

مجزوءة: الجريمة المنظمة العابرة للحدود

ماستر: قانون الجنائي والتعاون الجنائي الدولي
الوحدة: السادسة التاسعة

عرض حول:

الجريمة المعلوماتية

تحت إشراف الدكتور:

نور الدين العمراني

من إعداد الطلبة:

فؤاد محسين

محمد رضى بنخيرة

نعيمة الشركي

السنة الجامعية

2018 - 2017

المقدمة:

عرفت الجريمة منذ فجر البشرية، وقد ناهضها الإنسان منذ اللحظة الأولى التي استشعر فيها بخطر يهدد كيانه وتقدمه بل ويهدد أدميته، فالجريمة هي إفراز للمجتمع ومظهر من مظاهره ومن ثم تعكس كافة ما تموج به المجتمعات من ظروف وأسباب حيث أن ذلك مرجعه إلى ما يحتويه السلوك الإنساني في علاقاته المتشابكة من جمع العنصري الخير والشر وتصارعهما بصفة دائمة في دورة الحياة اليومية وبالتالي يستحيل تصور خلو الحياة دون اجتماع مظهريهما¹، لهذا تعد الجريمة ظاهرة إنسانية بامتياز فهي أيضا تعتبر ظاهرة طبيعية لكونها تتلازم مع مختلف أوجه الحياة أينما وجدت²، إلا أن الجريمة لا تعرف الثبات بل تتصف بالمرونة حيث تتغير وتتطور مع مرور الزمن والوقت، وتؤكد ذلك باللموس خلال السنوات الأخيرة من القرن العشرين وبداية القرن الحادي والعشرين، وهي الحقبة التي برزت فيها الثورات التكنولوجية وما منحتها هذه الأخيرة من امتيازات الإنسانية، بيد أنه للأسف أضحت تستخدم كوسيلة ومحطة لارتكاب جرائم تختلف صورها سواء سرقة أو تزيف أو تزوير وقس على ذلك.

وهذا التطور إذن أدى إلى بروز جرائم حديثة، تشكل تحديا جديدا في عالم الجريمة تعرف بالجرائم الالكترونية، والتي يقصد بها "نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غيرها كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"³.

وبناء على بروز هذا النوع من الجرائم فرضت الضرورة على المشرع بأن يتدخل بموجب نصوص تشريعية جنائية تقف ندا للند أمام مرتكبي هذا النوع من الجرائم.

وعلى مستوى التاريخي، فمنذ القدم والإنسان في تطلعه لحياة أفضل يحاول أن يبتدع الوسائل التي ترفع عن كاهله عبء القيام بعدة مهام، فتم ابتكار الوسائل التكنولوجية لتوفير المساعدة الإنسانية لكن سرعان ما أضحت هذه الوسائل تلحق ضررا بالبشرية عن طريق

¹ - أحمد خليفة الملط: الجرائم المعلوماتية، د.ط. دار الفكر الجامعي، الإسكندرية، سنة 2005، ص 5 و6.

² - محمد أحداق: علم الإجرام، الطبعة الثالثة، مطبعة سجماسة، مكناس، 2014-2015.

³ - عبد الفتاح بيومي حجازي: جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، سنة 2006، ص20.

الجرائم التي تستخدم بواسطتها، ومن هذا المنطلق ظهرت جرائم جديدة تدعى بالجرائم المعلوماتية ومن بين صورها جرائم النصب الالكتروني على الأموال العامة والخاصة أو من قبيل الدخول إلى نظم المعالجة الآلية للمعطيات سواء بتغييرها، وحذفها، وإحداث اضطراب في سيرها، أو تزيف أو تزوير وثائق المعلومات أي كان شكلها لإلحاق ضرر بالغير، أو صنع تجهيزات أو أدوات أو إعداد برامج للمعلومات وتملكها بدون وجه حق،¹ وازدياد هذه الخطورة بفعل التقدم الهائل وسائل الاتصال والتكنولوجيا بسبب ذلك تخطى هذا النوع من الجرائم الحدود الوطنية وأصبحت جرائم عالمية²، أصبحت بفعل ذلك الجريمة المعلوماتية تؤدي إلى نتائج وخيمة، إذ أنها أضحت تتيح بالدول، أو نشر إيديولوجية معينة أو التلاعب بالاقتصاد وقس على ذلك إهدار الأموال الطائلة بفعل التلاعب في المعطيات الرقمية وغيرها من التداعيات التي تخلفها الجريمة المعلوماتية .

ويكتسي موضوع الجريمة الالكترونية العابرة للحدود أهمية قصوى، تتمثل بشكل كبير في تنامي هذه الجريمة بشكل ملحوظ لاسيما في ظل التطور الملفت لوسائل الاتصال التكنولوجية التي ساهمت في بروز برائتين هذا النوع من الجرائم، بصدد ذلك ظهرت في أنواع جديدة من الجرائم ترتكب بشكل خفي، مما أصبح معه المجتمع الدولي برمته أمام ضرورة التصدي لهذا النوع من الإجرام، ولو أنه يعد صعب المنال في ظل الصعوبات التي تقف سدا منيعا دون التعرف على الجناة، بسبب سهولة التخلص من معالم الجريمة، لهذا الأمر تعد ظاهرة عالمية تهدد الأفراد والدول³.

¹ - صليحة الحاجي: الآليات القانونية لتكريس الأمن المعلوماتي، مجلة العلوم الجنائية العدد الثاني، سنة 2015، ص 6.

² - محمد الشناوي: جرائم النصب المستحدثة، دبط، دار البيان للطباعة والنشر، القاهرة، 2008، ص 5.

³ - نفس المرجع: ص 6.

وبناء على أهمية الموضوع تظهر إشكالية محورية مفادها:

إلى أي حد تمكنت الجهود الوطنية والدولية في مجال مكافحة الجريمة المعلوماتية ؟

وللإجابة عن هذه الإشكالية تقتضي الدراسة الاعتماد على التصميم التالي:

المطلب الأول: ماهية الجريمة المعلوماتية.

المطلب الثاني: الجهود المبذولة لمكافحة الجريمة المعلوماتية.

المطلب الأول: ماهية الجريمة المعلوماتية

تعتبر الجرائم المعلوماتية من نتائج التطور التكنولوجي في الوقت الراهن فقد تبث أن هناك علاقة ارتباط قوية بين استخدامات الحاسوب الآلي و ارتكاب بعض الجرائم المستحدثة أي استخدامه كأداة لارتكاب الأفعال غير المشروعة , سواء كانت الحاسبات الآلية محلا للجريمة المعلوماتية أو وسيلة لها, من خلال هذا المطلب سيتم التطرق إلى كل من مفهوم هذه الجريمة فقرة أولى وكذا طبيعتها القانونية فقرة ثانية ليتم عرض أنواع هذه الجرائم المعلوماتية في فقرة ثالثة .)

الفقرة الأولى: مفهوم الجرائم المعلوماتية

يعتبر مفهوم الجرائم المعلوماتية وما يرتبط بها من المفاهيم الشائكة والواسعة اختلف بشأنه شرح القانون بشكل عام و القانون الجنائي بشكل خاص لذلك وجب تحديد المقصود بهذه الجريمة أولا وكذا ما يقصد بنظم الحاسوب الآلي ومن يرتكب هذا النوع من الجرائم ثانيا ليتم التعرف على أهم خصائص هذه الجريمة ثالثا .

أولا: تعريف الجريمة المعلوماتية

إن استخدامات الحاسب الآلي المتعددة قد أفرزت بعض الاختلافات الجوهرية بين شراح القانون بصفة عامة و القانون الجنائي بشكل خاص, ويتعلق هذا الاختلاف بصعوبة وضع تعريف محدد لهذه الظاهرة المستحدثة فهناك من يطلق عليها ظاهرة الغش لمعلوماتي أو الاختلاس لمعلوماتي أو الجريمة المعلوماتية فصعوبة وضع تعريف محدد لهذه الجريمة جاءت مخافة البعض من حصرها في نطاق ضيق ومع ذلك فإن بعض الفقه يعرف هذه الظاهرة " بأنها كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات , يهدف إلى الاعتداء على الأموال المادية أو المعنوية " , كما عرفها جانب آخر من الفقه فإنها " عمل أو امتناع يأتيه الإنسان إضرارا بمكونات الحاسب و شبكات الاتصال الخاصة به التي يحميها قانون العقوبات و يفرض لها عقابا"¹

¹ - محمد علي العريان: الجرائم المعلوماتية، د-طدار الجامعة الجديدة للنشر، القاهرة، 2004

ويبدو أن أدق تعريف لهذه الجريمة هي " إن كل فعل إجرامي معتمد أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه وكسب يحققه الفاعل وتكون جديرة بالعقاب "

ثانياً: مفهوم الحاسب الآلي

لتحديد مفهوم الحاسب الآلي ونظم الحاسب الآلي يجب بداية تحديد المقصود به من خلال وضع تعريف له وكذا التعرف على مكوناته وأنواعه لمعرفة كيفية ارتكاب هذه الجرائم عليه

1- تعريف نظم الحاسب الآلي وأنواعه

أ- تعريف نظم الحاسب الآلي

إن تعريف الحاسب الآلي من قبل الباحثين سواء المختصين في هذا المجال أو المهتمين به بشكل عام لم يلقى الإجماع على تعريف واحد يعنى به فهناك من عرفه بأنه : " كل مكونات الحاسب المادية والمعنوية و شبكات الاتصال الخاصة به و التي يمكن بواسطتها تحقيق وظيفة أو هدف محدد"

كما أعطيت تعريفات للحاسب الآلي اصطلاحاً : فقد عرفه البعض بأنه مجموعة متداخلة من الأجزاء لديها هدف مشترك من خلال أداء التعليمات المخزنة أو هو آلة حسابية إلكترونية ذات سرعة عالية ودقة كبيرة يمكنها قبول البيانات وتخزينها و معالجتها للحصول على النتائج المطلوبة

و يعرف أيضاً بأنه عبارة عن جهاز إلكتروني يعمل طبقاً لتعليمات محدد سلفاً ويمكنه استقبال البيانات وتخزينها والقيام بمعالجتها دون تدخل الإنسان ثم استخراج النتائج المطلوبة.¹

وعموماً يمكن تعريف الحاسب الآلي بأنه ذلك الجهاز الإلكتروني الذي يستطيع أن يقوم بأداء العمليات الحسابية والمنطقية طبقاً للتعليمات المعطاة له بسرعة كبيرة فد تصل إلى عشرات الملايين من العمليات الحسابية في الثانية الواحدة وبدرجة عالية الدقة وله

¹ -محمد السامي الشوا: ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الثانية، دار النهضة العربية ، القاهرة، 1998، ص7.

القدرة على التعامل مع كم هائل من البيانات وكذلك تخزينها واسترجاعها عند الحاجة إليها.¹

❖ مرادفات الكمبيوتر

إن لفظ الكمبيوتر لفظ انجليزي ويطلق عليه أيضا لفظ "الحاسب الآلي" "الحاسب الالكتروني" أو "الحاسوب" وهذا المصطلح هو ما استخدمه المجتمع اللغوي واعتمدته المنظمة العربية للمواصفات والمقاييس .

ب : أنواع أجهزة الكمبيوتر

تنقسم أجهزة الكمبيوتر حسب طريقة أدائها إلى:²

❖ كمبيوتر رقمي : وفيه تخزن البيانات في ذاكرته على شكل أرقام فهي تعمل بأسلوب خاص الآ وهو نظام الترميز الرقمي لتمثل البيانات مهما كان نوعها (أرقام ' أحرف , رموز خاصة ...) , وبعبارة أخرى يحول الكمبيوتر الحروف و الأرقام والرموز الخاصة إلى الرقم "0" أو "1" ليتعامل معه .

❖ كمبيوتر قياسي: هو كمبيوتر محدد بالغرض الذي صمم له فقط وهو غالبا ما يستخدم في المجالات العلمية و المصانع و يكون الغرض من استخدامه قياس البيانات المتعلقة بالظواهر الطبيعية كالحرارة و الضغط وسرعة الرياح وكذا قياس الحرارة و الضغط في المعامل

كما تنقسم أجهزة الكمبيوتر حسب حجمها إلى كمبيوتر كبير الحجم وظهر في الخمسينيات وكمبيوتر صغير الحجم في الستينيات وهي تعتمد على استخدام الدوائر المتكاملة, ثم أجهزة مصغرة ظهرت في فترة الثمانينات وتنقسم غالى ثلاثة أنواع :

PERSONAL COMPUTER	❖ كمبيوتر شخصي
PORTABLE COMPUTER	❖ كمبيوتر محمول
HOME COMPUTER	❖ كمبيوتر منزلي ¹

¹ محمد علي العريان مرجع سابق , ص 56

² - محمد أمين الرومي , جرائم الكمبيوتر و الانترنت, دون طبعة, دار المطبوعات الجامعية, الإسكندرية, 2003 , ص 13 .

2- محل جرائم الكمبيوتر

تقع جرائم الكمبيوتر إما على ذاته أو ما يحتويه من معلومات و برامج و إما أن تقع على مكوناته النادية من أجهزة وآلات و شاشة ...

