، 2005
- نهلا عبد القادر المومني ، الجرائم المعلوماتية، دار الثقافة، عمان ، طبعة1، 2008
- هبة هروال ، الجوانب الإجرائية لجرائم الإنترنت، دار الفكر الجامعي، الإسكندرية، 2013

- هدى حامد قشقوش، جرائم الحاسب الالكتروني، دار النهضة العربية القاهرة ، 1992
- يوسف حسن يوسف، الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، القاهرة، طبعة 1، 2011
- **3- الأطروحات والمذكرات الجامعية**
- أحمد مداح، الجريمة الالكترونية في الفقه الجنائي الإسلامي ، أطروحة دكتوراه جامعة الحاج لخضر باتنة كلية العلوم الإنسانية والعلوم الإنسانية –قسم العلوم الإسلامية ، السنة الجامعية 2014-2015
- أكمل يوسف السعيد , الحماية الجنائية للأطفال ضد الاستغلال الجنسي , رسالة دكتوراه , كلية الحقوق المنصورة ، مصر ,2012
- ابوغليون عطوة مسلم، الجرائم الالكترونية بين الشريعة الإسلامية والقوانين الوضعية، رسالة ماجستير في القضاء الشرعي من كل الدراسات العليا بالجامعة الأردنية عام 2009
- بحر عبد الرحمن محمد ، معوقات التحقيق في جرائم الإنترنت ، دراسة مسحية على ضباط الشرطة في دولة البحرين، رسالة ماجستير غير منشورة، أكاديمية نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية.2000
- بدري فيصل، مكافحة الجريمة المعلوماتية ، أطروحة لنيل شهادة الدكتوراه، جامعة الجزائر كلية الحقوق، 2017،2018
- تركي بن عبد الرحمان المويشير، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فعاليتها، رسالة مقدمة لأجل نيل شهادة الدكتوراه، ،قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية،الرياض، السعودية،2009

- حماني سمير، التوثيق في المعاملات الإلكترونية دراسة مقارنة ، مذكرة لنيل شهادة الماجستير ، قسم الحقوق ، كلية الحقوق والعلوم السياسية، جامعة مولود معمري ، تيزي وزو، 2015
- جلاب حنان، السببية في جريمة القتل دراسة مقارنة بين الفقه الجنائي الإسلامي و قانون ع الجزائري، رسالة ماجستير في الشريعة والقانون ، جامعة باتنة ، السنة الدراسية 2004.
- ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، رسالة مقدمة لنيل شهادة دكتوراه، كلية الحقوق والعلوم السياسية ، قسم الحقوق ، باتنة ، 2015-2016
- سعيداني نعيم ، أليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير ع ق، كلية الحقوق و ع السياسية ، جامعة الحاج لخضر باتنة 2012-2013
- شيرين الياس دبابنة ،التأثير الاجتماعي والاقتصادي لجرائم الإنترنت في المجتمع الأردني ، رسالة لنيل شهادة الدكتوراه في علم الاجتماع ،كلية الدراسات العليا ، الجامعة الأردنية ، 2008
- عبد الله حسين آل حجراف القحطاني، تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية دراسة تطبيقية في هيئـــة التحقيق والادعاء العام بمدينة الرياض، رسالة ماجستير، الرياض.
- غازي عبد الرحمان هيان الرشيد، الحماية القانونية من جرائم المعلوماتية "الإنترنت"، مذكرة دكتوراه، جامعة السالمية، لبنان ،2004.
- فوزية عبد الستار، المساهمة الأصلية في الجريمة، تخصص القانون الخاص و العلوم الجنائية، رسالة دكتوراه، القاهرة، 1967

- فهد بن مبارك العرفج، التحريض على الجريمة في الفقه الإسلامي والنظام السعودي دراسة تأصيلية تطبيقية، تخصص لقانون الخاص و العلوم الجنائية، مذكرة ماجستير، جامعة نايف العربية للعلوم الأمنية، 2006
- محمد منصور، تأثير شبكات التواصل الاجتماعي على جمهور المتلقين، رسالة ماجستير، جامعة القاهرة، 2012
- محمد هشام عبد الفتاح ، جريمة الاحتيال دراسة مقارنة، رسالة ماجستير، نابلس، فلسطين، 2008
- هروال هبة نبيلة، جرائم الإنترنت دراسة مقارنة ، أطروحة دكتوراه، جامعة تلمسان ، 2013-2014
- يوسف صغير ، الجريمة المرتكبة عبر الانترنت ، رسالة ماجستير، جامعة مولود معمري، تيزي وزو، كلية الحقوق والعلوم السياسية ، 2013
- **4- المجلات والملتقيات**

- إبراهيم أبو الغار، سرقة المساكن في المناطق الحضرية بمدينة القاهرة، المجلة الجنائية القومية، العدد الأول، المجلد12 ، القاهرة، 1978
- إبراهيم إسماعيل عبده محمد، الاستغلال الجنسي للأطفال عبر شبكات التواصل الاجتماعي ، جامعة الملك سعود، الرياض، المملكة العربية السعودية ، مقال منشور في مجلة جيل العلوم الاجتماعية والإنسانية ، العدد 56
- أحمد عبد الحليم شاكر، دور الإنابة القضائية الدولية في مكافحة الجريمة، بحث منشور بمجلة الفكر الشرطي، المجلد 18 ،العدد 4 ،2007
- امجد حسان، الفيروسات إرهابا يهدد أنظمة المعلومات ، مقال مقدم إلى ملتقي الإرهاب ،جامعة الحسين بن طلال ، عمان في 2008
- امجد دخل الله ، القرصنة الإلكترونية ، مجلة المحامون ، العدد 4 ، سوريا، 2007

