وزارة التعليـــم العالـــي والبحـــث العلمـــي
جامعـــة الحـــاج لخضـــر
باتنـــة

كلية الحقوق والعلوم السياسية
قسم الحقوق

السلـــــــوك الإجرامـــــــي للمجـــــرم المعلومـــــــــاتي

بحث مكمل لنيل شهادة الماجستير في العلوم القانونية
تخصص: علم الاجرام وعلم العقاب

إعداد الطالب:
حمـــــزة بن عقون

إشراف الدكتورة
شـــــادية رحاب

أعضاء لجنة المناقشة

الإسـم واللقب	الرتبـــــة	الجامعـــــة	الصفـــــة
د/ قصيـــــر عـــلي	أستـــاذ محاضر	جامعـــة بـــاتنة	رئيســـــــا
د/ رحـــــاب شـادية	أستـــاذ محاضر	جامعـــة بـــاتنة	مشرفـــــة ومقررة
د/ مبـــــاركي دليلـــة	أستـــاذ محاضر	جامعـــة بـــاتنة	عضـــــوا مناقشـــا
أ.د/ بن الشيخ نور الدين	أستاذ التعليم العالي	جامعـــة سطيـــف	عضـــــوا مناقشـــا

السنة الجامعية 2011- 2012

إن الفكر القانوني يعيش مع أوائل القرن الحادي والعشرين مرحلة انتقالية اتجاه ظاهرة إجرامية عالمية حديثة، حيث عرف العالم منذ منتصف القرن العشرين ثورة جديدة اصطلح على تسميتها بالثورة المعلوماتية، وهذا إشارة إلى الدور البارز الذي أصبحت تلعبه المعلومات في الوقت الراهن، فقد أصبحت قوة لا يستهان بهـــا فـــي أيدي الدول والأفراد، وكان التطور الهائل الذي شهده قطاعي تكنولوجيا المعلومات والاتصالات والاندماج المذهل الذي حدث بينهما فيما بعد هو المحور الأساسي الذي قامت عليه هذه الثورة.

يعد الحاسب الآلي والإنترنت حجر الزاوية في مجال التقنية الحديثة التي هدفت لخدمة البشرية في مجالات عدة وتركت آثار ايجابية وشكلت قفزة حضارية نوعيـــة في حياة الأفراد والدول، حيث تعتمد القطاعات المختلفة في الوقت الحاضر في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية نظرا لمـــا تتميـــز بـــه مـــن عنصري السرعة والدقة في تجميع المعلومات وتخزينها ومعالجتها ومن ثـــم نقلهـــا وتبادلها بين الأفراد والجهات المختلفة، كما أصبحت هذه الأنظمة مستودعا لأسرار الأشخاص المتعلقة بحياتهم الشخصية أو بطبيعة أعمالهم المالية والاقتصادية.

غير أن هذا الجانب الايجابي والمشرق لعصر المعلوماتية لا ينفي الانعكاسات السلبية التي أفرزتها هذه التقنية العالية والمتمثلة فـــي إســـاءة اســـتخدام الأنظمـــة المعلوماتية واستغلالها على نحو غير مشروع، حيث أدى هذا التطور الهائـــل إلـــى ظهور أنماط مستحدثة من الجرائم اصطلح تسميتها بالجرائم المعلوماتية.

كما أن هذه الجرائم الحديثة يختلف مرتكبوها عن المجرمين العـــادين، فهـــذه الطائفة الجديدة من المجرمين يسمون بمحترفي جرائم المعلومات والاتصالات، كما أن هذه الجرائم تمارس من طرف أشخاص متمتعين بكامل صحتهم الجسدية، حاملي

الشهادات، ذوي مكانه اجتماعية، يعتمدون على تكوينهم الذهني، وبعبارة أخرى هو مجرم متخصص ومحترف، يستعمل الترغيب لا الترهيب، لا يميل إلـــى اســـتخدام العنف، بل أساليب تتسم بالهدوء وذات فاعلية كبيرة ومؤثرة، أي أن هـــذا التطـــور المذهل في التكنولوجيا والذي أدى إلى استحداث جرائم جديدة انعكست على السلوك الإجرامي للمجرم، والذي استغل هذا التطور في ابتكار أســـاليب جديـــدة للســـلوك الإجرامي يتمكن من خلاله الجناة من ارتكاب جرائمهم وهم بمنأى عـــن المراقبـــة والمتابعة.

1. أهمية الموضوع:

إن السلوكيات الإجرامية التي تقع عبر الإنترنت تعد من الموضوعات الحديثة التي فرضت نفسها على المستوى الوطني والدولي على حد سواء، والتي ينبغي على المشرع الجنائي مواجهتها بتشريعات حاسمة لمكافحتها وعقاب مرتكبيها.

وتبلور أهمية الموضوع في ما يلي:

- **أولا:** حيث أن الموضوع يتعلق بالتطور التكنولوجي والجرائم الناجمة عـــن هذا التطور وهي جرائم مستجدة مما يجعلها تختلف في ميكانيزماتهـــا عـــن الجرائم التقليدية.
- **ثانيا:** تثير المعلوماتية باعتبارها علم المعالجة الآلية للبيانات مشكلات قانونية عدة إذ يساء استخدامها لارتكاب الجريمة عن بعد من ناحيـــة، أو أن تكـــون محلا للاعتداء عليها من ناحية أخرى، مما يثير مسألة تكييف الاعتداء وما إذ كان يشكل جريمة أم لا.

- **ثالثا:** السلوك الإجرامي للمجرم المعلوماتي يختلف عن السلوك الإجرامي للمجرم التقليدي، فالمجرم المعلوماتي استغل هذا التطور في ابتكار أساليب جديدة وجب دراستها بالتحليل للتصدي لها ومعرفة كيفية التعامل معها.
- **رابعا:** تمثل المعلومة قوة اقتصادية مستحدثة مما ينبغي معه إحقاق مبدأ الحق في المعلومة، وذلك بتحقيق التوازن بين الاستخدام الحر والكامل للمعلومات وبين الحقوق والحريات، وذلك بحماية من تتعلق بهم المعلومات من المساس بشرفهم وحرمة حياتهم الخاصة أو استخدام هذه المعلومات على نحو غير مشروع في ارتكاب جرائم الغش المعلوماتي.

2. أسباب اختيار الموضوع:

هناك جملة من الأسباب دفعتني إلى اختيار هذا الموضوع، نذكرها فيما يلي:

- الجرائم الالكترونية من أخطر الجرائم في العصر الحديث، فآثارها لا تقتصر على فرد أو مؤسسة أو على الدولة الواحدة بل إنها تتجاوز الحدود الإقليمية لها.
- أهمية الوقوف على هذا النمط الجديد من الجرائم الذي بدأ يغزو المجتمعات خاصة مع زيادة استخدام هذا الجهاز في جميع مناحي الحياة وكثرة الانتهاكات الواقعة بواسطة الجهاز وقلة الحماية القانونية.
- كون هذه الجريمة تحتاج في مكافحتها تعاون الدول فيما بينها، وأصبحت أساليب هذه الجرائم مستعملة من طرف العصابات المنظمة.
- محاولة الإلمام ومعرفة الأساليب الحديثة والمتبعة من طرف المجرم المعلوماتي، ومحاولة التصدي لها عن طريق ما نص عليه المشرع

الجزائري في القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 من قانون العقوبات في القسم السابع تحت عنوان المساس بأنظمـــة المعالجـــة الآليـــة للمعطيات وذلك في المادة 394 مكرر إلى المادة 394 مكرر 7، إضافة إلى النص المستقل والمتمثل في القـــانون 04/09 المـــؤرخ فـــي 5 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

- ولقد وقع اختياري على دراسة هذا الموضوع إيمانا مني بأهمية الوقوف على هذا النمط المستحدث من السلوك الإجرامي الذي بدأ يغزو مجتمعاتنـــا مـــع زيادة استخدام الأنظمة المعلوماتية في مناحي الحياة كلها.

3. أهداف الدراسة:

يسعى هذا البحث إلى تحقيق هدفه الرئيسي والمتمثل في محاولة تقديم دراســـة تبين لنا ما المقصود بالمجرم المعلوماتي وذلك من خلال خصائص هـــذا المجـــرم ودافعه وفئات المجرم المعلوماتي.

محاولة الكشف على السلوك الإجرامي للمجرم المعلوماتي والأساليب الحديثـــة والمبتكرة في ارتكابه للجريمة من خلال استعراض مجموعة من الجرائم التي يسعى المجرم إلى ارتكابها ومعرفة موقف القانون الجزائري على وجه الخصـــوص فـــي مواجهة هذه السلوك الإجرامي المتبع من طرف المجرم المعلوماتي.

كما يسعى هذا البحث في النظر في مدى كفاية النصوص التشريعية القديمة في استيعاب هذا النوع المستحدث من الجرائم.

4. الدارسات السابقة:

بدأت الدارسات العربية في مجال جرائم المساس بأنظمة الكمبيوتر متأخرة بما هو عليه الحال في الدارسات الأجنبية التي رافقت انتشار الكمبيوتر ومن ثم ثـــورة الانترنت، وربما يعود سبب ذلك بشكل رئيسي إلى تأخر التقنية الحديثة في معظـــم الدول العربية ومنها الجزائر، ومن بين الدراسات المتخصصة في هذا المجال:

- رسالة ماجستير أنجزت من طرف الباحثة قـــارة آمـــال بعنـــوان الجريمـــة المعلوماتية، الجزائر، بن عكنون، 2002.
- رسالة ماجستير أنجزت من طرف الباحث العـــزام احمـــد حســـين بعنـــوان الحكومة الالكترونية في الأردن إمكانيات التطبيق، الأردن، 2001.

5. إشكالية الموضوع:

مع التطور التقني لأساليب ارتكاب الجرائم من طـــرف المجـــرم المعلومـــاتي يهدف هذا البحث إلى محاولة الإجابة على الإشكالية التالية:

فيمـــا تتمثل الأفعال الإجرامية التـــي تجســـد الســـلوك الإجرامـــي للمجـــرم المعلوماتي ؟

وسنحاول الإجابة عن ذلك من خلال الإجابة عن التساؤلات الآتية:

- ما هـــي الأنماط الأكثر شـــيوعا لجريمـــة المســـاس بأنظمـــة الكمبيوتـــــر والانترنت ؟
- من هم مرتكبي جرائم المعلوماتية ؟ وهل هم من مجرمين العادين ؟ ما هـــي دوافع المجرم المعلوماتي لارتكاب هذا السلوك ؟ كيف نواجه مرتكبي هـــذه الجرائم هل بحرمانهم من استخدام جهـــاز الحاســـوب ؟ أو الاســـتفادة مـــن خبراتهم في تطوير الأنظمة المعلوماتية ؟

- هل تكفي النصوص الجزائية التقليدية لمواجهة هذا السلوك الإجرامي المستحدث ؟
- ما مدى استيعاب المشرع الجزائري لمخاطر الظاهرة الإجرامية ؟

6. المناهج المتبعة:

أحاول من خلال هذا البحث بشكل مجمل تقديم صورة عامة لأبرز التحديات المصاحبة لشبكة الانترنت، وفق منهجية تطمح إلى تقديم نظرة للظاهرة الإجرامية على الشبكة المعلوماتية، ونظرا لطبيعة الموضوع، وغايته المتمثلة في محاولة تأصيل المفاهيم وسلوكيات المجرم المرتبطة بالظاهرة محل البحث سأعتمد على المنهج الوصفي التحليل، وذلك بوصف الجريمة والمجرم المعلوماتي وتحديد خصائصه وسماته ودوافعه إلى ارتكاب الجريمة، والمنهج التحليلي وذلك بذكر السلوك الإجرامي للمجرم المعلوماتي وتحليل الأساليب المعتمدة من طرفه والمرتكبة بواسطة المعلوماتية أو تكنولوجيا المعلومات.

ولمقتضيات البحث سأعتمد كذلك في بعض الأحيان على المنهج المقارن، وذلك لمعرفة الإجراءات المتخذة في بعض التشريعات لمواجهة هذا السلوك الإجرامي.

7. الصعوبات المعترضة:

وجهت أثناء إعداد هذه الدراسة عدة صعوبات أهمها قلة المراجع المتخصصة في المكتبة الجامعية في الجزائر حول الجرائم المعلوماتية وهذا باعتبارها من الجرائم المستحدثة، كما أن لكل تطور تقني انعكاساته على المستوى القانوني.

وحتى وان تمكنت من الحصول على بعض المراجع فإنها لا تتناول الموضوع في التشريع الجزائري.

وكذلك ندرة التطبيقات القضائية في هذا المجال، نظرا لحداثة الموضوع علـــى الساحة القانونية في الجزائر، ولاتصاله كذلك بالجانـــب التقنـــي والفنـــي بالنظـــام المعلوماتي بشقيه المادي والمعنوي أضف إلى ذلك فإن السلوكيات المرتكبـــة مـــن طرف المجرم المعلوماتي والتي تعبر عنها الجرائم المرتكبة لا يمكن حصرها، كما أن الفقه حتى هذه اللحظة لم يتبنى أو يأخذ معيارا موحدا وثابتا لتصـــنيف المجـــرم المعلوماتي أو تصنيف سلوكياته، فهناك من الفقه من صنفها إلى جـــرائم ســـلوك و نتيجة أولا، وجرائم سلوك مجرد ثانيا، وجانب آخر صنفها إلى جرائم تقع على الذمة المالية وأخرى تقع على الأشخاص، وآخرون صنفوها إلى جرائم يستخدم فيها النظام المعلوماتي وسيلة للاعتداء، وأخرى يكون فيها النظام المعلوماتي محلا للاعتـــداء، وهو التصنيف الذي اعتمدته في بحثي المتواضع هذا.

وفي سبيل إعداد هذا البحث ارتأيت تقسيم هذه الدراسة إلى ثلاثة فصول:

حيث نعرض في الفصل الأول الإطار المفاهيمي للجريمة المعلوماتية وذلك من خلال تناول تعريف الجريمة المعلوماتية وتحديد خصائصها هذا من خلال المبحـــث الأول، أما في المبحث الثاني فتطرقت إلى المجرم المعلوماتي وحاولت إلقاء الضوء على أنماط و فئات ودافع ارتكابه لهذا السلوك.

ولأن الإشكالية الأساسية تدور حول البحث عن الأفعال الإجرامية التي تجســـد هذا السلوك الإجرامي للمجرم المعلوماتي، فقد تم تخصيص الفصل الثاني في البحث عن سلوكيات المجرم المعلوماتي المرتكبة بواسطة المعلوماتية وقسمته بدوره إلـــى ثلاثة مباحث، تناولت في المبحث الأول الجرائم المرتبطة بالذمة الماليـــة والثـــاني

خصصته لدراسة الجرائم المتصلة بالحياة الخاصة وأخطار بنوك المعلومـــات، أمـــا المبحث الثالث فتناولت فيه الدخول والبقاء غير المصرح أو غير المشـــروع علـــى النظام المعلوماتي.

أما الفصل الثالث فقد عرضت فيه مختلف ســـلوكيات المجـــرم المعلومـــاتي المرتكبة على تكنولوجيا المعلومات وذلك بالكشف عن الجرائم المعلوماتيـــة التـــي يكون فيها النظام المعلوماتي محلا للاعتداء وهذا من خلال أربعـــة مباحـــث: الأول تطرقت فيه لسرقة المال المعلوماتي المعنوي، أما المبحث الثاني فخصصته لجريمة إتلاف المعومات والمبحث الثالث تناولت فيه جريمة التزوير المعلوماتي، أمـــا فـــي المبحث الرابع فخصصته للوضع القانوني لمكافحة هذا الســـلوك المســـتحدث فـــي الجزائر.

وأنهيت البحث بخاتمة ضمنتها النتائج المتوصل إليها، ثم ما تراءى لنـــا بعـــد الدراسة من اقتراحات.

الفصل الأول

الإطار المفاهيمي للجريمة المعلوماتية

في ظل عصر السرعة وثورة المعلوماتية لا يستطيع أحد أن ينكر أهمية الإنترنت، أحد أهم دعائم تكنولوجيا الاتصال والمعلومات. ولكن هناك على الجانب الأخر آثار سلبية من أهمها ظهور نوع جديد من الجرائم يدعى بجرائم المعلوماتية، ونتيجة لحداثة هذه الجريمة فقد كانت هناك اتجاهات مختلفة في تعريفها، كما أنها اتسمت بمجموعة من الخصائص والسمات التي ميزتها عن غيرها من الجرائم الأخرى، كما أفرزت معها طائفة جديدة من المجرمين أصطلح على تسميتهم بمجرمي المعلوماتية،والمجرم المعلوماتي ليس كأي مجرم بل هو مجرم متخصص ومحترف ولا يميل إلى استخدام العنف، إذ يعتمد على أساليب تتسم بالهدوء وذات فعالية كبيرة ومؤثرة. فهذا التطور المتسارع في ثورة المعلومات خلف صور جديدة للسلوك الإجرامي.

وفي هذا الفصل سوف أتناول تعريف الجريمة المعلوماتية وأهم الخصائص التي تميزها عن غيرها من الجرائم، كما سأتطرق إلى دراسة المجرم المعلوماتي من حيث سماته ودوافعه.

المبحث الأول: مفهوم الجريمة المعلوماتية وخصائصها

تعتبر الجرائم المعلوماتية أحد أهم ثمار التقدم السريع في شتى المجالات العلمية التي يتميز بها عصرنا الحاضر، فلقد صاحب التقدم الكبير في مجال العلوم والتقنية واستخداماتها لخير البشرية، تقدم أخر وموازي في مجال الجريمة.[1]

عصر الانترنت أو عصر السموات المفتوحة أو عصر التكنولوجيا الرقمية أو عصر المعلوماتية، كل هاته الأوصاف أنما تعبر عن مدى ضخامة القفزات العلمية

[1] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت، طبعة أولى، منشورات الحلبي الحقوقية، سوريا، 2007، ص. 15.

الهائلة التي تحققت ومدى تنوع الانجازات التي طرحت ثمارها بشكل ملحوظ في حياتنا في الفترة الأخيرة، ويبدوا بالفعل أن تكنولوجيا المعلومات هي وقود الثورة الصناعية الثالثة، وأن المعلومات في حد ذاتها هي المادة الخام الأساسية للإنتاج التي يعتمد المجتمع على تحصيلها والاستفادة منها، هذا الوجه المشرق لتقنية المعلومات يقابله من الجانب الأخر وجه مظلم الذي تمثل في الإجرام المعلوماتي والذي كان موجودا ليستغل هذه التقنيات المتطورة لتحقيق مصالح ومأرب تتنوع وتتعدد.[1]

المطلب الأول: تعريف الجريمة المعلوماتية

قبل التطرق إلى تعريف الجريمة المعلوماتية لابد أن نشير إلى انه لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها، فالبعض يطلق عليها جريمة الغش المعلوماتي، والبعض الأخر يطلق عليها جريمة الاختلاس المعلوماتي أو الاحتيال المعلوماتي، والبعض الأخر يطلق عليها الجريمة المعلوماتية.[2]

وهناك جانب يرى أن هذه الجريمة ناشئة أساسا من التقدم التكنولوجي ومدى التطور الذي يطرأ عليه، فهو متجدد بصفة دائمة ومستمرة وخاصة في مجال تكنولوجيا المعلومات، ويفضل أن يطلق عليها اصطلاح "جرائم التكنولوجيا الحديثة" التي تعتمد أساسا على الحواسيب وغيرها من الأجهزة التقنية قد تظهر في المستقبل، وهي كذلك جرائم حديثة نظرا لحداثتها النسبية من جهة، وارتباطها الوثيق بما قد

[1] احمد هلالي عبد اللاه، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، دار النهضة العربية، القاهرة، 2003، ص. 12.
[2] المعلوماتية هي كلمة مكونة من مقطعين، المقطع الأول Information والمقطع الثاني Automatique ويرجع الفضل في اقتراح مصطلح المعلوماتية إلى الأستاذ Drefus حيث استخدمه عام 1962 لتمييز المعالجة الآلية للمعلومات وتبنته بعد ذلك الأكاديمية الفرنسية في ابريل 1966، ومنحته التعريف الأتي "علم المعالجة المنطقية للمعلومات التي تعتبر بمثابة دعامة للمعارف الإنسانية والاتصالات في المجالات الفنية، الاقتصادية والاجتماعية، وذلك باستخدام معدات إلية". انظر سامي الشوى، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1994، ص. 4.

يظهر من أجهزة حديثة تكون ذات طاقة تخزينية وسرعة فائقة ومرونة في التشغيل.[1]

وفي الواقع فان الاتجاه الغالب يفضل استعمال اصطلاح الجريمة المعلوماتية على الجرائم المتعلقة بالحاسوب والانترنت، فاصطلاح الجرائم المعلوماتية عام ويشمل التقنيات الحالية والمستقبلية.

تعتبر التكنولوجيا الحديثة لا سيما تحديدا التكنولوجيا المتعلقة بتقنيات الحاسوب والانترنت متطورة ومتسارعة النمو، الأمر الذي يجعل من الصعب حصر صور الجرائم المعلوماتية وأنواعها، وفي هذا الإطار آثر المشرع الانجليزي في قانون إساءة استخدام الحاسوب عام 1990م عدم وضع تعريف محدد لجرائم الحاسوب، بغية عدم حصر القاعدة التجريمية في إطار أفعال معينة، تحسبا للتطور العلمي والتقني في المستقبل.[2]

في إطار تعريف الفقه للجريمة المعلوماتية نجد أن الاتجاهات متباينة في هذا السياق بين موسع لمفهوم الجريمة المعلوماتية ومضيق لمفهومها.

الفرع الأول: الاتجاه المضيق لمفهوم الجريمة المعلوماتية

من التعريفات المضيقة لمفهوم الجريمة المعلوماتية تعريفها على أنها "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازم لارتكابه، من ناحية لملاحقته وتحقيقه من ناحية أخرى".[3] وحسب هذا التعريف يجب أن تتوفر معرفة كبيرة بتقنيات الحاسوب ليس فقط لارتكاب الجريمة بل كذلك لملاحقتها والتحقيق فيها، وهذا التعريف يضيق بدرجة كبيرة من الجريمة المعلوماتية.

[1] عفيفي كامل، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية، دار الجامعة الجديدة، الإسكندرية، 2000، ص. 20.
[2] المناعسة، أسامة، الزعبي، جرائم الحاسب الآلي والانترنت، دار وائل للنشر، عمان، 2001، ص. 73.
[3] قورة نائلة، جرائم الحاسب الاقتصادية، دار النهضة العربية، القاهرة، 2004، ص. 21.

وكذلك عرفت الجريمة المعلوماتية أنها "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب، أو هي الفعل الإجرامي الذي يستخدم في اقترافه الحاسوب باعتباره أداة رئيسية".[1]

يرى الأستاذ Tredmann أن "الجريمة المعلوماتية تشمل أي جريمة ضد المال مرتبطة باستخدام المعالجة الآلية للمعلومات".[2]

ويرى الأستاذ Mass أن المقصود بالجريمة المعلوماتية "الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح".[3]

وعرفها الأستاذ Rosenblatt على أنها "نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو الوصول أو التي تحول عن طريقه".[4]

ومن الواضح فان هذا التعريف يضيق من مفهوم الجريمة المعلوماتية إذ يخرج من نطاقها العديد من الأفعال غير المشروعة التي يستخدم الحاسب أداة لارتكابها.

الفرع الثاني: الاتجاه الموسع لتعريف الجريمة المعلوماتية

ومقابل ذلك فان هناك تعريفات حاولت التوسع في مفهوم الجريمة المعلوماتية، فعرفها البعض أنها "كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية، يهدف إلى الاعتداء على الأموال المادية أو المعنوية".[5]

[1] احمد هلالي عبد اللاه، مرجع سابق، ص. 13.
[2] المرجع نفسه.
[3] المرجع نفسه، ص. 12.
[4] يونس عرب، دليل امن المعلومات والخصوصية- الجزء الأول- جرائم الكومبيوتر والانترنت، اتحاد المصارف العربية، الأردن، 2002، ص. 213.
[5] سامي الشوى، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1994، ص. 4.

وتم تعريفها كذلك أنها "كل سلوك سلبي أو ايجابي يتم بموجبه الاعتداء على البرامج أو المعلومات للاستفادة منها بأي صورة كانت".[1]

وقد عبر خبراء المنظمة الأوربية للتعاون الاقتصادي عن الجريمة المعلوماتية أنها "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها".[2]

وفي تقرير الجرائم المتعلقة بالحاسوب أقر المجلس الأوربي أنه تتحقق المخالفة (الجريمة) في كل حالة يتم فيها "تغيير معطيات أو بيانات أو برامج الحاسوب أو محوها أو كتابتها أو أي تدخل أخر في مجال انجاز البيانات أو معالجتها، وتبعا لذلك تسببت في ضرر اقتصادي، أو فقد حيازة ملكية شخص آخر، أو بقصد الحصول على كسب اقتصادي غير مشروع له آو لشخص آخر".[3]

ويتبنى الخبير الأمريكي Don Parker مفهوما واسعا للجريمة المعلوماتية، حيث يشير إلى أنها "كل فعل إجرامي متعمد أي كانت صلته بالمعلوماتية، ينشا عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل".[4]

كذلك يعرف الأستاذ Vivant والأستاذ Lestanc الجريمة المعلوماتية أنها "مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب".[5]

كما عرفت هذه الجريمة على أنها "سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة جرمية محله معطيات الحاسوب".[6]

---

[1] الهيتي محمد حماد، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع، عمان، 2004، ص. 152.
[2] قورة نائلة، مرجع سابق، ص. 23.
[3] السعيد كامل، جرائم الكومبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، دار النهضة العربية، القاهرة، 1993، ص. 324.
[4] أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية، 2008، ص. 25.
[5] سامي الشوى، مرجع سابق، ص. 6.
[6] محمود احمد عبابنة، محمد معمر الرازقي، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، 2005، ص. 17.

أما مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين فقد تبنى التعريف الأتي للجريمة المعلوماتية "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية".[1]

والملاحظ من هذا المفهوم أو التعريف انه حاول الإلمام والإحاطة قدر الإمكان بجميع الأشكال الإجرامية للجريمة المعلوماتية، سواء التي تقع بواسطة النظام المعلوماتي، أو داخل هذا النظام، على المعطيات والبرامج والمعلومات، كما شمل التعريف جميع الجرائم التي من الممكن أن تقع في بيئة الكترونية، فهذا المفهوم لم يركز على مرتكب الجريمة ومقدرته التقنية، ولا على وسيلة ارتكاب الجريمة أو على الغاية والنتيجة التي تسعى لها الجريمة المعلوماتية، بل أنه حاول عدم حصر الجريمة المعلوماتية في مجال محدد يتيح للعديد من صور هذه الجريمة الإفلات من دائرة العقاب.

ووفقا لكل ما سبق يمكن أن نعرف جرائم الحاسب الآلي بأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المعنوية (معطيات الحاسب) يكون ناتجا بطريقة مباشرة وغير مباشرة لتدخل التقنية المعلوماتية، فهذا التعريف يستند على أكثر من معيار لتحديد ماهية الجرائم المعلوماتية، فالمعيار الأول تمثل في إيراد التعريف للسلوك (كل فعل أو امتناع)، والمعيار الثاني طبيعة المحل أو موضوع الاعتداء (الأموال المعنوية)، والمعيار الثالث هو اتصال السلوك بمحل الاعتداء عن طريق تدخل التقنية المعلوماتية، فهذا التعريف جاء شاملا قائما على عدة معايير مجتمعة، لا هو بالمضيق ولا هو بالموسع، وهو حاليا يعد تعريفا مطلوبا ولو إلى

[1] مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين الذي عقد في فيينا بتاريخ 10 نيسان سنة 2000، انظر المناعسة، أسامة، الزعبي، مرجع سابق، ص. 78.

حين، وسبب ذلك أن هذه الجرائم في تطور مستمر بتطور التقنية المعلوماتية، الأمر الذي قد يؤدي إلى تصور مختلف إلى هذه الوقائع غير المشروعة.[1]

وبغض النظر عن كل هذا، فان هذا النوع من الجرائم قد تختلف، وهي تختلف فعلا عن بقية الجرائم، سواء بالنظر إلى طبيعتها الخاصة أوالى دوافع ارتكابها.

المطلب الثاني: خصائص الجريمة المعلوماتية

أدى ارتباط الجريمة المعلوماتية بجهاز الحاسوب وشبكة الانترنت إلى إضفاء مجموعة من الخصائص والسمات المميزة لهذه الجريمة عن الجرائم التقليدية ويمكن إجمالها في ما يلي:

الفرع الأول: الجريمة المعلوماتية متعددة الحدود (جريمة عابرة للدول)

المجتمع المعلوماتي لا يعترف بالحدود الجغرافية ولا يعيرها أي اهتمام فهو مجتمع منفتح عبر شبكات تخترق المكان والزمان دون أن تخضع لحرس الحدود، فبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالمقدرة التي تتمتع بها الحواسيب وشبكاتها من نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها ألاف الأميال قد أدت إلى نتيجة تتمثل في أن أماكن متعددة في دول مختلف قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد.[2]

[1] قورة نائلة، مرجع سابق، ص. 47.
[2] Ulrich Sieber، جرائم الكومبيوتر والجرائم الأخرى في مجال المعلومات، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، ترجمة سامي الشوى، دار النهضة العربية، القاهرة، 1993، ص. 58.

فالسهولة في حركة المعلومات عبر أنظمة وبرامج التقنية الحديثة جعل بالإمكان ارتكاب جريمة عن طريق الحاسوب موجود في دولة معينة بينها يتحقق الفعل الإجرامي في دولة أخرى.

هذه الخاصية التي تتميز به الجريمة المعلوماتية كونها جريمة عابرة للحدود خلقت العديد من المشاكل حول تحديد الدولة صاحب الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب التطبيق بالإضافة إلى إشكاليات تتعلق بإجراء الملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام.

تعتبر القضية المعروفة باسم مرض نقص المناعة المكتسبة من القضايا التي لفتت النظر إلى البعد الدولي للجرائم المعلوماتية، و تتلخص وقائع هذه القضية التي وقعت عام 1989م في قيام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج الذي هدف في ظاهره إلى إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة، إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس (حصان طروادة)، إذ كان يترتب على تشغيله تعطيل جهاز الحاسوب عن العمل ثم تظهر بعد ذلك عبارة على شاشة الحاسوب يقوم الفاعل من خلالها بطلب مبلغ مالي يرسل على عنوان معين حتى يتمكن المجني عليه من الحصول على مضاد الفيروس وفي الثالث من فبراير من سنة 1990 تم إلقاء القبض على المتهم (جوزيف بوب) في ولاية (أوهايو) بالولايات المتحدة الأمريكية، وتقدمت المملكة المتحدة بطلب لتسليمه لها لمحاكمته أمام القضاء الانجليزي، حيث أن إرسال هذه البرامج قد تم من داخل المملكة المتحدة، وبالفعل وافق القضاء الأمريكي على تسليم المتهم، وتم توجيه إحدى عشر تهمة ابتزاز إليه وقعت معظمها في دول مختلفة، إلا أن إجراءات

محاكمة المتهم لم تستمر بسبب حالته العقلية، ومهما كان الأمر فان لهذه القضية أهميتها من أمرين أو ناحيتين:[1]

- الأولى: أنها المرة الأولى التي يتم فيها تسليم متهم في جريمة معلوماتية.
- الثانية: أنها المرة الأولى التي يقدم فيها شخص للمحاكمة بتهم إعداد برنامج خبيث (فيروس).

ونتيجة لهذه الطبيعة الخاصة للجريمة المعلوماتية، ونظرا للخطورة التي تشكلها على المستوى الدولي، والخسائر التي تتسبب بها، ظهرت الأصوات الداعية إلى التعاون الدولي المكثف من أجل التصدي لهذه الجرائم.[2] والتعاون الدولي يتمثل في المعاهدات والاتفاقيات الدولية التي تعمل على توفير جو من التنسيق بين الدول الأعضاء، الأمر الذي يؤدي بالإيقاع بمجرمي المعلوماتية وتقديمهم للقضاء العادل.

تكمن أهم المشاكل المتعلقة بالتعاون الدولي حول الجريمة المعلوماتية، في أنه لا يوجد هناك مفهوم عام، مشترك بين الدول حول صور النشاط المؤدي أو المكون لهذه الجريمة، بالإضافة إلى نقص الخبرة لدى الشرطة وجهات الادعاء والقضاء في هذا المجال لتفكيك وتحليل عناصر الجريمة إن وجدت، وجمع الأدلة عنها للإدانة، فكل هذا يشكل عائقا كبيرا أمام التعاون في مجال مكافحة هذا النوع من الجرائم.[3]

---

[1] قورة نائلة، مرجع سابق، ص. 48.

[2] تجدر الإشارة في هذا المجال إلى مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاقبة المجرمين، والذي عقد في (هافانا) عام 1990، وفي قراره المتعلق بالجرائم ذات الصلة بالحاسوب ناشد المؤتمر الدول الأعضاء أن تكثف من جهودها كي تكافح بمزيد من الفاعلية عمليات إساءة استخدام الحاسوب، والتي تستدعي تطبيق جزاءات جنائية على الصعيد الوطني، بما في ذلك النظر إذا دعت الضرورة في تحديث القوانين والإجراءات الجنائية، واتخاذ تدابير من اجل ضمان أن الجزاءات والقوانين الراهنة بشان سلطات التحقيق وقبول الأدلة في الإجراءات القضائية تنطبق على الجرائم المعلوماتية، وإدخال تغييرات مناسبة عليها إذا دعت الضرورة، كما حث المؤتمر الدول الأعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي من اجل مكافحة الجرائم المتصلة بالحاسبات، بما في ذلك دخولها حسب الاقتضاء أطرافا في المعاهدات المتعلقة بتسليم المجرمين، وتبادل المساعدة في المسائل المرتبطة بالجرائم ذات الصلة بالحاسوب، انظر محمد معمر الرازقي، محمود احمد عبابنة، مرجع سابق، ص. ص. 361- 362.

[3] عوض محمد محي الدين، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، القاهرة، 1993، ص. 35.

وبالتالي،و من أجل التصدي للإجرام المعلوماتي، لابد أن تعمل الدول في اتجاهين:

- الأول: داخلي حيث تقوم الدول المختلفة بسن القوانين الملائمة لمكافحة هذه الجرائم.
- الثانية: دولي عن طريق عقد الاتفاقيات الدولية، حتى لا يستفيد مجرموا المعلوماتية من عجز التشريعات الداخلية من ناحية، وغياب الاتفاقيات الدولية التي تهدف لحماية المجتمع الدولي من نتائج وأثار هذه الجرائم.[1]

الفرع الثاني: صعوبة اكتشاف الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بصعوبة اكتشافها، وإذا ما اكتشفت فان ذلك يكون بمحض الصدفة عادة، حيث يبدو من الواضح أن عدد الحالات التي تم فيها اكتشاف هذه الجريمة قليلة إذا قورنت بما يتم اكتشافه مع الجرائم التقليدية.[2]

ويمكن رد الأسباب التي تقف وراء الصعوبة في اكتشاف الجريمة المعلوماتية إلى عدم ترك هذه الجريمة لأي اثر خارجي بصورة مرئية، فلا يوجد جثث لقتلى ولا أثار للدماء، كما أن المجرم يمكنه ارتكاب هذه الجريمة في دول وقارات مختلفة، إذ أن الجريمة المعلوماتية كما سبق واشرنا (جريمة عابرة للدول)، وكذلك فان قدرة

[1] من صور التعاون الفعال في مجال مكافحة الجريمة المعلوماتية، يمكن الإشارة إلى اتفاقية (بودابست) Budapest والتي حرص فيها مجلس أوربا على التصدي للاستخدام غير المشروع للحواسيب وشبكات المعلومات، وقد وقعت هذه الاتفاقية المتعلقة بالإجرام المعلوماتي في 23 نوفمبر 2001 إيمانا من الدول الأعضاء في هذا المجلس، والدول الأخرى الموقعة على هذه الاتفاقية بالتغيرات العميقة التي حدثت بسبب الرقمية. وتشير المذكرة التفسيرية لهذه الاتفاقية إلى أن "... سهولة الوصول إلى المعلومات في النظم المعلوماتية مع الإمكانيات اللامحدودة لتبادلها وإرسالها بصرف النظر عن المجالات الجغرافية، أدى إلى نمو هائل في حجم المعلومات المتاحة التي يمكن الحصول عليها بسهولة، ومن خلال الاتصال بخدمات الاتصالات والمعلومات يستطيع المستخدمون اصطناع فضاء جديد يسمى الفضاء المعلوماتي (Cyber Space) الذي يستعمل أساسا لأغراض شرعية ولكن يمكن أن يخضع لسوء الاستخدام، إذا أن هناك احتمالا لاستخدام شبكات الحاسوب والمعلومات الالكترونية في ارتكاب أعمال إجرامية. وعلى ذلك يجب على القانون الجنائي أن يحافظ على مواكبته لهذه التطورات التكنولوجية التي تقدم فرصا واسعة لإساءة استخدام إمكانيات الفضاء المعلوماتي وان يعمل على ردع هذه الأفعال الإجرامية، مع تطبيق السلطات القهرية المقررة في بيئة تكنولوجيا المعلومات. انظر احمد هلالي عبد اللاه، مرجع سابق، ص. ص. 29- 30.

[2] جميل عبد الباقي، القانون الجنائي والتكنولوجيا الحديثة، طبعة أولى، دار النهضة العربية، القاهرة، 1992، ص. 17.

الجاني على تدمير دليل الإدانة في قل من الثانية الواحدة يشكل عاملا إضافيا في صعوبة اكتشاف هذا النوع من الجرائم.[1]

فالجرائم المعلوماتية في أكثر صورها خفية لا يلاحظها المجني عليه، ولا يدري حتى بوقوعها، والإمعان في حجب السلوك المكون لها وإخفائه عن طريق التلاعب غير المرئي في الذبذبات الالكترونية التي تسجل البيانات عن طريقها أمر ليس بالعسير في الكثير من الأحيان بحكم المعرفة والخبرة في مجال الحاسبات غالبا لدى مرتكبيها.

ويكون للمجني عليه دورا أساسيا كذلك في صعوبة اكتشاف وتحديد نوع الجريمة المعلوماتية، حيث تحرص أغلب الجهات التي تتعرض أنظمتها المعلوماتية للقرصنة والانتهاك على عدم الكشف حتى بين موظفها عما تعرضت له، وتكتفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها، وتشير بعض التقديرات إلى أن ما يتراوح بين 20 و25% من جرائم الحسابات لا يتم الإبلاغ عنها مطلقا، خشية الإساءة إلى سمعة المؤسسة أو المصنع.[2] ويرى البعض أن للمجني عليه كذلك دورا مثيرا للريبة في بعض الأحيان، فهو قد يشارك بطريقة غير مباشرة في ارتكاب الفعل، وذلك بسبب وجوده في ظروف تجعل تعرضه للجريمة المعلوماتية أمرا مرتفعا بشكل كبير، ويرجع ذلك بشكل أساسي إلى القصور الأمني الذي يعتري الأنظمة المعلوماتية.

ويبدوا أن إحجام المجني عليه عن الإبلاغ عن وقوع الجرائم المعلوماتية أكثر وضوحا في المؤسسات المالية مثل البنوك والمؤسسات الادخارية ومؤسسات

[1] المرجع نفسه.
[2] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، عمان، 2008، ص. 55.

الاقتراض والسمسرة، حيث تخشى مجالس إداراتها من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم، أو اتخاذ الإجراءات القضائية حيالها، إلى تضاؤل الثقة فيها من جانب المتعاملين معها، حيث أن الجانب الأكبر من الجرائم المعلوماتية لا يتم الكشف أو التبليغ عنه. وهذا ما يؤثر بدوره على السياسة التي يمكن أن توضع لمكافحتها، وقد تم طرح عدة اقتراحات تكفل تعاون المجني عليه في كشف هذه الجرائم، وبالتالي إنقاص حجم الإجرام المعلوماتي الخفي، ومن بين الاقتراحات التي طرحت لحمل المجني عليه على التعاون مع السلطات في الولايات المتحدة الأمريكية مطالبة البعض بأن تفرض النصوص المتعلقة بجرائم الحاسبات التزاما على عاتق موظفي الجهة المجني عليها بالإبلاغ عما يصل علمهم به من جرائم في هذا المجال، مع تقرير خبراء على الإخلال بمبدأ الالتزام، غير أن هذا الاقتراح لقي رفضا، لأنه ليس من المقبول تحويل المجني عليه إلى مرتكب للجريمة.[1]

ومما يزيد الأمر تعقيدا أن هؤلاء القراصنة لا يهاجمون من أجهزة الحاسب الخاصة بهم، وإنما يدخلون إلى شبكات بعيدة عنهم ويهاجمون من خلالها.[2]

الفرع الثالث: صعوبة إثبات الجريمة المعلوماتية

يعتبر اكتشاف الجريمة المعلوماتية -أمر كما سبق وذكرنا- ليس بالهين والسهل، ولكن حتى في حال اكتشافها والإبلاغ عنها، فان إثباتها أمر تحيط به الكثير من الصعاب، فالجريمة المعلوماتية تتم في محيط غير تقليدي حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والانترنت مما يجعل الأمور تزداد صعوبة وتعقيدا لدى سلطات الأمن وأجهزة التحري والتحقيق والملاحقة، ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات الكترونية غير مرئية تنساب

[1] نهلا عبد القادر المومني، المرجع نفسه، ص. 55.
[2] محمد معمر الرازفي، محمود احمد عبابنة، مرجع سابق، ص. 37.

عبر النظام المعلوماتي، مما يجعل أمر محو الدليل وطمسه آليا من قبل المجرم أمرا في غاية البساطة والسهولة.[1]

وتجدر الإشارة إلى أن وسائل المعاينة وطرقها التقليدية لا تفلح في غالب الأحيان في إثبات هذه الجريمة نظرا لطبيعتها الخاصة التي تختلف عن الجريمة التقليدية، فالأخيرة لها مسرح تجري عليه الأحداث، حيث تخلف اثأر مادية تقوم عليها الأدلة، وهذا المسرح يعطي المجال أمام سلطات الاستدلال والتحقيق الجنائي في الكشف عن الجريمة، وذلك عن طريق المعاينة والتحفظ على الآثار المادية التي خلفتها الجريمة، لكن فكرة مسرح الجريمة في الجريمة المعلوماتية يتضاءل ويتلاشي دوره في إظهار الحقائق المؤدية للأدلة والبراهين المطلوبة، ويرجع ذلك لسببين اثنين هما:

- الأول: الجريمة المعلوماتية لا تخلف أثارا مادية.
- الثاني: إن كثيرا من الأشخاص يتعاقبون على مسرح الجريمة خلال الفترة من زمان وقوع الجريمة وحتى اكتشافها أو التحقيق فيها، وهي مدة طويلة نسبيا، الأمر الذي يعطي مجالا واسعا للجاني أو للآخرين أن يغيروا أو يتلفوا ويعبثوا بالآثار المادية إن وجدت، الأمر الذي يورث الشك في دلالة الأدلة المستقاة من المعاينة في الجريمة المعلوماتية.[2]

ومن الأمور التي زادت الأمر صعوبة وتعقيدا نقص الخبرة الفنية والتقنية لدى الشرطة وجهات الادعاء والقضاء، فهذا الأمر يشكل عائقا أساسيا أمام إثبات الجريمة المعلوماتية، ذلك أن هذا النوع من الجرائم يتطلب تدريب وتأهيل هذه

[1] محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2001، ص. 103.
[2] المعاينة يقصد بها إثبات حالة الأماكن والأشخاص والأشياء وكل ما يعتبر في كشف الحقيقة والمعاينة بهذا المعنى يستلزم الانتقال إلى محل الواقعة أو أي محل أخر توجد به أشياء أو أثار يرى المحقق أن لها صلة بالجريمة، انظر حجازي عبد الفتاح بيومي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت، الطبعة الأولى، دار الكتب القانونية، القاهرة، 2002، ص. 59.

الجهات في مجال تقنية المعلومات وكيفية جمع الأدلة والتفتيش والملاحظة في بيئة الحاسوب والانترنت، ونتيجة لنقص الخبرة وعدم إمكانية الشرطة في تقدير أهمية الجريمة المعلوماتية، فلا تبذل لكشف غموضها وضبط مرتكبيها جهودا تتناسب وهذه الأهمية، بل أن المحقق قد يدمر الدليل لمحوه محتويات الاسطوانة الصلبة عن خطا منه أو إهمال أو بالتعامل بخشونة مع الأقراص المرنة.[1]

وفي الأخير يمكن إجمال صعوبة إثبات الجريمة المعلوماتية في نقاط خمس، وهي:

- أنها جريمة لا تترك أثر.
- إنها جريمة يصعب فنيا الاحتفاظ بآثارها، إن تركت أثرا.
- إنها جريمة يصعب على المحقق التقليدي أن يفهم حدودها الإجرامية، وما تخلفه من أثار غير مرئية.
- إنها جريمة تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبها.
- إنها جريمة تعتمد على قمة الذكاء في ارتكابها.

الفرع الرابع: أسلوب ارتكاب الجريمة المعلوماتية

من خصائص الجريمة المعلوماتية أنها تبرز ذاتيتها بصورة أكثر وضوحا في أسلوب ارتكابها وطريقتها، فإذا كانت الجرائم التقليدية تتطلب نوعا من الجهد العضلي الذي قد يكون في صورة ممارسة العنف والإيذاء، كما هو الحال في جريمة القتل أو الاختطاف، أو في صورة الكسر وتقليد المفاتيح، هو كما الحال في

[1] حجازي عبد الفتاح بيومي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت، الطبعة الأولى، دار الكتب القانونية، القاهرة، 2002، ص. 28.

جريمة السرقة... فان الجرائم المعلوماتية هي جرائم هادئة بطبيعتها، لا تحتاج إلى العنف، بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة، كما تحتاج كذلك إلى وجود شبكة المعلومات الدولية (الانترنت) مع وجود مجرم يوظف خبرته أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو احتراق خصوصيات الغير أو التغرير بالقاصرين، كل ذلك دون الحاجة إلى سفك الدماء.[1]

الفرع الخامس: الجريمة المعلوماتية تتم عادة بتعاون أكثر من شخص

تتميز الجريمة المعلوماتية أنها تتم عادة بتعاون أكثر من شخص على ارتكابها، فغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والانترنت، يقوم بالجانب الفني من المشروع الإجرامي، وشخص أخر من المحيط أو خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه، والاشتراك في إخراج الجريمة المعلوماتية إلى حيز الوجود قد يكون اشتراكا سلبيا، وهو الذي يتضح بالصمت من جانب من يعلم بالجريمة في محاولة منه لتسهيل إتمامها، وقد يكون اشتراكا ايجابيا وهو الغالب في الكثير من الجرائم ويتمثل في المساعدة الفنية أو المادية.[2]

الفرع السادس: خصوصية مجرمي المعلوماتية

يتصف المجرم المعلوماتي بخصائص معينة تميزه عن المجرم الذي يرتكب الجرائم التقليدية (المجرم التقليدي)، فإذا كانت الجرائم التقليدية لا تتطلب مستوى علمي ومعرفي للمجرم في عملية ارتكابها، فإن الأمر يختلف بالنسبة للجرائم

[1] نهلا عبد القادر المومني، مرجع سابق، ص. 58.
[2] المرجع نفسه.

المعلوماتية، فهي جرائم فنية تقنية في الغالب الأعم، والأشخاص الذين يقومون بارتكابها عادة يكونون من ذوي الاختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه حد أدني من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الانترنت، ومثال على ذلك فإن الجرائم المعلوماتية ذات الطابع الاقتصادي مثل التحويل الالكتروني غير المشروع للأموال يتطلب مهارة وقدرة فنية وتقنية عالية جدا من قبل مرتكبيها.[1]

كما أن البواعث على ارتكاب المجرم المعلوماتي لهذا النوع من الجرائم قد تكون مختلفة عن بواعث ارتكاب الجرائم من قبل المجرم التقليدي.

في نهاية هذا المبحث، نقول أنه قد تعددت تعريفات الجريمة المعلوماتية، فهناك من عرفها تعريفا ضيقا، أي أنه يركز على عنصر دون الآخر، وهناك من عرفها تعريفا موسعا، محاولا الإلمام بجميع خصائص هذه الجريمة.

وبما أن جرائم المعلوماتية تتميز عن غيرها من الجرائم بمجموعة من الخصائص، كذلك فإن مرتكبيها يتميزون عن غيرهم من الجناة وهم موضوع بحثنا في المبحث القادم.

[1] المرزوقي محمد محمود، جرائم الحاسب الآلي، المجلة العربية للفقه والقضاء، إصدار الأمانة العامة لجامعة الدول العربية، العدد 28، 2003، ص. 63.

المبحث الثاني: المجرم المعلوماتي

الإنسان كائن مزدوج في طبيعته، خلق من مادة وروح، وأودع فيه نوعان من القوى، نوع تأخذ بيده إلى الخير وأخرى تدفعه إلى الشر، وهذه الحقيقة ذكرها القرآن الكريم، قال تعالى: "ونفس وما سواها، فألهمها فجورها وتقواها، قد أفلح من زكاها، وقد خاب من دساها"، تبع عن ذلك أن للإنسان نوعان من السلوك، ما يتفق مع الأخلاق والقانون والنظام، وما يختلف عنهما.[1]

فقد شهد القرن الماضي ثورة من نوع غير مألوف، اصطلح على تسميتها بثورة المعلومات، أو التقنية الجديدة، والتي أضافت الكثير من الايجابيات في حساباتنا، إلا أنها أفرزت أنماطا جديدة من الجريمة والمجرمين، فكان لتقدم العلوم المختلفة أثره على نوعية الجريمة، وأستغل المجرم تطور الاختراعات العلمية الجديدة لخدمة أهدافه الإجرامية، وبهذا فقد جلبت المعلوماتية نسلا جديدا من المجرمين، اصطلح على تسميتهم بمجرمي المعلوماتية.

والمعلومات ينظر إليها دائما بوصفها أداة محايدة، وأن مصدر ضعفها وانتهاكها هو الإنسان ذاته، فجوهر المشكلة يرتبط بالإنسان وشخصيته ودوافعه، وكما هو معروف فانه لا يمكن لأي عقوبة أن تحقق هدفها سواء في مجال الردع العام أو الردع الخاص ما لم تضع في الاعتبار شخصية المجرم، والذي ينبغي إعادة تأهيله اجتماعيا حتى يعود مرة أخرى مواطنا صالحا في مجتمعه.[2]

[1] نبيل محمد توفيق السمالوطي، الدراسة العلمية للسلوك الإجرامي، دار الشروق، جدة، 1983، ص. 20.
[2] يونس عرب، تطور التشريعات في مجال مكافحة الجرائم الالكترونية، ورقة رقم 4، بحث مقدم إلى هيئة تنظيم الاتصالات، مسقط، سلطنة عمان، بتاريخ 2-4 أفريل 2006، دون ترقيم.

