**جامعة محمد خيضر بسكرة**

**كلية الحقوق والعلوم السياسية**

**قسم الحقوق**

**عنوان المذكرة**

# جرائم المساس بالأنظمة المعلوماتية

مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق تخصص

قانون جنائي

إعداد الطالبة:

سمية مزغيش

تحت إشراف الأستاذة :

براهمي حنان

الموسم الجامعي: 2013 /2014

# كلمة شكر عرفان

يسرني أن أتقدم بجزيل الشكر والعرفان إلى اللجنة

الموقرة التي قبلت مناقشة هذا البحث المتواضع.

كما يسرني أن أتقدم بالشكر الجزيل إلى التي

شجعتني ووقفت وراء هذا العمل المتواضع

بمجوداتها و نصائحها القيّمة

أستاذتي المشرفة:براهمي حنان

# إهداء

إلى التي أهدتني نور الحياة و سقتني من دفقات حبها و رعايتها

إلى التي قدمت لي آيات الحب و الحنان، إلى أعذب كلمة رددها لساني

إلى من وضعت الجنة تحت قدميها، إلى أمي الحبيبة أطال الله في عمرها .

إلى الذي استلهمت منه معاني الثبات وزرع في قلبي حب العلم ووضع بين جنباتي القوة والعزيمة،إلى الذي وهبني كل رعايته واهتمامه،إلى أبي العزيز أدامه الله لي .

إلى قلبي وهو قلبي خطيبي مأمون

إلى من أشد بهم أزري أختي سماح والهام

إلى أخي الغالي عبد العزيز

إلى جميع الأصدقاء

# مقدمة

عرفت الجريمة منذ فجر البشرية فقد ناهضها الإنسان منذ اللحظة الأولى ، حيث استشعر فيها بخطر يهدد كيانه وتقدمه، فالجريمة وليدة ما تمر به المجتمعات من ظروف و أسباب ، حيث أن مرجع ذلك إلى ما يحويه السلوك الإنساني في علاقاته المتشابكة بين الخير والشر.

ومن الثابت أن الجريمة والنشاط المعادي للمجتمع اقتحمه نوع جديد من المجرمين إلى جانب المجرم التقليدي الذي عهدناه في الماضي و الذي كانت تقصر جرائمه على أبعادها الفردية والاجتماعية ، وذلك نتاج تطور نمط حياة الإنسان ولقد بلغ هذا التطور أوجه بظهور الدولة بمفهومها العاصر.

لقد عرفت العديد من الدول تطورا هاما في مختلف الميادين ومن نتائجه ظهور ما يعرف بالمعلوماتية ، هذه الأخيرة التي تعتبر سمة العصر والمقياس الذي يحدد مدى تقدم الشعوب وكذا مساهمتها في تسريع انجاز الأعمال فكان لزاما على الدول من اجل ضمان نهضتها و تماشيا مع عصر المعلوماتية أن تعمل على مواكبة التطور التكنولوجي الذي نجم عنه تحول العديد من الدول إلى مجتمعات الكترونية تعتمد على الرقمية في أداء أعمالها.

ولقد نجم عن هذه الثورة أثار سلبية أثرت على حقوق الأفراد و حرياتهم، نتيجة استغلال الأفراد والجهات للتقنية المعلوماتية في غير الغرض الذي خلقت من اجله و أضحى هذا النظام محلا للاعتداء وإساءة استخدامه، فقد ترتب على ذلك إحاطة هذه الظواهر بكثير من الغموض حتى دعا ذلك الكثيرين إلى القول أن الجريمة المعلوماتية هي أشبه بالخرافة و انه لا يوجد تهديد حقيقي بالحسابات الآلية فهي في حقيقتها جرائم يمكن بشأنها تطبيق النصوص التقليدية القائمة دون أن تتميز بأي سمات خاصة .

كما اختلفت آراء الفقه في شان تطبيق النصوص التقليدية عليها، وتضاربت أحكام القضاء في البلد الواحد بصفة عامة واتخذت بعض المحاولات طابعا إقليميا و البعض الأخر طابعا دوليا ، كما أظهرت هذه المحاولات الطبيعة الخاصة للجريمة المعلوماتية حتى في

الحالات التي تلبس فيهل هذه الجريمة ثوب بعض الجرائم التقليدية كالسرقة و النصب و التزوير و خيانة الأمانة .

ولهذا القي على عاتق المشرع الدولي و المشرع الجزائري مسؤولية موجهة الجرائم الالكترونية في ظل قصور نصوص قانون العقوبات عن الإحاطة بهده الجرائم.

وعليه فان موضوع جرائم المساس بالأنظمة المعلوماتية يعد من الموضوعات الهامة الجديدة التي باتت الحاجة إلى دراستها دراسة جديدة و متأنية من قبل دارسي القانون من الأمور الضرورية وهو الأمر الذي دفعنا إلى اختيار و إجراء دراستنا المتواضعة في هذا المجال القانوني الخصب، بالإضافة إلى انه موضوع يتسم بالمرونة والتطور الهائل في شتى الميادين.

هذا ما أدى بنا إلى طرح الإشكالية التي مفادها:فيما يكمن دور المشرع الدولي والمشرع الجزائري في مكافحة جرائم المساس بالأنظمة المعلوماتية؟

ويندرج تحت هذه الإشكالية التساؤلات الآتية:

هل ينطبق وصف الجريمة التقليدية على تلك الالكترونية ؟ وهل يمكن تطبيق أركان الجرائم التقليدية ذات الطبيعة المادة والملموسة على تلك القيم غير المادية المتولدة عن المعلوماتية؟

يسعى هذا البحث إلى تحقيق هدفه الرئيسي المتمثل في محاولة تقديم دراسة تكشف عن أهم التحديات القانونية وذلك عبر رصد جوانب مختلفة من ملامح الظاهرة الإجرامية لجرائم المساس بالأنظمة المعلوماتية، ولتحقيق هذا الهدف ستحاول الدراسة التعرف على عدد من المفاهيم المرتبطة بهذه الظاهرة وهذا على النحو التالي :

1-التعرف على الطبيعة الإجرامية لجرائم المساس بالأنظمة المعلوماتية .
2-تحديد أهم التصنيفات شيوعا باستخدام الكمبيوتر و شبكة الانترنت .
3-التعرف على دور التعاون الدولي لمكافحة جرائم المساس بالأنظمة المعلوماتية.
4-التطرق إلى موقف التشريعات العالمية والداخلية من جرائم المساس بالأنظمة المعلوماتية.

لذلك سنعالج موضوع الجريمة المعلوماتية متبعين منهجا يتماشى وطبيعة الموضوع، والمنهج الأفضل في رأينا للخوض في هذا البحث هو المنهج الوصفي التحليلي لان دراستنا ستعتمد على وصف الجرائم المعلوماتية ،وتحليل أهم النصوص القانونية المنظمة للجريمة المعلوماتية في مختلف التشريعات ،بالإضافة إلى المنهج المقارن كوننا سنقوم بالمقارنة بين التشريعات الدولية والداخلية.

ولأجل هذا الغرض قسمنا موضوع البحث إلى مبحث تمهيدي تعرضنا فيه إلى أسباب ظهور الجريمة المعلوماتية و دوافع ارتكابها، كما قسمناه إلى فصلين، فصل أول خصصناه لتحديد مفهوم الجريمة المعلوماتية من خلال تعريفها و خصائصها و أسس تصنيفها، وذلك في ثلاث مباحث.

أما الفصل الثاني القينا من خلاله الضوء على مكافحة جرائم المساس بالأنظمة المعلوماتية، ونفصل ذلك بالتعرض إلى أهم الاتفاقيات الدولية والجهود التشريعية الدولية والداخلية من خلال ثلاث مباحث.

## مبحث تمهيدي: أسباب ظهور جرائم المساس بالأنظمة المعلوماتية ودوافع ارتكابها

إذا كان الكمبيوتر أو الحاسوب هو الأدلة المستخدمة في ارتكاب الجريمة المعلوماتية فمنطقي أن يكون هناك محل لارتكابها وهذا ما بعرف بالمعلوماتية والذي سندرسه من خلال هذا المبحث.

### المطلب الأول: أسباب ظهور جرائم المساس بالأنظمة المعلوماتية

تعد الولايات المتحدة الأمريكية مهد المجتمع الالكتروني وهي أول بلد الكتروني في العالم إلى حد وصف فيه بعض كتاب الولايات المتحدة الأمريكية "بالجمهورية الالكترونية".

إذ تمثل الستينات من القرن العشرين فترة فريدة من نوعها في تاريخ الولايات المتحدة الأمريكية، ففي بدايتها وصلت الصواريخ النووية إلى كوبا، وارتفعت حدة الحرب الباردة مع روسيا إلى نقطة الغليان وأصبح تهديد السلاح النووي أحد الثوابت اليومية في العالم، هذه الحرب كان يغذيها الخوف العام، وكانت الاعتقاد كان الأنصار التكنولوجي هو الذي يحدد المنتصر[1].

وما كان يدعم الخوف الأمريكي أكثر هو حدوث انتصار تكنولوجيا سوفياتي في نهاية الخمسينات، عندما أعن راديو موسكو يوم 4 أكتوبر 1957 أن الاتحاد السوفياتي أطلق في الفضاء قمرا صناعيا يزن 83 كيلوغراما اسمه "سيوتنيك" وساد الاعتقاد أن الولايات المتحدة الأمريكية ستكون أولن يتعرض لهجوم نووي في حالة نشوب حرب نووية لذلك اتخذت الإدارة الأمريكية قرارا بصنع صاروخ أمريكي، وفي 06 ديسمبر 1956 كانت الأمة الأمريكية برمتها تشاهد على شاشة التلفزيون إطلاق هذا الصاروخ لكن انهار وانفجر غير أن واشنطن اعتبرت ذلك عملية ناجحة فأنشأت وكالة الفضاء الأمريكي–نازا "NASA"عام 1958 وقبل ذلك أي في عام 1957 أنشأت كتابة الدولة للدفاع وكالة "آربا" .advanced .Researd (A.R.P.A) Projects .Advanced لتدعيم البحث العلمي لأغراض عسكرية بسبب تزايد التخوفات من الانتصار السوفياتي، هذه الوكالة ستلعب دورا رئيسا في نشأن الانترنت "شبكة المعلومات

[1]- محمد سامي الشوا، **ثورة المعلومات وانعكاساتها على قانون العقوبات**، دار النهضة العربية، القاهرة، 1988، ص 30.

العالمية" ولما كانت التكنولوجيا هي التي تحدد المنتصر، فإن منتوجاتها ظلت تتوالى بشرعة بالغة وليس هناك مجالا يطور بشكل سريع الوتيرة مثل الكمبيوتر [1].

وكان السؤال الهام المطروح في الولايات المتحدة الأمريكية هو كيف يمكن حماية المعلومات العسكرية الأمريكية في حالة حدوث أي هجوم نووي سوفياتي؟ إن هذا السؤال يعتبر بمثابة "الأم" التي ولدت المعلومات العالمية.

إذ بحلول نهاية الستينات، كان لدى كل مركز بحث في الولايات المتحدة الأمريكية ممول فيدرالي بما في ذلك مراكز البحث للمشاريع المستهدفة للربح والجامعات ومرفق بكمبيوتر مجهز بأحدث التكنولوجيا التي وفرتها صناعة الكمبيوتر البادئة في الازدهار في أمريكا وبسرعة فائقة.

مما سبق نجد أن "الانترنت شبكة المعلوماتية" تولدت عن الرعب النووي بالولايات المتحدة الأمريكية وعندما تم التفكير في شبكة معلومات قادرة على الصمود أمام أي تدمير محتمل الوقوع، تم تكليف وكالة مشروعات البحوث المتقدمة "آربا" (A.R.P.A)التابعة لوزارة الدفاع بتحديد الطريق المثلى لربط بين مختلف مواقع الكمبيوتر وفي عام 1968م نجحت المخابر القومية للفيزياء ببريطانيا، في اكتشاف طريقة اتصال بين أجهزة الكمبيوتر المختلفة تسمى طريقة تحو يل الحشود (Switching paket) والتي توفر مرونة وجدارة هائلة في نقل الأوامر والبيانات من كمبيوتر إلى آخر، وهذه الطريقة هي التي حلت مشكلة إنشاء شبكة يمكن أن تنجو من أي هجوم نووي محتمل فطريقة تحو يل الحشود لا تعتمد على روابط بين جهازي كمبيوتر إلى آخر حتى تصل الجهاز المعني[2].

ويتم تقسيم الرسائل ضخمة الحجم إلى مجموعة من الحشود، يوضع لكل منها عنوان ور قم تسلسلي بحيث يمكن في نهاية الأمر تجميع الرسالة عندما تصل إلى مبتغاها.

وقد استفادت وكالة "آربا" من هذه التكنولوجيا، ووضعت أول شبكة عام 1969 تسمى شبكة آربنات. (arpanet)

وقد تم وضعها بجامعة كاليفورنيا بلوس أنجلوس (U.C.L.A) تربط بين أربعة أدمغة الكترونية إذ نجاح تجربة تحويل الحشود، شجع نمو الشبكات، لان أي كمبيوتر أصبح في مرتبة مساوية لأي كمبيوتر آخر داخل الشبكة وتم بذلك "إلغاء مركزية التحكم".

---

[1]– جميل عبد القادرة الصغير، **الانترنت والقانون الجنائي**، دار النهضة العربية ،القاهرة، 2002، ص 4 و ما بعدها.

[2]– جميل عبد القادر الصغير،المرجع السابق، ص 07، 08.

ولم تكد سنة1972 تحل حتى كان أربعين(40)موقعا مختلفا مرتبطا بشبكة "آربا" بعدها كانت عام 1969 تقتصر على أربعة مواقع فقط.

إن هذا النمو في الشبكات الالكترونية هو الذي أدى إلى عقد مؤتمر دولي للاتصالات بالكمبيوتر عام 1972 بواشنطن حضره عدة مختصين من عدة بلدان متقدمة مثل: فرنسا، بريطانيا.... ومن خلال عاين هؤلاء المختصون، التشغيل النموذجي لشبكة "آربا" وناقشوه فيه اتفاقية حول(بروتوكولات الاتصال) بين أجهزة الكمبيوتر والشبكات المعلوماتية المختلفة.

وبحلول عام 1974 أخرج (فنتوون سيرف) وهو أحد مؤسسي شبكة "آربا" بالولايات المتحدة الأمريكية، وأيضا(روبرت كان)من مؤسسي شبكة "آربا" بوتوكول الأنترنت (شبكة المعلومات العالمية) Internet Protocol ويرمز إليه بـ (IP) وبروتوكول التحكم في الإرسال الذي يرمز إليه شبكة المعلوماتية (T.C.P) ولهذين البرتوكولين الفضل في تحديد الطريقة التي تنتقل بها الرسائل والملفات والمعلومات بن شبكات الكمبيوتر داخل الانترنت.

وبين عامي 1972 و1974 ظهرت عدة بروتوكولات اتصالية، ظهر البريد الالكتروني (Email) في 1977.

إن شبكة "آربا" التي كان لها الفضل في هندسة الشبكة المعلوماتية وإنشائها عدلت من اسمها عام1973 إلى اسم وكالة مشروعات الأبحاث الدفاعية المتقدمة(D. A.P.A)

(Project agency defensy defense advenced research)

أما شبكة (آربانات) ففي عام 1983 انقسمت إلى شبكتين هما(آربانات) و(ميلنات) Milinet

وترتبط هذه الأخيرة مباشرة بالشبكة العسكري الأمريكية.

وظلت (الآربنات) بمثابة النخاع الشوكي لشبكة المعلومات(الانترنت) في الولايات المتحدة الأمريكية إلى غاية 1990.

وهي السنة نفسها التي أنتجت فيها (الآربانات) مع الشبكة القومية للعلوم N.S.F. Net وظلت هذه الأخيرة بدورها تمثل النخاع الشوكي للانترنت إلى غاية حيث عوض بمجموعة 1995 من الشبكات الكبرى المرتبطة فيما بينها كمثل: كومبيسيرف (Prodigy) وأمريكا على الخطAmerica On line وبهذا فإن العالم مزودا بأكبر شبكة معلوماتية في التاريخ وهي التي

أصبحت تمثل ما صار يعرف حديثا بـ(الطريق الدولي السريع للإعلام والمعلومات)[1] والسبب في ذلك هو النمو المطرد للشبكات الالكترونية اعتبارا من السبعينات من القرن العشرين، إلى أن وصف المختصون هذه السنوات بـ (سنوات الشبكات)، وما تجدر الإشارة إليه، هو أن هناك عدة عوامل ساعدت على نمو الشبكات وتطويرها بما في ذلك شبكة المعلوماتية(الانترنت) منها:

- ظهور الكمبيوتر الشخصي زهيد الثمن في أوائل السبعينات ظهر كمبيوتر الفاكس وفي نفس الوقت طور الباحثون نظاما يعمل على كمبيوتر ديجيتال الشخصي يسمى (Unix) وهذا النظام يستوعب الأداء الشبكاتي، وفي عام 1976 استحدث أحد الباحثين وهو "مايك لاسك Mike Lesk" نظام نسخ يسمى نظام النسخ من يونكس إلى يونكس (U.U.C.P) ويمكن بواسطة أي كمبيوتر مزود بالمدام(modem)أي(مضمن)أن أي كمبيوتر آخر مزود بمضمن وينقل له الملفات وفي عام 1977 بدأت برامج يونكس تغزو السوق- وقد سبق ذكر هذا.
- وفي مطلع عام 1979 نظم مؤسسو شبكة(ثيورينات) اجتماعا شارك فيه عدة باحثين من جامعة(ويس كونس) ووكالة "آربا" ومؤسسة شبكة هامة(N.S.F) وتمخض هذا الاجتماع ميلاد شبكة هامة كانت لها الكلمة في الميلاد الحقيقي لشبكة المعلوماتية الانترنت إنها شبكة البحث

في الإعلام الآلي ( Copputer Xience Research Net work) (C. S.net)

يعتبر العديد من الباحثين أن سنة 1980 هي سنة الميلاد الحقيقي للمعلوماتية(الانترنت) . هذه الشبكة ولدت بعد تمخض وبحث علمي مكثف دام أكثر من عشرين عاما.

وابتدءا من عام1981 بدأت لولايات المتحدة الأمريكية تحضر(حروب الجيل الثالث) جيل الإعلام والمعلومات والذكاء الإنساني وهي الحروب التي تتلاءم مع حيثيات المجتمع الجديد.

[1]- هيثن نيازي فهمي، **رحلة عبر شبكة الانترنت**، طبعة أولى،دون بلد نشر، 1969، ص 103.

## المطلب الثاني: دوافع ارتكاب جرائم المساس بالأنظمة المعلوماتية المعلوماتية

الدافع(الباعث)، الغرض، الغاية، تعبيرات لكل منها دلالته الاصطلاحية في القانون الجنائي، تتصل بما يعرف بالقصد الخاص بالجريمة، وهي مسألة تثير جدلا فقهيا وقضائيا واسعا ذلك أن القاعدة القضائية تقرر أن الباعث ليس من عناصر القصد الجرمي"[1]. وإن الباعث لا أثر له في وجود القصر الجنائي[2]، وإذا كان الاستخدام العادي للتعبيرات المشار إليها يجري على أساس ترافعها في الغالب، فإنه من حيث الدلالة تتمايز وتنتج عن تمايزها آثار قانونية على درجة كبيرة من الأهمية، فالباعث(الدافع) وهو العامل المحرك للإرادة الذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والانتقام. وللجريمة المعلوماتية عدة دوافع على ارتكابها فبعضها يرجع إلى دافع شخصي ومنها ما يرجع إلى دافع خارجي ومنها ما يكون خاضا بالمنشأة، وكل هذه الدوافع تكون مصدرها هو الرغبة الإجرامية، وسنتعرض لكل دافع في الفروع التالية:

### الفرع الأول: الدوافع الشخصية:

يمكن رد الدوافع الشخصية لدى مرتكب الجرائم المعلوماتية دوافع مالية ودوافع ذهنية ونمطية.

أ. **الدوافع المالية:** أحيانا يكون الهدف من ارتكاب الكمبيوتر الحصول على ربح مالي عن طريق المساومة على البرامج والمعلومات المتحصلة بطريق الاختلاس من جهاز الكمبيوتر أو عن طريق استعمال بطاقة سحب آلي مزورة أو منتهية الصلاحية. ولقد أشارت مجلة (Sécurite inform–atique). على لسان الأستاذ متخصصة(packer) وهي مجلة متخصصة في الأمن المعلوماتي أن 43% من حالات الغش المعلن عنه. قد بوشرت من أجل اختلاس أموال، 23.0 %من أجل سرقة المعلومات، 19.0 % أفعال أتلاف، 15.0 % سرقة وقت الآلة. أي الاستعمال غير المشروع لأجل تحقيق منافع شخصية[3].

---

[1]– نجيب حسني ،دروس في القانون الدولي الجنائي ،دار النهضة العربية،القاهرة ، ص 1052.

[2]– أحمد فتحي السرور،**الوسيط في قانون العقوبات (القسم العام)**،دار النهضة العربية، الطبعة السادسة ،القاهرة، 1991،ص427.

[3]– محمد أمين الرومي، **جرائم الكمبيوتر والانترنت**، دار المطبوعات الجامعية، الإسكندرية، 2003، ص 24.

فحب الفرد للمال هو عصب الحياة يدفعه للقرصنة أو السرقة أو الاختلاس، عن طريق الحاسوب للحصول على المال لتلبية حاجاته الأساسية والرغبة الأساسية والرغبة في الثراء السريع الغير المكلف.

ومنذ بداية الظاهرة، فإن الدراسات الأساسية أشارت إلى أنها المحرك الرئيسي لأنشطته.

**ب. الدوافع الذهنية أو النمطية:** الصورة الذهنية لمرتكبي جرائم الحاسوب والإنترنت، غالبا هي صورة البطل والذكي لذي يستحق الإعجاب لا صورة المجرم الذي يستوجب محاكمته فمرتكبو هذه الجرائم يسعون إلى إظهار تفوقهم ومستوى ارتقائهم ببراعتهم، لدرجة أنه إزاء ظهور لأي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغب الآلة، فيحاولون إيجاد وسيلة إلى تحطيمها أو التفوق عليها[1].

فيرى قراصنة الكمبيوتر أن الحصول على المعلومة يجب ألاّ يكون عليه قيد، فالقرصَان يكرس كل جهده في تعلم كيفية اختراق المواقع الممنوعة، وغالبا ما يكون القراصنة مجموعات يكون الهدف منها التعاون و تبادل المعلومات و تقاسم البرامج و الأخبار و يفضل القراصنة أن يكونوا مجهولين حتى يتمكنوا من الاستمرار في التواجد لأطول فترة ممكنة [2].