- السيد نجم، الاتجار في البشر والاستغلال الجنسي للأطفال، بحث في المؤتمر الدولي الثاني حول حماية المعلومات والخصوصية في قانون الإنترنت، القاهرة، يونيو 2008
- إلهام بن خليفة، جمال غريسي، التجسس الالكتروني كجريمة ماسة بأمن الدولة في التشريع الجزائري ، مجلة دفاتر السياسة والقانون المجلد: 11 ، العدد: 01، 2022
- أماني جمال مجاهد: الشبكات الاجتماعية في خدمات مكتبية متطورة، مجلة مركز دراسات المعلومات، القاهرة، ماي، العدد 08 ، جامعة المنوفية ،2011
- أنور طلبة، قانون العقوبات في ضوء أحكام النقض ، مجلة القضاة ، طبعة نادي القضاة سنة 1980
- بركات ،إبراهيم محمد "أهمية الإفصاح عن مخاطر المعاملات المالية المتعلقة بغسل الأموال في البنوك التجارية، بحث مقدم للمؤتمر العلمي: إدارة المخاطر والمحاسبة، جامعة الزيتونة الأردنية ،عمان ، الأردن 2007
- بقبق ليلى اسمهان، العمليات البنكية غير المشروعة وأثرها على الاقتصاد (عمليات تبييض الأموال) ، الملتقى الوطني حول الاقتصاد غير الرسمي في الجزائر، معهد العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، المركز الجامعي، مولاي الطاهر، ولاية سعيدة، الجزائر
- تومي فضيلة ، إيديولوجيا الشبكات الاجتماعية وخصوصية المستخدم بين الانتهاك والاختراق ، مجلة العلوم الإنسانية والاجتماعية ، جامعة قصدي مرباح ، الجزائر ، العدد 30 ، سبتمبر 2017
- حابت آمال ، التوجه التشريعي بخصوص التوقيع والمصادقة الالكترونية بين قانون رقم 05-10 القانون 15-04 ، مؤتمر وطني حول الأطر القانونية للتوقيع والتصديق الالكتروني في الجزائر ، كلية الحقوق والعلوم السياسية وجامعة محمد الشريف مساعدية ، سوق أهراس 2016
- حسن مظفر الرزو، الأمن المعلوماتي: معالجة قانونية ، مجلة الأمن والقانون ، اكادمية شرطة دبي، عدد1 ، 2004

- حسن علي كاظم ، *التطرف والإرهاب الفكري عبر الإنترنت ومواقع* التواصل، مجلة رابطة أمناء الشام، *العدد750، 2014*
- حسين نوارة ، آليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة إلكترونيا جامعة مولود معمري تيزي وزو، ملتقي آليات الجزائر مكافحة الجرائم الالكترونية في التشريع الجزائري، المنعقد في الجزائر العاصمة يوم 29 مارس 2017
- حنون نزهة، استخدام مواقع التواصل الاجتماعي وانعكاساتها على قيم المواطنة لدى الشباب الجزائري دراسة ميدانية على عينة من مستخدمي مواقع التواصل الاجتماعي، مجلة العلوم الإنسانية، العدد الثامن، 2017
- خالد محمد مصطفى ، المسئولية الجنائية لناشري الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل الاجتماعي ، مجلة رؤى استراتيجية ، مارس 2013
- – دوروتي اي ديينغ " Dorothee ay Dying " ، قراصنة أنظمة الحاسب الآلي ، المؤتمر القومي الثالث عشر لأمن الحاسب الآلي ، سنة 2002 ، ترجمة ، أمنة علي يوسف
- دينا عبد العزيز فهمى ، المسئولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي، بحث مقدم إلى المؤتمر العلمي الرابع بعنوان القانون والإعلام ؛ كلية الحقوق ، جامعة طنطا ؛ 23 – 24 أفريل ، 2016
- رشا خليل ، جرائم استغلال الأطفال عبر الإنترنت ، جامعة ديالي، كلية القانون ، مجلة الفتح، العدد2، 2006
- رضا ابن مقلة، الإعلام الإلكتروني المتطرف وسبل مواجهته: تنظيم داعش نموذجا، مجلة الحكمة للدراسات الإسلامية، مؤسسة كنوز الحكمة للنشر والتوزيع، الجزائر، 2015
- سعد حماد صالح القبائلي ، الجرائم الماسة بحق الإنسان في السمعة و الشرف والاعتبار عبر الإنترنيت، المؤتمر المغاربي الأول حول المعلوماتية والقانوني ، مدينة طرابلس– ليبيا ، أكتوبر 2009

- سلمى مانع ، دور الأمن المعلوماتي في مكافحة الجرائم المعلوماتية، بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16و 17 نوفمبر 2015، كلية الحقوق ، جامعة بسكرة، الجزائر
- سيد شوربجي عبد المولى، عمليات غسل الأموال وانعكاساتها على المتغيرات الاقتصادية والاجتماعية، المجلة العربية للدراسات الأمنية والتدريب، العدد :28 345، الرياض،1420
- عبد الحميد أحمد شهاب، "نظرية الفاعل المعنوي(دراسة مقارنة)"، مجلة الفتح، كلية القانون، جامعة ديالي، العدد 34 ،2008
- عبد الرحيم سلطان العلماء ، جرائم الانترنت والاحتساب عليها ، المجلة العربية للدراسات الأمنية والتدريب .
- عبد الفتاح بيومي حجازي ، مكافحة جرائم المصارف الإلكترونية، ورقة عمل ضمن ندوة المصارف الالكترونية، تحت إشراف الجمعية المصرية لقانون الانترنت، بتاريخ 13 ماي 2007
- عثمان بكر عثمان ، المسئولية عن الاعتداء على البيانات الشخصية عبر شبكات مواقع التوصل الاجتماعي ، كلية الحقوق ، جامعة طنطا
- عز الدين عثمان ، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية – مخبر المؤسسات الدستورية والنظم السياسية ،العدد الرابع ،جانفي 2018
- عدنان ابراهيم سرحان ، الوفاء (الدفع الالكتروني) ، بحث مقدم إلى مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون ، جامعة البحرين، 2006/12/10
- عدي جابر هادي، الجناية الجزائية للبريد الالكتروني، مجلة رسالة الحقوق، جامعة القادسية، العدد 3
- عرب يونس، جرائم الكمبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، 2002