وبعبارة أخرى، وبما أن الصلة وطيدة بين الجريمة والمجتمع، فان القرابة وطيدة بين تطور المجتمع الحضاري والعلمي والتكنولوجي والجريمة، وقد تكون تلك العلاقة بين الجريمة والتطور مثيرة للدهشة ولكن سرعان ما تكشف هذه الدهشة ستارها عندما نعلم أن تطور المجتمع وما يصاحبه من تطور علمي وتكنولوجي ينعكس أثره على تطور الجريمة، فالجريمة باعتبارها إحدى صور إفرازات المجتمع يصلها ما يصل المجتمع من تطور، ومرجع ذلك أن مرتكب الجريمة وضحيتها عضوان في هذا المجتمع ويتأثران بحياته وثقافته وتطوره.[1]

والمجرم المعلوماتي هو كل شخص سواء، طفل، رجل، أنثى، يأتي أفعالا إرادية تشكل سلوكا ايجابيا أو سلبيا باستخدام تقنية المعلوماتية لإحداث نموذج إجرامي بالاعتداء على حق أو مصلحة، وسمات المجرم المعلوماتي تشبه في كثير من الأحيان سمات المجرمين ذوي الياقات البيضاء.[2] حيث أن كل من هؤلاء المجرمين قد يكونوا من ذوي المناصب الرفيعة والمستوى العالي، ومن ذوي التخصصات والكفاءات العالية، ويتمتعون بالذكاء والقدرة على التكيف الاجتماعي في المحيط الذي يعيشون فيه، بل إن بعضهم يتمتع باحترام وثقة عالية من الأشخاص المحيطين بهم في مجال العمل أو في المحيط الاجتماعي.

وسوف أتناول في هذا المبحث دراسة شخصية المجرم المعلوماتي من حيث سماته في المطلب الأول، وأتعرض بعد ذلك إلى أبرز طوائف وفئات مجرمي

---

[1] انظر الموقع الالكتروني:

http://www.chawkitabib.info/spip-php?article477

بتاريخ 16- 07- 2010 على الساعة 15: 17

[2] مصطلح المجرمين ذوي الياقات البيضاء، مصطلح حديث نسبيا، وأول من أطلقه هو عالم الاجتماع "Suther Land" حيث وضح أن هذه الجرائم ترتكب من قبل الطبقة الراقية في المجتمع، ذوي المناصب الإدارية الكبيرة، وتشمل أنواعا مختلفة من الجرائم، كغسيل الأموال وتجارة الرقيق، وتزوير العلامات التجارية وغير ذلك من الجرائم التي يقومون بارتكابها وهم جالسون في مكاتبهم الفخمة. انظر الموقع الالكتروني:

www.minishawi.com

بتاريخ 16- 07- 2010 على الساعة 00: 16

المعلوماتية، وذلك في المطلب الثاني، وأخيرا أوضح أهم الدوافع التي تحمل المجرم المعلوماتي على ارتكاب هذا السلوك الإجرامي، وذلك في المطلب الثالث.

المطلب الأول: السمات الخاصة بالمجرم المعلوماتي

حتى تحقق العقوبة أهدافها، ، يجب أن نضع في الاعتبار شخصية المجرم، وذلك لإعادة تأهيله اجتماعيا حتى يعود مواطنا صالحا مرة أخرى ويندمج مع المجتمع، وينطبق هذا القول على المجرم المعلوماتي مثلما ينطبق على المجرم التقليدي. ويمكن القول بأن المجرم المعلوماتي يتمتع بقدر كبير من الذكاء يميزه عن غيره من المجرمين، واتصافه بسمات معينة جعلت منه محلا للعديد من الأبحاث والدراسات، ويتميز المجرم المعلوماتي بعديد من السمات والخصائص أهمها:

الفرع الأول: المجرم المعلوماتي كانسان يتمتع بالمهارة والمعرفة والذكاء

تحفظ البعض من الفقه حيال رسم صورة عامة للمجرم المعلوماتي متسمة بصفة الذكاء، وذلك على سند من القول أن بعض أنماط الجريمة المعلوماتية مثل إتلاف الحاسوب الآلي أو تدميره كليا أو جزئيا، أو سرقة المعلومات المخزنة داخل الحاسب الآلي، لا تحتاج في مرتكبها أن يكون على قدر كبير من الذكاء.[1]

والواقع أنه لا يمكن وصف كل جريمة تتصل بالحاسب الآلي بأنها نمط من أنماط الجريمة المعلوماتية، حيث أن المقصود بالإجرام المعلوماتي بالمعنى الدقيق هو الإجرام الذي ينشا عن تقنيات التدمير الناعمة التي تتمثل في التلاعب بالمعلومات والكيانات المنطقية (البرامج) فلكي ينشأ هذا النوع من الإجرام فانه يلزم

[1] حاتم عبد الرحمن منصور الشحات، الإجرام المعلوماتي، دار النهضة العربية، القاهرة، 2003، ص. 88.

استخدام تقنية خاصة تتعامل مباشرة مع البرامج أو البيانات ، وهو بذلك يتميز عن الإجرام العنيف الموجود ضد النظام المعلوماتي.[1]

ولهذا يتميز المجرم المعلوماتي غالبا بالذكاء، حيث أن الجريمة المعلوماتية تتطلب مقدرة عقلية وذهنية عميقة، خاصة في الجرائم المالية التي تؤدي إلى خسارة مادية كبيرة تلحق بالمجني عليه، فالمجرم المعلوماتي يستخدم مقدرته العقلية ولا يلجا إلى استخدام العنف أو الإتلاف المادي بل يحاول أن يحقق أهدافه بهدوء، فالإجرام المعلوماتي هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف، فالمجرم المعلوماتي يسعى بشغف إلى معرفة طرق جديدة مبتكرة لا يعرفها أحد سواه، وذلك من أجل اختراق الحواجز الأمنية في البيئة الالكترونية، ومن ثم تحقيق مراده.

الفرع الثاني: المجرم المعلوماتي إنسان اجتماعي

باستطاعتنا القول بأن المجرم المعلوماتي بصفته إنسان ذكي فهو اجتماعي، فهو لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به، بل انه إنسان يستطيع التوافق والتصالح مع مجتمعه، فهو شخص مرتفع الذكاء مما يساعده على عملية التكيف مع المجتمع، فالذكاء في نظر الكثيرين ليس سوى القدرة على التكيف، ولا يقصد بذلك التقليل من شأن المجرم المعلوماتي، بل أن خطورته الإجرامية قد تزداد إذا زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه.[2]

فإحساس المجرم أنه محل ثقة من مجموعته، وشعوره أنه خارج إطار الشبهات قد يدفعه إلى التمادي في ارتكاب جرائمه التي قد لا تكتشف، وإذا اكتشفت

[1] Rose (Philipe), La criminalité informatique, que sais-je, 2eme édition ? Edition P.U.F, Paris, 1995, P. 59.

[2] عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة الكترونيا دراسة مقارنة، دار النهضة العربية، القاهرة، 2010، ص. ص. 80_81.

فإنها تواجه صعوبة في الإثبات ونقص الأدلة ونقص الخبرة لدى المحققين ولدى رجال القضاء.

الفرع الثالث: خوف المجرم المعلوماتي من كشف جريمته

يعرف عن مجرموا المعلوماتية خوفهم من انكشاف جرائمهم وانفضاح أمرهم، وبالرغم من أن هذه الخشية تصاحب المجرمين على اختلاف أنماطهم إلا أنها تميز مجرمي المعلوماتية بصفة خاصة لما يترتب عن كشف أمرهم من فقدان لمراكزهم في الكثير من الأحيان، ويساعد مجرمي المعلوماتية على الحفاظ على سرية أفعالهم طبيعة الأنظمة المعلوماتية نفسها، وذلك أن أكثر ما يعرض المجرم إلى اكتشاف أمره هو أن يستجد أو يطرأ أثناء تنفيذه لجريمته مجموعة من العوامل غير المتوقعة والتي لا يمكن التكهن والتنبؤ بها، في حين أن أهم الأسباب التي تساعد على نجاح الجريمة المعلوماتية هي أن الحواسيب إنما تؤدي عملها غالبا بطريقة آلية، بحيث لا تتغير المراحل المختلفة التي نمر بها.[1]

فخوف المجرم المعلوماتي من انكشاف فعله مرده انتمائه في الغالب الأعم إلى وسط اجتماعي متميز، سواء من حيث التعليم أو الثقافة أو المستوى المهني وطبيعة العمل.

الفرع الرابع: المجرم المعلوماتي يبرر ارتكابه الجريمة

يتولد لدى مرتكب فعل الإجرام المعلوماتي إحساس وشعور بأن ما يقوم به لا يعتبر من عداد الجرائم، أو بمفهوم أخر أنه لا يمكن لهذا العمل والفعل أن يصنف بعدم الأخلاقية وخاصة في الحالات التي يقف فيها السلوك عند حد قهر نظام

[1] قورة نائلة، مرجع سابق، ص. 56.

الحاسوب وتخطي الحماية المفروضة حوله، حيث يميز مرتكبو هذه الجرائم بين الإضرار بالأشخاص الأمر الذي يعدونه غاية في اللا أخلاقية وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم.[1]

يبدوا أن الاستخدام المتزايد لأنظمة المعلوماتية قد أنشأ مناخا نفسيا مواتيا وملائما لتصور استبعاد فكرة الخير والشر وقد ساعد على ذلك عدم وجود احتكاك مباشر بالأشخاص، وما لا شك فيه أن هذا التباعد في العلاقة الثانية بين الفاعل والمجني عليه يسهل المرور إلى الفعل غير المشروع، ويساعد على إيجاد نوع من الإقرار الشرعي بهذا الفعل[2] ففي الكثير من الأحيان يقوم العاملون بالمؤسسات المختلفة باستخدام أجهزة الحاسوب لأغراض شخصية بوصفه سلوكا شائعا بين الجميع، ولا ينظر إليه بوصفه فعلا إجراميا[3] غير أن هذا لا يدل أو يعني أن عدم الشعور بعدم أخلاقية هذه الأفعال الإجرامية المعلوماتية لدى فئة كبيرة من مرتكبيها ينفي وجود مجرمين يرتكبون الإجرام المعلوماتي وهم على علم وإدراك بعدم مشروعية وأخلاقية هذا الفعل، فهناك فئة تملك اتجاه إجرامي خطير، وسوء نية واضحة وهم على دراية عامة بخطورة أعمالهم وأفعالهم.

الفرع الخامس: المجرم المعلوماتي يتمتع بالسلطة اتجاه النظام المعلوماتي

نعني بالسلطة المزايا والحقوق التي يتمتع بها المجرم المعلوماتي، والتي تمكنه من ارتكاب جريمته، فمعظم مجرمي المعلوماتية لديهم سلطة مباشرة أو غير

---

[1] قورة نائلة، المرجع نفسه، ص. 54.

[2] سامي الشوى، الغش المعلوماتي ظاهرة إجرامية مستحدثة، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، القاهرة، ص. 245.

[3] يقول الأستاذ "باركر" وهو احد أهم الباحثين الذين اهتموا بالجريمة المعلوماتية بشكل عام وبالمجرم المعلوماتي بشكل خاص، أن الفاعل في هذه الجرائم لا يتصور أن سلوكه يمكن أن يتصف بالعمل الإجرامي، وانه سيتبع ذلك توقيع عقاب عليه، فمن خلال لقائه بشخصين من المحكوم عليهم بسبب استعمال الحواسيب الخاصة برؤسائهم لأغراض شخصية، وهو ما يندرج تحت جريمة الاستعمال غير المصرح به للنظام المعلوماتي، ذكر المتهمان أن ما فعلاه هو سلوك شائع ومقبول في المؤسسة التي يعملان بها، وان العاملين في المؤسسة يقومون =باستخدام النظام لأغراض شخصية، بعضها لتحقيق ربح مادي، والبعض الآخر لمجرد التسلية في أوقات الفراغ. انظر قورة نائلة، مرجع سابق، ص. 55.

مباشرة في مواجهة المعلومات محل الجريمة، وقد تتمثل هذه السلطة في الرقم السري الخاص للولوج إلى النظام الذي يحتوي على المعلومات، والتي تمد الفاعل بمزايا متعددة كفتح الملفات وقراءتها وكتابتها ومحو المعلومات أو تعديلها، وقد تتمثل هذه السلطة في الحق في استعمال الأنظمة المعلوماتية، أو إجراء بعض التعاملات، أو مجرد الدخول إلى الأماكن التي تحتوي على هذه الأنظمة.[1]

وهناك في الفقه الجنائي من لخص سمات المجرم المعلوماتي في الآتي:[2]

- المجرم المعلوماتي مجرم متخصص، فقد ثبت في العديد من القضايا أن عددا من المجرمين لا يرتكبون سوى جرائم الكومبيوتر، أي أنهم متخصصون في هذا النوع من الجرائم.
- المجرم المعلوماتي مجرم عائد إلى الإجرام، حيث يعود الكثير من مجرمي المعلومات إلى ارتكاب جرائم أخرى في مجال الكومبيوتر انطلاقا من الرغبة في سد الثغرات التي أودت إلى التعرف عليهم، وتقديمهم إلى المحاكمة في المرة السابقة، ويؤدي ذلك إلى العودة إلى الإجرام وقد ينهي بهم الأمر كذلك في المرة التالية إلى تقديمهم إلى المحاكمة.
- المجرم المعلوماتي مجرم محترف، ذلك أنه لا يمكن للشخص العادي، إلا في حالات قليلة، أن يرتكب جرائم عن طريق الكومبيوتر، فالأمر يقتضي كثيرا من الدقة والتخصص في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكومبيوتر، كما يحدث في البنوك على سبيل المثال.

[1] قورة نائلة، مرجع سابق، ص. 56.
[2] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية، 2006، ص. 45.

المطلب الثاني: الفئات المختلفة للمجرم المعلوماتي

تتمايز الأفعال في الجريمة المعلوماتية على نحو يسير في مضمونها وتنفيذها ومحو أثارها عن تلك الأفعال الخاصة بالإجرام التقليدي، حيث يكتفي المجرم المعلوماتي بلمس لوحة مفاتيح الحاسب الآلي، والتي تقوم على الفور بعمليات الحساب والتحليل وإسقاط الحواجز وأساليب الحماية الأكثر خداعا فالنمو المذهل الذي يشهده عالم المعلوماتية والتقنيات الرقمية الحديثة انعكس بدوره على الجرائم التي ترتكب في البيئة التقنية الالكترونية، فأصبحنا أمام جرائم مستحدثة سريعة التطور مرتكبوها ماهرون في ابتكار الأساليب الحديثة لخرق الحواجز الأمنية في هذا العالم الرقمي مستخدمين خبراتهم ومهاراتهم الذهنية والعقلية.[1] ففي بداية الظاهرة شاع الحديث عن المجرمين الصغار الذين يرتكبون مختلف أنواع الاعتداءات على نظم الكومبيوتر تحديدا الاختراقات بدافع التحدي، وكان ثمة حديث عن استغلال منظمات الجريمة لهؤلاء النابغين، وتحديدا استغلال ميول التحدي لديهم، وأحيانا احتياجاتهم المادية لتسخيرهم للقيام بأنشطة جرمية تتصل بالتقنية تدر منافع مالية كبيرة للمنظمات الإجرامية، ومع تنامي الظاهرة وتعدد أنماط هذه الجريمة، ونشوء أنماط جديدة متصلة بشبكات الكومبيوتر وتحديدا الانترنت، اتجهت جهات البحث وتحديدا الهيئات العاملة في ميدان السلوك الإجرامي لمحاولة تصنيف مرتكبي جرائم الكومبيوتر والانترنت، وبيان السمات الأساسية لكل فئة، بغرض بحث أنجع الوسائل لردع هذه الفئات أو الحد من نشاطها، باعتبار ذلك من المسائل الموضوعية اللازمة لتحديد اتجاهات المكافحة.[2]

---

[1] انظر الموقع الالكتروني:
http://www.tashreaat.com
بتاريخ: 08- 09- 2010 على الساعة 05: 22

[2] السعدي واثبة، الحمـاية الجنائية لمعلومات وبرامج الحاسوب، بحث مقدم إلى مؤتمر القانون والحـاسوب، جامعة اليرمـوك، الأردن، 12-14، 2004.

إن دراسات علم الإجرام الحديث في ميدان إجرام التقنية تسعى في الوقت الحاضر إلى إيجاد تصنيف منضبط لمجرمي التقنية، لكنها تجد صعوبة في تحقيق ذلك بسبب التغير السريع الحاصل في نطاق هذه الظاهرة والمرتبط أساسا بالتسارع الرهيب في ميدان الكومبيوتر والانترنت، فالمزيد من الوسائل والمخترعات التقنية يساهم في تغيير أنماط الجريمة وتطور فعاليات ووسائل الاعتداء، وهذا بدوره يساهم ويساعد في إحداث تغيرات على السمات التي يتسم بها مجرموا التقنية، على الأقل السمات المتصلة بالفعل نفسه وليس بالشخص، ولهذا يتجه الباحثون مؤخرا إلى الإقرار بان أفضل تصنيف لمجرمي التقنية هو التصنيف القائم على أساس أغراض الاعتداء، وليس على أساس التكتيك أو الآلية الفنية المرتكبة في الاعتداء أو على أساس الوسائط محل الاعتداء.[1]

ومن بين أفضل التصنيفات لمجرمي التقنية التصنيف الذي أورده كل من: Karl Seger، David Icovr وWilliam Vonstarch في مؤلفهم جرائم الكومبيوتر الصادر عام 1995 حيث تم تقسيم مجرمي التقنية إلى ثلاثة طوائف: المخترقون، المحترفون والحاقدون كما أن من بين التصنيفات الهامة التمييز بين صغار السن من مجرمي الكومبيوتر، وبين البالغين الذين يتجهون للعمل معا لتكوين المنظمات الإجرامية الخطرة.[2]

ولهذا يمكن لنا وفقا لما توصلت له الدراسات والأبحاث التي تناولت مجرمي المعلوماتية أن نبين بعض هذه الأنماط لهؤلاء المجرمين، ولكن لابد من الإشارة أولا إلى أن هذه التصنيفات لا تعني أن كل مجرم معلوماتي يندرج تحت فئة محددة دون

[1] السعدي واثبة ،المرجع نفسه.
[2] حاتم عبد الرحمن منصور الشحات، مرجع سابق، ص. 93.

غيرها من الفئات المذكورة بل يمكن أن يكون المجرم الواحد مزيجا من طائفة وطائفة أخرى.

الفرع الأول: طائفة صغار السن

يطلق عليهم البعض الأخر صغار نوابغ المعلوماتية ويقصد بهم الشباب البالغ المفتون بالمعلوماتية وأنظمتها.[1] إلا انه في الحقيقة توجد فئة لا تزال دون سن الأهلية مولعين بالحاسوب والاتصال، وقد تعددت أوصافهم في الدراسات الاستطلاعية والمسحية، وشاع في نطاق الدراسات الإعلامية والتقنية وصفهم بمصطلح (المتلعثمين)، الدال حسب تعبير الأستاذ توم فورستر على "الصغار المتحمسين للحاسوب، شعور بالبهجة، دافعهم التحدي لكسر الرموز السرية لتركيبات الحاسوب".[2] ويسميهم البعض كذلك بمجانين معدلات ومعدلات العكسية بالاستناد إلى كثرة استخدامهم لتقنية المعدل والمعدل العكسي (المووديم)، الذي يعتمد على الاتصال الهاتفي لاختراق شبكة النظم، ويثير مجرموا المعلوماتية من هذه الطائفة جدلا واسعا، في الوقت الذي كثر الحديث فيه عن مخاطر هذه الفئة، على الأقل من جانب مواصلتها العبث بالحواسيب، فظهرت دراسات ومؤلفات تدافع عن هذه الفئة لتخرجها من دائرة الإجرام إلى دائرة العبث، وأحيانا البطولة، ومن بين هذه المؤلفات على سبيل المثال، كتاب (خارج نطاق الدائرة الداخلية) لمؤلفه الأمريكي "بيل لاندريت"، وكتاب (الدليل الجديد للمتلعثمين) لمؤلفه "هوجو كورن" في المملكة المتحدة، وكتاب (المتلعثمون أبطال ثورة الحاسوب لمؤلفه "ستيفن ليفي".[3]

[1] سامي الشوى، مرجع سابق، ص. 39.
[2] انظر الموقع الالكتروني: http://sciencesjuridiques.blogspot.com بتاريخ 03- 10- 2010 على الساعة 20: 23
[3] عمر أبو الفتوح عبد العظيم الحمامي، مرجع سابق، ص. 85.

ومن الأمثلة الشهيرة لجرائم الحاسوب التي ارتكبت من هذه الفئة، العصابة الشهيرة التي أطلق عليها (عصابة 414) والتي نسب إليها ارتكاب 60 فعل تعد في الولايات المتحدة الأمريكية على ذاكرات الحاسوب. نجم عنها أضرار كبيرة لحقت بالمنشات العامة والخاصة، كما سبب متلعثموا ألمانيا الغربية في عام 1984، فوضى شاملة، عندما دخلوا شبكة (الفيديو تكس)، ونجح بعض المتلعثمون الفرنسيون في إيجاد مدخل إلى الملفات السرية لبرنامج ذري فرنسي.[1]

ويمكن رد الاتجاهات التقديرية لطبيعة هذه الفئة، وسمات أفرادها، ومدى خطورتهم في نطاق ظاهرة جرائم الحاسوب إلى ثلاثة اتجاهات:[2]

- **الاتجاه الأول**: اتجاه لا يرى إصباغ أية صفة جرمية على هذه الفئة، أو على الأفعال التي تقوم بها، ولا يرى وجوب تصنيفهم ضمن الطوائف الإجرامية لمجرمي المعلوماتية، استنادا إلى أن صغار السن لديهم ببساطة ميل للمغامرة والتحدي، والرغبة في الاكتشاف، ونادرا ما تكون أهداف أفعالهم المحظورة غير شرعية، واستنادا إلى أنهم لا يدركون، ولا يقدرون مطلقا النتائج المحتملة التي يمكن أن تؤدي إليها أفعالهم غير المشروعة بالنسبة لنشاط منشاة أو شركة تجارية.
- **الاتجاه الثاني**: هذا الاتجاه يحتفي بهذه الفئة ويناصرها ويعتبرها ممن يقدم خدمة لأمن المعلومات ووسائل الحماية ويصفهم بالأخيار وأحيانا بالأبطال الشعبيين، ويتمادى هذا الاتجاه في تقديره لهذه الطائفة أو الفئة بالمطالبة بمكافئتهم باعتبارهم لا يسببون ضررا للنظام، ولا يقومون بأعمال احتيال، وينسب إليهم الفضل في كشف الثغرات الأمنية في تقنية المعلومات، ومثل

[1] عمر أبو الفتوح عبد العظيم الحمامي، المرجع نفسه، ص. 86.
[2] عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة دراسة في الظاهرة الإجرامية المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2008، ص. 89.

هذا الرأي قال به أحد أشهر المدافعين عن الهاكرز الصغار "هيوجوكورن" وعكس أفكاره في مؤلفه المذكور سابقا.

- **الاتجاه الثالث:** يرى هذا الاتجاه أن مرتكبي جرائم المعلوماتية من هذه الطائفة، يصنفون ضمن مجرمي الحاسوب كغيرهم دون تمييز استنادا إلى أن تحديد الحد الفاصل بين العبث في الحواسيب وبين الجريمة أمر عسير من جهة، ودونما أثر على وصف الفعل قانونا من جهة أخرى، واستنادا إلى أن خطورة أفعالهم التي تتميز بانتهاك الأنظمة واختراق الحواسيب، وتجاوز إجراءات الآمن، والتي تعد بحق من أكثر جرائم الحاسوب تعقيدا من الوجهة التقنية، عوضا عن مخاطرها المدمرة ويدعم صحة هذا الاتجاه التخوفات التي يثيرها أصحاب الاتجاه الأول ذاتهم، إذ يخشون من الخطر الذي يواجه هذه الطائفة، والمتمثل باحتمال الانزلاق من مجرد هاو صغير لاقتراف الأفعال غير المشروعة إلى محترف لأعمال السلب والاحتيال، هذا إلى جانب خطر آخر أعظم يتمثل في احتضان منظمات الإجرام ومجرمين غارقين في الإجرام لهؤلاء الشباب، أي استغلالهم من طرف منظمات الجريمة المنظمة.

الفرع الثاني: طائفة القراصنة

قراصنة المعلومات هم في الغالب مبرمجون من أصحاب الخبرة يهدفون إلى الدخول إلى أنظمة المعلوماتية غير المسموح لهم بدخولها وكسر الحواجز الأمنية المحيطة بهذه الأنظمة، ويمكن تصنيفها إلى صنفين هما:

- **القراصنة الهواة العابثون Haekers:**[1] هذا القسم من القراصنة أو ما اصطلح على تسميتهم "بالهاكرز" يرون في اختراق الأنظمة المعلوماتية تحديا لقدراتهم الذاتية، وهذه الطائفة غالبا ما تكون من هواة الحاسوب، فيقومون بأعمالهم هذه لمجرد إظهار أنهم قادرون على اقتحام المواقع الأمنية أحيانا أو مجرد ترك بصماتهم التي تثبت وصولهم إلى تلك المواقع أحيانا أخرى.[2]

وهم يدعون أنه لا توجد هناك دوافع تخريبية وراء أعمالهم، بل قد يكون الفضول وحب المعرفة والتعمق في عمل الأنظمة المعلوماتية هو دافعهم الأول، ومجرموا المعلوماتية من هذا الصنف هم عادة أشخاص عاديون يشغلون مناصب محل ثقة، ولديهم الكفاءة الخاصة والمعرفة والمهارة المطلوبة في مجال الحواسيب والشبكات الالكترونية.[3]

ففي مقابلة سرية أجرتها صحيفة التايمز مع أحد القراصنة، والذي كان يشتغل استشاري تنفيذ المعلومات، قال: "إن اختراق الموقع الأمني مسالة سهلة جدا، فهي أشبه بمن يبحث عن مفتاح معين في مجموعة صناديق، ثم تجد أمامه بوابة جانبية مفتوحة على مصرعيها".[4]

وهناك القراصنة الأخلاقيون، الذين يقولون أنهم يعملون من أجل المصلحة العامة، فشكلوا لهم منظمات خاصة، مثل منظمة القراصنة ضد المواقع الإباحية للأطفال التي استطاعت القيام بحملات تأديبية لتعطيل قدرة بعض المواقع الالكترونية عن عرض مواد غير أخلاقية.[5]

---

[1] الهاكرز هو مصطلح في اللغة الانجليزية، يطلق على الشخص المتخصص في نظم المعلومات والبرمجيات، والقادر على ابتكار البرامج، والتعامل مع شبكات الحاسب الآلي، وحل جميع المشاكل المتعلقة به، وإتقان لغات البرمجة المعروفة، لذلك فان مصطلح الهاكرز كانت له مدلولات ايجابية، وكان يطلق على المبرمج من قبيل المدح. انظر: إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان، دار الجامعة الجديدة، الإسكندرية، 2007، ص.

[2] الزيدي وليد، القراصنة على الانترنت والحاسوب، الطبعة الأولى، دار سامة للنشر، عمان، 2003، ص. 40.

[3] المرجع نفسه، ص. 41.

[4] انظر الموقع الالكتروني:

www.tashreaat.com

بتاريخ 13- 09- 2010 على الساعة 45: 18

[5] محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري، دار الجامعة الجديدة، الإسكندرية، 2007، ص. 36.

كما أن هناك سمة مميزة لهذه الفئة من القراصنة، ألا وهي تبادلهم للمعلومات فيما بينهم، وتحديدا التشارك في وسائل الاختراق وآليات نجاحها في مواطن الضعف في نظام الحاسوب، كما أن هناك حقيقة لا يجب أن نخفيها، هي أن هؤلاء القراصنة الهواة ساهموا في كشف الفجوات الأمنية للأنظمة المعلوماتية في المؤسسات المالية وغيرها، الأمر الذي ساهم في تطوير نظم الأمن ضد الاختراقات الأمنية التي يقوم بها مجرموا المعلوماتية.

- **القراصنة المحترفون Crackers**:[1] هذه الفئة تعكس اعتداءاتهم ميولات إجرامية خطيرة تنبئ عن رغبتها في إحداث التخريب، ويتميز هؤلاء بقدراتهم التقنية الواسعة وخبرتهم في مجال أنظمة الحاسوب والشبكات، وهم أكثر خطورة من الصنف الأول،[2] فهم يستخدمون برامج التقنية في محاولات لاختراق الأنظمة والأجهزة للحصول على المعلومات السرية،[3] أو القيام بعمليات تخريبية معينة، كاختراق مزودات الشركات، لحذف وإضافة المعلومات أو لمجرد الإطلاع عليها، أو للدخول إلى مزودة خدمة الانترنت والتلاعب بمحتويات الصفحة، أو الاستيلاء على أرقام البطاقة الائتمانية واستخدامها، وكذا القيام بمحاولة إزالة أو فك الحماية التي تصنعها شركات إنتاج البرمجيات على برامجها لمنع عمليات النسخ غير القانوني.[4]

وعادة ما يعود المجرم المحترف بالجريمة المعلوماتية إلى ارتكاب الجريمة مرة أخرى، حيث تزداد سوابقه القضائية وهو يعيش لسنوات طويلة

---

[1] كراكرز هو مصطلح في اللغة الانجليزية، مستمدة من الفعل Crack ويعني الكسر أو التحطيم.

[2] نهلا عبد القادر المومني، مرجع سابق، ص. 84.

[3] يعتبر أشهر كراكرز في العالم حتى الآن، الأمريكي (كيفين ميتينك)، الذي أصبح أسطورة الكراكرز ومثلهم الأعلى، نظرا لموهبته الفذة، وقدرته الفائقة في السرقة، وتدمير الأجهزة، والشبكات والمواقع بشكل عام، وقد أصبح أشهر كراكرز بعدما نفذ اكبر عملية سرقة تاريخية الكترونية عرفها العالم، حيث سرق حوالي مئتي ألف رقم لبطاقات ائتمان عام 1995، وتم القبض عليه وسجن، إلا أن أنصاره والجماعات المؤيدة له تقوم باختراق بعض المواقع الهامة للتأثير على الحكومة الأمريكية للإفراج عنه، وهذا ما وقع لصحيفة النيويورك تايمز على شبكة الانترنت. انظر الموقع: www.chawkhtabib.info/spip.php.article478
بتاريخ 14- 09- 2010 على الساعة 00: 18

[4] إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان، دار الجامعة الجديدة، الإسكندرية، 2007، ص. 135.

من عائد جرائمه، وهذا المجرم لا يفضل الأفكار المتطرفة، وإنما الأفكار التي تدر عليه الأرباح الشخصية، وتوضح الدراسات التي أجراها أحد المعاهد المتخصصة أن محترفي الجرائم المعلوماتية من الجيل الحديث هم في الغالب من الشباب الذي تتراوح أعمارهم من 25 إلى 45، وتبين الإحصاءات في هذا المجال ما يلي:[1]

- 25% من أفعال الغش المعلوماتي يرتكبها المحلل.
- 18% من هذه الأفعال يرتكبها المبرمج.
- 17% يرتكبها المستخدم الذي لديه أفكار خاصة بنظم المعلومات.
- 12% يرتكبها الشخص الأجنبي عن المكان الذي تتواجد فيه نظم المعلومات.
- 11% من هذه الأفعال ترتكب في التشغيل.

الفرع الثالث: طائفة مجرموا المعلومات أصحاب الآراء المتطرفة

المتطرفون الفكريون طائفة من الناس نزلت بهم عقولهم إلى مستنقع الشطط في التفكير، متطرفون لأفكارهم وأرائهم، ومتجاوزون بذلك كل الحدود المعقولة والمقبولة للتحاور والنقاش، وذلك بخصوص قضية أو غاية ليس لها علاقة بمصالحهم الشخصية، وهم في سبيل تحقيق ما يعتقدونه، على استعداد لارتكاب أنشطة إجرامية مختلفة، وتخلف وراءها أضرار جسيمة سواء على أفراد من المجتمع أو على قطاعات كاملة منه هادفين من ذلك تحول المجتمع إلى الأفضل من جهة نظرهم بدون قيد أو شرط، وعلى ذلك يختلف المجرم العادي عن المجرم المعلوماتي المتطرف، فالأول لا يبغي سوى تحقيق منفعته الشخصية، أما الثاني

[1] عمر أبو الفتوح عبد العظيم الحمامي، مرجع سابق، ص. 88.

فيكون مدفوعا ببعض البواعث التي قد تكون ذات طبيعة سياسية أو اقتصادية أو تتعلق بحقوق الإنسان أو مرتبطة بشؤون البيئة أو دينية.[1]

هذا التطرف الفكري مجسد اليوم فيما يعرف بصراع الحضارات، حيث أطلق العديد من المتطرفين عديموا الفهم والمتشددون الخلاف إلى الوراء بالزج بالدين إلى جلسة الصراع، فقد ادعى بعضهم بأفضلية أحد الأديان عن الأديان الأخرى من حيث المساهمة في التقدم الحضاري الذي وصلت إليه البشرية.

ويمكن أن نشير هنا إلى منظمة الأولوية الحمراء الايطالية التي استهدفت نظم المعلومات المتعلقة ببعض الهيئات، ومن ذلك اعتدائها على مكتب المرور الرئيسي في ايطاليا –منذ بضع سنوات- مما أدى إلى أضرار جسيمة دمرت معظم المعلومات الخاصة باللوحات المعدنية ورخص القيادة بما فيها النسخ الاحتياطية، وظل الايطاليون لمدة عامين متتاليين لم يكن لديهم أي مستند يثبت ملكيتهم لسياراتهم، أو لم يكن لديهم رخص قيادة صحيحة أو سليمة.[2]

وكذلك ظهرت في فرنسا منظمة أو هيئة إزالة أو تدمير الحاسبات أو نظم المعلومات لذا فقد أيقنت المنظمات الإرهابية أن في استطاعتها وبمجهود بسيط أن تلحق إضرار جسيمة داخل أي مشروع أو مؤسسة عن طريق تدمير المركز المعلوماتي.

[1] حاتم عبد الرحمن منصور الشحات، مرجع سابق، ص. 97.
[2] سامي الشوى، مرجع سابق، ص. 44.

وأخيرا نستطيع القول أن أفراد هذه الطائفة من المجرمين لديهم اتجاه إجرامي خطير، وذو نية بالغة السوء، وذلك لأنهم لا يبالون بالأضرار الجسيمة التي أصابت الأفراد أو المجتمع أو بعض قطاعاته.[1]

الفرع الرابع: طائفة الموظفون العاملون في مجال الأنظمة المعلوماتية

بحكم طبيعة عمل هؤلاء، ونظرا لأن النظام المعلوماتي هو مجال عملهم الأساسي، ونظرا للمهارات والمعرفة التقنية التي يتمتعون بها، فإنهم يقترفون بعض الجرائم المعلوماتية التي من الممكن أن تحقق أهدافهم الشخصية، وأهمها الكسب المادي، فالعلاقة الوظيفية التي تربط بين الموظف والمجني عليه تجعل عملية ارتكاب الجريمة المعلوماتية أسهل نظرا للثقة التي يتمتع بها.

وهناك فئة من الموظفين الحاقدين على عملهم أو على مؤسساتهم، الذين قد يقدمون على أعمال إجرامية لا تهدف إلى الكسب المادي، أو لتحقيق هدف سياسي، إنما يحرك أنشطتهم الرغبة في الانتقام والثأر، وهذه الفئة يذهب البعض إلى تسميتها بفئة مجرمي المعلوماتية الحاقدين.[2]

الفرع الخامس: مجرموا المعلوماتية في إطار الجريمة المنظمة

تتخذ الجريمة المنظمة مفهوما أكثر اتساعا من عصابات المافيا، حيث تشمل كل منظمة ذات هيكل محدد، وتوزع عائد أنشطتها الإجرامية على أعضائها، إلا أن الجريمة المنظمة بالمعنى الدقيق تطلق على عصابات المافيا، ورغم عدم دخول الجريمة المنظمة عالم الإجرام المعلوماتي بشكل كبير حتى الآن، إلا أنه من المتوقع دخولها هذا المجال على نحو واسع، وذلك لارتفاع عائد الجريمة المعلوماتية، ورغبة

[1] جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة، 2001، ص. 33.
[2] محمد سليمان مصطفى، جرائم الحاسوب وأساليب مواجهتها، مجلة الأمن والحياة، 1999، العدد 199، ص. 50.

منها في عدم اقتصار نشاطها على الجرائم التقليدية مثل المخدرات والسطو والألعاب ويطلق على هذا الشكل الإجرامي الحديث أحيانا إجرام ذوي الياقات البيضاء الذي يعبر عن حالة الطمع والجشع لدى مرتكبي هذه الأفعال.[1]

ومن التعريفات التي قيلت في الجريمة المنظمة أنها: "تعبير عن مجتمع إجرامي يعمل خارج إطار الشعب والحكومة ويظم بين طياته ألاف المجرمين الذين يعملون وفقا لنظام بالغ الدقة والتعقيد، يفوق النظم التي تتبعها أكثر المؤسسات تطورا وتقدما، كما يخضع أفرادها لأحكام قانونية سنوها لأنفسهم، وتفرض أحكام بالغة القسوة على من خرج عن أعراف الجماعة، ويلتزمون في أداء أنشطتهم الإجرامية بخطط دقيقة يلتزمون بها ويجنون من ورائها الأموال الطائلة."[2]

منظمات الجريمة المنظمة تطور أساليب عملها باستمرار بما يحقق أهدافها، وغاياتها والعوامل المساعدة في تطوير هذه المنظمات لطرق عملها المالية والاقتصادية التي تتمتع بها، فهي تسعى دوما إلى استغلال الوسائل التقنية الحديثة في القيام بنشاطها، فاستفادت هذه المنظمات عبر سنوات عملها من أحدث وسائل الاتصال حتى تؤمن الترابط بين أفرادها وجماعاتها، وتسعى هذه المنظمات إلى الاستفادة من أجهزة التقنية المعلوماتية الحديثة، المتمثلة في جهاز الحاسوب والانترنت لتسوية أعمالها وتسهيل تنفيذها، فلقد وجدت هذه المنظمات في شبكة الانترنت وسيلة لا تضاهيها أخرى للقيام بعمليات تبييض الأموال على نطاق ومجال واسع، وكذلك لتدعيم تجارة الرقيق الأبيض، وتجارة الأعضاء البشرية.

كما تقوم هذه المنظمات الإجرامية المنظمة بتبني أصحاب الكفاءات والخبرة والموهوبين في مجال تقنية المعلومات، وذلك بإغرائهم بالمال لينظموا إلى صفوفها،

[1] عمر أبو الفتوح عبد العظيم الحمامي، مرجع سابق، ص. 102.
[2] هذا التعريف للفقيه (اوجيت ناكاوي)، انظر المرجع: عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة... مرجع سابق، ص. 62.

ويمارس مجرموا المعلوماتية في نطاق هذه المنظمات نشاطات تدر على المنظمة أرباحا هائلة، فيقومون بتزوير البرامج وتقليدها، واختراق شبكات المعلومات الخاصة بالدول والمؤسسات المالية الكبرى، كما يمارسون أعمال التجسس الصناعي والتجاري، كما تشكل أي الجرائم المعلوماتية عامل جذب كبير لهذه المنظمات الإجرامية، فبالإضافة إلى الأرباح المادية المرتفعة التي تنتج من هذه الجرائم، فان صعوبة الكشف عنها، وصعوبة إثباتها يعتبران عاملي جذب لهذه المنظمات الإجرامية.[1]

الفرع السادس: طائفة الحكومات الأجنبية

قد يضن البعض أن الإجرام المعلوماتي يقتصر على الأفراد أو الشركات والمؤسسات، ولكن مما لا شك فيه أن تجسس الحكومات على بعضها البعض يضرب بجذوره في أعماق التاريخ، فالدول تبحث عن المعلومات لدى الغير سواء كان من الأعداء أم لا من أجل تفادي المخاطرة والتفوق عليه، وكان التجسس في ما مضى يرتكز على الأمور العسكرية، ولكن في الوقت الحاضر لم يعد التفوق العسكري وحده الفاصل في المعارك، وإنما يلزم التفوق الاقتصادي والتكنولوجي، ولذلك فان التجسس يرتكز الآن على التطور التكنولوجي في أكثر صوره، وذلك تجسيدا للتقدم الصناعي، والمتمثل في ثورة المعلومات.[2]

فقد حاولت شركة (هيتاش) و(ميتسوبيشي) اليابانيتين التجسس على شركة (IBM) الأمريكية المتخصصة في مجال الحاسبات، وكذلك الشأن حاولت أجهزت الاستخبارات الفرنسية التجسس على الشركة الأمريكية لحساب الشركة الفرنسية المصنعة لأجهزة الحاسب (BU2)، كذلك قيام بعض القراصنة المتواجدين على

[1] عمر أبو الفتوح عبد العظيم الحمامي، مرجع سابق، ص. 103.
[2] المرجع نفسه، ص. 104.

الأراضي الروسية باختراق نظم حاسبات حكومية في الولايات المتحدة الأمريكية لمدة عام كامل، حيث قاموا بسرقة معلومات غير سرية ولكنها حساسة من أجهزة حاسبات عسكرية، كما أغار القراصنة على شبكات غير سرية في وكالة الفضاء الأمريكية ناسا NASA.[1]

المطلب الثالث: دوافع المجرم المعلوماتي لارتكاب الجريمة المعلوماتية

مما سبق يتضح لنا أن فئات مرتكبي الجريمة المعلوماتية تختلف عن مرتكبي الجرائم التقليدية، لذا من الطبيعي أن نجد نفس الاختلاف في الأسباب والعوامل التي تدفع إلى ارتكاب الفعل غير المشروع.

فالدافع (الباعث)، الغرض، الغاية، تعبيرات لكل منها دلالته الاصطلاحية في القانون الجنائي، تتصل بما يعرف بالقصد الخاص في الجريمة، وهي مسالة تثير جدلا فقهيا وقضائيا واسعا، ذلك أن القاعدة القضائية تقرر أن الباعث ليس عنصرا من عناصر القصد الجرمي، وأن الباعث لا أثر له في وجود القصد الجنائي، وإذا كان الاستخدام العادي للتعبيرات المشار إليها يجري على أساس ترادفها في الغالب، فإنها من حيث الدلالة تتمايز، وينتج عن تمايزها أثار قانونية على درجة كبيرة من الأهمية، فالدافع هو العامل المحرك للإرادة، والذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والانتقام، وهو إذن قوة نفسية تدفع الإرادة إلى الاتجاه نحو ارتكاب الجريمة ابتغاء تحقيق غاية معينة، وهو يختلف من جريمة إلى أخرى تبعا لاختلاف الناس من حيث السن والجنس ودرجة التعلم.

أما الغرض فهو الهدف الفوري المباشر للسلوك الإجرامي، ويتمثل بتحقيق النتيجة التي انصرف إليها القصد الجنائي أو الاعتداء على الحق الذي يحميه قانون

[1] احمد هلالي عبد أللاه، مرجع سابق، ص.21.

العقوبات، وأما الغاية فهي الهدف البعيد الذي يرمي إليه الجاني بارتكاب الجريمة، كإشباع شهوة الانتقام، أو سلب مال المجني عليه في جريمة القتل.[1]

وبالنسبة لجرائم الكومبيوتر والانترنت، فثمة دوافع عديدة تحرك الجناة لارتكاب أفعال الاعتداء المختلفة المنضوية تحت هذا المفهوم، وأهم هذه الدوافع هي:

الفرع الأول: السعي إلى تحقيق الكسب المالي (الدوافع المادية)

يعد هذا الدافع والذي يمثل في الحقيقة غاية الفاعل من بين أكثر الدوافع تحريكا للجناة لاقتراف جرائم الحاسوب، ذلك أن خصائص هذه الجرائم، وحجم الربح الكبير الممكن تحقيقه من بعضها، خاصة غش الحاسوب أو الاحتيال المرتبط بالحاسوب يتيح تعزيز هذا الدافع ومنه بداية الظاهرة، فالدراسات أشارت إلى أن المحرك الرئيسي لأنشطة احتيال الكومبيوتر ، هو تحقيق الكسب المادي، ففي دراسة تعرض لها الفقيه Parker يظهر أن 43% من حالات الغش المعلن عنها قد تمت من أجل اختلاس الأموال، و23% من أجل سرقة معلومات، 19% أفعال إتلاف، أما 15% فلسرقة وقت الآلة، أي استعمال غير مشروع للحاسوب لأجل تحقيق منافع شخصية.[2]

الفرع الثاني: الرغبة في التعلم

إن الرغبة الشديدة في تعلم كل ما يتعلق بأنظمة الحاسوب والشبكات الالكترونية قد يكون الدافع وراء ارتكاب الجرائم المعلوماتية، فالأستاذ (ليفي) يشير

[1] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية... مرجع سابق، ص. 40.
[2] عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، 2001، ص. 71.

في مؤلفه كتاب قراصنة الأنظمة إلى أخلاقيات هؤلاء القراصنة التي ترتكز على مبدأين أساسيين هما:[1]

- إن الدخول إلى أنظمة الحاسوب يمكن أن يعلمك كيف يسير العالم.
- إن عملية جمع المعلومات يجب أن تكون غير خاضعة للقيود.

هناك من يرتكب جرائم الحاسوب بغية الحصول على الجديد من المعلومات، وهؤلاء الأشخاص يقومون بالبحث واكتشاف الأنظمة والعمل من خلال الجماعة وتعليم بعضهم، ويفضل هؤلاء القراصنة البقاء مجهولين أكبر وقت ممكن حتى يتمكنوا من الاستمرار في التواجد داخل الأنظمة.[2]

وخلاصة القول أن هؤلاء المجرمون يرون أن جميع المعلومات المفيدة يجب أن تتاح حرية نسخها والإطلاع عيها، إلا أنهم يقرون بضرورة إغلاق بعض نظم المعلومات، وعدم السماح بالوصول إلى بعضها، خاصة المعلومات السرية التي تخص الأفراد.[3]

الفرع الثالث: الإثارة والرغبة في قهر النظام المعلوماتي واثبات الذات

يشكل اختراق الأنظمة الالكترونية، وكسر الحواجز الأمنية المحيطة بهذه الأنظمة متعة كبيرة وتسلية تغطي أوقات الفراغ، ويمكن أن نوضح ذلك من خلال ما ذكره أحد قراصنة الحاسوب: "كانت القرصنة هي النداء الأخير الذي يبعثه دماغي، فقد كنت أعود إلى البيت بعد يوم أخر في المدرسة، وأدير جهاز الحاسوب، وأصبح عضوا في نخبة قراصنة الأنظمة، كان الأمر مختلفا برمته حيث لا وجود لعطف الكبار، وحيث الحكم هو موهبتك فقط. في البدء كنت أسجل اسمي في لوحة

[1] عبد الله علي حسين محمود ،المرجع نفسه.
[2] نهلا عبد القادر المومني، مرجع سابق، ص. 90.
[3] المرجع نفسه.

النشرات الخاصة حيث يقوم الأشخاص الآخرون الذين يفعلون مثلي بالتردد على هذا الموقع، ثم أتصفح أخبار المجتمع، وأتبادل المعلومات مع الآخرين في جميع أنحاء البلاد، وبعد ذلك ابدأ عملية القرصنة الفعلية، وخلال ساعة واحدة يبدأ عقلي يقطع مليون ميل في الساعة، وأنسى جسدي تماما بينما أنتقل من جهاز حاسوب إلى أخر، محاولا العثور على سبيل للوصول إلى هدفي، لقد كان الأمر يشبه سرعة العمل في متاهة، إلى جانب الاكتشاف الكبير لأعداد ضخمة من المعلومات ، وكان يرافق تزايد سرعة الأدرنالين الإثارة المحظورة بفعل شيء غير قانوني، وكل خطوة أخطوها يمكن أن تسقطني بيد السلطات، كنت على حافت التكنولوجيا واكتشاف ما وراؤها واكتشاف الكهوف الالكترونية التي لم يكن من المفترض وجودي بها".[1]

وعلى صعيد أخر قد يكون الدافع إلى ارتكاب الجرائم الالكترونية هو الرغبة في قهر النظام (الأنظمة الالكترونية والتغلب عليها)، إذ يميل مرتكبو هذه الجرائم إلى إظهار تفوقهم على وسائل التكنولوجيا الحديثة.[2]

الفرع الرابع: الرغبة في الانتقام

قد تكون الرغبة في الانتقام من أهم الجرائم في ارتكاب الجريمة المعلوماتية، هذه الرغبة في الانتقام قد تتجلى في شخص ما أو مؤسسة ما أو حتى بعض الأنظمة السياسية في بعض الدول، أو الانتقام من رب العمل، فعلى سبيل المثال دفع الانتقام بمحاسب شاب إلى أن يتلاعب بالبرامج المعلوماتية بحيث تختفي كل البيانات الحسابية الخاصة بديون هذه المنشاة بعد رحيله بعدة أشهر، وقد تحقق هذا في التاريخ المحدد.[3]

[1] عبد الله حسين علي محمود، مرجع سابق، ص. 73.
[2] إيهاب فوزي السقا، مرجع سابق، ص. 138.
[3] المرجع نفسه، ص. 139.

الفرع الخامس: دوافع أخرى

لا تعتبر الدوافع السابقة الذكر هي الدوافع الوحيدة التي تدفع بالمجرم المعلوماتي إلى ارتكاب الجريمة المعلوماتية، فمثلا قد يعد التسابق الفضائي والعسكري بين الدول دافعا لهذه الجريمة.[1]

و يمكن اعتبار التنافس السياسي والاقتصادي دافعا لارتكاب هذا السلوك الإجرامي.

كما أن مناهضة العولمة قد تكون إحدى الأسباب لارتكاب هذا الفعل، فقد تم اختراق النظام المعلوماتي للمنتدى الاقتصادي العالمي في دافوس سويسرا، وتمت عملية سرقت معلومات سرية تتعلق بعدد من الشخصيات الثرية والمؤثرة التي شاركت في المؤتمر وأرسلت إلى إحدى الصحف السويسرية.

وأخيرا، لا يمكن حصر أو ذكر كل الدوافع والبواعث التي قد تدفع المجرم المعلوماتي إلى ارتكاب هذا الفعل المجرم.

يمكن القول، أنه وبالرغم من الأهمية القانونية الضئيلة لسمات ودوافع المجرم المعلوماتي، كونها لا تعتبر من عناصر التجريم إلا إذا نص القانون على خلاف ذلك، غير أن هذا لا يلغي أهميتها من حيث أنها تساهم في تفسير وتحليل سلوك المجرم المعلوماتي، ومحاولة الوقاية من الجريمة المعلوماتية.

[1] نهلا عبد القادر المومني، مرجع سابق، ص. 91.

خلاصة

حاولت في هذا الفصل الأول تحديد مفهوم الجريمة المعلوماتية من خلال استعراض المقصود بها، كتعريفها وتحديد مختلف خصائصها وخصائص مرتكبيها.

لم يتم التوصل إلى تعريف محدد للجريمة المعلوماتية، ولكن ما نراه أن هذه التعاريف قد ساهمت في إبراز وتحديد صفات وخصائص الجريمة المعلوماتية، وبيان مدى خطورتها وضرورة إيجاد حلول سريعة للحد من انتشارها.