**الفرع الثاني: الدوافع الخارجية:**

لارتكاب بعض الجرائم المعلوماتية قد يتأثر الإنسان بمؤثرات ودوافع خارجية، نتيجة لوجوده في بيئة المعالجة الآلية للمعلومات، هذا وتعد المؤثرات التي تدفع الإنسان إلى اقتراف مثل هذا السلوك سواءًا بدافع الانتقام، جنوح العظمة، التعاون والتواطؤ على الإضرار والتهديد.

**أ. الانتقام من رب العمل وإلحاق الضرر به:** الباعث على ارتكاب الجريمة المعلوماتية قد يكون الرغبة في الانتقام من شخص ما أو مؤسسة ما أو حتى من بعض الأنشطة السياسية في بعض الدول أو من رب العمل[3].

والانتقام موجود داخل النفس البشرية، فكثير من الأفراد يفصلون تعسفيا أو بغير وجه حق من الشركة أو منظمة حكومية، أو حتى مصرف، وهم يملكون المعلومات والتدريب اللازم والمعرفة الكافية بخفايا هذه الجهة لذا يرتكب الجاني الجريمة رغبة منه في الانتقام ليجعل

---

[1]– نسرين عبد الحميد نبيه، **الجريمة المعلوماتية والمجرم المعلوماتي**، منشأة المعارف، الأردن، بدون سنة ، ص44– 45.

[2]–محمد أمين الرومي، المرجع السابق، ص24.

[3]– نهلا عبد القادر المومني، **الجرائم المعلوماتية**، دار الثقافة للنشر والتوزيع، الطبعة الثانية ،2001، ص 94.

الشركة أو المؤسسة تتكبد الخسَائر المالية الكبيرة من جراء ما يسببه لها من ضرر يحتاج لإصلاحه إلى وقت لا بأس به[1].

فقد دفع الانتقام بمحاسب شاب إلى أن يتلاعب في برامج الكمبيوتر الخاصة بالشركة التي يعمل بها، حيث برمجها على أن تختفي كل البيانات الخاصة بديون الشركة بعد مضي ستة أشهر من تاريخ تركه للعمل وحدث ما أراد بالفعل فبعد أن ترك العمل ومرت ستة أشهر اختفت البيانات الخاصة بديون الشركة نهائيا عن جهاز الكمبيوتر[2].

**ب. الرغبة في كسر النظام والتفوق على تعقيد وسائل تقنية:** اختراق الأنظمة الالكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة كبيرة لمرتكبها وتسلية تغطي أوقات فراغه، ويمكن لنا أن نوضح هذا الأمر من خلال ما ذكره أحد قراصنة الحاسوب: «كانت القرصنة هي النداء الأخير الذي يبعثه دماغي فقد كنت أعود إلى للبيت بعد يوم آخر في الدراسة وأدير تشغيل جهاز الحاسوب وأصبحت عضوا في لجنة قراصنة الأنظمة».

فعلى صعيد آخر قد يكون الدافع وراء ارتكاب الجرائم المعلوماتية هو الرغبة ي قهر الأنظمة الالكترونية والتغلب عليها، إذ يميل مرتكبو هذه الجرائم إظهار تفوقهم على وسائل التكنولوجيا الحديثة.

فمجرمو المعلوماتية يتملكهم شعور بالبحث عن القوة ويؤدي إلى الإحساس بالدونية ففي بعض الأحيان وجد أن مجرد إظهار شعور جنون العظمة هو الدافع وراء ارتكاب الغش المعلوماتي، وفي هذا الشأن نجد المحلل أو المبرمج ألمعلوماتي وهو مفتاح سر كل نظام فيها وقد يندفع تحت تأثير رغبة قوية من أجل تأكيد قدراته التقنية لإدارة المنشأة لارتكاب الجريمة المعلوماتية[3].

---

[1]– نسرين عبد الحميد نبيه، المرجع السابق، ص25.

[2]– محمد أمين الرومي، المرجع السابق، ص 24.

[3]– نهلا عبد القادر المومني، المرجع السابق، ص 92.

## الفصل الأول: مفهوم جرائم المساس بالأنظمة المعلوماتية

إن موضوع الجريمة المعلوماتية يعتبر بحد ذاته موضوع الساعة ومشكل كل الدول العامة ولاسيما الجزائر وتزداد أهمية تلك المسألة أمام الطابع الدولي والعالمي لشبكة الإنترنت فهذه الأخيرة تعتبر سلاح ذو حدين، يعمل بين جنبيه الظلمة والنور ويعكس وجهي الخير والشر في الإنسان، فهو وسيلة للربط والاتصال والتقارب وتبادل المعلومات والمنافع بين بني الإنسان إلاَّ أنه يمكن أن يكون أداة تزوير وتضليل ولبٌ الرذيلة والتعدي على حقوق الآخرين، لذا ظهرت الحاجة الماسة في الحد من هذا الجانب المظل.

ومن خلال هذا الفصل سنحاول استعراض الجريمة المعلوماتية وخصائصها وكذا أسس تصنيف الجرائم المعلوماتية.

### المبحث الأول: تعريف جرائم المساس بالأنظمة المعلوماتية وخصائصها

تعددت تعريفات الجريمة المعلوماتية وتباينت فيما بينها ضيقا واتساعًا وقد أسفر ذلك على تعذر إيجاد فهم مشترك لظاهرة الجريمة المعلوماتية، وما سيتبع ذلك من تسهيل للوصول إلى الحلول المناسبة لمواجهتها، ولسوف نحاول من خلال هذا المبحث الوصول إلى تعريف يتلاءم مع طبيعة الجريمة المعلوماتية لننتقل فيما بعد إلى خصائصها.

#### المطلب الأول: تعريف جرائم المساس بالأنظمة المعلوماتية.

أدت الحداثة التي تتميز بها الجريمة المرتكبة عبر الإنترنت، واختلاف النظم القانونية والثقافية بين الدول، إلى عدم الاتفاق على مصطلح موحد للدلالة عليها، وعدم الاتفاق هذا انجر عنه عدم وضع تعريف موحد لهذه الظاهرة الإجرامية وذلك خشية حصولها في مجال ضيق[1] ، ولذلك فإن الفقه قد انقسم إلى عدة اتجاهات تقوم على أسس مختلفة في تعريف الجريمة المعلوماتية وهي:

[1]– محمد علي عريان، **الجرائم المعلوماتية**، دار الجامعة الجديدة، الإسكندرية، 2004، ص 43.

**الفرع الأول:تعريف الجريمة المعلوماتية على أساس وسيلة ارتكاب الجريمة**

إن أصحابها ينطلقون من أن الجريمة المعلوماتية تتحقق باستخدام الكمبيوتر كوسيلة لارتكاب الجريمة، ومن ذلك تعريف مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها الجرائم التي تلعب فيها البيانات الكمبيوترية دورًا رئيسا[1].

كما عرف الفقه الجريمة المرتكبة عبر الإنترنت بأنها:«هي نشاط إجرامي تستخدم فيه التقنية الالكترونية (الحاسوب الآلي الرقمي وشبكة الإنترنت) بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف»[2].

عرفها الفقيه الألماني تاديمان بأنها: «هي شكل من أشكال السلوك غير المشروع أو الضار بالمجتمع و الذي يرتكب باستخدام الحاسب الآلي»[3]،كما تعرف بأنها : «كل نشاط إجرامي يؤدي فيه نظام الحاسب الآلي دورا لإتمامه على أن يكون هذا الدور على قدر من الأهمية»[4]، وفي ذات الاتجاه عرفت بأنها:« الجرائم التي يكون دور الحاسوب فيها ايجابيا أكثر منه سلبيا»[5]، كما تعرف جرائم الإنترنت «أنها تلك الجرائم الناتجة عن استخدام المعلوماتية والتقنية الحديثة المتعلقة بالكمبيوتر والإنترنت في أعمال وأنشطة إجرامية بهدف أن تحقق عوائد مالية ضخمة يعاد ضخها في الاقتصاد الدولي عبر شبكة الإنترنت باستخدام النقود الالكترونية أو بطاقات السحب التي تحمل أرقاما سرية بالشراء عبر الإنترنت باستخدام النقود أو تداول الأسهم وممارسة الأنشطة التجارية عبر هذه الشبكة»

إن تعريف الجريمة المعلوماتية المعتمد على الوسيلة المستخدمة في ارتكابها، قد تعرض إلى

---

[1]– محمد عبيد الكعبي، **الجرائم الناشئة عن الاستخدام الغير المشروع لشبكة الإنترنت**، دار النهضة العربية، القاهرة، بدون سنة، ص 33.

[2]– عبد الله عبد الكريم عبد الله، **جرائم المعلوماتية والإنترنت(الجرائم الالكترونية)**، منشورات الحلبي الحقوقية، بيروت، طبعة أولى، 2007، ص 15.

[3]– عبد الفتاح بيومي حجازي، **مكافحة جرائم الكمبيوتر والانترنت في القنون العربي النموذجي**،دار الفكر الجامعي، الإسكندرية،2006،ص22.

[4]– نائلة عادل فريد قورة ، **جرائم الحاسب الاقتصادية( دراسة نظرية تطبيقة)**،دار النهضة العربية ،الإسكندرية،2004، ص26.

[5]– عبد الفتاح حجازي بيومي، المرجع السابق،ص 24.

عدة انتقادات مفادها أن تعريف الجريمة يستوجب الرجوع إلى الفعل و الأساس المكون لها ، ليس لمجرد أن الحاسب استخدم في جريمة يتعين أن نعتبرها من جرائم الإنترنت.

**الفرع الثاني:تعريف الجريمة المعلوماتية على أساس شخصي**

يستند أنصار هذا الاتجاه إلى معيار شخصي يستوجب أن يكون فاعل هذه الجرائم ملما بتقنية المعلومات[1]، ومن بين هذه التعريفات نجد تعريف في وزارة العدل في الولايات الأمريكية التي عرفت الجريمة المرتكبة عبر الإنترنت بأنها: «أية جريمة لفاعلها معرفة فنية بتقنية الحاسبات يمكن من ارتكابها»[2]، ومن قبيل هذا التعريف جاء تعريف الأستاذ " David thonasém" لجريمة الإنترنت بأنها«أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب»[3].

إن قصور هذا التعريف واضح إلى أن مجرد توافر المعرفة التقنية بعلم ما لا يكفي في ضوء عدم توافر العناصر الأخرى لتصنيف لجريمة ضمن الجرائم المتعلقة بذلك العلم[4].

**الفرع الثالث: تعريف الجريمة المعلوماتية على أساس موضوع الجريمة**

يذهب اتجاه آخر إلى التركيز على الجانب الموضوعي باعتبار أن هذه الجريمة ليست الجريمة يستخدم الحاسب الآلي كأداة في ارتكابها فحسب بل تقع على الحاسب الآلي وفي داخل نظامه [5]، يرى واضعو هذا التعريف أن الجريمة المرتكبة ليست هي التي يكون النظام المعلوماتي أداة ارتكابها، بل هي التي تقع عليه أو في نطاقه[6].

---

[1]– محمود أحمد عبابنة، **جرائم الحاسوب وأبعادها الدولية**، دار الثقافة للنشر والتوزيع، الأردن، 2005، ص 16.

[2]– محمد عبيد الكعبي، المرجع السابق ، ص 34.

[3]– هشام محمد فريد رستم، "**الجرائم المعلوماتية. أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية موحدة للتدرب التخصصي**"، بحوث مؤتمر القانون والكمبيوتر والإنترنت، من 1–3 ماي 2000، بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثاني، الطبعة الثالثة، 2004، ص 407.

[4]– محمد عبيد الكعبي، المرجع السابق، ص 34.

[5]– عبد الفتاح بيومي حجازي،المرجع السابق،ص 26.

[6]– أحمد خليفة الملط، **الجرائم المعلوماتية**، دار الفكر الجامعي، الإسكندرية، الطبعة الثانية، 2006، ص85،86.

ويوسع البعض من مفهوم هذه الجريمة حيث يعرفها الخبير الأمريكي"Parcker":« كل فعل إجرامي معتمد أيا كانت صلته بالمعلوماتية ينشأ عن خسارة تلحق بالمجني عليه فعل أو مكسب يحققه الفاعل»[1] .

أما في الوقت الحاضر فقد تبين مؤتمر الأمم المتحدة لمنع الجريمة ومعاقبة المجرمين تعريفا جامعا لجرائم الحاسب الآلي وشبكاته؛ حيث عرف الجريمة المعلوماتية بأنها: «أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي» أو شبكة حاسوبية، أو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية؛ جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية[2].

أما تلك التعريفات المتعددة والصادرة عن وجهات نظر قانونية واجتماعية وفلسفية أحيانا، ويمكن بدورنا أن نضع لها تعريف آخر، يتمثل في أن «جرائم تكنولوجيا المعلومات هي كل فعل و عمل وكل سلوك غير مشروع أو غير أخلاقي أو غير مسموح به صادر عن أرادة جنائية يقوم به شخص ما له دراية و معرفة بتكنولوجيا المعلومات المختلفة (تكنولوجيا، التخزين، والاسترجاع وتكنولوجيا اتصالات الحديثة) ويوجه ضد المصلحة العامة والخاصة»، وتشمل تلك الجرائم من الناحية المبدئية جميع الجرائم التي يمكنّ أن ترتكب فيه أو عبر وسط الكتروني، ويقر لها الفانون عقوبة أو تدبير؟

## المطلب الثاني: خصائص جرائم المساس بالأنظمة المعلوماتية

تتميز الجريمة المعلوماتية بصفة عامة عن الجريمة التقليدية في عدة نواح، سواء كان هذا التمييز في السمات العامة لها أو كان في الباعث على تنفيذها أو في طريقة هذا التنفيذ ذاته كما تتميز بطابعها الدولي في أغلب الأحيان حيث تتخطى آثارها هذه الجريمة حدود الدولة الواحدة، ولسوف نبين هذه الخصائص التي ميزت الجريمة المعلوماتية مرتبط بذات الإنسان وشخصيته.

### الفرع الأول: خصوصية الجريمة المعلوماتية:

[1]– محمد أمين أحمد الشوابكة، **جرائم الحاسوب والانترنت(الجريمة المعلوماتية)**، عمان، مكتبة دار الثقافة، 2004، ص 15.

[2]– جعفر حسن جاسم الطائي، **جرائم تكنولوجيا المعلومات(رؤية جديدة للجريمة المعلوماتية)**، دار البداية، عمان، 2007، ص 110.

تتسم الجريمة المعلوماتية بمجموعة من الخصائص التي تميزها عن غيرها من الجرائم التقليدية:

**أولا: صعوبة اكتشاف الجريمة المعلوماتية:** تتسم الجرائم الناشئة عن استخدام الانترنت بأنها خفية ومستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنه من جريمته بدقة. مثلا عند إرسال الفيروسات وسرقة الأموال والبيانات الخاصة أو إتلافها، والتجسس وسرقة المكالمات وغيرها من الجرائم[1].

كما أن وسيلة تنفيذها التي تميز في أغلب الأحيان بالطابع التقني الذي يضفي عليها الكثير من التعقيد بالإضافة إلى الأحجام عن الإبلاغ عنها في حالة اكتشافها لخشية المجني عليهم في فقدان عملائهم فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل الإثبات في مدة تقل عن الثانية الواحدة[2].

كما أن المجني يلعب دورًا رئيسيا في صعوبة اكتشاف وقوع الجريمة المعلوماتية حيث تحرض أكثر الجهات التي تتعرض أنظمتها المعلوماتية لانتهاك أو تمنى بخسائر فادحة من جراء ذلك على عدم الكشف حتى بن موظفيها عما تعرض له وتكتفي عادة بإجراءات داخلية إدارية دون الإبلاغ عنها السلطات المختصة تجنبا للأضرار أو بسمعتها ومكانتها وهو الثقة في كفاءتها[3].

**ثانيا: صعوبة إثبات الجريمة المعلوماتية:** فالجريمة المعلوماتية تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والإنترنت مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة[4]، ونظرا لما تتطلبه هذه الجرائم من تقنية لارتكابها فهي تتطلبه لاكتشافها والبحث عنها، وتستلزم أسلوب خاص في التحقيق والتعامل، الأمر الذي لم يتحقق في الجهات الأمنية والقضائية لدينا، نظرا لنقص المعارف التقية وهو ما يتطلب تخصص في التقنية لتحصين الجهاز الأمني والقضائي الذي ضد هذه الظاهرة.

---

[1]– محمد عبيد الكعبي، المرجع السابق، ص 32.

[2]– نهلا عبد القادر المومني، المرجع السابق، ص 54.

[3]– نهلا عبد القادر المومني ،المرجع السابق، ص 56.

[4]– محمد عبيد الكعبي، المرجع السابق، ص 4.

لم تعد قادرة القوانين التقليدية على مواكبة السرعة الهائلة في التكنولوجيا والتي أدت إلى تطور الجريمة من خلالها، وظهور جرائم لم تكن موجودة في السابق، وباتت القوانين التقليدية القائمة عاجزة عن مواجهتها[1]. ما يشكل عائقا أساسيا أمام إثبات الجريمة المعلوماتية.

**ثالثا: أسلوب ارتكاب الجريمة المعلوماتية:** ذاتية الجرائم المعلوماتية تبرز بصورة أكثر وضوحا في أسلوب ارتكابها وطريقتها فإذا كانت الجريمة التقليدية تتطلب نوعا من الأسلوب العضلي الذي قد يكون في صورة أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو حال جريمة السرقة[2]. وتحتاج كذلك إلى وجود شبكة المعلومات الدولية (الإنترنت مع وجود مجرم يوظف خبرته وقدراته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير لتغرير أو التغرير بالقاصرين كل ذلك دون الحاجة لسفك الدماء).

**رابعا: الجريمة المعلوماتية تتم عادة بتعاون أكثر من شخص:** تتميز الجريمة المعلوماتية عادة أنها تتم بتعاون أكثر من شخص على ارتكابها إضرار بالجهة المجني عليها، وغالب ما يشترك في إخراج الجريمة المعلوماتية إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والإنترنت يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه.

والاشتراك في إخراج الجريمة المعلوماتية إلى حيز الوجود قد يكون إشراكا سلبيا وهو الذي يترجم بصمت من جانب من يعلم بوقوع الجريمة في محاولة منه لتسهيلها وإتمامها ، وقد يكون اشتراكا إيجابيا وهو غالبا كذلك ما يتمثل في مساعدة فنية ومادية.

**خامسا: خصوصية مجرمي المعلوماتية:** المجرم الذي يرتكب الجريمة المعلوماتية الذي يطلق عليه المجرم ألمعلوماتي يتسم بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية (المجرم التقليدي).

فإذا كانت الجرائم التقليدية لا أثر فيها للمستوى العلمي والمعرفي للمجرم في عملية ارتكابها– باعتبارها قاعدة عامة– فإن الأمر يختلف بالنسبة للجرائم المعلوماتية فهي جرائم فنية تقنية في الغالب الأعم، ومن يرتكبها عادة ما يكون من ذوي الاختصاص في مجال تقنية المعلومات، أو

[1]– محمد عبيد الكعيبي ،المرجع السابق، ص40

[2]– نهلا عبد القادر المومني، المرجع السابق، ص57، 58.

على الأقل شخص لديه حد أدنى من المعرفة والقدرة عل استعمال جهاز الحاسوب والتعامل مع شبكة الانترنت[1].

**سادسا: الجريمة المعلوماتية جريمة عابرة للحدود:** بعد ظهور شبكات المعلومات لم يعد هناك كحدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالمقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال قد أدت إلى نتيجة مؤداها أنّ أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد[2]، فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة مما جعل بالإمكان اِرتكاب جريمة عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى. هذه الطبيعة تتميز بها الجريمة المعلوماتية كونها جريمة عابرة الحدود خلقت العديد من المشاكل حول تحديد الدولة صاحبة اختصاص القضائي بهذه الجريمة[3]. فهل هي الدولة التي وقع بها النشاط الإجرامي، أم تلك التي أضرت مصالحها نتيجة لهذا التلاعب، كما أثارت الطبيعة أيضا الشكوك حول مدى فعالية القوانين القائمة في التعامل مع الجريمة المعلوماتية وبصفة خاصة فيما يتعلق بجمع وقبول الأدلة[4].

الحقيقة أن عملية التباعد الجغرافي بين الفعل وتحقيق النتيجة من أكثر الوسائل التي تثير الإشكالات في مجال الحاسوب، وبشكل خاص الإجراءات الجنائية والاختصاص والقانون والواجب والتطبيق، وهذا بدوره عامل رئيسي في نماء دعواته تضافر الجهود الدولية لمكافحة هذه الجرائم، ولعل هذه السمة تذكرنا بإرهاصات جرائم المخدرات والاتجار بالرقيق وغيرها من الجرائم التي وقف تباين الدول واختلاف مستويات الحماية الجنائية فيها حائلا دون نجاعة أساليب مكافحتها، فلم يكن من يد غير الدخول في سلسلة اتفاقيات ومعاهدات دولية لمكافحتها[5].

---

[1]– نهلا عبد القادر المومني، المرجع السابق، ص 58، 59.

[2]-Mascala corinne, «**criminalité et contrat électronique**», Travaux de l'associatio, CAPITANT Henir, journées national, paris, 2000, p119.

[3]– نهلا عبد القادر المومني، المرجع السابق، ص 55.

[4]– نائلة عادل محمد فريد قورة، ،المرجع السابق ،ص 54.

[5]– جعفر حسن جاسم الطائي، المرجع السابق، ص 142.

**الفرع الثاني: السمات الخاصة بالمجرم المعلوماتي**

تتطلب الجريمة المعلوماتية مقدرة عقلية وذهنية خاصة لدى الجاني حيث أن الاعتداءات المرتكبة لا تتطلب إجراءات تميل إلى العنف بقدر ما تتطلب الامامًا بقدر معين من المعرفة، فهو مجرم ذو كفاءة عالية في مجال التقنّية يحتاج إلى جهاز حاسوب موصول بشبكة الإنترنت إلى جانب درايته بمختلف الأنظمة المستعملة في هذا المجال ويمكن حصر هذه السمات عل النحو التالي:

**أولا: المعرفة والمهارة والذكاء:** تعني المعرفة التعرف على كافة الظروف التي تحيط بالجريمة المواد وتنفيذها، وإمكانيات نجاحها، واحتمالات فشلها، فالجناة عادة يمهدون لارتكاب جرائهم بالتعرف على كافة الظروف المحيطة بهم، لتجنب الأمور غير المتوقعة التي من شأنها ضبط أفعالهم والكشف عنهم، وتميز المعرفة بمفهومها السابق مجرمي الانترنت، حيث يستطيع مجرم الانترنت أن يكون تصورا كاملا لجريمته[1].