- عرب يونس ، قراءة في الاتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية، ملتقى تجربة سلطنة عمان، تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية ، 2- 4 افريل 2006
- على بن سالم العدوي، مكافحة التجسس الإلكتروني في القانون العماني مقارنة بالشريعة الإسلامية والقانون الجنائي الدولي، المؤتمر الدولي الأول ، كلية العلوم الشرعية، تحديات الواقع وآفاق المستقبل، ديسمبر 2018
- غادة البطريق، تعرض الشباب العربي للمواقع الإلكترونية المتطرفة فكريا وعلاقته بإدراكهم للمنطق الدعائي للتنظيمات الإرهابية : دراسة ميدانية في إطار نظرية تأثير الشخص الثالث، مجلة بحوث العلاقات العامة الشرق الأوسط، الجمعية المصرية للعلاقات العامة، القاهرة، ديسمبر 2016
- غزالي نزيهة ، تامين وسائل الدفع بالية التصديق الالكتروني في الجزائر التوقيع ، مؤتمر وطني حول الإطار القانوني للتوقيع والتصديق الالكتروني في الجزائر ، كلية الحقوق والعلوم السياسية وجامعة محمد الشريف مساعدية ، سوق اهراس 2016 - وأنظر المرسوم التنفيذي رقم 09-410
- فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، كلية الحقوق جامعة محمد خيضر ، بسكرة، مجلة الحقوق والحريات، العدد الثاني،،2015، ص18
- كريم مزعل شبي، مفهوم الإرهاب دراسة في القانون الدولي و الداخلي ، مجلة اهل البيت ، كربلاء ، العدد 2، 2005
- لوكال مريم، الحماية القانونية للبيانات ذات الطابع الشخصي في العالم الرقمي ، بالملتقى الوطني الموسوم بـ: الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المنعقد بالمركز الجامعي غليزان يومي 7 و8 فبراير 2017
- محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الإلكترونية، المجلة الأكاديمية للبحث القانوني، المجلد14، العدد 02 -20

- محمدي فوزية وخدة فاطمة الزهراء، تأثير العنف الالكتروني في مواقع التواصل الاجتماعي على العلاقات الاجتماعية لدى الشباب، مقال نشر في مجلة جيل العلوم الإنسانية والاجتماعية العدد 40،،جامعة ورقلة
- محمد عبد الله المؤيد ، صور المسؤولية التقصيرية الناشئة عن الاعتداء على بيانات الكمبيوتر والتعامل عبر الإنترنت وتسوية منازعاتها ، مجلة الدراسات الاجتماعية ، العدد الثامن والعشرون ، جانفي ،2009
- محمد عبد السلام سلام، جرائم غسل الأموال إلكترونياً في ظلّ النظام العالمي الجديد للتجارة الحرّة ، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، وغرفة تجارة وصناعة دبي، دبي، 10 . 12 مايو2003
- مجدي الداغر، دور الإعلام الجديد فى تشكيل معارف واتجاهات الشباب الجامعى نحو ظاهرة الإرهاب على شبكة الإنترنت: د م، مجلة الآداب وعلوم الاجتماع، عدد 36، الكويت، 2016
- مجدوب عبد المؤمن، سفيان، دور شبكات التواصل الاجتماعي في عملية التحول السياسي بتونس 2011-2014 ، المجلة الجزائرية للأمن والتنمية، العدد13 ، 2018
- مراد رشدي، غسل الأموال عبر الوسائل الإلكترونية،المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية منظم المؤتمر : أكاديمية شرطة دبي – مركز البحوث والدراسات تاريخ الإنعقاد : 26 /2003/4: دبي ،الأمارات العربية المتحدة
- ممدوح عبد الحميد عبد المطلب ، جرائم استخدام شبكة المعلومات العالمية ، الجريمة عبر الإنترنت، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنيت ، بيروت ، 2000
- موسي عيسى العامري ، الشيك الذكي ، بحث مقدم إلى مؤتمر الاعمال المصرفية الالكترونية بين الشريعة والقانون ، جامعة البحرين ، 2006/12/10

- موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، مقال مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 2009،
- هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة ، المجلد الثاني ،الطبعة الثالثة، ماي 2000
- هشام غرايبة، التأثير الاقتصادي لعمليات غسل الأموال على المجتمع، مقال مقدم للحلقة العلمية ، أكاديمية نايف العربية للعلوم الأمنية عام،2001
- نوال العيسي ، القذف الإلكتروني ، مجلة الرياض ، الاثنين 15 ذو القعدة 1433 هـ ، 1 أكتوبر 2012م ، العدد 161
- التوصيات الصادرة عن مؤتمر الحق في الحياة الخاصة المنعقد في الإسكندرية في الفترة من 4، 6 جويلية 1987
- مؤتمر فيينا في الفترة ما بين 10-17 أفريل 2000
- **5- المواقع الالكترونية**