ويرجع السبب في ذلك، إلى أن هذا النمط أو النوع الإجرامي المستحدث يطال المعلومات التي لها اتجاهات فقهية مختلفة بخصوص تحديد المقصود بها وبطبيعتها. وبما أن الجريمة المعلوماتية تختلف عن غيرها من الجرائم التقليدية، فإن مرتكبيها يتميزون عن غيرهم من الجناة، سواء من حيث السمات أو الدوافع، وقد تم تصنيف مرتكبي هذه الأفعال إلى طائفتين، الأولى طائفة صغار السن والثانية طائفة البالغين، غير أن هذا التصنيف لا أجد له أي فائدة تذكر، إذ أن هناك العديد من الأفعال قد ترتكب من الصغار والكبار معا، وبالتالي تتداخل وتتشابك، وكما كان لتحديد مفهوم الجريمة المعلوماتية تعاريف مختلفة فإن لتصنيف مرتكبي هذه الجرائم تصنيفات مختلفة أيضا.

وبغض النظر عن ذلك، فإن دراسة سمات وفئات ودوافع هذا النمط من السلوك الإجرامي تساعدنا في تفسير ارتكاب هذا النوع من الإجرام، وبالتالي إيجاد الحلول المناسبة لمقاومتها والتغلب عليها.

الفصـــــل الثاني

سلوكيات المجرم المعلوماتي المرتكبة بواسطة المعلوماتية

مكنت الثورة الرقمية Digital Révolution للمجرم المعلوماتي تسخير الفضاء الكوني لتحقيق أغلب صور الإعتداء على الأشخاص من جنح بسيطة إلى جنايات كبرى، إما كفاعل أصلي أو كفاعل معنوي وبأبسط الأساليب من خلال التلاعب ببرمجة البيانات عن بعد وبضغطة زر واحدة.

وموضوع بحثي هنا، يرتكز على الحالات التي يستعان فيها بالمعلوماتية لارتكاب الجريمة، أي باستخدامها كوسيلة لتنفيذها، فليس الحاسب الآلي هو موضوع الحماية، بل أموال الغير، وحياته الخاصة، ومن أبرز صور هذه الجرائم سحب الأموال من المصارف بدون وجه حق، والاعتداء على الحياة الخاصة للأفراد بالإطلاع على بياناتهم والتجسس عليها وجرائم الذم والقدح والتحقير، وجرائم الاستغلال الجنسي للأطفال عبر الإنترنت، ويتمثل الركن المادي في جرائم الانترنت أن النشاط أو السلوك المادي في هذه الجرائم يتطلب وجود بيئة رقمية واتصال بالإنترنت، ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه، ومثال ذلك قيام مرتكب الجريمة بتجهيز الحاسب لكي يحقق له حدوث الجريمة فيقوم بتحميل الحاسب ببرامج اختراق أو أن يقوم بإعداد هذا البرامج بنفسه، وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة وتحميلها على الجهاز المضيف، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيدا لبثها.

وفي حقيقة الأمر ليس كل جريمة تستلزم وجود أعمال تحضيرية، وفي نفس الوقت يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في جرائم الكمبيوتر والإنترنت، إلا أنه في مجال تكنولوجيا المعلومات فالأمر يختلف بعض الشيء، فشراء برامج الاختراق ومعدات لفك الشيفرات تمثل جريمة في حد ذاتها، ومن المشاكل التي يثيرها هذا الصنف من الجرائم مسألة النتيجة الإجرامية، فعلى

سبيل المثال مكان وزمان تحقق النتيجة الإجرامية، فلو قام أحد المجرمين في أمريكا اللاتينية باختراق جهاز خادم Server أحد البنوك في الإمارات، وهذا الخادم موجود في الصين فكيف يمكن معرفة وقت حدوث الجريمة،[1] أما الركن المعنوي فهو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، وقد تنقل المشرع الأمريكي في تحديد الركن المعنوي للجريمة بين مبدأ الإرادة ومبدأ العلم، فهو تارة يستخدم الإرادة كما هو الشأن في قانون العلامات التجارية، وأحيانا أخرى أخذ بالعلم كما هو حال في قانون مكافحة الاستنساخ، وبرزت تلك المشكلة في قضية موريس الذي كان متهما في قضية دخول غير مصرح به على جهاز حاسب فيدرالي وقد دفع محامي المتهم على انتفاء الركن المعنوي، الأمر الذي جعل المحكمة تقول "هل يلزم أن يقوم الادعاء بإثبات القصد الجنائي في جريمة الدخول غير المصرح به، بحيث تثبت نية المتهم في الولوج إلى حاسب فيدرالي، ثم يلزم إثبات نية المتهم في تحدي الحظر الوارد على استخدام نظم المعلومات في الحاسب وتحقيق خسائر، ومثل هذا الأمر يستدعي التوصل إلى تحديد أركان جريمة الدخول دون تصريح". وبذلك ذهبت المحكمة إلى تبني معيارين هنا هما الإرادة بالدخول غير المصرح به، وكذا معيار العلم بالحظر الوارد على استخدام نظم معلومات دون تصريح، أما بالنسبة للقضاء الفرنسي فإن منطق سوء النية هو الأعم في شأن جرائم الانترنت، حيث يشترط المشرع الفرنسي وجود نية في الاعتداء على بريد الكتروني خاص بأحد الأشخاص.[2]

وتبدو الجرائم التي ترتكب بواسطة المعلوماتية ظاهرة في عدة محاور منها ما يضم تلك الأفعال التي تطال في اعتداءاتها الذمة المالية، كجريمة غش الحاسب

[1] فؤاد جمال، الجرائم المعلوماتية، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، المنعقد بكلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2000، ص. 13.
[2] المرجع نفسه، ص. 14.

الآلي (التحايل المعلوماتي) وكجريمة إساءة استعمال البطاقة الممغنطة، ومنها ما يضم الأفعال التي تنطوي على المساس بالحياة الخاصة وجرائم القذف والشتم، ومن الصعب حصر جميع الجرائم المعلوماتية التي قد تقع تحت هذه الطائفة إلا أنني سأتناول بعض صور هذه الجرائم المعلوماتية في ثلاث مباحث على النحو الآتي:

المبحث الأول ويعالج التحويل الالكتروني غير المشروع للأموال (الجرائم المرتبطة بالذمة المالية)، ثم المبحث الثاني الذي يتطرق إلى الجرائم المتصلة بالحياة الخاصة، وأخيرا المبحث الثالث الذي يهتم بالدخول والبقاء غير المصرح بهما إلى النظام المعلوماتي.

المبحث الأول: التحويل الالكتروني غير المشروع للأموال (الجرائم المرتبطة بالذمة المالية)

اكتسب التعامل بالأموال في عصر المعلوماتية صفة البيانات الإلكترونية المختزنة 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 المختزنة في ذاكرة الحاسب الآلي أو في برامجه وإجراء تحويلات في كل أو بعض أرصدة الغير أو فوائدها وإدخالها في حسابه.[1]

ومن العوامل التي كان لها التأثير الكبير والتي شجعت على جرائم الأموال أيضا استعمال وسائل التزوير والنصب من الأجهزة الحديثة والمتطورة التي أصبحت أدوات فعالة في أيدي المجرمين، وهذا ما أثر عل السلوك الإجرامي للمجرم، من مجرم تقليدي إلى مجرم معلوماتي، ففي فرنسا أعلنت الحكومة عن ارتفاع عدد الجنح بنسبة 70% بسبب الاعتماد على التكنولوجيا الجديدة وهي كلها جنح اقتصادية مثل سرقة البطاقات المصرفية. فالتكنولوجيا الحديثة فتحت آفاق جديدة أمام التجسس والخداع والنصب حتى أن الكونغرس الأمريكي بدأ يبحث مشروعات قانونية لحماة الحياة الخاصة على الانترنت، لأن استخدام الشبكة العنكبوتية بدأ يفرض على المستخدم الإفصاح عن معلومات خاصة وسرية تتيح لشركات التسويق والإعلان استخدامها في مجال عملها.[2]

وغالبا ما يتم ولوج مخترقي شبكات الإنترنت إلى بيانات حساب الآخرين من خلال الحصول على كلمة مرور مدرجة في ملفات أنظمة الكمبيوتر الخاصة بالمجني عليه، فإذا ما تم الاستيلاء على كلمة المرور وإدخالها في أنظمة الحاسب

[1] محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنت، دار الثقافة، الأردن، 2004، ص. 178.
[2] منصور رحماني، علم الإجرام والسياسة الجنائية، دار العلوم، عنابة، 2006، ص. 122.

الآلي، فإنها سوف تنسجم وتقترن بالملف ومن ثم تسمح للمخترق بالولوج إلى النظام المعلوماتي، وبعكس ذلك فإن المستخدم يمنع من الولوج. ويحصل مجرموا المعلوماتية على كلمات المرور الخاصة بالغير إما بالتقاطها أثناء تواجدهم في النظام المعلوماتي، أومن خلال بث برامج تتعقب الأنظمة المعلوماتية التي يتجه إليها أكثر المستخدمين وسرقة كلمات المرور الخاصة بهم، والحصول على البيانات الخاصة بالجاني واستخدام المفيد منها في إجراء التحويلات المالية الالكترونية من حساب المجني عليه وإدخالها في أرصدتهم وفي النظام المعلوماتي الخاص بهم.[1]

والحصول على المعلومات والبيانات المتعلقة بالمستخدمين قد يتم من قبل العاملين على إدخال البيانات في ذاكرة الحاسوب أو من قبل المتواجدين على الشبكة أثناء عملية تبادل البيانات، وذلك بفعل الالتقاط أو بالتحايل أثناء عملية تبادل البيانات.

وقد قام بالفعل مبرمج في أحد البنوك بدوره وذلك بإعداد البرامج المتعلقة بإعادة المال الزائد من مالكي بطاقات الفيزا ،عن طريق استقطاع (25 سنت) من حاملي البطاقات وبطريقة عشوائية وإدخالها في حساب الفيزا الخاص به، ولم يكتشف هذا المستخدم إلا بعد ملاحظة التغير الكبير في نمط حياته، وقد وجه إليه تهمة الاحتيال على البنك، وقد تكون عملية الاحتيال لتحويل الأموال الكترونيا نتيجة تواطؤ، وذلك ما حدث بالفعل من إحدى الشركات الأوروبية عندما تمكن مراقب يعمل في إحدى الشركات من الحصول على كلمات المرور الخاصة بالغير وإعطائها لعامل آخر ليقوم بدوره بتحويل أكثر من (50) مليون دولار إلى حسابه الخاص في إحدى البنوك بمدينة لوزان السويسرية.[2]

[1] محمد أمين أحمد الشوابكة، مرجع سابق، ص. 178.
[2] المرجع نفسه، ص 181.

المطلب الأول: الاحتيال في نطاق المعلوماتية

قبل أن نتطرق إلى ماهية الاحتيال المعلوماتي والأساليب التقنية المستخدمة في ارتكابه لابد أن نشير إلى أن عمليات الاحتيال المعلوماتي تشهد تزايدا واضحا في المنطقة العربية وخاصة في ظلا انتشار واستخدام الأنظمة المعلوماتية، وتعد دولة الإمارات المتحدة من أكثر الدول العربية تعرضا لهذا النمط الإجرامي المستحدث نظرا لاعتمادها الكبير على أجهزة الحاسوب وعلى شبكات المعلوماتية في إنجاز أعمالها، خاصة وأن دولة الإمارات قطعت مراحل متقدمة في مجال تطبيق مشروع الحكومة الالكترونية، وقد كشف أحد المواقع الالكترونية مؤخرا أن خمسة وخمسين مواطن إماراتي خلال فترة وجيزة كانوا ضحية لعمليات الاحتيال المعلوماتي.[1]

الفرع الأول: تعريف الاحتيال المعلوماتي

يرى البعض أن الاحتيال المعلوماتي أو الغش المعلوماتي هو"كل سلوك احتيالي يرتبط بعملية التحسيب الالكتروني بهدف كسب فائدة أو مصلحة مالية".[2]

هذا التعريف في حقيقة الأمر يشمل كل أشكال غش الحاسوب، والمتمثلة بالاعتداء على المعطيات المختزنة في النظام المعلومات والمتبادلة عبر قنوات النظام، بما تمثلها من أموال وخدمات بغرض الحصول على منفعة مادية.

وقد تعددت التعريفات التي قيلت في شأنه، ومن هذه التعريفات:

[1] انظر الموقع الالكتروني:
www. G4me.com/etesalat/article.jsp
بتاريخ 09- 08- 2010 على الساعة 30: 9

[2] محمد أمين أحمد الشوابكة، مرجع سابق، ص. 181.

"إن الاحتيال المعلوماتي يتحقق كلما كانت هناك نية تحقيق ربح مادي غير مشروع للجاني، ينتج عنه خسارة مادية تلحق بالمجني عليه وكان استخدام الحاسوب وسيلة لارتكاب الاحتيال أو تسهيله أو التعجيل بتنفيذه".[1]

كما عرفته هيئة الأمم المتحدة أنه: "إدخال البيانات أو محوها أو تعديلها أو كتابتها أو برامج الحاسوب أو التدخل المؤثر في معالجة البيانات التي تسبب خسارة اقتصادية أو فقد حيازة ملكية شخص آخر بقصد الحصول على كسب اقتصادي غير مشروع له أو لشخص آخر".[2]

كما عرفته إحدى الدراسات التي أجريت في الولايات المتحدة الأمريكية أنه: "فعل أو مجموعة من الأفعال غير المشروعة والمتعمدة التي ترتكب بهدف الخداع أو التحريف للحصول على شيء ذو قيمة، ويكون نظام الحاسوب لازما لارتكابها".[3]

ويذهب البعض الآخر إلى تعريفه أنه: "التلاعب العمدي بمعلومات وبيانات تمثل قيما مادية، يختزنها النظام المعلوماتي أو الإدخال غير المصرح به لمعلومات وبيانات صحيحة أو التلاعب في الأوامر والتعليمات التي تحكم عملية البرمجة أو أية وسيلة أخرى من شأنها التأثير على الحاسوب حتى يقوم بعملياته بناء على هذه البيانات أو الأوامر أو التعليمات، من أجل الحصول على ربح غير مشروع وإلحاق ضرر بالغير".[4]

والربح غير المشروع الذي يحققه الجاني باعتباره نتيجة لارتكاب جريمة الاحتيال المعلوماتي قد يتخذ أحد الشكلين:

---

[1] قورة نائلة، مرجع سابق، ص. 443.
[2] قدح خليل، الجرائم المرتكبة بواسطة المعلومات، ورقة عمل مقدمة لمؤتمر القانون والحاسوب، جامعة اليرموك، ص. 6.
[3] يونس عرب، دليل أمن المعلومات والخصوصية، مرجع سابق، ص. 416.
[4] قورة نائلة، المرجع نفسه، ص. 444.

- الأول: يتحقق بشكل مباشر، كقيام الفاعل بتحويل مبلغ من المال إلى حسابه الخاص.
- الثاني: يتحقق بشكل غير مباشر عندما يتخلص الفاعل من تسديد مبلغ من المال يقع على عاتقه التزاما بأدائه، ومن الأمثلة على ذلك الاستخدام غير المصرح به من قبل الفاعل للشيفرة أو الكلمة السرية لشخص آخر للدخول إلى إحدى النظم المعلوماتية، ويترتب على ذلك أن يتحمل المجني عليه نفقات هذا الدخول.

والاحتيال المعلوماتي شأنه في ذلك شأن جرائم المعلوماتية بوجه عام، يمكن أن يكون مرتكبه من المصرح لهم باستخدام الحاسوب والدخول إلى نظامه أو أن يكون غير مصرح لهم بذلك، إلا أنه من الثابت أن حالات الاحتيال بواسطة الحاسوب لجني المال تأتي في جانبها الأكبر من داخل الجهات المجني عليها لا من خارجها، فمرتكبي الاحتيال المعلوماتي هم عادة أشخاص لديهم السلطة في التعامل مع المعلومات التي يحتويها النظام المعلوماتي، حتى أنه قد أطلق على التحايل المعلوماتي أنه جريمة داخلية إشارة إلى حدوثه داخل المؤسسة المجني عليها وبواسطة أحد المنتمين إليها.[1]

وقد أثبتت دراسة أجريت في ألمانيا أن أكثر من 90 % من حالات التلاعب المعلوماتي التي تم اكتشافها قد تم ارتكابها بواسطة عاملين في المؤسسات المجني عليها.[2]

وفي دراسة أجراها معهد بنيويورك للأبحاث، تبين أن ثلاثة أرباع حالات الاحتيال المرتبط بالحاسوب قد تمت عن طريق أشخاص من داخل المؤسسات

[1] محمد أمين أحمد الشوابكة، مرجع سابق، ص. 183.
[2] قورة نائلة، مرجع سابق، ص. 445.

المجني عليها، وهناك دراسة أخرى أجريت في السويد على مجموعة من قضايا الاحتيال التي استخدم الحاسوب في ارتكابها، حيث تبين أن 81% من مرتكبي الاحتيال ينتمون وظيفيا إلى الجهات المجني عليها.[1]

من خلال الملاحظة في هذه المعلومات يتضح أن مرتكبي هذه الجريمة من نخبة المجتمع، أي من ذوي المناصب الرفيعة المستوى وذوي التخصصات والكفاءات العالية، ويتمتعون بالذكاء وبالقدرة على التكيف الاجتماعي، فللاحتيال المعلوماتي هو إجرام الأذكياء بالمقارنة بالاحتيال التقليدي.

فالسلوك الإجرامي للمجرم المعلوماتي يعتمد على التقنيات الحديثة من حيث استغلاله للتطور التكنولوجي الذي تشهده المعلوماتية ويتضح ذلك من خلال الوسائل التي يستخدمها المجرم في تنفيذه لجريمته.

الفرع الثاني: وسائل الاحتيال المعلوماتي

أساليب ارتكاب جريمة الاحتيال المعلوماتي متنوعة ومتطورة تبعا للتطور التكنولوجي الذي تشهده المعلوماتية، وكان لتنوع أنظمة التحويل الالكتروني للأموال دور كبير في تنامي هذه الجريمة وتطور أساليب ارتكابها، وخاصة مع زيادة عدد المبرمجين والمشتغلين في مجال الأنظمة المعلوماتية.

وسنقوم بعرض أهم الأساليب التقنية المستخدمة في ارتكاب جريمة الاحتيال المعلوماتي، ونعرض كذلك بعض الأمثلة العملية التي تم فيها استخدام هذه الأساليب التقنية لفهم طبيعة عملها بشكل أوضح.

- **التلاعب في مرحلتي إدخال وإخراج البيانات:** يعد هذا السلوك من أكثر حالات الاحتيال المعلوماتي حدوثا نظرا لما يتميز به من سهولة، وقد ظهر

[1] المرجع نفسه، ص. 446.

أن 62 % من حالات الاحتيال المعلوماتي التي تم اكتشافها في الولايات المتحدة الأمريكية تنطوي على تلاعب بالبيانات قبل وأثناء إدخالها إلى جهاز الحاسوب.[1]

وتتمثل عملية إدخال المعلومات المزورة في تغذية النظام المعلوماتي بالمعلومات المراد معالجتها آليا، وقد تتم عملية الإدخال عن طريق الشخص نفسه الذي قام بالتلاعب في المعلومات، أو عن طريق شخص آخر قد يكون حسن النية، وهناك وسائل عدة للتلاعب بالمعلومات والبيانات في هذه المرحلة سواء أتم ذلك أثناء عملية الإدخال أو في مرحلة إعداد المعلومة للإدخال، ويمكن حصرها في ثلاثة وسائل رئيسية:[2]

أ. الوسيلة الأولى: تتمثل هذه الوسيلة في تغيير المعلومات والبيانات المراد إدخالها إلى النظام دون أن يتضمن ذلك حذفا لجزء أو أجزاء منها، سواء أتم ذلك في مرحلة الإدخال أو قبل ذلك أي أثناء إعداد هذه المعلومات للإدخال، وقد يكون هذا التغيير كليا أي يشمل المعلومة بأكملها، أو جزئيا يتعلق بجزء دون الآخر، كما قد يتمثل في إضافة جزء لها ليس فيها أو استبدال معلومة أخرى، ويؤدي كل ما سبق إلى تغيير معنى المعلومة حيث تصبح غير معبرة عن الحقيقة التي كانت تمثلها.

ب. الوسيلة الثانية: من أساليب التلاعب بالبيانات في مرحلة الإدخال حذف لجزء من المعلومة أو لعدة أجزاء منها، بل إن الأمر قد يتعدى ذلك

[1] انظر الموقع الالكتروني:
www.almyaseer.gov.sa./forum/topic.asp.arctlive
بتاريخ: 13- 10- 2010 على الساعة 30: 15

[2] نهلا عبد القادر المومني، مرجع سابق، ص. 190.

إلى حذف المعلومة بأكملها أو عدم إدخالها إلى النظام المعلوماتي ويترتب على ذلك أيضا تغيير معنى المعلومة أو عدم وجودها ابتداء.

ج. الوسيلة الثالثة: تتمثل هذه الوسيلة في إعاقة المعلومة عن أداء وظيفتها ويتم ذلك عن طريق إدخال المعلومة مع إخفائها وذلك بأن يتم إدخالها في غير المكان المخصص لها، وهو ما يؤدي إلى إعاقة هذه المعلومة عن أداء الدور الذي كان مقررا لها.

ومن بين الأمثلة على الاحتيال المعلوماتي الذي يتم عن طريق التلاعب بالبيانات المدخلة:

بناء على إرسالية واردة من وزارة العدل الأمريكية (المكتب الفدرالي للتحقيقات) تفيد بتعرض المنظومة المعلوماتية لمؤسسة أمريكية (ساقونات واركس) Sago Net Works التي تعتبر بنك معلوماتية جهوية كبيرة بولاية فلوريدا الأمريكية، وتعود الوقائع إلى تاريخ 2009/04/08 أين استلمت مؤسسة ساقونات واركس في بريدها الإلكتروني من طرف شخص مجهول صاحب علبة البريد الالكتروني White hartary@gmail. Com وأكد من خلاله أنه اكتشف طريقة للدخول عن طريق الغش إلى المعطيات الالكترونية لهذه المؤسسة عبر نظام المشتغل Logiciel والمسمى Ubersmith المرتبط بشبكة الإنترنت، وبتاريخ 2009/04/10 تلقت نفس المؤسسة بريدين الكترونيين من العنوان:White hartax@gmail. Com يحمل تصريح صاحبه بأن جميع المعطيات والمعومات الخاصة بمؤسسة SAGO تم استئنافها وهي بحوزته وتضمن البريد صورة شاشة لقائمة المواد الإلكترونية التابعة للمؤسسة، أمما البريد الثاني فجاء فيه عبارة Bonne Tentative كرد للمؤسسة بعد اكتشافها للاختراق الواقع على نظامها

المعلوماتي، وقد استعمل الشخص المجهول عناوين الالكترونية موزعة بالجزائر والتابعة لاتصالات الجزائر "فوري" وبعدها بتاريخ 2009/04/10 تلقت مؤسسة SAGO رسالة مجهولة يطلب من خلالها مبلغ مالي مستعملا العنوان الالكتروني: 412211637 التابع لاتصالات الجزائر "فوري" وبتاريخ 2009/04/16 تلقت المؤسسة بريدا الكترونيا من طرف صندوق بريد يحمل عنـــوان manoj@yahoo.com Schizophrenic يخطرهم بأن نظامهم قد اخترقه وأن المعلومات الخاصة بالصرف التي تسمح باختراقه معروضة للبيع على موقع Unknown.wn.

ومن خلال مجموعة من المعلومات تمكنت الضبطية القضائية بالجزائر من تحديد هوية الشخص الذي اخترق الموقع والمعطيات الالكترونية لشركات أجنبية بما فيها شركة ساقونات ووركس والذي كان يستعمل الخط الهاتفي لشخص آخر يقيم بمدينة باتنة (الجزائر)، وقد تعرفوا بأن المشتبه فيه هو شخص آخر كان يستعمل شبكة الانترنت ADSL FAWRI غير صاحب الخط الأصلي، وتم استعمال عنوان بروتوكول الانترنت (IP) وهو 113. 110. 97. 41 تابع لمؤسسة اتصالات الجزائر فوري وتم الدخول من قبل المشترك على خط شخص آخر، وبعد توقيفه من طرف الضبطية القضائية تم العثور على أجهزة الإعلام الآلي وملحقاته ومبلغ مالي بالعملة الوطنيـــة مقدر بـــ"21900 دج"" وكذلـــك31 وصل للحوالات المالية عن طريق وسترن يونيون باسمه، وقد أكد المتهم أنه فعلا قام باختراق عدة مواقع ومعطيات معلوماتية لعدة شركات أجنبية وذلك عن طريق القرصنة وأنه كان يستعمل خلال هذه العمليات عدة عناوين الكترونية

واستحدث من خلالها أسماء خاصة بها أرقام سرية، كما أقر أنه يقوم بعمليات الاختراق والقرصنة منذ 2006.[1]

قيام أحد مدخلي البيانات العاملين في إحدى الشركات المساهمة عام 1994 في الأردن بتسجيل (87300) سهم بأسماء شركات وهمين وإخراج شهادات بملكية الأسهم لمالكيها، ومن ثم قيامه ببيعها في السوق المالية وبمبلغ يزيد على (190) ألف دينار أردني.[2]

أما التلاعب في مرحلة إخراج البيانات، فهذه الوسيلة تعد أقل حدوثا بالمقارنة بغيرها من وسائل الاحتيال المعلوماتي، ففي التقرير الصادر عن لجنة المراجعة في المملكة المتحدة عام 1985 كانت هناك حالتان فقط من بين 77 حالة احتيال معلوماتي قد تمت عن طريق التلاعب بالبيانات في اللحظة التي يتم فيها إخراجها من جهاز الحاسوب، فالاحتيال في هذه الحالة أن المعلومات دخلت صحيحة إلى النظام المعلوماتي وأن التلاعب تم قبل عملية إخراج المعلومات.[3]

- **التلاعب في البرامج:** تتميز هذه الوسيلة أنها على قدر كبير من التعقيد، وتحتاج إلى خبرة ومعرفة فنية في مجال البرمجة، كما أنها تعتبر من أكثر وسائل الاحتيال المعلوماتي خطورة، ويتم التلاعب في البرامج بصفة عامة عن طريق إحدى الوسيلتين:[4]

أ. **الوسيلة الأولى:** تتمثل هذه الوسيلة في تغير البرامج المطبقة بالفعل داخل المؤسسة المجني عليها، بإدخال تعديلات غير مرخص بها على البرامج المستخدمة، فكثير من البرامج بعد إعدادها واختبارها قد تمر

[1] مجلس قضاء باتنة، الغرفة الجزائية، قرار رقم 10/05805 المؤرخ في 2010/07/04، ص. ص. 2_3، غير منشور.
[2] قندح خليل، مرجع سابق، ص. 08.
[3] قورة نائلة، مرجع سابق، ص. ص. 458_459.
[4] المرجع نفسه، ص. ص. 462_463.

ببعض التعديلات لتصويب أخطاء اكتشفت بعد العمل بها وهو ما يتيح في هذه الحالة إدخال تغييرات من شأنها أن تساعد الجاني على إتمام جريمته وكذلك إخفائها، كما قد يتم إجراء هذا التعديل عن طريق استخدام البرامج الخبيثة (الفيروسات).

ب. **الوسيلة الثانية:** تتمثل هذه الوسيلة في تطبيق برامج إضافية، وهذه البرامج الإضافية قد يتم كتابتها عن طريق الجناة أنفسهم أو قد تكون برامج معدة سلفا تهدف بشكل أساسي إلى تعديل المعلومات في الحواسيب عن طريق إجراء تعديلات مباشرة في ذاكرتها.

ومن بين الأمثلة التي تبين ماهية التلاعب بالبرامج كوسيلة من وسائل الاحتيال المعلوماتي:

قيام مبرمج يعمل بأحد البنوك في الولايات المتحدة الأمريكية بتعديل برنامج إدارة الحاجات الخاصة بالبنك، حيث يضيف عشرة سنتات لمصاريف إدارة الحسابات الداخلية على كل عشرة دولارات ودولارا واحدا على الحسابات التي تتجاوز عشرة دولارات، وذلك باستخدام تقنية تدعى تقنية (Salami)،[1] وقد تم تسجيل المصاريف الزائدة في حساب خاص فتحه باسم مستعار هو (ZZwiche) وبهذه الطريقة حصل على عدة مئات من الدولارات في الشهر، وكان بالإمكان أن يستمر هذا الأمر والسلوك الإجرامي لولا أن البنك أراد بمناسبة تأسيس شركة جديدة للدعاية أن يكافئ أول وآخر عميل له وفقا للترتيب الأبجدي للحروف وحينئذ اكتشف عدم وجود ما يسمى(ZZzwicke).[2]

[1] يطلق الخبراء اسم SALAMI على عملية استقطاع الشرائح الصغيرة من حسابات متعددة لصالح فرد واحد، ويطلق هذا الأسلوب بكثرة في البنوك حيث تقرر الفوائد على الحسابات الجارية التي ترتضي حساباتها الشهرية بإزالة الكسور العشرية التي تمثل مبالغ لا تكاد تذكر،أنظر محمد أمين الشوابكة

[2] محمود أحمد عبابنة، مرجع سابق، ص. 121.

تقنية أخرى تدعى (Pereoque) تقوم على برمجة الحاسوب حيث يستقطع بعض السنتيمات من الإيداعات الدورية و تحويلها إلى حسابه الخاص.[1]

- **التلاعب في البيانات التي يتم تحويلها عن بعد:** هذه الوسيلة من وسائل الاحتيال المعلوماتي يتم ارتكابها عادة من قبل أشخاص من خارج المؤسسة المجني عليها، وقد كان للتزايد الكبير في استخدام نظم معالجة البيانات عن بعد في السنوات الأخيرة تأثير كبير في تطوير الوسائل المختلفة المستخدمة في مجال تكنولوجيا المعلومات.

فالتلاعب في البيانات عن طريق النهاية الطرفية أيا كان موقعها جعل الاحتيال أكثر سهولة من ناحية وأكثر صعوبة في اكتشافه من ناحية أخرى، فيكفي أن يكون الحاسوب متصلا بوحدة التشغيل المركزية عن طريق شبكة الخطوط الهاتفية العادية أو غيرها من وسائل الاتصال حتى يتمكن الفاعل من إتمام عملية الاحتيال من داخل منزله مستخدما وحدته الطرفية دون الحاجة إلى الدخول إلى المؤسسة المجني عليها.[2]

فهذه الوسيلة التقنية تمكن الجاني من أن يرتكب السلوك الإجرامي المكون للركن المادي لجريمته في دولة ما، وتحقيق النتيجة الإجرامية في دولة أخرى.

ومن أمثلة ذلك قيام خبير برمجة يعمل في مصرف أمريكي ويدعى (Stanly Kifkin) بالوصول إلى غرفة توصيلات النقل لبنك (Security Pacific) وتمكن من الحصول على الشيفرة التي يستخدمها هذا البنك، وقام بعد ذلك بالاتصال بشبكة معلومات البنك عن طريق الهاتف

[1] المرجع نفسه، ص. 122.
[2] نهلا عبد القادر المومني، مرجع سابق، ص. 194.

مستخدما الشيفرة التي حصل عليها وقام بزرع فيروس في الشبكة مهمته تحويل مبالغ مالية من حسابات العملاء إلى حسابه الخاص في نيويورك.[1]

- **استعمال كلمة سرية غير صحيحة للدخول إلى نظام مدفوع الأجر**: تعد هذه الوسيلة صورة من صور الاحتيال المعلوماتي التي قد يستعين بها الجاني لتحقيق كسب غير مشروع، ويعد استعمال شيفرة غير صحيحة من أهم الوسائل للدخول غير المشروع إلى نظام مدفوع الأجر، والمقصود باستعمال شيفرة غير صحيحة هو الدخول إلى الأنظمة المعلوماتية مدفوعة الأجر باستعمال كلمة سر مملوكة إلى شخص آخر أو باستعمال شيفرة مملوكة للنظام نفسه، فليس المقصود أن تكون هذه الشيفرة غير صحيحة في ذاتها وإنما تستمد عدم صحتها من استخدامها من قبل شخص لا حق له في ذلك.

الفرع الثالث: مدى إمكانية انطباق نصوص جريمة الاحتيال التقليدية على جريمة التحايل المعلوماتي

يعرف الاحتيال بأنه، كل تظاهر أو إيحاء يكون صالحا لإيقاع المجني عليه في الغلط بطريقة تؤدي إلى الاقتناع المباشر بالمظهر المادي الخارجي، أي أن المجني عليه في جريمة الاحتيال هو: من جازت عليه حيلة الجاني فانخدع بها وسلمه ماله.[2]

والاحتيال لا يقع على الشخص الطبيعي فقط، بل إنه من المسلم به صلاحية الشخص المعنوي لاعتباره مجنيا عليه، فالشركات والمؤسسات العامة أو الخاصة هي من الأشخاص الاعتبارية في نظر القانون، وحيث أن الحاسوب والشبكات

[1] المرجع نفسه.
[2] محمد أمين أحمد الشوابكة، مرجع سابق، ص. 185.

الداخلية للمنشأة تعد من فروع الشركة أو المؤسسة، فإنها تكون صالحة لوقع فعل الخداع أو التحايل عليها.[1]

وقد نص قانون العقوبات الجزائري في نص المادة 372 ق. ع على ما يأتي: "كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات أو إلى الحصول على أي منها أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500 إلى 20.000 دج".[2]

ويتضح من استقراء نص المادة 372 ق. ع الجزائري أن أركان جريمة النصب تتمثل في الركن المادي والذي يتكون من فعل الاحتيال (سلوك) ثم استيلاء الجاني على منقول مملوك للغير(نتيجة)، وعلاقة سببية بين السلوك والنتيجة الإجرامية التي تحققت، والركن الآخر هو الركن المعنوي والذي يتطلب توافر قصد خاص بجانب القصد الجنائي العام.

غير أن هذه المادة من قانون العقوبات الجزائري لم تعالج صورة الاحتيال المعلوماتي بصورة مباشرة، فالإشكالية تطرح في الحالة التي يتلاعب فيها الجاني في البيانات المعالجة آليا أو البرامج المعلوماتية توصلا للاستيلاء على مال الغير. ومثال ذلك قيام الجاني بالتلاعب في البيانات المخزنة أو المدخلة إلى الحاسب الآلي

[1] المرجع نفسه.
[2] قانون العقوبات الجزائري، القانون رقم 06-23 المؤرخ في 20 ديسمبر سنة 2006.

أو التلاعب في البرامج المعلوماتية أو التلاعب في النبضات الالكترونية المرسلة من الحاسب الآلي إلى الحاسبات ذات النهايات الطرفية.[1]

وقد تم سد الفراغ القانوني الذي عرفه هذا المجال بصدور القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات الذي نص على حماية جزائية لأنظمة المعلوماتية من خلال تجريم كل أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات بغرض القيام بأفعال الاحتيال والغش المعلوماتي. ومن خلال المادة 394 مكرر يتبين لنا أن الغش المعلوماتي يتخذ صورتين هما:

- الدخول في منظومة معلوماتية.
- المساس بمنظومة معلوماتية.

وسنتطرق إلى المواد 394 مكرر و394 مكرر 7 بالتحليل في مبحث تفاديا للتكرار.

وبوجه عام وبالرجوع إلى القسم الثاني من قانون العقوبات الجزائري والذي نظم فيه جريمة النصب والاحتيال تحت نص المادة 372 ق. ع،[2] نجد أن المشرع الجزائري قد أورد ثلاث طرق للاحتيال هي:

- استعمال وسيلة من وسائل التدليس وذلك باستعمال أسماء أو صفات كاذبة غير صحيحة ولو لم يصحب ذلك استعمال مناورات احتيالية، أي أن هذه

[1] يرى البعض عدم صلاحية البرامج للخضوع للنشاط الإجرامي للنصب، على سند من القول أنه لا يوجد نشاط مادي يتحقق به التسليم والاستيلاء في جريمة النصب، وحتى ولو فرضنا جدلا إمكانية وقوع التسليم والاستيلاء في هذه الحالة فإنه لن ينتج عن ذلك حرمان المجني عليه من المعلومات التي نقلها بالقول بل تظل تحت سيطرة من نقلها وفي حوزته، وهو ما يعني أن ما سبق قوله يتفق مع طبيعة المعلومات والبرامج المعلوماتية، في حين لا يتفق مع طبيعة النشاط الإجرامي في جريمة النصب. انظر: محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004، ص. 118.

[2] يقابل هذه المادة في القانون الفرنسي المادة 405 ع. ف وتناولها القانون المصري في المادة 336 ع. م والذي نص على أن جريمة النصب يتطلب لتوافرها أن يكون ثمة احتيال وقع من المتهم على المجني عليه بقصد خداعه والاستيلاء على ماله فيقع المجني عليه ضحية هذا الاحتيال الذي يتوافر باستعمال طرق احتيالية، كاتخاذ اسم كاذب أو انتحال صفة غير صحيحة أو التصرف في مال الغير ممن لا يملك التصرف فيه. انظر: محمد علي العريان، الجرائم الالكترونية، دار الجامعة الجديدة، الإسكندرية، 2004، ص. 123.

الجريمة بانتحال شخصية الغير أو اسم الغير بحيث تنخدع الضحية، وقد قضي في فرنسا بقيام جريمة النصب عن طريق استعمال اسم كاذب في حق شخص يستعمل بطاقات دفع مسروقة لتسديد قيمة البضائع التي يشتريها وذلك بالتوقيع على الوثائق التي يقدمها له الباعة.[1]

- استعمال المناورات الاحتيالية، يمكن تعريفها بأنها كذب مصحوب بمظاهر خارجية، فلا تتحقق المناورة الاحتيالية بمجرد الأقوال والادعاءات الكاذبة ولو كان قائلها قد بالغ في التوكيد، بل أن المناورة تتحقق إذا اصطحب الكذب أعمال مادية أو مظاهر خارجية يستعين بها المتهم لإقناع الضحية، كإيهام الناس بوجود مشاريع كاذبة، أو الإيهام بوجود سلطة خيالية أو اعتماد مالي خيالي أو إحداث الأمل في الفوز أو الخشية من وقوع حادث أو واقعة وهمية.
- الاستيلاء على مال الغير ويتعلق الأمر بالأموال والمنقولات والسندات والتصرفات والأوراق المالية والوعود والمخالصات والإبراءات من الالتزامات.[2]

عرفت المادة 1/313 من قانون العقوبات الفرنسي الاحتيال (النصب) على أنه: "واقعة خداع شخص طبيعي أو معنوي، سواء باستعمال اسم كاذب أو صفة كاذبة أو التعسف في صفة غير صحيحة أو باستعمال حيلة تدليسية من شأنها حمل الغير على تسليم أموال أو قيمة أو مال أو تقديم خدمة أو الموافقة على عمل ينتج عنه التزام أو تحرر من التزام".[3]

[1]. احمد بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، دار هومة، الجزائر، 2009، ص. 317.
[2] المرجع نفسه.
[3] محمد أمين أحمد الشوابكة، مرجع سابق، ص. 182.

فإذا كان سلوك ممارسة الأفعال الاحتيالية على الأشخاص الطبيعية أو الاعتبارية ممكنا فإن التساؤل المطروح هو مدى إمكانية ممارسة أفعال الاحتيال على الحاسب الآلي وإيقاعه في الغلط ؟

- **مدى إمكانية الاحتيال على الحاسوب والنظام المعلوماتي المرتبط به:** ذهب جانب من الفقه إلى القول بأن التلاعب في البرامج والبيانات والتغيير فيها بما ترتب عليه إيهام المجني عليه بصحتها مما يجعله يسلم بها، يعد من أحد أساليب التحايل، وحسب هذا الاتجاه فإن الحاسوب ليس سوى مجرد وسيط للتحايل.[1]

أما في الفقه الفرنسي، فقد ذهب البعض إلى أن غش الحاسوب وخداعها للاستيلاء على الأموال تتحقق به صفة الطرق الاحتيالية، وبالتالي قيام جريمة الاحتيال، واستندوا في ذلك على أن إدخال وسائل الغش أو خداع الأنظمة المعلوماتية يدخل ضمن الطرق الاحتيالية، وأن خداع الآلة يمكن تصوره على أساس أنه يوجد خلف الآلة إنسان، وهو من قام ببرمجة هذه الآلة، ويعتبر هذا الرأي أن المعلومات المدخلة إلى النظام المعلوماتي تمثل وقائع تدعم الكذب المصاحب للخداع.[2]

ويذهب البعض الآخر إلى القول بعدم تحقيق واقعة الاحتيال على الحاسب الآلي ونظامه المعلوماتي، وأن استخدام وسائل الغش والخداع في أنظمة الحاسب للاستيلاء على الأموال لا تدخل ضمن نطاق الطرق الاحتيالية، وحجتهم في ذلك ما تبنته الأحكام الفرنسية التي تنطوي بالضرورة

[1] هدى حامد قشقوش، جرائم الحساب الالكتروني في التشريع المقارن، دار النهضة، القاهرة، 1992، ص. 133.
[2] محمد أمين الشوابكة، المرجع نفسه، ص. 185.

على وجود علاقة مباشرة بين شخصين (المخادع والمخدوع) وهو ما ينتفي في هذه الحالة.[1]

وقد تباينت التشريعات في مدى تحقق ممارسة أفعال الاحتيال على الحاسب الآلي وإيقاعه في الغلط، وهذا ما يتضح في ثلاث اتجاهات:

أ. **الاتجاه الأول:** تشريعات هذا الاتجاه تستلزم لقيام جريمة الاحتيال أن يكون المخدوع شخصا طبيعيا (إنسان)، ومن ثم لا يعقل -وفقا لهذا الاتجاه- خداع الحاسب الآلي بوصفه آلة، وبالتالي عدم انطباق نصوص الجريمة الاحتيال التقليدية على خداع الحاسب الآلي ونظامه المعلوماتي لافتقاره لأحد العناصر الضرورية.[2]

وبناء على هذا الاتجاه فإن من يمارس وسائل احتيالية في مواجهة نظم المعالجة الآلية للبيانات بغية تحقيق منفعة مادية أو الحصول على خدمة لا يسأل عن جريمة الاحتيال بمفهومها التقليدي، إذ يفترض في عملية الخداع أن تفوت على المجني عليه التفكر فيما يعرض عليه من أمور مغايرة للحقيقة أو الصواب، مما يؤدي إلى إيقاعه بالغلط والتصرف تبعا لذلك.

فنظام معالجة البيانات –العقل الالكتروني– يفتقر إلى خاصية التفكير فهو ينفذ أوامر يتلقاها مسبقا أو يتلقى أسلوب معالجتها. علاوة على أن معطيات الحاسوب (محل الجريمة) ذات طبيعة معنوية، وتفتقر إلى كونها مالا منقولا، ذات طبيعة مادية، وهو ما اشترطه المشرع في محل جريمة الاحتيال.[3]

[1] علاء الدين مغايرة، الأوجه الحديثة للجرائم المعلوماتية، دار الحكمة، بيروت، 2002، ص. 31.
[2] سامي الشوا، مرجع سابق، ص. ص. 124_125.
[3] محمد أمين أحمد الشوابكة، مرجع سابق، ص. 187.

ووفقا لهذا الاتجاه فلابد من استحداث نصوص عقابية تجرم الاحتيال المعلوماتي، وذلك بما يتناسب مع طبيعة هذه الجريمة المستحدثة وهذا السلوك الإجرامي.

ب. **الاتجاه الثاني:** ترى تشريعات هذا الاتجاه إمكانية تطبيق النصوص الخاصة بجريمة النصب على الاحتيال المعلوماتي، ومن بين هذه التشريعات، تشريعات الدول الأنجلو سكسونية Anglo Saxon.[1]

ففي إنجلترا، فإن التفسير الموسع لنصوص قانون السرقة يشمل التلاعب في البيانات من أجل الحصـــول على منفعة ماديـــة، فنصـــت المادة 16 من قانون السرقة الصادرة سنة 1978 على أنه، يعاقب كل من حصل على نحو غير مشروع وبأي وسلة خداع –سواء لنفسه أو لغيره- على منفعة مالية.[2] وقد أدان القضاء الإنجليزي المتهم Thomson.V.R بجرم الاحتيال، وذلك في واقعة تتلخص في قيام (Thomson) الذي كان يعمل مبرمجا في أحد البنوك في الكويت بالإعتماد على برنامج، أمر الكمبيوتر بموجبه بتحويل كميات من حسابات بعض الزبائن المحفوظة على الكمبيوتر، والتي لم يجر عليها أي صفقات مالية لمدة من الزمن، لصالح حسابات أخرى كان قد فتحها بعد عودته إلى المملكة المتحدة في بعض البنوك، وكان قد علق تحويل هذه الأموال على تركه للخدمة في البنك المحول منه، وعندما فعل ذلك قام بعد عودته إلى انجلترا بالكتابة إلى مدير البنك آمرا إياه

[1] سعيد كامل، مرجع سابق، ص. 330.
[2] المرجع نفسه

بتحويل الأرصدة من حساباته في الكويت، وقد تم ذلك بالفعل، وعندما كشف أمره تمت إدانته بتهمة الحصول على أموال بطريق الخداع.[1]

وقد جرم المشرع الإنجليزي مسألة غش الكمبيوتر، بعد تصديقه لقانون استخدام الكمبيوتر عام 1990،[2] وهذا ما قام به المشرع الجزائري في القانون رقم 04-15 تحت عنوان المساس بأنظمة المعالج الآلية للمعطيات.

وفي كندا فإن المادتين (387-388) من قانون العقوبات يسهل تطبقها على النصب المعلوماتي، حيث أدان القضاء الكندي المتهمين بجريمة الشروع في النصب لاستخدامهم رقم حساب شخص آخر للولوج في النظام المعلوماتي، وكذلك الأمر بالنسبة لأستراليا، التي تبنت تفسيرا واسعا لمفهوم الاحتيال مستوحى من القانون الإنجليزي.[3]

ج. **الاتجاه الثالث:** تطبق تشريعات هذا الاتجاه القوانين الخاصة بالغش في مجال البريد والتلغراف والبنوك، وتطبيقها أيضا على الاتفاق الجرمي لأغراض ارتكاب الغش على حالات النصب المعلوماتي، ومنها تشريعات الولايات المتحدة الأمريكية، فقد أضفت بعض القوانين الفدرالية مفهوما واسعا للمال بحيث يشمل كل شيء ينطوي على قيمة،

---

[1] احمد الكركي، جرائم الحاسوب، ورقة عمل مقدمة إلى أكاديمية الشرطة الملكية، عمان، 1996، ص. 29.

[2] سعيد كامل، مرجع سابق، ص. 331.

[3] تنص المادة 387 من قانون العقوبات الكندي على أنه: يعد مرتكبا لعمل آثم كل من باشر عمدا:
أ. إتلاف أو تعديل البيانات.
ب. سرقة البيانات أو جعلها غير صالحة أو عديمة الفائدة.
ج. منع أو أعاق الاستخدام المشروع للبيانات.
د. منع أو أعاق شخص في استخدام حقه المشروع للبيانات أو رفض ولوج شخص له الحق في البيانات.
وقد استحدث قانون العقوبات الكندي المادة 1/301 والتي تنص على:
أ. كل من حصل بطريق الغش بواسطة جهاز الكتروني أو صوتي أو آلي مباشرة أو غير مباشرة على خدمات من حاسب آلي.
ب. كل من ولج بنية الغش بواسطة جهاز الكتروني أو صوتي أو آلي مباشرة أو بطريقة غير مباشرة إلى الحاسب الآلي.
ج. كل من استعمل حاسب آلي بطريقة مباشرة أو غر مباشرة بغرض ارتكاب جريمة منصوص عليها في الفقرة (أ- ب)، أو جريمة منصوص عليها في المادة 387 خاصة ببيانات أو بحاسب آلي عد مرتكبا لفعل إجرامي ويعاقب بالحبس لمدة 10 سنوات.
أنظر محمد سامي الشوا، مرجع سابق، ص. 162.

ويندرج تحت هذا التعريف الأموال المعنوية والبيانات المعالجة، وتعاقب هذه القوانين على الاستخدام غير المسموح به للحاسب الآلي، بغرض ارتكاب أفعال الغش أو الاستيلاء على الأموال.[1]

وقد تقدمت وزارة العدل الأمريكية في أوت 1984 بمشروع قانون يستهدف مباشرة حالة الغش المعلوماتي، والذي يعاقب كل من رتب أو صمم خطة ما أو حيلة بغرض ارتكاب غش أو الاستيلاء على مبلغ من النقود أو مال لا يخصه، وولج أو حاول الدخول في حاسب آلي بغرض تنفيذ أو محاولة تنفيذ هذه الخطة أو الحيلة أو لارتكاب أو محاولة ارتكاب مثل هذا النصب أو هذه السرقة أو الاختلاس.[2]

- **مدى اعتبار تسليم الأموال الكتابية (البنكية) عن طريق عملية القيد الكتابي تسليما ماديا تتحقق من خلاله النتيجة الجرمية لجريمة الاحتيال:** يقصد بالنقود الالكترونية (البنكية أو الكتابية)، تلك النقود التي يتم تداولها عن طريق نظم المعالجة الآلية للمعلومات، وبصفة خاصة في ظل نظم التحويل الالكترونية للأموال التي تعتمد على نظام معين بصورة متكاملة حيث يتم نقل الأموال من خلاله بشكل فوري.[3]

---

[1] محمد سامي الشوا، المرجع السبق، ص. 128.

[2] يعد من قبيل المال وفقا لمشروع القانون –السالف ذكره– كل الوسائل المالية والمعلوماتية التي تحتوي على بيانات معالجة والمكونات الالكترونية والكيانات المنطقة وبرامج الحاسب الآلي سواء بلغة الآلة أو بلغة مقروءة للإنسان، وكل قمة أخرى ذات طابع مادي أو معنوي، ويعد الولوج إلى أنظمة الحاسب الآلي جريمة تحت القانون الفيدرالي وقانون الاحتيال وإساءة استخدام الكمبيوتر متى كان هذا الدخول غير شرعي إلى:

أ. كمبيوترات الحكومة.

ب. أي حاسب آلي يحتوي على أسرار أو معلومات حكومية محددة كالبيانات المتعلقة بالدفاع الوطني أو العلاقات الأجنبية.

ج. أي كمبيوتر يسهل الحصول على تسجيلات مالية، وتكوين الأموال.

د. أي كمبيوتر يستخدم للحصول على معلومات بطاقات الائتمان.

تتراوح العقوبة الجنائية-بناء على شكل الاعتداء– بين الغرامة أو السجن من سنة واحدة وحتى 10 سنوات، وفي حالة العود تتراوح العقوبة بالسجن من عام حتى 20 عاما حسب الاعتداء المنوط به. انظر هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، ص. 153.

[3] عفيفي كامل، مرجع سابق، ص. 151.