وإما أن تقع باستخدامه بحيث يعد أداة في يد الجاني لتحقيق جريمته

. ففي حالة الجرائم التي تقع على مكونات جهاز الكمبيوتر لا توجد مشكلة في خضوع هذا الفعل لقانون العقوبات كان يقوم شخص بسرقة جهاز كمبيوتر أو جزء منه (جريمة السرقة)، أو أن يقوم بحرق أو إتلاف قطعة منه (جريمة الحرق أو جريمة الإتلاف).

لكن الإشكال يثار في حالة الجرائم الواقعة على المعلومات والبرامج الموجودة داخل الكمبيوتر سواء كانت مخزنة على ديسك مرن أو قرص صلب أو أقراص مضغوطة (سي دي) , وتتمثل هذه الجرائم في تقليد البرامج أو سرقة أو تدميره أو إتلافه أو تعطيل حركته أو العبث في البيانات المخزنة في ذاكرة الجهاز , أيضا يثار المشكل عند استعماله كأداة لتنفيذ الجريمة ومن أمثلتها : جرائم التجسس و التصنت و التزوير في عمليات سحب جوائز المسابقات و تحويل الأموال من حساب إلى آخر أو فك شفرة القنوات التلفزيونية الخاصة التي يمكن مشاهدتها عن طريق الاشتراك و الحصول على بطاقة التشفير وكذلك تحويل مسار الطائرات و السيارات إلى طريق آخر أو القتل عن طريق برمجة الجهاز ليقوم المجرم بتفجير نفسه عن بعد².

¹ محمد أمين الرومي , مرجع سابق ص 14

² نفس المرجع: ص 19 و 20

ثالثا : الجاني والمجني عليه في الجرائم المعلوماتية

لاشك إن الشخص الذي يرتكب الفعل غير المشروع ويعتدي فيه على حق من حقوق الغير بالمعنى الواسع يعد في نظر القانون مجرما يستحق العقاب و فعله هذا يخلف لا محال ضحايا أو مجني عليهم قد تضرر من ذلك الفعل الإجرامي بشكل أو بآخر خاصة أن هؤلاء المجرمين يرتكبون جرائمهم بدقة وذكاء متناهي وتكون نتائجها جد وخيمة

لذلك سيتم التطرق في هذا المحور التعرف على هذين الصنفين أي الجاني و المجني عليه المعلوماتي و كذا أهم الصفات التي يمتازون بها.

1 المجرم المعلوماتي

إن الفقهاء و الباحثين في هذا المجال القانوني بشكل عام يكاد يجمعون على انه لا يوجد تعريف معين للمجرم المعلوماتي لكنهم يجمعون على انه يمتاز بصفات تميزه عن المجرم العادي أو التقليدي أهمها الذكاء و عدم الميل إلى استخدام القوة أو العنف ولا يضع نفسه في حالة عدااء سافر مع المجتمع . ومن خلال هذا المحور سيتم توضيح هذه الصفات (أ) بشكل دقيق وكذا تبيان أنواع المجرمين (ب) و الدوافع المؤدية بهم إلى ارتكاب هذا النوع من الجرائم (ج).

أ: صفات المجرم المعلومات

رغم عدم إيجاد تعريف لهذه الفئة الخاصة من المجرمين إلا انه يمكن تقريب الصورة للتعرف عليهم عن كثب من خلال مجموعة من الصفات التي يمتاز بها هؤلاء المجرمين نجملها فيما يلي :

❖ المجرم المعلوماتي هو إنسان اجتماعي بطبعه

يختلف المجرم المعلوماتي عن المجرم التقليدي في كونه إنسان يحيا وسط المجتمع و يمارس عمله في المجال المعلوماتي أو غيره من المجالات الأخرى أي انه إنسان اجتماعي , ويرتكب جريمته المعلوماتية إما بدافع الكبرياء (طرد مستخدم من عمله) أو بدافع الحسد أو بدافع اللهو أو التحدي أو التفوق في مواجهة امن

الأنظمة المعلوماتية و مبتغاة هو إرضاء غروره و التفاخر بإعماله الإجرامية أمام أقرانه أو تحقيق منفعة مالية .

❖ المجرم المعلوماتي هو إنسان محترف ودكي

ويتسم أيضا المجرم المعلوماتي في هذا الإطار بذكاء متميز يمكنه من احتراف تقنيات التدمير الناعمة وبمعنى آخر يكفي أن يقوم هذا الأخير بالتلاعب في بيانات برامج الحاسب الآلي لكي يمحو هذه البيانات أو يعطل استخدام البرامج فليس عليه إلا زرع الفيروسات فيها أو استعمال تقنيات ذكية لشل حركة النظام المعلوماتي و جعله غير قادر على القيام بوظائفه , وما يقال على الفرد يقال أيضا على الجماعة المنظمة التي تحترف هذا النوع من الإجرام¹.

ب: أنواع المجرم المعلوماتي

تختلف أنواع مرتكب جرائم الكمبيوتر حسب سنهم بين هواة يعشقون عالم المعلومات و الخوض في غماره ويطلق عليه صغار نوابغ المعلوماتية و هناك نوع آخر احتراف الإجرام بكافة السبل و الطرق المتاحة في مجال المعلومات و يطلق عليهم الجرمين المحترفين و بالتالي فان أنواع الجرمين المعلوماتيين تنقسم إلى طائفتين:

❖ الطائفة الأولى: صغار نوابغ المعلوماتية

وهم غالبا ما يكون من طائفة الشباب الذين لديهم معلومات لباس بها عن أنظمة تشغيل الكمبيوتر و غالبا ما يرتكبون هذه الجرائم عن طريق الصدفة البحثية, أي أن الدافع الإجرامي لم يكن متوافر لديهم عند اتصالهم بجهاز الكمبيوتر².

❖ الطائفة الثانية: المجرمين المحترفين

وهم أكثر خطورة من الطائفة الأولى و يحدثون إضرار كبيرة في البرامج و المعلومات و غالبا ما يكونوا من مستخدمي الكمبيوتر و لهم دراية كبيرة جدا

¹-محمد العريان: مرجع سابق، ص 62 و 63.

² محمد سامي الشوا , م س , ص 39

بتقنيات التلاعب أو التدمير أو التعطيل أو شل النظام المعلوماتي بحسب الغرض الذي يسعون إلى تحقيقه من خلال إجرامهم هذا.¹

ج: الأسباب الدافعة إلى ارتكاب جرائم الكمبيوتر

هناك العديد من الأسباب و الغايات التي تدفع الشخص إلى ارتكاب إحدى جرائم الكمبيوتر ومنها:

❖ الشغف بالالكترونيات

إن من أهم الأسباب الدافعة إلى ارتكاب هذا النوع من الجرائم الحصول على الجديد في المعلومات فيرى قراصنة الكمبيوتر إن الحصول على المعلومة يجب إلا يكون عليه أي قيد فالقرصان يكرس كل جهده في تعلم كيفية اختراق المواقع الممنوعة وغالبا ما يكون القراصنة مجموعات يكون الهدف منها التعاون و تبادل المعلومات وتقاسم البرامج والأخبار .

ويفضل القراصنة أن يكونوا مجهولين حتى يتمكنوا من الاستمرار في التواجد داخل الأنظمة لأطول فترة ممكنة.²

❖ تحقيق مكاسب مالية

قد يكون الهدف من ارتكاب جرائم الكمبيوتر الحصول على ربح مالي عن طريق المساومة على البرامج أو المعلومات المتحصلة عن طريق الاختلاس من جهاز الكمبيوتر أو عن طريق استعمال بطاقة سحب آلي مزورة أو منتهية الصلاحية

وفي الواقع فإن المحرك لاقتراف فعل الغش المعلوماتي هو النجاة من غرق الديون المستحقة أو الفقر أو من إدمان المخدرات ويمكنك ذكر واقعة استيلاء مبرمج يعمل لدى إحدى الشركات الألمانية على اثنين و عشرين شريطا تحتريزي غلى معلومات هامة بخصوص عملاء و إنتاج الشركة وقد هدد السارق ببيعها للشركات المنافسة ما لم تدفع له فدية تقدر بالدولارات وقد قامت الشركة بدفع المبلغ مقابل

¹ محمد علي العريان، م س، ص 63 وما بعدها

² -محمد أمين الرومي: مرجع سابق، ص 23 وما بعدها

عدم خسارتها للشرائط الممغنطة المسروقة لان إفشاء محتواها سيكلف الشركة
خسارة لا تقدر وتفوق المبلغ المطلوب بكثير.

❖ الدوافع الشخصية

غالبا ما يرتكب المبرمج جرائم الكمبيوتر نتيجة إحساسه بالقوة و بقدرته على
اقتحام النظام فيندفع تحت تأثير الرغبة القوية في تحقيق الذات ومن اجل تأكيد
قدرته الفنية الفنية على ارتكاب الجرائم المعلوماتية

وقد يكون الهدف من ارتكابها الحقد و الكراهية و بالتالي اللجوء إلى أسلوب
الانتقام من الشركة المشغلة عن طريق التلاعب في برامج الحاسوب الخاص بها
(فقد قام شاب يعمل لدى إحدى الشركات ببرمجة الحاسب الآلي على إن تختفي كل
المعلومات الخاصة بديون الشركة بعد مضي ستة أشهر من تاريخ تركه للعمل
وفعلا حدث ذلك بعد مرور تلك المدة اختفت كل البيانات الخاصة بديون الشركة
نهائيا).¹

2 : المجني عليه في الجرائم المعلوماتية

إن تقدير بعض الخبراء الصندوق الدولي للبنوك F.B.I. فانه من المستحيل
أن تحدد على نحو دقيق نطاق الجرائم المعلوماتية
ولا يعلم ضحايا هذه الجرائم شيئا عنها إلا عندما تكون أنظمتهم المعلوماتية
هدفا لفعل الغش و حتى عندما يعلمون فهم يفضلون عدم إفشاء الفعل فلا يوجد من
يريد الاعتراف بانتهاك نظامه المعلوماتي .

وعلى الرغم من ذلك فقد استطاع اتحاد البنوك في جنيف أن يقدر خسائر
أوروبا الغربية من ظاهرة الغش المعلوماتي حيث بلغت حوالي 45 مليون فرنك
فرنسي 1988 كما قدرت خسائر الاقتصاد الأمريكي الناشئة عن هذه الظاهرة
بحوالي 400 مليون دولار وفقا لما أشار إليه ² Parker

¹ محمد سامي الشوام م س , ص 47 و ما بعدها

1-انضر ايضا محمد علي العريان م س , ص 67

أ: القطاعات المستهدفة

إن القطاعات المستهدفة في هذا المجال والتي تستخدم الحاسب الآلي تكون جميع أنشطتها عرضة لخطر ظاهرة الغش المعلوماتي لأي قطاع من الأنشطة ليس بمنأى عن ذلك. و يبدو بجلاء إن انتهاك هذه الأنظمة المعلوماتية هو الأكثر توفيراً بالنسبة للمحتالين.

ويلاحظ من ذلك إن الاتجاه الأساسي للغش المعلوماتي يستهدف البنوك ووفقاً لتحقيق باشرته مجلة *ressour ces informatiques* تبين أن:

- 19% من أفعال الغش المعلوماتي تستهدف البنوك.
- 16% للإدارة
- 10% للإنتاج الصناعي
- 10% للمعلومات

ثم يلي ذلك شركة التأمين و الشركات الخاصة¹.

ب: المعلومات المستهدفة

إن الغش المعلوماتي في الحقيقة يستهدف المنشآت المالية ثم المعلومات كأحد المصالح المستهدفة بعد النقود.

ولقد نمت إلى جوار "السوق الشرعي للمعلومات" "السوق السوداء للمعلومات" وفيه تتم مقايضة و بيع المعلومات المسروقة أو المقتبسة من أصحابها الحقيقيين و الشرعيين و يمكن يصوره بالنسبة للمعلومات التالية:

- **المعلومات المالية :** تمس هذه الظاهرة الإجرامية المركز الحسابي و الإداري و تنقلات الأموال و الاستثمارات سواء في المنشآت العامة أو الخاصة.
- **المعلومات التجارية و الصناعية:** حيث تستهدف هذه الظاهرة الدراسات الخاصة بالأسواق و مشاريع التصنيع و الإنتاج والتجارة و التوزيع و الأسعار و مراكز البيع و القطاع الصناعي للإنتاج.

¹ محمد سامس الثنوا : م س ، ص 57

- **المعلومات الشخصية:** وهي تلك المخزنة في ذاكرة الحاسبات الآلية للبنوك و شركة التأمين و لدى المحامين و أقسام الشرطة.... , وقد تهدد هذه الاعتداءات مباشرة قدسية و سرية الحياة الخاصة أو الحرية السياسية.
- **المعلومات العسكرية:** التي تتمثل في أسرار الدولة و المشروعات النووية و التصنيع الحديث للأسلحة ...