- https://www.aljazeera.net/blogs/2023/5/7
- أخر إحصائيات مستخدمي الانترنيت وشبكات التواصل بالجزائر على الموقع: https://www.echoroukonline.com
- -الإنترنت في الجزائر الموقع https://www.marefa.org
- حسين بن سعيد الغافري ، جهود سلطنة عمان في مواجهة الجرائم المتعلقة بشبكة الانترنت:

http://hussain-alghafri.blogspot.com

- محمد على القرى ، سرية عمليات المصرف ومفهومها وضوابطه:
  - http// :www.elgari Article
- صالح عطاالله ،الجرائم الالكترونية والمعلوماتية، مجلة شمس المستقبل: http://newssparrow.blogspot.com

- القذف عبر الوسائل الالكترونية : https://akhbarelyom.com/news/newdetails
- –التشهير بالناس على الطريقة الإلكترونية: https://ar.islamway.net/article
- القمار الالكتروني: /https://alarab.co.uk
- محمد طه ،الجنس و العلاقة الجنسية ، بحث منشور على الرابط التالي
- https://www.sehatok.com/psychology
- *ميلود بن عبد العزيز ،لجرائم الإباحية وأثرها على المجتمع من منظور شرعي وقانوني، مقال منشور على الرابط التالي:* https://www.asjp.cerist.dz/en/article/
- موقع الشروق ،*الجزائر الخامسة عربياً في تصفح المواقع الإباحية ،على الرابط التالي:* https://www.echoroukonline.com
- موقع الشروق ،*الجزائر الخامسة عربياً في تصفح المواقع الإباحية ،على الرابط التالي*
https://www.echoroukonline.com
- موقع اخبار اليوم ، مواقع التطرف والمواقع الإباحية التي تدمّر المجتمع ، نشر المقال بتاريخ يوم 07 – 05 – 2017 على الرابط التاليhttps://www.djazairess.com
- البورنغرافيا أو الفن الإباحي، مقال للكاتب إي وايت، بحث منشور على الرابط التالي : www.risalatalkaime.com =٩٢٨/:
- علي كريمي , الشباب وتشريعات الإنترنت العربية جريمة الاستغلال الجنسي للأطفال نموذجا WWW.maroc.reunis.fr
- هاني جورجي , مناهضة الاستغلال الجنسي للأطفال والعنف الأسري , من إصدارات المجلس القومي للطفولة والأمومة , وحدة مناهضة الاتجار بالأطفال , بحث منشور على الرابط التالي:

WWW.Child١٣٠٩٣٣٩٠٢٦٧١٦٢ .Trafficking . Info/Upload/Files/

- الجرائم الجنسية المرتكبة ضد الأطفال , بحث منشور على الرابط التالي :

com/biblio the que – collgue- docx WWW.emloffice

- البروتوكول الاختياري لاتفاقية حقوق الطفل وبغاء الأطفال واستخدامهم في العروض والمواد الإباحية , وقد صدر هذا البروتوكول عن الأمم المتحدة بعد اعتماد الجمعية العامة في 25 ماي 2000 بموجب القرار رقم263/54 ودخل حيز التنفيذ في 18 /01/ 2002 :الرابط التالي :

.http://www.umnedu/humanrts/arab/pro-shpid html

- الجرائم الجنسية المرتكبة ضد الأطفال , بحث منشور على الرابط التالي :
- WWW.emloffice.com/biblio the que – collegue/201157/57. – docx
- -حقائق عن استغلال الأطفال جنسيا، على الرابط التالي:

https://www.alhurra.com/a/internet-watch-foundation-annual-report/432910.html

- -احمد لطفي السيد مرعي، إستراتجية مكافحة جرائم الاتجار بالبشر ، بحث منشور على الرابط التالي : https://books.google.dz/books?id
- تعريف المواقع الإباحية ، على الرابط التالي :

https://ar.wikipedia.org/wiki

- -جريدة التحرير الجزائرية ، انتحار شابة بسبب فضيحة على الفايسبوك ، مقال منشور على الرابط التالي:
- https://www.altahrironline.com/ara/articles/71489
- -الهروب من الابتزاز الجنسي الإلكتروني إلى الانتحار ، الإمارات اليوم ، مقال منشور على الرابط :

https://www.emaratalyoum.com/local-section/accidents

- -ابتزاز مئات الأطفال في بريطانيا" عبر الإنترنت ،مركز مكافحة استغلال الأطفال وحمايتهم على الإنترنت في بريطانيا ، إحصائيات نشرت على الرابط الأتي