وتقتضي جريمة الاحتيال التقليدي كما أسلفنا الذكر أن يقوم الجاني بحيازة المال محل الجريمة حيازة مادية وهي تستلزم كذلك أن يكون الاستيلاء ماديا من قبل هذا الجاني على المال، ولكن الصعوبة تأتي عبر كون هذا الاستيلاء قد تم عن طريق القيد الكتابي، كأن يتلاعب شخص في البيانات المخزنة في الحاسب الآلي كي يحول أرصدة الغير إلى حسابه.[1] فهل يعتبر هذا الاستيلاء استيلاء ماديا ومحققا للنتيجة الإجرامية لجريمة الاحتيال ؟

يرى البعض أن العبرة في الاحتيال المعلوماتي هو بقيام الحاسوب بوضع المال محل النشاط الإجرامي تحت تصرف الجاني وتحت تأثير الأساليب الاحتيالية التي مارسها الأخير، ولا يشترط أن يتم التسليم أو الاستيلاء بطريقة مادية وذلك بالمناولة اليدوية، وبالتالي فإن التحويل الالكتروني غير المشروع للأموال عن طريق عملية القيد الكتابي لا يتعارض مع مفهوم التسليم في جريمة الاحتيال التقليدي.[2]

وهذا ما يذهب إليه جانب كبير من الفقه الفرنسي، وهو الأمر الذي أكده كذلك القضاء الفرنسي، حيث ساوت محكمة النقض الفرنسية في بعض أحكامها بين تسليم النقود وبين الدفع الذي يتم عن طريق القيد الكتابي، فلقد ابتكرت المحكمة نظرية جديدة تعرف باسم نظرية "التسليم العادل" التي وضعت لمواجهة حالات الاحتيال الواقعة على ضريبة المبيعات وعلى عداد موقف السيارات وعلى الهواتف، وبعد ذلك أخذ الفقه بهذه النظرية حتى يلاحق بها أشكال النصب كلها باستخدام النظام المعلوماتي.[3] فالمحكمة عدلت

[1] محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004، ص. 128.
[2] الرومي محمد أمين، جرائم الكمبيوتر والانترنت، دار النهضة، القاهرة، 2003، ص. 66.
[3] سامي الشوا، مرجع سابق، ص. 132.

عن المفهوم التقليدي لفكرة التسليم واعتبرت أن مجرد القيد الكتابي يعادل التسليم.[1]

وقد اتجهت تشريعات الدول المختلفة من هذه المسألة إلى عدة اتجاهات متباينة:[2]

أ. اتجهت بعض الدول إلى الاعتراف للأموال الكتابية أو البنكية بصفة الأموال التي تصلح لأن تكون محلا لجرائم السرقة والاحتيال وخيانة الأمانة بالرغم من طابعها غير الملموس ومن هذه الدول كندا المادة (282/ 2 عقوبات) وهولندا المواد (310، 312، 223 عقوبات)، وسويسرا المواد (137، 140، 141 عقوبات)، وفي معظم الولايات المتحدة الأمريكية.

ب. اتجهت دول أخرى إلى عدم اعتبار النقود البنكية أو الكتابية من قبيل الأموال المادية، بل ينظر إليها باعتبارها ديونا لا تصلح محل لجرائم الاحتيال أو السرقة، كما هو الحال في التشريع الألماني، والياباني.

ج. دول أخرى التزمت قوانين العقوبات فيها الصمت فيما يتعلق بهذه المسالة، كما هو الحال في معظم تشريعات الدول العربية.

المطلب الثاني: الاحتيال باستخدام بطاقات الدفع الإلكتروني

تعتبر بطاقات الدفع الإلكتروني، أو بطاقات الائتمان[3] وسيلة دفع الكترونية تصدرها الجهة المصدرة لعملائها، بهدف تأدية الخدمات المصرفية

[1] جاء في الحكم الذي تبنت من خلاله المحكمة هذه النظرية (... وبالنظر إلى أن السند المثبت للانقضاء عن طريق الخصم من الدين المستحق لخزينة الدولة قد اصطنع من قبل الخاضع للضريبة، فهذا لا ينفي أحد العناصر المادية لجريمة النصب، ويظل الحال كذلك حتى لو لم يكن هناك تسليم لنقود طالما أن الدفع تم عن طريق العملة الكتابية التي تعادل تسليم النقود ...). انظر: محمود أحمد عبابنة، مرجع سابق، ص. 61.

[2] محمد علي العريان، مرجع سابق، ص. 128.

[3] ظهرت فكرة بطاقات الائتمان بالولايات المتحدة الأمريكية عام 1914 عندما قامت General Patroleum Corporation وتسمى الآن Mobil بإصدار بطاقة ائتمان للعاملين بها وبعض العملاء المميزين لديها، تمنحهم ائتمانا قصير الأجل لشراء احتياجاتهم من منتجات الشركة، على أن يقوموا بتسديد تلك المشتريات نهاية كل شهر، وسميت تلك البطاقة ببطاقة تسديد المدفوعات، وفي عام 1915، نقلت

بطريقة الكترونية عن طريق الحاسب الآلي، والتي تتولى القيام نيابة عن موظفي البنك بتأدية هذه العمليات المصرفية، من سحب نقود، لتحويل الأرصدة، وشراء السلع والخدمات وغير ذلك، وهذا ما شجع البعض من محترفي النصب على الدخول لمجال بطاقات الائتمان لتزويرها واستخدامها في النصب على التجار والبنوك.[1]

ويعتمد نظام بطاقات الدفع الالكتروني على عمليات التحويل الالكتروني من حساب بطاقة العميل بالبنك المصدر للبطـــاقة إلى رصيد التاجر بالبنك الذي يوجـــد به حسابه، وذلك من خلال شبكة التسويـــة الالكترونية للهيئات الدوليـــة[2] (هيئة الفيزا كارد Visa Card هيئة الماستر كارد Master Card).[3]

الفكرة لبعض المحال التجارية وقامت بإصدار بطاقة معدنية لعملائها المميزين، إلا أن هذه البطاقات لم تحقق الهدف المرجو منها، بسبب الظروف الاقتصادية التي كانت تواجه العالم نتيجة الحرب العالمة الأولى، ولكن في عام 1943 عادت فكرة البطاقات الائتمانية مرة أخرى على يد رجلين من رجال الأعمال يدعان Robert وRalph Schneider حيث أسسا مؤسسة تسمى بالداينرز كلوب Diners Club تكون وسيطا بين رجال الأعمال ومطاعم المدينة، وبعد نجاح الفكرة تم توسعة خدمت تلك المؤسسة لتشمل الفنادق والمطاعم و خطوط الطيران مع الحصول على عمولة نظير كل عملية دفع واشتراك سنوي من صاحب البطاقة، وانتشرت هذه البطاقة بين رجال الأعمال حتى وصلت في عام 1952 إلى 20 ألف بطاقة، وسرعان ما وصلت إلى مليون بطاقة في عام 1959، وفي إطار دخول البنوك تجربة الدفع بالبطاقة قام بنك Bank of American عام 1958 وهو أكبر بنك في و.م.أ بإصدار بطاقة Bank American card وقام بتعميم إصدارها لجميع فروعها المنتشرة في الساحل الغربي للولايات المتحدة الأمريكية. وفي الوقت نفسه قام بنك Chase Manhattan وهو ثاني أكبر البنوك في أمريكا بالسير على المنهج نفسه، وأول ظهور للبطاقات في أوربا كان عام 1963 حينما أصدرت الأمريكان إكبرس بطاقتها في إنجلترا، أما في فرنسا فقد قامت خمسة بنوك كبرى عام 1967 بالاتفاق على إصدار بطاقة وفاء سميت بالبطاقة الزرقاء La carte bleu للوقوف أمام زحف البطاقات الأمريكية. أنظر إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان، دار الجامعة الجديدة، الإسكندرية، 2007، ص. 33.

[1] جون كبريلك، موسوعة الهاكرز، ترجمة خالد العمري، دار الفاروق، الطبعة الثانية، 2003، ص. 45.

[2] ومن هذه الهيئات والمنظمات:

أ. مؤسسة الفيزا العالمية Visa International Service Association: المقر الرئيسي لها في الولايات المتحدة الأمريكية (كاليفورنيا)، أعضاؤها: المؤسسات والمنظمات المالية (البنوك التجارية)، وطبقا للإحصاءات أصدرت هذه المؤسسة 1.1 بليون بطاقة حول العالم: منها 5 ملايين بطاقة بمنطقة الشرق الأوسط وتعد بطاقتها بطاقة جمهور المتعاملين.

ب. مؤسسة ماستر كارد Master Card International Organization: كانت تسمى سابقا مؤسسة Master Chargeوالمقر الرئيسي لها: الولايات المتحد الأمريكية (سانت لويس، نيويورك) وأعضاؤها: المؤسسات والمنظمات المالية (البنوك التجارة)، وأصدرت حتى الآن 519 مليون بطاقة، 52 % منها داخل الولايات المتحدة الأمريكية و48 % في باقي دول العالم. ولديها 750.000 ماكينة ATM حول العالم و24 مليون تاجر يتعاملون بأجهزتها في 130 دولة.

ج. مؤسسة أمريكان إكسبريس American Express: المقر الرئيسي لها: و.م.أ أعضاؤها: فروع بنك أمريكان إكسبريس حول العالم فقط، لديها 55.2 مليون بطاقة في 77 دولة بقيمة تعاملات سنوية 297 بليون دولار.

د. مؤسسة الداينرز كلوب Diner's club international: المقر الرئيسي لها: الولايات المتحدة الأمريكية، وأعضاؤها: شركات السياحة، والفنادق، والمطاعم الكبرى، والبنوك التجارية، أصدرت 8 ملايين بطاقة في 200 دولة، ويتعامل من خلالها 6 ملايين تاجر، بقيمة تعاملات سنوية 35 بليون دولار.

ه. مؤسسة يورو كارد Euro Card: المقر الرئيسي لها: السويد، وأعضاؤها: معظم دول غرب أوروبا، وكانت تستخدم أولا كبطاقة ضمان للشيك، ثم تطورت بعد ذلك لتصبح بطاقات ائتمان ووفاء، وهذه المؤسسة ليس لها وجود فعلي، بمنطقة الشرق الأوسط.

و. مؤسسة J.C.B: المقر الرئيسي لها: اليابان، وأعضاؤها: المؤسسات المالية اليابانية، وتحمل هذه المؤسسات صفة العالمية، ولكنها لم ترق إلى مستوى المنظمات الأمريكية في حجم تعاملاتها وانتشارها حول العالم.

أنظر: إيهاب فوزي السقا، مرجع سابق، ص. 48.

[3] أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، 2000، ص. 113.

وكما أشرنا سابقا فقد أتاحت الثورة الرقمية لقراصنة المعلوماتية (المجرم المعلوماتي) إمكانية الحصول على أرقام البطاقات الائتمانية بواسطة برامج تشغيل، وذلك من خلال تزويد الحاسب بالرقم الخاص بالبنك مصدر البطاقة، إضافة إلى إمكانية التقاط هذه الأرقام عبر قنوات الإنترنت المفتوحة واستخدامها بطريقة غير مشروعة في عمليات التسوق عبر الشبكة، بحيث يتم خصم قيمة السلع من العملاء الشرعيين لهذه البطاقات.[1]

وبطبيعة الحال فإن بطاقة الائتمان بصورتها المادية لا تثير شكوكا في انطباق وصف الجرائم التقليدية للاعتداء على الأموال، ولكن التساؤل الذي يثور في هذا الصدد هو مسألة الاعتداء على البيانات السرية الخاصة ببطاقات الدفع الالكترونية، ومسؤولية الحامل الشرعي أو الغير(مصدر البطاقة، التاجر وغيرهم) عن فعل الالتقاط غير المشروع للبيانات السرية لبطاقة الائتمان عبر شبكة الإنترنت.

الفرع الأول: الغش باستخدام بيانات بطاقة الائتمان من قبل حاملها الشرعي

يقع الغش من قابل الحامل الشرعي لبطاقات الائتمان عبر شبكة الإنترنت إما بإساءة استخدام بيانات البطاقة أثناء مدة صلاحيتها، أو باستخدام بيانات البطاقة الائتمانية بعد انتهاء مدة صلاحيتها أو إلغائها، وذلك على النحو التالي:

- **إساءة استخدام بيانات البطاقة الائتمانية أثناء مدة صلاحيتها:** تتم إساءة استخدام بطاقة الدفع الالكترونية من قبل صاحبها عبر شبكة الانترنت عن طريق دفع ثمن السلع والخدمات التي تقدمها الشبكة بملء الاستمارة الالكترونية رغم علمه بأن رصيده بالبنك غير كافي لتغطية هذا المبلغ، أو أن

[1] محمد أمين احمد الشوابكة، مرجع سابق، ص. 193.

يقوم بإجراء تحويل الكتروني من رصيد لآخر متجاوزا رصيده في البنك مصدر البطاقة.[1]

وقد تأرجح موقف القضاء الفرنسي في اعتبار هذا الفعل جريمة حث ذهبت بعض الأحكام إلى اعتبار هذا السلوك سرقة، بينما ذهبت أحكام أخرى إلى اعتبار هذا السلوك من قبيل الطرق الاحتيالية التي تقوم بها جريمة النصب.[2]

وعلى العكس من ذلك ذهبت بعض الأحكام القضائية إلى أن استيلاء حامل البطاقة على مبالغ تتجاوز رصيده بوضعها في أحد أجهزة التوزيع الآلي المعدة لذلك لا تشكل أية جريمة جنائية، وقد أيدت محكمة النقض الفرنسية هذا الحكم عام 1982، حيث جاء في حيثيات حكمها "نظرا لأن محكمة الاستئناف ومن أجل الحكم ببراءة المتهم أثبتت أنه لكي يتمكن المتهم من إجراء السحوبات غير المشروعة فقد استخدم طبقا للقواعد الفنية لاستعمال الجهاز البطاقة بوصفه صاحبها، وحيث أنه بالنظر إلى ذلك، فقد بررت محكمة الاستئناف حكمها ".[3]

وقد اختلف أيضا موقف الفقه فما يخص تكييف الواقعة بين مؤيد ومعارض، فعارض أغلبية الفقه اعتبار أن فعل صاحب البطاقة المتجاوز الرصيد يعد نصبا استنادا إلى أن الجهاز مبرمج بواسطة البنك وهو القائم بالسماح للعميل بالسحب من عدمه، فإذا سمح الجهاز بتسليم النقود فلا تتوافر الطرق الاحتيالية لحمل الجهاز على تسليمه النقود، ولكن العميل قد اتبع

[1] محمد امين احمد الشوابكة، المرجع نفسه، ص. 194.
[2] جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، دار النهضة، القاهرة، 1999، ص. 42.
[3] محمود أحمد عبابنة، مرجع سابق، ص. 64.

الطرق الاعتيادية لاستعمال البطاقة البنكية، ولم يحدث أن استعمل طرقا احتيالية لإقناعه بوجود إئتمان وهمي.[1]

وينفي الفقه المعارض إصباغ وصف السرقة على الفعل، إذ أنه من المتعذر القول بأن حامل البطاقة قد اختلس المبالغ، التي حصل عليها عن طريق بطاقته دون رضاء البنك، حيث لا يستقيم هذا القول مع البرمجة الالكترونية لهذه الأجهزة على نحو يجعلها تستجيب لكل طلب مطابق للنظام المحدد سلفا من جانب البنك، فالتسليم تم عن رضا البنك وليس رغما عنه، وان المقدار الزائد من التسليم تم عن طريق الخطأ مما يحق للبنك بمطالبة العميل برد ما حصل عليه زيادة عن رصيده.[2]

كما ينكر أيضا هذا الفقه تطبيق وصف خيانة الأمانة على هذا السلوك، حيث إنه وإن صح أن البطاقة تظل بمقتضى العقد ملكا للجهة المصدرة لها، وبإمكانها إلغاؤها وطلب استردادها في أي وقت، ويتعين على العميل في هذه الحالة إعادتها للبنك وإلا اعتبر مرتكبا لجريمة خيانة الأمانة، إلا أن استيلاء حامل البطاقة على مبالغ نتيجة استخدامه للبطاقة أثناء فترة صلاحيتها ولو بالمخالفة لشروط العقد يشكل إخلالا بالتزام تعاقدي، ويذهب أنصار هذا الاتجاه إلى الحكم الذي تبنته محكمة النقض الفرنسية بقولها: "إن فعل العميل الذي يسحب بواسطة بطاقة ممغنطة مبالغ تجاوز رصيده في البنك لا يعدو أن يكون مجرد إخلال بالتزام تعاقدي ولا يقع تحت طائلة أي نص جنائي"، هذا الحكم فرق بين حالة قيام الحامل بإصدار شيك بدون رصيد، وبين حالة قيامه بسحب مبالغ تتجاوز رصيده لدى البنك، فالفعل الأول معاقب عليه

[1] أحمد حسام طه تمام، مرجع سابق، ص. 531.
[2] محمد سامي الشوا، مرجع سابق، ص. 109.

والثاني لا يقع تحت طائلة التجريم مع أن كلاهما أدوات وفاء، وكان من الأجدر على المشرع ألا يفرق بينهما.[1]

- **الغش باستخدام بيانات البطاقة الائتمانية بعد انتهاء مدة صلاحيتها أو إلغاؤها:**

أ. الاستخدام غير المشروع للبطاقة الملغاة في الوفاء: قد يقوم البنك مصدر البطاقة بإلغائها أثناء مدة صلاحيتها، وذلك كجزاء لسوء استخدام البطاقة من طرف العميل، فإذا ما تم إلغاء البطاقة من جانب البنك وتم إخطار العميل بذلك فإنه يتعين على هذا الأخير إعادة البطاقة لمصدرها، ومع ذلك قد يمتنع العميل عن ردها إلى مصدرها ويستمر في استخدام بياناتها، الأمر الذي يؤدي إلى التزام البنك بالوفاء بهذه المبالغ للتاجر، طالما أن هذا الأخير لا يعلم بإلغائها، إذ ينبغي على البنك أن يزود المتاجر بقائمة البطاقات الملغاة.

والتساؤل الذي يثور في هذا الصدد عن التكيف القانوني لفعل استعمال بيانات البطاقة الملغاة بمعرفة الحامل في الوفاء ؟ وللإجابة على هذا التساؤل نفرق بين حالتين:

1. حالة امتناع الحامل عن رد البطاقة بعد طلبها من البنك: إذ أن العلاقة ما بين العميل وبين البنك مصدر البطاقة الائتمانية هي علاقة تعاقدية تبقي بطاقة الائتمان بموجبها ملكا لمصدرها (البنك)، الذي يعهد إلى العميل استعمالها عند طلب البنك ذلك بناء على عقد بينهما، وهو أحد عقود الأمانة المنصوص عليها، ويمثل استخدام العميل للبطاقة الائتمانية بعد أن يتم إعلانه

[1] هدى حامد قشقوش، الصور الإجرامية لحالات السحب الإلكتروني من الرصيد، ورقة عمل مقدمة إلى ندوة الصور المستحدثة لجرائم بطاقات الدفع الإلكتروني، القاهرة، 1998، ص. 20.

لسحب البطاقة وامتناعه عن ردها تبديدا لشيء تم تسليمه على سبيل الاستعمال، وهو ما يشكل اختلاسا تقوم به جريمة خيانة الأمانة، ويكفي لتوافر الاختلاس لأن ينكر الحامل وجود البطاقة في حيازته لكي يتخلص من التزامه بالرد، ولا يشترط قيامه باستعمالها رغم مطالبة البنك بها.[1]

2. حالة استعمال الحامل للبطاقة الملغاة في الوفاء للتاجر: يعتبر استخدام الحامل لبيانات بطاقات الدفع الالكتروني الملغاة في الوفاء للتجار جريمة نصب، وذلك لأن مجرد ملء هذه البيانات على النموذج الإلكتروني يهدف إلى الإقناع بوجود ائتمان وهمي لا أ ثر له في الواقع، وليس مجرد كذب، ولا سيما أن إلغاء البطاقة يخلع عنها قيمتها كأداء ائتمان، وهذا بالإضافة إلى تحقق عنصر التسليم الذي يتمثل في قيام التاجر بتسليم المشتريات إلى الحامل الشرعي، أو تمكينه من الاستفادة بخدماته.[2]

ويرى البعض أن قيام الحامل الشرعي باستعمال البطاقة الملغاة في سحب النقود وإجراء التحويلات الالكترونية لأوراق لا يشكل جريمة إذ يفترض في أجهزة السحب الالكتروني المرتبطة مباشرة (On line) بحسابات العملاء في البنك أن ترفض إجراء أي سحب أو تحويل للنقود التي يطلبها الحامل إذ كانت تزيد عن رصيده في البنك.[3]

[1] جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان، مرجع سابق، ص. 78.
[2] المرجع نفسه، ص. 79.
[3] راجع الفقيه (JEAN DIDIER)، مشار إليه عند: جميل الصغير، نفس المرجع، ص. 82.

ب. الاستعمال غير المشروع للبطاقة منتهية الصلاحية في الوفاء: تسلم بطاقة الائتمان لمدة معينة ولأجل معين، عادة أو في غالب الأحيان تكون محددة بعام واحد، فإذا ما حل تاريخ الأجل وجب على العملاء أو حامل هذه البطاقة إعادتها إلى البنك الذي أصدرها، ولكن قد يحدث أن يمتنع العميل عن إعادتها إلى مصدرها ويستمر في استخدامها، مما يثير التساؤل عن التكيف القانوني لهذا الفعل.

ذهب الفقه إلى القول بأن الحامل الشرعي للبطاقة لا يرتكب جريمة النصب إذا ما قام بالوفاء للتاجر بموجب بطاقة منتهية الصلاحية، لأن الكذب الصادر عن الحامل ينصب على مدى صلاحية البطاقة لا على الإقناع بوجود ائتمان وهمي، وهو ما يمكن الكشف عنه بسهولة بواسطة التاجر الذي يلزم تعاقديا بالإطلاع على تاريخ صلاحية البطاقة المدون، ويرى هذا الفقه أن المسؤولية هنا تقع على التاجر، فيتحمل الضرر وحده إذا ما قبل الوفاء باستخدام بيانات بطاقة منتهية الصلاحية، لأنه أخل بأحد التزاماته التعاقدية كفحص تاريخ صلاحية البطاقة.[1] وكذلك يسأل التاجر كشريك في جريمة احتيال (النصب) إلى جانب الحامل الشرعي باعتباره فاعلا، إذا ما اتفق مع هذا الأخير على قبول الوفاء بالبطاقة منتهية الصلاحية إضرارا بالبنك المصدر، وذلك كأن يقوم التاجر بتزوير تاريخ انتهاء الصلاحية البطاقة على إشعار البيع (الفاتورة) أو يعلن عمدا تاريخ غير صحيح

[1] إيهاب فوزي السقا، مرجع سابق، ص. 176.

لانتهاء صلاحية البطاقة عند طلب الإذن أو يقوم بتقدم تاريخ عمليات الوفاء المنفذة.[1]

الفرع الثاني: الغش باستخدام بيانات بطاقة الائتمان بواسطة الغير

تكون عملية نقل البيانات عبر شبكة الإنترنت، ومنها البيانات المتعلقة ببطاقة الائتمان -كالرقم السري- عرضة للإسقاط من قبل الغير-سيء النية- وبالتالي استخدامها بطرق غير مشروعة في سحب النقود الرقمية أو الوفاء بها كنتيجة لما جاءت به التجارة الالكترونية بدلا من العملة الورقية، وكذلك فإن التقنية الحديثة سمحت بإمكانية اصطناع أرقام بطاقات ائتمانية أو استغلال الأرقام الخاصة بالغير واستخدامها بصورة غير مشروعة.

والتساؤل المطروح هو حول التكييف القانوني لاستخدام بيانات بطاقات الائتمان من قبل الغير عبر شبكة الإنترنت ؟ وإجابة عن هذا التساؤل نبحث في حالتين:

- **حالة استخدام بيانات بطاقة ائتمان مزورة:** قد تفقد بطاقة الائتمان من العميل، وقد تسرق منه، فيتلقفها الغير ويقوم باستبدال ما بها من بيانات ومعلومات، ويقوم باستخدامها في عمليات الشراء والسحب فيشكل ذلك اعتداء ليس على البنك المصدر للبطاقة فحسب ولكن يمتد الاعتداء ليشمل حامل البطاقة أيضا، وهذا الاعتداء يشكل في رأي جمهور الفقهاء جريمة تزوير.[2]

يعرف الفقه التزوير على انه:[3] تغيير الحقيقة في محرر بإحدى الطرق التي نص عليها القانون تغييرا من شأنه إحداث ضرر ومقترن بنية استعمال المزور فيما أعد له.

[1] المرجع نفسه، ص. 177.
[2] فايز نعيم رضوان، بطاقات الوفاء، دار النهضة العربية، القاهرة، 1999، ص. 206.
[3] محمد فتحي عيد، الإجرام المعاصر، أكاديمية نايف للعلوم الأمنية، الرياض، 1999، ص. 98.

وإذا كان تعريف الفقه ينطوي على التزوير في المحررات المادية الملموسة، فإن التزوير في مجال المعالجة الآلية للبيانات عبر شبكة الإنترنت يعد من أخطر طرق الغش التي تقع في هذا المجال، ولا سيما بحلول الحاسب الآلي والمحررات الالكترونية محل الأوراق في كافة المجالات، مما يزيد من صعوبة اكتشاف وإثبات التزوير الذي يقع في هذا المجال،[1] وتزوير بطاقات الائتمان في نطاق شبكة الإنترنت والمعلوماتية تأخذ عدة صور، من بين هذه الصور اصطناع أرقام بطاقات ائتمان خاصة ببنك معين، من خلال تزويد الحاسب بالرقم الخاص للبنك مصدر البطاقة بواسطة برامج تشغيل خاصة.[2]

وقد لاحظت بعض البنوك تكرار اعتراض بعض حاملي البطاقات الدفع الالكتروني على عمليات لم يقوموا بإجرائها، وتبين للبنوك أنها عمليات تم إجراؤها عن طريق شبكة الإنترنت بواسطة بعض الهواة المتطفلين (hackers) والمخربين (Crackers) الذين استطاعوا التقاط واكتشاف أرقام لبطاقات الدفع الالكتروني الخاصة ببعض العملاء على الشبكة واستغلالها في الحصول على السلع والخدمات، ولاسيما أنه لا توجد شيفرة خاصة لاستخدام بطاقات الفيزا كارد والماستر كارد.[3]

ويتضح أن استخدام بيانات بطاقة دفع الكتروني خاصة بالغير عبر شبكة الإنترنت يشكل جريمة احتيال، إذ يتخذ الجاني اسم كاذب وصفة غير صحيحة بطرق احتيالية بغية الحصول على منفعة مادية، مع التحفظ على ما تثيره طبيعة اختلاس الأموال اللامادية من تساؤلات وأن الحصول على بيانات بطاقات الائتمان الخاصة بالغير أو المستخدمة من قبل آخرين تشكل

[1] جميل عبد الباقي، الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان، مرجع سابق، ص. 90.
[2] خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، 2008، ص 234.
[3] بينت شركة Tower Group أن 0.11 % من المبادلات بواسطة البطاقات الائتمانية عبر شبكة الإنترنت مزورة، وأن قيمة أعمال التزوير عبر الإنترنت تصل إلى 43 مليون دولار. انظر: محمود أمين الشوابكة، مرجع سابق، ص. 201.

تعدادا معنويا للجرائم، حيث أنه ينصب عليها وصف التزوير واستعمال المزور، وكذلك ينطبق عليها وصف الاحتيال، وذلك إذا ما استخدمت في الولوج إلى النظام المعلوماتي من أجل الحصول على السلع والخدمات التي توفرها الشبكة.[1]

وقد قضت محكمة (Rennes) بأن استخدام البطاقة المزورة يعد من قبيل الطرق الاحتيالية التي تقوم بها جريمة النصب.[2]

ولمحاربة ما سبق بيانه من إساءة استخدام بطاقات الدفع الإلكتروني عبر شبكة الإنترنت لجأت شركة الفيزا كارد الماستر كارد إلى تصميم نظام (Set) Secure Electronic Transactions [3] بالإضافة إلى ظهور صور جديدة للسداد عبر الإنترنت مثل النقود الرقمية، حيث يتم تخزن مبلغ الكتروني على القرص الصلب للحاسب الآلي الخاص بالمشتري -تأخذ شكل حافظة نقود– ليستخدمها في سداد مشترياته، بالإضافة إلى إصدار بطاقات ائتمانية مدفوعة مسبقا أو بحد ائتمان بسيط، وهي خاصة للاستعمال عن طريق الإنترنت، بحيث إذا ما تعرضت للاستيلاء والاستخدام من قبل الغير كانت الخسائر محدودة.[4]

- **حالة سرقة بيانات بطاقة الائتمان:** إن ما جرت عليه العادة في منح بطاقات الائتمان، أخذ البنك المصدر للبطاقة التزاما من قبل العميل بأن لا يعطي الرقم السري للبطاقة لأي شخص، حتى لا يكو ن عرضة لعمليات السرقة أو الاحتيال أو الاستخدام غير المشروع لها من قبل الغير، وبالتالي فإن العميل وحده يكون مسؤولا عن الإدلاء بأرقام البطاقة الائتمانية عبر شبكة الإنترنت،

[1] خالد ممدوح إبراهيم، مرجع سابق، ص. 237.
[2] أحمد حسام طه تمام، مرجع سابق، ص. 539.
[3] عطية سالم عطية، ورقة عمل، الصور المستحدثة لجرائم بطاقات الدفع الالكتروني، القاهرة، 1998، ص. 91.
[4] مدحت رمضان، الحماية الجنائية للتجارة الالكترونية، دراسة مقارنة، دار النهضة العربية، القاهرة، 2000، ص. 137.

وعن تعرضها للاحتيال سواء بفعل التجسس أو الخداع، أو الحصول عليها باستخدام تقنية التفجير(إغراق الموقع).[1]

وإذا كانت عمليات الشراء والانتفاع بالخدمات التي تتيحها التجارة الالكترونية، تتطلب من المستخدم ملء النموذج الالكتروني ببيانات بطاقته الائتمانية ومنها الرقم السري، لبطاقته واستخدامه بصورة غير مشروعة من الجاني أو فقدان الرقم داخل النظام المعلوماتي ولا سيما أن البيانات المتعلقة بها يمكن أن تتلف أو تفقد أثناء عملية الاتصال.[2]

مما لاشك فيه أن مسؤولية الحامل الشرعي للبطاقة تنتفي من اللحظة التي يتم فيها الإبلاغ عن سرقة أو فقدان البيانات السرية لبطاقة الائتمان، فلا يسأل عن البطاقة واستعمالها غير المشروع، ومن واجب البنك المصدر للبطاقة أن يقوم بإيقاف عمل البطاقة وعدم التعامل معها وإلا كان مسؤولا عن عمليات السحب والدفع الالكتروني أو التحويلات الالكترونية التي تتم بواسطتها.[3]

اتجهت أحكام المحاكم الفرنسية، يساندها بعض الفقه إلى أن سرقة الأرقام والبيانات السرية الخاصة ببطاقة الائتمان واستخدامها بصورة غير مشروعة من قبل الغير، يشكل جريمة نصب،[4] على اعتبار أن المتهم قد انتحل اسما كاذبا، ومن ثم يكون قد استخدم وسيلة احتيالية لإيقاع المجني عليه بوجود ائتمان.[5] بينما يذهب جانب آخر من الفقه إلى أن هذا الفعل يشكل

---

[1] إيهاب فوزي السقا، مرجع سابق، ص. 194.
[2] مدحت رمضان، مرجع سابق، ص. 136.
[3] المرجع نفسه، ص. 140.
[4] ففي الولايات المتحدة الأمريكية فإن تعمد الإدخال الخاطئ للبيانات الائتمانية إلى أجهزة الحاسوب المرتبطة بالشبكات الداخلية أو العالمية ومحاولة التلاعب وتركيب الأرقام السرية لكشف حسابات صحيحة هي أفعال مجرمة تحت تشريع احتيال بطاقات الائتمان الفيدرالي (CCFA) وبواسطة تشريعات الولايات المتحدة ومن الأمثلة الواقعية لاحتيال بطاقات الائتمان واقعة المتطفل (Hacker) كيفين ميتنك (Kevin mitinick) الذي أسندت إليه تهمة استخدام وسيلة دخول احتيالية والاحتيال على الكمبيوتر من أجل الحصول على (20.000) بطاقة ائتمانية من شركة (Net Com) للاتصالات في سان جوس (San Jose) كاليفورنيا، انظر: خالد ممدوح رمضان، مرجع سابق، ص. 123.
[5] محمد سامي الشوا، المرجع السابق، ص. 117.

جريمة سرقة باستعمال مفتاح مصطنع،[1] باعتبار أن البطاقة الائتمانية تعد من قبيل المفاتيح المصطنعة، وذلك استنادا على أن نصوص القانون لم تحدد على وجه الدقة ماهية المفتاح المصطنع.

[1] انظر الفقيه (C.ERKELENS) مشار إليه عند: محمد سامي الشوا، مرجع سابق، ص. 117.

المبحث الثاني: الجرائم المتصلة بالحياة الخاصة وأخطار بنوك المعلومات

حظيت الحياة الخاصة للأفراد بحماية دستورية وقانونية في مختلف تشريعات الدول المتقدمة، لما لها من أهمية قصوى على كيان الفرد والمجتمع معا.[1]

ولقد كانت مهمة القانون في بادئ الأمر حماية نفس الإنسان وحماية ملكيته، فاعترف القانون بالحق في الحياة وفي سلامة الجسم، وفي مرحلة لاحقة اعترف بضرورة حماية الجانب أو الكيان المعنوي والروحي للإنسان.[2]

وفكرة الحق في الخصوصية قد تبدو مثيرة وجذابة بالنسبة لعلماء الاجتماع، أما بالنسبة للقانون فإن الكثير من العقبات تواجه هذه الفكرة من ناحية، وصعوبة التمييز بحدود واضحة بين ما يعد من قبيل الحياة الخاصة للإنسان، وما يعد من الحياة العامة له.[3]

وحاليا ونحن نعيش ثورة هائلة ومتسارعة في مجال تكنولوجيا المعلومات وتطور وسائط الاتصال، كان لا بد من البحث في المفهوم الحديث للحياة الخاصة وخاصة مع ظهور ما أطلق عليه بنوك المعلومات،[4] وهي عبارة عن جهات تقوم بتجميع المعلومات المتصلة بموضوع معين بقصد معالجتها آليا تمهيدا لاستغلالها، الأمر الذي دفع بأصوات حماية الحق في الخصوصية تتعالى لحماية حقوق الإنسان

[1] يستخدم الفقه في النظم اللاتينية مصطلح الحق في الحياة الخاصة La vie privé ويطلق مصطلح الحق في الخصوصية Privacy عند فقه النظم الأنجلو سكسونية، ورغم أن الدساتير والتشريعات الحديثة قد اتفقت على حماية حرمة الحياة الخاصة، إلا أن تعريف الحق في الخصوصية ما زال يثير جدلا وخلافا في القانون المقارن، وقد اتفق الفقه على صعوبة تحديد هذا المضمون بصورة تتلاءم مع مقتضيات العلم القانوني. انظر: فادية أبو شهاب، الحق في الخصوصية، المجلة الجنائية، إصدار المركز القومي البحوث الجنائية، القاهرة، 1997، ص. 293.

[2] حسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة (الحق في الخصوصية)، دار النهضة العربية، القاهرة، 2006، ص. 26.

[3] المرجع نفسه، ص. 14.

[4] يقصد بمصطلح بنوك المعلومات تكوين قاعدة بيانات تفيد موضوع معين، وتهدف لخدمة غرض معين، ومعالجتها بواسطة أجهزة الحاسبات الالكترونية لإخراجها في صورة معلومات تفيد مستخدمين مختلفين في أغراض متعددة، ويعرفها البعض بأنها: "مجموعة المعلومات التي يتم معالجتها الكترونيا، وذلك من أجل بثها عبر شبكة الإنترنت، بحيث يمكن للمشترك الوصول إليها من خلال ربط الكمبيوتر الخاص به بشبكة الإنترنت". انظر: فاروق محمد الأباصيري، عقد الاشتراك في قواعد المعلومات عبر شبكة الإنترنت، دار الجامعة الجديدة، الإسكندرية، 2002، ص. 51.

من أخطار التطور التكنولوجي المتسارع، ولعل أبرزها تلك الاعتداءات التي تتم بواسطة الحاسب الآلي على الحياة الخاصة. والتساؤل المطروح هو كيف يمكن للحاسب الآلي أن يكون أداة للاعتداء على الحياة الخاصة ؟

وللإجابة على هذا التساؤل نقول أنه إذا كان الحاسب الآلي يحتوي على كم هائل من المعلومات المخزنة، فإن مكمن الخطورة لدى هذا الحاسب تتمثل في الأوجه التي قد تنجم من الاستخدام الخاطئ أو غير المشروع لهذه المعلومات، وبذلك فإن خصوصية المعلومات هي المحور الذي ترتكز على حماية الحياة الخاصة في مواجهة الحاسب الآلي، وهذا ما دفع الأستاذ (Frosini) إلى القول: "بأن الخصوصية وعلاقتها بالحاسب الآلي تعني أنه لا وجود اليوم لحرية رفض إعطاء المعلومات ذات المصلحة العامة والمتصلة بالبيانات الشخصية ولكن بدلا من ذلك فإن الحرية استقرت في القدرة على السيطرة على المعلومات الشخصية التي أدخلت في برنامج الحاسب الآلي وترتيبا على ذلك يجب التأكد على وجوب سلامة أمن الوصول إلى بنوك المعلومات وسلامتها وسريتها ومراقبة حق السماح بنشرها، فكل هذه الحقوق تشكل اليوم ما يسمى بالخصوصية بالمفهوم الحديث".[1]

ومن هنا كان لابد من التصدي لهذا السلوك الإجرامي الذي قد يطال حقا من أهم حقوق الإنسان وهو الحق في الحياة الخاصة.

المطلب الأول: الحياة الخاصة في مواجهة المعلوماتية

إن تعريف الحياة الخاصة أمر لا يخلو من الصعوبة وهذا ما يقرره الفقه، نظرا لاختلاف نطاق الخصوصية من فرد لآخر، فهناك من يجعل حياته الخاصة كتابا مفتوحا، وهناك من يجعل حياته الخاصة سرا غامضا، كما يختلف مضمون

[1] محمود أحمد عبابنة، مرجع سابق، ص. 71.

الحياة الخاصة من مجتمع لآخر نتيجة لاختلاف القيم الأخلاقية والتقاليد والثقافة، ولكن يجب التأكيد على أن الخلاف ينصب على نطاق الحق في الحياة الخاصة لكنه لا يمتد إلى الحق في الخصوصية فهو حقيقة مؤكدة لجميع الأفراد في كل المجتمعات.[1]

الفرع الأول: تعريف الحق في الحياة الخاصة

في حقيقة الأمر توجد تعريفات متعددة ومتنوعة في الفقه قيلت بشأن الحق في الحياة الخاصة، فقد عرفه البعض أنه: "الحق الذي يكون للأفراد والجماعات والهيئات والمؤسسات في أن يحددوا لأنفسهم متى وكيف وبأي قدر يمكن إيصال المعلومات الخاصة بهم إلى غيرهم".[2]

وقد ذهب البعض الآخر إلى أن الحق في الحياة الخاصة والحقوق الشخصية يكاد أن يكونان متطابقين لأنهما يقرران حق الفرد في حماية اسمه ومراسلاته واتصالاته وشرفه وحياته المهنية والعائلية وكل ما له تأثير على حياته الشخصية.[3]

أما مؤتمر ستوكهولم لرجال القانون الذي عقد عام 1967 فقد تبنى تعريفا مقاربا للتعريفات السابقة حيث عرفه: "الحق في أن يكون الفرد حرا وأن يترك ليعيش كما يريد مع أدنى حق للتدخل الخارجي".[4]

وفي الواقع فإن أغلب الفقهاء الذين تناولوا تعريف الحق في الحياة الخاصة يجمعون على أنه من الصعوبة إن لم يكن من المستحيل إعطاء فكرة قانونية عامة لمفهوم الحق في الخصوصية، فهناك ازدواج في حياة الإنسان العامة والخاصة.[5]

[1] محمد أمين احمد الشوابكة، مرجع سابق، ص. 65.
[2] تعريف الفقيه الأمريكي (Allen Wesin) مشار إليه عند: حسام الدين كامل الأهواني، مرجع سابق، ص. 50.
[3] تعريف الفقيه الفرنسي (Ean Malherbe) مشار إليه عند: حسام الدين كامل الاهواني، ص. 51.
[4] حسام الدين كامل الاهواني، مرجع سابق، ص. 54.
[5] عمرو أحمد حسبو، حماية الحريات في مواجهة نظم المعلومات، دراسة مقارنة، دار النهضة العربية، القاهرة، 2000، ص. 143.

ولهذا السبب اتجه الفقه تدريجيا إلى العدول عن البحث عن تعريف للحق في الحياة الخاصة واتجه إلى وضع قائمة للقيم التي تعطيها فكرة الخصوصية، وهذا ما فعله الفقهاء الفرنسيون فحاولوا وضع قائمة بالحالات والأمور التي تدخل في إطار الحياة الخاصة فذكروا الحياة العائلية، والحياة المهنية، والحق في الصورة، وكشف الضرائب، والراتب، والمرض، والموارد المالية، ومكان قضاء أوقات الفراغ، وقد أضاف البعض الآخر الحق في الاسم والحق في الشرف والاعتبار والحق في النسيان، وأضاف البعض الآخر الحياة الروحية الداخلية التي يمارسها الإنسان خلف بابه المغلق.[1]

وأمام صعوبة وضع تعريف محدد للحياة الخاصة ذهب البعض إلى أنه من الأفضل أن يترك الأمر للقضاء وفقا للتقاليد والثقافة والقيم الدينية السائدة والنظام السياسي في كل مجتمع بما يضمن للفرد احترام ذاتيته ويحقق له الأمان بعيدا عن التدخل من الآخرين في حياته.[2]

والحق في الحياة الخاصة له وجهان متلازمان، هما حرية الحياة الخاصة وسرية هذه الحياة، وحرية الحياة الخاصة تعني حرية الفرد في اختيار أسلوب حياته دون التدخل من الغير أو السلطة، لكن هذه الحرية ليست مطلقة بل مقيدة بالنظام الاجتماعي داخل المجتمع ويضع القانون حدودها من أجل تنظيم كيفية ممارستها كي لا تضر بالآخرين، أما بالنسبة لسرية الحياة الخاصة فتعني سرية كل ما ينتج عن ممارسة الفرد لحياته الخاصة، ونطاق هذه السرية نطاق شخصي يرتبط بالفرد ذاته، فهو يشمل جميع البيانات والوقائع التي يقرر الشخص أن مصلحته الاحتفاظ بها لنفسه أو لغيره من الأشخاص المتصلين به ويريد إطلاعهم عليها.[3]

[1] حسام الدين كامل الأهواني، مرجع سابق، ص. 58.
[2] المرجع نفسه، ص. 60.
[3] المرجع نفسه، ص. 61.

والمساس بالحياة الخاصة للأفراد يزداد بشكل يبعث عن القلق في ظل المجتمع المعلوماتي خاصة مع انتشار بنوك المعلومات.

الفرع الثاني: طبيعة المعلومات المتعلقة بالحياة الخاصة

من المبادئ الأساسية أن تخزين المعلومات لا يعني أن هذه المعلومات انتقلت من الخصوصية إلى العلنية، كما أن الرضا بالتجميع والتخزين لا يعني حرية تداول ونقل المعلومات إلى الكافة.[1]

وبالرغم من أن الوسائل الحديثة ممثلة في شبكة الإنترنت ساعدت على سهولة وسرعة التبادل الإلكتروني للبيانات، فإن ذلك لا يعني ترك البيانات الشخصية المعطاة عرضة للمتطفلين الهواة Hachers أو حتى المخربين Crackers دون رقيب وذلك لأهمية هذه البيانات بالنسبة لأشخاصها المتعلقة بهم و سريتها.[2]

وفي هذا الصدد تكمن الصعوبة في تحديد المعلومات التي تعرض خصوصية الأفراد في إطار مجتمع المعلومات الالكترونية للانتهاك، فهل كل معلومة يتم تداولها عبر شبكة الإنترنت تثير مسألة الخصوصية الشخصية ؟

من الطبيعي أن المعلومات المجهولة –التي لا تدل على من تتعلق به- لا تثير أية صعوبة، حيث أن المجهول لا خصوصية له، ولكن الأمر يختلف في حالة المساس بالمعلومات المتعلقة بأشخاص معرفين، مما يؤدي إلى المساس بخصوصياتهم، فتكون بذلك المعلومة اسمية، إذ أنها تسمح بالتعرف على الشخص محل هذه المعلومة بطريقة مباشرة أو غير مباشرة.

[1] عمرو أحمد حسبو، مرجع سابق، ص. 155.
[2] السيد عتيق، جرائم الإنترنت، دار النهضة، القاهرة، 2000، ص. 61.

وقد تكون المعلومة موضوعية أي لا تعكس آراء شخصية -تتعلق بمعلومات مجردة- مثل الاسم، الموطن، الحالة المدنية، العقوبات، ومن ثم تعتبر من مميزات الشخصية لمن تتعلق به المعلومة.[1]

وكذلك قد تكون المعلومة ذاتية –تحمل رأيا ذاتيا عن الغير- فمؤلفها يختلف عن الشخص موضوع المعلومة، كالمقال الصحفي أو الملف الإداري.[2]

وإذا كانت المعلومة الموضوعية أو الذاتية غالبا ما تتعلق بالحياة العامة للأفراد، فإن المعلومات الاسمية المختزنة في بنوك المعلومات هي التي تمس الحياة الخاصة للأفراد، والحق في الخصوصية المعلوماتية.[3]

وتعرف البيانات الاسمية على أنها: "البيانات الشخصية التي تتعلق بالحق في الحياة الخاصة للمرء، كالبيانات الخاصة بحالته الصحية والمالية والوظيفية والمهنية والعائلية، عندما تكون هذه البيانات محلا للمعالجة الآلية".[4]

وموضوع البيانات الاسمية المتعلقة بالحياة الخاصة ليست المعلومات المختزنة بحد ذاتها، إنما تتمثل في المصالح التي تتهددها هذه المعلومات غير الصحيحة أو المشوهة، وبما أن الإنترنت يتمتع ببنية شبكية عالمية، فإنه يمكن الربط بسهولة بين المعلومات الشخصية التي تجمع عن المستخدم، سواء تم الحصول على هذه البيانات من خلال الإستمارات الإلكترونية التي تعبأ من قبل المستخدم أو من خلال إستخدام برمجيات خاصة بالتجسس تجمع معلومات مختصرة عن طريق إستخدام الإنترنت، متضمنة معلومات حساسة مثل أرقام بطاقات الائتمان الخاصة،

[1] نهلا عبد القادر المومني، مرجع سابق، ص. 168.
[2] سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، (الجرائم الواقعة في مجال تكنولوجيا المعلومات)، دار النهضة، القاهرة، 1999، ص. 34.
[3] المرجع نفسه، ص. 35.
[4] المرجع نفسه، ص. 36.

أو تستخدم مثل تلك البيانات لإنتحال شخصية صاحب الحق في هذه البيانات واستخدامها بشكل غير مشروع.

وبما أن الحق في المعلومات يصح أن يكون محلا للحقوق الشخصية والمالية، فإنه يجب أن تحمى خصوصية الأفراد بقوانين حديثة، وذلك بالتخلي عن حرفية النص الجنائي فيما يتعلق بالحماية الجنائية للحق في الخصوصية وعن العناصر المبهمة المكونة للجريمة،[1] وذلك للحفاظ قدر الإمكان على خصوصية المعلومات الخاصة بالأفراد من مخاطر الإنترنت واستخداماته والتي أصبحت من الوسائل القامعة للحرية الفردية إذا ما أسيء استخدامها.[2]

وهذا المساس بالمعلومات الشخصية للأفراد، قد يكون مصدره هواة متطفلون لا يلحقون أي ضرر أو أذى بصاحب البيانات، إنما يكون هدفهم إثبات مقدرتهم على التفوق التقني واختراق حواجز الأمن ، أو للتسلية باستخدام هذه المعلومات بإزعاج الآخرين، أو حتى صاحب المعلومات برسائل البريد الالكتروني غير المرغوب فيه، وقد يكون مصدر هذا المساس أشخاص مخربون يجدون في بيئة الانترنت المكان الأنسب لممارسة هواياتهم الإجرامية بخفاء، وذلك بالاعتداء على البيانات الشخصية للآخرين وانتهاكها بشتى الصور.

والمقصود بالمعالجة الآلية للمعلومات الاسمية: "مجموعة العمليات التي تتم آليا أي باستخدام الحاسوب وتتعلق بالتجميع والتسجيل والإعداد والتعديل والاسترجاع والاحتفاظ ومحو المعلومات الاسمية، وكذلك مجموعة العمليات التي تتم آليا بهدف استغلال المعلومات وعلى الأخص عمليات الربط والتقريب وانتقال

[1] سعيد عبد اللطيف حسن، المرجع نفسه، ص. 33.
[2] نهلا عبد القادر المومني، مرجع سابق، ص. 169.

المعلومات الاسمية ودمجها مع بيانات أخرى أو تحليلها للحصول على معلومة ذات دلالة خاصة".[1]

ويبدو أن الخطورة التي تشكلها بنوك المعلومات ونظم المعلومات بشكل عام على الحق في الحياة الخاصة لم تكن محل إجماع، فقد حدث خلاف في الفقه حول ما إذا كانت هذه الوسائل التقنية المستحدثة وهذا السلوك الإجرامي المستحدث يشكل خطرا حقيقيا على الحق في الخصوصية للأفراد، وقد كان هناك اتجاهان فيما يتعلق بهذا الأمر:

- **الاتجاه الأول:** يرى أنصار هذا الاتجاه أن إدخال نظام الكمبيوتر واستخدامه في مجال المعلومات والبيانات الشخصية ما هو إلا مرحلة تكنولوجية جديدة من مراحل تطور الحياة الاجتماعية، حيث تؤكد الدراسات التي أجريت في بعض الدول –في هذا الخصوص– أن سرعة التقدم التكنولوجي من الممكن أن تساعد على توسيع احتمال إلحاق الأذى بالأفراد.[2]

  ويرى أصحاب هذا الرأي أنه من الممكن حماية هذه المعلومات المختزنة في ذاكرة الحاسوب من تسربها أو العبث بها، عن طرق الحماية التقنية باستخدام الشيفرة (أنظمة التشفير).[3]
- **الاتجاه الثاني:** وهو الاتجاه الغالب، حيث يرى أن الأنظمة المعلوماتية وخاصة بنوك المعومات تشكل خطرا حقيقيا على الحياة الخاصة للأفراد، الأمر الذي يستدعي وضع نصوص قانونية خاصة لمواجهة هذه السلوكيات الإجرامية المستحدثة.

---

[1] هذا التعريف للمعالجة الآلية للمعلومات الاسمية كما نصت عليه المادة الخامسة من القانون الفرنسي الصادر في 6 جانفي 1978 الخاص بالمعالجة الالكترونية والحريات، مشار إليه عند: عمرو أحمد حسبو، مرجع سابق، ص. 50.

[2] آدم عبد البديع آدم حسين، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2000، ص. 497.

[3] عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، دار النهضة، القاهرة، 1995، ص. 52.