يتمتع مجرمي الانترنت بقدر لا يستهان به من المهارة بتقنيات الحاسوب والإنترنت، بل إن بعض مرتكبي هذه الجرائم هم من المتخصصين في مجال معالجة المعلومات آليا، فتنفيذ جريمة الإنترنت يتطلب قدرا من المهارة لدى الفاعل التي قد يكتسبها المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات[2].

إجرام الإنترنت هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف، فمجرم الإنترنت يسعى بشغف إلى المعرفة طرق جديدة مبتكرة لا يعرفها أحد سواه وذلك من أجل اختراق الحواجز الأمنية في البيئة الالكترونية ثم نيل مبتغاه.

**ثانيا: مجرم الانترنت يبرر ارتكاب جريمته:** يوجد شعور لدى مرتكب فعل إجرام الانترنت أن ما يقوم به لا يدخل في عداد الجرائم أو بمعنى آخر لا يمكن لهذا الفعل أن يتصف بعدم الأخلاقية وخاصة في الحالات التي يقف فيها السلوك عند قهر نظام الحاسوب وتخطي الحماية المفروضة حوله، حيث يفرق مرتكبو هذه الجرائم بين الإضرار بالأشخاص، الأمر الذي يعدونه

---

[1]– طارق إبراهيم الدسوقي عطية، **(الأمن ألمعلوماتي، النظام القانوني لحماية المعلوماتي)**، دار الجامعة الجديدة للنشر، الإسكندرية، 2009، ص 176، 177.

[2] –Mascala courinne, «**criminolité et contrat électronique**», Op–cit, p118.

غاية في اللاأخلاقية وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم.

فهؤلاء الأشخاص لا يدركون أن سلوكهم يستحق العقاب ويبدو أن الاستخدام المتزايد للأنظمة المعلومات قد أنشأ مناخًا نفسيا موائما لتصور استبعاد فكرة الخير والشر قد ساعد على عدم وجود احتكاك مباشر بالأشخاص ومما لا شك فيه أن هذا التباعد في العلاقة الثنائية بين الفاعل والمجني عليه يسهل المرور إلى الفعل غير المشروع ويساعد على لإيجاد نوع من الإقرار الشرعي الذاتي بمشروعية هذا الفعل[1].

**ثالثا: الخوف من كشف الجريمة:** يتصف المجرمون عبر الانترنت بالخوف من كشف جرائمهم وافتضاح أمرهم، وبالرغم من هذه الخشية تصاحب المجرمين على اختلاف أنماطهم إلاّ أنّها تميز مجرمي الانترنت بصفة خاصة لما يترتب على كشف أمرهم من ارتباك مالي وفقد المركز الوظيفي في كثير من الأحيان[2].

تساعد طبيعة الأنظمة المعلوماتية نفسها مجرمي الانترنت على الحفاظ على سرية أفعالهم، ذلك أن الكثير ما يعرض المجرم إلى اكتشاف أمره هو أن يطرأ في أثناء تنفيذه لجريمته عوامل غير متوقعة لا يمكن التنبؤ بها في حين أن أهم الأسباب التي تساعد على نجاح الجريمة المرتكبة عبر الانترنت هي الحواسيب إنّما تؤدي عملها غالبا بطريقة آلية بحيث لا تتغير المراحل المختلفة التي تمر بها أي من العمليات التي يقوم بها من مرة إلى أخرى.

**رابعا: الميل إلى التقليد:** يبلغ الميل إلى التقليد أقصاه حينما يوجد الفرد وسط الجماعة، إذ يكون عندئذ أسهل وأسرع انسياقا لتأثير الغير عليه، ويظهر ذلك في مجال الجريمة المرتكبة عبر الانترنت لأن أغلب الجرائم تتم من خلال محاولة الفرد تقليد غيره بالمهارات الفنية مِما يؤدي به الأمر إلى ارتكاب الجرائم.

ولا شك أن ذلك نتيجة لعدم الاستواء في شخصية الفرد الذي يتأثر بخاصية الميل إلى التقليد بسبب عدم وجود ضوابط يؤصلها الفرد في ذاته مما يحجم لديه غريزة التفاعل ما الوسط المحيط، وينتهي به الأمر إلى التقليد وارتكاب الجريمة[3].

---

[1]– نهلا عبد القادر المومني، المرجع السابق، ص 55.

[2]–نهلا عبد القادر المومني، المرجع السابق، ص 79.

[3]– أيمن عبد الحفيظ، الاتجاهات الفنية و الأمنية لمواجهة الجرائم المعلوماتية، دون دار النشر، دون بلد النشر، ص 34.

**خامسا: التخطيط التنظيم:** في عالم الشبكات الالكترونية وخاصة شبكة العالمية للانترنت، كما هو الحال في العالم الحقيقي يقوم بمعظم الأعمال الإجرامية أفراد أو مجموعات صغيرة، حيث ترتكب أغلب الجرائم من مجموعة مكونة من عدة أشخاص يحدد لكل شخص دور معين ويتم العمل بينهم وفقا لتخطيط وتنظيم سابق على ارتكاب الجريمة، فغالبا ما يكون متضمنا فيها متخصص في الحاسبات يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية التلاعب ولتحويل المكاسب إليه، كما أن من عادة من يمارسون التلصص والقرصنة على الحاسبات وشبكات المعلومات بصفة منتظمة حول أنشطن هم عقد المؤتمرات[1].

**سادسا: التكيف الإجتماعي:** تعتبر هذه الخاصية امتدادًا لسمة التخطيط والتنظيم، حيث أن التكيف الاجتماعي ينشأ بين مجموعة لها صفات مشتركة فمثلا جماعة صغار نوابغ المعلوماتية لا شك أنهم يتكيفون في أفكارهم فيما بينهم، وتنشأ بالتالي بينهم صفات وروابط تساعدهم على ارتكاب جرائمهم وتتعدى تلك الروابط والصلات النطاق المحلي بحيث تنشأ بينهم روابط دولية تتفق مع أفكارهم ومنهجهم في استثمار تلك المعرفة والتقدم العلمي، ولاشك أن إقامة تلك المؤتمرات الدولية في هؤلاء المجموعات خير دليل على وجود تلك الصلات والروابط الدولية بينها[2].

بالإضافة إلى أن مجرمي الإنترنت هم عادة أناس اجتماعيون قادرين على التكيف في بيئتهم الاجتماعية، ولا يضعون أنفسهم في حالة عداء مع المجتمع الذي يحيط بهم، بل قادرين على التوافق والتصالح مع مجتمعهم باعتبارهم أناس مرتفعو الذكاء، بل أن خطورتهم الإجرامية قد تزداد إذا زاد تكيفهم الاجتماعي مع توافر الشخصية الإجرامية لديهم.

**سابعا : التطور في السلوك الإجرامي:**يساهم وجود المجرم في الانترنت في جماعة إجرامية إلى التأثير في قدرته العقلية وسرعة اكتسابه المهارة التقنية التي تؤدي به إلى التمرد الذاتي على محدودية الدور الذي يقوم به في تنفيذ الجريمة إلى أعلى معدلات المهارة التقنية المتمثلة في اثبات قدرته على القيام بالدور الرئيسي في تنفيذ الجريمة[3].

---

[1]–هشام محمد فريد رستم، المرجع السابق، ص 436، 437.

[2]– أيمن عبد الحفيظ، المرجع السابق، ص16، 17.

[3]–أيمن عبد الحفيظ ،المرجع السابق ،ص 17.

وبناءًا على ما تقدم يمكن أن نقسم المجرم ألمعلوماتي إلى مجموعة من الطوائف المختلفة:

**1) المخترقون أو المتطفلون:** يتحد في هذا الإطار نوعين من المخترقين أو المتطفلين:

أ.الهاكرز (Les hackers): يعرف الهاكرز بأنه الشخص الذي يقوم بإنشاء وتعديل البرمجيات والعتاد الحاسوبي[1]، ويقصد بهم الشباب البالغ المقترن بالمعلوماتية، والحاسبات الآلية، وبعضهم يطلق عليهم صغار نوابغ المعلوماتية، وأغلب هذه الطائفة هم من الطلبة والشباب حاصلين على معرفة في مجال التقنية المعلوماتية، والباعث الأساسي لهذه الطائفة هو الاستمتاع باللعب والمزاح باستخدام هذه التقنية، لإثبات مهاراتهم وقدراتهم باكتشاف وإظهار مواطن الضعف في الأنظمة المعلوماتية، دون أي إلحاق ضرر بها،لديهم الرغبة في المغامرة والتحري والرغبة في الاكتشاف2.

ب. الكراكز :(Les Crackers) : المقتحم وتعرف هذه الطائفة بالمجرمين البالغين أو المخربين المهنيين أو (Crackers) وأعمارهم تتراوح بين25-45 عامًا ومن أبرز سمات وخصائص أفراد هذه الطائفة، أنهم ذوي مكانة في المجتمع وأنهم دائما ما يكونوا من المتخصصين في مجال التقنية الالكترونية. أي أنهم يتمتعون بالمهارات، و معارف فنية في مجال الأنظمة الالكترونية أو المعلوماتية تمكنهم من الهيمنة الكاملة في بيئة المعالجة الآلية للمعلومات[3].

**2) مجرمو الكمبيوتر المحترفون:**

تتميز هذه الطائفة بسعة الخبرة والإدراك الواسع للمهارات التقنية، كما تتميز بالتنظيم والتخطيط للأنشطة التي تتركب من قبل أفرادها. لذا فإن هذه الطائفة تعد الأخطر من بين مجرمي التقنية حيث تهدف اعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم وللجهات التي

---

[1]– أسامة سمير حسين، **الاحتيال الالكتروني(الوجه القبيح للتكنولوجيا)**، الحنادرية للنشر والتوزيع، الأردن، الطبعة الأولى، 2011، ص 134.

[2]–عبد الفتاح بيومي حجازي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت**، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2006، ص46.

[3]–محمد دباس الحميد، ماركو إبراهيم نينو، **حماية أنظمة المعلومات**، دار حامد للنشر والتوزيع، عمان، الطبعة الأولى، 2007، ص73.

كلفتهم اعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم أو للجهات التي كلفتهم وسخرتهم لارتكاب جرائم الكمبيوتر، كما تهدف اعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي[1].

هذه الفئة تعكس اعتداءاتهم ميولا إجرامية خطيرة تنبئ عن رغبتها في إحداث التخريب ويتميز هؤلاء بقدراتهم التقنية الواسع وخبرتهم في مجال الحاسوب والشبكات وهم أكثر خطورة من الصنف الأول فقد يحدثون أضرارًا كبيرة.

**3) الحاقدون:**

هذه الطائفة لا يغلب عليها عدم توافر الأهداف وأغراض الجريمة المتوفرة لدى الطائفتين المتقدمتين، فهم لا يسعون إلى إثبات المقدرات التقنية و المهارية وبنفس الوقت لا يسعون إلى مكاسب مادية أو سياسية، إنما يحرك أنشطتهم الرغبة بالانتقام والثأر كأثر لصاحب العمل معهم أو لتصرف المنشأة المعنية معهم عندما لا يكونوا موظفين فيها، ولهذا فإنهم ينقسمون إما إلى مستخدمي للنظام بوصفهم موظفين أو مشتركين أو علاقة بالنظام محل الجريمة، وإلى غرباء عن النظام تتوفر لديهم أسباب الانتقام من المنشأة المستهدفة في نشاطهم.

ولا يتسم أعضاء هذه الطائفة بالمعرفة التقنية الاحترافية، ومع ذلك يشقى الواحد إلى كافة عناصر المعرفة المتعلقة بالفعل المخصوص الذي ينوي ارتكابه، وتغلب على أنشطتهم من الناحية التقنية واستخدام تقنيات الفيروسات والبرامج تعطيل النظام أو الموقع المستهدف إن كان من مواقع الانترنت.

وليس هناك ضوابط محددة بشأن أعمارهم، كما لا تتوفر عناصر التفاعل بين أعضاء هذه الطائفة ولا يفاخرون بأنشطتهم بل يعمدون على إخفاءها، وهم الطائفة الأسهل من حيث كشف الأنشطة التي قاموا بارتكابه لتوفر ظروف وعوامل تساعد على ذلك[2].

**4) صغار السن:**

كما يسميهم البعض (صغار نوابغ المعلوماتية) يصفهم بأنهم: "الشباب البالغ المفتون بالمعلوماتية والحاسبات الآلية؛ فإن من بينهم في الحقيقة فئة لم تزل دون سن الأهلية مولعين

[1]– جعفر حسن جاسم الطائي، المرجع السابق، ص 162.

[2]– نسرين عبد الحميد نبيه، المرجع السابق، ص42.

بالحوسبة" والاتصال وقد تعددت أوصافهم في الدراسات الاستطلاعية والمسحية، وشاع في نطاق الدراسات الإعلامية والتقنية وصفهم بمصطلح المتعثلمين، الدال حسب تعبير الأستاذ "**توم فورلستر**" على الصغار المتحمسين للحاسوب، بالشعور بالبهجة، دافعهم التحدي لكسر الرموز السرية لتركيبات الحاسوب ويسميهم البعض كذلك بمجانين(معدلات ومعدلات عكسية) بالاستناد إلى كثرة استخدامهم لتقنية المعدل والمعدل العكسي(الموديم)، الذي يعتمد على الاتصال الهاتفي لاختراق شبكة النظم، ويثير مجرمو الحوسبة من هذه الطائفة جدلا واسعا ففي الوقت الذي كثر الحديث فيه عن مخاطر هذه الفئة، على الأقل مواصلتها العبث بالحواسيب ظهرت مؤلفات ودراسات تدافع عن هذه الفئة، لتخرجها من دائرة الإجرام( إلى دائرة العبث وأحيانا البطولة من هذه المؤلفات على سبيل المثال، كتاب(خارج نطاق الدائرة الداخلية كيف تعملها؟) لمؤلفه الأمريكي "لبيل لاندريث". وكتب(الدليل الجديد للمتعثلمين) لمؤلفه "هوجوكوزن"، وكتاب(المتعثلمين–أبطال ثورة الحاسوب) لمؤلفه "ستيفن ليفي"[1].

## المبحث الثاني: أسس تصنيف جرائم المساس بالأنظمة المعلوماتية

تعتبر الجرائم المرتكبة عبر الانترنت من الجرائم المستحدثة، وهي تستهدف الكثير من القطاعات مما جعل تحديدها وتصنيفها يتميز بالصعوبة على عكس الجريمة التقليدية التي يمكن تصنيفها بسهولة فائقة.

ولم يستقر الفقهاء لتصنيف الجريمة المعلوماتية على معيار واحد نظرا لتشعبها فبعضهم يقسمها إلى جرائم ترتكب على نظم الحاسوب وأخرى ترتكب بواسطته، وبعضهم يصنفها إلى ضمن فئات بالاستناد إلى الأسلوب المتبّع في الجريمة، وآخرون يستندون إلى الباعث لارتكاب الجريمة، وغيرهم يؤسس تقسيمه على تعدد محل الاعتداء وكذا الحق المعتدي عليه، فتوزع الجرائم المعلوماتية وفق هذا التقسيم إلى الجرائم الواقعة على الأشخاص، ثم الجرائم الواقعة على الأموال، وأخيرا على أساس الجرائم الواقعة على أمن الدولة.

وهذا ما سنتناوله في المطالب الآتية:

[1]– جعفر حسن جاسم الطائي ،المرجع السابق ،ص163.

## المطلب الأول: الجرائم الواقعة الأشخاص

يعد الهدف الأول والأسمى لوضع القوانين وسن التشريعات، حماية لسلامة الأشخاص من مختلف الانتهاكات التي قد يتعرضون لها، سواء في أبدانهم أو في حياتهم الخاصة أو في سمعتهم أم في شرفهم.

وبتطور الأمر بعد ذلك مع ظهور شبكة الانترنت ورغم الفوائد التي أتت بها، والتسهيلات التي قدمتها في الحياة اليومية للفرد والمجتمع على حد سواء، إلاّ أنها أصبحت سلاح فتاك في يد المجرمين، بالإضافة إلى ذلك فإن المعلومات المتعلقة بالأفراد متداولة بكثرة عبرها، مما يجعلها عرضة للانتهاك والاستعمال من طرف هؤلاء المجرمين، وجعلت سمعة وشرف الأفراد مستباحة.

### الفرع الأول: جرائم القذف والسب وتشويه السمعة

تعد جرائم السب والقذف الأكثر شيوعا في نطاق الشبكة، حيث يستعمل الجاني حسب القواعد العامة جرائم القذف والسب عباراته بذيئة تمس وتخدش شرف المجني عليه، بل إن إرادته اتجهت لذلك بالذات. وبالتطور أصبحت الانترنت إحدى هذه الوسائل إن لم نقل أكثرها رواجا–فعادة ترسل عبارات السب والقذف عبر البريد الصوتي أو ترسم أو تكتب على صفحات الويب ما يؤدي بكل من يدخل هذا الموقع لمشاهدتها أو الإستماع إليها، ويتحقق بذلك ركن العلنية الذي تطلبه الكثير من التشريعات في السب العلني، وإذا لم يطلع عليها أحد فإنه يمكن تطبيق مواد السب أو القذف غير العلني[1].

تعتبر شبكة الانترنت مسرح غير محدود، تتلقى كل ما يدرج عليها دون قيد أو رقابة، لذلك تشكل في بعض حالات سوء استخدامها حالات سلبية شاذة تؤذي البعض إذا تم الشهير بهم عبر إيراد معلومات مغلوطة[2]،حيث يقوم المجرم بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن الضحية، والذي قد يكون فردًا أو مجتمع أو مؤسسة تجارية أو سياسية تتعدد الوسائل المستخدمة في هذا النوع من الجرائم، لكن في مقدمة قائمة هذه الوسائل إنشاء موقع

[1]– محمد عبيد الكعبي، المرجع السابق، ص 88.

[2] – محمد دباس، ماركو ابراهيم نينو، المرجع السابق، ص 68.

على الشبكة يحوي المعلومات المطلوب نشرها أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين[1].

**الفرع الثاني: صناعة ونشر الإباحة**

إذا كان لشبكة الانترنت وجه إيجابي فإن لها وجه سلبي أيضا، ومن هذه الأوجه وجود مواقع شبكة الانترنت تحرض على ممارسة الجنس للكبار والصغار على حد سواء، وتقوم هذه المواقع بنشر صور جنسية فاضحة للبالغين والأطفال[2]، وإذا كانت الدعوى لممارسة الجنس الموجه للبالغين يمكن أن تلاقي الرفض لتوافر تمام العقل لديهم، فإن الوضع بالنسبة للطفل يختلف لصغر وعدم اكتمال نضجه العقلي[3]، حيث يضر استخدام الأطفال المستخدمين في إنتاج هذه المواد اعتداء ويمثل عليهم في كل مرة يتم فيها عرض هذه الصورة، وبهذه الطريقة يظهر كل الأطفال كأهداف للاستغلال الجنسي[4]، ويتخذ الاستغلال الجنسي الأطفال على الانترنت أشكالا متعددة انطلاقا من الصور ووصولا إلى التسجيلات المرئية لجرائم الجنسية العنيفة، وتستمر معاناة الضحايا حتى بعد الانتهاء الفعلي الذي تعرضوا له بسبب إمكان تنقل الصور على الانترنت إلى مالا نهاية.

**الفرع الثالث: جريمة التهديد والمضايقة**

يقصد بالتهديد الوعيد بالشر، وهو زرع الخوف في النفس بالضغط على إرادة الإنسان، وتخويفه من أضرار ما سيلحقه أو سيلحق أشياء أو أشخاص له بها صلة[5]، ويعد تهديد الغير من خلال البريد الالكتروني واحدًا من أهم الاستخدامات غير المشروعة للانترنت حيث يقوم

---

[1] – محمد أمين أحمد الشوابكة، المرجع السابق ، ص 32،91.

[2]-Fauchoux. Vincent- Deprerz pierre,**le Droit de l'internet (loi, contra et u sage),** édition, litec, Paris, 2008, p 215.

[3]–عبد الكريم خالد الشامي،« **جرائم الكمبيوتر والانترنت في التشريع الفلسطيني**»، ص19،: http://www-pal-ip. org

[4]–كريستينا سكولمان، «**عن جرائم الانترنت: طبيعتها وخصائصها**»، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، أيام19 –20 يونيو 2007، ص40.

[5]– محمد عبيد الكعبي، المرجع السابق، ص 88.

الفاعل بإرسال رسالة الكترونية للمجني عليه تنطوي على عبارات تسبب خوفا أو ترويعا لمتلقيها[1].

تتم في هذا النطاق جرائم الملاحقة عبر شبكة الانترنت باستخدام البريد الالكتروني أو وسائل الحوارات الآنية المختلفة على الشبكة، وتشمل الملاحقة رسائل تخويف ومضايقة، وتتفق مع مثيلاتها في خارج الشبكة في الأهداف المجسدة في رغبة التحكم في الضحية، وتتميز عنها بسهولة إمكانية إخفاء هوية المجرم علاوة على تعدد وسهولة وسائل الاتصال عبر الشبكة، الأمر الذي ساعد في تفشي هذه الجريمة[2].

**الفرع الرابع: انتحال الشخصية والتغرير والاستدراج**

يقصد بانتحال الشخصية ما يعيد إليه المجرم من استخدام شخصية شخص آخر للاستفادة من سمعته مثلا أو ماله أو صلاحياته، ولذلك فهذا سبب وجيه يدعو للاهتمام بخصوصية وسرية المعلومات الشخصية للمستفيدين على شبكة الانترنت، وتتخذ جريمة انتحال الشخصية عبر الانترنت أحد الوجهين التالين: انتحال شخصية الفرد وانتحال شخصية المواقع.

ولقد سماها بعض المتخصصين في أمن المعلومات جريمة الألفية الجديدة وذلك نظرا لسرعة انتشار ارتكابها في الأوساط التجارية[3].

أما فيما يخص التغرير والاستدراج فغالبا ضحايا هذا النوع من الجرائم هم صغار السن من مستخدمي الشبكة، حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين صداقة على الانترنت والتي قد تتطور إلى التقاء مادي بين الطرفين، إن مجرمي التغرير والاستدراج على شبكة الانترنت يمكن لهم أن يتجاوزا الحدود السياسية فقد يكون المجرم في بلد والضحية في بلد آخر، وكون معظم الضحايا هم من صغار السن، فإن كثير من الحوادث لا يتم الإبلاغ عنها، حيث لا يدرى كثير من الضحايا أنهم غرّر بهم.