https://www.bbc.com/arabic/worldnews/2013/09/130920_cyber_blackmail_childeren

- قانون الجزائر الجديد لمكافحة الجريمة الالكترونية، مقال منشور على الرابط الأتي https://al-ain.com/article/algeria-law-electronic-crimes
- الموقع الالكتروني : https://www.maghress.com/search
- منظمة الشرطة الأوروبية 'يوروبول' الموقع التالي:
- http://www.jo24.net/post.php?id=87740
- مباحث المعلومات الموقع ،http://www.youm7.com
- -هجوم الكتروني على مستشفى ألماني، الموقع ، http://www.youm7.com
- مباحث المعلومات: يمكن ارتكاب كل الجرائم عبر الإنترنت بما فيها القتل، الموقع التالي:
- https://www.youm7.com
- جرائم الانترنت ، الموقع اطلع عليه في 2017/06/29
- /https://www.nippon.com/ar/features/c05701.
- -جرائم تسببت فيها مواقع التواصل الاجتماعي، تقرير نشرته "عربي21"على الرابط الأتي : /https://www.alalamtv.net/news/1832323
- وليد احمد ، جرائم ساهم الانترنت في انتشارها ، مقال منشور على الرابط الاتي : /https://www.tech-wd.com/wd/2013/08/12/internet-crimes
- عبد الرحمن حراب الحربي، الوقاية من الاحتيال المنظم وتجريمه، 2008، الموقع الإلكتروني: 9،www.almoslim.net/node/16321،
- علي عدنان الفيل، الجرائم الالكترونية، تم الاقتباس عن الموقع الالكتروني ستار تايمز، شؤون قانونية: http://www.startimes.com
- مجلة الشروق عدد 21ماي 2022م, الموافق ل 19 شوّال 1443هـ الموقع الإلكتروني :
- https://www.echoroukonline.com
- انطوني كاثبرتسون ، مجرمو الإنترنت الخفي، مقال منشور على الموقع الأتي : https://www.independentarabia.com/node/12881
- القرصنة الفكرية : مقال منشور على الرابط الاتي : https://m.annabaa.org

- الموقع الإلكتروني :
https://www.un.org/ar/un75/new-era-conflict-and-violence
- معجم المعاني الجامع الإلكتروني على العنوان الإلكتروني
http://www.almaany.com/ar/dict/ar-ar:
- وداد حمدى، استغلال مواقع التواصل الاجتماعي من قبل التنظيمات الإرهابية:
- http://ajo-ar.org : تقرير، نشر بتاريخ 7 أبريل 2017 .
- مرصد الأزهر، استخدام داعش لوسائل التواصل الاجتماعي، تاريخ النشر: 2015/12/4، http://www.azhar.eg/observer/replies :
- كيف غيرت التكنولوجيا أساليب التجسس؟ على الموقع التالي:
- https://www.noonpost.com
- أساليب التجسس الإلكتروني المتقدمة. على الموقع:https://futureuae.com
- التجسس الرقمي، على وسائل التواصل الاجتماعي على الموقع التالي:
- https://www.europarabct.com
- تحذيرات من ارتفاع تكلفة الجرائم الإلكترونية لـ10.5 تريليون دولار: على الموقع التالي
https://www.independentarabia.com
- فيس بوك يحتل الصدارة ، على الموقع التالي : https://alghad.com
- عدد مستخدمي يوتوب على الموقع https://abuomar.ae
- عدد مستخدمي الإنستغرام، https://abuomar.ae/
- سلطان مصف مبار ك الصاعدي، الشبكات الاجتماعية خطر أم فرصة، المملكة العربية على الموقع: http://www.conference.ncwegypt
- 45 صورة متعلقة بالاستغلال الجنسي للأطفال ،إحصائيات منشورة على الرابط التالي: https://www.aa.com.tr/ar
- استغلال الأطفال عبر الانترنت، بحث منشور على الرابط :
https://forums.graaam.com

- -جريمة الاستغلال الجنسي للأطفال عبر الإنترنت، على الموقع التالي: https//academia-arabia.com
- الجزائر عام حبس لمؤثرين في قضية احتيال. مقال منشور على الموقع التالي : https//www.alarabya.net
- مركز معلومات G8-على الموقع الالكترونيhtml.G8/net.CybercimeLaw
- انتحار فتاة مصرية" ابتزاز وصور مفبركة" مقال منشور على الموقع التالي: https//www.bbc.com
- الاستغلال الجنسي للأطفال، إحصائيات منشورة على الرابط التالي: https://www.aa.com.tr/ar
- الآثار السلبية لشبكة الإنترنت https://www.annajah.net article-23110
- المشاهدة الجنسية تتلف الدماغ : موقع عبد الدائم الكحيل : http//www .kaheel 7.com
- -إدمان المواد الإباحية تدمير للفرد والمجتمع : مقال منشور على الموقع: http//www .afrigatenews.net
- إدمان الزوج للمواقع الاباحية: مقال منشور على الموقع التالي : http//www .aljazeera.net
- كريم احمد ،أضرار مشاهدة الأفلام الإباحية: مقال منشور على الموقع التالي :http//www .almawdoo3.com - أضرار المخدرات على جسم الإنسان : مقال منشور على الموقع التالي :http//www .hopeeg.com
- الجرائم الإلكترونية https://www.mcit.gov.sa
- تقرير جرائم الإنترنت https://www.alittihad.ae/article/13882/2018
- أنواع التعدي على حقوق المؤلف، مقال منشور على الموقع التالي: https://riadrobinho/blogspot.com
- النشر العلمي الالكتروني في الجزائر ، مقال منشور على الموقع التالي: https://journals/ju.edu.jo

- القضاء يوقف نشاط نابستر، مقال منشور على الموقع التالي: https:/www.al-jazirah.com
- اخبار 7.45 لقناة M6 الفرنسية