وتظهر خطورة الأنظمة المعلوماتية وتحديد بنوك المعلومات على الحق في الخصوصية في عدة مواقع إذ أن الحاسوب يتميز بالسرعة الفائقة في العمل وسعة غير محدودة في تخزين المعلومات المختلفة عن الأفراد وتنظيمها في ذاكرته والقدرة على استرجاعها في أي وقت، الأمر الذي يمكن القول معه بإمكانية الإطلاع على قدر لا يستهان به من هذه البيانات التي قد تكون متكاملة ومتصلة بجوانب الحياة الخاصة للفرد.[1]

وتزداد الخطورة على الحياة الخاصة للأفراد إذا ما تم ربط هذه الحاسبات ببعض أو بحاسوب مركزي أو بنوع من الشبكات العامة المخصصة للاتصال على شكل يسمح بأن تتبادل هذه الحواسيب البيانات فما بينها، حيث يكون من شأن ذلك أن يتم ربط هذه البيانات ببعضها البعض على نحو يجعل الفرصة مواتية لاستكمالها والقيام بتحليلها ومعالجتها بصورة قد تؤدي في الكثير من الأحيان للتوصل إلى معلومات أو بيانات جديدة سواء أكانت خاصة بفرد واحد أو مجموعة من الأشخاص.[2]

ومن مخاطر بنوك المعلومات كذلك عندما تقوم الدول بإنشاء بنوك أو مراكز للمعلومات تجمع فيها ما تشاء من البيانات عن الأفراد وتقوم بتحليلها وتنظيمها والربط بينها ومن ثم تخزينها في النظام المعلوماتي، مما يتيح للدول فرض رقابة على مواطنيها ومعرفة أدق التفاصيل عن حياتهم مما يشكل مساسا بحقهم في الخصوصية.[3]

وقد تعالت الاحتجاجات في بعض الدول كفرنسا والو.م.أ وألمانيا ضد إنشاء النظام الموحد للمعلومات، والمقصود بهذا النظام إمكانية جمع

---

[1] المرجع نفسه، ص. 53.

[2] عفيفي كامل، مرجع سابق، ص. 254.

[3] في هذا الشأن يقر (Ianes arlim) أن الحكومة الأمريكية تحتفظ في الحاسبات الخاصة بها، بما يوازي 03 بليون ملف تحتوي على معلومات شخصية، حيث يكون نصيب كل مواطن أمريكي في المتوسط ما يقارب 100 ملف. انظر: عفيفي، مرجع سابق، ص. 250.

المعلومات المتصلة بالفرد في حاسوب مركزي واحد، فيمكن بالتالي جمع المعلومات الضريبية والاجتماعية والدينية والسياسية والحالة الصحية والمالية والنشاط الحزبي والنقابي لهذا الفرد ... إلخ

الأمر الذي دفع بعض الدول إلى تجريم إيجاد نظام موحد للمعلومات فيها كما هو الحال في البرتغال والنمسا،[1] فهذا النظام المعلوماتي يمكن المجرم المعلوماتي من الوصول إلى كل المعلومات التي يود الحصول عليها على شخص معين أو عدة أشخاص إذا تمكن من اختراقه.

وتزداد مخاطر البنوك المعلومات على الحياة الخاصة إذا كان لكل مواطن رقم وطني،[2] حيث تتمثل خطورة هذا الرقم في تيسير الإطلاع على ما يمس الحياة الخاصة للأفراد، فمعرفة الرقم الوطني تمكن من الإطلاع على كم هائل من المعلومات المخزنة لدى الجهات المختلفة خلال لحظات.

من متطلبات التوجه نحو الحكومة الالكترونية الحصول على المعلومات والبيانات الاسمية عن المواطنين وتخزينها في الحواسيب مع توافر إمكانية تبادلها بين الدوائر الحكومية وذلك لتسهيل إنجاز المعاملات المختلفة، وإذا كانت اعتبارات المصلحة العامة والأمن الوطني تتطلبان أحيانا الوقوف على تفاصيل خاصة ودقيقة في حياة الأفراد، فإن ذلك كله يستدعي في ذات الوقت ضمانات قانونية تكفل عدم المساس بالبيانات الاسمية للأفراد واستخدامها لغير الغرض الذي جمعت من أجله.

فإذا كانت الخطورة المهددة للحياة الخاصة عبر شبكة الانترنت متمثلة في تجسس المخربين على أسرار الحياة الخاصة باستغلال التقنية الحديثة،

[1] مغبغب نعيم، مخاطر المعلوماتية والإنترنت، منشورات الحلبي، بيروت، 1998، ص. 163.
[2] عمرو أحمد حسبو، مرجع سابق، ص. ص. 63_64.

فإن الأمر يبلغ أشده فيما لو قامت الحكومات بذاتها بالتجسس على مراسلات الأفراد ومكامن خصوصياتهم عن طريق التصنت أو الرقابة الالكترونية.[1]

وتتجلى كذلك خطورة الأنظمة المعلوماتية على الحق في الخصوصية إذا ما تمت معالجة البيانات من أجل استخلاص حكم أو تقييم للشخصية اعتمادا على بيانات دون دراسة شخصية الإنسان نفسه، الآمر الذي ينتج عنه استخلاص نتائج غير دقيقة عن سلوكه أو صفاته أو سمعته مما يؤدي إلى المساس به.[2]

ولهذا تنص المادة الثانية من القانون الفرنسي بشأن المعالجة الالكترونية والحريات على حظر اعتماد الأحكام القضائية أو القرارات الصادرة من السلطة الإدارية أو من الأفراد في تقديرها للسلوك البشري فقط على الدليل المستمد من المعالجة الآلية للمعلومات الاسمية.[3]

وإذا كانت الثورة الرقمية التي أحدثتها تكنولوجيا الاتصالات ممثلة في شبكة الانترنت تؤثر بصورة مباشرة على خصوصية المستخدمين والمشتركين، فإن ما ولدته هذه الثورة يكمن في مسألة خصوصية المستهلكين والمتسوقين عبر الشبكة وفق ما عرف بالتجارة الالكترونية، حيث تتيح أنظمة التبادل الإلكتروني للبيانات إمكانية إجراء المبادلات التجارية، من بيع وشراء، وتتطلب عملية التبادل الالكتروني للبيانات في ميدان التجارة الالكترونية معرفة بعض البيانات الشخصية التي تسمح بالتعرف على الشخص بشكل أوفى.

---

[1] يشير تعبير الرقابة الالكترونية إلى الفرض الذي يقوم فيه طرف ثالث بالتصنت على محادثة شفوية للغير من خلال جهاز الكتروني، ويكون التصنت إما عن طريق استراق الأسلاك أي التدخل بقصد استراق السمع على الاتصالات تنفيذا الكترونيا، وعادة ما تكون خارج مكان الحديث ولا تتطلب دخولا إليه، أو عن طريق استراق السمع أي التصنت على محادثات الغير بواسطة أي وسيلة علمية موضوعة بالقرب من المتحدثين. انظر: أحمد عوض بلال، قاعد استبعاد الأدلة المتحصلة بطرق غير مشروعة، الطبعة الثانية، دار النهضة، القاهرة، 2008، ص. ص. 340_341.

[2] عمر فاروق الحسيني، مرجع سابق، ص. 56.

[3] المرجع نفسه.

وقد تمتد هذه البيانات إلى معرفة أرقام بطاقات الائتمان لإكمال عملية الشراء والتعاقد، وهي بدورها تشكل أكثر البيانات الشخصية المعرضة للاعتداء.[1]

المطلب الثاني: صور التهديد المعلوماتي للحياة الخاصة

إن عصر الاختراعات التكنولوجية البالغة الدقة قد أغنى الإنسان عن الكثير من الأمور، إذ أن حريته الخاصة أو الخصوصية بمعنى أدق أصبحت هي الضحية الفعلية لهذه الاختراعات الحديثة،[2] فالحياة الخاصة قطعة غالية من كيان الإنسان لا يمكن انتزاعها منه، وإلا تحول إلى مادة صماء خالية من القدرة على الإبداع الإنساني، فالإنسان بحكم طبيعته له أسراره الشخصية ومشاعره الذاتية وخصائصه المتميزة ولا يمكنه أن يتمتع بهذه الملامح إلا في إطار مغلق، يحفظها ويهيئ لها سبل البقاء، وتقتضي حرمة هذه الحياة أن يكون للإنسان الحق في إضفاء السرية على مظاهرها،[3] وفي إطار المعلوماتية تبرز خطورة التهديد المعلوماتي للحياة الخاصة بشكل أساسي في إساءة استخدام المعلومات والبيانات المتعلقة بالأفراد.

وصور سلوك الاعتداء على الحياة الخاصة يصعب حصرها، لأنها متطورة نتيجة تطور تكنولوجيا المعلومات باستمرار، إلا أنه يمكن أن نشير إلى أبرز الانتهاكات التي قد تطال حق الأفراد في حرمة حياتهم الخاصة نتيجة لاستخدام الأنظمة المعلوماتية.

[1] مدحت رمضان، الحماية الجنائية للتجارة الالكترونية، مرجع سابق، ص. 87.
[2] رضا محمد عثمان دسوقي، الموازنة بين حرية الصحافة وحرمة الحياة الخاصة (دراسة مقارنة)، دار النهضة، القاهرة، 2008، ص. 499.
[3] حسام الدين الأهواني، مرجع سابق، ص. 64.

الفرع الأول: جمع البيانات وتخزينها على نحو غير مشروع

يتمثل فعل الانتهاك للحق في الحياة الخاصة للأفراد في عملية جمع وتخزين بيانات صحيحة عنهم لكن على نحو غير مشروع وغير قانوني، ويستمد هذا الجمع أو التخزين صفته غير المشروعة عن طريق الأساليب المستخدمة للحصول على هذه البيانات والمعلومات، أو من طبيعة مضمونها.

وتتجلى هذه الأساليب غير المشروعة في أن يتم الاعتماد على وسائل تشكل انتهاكا واضحا للخصوصية وذلك من أجل جمع المعلومات والبيانات عن الأفراد ومن ضمن هذه الأساليب القيام بالتقاط الارتجاجات التي قد تحدثها الأصوات في الجدران الإسمنتية للحجرات وترجمتها إلى عبارات وكلمات بواسطة حاسوب مزود ببرنامج خاص، وكذاك قد يتم مراقبة الرسائل المتبادلة واعتراضها والتقاطها عن طريق البريد الالكتروني أو توصيل أسلاك بطريقة خفية إلى الحاسوب الذي تختزن بداخله البيانات أو التوصل بطريق غير مشروع إلى ملفات بيانات تخص آخرين، أو أي وسيلة أخرى غير مشروعة كالتدليس والغش أو التصنت على المكالمات التي تتم عن طريق شبكة الإنترنت.[1]

أما الجانب الآخر الذي يضفي صفة عدم المشروعية على جمع وتخزين البيانات هو أن تكون هذه البيانات غير صالحة للجمع والتخزين بسبب مضمونها.[2]

وفي واقع الأمر إن عدم وجود ضوابط قانونية في هذا المجال قد يؤدي إلى إمكانية جمع وتخزين ونقل كم كبير من المعلومات التي تتعلق بأدق التفاصيل الخاصة بالأفراد، فالبيانات والمعلومات الاسمية التي تتصل بالحياة الخاصة يجب حظر تجميعها وتخزينها ومعالجتها داخل جهاز الحاسوب، حيث أن مضمون هذه

[1] عفيفي كامل، مرجع سابق، ص. 258.
[2] قورة نائلة، مرجع سابق، ص. 244.

البيانات من المفترض أنه يدخل في إطار الأمور التي يحرص الأفراد على سريتها، مع التأكيد على أن فكرة الحياة الخاصة تشتمل على قدر من المرونة، حيث تلعب إرادة الشخص دورا في تحديد ما يدخل في إطارها، فهناك أمور تدخل في نطاق الحياة الخاصة لشخص ما ولا تدخل في نطاقها بالنسبة لشخص آخر.[1]

كما أن المعلومات المتصلة بالجرائم والعقوبات بالنسبة للأشخاص يجب أن تكون بمنأى عن آي تجميع أو حفظ من قبل الأفراد، فلا يجوز أن يقوم بتجميع هذه المعلومات وتخزينها في الحواسب إلا الجهات القضائية والسلطات العامة في الدولة وفي حدود اختصاصاتها القانونية، وذلك حفاظا على سمعة الأشخاص، وتأثيرها على مستقبلهم العملي، كما أن المعلومات والبيانات الاسمية المتعلقة بالمعتقدات الدينية والسياسية والانتماءات الحزبية والأصل العرفي للأفراد لا بد أن تكون بعيدة عن عمليات التجميع في الحواسيب، لأن مضمون هذه البيانات يدخل في نطاق الحياة الخاصة للأفراد.[2]

الفرع الثاني: الخطأ في المعلومات أو البيانات الاسمية

إحدى الانتهاكات التي قد تنال من الحق في الحياة الخاصة للأفراد حدوث الأخطاء التقنية أو البشرية في النظام المعلوماتي.

فالأخطاء التقنية أو الفنية من الممكن أن تقع عند تخزين المعلومات في النظام المعلوماتي ومعالجتها الكترونيا مما قد يكون له أسوأ الأثر في استخلاص نتائج معينة عن الحياة الخاصة للشخص.

وهذه الأخطاء قد يكون مرجعها عيبا فنيا في الجهاز نفسه، أو اختلال الضغط الكهربائي الذي يترتب عليه دمج البيانات المختلفة، أو اختلال في تصنيفها وتنظيمها

[1] عمرو أحمد حسبو، مرجع سابق، ص. 111.
[2] المرجع نفسه، ص. ص. 112_113.

الأمر الذي ينتج عنه نسبة معلومات معينة لأشخاص لا تتعلق بهم، ويعطي صورة غير حقيقية عن حالتهم الاجتماعية أو وضعهم الحقيقي من الناحية المالية أو السياسية أو المهنية أو الصحية وبذلك التوصل إلى نتائج غير صحيحة.[1]

أما الأخطاء البشرية فيكون وقوعها عادة من قبل الأشخاص القائمين بعملية التجميع والتخزين للبيانات الاسمية وترتيبها وتصنيفها وتوزيعها، فالخطأ قد يحدث في أي مرحلة من هذه المراحل.

فالمعلومات التي يتم تجميعها عن فرد معين قد تكون غير صحيحة وغير دقيقة أو غير مطابقة للواقع، الأمر الذي يترك آثار سيئة على سيرة هذا الشخص ويلحق به أضرارا وأخطارا كبيرة خاصة على مستقبله الوظيفي والاجتماعي، ومثالا عن ذلك وجود خطأ في المعلومات المتعلقة بالظروف المالية للشخص الذي قد يؤدي إلى عدم استفادته من خدمات المصارف وهيئات الائتمان.[2]

الفرع الثالث: الاعتداء على سرية الاتصالات والمراسلات

يعتبر الحق في حرمة الاتصالات والمراسلات وسريتها فرع من فروع حرمة الحياة الخاصة، فالاتصالات والمحادثات –أيا كان نوعها– التي يقوم بها الشخص تعتبر من عناصر الحق في الحياة الخاصة، فهذه الاتصالات قد تشتمل على أسرار وخفايا يحرص الفرد على أن لا يطلع عليها احد.

كما أن الحق في سرية المراسلات يدخل أيضا في إطار حق الفرد في الخصوصية، فالرسائل تعتبر ترجمة مادية لأفكار شخصية أو أراء خاصة لا يجوز لغير مصدرها ومن توجه إليه الإطلاع عليها، وفي حالة الكشف عنها من قبل الغير

[1] محمد أمين احمد الشوابكة، ص. ص. 65_ 66.
[2] رضا محمد عثمان دسوقي، مرجع سابق، ص. 733.

يعتبر ذلك انتهاكا لحرمة المراسلات وبالتالي انتهاكا للحياة الخاصة، لأن الرسالة قد تكون مستودعا لسر الإنسان وخصوصياته.[1]

والحق في حماية الاتصالات والمرسلات من الاعتداء على سريتها يمتد ليشمل وسائل الاتصال الحديثة كلها التي قد تتم عن طريق النظام المعلوماتي، فالتصنت على المحادثات الخاصة التي تجري عبر شبكة الإنترنت أو الإطلاع على مضمون الرسائل الالكترونية التي يتم تبادلها عبر الشبكة أيضا سواء أتم ذلك بالحصول على كلمة السر الخاصة بالمستخدم أو باعتراض هذه الرسائل والإطلاع على مضمونها، فإن ذلك كله يعد انتهاكا لحرمة الحياة الخاصة للأفراد الأمر الذي يستوجب العقاب والمساءلة القانونية.[2]

وتجدر الإشارة إلى أن التقاط الصور ونقلها يعد من الانتهاكات التي قد تمس الحق في الحياة الخاصة لأن صورة الإنسان تعد من مظاهر الخصوصية التي يحظر على الغير التقاطها دون إذن صاحبها ونقلها عبر شبكة المعلوماتية إلى الغير وتداولها بصورة غير مشروعة.[3]

الفرع الرابع: إساءة إستعمال البيانات أو المعلومات الاسمية

المعلومات والبيانات الإسمية التي يتم تجميعها وتخزينها ومعالجتها في جهاز الحاسوب يتعين أن يكون لها هدف محدد وواضح ومعين سلفا، ويشترط في هذا الهدف أو الغاية أن لا تكون متعارضة مع النظام العام والآداب.

وقد قضت المحكمة الدستورية لألمانيا الاتحادية: "أنه لا حرية رأي أو حرية اجتماع ولا حرية مؤسسات يمكن أن تمارس كاملة مادام الفرد غير متيقن في ظل

[1] أحمد عبابنة، مرجع سابق، ص. 72.
[2] ، المرجع نفسه، ص 73.
[3] رضا محمد عثمان دسوقي، مرجع سابق، ص. 738.

أي ظروف ولأجل أي هدف جمعت عنه المعلومات الفردية وعولجت آليا في الحاسوب".[1]

ويجب على الجهة القائمة على النظام المعلوماتي الالتزام بالغاية التي من أجلها قامت بتجميع المعلومات ومعالجتها الكترونيا، فلا يجوز تخزين البيانات أو المعلومات الاسمية إلا بالقدر الذي تكون مرتبطة فيه بالهدف من إقامة نظام المعالجة المقصود.

فالبيانات الاسمية يتعين أن تكون متناسبة وضرورية لهذا الهدف كما يجب أن يكون الغرض مرتبطا بمهمة ووظيفة الجهة القائمة على النظام المعلوماتي.[2]

وتطبيقا لذلك قضت المحاكم الألمانية بوقف إحصاء عن عدد السكان في عام 1984 بعد أن ثبت لها أن وزارة الداخلية استطاعت من خلال استمارات الإحصاء الحصول على عناوين مجموعة متطرفة إرهابية الأمر الذي يعد إساءة لاستخدام البيانات التي جمعت من أجل غاية محددة وهي الإحصاء السكاني.[3]

فإذا تم تجميع المعلومات أو البيانات الاسمية لهدف محدد من قبل شخص أو جهة ما، ثم وصلت هذه المعلومات إلى جهة أخرى تقوم بجمع المعلومات لغاية أخرى، وجب على المشرع أن يتدخل كي يقوم بمنع أي جهة كانت عامة أو خاصة من إعطاء هذه المعلومات إلى جهة أخرى مختلفة عنها في الغاية،[4] وإذا ما تم هذا الأمر فإنه يجب أن يكون وفق ضوابط وقيود تحكم هذه المسألة.

[1] نعيم مغبغب، مرجع سابق، ص. 246.
[2] عمرو احمد حسبوا، مرجع سابق، ص. 128.
[3] نعيم مغبغب، المرجع نفسه، ص. 247.
[4] ، المرجع نفسه، ص. 242.

الفرع الخامس: الإفشاء غير المشروع للبيانات والمعلومات الاسمية:

من المبادئ الأساسية أن تخزين المعلومات لا يعني أن هذه المعلومات قد انتقلت من الخصوصية إلى العلانية، كما أن الرضا بالتجميع والتخزين لا يعني حرية تداول ونقل المعلومات إلى جميع الناس.[1]

وانتهاك الحق في الحياة الخاصة قد يتخذ صورة الإفشاء غير المشروع للبيانات والمعلومات الاسمية، فالجمع للمعلومات في هذا الفرض يكون قد تم بصورة مشروعة إلا أن هذه البيانات والمعلومات يمكن الإطلاع عليها من قبل عدد كبير من الأشخاص العاملين في حقل المعلوماتية وبالتالي قد تكون معرضة لخطر انتهاك سريتها وخصوصيتها وإفشائها للغير.

وقد يتم الحصول على المعلومات المختزنة عن الأفراد في جهاز الحاسوب أو في بنوك المعلوماتية والتي تكون على درجة من الحساسية والأهمية بغرض استخدامها في ابتزاز الشخص الذي تتعلق به هذه المعلومات.

وفي الواقع إن من شأن استخدام الأنظمة المعلوماتية في المجال الأمني وقطاع الشرطة والاحتفاظ بكم هائل من المعلومات الخاصة بالملايين من الأشخاص وبالتالي فإن خطر إفشائها وارد من قبل أشخاص من المفترض أنهم أمناء عليها، وللتدليل على خطورة هذا الأمر نشير إلى ما قام به ضابط شرطة نمساوي حيث قام بإعطاء أحد المخبرين معلومات قيمة تخص بعض الأفراد متعلقة بحالتهم الجنائية والمختزنة في ذاكرة الحاسوب الذي تستخدمه الشرطة.[2]

[1] أحمد حسبو، مرجع سابق، ص. 155.
[2] كامل عفيفي، مرجع سابق، ص. 259.

المطلب الثالث: موقف الأنظمة القانونية من حماية الحياة الخاصة في مواجهة سلوكيات المجرم المعلوماتي

بما أن صور انتهاك الخصوصية في مجال نقل البيانات في شبكة الإنترنت لا تتمتع بأمن كامل لسرية ما ينقل عبرها من بيانات، فإن إمكانية مراقبة واعتراض وتفريغ الرسائل المتبادلة عن طريق البريد الالكتروني والتوصل بطريق غير مشروع إلى بيانات تخص الآخرين، أصبح عرضة للعديد من الانتهاكات، مما يثير التساؤل حول الجهود المبذولة في مواجهة انتهاك خصوصيات الأفراد، والتي أصبحت تزادا بازدياد مستخدمي شبكة الإنترنت والمتعاملين مع نظم المعلومات.

وإذا كانت العقوبات وتدابير الأمن كالرقابة (رقابة الأفراد أو رقابة الدولة) تثير الكثير من المخاوف والمشكلات القانونية، ولاسيما أنها تؤدي إذا ما أسندت للدولة إلى المركزية والى المزيد من الانتهاكات كما سبق بيانه، وإذا ما أسندت إلى الأفراد فأنها تؤدي إلى قيام المسؤولية المدنية (التقصيرية- العقدية)، أو حتى قيام المسؤولية الجنائية لمزودي خدمة الإنترنت إذا ما افترض فيهم الرقابة على مستخدمي الشبكة، ولاسيما إذا ما تم إخطارهم بولوج غير شرعي إلى بياناتهم الشخصية، وذلك للقيام باعتراض هذا الولوج.[1]

ومع ذلك نرى أن إعطاء قدر من تنظيم التدابير الوقائية لمستخدمي ومشتركي شبكة الإنترنت فما يتعلق بخصوصياتهم، أفضل بكثير من ترك الأمور دون حد أدنى من الرقابة والتنظيم.

[1] يونس عرب، تطور التشريعات في مجال مكافحة الجرائم الالكترونية، ورقة رقم 3، بحث مقدم لهيئة تنظيم الاتصالات مسقط، سلطنة عمان، 2-4 أفريل 2006، دون ترقيم.

ونعرض فيما يلي للجهود المبذولة لحماية حرمة الحياة الخاصة في مواجهة نظم المعلومات، حيث نبين الجهود الدولية والإقليمية ثم نوضح مسلك التشريعات الداخلية.

الفرع الأول: الجهود الدولية المبذولة لحماية الحياة الخاصة في مواجهة المجرم المعلوماتي

أخذت مسألة الحياة الخاصة للأفراد اهتمام المنظمات العالمية والإقليمية، والتي أكدت على حق الإنسان في حرمة حياته الخاصة من أخطار الاعتداء على البيانات الشخصية (البيانات الاسمية) حيث برز في هذا الإطار جهود منظمة الأمم المتحدة والمجلس الأوروبي والجماعة الأوروبية ومنظمة التعاون الاقتصادي ومجلس وزراء العدل العرب.

توجت جهود منظمة الأمم المتحدة في ميدان حماية الحياة الخاصة في مواجهة التقدم التقني والمعلوماتي، وذلك في المؤتمر الدولي الأول لحقوق الإنسان المتعلق بأثر التقدم التكنولوجي على حقوق الإنسان (مؤتمر طهران 1968) والتي تبنت الجمعية العامة للأمم المتحدة توصياته، وأبرز ما جاء فيها أن الحاسبات الاليكترونية تمثل أكبر تهديد للحياة الخاصة والحرية الشخصية، واعتبارها من أدوات المراقبة وأجهزة التصنت، والتطفل الحديث، وخاصة إذا تم تخزين البيانات الشخصية على الحاسب الآلي وتحليلها، مما يجعل كل أشكال التعاملات والعلاقات مكشوفة.[1]

أما على الصعيد الإقليمي ظهر دور مجلس أوروبا والسوق الأوروبية المشتركة، ففي مجلس أوروبا برز جهد المجلس في 17 سبتمبر 1980 بتوقيع

[1] محمد أمين احمد الشوابكة، مرجع سابق، ص. 73.

معاهدة مجلس أوروبا الخاصة بحماية الأشخاص من مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية، وقد وضعت الاتفاقية للتوقيع في جانفي 1981 وقد بدأ السريان الفعلي لهذه الاتفاقية في أكتوبر1985،[1] ويقتصر نطاق تطبيق هذه الاتفاقية على الأشخاص الطبيعيين، وتسري على القطاعيين العام والخاص فيما يتعلق بالملفات المعدة آليا، حيث تحظى بإلزامية أحكامها لتحقيق حماية البيانات الشخصية المعالجة آليا.

كما صدر عن مجلس أوروبا العديد من التوصيات لتوسيع نطاق الحماية لتشمل قطاعات الأنشطة الخاصة كالبيانات الطبية والبحثية والإحصائية.[2]

كما صدر أيضا عن البرلمان الأوروبي عدة قرارات منها قرار 8 جانفي 1979 الخاص بحماية الفرد في مواجهـــة التطور التقني للمعلوماتية، وكذلك القرار الصادر في 8 فيفري 1979 والمتعلق بحقوق الفرد في مواجهة التطورات التقنية في مجال البيانات، وأيضا القرار الصادر في 9 مارس 1982 المتعلق بحماية الفرد في مواجهة التطورات التقنية في مجال معالجة البيانات.

وإذا كانت الحماية الأوربية للبيانات الشخصية لم تتوج إلى الآن حول حماية هذه البيانات في الفضاء الاليكتروني، إلا انه صدر قرار أوروبي يحمـــل الرقم 96/9/ CE بتاريخ 11 مارس 1996 يتعلق بالحماية القانونية لقواعد البيانات حيث يمتاز هذا القرار بمنحه جمع قواعد البيانات (بما فيها البيانات غير الالكترونية).[3]

ومن الجهود التي أرست مبادئ حماية الخصوصية بشأن البيانات الشخصية، تلك المتعلقة بمنظمة التعاون الاقتصادي والتنمية (OECD) وقد تبنى مجلس

[1] وقعت على هذه الاتفاقية كل من (النمسا، بلجيكا، الدنمرك، ألمانيا الغربية (قبل الاتحاد)، فرنسا، اليونان، أيسلندا، إيطاليا، لوكسمبورغ، النرويج، البرتغال، السويد، تركيا، بريطانيا). انظر: محمد أمين احمد الشوابكة، مرجع سابق، ص. 73.
[2] عبد الله علي محمود، مرجع سابق، ص. 409.
[3] طوني عيسى، الجرائم المعلوماتية، بحث مقدم إلى جمعية إتمام المعلوماتية القانونية في لبنان، بيروت، 1998، ص. 05.

المنظمة سنة 1980 مجموعة من القواعد الإرشادية بشأن حماية الخصوصية ونقل وتدفق البيانات الشخصية،[1] هذه القواعد لا تتمتع أحكامها بصيغة إلزامية من الناحية القانونية وذلك راجع إلى اعتبارها قواعد إرشادية.

كما اعتمد مجلس وزراء العدل العرب[2] للقانون الجزائي العربي الموحد رقم 229 لسنة 1996، وبالرجوع إلى المذكرة التوضيحية لهذا القانون، وباستعراض الباب السابع الخاص بالجرائم ضد الأشخاص، نجد أن الفصل التاسع من هذا الباب جاء معالجا للاعتداء على حقوق الأشخاص الناتج عن المعالجات المعلوماتية، حيث نظمت في المواد 461-464.[3]

حيث أشارت المادة 462 من هذا القانون إلى الحبس مدة لا تزيد عن سنة وبالغرامة على كل من حصل على معلومات اسمية للغير أثناء تسجيلها أو ترتيبها أو إرسالها بأي وسيلة من وسائل المعالجة التي من شأن إفشائها المس بسمعة المعني بالأمر أو بحياته الشخصية مما يسمح للغير بالإطلاع على تلك المعلومات دون إذن المعني بالأمر.

الفرع الثاني: دور التشريعات الداخلية لحماية الحق في الخصوصية في موجهة التقنية المعلوماتية

تعتبر حماية الحق في حرمة الحياة الخاصة في مواجهة أخطار المعلوماتية في مختلف الأنظمة القانونية أحد الإشكالات المطروحة وذلك راجع إلى أن الدول لم تسلك مسلكا موحدا لحماية الحق في حرمة الحياة الخاصة في مواجهة الأخطار

[1] طوني عيسى، المرجع نفسه، ص. 08.
[2] أنشأ بموجب الإعلان الصادر عن المؤتمر العربي الأول لوزراء العدل العرب بشأن التعاون العربي في المجالات التشريعية والقضائية الذي عقد بمدينة الرباط المغربية سنة 1977.
[3] القانون الجزائي العربي رقم 229-1996 الجزء الثاني، الإدارة العامة للشؤون القانونية، الأمانة الفنية لمجلس وزراء العدل العرب، جامعة الدول العربية.

الناتجة عن استخدام الحاسب الآلي كبنك للمعلومات. ويمكننا تقسيم موقف هذه التشريعات إلى ثلاثة اتجاهات:[1]

- **الاتجاه الأول**: دول نصت دساتيرها على حماية الحياة الخاصة في مواجهة أخطار بنوك المعلومات، ومن هذه الدول إسبانيا، البرتغال، النمسا، حيث كفلت دساتير هذه الدول الحماية لهذه البيانات الشخصية والتي تخضع للمعالجة الالكترونية.
- **الاتجاه الثاني**: دول وضعت تشريعات خاصة لحماية الحياة الخاصة في مواجهة أخطار المعلومات. ومن هذه الدول:

أ. فرنسا: أصدر المشرع الفرنسي القانون رقم 17 لسنة 1978 والخاص بالمعالجة الالكترونية للبيانات الاسمية، والذي اشتهر باسم قانون معالجة المعلومات والحريات، والذي نص في المادة الأولى منه أن معالجة المعلومات يجب أن تكون في خدمة كل مواطن. وقد دعم المشرع الفرنسي هذا المبدأ بوضع عدة قوانين، لتواكب التطور التكنولوجي في عالم الاتصالات والكمبيوتر منها:[2]

قانون 12 نوفمبر 1980 المتعلق بإثبات التصرفات القانونية ذات المعالجة الالكترونية.

قانون 29 جانفي 1982 والذي اقر فيه مبدأ حرية الاتصال السمعي والبصري. وقد بين هذا القانون المقصود من مفهوم الاتصال عن بعد.

[1] آدم عبد البديع آدم حسين، مرجع سابق، 2000، ص. 53.
[2] محمد السعيد رشدي، الانترنت والجوانب القانونية لنظم المعلومات، بحث مقدم الى مؤتمر الاعلام والقانون، كلية الحقوق، جامعة حلوان، 9-10 مارس 1999، ص. 51.

قانون 30 سبتمبر 1986 المعدل بقانون 17 جانفي 1989 بشأن الاتصالات السمعية والبصرية والذي حل محل قانون 1982.

قانون العقوبات لعام 1992 والمعمول به منذ سنة 1994.

ب. الولايات المتحدة الأمريكية: أصدرت و.م.أ تشريعا خاصا لحماية الحياة الخاصة في عام 1974، وكان الهدف من هذا القانون هو تقرير حماية كل فرد ضد الاعتداء على حياته الخاصة، ووضع قواعد لحماية الفرد من الإطلاع على المعلومات الخاصة به والمحفوظة في الكمبيوتر.[1]

كما فرض المشرع الأمريكي حماية لخصوصية الأفراد أثناء عمليات الاتصال وتبادل المعلومات، وذلك بإصداره لقانون خصوصية الاتصالات الالكترونية لعام 1986.[2]

ج. الصين: أصدرت الصين مرسوما في فيفري 1996 بشأن تنظيم استخدام الإنترنت، حيث فرضت على كل مستخدم لبرامج بث المعلومات عبر الشبكة أن يحصل على موافقة مسبقة من وزارة البريد والاتصالات، وأنه يحظر عليه بث أية معلومة يكون من شأنها المساس بالنظام العام،[3] وكذلك الحال بالنسبة إلى كل النمسا، بلجيكا، ألمانيا، السويد، حيث أصدرت عدة تشريعات.

د. تونس: أقر المشروع التونسي حماية خاصة للمعطيات الشخصية في مواجهة التطور التقني في المواد 38-42 من قانون التجارة

[1] أسامة احمد المناعسة، مرجع سابق، ص. 223.
[2] المرجع نفسه، ص. 224.
[3] محمد السعيد رشدي، مرجع سابق ، ص.52.

الإلكترونية لعام 2000، وفرض عقوبات أصلية وعقوبات تكميلية على الأفعال التي تقع بالمخالفة لتلك المواد.[1]

و. الجزائر: أما المشروع الجزائري فقد نص في القانون رقم 06-23 المؤرخ في 20 ديسمبر من 2006 على عقوبة الحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 50.000 دج إلى 300.000 دج على أي شخص كان متعمدا المساس بحرمة الحياة الخاصة وبأية تقنية كانت، وذلك عن طريق الالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، دون إذن صاحبها أو رضاه، أو بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها.[2]

كما نص على معاقبة أي شخص احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير، واستخدم في ذلك أي وسيلة كانت من التسجيلات أو الصور أو الوثائق.[3]

فالملاحظة هنا أن المشرع الجزائري لم يبين بصورة دقيقة الأساليب المستخدمة بل ذكر بأي تقنية كانت، واستخدم كذلك عبارة "... أو استخدام بأية وسيلة كانت ..."

أما القسم الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات القانون رقم 26-23 المؤرخ في 20 ديسمبر سنة 2006 فتضمن صورا أخرى للغش، في حين أبقى خارج دائرة التجريم بعض الأفعال نذكر منها المساس بحقوق الأشخاص عن طريق المعلوماتية ومنها جمع المعلومات حول الشخص.

[1] محمد السعيد رشدي ،المرجع نفسه.
[2] المادة 303 مكرر، القانون رقم 06-23 المؤرخ 20 ديسمبر 2006.
[3] المادة 303 مكرر1.

- **الاتجاه الثالث:** دول التزمت الصمت نحو أخطار بنوك المعلومات على الحياة الخاصة هذه الدول اكتفت بالنصوص الخاصة بحماية الأسرار، وهي غالبية الدول النامية.

ومهما يكن من أمر، فالواضح أن سلوك المجرم المعلوماتي اعتمد على التقنية الحديثة للوصول إلى البيانات الشخصية للأفراد (البيانات الاسمية) وبالتالي الاعتداء على حرمة الحياة الخاصة، وهذا ما أبقى النصوص التقليدية تقف عاجزة أمام هذه الخرقات والاعتداءات على خصوصيات الأفراد وأسرارهم، لذا فإن الحاجة ملحة، لسد كل فراغ تشريعي في حماية ما يتم تداوله من معلومات وأسرار على هذه الشبكة.

المبحث الثالث: الدخول والبقاء غير المصرح بهما إلى النظام المعلوماتي

مكن التطور الكبير في نظم الاتصالات وتنامي شبكات المعلوماتية إلى انتشار ظاهرة اختراق النظام المعلوماتي من قبل الأفراد غير المصرح لهم بالدخول إليه أو البقاء فيه، ويذهب البعض من الفقه إلى تصنيف هذه الجريمة تحت باب الجرائم المعلوماتية المرتكبة بواسطة النظام المعلوماتي،[1] أما البعض الآخر، فيطلق على هذا النموذج للسلوك الإجرامي بجرائم الاعتداء على نظم المعالجة الآلية للبيانات أو جرائم السلوك المجرد المتصلة بنظام المعالجة الآلية للمعلومات.[2]

وبالرغم من أن الدخول أو البقاء غير المصرح بهما إلى النظام المعلوماتي يعد مرحلة سابقة وضرورية لارتكاب الجرائم المعلوماتية الأخرى مثل سرقة المعلومات وتزويرها أو التجسس المعلوماتي أو جريمة الاحتيال المعلوماتي أو الاعتداء على حرمة الحياة الخاصة وغير ذلك من الجرائم، إلا أن مرتكب هذا السلوك قد يقصده بحد ذاته دون أن يهدف إلى ارتكاب جريمة أخرى من ورائه.

هذه الحالة جلبت معها خلافا حول مدى انطباق وصف الجريمة المعلوماتية عليها، وبالتالي إذا كانت تستوجب الحماية الجنائية أم لا ؟

- **الاتجاه الأول:** يذهب هذا الاتجاه إلى أنه لا توجد ضرورة تستدعي تجريم مجرد الدخول أو البقاء غير المصرح بهما إلى النظام المعلوماتي، وخاصة إذا لم يكن لدى الفاعل نية ارتكاب جريمة لاحقة على هذا الدخول أو البقاء، ويبرر هذا الاتجاه رأيه أن هذا السلوك لا يخرج عن كونه طريقة لعرض

[1] أحمد حسام طه تمام، مرجع سابق، ص. 259.
[2] حجازي عبد الفتاح بيومي، الدليل الجنائي والتزوير في جرائم الكمبيوتر، مرجع سابق ، ص. 235.

القدرات التقنية والذهنية التي يتمتع بها الشخص الذي قام بهذا الفعل، وهذا الأمر بحد ذاته لا يشكل جريمة تستدعي العقاب.[1]

- **الاتجاه الثاني:** ويذهب إلى ضرورة تجريم السلوك المستحدث، حتى ولو لم يكن ذلك بقصد ارتكاب جريمة لاحقة فيما بعد. ويبرر هذا الاتجاه رأيه بالإشارة إلى أن هناك خسائر مادية قد تترتب على حالات الدخول غير المصرح به للنظام المعلوماتي، قد تكون هذه الخسائر نتيجة محاولة وقف هذا الدخول. ويمكن الإشارة في هذا الصدد إلى الخسائر التي تحملتها إحدى المعامل الخاصة بتصنيع الأسلحة النووية في كاليفورنيا والتي قدرت بحوالي مئة ألف دولار أمريكي، وهي تكلفة الأبحاث التي أجريت لمحاولة وقف الدخول غير المصرح به الذي قام به أحد الأشخاص إلى نظام الحاسوب الخاص بهذا المعمل.[2]

والأجدر هو الأخذ بما جاء به الاتجاه الثاني الداعي إلى تجريم هذا السلوك بحد ذاته، لأنه يعد مرحلة أساسية لارتكاب بقية الجرائم المعلوماتية الأخرى، كما أن المعلومات التي قد يقع عليها هذا السلوك تكون على قدر من الأهمية، كما هو الحال بالمعلومات المتعلقة بالأسرار العسكرية للدولة وكذلك البيانات الخاصة بالعملاء في البنوك أو الخاصة بالمواطنين في سجلات الحالة المدنية، وقد يهدد هذا السلوك الأبحاث العلمية أو الطبية وغير ذلك من المعلومات المختلفة، إذ أن مجرد الدخول أو البقاء في النظام المعلوماتي والإطلاع على المعلومات التي يحتويها يعد مساسا بها، حتى ولو لم يتم ارتكاب جريمة لاحقة على هذا الفعل، وحتى ولو كان الهدف من ذلك السلوك هو إثبات الذات، والقدرة على اختراق الحواجز الالكترونية للنظام

[1] قورة نائلة، مرجع سابق، ص. 323.
[2] المرجع نفسه، ص. 327.

المعلوماتي، وترك هؤلاء الأشخاص دون عقاب يؤدي إلى التمادي في الاعتداء على الأنظمة المعلوماتية.

المطلب الأول: الدخول غير المشروع للنظام المعلوماتي

تقوم هذه الجريمة بتحقق فعل الدخول إلى النظام المعلوماتي، ونعني بكلمة الدخول إلى كل الأفعال التي تسمح بالولوج إلى النظام المعلوماتي والإحاطة والسيطرة على المعطيات والمعلومات التي يتكون منها.[1]

وفعل الدخول الذي يشكل الركن المادي في هذه الجريمة لا يقصد به الدخول المادي إلى المكان الذي يتواجد به الحاسوب ونظامه، بل يقصد به الدخول باستخدام الوسائل الفنية والتقنية إلى النظام المعلوماتي، ولا تغير طريقة الدخول من الأمر شيئا، سواء تم الدخول بطريق مباشر إلى المعلومات أو تم عن طريق الاعتراض غير المشروع لعمليات الاتصال من أجل الدخول إلى النظام المعلوماتي، هذا السلوك قد لا يتطلب سوى تشغيل جهاز الحاسوب وفي بعض الأحيان يتطلب أمورا أكثر تعقيدا كما هو الحال بمحاولة الحصول على الرقم السري حتى يكون بالإمكان الدخول إلى النظام، وقد يتم ذلك أحيانا أخرى باستعمال برامج خبيثة يتم دمجها في أحد البرامج الأصلية لجهاز الحاسوب، حيث تعمل كجزء منه، وتقوم هذه البرامج بتسجيل الشيفرات التي يتعامل بها المستخدمون الشرعيون، وهناك وسائل أخرى تعتمد على ضعف الأنظمة ذاتها.[2]

وفعل الدخول إلى النظام المعلوماتي لا يعتبر بحد ذاته سلوكا غير مشروع، وإنما يستمد هذا الفعل وصفه الجرمي انطلاقا من كونه قد تم دون وجه حق أي دون

[1] قورة نائلة، المرجع نفسه، ص. 343.
[2] المرجع نفسه، ص. 325.

تصريح، ومثال ذلك دخول الفاعل إلى النظام المعلوماتي دون الحصول على تصريح المسؤول عنه، وقد يكون الفاعل يملك تصريح جزئي أي يسمح له بالدخول إلى جزء من النظام إلا أنه يتجاوز هذا التصريح الممنوح له ويدخل إلى كامل النظام، وهذا الفرض يتم من قبل العاملين في المؤسسات التي يتواجد بها النظام المعلوماتي.[1]

كما أن عدم التصريح بالدخول ينصرف إلى الحالات التي يكون فيها هذا الدخول مشروطا بدفع ثمن محدد ورغم ذلك يقوم الفاعل بالدخول إلى النظام دون أن يقوم بتسديد هذا المبلغ، أما إذا كان الولوج إلى النظام المعلوماتي بالمجان أي أنه متاح للجمهور ففي هذه الحالة يكون الدخول إليه من الحقوق.[2]

تعد جريمة الدخول غير المصرح به إلى النظام المعلوماتي من الجرائم الشكلية التي لا يتطلب قيام الركن المادي فيها نتيجة ما، وبالرغم من إمكانية حدوث أضرار معينة بالمعلومات بمحوها أو تعديلها أو إفساد نظام التشغيل نتيجة لهذا السلوك، إلا أن ذلك لا يغير من طبيعة الجريمة باعتبارها جريمة شكلية.[3]

كما أن هناك خلاف فقهي حول مدى أحقية النظم المعلوماتية التي لا تحميها أنظمة أمنية معينة بالحماية الجنائية ضد الدخول غير المصرح به، وقد كان هناك رأيان:

- الرأي الأول: اتجه إلى أنه من غير المعقول توفير حماية جنائية لمعلومات على درجة من الأهمية تركت دون أي إجراءات أمنية توفر لها الحماية اللازمة، ويبرر أصحاب هذا الاتجاه وجهة نظرهم بالإشارة إلى أن القانون

[1] محمد حماد الهيتي، مرجع سابق، ص. 213.
[2] احمد هلالي عبد اللاه، مرجع سابق، ص. ص. 72_73.
[3] جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان، مرجع سابق، ص. 150.

الجنائي لا ينبغي أن يقوم بحماية الأشخاص الذين لا يأخذون الاحتياط اللازم المطلوب من الإنسان متوسط الذكاء، فوجود نظام حماية يمكن اعتباره التزاما مفروضا على كل من يقوم بإدارة نظام معلوماتي.[1]

- الرأي الثاني: ذهب إلى ضرورة حماية الأنظمة المعلوماتية سواء كانت هناك تدابير أمنية تحميها أم لم تكن، ويعزز هذا الاتجاه وجهة نظره بالإشارة إلى أن تطلب هذا الشرط يؤدي إلى قصر نطاق الحماية على الأنظمة المحمية فقط دون الأنظمة المفتوحة للجمهور،[2] مما يعني توسيع دائرة الإفلات من العقاب. كما يذهب أنصار هذا الرأي إلى أنه لا ينبغي أن ينظر إلى وجوب توفر الأنظمة الأمنية كشرط لتجريم هذا الدخول غير المصرح به إلى النظام المعلوماتي وإنما يمكن النظر إليها باعتبارها قرينة على تحقق القصد الجنائي.[3]

ولاكتمال عناصر جريمة الدخول غير المصرح به للنظام المعلوماتي يستدعي ذلك توافر القصد الجنائي والمتمثل في عنصري العلم والإرادة، فالفاعل لابد أن يعلم أنه يقوم بفعل الدخول غير المصرح به إلى النظام المعلوماتي، ولابد أن تكون إرادته متجهة لارتكاب هذا الفعل، وينبغي أن يكون القصد الجنائي معاصرا للنشاط الإجرامي بمعنى أن تخلف القصد لحظة بدء فعل الدخول غير المصرح به ينفي الصفة الإجرامية عن هذا السلوك.[4]

[1] احمد حسام طه تمام، مرجع سابق، ص. 260.
[2] جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان، مرجع سابق، ص. 151.
[3] قورة نائلة، مرجع سابق، ص. 371.
[4] عمر الفاروق الحسيني، مرجع سابق، ص. 129.

المطلب الثاني: البقاء غير المصرح به في النظام المعلوماتي

يقصد بفعل البقاء غير المشروع داخل النظام المعلوماتي التواجد داخل هذا النظام بالمخالفة لإرادة الشخص صاحب النظام أو من له السيطرة عليه،[1] ويتحقق الركن المادي لجريمة البقاء غير المصرح به داخل النظام المعلوماتي في الحالة التي يجد فيها الشخص نفسه داخل النظام عن طريق الخطأ أو الصدفة غير أنه يقرر البقاء داخل النظام وعدم قطع الاتصال به.

فالركن المادي في هذه الحالة لا يتمثل في إقامة الاتصال مع النظام، فالفرض هنا أن هذا الاتصال لم يقصده الجاني،[2] ويمكن توضيح ذلك في حالة ما إذا كان الشخص في سبيله للدخول إلى نظام معلوماتي له الحق في الدخول إليه إلا أنه يجد نفسه ولسبب ما استخدام رقم سري خاطئ داخل نظام آخر.

وتعد جريمة البقاء غير المشروع داخل النظام المعلوماتي من الجرائم التي يصعب تقديم دليل على إثباتها، حيث أن المتهم يزعم في حالة القبض عليه أنه كان على وشك الانفصال على النظام المعتدى عليه.

تعد جريمة البقاء غير المشروع داخل النظام المعلوماتي من الجرائم الشكلية كذلك والتي لا يشترط فيها حدوث نتيجة جرمية معينة فيكفي البقاء غير المصرح به داخل النظام المعلوماتي ليقوم الركن المادي لهذه الجريمة. وتعد هذه الجريمة من الجرائم المستمرة،[3] وذلك نظرا لاستمرار الاعتداء على المصلحة التي يحميها القانون طالما استمر البقاء غير المصرح به داخل النظام، كما تعد كذلك من الجرائم

[1] حجازي عبد الفتاح بيومي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت، مرجع سابق، ص. 235.
[2] عمر الفاروق الحسيني، مرجع سابق، ص. 105.
[3] الجريمة المستمرة: هي الجريمة التي يتكون ركنها المادي من تصرف أو حالة تحتمل بطبيعتها الاستمرار لفترة زمنية غير محددة من الوقت أنظر: رمسيس بهنام، النظرية العامة للقانون الجنائي، الطبعة الثالثة، منشأة المعارف الإسكندرية، 1997، ص. 588.

الوقتية،[1] حيث أن هذه الجريمة تتم بمجرد تحقق فعل الدخول غير المصرح به، وتجدر الإشارةَ إلى أنه في الحالة التي يتم فيها الدخول غير المصرح به إلى النظام المعلوماتي ومن ثم البقاء فيه فترة من الزمن يتحقق الاجتماع المادي للجرائم.[2]

تعتبر جريمة البقاء غير المصرح به داخل النظام المعلوماتي جريمة عمدية، يستلزم قيامها توافر القصد الجنائي والمتمثل في عنصري العلم والإرادة، أولا علم الجاني بأنه يقوم بالتجول داخل نظام معلوماتي من غير إذن أو تصريح، وثانيا اتجاه إرادته في نفس الوقت إلى البقاء فيه وعدم قطع الاتصال مع هذا النظام.

وفي هذا المجال نشير إلى ما نصت عليه اتفاقية بودابست لمكافحة الإجرام المعلوماتي في المادة الثانية منها، حيث نصت: "يجب على كل طرف في الاتفاقية أن يتبنى الإجراءات التشريعية أو أية إجراءات يرى أنها ضرورية من أجل اعتبار جريمة جنائية للولوج العمدي لكل أو لجزء من جهاز الحاسوب دون حق، كما يمكن أن تشترط التشريعات أن ترتكب الجريمة من خلال انتهاك إجراءات الأمن".[3]

وفي هذا الصدد نشير بأن المشرع الجزائري قد جرم هذا السلوك وهذا في نص المادة 394 مكرر: "يعاقب بالحبس من ثلاثة (03) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 200.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين

[1] الجريمة الوقتية هي: الجريمة التي يتكون ركنها المادي من تصرف يقع في وقت محدود أي فترة زمنية قصيرة وتنتهي بوقوع الجريمة، أنظر: رمسيس بهنام، المرجع نفسه.
[2] محمد أحمد أمين الشوابكة ، مرجع سابق ، ص. ص. 25_26.
[3] مشار إلى هذه المادة عند: محمد هلالي عبد اللاه، مرجع سابق، ص. 68.

والغرامة 50.000 دج إلى 300.000 دج".[1] هذا يبين لنا أن فعل الدخول في منظومة معلوماتية يشمل فعلين هما:

- الدخول: تتسع هذه العبارات على إطلاقها لتشمل كن فنيات الدخول الاحتيالي في منظومة، محمية كانت أو غير محمية، كما تشمل استعمال من لا حق له في استخدام مفتاح الدخول الغير.
- البقاء: ويتسع ليشمل البقاء بعد الدخول الشرعي أكثر من الوقت المحدد وذلك بهدف عدم دفع إتاوة.

وتقوم الجريمة سواء حصل الدخول مباشرة على حاسوب أو حصل عن بعد، كما يحرم البقاء حتى لو حصل الدخول بصفة عرضية أي صدفة أو عن طريق الخطأ، وأصر الفاعل على البقاء داخل هذه المنظومة المعلوماتية.