---

[1]–عبد الله بن معيض العبيدي، **الحماية الجنائية للتعاملات الالكترونية في نظام المملكة العربية السعودية (دراسة تحليلية مقارنة)** ، بحث مقدم استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص سياسة جنائية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجناية، الرياض، 2009، ص 52.

[2]– إلياس بن سمير الهاجري، « **جرائم الانترنت** »، الدورة التدريبية لمكافحة الجرائم الارهابية المعلوماتية المنعقدة بكلية التدريب، قسم البرامج التدريبية، القنيطرة، المملكة المغربية من9– 13، 2006، ص 58.

[3]– عمرو موسى الفقهي، **الجرائم المعلوماتية(جرائم الحسب الآلي والانترنت في مصر والدول العربية)**، المكتب الجامعي الحديث، الإسكندرية، 2006، ص 102.

## المطلب الثاني: الواقعة على الأموال

صاحب ظهور شبكة الانترنت تطورات كبيرة في شتى المجالات، حيث أصبحت معظم المعاملات التجارية تتم من خلال هذه الشبكة، مثل البيع والشراء، مما أنجز عنه تطور و سائل الدفع والوفاء وأضحت جزء لا يتجزأ من هذه لمعاملات، وفي خضم هذا التداول المالي عبر الانترنت انتهز بعض المجرمون من أجل السطو عليها، حيث ابتكرت عدة طرق من أجل ذلك، على غرار السرقة والسطو والتحويل الالكتروني غير المشروع للأموال وقرصنة أرقام البطاقات الممغنطة.

### الفرع الأول: السرقة عبر الانترنت:

تعرف السرقة بأنها اختلاس الشيء منقول مملوك للغير بدون رضاه بنية امتلاكه[1]، وتتم سرقة المال المعلوماتي إن أمكن الوصف–عن طريق اختلاف البيانات والمعلومات، والإفادة منها باستخدام السارق للمعلومات الشخصية– مثل الاسم، العنوان، الأرقام الخاصة بالمجني عليهم، والاستخدام غير الشرعي لشخصية المجني عليه ليبدأ بها عملية السرقة المتخفية عبر الانترنت بحيث يؤدي بالغير إلى تقديم الأموال–الالكترونية أو المادية–إلى الجاني عن طريق التحويل البنكي[2].

تتجسد جريمة السطو على أموال البنوك عن طريق استخدام الشخص الآلي للدخول إلى شبكة الإنترنت و الوصول غير المشروع إلى البنوك و المصارف و المؤسسات المالية.[3]

### الفرع الثاني: جرائم السطو على أرقام بطاقات الائتمان والتحويل الالكتروني غير المشرع للأموال.

واكب استخدام البطاقات الائتمانية من خلال شبكة الانترنت ظهور الكثير من المتسللين للسطو عليها. باعتبارها نقودا الكترونية، خاصة من جهة أن الاستيلاء على بطاقات الائتمان أمر ليس بالصعوبة كما كان، فلصوص بطاقات الائتمان مثلا يستطيعون الآن سرقة مئات

---

[1]– نايف بن محمد المرواني، **جريمة السرقة(دراسة نفسية اجتماعية)** جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2011، ص 59.

[2]– محمد أمين أحمد الشوابكة، **جرائم الحاسوب والانترنت**، مكتبة دار الثقافة للنشر والتوزيع، عمان، 2004، ص 138.

[3]-عباس أبو شامة عبد المحمود ، **عولمة الجريمة الاقتصادية**، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007، ص 20.

الألوف من أرقام البطاقات في يوم واحد من خلال شبكة الانترنت ومن ثم بيع هذه المعلومات للآخرين[1].

تتم عملية التحويل الالكتروني غير المشرع للأموال من خلال الحصول على كلمة السر المدرجة في ملفات أنظمة الكمبيوتر الخاصة بالمجني عليه. مما يسمح للجاني بالتوغل في النظام المعلوماتي وعادة ما يكون هؤلاء من العاملين على إدخال البيانات في ذاكرة الجهاز أو من قبل المتواجدين على الشبكة أثناء عملية تبادل البيانات[2]، وتتم عملية التحويل الالكتروني غير المشروع للأموال بأحد الطرق الموالية:

أ. **الاحتيال:** ويتم ذلك بطريقة احتيالية يوهم من أجلها المجني عليه بوجود مشروع كاذب أو يحدث الأمل لديه بحصول ربح، فيسلم المال للجاني بطريق معلوماتي أو من خلال تصرف الجاني في المال وهو يعلم أن ليس له صفة التصرف فيه[3].

**ب. الاحتيال باستخدام بطاقات الدفع الالكتروني:** يعتمد نظام بطاقات الدفع الالكتروني على عمليات التحويل الالكتروني من حساب بطاقة العميل بالبنك المصدر للبطاقة إلى رصيد التاجر أو الدائن الذي يوجد به حسابه وذلك من خلال شبكة التسوية الالكترونية للهيئات الدولية«هيئة الفيزا كارد»، «هيئة الماستر كارد»[4]، وتعطي بطاقة الدفع الالكتروني الحق للعميل بالحصول على السلع والخدمات على الشبكة عن طريق تصريح كتابي أو تلفوني، بخصم القيمة على حساب بطاقة الدفع الالكتروني الخاصة به، وتتم العملية بدخول العميل أو الزبون إلى موقع التاجر ويختار السلع المراد شراءها ويتم التعاقد بملأ النموذج الالكتروني ببيانات بطاقة الائتمان

---

[1]– حسن طاهر داود، **جرائم نظم المعلومات**، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2000، ص 73.

[2]– خالد ممدوح إبراهيم، **أمن الجريمة المعلوماتية**، الدار الجامعية، الإسكندرية، 2010، ص 76.

[3]– يونس عرب، «**قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وتجربة سلطة عمان**»، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، المنعقدة بمسقط، سلطة عمان، 2–4أفريل، 2006، ص16.

[4]–عمر الشيخ الأصم، «**البطاقات الائتمانية المستخدمة الأكثر انتشارا في البلاد العربية**»، أعمال ندوة تزوير البطاقات الائتمانية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2002، ص 12.

الخاصة بالمشتري[1]، وأمام التطور التكنولوجي أصبحت إمكانية خلق مفاتيح البطاقات والحسابات البنكية بالحساب غير المشروع ممكنة عبر قنوات شبكة الانترنت.

**الفرع الثالث: القمار وغسيل الأموال عبر الانترنت:**

كثيرا ما تتداخل عملية غسيل الأموال مع القمار عبر شبكة الانترنت مما زاد من انتشار أندية القمار الافتراضية، الأمر الذي جعل مواقع الكازينوهات الافتراضية عبر انترنت محل اشتباه ومراقبة، ومن البديهي أن يأخذ المجرمون بأخذ ما توصلت إليهم التقنية لخدمة أنشطتهم الإجرامية ويشمل ذلك بالطبع طرق غسيل الأموال التي استفادت من عصر التقنية فلجأت إلى الانترنت لتوسعت وتسريع أعمالها في غسيل أموالها غير المشروعة[2].

وقد ساعدت شبكة الانترنت القائمون بعمليات غسيل الأموال بين الدول وتفادي القوانين التي قد تضعها الدول من أجل إعاقة هذا النشاط وكذا تشفير عملياتهم مما يعطيها قدر كبير من السرية، وخاصة في تسهيل مرتكبي جرائم غسيل الأموال نقلها إلى أي مكان في العالم[3].

**الفرع الرابع: تجارة المخدرات عبر الانترنت**

أظهر عصر الانترنت مخاوف من مواقع السوء إن صح التعبير وهو تعريف مقارب لرفيق السوء، ومن تلك المواقع طبعا المواقع المنتشرة عبر الانترنت والتي لا تتعلق بالترويج للمخدرات وتشويق النشء لاستخدامها بل تتعداه إلى تعليم كيفية زراعة وصناعة المخدرات بكافة أصنافها وأنواعها وبأبسط الوسائل المتاحة[4].

والأمر هنا لا يحتاج إلى رفاق سوء بل يمكن للمراهق الانزواء في غرفته والدخول إلى هذه المواقع ومن ثم تطبيق ما يقرأه ويؤكد هذه المخوف أحد الخبراء التربويين في بتسبيرج بالولايات

---

[1]–محمد عبد الرسول خياط، «**عمليات تزوير البطاقات الائتمانية**»، أعمال ندوة تزوير البطاقات الائتمانية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2002، ص 41.

[2]– محمد زيدان، محمد حمو،«**متطلبات أمن المعلومات المصرفية في بيئة الانترنت**»، المؤتمر السادس لجمعيات المكتبات والمعلوماتى السعودية، بيئة المعلومات الآمنة المفاهيم والتشريعات والتطبيقات، 6–7أفريل 2010، الرياض، ص 9.

[3]– خالد بن عبد الله بن معيض العبيدي، **الحماية الجنائية للتعاملات الالكترونية**،في نظام المملكة العربية السعودية جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم الجناية، الرياض، 2009، ص 50.

[4]–محمد محمد صالح الألفي،«**أنماط جرائم الانترنت**»، ص11،**http://www-eastlaws. com**

المتحدة الأمريكية والذي أكد أنه ثمة علاقة يمكن ملاحظتها بين ثالوث المراهقة والمخدرات والانترنت.

## المطلب الثالث: جرائم واقعة أمن الدول

استغلت الكثير من الجماعات المتطرفة الطبعة الاتصالية للانترنت من أجل بث معتقداتها وأفكارها، بل تعداه الأمر إلى ممارسات تهدد أمن الدولة المعتدى عليها، خاصة المتمثلة في الإرهاب والجريمة المنظمة، اللذان أخذا معنى آخر في استعمال الانترنت، التي سمعت لهم في ارتكاب جرائم غاية الشك في حق المجتمعات والدول، بل الأخطر من ذلك أتاحت، الانترنت لكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالاطلاع على مختلف الأسرار العسكرية الاقتصادية لهذه الأخيرة، خاصة فيما يتعلق بالدول التي يكون فيها نزاعات، ويبقى المساس بالأمن الفكري من بين اخطر الجرائم المرتكبة عبر الانترنت ،حيث تعطي الانترنت فرصا للتأثير على معتقدات وتقاليد مجتمعات بأكملها مما يسهل خلق الفوضى.

### الفرع الأول: الجرائم الماسة بالأمن الفكري

ينطوي الخوف من عواقب الخوف من عواقب الثورة المعلومات والاتصال على تيار عاطفي خفي وقوي، يتمسك بثقافة وقيم ومفاهيم أخذت قاعدتها الاجتماعية والمادية والتربوية تتزعزع، وغدا باديا للعيان أنها اليوم تترفع تحت وطأة قوى التكنولوجيا والمعلوماتية والاتصالية التي تلح علينا بالانفتاح بالمعرفة والصوت والصورة، وإذا كنا قد تغيرنا عن آبائنا دون ضجة كبيرة كالحاصلة اليوم، فهل يمكن أن نتوقع غير ذلك بصدد أولادنا؟

تتجسد الإجابة بناء على خصائص الشبكة العالمية الانترنت التي منحت المستخدم الكثير من الخيارات، من خلال عدم خضوعها لأي رقابة وعبورها للحدود الجغرافية بين الدول، ونموها السريع المتواصل، وإمكانية مشاركة الجميع من مختلف دول العالم، مع ما تمنحه من القدرة على التخفي وعدم المواجهة نتيجة لافتراضية التي تعد من أهم خصائص هذه الشبكة، إضافة إلى الكم الهائل من المعلومات التي يمكن الحصول عليها من عدة مصادر لا يمكن التحكم فيها ومتابعتها أو الإشراف عليها، كل ذلك جعل هذه الشبكة، من أهم مقومات المجتمع

المعلوماتي التي تؤدي إلى الانحراف الفكري من خلال تعرض الشخص إلى الكثير من المؤثرات الفكرية التي تستخدم الشبكة العلمية للانترنت، وتهدد الأمن بأبعاده كافة[1].

تتوالى عبر الانترنت الهجمات الثقافية، والحضارية التي قد تزعزع الأمن الفكري والعقدي للشعوب المغلوبة على أمرها، وتنشر عبرها القوى الغالبة لفكرها، ولغتها وقيمها.

**الفرع الثاني: الجريمة المنظمة**

تعرف الجريمة المنظمة بأنها تعبير عن مجتمع إجرامي يعمل خارج إطار الشعب والحكومة ويضم بين طياته آلاف المجرمين الذين يعملون وفقا لنظام بالغ الدقة والتعقيد يفوق النظم التي تتبعها أكثر المؤسسات تطورا وتقدما، كما يخضع أفرادها لقواعد قانونية سنّوها لأنفسهم وترفض أحكاما بالغة القسوة على من يخرج عن نظام الجماعة ويلتزمون في أداء أنشطتهم الإجرامية بخطط دقيقة مدروسة يلتزمون بها ويجنون من ورائها الأموال الطائلة[2].

الجريمة المنظمة ليست وليدة التقدم والسهولة وإن كانت استفادت منه فالجريمة المنظمة وبسبب تقدم وسائل الاتصال والتكنولوجيا أصبحت غير محددة لا بقيود الزمان ولا بقيود المكان، بل أصبح انتشارها على نطاق واسع وكبير وأصبحت لا تحدها الحدود الجغرافية، كما استغلت عصابات الجريمة المنظمة الإمكانات المتاحة في وسائل الانترنت في تخطيط وتمرير وتوجيه المخططات الإجرامية وتنفيذ وتوجيه العمليات الإجرامية بيسر وسهولة[3].

اكتشفت جماعات الجريمة المنظمة استخدام التكنولوجيات بصفتها فرص استغلال وتحقيق أرباح غير مشروعة، وفطن المجرمون أيضا أن شبكة الانترنت تستطيع أن تؤمن فرصا جديدة وفوائد جمة للأعمال غير المشروعة.

يعد الترابط بين الجريمة المنظمة و شبكة الانترنت ليس طبيعيا فقط، ولكنه ترابط من المرجح أن يتطور إلى حد بعيد في المستقبل فشبكة الانترنت تؤمن الأقنية والأهداف في نفس

---

[1]– ناصر محمد البقهي، «**اثر التحويل مجتمع معلوماتي على الأمن الفكري**»،المؤتمر الوطني الأول للأمن الفكري المفاهيم والتحديات، كرسي الأمير نايف بن عبد العزيز لدراسات الأمن لفكري بجامعة الملك سعود، المملكة السعودية،22–25جمادى الأولى1430هـ، ص 18.

[2]– نهلا عبد القادر المومني، المرجع السابق، ص 87.

[3]– سامي علي عياد، **الجريمة المعلوماتية والانترنت(الجرائم الالكترونية)**، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2007، ص 83.

الوقت للجريمة، وتمكن من استغلال هذه الأقنية والأهداف لتحقيق أرباح كبيرة بأقل قدر ممكن من المخاطر، وجماعات الجريمة المنظمة لا تريد أكثر من ذلك، ولهذا السبب من الأهمية بمكان تحديد بعض الطرق التي تتداخل فيها الجريمة المنظمة حاليا مع الجريمة التي ترتكب من خلال الشبكات الالكترونية[1].

**الفرع الثالث: الإرهاب**

أصبح الإرهاب في الوقت الراهن ظاهرة عالمية ترتبط بعوامل اجتماعية وثقافية وسياسية وتكنولوجية أفرزتها التطورات السريعة والمتلاحقة في العصر الحديث، فقد شهدت العقود الأخيرة من القرن العشرين بروز العديد من التنظيمات المسلحة والعمليات الإرهابية في مختلف أنحاء العالم[2].

يتم بث ثقافة الإرهاب عبر الانترنت عن طريق تأسيس مواقع افتراضية تمثل المنظمات الإرهابية، وهي مواقع آخذة في الازدياد مع زيادة المنظمات الإرهابية حيث تعلن عبر هذه المواقع تحملها مسؤولية إحدى الهجمات التي ارتكبت، أو بيانات تنفي أو تعلق على أخبار صادرة على منظمات أو جهات دولية أخرى.

تجند الجماعات الإرهابية من خلال الانترنت عناصر إرهابية جديدة تساعدهم على تنفيذ أعمالهم الإرهابية، وهم في ذلك يعتمدون على فئة الشباب، خصوصا ضعاف العقل والفكر، فتعلن الجماعة الإرهابية عبر مواقعها على الانترنت حاجتها إلى عناصر انتحارية كما لو كانت تعلن عن وظائف شاغرة للشباب، مستخدمة في ذلك الجانب إلى الجهاد وحثهم إلى الاستشهاد في سبيل الفوز بالجنة[3].

الجدير بالذكر أنه إذا كانت الجماعات إرهابية تسعى إلى الدعاية والترويج لنفسها عن طريق آليات مختلفة منها جذب انتباه وسائل الإعلام المعروفة لتغطية أخبار الجماعة وأنشطتها، إلاّ أن السياسات التحريرية لهذه الوسائل، و المعايير الخاصة بها في نشر أخبار معينة وإسقاط

---

[1]– عبد الله عبد الكريم عبد الله، المرجع السابق، ص 42،43.

[2]– عبد الله بن عبد العزيز اليوسفي، **أساليب تطور البرامج والمناهج التدريبية لمواجهة المستحدثة**، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2004، ص 25.

[3]– محمد سيد سلطان، **قضايا قانونية في أمن المعلومات وحماية البيئة الالكترونية**، دار ناشري للنشر الالكتروني، 2004، ص13، www.Nashiri.net

أخرى كل ذلك يمثل قيودًا على استفادة الجماعات عن نشر وسائل الإعلام عنها، بينما في المقابل تتيح المواقع الالكترونية للجماعات الإرهابية قدرا كبيرا من التحكم في المعلومات والرسائل الإعلامية التي تريد توجيهها، بل تتيح لها المرونة في توجيه الرسائل لفئات مختلفة من الجمهور المستهدف، ورسم صورة ذهنية عن الجماعة وعن أعدائها أيضا[1].

**الفرع الرابع: جريمة التجسس**

ينتج عن الاستخدام المتزايد الحاسبات الآلية في العديد من المجالات، تجميع المعلومات بدرجة كبيرة في موضوع واحد، ويؤدي هذا التخزين في الحاسبات المركزية إلى سهولة التجسس عليها، وعلى المعلومات المخزنة فيها بمختلف درجات سريتها.

ويقصد بالتجسس في هذا الموضوع هو الاطلاع على معلومات خاصة بالغير مؤمنة في جهز آخر، وليس مسموحا لغير المخولين الاطلاع عليها[2].

سهلت شبكة الانترنت الأعمال التجسسية بشكل كبير، حيث يقوم المجرمون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية، وتستهدف عملية التجسس في عصر المعلومات ثلاثة أهداف رئيسية، وهي التجسس العسكري، التجسس السياسي، التجسس الاقتصادي[3].

---

[1]- Debray stéphan, internet face aux substances illicites: complice de la cyber criminalité ou outil de prevention ?, Dess média eléctronique & internet, Université de paris, 8.2002-2003, p 13.

[2]– محمد عبد الرحيم سلطان العلماء،« **جرائم الانترنت والاحتساب عليها**»، مؤتمر القانون والكمبيوتر والانترنت، المنعقد من1–3ماي2000، بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثالث، الطبعة الثالثة، 2004، ص 880.

[3]– علي عدنان الفيل، **الإجرام الالكتروني**، الطبعة الأولى، منشورات زين الحقوقية، دمشق، 2011، ص 96،97.

## الفصل الثاني : مكافحة جرائم المساس بالأنظمة المعلوماتية

فرض الإجرام المعلوماتي نفسه كظاهرة سلبية على المجتمعات بعد التطور المعلوماتي الذي وصل إليه هذه الأخيرة، فبدأ التأثير السلبي لهذا الإجرام واضحا مهددًا للأفراد والجماعات والأموال والحكومات على حد سواء، ولتدارك هذا الخطر بدت عملية المكافحة لجريمة المعلوماتية ضرورة حتمية يجب التصدي لها. خاصة وقد وجدت الدول نفسها عاجزة عن أداء واجبها الدستوري والقانوني لحماية الأفراد وتحقيق هذا النوع الجديد من الإجرام بسب الفراغ القانوني لمكافحته وذلك بتعديل قوانين عقوباتها القائمة وإصدار قوانين عقابية جديدة تتصدى لمكافحة أنواع الإجرام المعلوماتي الجديد. خاصة تلك الرائدة في مجال التطور المعلوماتي كفرنسا وأمريكا والمملكة المتحدة...إلخ، ومدى إخضاع هذه القوانين إلى مبدأ الشرعية. كما أن خطورة هذه الجريمة وعجز الدول منفردة في مكافحتها جعلها توحد جهودها.

فعقدت اتفاقيات ومؤتمرات تأثرت بها القوانين الداخلية إلى حد كبير وهذا ما سنحاول التعرض له في هذا الفصل.

### المبحث الأول: الجرائم المعلوماتية المعاقب عليها في الاتفاقيات الدولية

أمام الصعوبات الكبيرة التي واجهتها الدول في مكافحة الجريمة المعلوماتية عبر قوانينها الداخلية وفي مواجهة أصعب خاصية لها كونها جريمة متعدية الحدود، وجدت الدول نفسها مضطرة لنجاح المكافحة ومن أهم الاتفاقيات الدولي التي تناولت الإجرام ألمعلوماتي، اتفاقية بودابست المنبثقة عن اتفاقيات المجلس الأوروبي كذلك المعاهدات والقوانين الخاصة بحماية الملكية الفكرية واتفاقية العربية المجسدة في إطار القانون النموذجي لمكافحة الجريمة المعلوماتية في المطالب الآتية:

#### المطلب الأول: اتفاقية بودابست 2001 لمكافحة الجريمة المعلوماتية.

شهدت العاصمة المجرية بودابست في أواخر عام 2001 ميلاد أولى المعاهدات الدولية تكافح جرائم الانترنت "Internet Crimes" وتبلور التعاون والتضامن الدولي في محاربتها ومحاولة الحد منها لاسيما بعد أن وصلت تلك الجرائم إلى حد خطير أصبح يهدد الأشخاص والممتلكات.

لقد جاءت بودابست لمكافحة جرائم الانترنت في أي العديد من الدول التي لا تستطيع بمفردها مواجهة تلك الجرائم، نظرا لكون تلك الجرائم هي من الجرائم عابرة الحدود التي لا يقف أمامها أي عائق جغرافي، وبالتالي فتلك الدول تفضل الانضمام إلى المعاهدات الدولية التي تبرم في هذا المجال نظرا لكبر حجم الأضرار عن طريق الانترنت، لأن العديد من الدول حتى المتقدمة منها لا تستطيع مواجهة تلك الأخطار بمفردها دون تعاون وتضامن دولي ليتم نجاح أي مجهودات تبذل في مكافحة الجرائم التي ترتكب عبر الانترنت، أن التعاون الدولي في تطبيق تلك القوانين هو الطريق الوحيد ليتم احترام حقوق الإنسان مثل الحقوق الملكية الفكرية للإنسان[1].