المراجع الأجنبية

1- المراجع بالإنجليزية

- Adrianrolden, computer crime and the law, c.l.J- 1991- vil
- Alexander Michael, Computer Crime K Ugly Secret For business, Computer World, vol 24-No- 11 March 21- 1990
- Benson Carl, Andrew Jablan , Paul Kaplan And Mara Rosenthal, Computer Crimes, American C.L.R.N 1997 vol 34 , N2
- Bensoussan A, Cryptologie et Signature Electronique, aspects juridique, Hermès Science, Publication, paris, 1999
- Bensoussan A, internet, Aspects Juridiques, 2nd Edition Revue Et Augmen. Tee, Hermes, 1998
- Chu James, Law Enforcement Information Tevhnology, CrcPress, Usa, 2001
- Clarke R, Technology Criminel and Crime Science, European Journal on Criminal Policy and Research ,2010
- Drugs in the mail: how can it be stopped? hearing before the Subcommittee on Criminal Justice, Drug Policy, and Human Ressources of the Committee on Government Reform, House of Representatives, One Hundred Sixth Congress, second session, May 26, 2000.
- Eecke Patrick V, Jos Dumortier, Legal issue and the internet , Internet Européen Compared Law xv th International Congrès of comparative Law , Bristol , 26 Juil-1 aout 1998 , Bruxelles, 2000
- Falgun Rathod: Handbook on Cyber Crime and Law in India Compiled, Falgun Rathod, India, 2014
- Fred H cate-privacy in the information age-The Brooking institution, 1997
- Geoff Gilbert , Aspects of extradition law,london, kluwer, academic, 1991

- Gibbons Don.C., Society crime and criminel law, Sweet and max well, London, 1982,
- Grabosky Peter, Russell Smith-Gillian Dempsey – Electronic Theft Unlawful acquisition in Cyberspace. Cambridge University.
- Henry B, Computer and Security, Jean Frayssinet, Atteintes aux droits de la personne résultant des Fichiersou des traitements informatiques, juris, classeur penal, Articles 226-16 a 226-24,fasc, 1991
- Icove David, K Karl Serger ,Karl , WilliamVonstorch Computer Crime , O'Reilly and Associates , Inc K 1995
- Kaymona Gay, Droit De L'enfance Et De L adolescences, Litec, 2002
- Kuntz Micheal and patrick Welson , Computer Crime and Computer Frauf , Report to The Montgomery County Criminal Justice Coordating Commission, Fall 2004
- Malcom Anderson ‹Policing the world : Interpol the Politics of International Police Co- Operation, Clarendon press. Oxford, 1989
- Mark A. Fox Internet Banking, E money and the internet Gift economy, First Monday, December 2005
- Michael L, Stevens-Identifying and Charging Computer Crimes I, The military , M L Rev ,1985, Vol 110
- Queminer Myriam, Yves Charpen, la cybercriminalite, O'Brien – Managment Information Systems – J.a.5th ed. 2001
- Richard Milchir M, Marques et noms de Dmaine de quelques Problemes Actuels, lamydrois commercial n 135 juillet, 2000 bulletin d'actualite
- Rouse Margaret, "Instagram" ‹searchcio.techtarget.com, Retrieved 16-10-2020. Edited.
- Smith JC -B Hogan, Criminel Law, Fifth Edition, Butter worths, London, 1983
- Smith Michael, International Review of the Red Cross: Humanitarian Dialogues in Law, Politics and Humanitarian Action, 2002
- Sophie Paillard, Les risques des technologies nouvelles de l'information Le Gazette du palais, 1997

- Straub. D, Carlson P and Jones E, Deterring Highly Motivated Computer Abusers , A Field Experiment In computer Security. In G. Gable and Caelli, IT Security, the Needs For International Cooperation Amsterdam, Elsevier Science Publishers, 1992,
- Streling B ,Thje Hacker Crackdown , Law and Electronic Fointer, London Viking , 1993 Peter Graaposky , Russell Smith , Gillian Dempsey , Eliectronic Theft, , Unlawful acquisition in cyberspace , cambridge university press, 1st publishd, 2001
- Taylor Paul, Hacktivisim in search of listethics, Crime and The Internet KEfited by David Wall k Routldge Taylor and Francid group ,1st Edition 2001
- The No Electronic Theft (NET) Act, enacted in 1997 by the U.S. Congress, amended titles 17 and 18, United States Code, to provide greater protection for copyright owners by amending criminal copyright infringement provisions, and for other purposes.
- Thompson David - Computer Crime and Security Survey- Information Management and Computer Security- 1998
- Thompson David, Current trends in Computer Crime , Computer Control Quar , trely , Vol 9 , N 1 ,1991
- Tournier .J, Internet Censure A Domicile, le Monde, Supplément MultiMedia, 1996
- Wall David – Cyber crimes and the Internet (crime and the internet) – Routldge Taylor and Francis group- 1st Edition 2001-
- FeralSchul ,cyberdroit, leFroit a L'epruve De L'internet , Dalloz, 3ed, 2002
- IEEE Security and Privacy Magazine Journal uri icon. Overview; Identity; View All Computer Security Education and Research in Australia. 2016
- Isabelle Wekstein, Droit Voisins Du Droit D'auteur Et Numérique, Litec, 2002
- Kenneth R osenblat, High Technology Crime, Investigating Cases, London, K,S,K, Publication , 1995
- Thierry Piette Coudol ,Andre Bertrand , Internet Et La Loi , Dalloz, 1997
- V - Sadaillan , Principe General Du Droit D La Responsabilité Et Responsabilité Des Acteurs De L'internet .
- Valerie Sadaillan ,Droit De l'internet, collection , AUI
- W. Elliott.and Selia Wells, Case Book on criminal law, Sweet and Max Well, London, 1982

- Wilson Computer Crime and Computer Fraud – Report to the montgmery county criminal Justice Coordinating Commission University of Mayrland Fepartment of Criminology and Criminal Justice Fall – 2004