ويبدو إن هذه المعلومات الأخيرة هي الأكثر رواجاً في سوق المعلومات السوداء. وعموماً فإن الإشكال المثار في هذا الشأن هي ردود الفعل السلبي لضحايا الجرام المعلوماتية وسكوت هؤلاء فهم يميلون إلى الحفاظ على سمعتهم و مكانتهم المرموقة تضاف إليها مشكلة صعوبة الإثبات المادي لفعل الغش وأمام إصرارهم على إخفاء الجرائم التي وقعوا ضحيتها وكذا صعوبة الإثبات يجعل المجرمين ينعمون في تماديهم في ارتكاب أفعالهم المشينة بأريحية مطلقة.¹

رابعاً : خصائص الجريمة المعلوماتية وأساليب ارتكابها

تعتبر الجرائم المرتكبة عبر شبكة الانترنت جرائم ذات خصائص متفردة لا تتوفر في الجرائم التقليدية في أسلوبها و طريقة ارتكابها و أهمها :

1 : خصائص الجريمة المعلوماتية

إن الجرائم المعلوماتية تمتاز بمجموعة من الخصائص أهمها إن الحاسب الآلي يستعمل كوسيلة لتنفيذ الجريمة كما إنها تمتاز بكونها عابرة للحدود و إن مرتكبها يمتاز بنوع من الاحتراف و الذكاء وغيرها من المميزات التي سيتم تفصيلها .

أ : الحاسب الآلي أداة لارتكاب الجريمة

حيث يعتبر الحاسب الآلي في هذه الخاصية هو دائماً أداة لارتكاب الجريمة المعلوماتية وهي خاصية جد متفردة لكونه الأداة الوحيدة التي تمكن الشخص من الدخول على شبكة الانترنت و قيامه بتنفيذ جريمته أياً كان نوعها و عليه فالحاسب الآلي هو الأداة الوحيدة لارتكاب أي جريمة إلكترونية.

¹ محمد سامي الشوا م س ص 59

ب :خبرة المجرم المعلوماتي في استخدام الحاسب الآلي

لاستخدام الحاسب الآلي في ارتكاب الجريمة على شبكة الانترنت لابد أن يكون مستخدم هذا الحاسب على دراية فائقة ودو خبرة كبيرة في مجال استخدامه لذلك يستشف أن معظم من يرتكب تلك الجرائم هم من الخبراء في مجال الحاسب الآلي حتى أن الشرطة أول ما تبحث عنه عند ارتكاب الجرائم هم خبراء الكمبيوتر.

ج : الجريمة المعلوماتية لا حدود لها

لقد ألغت شبكة الانترنت كل الحدود الجغرافية فيما بين الدول إذ يمكن التحدث بين الأشخاص في بلدان مختلفة أو قارات وفي زمن واحد عبر شبكة الانترنت و بالتالي فان تخطيها لكل الحدود الدولية تجعل من سهولة ارتكاب الجرائم المعلوماتية دون أدنا صعوبة.¹

د: الجريمة المعلوماتية يصعب اكتشافها

تتميز الجريمة المعلوماتية بصعوبة اكتشافها، ويعود السبب في ذلك إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية، بحكم أن الجاني يعمل من جهته على تدمير دليل الإدانة مباشرة بعد اقترافه الجريمة. فالجرائم المعلوماتية في أكثر صورها خفية يلحظها المجني عليه، أو لا يدري حتى بوقوعها، وذلك بحكم الفارق في المعرفة والخبرة الإلكترونية بين الجاني عليه والجاني، ذلك أن هذا الأخير غالبا ما يعمل على حجب السلوك المكون لجريمته وإخفائه عن طريق التلاعب غير المرئي في النبضات والذبذبات التي تسجل البيانات عن طريقها.

2 : الأساليب المستخدمة لارتكاب الجريمة المعلوماتية

كثيرا ما يتواءم المجرمون و التقدم التقني شأنهم في هذا المجال شان المستخدمين الشرعيين للأجهزة المعلوماتية ويظهر مرتكبو أفعال الغش كل أنواع الحيل و المكائد لخداع الحاسب الآلي ومن تم إسقاط حواجز الأمن سواء كانت مادية أو الكترونية وسيتم التعرف على كيفية ارتكاب هذه الجرائم من خلال أداء الحاسب الآلي لوظائفه الطبيعية وأيضا من خلال التعدي عليها و تعطيل.

أ: أساليب ارتكاب الجرائم أثناء أداء الحاسب الآلي لوظائفه الطبيعية

¹ - منير محمد الجنيهي و ممدوح محمد الجنيهي: جرائم الانترنت و الحاسب الآلي ووسائل مكافحتها، د. ط. دار الفكر الجامعي، الإسكندرية، 2004 ، ص 13 وما يليها.

إن التقنيات الإجرامية المرتكبة في هذا الإطار لا تستلزم تدخلا للمجرم لإتلاف الوظائف الطبيعية للحاسب الآلي ولا أي تعديل على بيانات المعالجة بل ستلزم ولوجا ماديا من جانب البعض في مركز المعالجة و أداة الكترونية مصطنعة تسمح بالنقاط المعلومات والتصنت عليها عن بعد .

✚ الالتقاط الغير المشروع للمعلومات المعالجة بواسطة الحاسب الآلي : يكفي التواجد في صالات الحاسبات الآلية ويتمثل الفعل غير المشروع في الاطلاع غير المصرح به بالمعلومات المخزنة في ذاكرات الحاسبات الآلية وهذا الفعل له عدة صور :

✚ سرقة القائمة: يكفي فيها السارق بسحب القائمة من الطباعة

✚ الاطلاع على المعلومات : أي التي تظهر على شاشة كاتودية و المتصلة

بالحاسب الآلي

✚ التصنت المجرد على المعلومات: وذلك عن طرق وسيط مكبر الصوت و الذي يلتقط المعلومات و البيانات المعالجة ويعد هذا النوع من الالتقاط من اكر الأفعال غير المشروعة ارتكابا وأسهلها من حيث التنفيذ¹

ب: أساليب تستلزم التعدي على الوظائف الطبيعية للحاسب الآلي

ابرز ارتكاب مجموعة أخرى من الجرائم المعلوماتية السمة العالية لتقنية أفعال تعدي المحتالين والتي تتجسم في صورة المعالجة غير المشروعة سواء للمعلومات او البرامج ذاتها.

✚ التعدي على المعلومات : يعد التلاعب في المعلومات - وفقا لأراء الخبراء- من أكثر أفعال الغش ارتكابا في أوروبا. و يتم هذا التلاعب إما عن طريق إدخال معلومات مصطنعة أو إتلاف المعلومات الموجودة بالآلة.

● إدخال معلومات مصطنعة: كضم مستخدمين غير موجودين بالفعل أو اختلاس النقود كالعامل على تحويل نقود وهمية عن طريق استخدام الحاسب الآلي الخاص بالبنك

¹ محمد سامي الشوا م س , ص 63 وما بعدها
انظر أيضا محمد علي العريان , م س , ص 69 وما بعدها

• إتلاف المعلومات: حيث يمكن للمسؤولين عن حفظ المعلومات وبمنتهى البساطة أن يغيروا ويتلفوا المعلومات المكلفين بحفظها داخل الحاسب الآلي وأيضا يمكن التلاعب في الرائط الممغنطة أو محو المعلومات أو التلاعب بالمعلومات عن بعد

✚ التعدي على برنامج الحاسب الآلي ويستلزم هذا النمط من الجرائم معرفة فنية كبيرة في مجال البرمجة وتنفيذه كالتعديل في برنامج تطبيقي و تعديل برامج التشغيل أو اصطناع برامج من اجل التخطيط للجريمة و مراقبتها و تنفيذها أي اصطناع برنامج كامل و مخصص فقط لارتكاب فعل الغش المعلوماتي .

✚ سرقة وقت الآلة وهي من الجرائم الشائعة في العديد من مراكز الأبحاث في فرنسا و يعد هذا الوقت للحاسب الآلي من الأمور المكلفة جدا وقد يتسبب محاسب غير مسؤول في إحداث خسائر لمنشأة نتيجة لاقترافه هذه الجريمة.¹

الفقرة الثانية: الطبيعة القانونية للجريمة المعلوماتية

يثار التساؤل بخصوص الوضع القانوني للمعلومة هل للمعلومة قيمة في ذاتها أم على العكس لها قيمة تتمثل في أنها مجموعة مستحدثة من القبو ويرجع هذا التساؤل إلى أن إذا كانت المعلومات لها قيمة وتعتبر من تمت من قبيل القيم القابلة للاستثناء وبالتالي يمكن الاعتداء عليها بأي طريقة.

وقد انقسم الفقه إلى اتجاهين اتجه يرى أن المعلومة لها طبيعة من نوع خاص و الثاني يرى إن المعلومة ما هي إلا مجموعة مستحدثة من القيم.

• المعلومات طبيعة من نوع خاص

يرى هذا الاتجاه التقليدي أن المعلومة لها طبيعة من نوع خاص و ذلك انطلاقا من حقيقة مسلم بها هي إن وصف القيمة يضيف على الأشياء المادية وحدها أي أن المعلومة

¹ محمد سامي الشوام س , ص 71 وما بعدها.

يمكن الحديث هنا على واقعة اثنين من مستخدمي شركة غاز بريطانية قاما عن طريق إعلانات صغيرة ببيع رسومات صممت بواسطة الناظم المعلوماتي الخاص بهذه الشركة و هذا يساوي من الناحية العلمية " العمل في الظلام " على الحاسب الآلي مملوك لرب العمل و لكنه بدون علمه وهناك أيضا المثال الخاص ب مستخدمين الدين قاما باستخدام الحاسب الآلي الخاص بمركز تصنيع و حماية الصواريخ النووية من أجل تخزين ألعاب البانصيب و الخطابات الشخصية ، أنظر نفس مرجع ، ص: 72

لها طبيعة معنوية فلا يمكن اعتبارها من قبيل القيم القابلة للحيازة إلا في الحقوق و الملكية الفكرية .

• المعلومات مجموعة مستحدثة من القيم

ويرى الاتجاه الحديث إن المعلومات ماهية إلا مجموعة مستحدثة من القيم ويرجع الفضل في ذلك إلى الأستاذين فيفان و كاتالا Vivan et catala ويذهب الأستاذ كاتالا إلى قابلية المعلومة للاستحواذ كقيمة و استقلالاً عن دعايتها المادية وإنها تقوم وفقاً لسعر السوق متى كانت غير محظورة تجارياً وأنها تنتج بصرف النظر عن دعائها المادية عن عمل من قدمها وإنها ترتبط بمؤلفها عن طريق علاقة قانونية تتمثل في علاقة المالك بالشئ الذي يملكه وهي تخص مؤلفها بسبب علاقة التبني التي تجمع بينهما.

أي أن هذا الرأي يؤسس حجيتين لإعطاء وصف القيمة على المعلومة الأولى قيمة المعلومة الاقتصادية و الثانية وجود علاقة تبني تجمع بين مؤلفها.

ويؤكد الأستاذ الدكتور محمد سامي الشوا إن المعلومة بالنظر إلى حقيقتها الذاتية و استقلالها تعد قيمة في ذاتها ولها بالتأكيد مظهر معنوي و لكنها تملك قيمة اقتصادية مؤكدة .

ويبدو أن المعلومات مال قابل للملك أو الاستغلال يستحق الحماية القانونية.¹

الفقرة الثالثة: أنواع الجريمة المعلوماتية

للتمكن من رصد الجرائم التي ترتكب بواسطة الوسائل المعلوماتية يجب وضعها في إطارها العام و الذي ينقسم محورين رئيسيين (الأول) يضم الأفعال الماسة بالذمة المالية، و(الثاني) يضم الأفعال الماسة بالأشخاص.

أولاً: الجرائم المعلوماتية الماسة بالذمة المالية

صدق من قال بأن الثورة المعلوماتية تعد بمثابة سلاح ذو حدين صحيح أنها تعد تطوراً في إنجاز العمليات بصورة دقيقة وسريعة، فالمقابل رافقه تطور آخر في ارتكاب

¹ محمد علي العريان م س ، ص 49 وما بعدها
انظر أيضاً محمد سامس الشوا م س ، ص 178 وما بعدها

عدد من الجرائم المتصلة بثورة التقنية العالية من بينها الجرائم المرتبطة بالذمة المالية والتي نجد من بينها:

(1) غش الحاسب الآلي (التحايل المعلوماتي)

بعد ازدياد اعتماد المصاريف على أنظمة التحويل الإلكتروني للأموال زادت فرص ارتكاب غش الحاسب الآلي وبشكل كبير، معتمدة في ذلك أساليب مختلفة، (كالتلاعب في البيانات المدخلة) إما أثناء إدخال البيانات أو بتعديلها بعدم الإدخال أو إضافة بيانات وهمية إلى الحاسب الآلي¹، ومن أساليب الغش الحاسب الآلي أيضا (التلاعب في البرامج)، وتتم هذه الجريمة بعد قيام مرتكبها - عادة المبرمج - بتعديل البرنامج الذي تعمل به المؤسسة أو اصطناع برنامج وهمي، ويتم هنا استغلال هذا التعديل في البرنامج الوهمي الجديد من قبل المبرمجين القادرين على التحكم بنظام تشغيل الحاسب²، ومن الأساليب أيضا (التلاعب في المعطيات) وتتم هذه الجريمة بعد قيام مرتكبها وعادة ما يكون شخص خارج المنشأة، ليس مدخلا لبيانات ولا مبرمجا، بعد فك رموز التشغيل الخاصة، يقوم بتحويل الأموال لحسابه أو لحساب غيره³.

(2) إساءة استعمال البطاقات الائتمانية

يمكن للغير أن يرتكب جرائم إساءة استخدام البطاقات الائتمانية من خلال حالتين⁴:
حالة السرقة للبطاقة أو فقدها، وتعتبر سرقة البطاقات الائتمانية أو فقدها من أهم المشكلات القانونية التي تثير التعامل ببطاقات الائتمان حيث يقوم السارق باستخدامها للحصول على السلع والخدمات من الغير أو يقوم بسحب مبالغ بموجبها من أجهزة التوزيع الآلي.