وفي إطار التصدي أكثر لمكافحة الجريمة المعلوماتية عقد المجلس الأوروبي في 11 ديسمبر 1995 مؤتمر وزراء الدول الأعضاء لبحث مشاكل صياغة اتفاقيات لمكافحة الجريمة المعلوماتية بعقد اتفاقية بودابست في 23 نوفمبر 2001، ولقد بينت المذكرة التفسيرية لهذه الاتفاقية أن تحديد الجرائم المعلوماتية فيها هدفه تحسين وإصلاح وسائل منع وقمع الجريمة المعلوماتية، من خلال تحديد معيار بالحد الأدنى المشترك، الذي يسمح باعتبار بعض التصرفات من قبل الجرائم المعلوماتية، وأنه بالإمكان أن يتم استكمال هذه القائمة في القوانين الداخلية، كما أنه يأخذ في الاعتبار الممارسات غير المشروعة الأكثر حداثة والمرتبطة بالتوسع في استخدام شبكات الاتصال عن بعد.

**الفرع الأول: تصنيف الجريمة المعلوماتية حسب اتفاقية بودابست**

حددت الاتفاقية (اتفاقية بودابست)الجرائم المعلوماتية وصنفتها في خمسة عناوين في القسم الأول من الاتفاقية.

**العنوان الأول:** ويضم جوهر جرائم الحاسب الآلي، أو الجرائم المعلوماتية، وهي تلك الجرائم التي تعرف بالجرائم ضد سرية البيانات و سلامتها وسلامة النظم وإبّاحة البيانات والنظم.

**العنوان الثاني:** ويضم الانتهاكات الممارسة بواسطة الحاسب الآلي، التي تمس بعض المصالح القانونية تحميها قوانين العقوبات، وتضم أيضا قوانين الغش المعلوماتي والتزوير المعلوماتي.

[1] – جعفر حسن جاسم الطائي، المرجع السابق، ص 227–228.

**العنوان الثالث:** ويشمل الانتهاكات والجرائم المرتبطة بالمحتوى، وهي التي تخص الإنتاج والنشر غير المشرع للمواد الإباحية الطفولية عبر النظم المعلوماتية، في المادة التاسعة من الاتفاقية.

**العنوان الرابع:** ويشمل الجرائم المتعلقة بالاعتداء على الملكية الفكرية والحقوق المرتبطة بها في نص المادة العاشرة من الاتفاقية.

**العنوان الخامس:** وهو يشمل على أحكام إضافية بخصوص الشروع والاشتراك وأيضا الجزاءات والإجراءات والتدابير طبقا للمعايير الدولية الحديثة بالنسبة لمسؤولية الأشخاص المعنوية[1].

**الفرع الثاني: الشروط وصف الجريمة المعلوماتية حسب اتفاقية بودابست**

وقد أوجبت اتفاقية بودابست مجموعة من الشروط حتى تأخذ الأفعال السابقة وصف هذه الجريمة وده الشروط هي:

**أ.** أن ترتكب الجرائم المذكورة في الجريمة دون وجه حق.

**ب.** أن ترتكب الجرائم المذكورة بطريقة عمدية من أجل إقرار المسؤولية الجنائية. ولدراسة المكافحة الموضوعية للجريمة المعلوماتية في اتفاقية بودابست ارتأيت دراسة أهم المواد التي جاءت لمكافحة هذه الجريمة كالتالي مع التعليق عليها:

الجرائم الوارد العناوين من1 إلى4 قد نصت عليها المواد من 2 إلى 10 من اتفاقية بودابست وهي:

**المادة الثانية:** جريمة الولوج أو الدخول غير القانوني التي تنص على أنه "يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية وفقا لقانونه الداخلي للولوج العمدي لكل أو جزء من جهاز الحاسوب دون حق، كما يمكن له أن ترتكب الجريمة من خلال انتهاك إجراءات الأمن بنية الحصول على بيانات الحاسب، أو أية نية إجرامية أخرى وأن ترتكب الجريمة في حاسب آلي يكون متصلا عن بعد بحاسب آخر فيدخل بالتالي في عداد هذه الجرائم كل من الأفعال: القرصنة والسطو والدخول غير المشروع في النظام المعلوماتي[2].

---

[1]– طارق إبراهيم الدسوقي عطية، المرجع السابق، ص 302.

[2]– خالد إبراهيم ممدوح، **الجرائم المعلوماتية**، دار الفكر الجامعي، بدون بلد، الطبعة الأولى، 2009، ص 277.

**المادة الثالثة:** تنص على جريمة الاعتراض غير القانوني الهدف منها حماية الحق في احترام نقل البيانات و الاتصالات ، والتسجيل التقليدي للمحادثات التليفونية بين الأشخاص و هذه الحقوق كانت مكفولة سابقا بنص المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان.

**المادة الرابعة:** تنص على أشكال الاعتداء على سلامة البيانات ونصها كالأتي " يجب على كل طرف أن يتبنى الإجراءات التشريعية ، وأية إجراءات أخرى يرى أنها ضرورية للتجريم تبعا لقانونه الداخلي إذا حدث ذلك عمدا ودون حق، أي إضرار أو محو أو تعطيل أو إتلاف أو طمس لبيانات الحاسب".

**المادة الخامسة:** تنص هذه المادة على جريمة الاعتداء على سلامة النظام كالتالي:

"يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية للتجريم في قانونه الداخلي: الإعاقة الخطيرة إذا تم ذلك عمدًا ودون حق لوظيفة نظام الحاسب عن طريق إدخال أو نقل أو إضرار أو محو أو تعطيل أو إتلاف أو طمس البيانات المعلوماتية".

هدف هذه المادة هو تجرم الإعاقة العمدية للاستخدام الشرعي للنظم المعلوماتية، بما في ذلك نظم الاتصال باستخدام أو التأثير على بيانات الحاسب والمصالح القانونية المحمية بنص هذه المادة هي مصلحة مشغلي ومستخدمي نظام الحاسب الآلي، أو نظام الاتصالات في عمل هذه الأجهزة بدقة وقد شمل نص هذه المادة على كل من أفعال الإدخال أو النقل أو الإضرار أو محو أو تعطيل أو إتلاف أو طمس البيانات المعلوماتية وهذه المصطلحات كلها يمكن اختصارها تجريم فعل الإعاقة الذي يضمها كلها والتي يجب أن تكون جسيمة وبدون وجه حق حتى تعتبر فعلا مجرما ومعاقب عليه[1].

**المادة السادسة:** تنص المادة 6 من اتفاقية بودابست على جريمة إساءة استخدام أجهزة الحاسب. اعتبر نص هذه المادة أن ارتكاب مجموعة من الأفعال عمدًا التي ترتبط ببعض الأجهزة، أو بيانات الولوج أو الدخول من حيث إساءة استخدامها وبغرض ارتكاب جريمة والتي

[1]– هدى حامد قشقوش، **جرائم الحواسب الالكترونية في التشريع المقارن**، دار النهضة العربية، القاهرة، 1992، ص 106 وما بعدها.

حددها في كل من الأفعال التالية: إنتاج أو بيع أو الحصول من أجل الاستخدام أو استيراد أو نشر أو أي أشكال أخرى للوضع تحت التصرف:

أ. جهاز يحتوي على برنامج معلوماتي بشكل أساسي لغرض ارتكاب الجرائم المنصوص عليها في المواد 2 و5 السابقة الذكر.

**ب.** كلمة المرور أو شفرة الدخول أو أية بيانات أخرى مماثلة تسمح بالولوج إلى كل أو إلى جزء من نظام الحاسب. بنية استخدامها لغرض ارتكاب جريمة من الجرائم المنصوص عليها في المواد من 2 إلى 5، وقد اشترطت المادة أن ينطبق التجريم على الأجهزة المصممة أساسا من أجل ارتكاب جريمة كما اشترط أن ترتكب الأفعال السابقة عمدا وبدون وجه حق وهذا تجنبا لخطر العقاب المبالغ فيه.

**المادة السابعة:** نصت على جريمة التزوير المعلوماتي لخطورة هذه الجريمة وسهولة ارتكابها حيث جاءت هذه المادة بغرض إنشاء جريمة في قوانين موازية لجريمة تزوير المستندات الورقية، وهي تنص على أنه "يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية للتجريم وفقا لقانونه الداخلي نية الغش أو نية إجرامية مشابهة من أجل تقرير غير مصرح به لبيانات المسجلة، بطريقة من المصالح القانونية المحمية، والأمن والثقة في البيانات المخزنة، عمليات الإدخال والإتلاف والمحو أو الطمس تشكل أعمالا مماثلة لجريمة التزوير محور صحيح[1].

**المادة الثامنة:** وتخص جريمة الغش المعلوماتي تنص هذه المادة على أنه يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية للتجريم: التسبب عمدا أو دون حق في إحداث ضرر مالي للغير عن طريق:

أ. الإدخال، الإتلاف، المحور أو الطمس، لبيانات الحاسوب.

**ب.** كل شكل للاعتداء على وظيفة الحاسب بنية الغش أو أية نية إجرامية مشابهة من أجل الحصول دون حق على منفعة اقتصادية له أو لغيره، مضمون هذه المادة يتلخص في مكافحة الجرائم التي تتم من خلال تلاعبات بمداخلات النظام، وتغذيته ببيانات غير صحيحة بالتلاعب

[1]– طارق إبراهيم الدسوقي عطية، المرجع السابق، ص 323.

في البرامج من أجل ارتكاب جرائم الغش الاقتصادية وجرائم النصب في بطاقة الائتمان التي شاع استعمالها[1].

**المادة التاسعة:** تنص هذه المادة على أنه يجب تجريم السلوكيات التالية إذا ارتكبت عمدا أو دون حق:

- إنتاج مواد إباحية طفولية بغرض نشرها عبر النظام المعلوماتي.
- تقديم أو إتاحة مادة إباحية طفولية عبر نظام معلوماتي.
- النشر والنقل لمادة إباحية طفولية عبر نظام معلوماتي.
- دافعة التزود أو تزويد الغير بمادة إباحية طفولية عبر نظام معلوماتي.
- حيازة مادة إباحية طفولية في نظام معلوماتي أو في أي وسيلة لتخزين البيانات المعلوماتية

والهدف من نص هذه المادة هو تدعيم الإجراءات التي تحمي الأطفال وحمايتهم من الاستغلال الجنسي، وذلك بتحديث قوانين العقوبات بطريقة أكثر فعالية، بحيث تصبح هذه القوانين تحتوي على نصوص تجريم استخدام نظم الحاسبات الآلية في ارتكاب الجرائم الجنسية ضد الأطفال وقد جاء نص هذه المادة متوافقا مع التوهج الدولي لمكافحة جرائم دعارة الأطفال، ومتوافقا مع المبادرة الحديثة للجنة الأوروبية المتعلقة بمكافحة الاستغلال الجنسي الأطفال والمواد الإباحية الطفولية رقم 854 لسنة 2000.

أما **المادة العاشرة:** من اتفاقية بودابست 2001 فتنص على أنه: "على كل طرف تبني الإجراءات التشريعية أو أية إجراءات أخرى لتجريم":

أ. انتهاكات الملكية الفكرية المعرفة في القانون ذلت الطرف وفقا الالتزامات التي تم التوقيع عليها في ظل الاتفاقية العالمية لحماية حقوق المؤلف الموقعة في باريس في 24 جويلية 1971 واتفاقية بن لحماية الأعمال الأدبية والفنية واتفاقية المنظمة العالمية للملكية الفردية (OMPI) باستثناء أي حق معنوي ممنوح بواسطة هذه الاتفاقية إذا ما ارتكبت عمدا وعلى نطاق تجاري وبواسطة نظام معلوماتي.

[1]– نائلة عادل فريد قورة، المرجع السابق، ص 190 وما بعدها.

**ب.** يجب تجريم انتهاكات الحقوق المجاورة المعرفة في قانون هذا الطرف وفقا للالتزامات التي تتم التوقيع عليها في ظل الاتفاقات الدولية لحماية الفنانين المؤدبين أو العازفين ومنتجي الصوتيات ومنظمات البث المبرمة في اتفاقية روما واتفاقية الجوانب التجارية لحقوق الملكية الفكرية واتفاقية المنظمة الدولة للملكية (OMPI) بالنسبة للأداء والعزف باستثناء أي حق معنوي منصوص عليه بواسطة الاتفاقيات إذا تم ارتكابها عمدًا وعلى نطاق تجاري وبواسطة نظام معلوماتي[1].

**ج.** يمكن لأي طرف في ظل ظروف محددة للغاية أن يحتفظ بالحق في عدم تطبيق المسؤولية الجنائية بالنسبة للفقرتين1 و2 من هذه المادة بشرط توافر طرق أخرى فعالة وجاهزة وإلاّ يكون في هذا التحفظ ما يحمل على اعتداء على الالتزامات الدولية المشار إليها في الفقرتين 1 و2 من هذه المادة.

مضمون المادة العشرة يتلخص في وجوب تجيم الانتهاكات العمدية على الملكية الفكرية التي زاد انتشارها مع زيادة استعمال الحاسبات الآلية وسهولة اقتنائها وتجريم الانتهاكات العمدية الواقعة على الحقوق المتصلة والتي يطلق عليها بالحقوق المجاورة.

وما يعاب على هذه المادة على أنها لا تغطي بالتجريم كل انتهاكات الملكية الفكرية كانتهاكات حقوق و براءات الاختراع والعلامات التجارية.

## المطلب الثاني: المعاهدات والقوانين الخاصة بحماية الملكية الفكرية

مما لا شك أن حقوق الملكية الفكرية هي من أكثر الحقوق التي يتم انتهاكها يوميا على شبكة الانترنت أو على كافة شبكات الاتصال والمعلومات على مستوى العالم وعليه فوجود معاهدات دولية تمنع تلك الانتهاكات وإصدار كل دولة قوانين خاصة بها تعمل على حماية حقوق الملكية الفكرية كل ذلك يؤدي إلى الحفاظ على تلك الحقوق من الانتهاك الذي يوميا دون أي رادع يحمي أصحاب تلك الحقوق.

ومن أهم المعاهدات التي تم إبرامها في مجال حماية حقوق الملكية الفكرية[2].

---

[1]– نعيم مغبغب، **(حماية برامج الكمبيوتر الأساليب والثغرات–دراسة في القانون المقارن)**منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، 2006، ص 19،20.

[2]– جعفر حسن جاسم الطائي، المرجع السابق، ص238.

**الفرع الأول: معاهدة برن لحماية المصنفات الأدبية والفنية**

تعد معاهدة برن والتي تم التوقيع عليها في عام 1971 في سويسرا هي حجر الأساس في مجال الحماية الدولية لحق المؤلف، وقد وقعت على هذه الاتفاقية(120) دولة، وتعد المادة التاسعة من تلك الاتفاقية هي أساس تلك الاتفاقية، لأنها تنص على منح أصحاب حقوق حق استئثاري في التصريح بعمل نسخ من هذه المصنفات بأي طريق وبأي شكل كان.

فضلا عن ذلك تمنح اتفاقية برن صاحب حق المؤلف، الحق في أن يرخص أو يمنع أي ترجمة أو اقتباس أو بث إذاعي أو توصيل إلى الجمهور لمصنفه، وكذلك تلتزم الاتفاقية بتوقيع جزاءات سواء كان المؤلف المعتدي عليه وَطنيا أم أجنبيا[1].

**الفرع الثاني: معاهدة تريبس**

شملت معاهدة التريبس[2]الخاصة بأوجه التجارة المتصلة بحقوق الملكية الفكرية على مكافحة الجريمة المعلوماتية بالنص في المادة 1/10على أنه"تتمتع برامج الحاسب الآلي أو الكمبيوتر سواء كانت بلغة المصدر أو بلغة الآلة بالحماية باعتبارها أعمالا أدبية بموجب معاهدة برن 1971، كما نصت فقرتها الثانية على حماية البيانات المجمعة أو المواد الأخرى بشروط معينة، كشرط الأصالة سواء أكانت مقروءة آليا أو بشكل آخر، وإذا كانت تشكل خلقا فكريا نتيجة انتقاء أو ترتيب محتوياتها.

ولفعالية هذه المكافحة اشترطت الاتفاقية على الدول الأعضاء لحماية حقوق الملكية المنصوص عليها–في هذه الاتفاقية– وبهدف تسهيل اتخاذ تدابير فعالة ضد أي تعد على حقوق الملكية الفكرية تناولتها الاتفاقية، يجب اتخاذ إجراءات سريعة لمنع التعديات والانتهاكات الحالة في المادة41 من الاتفاقية، وضرورة توافر لإجراءات قضائية ومدنية إلى جانب إجراءات إدارية أخرى في المادة 42 منها.

هذا ونصت المادة التاسعة من الاتفاقية على أنه على الدول الأعضاء فيها الالتزام بأحكام المواد من1إلى 21 من معاهدة برن1971، مع مراعاة أن الحماية تسري على المنتوج وليس على مجرد الأفكار أو الإجراءات أو أساليب العمل أو المفاهيم الرياضية، كما نصت على

---

[1]– منير محمد الجنيهي: ممدوح محمد الجنيهي، **جرائم الانترنت والحاسب وسائل مكافحتها**، الإسكندرية، دار الفكر الجامعي، 2004، ص 113.

[2]– وقعت في مراكش بالمغرب بتاريخ، 1994/04/15.

الحماية الزمنية لهذه المصنفات وحددتها بطول حياة المؤلف بالإضافة إلى مدة خمسين عامًا بعد وفاته[1]. فربطت بذلك بين المعايير الدولية والمعايير المحلية[2].

## المطلب الثالث: الجرائم المعلوماتية في القانون العربي النموذجي.

أدى رواج المعلومات في كل الدول العربية إلى ظهور عدة ممارسات إجرامية في هذا النطاق مما حذا بهذه الدول إلى المحاولة لإيجاد سبل تشريعية إجرائية ناجعة لمواجهة هذا النوع من الجرائم المتجسدة[3].

نجد من تلك الجهود القرار الصادر عن قرار مجلس وزراء العرب الخاص بإصدار القانون الجزائي الموحد، كقانون عربي نموذجي.

وقد جرم القانون العربي النموذجي لمكافحة الجريمة المعلوماتية، مجموعة من الأفعال مرتبطة بإساءة تقنية المعلومات، والتي اعتبرها جرائم مستحدثة يجب التصدي لها ومكافحة خطورتها الكبير على الأفراد والمجتمع وبين هذه الجرائم سنتناول بالدراسة مجموعة منها كمايلي:

### الفرع الأول: جريمة غسيل الأموال عبر الوسائط الالكترونية

تنص المادة التاسعة عشر من القانون العربي النموذجي لمكافحة الجريمة المعلوماتية، على أنه "كل من قام بتحويل الأموال غير المشروعة أو نقلها أو تمويه المصدر غير لها أو إخفائه أو قام باستخدام أو حيازة الأموال مع العلم بأنها مستمدة من مصدر غير مشروع أو بتحويل المواد أو الممتلكات مع العلم بمصدرها غير المشروع وذلك عن كطريق استخدام نظام الحاسب الالكتروني أو شبكة المعلومات الدولية بقصد إضفاء الصفة المشروعة على تلك الأموال يعاقب بـ... وتترك العقوبة وفقا لتقدير كل دولة.

ولتجريم سلوك غسيل الأموال بمفهومها السابق يجب أن تتوافر الآتي:

**أولا: الركن المادي:** والمتمثل في صور السلوك الإجرامي حتى تقوم هذه الجريمة وهي:

---

[1]– محمد علي العريان، **الجرائم المعلوماتية**، دار الجامعة الحديدة، الإسكندرية، 2004، ص 33.

[2]– منير محمد الجنيهي: ممدوح محمد الجنيهي، المرجع السابق، ص 113.

[3]–عباس محمود أبو شامة، المرجع السابق، 50.

أ. **تحويل الأموال أو نقلها:** ويقصد به جميع العمليات المصرفية التي يتم تحويل الأموال بمقتضاها والعمليات غير المصرفية التي تتم بوسائل الكترونية بسيطة أو معقدة كالتحويل البرقي للنقود، والتحويل من حساب إلى حساب عن طريق شبكة الانترنت، كما يتم تحويل الأموال عن طريق تغيير شكلها كأن تشتري مجوهرات أو سبائك ذهب بالعملة المحلية ثم يعاد بيعها، وأيضا عن طريق بطاقات الائتمان المزورة أو التحويل عن طرق تحويل العملة الوطنية إلى عملة أجنبية عندما لا توجد قيود تشريعية على عمليات التحويل.

ب. **إخفاء وتمويه حقيقة الأموال:** ويقصد بها السلوك إبعاد الأموال عن مصدرها الإجرامي المستمد منه بإتباع أساليب بالغة التعقيد من التحولات المالية، بهدف إخفاء مصدرها غير المشروع.

ج. **اكتساب أو حيازة أو استخدام الأموال المتحصلة من الجريمة:** ويقصد بهذا السلوك أن مجرد اكتساب أو حيازة أو استخدام الأموال مع علم الفاعل بأن تلك الأموال متحصلة من جريمة من الجرائم يعد ذلك السلوك مجرما ويعاقب عليه.

د. **محل السلوك الاجرامي:** تتفق معظم التشريعات في كافة الدول "كالتشريع المصري في القانون رقم 80 الصادر في ماي 2002 والمتعلق بكافة غسل الأموال والتشريع التونسي في القانون رقم 75 الصادر سنة 2003 والتشريع السويسري الصادر في أفريل 1998"[1].

وقد نص المشرع العربي في القانون النموذجي على محل الجريمة غسل الأموال الالكترونية بأنه "الأموال غير المشروعة" حيث جاءت هذه العبارة عامة حتى يمكنها احتواء كل المصطلحات والمفردات الخاصة بالأموال سواءً كانت منقولة أم غير منقولة ما دامت أنها محل لغسل الأموال.

هـ. **النتيجة الإجرامية:** تنص المادة التاسعة عشر من القانون النموذجي العربي في شأن جريمة غسل الأموال الالكترونية على النتيجة الإجرامي هو إخفاء المال وتمويه وتغيير حقيقته وطبيعته على النحو الذي يتم الحصول عليه من الجريمة الأصلية.

**ثانيا: الركن المعنوي:** فحسب نص المادة التاسعة عشر من القانون العربي النموذجي العربي شأن مكافحة الجريمة المعلوماتية تعتبر جريمة غسل الأموال في صورتها الالكترونية من

[1] –عبد الله عبد الكريم عبد الله، المرجع السابق، ص 277.