ومن الدول العربية التي جرمت الدخول والبقاء غير المشروع في النظام المعلوماتي بنصوص صريحة سلطنة عمان والتي نص قانون العقوبات فيها على أنه:[2] يعاقب بالسجن مدة لا تقل عن ثلاث أشهر ولا تزيد عن سنتين وبغرامة 1000 ريال إلى 5000 ريال أو بإحدى هاتين العقوبتين كل من تعمد استخدام الحاسوب في ارتكاب أحد الأفعال التالية:

1. الالتقاط غير المشروع للبيانات.
2. الدخول غير المشروع إلى أنظمة الحاسوب.

كما نجد المشرع الأمريكي قد جرم فعل الدخول غير المشروع إلى أنظمة المعلوماتية وذلك في قانون الاحتيال وإساءة استخدام الكمبيوتر عام 1996 وذلك في

[1] القانون رقم 06- 23 المؤرخ في 20 ديسمبر سنة 2006.
[2] المرسوم السلطاني 2001/72 وهو تعديل بعض أحكام قانون الجزاء العماني. مشار اليه عند: الرومي، مرجع سابق، ص. 07.

المادة (1030) وهي متجهة بشكل كبير إلى حماية الحكومة الفدرالية بالإضافة إلى الأموال وأجهزة حاسوب المؤسسات الطبية.[1]

أما المشرع الفرنسي فقد نص في قانون العقوبات الفرنسي في المادة 1/323 على تجريم الدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه بطريقة غير مشروعة، حيث نص المشرع على أن:[2] "الدخول أو البقاء – بطريق الغش- داخل كل أو جزء من نظام المعالجة الآلية للمعطيات، يعاقب عليه بالحبس لمدة سنة، وغرامة مقدراها 15.000 يورو ، فإذا نجم عن هذا الدخول محو أو تعديل في المعطيات المختزنة فيه أو إتلاف تشغيل هذا النظام تكون العقوبة الحبس لمدة سنتين وغرامة مقدارها 30.000 يورو".

ونلاحظ هنا أن المشرع الفرنسي قد جرم مجرد الدخول أو البقاء غير المشروع داخل النظام المعلوماتي حتى ولو لم ينجم عن هذا الفعل ضرر يذكر بالنظام المعلوماتي، وشدد العقوبة في حالة أن نجم عن هذا السلوك محو أو تعديل أو إتلاف للمعلومات، وهو مسار عليه المشرع الجزائري.

[1] محمد أحمد أمين الشوابكة، مرجع سابق، ص . ص. 19_20.
[2] ، المرجع نفسه، ص. 21.

خلاصة

تعرضنا في هذا الفصل لمختلف السلوكيات المستحدثة التي يعتمد عليها المجرم المعلوماتي في ارتكاب جرمه وذلك بالاعتماد على التقنية الحديثة، أي الجرائم المعلوماتية التي تقع بواسطة النظام المعلوماتي.كما أن الملاحظ من كل ذلك أن هذا السلوك المعتمد من طرف المجرم يخص طائفة من المجرمين دون غيرهم.

ومن بين هذه الجرائم نذكر جريمة الاحتيال المعلوماتي، حيث يقوم الجاني بسلوك احتيالي يعتمد فيه على أحد التقنيات الحديثة من تحويل أرصدة مالية وذلك باستخدام البريد الالكتروني للحصول على المعلومات المتناقلة عبر شبكة المعلومات أو القيام باختلاس الأموال من خلال إدخال معلومات أو تعديل معلومات أو تعطيلها أو إنشاء نظام معلوماتي جديد وبطبيعة الحال تكون هذه المعلومات المدخلة وهمية، أو بالاعتماد على سرقة الأرقام السرية لبطاقات الائتمان أو جريمة الاعتداء على حرمة الحياة الخاصة للأفراد وذلك بالتعدي على بياناتهم الاسمية ونشرها على شبكة الإنترنت واستخدامها في ابتزاز الأشخاص، أو قيام المجرم المعلوماتي بجريمة الدخول والبقاء غير المشروع داخل النظام المعلوماتي، هذه الجريمة بالخصوص، وجب التشدد في عقاب مرتكبيها سواء تبع هذه الجريمة جريمة أخرى من إتلاف أو نشر أو اتجار في معطيات مخزنة أو لم يتبعها، وذلك راجع إلى أنها أول خطوة يقوم بها المجرم لارتكاب أي جريمة معلوماتية سواء كانت جريمة احتيال معلوماتي أو تعدي على حق في الحياة الخاصة أو غيرها من الجرائم التي تعتمد في ارتكابها على التقنية الحديثة.

كما وجب على المشرع مواكبة تطور هذه السلوكيات الإجرامية وذلك بنصوص قانونية، تحدد بشكل واضح ودقيق صور هذه الجرائم.

الفصل الثالث

سلوكيات المجرم المعلوماتي المرتكبة على تكنولوجيا المعلومات

يتكون النظام المعلوماتي من مكونات مادية (الحاسوب والأجهزة الملحقة به والشبكات المعلوماتية) ومكونات معنوية تتجسد في المعلومات بكل صورها.

فإذا كان موضع الاعتداء على الأموال في نطاق المعالجة الآلية للمعلومات ينصب على الحاسب الآلي ذاته وما يرتبط من أسلاك وما يتصل به من ملحقات، كسرقة الجهاز أو القيام بإتلافه، هذه الجرائم هي جرائم تقليدية وبالتالي يسأل مرتكبها بموجب النصوص العقابية في قانون العقوبات ولا تثير حالات الاعتداء على المكونات المادية للنظام المعلوماتي أي إشكال في الواقع العملي نظرا لأن هذه المكونات تعتبر مالا (ماديا منقولا) يخضع للحماية الجنائية بموجب نصوص قانون العقوبات.

أما إذا وقع الاعتداء على ما يتعلق بالمكونات المعنوية للنظام المعلوماتي ممثلة بالمعلومات أو برمجيات ونظم معلوماتية، فقد تتم سرقة هذه المعلومات أو إتلافها أو تزويرها والعبث بها وغير ذلك من الأفعال غير المشرعة، وفي هذه الحالة تبدو النصوص التقليدية قاصرة عن تحقيق الحماية الكافية والمتكاملة للمعلومات بما لهذا المال المستحدث من طابع خاص غير تقليدي. حيث أن الجرائم الواقعة على المكونات المادية للنظام المعلوماتي لا تثير أي مشكلة قانونية كونها مشمولة بالحماية الجزائية، فإننا سنقوم في هذا الفصل بتناول أبرز السلوكيات الإجرامية الواقعة على المكونات المعنوية للنظام المعلوماتي.

المبحث الأول: سرقة المال المعلوماتي المعنوي(سرقة المعلومات)

لم تقتصر أساليب إساءة استخدام الثورة التقنية على الاعتداء على الأشخاص، بل تعدتها لتطال الذمة المالية للغير، مما يشكل اعتداء على أموالهم المادية وكذلك الأموال المعنوية.

إن الصورة الغالبة لسرقة المال المعلوماتي المعنوي، تأخذ صورة اختلاس البيانات والمعلومات، وذلك باستخدام السارق للمعلومات الشخصية كالاسم والعنوان، الأرقام السرية الخاصة بالمجني عليهم. ونظرا لما تشغله المعلومات من قيمة اقتصادية كبيرة كان هناك تنافس من قبل الأفراد والمؤسسات المختلفة وكذلك الدول للحصول عليها من أجل تسريع عملية التقدم، ومقابل ذلك كانت هناك طائفة تقوم بالاستغلال غير المشروع لهذه المعلومات بكل الأساليب المتاحة لها، وذلك بسرقة المعلومات المختزنة في جهاز الحاسوب أو المتبادلة عبر الشبكة العالمية للمعلومات (الانترنت)، وهي إحدى أكثر الأساليب انتشارا في مجال الاعتداء على المعلومات ويطلق البعض على هذه الجريمة "جريمة قرصنة المعلومات".[1]

ويقصد بالقرصنة المعلوماتية نسخ البرامج على نحو غير مشروع أو الحصول دون وجه حق على معلومات مخزنة في ذاكرة الحاسوب بطريقة مباشرة أو غير مباشرة،[2] وعمليات القرصنة المعلوماتية ينتج عنها خسائر كبيرة، فعلى سبيل المثال تسببت عمليات النسخ غير القانوني للبرامج سنة 2000 بخسائر قدرت 11.75 مليار دولار في عموم العالم،[3] الأمر الذي يظهر بوضوح أن هذه السلوك الإجرامي أصبح يشكل خطرا حقيقيا يهدد صناعة المعلوماتية.

ويثور التساؤل فيما إذا كان الاعتداء بسرقة المعلومات المعنوية والمختزنة في قواعد البيانات أو المتبادلة على شبكة الانترنت تشكل جريمة سرقة أم لا ؟

بالرجوع إلى نصوص قانون العقوبات الجزائري فيما يتعلق بجريمة السرقة، نرى أن المشرع الجزائي عرف جريمة السرقة في المادة 350 على أنها "كل من

[1] الزيدي وليد، مرجع سابق، ص. 32.
[2] محمد شتا، مرجع سابق، ص.91.
[3] الزيدي وليد، المرجع نفسه، ص. 33.

اختلس شيئا غير مملوك له يعد سارقا ...".[1] ومن هذا التعريف يتضح لنا أن جريمة السرقة تقوم على ثلاثة أركان وهي:

- فعل الاختلاس، وهو الركن المادي للجريمة.
- محل الجريمة، ويتمثل في شيء منقول مملوك للغير.
- القصد الجنائي، وهو الركن المعنوي للجريمة.

مع ملاحظة أن المشرع الجزائري لم يذكر صراحة وجوب أن يكون محل السرقة منقولا وأشار إلى ذلك بلفظ شيء.

المطلب الأول: الطبيعة القانونية للمال المعلوماتي محل السرقة

قبل أن نتطرق إلى مدى انطباق وصف المال على المعلومة، نشير أولا إلى تعريف المعلومة وبيان الشروط الواجب توافرها في المعلومات حتى تتمتع بالحماية القانونية.

الفرع الأول: تعريف المعلومات

عرف الأستاذ "باركر" المعلومات بأنها "مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال أو التفسير والتأويل أو المعالجة بواسطة الأفراد أو الأنظمة الالكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها أو نقلها بوسائل وأشكال مختلفة".[2]

كما عرفها البعض أنها " كل نتيجة مبدئية أو نهائية مترتبة على تشغيل البيانات أو تحليلها أو استقراء دلالاتها أو استنتاج ما يمكن استنتاجه منها وحدها أو متداخلة مع غيرها أو تفسيرها على نحو يثري متخذي القرار ومساعدتهم على الحكم

[1] القانون رقم 06-23 المؤرخ في 20 ديسمبر سنة 2006، يقابل هذه المادة في القانون المصري المادة 311 من قانون العقوبات على أن " كل من اختلس منقولا مملوكا لغيره فهو سارق" والمادة 1/399 من قانون العقوبات الأردني " كل من أخذ مال الغير المنقول دون رضاه"

[2] مشار له عند قورة نائلة مرجع السابق، ص. 93.

السديد على الظواهر والمشاهدات أو يسهم في تطوير المعارف النظرية أو التطبيقية".[1]

وتعرف البيانات أنها "المعطيات الخام أو الأولية التي تتعلق بقطاع أو نشاط ما".[2] وتسمى العلاقة بين البيانات والمعلومات بالدورة الاسترجاعية للمعلومات، إذ يتم تجميع وتشغيل البيانات للحصول على المعلومات ثم يتم استخدامها في إصدار قرارات تؤدي بدورها على مجموعة إضافية من البيانات والتي يتم تجميعها ومعالجتها مرة أخرى للحصول على معلومات إضافية يستند عليها في إصدار قرارات جديدة.[3]

وعرف الأستاذ (CATALA) المعلومة أنها "رسالة معبر عنها في شكل يجعلها قابلة للنقل أو الإبلاغ للغير".[4]

كما أن المعلومات بصفة عامة تتميز بقابليتها للدمج فقد تضاف معلومة إلى معلومة أخرى لتكونا معا معلومة جديدة تختلف في قيمتها وأهميتها عما كانت عليه قبل الدمج. من خلال هذه التعريفات يتضح لنا ووفقا لما استقر عليه الفقه أن المعلومات هي من قبيل الأشياء المعنوية لا المادية، وهو الأمر الذي كون عقبة في مجال تطبيق نصوص جريمة السرقة التقليدية على سرقة المعلومات.

الفرع الثاني: الشروط الواجب توافرها في المعلومات

حتى تتمتع المعلومة بالحماية القانونية لابد أن تتوافر فيها مجموعة من الشروط، وتتجلى هذه الشروط في ما يلي:

- **أن يكون في المعلومة التحديد والابتكار:** إن المعلومة التي لا يتوافر فيها صفة التحديد لا يمكن أن تكون معلومة بالمعنى الحقيقي، فالمعلومة بوصفها

[1] محمد شتا، مرجع سابق، ص. 62
[2] المرجع نفسه، ص. 61
[3] نهلا عبد القادر المومني، مرجع السابق، ص. 102.
[4] عبد الله حسين على محمود، مرجع سابق، ص. 155.

مخصصة للتبليغ يجب أن تكون محددة، كما أن المعلومة المحددة هي التي يمكن حصرها في دائرة خاصة بها من الأشخاص.[1]

أما فيما يتعلق بالابتكار، فانه ينبغي أن تنصب هذه الصفة على الرسالة التي تحملها المعلومة، فالمعلومة غير المبتكرة هي معلومة عامة شائعة ومتاحة للجميع ويمكن للعامة الوصول إليها ولا يمكن نسبها على شخص محدد.[2]

- **أن يتوافر في المعلومة السرية والاستئثار:** كلما اتصفت المعلومة بالسرية كان المجال الذي تتحرك فيه الرسالة التي تحملها هذه المعلومات محددا بمجموعة من الأشخاص، غير أن انعدام هذا التحديد يبعد الأفكار الخاصة بالسرقة أو النصب، فالمعلومة غير السرية تكون صالحة للتداول ومن ثم تكون بمنأ عن أي حيازة، وهذا ما ينطبق على المعلومات التي تتعلق بحقيقة معينة كدرجة الحرارة في وقت معين أو المعلومات التي ترد على حوادث معينة كالبراكين والفيضانات، فهي قابلة للنقل والتداول بسهولة وبساطة بين كل الأشخاص، والوصول إلى المعلومة بسهولة يتعارض والطابع السري لها.[3]

وقد تستمد المعلومة سريتها من طبيعتها كاكتشاف في أحد المجالات التي تتميز بالسرية أو على إرادة الإنسان أو للسببين معا، كما هو الحال في الرقم السري لبطاقات الائتمان.[4]

كما تعد خاصية الاستئثار (L'exclusivité) أمرا هاما في جميع الجرائم التي تنطوي على اعتداء قانوني على الأموال، فالفاعل الذي يستولي

[1] عبد الله حسين علي محمود، المرجع نفسه، ص. 155.
[2] سامي الشوا، مرجع سابق، ص. 175.
[3] عبد الله حسين علي محمود، المرجع نفسه، ص. 156.
[4] ، المرجع نفسه.

على شيء يستأثر على ميزة تخص الغير، وفي مجال المعلومات تتوافر صفة الاستئثار إذا كان الوصول إليها غير مصرح به إلا لأشخاص محددين، ويمكن أن ينبع الاستئثار من سلطة شخص أو جهة ما على المعلومة (يستشعر بالاستئثار عندما تكون المعلومة محلا لفكرة أو عمل ذهني، فصاحب هذه الفكرة أو هذا العمل ينظر إليها بوصفها مملوكة له).[1]

الفرع الثالث: مدى انطباق وصف المال على المعلومات

أثير جدل فقهي وقضائي حول ما إذا كانت المعلومات صالحة أن تكون محل سرقة.

نشير في بداية الأمر إلى أن الاتجاه الذي كان سائدا في تحديد مدى انطباق وصف المال على الأشياء كان يعتمد على الصفة المادية في الأشياء لاعتبارها مالا. فقد كان هذا الاتجاه يعرف المال أنه "كل شيء يمكن حيازته ماديا"[2] فقد كان ينظر إليها باعتبارها أما عديمة القيمة أو ذات قيمة منخفضة.

هذا الرأي يدافع عنه جانب من الفقه الذي يعتمد في تحليله على كون الأموال غير المادية هي أموال غير مجسدة ومن ثم فإن المعلومة وحدها تكون غير قابلة للسرقة إن كانت منفصلة عن سندها المادي.[3]

إلا أن التطورات التي حدثت في العقود الماضية والتي مازالت مستمرة للآن في مجال تكنولوجيا المعلومات جعلتها تنتشر بصورة كبيرة في كافة المجالات والمعاملات مما أدى في بعض الأحيان إلى ارتفاع قيمتها عن قيمة الأموال المادية،

[1] عبد الله علي حسين محمود،المرجع نفسه.
[2] أسامة الزغبي، المناعسة، مرجع سابق، ص. 114.
[3] أحسن بوسقيعة، مرجع سابق، ص. 270.

كما أن التفاعل الذي حدث بين علم المعلوماتية وعلم الاتصال أسفر عنه تحول العالم إلى وحدة سكنية واحدة.

هذا التطور أدى بالفقه الحديث إلى البحث عن معيار آخر غير معيار مادية المال، حيث تم اللجوء إلى معيار القيمة الاقتصادية للشيء.[1] إذ لا يعتبر الشيء مالا بالنظر إلى كيانه المادي الملموس وإنما بالنظر إلى قيمته الاقتصادية.

ووفقا لهذا الاتجاه يمكن إصباغ صفة المال على المكونات المعنوية للنظام المعلوماتي على أساس ما تتمتع به من قيمة اقتصادية.

كما أن القضاء الفرنسي تطور في اتجاه الإقرار بسرقة المعلومات، و يتضح ذلك من القرارين اللذين أصدرتهما محكمة النقض الفرنسية في قضيتي "بركان" "Bourquin" و"لوقابوكس" "Logabox" ففي القضية الثانية، أبدت محكمة النقض في قرارها الصادر في 1989/01/12 إدانة شخصين من أجل سرقة 70 قرصا ممغنطا وسرقة محتوى المعلومات التي يحويها 47 قرص منها خلال الفترة الضرورية لنقل المعلومات إلى سند آخر.[2] هذا القرار يوضح لنا أن القضاء الفرنسي قد خلص إلى أن المعطيات المعلوماتية صالحة أن تكون محلا للسرقة، وتتحقق هذه الأخيرة بتحويل ما يحتويه قرص من المعلومات إلى سند آخر، حتى ولو كان الاختلاس مؤقتا و لم يدم إلا الوقت اللازم لنقل ما يحتويه القرص إلى ذلك السند.

وقد تأكد هذا الاتجاه في قضية "أنطونيولي" "Antoniolli" حيث أبدت محكمة النقض الفرنسية حكما يقضي بإدانة محاسب شركة لكونه أطلع شركة منافسة على معلومات تحتوي على جداول وخطوط بيانية أعدها بناء على وثائق الحسابات التابعة

[1] عفيفي كامل، مرجع سابق، ص. 112.
[2] أحسن بوسقيعة، مرجع سابق، ص. 270.

للشركة التي يعمل بها، معتبرة ذلك سرقة على أساس أن المعطيات الحسابية المستنتجة من الوثائق والمسلمة إلى الغير تشكل أموالا غير مجسدة تعود ملكيتها إلى المؤسسة دون سواها.[1]

غير أن المدقق والمتمعن في هذه القرارات وغيرها يلاحظ أن أحكام المحاكم الفرنسية لا تميل لاعتبار الاستيلاء على المعلومات من قبل السرقة إلا بشرط أن تكون مثبتة على دعائم مادية كالأسطوانات، ومما يؤكد ذلك الحكم في قضية "بوركان" "Bourquin".

كما ظهر اتجاه حديث في فرنسا ينادي بصلاحية المعلومات بذاتها لتكون محلا للسرقة استنادا إلى لفظ "الشيء" التي وردت بتعريف السرقة وهو نفس اللفظ المستعمل في تعريف السرقة في قانون العقوبات الجزائري، ووفقا للقانون الفرنسي تمتد لتشمل الأشياء المعنوية (غير المادية) ومنها المعلومات، ولفظ الشيء ورد مطلقا والمطلق يؤخذ على إطلاقه.[2]

غير أن الواقع والتطور المتسارع في مختلف المجالات وضع المعلومة وهي مستقلة عن دعامتها المادية من قبيل المال القابل للحيازة.

و قد اعتمد الأستاذ Catala من أجل إضفاء وصف المال على المعلومة على قيمتها الاقتصادية من ناحية وعلاقة التبني التي ترتبط بينها وبين المؤلف من ناحية أخرى.[3]

[1] المرجع نفسه، ص. 271.
[2] محمود أحمد عبابنة، مرجع سابق، ص. 98.
[3] عبد الله حسين محمود، مرجع سابق، ص. 168.

المطلب الثاني: أنماط سرقة المال المعلوماتي المعنوي:

تعد البيانات والمعلومات اللامادية المخزنة في قواعد البيانات والمتبادلة عبر خطوط شبكة الانترنت، هدف الجاني وغايته، فإذا ما اختلست تلك المعلومات بطريقة ما، فإن ذلك يمثل اعتداء على المال المعلوماتي، وسببا لقيام وصف السرقة أو الاحتيال أو خيانة الأمانة وذلك حسب طبيعة الاختلاس ونية الجاني.

وعملية اعتراض وجمع وتحليل الرسائل والمعلومات المنقولة عبر الشبكة الانترنت تتم بواسطة محطات الالتقاط المنتشرة على الشبكة، ومن ثم سحب نسخة من الجهاز الخادم، أو أن يتم استنساخ الرسالة أو المعلومة أثناء طريقها إلى الجهاز الخادم ليتم ادعاها في بنوك عملاقة للمعلومات بعد تصنيفها حسب اللغة، وبعد ذلك يتم فحص المحتويات وباستخدام تقنية الكلمات الحساسة مما يسمح في بناء مرجع الكتروني للكلمات الخطيرة والمثيرة للشبهة، ومن هذا المنطلق نستخدم هذه المعلومات في مجالات ايجابية مختلفة أو سلبية، وذلك بإساءة استخدام هذه المعلومات المعترضة في ارتكاب الجرائم عبر خطوط الشبكة.[1]

وقد يقوم الجاني باستخدام واستغلال جهد ووقت الحاسب الآلي في غير الأحوال المصرح بها، ليقوم بتحقيق منفعة شخصية أو بغرض التسلية.

الفرع الأول: الالتقاط غير المشروع للبيانات

يمثل الدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه دون إذن سلوك من سلوكيات المجرم المعلوماتي المتبعة من أجل تحقيق مكاسب شخصية متباينة ومتعلقة بذات المجرم، حيث يمكن هذا السلوك المجرم من التقاط البيانات المخزنة في قواعد البيانات أو المتبادلة عبر شبكة الانترنت واستعمالها بطرق غير

[1] مجلة انترنت العالم العربي، السنة الرابعة، العدد الثامن، 2001، ص. 58.

مشروعة. ويتمكن المجرم المعلوماتي من التقاط البيانات إما عن طريق التجسس المعلوماتي أو عن طريق الاحتيال (الخداع) أو عن طريق تفجير الموقع المستهدف.

- **أسلوب الخداع:** يتمثل هذا الأسلوب في قيام قراصنة الانترنت بإنشاء مواقع وهمية خاصة بهم، مشابهة للمواقع الأصلية للشركات والمؤسسات التجارية المتعاملة بالتسويق عبر الانترنت، ويتم من خلال هذه المواقع الوهمية استقبال جميع المعاملات التجارية والمالية، ومن بينها البيانات الاسمية والمعلومات السرية كالرقم السري لبطاقات الدفع الالكتروني،[1] ويعتبر أسلوب الخداع المتبع من قبل قراصنة الكمبيوتر للحصول على البيانات والمعلومات أقرب إلى وصف الاحتيال، فالمجرم المعلوماتي يقوم بإتباع سلوك لإيهام المجني عليهم بوجود مشروع كاذب بغرض الحصول على هذه المعلومات واستغلالها بصورة غير مشروعة من أجل تحقيق منفعة شخصية كاستخدام هذه البيانات في عمليات التعاقد الالكتروني كالبيع أو التحويل الالكتروني من أرصدة المجني عليهم إلى أرصدة الجناة.
- **أسلوب التجسس المعلوماتي:** يتمثل هذا السلوك في قيام المجرم المعلوماتي باستخدام البرامج التي تتيح له الإطلاع على البيانات والمعلومات الخاصة بالمتعاملين على شبكة الانترنت، ومن ثم استخدام هذه البيانات والمعلومات في ممارسة الأنشطة الجنائية.[2]

وتقاس خطورة التجسس بحسب أهمية المعلومات الملتقطة والتي تكون معلومات سرية تجارية (اقتصادية، أو معلومات عسكرية، أو معلومات

[1] جميل عبد الباقي الصغير، مرجع سابق، ص. 38.
[2] المرجع نسفه، ص36

خاصة ببيانات بطاقة الإئتمان، أو غير ذلك من المعلومات،[1] هذا ما جعل الحكومة الفرنسية تأخذ العديد من الإجراءات من بينها سن تشريع مستلهم من قانون التجسس الاقتصادي (EEA) الذي تم المصادقة عليه في الولايات المتحدة الأمريكية سنة 1996 والذي ينص على تسليط عقوبة السجن وغرامات مالية مرتفعة على أي شخص يحصل أو يستعمل أو يطرح معلومة اقتصادية تم الحصول عليها بطريقة غير شرعية،[2] ويتمكن مجرموا الإنترنت من التقاط البيانات والمعلومات بصورة غير مشروعة باستخدام أساليب فعالة في قرصنة كلمة المرور، عن طريق التعقب والتسلل للبرامج التي تتجه إليها أكثر أسماء المستخدمين، ومن ثم سرقة كلمات المرور، حيث تقارن البرامج المتعقبة كلمات المرور المستقرة مع قاموس للكلمات العامة، فإذا ما تقاربت كلمة المرور الملتقطة مع الكلمة في القاموس فإن المجرم المعلوماتي يتمكن من الحصول على اسم مستخدم جديد وكلمة مرور جديدة تمكنه من الولوج إلى النظام وإجراء التلاعب في البيانات والاستفاع بها.[3]

ومن الأمثلة الواقعية على ذلك ما قام به أحد التلاميذ في بريطانيا، حيث تمكن من الوصول إلى معظم الملفات السرية المخزنة بجهاز حاسوب إحدى الشركات الكبرى التي تدير نظاما للمشتركين في خدمات الكمبيوتر، وذلك بأن حصل على كشوفات نظام التشغيل وتحليلها بالإضافة إلى الأرقام السرية الخاصة بالمشتركين، والتي تتيح له الولوج إلى النظام والإطلاع على الملفات السرية الخاصة بهم.[4]

---

[1] في الولايات المتحدة الأمريكية، صدق على قانون التجسس الاقتصادي Économique Espionage في عام 1996، وبموجبه أصبحت من الجرائم الفيدرالية أخذ أو نقل أو الحصول على معلومات سرية تجارية بدون رضا مالكها، انظر محمد احمد أمين الشوابكة، مرجع سابق، ص. 167.

[2] Olile Boizard, veille ou Intelligence économique Faut il choisir , Euromed Marseille, école de Management ,2006, p. 03.

[3] جميل عبد الباقي الصغير، مرجع سابق، ص. 40.

[4] محمد أمين احمد الشوابكة ، مرجع سابق، ص. 168.

كما تتحقق صورة التجسس المعلوماتي من خلال سرقة نصوص ملفات تحتوي على معلومات أو بيانات ذات قيمة.

وبالتطرق إلى القانون رقم 04/09 المؤرخ في 14 شعبان عام 1430 الموافق لـ 5 أوت سنة 2009، والمتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها نجد بأن المشرع الجزائري عرف الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في المادة 2 /أ على أنها "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية".[1]

فالمشرع قصد هنا الجرائم المنصوص عليها في قانون رقم 15/04 المؤرخ في 20 ديسمبر سنة 2006 والمحددة في المواد 394 مكرر إلى 394 مكرر 7، وأضاف عليها بصفة عامة أي جريمة أخرى يسهل ارتكابها عن طريق المنظومة معلوماتية،[2] أو نظام للاتصالات الالكترونية، وعرف المشرع الجزائري الاتصالات الالكترونية في المادة 2/و على أنها "أي تراسل أو إرسال أو استقبال علامات أو أشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية".

والمفهوم من ذلك أن اعتراض أي رسالة الكترونية أو الحصول على صور أو أصوات أو أي معلومة أخرى تخص الغير عن طريق وسيلة الكترونية فإن المشرع جرم ذلك كما ذكرنا سابقا في القانون رقم 04-15.

[1] القانون رقم 09- 04 المؤرخ في 14 شعبان عام 1430 الموافق لـ 5 غشت سنة 2009، الجريدة الرسمية للجمهورية الجزائرية العدد 47 ص. 5.

[2] عرف المشرع الجزائري المنظومة المعلوماتية في المادة 2/ب من قانون 09- 04 على أنها أي نظام منفصلا أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين، أنظر: الجريدة الرسمية للجمهورية الجزائرية، العدد 47، ص. 5.

ومن خلال ذلك يتضح أن الأفعال المجرمة تقضي بالضرورة إلى الإطـــلاع على محتوى هذه الرسائل المتبادلة، مما يشكل بالتالي فعـــل الالتقـــاط غيـــر المشروع لها، وبالتالي استخدام البيانات أو المعلومات التي تتضمنها للقيـــام بأفعال غير المشروعة ومثال ذلك اعتراض بريـــد الالكترونـــي (E-MAIL) يتضمن بيانات متعلقة بأرقام حساب أو أرقام بطاقات الائتمـــان، ومـــن ثـــم استخدام هذه البيانات في إجراء التحويلات الالكترونية للأموال.

- **أسلوب أو تقنية الموقع المستهدف:** يعتمد هذا الأسلوب على ضخ كميات كبيرة من الرسائل الالكترونية من جهاز الحاسب الآلي للجاني إلى الجهاز المستهدف، بقصد التأثير على ما يعرف (بالسعة التخزينية)، بحيث يشكل هذا الكم الهائل من الرسائل الإلكترونية ضغطا يؤدي في النهاية إلى تفجير الموقع العامل على الشبكة لتشتيت المعلومات والبيانات المخزنة فيه لتنتقل بعد ذلك إلى الجهاز الخاص بالمجرم أو تمكن هذا الخير من حرية التجول في الموقع المستهدف بسهولة ويسر، والحصول على كل ما يحتاجه الجاني من أرقام ومعلومات وبيانات مملوكة للغير.[1]

الفرع الثاني: سرقة منفعة الحاسب الآلي

إن الانتشار الواسع للحواسيب ولشبكات المعلوماتية التي تربط بينهما والاعتماد الكبير من قبل القطاعين العام والخاص على الأنظمة المعلوماتية في سبيل انجاز الأعمال المختلفة أوجد معه تساؤلا حول مدى مشروعية الاستعمال غير المصرح به لهذه الأنظمة من قبل البعض من الأفراد.

[1] عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، دار الفكر الجامعي، الإسكندرية، 2002، ص. 132.

هناك عدة مصطلحات تستخدم للدلالة على هذا السلوك حيث يطلق عليه البعض "سرقة الخدمات التي يقدمها الحاسوب" أو "تشغيل الحاسوب دون مقابل" أو "سرقة منفعة الحاسوب"، ويمكن تعريف الاستعمال غير المصرح به للنظام المعلوماتي على أنه "كل استعمال للوظيفة التي يؤديها الحاسوب خلال فترة زمنية دون أن يكون مصرحا بذلك للفاعل، وبمعنى آخر هو كل استخدام للحاسوب ولنظامه للاستفادة من الخدمات التي يقدمها دون أن يكون للشخص الذي يمارس هذا الاستخدام الحق في ذلك".[1]

وبعبارة أخرى يقصد بسرقة منفعة الحاسب الآلي، استخدامه لأغراض شخصية أو تجارية بدون علم مالكه أو حائزه القانوني، وينتج عن ذلك حتما استخدام وقت الحاسب الآلي أو وقت الآلة من أجل أغراض شخصية مما يخلق طائفة جديدة من الجرائم المعلوماتية تتمثل بسرقة وقت الحاسب الآلي.

ويمكن القول أن معظم أرباب العمل يتقبلون أن يستعمل موظفوهم الهاتف مرة أو اثنين في اليوم لإجراء بعض المكلمات الخاصة والقصيرة بطبيعة الحال، ولكن أن يتعلق الأمر بالوسائل الالكترونية ودخول غرف الشات (الدردشة الالكترونية) أو استعمال الانترنت لأغراض شخصية، فهذا ما لن يتقبله رب العمل منطقيا، خاصة إذا علمنا أن هذا النوع من وسائل الاتصال إذ ما استعمل لوسائل ترفهيه فإنه سيأخذ الكثير من الوقت. كل هذا دفع بالمشرع (في إطار أن رب العمل ينتظر من موظفه أن يقوم بعمله بكل أمانة وإخلاص احتراما لبنود العقد) إلى اعتبار كل موظف يقوم باستعمال الانترنت في أوقات العمل لأغراض شخصية مخالفا للقانون، ويعطي الحق

[1] قورة نائلة، مرجع سابق، ص. 392.

للرب العمل بفصل الموظف الذي يقوم بذلك في أوقات العمل ويستخدم وسائل المؤسسة.[1]

ولابد أن نشير إلى أن الغالبية العظمى من أفعال الاستعمال غير المصرح به يقوم بها العاملون والموظفون في القطاعين العام والخاص اللذين يكون لهم الحق في استخدام النظام المعلوماتي، وفي واقع الأمر فإن هذا السلوك شائع ومنتشر بين أوساط العاملين في المؤسسات المختلفة، وذلك لعدم وجود شعور بعدم أخلاقية أوعدم مشروعية الفعل،[2] بين هؤلاء المستخدمين.

وبالرغم من أن الاستعمال غير المصرح للنظام المعلوماتي لا يسبب خسائر كبيرة مقارنة بالجرائم المعلوماتية الأخرى، إلا أنه يمس مصالح جديرة بالحماية، كالمصالح الاقتصادية للمؤسسة التي قد يصبها الكثير من الضرر نتيجة عدم حماية النظام المعلوماتي من هذا الاستعمال، إذ قد يتسبب هذا الاستعمال كذلك في أن تفقد المؤسسة خدماتها أو عملائها بسبب إعاقة النظام عن أداء عمله وزيادة تحميله، وهو ما يؤدي إلى تعطيله في كثير من الحالات.[3]

والصورة الغالبة لحالات سرقة منفعة الحساب الآلي لا تهدف إلى تحقيق غرض إجرامي، بل قد يلجا إليها بعض الأشخاص على سبيل القيام ببعض الألعاب في أوقات الفراغ أو لنسخ هذه الألعاب، وقد يتم استخدام النظام لانجاز أعمال خاصة تهدف لتحقيق غايات تجارية أو إجرامية أو غير ذلك.

---

[1] Féral-Schuhl Christian, Cyber droit (Le droit à l'épreuve de l'internet), Edition Dolloz, 2eme édition, 2000, P. 114.

[2] في استطلاع للرأي قامت به المؤسسة العامة لشركات التأمين ضد الحرائق والمخاطر في فرنسا (APSAIRD) حيث كان السؤال المطروح على العاملين في لمؤسسة: هل من الممكن أن تستخدموا الأنظمة المعلوماتية داخل المؤسسات التي تعملون بها لأغراض شخصية؟ وكانت نتيجة الاستطلاع أن أجاب 23 % بالنفي (أي عدم استعمال هذه الأنظمة لأغراض شخصية)، في حين أن 77% أجاب بالإيجاب على اعتبار أن ذلك يعد عملا مألوفا، ومن بين المجيبيـن بنعم قام 19% فعلا باستخدام الحاسوب لأغراض شخصية، مشار إليه عند: قورة نائلة، مرجع سـابق، ص. 396.

[3] قورة نائلة، المرجع نفسه، ص. 388.

ويتم سرقة منفعة الحاسب الآلي، بالاستخدام غير المشروع لأنظمة المعلوماتية أو لسرقة الخدمات المعلوماتية أو سرقة الوقت، وهي واسعة الانتشار في مجال المعلوماتية، كاستخدام أرقام حسابات الشركة أو التلاعب ببيانات الحاسب الآلي، لمعرفة على سبيل المثال الوقت الفعلي لدفع الأجرة أو لمعرفة زبائن شركة ما أو الخدمات التي تقدمها.[1]

كما أن الآراء الفقهية قد تضاربت فيما يتعلق بالوصف والتكييف القانوني الذي يمكن إضافته على فعل أو سلوك سرقة وقت الحاسب، ونبين ذلك فيما يلي:

- **الاتجاه الأول، وصف السرقة:** يرى جانب من الفقه،[2] أنه بالإمكان العقاب على سرقة منفعة الحاسب الآلي، وذلك باعتبار أن هذا السلوك يشكل سرقة للتيار الكهربائي أو الطاقة، وقد تم انتقاد هذا الرأي استندا إلى أنه لا يوجد في هذه الحالة استخدام لموصل مخصص لسحب الطاقة بانتظام.[3]

كما أنه لا يمكن تطبيق النصوص الخاصة بجريمة السرقة على هذا الفعل، ذلك أن الفاعل لا يقوم بالاستيلاء على مال مادي منقول، كما أنه لا يخرج شيئا من حيازة مالكه ويدخله في حيازته، بل أن القصد الجرمي الخاص والمطلوب توافره في جريمة السرقة (نسبة التملك) غير متوافر، حيث أن فعل الجاني يقتصر على استعمال الخدمات المعلوماتية.[4]

- **الاتجاه الثاني، وصف الاحتيال (النصب):** وفقا لهذا الاتجاه فان استخدام الفاعل كلمة السر أو الشيفرة الخاصة للدخول إلى النظام المعلوماتي (الحاسب

[1] محمد أحمد أمين الشوابكة، مرجع السابق، ص. 181.
[2] من هؤلاء الفقهاء، الفقيه (Ber Tand) والفقيهان (Vivante et Lestanc)، مشار إليه عند: محمد سامي الشوا، مرجع سابق، ص. 222.
[3] الفقيهان (Pradel et Feuillard)، مشار إليه عند: محمد سامي الشوا، المرجع نفسه.
[4] قورة نائلة، مرجع سابق، ص. 403.

الآلي المعتدى عليه) وذلك بانتحال اسم كاذب أو صفة غير صحيحة،[1] يشكل بدوره جريمة احتيال.

غير أنه من الصعب قبول هذا التكييف، خاصة في الحالة التي يكون فيها الموظف العامل مسموح له بالدخول إلى النظام المعلوماتي للقيام بغرض معين، إلا أنه يستخدمه لأغراض شخصية أو تجارية، حيث لا يوجد هنا استخدام لطرق احتيالية، وذلك باعتبار أن الموظف يملك الشفرة الخاصة بالدخول إلى النظام.

- **الاتجاه الثالث، وصف خيانة الأمانة (إساءة الائتمان):** يذهب أصحاب هذا الاتجاه،[2] إلى أن سرقة منفعة الحاسب الآلي التي ترتكب بواسطة مستخدم بدون علم رب العمل، يسمح بتكييف الفعل أو السلوك غير المشروع على أنه خيانة أمانة إذا كان الحاسب الآلي قد سلم إليه بناء على عقد من عقود الأمانة.

أما إذا تمت سرقة منفعة الحاسب الآلي دون وجود عقد من عقود الأمانة فلا يقع هذا الفعل تحت أي وصف جنائي، حيث لا يوجد هناك انتهاك لأي علاقة تعاقدية وفقا لهذا الاتجاه.

أما عن موقف القضاء المقارن، فقد رفضت المحكمة العليا لولاية "إنديانا" الأمريكية إضفاء أو إسناد وصف السرقة على هذا الفعل وذلك في قضية Mc Graw[3]، وكذلك رفضت محكمة استئناف باريس في حكم لها عام 1987 إضفاء وصف السرقة على واقعة استعمال جهاز فك الشيفرات،

[1] الفقيه (R.Gassin)، مشار له عند: محمد سامي الشوا، المرجع نفسه، ص. 223.
[2] محمود احمد عبابنة، مرجع سابق، ص. ص. 89_90.
[3] المرجع نفسه، ص. 90.

وذلك لمشاهدة إرسال تلفزيوني مشفر، حيث أن هذا السلوك لا يخرج حيازة الخدمة من مالكها ولا يحرم المشاهد من استقبال الإرسال.[1]

وفيما يخص موقف التشريعات الجزائية المقارنة، فالملاحظ أن أغلب هذه التشريعات لم تفرد نصوصا لسرقة منفعة الحاسب الآلي، وإن كانت أفردت نصوصا لاستعمال أشياء الغير دون وجه حق، وهذا عكس القوانين الفيدرالية للولايات المتحدة الأمريكية التي جرمت هذا الفعل وبصراحة. كالقانون الخاص بولاية "فرجينيا" وولاية "نيوجيرسي" اللذان اعتبرا: أن هذا السلوك يشكل سرقة خدمة حاسب آلي.[2]

وفيما يخص القانون الفرنسي فإنه قد أورد فصلا للمعالجة الآلية للبيانات، وذلك في القانون الذي بدا العمل به سنة 1993 وذلك في المادة 323 وفي الفقرات من 1 إلى7، إلا أنه لم يتضمن نصا صريحا يجرم سرقة منفعة الحاسب.

أما فيما يخص قانون العقوبات الجزائري فهو لم يخرج عن هذا الصف، ولم يجرم فعل السرقة منفعة أو وقت الحاسب بشكل صريح، فيما أورده من نصوص سواء في القانون رقم 04-15 الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات أو القانون رقم 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، غير أن ذلك لا يمنع من إمكانية إعمال نص المادة 394 مكرر والتي تحضر استخدام منظومة معلوماتية عن طريق الدخول إلى نظام المعالجة الآلية للمعطيات بطريقة غير مشروعة (الغش).

[1] مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، مكتبة دار النهضة العربية، القاهرة، 2000، ص. 36.
[2] علاء الدين مغايرة، مرجع سابق، ص. 88 .

نخلص في الأخير إلى عدم إشارة معظم التشريعات إلى سرقة المعلومات، وكأن بهذا إشارة إلى أن هذه النصوص التشريعية لا تعترف بسرقة المعلومات، بل عالجت الوصول غير المصرح لها واختراقها وتقليدها أو نسخها نسخا غير مشروع، وهذا راجع إلى تضارب الآراء الفقهية فيما يخص الطبيعة القانونية للمعلومة فيما إذا كانت من قبيل الأموال أو لا.

المبحث الثاني: إتلاف المال المعلوماتي المعنوي

الإتلاف هو التأثير في مادة الشيء على نحو يذهب أو يقلل من قيمته الاقتصادية عن طريق الإنقاص من كفاءته للاستعمال المعد له.[1] فجوهر الإتلاف هو إفقاد المال المتلف منفعته أو صلاحيته للاستعمال في الغرض أو الهدف الذي اعد من أجله، وفعل الإتلاف في مجال المعلوماتية قد يقع على المكونات المادية للنظام المعلوماتي، وقد يقع على المكونات المعنوية لهذا النظام المتمثلة في المعلومات دون أن يؤدي ذلك إلى إتلاف أي عنصر مادي.

ففي الحالة الأولى، والتي يقع فيها الإتلاف على المكونات المادية للنظام المعلوماتي، كالإتلاف الذي يقع على شاشات العرض، وغير ذلك، يخضع للنصوص التقليدية في قانون العقوبات التي تتناول تجريم فعل الإتلاف أو التخريب.

أما فيما يتعلق بالحالة أو الصورة الثانية، والمتعلقة بإتلاف المال المعلوماتي المعنوي عبر شبكة الانترنت، والتي تتمثل في الاعتداء على سير نظام المعالجة الآلية للبيانات بمختلف التصرفات التدليسية المتمثلة بالدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه، وبما يترتب عليه من إتلاف للبيانات والبرامج أو بما يؤدي إليه من تعطيل أو إفساد نظام التشغيل.

ويقع الإتلاف على النظام المعلوماتي سواء كان ذلك بالدخول العمدي للنظام أو باستخدام الجاني الطرق الفنية والتقنية كالفيروسات (Virus) أو كان ذلك نتيجة الخطأ أثناء التواجد بالنظام أو الخروج منه، وإذا كانت التشريعات العقابية العربية لم تأخذ بعين الاعتبار الطبيعة اللامادية للأموال وما إذا كانت محلا لجريمة الإتلاف على خلاف المشرع الجزائري الذي قدم حماية لهذه الأموال من الاعتداء عليها عن طريق الإتلاف، وكذلك فعلت التشريعات المتقدمة والتي أضفت حماية لهذه الأموال

[1] جميل عبد الباقي الصغير، مرجع سابق، ص. 153.

وخاصة التشريع الأمريكي في قانون الاحتيال وإساءة استخدام الكومبيوتر لعام 1996، وكذلك التشريع الفرنسي في قانون العقوبات لعام 1992 والمعمول به منذ عام 1994 والذي فرق بين الاعتداء على سير عمل النظام المعلوماتي بإعاقته (إفساده أو تعطيله) وبين الاعتداء عليه بإتلاف البيانات والمعلومات.

المطلب الأول: إعاقة سير العمل في نظام المعالجة الآلية للبيانات

يعتبر إعاقة سير العمل في النظام المعلوماتي وجه من أوجه إتلاف المال المعلوماتي، وذلك أن هذا السلوك يسبب تباطؤ في عمل نظام المعالجة الآلية للبيانات أو إرباكه، مما يؤدي إلى تغيير حالة عمل النظام على نحو يصيبه بالشلل المؤقت،[1] وتتمثل أساليب الإعاقة في تعديل البرامج في نظام المعالجة أو عمل برنامج احتيالي، أو من خلال إجراء التحويلات الالكترونية كإغراق موقع على الشبكة بالرسائل الالكترونية مما يؤدي إلى شله.[2]

وقد تناول المشرع الفرنسي الأحكام المتعلقة بجرائم الإتلاف والتخريب في المواد (1/322) إلى (14/322) من قانون العقوبات، ويمكن القول بأن هذه النصوص تعاقب على مختلف صور الإتلاف التي يمكن أن تلحق بسير العمل في نظام المعالجة الآلية للبيانات، ولا سيما نص المادة 323 والتي يقابلها في قانون العقوبات الجزائري المادة 394 مكرر، وكذلك فعل المشرع الأمريكي في قوانينه الفيدرالية المختلفة، حيث جرم الاعتداء على النظام المعلوماتي وإتلاف البيانات والبرامج، ولا سيما في القانون الفيدرالي للاحتيال وإساءة استخدام الكمبيوتر، وقانون خصوصية الاتصالات الإلكترونية، والتي تقع بعد جريمة الدخول غير المشروع إلى نظام معلوماتي أو البقاء غير المشروع فيه.[3]

---

[1] Eurlich Sieber، ترجمة سامي الشوا، مرجع سابق، ص. 78.
[2] عمر الفاروق الحسيني، مرجع سابق، ص. 75.
[3] أحمد أمين محمد الشوابكة، مرجع سابق، ص. 223.

تنص المادة (394 مكرر) من قانون العقوبات الجزائري يقابلها نص المادة (1/323 قانون العقوبات الفرنسي) على أن "يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 200.000 دج 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 أو تغيير لمعطيات المنظومة. وإذا ترتب على الأفعال المذكورة أعلا تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستـــة (6) أشهر إلى ســـنتين (2) والغرامة من 50.000 دج إلى 300.000 دج".[1] فالمشرع الجزائري عاقب على جريمة الدخول والبقاء داخل جزء أو كل نظام معلوماتي كما أسلفنا الذكر، وضاعف العقوبة في حالة ما إذا أسفر هذا الدخول والبقاء على محو وحذف أو تغيير معالم المعطيات المتوافرة في المنظومة.

وفي الفقرة الثالثة من المادة 394 مكرر جرم المشرع الجزائري إعاقة أو تعطيل سير العمل في النظام المعلوماتي من خلال إفساد تشغيل المنظومة وذلك بالنص على أن "إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس ...".

وإذا ما انتقلنا إلى نص المادة 394 مكرر 1 من القانون 04-15 والتي نصت على "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث سنوات (3) وبغرامة من 500.000 دج إلى 4.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها". يقابل هذه المادة في القانون الفرنسي المادة 3/323 ق.ع، وعلى ذلك فإن الفعل المجرم يتخذ صورتين:

[1] قانون رقم 04-15، مؤرخ في 10 نوفمبر 2004.

- إدخال معطيات في نظام المعالجة الآلية، حيث تكون هذه المعطيات غريبة عن النظام المعلوماتي وهذا بطبيعة الحال يؤدي إلى إعاقة سير نظام المعالجة.
- تخريب (إفساد) المعطيات التي يتضمنها نظام المعالجة الآلية، ومن التطبيقات القضائية لهذه الجريمة ما قضي في فرنسا بأنه يقع تحت طائلة نص المادة 3/323 قانون العقوبات الفرنسي، يقابلها المادة 394 مكرر 1 قانون العقوبات الجزائري كل من تعتمد إدخال "فيروس المعلوماتية" في برنامج (Logiciel) الغير وكذا الامتناع عن إخبار هذا الأخير بإدخال هذا الفيروس ولو حصل ذلك بصفة عرضية.[1]

ويثور التساؤل، عما إذا كان المشرع الجزائري يشترط لوقوع هذه الجريمة أن يقع إتلافا كليا أو جزئيا للمعطيات، كمحو أو تعديل المعلومة، أم أنه يكفي مجرد الإضرار بسير العمل في نظام المعالجة الآلية للبيانات ؟

ذهب البعض إلى أن مجرد عرقلة العمل بالنظام يؤدي إلى قيام الجريمة، ومرد ذلك أن هذه الحالة هي نفسها كحالة محو أو تعديل أو إلغاء المعلومات، بل هي تأخذ شكلا أكثر اتساعا من الأشكال المتبعة في قرصنة المعلومات.[2] وبالتالي فإن نص المادة ينطبق على كل إضرار بسير العمل، سواء نجم عنه إتلاف للمعطيات أو كان يحاول أن يؤدي إلى ذلك.

وتشمل جريمة إعاقة سير العمل في نظام المعالج الآلية للبيانات كل إعاقة مادية (أي وجود مانع يعترض سير العمل) كإتلاف الكيان المنطقي أي البرامج

[1] أحسن بوسقيعة، الوجيز في القانون الجزائري الخاص، مرجع سابق، ص. 446.
[2] أحمد طه تمام، مرجع سابق، ص. 352.

(logiciel) وكذلك تشمل كل إعاقة معنوية كاستخدام الفيروسات أو القنابل المنطقية.[1]

المطلب الثاني: الأساليب المتبعة في إتلاف المعلومات

عرف البعض من الفقه الإتلاف بأنه لا يخرج عن كونه التأثير على مادة الشيء، على نحو يذهب أو يقلل من قيمته الاقتصادية عن طريق الإنقاص من كفاءته للاستعمال ومن قيمته.[2]

وكما ذكرنا سابقا أن للحاسوب والانترنت خدمات وتسهيلات ومعارف، بل ومصطلحات جديدة، فقد أمد كذلك عالم الجريمة أبعاد جديدة فصار من الممكن ارتكاب جريمة اختلاس أو سرقة أو إتلاف عن بعد.

يأخذ الاعتداء على البيانات والبرامج داخل النظام المعلوماتي بإتلافها إحدى الصورتين: [3]

- أن يتم محو البيانات والمعلومات كلية وتدميرها إلكترونيا.
- أن يتم تشويه المعلومة أو البرنامج عن طريق تعديل البيانات أو تعديل طرق معالجتها.