2- المراجع بالفرنسية

- Axel Lefebvre , Etienne Montero , Informatique et Droit , Vers une Subversion De L'ordre Juridique , facultés universitaires Notre Dame de Paix de Namur, Bruylant Bruxelles , 1999
- Coralie Dumas, Le Droit De La Personnalité Et Les Réseaux Sociaux, Mémoire, Faculté De Droit, Université De Montpellier, 2015
- Clémence Dani, Laura Garino, M. Gianni Giordano, Elisa Sicard, Réseaux Sociaux Et Protection Des Données Personnelles, Rapport Réalisé Sous La Direction De M. Le Professeur Jean Frayssinet Et M. Le Professeur Philippe Mouron, université de Aix Marseille, faculté de droit, 2014.
- Catala, la propriété de l'information et masse : la délinquance informatique aspects de droit pénal international in le criminel.
- Claude Colombet , Propriété littéraire et droit voisins,9eme edition, dalloz, delta, 1999,
- Francois Rigaux, L'élaboration d'un « Right of Privacy » par la jurisprudence Américaine, Revue international de droit compare, Vol 32, N°4, October -December 1980
- Jean Frayssinet, Atteintes aux droits de la personne résultant des Fichiers ou des traitements informatiques, juris, classeur pénal, Articles 226-16 a 226-24, fasc, 1991
- J Robert, les réponses juridiques, Dossier internet et les libertés, les petites offices, n 224 du novembre 1999
- j Larreu, Protection d'une Marquée Renommée Contre le Cyber piratage, Expertises, aout, Septembre 1999
- Lamy, Droit de l informatique et des Réseaux, n 2308
- Mallorie Wozny, Exploitation des données personnelles : raison commerciale, raison d'état et opportunités, mémoire, université de Lyon, faculté de droit, 2017
- Morgan Layanchy , La responsabilité Délictuelle sur Internet En Durit suisse.

- Tiefemann fraude et autres, délits D'affaires commis a l'aide ordinateurs électroniques, RFPC-1984-N7
- Vivant et autres – Informatique et droit pénal – les bien informatique objets de fraude Lamy informatique -1991- n3445

3- المواقع الالكترونية

- HYPERLINK "https://www.commentcamarche.net/contents
- SUPER PROF MAGASINE- https://www.superprof.fr/blog/l-interieur-d-un-personal-computer
- SERGE LEBLAL- publié le 24 Mars 2015 https://www.lemondeinformatique.fr/actualites/lire-les-4-composants-phares-des-smartphones
- Internet Crime Complaint Center- IC3- Internet Crime raport 2007 https://www.ic3.gov
- https://www.pcmag.com/encyclopedia/term/40473/criminal-hacker
- https://www.neelwafurat.com/itempage.asp
- https://searchsecurity. techtarget.com/définition/hacker, DEFINITION Hacker
- - https://searchsecurity.techtarget.com/definition/hacker Types of hackers
- --https://searchsecurity.techtarget.com/definition/hacker ، The Crackers
- https://www.aljazeera.net/knowledgegate/newscoverage
- Cyber Criminal are adaptingthertactis to traget people worried about ther finances and job securityduring the finzncialcrisis, experts have warned .http// : www.mxlogic.com
- -Verton F 2001 technology Vendors Détail Plans To Share Security Information Computer world - http//www.computerworld.com/cwi/story/0-1199 – NAV47-STO56410- 00 -html
- -Encrypt: www.computerhope.com
- -Thoumyrel L- les enjeux de la cryptographie une analyse compare des des enjeux de la cryptographie au canada et états unis- www.juriscom.net
- National Institute of Justice. Justnet- Justice Tecgnology Information Net – work .http//www.nlectc.org/assistance/justenet.html.

- Maher L ,Provingyour computer Security , www.certconf.org
- Calderbank Michael, Le cryptosystème RSA: historique, algorithme, avantages , www.theses.fr
- https://www.cyberpatrol.com
- https://www.hudsonvlle .org /libiraryInternetpolicy.html
- -https://www.isok.org/pubpolpillar/docs/bp.interconnection .ar.pdf. .
- -la loi n 2000-719 du 1er aout morfiaient la loi n86 du 30 septembre 1986 relative a la liberté de communication , JO , N177 du aout 2000 .www egifrance /gouv/fr
- -Wiley D Parker ,Fighting Computer Crime , A New Framework for Protecting PuBlishing , NewYork
- https://www.kaspersky.com/resource-center/definitions/web-filter , et https://ncac.org/resource/internet-filters-2
- -Alfred Kagan ,The Electonic Ineormation Gap , Social Responsabilités Discussion Groupe Paper , Amsterdam 16 august 1998 international Fédération of Libirary Asqociation and Institutions , http ://www.ifla.org
- -Ashley Madison Hack Could Have A Devastating Psychological Fallot, http://www.huffingtonpost.com/entry/ashley-madison-hack-psychological-fallout_55d4afcee4b07addcb44f5d4 .
- https://www.collinsdictionary.com/dictionary/english/gamble
- https://www.aljazeera.net/news/miscellaneous/2013/1/27/
- U.Sieber , Legal aspects of computer – Related Crime in the information Society Legal Advisory Broad, European Commission ,Available AT M www.eurropa.eu .int /ispo/legal/encomcrime/siber.lhtml
- -https://www.nouvelobs.com/rue89/rue89.html . comment internet a modifie la prostitution
- Online child sexual exploitation ,https://www.ecpat.org/what-we-do/online-child-sexual-exploitation
- ttps://www.larousse.fr/dictionnaires/francais/pédophilie