¹ - محمود أحمد عبانة: جرائم الحاسوب وأبعادها الدولية، د.ط، دار الثقافة للنشر والتوزيع، عمان، سنة 2005، ص 56

² - عمر محمد بن يونس: غسيل الأموال عبر الانترنت، د.ط، دار النهضة العربية، القاهرة، 2004، ص 55

³ - نفس المرجع، ص 57.

⁴ - محمود أحمد عبانة: مرجع سابق، ص 57-58.

⁵ - أحمد خليفة الملط: مرجع سابق، ص 232.

حالة السحب باستخدام بطاقة مزورة حيث ظهرت فكرة تزييف البطاقات الممغنطة كوسيلة يتحايل بها الجاني على أجهزة التفتيش الآلي للمواصلات حتى يمكن المرور منها بدون دفع أجره كما يستخدمها الجاني في أجهزة التوزيع الآلي للنقود.

(3) سرقة المال المعلوماتي المعنوي

إن الصورة الغالبة لسرقة المال المعلوماتي، تأخذ صورة اختلاس البيانات والمعلومات، والإفادة منها باستخدام السارق للمعلومات الشخصية (مثل الاسم، العنوان، الأرقام السرية) الخاصة بالمجني عليهم، والاستخدام غير الشرعي لشخصية المجني عليه، ليبدأ بها عمليات السرقة الخفية عبر الانترنت، بحيث تؤدي بالغير إلى تقديم الأموال الإلكترونية إلى الجاني، عن طريق التحويل البنكي¹.

(4) التحويل الإلكتروني غير المشروع للأموال

لقد اكتسب التعامل بالأموال في عصر المعلوماتية صفة البيانات الإلكترونية المخزنة في ذاكرة الحاسب الآلي، وأدت الثورة الرقمية إلى إمكانية إجراء تحويلات ومبادلات لهذه الأموال من أي مكان في العالم. وتكمن خطورة الأمر في إمكانية تلاعب الجاني في هذه البيانات المخزنة في ذاكرة الحاسب الآلي أو في برامجه، وإجراء تحويلات في كل أو بعض أرصدة الغير أو فوائدها وإدخاله إلى حسابه².

ثانياً: الجرائم المعلوماتية الماسة بالأشخاص

لا تنحصر الجريمة المعلوماتية فقط على تلك التي تطال الذمة المالية، بل ترتكب حتى على الأشخاص وهي متعددة، ولكن سيتم الاختصار فقط على بعضها:

(1) -نقل أو تسجيل المحادثات الخاصة بالأشخاص

إن نقل أو تسجيل المحادثات الخاصة بالأشخاص تعد من الجرائم التي تمس الحياة الخاصة، فبعد التطور في وسائل الاتصال وارتباطها بالحاسب الآلي بات من المتيسر

¹- عبد الكريم عباد: الجريمة المعلوماتية، المجلة الوطنية للعلوم القانونية والقضائية، العدد الأول، دون سنة، ص58.

²- نفس مرجع، ص62

اختراق هذه الوسائط والتصنت عليها وتسجيلها واشترطت بعض التشريعات كالجناحي الفرنسي والمصري أن تتم هذه المحادثات في مكان خاص حتى تعد جريمة¹.

(2)-إفشاء البيانات الشخصية السرية

يعد إفشاء البيانات الشخصية السرية سواء تم عن طريق الخطأ أو بهدف التشهير والإساءة أو التهديد بنشرها من صور الاعتداءات الماسة بالحياة الخاصة لأن قيام شخص بإيداع بيانات لدى مؤسسة ما تحوز على ثقته، وقيام تلك المؤسسة بإفشائها خطأ أو بقصد التشهير به والإساءة إلى سمعته تعد من الجرائم التي تمس حياته الخاص، ولا يشترط القانون أن تكون هذه البيانات حقيقية أو مزورة، بل يكفي أن تتعلق بشرفه واعتباره².

(3)-جريمة الاستغلال الجنسي للأطفال عبر الانترنت

لا شك أن عالمية نطاق الانترنت أدى إلى تحولها إلى ساحة مفتوحة لممارسة جميع أنواع الجرائم الممكنة والمحتملة، ومن ضمنها الأعمال المخلة بالآداب العامة والأخلاق، والتي تتباين من بلد لآخر، بحيث يمكن لكل مستخدم أو مشترك في شبكة الإنترنت الحصول على بيانات محظورة في قوانين مصدر هذه البيانات.

لعرض صور إباحية مخلة digital ويستغل المجرمون شبكة الانترنت باستخدام التقنية الرقمية بالآداب والأخلاق العامة، الأمر الذي استدعى تظافر جهود المجتمع الدولي للحد هذه الجرائم، والتي تزداد بازدياد مستخدمي الشبكة. وقد تكلل مساعي هذا الأخير بعقد المؤتمر الدولي لمكافحة الاستغلال الجنسي للأطفال سنة 1999 بفيينا، وكان يهدف إلى توعية المستخدمين لمواجهة الاستغلال الجنسي للأطفال عبر الأنترنت، حيث أكد المؤتمر على مبدأ أساسي، يتمثل في تدعيم التعاون الدولي لمكافحة الاستغلال الجنسي للأطفال عبر الأنترنت، وذلك من خلال تكثيف الجهود الدولية في الأخذ بالمبادئ التي تؤكد وتؤطر هذا المبدأ³.

¹- محمود أحمد عابنة: مرجع سابق، ص 72.

²- نفس مرجع، ص 73.

³- عبد الكريم عباد: مرجع سابق، ص 51.

4) الجرائم الماسة بأسرار الدولة

الدولة كشخص اعتباري هي الأخرى تعد معرضة للجريمة المعلوماتية من طريق ارتكاب جريمة إفشاء أسرارها، وبناء على ذلك حمت التشريعات الوطنية الإرادة وجرمت إفشاء هذه الأسرار سواء كانت اقتصادية أو مالية أو عسكرية أو سياسية، ويعتبر استخدام النظام المعلوماتي في الجرائم الواقعة على أسرار الدولة من أخطر أنواع الجرائم المعلوماتية في الوقت الحاضر¹.

¹ - أحمد خليفة الملط: مرجع سابق، ص 234.

المطلب الثاني : الجهود المبذولة لمكافحة الجريمة المعلوماتية

إن الجريمة المعلوماتية لا يماري أحد بخصوص خطورتها في جل المجتمعات، الأمر الذي جعل المجتمع الدولي من جهة والوطني من جهة ثانية بأن يضعوا خطط وسياسات تهدف إلى مكافحة هذا النوع من الجرائم، ومن خلال هذا سيتم النظر في (الفقرة الأولى) إلى الجهود الدولية، ثم في (الفقرة الثانية) إلى الجهود الوطنية .

الفقرة الأولى : الجهود الدولية لمكافحة الجريمة المعلوماتية

أصبح المجتمع الدولي أمام ضرورة ملحة متمثلة في مواجهة التطور التي صارت تعرفه الجريمة العابرة للحدود ، خاصة وأنها مع مرور الوقت أصبحت ترتكب عن طريق الوسائل الالكترونية، والمجتمع الدولي لم يقف موقف المتفرج في هذا الصدد بل حاول بما أمكن مواجهة هذا النوع من الجرائم سواء على المستوى مجال (إبرام الاتفاقيات الدولية) من جهة أو على مستوى (الأجهزة والمؤسسات الدولية) من جهة أخرى.

أولاً: الاتفاقيات الدولية الخاصة بمواجهة الجرائم الالكترونية

بعد انتشار الجريمة الالكترونية بشكل كبير ولا سيما حينما أصبحت تخترق حدود الدول والقارات، أصبح من اللازم على الدول بأن تنخرط في مجال إبرام اتفاقيات دولية تهدف بالأساس إلى مواجهة الجريمة الالكترونية العابرة للحدود، وفي هذا الصدد تتعدد الاتفاقيات الدولية في هذا الخصوص، غير أنه سيتم الاقتصار فقط على بعض أهمها:

1-اتفاقية بودابست لجرائم الالكترونية

مع التطور الهائل في تكنولوجيا المعلومات والاتصالات ظهرت سلبيات خطيرة تهدد اقتصاد البلاد وأمنها، فيما يسمى بالجرائم الالكترونية، سواء أكانت الجرائم التي ترتبط بالحاسب الآلي، أم من خلال استخدام الإمكانيات التي تقدمها شبكة الانترنت، وظهر نوع من المجرمين يمكن تسميته "المجرم المعلوماتي"¹، وجاءت اتفاقية بودابست لتهدف إلى توحيد السياسة الواجب إتباعها في مكافحة هذا النوع من الجرائم في الفضاء الافتراضي

¹ - محمد الشناوي: مرجع سابق، ص 44.

وإلى التنسيق بين التشريعات الوطنية لتسهيل مكافحة الإجرام المعلوماتي وتطبيق إجراءات تحقيق وملاحقة تتلاءم مع الفضاء الافتراضي، ووضع نظام تعاون دولي يتميز بالسرعة والفعالية في التنفيذ¹، وتعد النصوص الإجرائية القواعد التي فازت بنصيب الأسد وحيزا هاما ضمن الاتفاقية المجرية "بودابست" التي تم صياغتها من قبل مجلس أوروبا بتاريخ 23 نونبر 2001 وذلك من خلال تخصيص حوالي 22 مادة من أصل 48 مادة مكونة لاتفاقية المذكورة للقواعد الإجرائية لأغراض التحريات والإجراءات الجنائية²، كما أكدت هذه الاتفاقية نصت على عدة آليات تهدف إلى خلق جوا من التعاون الدولي لاسيما في الشق الإجرائي على مستوى الحماية السريعة لبيانات مخزنة في نظم معلوماتية³، نظرا لاعتبار المجال الافتراضي مكانا لهذه النظم مع اعتبار هذا الأخير حسب ما جاءت به الأعمال التحضيرية لاتفاقية بودابست مجالا شاسعا وصعب التحديد⁴.

وبالتالي فإن معاهدة بودابست تهدف إلى توحيد الجهود في محاربة الجرائم المعلوماتية التي انتقلت من مرحلة التسلل البري إلى الاحتيال والاختلاس وجرائم تهدد الحياة، وهي قضايا يعتبرها الأوروبيون بأنها تعرض حياة الكثيرين للخطر. ووقع عليها وزراء الداخلية ومسؤولو تطبيق القانون في الدول الأوروبية إضافة إلى الولايات المتحدة الأمريكية واليابان وكندا وجنوب إفريقيا، وقد بلغ عهد الدول التي وقعت على هذه الاتفاقية أكثر من ثلاثين دولة⁵.

2- اتفاقية الكايط المنعقدة بمراكش بتاريخ 15 فبراير 1994

عالجت هذه الاتفاقية وخاصة في المادة 61، حماية حقوق الملكية الفكرية المتعلقة بالتجارة، وفرضت على الدول الأعضاء وضع عقوبات للجرائم الرامية إلى تزوير العلامات التجارية والقرصنة التي غالبا ما تتم عن طريق شبكة الأنترنت.

¹ - فريد منعم جبور: حماية المستهلك عبر الأنترنت ومكافحة الجرائم الالكترونية، دراسة مقارنة، الطبعة الأولى، مطبعة دار النهضة العربية، القاهرة، سنة 2003، ص 25.

² - أنظر مقتضيات اتفاقية بودابست الصادرة من قبل المجلس الأوروبي بتاريخ 23 نونبر 2002.

³ - جميلة عباوي: الحماية الجنائية للمعاملات الالكترونية، المجلة المغربية للقانون الجنائي والعلوم الجنائية، العدد الثالث، سنة 2016، ص 83.

⁴ - صليحة الحاجي: مرجع سابق، ص 5.

⁵ - أحمد خليفة الملط: مرجع سابق، ص 676.

وقد شرعت دول الاتحاد الأوروبي في تطبيق بنود هذه الاتفاقية ابتداء من 29-02-2004 تاريخ صدور الأمر المتعلق بالإجراءات اللازمة لغرض احترام حقوق الملكية الفكرية ومواجهة مرتكبي جرائم التزوير والقرصنة¹.

3- اتفاقية الأمم المتحدة "باليرمو" لمكافحة الجريمة المنظمة عبر الوطنية

صدرت هذه الاتفاقية في ديسمبر سنة 2000، نصت في موادها على ضرورة تعزيز أوجه التعاون الدولي لمختلف الأنماط الأخيرة للجريمة المنظمة العابرة للحدود ومن بينها الجرائم الالكترونية ومكافحتها على أحسن وجه ولاسيما جرائم غسيل الموال الالكترونية والإرهاب الالكتروني²، لأن الجرائم الالكترونية إما أن تتمثل في تلاعب في نظم المعالجة الآلية المعطيات أو تمثل في استغلال الأجهزة الالكترونية من أجل اقتراف جرائم أخرى لا تقل أهمية هي الأخرى الاتجار في المخدرات وغسيل الموال والإرهاب وقس على ذلك.