إن إتلاف البيانات والأموال اللامادية سواء بمحوها وتدميرها الكترونيا أو بتشويهها أو تعديل طرق معالجتها يثير اختلافا "جنائيا ملموسا" فيما يخص تكييفها بحسب الغاية التي هدف إليها المجرم المعلوماتي من خلال سلوكه و قيامه بفعل الإتلاف، وذلك على فرضيتين: [4]

[1] محمد سامي الشوا، مرجع سابق، ص. 201.
[2] قارة آمال، الجريمة المعلوماتية، رسالة لنيل درجة الماجستير في القانون الجنائي، جامعة بن عكنون، 2002، ص. 106.
[3] هدى حامد قشقوش، مرجع سابق، ص.567.
[4] أحمد طه تمام، مرجع سابق، ص. 358.

- **الفرض الأول:** يشكل هذا السلوك أي (الفعل) إتلافا بالمعنى القانوني إذا كانت هذه المعلومات أو البرامج هي هدف الجاني، ويقصد الإضرار بالغير، دون أن تتجه إرادته إلى ارتكاب جريمة أخرى.

ومن التطبيقات القضائية للقضاء الفرنسي، ما ذهبت إليه محكمة الاستئناف بإدانة متهم بالجنحة المنصوص عليها في المادة 3/323[1] قانون العقوبات الفرنسي، لقيامه بتعديل المعطيات التي سبق وأن قام بتسجيلها عن طريق نظام آلي للمحاسبة والتي قام بالإشراف عليها، وقد أيدت محكمة النقض الفرنسية في قرارها في 8 ديسمبر 1999 واقعة التعديل أو الإلغاء لمعطيات يحتوي عليها نظام المعالجة لآلية بالمخالفة للوائح المطبقة.[2]

- **الفرض الثاني:** تكييف بعض الأفعال الجرمية على أساس أنها جريمة نصب أو تزوير، ومثال ذلك تكييف واقعة قيام محاسب بمحو بيانات ومعلومات معالجة آليا تخص إحدى الشركات على أنها تشكل نصب معلوماتي، إذ اعتبر المحو الذي وقع بالاعتداء على البيانات الموجودة بالبرنامج المحاسبي على أنه يشكل جريمة احتيال على الرغم من أن المحو (الإزالة) من وسائل الإتلاف،[3] وكذلك قد يكيف الاعتداء بتغير أو تعديل بيانات إلكترونية على أنه يشكل جريمة تزوير.

وصور الإتلاف قد تكون عن طريق التدخل في الكيان المنطقي، ويقصد به البرامج المخصصة للقيام بالمعالجة عن طريق الحاسب الآلي (logiciel) أو عن طريق طرائق فنية لإتلاف المال المعلوماتي المعنوي.

---

[1] المادة 3/323 تنص "إن إدخال البيانات بطريق الغش في نظام المعالجة الآلية، أو محوها أو التعديل بطريق الغش للمعطيات التي يحتويها، يعاقب عليه بالحبس لمدة ثلاث سنوات وبغرامة مقدارها 150.000 €" أنظر: محمد أمين الشوابكة، مرجع سابق، ص. 224.

[2] احمد طه تمام، المرجع نفسه،ص358.

[3] المرجع نفسه، ص. 356.

الفرع الأول: التدخل في الكيان المنطقي.

يمثل الكيان المنطقي (Logiciel) مجموعة البرامج المخصصة للقيام بالمعالجة عن طريق الحاسب الآلي، ويتجسد الإتلاف هنا إما بتعديل البرنامج أو بخلق برنامج جديد[1] أو بالاقتحام والتسلل.

- **تعديل البرنامج:** يعد البرنامج كيانا ماديا يمكن رؤيته على شاشة الحاسب كترجمة لمجموعة من الأفكار، كما يمكن الاستحواذ عليه عن طريق تشغيله في الحاسوب،[2] ويأخذ هذا الفرض أي إمكانية الاستحواذ على هذا البرنامج عدة صور منها:[3]

أ. التلاعب في البرامج: ويتم ذلك ببرمجة الجهاز الآلي والنظام المعلوماتي بشكل يؤدي إلى اختفاء البيانات بشكل كلي أو جزئي.

ب. اختلاس نتائج الحساب: ويتم ذلك عن طريق إعادة نسخ المعطيات عن بعد أو عن طريق عملية النقل الإلكتروني للبيانات، وذلك بإتباع أسلوب التجسس المعلوماتي عن طريق بث برامج خاصة بالتقاط البيانات المتبادلة عبر شبكة الإنترنت.

ج. تغيير نظام التشغيل: ويتجسد ذلك بتزويد برنامج نظام التشغيل بمجموعة تعليمات إضافية يسهل الوصول إليها بواسطة كلمة السر أو مفتاح الشيفرة وأداة الربط بحيث تتيح الوصول إلى جميع المعطيات التي يتضمنها الحاسب الآلي.

[1] البرنامج هو عبارة عن مجموعة تعليمات، مكتوبة بلغة ما، موجهة إلى الحاسب الآلي بغرض الوصول إلى نتيجة معينة، أنظر: محمد أمين الشوابكة، مرجع سابق، ص. 240.
[2] هدى حامد قشقوش، مرجع سابق، ص. 568.
[3] محمد سامي الشوا، الغش المعلوماتي ظاهرة مستحدثة، مرجع سابق، ص. 555.

- **اصطناع برامج جديد:** تتمثل هذه الحالة في أن يكون البرنامج المصطنع وهميا أو أن يكون برنامجا ناقصا من الناحية الفنية.

أ. إعداد برنامج ناقص متن الناحية الفنية: وفي هذه الحالة يقوم المجرم المعلوماتي وهو في غالب الأحيان يكون المبرمج بإدخال فجوات في برنامج الحاسب الآلي حتى يتمكن من تنفيذ التعديلات الضرورية بإدخال أرقام سرية إضافية أو إحداث مخارج وسيطة.[1] وإذا كان يفترض في المبرمج نزع هذه الفجوات عند الانتهاء من البرمجة، إلا أن سيء النية من المبرمجين قد يتغاضون عن استعباد هذه الفجوات لممارسة أفعال الغش والاستمرار في استغلال البرنامج المعيب من الناحية الفنية، أو أنها قد تنسى بطريق الخطأ بسبب عيب في التصميم، مما يعطي للمجرم المعلوماتي فرصة الولوج من خلالها.[2]

ب. خلق برنامج وهمي: أي اصطناع برنامج كامل ومخصص فقط لارتكاب فعل أو سلوك الغش المعلوماتي، ومثال ذلك ما قامت به إحدى الشركات الأمريكية باصطناع عددا وهميا من المؤمن عليهم بواسطة وثائق تأمين بلغ عددها 64.000 وثيقة أقتصر دورها على إدارة الحسابات، ولزيادة التضليل قام الجناة بوضع رقم سري خاص بالبرنامج، تمت برمجته بدقة تامة، بحيث لا يظهر في الشاشة إلا الوثائق السليمة تماما وقد حصل الجناة في هذه العملية على مبلغ 200 مليون دولار.[3]

[1] جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا، مرجع سابق، ص. 54.
[2] محمد احمد أمين الشوابكة، مرجع سابق، ص. 237.
[3] المرجع نفسه.

- **الاقتحام أو التسلل:** وتشمل الاختراقات سواء المواقع الرسمية أو الشخصية أو التسلل إلى الأجهزة الشخصية، كاختراق البريد الالكتروني أو الاستيلاء عليه والاستحواذ على اشتراكات الآخرين وأرقامهم السرية، ولكي يتم الاختراق يستخدم المتسللون ما يعرف بحصان طروده،[1] وهو برنامج صغير يتم تشغيله داخل جهاز الحساب لكي يقوم بأغراض التجسس على أعمال الشخص، فهو في أبسط صورة يقوم بتسجيل كل طريقة قام بها على لوحة المفاتيح منذ أول لحظة للتشغيل ويشمل ذلك كل بياناته السرية أو حساباته المالية أو محادثاته الخاصة على الانترنت أو رقم بطاقة الائتمان الخاصة.[2]

ويعد الهجوم على المواقع المختلفة في شبكة الانترنت من الجرائم الشائعة في العالم، وقد تعرضت لهذه النوع من الجرائم العديد من المواقع كموقع وزارة العدل والمخابرات المركزية للولايات المتحدة الأمريكية كما تعرض له حزب العمال البريطاني، كما أن مواقع الصحف والمجلات كانا في كثير من الأحيان عرضة للتخريب. يعتبر مصطلح "حصان طروادة" مصطلح أسطوري يضفي طابع كلاسيكي على هذه الوسيلة الإجرامية والتي لم يتم اكتشاف سوى حالات قليلة من هذا النوع من الجرائم، ولكن يكثر الحديث عن هذه التقنية نظرا لنجاحها في غالبية الأحوال، وأن هناك عدد ضئيل من الذين يملكون المهارة والمعرفة لممارسة هذه التقنية،[3] أو لوجود تقنيات إجرامية أسهل وأقل حرفية مثل تقنية إتلاف المعلمات، وهذا ما يميز

[1] برامج حصان طروادة هي تلك البرامج التي تبدو وكأنها قطع جذابة مضافة إلى البرامج، إلا أنها تملك القدرة على الإضرار بالبيانات، وعلى عكس الفيروسات فهي لا تقوم بنسخ نفسها أليا، وبدأ هذا البرنامج في الظهور في أواخر السبعينيات نتيجة انتشار استخدام اللوحات الالكترونية للبيانات والتي تتيح إما تخفيف أو زيادة تحميل البرنامج، وبرنامج حصان طروادة يتمثل في إدخال أوامر على نحو غير مشروع إلى الحاسب الآلي بهدف تحقيق أغراض إجرامية أنظر: حسين علي محمود، مرجع سابق، ص. 113.

[2] علي جبار الحسيناوي، جرائم الحاسوب والانترنت، دار اليازوري، عمان، 2009، ص. 105.

[3] حسين علي محمود، مرجع سابق، ص. 113.

السلوك الإجرامي للمجرم المعلوماتي، هذا السلوك الذي يتطلب المعرفة والخبرة، والذي يعتمد على أساليب وتقنيات جد معقدة تختلف تماما على السلوك الإجرامي المتبع من طرف المجرم التقليدي.

الفرع الثاني: الطرق الفنية لإتلاف المعلومات.

من البشر من هم بناءون، كما أن منهم أيضا هدامون، منهم من يطور برامج مفيدة هادفة، ومنهم من يطور برامج خبيثة تستخدم في إتلاف واستنزاف الموارد، ودوافع ذلك كما أشرنا في السابق أن لكل مجرم معلوماتي دافعه الخاص، فمنهم من يقوم بذلك لمجرد أن يثبت لنفسه أو لغيره قدرته على تطوير برامج تستطيع الاختراق أو التجسس أو التخريب، ومنهم من يقوم بذلك لسرقة المعلومات، سواء على مستوى الأفراد أو الشركات، وآخرون كان دافعهم الانتقام من الشركة التي يعمل بها، أو ابتزاز شركة ما بعد ما يقوم بسرقة معلومات مهمة لهذه الشركة، ثم يقوم بمساومة الشركة على تلك المعلومات.

إن القيام بإتلاف المعلومات المخزنة في جهاز الحاسوب أو المتبادلة عبر شبكة الإنترنت يؤدي إلى تدميرها أو محوها أو تشويهها بشكل يؤثر في عمل النظام المعلوماتي.

وتتنوع أساليب إتلاف المعلومات وأنماطها، ولا يمكن عمليا حصرها، والاعتداء على المعلومات بالإتلاف أو التخريب قد يتحقق بالإدخال غير المشروع للمعلومات أو للبرامج أو البيانات التي لم تكن موجودة من قبل في نظام معلوماتي ما من أجل التشويش على المعلومات أو البيانات الموجودة ، وهذا ما يؤدي إلى التأثير على قيمتها كمعلومة.[1]

[1] نهلا عبد القادر المومني، مرجع سابق، ص. 125.

وأكثر الأساليب انتشارا هو إدخال البرامج الخبيثة (الفيروسات) إلى النظام المعلوماتي لغرض إتلافها، حيث أنها تستخدم في الوقت الراهن على نطاق واسع وتسبب خسائر اقتصادية فادحة بمختلف القطاعات وذلك لسهولة انتشارها وسرعة عملها، هذه الوسائل المستخدمة في إتلاف البيانات والبرامج، بدءا من فيروسات الحاسب الآلي ومرورا ببرامج الدودة وانتهاء بالقنبلة المنطقية أو الزمنية، يتفق الفقهاء على أن المشكلات القانونية التي تنشأ عن جميع الفيروسات واحدة، فلا وجه للتفرقة بين الفيروس والدودة و حصان طروادة، فهي نفسها وتختلف في تقنية عملها ويترتب عليها نفس المشكلات القانونية.[1]

- **فيروسات الحاسب الآلي:** يمكننا القول أنه لا يوجد أحد لم يسمع بالفيروسات الحاسوبية بل يمكننا أيضا أن نقول أن القليل من يسلم منها، فعند إجراء مسح لعدد كبير من الشركات، في سنة 2000 م وجد أن 99.67 % منهم تعرضوا على الأقل لفيروس واحد، ويتراوح عدد الفيروسات الجديدة كل يوم ما بين 10 إلى 20 فيروس جديد، بل أن أحد الشركات المتخصصة في مكافحة الفيروسات أضافت 1418 تعريفا لفيروس جديد خلال شهر نوفمبر عام 2004، ويقدر عدد الفيروسات المعروفة بقرابة مئة آلف فيروس.[2]

والفيروس كما حدده وعرفه أحد التقارير الصادرة عن المركز الوطني الأمريكي للحواسب، عبارة عن "برامج مهاجمة تصيب أنظمة الحسابات بأسلوب يماثل إلى حد كبير أسلوب الفيروسات الحيوية التي تصيب الإنسان".[3]

[1] محمد أمين الشوابكة، مرجع سابق، ص. 238.
[2] خالد بن سليمان الخثبر، محمد بن عبد الله القطحاني، آمن المعلومات، مكتبة الملك فهد الوطنية، للنشر، الرياض، 2009، ص. 65.
[3] عفيفي كامل، مرجع سابق، ص. 197.

وهي عبارة عن برامج حاسوبية خبيثة مضرة بالحواسب، وتنتقل بين أجهزة الكمبيوتر بعدة طرق، ويتكاثر بالاعتماد على ملفات أخرى،[1] وبعبارة أخرى "هي برامج مشفرة مصممة بقدر كبير على التكاثر والانتشار من نظام إلى أخر، إما بواسطة قرص ممغنط أو عبر شبكات الاتصالات بحيث يمكنه أن ينتقل عبد الحدود من أي مكان إلى آخر في العالم، وهو يسمى عادة باسم أول مكان اكتشف فيه، والبرامج الفيروسية لها قدرة على الاختفاء، داخل برنامج سليم حيث يصعب اكتشافها، كما أنها قد تكون مصممة لتدمير برامج أخرى أو تغيير معلومات ثم تقوم بتدمير نفسها ذاتيا دون أن تترك أثر يدل عليها، أو على مستخدمها، وعلى الرغم من تدميرها للبرامج والمعلومات إلا أنها لا تسبب عادة تدمير لأي من المكونات المادية للنظام.[2]

وفي تعريف مقتضب يمكن تعريف الفيروس الإلكتروني هو برنامج صغير يسكن القرص الصلب أو ذاكرة الكمبيوتر لهدف التخريب وإتلاف وظائفه الطبيعية.[3]

كما أن للفيروس الإلكتروني تأثير على سير النظام المعلوماتي إذا أن النظام يقوم بنسخ الفيروس وهذا ما يؤدي إلى إتلاف السير الطبيعي للنظام.[4]

وكان أو ما فكر في فيروس الحاسوب هو (جون نيومان) عام 1949 عندما طرح الفكرة الأساسية في تصميم الفيروس الإلكتروني في مقال شركة تحت عنوان "نظرية التعقيد الأوتوماتيكي" ومفاده أن جهاز الحاسوب يمكن أن

[1] خالد سليمان الخثير، المرجع نفسه، ص. 66.
[2] قوورة نائلة، مرجع سابق، ص. ص. 191_192.
[3] Nasim Derdour, les informations Informatiques au regard du droit Français et les cas du droit Algérienne, mémoire de fin d'étude en vue de l'obtention d'un diplôme de (D.E.A), Universitaire de perpignan, 2003, p. 24.
[4] Pansier Frédéric-Jérôme, jez Emmanuel, Initiation à l'Internet, Juridique, édition litec (2 édition), 1er trimestre 2000, p. 67.

يدمر نفسه، ولم يلق هذا المقال في حينه أهميته لقلة انتشار الحواسيب،[1] وتتمتع الفيروسات بقدرة هائلة على مهاجمة أجهزة الحاسوب والشبكات المعلوماتية، فهي تعطل الاتصالات وتشوه البيانات بل وتضلل المستخدم أحيانا ببيانات خاطئة، والفيروس قد يؤدي إلى تغير الحقيقة، أو تعديل المعلومات، هذه الوسيلة التقنية المستخدمة في مجال ارتكاب الجرائم المعلوماتية تشكل رعبا حقيقيا لكل مستخدمي أجهزة الحاسوب وشبكة الإنترنت العالمية وذلك نظرا للتزايد الهائل في حجم الاعتماد على تقنيات نظم المعلومات لدى الأفراد والمؤسسات والشركات وكذلك الدول في تسيير مختلف الأعمال ومثال ذلك مشروع برنامج الجزائر الإلكترونية 2013.

وتترتب عن هذه الفيروسات باعتبارها وسيلة تقنية مستخدمة في ارتكاب جريمة تدمير المعلومات وإتلافها خسائر مادية فادحة يقدر بملايين الدولارات فضلا "في تعطيل الأنظمة المعلوماتية لفترة قد تطول وقد تقصر مما ينتج عنه خسائر ضخمة.

ومن الأمثلة التي تعكس خطورة هذا النوع من الإجرام قيام أحد المبرمجين بإطلاق فيروس من جهاز حاسوب إستهدف شبكة أربانت (ARPANET) التي تربط حواسيب مؤسسات على درجة كبيرة من الأهمية من الجيش والجامعة وإدارة البحث العلمي في الولايات المتحد الأمريكية هذا فيروس قام بنسخ نفسه عدة مرات في هذه الشبكة ونتجت عنه أضرار مادية قدرت بـــ 96 مليون دولار أمريكي".[2]

ويستخدم الفيروس بشكل عام لتحقيق أحد الفرضيتين.[3]

[1] مخبخب نعيم، المرجع السابق، ص 218.
[2] كامل عفيفي، المرجع السابق، ص. 198.
[3] ساعي الشوا، المرجع السابق، ص. 190

أ. الغرض الحمائي: ويكون ذلك لحماية البيانات والبرامج من خطر النسخ غير المشروع (المرخص به)، إذ ينشط الفيروس بمجرد النسخ ويدمر نظام الحاسوب الذي يعمل عليه.

وهناك عدة اتهامات تشير إلى الشركات الكبرى التي قد تلجأ أحيانا إلى هذه الحيلة لحماية برامجها من النقل غير المشروع الذي يهدد استثماراتها في هذا المجال حيث يتم إطلاق هذه الفيروسات عند محاولة النقل غير المشروع.[1] غير أن هذا الأسلوب المتبع من طرف الشركات لا يمكن اعتباره غير قانوني فهو يحمي منتجاته من السرقة والنسخ المجاني لبرامجه أي يمكن استعمال الفيروس كوسيلة لمحاربة سلوك من السلوكيات المتبعة من طرف المجرم المعلوماتي.

ب. الغرض التخريبي: يتم إعداد هذه الفيروسات من قبل فئة مريضة من خبراء البرامج وذلك بهدف الدعاية أو الابتزاز فيصبو صانع الفيروس إلى التخريب بحد ذاته أو إلى التخريب بهدف الحصول على منافع شخصية، حيث تكون هذه الفيروسات مرافقة ومخزنة على البرامج التطبيقية وبرامج التشغيل وتنشط في حالة النسخ من جهاز لآخر أو عن طريق نقل المعلومات المباشرة من شبكة لأخرى بحيث تكون مختبئة داخل رسائل البريد الالكتروني والوثائق والمعلومات التجارية والمالية عبر الشبكة.[2]

تنقسم أنواع فيروسات الحاسب الآلي من حيث تكوينها وأهدافها إلى:[3]

[1] محمد أمين أحمد الشواكة، المرجع السابق، ص. 238
[2] سامي الشوا، مرجع سباق، ص.191
[3] نهلا عبد القادر، مرجع السابق، ص. 128

أ. فيروس عام العدوى: وهو ينتقل إلى أي برنامج أو ملف ويهدف على تعطيل نظام التشغيل بكامله.

ب. فيروس محدد العدوى: وهو يستهدف نوعا معينا من النظم لمهاجمته ويتميز عن النوع السابق بأنه أبطأ في الانتشار، وصعوبة اكتشافه.

ج. فيروس عام الهدف: ويتميز بسهولة إعداده واتساع مدى تدميره وتندرج تحته غالبية الفيروسات.

د. فيروس محدد الهدف: ويقوم بتغيير الهدف من عمل البرامج دون تعطيلها وهو يحتاج إلى مهارة عالية والمجني عليه في معظم الأحيان لا يعرف من المجرم المعلوماتي الذي صمم الفيروس كما أنه قد لا يعرف لمدة طويلة إصابة برامجه بالفيروس كما أن المجني عليه قد لا يرغب في الإعلان عن إصابة نظامه بهذا الفيروس خصوصا إذا كانت مؤسسة مالية.[1]

ويعود سبب انتشار الفيروسات بشكل كبير إلى وجود الشبكة العالمية للمعلومات فقبل ظهور الإنترنت كان انتشار فيروس معين في جميع أنحاء العالم يستغرق عامين إلى خمسة أعوام أما الآن فيستغرق الأمر ساعات محدودة.[2] ومن أشهر الفيروسات الموجهة ضد الحواسيب والشبكات العالمية:[3]

أ. فيروس الإبطاء ويتمثل عمله في إبطاء عمل جهاز الحاسوب بصورة تدريجية تمهيدا لإيقافه عن العمل.

[1] عفيفي كامل، مرجع سابق، ص. 200
[2] نهلا عبد القادر المومني، المرجع نفسه، ص. 129.
[3] سامي الشوا، مرجع سابق، ص. 193.

ب. الفيروسات النائمة وهي خطيرة جدا وتكمن خطورتها في كونها تظل منكمشة فترة من الزمن ثم تنطلق لتنفيذ أهدافها التخريبية.

ج. الفيروسات التطورية: وهي فيروسات لها القدرة على أن تقوم بتغيير شكلها بمرور الوقت وبذلك تستطيع أن تقوم بمهمة تدمير برامج وبيانات الحاسوب دون صعوبة تذكر.

وهناك بعض الفيروسات تم تصنيعها في مناسبات معينة إما للتعبير عن الاحتفال بها أو للاحتجاج عليها منها: [1]

أ. فيروس مايكل أنجلو: أطلق هذا الفيروس يوم 06 مارس عام 1992 بمناسبة الاحتفال بذكرى ميلاد الرسام الايطالي الشهير وأصاب هذه الفيروس العديد من أجهزة الحاسوب الشخصية عبر العالم.

ب. فيروس ناسا: وهو فيروس أطلق احتجاجا على إنتاج الأسلحة النووية، فهو عبارة عن برنامج يحمل رسالة مناهضة للأسلحة النووية وتظل هذه الرسالة تكرر نفسها وتتكاثر بشكل مدمر للبرامج الأخرى.

- **برامج الدودة:** أطلق في عام 1988 عبر شبكة الانترنت في الولايات المتحدة الأمريكية برنامج يعرف بالدودة والذي سبب لأجهزة الحاسب الآلي من خلال شبكة المعلومات العالمية انهيار في قيادة وتوجيه الجامعات والمعدات العسكرية ومنشآت الأبحاث الطبية.[2]

هذه البرامج تكون مصممة للانتقال عبر شبكات الاتصال من جهاز إلى آخر وهو ما يؤدي إلى عجز النظام المعلوماتي عن أداء عمله عن طريق محو عدة أجزاء من المعلومات وفيروس الدودة يصيب جزءا محددا من نظام

[1] محمد أمين الشواكة، مرجع سابق، ص. 239
[2] هدى حامد قشقوس ، المرجع السابق، ص. 122.

المعالجة الآلية للبيانات وهو الجزء الخاص بنظام التشغيل.[1] ويهدف هذا البرنامج إلى تشغل أكبر حيز ممكن من سعة الشبكة ومن ثم العمل على تقليل أو خفض كفاءتها وأحيانا تتعدى هذا الهدف لتبدأ بعدها بالتكاثر والانتشار في التخريب الفعلي للملفات والبرامج ولنظم التشغيل.[2]

وقد أطلقت دودة الانترنت عن طريق طالب أمريكي يدعى روبرت موريس وهو طالب في قسم علوم الكمبيوتر بجامعة كورنيل بولاية نيويورك، حيث تعمد بث البرامج لكي يثبت عدم ملائمة أساليب ووسائل الآمان في شبكات الكمبيوتر ولكنه تسبب في تدمير الآلاف من شبكات الحاسب الآلي المنتشرة في الولايات المتحدة الأمريكية بالإضافة إلى إعاقة سير النظام المعلوماتي هذا بجانب خسائر مادية كبيرة وقد أدين بانتهاك قانون الاحتيال وإساءة استخدام الكمبيوتر وحكم عليه بالحبس لمدة ثلاث سنوات وبالعمل أربعمائة ساعة في الخدمة الاجتماعية وغرامة قدرها 10.500 دولار.[3]

- **القنبلة المعلوماتية:** أو ما يسمى بالقنبلة المنطقية و الزمنية، وهو اصطلاح يطلق على أنواع من البرامج التي تهدف إلى تدمير المعلومات كوسيلة لارتكاب جريمة الإتلاف، وتنقسم القنبلة المعلوماتية إلى:

أ. القنبلة المنطقية: وهي عبارة عن برامج صغيرة تم إدخالها بطرق غير مشروعة ومخفية مع برامج أخرى، وتهدف إلى تدمير وتغيير برامج ومعلومات النظام في لحظة محددة أو في فترة زمنية منتظمة، بحيث تعمل على مبدأ التوقيت فتحدث تدميرا وتغييرا في المعلومات والبرامج عند إنجاز أمر معين في الحاسب الآلي.[4] أي أن القنابل

[1] سامي الشوا، المرجع السابق، ص. 193.
[2] علي جبار الحسناوي، مرجع سابق، ص. ص. 105-106.
[3] محمد أمين الشوابكة، مرجع سابق، ص. 240.
[4] المرجع نفسه.

المنطقية تظل في حالة سكون ولا يتم اكتشافها مدة من الزمن قد تطول أو تقصر وهذه المدة يحددها المؤشر الموجود داخل برنامج القنبلة، هذا المؤشر لا يقتصر على مدة معينة، وإنما قد يمتد إلى ما يعرف بتوافر شروط منطقية معينة داخل برنامج أو ملف معين وذلك كما سبق وأشرنا حسب الرمز الذي يحدده برنامج القنبلة فإذا ما توافرت الشروط بدأ البرنامج في القيام بمهامه التخريبية.[1]

ومن الأمثلة على ذلك زرع القنبلة المنطقية لتعمل لدى إضافة سجل موظف، بحيث تنفجر سجلات الموظفين، الموجودة في المنشأة.[2]

ب. القنبلة الزمنية: سميت كذلك لقيامها بالعمل التخريبي في وقت يحدد مسبقا، فعلى سبيل المثال يمكن للمجرم المعلوماتي كتابة برنامج وظيفته مسح الكشوفات التي تحمل أسماء الموظفين وبياناتهم اللازمة لدفع رواتبهم قبل استلام رواتبهم بساعة، مما يؤدي إلى تأخير عملية الدفع وإرباك أعمال الشركة والإساءة لسمعتها.[3]

والقنبلة الزمنية أو الموقوتة عبارة عن برامج يتم إدخالها بطرق مشروعة متخفية مع برامج أخرى، وتهدف إلى تدمير برامج ومعلومات النظام وتغييرها.

كما تمكن القنابل الزمنية مستخدمها من تحقيق العديد من الأهداف:[4]

[1] عفيفي كامل، مرجع سابق، ص. 207.
[2] محمد سامي الشوا، المرجع السابق، ص. 196.
[3] أسامة محمد عوض، مرجع سابق، ص. 427.
[4] المناعسة أسامة، وآخرون، مرجع السابق، ص. 157.

يمكن من خلال هذه القنابل توقيت القيام بعملية التخريب وجعل هذه القنبلة تنفجر في وقت يلحق أكبر ضرر ممكن بالنظام المعلوماتي.

من شأن تأجيل التفجير أن يجعل التوصل إلى معدي هذه البرامج صعب إن لم يكن في بعض الأحيان مستحيلا.

التأجيل يتيح انتقال القنبلة للنسخ الاحتياطية للبرامج التي تقوم الجهة المستهدفة بإعادة إنتاجها.

ومن الأمثلة الواقعية، قيام محاسب خبير في نظم المعلومات، بوضع قنبلة زمنية في شبكة المعلومات الخاصة بالشركة وذلك بدافع الانتقام من المنشأة التي يعمل بها لفصله منها، حيث انفجرت بعد مضي ستة أشهر من رحيله من الشركة وترتب عن ذلك إتلاف كل البيانات المتعلقة بها.[1]

وفي الأخير فأن الفيروسات تتقاسم فيما بينها الصفات التالية:[2]

- خاصية التسلل والعمل في الخفاء.
- خاصية التكاثر ويعني بأن يصيب الفيروس جهاز الكمبيوتر ويقوم بنسخ نفسه عدة مرات بهدف الانتشار والالتصاق بالملفات.
- خاصية التخزين في برامج بدء التشغيل وهذه من الفيروسات الذكية.

في ختام بحثنا يمكن القول بأن التشريعات الغربية ومعها التشريع الجزائري قد نص على محاولة تجريم لكل فعل أو سلوك يؤدي إلى إتلاف المال المعلوماتي المعنوي وذلك في نص المادة 394 مكرر1 من قانون العقوبات الجزائري غير أن

[1] محمد سامي الشوا، المرجع نفسه، ص. 196.
[2] مجلة الأمن والحياة،العدد،199،2000،ص.50.

هذا لا يعد كافيا لحماية النظم المعلوماتية، من الاعتداءات المتزايدة من طرف المخربين (cracker) والذين يعتمدون على أساليب فنية تتطور بتطور النظم المعلوماتية.

المبحث الثالث: التزوير المعلوماتي

حرص المشرع الجزائي في كل دول العالم على تجريم التزوير في المحررات إيمانا منه بأن التزوير في المحررات يهدد الثقة العامة للأفراد بها، وبتالي يخل ويضر بالإستقرار في المعاملات وسائر نواحي الحياة القانونية في المجتمع.

والسبب في ذلك يرجع إلى أن المحرر المكتوب يعتبر وسيلة أساسية من وسائل الإثبات المدنية والتجارية في كل الأمور التي تتطلب إثباتا بالكتابة، فالمحررات هي وسيلة لحسم المنازعات واثبات الحقوق ولا يتاح للكتابة هذا الدور المهم الذي تقوم به إلا إذا منحها الناس ثقتهم.[1]

وفي مجال المعلوماتية الحديثة أصبح الحاسوب ونظامه المعلوماتي جزءا لا يتجزأ من حياة الأفراد اليومية، بل إنه أصبح يحل محل الأوراق في العديد من مجالات الحياة، مثل عمليات الدفع وطلابيات البضائع وتحويل الأموال من مصرف إلى آخر.[2]

كما أن معظم الهيئات الحكومية وهيئات القطاع الخاص تعتمد على الحاسوب في تسيير أعمالها، فأجهزة الحاسب الآلي تستخدم لحفظ المستندات ومعالجتها أليا.

وفي ظل هذا الانتشار المتزايد لتقنية المعلومات أصبح هناك قلق متزايد من ارتكاب جرائم تزوير البيانات والمعلومات المخزنة أو المنقولة عبر شبكة الانترنت، أو أن يتم تزوير مستخرجات النظام المعلوماتي من مستندات أو شرائط ممغنطة أو دعامات مسجل عليها المعلومات.

[1] أحمد حسام طه تمام، مرجع سابق، ص. 387
[2] جميل عبد الباقي الصغير، مرجع سابق، ص. 162.

ومما لاشك فيه أن جريمة التزوير المعلوماتي سيكون لها انعكاس سلبي على الثقة التي يوليها الأفراد للنظام المعلوماتي وما يحتويه من معلومات وما يتم استخراجه منه.

المطلب الأول: مدى انطباق أركان جريمة التزوير التقليدية على التزوير المعلوماتي

عرف الفقيه "غارسون" التزوير أنه تغيير الحقيقة بقصد الغش في محرر بإحدى الطرق التي قد تنص عليها القانون، تغيرا من شأنه أن يسبب ضررا، ويقترن بنية استعمال المحرر المزور فيما أعد من أجله.[1]

وبالرجوع إلى قوانين العقوبات التقليدية سواء التي أوردت تعريف للتزوير أم لم تورد تعريفا له، فإن كل هذه التشريعات تتفق في أن التزوير هو الذي ينصرف إلى المحررات، وعليه فإن الإجابة على التساؤل الذي طرحناه والذي مفاده مدى انطباق أركان جريمة التزوير التقليدية على التزوير المعلوماتي، ترتبط الإجابة عليه بمدى اعتبار المعلومات المخزنة في النظام المعلوماتي من قبيل المحررات ؟

وباستعراض الركن المادي لجريمة تزوير المحررات والذي يتمثل في تغيير الحقيقة في محرر بوسائل نص عليها القانون ويكون من شأن هذا التغيير أن يسبب ضررا.

والمشكلة التي تطرح نفسها هي شكل المحرر، والذي يشترط أن يكون في شكل كتابة أو عبارات خطية، وعلى هذا الأساس لا يعد محررا كل ما هو غير مكتوب كالعداد الحاسب لاستهلاك الكهرباء أو المياه أو الغاز أو الأختام المنسوبة

[1] محمود احمدعبابنة ، مرجع سابق، ص. 108

إلى فرد، ولنفس السبب أيضا لا تعد محررات الأفلام والأسطوانات وأشرطة التسجيل والأقراص الممغنطة أي كانت أهميتها القانونية.[1]

والتزوير المعلوماتي الذي يقع على المعلومات أو البيانات والمعطيات التي يحتويها النظام المعلوماتي قد يأخذ إحدى الصور التالية:

الفرع الأول: إدخال معلومات وهمية

تتمثل هذه الصورة في إدخال معلومات غير الصحيحة إلى النظام المعلوماتي، أو بمعنى آخر إدخال معلومات مصطنعة أي إدخال بيانات في نظام المعالجة الآلية لم تكن موجودة من قبل، وقد يتم إدخال هذه البيانات بقصد التشويش على صحة البيانات القائمة.[2]

ولعل اصطناع المعلومات هو الأسلوب الأكثر سهولة في التنفيذ ولاسيما في المنشآت ذات الأموال، حيث يعد المسؤول عن القسم المعلوماتي في أفضل وضع يؤهله لارتكاب هذا السلوك غير المشروع من التلاعب، والذي يكون بضم مستخدمين غير موجودين بالفعل أو الإبقاء على مستخدمين تركوا العمل.[3]

ومثال ذلك قيام أحد المسؤولين من القسم المعلوماتي بأحد الشركات الفرنسية بإعادة ملفات المستخدمين السابقين والذين لهم حقوق مالية وقام بتحويلها إلى حسابه وحسابات أخرى تم فتحها خصيصا لهذا الغرض حيث تم اختلاس أكثر من مليوني فرنك فرنسي.[4]

[1] أحسن بوسقيعة، الوجيز في القانون الجنائي الخاص، الجزء الثاني، دار هومة، 2009، ص. 336.

[2] هدى حامد قشقوش، مرجع سابق، ص. 569.

[3] نهلا عبد القادر المومني، مرجع سابق، ص. 149.

[4] محمد سامي الشوا، مرجع سابق، ص. 546.

الفرع الثاني: إدخال معلومات مزورة

تتمثل في التلاعب بالمعلومات داخل النظام المعلوماتي لتغيير الحقيقة فيها، وهذا التلاعب قد يتم عن طريق تعديل هذه المعلومات أو من خلال محو جزء أو عدة أجزاء منها.

وبتوضيح أدق، يعني تزوير المستندات والبيانات المخزنة على الكمبيوتر، وتزوير المعلومات وضع معلومات بديلة للمعلومات الحقيقة، وتزييف المخرجات، وتستهدف جريمة تزوير المستندات والبيانات بشكل وساع البيانات الممثلة للمستحقات المالية والإيداعات المصرفية وحسابات ونتائج الميزانيات وأوامر الدفع وقوائم المبيعات وأنظمة التحويل الالكترونية للأموال والودائع المصرفية.[1]

ويتم التزوير كما ذكرنا سابقا إما عن طريق استبدال المعطيات أو عن طريق المحو المنتقى للمعطيات.

الفرع الثالث: نظرة المشرع الجزائري للتزوير المعلوماتي

وبالرجوع إلى النصوص التقليدية المنظمة لجريمة التزوير نرى أن هذه النصوص لا يمكن أن تنطبق على تغيير أو تحوير الحقيقة في البيانات الالكترونية، حيث يعد التزوير وفقا لهذه النصوص التقليدية تغييرا في محرر بإحدى الطرق التي نص عليها القانون تغييرا من شأنه إحداث ضرر،[2] وهذا ما جاء في نص المواد من 214 إلى 229 من قانون العقوبات الجزائري.

وتعريف التزوير بهذه الصورة يخرج صورة التزوير الالكتروني بالتلاعب بالمعطيات، حيث يشترط أن يقع التزوير على محرر مكتوب وهو ما لا ينطبق على

[1] كمال احمد الكركي، النواحي الفنية لإساءة استخدام الكمبيوتر، بحث مقدم إلى ندوة الجرائم الناجمة عن التطور التقني المنعقدة بعمان، دار الثقافة، 1998، ص. 7.
[2] أحسن بوسقيعة، مرجع سابق، ص. 339

معطيات النظام المعلوماتي قبل أن تأخذ شكل المحرر أو المستند الالكتروني، والتي تمثل أحد مستخرجات الحاسب الآلي. كذلك هو الحال بالنسبة للمعلومات المسجلة كهرومغناطيسيا على وسائط التخزين الخاصة إذ لا يمكن مشاهدة هذه المعلومات عن طريق النظر المباشر،[1] فهذه المعلومات مخزنة في ذاكرة الحاسوب أو في الأقراص الممغنطة أو المدمجة أو على أي دعامة مادية ليست مقروءة، إذ لا يمكن بهذا الشكل قراءة المعلومات المحمولة عليه، وبتالي فإنها تفتقر على صفة المحرر.

أما مستخرجات الحاسوب من المحررات أو المستندات المعلوماتية الالكترونية فإنها مشمولة بالنص الخاص بجريمة التزوير في قانون العقوبات الجزائري، أما مستخرجات الحاسب الآلي الأخرى كالدعامات والأشرطة الممغنطة والتسجيلات فتفتقر إلى صفة المحرر، وبتالي فإن النصوص تأتي قاصرة على شمولها، وهذا ما اشترطه المشرع الجزائي الجزائري في شكل المحرر في أن يكون في شكل كتابة أو عبارات خطية، وهذا ما جعل المشرع الفرنسي نظرا للتطورات التقنية التي شهدها العالم في هذا المجال، وللمكانة التي تحتلها هذه الوسائل في الحياة اليومية إلى إضافة "كل سند آخر للتعبير عن فكر أو فكرة ..." إلى محرر،[2] ولا تهم طريقة الكتابة، فقد تكون بخط اليد أو بالآلة الكاتبة أو الإعلام الآلي أو بالطابعة.

فالتغيير أو التبديل الذي يقع على المعطيات أو الأوامر المختزنة والمنقولة عبر الشبكة لا تنطبق نصوص التزوير عليها، إذ أن الاعتداء على البيانات بتغيير الحقيقة لا يعد تزويرا إلا إذا أخرجت في صورة محرر مكتوب، ولكن قد تقع جريمة أخرى

[1] قورة نائلة، مرجع سابق، ص. ص. 602_603.
[2] أحسن بوسقيعة، مرجع سابق، الجزء الثاني، ص. 336.

هي جريمة التقليد لمصنف وفقا لقانون حماية حق المؤلف متى توافرت له الشروط والأوضاع القانونية المطلوبة لذلك.[1]

وهذا ما أدى إلى ظهور اتجاه قوي في دول مختلفة ينادي بالمساواة بين المستند الورقي ومستخرجات الحاسب الآلي من أسطوانات ممغنطة وما يسجل في الحاسب الآلي.[2]

ويكون تغيير الحقيقة في نطاق المعالجة الآلية للمعلومات عن طريق الحذف أو بإزالة كلمة أو رمز معين أو عن طريق الإضافة بزيادة عبارات أو بيانات غير صحيحة، أو بتغيير محتوى الرسائل المنقولة، فمثلا قد يستولي الفاعل على أمر دفع موجه من بنك لآخر ويزيف أو يزور الرسالة، بحيث يتم الدفع لحسابه، أو قد يتم اصطناع بيانات ليس لها وجود من قبل وينسبها كذبا إلى غير مصدرها، أو أن يلجأ الجاني إلى أحد طرق التزوير المعنوي،[3] لتحقيق جريمته بالتدخل بنظام الحاسب الآلي لتسجيل بيانات لم تصدر عن المتعاقدين أو إثبات واقعة كاذبة أو غير معترف بها أو إهمال وإغفال معلومة مما يسبب تحريفا للحقيقة في محررات الحاسب الآلي.[4]

وتفاديا للعقبات التقليدية نادي البعض بتوسيع فكرة المحرر أو المستند ليشمل كل أسلوب لتحديد فكر أو فكرة على ورقة مكتوبة أو من خلال صوت أو صورة مسجلة ولا سيما أن المستند الالكتروني هو المفهوم الحديث للمحرر في جريمة التزوير،[5] وإذا نظرنا إلى المشرع الجزائي الجزائري نجده جرم كل من أدخل

[1] عمرا لفاروق الحسيني، مرجع سابق، ص. 86.
[2] السيد عتيق، مرجع سابق، ص. 123.
[3] وقد حددها المشرع الجزائري بطريقتين، هما:
أ. اصطناع واقعة أو اتفاق خيالي.
ب. انتحال شخصية الغير.
انظر: أحسن بوسقيعة، الجزء الثاني، مرجع سابق، ص. 348.
[4] نهلا عبد القادر المومني، مرجع سابق، ص. 149.
[5] هلالي عبد اللاه احمد، مرجع سابق، ص. 214.

بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أي معلومة أو غيرها بتعديل المعطيات، وهذا ما أقرتـــه إليه المادة 394 مكرر 1 حيث نصت على أنه "يعاقب بالحبس من ستـــة أشهر إلى ثلاثة سنوات وبغرامـــة من 500.000 إلى 4000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".[1]

وعلى ذلك يأخذ السلوك المجرم صورتين:

- إدخال معطيات غريبة في نظام المعالجة الآلية، هذا الإدخال قد يسبب إما جريمة الإتلاف والتخريب التي تكلمنا عنها سابقا وذلك بإدخال برنامج أو فيروس بغرض التخريب، وإما يتسبب في جريمة التزوير المعلوماتي وذلك بإدخال معلومات أو معطيات جديدة في نظام المعالجة الآلية بغرض التزوير.
- أما الصورة الثانية، فهي تخريب أو إفساد المعطيات التي يتضمنها نظام المعالجة الآلية، فالتخريب هنا قد يكون بغرض تعديل المعطيات أو إزالة معطيات من نظام المعالجة وذلك بهدف تغيير الحقيقة في مستند أو محرر إلكتروني.

غير أن هذه المادة تستوعب فقط التزوير أو التحريف الذي يقع على المعطيات الموجودة في نظام المعالجة الآلية، كما يتضمن مستخرجات الحاسب الآلي التي يتوفر فيها شكل محرر، أما المستخرجات الأخرى المتمثلة في الدعامات مثل الشرائط الممغنطة والمسجلة والقرص الصلب وما يحتويه من معلومات لا تدخل ضمن ما جرمه المشرع الجزائري.

[1] القانون رقم 15/04 المؤرخ في10 نوفمبر 2004 المتعلق بالمساس بأنظمة المعالج الآلية للمعطيات.

وفيما يتعلق بالتشريع الفرنسي فقد استحدث المشرع في باب التزوير نصا جديدا في المادة 1/441 من قانون العقوبات، والتي تنص على أنه يعتبر تزويرا كل تغيير تدليسي للحقيقة، يكون من طبيعته أن يسبب ضررا، ويتم بأية وسيلة مهما كانت في محرر أو أي سند للتعبير عن فكرة، والذي يكون له أثر في إنشاء دليل على حق أو فعل تكون له نتائج قانونية، ويعاقب على التزوير واستخدام المحرر المزور بالسجن ثلاث ســـــنوات وغرامة4.500 €.[1] فالمشرع الفرنسي جعل نص هذه المادة يستوعب التزوير العادي في المحررات بجانب تزوير الوثيقة المعلوماتية واستخدامها بالنص على لفظ أي سند أو دعامة وبأي وسيلة، فهذه المادة تشمل كل أشكال التزوير العادية، وأيضا الوسائل الأخرى المستحدثة التي تدخل ضمنها مستخرجات الحساب الآلي، وأيضا المستندات المعلوماتية والدعامات مثل الشرائط الممغنطة والمسجلة،[2] وبهذا فإن طرق التزوير بتغيير الحقيقة لم تعد محددة على سبيل الحصر.

والمشرع بذلك قد قام بالفصل بين تغيير الحقيقة في البيانات المسجلة في ذاكرة النظام الآلي لمعالجة المعطيات وذلك في نص المادة (3/323) قانون العقوبات الفرنسي، وبين تغييرها في محررات النظام الآلي لمعالجة المعلومات في نص المادة (1/441) قانون العقوبات الفرنسي، حيث جعل نصا خاصا للمسألة الأولى بينما احتوى المسالة الثانية في النص العام للتزوير.[3]

[1] احمد طه تمام، مرجع سابق، ص. 403.
[2] المرجع نفسه، ص. 405.
[3] عمر الفاروق الحسيني، مرجع سابق، ص. 88.

المطلب الثاني: موقف التشريعات من جريمة التزوير المعلوماتي

مما لاشك فيه أن جل الدول المتقدمة تساير مختلف التطورات التقنية التي شهدها العالم وما لهذه التقنيات الجديدة من تأثير في الحياة اليومية، فنجد معظم التشريعات الأوروبية والأمريكية قد عالجت مسألة التزوير المعلوماتي، وهذا ما سنوضحه فيما يلي:

- في كندا شمل تعديل قانون العقوبات عام 1985 تعريف المحررات في جريمة التزوير ليشمل أي شيء مادي يمكن أن يتم عليه تسجيل معلومات يمكن قراءتها أو فهمها بواسطة أنظمة الحواسيب أو بواسطة أي جهاز آخر.[1]
- أما قانون العقوبات الألماني لسنة 1986 استحدث المشرع نص المادة (269) من قانون العقوبات الألماني والتي تنص على "كل من باشر بغرض التحايل على الروابط القانونية:

1. التخزين الالكتروني أو المغناطيسي غير المشروع أو بأي وسيلة أخرى غير مرئية أو غير مقروءة مباشرة لبيانات متخصصة لكي تستعمل كوسائل إثبات.
2. أو التعديل غير المشروع لهذه البيانات المختزنة سواء بوسيلة قانونية أو غير قانونية.
3. أو استعمل هذه البيانات المختزنة أو عدلها يعاقب ..."[2]

فنص هذه المادة يجرم التزوير في بيانات ذات أهمية قانونية، فلم يطلب المشرع الألماني الإدراك البصري للمستند، وقرر عقوبة الحبس لمدة لا تزيد عن خمس 05 سنوات والغرامة على كل من يقوم بهدف التحايل على

[1] المادة 321 من قانون العقوبات الكندي لسنة 1985، مشار له عند: فورة نائلة، مرجع سابق، ص. 610.
[2] محمد احمد عبابنة، مرجع سابق، ص. 111.

الروابط القانونية بتخزين أو تغيير بيانات أنتجت مستندا غير أصلي أي مزور.

- أما فيما يتعلق بالتشريع الهولندي والنرويجي والسويدي، فلقد اعتبرت جميعها المحررات الالكترونية مساوية للمحررات في مفهومها التقليدي متى كان من الممكن قراءتها والإطلاع عليها عن طريق الأجهزة الالكترونية اللازمة لذلك.[1]
- وفي استراليا، فإن قانون العقوبات الخاص بالكومنولث الأسترالي جرم هذا السلوك ونص على أنه يعد مرتكبا لجريمة التزوير كل من يقوم بتزوير محرر أو توقيع أو تسجيلات ويشمل لفظ تسجيلات ليسع المعلومات المسجلة الكترونيا، ومنذ عام 1986و بمقتضى التعديل الذي طرأ على قانون العقوبات يعد مرتكبا لجريمة التزوير كل من يقوم بخلق أو استخدام أداة مزورة أو نسخة من هذه الأداة بنية إقناع شخص آخر بقبولها بوصفها أداة حقيقة للقيام أو الامتناع عن العمل، وعرف القانون الاسترالي هذه الأداة بأنها كل محرر رسميا كان أم عرفيا وأدخل في مفهومها البطاقات الائتمانية، والأسطوانة المدمجة أو الأقراص الممغنطة والشريط الصوتي أو أي جهاز آخر سجلت أو حفظت فيه أو عليه أية معلومة بوسائل ميكانيكية أو وسائل أخرى.[2]
- أما في فرنسا فقد كان هناك جانب من الفقه[3] يذهب إلى إمكانية تطبيق نصوص التزوير التقليدية على التزوير المعلوماتي، مستندين في ذلك والى أن الكتابة كانت مطلبا تقليديا في جرائم تزوير المحررات إلا أنه بالإمكان تغليب روح أو فحوى النصوص على الألفاظ واعتبار ما يظهر على شاشة

[1] فورة نائلة، مرجع سابق، ص. 279.
[2] قورة نائلة، المرجع نفسه، ص. 609.
[3] عفيفي كامل، مرجع سابق، ص. 225.

الحاسوب شكل مستحدث للمحرر كما ذهب هذا الاتجاه أيضا إلى أنه بالرغم من أن وجود محرر شرط مفروض في جريمة التزوير، إلا أن القضاء لا يفرق بين محرر منسوخ مشفر وفقا للغة المعلوماتية.[1]

إلا أن المشرع الفرنسي قد حسم الجدل في قانون العقوبات الفرنسي لسنة 1992 والمعمول به منذ عام 1994 وذلك في المادة (3/2/1/323) عقوبات، المتضمن فصلا للمعالجة الآلية للمعلومات، وشملها كذلك بنص المادة (1/441) والتي توسعت في مفهوم المحرر الذي يقع عليه التزوير حيث أصبحت تشمل إلى جانب المحرر بشكله التقليدي كل وسيط وآخر للتعبير عن فكرة ويشمل ذلك بطبيعة الحال الأقراص الممغنطة والأسطوانات المدمجة وغيرها من وسائط تخزين المعلومات، ويشترط القانون أن يكون من الممكن استخدام المحرر أو الوسيط الذي تم تزويره لممارسة حق أو تصرف وأن يكون صالح لإثبات حق أو تصرف له آثار قانونية.