الجرائم العمدية التي تقوم القصد الجنائي العام بعنصريه العلم والإرادة بالإضافة إلى القصد الجنائي الخاص.

فالقصد الجنائي العام معناه علم الجاني بأنه يمارس نشاطا غير مشروع وهو غسل الأموال المتحصلة من جريمة وانصراف نيته. إلى إتيان هذا الفعل وقبول النتائج المترتبة عليه أي العلم والإرادة، أما القصد الخاص يقصد به أن تتجه نية الفاعل من جريمة غسل الأموال إلى إخفاء المال أو طبيعته أو مصدره أو مكانه أو صاحبه أو صاحب الحق فيه أو تغيير حقيقته والحيلولة دون اكتشاف ذلك، أو عرقلة الوصول إلى شخص من ارتكاب الجريمة المتحصل منها على المال1.

ولقد نصت المادة التاسعة عشر من القانون العربي النموذجي على وجوب توفر القصد الجنائي الخاص في جريمة غسل الأموال الالكترونية، بارتكابه الجريمة المنظمة عن طريق استخدام نظام الحاسب الالكتروني أو شبكة المعلومات الدولية بقصد إخفاء الصفة المشروعة تلك الأموال، بإضفاء صفة المشروعية عليها ما هو إلاّ قصد جنائي خاص يتمثل في إظهار المال المغسول بمظهر المال المشروع، مع العلم أنه متحصل من مصدر غير مشروع، وتأخذ جريمة غسل الأموال الالكترونية صورا عديدة لارتكابها من هذه الصور على سبيل المثال.

أ. **استخدام بطاقة الائتمان:** لشراء مجوهرات أو أشياء ثمينة كلوحات فنية باهظة الثمن، يتم سداد الفاتورة الخاصة بها لاحقا بالنقود المتحصل عليها من جرائم الاتجار بالمخدرات.

ب. **أعمال الصيرفة الالكترونية:** تتلخص في عملية امتلاك مصرف وإدارته بمساعدة لآخرين بحيث يمكن لأي شخص شراء مصرف وإدارة أعمال الصيرفة الالكترونية

(سويفت Swift) وهي خدمة خاصة بنقل الأموال وتقديم خدمات مالية إلى الوسطاء. وتجار السندات وشركات المقاصة والأسواق المالية الكبرى، وسهولة أعمال الصيرفة الالكترونية ساعد على انتشار جريمة غسل الأموال الالكترونية لسيطرة عصابات الجريمة المنظمة على المصارف، وبالتالي أصبح لديها حرية واسعة في غسل كميات كبيرة من غسيل الأموال ليس لنفسها فقط بل وحتى للمنظمات الاجرامية الأخرى2.

---

[1]–عبد الفتاح بيومي حجازي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت**، المرجع السابق ص 119.

[2]–إيهاب فوزي السقا، **جرائم التزوير في المحررات الالكترونية**، دار الجامعة الجديدة، الإسكندرية، 2008، ص42..

**الفرع الثاني: جريمة اختراق النظم المعلوماتية**

تنص المادة الثالثة على أنه "كل من توصل بطريقة التحايل لاختراق نظم المعالجة الآلية للبيانات يعاقب بالحبس والغرامة(تترك العقوبة لتقدير كل دولة)، وإذا نتج عن هذا الفعل محو أو تعديل للبيانات المخزنة بالحاسب أو تعطيل تشغيل النظام بسبب تسريب للفيروسات أو غيرها من الأساليب المعلوماتية، تكون العقوبة بالحبس والغرامة المالية" وتترك العقوبة لتقدير كل دولة.

وحسب نص المادة تتحقق جريمة اختراق النظم المعلوماتية بارتكاب:

**أ.** كل من جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي بأي وسيلة تقنية ،كانتهاك كلمة السر الحقيقية أو عن طريق استخدام برنامج أو شفرة خاصة ، ويتحقق هذا الدخول متى دخل الجاني إلي النظام المعلوماتي كله أو جزء منه دون وجه حق، أي دون موافقة صاحب النظام أو من له حق السيطرة عليه، أما فعل البقاء غير المشروع داخل النظام المعالجة الآلية للمعطيات فقد كان الهدف من تجريمه هو تجريم البقاء غير المشروع داخل النظام المعلوماتي لمن كان دخوله إلى هذا النظام بطريق الصدفة ودون قصد جنائي ومع ذلك يبقى داخل النظام وتتصرف إرادته لذلك[1].

**ب.** حسب نص المادة الثالثة من القانون النموذجي العربي لمكافحة الجريمة المعلوماتية فقد عاقب المشرع على فعل إعاقة تشغيل نظم معالجة البيانات بفعلي التعطيل بأي وسيلة كانت كسبب التسريب للفيروسات، ومثالها استخدام "القنبلة المنطقية" أو استخدام فيروس "حصان طروادة" التي مفادها "القنبلة المنطقية" أنها عبارة عن برنامج أو جزء منه ينفذ في لحظة محددة أو كل فترة زمنية منتظمة في شبكة المعلوماتية من أجل تسهيل تنفيذ عمل غير مشروع، أما برنامج حصان طراودة فهو برنامج يقوم بتغيير محسوس في برنامج والمعطيات، كذلك هناك فيروس "الدودة" وهو عبارة عن برنامج يتميز بقدرة فائقة على تعطيل وإيقاف نظام الحاسب، وهذه الفيروسات تقوم بإفساد البرامج والمعطيات المعلوماتية.

[1]–عبد الفتاح بيومي حجازي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت** ،المرجع السابق، ص325.

**ج.** أما المحو المذكور في المادة الثالثة من القانون النموذجي العربي فيقصد به ذلك السلوك الإجرامي بإزالة جزء من المعطيات المسجلة على الدعامة لموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل وتخزين المعطيات إلى المنطقة الخاصة بالذاكرة.

**د.** التعديل ويقصد به تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى، ويتم التلاعب في المعطيات عن طريق استبدالها أو التلاعب في البرنامج أو إمداده بمعطيات مغايرة تؤدي إلى نتائج غير التي صمم لها البرنامج.

وجريمة اختراق النظم المعلوماتية هي جريمة عمدية في كل صور السلوك الإجرامي التي رأيناها سابقا وصورة الركن المعنوي فيها هو القصد الجنائي العام بركنيه العلم والإرادة أي باتجاه إرادة الجاني إلى فعل الاختراق أو البقاء غير المشروع أي اتجاه إرادته إلى أفعال الدخول والإدخال والمحو والتعديل...التي هي صور السلوك الإجرامي في هذه الجريمة واتجاه إرادته إليها مع العلم بأن نشاطه وسلوكه هذا غير مشروع[1].

وقد عاقب المشرع العربي في القانون النموذجي على الشروع في الجرائم السابقة المشارة لها وبنصف العقوبة المقررة لها في حالة الجريمة التامة في المادة 24 منه.

**الفرع الثالث: جريمة التزوير المعلوماتي**

نصت المادة الرابعة من القانون النموذجي العربي الموحد بشأن مكافح الجريمة المعلوماتية على أنه«كل من زور المستندات المعالجة آليا أو البيانات المخزنة في ذاكرة الحاسوب أو على شريط أسطوانة ممغنطة أو غيرها من الوسائط يعاقب ب.. وتترك العقوبة وفقا لكل دولة »

كما نصت الفقرة الثانية من المادة الرابعة من نفس القانون على أنه "كل من استخدام المستندات المزورة آليا مع علمه بتزويرها يعاقب بنفس عقوبة التزوير فإذا كان المستخدم هو نفسه مرتكب فعل التزوير يعاقب وفقا للقواعد العامة المعمول بها في هذا الشأن". فالتزوير في صورته التقليدية هو تغيير الحقيقة في محرر بإحدى الطرق التي حددها القانون تغييرا من شأنه أن يرتب ضررا للغير وبنية استعمال هذا المجرم فيما أعده له.

[1]– عبد القادر القهوجي، **الحماية الجنائية لبرنامج الحاسب الآلي**، دار الجامعة الحديث، الاسكندرية، 2006، ص30.

أما التزوير المعلوماتي فهو "تغيير الحقيقة في المستندات المعالجة آليا والمستندات المعلوماتية وذلك بنية استعمالها1.

فيتغير الحقيقة في النظام الآلي في المعالجة المعلوماتية يتم بتغيير البيانات أو المعلومات أو صنفها أو إضافتها أو التلاعب فيها بأي صورة سواءًا كانت هذه البيانات مخزنة في ذاكرة الحاسب أو كانت تمثل جزءًا من برنامج التشغيل أو برنامج التطبيق شرط أن تطبع هذه البيانات على دعامة مكتوبة أو مسجلة بحيث يكون لها كيان مادي يمكن إدراكه.

**الفرع الرابع: السرقة المعلوماتية**

نص المشرع العربي في المادة الرابعة عشر على سرقة المعلومات بتجريم كل من عمليات نسخ ونشر لمصنفات الفكرية أو الأدبية، أو الأبحاث العلمية، أو ما في حكمها إذا ما ارتكب دون وجه حق، بعقوبة الحبس الذي يترك تقديرها وفقا لقانون كل دولة، ودون الاختلال بنصوص الخاصة بالملكية الفكرية لكل بلد.

أما المادة الحادية عشر من القانون النموذجي العربي فهي تعاقب على الاستيلاء على نقود الغير أو ماله إذا تم بطريق بطاقات الائتمان حيث تنص "كل من استخدم بطاقة ائتمان للسحب الالكتروني من الرصيد خارج حدود رصيده الفعلي أو قام باستخدام بطاقة مسروقة أو تحصل عليها بأي وسيلة يعاقب ويترك العقوبة لتقدير كل دولة".

هذا ولم يصل المشرع العربي في القانون النموذجي لمكافحة الجريمة المعلوماتية الاهتمام بنص على مكافحة الجرائم الخاصة بالاعتداء على حرمة الحياة الخاصة لما لهذه الأفعال من آثار وخيمة على حياة الأشخاص وأمرهم ، وبالتالي على المجتمع الدولي ككل لذلك النص على تجريم أفعال التنصت على المراسلات الالكترونية وذلك في المادة الثامنة من هذا القانون.

أما في المادة التاسعة عشر فقد جرم فيها مجموعة من الأفعال التي تمس العقوبات القانونية والآداب العامة وهذه الأفعال المجرمة هي:

**أ.** أفعال الاعتداء على القيم الدينية كالإساءة إلى إحدى المقدسات والعشائر المقررة في، الأديان الأخرى و الإساءة إلى إحدى المقدسات والشعائر الإسلامية.

**ب.** وسب أحد الأديان السماوية المعترف بها(كالمسيحية والإسلام واليهودية).

---

[1]–فوزية عبد الستار، **قانون العقوبات(القسم الخاص)**، دار النهضة العربية، بدون بلد، 1988، ص244.

هذا و قد نصت في المادة 17 على مكافحة جرائم العرض والاتجار بالبشر من خلال نظام الحاسب الآلي لخطورة هذه الجرائم[1].

غير أنة الملاحظ في هذه المحاولات على المستوى العربي هو اعتمادها على علاج نقص التشريعات والأنظمة الخاصة بموضع جرائم الانترنت. كما شملت هذه المحاولات العديد من تعليمات أمن المنشآت الحاسوبية، والأجهزة والبرامج وبعض القواعد العامة المنظمة لارتباط المنشأة الحكومية بالشبكة العالمي.

## المبحث الثاني: الجهود التشريعية للحد من الجريمة المعلوماتية

دأبت المجتمعات والدول عبر حقب زمنية مختلفة في سن تشريعات وقوانين من أجل مواجهة كل من تسول له نفسه خرق الآداب العامة بأعمال غير مشروعة، ومن ذلك الجرائم المعلوماتية، إذ رغم قلتها إلاّ أنَها تعتبر محاولات هامة في هذا المجال، وتتمثل هذه الجهود على المستوى الدولي في الجهود التي تبذلها مختلف الهيئات والمنظمات العالمية، بالإضافة إلى المنظمات الإقليمية، والتي تعتبر كإطار دولي يوازي عالمية الجريمة المعلوماتية.

تعتبر الجهود الدولية، دعامة للجهود التي تبذلها مختلف الدول في تشريعاتها الداخلية، فهي تعتبر بمثابة قوانين استرشادية بالنسبة لها، فهناك الكثير من الدول التي اتخذت سبيل تطوير قوانينها وفي هذا الإطار نستعرض تجربة المشرع الجزائري من أجل مكافحة ومواجهة الجريمة المعلوماتية.

### المطلب الأول: تطور الحماية الجنائية المستوى الدولي

إن الطابع الدولي للجريمة المعلوماتية نطاقه لا يعني كونها من الجرائم الدولية التي يتناولها القانون الدولي الجنائي، فهي جرائم داخلية وإن كانت جرائم عالمية، وهو ما جعل كل دولة تقف بمفردها عاجزة عن التصدي لها.

[1]–عبد الفتاح بيومي حجازي ، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت**، المرجع السابق ،ص 678.

وسنبين الجهود الدولية في مواجهة الجريمة المعلوماتية أولا ثم نتطرق إلى الجهود الداخلية ثانيا.

**الفرع الأول: الأمم المتحدة**

بدأ اهتمام الولايات المتحدة الأمريكية المتحدة بمكافحة الجريمة المعلوماتية في 1966 في أول قضية HANCOCKE USTATE تعرض لموضوع إساءة استخدام الحاسبات الآلية وتتلخص وقائع هذه القضية في اتفاق مبرمج لحاسبات آلية بإحدى الشركات بالاتفاق مع صديق له يعمل بشركة أخرى على أن يقوم الأول بطبع المعلومات التي يحتوي عليها 59 برنامجا ملكا للشركة التي يعمل بها والتي هي ذات أهمية كبيرة وتسليمها للشركة الأخرى مقابل تلقيه 5 ملايين دولار وأثناء التسليم، تم القبض على المتهم وقدم للمحاكمة بتهمة السرقة[1].

تسعى الأمم المتحدة من خلال هيئتها والوكالات التابعة لها لوضع الإطار التشريعي لهذه الظاهرة الإجرامية المستحدثة وكانت الانطلاقة في المؤتمر السابع المنعقد بميلانو 1985 والذي أكدت على الاستفادة من التطورات العلمية والتكنولوجية في مواجهة هذه الظاهرة، وقد أشارت إلى مسألة الخصوصية واختراقها بالاطلاع على البيانات الشخصية المخزنة داخل نظام الحاسب الآلي وضرورة اعتماد ضمانات لحماية سريتها.

كما أكدت اللجنة على ضرورة تشجيع التشريعات الحديثة التي تتناول هذه الجرائم بصفتها نمط من أنماط الجريمة المنظمة، وفي سنة 1990 انعقد مؤتمر هافانا لعام 1990أرست توصياته على مجموعة من المبادئ التالية:

**1.** تحديد القوانين الجنائية الوطنية.

**2.** .تطوير أمن الحاسب الآلي والتدابير المنعية.

**3.** اعتماد إجراءات تمنع كافة الموظفين والوكالات المسؤولة لمنع الجرائم المتعلقة بالحاسب الآلي والتحري والادعاء فيها.

**4.** .تلقين آداب الكمبيوتر كجزء من مفردات الاتصال والمعلومات.

**5.** .اعتماد سياسات تعالج المشكلات المتعلقة بالمجني عليهم في تلك الجرائم[2].

---

[1]– نائلة عادل قورة، المرجع السابق، ص147.

[2]– هلالي عبد الله أحمد، **الجوانب الموضوعية والاجرائية للجريمة المعلوماتية على ضوء اتفاقية بودابست الموقعة في 2001/11/23**، دار النهضة العربية، القاهرة، 2003، ص62.

تزايد الجرائم المرتكبة عبر الانترنت وما تثيره من مشاكل أدى بمنظمة الأمم المتحدة إلى عقد الاتفاقية الخاصة بمكافحة إساءة استعمال التكنولوجيا إجرامية لسنة 2000، أين أكدت على الحاجة إلى تعزيز التنسيق والتعاون بين الدول في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامي، بالإضافة إلى الدور الذي يمكن أن تقوم كل من منظمة الأمم المتحدة والمنظمات الإقليمية[1].

عقدت كذلك الأمم المتحدة المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية في البرازيل أيام 17-19 أفريل 2010، حيث ناقشت فيه الدول الأعضاء ببعض التعمق مختلف التطورات الأخيرة في استخدام العلم و التكنولوجيا من جانب المجرمين والسلطات المختصة الجريمة بما في ذلك الجريمة الحاسوبية، حيث احتل هذا النوع من الجرائم موقعا بارزا في جدول أعمال المؤتمر وذلك تأكيدا على خطورتها والتحديات التي تطرحها[2].

دأبت منظمة الأمم المتحدة وذلك استمرارًا لتلك الجهود المبذولة لمكافحة جرائم الانترنت على عقد مؤتمرات، فلم تكن المؤتمرات السابقة الذكر الأولى ولن تكون الأخيرة، حيث عمدت اللجنة الاقتصادية والاجتماعية لغربي آسيا التابعة للمجلس الاقتصادي والاجتماعي وذلك تحت غطاء منظمة الأمم المتحدة على عقد ورشة عمل حول التشريعات السيبيرانية وتطبيقها في منظمة الاسكوا عام 2008.

بالإضافة إلى تلك المؤتمرات التي عقدتها أطراف اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المعقدة بفيينا في أكتوبر 2010، حيث بين المؤتمر فهرس الأمثلة المعلقة بتسليم المجرمين وتبادل المساعدة القانونية وأشكال أخرى من التعاون الدولي في المسائل القانونية، استنادا إلى اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية[3].

---

[1]- اتفاقية مكافحة استعمال تكنولوجيا المعلومات لاغراض اجرامية ، رقم (55/63) ، الصادرة عن هيئة الامم المتحدة، الجلسة العامة81، ديسمبر2000 .

[2]- مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، البند الثامن من جدول الأعمال المؤقت، التطورات الأخيرة، في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة بما فيها الجرائم الحاسوبية، المنعقد بالبرازيل 12-19 أفريل 2010، رقم213/09. A/Conf.

[3]- مؤتمر هيئة الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المعلوماتية عبر الوطنية، المنعقد بفيينا في 18-22، أكتوبر 2010، رقم:5 crp / CTOC/Cop/2010.

تبقى هيئة الأمم المتحدة الإطار الأمثل لمكافحة هذا النوع من الإجرام، وسوف تبقى تبذل مجهودا أكثر مادام هناك مجرمين يجوبون الفضاء السيبيراني.

**الفرع الثاني: القوانين المقارنة**

من هته القوانين القانون الفرنسي،حيث كانت أولى المحاولات لمد سلطان قانون العقوبات لحماية المال المعلوماتي من فرنسا من طرف وزير العدل سنة 1995، عندما تقدم بمشروع قانون عقوبات جديدة أضاف بموجبه بابا رابعا للكتاب الثالث منه بعنوان: الجرائم في المادة المعلوماتية كان يتكون من 8 مواد من 1/307 إلى 8/307 لكن هذه المحاولة لم يكتب لها النجاح إلاّ في 1986/08/05 عندما تقدم النائب "Jacque Godfrain" ونواب آخرون إلى الجمعيات الوطنية باقتراح مشروع قانون عن الغش المعلوماتي، قد حاولوا تعديل بعض النصوص القائمة في قانون العقوبات والتي تتناول جرائم تقليدية كالسرقة وخيانة الأمانة والتزوير والإتلاف والإخفاء وذلك لتشمل العدوان على المال المعلوماتي، وبعد مناقشات طويلة استمرت عاما ونصف العام أسفرت عن صدور قانون يختلف تماما عن المشروع الذي قدم ويتشابه إلى حد كبير مع المشروع الذي قدمه وزير العدل في 1985. وقد تضمن النص على الجرائم التالية:

**1.**الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو جزء منه وتشديد العقوبة في حالة محو أو تعديل المعطيات الموجودة داخل هذا النظام وإفساد وظيفته.

**2.**إدخال معطيات في النظام أو محو أو تعطيل المعطيات الموجودة فيه عمدًا وبدون مراعاة حقوق الغير.

**3.**كل فعل من شأنه أن يعرقل أو يفسد عمدا بدون مراعاة حقوق الغير أداء النظام لوظيفته.

**4.**تزوير مستندات المعالجة آليا أيا كان شكلها واستعمال هذه المستندات.

**5.**الشروع في ارتكاب الجرائم السابقة.

**6.**الاتفاق الجنائي على ارتكاب الجرائم السابقة.

أما المحطة السابقة من محطات التجريم المعلوماتي فكانت عام 1994 بعد تعديل قانون العقوبات الفرنسي وقد استخدم هذا التعديل مصطلح: الغش المعلوماتي، كما طور في جريمة

التزوير المعلوماتي إلى جريمة تزوير المستندات المعلوماتية [1]. قد أوكل هذا القانون إلى النيابة العامة سلطة التحقيق بما في ذلك طلب عمل التحريات وسماع الأقوال والشهود[2].

وكما أقر التعديل على مسؤولية الشخص المعنوي بعدما كان الفقه والقضاء الفرنسي منقسما بشأنها.

وبعد عشر سنوات من هذا التعديل جاء تعديل آخر لقانون العقوبات الفرنسي سنة 2004 أضاف بموجبه المشرع جريمة أخرى هي جريمة التعامل في وسائل المكتب يمكن أن ترتكب بها جريمة، أي الوسائل التي تصلح لأن ترتكب بها جريمة الدخول أو البقاء غير المصرح بهما أو جريمة التلاعب بالمعطيات أو الإعاقة وإفساد الأنظمة المعالجة الآلية للمعطيات[3].

في كندا فهي تطبق قوانين متخصصة ومفصلة للتعامل مع جرائم، حيث عدلت في (1985) قانونها الجنائي بحيث شمل قوانين خاصة بجرائم خاصة بجرائم الحاسب الآلي والإنترنت كما شمل القانون الجديد أيضا تحديد للعقوبات المطبقة على المخالفات الحاسوبية وجرائم التدمير وجرائم الدخول غير المشروع على المعاملات الالكترونية، كما وضح القانون صلاحيات جهات التحقيق، كما جاء في قانون المنافسة الذي يخول لمأمور القبض القضائي متى حصل على أمر قضائي حق التفتيش على أنظمة الحاسب الآلي والتعامل معها وضبطها.

أما في الدنمارك فقد انتهت لهذا الأمر مبكرا أيضا فقد سنت أول قانون خاص بها في مجال مكافحة جرائم الانترنت والحاسب الآلي(1985)، وقد شمل القانون العقوبات المحددة على ما يرتكب من جرائم مثل الدخول غير المشروع إلى الحاسب الآلي أو تزوير البيانات سواءًا كان هذا التزوير بالحذف أو بالإضافة أو بالتعديل[4].