وكذلك من بين ما جاءت به اتفاقية باليرمو هو حث الدول على تجريم مختلف أوجه الجريمة المنظمة العابرة للحدود، ونصت على مجموعة من الحكام تطبق على كل أصناف الجريمة المنظمة بما فيها الجرائم الالكترونية والتي من شأنها تفعيل وتعزيز وسائل المكافحة ومن ذلك مؤسسة تسليم المجرمين والمساعدة القضائية المتبادلة والتعاون الدولي لأغراض المصادرة والأحكام المتعلقة بالأشخاص المعنوية وقس على ذلك³، فالركن الدولي الذي قد تكتسبه جرائم الحاسب الآلي ذات الركن المكون للجرائم الدولية، بل ركن آخر يتصل بالجرائم العلمية التي تعبر في حقيقتها من الجرائم الداخلية التي يعاقب عليها قانون العقوبات الوطني⁴.

1- حليلة بن حفو: محاربة الجرائم الالكترونية على الصعيد الدولي (الواقع والأفاق)، مجلة العلوم الجنائية، العدد الأول، سنة

2014، ص 203

2- شريف سيد كامل: الجريمة المنظمة في القانون المقارن، الطبعة الأولى، دار النهضة العربية، القاهرة، سنة 2001،

ص 139.

3- نفس المرجع، ص 128.

4- محمود أحمد عيابة: مرجع سابق، ص 118.

4- قرار الجمعية العامة للأمم المتحدة لمكافحة استغلال تكنولوجيا المعلومات لأهداف إجرامية¹.

صدر هذا القرار بتاريخ 2001/12/19 وقد حث الدول الأعضاء على ضرورة تنسيق أجهزة الردع، وكذلك على تبادل المعلومات حول العراقيل التي تواجههم أثناء مكافحة الجرائم الالكترونية. أيضا أبرز الدور الهام لأنظمة المساعدة القانونية المتبادلة، والمتجلي في إجراء التحقيقات بكيفية سريعة في قضايا استغلال تكنولوجيا المعلومات لتحقيق أهداف غير مشروعة.

والقمة العالمية لمجتمع المعلومات المنعقدة بتونس تحت رعاية الأمم المتحدة:

خرجت هذه القمة بمجموعة من التوصيات يمكن إجمالها فيما يلي²:

- العمل على متابعة مرتكبي الجرائم الالكترونية.
- تعزيز التعاون الدولي في مجال مكافحة الجرائم الالكترونية من خلال توفير الآليات والوسائل الفعالة وطنيا ودوليا.
- الدعوة إلى وضع نصوص قانونية تسمح بإجراء تحقيقات في الجرائم المعلوماتية وملاحقة مرتكبي هذه الجرائم.
- ضرورة احترام الحياة الخاصة وحرية التعبير المنصوص عليها في الإعلان العالمي لحقوق الإنسان وإعلان جنيف للمبادئ، وذلك عند مكافحة الجرائم المعلوماتية.

5- مؤتمر الأمم المتحدة الثامن المنعقد بهافانا سنة 1990

خرج هذا المؤتمر بمجموعة من التوصيات، أكدت على ضرورة تكثيف جهود الدول الأعضاء لمكافحة الجرائم المعلوماتية، وذلك عن طريق الانضمام إلى الاتفاقيات الدولية

¹ قرار عدد 56/121 منشور في مقال: حليلة بن حقو، مرجع سابق، ص 204

² نفس مرجع، ص 204 و 205

والمعاهدات المتعلقة بتسليم المجرمين وتبادل المساعدة في المسائل الجنائية وخاصة على مستوى مكافحة الجرائم المعلوماتية¹.

6- اتفاقيتي مجلسي وزارة العدل والداخلية العرب المنعقدة بالقاهرة بتاريخ

21 دجنبر 2010

تم خلال اجتماع وزاري مشترك لمجلسي وزراء العدل والداخلية العرب، إبرام اتفاقيتين الأولى تهتم مكافحة الفساد والثانية تخص مكافحة جرائم تقنية المعلومات.

فاتفاقية مكافحة الفساد، تهدف أساسا تعزيز التدابير الرامية إلى الوقاية من الفساد وكشف تجلياته وسائر الجرائم المتصلة به وملاحقة مرتكبيها، ولذلك على اعتبار أن الفساد ظاهرة إجرامية متعددة الأشكال، عابرة للحدود الوطنية، وذات آثار سلبية على القيم الأخلاقية، كذلك على المستوى الاقتصادي والاجتماعي والسياسي.

أما اتفاقية مكافحة جرائم تقنية المعلومات، فإنها تهدف إلى تعزيز التعاون بين الدول العربية في مجال مكافحة هذه الجرائم².

ثانيا: المؤسسات الدولية لمحاربة الجريمة المعلوماتية

لا يمكن الاتفاقيات الدولية أن تبرز فعاليتها في مكافحة الجريمة المنظمة العابرة للحدود بوجه عام والجريمة الالكترونية على وجه الخصوص إلا في ظل وجود آليات مؤسساتية وأجهزة فعالة تساعد على تحقيق هدف التصدي لها، ومن هذه المؤسسات:

1- منظمة الأمم المتحدة

تتجلى جهود الأمم المتحدة بمجال منع الجريمة ومعاملة المجرمين المتعلقة بالجرائم التقنية أو جرائم الحاسب الآلي في مؤتمراتها الخاصة بهذا المجال ولاسيما المؤتمر السابع لمنع الجريمة ومعاملة المجرمين الذي تم انعقاده في مدينة ميلانو بإيطاليا في عام 1980م، والذي انبثقت عنه مجموعة من القواعد التوجيهية والتي اكتملت صياغتها في الاجتماعات

¹ نفس المرجع: ص 205

² حليلة بن حفو: مرجع سابق، ص 205

الإقليمية التحضيرية للمؤتمر الثامن¹. الذي أجاز هذه المبادئ والذي عقد في هافانا بكوبا في العام 1990، ومن بين التوصيات التي تم الخروج بها من هذا المؤتمر².

- تحسين أمن الحاسب الآلي والتدابير المنعوية.
- تلقين آداب الحساب الآلي كجزء من مفردات مقررات الاتصالات والمعلومات.
- اعتماد سياسات تعالج المشكلات المتعلقة بالمدني عليهم في تلك الجرائم.
- زيادة التعاون الدولي من أجل مكافحة هذه الجرائم.
- اعتماد إجراءات تدريب كافية للموظفين والوكالات المسؤولة عن منع الجريمة الاقتصادية والجرائم المتعلقة بالحاسب الآلي والتحي والإدعاء فيها.

2- دور المنظمة العالمية للملكية الفكرية في مجال الحماية من جرائم الحاسب الآلي

وحماية البرامج

وقعت في العام 1967 في ستوكهولم في السويد اتفاقية المنظمة العالمية للملكية الفكرية³. وأصبحت هذه المنظمة إحدى الوكالات المتخصصة التابعة للأمم المتحدة اعتباراً من السابع من ديسمبر في عام 1974م، ومن أهم الوظائف لهذه المنظمة:

✓ العمل على دعم اتخاذ الإجراءات التي تهدف إلى تيسير الحماية الفعالة للملكية الفكرية في جميع أنحاء العالم وإلى تنسيق التشريعات الوطنية في هذا المجال.

✓ تشجيع إبرام الاتفاقيات الدولية التي تهدف إلى تدعيم حماية الملكية الفكرية لاسيما من الجرائم الالكترونية

✓ تعرض تعاونها على الدول التي تطلب المساعدة القانونية الفنية في مجال الملكية الفكرية.

✓ حماية برامج الحاسب الآلي من الاختراقات.

¹ - محمود أحمد عبابنة، مرجع سابق، ص 156 و 157.

² - نفس المرجع، ص 159.

³ - "وتتضمن المنظمة في عضويتها وفقاً لما ورد في إحصاء منشور في العام 1999 قرابة المائة والسبعين دولة، بينها حوالي ثمانية عشر دولة عربية، أنظر محمود أحمد عبابنة، مرجع سابق، ص 159.

3-المجلس الأوروبي

تأخر المجلس الأوروبي بما حدث في منظمة التعاون والإنماء الاقتصادي وما ورد في تقريرها وبناء عليه أصدر المجلس الأوروبي عام 1980 إرشادات للمشرعين كي يساعدتهم في بيان الأنشطة المتعلقة بالنظام المعلوماتي التي يجب حظرها بنماذج إساءة استخدام النظم المعلوماتية¹.

وقد اقترحت هذه الإرشادات أيضا مجالات أخرى للبحث منها:

- ✓ المنع والوقاية من أنشطة الكمبيوتر الضارة
 - ✓ المسائل المتعلقة بالتفتيش والضبط بالنسبة لمعلومات البنوك
 - ✓ التعاون الدولي في مجال التحري والإدعاء بالنسبة لجرائم الكمبيوتر
- كما عمل المجلس الأوروبي بتاريخ 24-02-2005 على إصدار قرار يهدف إلى مكافحة الهجوم على نظم المعالجات².

4-المنظمة الدولية للشرطة الجنائية(الأنتربول)

لاشك أن التعاون الدولي الأمني غالبا ما يتم تكوين أو إنشاء أنظمة لتبادل وتحليل المعلومات بين المصالح الأمنية، ومن هذا المنطلق فالشرطة الجنائية الأنتربول يعد جهازا دوليا مكون من عناصر تابعة لمصالح الشرطة القضائية لمختلف دول الأعضاء، ومن بين اهتمامات هذه المنظمة على مستوى مواجهة برائين الجريمة المنظمة العابرة للحدود، أيضا يوجد هدف مكافحة الجريمة الالكترونية من بين وظائفها الأساسية³.

5- مجلس وزراء العدل العرب

لعل أبرز ما يمكن أن يقال عن الجهود العربية المبذولة من أجل الحماية من جرائم الحاسب الآلي اعتماد مجلس وزراء العدل العرب للقانون الجزائي العربي الموحد كقانون نموذجي بموجب القرار رقم 229 لسنة 1996م، بالرجوع إلى المذكرة الإيضاحية لهذا القانون وباستعراض الباب السابع الخاص بالجرائم ضد الأشخاص نجد هذا القانون قد

¹ - أحمد الخليفة الملط: مرجع سابق، ص 675.

² - حليلة بن حفو: مرجع سابق، ص 203.

³ - شريف سيد كامل: مرجع سابق، ص 53.

احتوى على فصل خاص بالاعتداء على حقوق الأشخاص الناتج عن الجاذبات والمعالجات المعلوماتية وذلك في المواد 461-464، حيث أشارت المواد 461 و463 على وجوب حماية الحياة الخاصة وأسرار الأفراد من خطر المعالجة الآلية، وكيفية جمع المعلومات الاسمية وكيفية الاضطلاع عليها، أما المادة 464 فلقد نصت على عقاب من يقوم بفعل الدخول بطريق الغش إلى كامل أو جزء من نظام المعالجة الآلية للمعلومات، وعرقلة أو إفساد نظام التشغيل عن أداء وظائفه المعتادة، وتغيير المعلومات داخل النظام، وتزوير وثائق المعالجة الآلية وسرقة المعلومات¹.

6- شبكة مجموعة الثمانية (G8)

اعتمد وزراء العدل والداخلية التابعين لبلدان مجموعة الثمانية في اجتماعاتهم المختلفة سياسات لمكافحة العديد من جرائم الانترنت تستند إلى المبادئ التالية: عدم إتاحة ملاذات آمنة للمعتدين على تكنولوجيا المعلومات، التنسيق بين جميع الدول المعنية في ملاحقة مرتكبي جرائم الانترنت ومحاكمتهم بغض النظر عن مكان حدوث الضرر، تدريب الموظفين المكلفين بتنفيذ القوانين وتجهيزهم بالمعدات الضرورية للتعامل مع الجرائم ذات التقنية العالية.

7- الشرطة الجنائية في دول الاتحاد الأوروبي

أنشأ المجلس الأوروبي شرطة أوربية (اليوروبول)، قصد مكافحة الجرائم الإلكترونية من خلا تيسير الاتصال بين الدول الأعضاء، وضمان تبادل المعلومات بشكل فعال في مختلف المجالات².

الفقرة الثانية : الجهود الوطنية لمكافحة الجريمة المعلوماتية

عمل المغرب كغيره من الدول على وضع سياسة جنائية تهدف بالأساس إلى مواجهة الجريمة المعلوماتية، وذلك من خلال نصوص قانونية تجرم وتعاقب على هذا النوع من

¹ - محمود أحمد عابنة: مرجع سابق، ص 180 و181.

² - حليلة بن حفو: مرجع سابق، ص 206.

الجرائم (أولاً)، ومن جهة أخرى إحداث آليات مؤسسية تساهم بدورها في مجال مكافحة الجريمة المعلوماتية (ثانياً).

أولاً: النصوص الجنائية الوطنية التي تجرم الجريمة المعلوماتية

لقد تصدى المشرع المغربي للجرائم المعلوماتية، من خلال استحداثه لمجموعة من النصوص القانونية الجنائية في مجالات مختلفة، تضمنتها مجموعة القانون الجنائي المغربي، وتشريعات أخرى لها ارتباط بالمعاملات الالكترونية عموماً، وسيتم التطرق إليها وفق الشكل التالي:

1: القانون 03.07 المتعلق بسير نظم معالجة الآلية لمعطيات¹.

سارع المشرع المغربي لاحتواء تطور الإجرام المعلوماتي بواسطة إصدار عديد القوانين لكن قبل ذلك عمد على تعديل نصوص القانون الجنائي الحالي وتحيينه وذلك بإصدار قانون 03.07 المتعلق بالإخلال بسير نظم المعالجة الآلية لمعطيات والذي يعد القانون الأساسي لمكافحة الجرائم المعلوماتية بالمغرب².