- أما في بريطانيا فقد صدر قانون التزوير والتزييف الخاص بالمحررات عام 1981 والذي تم فيه تعريف السند القابل للتزوير بأنه "كل اسطوانة أو شريط ممغنط أو شريط صوتي أو أي جهاز آخر سجل فيه أو عليه معلومات، أو حفظت بوسائل ميكانيكية أو الكترونية أو بوسائل أخرى"، ثم صدر قانون إساءة استخدام الكمبيوتر عام 1990 الذي صدر استجابة لفشل النيابة في الاتهام أو الحصول على الإدانة في قضايا مختلفة بموجب قانون 1981.[2]
- وفي الولايات المتحدة الأمريكية فتناول القانون الفيدرالي رقم 18 في مادته (1029) المتعلقة بالاحتيال والنشاط المتعلق بالاتصال مع أدوات الوصول إلى الحاسب الآلي، تجريم أفعال التزوير المرتبطة بمعطيات الكومبيوتر وذلك

[1] سامي الشوا، مرجع سابق، ص. 159.
[2] السعيد كامل، مرجع سابق، ص. 332.

في الفقرة (A) من البند الثالث والعقاب عليها بالسجن لمدة لا تزيد عن عشر سنوات أو بالغرامة أو بالعقوبتين معا.[1]

وإجمالا يمكن اعتبار جرائم التزوير الالكتروني هي تلك التي يقصد بها التلاعب بالمعلومات المخزنة في أجهزة الحاسب الآلي أو نظام المعالجة الآلية للمعطيات سواء بتعديل أو إزالة بعض أو كل المعلومات المكونة للنظام، أو تلك المستخرجات التي يتضمنها الحاسب الآلي، وأيضا المستندات المعلوماتية مثل الشرائط المسجلة والممغنطة، وهنا يجب على المشرع الجزائي الجزائري إعطاء تعريف موسع للمحرر ليشمل كل الوسائل المستحدثة تماشيا مع التطور المعلوماتي والذي نتج عنه ولادة سلوكيات إجرامية حديثة.

[1] محمود احمد عبابنة، مرجع سابق، ص. 112.

المبحث الرابع: الوضع القانوني لمكافحة هذا السلوك المستحدث في الجزائر

عرف نظام المعلوماتية تطورا بطيئا في الجزائر بالرغم من الإمكانيات الاقتصادية والمالية والبشرية التي تزخر بها مقارنة بالكثير من دول العالم الثالث، وبالأخص جيرانها من دول المغرب العربي، فالمشكل لم يكن يكمن في مجال نقص العتاد المعلوماتي بقدر ما هو التخطيط العقلاني المساير للواقع إضافة على التأخر في صدور قوانين لتنظيم الشبكة المعلوماتية، عكس شبكة الاتصالات التي وضعت لها قوانين واكبت التطور.

فالجزائر لم تعرف قوانين قبل سنة 2004 تطبق بشكل خاص على نظام المعلوماتية أو على تكنولوجيا الإعلام والاتصال، ما عدا شبكة الاتصال السلكية واللاسلكية ووسائل الإعلام السمعية والبصرية.

والواقع أن هناك العديد من التشريعات والاتفاقيات الدولية التي كانت تطبق في مجال المعلوماتية، منها الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 والمتضمن قانون العقوبات المعدل والمتمم، والأمر رقم 66-155 المؤرخ في 8 يونيو 1966 والمتضمن قانون الإجراءات الجزائية، والأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975 والمتضمن القانون المدني، وكذلك القانون 2000-03 المؤرخ في 5 أوت سنة 2000 الذي يتضمن القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، والأمر رقم 03-05 المؤرخ في 19 يوليو سنة

2003 والمتعلق بحقوق المؤلف والحقوق المجاورة.[1] هذا بالنسبة للتشريعات الوطنية.

أما الاتفاقيات الدولية فهناك جملة من هذه الاتفاقيات التي صادقت الجزائر، وأصبحت تعتبر من النظام القانوني الجزائري، ومن أهمها نذكر: اتفاقية باريس لحماية الملكية الصناعية، والاتفاقية العالمية حول حق المؤلف لسنة 1952 والمراجعة في باريس 24 يوليو 1971 وذلك تحت الأمر رقم 73-26 المؤرخ في 5 يوليو 1973، اتفاقية إنشاء المنظمة العالمية للملكية الفكرية الموقعة بستوكهولم في 14 يوليو 1967، واتفاقية بارن لحماية المصنفات الفكرية والأدبية وذلك تحت المرسوم الرئاسي رقم 97-341 المؤرخ في 13 سبتمبر 1997، ... بالإضافة إلى الانضمام إلى بعض التوصيات والبروتوكولات المتعلقة بتكنولوجيا الإعلام والاتصال.[2] ونشير هنا إلى عدم انضمام الجزائر إلى الاتفاقية الدولية لمحاربة الجرائم الالكترونية ببودابست سنة 2001.

ولمسايرة التطور التكنولوجي كان لابد للجزائر على غرار الدول المتقدمة من إيجاد الإطار القانوني المناسب لحماية المنظومة المعلوماتية من السلوكيات الإجرامية المستحدثة، فصدر القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات وتلاه القانون رقم 09-04 المؤرخ في 5 أوت 2009، وسنتعرض خلال هذا المبحث لكل قانون على حدا.

[1] احمد عمراني، نظام المعلوماتية في القانون الجزائري واقع وأفاق، بحث مقدم إلى المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، المنعقد بالرياض، 2010، ص. 12.
[2] المرجع نفسه، ص. 13.

المطلب الأول: قانون 04-15 المؤرخ في 10 نوفمبر 2004

من أجل سد هذا الفراغ القانوني الذي عرفه هذا المجال جاء هذا القانون الذي نص على حماية جزائية لأنظمة المعلوماتية من خلال تجريم كل أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات، وقد ورد هذا القانون في القسم السابع مكرر من قانون العقوبات تحت عنوان المساس بأنظمة المعالج الآلية للمعطيات وذلك في المواد 394 مكرر إلى 394 مكرر 7.

الفرع الأول: صور الاعتداءات على نظام المعالجة الآلية للمعطيات

تأخذ صور الاعتداء على النظام المعلوماتي في قانون العقوبات الجزائري صورتين أساسيتين وهما:

- الدخول والبقاء في منظومة معلوماتية.
- المساس بمنظومة معلوماتية.

كما تضمن قانون العقوبات صور أخرى للغش في حين أبقي خارج دائرة التجريم بعض الأفعال منها: المساس بحقوق الأشخاص عن طريق المعلوماتية كجمع المعلومات حول شخص وتحويل المعلومات الاسمية عن مقصدها.[1]

- **الدخول أو البقاء في منظومة معلوماتية:** تنص المادة 394 مكرر على معاقبة كل شخص يدخل أو يبقى بواسطة استعمال الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك ... وإذا نتج عن هذا الدخول أو البقاء تخريب في النظام المعلوماتي فإن العقوبة تضاعف. فالصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء، بينما الصورة

[1] أحسن بوسقيعة، مرجع سابق، الجزء الأول، ص. 445.

المشددة تتحقق في الحالة التي ينتج فيها عن هذا الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام.

أ. **فعل الدخول:** لا يقصد بالدخول هنا الدخول بالمعنى المادي، أي الدخول إلى مكان معين كمنزل أو حديقة ... وإنما ينضر إليه كظاهرة معنوية تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكية التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات،[1] وتقع هذه الجريمة من كل إنسان أيا كانت صفته، سواء كان هذا الشخص يعمل في مجال المعلوماتية أو لا يعمل، وسواء كان يستطيع أن يستفيد من هذا الدخول أم لا. فيكفي أن يكون الجاني ممن ليس لهم الحق في الدخول إلى النظام أو من الذين ليس لهم الحق في الدخول بالطريقة التي دخلوا بها. كما تقع الجريمة سواء تم الدخول إلى النظام كله أوالى جزء منه فقط، أي أن الجريمة تقوم بفعل الدخول إلى النظام مجردا عن أي نتيجة أخرى، فلا يشترط لقيامها التقاط أو حصول الشخص على المعلومات الموجودة داخل النظام أو البعض منها، بل إن الجريمة تتوافر حتى ولو لم تكن لدى الجاني القدرة الفنية على تنفيذ العمليات على النظام.

ففعل الدخول يتسع ليشمل كل فنيات الدخول الاحتيالي في منظومة محمية كانت أو غير محمية، كما تشمل استعمال من لا حق له في ذلك المفتاح للدخول إلى المنظومة.[2]

ب. **فعل البقاء:** قد يتخذ السلوك الإجرامي صورة البقاء داخل النظام، ويقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد

[1] قارة أمال، مرجع سابق، ص. 42.
[2] أحسن بوسقيعة، مرجع سابق، الجزء الأول، ص. 445.

إرادة من له الحق في السيطرة على هذا النظام، وقد يتحقق فعل البقاء المعاقب عليه مستقلا عن الدخول عن النظام وقد يجتمعان ويكون البقاء معاقبا عليه استقلالا حين يكون الدخول إلى النظام مشروعا، ومن أمثلة ذلك إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ، وهنا يجب على المتدخل أن يقتطع وجوده داخل النظام وينسحب، فإذا بقى رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع. ويكون البقاء جريمة في الحالة التي يطبع الشخص فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيها الإطلاع فقط، ويتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات الهاتفية، والتي يستطيع الجاني فيها الحصول على الخدمة دون أن يدفع المقابل الواجب دفعه، أو يحصل على مدة أطول من المدة التي دفع مقابلها.[1] ففعل البقاء يشمل البقاء بعد الدخول الشرعي أكثر من الوقت المحدد وذلك بغية عدم الدفع، كما تقوم الجريمة سواء حصل الدخول مباشرة على الحاسوب أو حصل عن بعد، كما يحرم البقاء حتى لو حصل الدخول بصفة عرضية.

- **المساس بمنظومة معلوماتية:** تنص المادة 394 مكرر 1 بمعاقبة كل شخص قام بإدخال معطيات في نظام المعالجة الآلية، أو أزال أو عدل هذه المعطيات وذلك عن طريق استعمال الغش.

هذا السلوك الإجرامي يتجسد في ثلاث صور هي الإدخال، المحو والتعديل. كما أن المشرع لم يشترط اجتماع هذه الصور، بل يكفي أن يصدر عن الجاني إحداها فقط لكي يتوافر الركن المادي، وأفعال الإدخال والإزالة

[1] قارة أمال، مرجع سابق، ص. 44.

والتعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات، سواء بإضافة معطيات جديدة غير صحيحة، أو محو أو تعديل معطيات موجودة من قبل.

كما أن هذا السلوك يجسد فعل التخريب وإفساد المعطيات التي يتضمنها نظام المعالجة الآلية مثال ذلك إدخال فيروس المعلوماتية في البرامج من أجل إتلافها.[1]

- **أعمال أخرى:** جرمت المادة 394 مكرر 2 الأعمال الآتية: تصميم أو بحث أو تجميع أو توفير أو نشر أو الإيجار في معطيات مختزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها إحدى جرائم الغش المعلوماتي سابقة الذكر. كما جرم المشرع كذلك أفعال الحيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصلة من إحدى جرائم الغش المعلوماتي لأي غرض.

الفرع الثاني: الجزاء المقرر

تختلف العقوبات المقررة لجرائم الغش المعلوماتي في قانون العقوبات الجزائري من جريمة إلى أخرى:

- **الدخول أو البقاء في منظومة معلوماتية:** تعاقب المادة 394 مكرر قانون العقوبات على هدا الفعل بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى 200.000 دج وتطبق العقوبات نفسها على المحاولة. كما أن العقوبة تضاعف إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة، وإذا نتج عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة

[1] أحسن بوسقيعة، مرجع سابق، الجزء الأول، ص. 446.

المعلوماتية تكون العقوبة من ستة أشهر إلى سنتين والغرامة المالية من 50.000 دج إلى 300.000 دج.

- **المساس بمنظومة معلوماتية:** تعاقب المادة 394 مكرر 1 على هذا الفعل بالحبس من ستة أشهر إلى ثلاثة سنوات وبغرامة من 50.000 دج إلى 4.000.000 دج.
- **الأعمال أو الفعال الأخرى:** تعاقب المادة 394 مكرر 2 بالحبس من شهرين إلى ثلاثة سنوات وبغرامة من 1.000.000 دج إلى 10.000.000 دج، كل من يقوم عمدا وعن طريق الغش بالفعال المذكورة سابقا (تصميم أو بحث أو تجميع أو نشر أو الإتجار أو الحيازة ...).

الفرع الثالث: القواعد المشتركة بين كل الجرائم

يمكننا القول بأن هذه الجرائم تشترك في مجموعة من القواعد يمكن إجمالها في ما يلي:[1]

- مضاعفة العقوبة (المادة 394 مكرر 3): تتضاعف العقوبات المقررة لجرائم الغش المعلوماتي إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد.
- المشاركة في جمعية أشرار (الماد 394 مكرر 5): كل شخص شارك في مجموعة أو اتفاق يكون من أجل الإعداد لجريمة أو أكثر من جرائم الغش المعلوماتي، وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها.

[1] أحسن بوسقيعة، مرجع سابق، الجزء الأول، ص. 448.

- المصادرة (394 مكرر 6): مع احتفاظ الغير الحسن النية بكامل حقوقه، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من جرائم المعلوماتية، زيادة على إغلاق المحل أو مكان الاستقبال إذا ارتكبت الجريمة بعلم صاحبها.
- جرائم الشخص المعنوي (المادة 394 مكرر 4): يعاقب الشخص المعنوي الذي يرتكب إحدى جرائم الغش المعلوماتي بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.
- الشروع (المادة 394 مكرر 7): يعاقب على الشروع في ارتكاب جنح الغش المعلوماتي بالعقوبات المقررة للجنحة ذاتها في حالة ارتكابها.

المطلب الثاني: القانون 09-04 المؤرخ في 5 أوت 2009

جاء هذا القانون بمجموعة من القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، آخذا بعين الاعتبار الصعوبات التي تثيرها المصطلحات القانونية المتعلقة بهذه المادة، لذلك جاء عنوانه القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها حتى لا يكون النص مرتبطا بتقنيات تشهد تطورا مستمرا بقدر ما يرتبط بالأهداف والغايات التي ترمي إليها هذه التكنولوجيا، كما أن التركيز على مجالي الإعلام والاتصال يوضح مقاصد النص الذي يهدف إلى جعل المتعاملين في مجال الاتصالات السلكية واللاسلكية شركاء في مكافحة هذا الشكل من الإجرام والوقاية منه. وكان لزاما سد الفراغ القانوني الذي عرفه هذا المجال بصدور القانون رقم 04-15 الذي نص على حماية جزائية للأنظمة المعلوماتية من خلال تجريم كل أنواع الاعتداءات التي تستهدف المعالجة الآلية للمعطيات، ويأتي هذا القانون بتعزيز نفس هذه القواعد من خلال

وضع إطار قانوني أكثر ملائمة. كما تكمن أهمية هذا القانون في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها.

كما أخذ المشرع الجزائري بعين الاعتبار الصعوبات التي تثيرها المصطلحات القانونية المتعلقة بهذه المادة، حيث جاء هذا القانون مقسما على ستة فصول:

- نص الفصل الأول على الأحكام العامة التي تبين الأهداف المتوخاة من القانون، وتحدد مفهوم مصطلح التقنية الواردة فيه، وكذا مجال تطبيق أحكامه. حيث عرف الجرائم المرتكبة بتكنولوجيا الإعلام والاتصال، على أنها هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الالكترونية. كما عرف المنظومة المعلوماتية على أنها أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المترابطة، ويقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين، أما المعطيات المعلوماتية فعرفها المشرع الجزائري على أنها أي عملية عرض وطرح للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شانها جعل المنظومة المعلوماتية تؤدي وظيفتها، وعرف الاتصالات الالكترونية والتي تكون في غالب الأحيان هي المعرضة الأولى للقرصنة

على أنها أي تراسل أو إرسال أو استقبال علامات أو أشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية.[1]

- أما الفصل الثاني فقد جاء بأحكام خاصة بمراقبة الاتصالات الالكترونية، وقد روعي في وضع هذه القواعد خطورة التهديدات المحتملة وأهمية المصالح المحمية، هذا كله لحماية النظام العام أو لمستلزمات التحريات والتحقيقات القضائية الجارية، وسنوضح فيما يلي الحالات التي يسمح فيها باللجوء إلى المراقبة الالكترونية:[2]

أ. للوقاية من السلوكيات الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ب.في حالة توافر معلومات على احتمال القيام باعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الاقتصاد الوطني.

ج. لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

د. في مجال تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

وقيد المشرع إجراء هذه العمليات من المراقبة إلا بإذن مكتوب من السلطات القضائية المختصة، ويكون الاختصاص في الحالة الأولى للنائب العام لدى مجلس قضاء الجزائر.

- أما الفصل الثالث فتضمن القواعد الإجرائية، وهذا بالنص على قواعد إجرائية خاصة بالتفتيش والحجز في مجال الجرائم المتصلة بتكنولوجيا الإعلام

[1] المادة 2 من القانون 09-04 المؤرخ في 5 أوت 2009.
[2] المادة 4 من القانون 09-04 المؤرخ قي 5 أوت 2009.

والاتصال، وذلك وفقا للمعايير العالمية المعمول بها في هذا الشأن ومع مراعاة ما تضمنه قانون الإجراءات الجزائية من مبادئ عامة.

- وتطرق الفصل الرابع إلى الالتزامات المتعلقة بالمتعاملين في مجال الاتصالات الإلكترونية، ولا سيما إلزامية حفظ المعطيات المتعلقة بحركة السير والتي من شأنها المساعدة في الكشف عن الجرائم ومرتكبيها، وهذا بهدف إعطاء مقدمي الخدمات دورا إيجابيا في مساعدة السلطات العمومية في مواجهة الجرائم وكشف مرتكبيها.[1]
- أما الفصل الخامس، والذي جاء بإجراء مهم لمحاربة الإجرام المعلوماتي، من خلال الإشارة إلى الهيئة الوطنية للوقاية من الإجرام المتصل بتكنولوجيا الإعلام والاتصال ومكافحته، إذ نص على إنشاء هيئة وطنية تنسيقية في مجال الوقاية من هذا النوع من الجرائم، وقد تمت الإحالة على التنظيم تحديد كيفيات سير هذه الهيئة.

وحددت مهام هذه الهيئة فيما يلي:[2]

أ. تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

ب.مساعدة السلطات المختصة في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

[1] المواد 10، 11 و12 من القانون 09-04 المؤرخ في 5 أوت 2009.
[2] المادة 14 من القانون 09-04 المؤرخ في 2009.

ج. تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي هذا النوع من السلوك الإجرامي وتحديد مكان تواجدهم.

- أما الفصل السادس والأخير، فنص على التعاون والمساعدة القضائية الدولية، إذ تناول قواعد الاختصاص القضائي والتعاون الدولي بوجه عام.

ففيما يخص الاختصاص القضائي وفضلا عن قواعد الاختصاص العادية، فقد تم توسيع اختصاص المحاكم الجزائرية للنظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال التي ترتكب من طرف الرعايا الأجانب عندما تكون المصالح الإستراتيجية للجزائر مستهدفة.

وفيما يتعلق بالتعاون الدولي فهو يقوم على مجموعة من المبادئ العامة في مجال التعاون الدولي لمكافحة هذا النوع من الجرائم خاصة ما يتعلق منها بالمساعدة وتبادل المعلومات، حيث تم اعتماد مبدأ التعاون على أساس المعاملة بالمثل.

من خلال استعراضنا للقانونين 04-15 و04-09 نجد بأن المشرع الجزائري عالج أو تطرق لمختلف الأخطار التي قد تصيب النظام المعلوماتي، مع إغفال بعض السلوكيات المتبعة من طرف المجرم المعلوماتي والتي لم يعالجها كذلك في القانون 09-04 والذي جاء في مجمله كمحاولة للوقاية من هذا النوع من الجرائم، ومكافحتها.

الخلاصة

حاولت في هذا الفصل إبراز أهم السلوكيات المعتمدة من طرف المجرم المعلوماتي لارتكاب جرائمه التي يكون فيها النظام المعلوماتي محلا للاعتداء، وتناولت تحديدا الجرائم التي تقع على الشق المعنوي لهذا النظام، حيث تترقت إلى جريمة سرقة المال المعلوماتي المعنوي، وحاولت هنا في الخصوص الإجابة فيما إذا كانت تعتبر المعلومات المعنوية والمختزنة في قواعد البيانات أو المتبادلة على شبكة الإنترنت قابلة للسرقة أم لا، وخلصت إلى اعتبار أن المعلومات يمكن أن تترجم إلى قيم مالية نظرا لقابليتها للاستغلال، وبالتالي فإن الاستحواذ عليها بالطرق غير المشروعة يشكل اعتداء على حقوق الاستغلال المالي، ثم عرجت إلى إتلاف المعلومات أو جريمة إتلاف المال المعلوماتي والتي أبرزت فيها أنها تتخذ عدة صور وأساليب لارتكابها من إعاقة سير العمل ومن إتلاف البرامج سواء بتعديلها أو اصطناع برامج جديدة أو باستعمال فيروسات الحاسب الآلي، والملاحظ أن مختلف التشريعات قد حاولت محاربة هذا السلوك من خلال مجموعة من القوانين التي نصت على تجريم هذا الفعل.

وحرصت على التطرق إلى جريمة التزوير المعلوماتي وحاولت الوصول إلى مدى تطابق أركان جريمة التزوير التقليدية على التزوير المعلوماتي، واتضح أن الإشكال القائم يكمن في شكل المحرر والذي يشترط فيه مجموعة من الميزات أو الصفات، غير أن الكثير من التشريعات عالجت هذا الإشكال بإعطاء تعريف موسع لشكل المحرر وهذا ما لم يقيم به المشرع الجزائري، غير أنه عاقب على الأشكال الأخرى من التزوير التي تطال المعطيات المعالجة في النظام المعلوماتية.

وأخيرا حاولت إيضاح الوضع القانوني في الجزائر لمحاربة أو مكافحة هذا النوع المستحدث من الجرائم سواء بالتطرق إلى القانون 04-15 أو القانون 09-04 وهذا في محاولة للمشرع الجزائي في تغطية مختلف الجرائم المرتكبة بواسطة المعلوماتية.

خاتمة

لقد بات من المحتم على شعوب العالم الانصـــهار التـــدريجي فـــي بوتقـــة المعلوماتية، كنتيجة حتمية لمواكبة التطور التقني والتكنولوجي فـــي ظـــل التحـــول الإلكتروني لمختلف نواحي الحياة لتحقيق المجتمع الافتراضي، في ظل عالم مفتوح تتسيده المعلومات، والتي أضحت وبحق مصدر القوة والمعرفة، وأضحت المعيـــار المحدد لتطور ونمو الشعوب ومستقبلها، وذلـــك بزيادتهـــا للفـــوارق الاقتصـــادية والاجتماعية القائمة بين مجتمع وآخر.

ونتيجة للتطور العلمي الهائل، فإن المحاسن التي جلبتها المعلوماتية قد جلبت إلى جانبها أيضا مخاطر عدة ناجمة عن إساءة استخدام شبكة الإنترنت وتطويعهـــا لصالح المجرم المعلوماتي لممارسة نشاطاته الجرمية، ولهذا يرى البعض أن ارتفاع مستوى التعليم يؤدي إلى رفع مستوى الأداء الإجرامي للمجرمين المحتـــرفين، أي مستوى الإتقان والاحتراف، استعانة بالمعارف والعلوم والتقنيات المعرفية العلميـــة، ومن ثم تؤدي إلى ارتكاب أفعال إجرامية أكثر دقة، في التخطيط، وأكثر براعة فـــي التنفيذ وهذا من شأنه أن يصعب إمكانية اكتشافها، فالتقنية الحديثة ســـهلت ظهـــور طائفة جديدة من الجرائم المستحدثة، والتي تعجز النصوص العقابية التقليدية علـــى مواجهة أغلب صورها، وإن وجدت نصوص عقابية حديثـــة فـــلا بـــد أن تكملهـــا استراتيجيات مختلفة على المستوى الفني والتقني والقضائي، وذلك لمراقبة الأمن في مجال تقنية المعلومات أو في مجال التدريب، أو في مجال التعاون والتنسيق الدولي لمواجهة هذا النوع المعقد من السلوك الإجرامي.

ومن خلال هذا البحث توصلنا إلى جملة من نتائج والاقتراحات سنوردها فيما يلي:

- **أولا. النتائج:**

فنظرا لحداثة هذا السلوك الإجرامي والذي يتجسد في الجريمة المعلوماتية، فإنه لا يوجد لحد الآن إجماع فقهي على تعريف موحد لها مما أدى إلى القول بـــأن الجريمة المعلوماتية تقاوم التعريف، ومن خلال استعراضنا للتعريفات الفقهية والتي جاءت متفاوتة فيما بينها ضيقا واتساعا توصلنا إلى أن الإخفاق في تعريف الجريمة المعلوماتية يفسره اتجاه يسمح بسهولة إضفاء وصف الجريمة المعلوماتية علـــى أي واقعة لها علاقة بالحاسوب أيا كانت هذه العلاقة وأيا كان دور الحاسوب فيها، سواء كان وسيلة أو مناسبة لارتكاب الجريمة، أو كان موضوعا لها، وعليه فإننا نقتـــرح التعريف التالي: تعد جريمة معلوماتية كل جريمة يمكن ارتكابها بواســـطة شـــبكة حاسوبية أو داخل نظام معلوماتي، وتشمل تلك الجريمة جميع الجرائم التـــي يمكـــن ارتكابها سواء على تكنولوجيا المعلومات أو المرتكبة بواسطة المعلوماتية.

وعليه فالركن الشرعي للجريمة المعلوماتية يستهدف تجـــريم كـــل أشـــكال الاعتداء على النظام المعلوماتي وحماية النظام يعني حمايـــة المعلومـــة، وبالنســـبة للركن المادي للجريمة المعلوماتية فهو يشمل صورتين:

- الاعتداء على نظام المعالجة الآلية للمعطيات
- الاعتداء على منتجات النظام (التزوير المعلوماتي) فالبنسبة للركن المعنـــوي للجريمة المعلوماتية فيختلف باختلاف أشكالها، وعليه فإن الـــدخول والبقـــاء بالغش والاعتداء على المعطيات الموجودة داخل النظام تستلزمان قصد جنائيا وقصدا خاصا متمثلا في نية الغش، أما التزوير المعلوماتي فيخضع لأحكـــام الركن المعنوي لجريمة التزوير في المحررات، والمتمثل في القصد الجنائي العام والمتجسد في العلم وإرادة تغيير الحقيقة في مستند معلوماتي، وما يميز الركن المعنوي للجريمة المعلوماتية عموما هو صعوبة إثباته.

- ومن النتائج المستخلصة والتي أثارت الكثير من الجدل في مختلف الاتجاهات القانونية، مسألة تحديد قائمة بجرائم الكمبيوتر والانترنت والتـــي يتعـــين أن تكون محلا للجريمة، وتحديد أنماط السلوك الإجرامي والأفعال المكونة لـــه، وتوضيح القوام القانوني لهذه الجرائم.
- إن جرائم الكمبيوتر تستهدف المعطيات ذات الطبيعة المعنوية فعندما يكـــون جهاز الحاسوب هدفا للجريمة فإن السلوك يستهدف المعلومات المخزنة فيه أو المنقولة منه أو إليه، وعند ما يكون وسيلة لارتكاب الفعـــل، فـــإن الســـلوك يستهدف بيانات تمثل قيما مالية، ويجري الفعل أو السلوك باســـتخدام طـــرق تقنية في بيئة معنوية وليست في بيئة سلوكيات مادية.
- أن مبدأ الشرعية الجنائية يمنع المساءلة الجنائية ما لم يتوفر النص القـــانوني فلا جريمة ولا عقوبة إلا بنص، ومتى ما انتفى النص على تجريم مثل هـــذه الأفعال التي لا تطالها النصوص القائمة امتنعت المسؤولية وتحقق القصـــور في مكافحة هذه الجرائم.
- أن القياس في النصوص الجنائية الموضوعية محضور وغير جائزا، ومؤدى ذلك امتناع قياس أنماط جرائم المعلوماتية على الجرائم التقليدية التي تستهدف الأموال، كقياس جريمة سرقة المعلومات أو وقت الحاسب الآلي على جريمة الاستيلاء على الكهرباء بطريقة غير مشروعة.
- ومن الدراسة لاحظنا أن شبكة الانترنت كأداة لارتكاب الجريمة إما أن تكون أداة إيجابية أو أداة سلبية للمجرم المعلوماتي، أي أن تكون وسيلة لارتكـــاب الجريمة، أو محلا لها، فهي في الصورة الأولى تسهل للمجـــرم المعلومـــاتي ارتكاب جرائم أخرى معاقب عليها، وهي تشكل أغلب جرائم الاعتداء علـــى الأشخاص كجرائم الاعتداء على حق الإنسان في حرمـــة حياتـــه الخاصـــة،

وجريمة الاعتداء على شرفه وسمعته، وتتحقق الصورة الثانية كأداة سلبية فيها لو كانت هي هدف الجاني وغايته وذلك بالحصول على البيانات والمعلومات المنقولة عبرها والاستفادة منها بصورة غير شرعية، أو الاعتداء على هذه المعلومات والبرامج بإتلافها أو تزويرها.

- تتسم الجريمة المعلوماتية بطابع التعقيد والغموض إذا يصعب وضع قواعد قانونية منضبطة تحكم جميع السلوكيات، لأن هاته السلوكيات تتطور بتطور التقنية.
- هناك بعض السلوكيات الإجرامية المستحدثة يصعب تحديد الركن المادي لها، ويصعب تكييفها، كطبيعة المال المعلوماتي وملكيته حيث أن المشرع الجزائري من خلال النصوص العقابية يحمي الأموال المادية الملموسة دون الأموال المعنوية في جريمة السرقة، وهي أولى من الرعاية في الكثير من الأحيان، وكذلك الحال فيما يتعلق بطبيعة الاعتداء على حرمة الحياة الخاصة وعدم الاعتداء على البيانات الاسمية للأشخاص.
- أن الأفعال الإجرامية التي تجسد السلوك الإجرامي للمجرم المعلوماتي تتطور وتأخذ أساليب جديدة بتطور نمط السلوك الإجرامي والذي يعتمد بدوره على التطور التكنولوجي.
- أثارت شبكة الإنترنت أعقد المشاكل في مسألة الاختصاص القضائي والقانون الواجب التطبيق على الممارسات الإجرامية في نطاق الشبكة، مما يثير مسألة تطبيق النصوص الجزائية من حيث الزمان أو النصوص الجزائية من حيث المكان، ومدى صلاحيتها للتطبيق على هذه الممارسات، ولاسيما أنها قد تكون خاضعة للعقاب في دول ومباحة في دول آخري.

- وفي الأخير لا يسعنا إلا التنويه بالسياسة التشريعية التي تسير عليها الجزائر في إطار مكافحة الجريمة المعلوماتية حيث أورد المشرع قـانون المسـاس بأنظمة المعالج الآلية للمعطيات رقم 04-15 في 10 نـوفمبر 2004، كمـا أصدر القانون رقم 09-04 في 5 أوت 2009 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها، لـذلك نستخلص أن موقف المشرع الجزائري اتسم بالإيجابية فـي محاربـة هـذا السلوك الإجرامي، ولكن هذا لا ينفي وجود بعض النقائص.

- **ثانيا. الاقتراحات:**

في ضوء النتائج السابقة التي أظهرتها الدراسة خلصت إلى بعض التوصيات وتتمثل في:

1. ضرورة تخلي المشرع الجزائي الجزائري على حرفيـة الـنص الجنـائي التقليدي وتبنيه مفهوما أشمل للمال والمنقول، بحيث تشمل الأموال المعلوماتية المعنوية، وذلك بإصدار نصوص قانونية خاصة تشمل الطائفة الأخيرة مـن الأموال غير المحمية بالخصوص من جريمة سرقة المعلومات، أو الاستخدام غير المستحق للشبكة العالمية أو لجهاز الحاسب الآلي.
2. ضرورة إعطاء تعريف موسع للجريمة المعلوماتية، وإعطاء لكـل سـلوك إجرامي نص مجرم له، وذلك بالتحديد الواضح والدقيق لصور السلوك المراد تجريمها.
3. وجوب إعطاء المحرر تعريف موسع في قانون العقوبات الجزائري ليشـمل كافة الأشكال كالأقراص المرنة والمدمجة.
4. خلق ثقافة اجتماعية جديدة تصور جرائم الانترنت على أنهـا أعمـال غيـر مشروعة مثلها مثل أنماط الجرائم الأخـرى، والتأكيـد علـى أن المجـرم

المعلوماتي يستهدف الإضرار بالآخرين، ويستحق العقوبة بدل نظرات وعبارات الإعجاب.

5. ضرورة تدريب وتأهيل أفراد الضبطية القضائية من العاملين من الإدعاء العام (النيابة) والقضاء على كيفية التعامل مع هذا النوع من الإجرام وتحقيق التعاون مع التقنيين من أصحاب الخبرة، وذلك بعقد دورات تدريبية بشكل دوري ودائم للاستفادة من خبراتهم وإرشاداتهم، ابتداء من مرحلة الاستدلال وجمع الأدلة، وانتهاء بقرارات المحاكم.
6. تدريس مواد الأنظمة المعلوماتية والجرائم التي قد تنشأ منها في كليات الحقوق والمعاهد القضائية.
7. النص بشكل واضح وصريح على مسؤولية الشخص المعنوي على جرائم الحاسب الآلي وإفراد العقوبات المناسبة لها.
8. تبني فلسفة تدريبية تكفل لجهاز الشرطة زيادة معدل معرفة أفراده بتقنيات الحاسبات والمعلومات وطرق وكيفية إساءة استخدامها في ارتكاب الجرائم بما يكفل حسن تطبيق القانون في المجال المعلوماتي.
9. تفعيل دور الأسرة في متابعة الأبناء لوقايتهم من الآثار السلبية والمخاطر المترتبة عن الاستخدام غير الآمن لشبكات الإنترنت.
10. التطوير المستمر للتشريعات القائمة بما يحقق مرونتها ومواكبتها للتطورات المتسارعة في مجال تكنولوجيا المعلومات.
11. محاولة الاستفادة من الإمكانيات التي يمتلكها المجرم المعلوماتي وتوظيفها في خدمة المجتمع وفقا للقانون رقم 01/09 المتعلق بالعمل للنفع العام.

12. إعطاء صلاحيات واسعة للهيئة الوطنية للوقاية من الإجرام المتصـــل بتكنولوجيا الإعلام والاتصال ومكافحته.

13. ضرورة التعاون الدولي لمواجهة الجـــرائم فـــي البيئـــة المعلوماتيـــة الإلكترونية وذلك من خلال الدخول في الاتفاقيات ومعاهدات تجرم صور هذه الجرائم كلها وتبين كذلك الاختصاص المكاني في حال وقوعها وكيفية تسليم مجرمي المعلوماتية وغير ذلك من الأمور، كما يمكن أن تنص هذه الاتفاقيات على تبال الخبرات والمعلومات في المسائل المتعلقة بـــالجرائم المعلوماتيـــة، وهذا ما يجب أن يحدث بالنسبة للجزائـــر وضـــرورة انضـــمامها لاتفاقيـــة بودابست 2001 لمكافحة الجريمة المعلوماتية.

ونود أن نؤكد في نهاية بحثنا، على أن تنظيم استخدام شبكة الإنترنت وتلاشي مخاطرها لا يكون إلا بتحقيق التنظيم الذاتي لسلوك المستخدم، وهذا راجع إلـــى أن هذا السلوك هو المؤطر والمحدد لأبعاد هذه الظاهرة الإجرامية.

الملاحق

الملخص

تتناول هذه الدراسة الجريمة المعلوماتية التي يتجسد فيها السلوك الإجرامي للمجرم المعلوماتي، وكيفية معالجة المشرع الجزائري لهذا النوع الخطير والمستجد من السلوك الإجرامي.

وتهدف هذه الدراسة إلى التعرف على الجريمة المعلوماتية من حيث ماهيتها وخصائصها وأهمية الحماية الجنائية للمعلومات من السلوكيات الإجرامية التي قد تقع عليها، كما كان محور هذه الدراسة تسليط الضوء على مرتكب هذه الجريمة الذي اصطلح على تسميته بالمجرم المعلوماتي، وذلك بمعرفة سماته وفئاته ودوافعه لارتكاب الجريمة المعلوماتية، حيث أن دراسة شخصية المجرم تعتبر خطوة هامة في وضع التشريعات العقابية التي تكفل إصلاحه وردعه في آن واحد.

كما عمدت هذه الدراسة إلى إيضاح السلوكيات المتبعة من طرف المجرم المعلوماتي والتي ارتكبت سواء بواسطة المعلوماتية أو التي ارتكبت على تكنولوجيا المعلومات والتي أثبتت النصوص التقليدية فشلها في محاربة هذه السلوكيات حيث أن المبدأ الأساسي الذي يحكم القانون الجنائي هو مبدأ شريعة الجرائم والعقوبات، حيث لا جريمة ولا عقوبة إلا بنص وعدم جواز التوسع في تفسير النصوص الجنائية.

كما تعرضت هذه الدراسة لموقف المشرع الجزائري في مجال مكافحة الجريمة المعلوماتية، وكيفية معالجته لها ضمن القانون الجنائي الوطني وذلــك من خلال القانــون 04-15 من قانون العقوبات والمتعلق بالمساس بأنظمة المعالج الآلية للمعطيات والقانــون 09-04 والمتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، حيث أفرد المشرع بعض الإجراءات والوسائل لمحاربة هذا السلوك المستحدث. وقد توصلت الدراسة إلى عدد من التوصيات منها:

ضرورة تدخل المشرع الجزائي لتعديل بعض النصوص تراعى فيها طبيعة المعلومات وخصوصيتها واستحداث نصوص تكفل الحماية الجزائية للمعلومات باعتبارها من الأموال، كما خلصت الدراسة إلى ضرورة تأهيل جهازي الشرطة والقضاء ليكونا قادرين على التعامل مع هذا النوع المستحدث من السلوكيات الإجرامية.

Cette étude se penche sur le crime informationnel où le comportement criminel des individus est mis en valeur ainsi que le traitement que réserve la législation Algérienne à ce nouveau et dangereux genre de crime.

Cette étude à pour but l'identification du crime informationnel: définition, caractéristiques et importance de la protection pénale de l'information; comme elle s'est articulée principalement sur l'auteur de ce crime appelé communément le criminel informationnel et cela en faisant apparaitre ses penchants, les groupes auxquels il appartint et les mobiles qui le poussent à commettre de tels crimes, sachant que la connaissance de la personnalité constitue un premier pas quant à l'instauration des textes répressifs et ceux qui préparent son insertion dans la société.

Nous avons aussi nuancé le fait d'utiliser le système informationnel comme moyen pour commettre des crimes et le fait de commettre des crimes au préjudice du système informationnel. La nous soulignerons que les textes antérieurs ont prouvés leur échec relativement à la lutte contre ces agissement.

Cette thèse n'a pas ignoré les solutions apportées par la législation Algérienne à ce genre de crime et cela par le biais de la loi 04/ 15 du code pénal et la loi 09/ 04 où le législateur s'est distingué par l'apport de quelque procédures et moyens de lutte contre ce nouveau fléau.

En fin, notre étude nous a menés a proposés plusieurs recommandation; dont: l'obligation de l'intervention de la législation pénale pour amender et créer de nouveaux textes sensés garantir la protection pénale de l'information considérée comme un bien; la réhabilitation et la mise en adéquation des institutions policière et judiciaire afin qu'elles puissent faire face à ce nouveau comportement criminel.

قائمة المراجع

أولا: المراجع باللغة العربية

أ. الكتب العامة:

1. أحمد بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، دار هومة، الطبعة العاشرة ،2009.
2. أحمد بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الثاني، دار هومة، الطبعة العاشرة، 2009.
3. أحمد بوسقيعة، قانون العقوبات في ضوء الممارسة القضائية، منشورات بيرتي، 2010.
4. رمسيس بنهام، النظرية العامة للقانون الجنائي، دار المعارف، الإسكندرية، الطبعة الثالثة، 1997.
5. سليمان عبد المنعم، النظرية العامة لقانون العقوبات، دار الجامعة الجديدة، الإسكندرية، 2000.

ب. الكتب المتخصصة:

1. أحمد حسام طه، الجرائم الناشئة عن استخدام الحاسب الآلي، الحماية الجنائية للحاسب الآلي، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، 2000.
2. أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة، الطبعة الثانية، دار النهضة العربية، القاهرة، 2008.
3. أحمد هلالي عبد اللاه، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2003.

4. أسامة احمد المناعسة، جلال محمد الزعبي، جرائم الحاسب الآلي والانترنيت، دار وائل للنشر، عمان، 2001.
5. السعيد الكامل، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، دار النهضة العربية، القاهرة، 1993.
6. أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية، 2008.
7. إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان، دار الجامعة الجديدة، الإسكندرية، 2007.
8. جميل عبد الباقي الصغير، الانترنيت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالانترنيت، دار النهضة العربية، القاهرة، 2001.
9. جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، دراسة تطبيقية في القضاء الفرنسي والمصري، الطبعة الأولى، دار النهضة العربية، القاهرة، 1999.
10. جون كيريلك، موسوعة الهاكرز، ترجمة خالد العمري، دار الفاروق، الطبعة الثانية، 2003.
11. حاتم عبد الرحمان منصور الشحات، الإجرام المعلوماتي، دار النهضة العربية، القاهرة، الطبعة الأولى، 2003.

12. حجازي عبد الفتاح بيومي، الجريمة في عصر العولمة، دراسة في الظاهرة الإجرامية المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2008.

13. حجازي عبد الفتاح بيومي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2002.

14. حجازي عبد الفتاح بيومي، النظام القانوني لحماية التجارة الالكترونية، دار الفكر الجامعي، الإسكندرية، 2002.

15. حجازي عبد الفتاح بيومي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2006.

16. حسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة، الحق في الخصوصية، دراسة مقارنة، دار النهضة العربية، القاهرة.

17. خالد بن سليمان الخثبر، محمد بن عبد الله القحطاني، أمن المعلومات، مكتبة الملك فهد الوطنية للنشر، الرياض، 2009.

18. خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، الدار الجامعية، الإسكندرية، 2008.

19. رستم هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، الطبعة الثانية، 1998.

20. رضا محمد عثمان دسوقي، الموازنة بين حرية الصحافة وحرمة الحياة الخاصة (دراسة المقارنة)، دار النهضة، القاهرة، 2009.

21. سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، الطبعة الأولى، 1994.

22. سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، دار النهضة العربية، القاهرة، الطبعة الأولى، 1999.

23. عبد الله حسن علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الأولى، دار النهضة العربية، القاهرة، 2001.

24. عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنيت، الجرائم الالكترونية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2007.

25. عتيق السيد، جرائم الانترنت، دار النهضة العربية، القاهرة، الطبعة الأولى، 2000.

26. عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، الطبعة الأولى، بدون ناشر، 2000.

27. علاء الدين منصور المغايرة، الأوجه الحديثة للجرائم المعلوماتية، دار الحلبي الحقوقية، بيروت، 2002.

28. علي جبار الحسيناوي، جرائم الحاسوب والانترنت، دار اليازوري، عمان، 2009.

29. عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا، دراسة مقارنة، دار النهضة العربية، القاهرة، 2010.

30. عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، دار النهضة العربية، القاهرة، الطبعة الثانية، 1995.

31. عمرو أحمد حسبو، حماية الحريات في مواجهة نظم المعلومات، دار النهضة العربية، القاهرة، الطبعة الأولى، 2000.

32. فاروق محمد الأباصري، عقد الاشتراك في قواعد المعلومات عبر شبكة الانترنت، دار الجامعة للنشر، بيروت، الطبعة الأولى، 2002.

33. فايز نعيم رضوان، بطاقات الوفاء، دار النهضة العربية، القاهرة، 1999.

34. قورة نائلة، جرائم الحاسب الاقتصادية، دار النهضة العربية، القاهرة، 2004.

35. محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت، دار الثقافة للنشر، عمان، الطبعة الأولى، 2004.

36. محمد أمين الرومي، جرائم الكمبيوتر والانترنت، دار النهضة العربية، القاهرة، الطبعة الأولى، 2003.

37. محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري، دار الجامعة الجديدة، الإسكندرية، 2007.

38. محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائية، دار الثقافة للنشر، عمان، الطبعة الأولى، 2004.

39. محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004.

40. محمد فتحي عيد، الإجرام المعاصر، أكاديمية نايف الأمنية، الرياض، الطبعة الأولى، 1999.

41. محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2001.

42. محمود أحمد عبابنة، محمد معمر الرازقي، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر، عمان، 2005.

43. مدحت رمضان، الحماية الجنائية للتجارة الالكترونية، دراسة مقارنة، دار النهضة العربية، القاهرة، الطبعة الأولى، 2001.

44. مدحت رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة، 2000.

45. منصور رحماني، علم الإجرام والسياسة الجنائية، دار العلوم، عنابة، 2006.

46. نبيل محمد توفيق السمالوطي، الدراسة العلمية للسلوك الإجرامي، دار الشروق، جدة، 1983.

47. نعيم مغبغب، مخاطر المعلوماتية والانترنت المخاطر على الحياة الخاصة وحمايتها، دراسة مقارنة، بدون ناشر، 1998.

48. نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر، عمان، 2008.

49. هدى حامد قشوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، الطبعة الأولى، 1992.

50. وليد الزيدي، القرصنة على الانترنت والحاسوب، دار أسامة للنشر، عمان، الطبعة الأولى، 2003.

51. يونس عرب، دليل أمن المعلومات والخصوصية، الجزء الأول، جرائم الكمبيوتر والانترنت، اتحاد المصارف العربية، بيروت، الطبعة الأولى، 2002.

ج. القوانين:

1. القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 المعدل لقانون العقوبات.

2. القانون رقم 09-04 المؤرخ في 05 غشت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها.

3. القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتعلق بالمساس بأنظمة المعالج الآلية للمعطيات.

4. القانون الجزائي العربي رقم 229-1996 الجزء الثاني، الإدارة العامة للشؤون القانونية، الأمانة العامة لمجلس وزراء العدل العرب، جامعة الدول العربية.

د. الأحكام:

1. مجلس قضاء باتنة، الغرفة الجزائية قرار رقم 10/05805 المؤرخ في 2010/07/04، غير منشور.

و. الأبحاث العلمية:

1. أحمد عمراني، نظام المعلوماتية في القانون الجزائري، واقع وأفاق، بحث مقدم إلى المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، المنعقدة بالرياض، 2010.
2. السعدي واثبة، الحماية الجنائية لمعلومات وبرامج الحاسوب، بحث مقدم إلى مؤتمر القانون والحاسوب، جامعة اليرموك، الأردن، 2004.
3. خليل قندح، الجرائم المرتكبة بواسطة المعلوماتية، بحث مقدم إلى مؤتمر القانون والحاسوب، جامعة اليرموك، الأردن، 2004.
4. سامي الشوا، الغش المعلوماتي ظاهرة إجرامية مستحدثة، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، القاهرة، 1993.
5. عطية سالم عطية، الصور المستحدثة لجرائم بطاقات الدفع الالكتروني ورقة عمل، القاهرة، 1998.
6. عوض محمد محي الدين، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، القاهرة، 1993.

7. عيسى طوني، الجرائم المعلوماتية، بحث مقدم إلى جمعية إتمام المعلوماتية القانونية، لبنان، بيروت، 1998.
8. فؤاد جمال، الجرائم المعلوماتية، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، المنعقد بكلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2000.
9. كمال احمد الكركي، النواحي الفنية لإساءة استخدام الكمبيوتر، ورقة عمل مقدمة إلى ندوة الجرائم الناجمة عن التطور التقني المنعقدة بعمان، دار الثقافة، 1998.
10. محمد السعيد رشدي، الانترنت والجوانب القانونية لنظم المعلومات، بحث مقدم إلى مؤتمر الإعلام والقانون، كلية الحقوق، جامعة حلوان، 9 إلى10 مارس 1999.
11. هدى حامد قشقوش، الصور الإجرامية لحالات السحب الالكتروني من الرصيد، بحث مقدم إلى ندوة الصور المستحدثة لجرائم بطاقات الدفع الالكتروني، 1998.
12. يونس عرب، تطور التشريعات في مجال مكافحة الجرائم الالكترونية ورقة عمل رقم 2-3، مقدمة لهيئة تنظيم الاتصالات، مسقط، عمـــان، مـــن 2 إلى 4 أفريل 2006.
13. URICH SEIBER جرائم الكمبيوتر والجرائم الأخرى في مجال المعلومات، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية

المصرية للقانون الجنائي (ترجمة سامي الشوا)، دار النهضة العربية، القاهرة، 1993.

ه. المجلات:

1. المرزوقي محمد محمود، جرائم الحاسب الآلي، المجلة العربية للفقه والقضاء، إصدار الأمانة العامة لجامعة الدول العربية.
2. فاديه أبو شهاب، الحق في الخصوصية، المجلة الجنائية، إصدار المركز القومي للبحوث الجنائية، القاهرة، 1997.
3. محمد سليمان مصطفى، جرائم الحاسوب وأساليب مواجهتها، مجلة الأمن والحياة، العدد 199، 1999.
4. مجلة انترنت العالم العربي، السنة الرابعة، العدد الثامن، 2001.

ن. الرسائل الجامعية:

1. آدم عبد البديع آدم حسين، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكلفها القانون الجنائي، رسالة الدكتوراه، كلية الحقوق، جامعة القاهرة، 2000.
2. أمال قارة، الجريمة المعلوماتية، رسالة لنيل درجة الماجستير في القانون الجنائي، جامعة بن عكنون، 2001.

ثانيا: المراجع باللغة الفرنسية

A. Livre:

1. Feral-Schuhl, Christian, Cyber Droit (Le Droit A L'épreuve de L'internet), Edition Dollez, 2eme Edition, 2000.
2. Pansier Frédéric , Jérôme, Jez Emmanuel, Initiation a l'internet juridique, Edition Litec, 2eme Edition, 1er Trimestre, 2000.
3. Rose Philipe, La Criminalité Informatique, Qui Sais-Je ? Paris, P.U.F 2ed, 1995.

B. Siminaire et travaux de recherche

1. Nasim Derdour, Les Informations informatiques au Regard du droit française et le cas du droit Algérien, Mémoire de fin d'étude en Vue de l'obtention d'un diplôme de (D.E.A), Université de Perpignan, 2003.
2. Odile Boitard, Veille ou Intelligence Economique, Faut il choisir, Euromed Marseille, Ecole de management, 2006.

ثالثا: المواقع الالكترونية

1. http :www.kenanaonline.com/wsdrabakly/blog/78971
2. http : //scinceesjuridique.blogspot.com
3. www.tashreaat.com.
4. www.minishawi.com.
5. http.//www.chawkitabib.infospip-php ?articale.477.
6. www.G4me.comletesalat larticle-jsp
7. www.alyasur.gov-sa/orum/tapic-asp.arctlive

فهرس الموضوعات

الموضوعـات صفحة