أما هولندا فقد قامت هي الأخرى بتعديل القوانين الخاصة بها للتواؤم مع تلك الجرائم الحديثة ليكون في إمكانها التعامل مع محاولة السيطرة عليها، فقد قامت بتعديل القوانين الخاصة بها، ونصت في تلك القوانين على أنه من حق القاضي أن يصدر أوامره بالتصنت على شبكات

---

[1]– محمد سامي الشوا، المرجع السابق ،ص 200.

[2]– جعفر حسن جاسم الطائي، المرجع السابق، ص 162.

[3]– عبد القادر القهواجي، المرجع السابق ، ص 69.

[4]– جعفر حسن جاسم الطائي، المرجع السابق، ص 230.

الحاسب الآلي متى ما كانت هناك جريمة خطيرة، ومتى كان التصنت على قدر من الأهمية للكشف عن تلك الجريمة.

أما فنلندا فهي الأخرى تم تعديل القوانين الخاصة بها وأصبح للقاضي الحق في إصدار أوامره بمراقبة اتصالات الحاسب الآلي وتسجيلها والتعامل معها إلاّ أن القانون قد أعطى ذلك المحقق بشرط إلاّ في مدة أقصاها ثلاثة أيام.

أما في اليابان فقد قامت هي الأخرى بسن القوانين الخاصة بها لتستوعب المستجدات الإجرامية المتمثلة في جرائم الانترنت والحاسب الآلي وقد نصت تلك على أنه لا يلزم مالك الحاسب الآلي المستخدم في جريمة ما لتعاون مع جهات التحقيق وإنشاء كلمة سر التي يستخدمها إذا ما كان ذلك سيؤدي إلى إدانته كما أقرت في قانون خاص سنته عام(1991)، شرعية التصنت على شبكات الحاسب الآلي فقط إذا ما كان ذلك في مجال البحث عن الأدلة الخاص بإحدى الجرائم الالكترونية.

قامت دولة المجر هي الأخرى بدورها تماشيا مع الوضع الجديد، بسن القوانين خاصة بها لتجرم الجرائم الالكترونية وقد نصت تلك القوانين التي سنتها على كيفية التعامل مع مثل هذا النوع من الجرائم، وأيضا كيفية التعامل مع المتهمين بارتكاب الجرائم، وهي الإجراءات التي تسهل على عمل الجهات المنوطة بها مواجهة مثل تلك الجرائم والقبض على المتهمين بارتكابها[1].

كذلك دولة بولندا قامت بسن قوانين خاصة بها فتلك القوانين التي سنتها تنص على أن للمتهم بارتكاب الجرائم الحق في عدم طبع أي سجلات خاصة بالحاسب الآلي وإنشاء كلمة السر المستخدمة أو حتى الأكواد الخاصة بالبرامج، كما أنها تنص على حقوق أخرى بالنسبة لشهود في تلك الجرائم فهي تعطي الشاهد الحق في الامتناع عن طرح المعلومات المسترجعة من الحاسب الآلي متى ذلك قد يؤدي إلى إدانته أو إدانة أي من أقاربه، بل إن تلك القوانين تذهب إلى مدى أبعد من ذلك فتلك القوانين تنص على أنه لا يقابل ذلك إي إجراء قسري قد يتخذ وتكون من نتائجه إدانة بالمتهم[2].

[1]– منير محمد الجنيهي، ممدوح محمد الجنيهي المرجع السابق، ص 106.

[2]– منير محمد الجنيهي، محمد الجنيهي المرجع السابق، ص 107.

## المطلب الثاني: تطور الحماية الجنائية على المستوى الداخلي

الجزائر ليست بمنأى عن الثورة آليا أحدثها المعلوماتية إن لم تبلغ المصاف الأخير كالدول المتقدمة فإنها قد تأثرت بهذه الثورة فكان على المشرع الجزائري أن يسايرها بإحداث تعديل في قانون العقوبات ولقد جاء في عرض الأسباب هذا التعديل.(**إن** التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدى إلى إبراز أشكال جديدة من الإجرام مما دفع بالكثير من الدول إلى النص على معاقبتها وإن الجزائر على غرار هذه الدول تسعى من خلال هذا المشروع إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات وأن هذه التعديلات من شأنها سد الفراغ القانوني في بعض المجالات، وسوف يمكن لا محالة من مواجهة بعض أشكال الإجرام الجديد). فكانت المحاولات من الحد من هذه الظاهرة المستحدثة على النحو التالي:

### الفرع الأول: مكافحة الجريمة المرتكبة عبر الانترنت في قانون العقوبات:

تدارك المشرع الجزائري خلال السنوات الأخيرة ولو نسبيا الفراغ القانوني في مجال الإجرام المعلوماتي عموما والإجرام عبر الانترنت خصوصا بموجب القانون 04-15[1]. المتضمن تعديل قانون العقوبات، الذي بموجبه جرم المشرع بعض الأفعال المتصلة بالمعالجة الآلية للمعطيات وهي:

**أولا: جريمة التوصل أو الدخول غير المصرح به:** تقوم هذه الجريمة بمجرد ما يتم الدخول غير المرخص به وعن طريق الغش إلى المنظومة المعلوماتية، سواء مس ذلك الدخول أو البقاء كامل المنظومة أو جزء منها فقط[2]، وهو ما أشارت إليه المادة394 كرر من قانون العقوبات بنصها على:

«يعاقب بالحبس والغرامة كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك وتضاعف العقوبة إذا ترتب على ذلك حذف

---

[1]- قانون04-15مؤرخ في 10-11-2004المتضمن قانون العقوبات، الجريدة الرسمية عدد 71الصادر في10-11-2004.

[2]-انظر في ذلك محاضرة ألقيت من طرف بورزام أحمد، وكيل الجمهورية لدى باتنة،تحت عنوان الجرائم المعلوماتية، المجلس القضائي بباتنة يوم 20جوان 2006،ص14.

أو تغيير لمعطيات المنظومة أو ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظومة».
أورد المشرع طرفين لتشدد عقوبة الدخول غير المشروع إلى المنظمات المعلوماتية، أوله حذف أو تغيير المعطيات، والطرف الثاني هو تخريب نظام اشتغال المنظومة، وقد أشار المشرع في المادة المذكورة أعلاه على تجريم فعل الشروع في جريمة الدخول غير المصرح به، ذلك بقوله أو يحاول ذلك.

**ثانيا: جريمة التزوير المعلوماتي:** النشاط الإجرامي في هذه ينحصر في أفعال الإدخال والمحو والتعديل، ولا يشترط اجتماعها معا حتى يتوافر النشاط الإجرامي فيها إذ يتوفر الركن المادي لجريمة بمجرد القيام بفعل واحد على حدا، لكن القاسم المشترك في هذه الأفعال جميعا هو انطواؤها على التلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة غير صحيحة أو محو أو تعديل آخر قائمة[1]. ولقد أكد المشرع على معاقبة هذه الجرائم في المادة394 مكرر1 بنصها:

«يعاقب بالحبس والغرامة كل من أدخل بطريق الغش معطيات نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها».

**ثالثا: جريمة الاستيلاء على المعطيات:** تعد هذه الجريمة من بين أكثر الجرائم وقوعا في العالم الافتراض، وهي ما أقرته المادة394 مكرر2 بنصها على:

« كل من يقوم عمدا أو بطريق الغش1- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو مرسلة أو معالجة عن طريق منظومة معلوماتية 2-حيازة أو إنشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم ».

**رابعا: جريمة إتلاف وتدمير المعطيات:** تطرق المشرع الجزائري بالمادة 394 مكرر 1 من قانون العقوبات والتي تنص على:

[1]- خثير مسعود، **الحماية الجنائية لبرامج الكمبيوتر(أساليب وثغرات)**، دار الهدى، عين مليلة، الجزائر، 2010، ص 123.

«يعاقب بالحبس والغرامة كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي تضمنها».

**خامسا: جريمة الاحتيال المعلوماتي:** تطرقت إليه فحوى 394 مكرر2/ 1من خلال نصها على:

«يعاقب بالحبس والغرامة كل من قام بطريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية...» أي أن يهدف مرتكبها إلى جني فوائد مالية جرَاء ذلك[1].

**سادسا: أنشطة الانترنت المجسدة لجرائم المحتوى الضار والتصريف غير القانوني:** نصت المواد القسم السابع مكرر من ق. ع وخاصة المادة 394 مكرر2/2 على تجريم أفعال الحيازة، الإفشاء والنشر التي تطرأ على المعطيات الآلية بهدف المنافسة غير المشروعة، الجوسسة، الإرهاب، التحريض على الفسق، جمع الأفعال غير المشروعة، وذلك بعقوبتي الحبس والغرامة إضافة إلى ما نصت عليه المادة 394 مكرر 6 بتوقيع عقوبة تكميلية في غلق المواقع التي تكون محلا لجريمة من الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات[2].

تمثل الجزاءات المقررة بموجب الفصل السابع مكرر في العقوبات الأصلية وهي:

عقوبة الحبس والغرامة، وعقوبات تكميلية بموجب نص المادة 394 مكرر 6 والمتمثلة في: المصادرة الأجهزة والبرامج والوسائل المستخدمة وإغلاق المواقع والمحل وأماكن الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها، ومثال ذلك إغلاق مقهى الانترنت الذي ترتكب فيه هذه الجرائم بشرط عام مالكه أو المشرع ظروفا تشدد بها لعقوبة الجريمة وهي:

- حالة الدخول والبقاء غير المشروع إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو تخريب للنظام،
- إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.

[1]–المواد 394 مكرر 2 و394 مكرر 1 و394 مكرر 1/2 من قانون 04-15 المؤرخ في 2004/11/10.

[2]– أنظر المواد 394 مكرر 2 و394 مكرر 6 من قانون 04-15 المؤرخ في 2004/11/10.

أكد المشرع الجزائري أيضا بموجب المادة 394 مكرر5.[1]على تجريم الاشتراك(سواء شخص طبيعي أو معنوي) في مجموعة أو اتفاق بغرض الإعداد لجريمة من الجرائم الماسة بالأنظمة المعلوماتية-بعقوبة الجريمة- وكان التحضير مجسدًا بفعل أو بعدة أفعال مادية[2]. أي بمعنى آخر فإن المشرع استثنى العقاب الأعمال التحضيرية للجرائم المعلوماتية المرتكبة من طرف شخص منفرد.

كما نصت المادة 394 مكرر 4 على توقيع العقوبة على الشخص المعنوي الذي يرتكب إحدى الجرائم الواردة في الفصل السابع مكرر بغرامة تساوي 5 مرات الحد الأقصى للغرامة المحددة للشخص الطبيعي[3]. غير أن المسؤولية الجزائية للشخص المعنوي ستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء في نفس الجريمة، والشروع في الجريمة المعلوماتية يعاقب عليه بالعقوبة المقررة للجريمة ذاتها وهو ما نصت عليه المادة 394 مكرر7 من قانون العقوبات.

نص المشرع الجزائري على حماية الأشخاص من التعدي على حياتهم الخاصة وذلك من خلال المادة 303 مكرر، حيث حددت هذه المادة الحالات التي يتم فيها المساس بحرمة الحياة الخاصة وذلك بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية أو صور في مكان خاص بغير إذن صاحبها أو رضاه.

نخلص إلى أن المشرع الجزائري رغم تداركه من خلال قانون 15-04 والمتضمن تعديل قانون العقوبات الفراغ القانوني في مجال الإجرام المعلوماتي وذلك بتجريم الاعتداءات الواردة على منتجات الإعلام الآلي، فلم يستحدث نصا خاصًا بالتزوير المعلوماتي، ولم يتبنى الاتجاه الذي تبنته التشريعات الحديثة التي عمدت على توسيع مفهوم المحرر ليشمل كافة صور التزوير الحديث.

---

[1]- تنص هذه المادة على أنه«كل من شارك في مجموعة أو أكثر من جرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدّا بفعل أو عدة الأفعال مادية؛ يعاقب بالعقوبات المقررة للجريمة ذاتها».

[2]- بورزام أحمد، المرجع سابق، ص15.

[3]- قارة آمال، **الحماية الجزائية للمعلومات في التشريع الجزائري**، دار هومة للطباعة والنشر والتوزيع، الجزائر، الطبعة الثانية، 2007، ، ص130.

**الفرع الثاني: مكافحة الجريمة المرتكبة عبر الإنترنت في قوانين الملكية الفكرية**

نظرا للاعتداءات التي تتعرض لها مختلف المنتجات الفكرية عبر الإنترنت ارتأينا البحث في مدى إمكانية الحماية من خلال نصوص قانون الملكية الفكرية، وسنفصل ذلك من خلال نقطتين أساسيتين:

**1)** الحماية في إطار قانون الملكية الصناعية.

**2)** الحماية في إطار قانون الملكية الأدبية والفنية.

**أولا: مكافحة الجريمة المرتكبة عبر الانترنت من خلال قوانين الملكية الصناعية.**

**أ. الأمر 06-03 المتعلق بالعلامات التجارية:**

تطرق المشرع الجزائري إلى تنظيم أحكام العلامات التجارية من خلال عدة قوانين آخرها الأم رقم 06-03 المؤرخ في 19-07-2003 والمتعلق بالعلامات التجارية[1].

نعلم أن كل برنامج يحمل اسما خاصا به، لذلك فقد عمد أصحاب البرامج إلى تسجيل هذا الاسم كعلامة تجارية للبرنامج، ولما كانت هذه الحماية قاصرة على الاسم دون المحتوى فقد لجأ أصحاب البرامج إلى وضع الاسم مقترنا به، غير أن الحماية بأحكام العلامات التجارية قد تكون فعالة بالنسبة للنسخ البسيط، لكن ليس الأمر كذلك بالنسبة للنسخ المعقد.

**ب. في الأمر 03-07المتعلق ببراءة الاختراع:**

عرفت المادة 02 من الأمر 03-07 الاختراع على أنه فكرة لمخترع تسمح عمليا بإيجاد حل لمشكل محدد في مجال التقنية، وبشأن الشروط التي يجب توافرها في الاختراع فتتمثل فيما يلي: (شرط الابتكار، شرط الجدة، القابلية للتطبيق الصناعي، المشروعية) 2.

يتحصل المخترع في حال توافر هذه الشروط على براءة الاختراع وهي الوثيقة التي تمنحها الدولة للمخترع فتخول له حق استغلال اختراعه والتمتع بالحماية القانونية المقررة لهذا الغرض وذلك لمدة محدودة وبشروط معينة والجهاز المانح لهذه الشهادة هو المعهد الجزائري لحماية

---

[1]- تجسدت هذه القوانين: أم 66-57 المؤرخ في 19-03-1966المتعلق بعلامات المصنع والعلامات التجارية، المعدل والمتمم بـ أمر رقم 67-233 مؤرخ في19-10-1967المتضمن أحكام العلامات التجارية والمعدل أمر رقم 03-06مؤرخ في 19 جويلية 2003 ، والمتعلق بالعلامات، الجريدة عدد 44 صادر بـ 23-جويلية 2003.

[2]- أنظر المادة 2من القانون03-07 المؤرخ في19-7-2003 المتعلق ببراءة الاختراع، الجريدة الرسمية عدد 44 صادر في 23-07-2003.

الملكية الصناعية[1]. غير أن السؤال المطروح هو هل تستفيد برامج الحاسب من الحماية بواسطة براءات الاختراع؟

التشريعات المعاصرة بصفة عامة تستبعد البرامج المعلوماتية من مجال الحماية بواسطة براءات الاختراع لأحد السببين:

- إما تجرد البرامج من أي طابع صناعي.
- إما صعوبة البحث في مدى جدة البرنامج لتقدير مدى استحقاقا البرنامج لبراءة فليس من الهين توافر شرط الجدة في البرمجيات وليس من الهين إثبات توافر هذا الشرط إذ يجب أن يكون لدى الجهة التي تقوم بالفحص الطالبات البراءة قدر معقول من الدراية لتقر ما إذا كان قد سبق تقديم اختراعات مشابهة الاختراع المقدم الطلب بشأنه أم لا، الأمر الذي يتطلب أن يكون هذه الجهة على درجة عالية من الكفاءة والتمييز في المجال التي تتولى بحثه[2].

إضافة إلى التحفظ العملي لمنتجي برامج الحاسب على استعمال قوانين براءة المخترع، ويتمثل هذا التحفظ في الإجراءات المعقدة للحصول على البراءة والتكلفة العالية والمدد الطويلة التي يستغرقها هذا التسجيل، فعمر البرنامج قصير نسبيا لا يتعدى ثلاثة سنوات بينما قد تمتد إجراءات تسجيل البراءة مثل ذلك أو أكثر وعليه يمكن للغير الوصول إلى سر البرنامج واستغلاله قبل صدور البراءة.

تجدر الإشارة إلى أن المشرع الجزائري قد استبعد البرامج المعلوماتية صراحة من مجال الحماية بواسطة براءة الاختراع والتي نصت على أنه :"لا تعد من قبل الاختراعات في مفهوم هذا الأمر برامج الحاسوب ".

**ثانيا: مكافحة الجريمة المرتكبة عبر الانترنت من خلال قوانين الملكية الأدبيّة والفنية.**

شهد النصف الأخير من القرن العشرين تطورا ملحوظا في مجال الاتصال رافقه تطور في وسائل نقل الإنتاج الفكري على اختلاف صوره من علوم وفنون وآداب، مما أوجد مصنفات

[1]– شبراك حياة، **حقوق صاحب براءة الاختراع في القانون التجار الجزائري**، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص قانون الأعمال، كلية الحقوق والعلوم الإدارية، الجزائر، 2002 ص17.

[2] –آمال قارة،المرجع السابق، ص 78–79.

جديدة جديرة بحماية حق المؤلف كانت محل اهتمام ودراسة من قبل المتخصصين في مجال الملكية الفكرية[1].

اتجه المشرع الجزائري صراحة إلى الاعتراف صراحة بوصف المصنف المحمي لمصنفات الإعلام الآلي، وذلك من خلال تعديله للأمر 73-14بموجب الأمر 97-10[2]. والذي يتبين من خلال استقراءنا له مايلي:

**1.** أن المشرع الجزائري وسع قائمة المؤلفات المحمية حيث أدمج تطبيقات الإعلام الآلي ضمن المصنفات الأصلية، والتي عبر عنها بمصنفات قواعد البيانات وبرامج الإعلام الآلي التي تمكن من القيام بنشاط علمي، أو أي نشاط من نوع آخر أو الحصول على نتيجة خاصة من المعلومات التي تقرأ بآلة وتترجم باندفاعات الكترونية بالحاسوب. أما قواعد البيانات فهي عبارة عن مجموعة من المصنفات والأساليب والقواعد، كما يمكن أن تشمل الوثائق المتعلقة بسير المعطيات وقد أشارت المادة5 إلى قواعد البيانات بنصها:" تعتبر أيضا مصنفات محمية الأعمال الآتية:مجموعات المعلومات البسيطة التي تأتي أصالتها من انتقاء مواردها أو تنسيقها أو ترتيبها".

**2.** أن الحماية تحدد من25سنة إلى 50سنة بعد وفاة المبدع تماشيا مع اتفاقية مع اتفاقية برن ، وبالتالي هذه المدة تشمل حتى مصنفات الإعلام الآلي.

**3.** تشديد العقوبات الناجمة عن المساس بحقوق المؤلفين لاسيما مؤلفي المصنفات المعلوماتية، إذ في السابق تجريم الاعتداءات على الملكية الفكرية تناولت المواد390-394من قانون العقوبات، لكنها أخرجت بموجب الأمر 97-10 من مضلة قانون العقوبات وأصبح لها

[1]- Fauchoux Uincent Deprez pierre.op-cit , p215.

[2]- أمر رقم 97-10 مؤرخ في 06-03-1997 المتعلق بحق المؤلف والحقوق المجاورة، الجريدة الرسمية عدد 13صادر في12-3-1997، معدل ومتمم بـ أمر 03-05 مؤرخ في 19-7-2003 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية عدد44 صادر في 2003/07/23 .

تجريم خاص، حَيث أن قانون العقوبات كان يقرر بموجب المادة393 الغرامة كعقوبة للاعتداء على حق المؤلف، بينما الأمر 97-10 وكذا الأمر 03-05 يقرر ان عقوبتي الحبس والغرامة[1].

اتضح مما سبق أن المشرع الجزائري سواءًا بدافع توفير الحماية الجزائية للمعلوماتية أو بدوافع خارجية قد واكب التطورات الحاصلة في المجال المعلوماتي، بأن أخضع المعلوماتية لقانون الملكية الفكرية موسعا بذلك من سلطة القاضي في تقرير العقوبة، وذلك ضمانا وحماية لحق المؤلف ومالك الحق المجاور.

**الفرع الثالث: مكافحة الجريمة المرتكبة عبر الانترنت قانون الوقاية من الجرائم بتكنولوجيات الإعلام والاتصال:**

سنتطرق فيما يلي إلى أسباب صدور القانون رقم 09-04 مؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وكافحتها، ثم إلى مضمون هذا القانون باختصار.

**أولا: أسباب صدور قانون مكافحة الجرائم المعلوماتية:**

دفع القصور الذي عرفه القانون رقم04-15 والمعدل لقانون العقوبات الذي نص على حماية جزائية نسبية لأنظمة المعلومات من خلال تجريم مختلف أنواع الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، بالمشرع الجزائري إلى سد الفراغ التشريعي الذي يعرفه مجال الجرائم المتعلقة بوسائل الإعلام والاتصال وخاصة الجرائم الناشئة عن استخدام غير المشروع لشبكة الانترنت، خاصة في ظل الثورة التي تعرفها في مجال استخدام الانترنت، وذلك بوضع هذا القانون من أجل تعزيز القواعد السابقة من خلال وضع إطار قانوني أكثر ملائمة مع خصوصي الجريمة المرتكبة عبر الانترنت[2].

كما تكمن أهمية هذا القانون في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة هذه والتدخل السريع لتحديد مصدرها والتعرف على مرتكبها.

---

[1]- آمال قارة، المرجع السابق، ص 78-79.

[2]- القانون رقم 09-04 المؤرخ في 2009/2/5 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلا والاتصال ومكافحتها، الجريدة الرسمية عدد 47 لسنة 2009.

**ثانيا: مضمون قانون مكافحة الجرائم المعلوماتية:**

يحتوي قانون09-04المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على ستة فصول نلخصها فيما يلي:

**الفصل الأول:** نص على الأحكام العامة التي تبين الأهداف المتوخاة من القانون وتحدد من المفهوم مصطلح التقنية الواردة وكذا مجال تطبيق أحكامها.