- se protéger de 5 piratages de données parmi les plus répandus,Frederic BERGÉ,https://bfmbusiness.bfmtv.com/hightech/comment-se-proteger-de-5-piratages-de-donnees-parmi-les-plus-repandus-1241613.html
- Fraud Types, https://www.westernunion.com/us/en/fraudawareness/fraud-types.html.
- How to Avoid Gift Card Scams:,https://www.consumerreports.org/gift-cards/how-to-avoid-gift-card-scams/
- FraudTypes, https://www.westernunion.com/us/en/fraudawareness/fraud-types.html.
- shttps://www.consumerreports.org/gift-cards/how-to-avoid-gift-card-scams/
- -Sniffer Program or Packet Sniffer, Computer , Définition https://www.yourdictionary.com/sniffer-program-or-packet-sniffer
- https://www.un.org/ar/un75/new-era-conflict-and-violence
- -https://www.francetvinfo.fr/monde/espionnage-d-internet/Espionnage américain
- YouTube", techterms.com,7-10-2009 ،Retrieved 19-7-2020. Edited.
- Computer Hope (16-11-2020) www.computerhope.com, Retrieved 19-7
- -2020. Edited
- What is YouTube?", edu.gcfglobal.org, Retrieved Retrieved 19-7-2020. Edite
- What is YouTube?", edu.gcfglobal.org, Retrieved Retrieved 19-7-2020. Edited
- -Elise Moreau (10-2-2020), "What Is YouTube? How Do I Use It?" ،www.lifewire.com, Retrieved 19-7-2020. Edited
- O'Connell, Cyber-Crime hits $ 100 Billion in 2007, ITU News related to ITU Corporate Strategy, 17.10.2007, available at: http://www.ibls.com
- http://www.arableagueonline.org
- https//www.interpol.net 2020
- coronavirus, Attention aux arnaques en ligne.
- https://www.20minutes.fr/societe/2743143-20200318. Vu le 16 septembre

الملخص

أتت دراستنا هاته بعنوان " مظاهر العدوان الإجرامي عبر الإنترنت ومدى تأثيره على المجتمع" والتي تهدف إلى معرفة مختلف المظاهر التي قد تتخذها الجريمة المرتكبة عبر الإنترنت، والجوانب السلبية لها.

لقد استطاعت تقنية الإنترنت خلال فترة قصيرة من الزمن أن تكون الأداة الأهم في حياة معظم الأشخاص وأصبحت جزء لا يتجزأ عن تعاملاتهم اليومية. وبسببها ظهر نوع جديد من الجرائم يعرف بالجريمة عبر الإنترنت حيث يستخدم المجرم جهاز الحاسب متصلا بشبكة الإنترنت لتنفيذ جريمته، وقد انتشرت هذه الجرائم بشكل مخيف ينبأ بخطر كبير ناتج عن خواصها التي تميزها عن الجريمة التقليدية. ويعود ذلك أساسا إلى الإمكانيات المتاحة للمجرمين وسهولة استخدام الإنترنت بالتخفي خلف شاشتهم والقيام بنشر الفيروسات، والاختراقات وتدمير مخازن المعلومات، وسرقة الأموال والقيام بعمليات الاحتيال والتهديد والابتزاز ونشر المواد الإباحية لغاية شخصية أو مادية، والقيام بالعمليات الإرهابية، إلى جانب العديد من الجرائم التي ساهمت الإنترنت في تطورها. كل هذا وبشكل متكرر أثر بشكل سلبي على كل نواحي الحياة سواء الاجتماعية أو الاقتصادية أو الأمنية وحتى الثقافية.

وعليه فالمواجهة التشريعية كانت ضرورية للتعامل مع الجوانب التقنية للجريمة الرقمية وذلك بقواعد قانونية غيـــــر تقليدية، وكان لابد للتشريع الجزائري أن يواكب هذا التطور الملحوظ في الجرائم عبر الإنترنت مثله مثل التشريعات العربية والغربية، واستوجب عليه تعديل قانون العقوبات وسن قوانين خاصة الهدف منها خلق قاعدة قانونية موضوعية تحدد بالتفصيل كل الجرائم المتعلقة بتقنية المعلوماتية بدون استثناء ووضع إطار لها حتى يتسنى للقضاء متابعتها وفقا لإجراءات خاصة. والله ولي التوفيق.

Résumé

Cette étude s'intitulait « Manifestations de l'agression criminelle via Internet et son impact sur la société », qui vise à connaître les différentes manifestations que peut prendre le crime commis via Internet, et ses aspects négatifs.

En peu de temps, la technologie Internet est devenue l'outil le plus important dans la vie de la plupart des gens et est devenue une partie intégrante de leurs transactions quotidiennes. À cause de cela, un nouveau type de crime est apparu, connu sous le nom de cybercriminalité, où le criminel utilise un ordinateur connecté à Internet pour commettre son crime.

Ces crimes se sont propagés d'une manière alarmante qui prédit le danger en raison de leurs caractéristiques qui les distinguent du crime traditionnel. Cela est principalement dû aux possibilités offertes aux criminels et à la facilité d'utilisation d'Internet en se cachant derrière leur écran et en propageant des virus, en piratant et en détruisant des banques d'informations, en volant de l'argent, en pratiquant des fraudes, des menaces, de l'extorsion et en diffusant de la pornographie à des fins personnelles ou matérielles. Outre les nombreux délits qu'Internet a contribué à son développement.

Tout cela à plusieurs reprises affecté négativement tous les aspects de la vie, qu'ils soient sociaux, économiques, sécuritaires ou même culturels.

Ainsi, la législation algérienne devait suivre ce développement remarquable de la cybercriminalité, tout comme la législation arabe et occidentale.

La confrontation législative est nécessaire pour traiter les aspects techniques de la criminalité numérique avec des règles juridiques non conventionnelles, ce qui a conduit à la modification du Code pénal et à l'émergence de lois spéciales visant à créer une base juridique objective qui définit en détail tous les crimes liés aux technologies de l'information. et établit un cadre pour eux afin que le pouvoir judiciaire puisse en assurer le suivi selon des procédures spéciales.