وفي نص القانون الجنائي وفق التعديلات الجديدة على عدة صور للجرائم الماسة بالنظم المعالجة الآلية للمعطيات.

فالمادة 607-3 نصت على فعل الدخول إلى مجموع أو بعض نظم المعالجة الآلية للمعطيات عن طريق الاحتيال، دون أن يتوقف قيام هذه الجريمة على حدوث النتيجة الإجرامية من عدمها وقد عاقبت المادة 607-3 على هذا الفعل بعقوبة حبسية من شهر إلى ثلاثة أشهر وبغرامة من 2000 إلى 10000 درهم أو بإحدى هاتين العقوبتين.

وتنص المادة أي المادة 607-3 على فعل البقاء في نظام المعالجة الآلية للمعطيات أو جزء منها دخل إليها عن طريق الخطأ دون وجوده، فالدخول عن طريق الخطأ بعناية

1- القانون رقم 03-07 القاضي بتتيميم مجموعة القانون الجنائي، الصادر بتنفيذه الظهير الشريف رقم 1-03-197 بتاريخ

16 رمضان 1424 (11 نونبر 2003) ج.ر. عدد 5171 بتاريخ 2013/12/22، ص 4284

2- عماد بولحبال، مكافحة الجرائم المالية المعلوماتية في التشريع المغربي، رسالة لنيل شهادة الماستر في القانون الخاص، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة مولاي إسماعيل مكناس، 2015-2016، ص 86.

ليس معاقبا عليه وإنما العقوبة تقع على البقاء بعد الدخول عن طريق الخطأ إلى نظم المعالجة الآلية للمعطيات أو جزء من دون أي يكون للشخص الحق في الدخول إليها.

وقد نصت المادة 3-607 على ظروف التشديد المتعلقة بهذا الفعل وتتمثل في حالة تنص عن فعل الدخول عن طريق الاحتيال أو البقاء داخل النص والآلية لمعالجة المعطيات بالدخول إليها عن طريق الخطأ دون حق إذا نتج ذلك حذف أو تغيير المعطيات المدرجة في نظام المعالجة الآلية للمعطيات واضطراب في سيره ونص الفعل 'أ' أيضا على الظرف المشدد، حيث نص على أنه تضاعف العقوبة إذا نتج عن ذلك حذف أو تغيير المعطيات المدرجة في نظام المعالجة الآلية للمعطيات واضطراب في سيره¹.

هذا وقد عاقب الفصل 4-607 كل من دخل إلى مجموع أ بعض المعالجة الآلية عن طريق الاحتيال، يفترض أنها تتضمن معلومات تخص الأمن الداخلي أو الخارجي للدولة وتهم الاقتصاد الوطني فيما يخص الأسرار بالحبس من ستة أشهر إلى سنتين وبالغرامة من 10000 إلى 100000 درهم وتشدّد العقوبة إذا تم ارتكاب هذه الأفعال من قبل موظف أو مستخدم أثناء مزاولته مهامه أو بسببها أو إذا سهل للغير القيام بها إضافة إلى ذلك المشرع جرم حتى من عرقل عمدا نظم المعالجة الآلية للمعطيات أو إحداث فيه خلل².

كما أن المشرع المغربي جرم حتى مسألة تغيير طريقة معالجة أو إرسال المعطيات عن طريق الاحتيال، حيث عاقب على هذا الفعل بموجب الفصل 6-607 من القانون الجنائي بالحبس من سنة إلى ثلاث سنوات وبالغرامة من 10000 إلى 200000 أو بإحدى العقوبات.

وعلاوة على ذلك نجد من صور جرائم نظم المعالجة الآلية للمعطيات نص المشرع في الفصل 7-607 من القانون الجنائي المغربي يتبين على أنه عاقب كل من يزور أو يزيف وثائق المعلومات أيا كان شكلها إذا كان من شأن التزوير أو التزييف إلحاق ضرر بالغير، حيث عاقب على ذلك بالحبس من سنة إلى خمس سنوات وبالغرامة من 10000

¹ - أنظر الفصل 7-607 من القانون الجنائي.

² - نص الفصل 5-607: عاقب الحبس من سنة إلى ثلاث أشهر والغرامة من 10000 إلى 200000 درهم أو بإحدى هاتين العقوبتين.

إلى 100000¹. وقد ذهبت بعض القرارات الصادرة عن محكمة الاستئناف بالرباط، على اعتبار أن قرصنة البطائق البنكية، من قبل مجموعة من الأشخاص، بمثابة تزوير في وثائق المعلومات، ومن هذه القرارات، قرار عدد 364 والذي جاء فيه²: "بالنسبة للمتهم (ع.ص) حيث اعترف المتهم بأنه كان يقوم بسحب المبالغ المالية من شبابيك إلكترونية، بواسطة بطائق ائتمان مزيفة، عن طريق قرصنة الحسابات البنكية لزبناء أبنائك أجنبية... وحيث إن المحكمة اقتنعت بثبوت الفعل المنسوب للمتهم، وأنه يشكل من حيث الوصف القانوني للتجريم، جريمة تزوير الوثائق المعلوماتية، واستعمالها طبقا للفصل 7-607 من ق ج، بعد إعادة التكييف لجريمة تزوير بطاقة الائتمان، واستعمالها، مما يتعين معه التصريح بإدانتها من أجل ذلك.

وبالنسبة للمتهم (ب.ك) حيث اعترف المتهم بأنه لقن كيفية قرصنة الحسابات البنكية، عن طريق المتهم (ع.ص) وحدد الطريقة التي تتم بها قرصنة الحسابات البنكية... وحيث إن الوقائع المعروضة تشكل من حيث الصف القانوني للتجريم جريمة المشاركة في تزوير وثائق المعلومات واستعمالها، طبقا للفصلين 129 و 7-607 ق ج بعد إعادة التكييف لجريمة تزوير بطاقة الائتمان واستعمالها، مما يتعين معه التصريح بمؤاخذته من أجلها".

أما فيما يخص المحاولة أو الشروع في الجرائم الواردة في هذا القانون خص المشرع المغربي في منظومة القانون الجنائي فصلا صريحا لهذه المسألة حيث خصص لها الفصل 8-607 الذي نص على أن المحاولة تعاقب بنفس عقوبة الجريمة التامة،

أما فيما يخص المشاركة في الجرائم الماسة بنظم المعالجة الآلية المعطيات، نجد أنه المشرع خصص لها مادتين:

المادة الأولى: المادة 9-607 أكد على تطبيق نفس عقوبة الجريمة المرتكبة أو العقوبة المطبقة على الجريمة الأشد على كل من اشترك في عصابة أو اتفاق تم لأجل

¹ - أنظر مقتضيات الفصل 7-607 من القانون الجنائي

² - قرار رقم 364 بتاريخ 17/04/2006 ملف عدد 22/05/740. قرار مشار إليه لدى عبد الكريم عباد: مرجع سابق، ص7

ارتكاب الجرائم المعاقب عليها أو تملكها أو حازها أو تخلى عنها للغير أو عرضها أو وضعها رهن إشارة الغير.

المادة الثانية: المادة 10-607 نص على أنه: "يعاقب بالحبس من سنتين إلى خمس سنوات وبالغرامة من 50000 إلى 2000000 درهم كل من منح تجهيزات أو أدوات أو أعد برامج للمعلومات أو أية معطيات أعدت خصيصا لأجل ارتكاب الجرائم المعاقب عليها في هذا الباب أو تملكها أو حازها أو تخلى عنها للغير أو عرضها أو وضعها رهن إشارة الغير). وهكذا مثلا، قررت الغرفة الجنائية بمحكمة الاستئناف بمدينة الدار البيضاء، في قرار لها بتاريخ 7 أبريل 2000 متابعة المتهم "أ.د." بتهمة التزوير في وثيقة إدارية، بعدما قام هذا الأخير، بإحداث تغيير عن قصد في المعلومات المسجلة بالناظمة الآلية الممسوكة، من طرف إدارة الجمارك، والتي اعتبرتها المحكمة بمثابة سجل للإدارة.

وتتخلص وقائع القضية في أن المتهم المذكور والموظف بإدارة الجمارك، أقر بأنه قام باستعمال رمزه السري للولوج إلى قاعدة البيانات المضمنة بالكمبيوتر لإدارة الجمارك، وسجل بها معلومات مخالفة للحقيقة، فتتمت متابعته لأجل جنحة التزوير في وثيقة إدارية والمشاركة طبقا للفصول 129 و 360 من ق ج المغربي¹.

أما بخصوص العقوبات الإضافية فقد خص المشرع المغربي الفصل 11-607 من القانون الجنائي للعقوبات الإضافية المقررة لجرائم المس بنظم المعالجة الآلية للمعطيات، والتي تتمثل في المصادرة والحرمان من الحقوق الوطنية أو المدنية أو العائلية الواردة في نفس القانون لمدة تتراوح ما بين سنتين وعشر سنوات كما يمكن أيضا الحكم بالحرمان من ممارسة الوظائف العمومية ونشر أو تعليق الحكم الصادر بالإدانة.

2: القانون المتعلق بتعزيز الحماية الجنائية للطفل والمرأة

وفي إطار المواكبة القانونية للمشرع للجرائم المعلوماتية لم يفعل حماية المرأة والطفل على الحماية والالذان يعتبران عرضة للاستغلال لاسيما في نظام الانترنت، ليصدر

¹ قرار جنائي عدد 2000/4/7 في الملفين عدد 410 و 99/5/298 عن الغرفة الجنائية بمحكمة الاستئناف بالدار البيضاء.

24-03¹ الذي غير وتمم بعض نصوص القانون الجنائي. والأمر يخص بالأساس المادتين 503-1 و 503-2 من القانون الجنائي.

فالمادة 503-1 نصت على التحرش الجنسي بواسطة وسائل خاصة بالتهديد أو وسائل لفكراه والغالب عليها بالحبس من سنة إلى سنتين وبالغرامة من 5000 إلى 50000 درهم ويمكن بالتالي إسقاط هذه الأفعال الواردة في هذا الفصل على التحرش الجنسي الذي يقع بواسطة الوسائل الالكترونية المرئية أما المادة 503-2 تنص على تحريض أو تشجيع أو تسويق استغلال الأطفال أقل من 18 سنة في مواد إباحية أو تصوير الأعضاء الجنسية لأغراض ذات طبيعة جنسية، ويعاقب على هذا الفعل بعقوبة حبسية تتراوح بين سنة وخمس سنوات وغرامة من 10000 إلى مليون درهم وهذه الأفعال يمكن أن تتم بواسطة الوسائل المعلوماتية والتي تدخل أيضا في نطاق هذه الجرائم وفضاء الانترنت قد يصبح مجالا خصبا للممارسة هذه الأفعال، لذلك جاءت هذه المقترحات سد الثغرات التشريعية في هذا الصدد².

3: قانون حماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع

الشخصي(08- 09)

نظرا لما تشكله الجريمة المعلوماتية من خطورة، فإن الأشخاص الذاتيين يعدون الهدف التي يأتي في مرمى قوس الخصم التي تشكله الجريمة المعلوماتية. لذلك عمل المشرع المغربي على حماية الأشخاص الذاتيين وتعاطيهم مع فضاء المعلومات وصيانة معطياتهم ذات الطابع الشخصي ليصدر المشرع قانون 08-09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي³.

1- قانون صدر بتنفيذه ظهير شريف رقم 1.03.207 صادر في 16 رمضان 1424 (11 نوفمبر 2005) الجريدة الرسمية عدد 5175 بتاريخ 05/02/2004، ص 121.

2- أنظر المواد 503-1 و 503-2 من القانون الجنائي.

3- صدر بتنفيذه الظهير الشريف رقم 1.09.15 صادر في 22 من صفر 1430 (18 فبراير 2009)، المنشور في الجريدة الرسمية عدد 5711 بتاريخ 2009/02/23، ص 552.

لذلك يضطلع هذا القانون حماية الأشخاص الذاتيين من هذا التي تشكلها المعاملات الالكترونية وحماية معطيائهم الشخصية¹.

وتتجلى الحماية التي يوفرها قانون **09.08** للأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، من خلال الباب السابع من القانون المذكور، هذا الباب جاء مختصا بالعقوبات.

ومن أهم المقتضيات الزجرية التي جاء بها قانون **09.08** نجد المادة 53 التي تتحدث عن رفض المسئول على معالجة المعطيات من الولوج أو التصريح أو التعرض المنصوص عليها في المواد 7 و 8 و 9 من نفس القانون وما ثبت بغرامة من 20000 إلى 100000 درهم².

وأیضا المادة 54 التي تنص على فعل جمع معطيات ذات طابع شخصي بطريقة تدليسية وعاقبت على هذا الفعل بالحبس من 3 أشهر وغرامة من 20000 إلى 200000 درهم.

ومن أهم المواد أيضا نجد المادة 60 من قانون **09.08** فعاقب عن عملية قفل المعطيات ذات الطابع الشخصي نمو دولة أخرى حسب حکام المادتين 42 و 44 من نفس القانون.