**الفصل الثاني:** حيث جسد أحكام خاصة بمراقبة الاتصالات الالكترونية؛ وقد روعي في وضع هذه القواعد خطورة التهديدات المحتملة وأهمية المصالح المحمية. حيث نص القانون على أربع حالات يسمح فيها للسلطات الأمنية لممارسة الرقابة المراسلات والاتصالات الالكترونية، منها الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب والجرائم التي تمس بأمن الدولة، وكذلك في حال توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام، ولمقتضيات التحريات والتحقيقات القضائية ما عنده يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية؛ وفي إطار تنفيذ الطلبات المساعدة القضائية الدولية المتبادلة.

**الفصل الثالث:** تضمن القواعد الإجرائية، الخاصة بالتفتيش والحجز في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وذلك وفقا لمعايير العالمية المعمول بها في هذا الشأن، ومع مراعاة ما تضمنه قانون الإجراءات الجزائية من مبادئ عامة وعلى هذا الأساس يجوز للجهات القضائية وضباط الشرطة القضائية الدخول والتفتيش ولو عن بعد إلى المنظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها، مع إمكانية اللجوء إلى مساعدة السلطات الأجنبية المختصة من أجل الحصول على المعطيات المبحوث عنها في

منظومة معلوماتية تقع في بلد أجنبي، ويسمح القانون للمحققين باستنساخ المعطيات محل البحث في حال تبين جدوى المعلومات المخزنة في الكشف عن الجرائم أو مرتكبيها[1].

**الفصل الرابع:** تطرق إلى التزامات المتعاملين في مجال الاتصالات الالكترونية وذلك من خلال تحديد الالتزامات التي تقع على عاتق المتعاملين في الاتصالات الالكترونية لاسيما التزام حفظ المعطيات المتعلقة بحرمة السير والتي من شأنها المساعدة في كشف الجرائم ومرتكبها، يهدف هذا القانون إلى إعطاء مقدمي الخدمات دور ايجابيا ومساعدًا للسلطات العمومية في مواجهة الجرائم وكشف مرتكبها. حيث ألزم هذا القانون مقدمي الخدمات الانترنت على التدخل الفوري لسحب المحتويات التي تم بإمكانهم الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقانون، وتخزينها أو جعل الدخول إليها غير ممكن، إضافة إلى وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام والآداب العامة وإخطار المشتركين لديهم وجودها.

**الفصل الخامس:** أشار إلى الهيئة الوطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام والاتصال ومكافحته، إذا نص القانون على إنشاء هيئة وطنية ذات وظيفة تنسيقية في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وقد تم الإحالة على التنظيم فيما يخص تحديد كيفية تشكيل وتنظيم هذه الهيئة[2].

يعتبر القانون رقم 09-04المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها نطاقا واسعا في مجال مكافحة الجرائم المرتكبة عبر الانترنت، حيث جاء كجريمة للأفعال المخالفة للقانون والتي ترتكب عبر وسائل الاتصال عاما.

---

[1]-فشار عطاالله، **«مواجهة الجريمة المعلوماتية في التشريع الجزائري»**،الملتقى المغربي حول القانون والمعلوماتية،أكاديمية الدراسات العليا، ليبيا، أكتوبر ،2009 ،ص35.

[2]-المواد13 و14من قانون09- المؤرخ في 2009/2/5.

## الخاتـــــــمة:

من خلال دراستنا لجرائم المساس بالأنظمة المعلوماتية فإنه يتبيّن لنا أنها من أكثر الجرائم خطورة ، و يرجع ذلك إلى ما تتصف به هذه الجرائم عن الجرائم التقليدية من اختلاف، أضف على ذلك أنها التحديات التي فرضتها على الجهات الخاصة بوضع القوانين و إنفاذها.

فجرائم المساس بالأنظمة المعلوماتية مشكلة من المشكلات التي أفرزتها المعلوماتية،فهذه الثورة على قدر ما قدمته من تسهيلات للأفراد والمجتمعات على حد سواء فإنها قد زعزعت سكينتهم بهذا النوع الجديد من الجرائم التقنية والعلمية المعقدة.

تميزت جرائم المساس بالأنظمة المعلوماتية عن الجرائم التقليدية بعدة خصائص، فقد تعددت التعريفات واختلفت في وصف هذه الظاهرة الإجرامية المستحدثة، كذلك تميزها بطابعها العابر للحدود، بالإضافة إلى ضعف القائمين على مكافحتها نظرا إلى تطورها التسارع في ارتكابها، و بالتالي فإن هذه الخصائص كان لها الدور الكبير في إبراز النشاط الإجرامي لهذه الجرائم المستحدثة و إيضاح الاختلاف الجوهري لها عن الخصائص العادية للجرائم التقليدية.

إن السمات التي انفرد بها المجرم المعلوماتي أضفت التميز لجرائم المساس بالأنظمة المعلوماتية، فهو يعتبر من الأشخاص الذين يتمتعون بنسب عالية من الذكاء و المهارة و المعرفة فهو يرتكب جرائمه في هدوء دون أن يلفت الانتباه،كما أن كثرة القطاعات المستخدمة للانترنت أمكنته من الاعتداء على أكثر من قطاع واحد عبر مختلف أنحاء العالم و ذلك من خلال الضغط على زر واحد، وهذا ما ليس باستطاعة المجرم التقليدي فعله.

و تعد أهم خصوصية تتمتع بها جرائم المساس بالأنظمة المعلوماتية هي عدم إمكانية تطبيق أحكام الجرائم التقليدية عليها وسبب ذلك هو صعوبة تصنيفها فهي تتسم بالتشعب و عدم إمكانية حصرها .

كل هذه الخصوصيات التي تتميز بها جرائم المساس بالأنظمة المعلوماتية جعلت مختلف الدول و الهيئات الدولية تدرك مدى خطورة هذه الظاهرة الإجرامية والتحديات التي تفرضها عليها،مما أدى بها إلى محاولة وضع أطر قانونية من خلالها يمكن وضع طرق فعالة لمكافحتها، و قد تمثلت هذه الجهود بالخصوص في اتفاقية بودابست 2001 لمكافحة الجريمة

المعلوماتية دون إغفال جهود المعاهدات و القوانين بحماية الملكية الفكرية،بالإضافة إلى هذه الجهود هناك جهود تبذل على المستوى العربي كالقانون العربي النموذجي، وعلى المستوى العالمي كجهود الأمم المتحدة والقوانين المقارنة،

أما بالنسبة إلى المشرع الجزائري فنجده قد واكب ولو بقدر قليل الحركية التشريعية التي فرضت نفسها عالميا، خاصة مع دخول الإنترنت في نواحي حياة المواطن الجزائري ، فبد الفراغ التشريعي الذي كانت تعاني منه الجزائر في لهذا المجال سعت لسده في بادئ الأمر بتعديل قانون العقوبات و ذلك بالقانون 04-15 ، لكن محدوديته دفعت بالمشرع الجزائري إلى إصدار قانون خاص 04-09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و محاولتها، بالإضافة إلى قوانين الملكية الفكرية.

إلى أن المشرع الجزائري يبقى بعيدا كل البعد عن التطور القانوني على المستوى العالمي من جهة ، و تطور أساليب ارتكاب جرائم المساس بالأنظمة المعلوماتية.

و إزاء هذا فإننا نقترح ما يلي :

1-إصدار تشريعات جديدة أو تعديل التشريعات الجزائية القائمة لمواجهة جرائم المساس بالأنظمة المعلوماتية و ذلك بتقرير الجرائم و تحديد العقوبات المناسبة لها بغية حماية النظام المعلوماتي.
2-اعتماد الدقة و الوضوح و الحبكة القانونية عند تحديد أنماط السلوك الإجرامي و الابتعاد عن التعبيرات الغامضة أو المطاطية التي تحمل أكثر من معنى .
3-عدم الاقتصار عند التجريم و العقاب على أنماط السلوك المحظور حاليا بل يجب مراعاة الأبعاد المستقبلية لأن تكنولوجيا المعلومات و الحواسيب في تطور سريع بل يكاد يكون مذهل.

## قائمة المراجع

### أ- القوانين الدولية:


1. اتفاقية مكافحة استعمال تكنولوجيا المعلومات لإغراض إجرامية ، رقم (55/63) ، الصادرة عن هيئة الأمم المتحدة، الجلسة العامة81، ديسمبر 2000 .
2. مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، البند الثامن من جدول الأعمال المؤقت، التطورات الأخيرة، في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة بما فيها الجرائم الحاسوبية، المنعقد بالبرازيل 12-19 أفريل 2010، رقم213/09. A/Conf.
3. مؤتمر هيئة الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المعلوماتية عبر الوطنية، المنعقد بفيينا في 18-22، أكتوبر 2010، رقم:5 crp / CTOC/Cop/2010.


### ب - النصوص القانونية:


1. أمر رقم 97-10 مؤرخ في 06-03-1997 المتعلق بحق المؤلف والحقوق المجاورة، الجريدة الرسمية عدد 13صادر في12-3-1997.
2. أمر رقم 03-07 المؤرخ في19-7-2003 المتعلق ببراءة الاختراع، الجريدة الرسمية عدد 44 صادر في 23-07-2003.
3. أمر رقم 03-05 مؤرخ في 19-7-2003 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية عدد44 صادر في 2003/07/23 .
4. أمر رقم 04-15 مؤرخ في 10-11-2004المتضمن قانون العقوبات، الجريدة الرسمية عدد 71الصادر في10-11-2004.
5. أمر رقم 09-04 المؤرخ في 2009/2/5 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47 لسنة 2009.
6. أمر رقم 03-06 مؤرخ في 19 جويلية 2003 ، والمتعلق بالعلامات، الجريدة عدد 44 صادر بـ 23-جويلية 2003.

**جـ –الكتب:**


1. أحمد خليفة الملط، **الجرائم المعلوماتية**، دار الفكر الجامعي، الإسكندرية، الطبعة الثانية، 2006.
2. أحمد فتحي السرور،**الوسيط في قانون العقوبات (القسم العام)**،دار النهضة العربية، الطبعة السادسة ،القاهرة،1991.
3. أسامة سمير حسين، **الاحتيال الالكتروني(الوجه القبيح للتكنولوجيا)**، الحنادرية للنشر والتوزيع، الأردن، الطبعة الأولى،2011.
4. آمال قارة، **الحماية الجزائية للمعلومات في التشريع الجزائري**، دار هومة للطباعة والنشر والتوزيع، الجزائر، الطبعة الثانية، 2007.
5. أيمن عبد الحفيظ ، **الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية**، دون دار النشر، دون بلد النشر، 2005.
6. إيهاب فوزي السقا، **جرائم التزوير في المحررات الالكترونية**، دار الجامعة الجديدة، الإسكندرية، 2008.
7. جعفر حسن جاسم الطائي، **جرائم تكنولوجيا المعلومات(رؤية جديدة للجريمة المعلوماتية)**، دار البداية، عمان، 2007.
8. جميل عبد القادرة الصغير، **الانترنت والقانون الجنائي**، دار النهضة العربية القاهرة،دار النهضة العربية، القاهرة، 2002.
9. حسن طاهر داود، **جرائم نظم المعلومات**، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2000.
10. حمد عبيد الكعبيي، **الجرائم الناشئة عن الاستخدام الغير المشروع لشبكة الإنترنت**، دار النهضة العربية، القاهرة، بدون سنة.
11. خالد ابراهيم ممدوح، **الجرائم المعلوماتية**، دار الفكر الجامعي، بدون بلد، الطبعة الأولى، 2009.
12. خالد بن عبد الله بن معيض العبيدي، **الحماية الجنائية للتعاملات الالكترونية**، في نظام المملكة العربية السعودية جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم الجناية، الرياض، 2009.

13. خالد ممدوح إبراهيم، **أمن الجريمة المعلوماتية**، الدار الجامعية، الإسكندرية، 2010.
14. خثير مسعود، **الحماية الجنائية لبرامج الكمبيوتر(أساليب وثغرات)**، دار الهدى، عين مليلة، الجزائر، 2010.
15. سامي علي عياد، **الجريمة المعلوماتية والانترنت(الجرائم الالكترونية)**، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت،2007.
16. طارق إبراهيم الدسوقي عطية، **(الأمن ألمعلوماتي، النظام القانوني لحماية المعلوماتي)**، دار الجامعة الجديدة للنشر، الإسكندرية،2009.
17. عباس أبو شامة عبد المحمود، **عولمة الجريمة الاقتصادية**، جامعة نايف العربية للعلوم الأمنية، الرياض،2009.
18. عبد الفتاح بيومي حجازي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت**، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى،2006.
19. عبد القادر القهوجي، **الحماية الجنائية لبرنامج الحاسب الآلي**، دار الجامعة الحديث، الاسكندرية، 2006.
20. عبد الله بن عبد العزيز اليوسفي، **أساليب تطور البرامج والمناهج التدريبية لمواجهة المستحدثة**، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى،2004.
21. عبد الله عبد الكريم عبد الله، **جرائم المعلوماتية والإنترنت(الجرائم الالكترونية)**، منشورات الحلبي الحقوقية، بيروت، طبعة أولى، 2007.
22. علي عدنان الفيل، **الإجرام الالكتروني**، الطبعة الأولى، منشورات زين الحقوقية، دمشق، 2011.
23. عمرو موسى الفقهي، **الجرائم المعلوماتية(جرائم الحسب الآلي والانترنت في مصر والدول العربية)**، المكتب الجامعي الحديث، الإسكندرية،2006.
24. فوزية عبد الستار، **قانون العقوبات–القسم الخاص**– دار النهضة العربية، بدون بلد، 1988.
25. محمد أمين الرومي، **جرائم الكمبيوتر والانترنت**، دار المطبوعات الجامعية، الإسكندرية، 2003.

26. محمد دباس الحميد، ماركو إبراهيم نينو، **حماية أنظمة المعلومات**، دار حامد للنشر والتوزيع، عمان، الطبعة الأولى،2007.
27. محمد سامي الشوا، **ثورة المعلومات وانعكاساتها على قانون العقوبات**، دار النهضة العربية، القاهرة، 1988.
28. محمد علي عريان، **الجرائم المعلوماتية**، دار الجامعة الجديدة، الإسكندرية، 2004.
29. محمود أحمد عبابنة، **جرائم الحاسوب وأبعادها الدولية**، دار الثقافة للنشر والتوزيع، الأردن، 2005.
30. محمود نجيب حسني ، دروس في القانون الدولي الجنائي ، دار النهضة الدولية القاهرة ،1960.
31. مصطفى محمد موسى، **أساليب إجرامية بالتقنية الرقمية (ماهيتها، مكافحتها)**، دار الكتب القانونية، مصر، 2005.
32. منير محمد الجنيهي: ممدوح محمد الجنيهي، **جرائم الانترنت والحاسب وسائل مكافحتها**، الإسكندرية، دار الفكر الجامعي، 2004.
33. نائلة عادل محمد فريد قورة، **جرائم الحاسب الآلي الاقتصادية دراسة نظرية و تطبيقية**، دار النهضة العربية،2004.
34. نسرين عبد الحميد نبيه، **الجريمة المعلوماتية والمجرم المعلوماتي**، منشأة المعارف، الأردن، بدون سنة.
35. نعيم مغبغب، **(حماية برامج الكمبيوتر الأساليب والثغرات–دراسة في القانون المقارن)**منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، 2006.
36. نهلا عبد القادر المومني، **الجرائم المعلوماتية**، دار الثقافة للنشر والتوزيع، الطبعة الثانية .
37. هدى حامد قشقوش، **جرائم الحواسب الالكترونية في التشريع المقارن**، دار النهضة العربية، القاهرة، 1992.
38. هلالي عبد الله أحمد، **الجوانب الموضوعية والاجرائية للجريمة المعلوماتية على ضوء اتفاقية بودابست الموقعة في 2001/11/23**، دار النهضة العربية، القاهرة، 2003.

39. هيثن نيازي فهمي، **رحلة عبر شبكة الانترنت**، طبعة أولى،دون بلد نشر، 1969.

**د- المذاكرات** :

1. خالد عبد الله بن معيض العبيدي، **الحماية الجنائية للتعاملات الالكترونية في نظام المملكة العربية السعودية (دراسة تحليلية مقارنة)** ، بحث مقدم استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص سياسة جنائية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجناية، الرياض، 2009.
2. شبراك حياة، **حقوق صاحب براءة الاختراع في القانون التجار الجزائري**، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص قانون الأعمال، كلية الحقوق والعلوم الإدارية، الجزائر،2002.
3. عبد الرحمن محمد بن بحر، **معوقات التحقيق في جرائم الإنترنت**، دراسة سطحية على ضباط الشرطة في البحرين، رسالة مقدمة إلى معهد الدراسات العليا استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية ،أكاديمية نايف للعلوم الأمنية، معهد الدراسات العليا، قسم العلوم الشرطية، الرياض، 1999.

**و- المقالات:**

1. إلياس بن سمير الهاجري، « **جرائم الانترنت** »، الدورة التدريبية لمكافحة الجرائم الإرهابية المعلوماتية المنعقدة بكلية التدريب، قسم البرامج التدريبية، القنيطرة، المملكة المغربية من9- 13، 2006.
2. عباس أبو شامة عبد المحمود، «**التعريف بالظواهر الاجرامية المستحدثة: حجمها، أبعادها ونشاطها في الدول العربية**»، الندوة العلمية للظواهر الاجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف للعلوم الأمنية؛ تونس، أيام28 -30 جوان 1999.
3. عبد القادر دوحة، محمد بن حاج الطاهر، «**مدى مواكبة المشرع الجزائري لتطور الجريمة الالكترونية**»، الملتقى الوطني الأول، النظام القانوني للمجتمع الالكتروني، المركز الجامعي خميسي مليانة، معهد العلوم القانونية والإدارية، 9-10-10مارس2008.

4. عبد الكريم خالد الشامي،« **جرائم الكمبيوتر والانترنت في التشريع الفلسطيني**»، ص19، http://www-pal-ip. org
5. عمر الشيخ الأصم، «**البطاقات الائتمانية المستخدمة الأكثر إنتشارا في البلاد العربية**»، أعمال ندوة تزوير البطاقات الائتمانية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2002.
6. فشار عطا الله،«**مواجهة الجريمة المعلوماتية في التشريع الجزائري**»، الملتقى المغاربي حول القانون والمعلوماتية، أكاديمية الدراسات العليا، ليبيا، أكتوبر، 2009.
7. كريستينا سكولمان، «**عن جرائم الانترنت: طبيعتها وخصائصها**»، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، أيام19 -20 يونيو 2007.
8. محمد سيد سلطان، **قضايا قانونية في أمن المعلومات وحماية البيئة الالكترونية**، دار ناشري للنشر الالكتروني، 2004، ص13. متوفر على الموقع التالي:www.Nashiri.net
9. محمد عبد الرسول خياط، «**عمليات تزوير البطاقات الائتمانية**»، أعمال ندوة تزوير البطاقات الائتمانية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2002.
10. محمد محمد صالح الألفي،«**أنماط جرائم الانترنت**»، ص11، http://www-eastlaws. com
11. ناصر محمد البقهي، «**اثر التحويل مجتمع معلوماتي على الأمن الفكري**»،المؤتمر الوطني الأول للأمن الفكري المفاهيم والتحديات، كرسي الأمير نايف بن عبد العزيز لدراسات الأمن لفكري بجامعة الملك سعود، المملكة السعودية،22-25جمادى الأولى1430هـ.
12. هشام محمد فريد رستم، "**الجرائم المعلوماتية. أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية موحدة للتدرب التخصصي**"، بحوث مؤتمر القانون والكمبيوتر والإنترنت، من 1-3 ماي 2000، بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثاني، الطبعة الثالثة، 2004.

13. يونس عرب، «**قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وتجربة سلطة عمان**»، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، المنعقدة بمسقط، سلطة عمان، 2-4أفريل، 2006.

## هـ-المراجع باللغة الأجنبية:

1. Debray stéphan, internet face aux substances illicites: complice de la cyber criminalité ou outil de prevention ?, Dess média eléctronique and internet, Université de paris, 8.20002-2003.
2. Fauchoux. Vincent- Deprerz pierre,**le Droit de l'internet (loi, contra et u sage),** édition, litec, Paris, 2008.
3. Mascala corinne, «**criminalité et contrat électronique**», Travaux de l'association CAPITANT Henir, journées national, paris, 2000.
4. Sedalian.. Valérie. **Droit de l'internet-Reglementation-Responsabilites,** Edition Net Press ,paris 1997.

**الفهرس:**

## ملخص

شهد العالم ثورة من نوع غير مألوف اصطلح على تسميتها بثورة المعلومات، كان بطلها جهاز الحاسب الآلي الذي تطور دوره بحيث تعدى إجراء العمليات الحسابية المعقدة ليشمل قضايا الناس في جميع معاملاتهم،إلاّ أنه واكب هذه الثورة آثار سلبية تجسدت في الجرائم المستحدثة التي ترتكب عن طريق الوسائل التقنية والتي يطلق عليها ب جرائم المساس بالأنظمة المعلوماتية.

يثير هذا الإجرام المعاصر الكثير من الإشكالات و في نواحي عديدة ، أهمها صعوبة اكتشاف هذه الجرائم وإثباتها، فالمجرم المعلوماتي يستطيع جرائم المساس بالأنظمة المعلوماتية دون أن يترك خلفه أية آثار خارجية ملموسة، خصوصا وأنه مجرم يتميز بالذكاء والمهارات التقنية العالية، كما أنه على دراية بمجال المعلومات و أنظمة برامج الحاسبات الآلية.

وأمام خصوصيات و خطورة جرائم المساس بالأنظمة المعلوماتية، كان لابد من تكاتف التشريعات الدولية والداخلية لمكافحتها وإيجاد إطار خاص بها لهذه الجريمة المستحدثة.

**résumé**

Le monde a connu une sorte de révolution inconnu appelé la révolution de l’information, il a défendu votre ordinateur ce rôle a évolué de telle sorte dépassé effectuer des calculs complexes pour inclure les questions de la population dans toutes leurs relations , mais il a accompagné cette révolution effets négatifs contenus dans les crimes créé perpétrés par des moyens crimes et techniques dits de systèmes informatiques de préjudice .

Cela soulève le lot contemporain du crime de problèmes et à bien des égards , notamment la difficulté de la découverte de ces crimes et de prouver , informatique crimes capables compromissent information sur les systèmes sans laisser derrière leur les effets des béton externe , en particulier comme un criminel , se caractérise par des compétences des renseignements et techniques des hauts niveau , comme il est familier avec le domaine de l'information systèmes et programmes d'ordinateurs .

L'avant des spécificités de la gravité des crimes et des systèmes préjudice de l'informatique , a dû être une législation internationale concertée et cadre de contrôle interne et la création de sa propre pour ce crime développé .