ونجد المادة 63 تعاقب على رفض كل مسئول // قرارات اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي، وعاقبت على هذا الفعل بالحبس من ثلاثة أشهر إلى سنة وغرامة ما بين 10000 إلى 100000 درهم. دون نسيان المقتضيات المتعلقة بالاستعمال التعسفي أو التدليسي للمعطيات التي نصت عليها وعلة عقوبتها المادة 61 من قانون **09.08** التي تنص على عقوبة حبسية من ثلاثة أشهر إلى سنة وغرامة من 20000

¹ - مقال بعنوان «المعاملات الالكترونية» في www.minculture.gov.ma تاريخ الولوج 2017/11/26 على الساعة 23:57 .

² - المادة 53 من قانون 09.08.

إلى 200000 درهم وتجدر الإشارة إلى أن إعادة 64 نصت على مضاعفة الغرامات إذا كان مرتكب الأفعال شخص معنوي.

4: قانون تبادل البيانات والمعطيات الكترونيا(53-05)¹

لقد عرقل المجتمع الدولي ثورة على المستوى الرقمي الذي أضحى أفرادها يرتكزون في معاملاتهم على الفضاء المعلوماتي، غير ذلك لا يخلو من خطورة تهدد أمنهم المعلوماتي لذلك تدخل المشرع بإصدار قانون 53.05 المتعلق بتبادل البيانات والمعطيات الالكترونية.

يتضمن قانون 54.05 43 مادة بالمجمل وقد جاء لمكافحة الجريمة المعلوماتية عامة، وتنظم المعاملات التجارية الالكترونية بصفة خاصة ووضع القواعد الخاصة لاسيما المعادلة من حيث الآيات بين الوثائق المحمولة على دعامة ورقية والوثائق المحمولة على دعامة الكترونية، وأيضا كيفية إبرام العقود الالكترونية وكذا تشفير البيانات والتوقيع الالكتروني والمصادقة الالكترونية وغيرها². ونص عن بعض مقتضيات المتعلقة بحماية المعطيات المتبادلة خاصة العقوبات التي جاءت في الباب الثالث من هذا القانون فبهذا المادة 29 جرمت تقديم خدمة المصادقة الالكترونية دون التوفر على الاعتماد³.

5: القانون المتعلق بحقوق المؤلف وحقوق المجاورة(قانون رقم 02-00)

إن حقوق الملكية الفكرية هي سلطة مباشرة يعطيها القانون للشخص على كافة منتجات عمله وتفكيره وتمنحه مكنة الاستثنائية والانتفاع بما تدر عليه هذه الأفكار من مردود مالي.

وقد أدت ثورة المعلومات إلى ظهور جيل جديد من المصنفات والمؤلفات الالكترونية سواء البرمجيات وقواعد البيانات وطبوغرافيا الدوائر المتكاملة وقد جاء قانون

1- صدر الأمر بتنفيذه ظهير الشريف رقم 1-07-129 صادر في 14 من ذي القعدة 1428 الموافق ل 30 نونبر 2007 منشور بالجريدة الرسمية عدد 5584 بتاريخ 6 دجنبر 2007، ص 3879
2- د. مصطفى مالك: قراءة في القانون المغربي للتبادل الالكتروني للمعطيات القانونية، مجلة المناهج القانونية، عدد مزدوج 14/13، سنة 2009، ص 33.
3- تنص المادة 24: "يعاقب بغرامة 10000 إلى 100000 درهم وبالحبس من ثلاثة أشهر إلى سنة كل من قدم حرمان المصادقة الالكترونية المؤمنة دون أن يكون معتمدا وفق الشروط المنصوص عليها في المادة 21 أعلاه أو واصل شاهد رغم سحبه اعتمادا أو أصدر أو سلم أو دبر شهادات الكترونية مؤمنة خلافا لأحكام المادة 20".

02.00 لحماية حقوق المؤلف والحقوق المجاورة¹. وخاصة حماية المؤلفات والبرمجيات وقواعد البيانات الالكترونية والدوائر المتكاملة إن تدخل في نطاق حماية هذا القانون².

مع تنصيب القانون الجنائي على بعض المقتضيات الزجرية كجريمة التقليد أو منع أو إنتاج أو مصنف // لمقتضيات قانون **02.00** بالمواد 575 و 576 من القانون الجنائي³.

6: مستجدات جاء بها مشروع قانون الجنائي فيما يخص المس بنظم المعالجة

الآلية للمعطيات

إن مشروع القانون الجنائي بدوره أشار إلى جريمة المس بالنظم الآلية للمعطيات من خلال المواد من 580 إلى 589.

- فيما يخص الدخول إلى نظام المعالجة الآلية للمعطيات أو جزء منها عن طريق الاحتيال يلاحظ أن المشرع شدد العقوبة الحبسية والغرامة، إذ أصبحت من ثلاثة أشهر إلى سنة وغرامة من 2000 إلى 20000 درهم، وبطبيعة الحال فقد تم تطبيق نفس العقوبة على البقاء في نظام المعالجة الآلية للمعطيات سواء كان قد دخل لها عن طريق الخطأ أو العكس، وبناء على هذا يلاحظ أن المشرع ضمن المشروع أضحى متشددا مقارنة بالقانون الجنائي النافذ. كما تضاعف العقوبة إذا نتج عن ذلك حذف أو تغيير المعطيات المدرجة في نظام المعالجة الآلية للمعطيات أو اضطراب في سيره.

- كما تم تشديد العقوبة داخل المشروع، فيما يخص الأفعال النصوص عليها في **المادة 580** والتي تتعلق بنظام المعالجة الآلية للمعطيات إذا كانت تخص الأمن الداخلي أو الخارجي للدولة أو أسرار الاقتصاد الوطني، إذ أصبحت العقوبة الحبسية من سنة إلى ثلاث سنوات وغرامة من 100000 إلى 1000000

¹ - صدر بتنفيذه هذا القانون الظهير الشريف 1.7.129 بتاريخ 30 نونبر 2007 (19 ذي القعدة 1428) نفس بالجريدة الرسمية عدد 5584 ب 6 دجنبر 2007، ص 3874.

² - فؤاد زلماط، محاضرات في مادة الملكية الفكرية، الجزء الأول، دون طبعة، مطبعة وراقعة سجالمة مكناس 2015، ص 26-27-28-29.

³ - وفي هذا الصدد نصت المادة 575 على فعل طبع أو إنتاج كتب أو تصانيف من أي نوع في المملكة بعقوبة الغرامة من 12 إلى 10000 درهم وإعادة 576 تعاقب على فعل التقليد المصنفات أو الإذاعة أو العرض حرصا لقانون حقوق المؤلف والحقوق المجاورة.

- درهم، وترتفع العقوبة من ثلاث سنوات إلى خمس سنوات إذا نتج عن الأفعال المرتكبة تغييراً أو حذف أو اضطراب في سير نظام المعالجة الآلية المعطيات.
- وفيما يخص العرقلة العمدية أو إحداث ضرر في نظام المعالجة الآلية المعطيات، فقد حافظ المشرع على نفس العقوبة الحبسية في المشروع وحتى الحد الأدنى للغرامة بينما رفع سقف الغرامة لتصل إلى 1000000 درهم في المادة 583 من مشروع القانون الجنائي.
- والمادة 584 بدورها حافظت على نفس العقوبة الحبسية المشار إليها في المادة 607-7 من القانون الجنائي الحالي والتي تعاقب على تزوير وثائق معلوماتية، بينما رفعت الحد الأدنى للغرامة إلى 10000 درهم وحافظت على الحد الأقصى لها.
- وقد سار المشروع على نفس نهج التشديد في المواد الموالية إلى حدود المادة 590.

ثانياً: الآليات المؤسسية الوطنية لمكافحة الجريمة المعلوماتية

إذا كن المشرع عمل على تطوير القوانين الداخلية، بهدف تأسيس حماية قانونية للنظم المعلوماتية، وعياً منه بأوجه الخلل والقصور في هذه القوانين، فإن إرساء دعائم هذه الحماية وتقويتها، رهين بإحداث أجهزة أمنية وقضائية متخصصة، لضبط الجرائم المعلوماتية، كما يتطلب الأمر إشراك مؤسسات ذات الطابع الاقتصادي في الإستراتيجية الأمنية المعتمدة، لرصد هذا النوع من الجرائم، إضافة إلى الشبكة المغربية للتعاون القضائي الدولي.

1- الأجهزة ذات الطابع الجزري

تتميز الجرائم المعلوماتية بكونها جرائم تقنية، تنشأ في الخفاء، يرتكبها مجرمون أذكفاء، يمتلكون أدوات المعرفة التقنية، التي توجه للنيل من الحق في المعلومات، وكل البيانات والمعطيات المنقولة، عبر نظم وشبكات المعلومات. لذا، فالتصدي لها يقتضي وجود عناصر خاصة من الضابطة القضائية، لها من التكوين العلمي والمعرفي، في ميدان

المعلومات، بما يكفي لمكافحة هذا النشاط الإجرامي الحديث. وهذا، لا يتحقق إلا بعد تلقيها التعليم والتدريب الكافيين على استخدام شبكات الاتصال، واستخدام الأجهزة الفنية الحديثة، والمعرفة الكافية باللغات الأجنبية، مما يسمح لها بالقيام بإجراءات التفتيش والضبط والتحفيز على الأدلة، التي تساعد على إثبات الجريمة المعلوماتية¹.

والأجهزة الزجرية أمر حتمي كون أن الجريمة المعلوماتية أصبحت تحتل المرتبة الثانية بعد جرائم الاختلاس ويتراوح حجم الخسائر الناجمة عن هذا النوع من الجرائم بين 300 و 950 مليار دولار، وفي هذا الإطار سجلت في المغرب 44 قضية من قضايا الجريمة المعلوماتية سنة 2008 توبع فيها 78 شخصا بتهم تتعلق بالدخول إلى نظام المعالجة الآلية للمعطيات والتزوير واستعمال بطائق الائتمان. كما سجلت قضية سنة 2010 توبع فيها 57 متهما، أما في سنة 2012 فقد تم تسجيل 13 قضية توبع فيها 16 متهما (الوكيل العام للملك لدى محكمة الاستئناف بالرباط)².

وفي إطار المقاربة الأمنية دائما للجريمة المعلوماتية، تم في سنة 2012 إحداث مختبر جهوي أول بمدينة فاس، خاص بتتبع هذا النوع من الجرائم، وكان السبب بالأساس هو تكثف الأنشطة الإرهابية³.

2- المؤسسات ذات الطابع الاقتصادي⁴

ثمة العديد من المؤسسات ذات الطابع الاقتصادي، التي تم استحداثها، للحد من الجرائم المعلوماتية، ولعل من أبرزها مركز النقديات والبنوك IMC المعلوماتية وشركات الاتصال.

ويلعب مركز النقديات والبنوك دورا مهما في مكافحة الجريمة المعلوماتية، ومعرفة مرتكبيها. فقد تم انتدابه للاتصال بمختلف البنوك، على الصعيد الوطني، بغية الإفادة عن

¹- عبد الكريم عباد: مرجع سابق، ص 88

²- أنظر تدخلات الأساتذة في إطار الندوة العلمية التي عقدت بمقر محكمة الاستئناف بالرباط حول: (الجريمة الالكترونية وتأثيرها على الائتمان المالي). بتاريخ 2013/12/6. منشورة في مقال الأستاذ عبد الكريم عباد، مرجع سابق، ص 37

³- عبد الكريم عباد: مرجع سابق، ص 90

⁴- نفس المرجع: ص 90 و 91

جميع عمليات السحب عبر الشبائيك البنكية، بواسطة بطائق الائتمان المزيفة، ولاسيما التي تم ابتلاعها من طرف هذه الشبائيك.

ويقوم هذا المركز بمساعدة الضابطة القضائية في التحريات التي تجريها، والتي بمقتضاها تتوصل إلى قراصنة بطائق الائتمان، وتقديمهم للعدالة، وهو ما يبرز دور هذا المركز في رصد الجريمة المعلوماتية، والتي تعتبر متطورة في المجال البنكي، لسهولة تعرض زبائنها كمستعملين للخدمات البنكية و التجارة الالكترونية ووسائل الأداء.

3- الشبكة المغربية للتعاون القضائي الدولي¹

تم تقديم هذه الشبكة في المؤتمر الدولي حول منع الجريمة والعدالة الجنائية بالسلفادور ما بين أيام 12 و 19 أبريل 2011. وهي شبكة من الجيل الجديد، أنشئت في إطار برنامج مغربي إسباني من طرف وزير العدل للبلدين، وذلك بهدف تحسين التعاون القضائي بين أوروبا والعالم العربي.

وتتضمن هذه الشبكة عددا من القضاة و الوكلاء العامين المغاربة الخبراء في مجال التعاون القضائي الدولي، ويبرز هذا التعاون جليا خاصة على مستوى نقل الإجراءات والإنابة القضائية الدولية و تسليم المجرمين، وتعد هذه الآليات من أبرز مظاهر التعاون الدولي في مجال محاربة الجريمة المعلوماتية.

الفقرة الثالثة : تحديات مكافحة الجريمة

لاشك في أن هناك جهود مبدولة وسياسة جنائية في مجال مكافحة الجريمة المعلوماتية، بيد أن الأمر لا يعتبر سهلا المنال، بل تصادفه عدة عراقيل وتحديات تحول دون تحقق غرض المكافحة ولعل أبرز هذه الصعوبات تكمن في:

1/ مشكل الإثبات

إن سهولة محو الدليل أو تدميره يعد من الصعوبات الجوهرية في الجرائم المعلوماتية، بحيث يمكن أن تعترض عملية الإثبات في هذا المجال سهولة محو أو تدمير

¹-حليمة بن حفوف: مرجع سابق، ص206

أدلة الإدانة في زمن قياسي فضلا عن سهولة تنصله من مسؤولية هذا الفعل ويتم إرجاعه حسبما تشهد بذلك وقائع عديدة سابقة إلى خطأ في نظام الحاسوب أو الشبكة أو في الأجهزة الأخرى.

فتتم الجريمة المعلوماتية في بيئة غير تقليدية، حيث تقع إطار الواقع المادي الملموس، لنقوم أركانها في بيئة الحاسوب والانترنت، مما يجعل الأمور تزداد صعوبة وتعقيدا لإثباتها من قبل سلطات الأمن وأجهزة التحقيق. ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي، مما يجعل أمر طمس الدليل ومحوه كليا من قبل الفاعل أمر في غاية السهولة، وفي هذا الصدد ومع صعوبة الإثبات، ومما يزيد الأمر تعقيدا، هو أن وسائل المعاينة وطرقها التقليدية لا تسعف غالبا في إثبات هذا النوع من الجرائم، ولا تنسجم معها لطبيعتها الخاصة التي تختلف عن الجرائم التقليدية، فمسرح أحداث هذه الأخيرة يخلق أثارا ماديا تقوم عليها الأدلة، التي من شأنها مساعدة سلطات التحقيق عن الكشف عن الجريمة، وذلك عن طريق المعاينة والتحفظ على الآثار المادية التي خلفتها الجريمة، لكن فكرة مسرح أحداث الجريمة المعلوماتية يتضاءل دوره في الإفصاح عن الحقائق المؤدية للأدلة المطلوبة لسببين:

- أن الجريمة المعلوماتية لا تخلق أثارا مادية.
- أن نقص الخبرة الفنية والتقنية لدى سلطات التحقيق، يشكل عائقا أمام إثبات الجريمة المعلوماتية، كما يشكل مجالا للجاني للإفلات من العقاب، خصوصا أ، هذا الأخير على دراية عالية بتقنية المعلومات وبإمكانه بسهولة إتلاف أو تغيير الآثار المادية للجريمة¹.

2/ نقص خبرة الأجهزة المكلفة بجمع الدليل

غالبا ما تواجه الأجهزة المنية مشكلة كيفية إدراك الأبعاد العلمية لمواجهة هذه الجرائم، التي تتكون عناصرها من تقنيات علوم حديثة لم تألفها هذه الأجهزة من ذي قبل، فالذي يرتكب اليوم على مسرح الجريمة ما هو إلا عبء جديد يتقل كاهل مؤسسات الأمن

¹ - عبد الكريم عباد: مرجع سابق، ص 44

فالكشف عن الجرائم المعلوماتية بوجه عام والمالية بصفة خاصة والوصول إلى مرتكبيها وملاحقتهم جنائياً، يتطلب بالضرورة استراتيجيات تحقيق وتدريب ومهارات خاصة لدى الأجهزة الأمنية، تسمح لهم بالتعامل مع تقنيات الحاسوب المتطور وأساليب التلاعب المعلوماتي المعقدة التي تستخدم في ارتكاب مثل هذا النوع من الجرائم، مما يجعل الضرورة حتمية للتخصص في هذه الجرائم كما هو الحال في التخصص في الجوانب القانونية¹.

3/ ضعف التعاون الجنائي الدولي في مجال ابحاث والتحقيق

يصير التعاون الدولي واسع المندى في مكافحة الجرائم الواقعة في بيئة المعالجة الآلية للمعطيات أمراً محتتما لا مفر منه، إلا أن هناك عقبات تقف في سبيله من قبيل عدم وجود اتفاق عام وموحد بين الدول حول نماذج الاعتداءات المعلوماتية الواجب تجريمها، ضف إلى ذلك عدم الاتفاق حول التعريف القانوني للنشاط الإجرامي الذي يمكن الاتفاق على تجريمه، ناهيك عن عدم التناسق بين قوانين الإجراءات الجنائية للدول المختلفة فيما يتعلق بالتحري والتحقيق في الجرائم المعلوماتية بالإضافة إلى عدم وجود اتفاقيات ثنائية أو جماعية كافية بين الدول تسمح بالتعاون الدولي في مكافحة هذا النوع من الجرائم².

وغيرها من الصعوبات والعراقيل التي من شأنها تشكيل حاجز يحول دون تحقيق المكافحة المرجوة للجرائم المعلوماتية خاصة تلك التي تعبر حدود الدول.

4/ انعدام نموذج موحد للنشاط الإجرامي

يحول اختلاف الدول من حيث العادات والتقاليد و الديانات والثقافات دون تحقيق التعاون الدولي،فما يكون مباحا في بعض النظم القانونية قد يشكل جريمة في غيرها، وهو ما يبرز صعوبة وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الانترنت الواجب تجريمها³.

¹ - عماد بولحبال: مرجع سابق، ص 241 و 242 و 243.

² - عماد بولحبال: مرجع سابق، ص 245 و 246.

³ - حليلة بن حفو: مرجع سابق، ص 208.

خاتمة:

عموما تعد الجريمة المعلوماتية من الجرائم المستحدثة ترتكب من خلال الوسائل التكنولوجية وبضبط بواسطة أجهزة الانترنت، وهي لا تقل خطورة عن الجرائم التقليدية الأخرى، بل أشد خطورة بحكم الآثار التي تخلفها لهذا الأمر كان لزاما على كل التشريعات الدولية والوطنية بأن تصدر نصوص قانونية وآليات مؤسسية لمواجهة مساوئ هذا النوع من الإجرام، وبالفعل بذلت جهود ملحوظة في هذا الإطار، إلا أنه هذه الجهود لم تحقق الهدف المنشود بحيث ظلت قاصرة ومحدودة بفعل التحديات والمعوقات التي تعرضت لها، وذلك على ضوء نوعية الجرائم المعلوماتية التي ترتكب في الخفاء وبالتالي صعوبة إثباتها، ومن هذا المنطلق تم الخروج بخلاصة تمثل حقيقة لا يجب في معظم الحيات نسيانها ولا التغاضي عنها هي ضرورة إعادة النظر في إستراتيجية السياسة الجنائية ووضع خطط وتدابير تواكب نوعية الجريمة ودرجة خطورتها والعمل على تكوين أجهزة أمنية وقضائية مختصة بهذا المجال هذه من جهة، ومن جهة أخرى مضاعفة تعزيز التعاون الجنائي الدولي عن طريق إبرام اتفاقيات دولية ثنائية منها والإقليمية، لأن من شأن كل هذا ليس الحد وإنما على الأقل التقليل من تدفق الجريمة المعلوماتية سواء التي ترتكب داخل دولة معينة أو العابرة للحدود وللتوضيح أكثر يمكن إجمال المقترحات على النحو التالي:

- ضرورة سن تشريع خاص بالجريمة المعلوماتية، لعدم كفاية النصوص الجنائية التقليدية.
- ضرورة ملائمة الجهاز القضائي بكل مكوناته مع هذا النوع من الجرائم، وذلك من خلال إنشاء شرطة قضائية متخصصة في هذا المجال، تجمع بين التكوين القانوني والتكوين التقني، وانفتاحها على باقي الأجهزة الأمنية، للدول الرائدة في مكافحة هذه الجرائم في إطار التعاون الأمني الدولي.
- يجب فتح أفاق التكوين والتدريب لمختلف المتدخلين في الميدان، من قضاة ومحامين وخبراء... بما يدعم خبراتهم، في اتجاه فهم طبيعة هذه الجرائم، وإشكالاتها.

- يجب العمل أيضا على تحديث وسائل الإثبات، بحيث تساعد القاضي في حل النزاعات المتعلقة بالجرائم المعلوماتية، ومسايرة الاجتهاد القضائي لثورة المعلومات، من خلا قبول الأدلة المستمدة من أجهزة الحاسوب، كلما كانت مقنعة له.
- يجب التوسع أكثر في اتجاه إنشاء أجهزة وهيكل إدارية فنية متخصصة، في التحري والتحقيق الجنائي، وتجهيزها بكل الوسائل الالكترونية اللازمة لإنجاح عملها.
- وضع إستراتيجية لدى جميع الدول من أجل التصدي لهذا النوع من الجرائم.
- السهر على المشاركة في المؤتمرات الدولية التي تعني بالتصدي لظاهرة الإجرام المعلوماتي مع الحرص على متابعة المستجدات الدولية في مجال مكافحة هذه الجرائم.

لائحة المراجع:

الكتب:

- شريف كامل السيد, الجريمة المنظمة في القانون المقارن, الطبعة الأولى, دار النهضة العربية, القاهرة, 2001
- فريد منعم جبور, المستهلك عبر الانترنت و مكافحة الجرائم الإلكترونية دراسة مقارنة, الطبعة الأولى, دار النهضة العربية, القاهرة, 2003
- محمد أمين الرومي, جرائم الكمبيوتر و الانترنت, دون طبعة, دار المطبوعات الجامعية, الإسكندرية, 2003
- محمد علي العريان, الجرائم المعلوماتية, دون طبعة, دار الجامعة الجديدة للنشر, القاهرة, 2004
- منير محمد الجنبهي و ممدوح محمد الجنبهي, جرائم الانترنت و الحاسب الآلي ووسائل مكافحتها, دون طبعة, دار الفكر الجامعي, الإسكندرية, 2004
- احمد خليف الملط, الجريمة المعلوماتية, دون طبعة, دار الفكر الجامعي الإسكندرية, 2005
- محمد احمد عبابنة: جرائم الحاسوب و أبعادها الدولية, دون طبعة, دار الثقافة للنشر و التوزيع, عمان, 2005
- محمد الشناوي جرائم النصب المستحدثة, دون طبعة, دار البيان للطباعة والنشر, القاهرة, 2008.
- عمر محمد بن يونس: غسيل الأموال عبر الانترنت, د-ط, دار النهضة العربية, القاهرة, 2004 .
- محمد سامي الشوا: ثورة المعلومات و انعكاساتها على قانون العقوبات, الطبعة الثانية, دار النهضة العربية, القاهرة, 1998
- محمد أحداف: علم الإجرام, الطبعة الثالثة, مطبعة سجلماسة, مكناس 2014-2015
- فؤاد زلماط: محاضرات في مادة الملكية الفكرية, الجزء الأول, دون ذكر الطبعة, مطبعة ووراقة سجلماسة, مكناس, 2015 .

الرسائل:

- عماد بولحبال: مكافحة الجرائم المالية المعلوماتية في التشريع المغربي, رسالة لنيل شهادة الماستر في القانون الخاص, كلية العلوم القانونية و الاقتصادية و الاجتماعية, مكناس 2015/2016

المقالات:

- جميلة عباوي: الحماية الجنائية للمعاملات الالكترونية، المجلة المغربية للقانون الجنائي والعلوم الجنائية، العدد الثالث، سنة 2016، ص 83.
- صليحة الحاجي: الآليات القانونية لتكريس الأمن المعلوماتي، مجلة العلوم الجنائية العدد الثاني، سنة 2015، ص 5.
- مصطفى مالك: قراءة في القانون المغربي للتبادل الالكتروني للمعطيات القانونية، مجلة المناهج القانونية، عدد مزدوج 14/13 2009
- حليلة بن حفو: محاربة الجرائم الالكترونية على الصعيد الدولي(الواقع والأفاق)، مجلة العلوم الجنائية، العدد الأول، سنة 2014
- عبد الكريم عباد: الجريمة المعلوماتية، المجلة الوطنية للعلوم القانونية والقضائية، العدد الأول، دون سنة.

المواقع الالكترونية:

- مقال بعنوان —المعاملات الالكترونية— في www.minculture.gov.ma
- تاريخ الولوج 2017/11/26 على الساعة 23:57

التصميم:

المقدمة:

المطلب الأول : ماهية الجريمة المعلوماتية

الفقرة الأولى مفهوم الجريمة المعلوماتية

أولاً: تعريف الجريمة المعلوماتية

ثانياً: مفهوم الحاسب الآلي

ثالثاً: الجاني والمجني عليه في الجرائم المعلوماتية

رابعاً: خصائص الجريمة المعلوماتية وأساليب ارتكابها

الفقرة الثانية : الطبيعة القانونية للجريمة المعلوماتية

الفقرة الثالثة : أنواع الجريمة المعلوماتية

أولاً: الجرائم المعلوماتية الماسة بالذمة المالية

ثانياً: الجرائم المعلوماتية الماسة بالأشخاص

المطلب الثاني: الجهود المبذولة لمكافحة الجريمة المعلوماتية

الفقرة الأولى: الجهود الدولية

أولاً: الاتفاقيات الدولية الخاصة بمواجهة الجرائم الالكترونية

ثانياً: المؤسسات الدولية لمحاربة الجريمة المعلوماتية

الفقرة الثانية: الجهود الوطنية

أولاً: النصوص الجنائية الوطنية التي تجرم الجريمة المعلوماتية

ثانياً: الآليات المؤسسية الوطنية لمكافحة الجريمة المعلوماتية

الفقرة الثالثة: التحديات التي تعيق مكافحة الجريمة المعلوماتية

الخاتمة: