بحث نهاية التدريب في موضوع

الجريمة المعلوماتية على ضوء العمل القضائي المغربي

إعداد الملحقة القضائية:

كوثر فرام

الفوج الرابع و الثلاثون

رقم التسجيل ...

تحت إشراف الأستاذ:

محمد العيماني

وكيل للملك بالمحكمة الابتدائية بالرباط

فترة التدريب: 2007-2009

مقدمة

مقدمـــة

شهدت البشرية في العقود الأخيرة ثورة في مجال المعلومات، بحيث غدت وسيلة العالم نحو الرقي الحضاري والاقتصادي، وشكل الوصول إلى المعلومات رهانا رئيسيا للإنسان لارتباطها بمختلف مجالات النشاط الإنساني وجوانب الحياة المعاصرة، إذ أصبح توفيرها وحسن استغلالها من المقومات الضرورية لدفع عجلة تقدم الأمم والمجتمعات، وصار وجودها دعامة أساسية لجهود التنمية والتحديث والرقي المعرفي، كما أن الوعي بأهميتها أضحى مؤشرا ومقياسا على تقدم الدول.

هذا، وقد تعددت التعاريف التي أعطيت للمعلومة، فهناك من عرفها بأنها رسالة معبر عنها في شكل يجعلها قابلة للنقل والإبلاغ للغير، أو بكونها رمزا أو مجموعة رموز تنطوي على إمكانية الإفضاء إلى معنى [1]، وهناك من اعتبرها مادة معرفة قابلة لأن تتمثل في إشارات متعارف عليها من أجل حفظها أو معالجتها أو بثها [2]، ولا يوجد لحد الآن تعريف قانوني جامع ومانع للمعلومة، باستثناء الإشارة البسيطة للقانون الفرنسي الصادر في 29 يوليوز 1982 الخاص بالاتصالات السمعية والبصرية، بحيث أعطى تعريفا عاما للمعلومة ينظر إليها بوصفها رنين صور الوثائق والبيانات أو الرسائل من أي نوع[3]، وفي ظل اختلاف هذه التعاريف، فإن التعريف الذي يبدو راجحا هو الذي يعرف المعلومات بأنها مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال أو للتغيير والتأويل أو

---

[1]– **محمد سامي الشوا:** "ثورة المعلومات وانعكاساتها على قانون العقوبات"، دار النهضة العربية، طبعة 1998، ص: 117 وما بعدها.

[2]– **علي كحلون:** "الجوانب القانونية لقنوات الاتصال الحديثة والتجارة الإلكترونية"، دار إسهامات في أدبيات المؤسسة، تونس، طبعة 2002، ص: 22.

[3]- Sons d'images de documents, de données ou de messages de toute nature, voir Frédérique touboul, le logiciel, analyse juridique, FEDUCI. LGD. J, 1986, p : 216.

للمعالجة سواء بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها أو نقلها بوسائل أو أشكال مختلفة [4]، ولكي تتمتع المعلومة بالحماية لابد من توفرها على شروط تتمثل في التجديد، والابتكار، والسرية، والاستئثار[5]، وإذا أردنا تمييزها عن البيانات أو المعطيات نجد أن بعض الفقه يذهب إلى كون البيانات تشكل المادة الخام التي يتم تشغيلها للحصول على المعلومات [6]، كما أن التوصية الصادرة عن منظمة التعاون والتنمية الاقتصادية في 26 نونبر 1992 الخاصة بحماية أنظمة الحاسوب وشبكات المعلومات، عرفت البيانات بأنها مجموعة من الحقائق والمفاهيم أو التعليمات التي تتخذ شكلا محددا يجعلها قابلة للتبادل والتفسير أو المعالجة بواسطة الأفراد أو بوسائل إلكترونية، أما المعلومات فهي المعنى المستخلص من هذه البيانات [7]، ويمكن القول أن المعلومات هي بيانات في حالة تبلور[8]، علما أن البيانات هي مرادف للمعطيات، رغم وجود اختلاف بين التشريعات المقارنة، بحيث نجد أن المشرعين المصري والتونسي استعملا كلمة بيانات، في حين استعمل المشرع الفرنسي كلمة معطيات، وهو نفس الاتجاه الذي سلكه المشرع المغربي في ق رقم 03-07 المتعلق بالجرائم الماسة بنظم المعالجة الآلية للمعطيات [9]، من هنا يبدو عدم جدوى التمييز بين المعلومات والبيانات ما دامت المعلومات هي المعنى المستخلص من البيانات، وتأتي أولوية الاهتمام بالتطور الحاصل في مجال

---

[4]- **نائلة عادل محمد فريد قورة:** "جرائم الحاسب الآلي الاقتصادية"، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى 2005، ص: 97.

[5]- المرجع السابق، ص: 113-114.

[6]- **محمد السعيد خشبة:** "مقدمة في التجهيز الإلكتروني للبيانات"، جامعة الأزهر القاهرة، طبعة 1984، ص: 4.

[7]- **نائلة عادل محمد فريد قورة:** مرجع سابق، ص: 98.

[8]- **محمد محمد شتا:** "الحماية الجنائية لبرامج الحاسب الآلي" دار الجامعة الجديدة للنشر، الإسكندرية، طبعة 2001، ص: 62.

[9]- يراجع: - قانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004.
- قانون التجارة الإلكترونية التونسي الصادر في 9 غشت سنة 2000.
- القانون رقم 88-19 الصادر في 05 يناير 1988 بشأن الغش المعلوماتي، والقانون رقم 2000-230 الصادر في 13 مارس 2000 في شأن الإثبات المتعلق بتكنولوجيا المعلومات.
- القانون رقم 03-07 المتمم لمجموعة القانون الجنائي المغربي فيما يتعلق بالجرائم المتعلقة بسير نظم المعالجة الآلية للمعطيات.

الاتصالات والمعلومات بالنظر إلى استقلال هذه الأخيرة بأنظمة خاصة أدت لظهور ما يعرف بالمعلوماتية [10]، التي برزت من جراء الاستخدام المتزايد للحاسوب كأداة لتخزين ومعالجة واسترجاع المعلومات، وكمساعد في عمليات التصميم والتصنيع والتحكم والإدارة، وتطورت تطبيقاته إلى أداء الخدمات في مجالات متعددة [11]، واقترنت بظهور شبكة الإنترنت التي يمكن من خلالها للشخص الذي يمتلك جهاز حاسوب مرتبط بهذه الشبكة الدخول إليها في أي وقت ومن أي مكان في العالم، يتبادل المعلومات مع غيره ويبرم الصفقات في أقصى أرجاء المعمور [12].

نتيجة هذا التطور في مجال المعلوماتية، ضعفت قدرة المراقبة والتحكم وازدهرت عمليات التجسس على المعلومات المعالجة آليا وسرقتها بشكل ملفت للنظر، حتى أصبحت تشكل تهديدا بالغا لسائر الهيئات التي تعتمد أعمالها على الحاسوب وشبكة الإنترنت، فارتفعت مخاطر استخدام الحاسوب، كما تهيأت الظروف المواتية لقرصنة البرامج وتداولها من غير منتجها الأصلي ولإنتاج الفيروسات وتمريرها من خلال الشبكات أو دسها في البرامج.

الشيء الذي أدى لظهور جرائم فنية سميت بالجرائم المعلوماتية [13]، فالجريمة هي إفراز للمجتمع ومظهر من مظاهره، تعكس ما تموج به المجتمعات من ظروف

---

[10]– عرفت التوصية الصادرة عن منظمة التعاون والتنمية الاقتصادية المعلوماتية بأنها تشمل الحاسبات الآلية ووسائل الاتصال وشبكات المعلومات والبيانات والمعلومات التي يمكن تخزينها ومعالجتها واسترجاعها ونقلها بواسطة هذه الحاسبات أو وسائل الاتصال أو شبكات المعلومات بما في ذلك البرامج المعلوماتية وجميع القواعد اللازمة لتشغيل هذه الأنظمة والحفاظ عليها.
– للمزيد انظر: **نائلة عادل محمد فريد قورة:** مرجع سابق، ص: 98.

[11]– **عبد الكريم غالي:** "قانون المعلوميات، الحماية القانونية للإنسان من مخاطر المعلوميات"، أطروحة لنيل دكتوراه الدولة في القانون الخاص، جامعة محمد الخامس، كلية العلوم القانونية والاقتصادية والاجتماعية بالرباط، السنة الجامعية: 1994–1995، ص: 6.

[12]– **طارق عبد الرحمان ناجي كميل:** "التعاقد عبر الإنترنت وآثاره"، دراسة مقارنة، رسالة لنيل دبلوم الدراسات العليا المعمقة في القانون الخاص، جامعة محمد الخامس، كلية العلوم القانونية والاقتصادية والاجتماعية بالرباط، السنة الجامعية 2003–2004، ص: 2.

[13]– **عبد الرحيم زروق:** "حماية المعلوميات من الجرائم المرتكبة عبر الإنترنت"، رسالة لنيل دبلوم الدراسات العليا المعمقة في القانون الخاص، جامعة محمد الأول، كلية العلوم القانونية والاقتصادية والاجتماعية بوجدة، السنة الجامعية 2006–2007، ص: 6.

وأسباب[14]، ولما كانت الجرائم المعلوماتية [15] ظاهرة حديثة لارتباطها بتكنولوجيا الحاسوب، فقد بذل المهتمون بدراسة هذا النمط الجديد من الإجرام جهدا من أجل الوصول إلى تعريف مناسب يتلاءم مع طبيعتها، لكن بدون جدوى حتى قيل إن الجريمة المعلوماتية تقاوم التعريف [16]، لذا اختلفت التعاريف التي تناولت هذه الظاهرة من الإجرام، فمنها من تناولها بالتعريف على نحو ضيق، ومنها من عرفها على نحو واسع[17]، مع ذلك تبقى هذه التعاريف قاصرة عن الإحاطة بأوجه ظاهرة الإجرام المعلوماتي، هذا وقد تبنى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين تعريفا جامعا للجرائم المعلوماتية بأنها كل جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية [18]، ويعد هذا التعريف من أفضل التعريفات التي تناولت ظاهرة الإجرام المعلوماتي إذ تشمل الجانبين المادي

---

[14]– **أحمد خليفة الملط:** "الجرائم المعلوماتية"، دار الفكر الجامعي، الإسكندرية، طبعة 2005، ص: 5.

[15]– أي الجريمة المتعلقة بالمعالجة الآلية للمعلومة، لأن كلمة معلومة هي اختصار مزجي لكلمة معلومة Information وكلمة آلي Automatique؛

– انظر: **أحمد حسام طه تمام** : "الجرائم الناشئة عن استخدام الحاسب الآلي"، الحماية الجنائية للحاسب الآلي، دار النهضة العربية، الطبعة الأولى: 2000، ص: 270.

[16]– **هشام محمد فريد رستم** : "قانون العقوبات ومخاطر تقنية المعلومات"، مكتبة الآلات الحديثة أسيوط، طبعة 1994، ص: 29.

[17]– من هذه التعريفات: كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية؛

يراجع: **عفيفي كامل عفيفي** : "جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون– دراسة مقارنة– منشورات الحلبي الحقوقية، بيروت، طبعة 2003، ص: 32.

– وذهب الفقيه Merlve إلى أن الجريمة المعلوماتية تتمثل في الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي"؛

انظر: **هلالي عبد الإله أحمد**: "التزام الشاهد بالإعلام في الجرائم المعلوماتية"، –دراسة مقارنة– دار النهضة العربية، الطبعة الأولى 2000، ص: 13.

– في حين ذهب جانب من الفقه إلى أنها: كل فعل أو امتناع عمدي ينشأ عن نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة في الحاسب أو التي تحول عن طريقه؛

راجع: **يونس عرب**: "موسوعة القانون وتقنية المعلومات"، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والإنترنت، الجزء الأول، منشورات اتحاد المعارف العربية، الطبعة الأولى، ص: 213.

[18]– انظر بهذا الخصوص: **أحمد المناعسة**، "جرائم الحاسب الآلي والإنترنت"، – دراسة مقارنة– دار وائل للنشر والتوزيع، عمان، ص: 8.

والمعنوي للحاسوب ومنها شبكة الإنترنت، كما أنه لم يقتصر على كون الحاسوب وشبكاته محلا للاعتداء، بل أيضا بوصفه وسيلة للاعتداء وارتكاب الجرائم، فالجريمة المعلوماتية قوامها سببين إما أن تكون المعلوماتية وسيلة للغش والتحايل والاعتداء، أو تكون المعلوماتية نفسها محلا للاعتداء.

وتكتسي معالجة هذا النوع من الجرائم أهمية بالغة بالنظر إلى الإشكالات العملية التي تطرحها على مستوى القضاء والقانون وارتباط ظهورها بتكنولوجيا الحاسوب والإنترنت، مما أسفر عن تميزها بمجموعة من الخصائص جعلتها تختلف عن غيرها من الجرائم واستوجب ضرورة التعامل معها بما يتلاءم مع هذه الخصوصية، ناهيك عن أن مرتكبيها يختلفون عادة عن المجرمين التقليديين باعتبارهم أشخاصا على مستوى عال من العلم والمعرفة، فالفاعل في الجرائم المعلوماتية أو ما يسمى بالمجرم المعلوماتي ليس شخصا عاديا إنما شخص ذو مهارات تقنية عالية قادر على استخدام قدراته لتغيير المعلومات، أو تقليد البرامج أو تحويل الحسابات عن طريق استعمال الحاسوب بشكل غير مشروع، هذا الجهاز الذي بالإمكان التلاعب فيه من خلال نسخ برامجه، أو إدخال معلومات غير حقيقية أو تعديل أو حذف المعلومات والبرامج بأشكال غير مشروعة، فهذه الجرائم ذات طبيعة خاصة لتعلقها من ناحية بأساليب المعالجة الإلكترونية للبيانات من خلال تجميعها وتجهيزها بغية الحصول على معلومات، ومن ناحية أخرى بأساليب معالجة الكلمات أو النصوص والوثائق المخزنة في الحاسوب بطريقة أوتوماتيكية، تمكن المستخدم من الاطلاع على وثائق الحاسوب وإجراء التعديلات عليها من محو وإضافة كما في حالات التقليد والتزوير.

وهي جرائم لا يستهان بها لمساسها بمصالح المجتمع خاصة فيما يتعلق بتعاملات البنوك الإلكترونية من سحب للأرصدة وإيداع عن طريق البطائق الممغنطة، وكذلك تقليد برامج الحاسوب والمساس بالحياة الخاصة للأفراد، وأمام هذه الجرائم بدت النصوص القانونية السائدة قاصرة إن لم تكن عاجزة عن تغطية الحالات الجرمية

المستجدة، وهو ما أدى إلى تضارب تطبيقات العمل القضائي، مما يستدعي ضرورة مراجعة النصوص القانونية الحالية المتعلقة بالتزوير والسرقة والاحتيال، وتقليد العلامات الفارقة.

وإذا ما كانت هناك إشكالات جوهرية قد تطرح نفسها بحدة بعد تحديث المشرع لترسانته القانونية فعموما يمكن إجمالها فيما يلي: هل استقر العمل القضائي المغربي على رؤية موحدة في معالجته للإشكالات التي تطرحها ظاهرة الإجرام المعلوماتي؟ وإذا كانت التطبيقات القضائية غير مستقرة في هذا المجال، فهل ذلك راجع لصعوبة الإحاطة بهذا النوع من الجرائم من قبل رجال القضاء؟ أم أن النصوص القانونية رغم حداثتها لم تستوعب جميع مظاهر الجريمة المعلوماتية؟ هذا ما سنحرص على رصده حين الوقوف عند كل نقطة من النقط المثارة أعلاه، مع إيلاء الاهتمام بالقوانين والأجهزة الكفيلة بمواجهة وضبط الجريمة المعلوماتية دون أن نغفل دور المجتمع الدولي، الذي إدراكا منه بأن المجهودات الفردية لكل دولة تقف عاجزة عن التصدي لهذا النمط المستحدث الذي توصف أفعاله المجرمة بأنها عابرة للحدود وتتخطى حدود الدول، اتخذ جملة من التدابير لمواجهتها.

وذلك وفق الشكل الآتي بيانه:

الفصل الأول: مظاهر تجريم جرائم نظم المعلوميات

الفصل الثاني: أوجه التصدي للجرائم الناشئة عن استخدام المعلوميات

الفصل الأول:
مظاهر تجريم جرائم نظم المعلوميات

الفصل الأول:
مظاهر تجريم جرائم نظم المعلوميات

إن إساءة استخدام المعلوماتية واستغلالها على نحو غير مشروع، أدى إلى ظهور طائفة جديدة من الجرائم عرفت بالجرائم المعلوماتية.

والتصدي لظاهرة الإجرام المعلوماتي يقتضي معرفة هذا النوع من الجرائم وطرق ارتكابها (الفرع الأول)، خصوصا وأنها تتخذ أنماطا مختلفة (الفرع الثاني).

الفرع الأول: الجرائم المعلوماتية ووسائل ارتكابها

ترتب عن الثورة الهائلة في مجال تكنولوجيا المعلوميات، أن أصبح العالم يعيش حياة زاخرة بالاتصالات السريعة ونقل المعلومات عبر المعمور، والتعامل مع نظم متقدمة للخبرة والذكاء الاصطناعي، كل هذا ما كان ليتحقق إلا بوجود الحاسوب، إلا أن ازدياد العمل به أدى إلى نشوء جرائم لم تكن مألوفة من قبل، لها سمات وخصائص تختلف عن الجرائم التقليدية (المبحث الأول)، ناهيك عن كونها جرائم تقنياتها عالية وفي تطور مستمر، تعتمد على الإبداع الذهني والتقني الهائل، الأمر الذي أدى إلى صعوبة إثباتها (المبحث الثاني).

المبحث الأول : خصائص الجرائم المعلوماتية والمجرم المعلوماتي

ارتبط ظهور الجرائم المعلوماتية وانتشارها بتكنولوجيا الحاسوب والإنترنت، وهو ما أضفى عليها صبغة خاصة جعلتها تختلف عن غيرها من الجرائم.

لذا فرصد مظاهر هذا النمط المستحدث من الجرائم يقتضي تحديد السمات التي تنفرد بها (المطلب الأول)، وتجعل مرتكبيها مجرمين من نوع خاص (المطلب الثاني).

المطلب الأول: سمات وأصناف الجرائم المعلوماتية

اتسعت تطبيقات جرائم المعلوميات في المجتمع، مما أعطاها طابعا قانونيا خاصا ميزها بمجموعة من الخصائص (الفقرة الأولى)، وأظهر تنوع أصنافها (الفقرة الثانية).

الفقرة الأولى: خصائص الجريمة المعلوماتية

تتميز الجرائم المعلوماتية بجملة من الخصائص لعل أبرزها ما يلي:

- **جرائم مستحدثة:** بحيث ظهرت تبعا للتطور الهائل في مجال التقنية العالية، وهو ما جعل أمر تحديد هذا النمط من الإجرام وإدراجه ضمن طائفة الجرائم التقليدية المعروفة يكتنفه صعوبات ترجع إلى الطبيعة الخاصة بها باعتبارها تطال المعلومات، ومن ذلك جرائم السطو على أرقام بطائق الائتمان، فقد أدى اعتماد هذه البطائق المصرفية للوفاء بالمعاملات التي تتم عبر الإنترنت إلى إمكانية قرصنتها واختراق البيانات الخاصة بها واستخدامها في عمليات شراء يدفع الثمن فيها أصحاب البطائق الأصليين، وكذلك تحويلها لأرقام وهمية تمكن الجناة من الحصول على أموال الغير، وتعد شبكة الإنترنت حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم باعتبارها ترتكب عبر هذه الشبكة، وهي خاصية أخرى تميز الجريمة المعلوماتية، ومن النماذج المدللة على ذلك، ما قام به أحد الأشخاص الذي سهلت له إقامته بروسيا، الإبحار في عالم الإنترنت والولوج إلى مواقع إلكترونية خاصة من بينها موقع "ميرك"، إذ تمكن من الحصول على مجموعة من الأقنان السرية الخاصة ببطائق ائتمان مقرصنة واستغلها في اقتناء المجلات والملابس الشخصية، وبعد عودته إلى المغرب قام بقرصنة مبالغ مالية من مؤسسة ويسترن يونيون، وبيع وحدات خاصة بالاتصالات الهاتفية عبر موقع سكايب لمجموعة من الأفارقة، كما أن تردده على نادي الإنترنت ساعده في التعرف على أشخاص آخرين أطلعوه على كيفية شراء الملابس والقبعات ذات الشهرة العالمية باستعمال بطائق ائتمان تخص أجانب يقيمون خارج المغرب

يحصلون على أرقامها عبر شبكة الإنترنت [19]، كما قام بتحويل أرقام بطائق بنكية إلى أرقام وهمية [20] مكنته من الحصول على مبالغ مالية، إلا أنه فطن بعدم نفع هذا الأسلوب داخل روسيا نظرا للحماية الإلكترونية التي تتميز بها شبابيك الأبناك الروسية، على عكس الأبناك الأمريكية إذ سبق أن خطط لإخراج مبلغ 500 روبل من شباك أحد الأبناك الروسية إلا أنه تراجع بعدما لاحظ أنها مجهزة بأجهزة تحكمية تحول دون نجاح العملية، وهو على يقين بأن استعمال نفس التقنية بإحدى شبابيك الأبناك الأمريكية سيكلل بالنجاح[21].

وما يعزز تنامي استخدام شبكة الإنترنت للقيام بأعمال إجرامية مماثلة، استغلال مواقع المحادثات الإلكترونية (Chat) لتبادل المعلومات عن كيفية قرصنة الحسابات البنكية، فقد تعرف المدعو (ع ص) على أجانب تعلم منهم تقنيات القرصنة ونظرا لعدم توفره على آلية (MSR) وبطائق لإتمام عمليات القرصنة داخل المغرب اضطر إلى تحويل المبالغ المختلسة إلى بعض أفراد عائلته بالخارج وتوصل بنصيبه منها عبر ويسترن يونيون[22]، كما أن قراصنة البطائق البنكية يربطون اتصالات مع نظرائهم

---

[19]– قرصنة أرقام بطائق الائتمان: استخدام البطائق المصرفية للوفاء عبر الإنترنت واكبه ظهور الكثير من القراصنة للسطو عليها إما بولوجهم للمواقع التجارية التي تتوفر بها قوائم تضم أرقام بطائق الائتمان وذلك باستخدامهم لقواعد بيانات عن طريق التحايل، أو بإنشائهم لمواقع وهمية للحصول على بعض هذه الأرقام السرية ومن تم القيام بسرقة الأموال، ولتفادي قرصنة أرقام البطائق يتم تشفيرها وترميزها بتحويلها إلى بيانات غير مفهومة وتداولها عبر شبكة الإنترنت، للمزيد انظر: محمد فواز محمد مطالقة: "آليات الوفاء بالبدل المالي عن طريق الإنترنت"، مقال منشور بالدليل الإلكتروني www.arablawinfo.com، تاريخ ولوج الموقع يوم السبت 22–11–2008 على الساعة الثالثة زوالا.

[20]– تحويل أرقام بطائق الائتمان لأرقام وهمية، يتم بالتلاعب بأنظمة المعالجة الإلكترونية للبيانات من خلال ولوج قاعدة هذه البيانات، وتعديل البيانات الموجودة بها أو إضافة معلومات مغلوطة، الشيء الذي يترتب عليه الاستيلاء على أموال الغير بتحويل أرصدة أصحابها الشرعيين إلى حساب المتلاعب.

[21]– قرار عدد 721 وتاريخ 12–09–2006، ملف عدد 600–06–22 ص: 4، أيد استئنافيا بقرار عدد 1203 وتاريخ 13–12–2006، ملف عدد 922–06–26، صادر عن محكمة الاستئناف بالرباط، غير منشور.

[22]– قرار عدد 364 وتاريخ 17–04–2006، ملف عدد 740–05–22 ص: 4، أيد استئنافيا بقرار عدد 865 وتاريخ 19–07–2006، ملف عدد 600–2006–26، صادر عن استئنافية الرباط غير منشور.

بمختلف الدول بواسطة البريد الإلكتروني لتبادل المعلومات والاستشارات بخصوص تطور مجال القرصنة[23].

- **ضرورة وجود حاسوب ومعرفة تقنية به :** والمقصود من وجود الحاسوب هنا، أن تتم الاستعانة به كوسيلة لتنفيذ هذه الجرائم كاستعماله في معالجة المعلومات المقرصنة من بطائق الائتمان بعد ربطه بآلة تقوم بتسجيل ونقل تلك المعلومات، ويتم نسخها على بطاقة أخرى تحمل إسم مرتكب الجريمة أو إسم مستعار تستخدم في سحب الأموال من الشبابيك الأوتوماتيكية[24]، وهذا النوع من الجرائم يتطلب إلماما كافيا بمهارات ومعارف فنية، كالمعرفة التقنية بالحاسوب واستخدامه، لأن مقترفي هذه الجرائم من المختصين في معالجة المعلومات آليا [25]،وعلى دراية فائقة بمجال الحاسب الآلي.

- **جرائم تطال معطيات الحاسوب:** أي أن الاعتداء يطال ما يمكن أن يسمى بفن الحاسوب كتدمير برامجه وسرقتها وتقليدها أو العبث ببياناته أو المعلومات المخزنة فيه، وهذه المعطيات ليست ذات طبيعة مادية ملموسة بل هي أقرب إلى الكيانات الذهنية أو المعنوية التي تم إدخالها إلى الحاسوب والتي تتطلب معالجة قانونية ذات طبيعة خاصة[26].

---

[23]– قرار عدد 300 وتاريخ 23-03-2006، ملف عدد 999-05-22 ص: 3-4، أيد استئنافيا بقرار عدد 1134 بتاريخ 27-11-2006، ملف عدد 499-06-26، صادر عن استئنافية الرباط، غير منشور.

[24]– قرار عدد 299 وتاريخ 23-03-2006 ملف عدد 736-05-22 ص: 6، أيد استئنافيا بقرار عدد 943 وتاريخ 20-09-2006، ملف عدد 520-06-26، صادر عن استئنافية الرباط، وطعن فيه أحد المتهمين بالنقض، قرار عدد 4/1586 وتاريخ 28-11-2007 ملف جنحي عدد 06/4/6/24123، غير منشور.

[25]– وهذا ما يؤكده القرار المستدل به عدد 299 وتاريخ 23-03-2006 أعلاه، ذلك أن مقترفي هذه الجرائم يستعينون بخبير في المعلوميات ينحصر دوره في معالجة المعلومات التي تسجل بالحاسوب.

[26]– **جميل عبد الباقي الصغير** : "الإنترنت والقانون الجنائي" الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية القاهرة، طبعة 2001، ص: 19.

- **صعوبة اكتشافها وإثباتها** [27]: ويعزى السبب في ذلك إلى أنها لا تترك أثرا خارجيا، وإذا اكتشفت الجريمة فلا يكون ذلك إلا بمحض الصدفة[28].

فالجرائم المعلوماتية لها طبيعة خاصة تكسبها هذه الخصوصيات، ويعد التطور التكنولوجي المتلاحق سببا رئيسيا لذلك، حيث إن شبكة الإنترنت انتشرت بها مواقع متخصصة بأعمال السطو وبيع المعلومات، وبالإمكان الاستعانة بها أو استئجار القراصنة المحترفين للقيام بالأعمال غير المشروعة المتصلة بالحاسوب مقابل مبالغ مالية يتفق عليها، ومما يزيد الأمر تعقيدا أن هؤلاء القراصنة قد لا يهاجمون من أجهزة الحاسوب الخاصة بهم وإنما يدخلون إلى شبكات غيرهم ويهاجمون من خلالها [29]، وهو ما يظهر خطورة هذا النمط الإجرامي الذي له تأثير على اختلاف تصنيفاته.

الفقرة الثانية: أصناف الجرائم المعلوماتية

تتنوع الجرائم المعلوماتية ما بين جرائم ذات طابع سياسي أو ذات ارتباط بالأمن القومي، كبت الأفكار المتطرفة أو قرصنة المعلومات المتعلقة بالأمن القومي أو العسكري، وبين جرائم ذات طابع اقتصادي، كقرصنة البرامج وعمليات غسيل الأموال، وجرائم تتعلق بسلامة الأفراد، كالتهديد بالقتل أو الجرائم المخلة بالآداب العامة، وأخيرا الجرائم التي تتعلق بسلامة شبكات المعلومات ذاتها كتعطيل وإفساد أنظمتها والاستيلاء على المعلومات التي يتم نقلها عبر الشبكة والاعتداء على المواقع الإلكترونية لإفسادها وذلك لتحقيق أغراض مختلفة[30].

ويمكن تصنيف الجرائم المعلوماتية كما يلي:

---

[27]– **محمد عبد الرحيم:** "جرائم الإنترنت والاحتساب عليها"، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، المجلد الثالث، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، الطبعة الثالثة 2004، ص: 877.

[28]– **جميل عبد الباقي الصغير:** "القانون الجنائي والتكنولوجيا الحديثة"، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، الطبعة الأولى 1992، ص: 17.

[29]– **انتصار نوري الغريب:** "أمن الكمبيوتر والقانون"، دار الراتب الجامعية، بيروت، طبعة 1994، ص: 32.

[30]– **أحمد خليفة الملط:** مرجع سابق، ص: 216.

- **الجرائم التي تعتمد في تنفيذها على الحاسوب:** تشكل أهم الجرائم التي تتصل بالمعلوماتية، ويعد الحاسوب فيها أداة رئيسية لارتكاب العمل الإجرامي نظرا لما يحتويه من معلومات وأصول، فالحاسب الآلي هنا ليس مجرد وسيلة لتسهيل النتيجة الإجرامية أو مضاعفة جسامتها، بل يمكن القول أن المعلومات والبيانات التي يحتويها تشكل الباعث على ارتكاب الجريمة[31]، كما هو الشأن في حالة التحويل غير المشروع من حساب بنكي لآخر، فاستخدام حاسوب متصل بوحدة للاتصال يعد ضروريا لتنفيذ هذا العمل الإجرامي كمن أعطى أمرا لوكالة بنكية بالولايات المتحدة الأمريكية بتحويل مبلغ 800 دولار لفائدة صديق له اقتسماه معا[32].

- **الجرائم التي يؤدي فيها الحاسوب دور ثانوي:** بحيث تتم الجريمة ولو استعان الجاني بوسيلة أخرى غير الحاسوب لارتكابها، إلا أن الحاسوب يلعب دورا في إتمامها كما في حالة استعمال آلات مخصصة لقرصنة المعلومات البنكية والمالية من بطائق الائتمان، ويتم ربط الحاسوب بهذه الآلات فيبدي عدد العمليات المسجلة وينقل المعلومات المضمنة بها لاستغلالها في صنع بطائق بنكية مزورة[33].

- **الجرائم التي يرتبط وجودها بوجود الحاسوب:** فوجود الحاسوب وأنظمته يعد ضروريا لارتكاب مثل هذه الجرائم، بحيث ترتكب في مواجهة الحاسوب أو بمساعدته، وتضم هذه الطائفة من الجرائم الدخول والاستعمال غير المصرح بهما لنظام الحاسب الآلي، النسخ أو الاستعمال غير المشروع لبرامجه [34]، ومن ذلك ماقام به مواطن

---

[31]– **محمد عبد الله أبو بكر سلامة** : "جرائم الكمبيوتر والإنترنت" منشأة المعارف الإسكندرية، طبعة 2006، ص: 116.

[32]– قرار عدد 721 وتاريخ 12–09–2006، ملف عدد 600–06–22 ص: 4، أيد استئنافيا بقرار عدد 1203 وتاريخ 13–12–2006 ملف عدد 922–06–26، صادر عن محكمة الاستئناف بالرباط، غير منشور.

[33]– قرار عدد 526 وتاريخ 29–05–2006، ملف عدد 887–05–22 ص: 3، أيد استئنافيا بقرار عدد 1024 وتاريخ 04–10–2006، ملف عدد 807–06–26، صادر عن استئنافية الرباط، غير منشور؛ وقرار عدد 37 وتاريخ 16–01–2006، ملف عدد 935–05–22 ص: 4، أيد استئنافيا بقرار عدد 884 وتاريخ 11–09–2006، ملف عدد 274–06–26، صادر عن استئنافية الرباط، غير منشور.

[34]– **محمد عبد الله أبو بكر سلامة:** مرجع سابق، ص: 111.

مغربي تمكن من تحميل برنامج قرصنة عبر شبكة الإنترنت واستطاع من خلاله أن يعبر إلى جهاز الشخص المراسل معه، ونسخ جميع المحتويات والمعلومات التي تخصه، كما قام عن طريق برنامج آخر بقرصنة الأقنان السرية لجميع العناوين الإلكترونية المسجلة بالحاسوب ومسح محتوى وحدة التخزين[35].

- **الجرائم التي يكون فيها الحاسوب محلا للنشاط الإجرامي:** إذا كان الحاسوب أحيانا أداة لارتكاب العديد من الجرائم فإنه في حالات أخرى يكون ونظامه هدفا للنشاط الإجرامي كأفعال التخريب والإتلاف التي قد توجه إلى الحاسوب ذاته أو غيره من الأشياء المادية ذات الصلة كالأسطوانات المدمجة أو الأشرطة المغناطيسية[36].

لاشك أن تنوع الجرائم المعلوماتية وعدم وجود صنف واحد لها يظهر بجلاء مدى خصوصيتها، وهو ما يستتبع بالضرورة إدراك احترافية مرتكبيها.

المطلب الثاني: طرفا الجريمة المعلوماتية

ينظر إلى المعلوماتية دائما بوصفها أداة محايدة وأن مصدر ضعفها وانتهاكها هو الإنسان الذي يقوم باستغلال الوسيلة المعلوماتية، لأن الحاسوب ليس بإمكانه ارتكاب الجرائم بمفرده، ولكن يمكن أن يستخدم كوسيلة لارتكابها، وكما هو معلوم فلكل جريمة طرفان: مرتكبها (المجرم المعلوماتي)، والمرتكب ضده الفعل الإجرامي الذي يقع ضحية له (المجني عليه في الجريمة المعلوماتية).

الفقرة الأولى: المجرم المعلوماتي

تتميز الجرائم المعلوماتية عن الجرائم التقليدية باختلاف صفات مرتكبيها عن غيرهم من المجرمين [37]، لأنهم في الغالب أشخاص على مستوى عال من العلم

---

[35]– حكم رقم 07/7794 وتاريخ 06-02-2008، ملف جنحي تلبسي تحت عدد 037 صادر عن ابتدائية الدار البيضاء، غير منشور.

[36]– **محمد عبد الله أبو بكر سلامة:** مرجع سابق، ص: 109.

[37]– **عبد الله العلوي البلغيتي:** "الإجرام المعاصر أسبابه وأساليب معالجته"، مقال مقدم في إطار سلسلة الندوات والأيام الدراسية لوزارة العدل، العدد 3، 2004، تحت عنوان: "السياسة الجنائية بالمغرب"، واقع وآفاق، المجلد

والمعرفة، ولا يمكن حصر مرتكب الجريمة في طبقة أو فئة معينة، فقد يكون من الراشدين كما هو الشأن لمجموعة من الطلبة في معهد دولي للدراسات العليا بالرباط، إذ قاموا بقرصنة أرقام بطائق ائتمان وأدوا بواسطتها ثمن مقتنيات عبر شبكة الإنترنت وتمت العملية انطلاقا من أجهزة حواسيب في حوزة المعهد الذي يدرسون به [38]، كما قد يكون مرتكب الجريمة حدثا، وكنموذج على ذلك قيام أحد الأحداث بالاستيلاء على أموال مجموعة من الأشخاص بالولايات المتحدة الأمريكية،وذلك بعد أخذه كل المعلومات الخاصة بحساباتهم البنكية من خلال شبكة الإنترنت على إثر استمارة قاموا بملئها بعدما وزعها عليهم عبر الشبكة، ولما توصل بجميع المعلومات خزنها في الحاسوب ثم وضعها على بطائق بنكية وقام بسحب مبالغ مالية مهمة من المؤسسات البنكية بالمغرب [39]، وذلك بمساعدة زميل له إذ قدر مجموع المبالغ المختلسة ثلاثين مليون سنتيم، كل عملية سحب تفوق أربعة آلاف درهم، يتسلم منها هذا الأخير ثلاثمئة درهم عن كل عملية وهو بدوره تلميذ ولا يكبره إلا بفارق أشهر جعلت منه راشدا عند عرض النزاع أمام المحكمة[40].

هذا وقد انتهت بعض الدراسات المتعلقة بمجرمي نظم المعلومات إلى تقسيم هذه الفئة لأربع فئات:

- **الفئة الأولى:** العاملون على أجهزة الحاسب الآلي في منازلهم لسهولة اتصالهم به دون تقيد بوقت محدد أو نظام معين يحد من استعمالهم للجهاز.

الأول، الأعمال التحضيرية أيام، 9 و 10 و 11 دجنبر 2004 بمكناس، منشورات جمعية المعلومة القانونية والقضائية ص: 224.

[38]– ملف جنائي عدد 971–04–22 وتاريخ 07–05–2007 ص: 3، تم تأييده استئنافيا بقرار عدد 908 وتاريخ 07–11–2007 ملف عدد 690–07–26، صادر عن استئنافية الرباط، غير منشور.

[39]– قرار عدد 23 وتاريخ 7–04–2006، ملف عدد 50–05–23، أيد استئنافيا، ملف عدد 23–08–29، صادر عن استئنافية الرباط، غير منشور.

[40]– قرار عدد 633 وتاريخ 26–06–2006، ملف عدد 461–05–22 ص: 3، أيد استئنافيا بقرار عدد 977 وتاريخ 25–09–2006، ملف عدد 816–06–26، صادر عن استئنافية الرباط، غير منشور.

- **الفئة الثانية:** الموظفون الساخطون على منظماتهم كتخريب المواقع الخاصة بها على شبكة الإنترنت أو إتلافها أو التشهير بها.

- **الفئة الثالثة:** فئة المتسللين " Hackers" ومنهم الهواة أو العابثون بقصد التسلية، وهناك المحترفين الذين يتسللون إلى مواقع مختارة بعناية ويعبثون أو يتلفون النظام أو يسرقون محتوياته، وتقع أغلب جرائم الإنترنت تحت هذه الفئة بقسميها.

- **الفئة الرابعة:** العاملون في الجريمة المنظمة[41].

ومن السمات العامة لمجرمي المعلوميات التي تميزهم عن غيرهم من المتورطين في أشكال الانحراف والإجرام الأخرى:

- السن: إذ تتراوح أعمار مقترفي تلك الجرائم عادة ما بين 17 و 46 سنة والمتوسط العمري 25 سنة؛
- المعرفة والقدرة الفنية الهائلة والحرص الشديد مع ارتفاع مستوى الذكاء؛
- الحرفية الفنية العالية، ويختفي أغلب مرتكبي هذه النوعية من الجرائم عبر دروب الإنترنت بحيث يمكن أن يختفوا تحت قناع فني يظهرهم من دولة لأخرى[42].

وتختلف دوافع ارتكاب الجرائم المعلوماتية بين دوافع ذاتية تتعلق بالرغبة في تحقيق الربح المادي بطريقة غير مشروعة كقرصنة بطائق ائتمان زبناء المطاعم [43]، أو المراكز التجارية الكبرى، أو المحطات المتواجدة بالمطارات وذلك بتمرير بطائق المسافرين الذين يسددون فواتير سفرهم بواسطتها بآلة مخصصة لقرصنة المعلومات

[41]- **محمد محمد الألفي** :" المسؤولية الجنائية عن الجرائم الأخلاقية عبر الإنترنت"، المكتب المصري الحديث، القاهرة، الطبعة الأولى: 2005، ص: 30-31.
[42]- المرجع السابق، ص: 31-32.
[43]- قرار عدد 37 وتاريخ 16-01-2006، ملف عدد 935-05-22، ص: 3، مشار إليه سابقا.

الخاصة بحساباتهم[44]، أو زبناء الفنادق [45]، وذلك بمساعدة المستخدمين بهذه المراكز مقابل مبالغ مالية تمنح لهم، كما قد تكون هذه الدوافع نفسية مرتبطة بالرغبة في إثبات الذات والتفوق، كالذي استفزه أحد الأشخاص بعرضه عليه وصل بضاعة توصل بها من الخارج عن طريق الشراء عبر الإنترنت باستعمال بطائق ائتمانية تخص أشخاصا أجانب مقيمين خارج المغرب حصل على أرقامها عبر شبكة الإنترنت، فاتصل هو بدوره بوكالة وسترن يونيون بالولايات المتحدة الأمريكية التي حولت لفائدة ذلك الشخص مبلغ 800 دولار حتى يؤكد تفوقه عليه[46].

إذا كانت الجرائم المعلوماتية بها العديد من الفوارق التي تميزها عن نظيرتها التقليدية إلا أنها لا تختلف عنها في وجود ضحية تتضرر مصالحه عندما يكون مستهدفا من قبل مرتكبيها.

الفقرة الثانية: المجني عليه في الجريمة المعلوماتية

ليس من السهل تحديد نطاق الجرائم المعلوماتية على نحو دقيق إذ يمكن أن يقع ضحيتها جميع الأشخاص سواء منها الطبيعية أو المعنوية، العامة أو الخاصة، ويرتبط هذا النوع من الجرائم بالأنشطة المالية والتجارية والشخصية، ويتخذ المجني عليه الأنماط التالية[47]:

- **المؤسسات المالية:** حيث تمس هذه الجرائم المركز الحسابي والإداري والمالي والاستثمارات وتنقلات الأموال في المؤسسات العامة أو الخاصة.

---

[44]– قرار عدد 299 وتاريخ 23–03–2006، ملف عدد 736–05–22 ، من ص 7 إلى ص: 10، مشار إليه سابقا.

[45]– قرار عدد 300 وتاريخ 23–03–2006، ملف عدد 999–05–22 ص: 7–8، مشار إليه سابقا.
– قرار عدد 526 وتاريخ 29–05–2006، ملف عدد 887–05–22 ص: 3، مشار إليه سابقا.
– قرار عدد 34 وتاريخ 16–01–2006، ملف عدد 778–05–22، ص: 3–4، أيد استئنافيا بقرار عدد 302 وتاريخ 06–03–2006، ملف عدد 170–06–26، صادر عن محكمة الاستئناف بالرباط، غير منشور.

[46]– قرار عدد 721 وتاريخ 12–09–2006، ملف عدد 60–06–22، ص: 4، مشار إليه سابقا.

[47]– **محمد سامي الشوا:** مرجع سابق، ص: 58.

- **المؤسسات التجارية والصناعية:** وتمس هذه الجرائم الدراسات الخاصة بالأسواق ومشروعات الاستثمارات والتصنيع والإنتاج والتجارة والتوزيع ومراكز البيع.
- **الأنظمة الشخصية:** تقع الاعتداءات فيها على المعلومات الشخصية المخزنة في ذاكرات الأنظمة المعلوماتية لدى البنوك وشركات التأمين[48].

ونشير إلى أن ضحايا الجرائم المعلوماتية ليسوا محصورين في هذه الفئات، بل هناك آخرين يختلفون باختلاف الهدف من الجريمة، فهناك مجرمين يستهدفون أشخاصا أو جهات بشكل مباشر عن طريق التهديد أو الابتزاز أو التشهير وتشويه السمعة، وذلك بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن ضحاياهم عبر إنشاء موقع على شبكة الإنترنت يضم تلك المعلومات، كما قد يستهدفون الأطفال من خلال استغلالهم جنسيا ولفت انتباهم للإباحية[49]، وتتمثل عناصر قيام هذه الجريمة في وجود:

1. قاصر (ذكر أو أنثى) لم يبلغ من العمر 18 سنة.
2. عرض مرئي أو مسموع يتضمن عرضا لطفل يقوم بارتكاب فعل أو سلوك جنسي سواء كان عرضا حقيقيا أو مجرد تمثيل.
3. الهدف منها هو عرض المادة الإباحية وتوزيعها ونشرها وكذا تحقيق الربح منها، وتتمظهر الأفعال المؤثمة قانونا في إنتاج مواد إباحية وفاضحة للأطفال بهدف توزيعها باستخدام جهاز كمبيوتر، وتسهيل عرضها للآخرين عن طريق هذا الجهاز ثم

---

[48]– **عبد الحكيم زروق:** مرجع سابق، ص: 48.

[49]– المفهوم القانوني للإباحية هو عرض أي شيء (صورة، فيلم، رسوم أو أي منتج باستخدام الكمبيوتر) بأي طريقة من طرق العرض، يظهر الأعضاء الجنسية لجسد الطفل، أو يقوم بارتكاب فعل أو سلوك جنسي واضح سواء كان ذلك واقعي وحقيقي أم خيالي.
انظر: ورقة تعريفية للجرائم المتعلقة بالرغبة الإشباعية باستخدام الكمبيوتر (الأعمال الإباحية وصور الأطفال الفاضحة)، أشغال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر التي أقيمت بالدار البيضاء أيام 19–20 يونيو 2007، في إطار برنامج تعزيز حكم القانون في بعض الدول العربية، مشروع تحديث النيابات العامة، غير منشورة.

شراء هذه المواد الإباحية وأخيرا حيازتها أو تخزينها على قاعدة معلومات شخصية [50]، والاستغلال الجنسي للأطفال له عواقب وخيمة إذ يخلف نتائج مباشرة وغير مباشرة، الأولى جسدية كالجروح والكدمات، أو انفعالية كمشاعر الرعب والقلق والعجز والغضب، أما الثانية فتتمثل في الآثار اللاحقة للاستغلال الجنسي وتشمل أثارا انفعالية ومعرفية واجتماعية، كظهور حالات من القلق والاكتئاب وضعف القدرة على ضبط الانفعالات والشعور بالذنب والخجل الشديد، فيكون هؤلاء الأطفال قليلي الثقة بأنفسهم وعدوانيين مع أقرانهم في المدرسة ومع أفراد أسرهم[51].

تأسيسا على ما سبق يتبين أن الجرائم المعلوماتية تأخذ تمظهرات مختلفة، مما يستدعي معرفة الوسائل المستخدمة في ارتكابها والمسهلة لقيامها ومدى إمكانية إثباتها.

المبحث الثاني: طرق ارتكاب الجرائم المعلوماتية وسبل إثباتها

تكمن جسامة وخطورة جرائم المعلوميات في طريقة ارتكابها بحيث يستغل الجاني مهارته وذكاءه ومكره بفضل تحكمه في استعمال وسيلة ارتكاب جريمته (المطلب الأول)، ولا يظهر للعيان لا الجاني ولا المجني عليه لكون الأفعال الإجرامية تقترف بشكل محبوك وبتقنية عالية لا يستطيع معها الشخص العادي أو حتى المتخصص

[50]– المرجع السابق.

[51]– **السيد نجم**: "الاتجار في البشر والاستغلال الجنسي للأطفال"، بحث مقدم في المؤتمر الدولي الثاني لحماية المعلومات والخصوصية في قانون الإنترنت، القاهرة، يونيو 2008، منشور بالدليل الإلكتروني www.google.com، تاريخ ولوج الموقع يوم السبت 22 نونبر 2008 على الساعة السادسة مساء.

اكتشاف الجريمة حين ارتكابها، الأمر الذي يطرح صعوبات حول إثباتها (المطلب الثاني).

المطلب الأول: أساليب ارتكاب الجرائم المعلوماتية

تتنوع طرق اقتراف جرائم المعلوميات ما بين زرع الفيروسات وتحميلها، وقرصنة البرامج والمعلومات باستخدام أجهزة تقنية متطورة، بالإضافة إلى جهاز الحاسوب.

1. **الفيروسات**[52]: تعتبر من أخطر أشكال النشاط الإجرامي الممارس على برامج الحاسوب والمعلوماتية بالنظر لتعدد أنواعها، وتتفاوت ما بين التخريب والإتلاف وظهرت كرد فعل يلجأ إليه مستخدموها لأهداف عديدة قد تكون مهاجمة برامج معينة أو شركات أو حتى للتسلية وإثبات الذات، ومن الأمثلة الواقعية على ذلك نستدل بما قام به تلميذ مغربي بغرض إبراز قدراته الشخصية في عالم الإنترنت أجرى تعديلات على إحدى الفيروسات وأرسله إلى مشترك تركي في موقع "ميرك" يدعى (كودر) الذي أدخل تغييرات على الوحدات المكونة للملف الذي يحمل بياناته وغير إسم الفيروس من "مايطون" إلى "زوطوب"، وأرسله لمختلف الأنظمة المعلوماتية الخاصة بمختلف المؤسسات والشركات العالمية، ومهاجمة المواقع الإلكترونية الخاصة بالمنظمات الدولية، وهو ما خلق مشاكل تقنية لدى العديد من الأنظمة المعلوماتية الأمريكية مما

---

[52]– يرى البعض أن الفيروس: مجموعة من التعليمات المرمزة تنتج لنفسها نسخا متطابقة تلتحق تلقائيا ببرامج التطبيقات ومكونات النظام المنفذ لتقوم في مرحلة معينة بالتحكم في أداء النظام الذي أصابته.

يراجع: **محمد فهمي طلبة**: "فيروسات الحاسب الآلي وأمن البيانات"، موسوعة دلتا، مطابع المكتب المصري الحديث، القاهرة، طبعة 1992، ص: 29.

وهناك من عرفه بأنه: برنامج يلحق ضررا بنظام المعلومات أو بالبيانات على أن تكون لديه القدرة على التضاعف والانتشار، بأن يقوم عند تشغيله بزرع نسخ منه في البرامج المصابة ويقوم عند دخوله إلى البرنامج المصاب، بتغيير بعض التعليمات فيه مما ينقل التحكم في البرنامج إلى الفيروس الذي يكون مخزنا في مكان آخر من الذاكرة، فيقوم بما هو مطلوب منه، ثم يعيد التحكم بعد انتهاء مهمته إلى البرنامج المصاب دون أن يترك وراءه أثرا يدل عليه.

يراجع: **حسن طاهر داود**: "جرائم نظم المعلومات"، أكاديمية نايف للعلوم الأمنية، مركز الدراسات والبحوث، الرياض، طبعة 2000، ص: 131.

جعل الأجهزة الأمنية الأمريكية تبحث عنه فغير لقبه من Diablo إلى كا (09) بعدما أعلمه التركي كودر بافتضاح أمره[53].

من هنا تظهر خطورة الفيروسات وقدرتها على التدمير إذ لا تهدد دولة واحدة فحسب أو نظام محدد، بل مختلف الدول ومختلف الأنظمة والقطاعات دون استثناء، ويتميز الفيروس عن باقي صور ارتكاب جرائم المعلوميات بـ:

- **سرعة الانتشار**: إذ يمكن أن ينتشر بسهولة وسرعة كبيرة ليطول أكثر من بلد أو جهة وأكثر من حاسوب، ويخلق مشاكل قد يحتاج حلها إلى شهور عديدة، علما أن شبكة الإنترنت ليست الوسيلة الوحيدة لسرعة انتشار الفيروسات، بل إن توافق نظم التشغيل واتباعها للمعايير أدى إلى زيادة انتشارها[54].

- **القدرة على التوالد:** وإنتاج نسخ من نفسه عندما يصيب برنامجا [55]، وتعد هذه الخاصية السبب المباشر في ضخامة حجم الخسائر التي يتسبب فيها أيا كان نوعه أو مصدره[56].

- **القدرة على الاختفاء:** إذ يمثل الفيروس برنامجا تم تزويده بإمكانية إخفاء نفسه على المستخدم والتمويه عليه[57].

- **القدرة على الاختراق:** والدخول والتسلل إلى النظام واختراق المواقع التي ينشئها المستخدم لجهاز الحاسوب، حيث يكون الفيروس في أغلب الأحيان موجودا

---

[53]– قرار عدد 721 وتاريخ 12–09–2006، ملف عدد 600–06–22، ص: 3–4–5، مشار إليه سابقا.

[54]– **فاروق حسين:** "الإنترنت الشبكة الدولية للمعلومات"، دار الراتب الجامعية، بيروت، طبعة 1997، ص: 26.

[55]– **هشام محمد فريد رستم:** مرجع سابق، ص: 164.

[56]– **أبو العلا علي أبو العلا النمر:** "الحماية الوطنية للملكية الفكرية"، دار النهضة العربية، القاهرة، طبعة 1998، ص: 199.

[57]– **محمد فهمي طلبة:** مرجع سابق، ص: 63.

في أحد البرامج المفيدة التي يحتاجها المستخدم لتشغيل الحاسوب بإمكانياته ثم يقوم بنفسه بتحميل هذه البرامج وإدخال الفيروس إلى النظام دون أن يشعر بذلك[58].

- **القدرة على التدمير:** فالفيروس برنامج يرتبط بآخر وعند تحميل هذا الأخير ينتقل إلى مكان في الذاكرة، ويظل ساكنا إلى أن يحين الموعد الذي يبدأ فيه العمل التدميري والذي قد يكون كلمة سر يكتبها المستخدم أو إشارة، في هذه الحالة يبدأ الفيروس في تدمير النظام ومسح البيانات المخزنة في ذاكرة الحاسوب[59].

وعموما، يمكن تصنيف الفيروسات إلى:

أ- الدودة المعلوماتية:

برامج معلوماتية صغيرة قائمة بذاتها وغير معتمدة على غيرها وضعت بهدف تدمير وإعاقة وتشويش الشبكات، أو بغرض سرقة بعض البيانات الخاصة ببعض المستخدمين أو لإلحاق الضرر بهم أو بالمتصلين بهم، وتتميز بسرعة الانتشار وفي نفس الوقت يصعب التخلص منها، لقدرتها الفائقة على التلون والتناسخ والمراوغة[60].

ب- القنبلة المعلوماتية:

تعرف كذلك بالشفرة المعيقة أو القنبلة الموقوتة، وهي عبارة عن برنامج يعد من قبل مصمم للنظام المعلوماتي يبثه بداخله وتكون الغاية منه جعله ينطلق أو يعمل بعد

---

[58]- المرجع السابق، ص: 64.

[59]- المرجع السابق، ص: .65

[4] – **منير محمد الجنبيهي وممدوح الجنبيهي** : "جرائم الإنترنت"، دار الفكر الجامعي الإسكندرية، طبعة 2004، ص: 62.

فترة محددة على استعمال النظام المعلوماتي بهدف تعطيله، كأن يتوقف عن العمل ويلصق رسالة أو صورة أو إشعار أو تدمير أو محو البيانات[61].

ج- الفخ أو الخبيئة:

وهو منفذ يجهز مسبقا في نظام معلوماتي من قبل مصممه من أجل إنزال برامج خاصة من شأنها أن تعيق سير عمل هذا النظام وأن تدخل إليه عناصر إعاقة لتطبيقاته[62].

د- حصان طراودة:

يعد الطريقة الغالبة في الاحتيال والتخريب بواسطة الحاسب الآلي وهي تمثل تغطية أوامر الحاسب الآلي لتمكينه من الإتيان بوظائف غير مصرح له بها، مع ترك البرنامج على حاله للاستمرار في تحقيق أهدافه[63].

2. القرصنة: نميز فيها بين قرصنة البرامج وبين قرصنة المعلومات المفضية إلى المساس بحقوق الأغيار.

أ- قرصنة برامج الحاسوب:

أدى التطور التكنولوجي لأجهزة ومعدات النسخ إلى ظهور صناعة نشطة متخصصة في استنساخ برامج الحاسوب وتسويقها محليا ودوليا، ويتمكن أصحاب هذه

---

[61]- **وليد الزيدي:** "القرصنة على الإنترنت والحاسوب"، دار أسامة للنشر والتوزيع، الأردن، الطبعة الأولى 2003، ص: 54.

[62]- **نبيلة هبة هروال :** "الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات"، دار الفكر الجامعي، الإسكندرية، طبعة 2007، ص: 60.

[63]- **محمد الأمين البشري:** "التحقيق في الجرائم المستحدثة"، جامعة نايف للعلوم الأمنية الرياض، الطبعة الأولى 2004، ص: 94.

الصناعة من الحصول على حصص مهمة من الأرباح والاستحواذ على نسبة مهمة من الزبناء، مما يلحق أضرارا كبيرة بأصحاب الحقوق على البرامج بتكبيدهم عدة خسائر[64]، لأن تسويق نسخ البرامج يكون أكثر بكثير من النسخ الأصلية.

ويمكن القول أن القرصنة لا تمثل سوى مجرد تعبير تقني وهي تقوم على استنساخ أعمال محمية دون الحصول على الإذن أو الترخيص من أصحاب الحقوق عليها لأجل تحقيق الربح[65].

وعلى الرغم من الوسائل الأمنية المعقدة التي تستخدم فيها جل أساليب التشفير والترميز من أجل الحفاظ على أمن البرامج وسرية البيانات المخزنة فيها، إلا أن إمكانية النفاذ إلى هذه البرامج ليس أمرا صعب المنال بالنظر للإلمام الواسع والخبرة الفنية لقراصنة برامج الحاسوب.

وتتنوع صور قرصنة البرامج المعلوماتية بتنوع الأهداف الكامنة وراء عمليات القرصنة ذاتها[66]، إلا أنها لا تخرج عن أمرين: تقليد البرامج المعلوماتية ونسخها.

- **تقليد البرامج المعلوماتية:** عرف البعض التقليد في ميدان البرامج بأنه محاكاة برنامج معين بصنع أو إنتاج نسخ مثله، بحيث تبدو عند تسويقها كالأصل [67]، وتأتي مسألة التقليد من خلال إنتاج برنامج يحمل في مضمونه نفس المعطيات التي يحتوي عليها البرنامج المقلد، وبالتالي ينعدم في البرنامج الجديد أي طابع ابتكاري لاستحقاق

---

[64]- انظر في تأثير القرصنة بأشكالها المختلفة على منتجي البرامج والاقتصاد ككل:
Travaux de l'association Henri capitan de la culture juridique française « les nouveaux moyen de reproduction : papier, sonores, audio visuels et informatique » rapport canadien.

[65]– **أحمد خليفة الملط:** مرجع سابق، ص: 74.

[66]– **انتصار نوري الغريب:** مرجع سابق، ص: 58.

[67]– **هشام محمد فريد رستم:** مرجع سابق، ص: 111.

حمايته، إذ ما هو سوى محاكاة للبرنامج المقلد والمحمي أصلا والذي تعرض لهذا الاعتداء مما يجعل مقترفه يستحق المتابعة والعقاب[68].

- **نسخ البرامج المعلوماتية:** وتتم بقيام الجاني بنسخ البرنامج بصفة كاملة أو بيعه دون الحصول على ترخيص بذلك من الجهات المعنية، كما لا يقوم بدفع أو سداد أنصبته من العائدات الناتجة عن بيعها[69].

وغالبا ما يتم اللجوء إلى هذا الشكل من النسخ لسهولة القيام به، بالإضافة إلى التكلفة المتواضعة حيث إن الدعامة المادية للبرنامج أو ركيزته التي تحتويه هي في متناول الجميع، وتعد أنظمة التشغيل المعقدة أو المتقدمة للحاسوب، إضافة إلى برامج الخدمات أو الترجمة، من أكثر المجالات التي يمارس فيها هذا النمط من القرصنة[70].

ب- قرصنة المعلومات:

من ذلك قرصنة المعلومات المضمنة ببطائق الائتمان واستغلال أرقامها في أداء ثمن مشتريات عبر الإنترنت[71]، وتتم عملية القرصنة بالاستعانة بآلات مخصصة لهذا الغرض تقرأ تلك المعلومات وتسجلها، وهذا النوع من القرصنة يتطلب تكوينا عاليا وخبرة في ميدان المعلوميات ومهارات في استقطاب العاملين بالمؤسسات التجارية والتغرير بهم من خلال منحهم مبالغ مالية لمساعدة المجرمين في عملهم الإجرامي، وتوزع المهام بين أفراد العصابة بحيث أن الرأس المدبر هو من يتولى البحث عن شركاء للتنفيذ، وهم المستخدمين بالمؤسسات التجارية والسياحية التي يكون زبناؤها من الطبقة الراقية ويتعاملون بالبطائق البنكية، كما يستعان بخبير في المعلوميات الذي

---

[68]- **أبو اليزيد المنبت** : "الحقوق على المصنفات الأدبية والفنية والعلمية"، منشأة المعارف الإسكندرية، الطبعة الأولى 1967، ص: 150.

[69]- **هشام محمد فريد رستم:** مرجع سابق، ص: 115.

[70]- المرجع سابق، ص: 115.

[71]-ملف جنائي عدد 971-04-22 وتاريخ 7-5-2007، ص: 3، مشار إليه سابقا.

ينحصر دوره في معالجة المعلومات التي تسجل في حاسوب ونسخ بطائق الزبناء، أما طريقة العمل التي ينهجها أفراد العصابة، فبعدما تسلم للمستخدم الشريك في العملية علبة صغيرة الحجم نوع TA 48 يدخل فيها البطاقة البنكية للزبون تقرأ وتسجل جل المعلومات الموجودة بها بإشارة من بلورة خضراء، بعد ذلك تسلم هذه الآلة لخبير المعلوميات الذي يربطها بالحاسوب ليطلع على عدد العمليات التي قام بها المستخدم وجمع المعلومات المتعلقة بهذه البطائق، بعدها يتم نسخ هذه المعلومات على بطاقة تحمل إسم المجرم أو إسم مستعار، وتنسخ البطاقة المقرصنة في عدة نظائر وبواسطتها يتمكن الجناة من تسديد مبالغ الفواتير المتعلقة بجميع الخدمات المقدمة لهم من طرف المؤسسات التجارية أو السياحية داخل التراب الوطني أو في الخارج حيث يسحبون مبالغ مالية من أرصدة الضحايا[72].

إن ارتكاب جرائم المعلوميات لا يقتصر على أسلوب القرصنة، فهو يتطلب بالإضافة إلى التكوين العالي العلمي لمرتكبيها في ميدان المعلوميات والتكنولوجيا المتطورة، توفر هؤلاء على مجموعة من الأجهزة الإلكترونية التي تستخدم في قراءة الأقنان السرية للبطائق البنكية وقرصنة المعلومات الخاصة بأصحابها وإعادة صياغتها في بطائق بنكية مزورة تسهل عملية اختلاس أموالهم.

3. الأجهزة الإلكترونية: وهي متعددة وإن كانت تؤدي نفس الدور وتسمى بالجهاز القاشط، وتتمثل في TA 90، TPE، MSR، TA 48 وآلة للطباعة 150.1 (ضاطاكارد) تساعد في تزوير البطائق البنكية[73].

يسلم الجهاز القاشط الذي قد يكون أحد الأنواع المذكورة سلفا للمستخدمين بمرافق مختلفة يرتادها زبناء يؤدون ثمن الخدمات المقدمة إليهم بالبطائق البنكية من قبل مجرمي المعلوميات، ودور المستخدم محدد في تمرير البطاقة البنكية للزبون بشكل

[72]- قرار عدد 299 وتاريخ 23-03-2006، ملف عدد 736-05-22، ص: 5-6، مشار إليه سابقا.

[73]- قرار عدد 299 وقرار عدد 526 وقرار عدد 300 وقرار عدد 37، مشار إليهم سابقا.

سري في الجهاز القاشط لقراءتها، ويستطيع أن يخزن بداخله معلومات الشرائط المغناطيسية التي تضم رقم البطاقة والإسم وسقف السحب وتاريخ الانتهاء ورقم التعريف الشخصي ورمز التحقق الذي يؤكد أن البطاقة صالحة عند استخدامها في نقاط البيع، ويتم نسخ بيانات هذه البطاقة من القاشط إلى جهاز كمبيوتر محمول، بعدها تؤخذ بطائق فارغة مزودة بصورة مجسمة وبواسطة آلة الطباعة تطبع ملصقات رقيقة تحمل نسخا من الأشرطة المغناطيسية وأشرطة التوقيع ليتم لصقها على البطائق الفارغة، ثم تشفر المعلومات المسروقة على شريط مغناطيسي باستعمال آلة كاتبة ويقوم المزورون في الأخير بنقش الأرقام والإسم وتفاصيل أخرى مختومة على البطاقة[74].

4. الحاسوب: يمكن أن يكون أداة لارتكاب العديد من الجرائم، كما في حالة استغلاله للاستيلاء على الأموال بإجراء تحويلات غير مشروعة، أو استخدام التقنية في عمليات التزييف والتزوير أو في الاستيلاء على أرقام بطائق الائتمان وإعادة استخدامها والحصول على الأموال بواسطتها، أو في معالجة المعلومات المقرصنة، حتى أنه يستخدم في جرائم القتل كما في حالة الدخول إلى قواعد البيانات الصحية والعلاجية وتحويرها أو تحوير عمل الأجهزة الطبية والمجهرية عبر التلاعب ببرمجياتها[75].

من البديهي أن الوسائل الحديثة تعد تقنيات يستغلها مجرمون متمرسون بهدف تحقيق أهداف إجرامية تلحق أضرارا جسيمة بضحايا جرائم المعلوميات، في حين يجنون من ورائها منافع مالية مهمة، واعتماد هؤلاء المجرمين المحترفين للتقنيات الحديثة أدى إلى صعوبة إثبات هذا النوع من الجرائم.

---

[74]- انظر الملحق، خطاطة توضيحية لطريقة قرصنة البطائق البنكية.

[75]- "**الجرائم المعلوماتية**": مقال بدون إسم صاحبه، منشور بالموقع الإلكتروني www.google.Com تاريخ ولوج الموقع يوم السبت 22 نونبر على الساعة السادسة مساء.

المطلب الثاني: الإثبات في جرائم المعلوميات

يكتنف إثبات الجرائم المعلوماتية صعوبات جمة ترجع لأسباب عديدة أهمها عدم وجود أثر مادي للجريمة المرتكبة، كما أن الجاني يستطيع تدمير دليل الإدانة في أقل من ثانية، والأكثر من ذلك أن الإجرام المعلوماتي لا يعترف بالحدود إذ أن الجريمة قد تتم من مسافات بعيدة عبر اتصال هاتفي يمكن للجاني من خلاله إعطاء تعليماته للحاسب الآلي، ومما يزيد من استعصاء إثبات هذه الجرائم أن المجني عليهم يحجمون عن الإبلاغ عن وقوعهم ضحية لها، بل حتى في حالة استطاعة السلطات المعنية وضع يدها على البعض منها فإن الضحايا يمتنعون عن مساعدة هذه السلطات أملا في استقرار حركة التعامل ويفضلون إخفاء أسلوب ارتكاب الجريمة مخافة إتاحة الفرصة للآخرين لتقليدها، كما أن الكشف عن الجرائم التي تقع ضحية لها بعض المؤسسات من شأنه الإضرار بها نتيجة ضياع ثقة المساهمين والمتعاملين معها، إذ يظهر لها أن المحافظة على ثقة مساهميها وعدم زعزعة سمعتها وشهرتها أفيد بكثير من الإبلاغ عن بعض الجرائم التي ترتكب ضدها، وقد لا تجني شيئا من وراء تقديم شكايات بشأنها لصعوبة إثباتها ولاستحالة العثور على مقترفيها، لذلك يبقى من الأفضل بالنسبة إليها تسوية المشكل داخليا حتى لو كلفها الأمر التضحية بمبالغ مالية كبيرة، أضف إلى ذلك أن مقترفي هذا النوع من الجرائم لا يخضعون لأي مراقبة قبلية أثناء إقدامهم وتصميمهم على ارتكابها، فغياب هذه المراقبة والتطور السريع الذي يعرفه مجال المعلوميات يساعد في ذلك[76].

إلى جانب ذلك فإن المعطيات المتداولة من صوت وصورة وكتابة، سواء اتخذت شكل تجميع للمعطيات أو برامج حاسوب تتمثل كلها في أنظمة التشغيل في شكل إلكتروني يتجسد في وحدات حسابية وفي أنظمة التطبيق، تندثر بسهولة فائقة إذ

[76]– **محمد كرام:** "صعوبة إثبات الجرائم المرتكبة عن طريق التقنيات الحديثة"، مجلة المحامي العدد 44–45، ص: 336–337.

يكفي الضغط على زر في لوحة الاستخدام لزوال ملفات أو قواعد معطيات وأنظمة بأكملها، من هنا تأتي مشكلة ضبط هذه المعلومات وإحرازها في شكل إلكتروني ووضعها في قالب قانوني لاستغلالها في الإثبات، وإذا كانت بعض التجهيزات تسمح بالوصول إلى هذه المعطيات التي تبقى في ذاكرة الحاسوب المستعمل إلا أنها تتطلب خبرة عالية، وينضاف إلى هذا مشكل الولوج إلى بعض المعلومات المحفوظة تحت رقم أو رمز سري أو المشفرة كليا، أما المستندات والوثائق التقليدية من أوراق مطبوعة أو كتابات خطية أو حتى دعامات إلكترونية من أقراص صلبة أو مرنة التي قد تساعد في تذليل صعوبات الإثبات، فإنها لا تتاح دائما لاسيما في مواجهة أشخاص سيئي النية أو مجرمين متمرسين، فعلاوة على لجوء هؤلاء إلى تطهير المحيط الذي يعملون فيه، فهم يعمدون دائما إلى حفظ المعطيات باستعمال أرقام أو رموز سرية أو حتى استعمال تقنية التشفير، كما أن المعالجة الآلية للمعطيات المسجلة في الملفات الإلكترونية أو المخزنة في ذاكرة الحاسوب والتي يتم حجزها يمكن أن تشكل عائقا أمام نسبة معطيات إلكترونية إلى شخص محدد بعينه بشكل يقيني، فالبصمات أو الآثار الشخصية أو التوقيع إن كان هناك توقيع أو بصمات فلا تدل على شخص معين، لأن هذه الآثار الشخصية لا تكون مجسدة ماديا أو حتى إلكترونيا في كثير من الأحيان بقدر ما يستدل عليها بقرائن الأحوال كحيازة حاسب آلي أو القن أو الرقم السري للولوج إلى المعلومات أو لاستخدامه، وأيضا التوفر على المهارة التقنية للقيام ببعض التطبيقات المعقدة أو للهجوم على قاعدة للمعطيات أو على نظام[77].

وعلى صعيد آخر فالمعطيات التي تعتبر أداة للجريمة وموضوعا لها، وأحيانا نتيجة متحصلة هي من الهشاشة، بحيث تكفي عملية نقر على رمز لمسح وإزالة المعطيات التي يمكن اعتمادها في الإثبات، كما أن شبكة الإنترنت توفر لمستعمليها

[77]– **أحمد آيت الطالب:** "تقنيات البحث وإجراءات المسطرة المتبعة في جرائم الإنترنت المعلوميات"، مجلة الملف، العدد 9 نونبر 2006، ص: 23–24.

هامشا كبيرا من الحرية للبقاء في الظل مادامت لا تتطلب التعريف بهوية القائمين بإحداث مواقع إلكترونية أو مستعملي خدمات البريد الإلكتروني، وحتى في مجال التجارة الإلكترونية التي يفترض فيها تعريف الطرفين البائع والمشتري كل واحد منهما بنفسه بالشكل الكافي لأداء الثمن عبر الشبكة بصورة إلكترونية فهو أمر ليس مضمونا دائما في مجال المعاملات عن طريق الإنترنت بسبب تفشي أعمال سرقة الهوية أو انتحالها أو استعمال هويات وهمية لإيقاع الغير بالغلط[78].

ولعل قرصنة بطائق الغير البنكية وأرقامها، والأمر بتحويل الأموال من حساب بنكي لآخر، وسحب الأرصدة المالية للغير خير دليل على ذلك إذ يصعب إثبات هذه الأفعال الجرمية في غالب الأحيان وإن تم اكتشاف مرتكبيها فبعد مشاق عديدة.

هذا ونشير إلى أن الحاسوب وإن كان يستخدم في ارتكاب جرائم إلكترونية، فإنه مع ذلك يلعب دورا مهما في اكتشافها وتتبع فاعليها رغم الصفات الاستثنائية التي يمتازون بها من ذكاء وعلم بليغ بوسائل التكنولوجيا، ذلك أن تحليل معلومات يحتويها جهاز حاسوب أحد المجرمين ساعد على تحديد مكان فندق بالرباط قرصنت به مجموعة من البطائق البنكية بلغ عددها خمسة وأربعين بطاقة، ومكن من التعرف على المستخدم الذي قام بالعملية لفائدة ذلك المجرم[79].

وغني عن البيان أن الحاسوب أصبح يشكل الركيزة الأساسية في إنتاج وتداول المعلومات إذ يعتمد في أسلوب عمله على البرنامج الذي يشكل القلب النابض بالنسبة إليه، فهو الذي يوجهه ويحدد مسار عمله وطريقة تنفيذه للأوامر والمعلومات الموجهة إليه[80]، كما أن التطور المستمر والمتنامي الذي تعرفه تكنولوجيا المعلومات بالموازاة

---

[78]– المرجع السابق، ص: 27.

[79]– قرار عدد 34 وتاريخ 16-01-2006، ملف عدد 778-05-22، ص: 3، مشار إليه سابقا.

[80]– **طارق بن عبد الله الشدي** : "مقدمة في الحاسب الآلي وتقنية المعلومات"، دار الوطن، الرياض، الطبعة الأولى 1995، ص: 10.

مع النمو السريع الذي عرفته تكنولوجيا الاتصال ساهم بدرجة كبيرة في تعدد أنماط جرائم المعلوميات.

الفرع الثاني: أنماط الجريمة المعلوماتية

إن انتشار شبكات الاتصال والمعلومات ودخول تطبيقاتها في بيئة المجتمعات المعاصرة ساهم ولاشك في تعزيز التواصل، إلا أنها ساعدت على شيوع الجريمة بمختلف أشكالها، والمتأمل في حال التطور التكنولوجي في مجالات الحواسيب والإنترنت يدرك ما قدمته هذه الوسائل من تسهيلات كبرى للأنشطة الإجرامية المنظمة والفردية على حد سواء، جاعلة الأمن الاقتصادي والاجتماعي لكثير من الدول عرضة لأنماط جديدة من الجرائم الذكية تتباين ما بين الاستعمال غير المشروع لبطائق الائتمان (المبحث الأول)، والاعتداءات المهددة للأنظمة المعلوماتية (المبحث الثاني).

المبحث الأول: الاستعمال غير المشروع لبطائق الائتمان

إن التعامل بالبطائق البنكية وإن كان حديث العهد نسبيا، فقد طرح استعمالها من قبل الغير استعمالا غير قانوني عدة إشكالات على مستوى العمل القضائي، بالنظر إلى تكييفها أحيانا ضمن جرائم الأموال (المطلب الأول)، وأحيانا أخرى ضمن جرائم تزوير المحررات (المطلب الثاني).

المطلب الأول: مدى إعمال القواعد العامة في جرائم الأموال لحماية بطائق الائتمان

صاحب انتشار بطائق الائتمان الممغنطة وشبكات التحويل الإلكتروني للنقود وتزايد حجم التعامل بهما نموا متزايدا في الجرائم المصاحبة لاستخدامها، حيث احترف البعض سرقة هذه البطائق (الفقرة الثانية)، أو استخدامها بالتحايل في الاستيلا ء على مال الغير (الفقرة الثالثة)، إلا أنه قبل مناقشة ذلك على ضوء العمل القضائي لا بأس أولا من تأطيرها قانونيا (الفقرة الأولى).

الفقرة الأولى: الإطار القانوني لبطائق الائتمان

بطائق الائتمان الممغنطة هي بطاقة مستطيلة مصنوعة من مادة البلاستيك تحمل إسم المؤسسة المصدرة لها وشعارها وتوقيع حاملها وبشكل بارز على وجه الخصوص رقمها وإسم حاملها ورقم حسابه وتاريخ انتهاء صلاحيتها، وبفضل هذه البطاقة يستطيع حاملها أن يسحب مبالغ نقدية من أجهزة التوزيع الأوتوماتيكي لأوراق البنكنوت، أو أن يحصل من فئة معينة من التجار المتعاملين بهذه البطاقة على ما يحتاجه من سلع وخدمات دون أن يضطر إلى الوفاء بثمنها فورا – نقدا أو بشيكات– كما يكتفي بتقديم بطاقته إلى التاجر الذي يدون بياناتها عادة باستخدام آلة طابعة إلكترونية أو يدوية في فاتورة من عدة نسخ يوقعها العميل ويرسل التاجر نسخة من هذه الفاتورة إلى الجهة المصدرة للبطاقة فتتولى سداد قيمتها وخصمها في نفس الوقت من الحساب الجاري للعميل لديها [81]، ويمكن تقسيم هذه البطائق إلى عدة أنواع وهي كالآتي:

[81]– **عبد الله حسين علي محمود** : "سرقة المعلومات المخزنة في الحاسب الآلي"، دار النهضة العربية، القاهرة، الطبعة الأولى 2001، ص: 226–227.

1. بطاقة السحب الآلي: تخول هذه البطاقة لصاحبها سحب مبالغ مالية محددة من حيث المقدار، ويكون ذلك عن طريق الشبابيك الأوتوماتيكية [82]، للبنك مصدر البطاقة سواء في المدينة التي يوجد فيها البنك المفتوح فيه حساب الزبون الحامل للبطاقة أو في غيرها، متى كانت الشبابيك الأوتوماتيكية متصلة بالبنك مصدر البطاقة أو في غيرها من الأبناك المشتركة في إصدار هذه البطاقة، حيث يحق للمستفيد في هذه الحالة استخدامها في جميع التراب الوطني لدى فروع تلك المؤسسات البنكية، على أن تجري المقاصة فيما بينها[83].

2. بطاقة الوفاء: تسمى أيضا ببطاقات الأداء، تخول حاملها وفاء ثمن السلع والخدمات التي يحصل عليها من بعض المحلات التجارية التي تقبلها بموجب اتفاق مع الجهة المصدرة لها وذلك بتحويل ثمن البضائع والخدمات من حساب العميل المشتري (حامل البطاقة) إلى حساب التاجر[84].

3. بطاقة الضمان: تستخدم هذه البطاقة على الخصوص لضمان الوفاء بالشيك في حدود المبلغ المتفق عليه، حيث يقوم الزبون ساحب الشيك (صاحب البطاقة) بتقديم هذه البطاقة لدائنه الذي يقوم بتعبئة بعض البيانات الرئيسية الواردة في البطاقة على ظهر الشيك [85]، فكتابة رقم البطاقة على الشيك والتوقيع عليه يضمن للمستفيد قيمته من طرف المؤسسة البنكية المصدرة للبطاقة سواء أكانت المؤونة غير متوفرة أم غير كافية لدى الزبون مصدر الشيك.

---

[82] – **GAVALDA (Christian) & Stoufflet (jean) :** « effets de commerce chéque cartes de paiement et de crédit », troisiéme édition, litec 1998, p : 392.

[83] – **محمد الشافعي:** "بطاقات الأداء والائتمان بالمغرب"، سلسلة البحوث القانونية 5، مراكش، الطبعة الأولى 2002، ص: 21.

[84] - **عبد الله حسين علي محمود:** مرجع سابق، ص: 224.

[85] - **محمد الشافعي:** مرجع سابق، ص: 23.

4. بطاقة الائتمان: تصدر عن تاجر أو مؤسسة ائتمان تخول لصاحبها الحصول على ائتمان في حدود السقف المتفق عليه مقابل عمولات وفوائد لقاء توفير الاعتماد لحاملها، فهي بمثابة قرض الاستهلاك يخضع لنظام القروض والفوائد، لذلك يطلق عليها بطاقة الائتمان الحقيقي[86].

فإلى أي حد كان القضاء المغربي منسجما مع روح القوانين المجرمة للاعتداءات التي تطال هذه البطائق من قبل الغير من خلال تكييفه لها؟

الفقرة الثانية: إساءة استعمال بطائق الائتمان من قبل الغير

إن الاستعمال غير المشروع للبطاقة بواسطة الغير، لا يتم من خلاله خرق شرعية البطاقة، فهي صحيحة ودخلت في حيازة الغير نتيجة السرقة أو الفقد، وإنما يتم خرق شرعية الحامل الذي هو غير شرعي، فالاستيلاء على أرقام بطائق الائتمان وتداولها بين العديد من الأشخاص واستعمالها في اقتناء مشتريات عبر الإنترنت اقتطع ثمنها من الحسابات البنكية لأصحابها الشرعيين، يعد سرقة موصوفة حسب ما ذهبت إليه محكمة الاستئناف بالرباط معللة قرارها بأن: "المتهمين جميعا وإن كانوا ينكرون تداول بطاقات الائتمان واستعمالها عبر الانترنت فإن المحكمة ثبت لديها أنهم بالفعل لهم علاقة مباشرة بما تم من أفعال، أحدهم بصفته فاعلا وهو المتهم (م م) الذي يعد الفاعل الأصلي لجريمة السرقة الموصوفة، وآخرون بصفتهم شركاء فيها بالنظر إلى دور كل واحد في هذه الأفعال، ذلك أن المتهم (ب) بعد أن استجمع كل العناصر والوسائل بما فيها أرقام بطاقات الائتمان إلى جانب زميله المتوفى (ع هـ) والحصول عليها من خلال بقية المتهمين ولاسيما المتهم (م هـ) الذي كان يعمل بفرنسا بإحدى الفنادق كمتدرب، فاستغل هذا الأخير تواجده وتوافد ترتيبات الفندق وبادر إلى اختلاسها

---

[86]– **أحمد البختي:** "استعمال الوسائل الإلكترونية في المعاملات التجارية"، رسالة لنيل دبلوم الدراسات العليا المعمقة في القانون الخاص، جامعة محمد الخامس، كلية العلوم القانونية والاقتصادية والاجتماعية السويسي بالرباط، السنة الجامعية 2003–2004، ص: 14.

وتمديدها إلى زملائه من المتهمين الذين عملوا فيما بينهم على تداولها إلى أن وصلت بيد الفاعل الأصلي الذي باشر عملية السرقة وترتب عن الاستعمال الاختلاس في حق الضحايا...ومحجوز الحواسب واللوائح التي وردت بها أسماء بعض المتهمين....كل هذه العناصر تدل دلالة قاطعة على قيام هذه الجريمة في حق هؤلاء المتهمين"[87].

الحقيقة أن هذا التكييف يبدو منطقيا، إلا أن ما يؤاخذ عليه أنه لم يناقش نية التملك باعتبارها قصدا خاصا في السرقة وعنصرا جوهريا، إذا وجد تتحقق وإن لم يتوفر لا تقوم السرقة ما دام أن بطائق الائتمان تسلمها المتهم العامل بالفندق من أصحابها لدفع مقابل الخدمات التي قدمت لهم بعين المكان، ولم يستول عليها بل ردها إليهم بعد أن أخذ أرقامها ومنحها لأشخاص آخرين استعملوها لأداء ثمن مشتريات عبر الإنترنت.

فالسرقة اختلاس مال منقول مملوك للغير بطريق الغش وبنية تملكه، وتستلزم لتحققها توفر ثلاث عناصر: الاختلاس، محل الاختلاس ويشترط فيه أن يكون مالا منقولا مملوكا للغير والذي يتخذ صورة القصد الجنائي الخاص، نية التملك والتي يقصد بها انصراف إرادة الجاني إلى الظهور على الشيء بمظهر المالك وتتألف هذه النية من عنصرين، عنصر سلبي وهو إرادة حرمان المالك من سلطاته على الشيء وعنصر إيجابي قوامه إرادة الجاني أن يحل محل المالك في سلطاته الفعلية على الشيء[88].

فإذا قام شخص باختلاس بطاقة ائتمان واتجهت نيته إلى تملكها فإنه يعد مرتكبا لجريمة السرقة، أيا كان الباعث الذي دفعه لذلك فتقوم جريمة السرقة ولو كانت نية

---

[87]- ملف جنائي عدد 971-04-22 وتاريخ 7-5-2007 ص: 11، أيد استئنافيا بقرار عدد 908 وتاريخ 07-11-2007، ملف عدد 690-07-26، ما عدا في الشق المتعلق بأحد المتهمين (ع م) إذ تمت إدانته من أجل إخفاء أشياء متحصل عليها من جناية طبقا للفصل 572 من ق ج بعد إعادة التكييف لجناية السرقة الموصوفة ص: 8، غير منشور.

[88]- **عفيفي كامل عفيفي:** مرجع سابق، ص: 136-158-159.

المتهم متجهة إلى مجرد الاحتفاظ بها وحرمان حاملها من استعمالها، بل وتقوم جريمة السرقة حتى لو كان الباعث شريفا يتمثل في منع الحامل من إساءة استعمالها.

لكن إذا حصل شخص على بطاقة ائتمان لا بنية تملكها لكن بنية استخدامها وإعادتها مرة أخرى لصاحبها وعلم الرقم السري الخاص بها فما هي الجريمة التي يمكن نسبتها إليه؟

بديهي أن انتفاء نية التملك يؤدي إلى انتفاء جريمة السرقة، إلا أنه يتعين عدم الخلط بين مجرد الانتفاع بالشيء بدون حق، وبين سلب قيمته، ونقصد بسلب قيمة الشيء الحالة التي يستولي فيها الشخص على شيء مملوك لغيره بنية استعماله على نحو يجرده من قيمته كلها أو بعضها ثم رده بعد ذلك إلى صاحبه فقصد الجاني هنا استنزاف قيمة الشيء كلها أو بعضها بحيث وإن أعاده كان عديم القيمة أو ناقصه فينبغي اعتبار فعله سرقة لأن القانون عندما يحمي الأشياء لأنها تمثل قيمة معينة تكون العبرة في نظره بقيمة الشيء لا مادته، ذلك أن استيلاء الشخص على شيء مملوك لغيره بغير رضاه أو استنزاف قيمته كلها أو بعضها رغم اتجاه نيته وقت استيلائه عليه إلى رده لصاحبه لا يحول دون اعتبار فعله اختلاسا محققا لجريمة السرقة، ويبدو واضحا أن استخدام رقم بطاقة الائتمان لدفع قيمة مشتريات يترتب عليه استنزاف قيمتها، فانتهاء الرصيد الخاص بحامل البطاقة أو المبلغ الموجود في رصيده بناء على الاتفاق القائم بينه وبين البنك يجعل البطاقة عديمة القيمة، وهذا يعني أن سرقة رقم بطاقة ائتمان بنية استعماله وإعادة البطاقة لصاحبها وبقائها في ذمته باعتباره مالكها يعد جريمة سرقة.

إلا أن هناك إشكالا قانونيا يطرح ويتعلق بالوضع القانوني للدفع الإلكتروني بالبطاقة الائتمانية في شبكة الإنترنت من قبل شخص غير صاحب الحساب البنكي؟

قبل أن تتحول معظم بطائق الائتمان إلى وسيلة دفع إلكترونية فعلية عن بعد يمنح حاملها رقما سريا يستخدمه في التوقيع الإلكتروني على عمليات الدفع، نشير إلى أن نظام استخدام بطائق الائتمان اقتصر طويلا على طريقتين تقليديتين:

- إما أن يصدر التاجر إيصالا ورقيا يوقعه الزبون حامل البطاقة.
- وإما أن يكتفي التاجر بتسجيل رقم البطاقة الظاهرة وتاريخ صلاحيتها من دون الحصول على توقيع الزبون، وهاتان الطريقتان في الدفع لا يبدو أنهما مناسبتين للدفع عبر شبكة الإنترنت، لأنه في الطريقة الأولى ليس في إمكان التاجر الحصول على إيصال موقع من زبونه لكون الصفقة تمت في شبكة الإنترنت عن بعد (أي بين غائبين)، أما في الطريقة الثانية، أي حين يتم الدفع بمجرد ذكر رقم البطاقة المصرفية فإن شبكة الإنترنت لا تقدم أي ضمانة لجهة مانح الأمر أو لجهة الغش والتحايل الحاصلين من جراء استعمال رقم البطاقة الظاهر من قبل الغير على نحو غير مشروع[89].

ونقصد بالدفع بواسطة البطاقة الائتمانية في شبكة الإنترنت، الدفع الحاصل بوسيلة إلكترونية فعلا، أي حين يمنح صاحب البطاقة أو غيره رقما أو رمزا سريا يستخدمه في عملية الدفع أو التحويل أو سحب الأموال النقدية إلى غير ذلك من الخدمات التي تحصل عبر شبكة الإنترنت.

يسمى استخدام الرمز السري للدفع بالبطاقة "بالتوقيع الإلكتروني"، وهذه التسمية تطلبت على المستوى القانوني إجراء تعريف جديد للمفهوم الكلاسيكي للتوقيع من منطلق التركيز على وظيفته وليس على شكله، أي التركيز على أن التوقيع ليس سوى

---

[89]- **طوني عيسى:** "حول الدفع الإلكتروني بالبطاقة الائتمانية في شبكة الإنترنت"، بحث تمت المشاركة به في أعمال المؤتمر العلمي السنوي لكلية الحقوق بجامعة بيروت العربية، منشور بكتاب تحت عنوان: "الجديد في أعمال المصارف من الوجهتين القانونية والاقتصادية"، الجزء الأول: "الجديد في التقنيات المصرفية"، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى 2002، ص: 210.

طريقة للتعريف عن هوية صاحبه وللتعبير عن رضاه وعن إرادة من يستعمله على الالتزام أو التعاقد[90].

على هذا الأساس يصير الدفع بواسطة البطاقة الائتمانية في إطار شبكة الإنترنت ممكنا لكنه يستتبع قيام مخاطر متصلة بالقرصنة المعلوماتية للأرقام السرية من خلال تعرض هذه الأرقام لاعتداءات ذات طابع احتيالي منها استخدامها في عمليات شراء يدفع الثمن فيها أصحاب البطائق الحقيقيين وهو ما يشكل تزويرا لتوقيع إلكتروني، وذلك بالتزوير والتلاعب في البيانات والمعلومات الخاصة بأصحاب بطائق الائتمان واستعمالها بدون وجه حق، مما يترتب عنه إلحاق ضرر بهم، يعرضهم للعقوبة المنصوص عليها بالفصل 7-607 من القانون الجنائي.

وفي قرار آخر ذهبت نفس المحكمة إلى أن المتهم تمكن هو وصديقه المتوفى قيد حياته من اقتراف السرقة عن طريق قرصنة البطائق البنكية معللة قرارها بأن "الأفعال المنسوبة إليه تشكل جناية السرقة الموصوفة طبقا للفصل 609 من القانون الجنائي لكون اختلاس أموال الضحايا اقترن بظرفي التعدد واستعمال مفاتيح مزورة ذلك أن استعماله للآلة نوع TA 48 التي تمرر فيها البطاقة البنكية للزبون والتي تقرأ وتسجل جميع المعلومات المضمنة بهذه البطاقة وربطها بالحاسوب ونسخ هذه المعلومات على بطاقة مقرصنة تحت إسم مستعار تعتبر بمثابة مفاتيح لكونه من خلال استعماله لهذه الآلة ونقله لهذه المعلومات عن طريق الحاسوب وكذا نقل رمز البطاقة من الآلة المذكورة عبر الحاسوب يتمكن من الدخول إلى الحساب البنكي

[90]- المرجع السابق، ص: 241.

للضحية ويتمكن بواسطة البطائق المزورة من اختلاس أموال الضحايا من الأبناك التي تعتبر دار للمال مخصصة لحفظه وحمايته لفائدة من له الحق فيه بطريقة قانونية"[91].

إن التكييف الذي ذهبت إليه المحكمة مجانب للصواب لأن الآلة TA 48 جهاز إلكتروني صغير بإمكانه التقاط المعلومات من البطاقة الائتمانية ومن تم إنتاج بطائق مزيفة بالرقم المسروق نفسه، فالبطاقة تحمل معلومات وبيانات على ظهرها ووجهها وتنقسم إلى نوعين: بيانات لا يمكن قراءتها إلا بواسطة أجهزة معدة خصيصا لهذا الغرض كما هو الشأن بالنسبة لهذه الآلة، ومعلومات ظاهرة يمكن قراءتها بالعين المجردة إسم وشعار المؤسسة المصدرة ونوع البطاقة، شعار المنظمات العالمية للبطائق (فيزا- ماستركارد)، إسم صاحب البطاقة ورقم خاص بالبطاقة وتاريخ صلاحيتها، لذا لا يمكن اعتبار الآلة مفاتيح مزورة لأنها لا تدخل في عداد المفاتيح المسروقة أو المصطنعة[92]، فالمفتاح المصطنع هو الذي يسمح بالدخول في مكان معد للسكن أو محل لحفظ النقود إلا أنه من المشكوك فيه تشبيه آلة القرصنة بالمفتاح لأنه من ناحية ليست الآلة مفتاح أو وسيلة مشابهة للمفتاح، ومن ناحية أخرى لا يدخل الجاني إلى المكان المسور – إذا اعتبرنا أن الموزع هو السور حول النقود- ولا يستعمل الآلة في الدخول، وإنما يستعمل البطاقة المزورة التي تتضمن معلومات خاصة بصاحب الحساب البنكي والمقرصنة بواسطة الآلة في إخراج النقود من البنك، وهذا لا يعني أن البطاقة المزورة هي المفتاح المصطنع لأنها ليست أداة دخول في مكان الجريمة وإنما هي أداة الجريمة، وبالتالي فاعتبار الآلة أو بطاقة الائتمان المزورة

---

[91]- قرار عدد 526 وتاريخ 29-05-2006، ملف عدد 887-05-22، صادر عن محكمة الاستئناف بالرباط، أيد استئنافيا بقرار عدد 1024 وتاريخ 04-10-2006، ملف عدد807-06-26، غير منشور، ص: 14-15.

[92]- المفتاح المصطنع هو كل مفتاح غير المفتاح الذي أعد خصيصا لباب المكان الذي ارتكبت السرقة في داخله، يراجع: **كيلاني عبد الراضي محمود** : "المسؤولية عن الاستعمال غير المشروع لبطاقات الوفاء والضمان"، دار النهضة العربية، القاهرة، طبعة 2001، ص: 130.

بمثابة مفتاح مصطنع يتعارض مع قاعدة عدم جواز اللجوء إلى القياس في التجريم الذي يحظره مبدأ شرعية الجرائم والعقوبات.

ومن الملاحظات المثارة بخصوص هذا القرار كذلك متابعة المتهم بتكوين عصابة إجرامية لكونه اتفق مع المتهم (ع ه) قيد حياته على قرصنة بطائق الائتمان، فهل يمكن الحديث عن جناية تكوين عصابة إجرامية في الجريمة الإلكترونية؟

يتطلب قيام هذه الجناية مجموعة من الشروط والشكليات لعل أهمها أن يكون الاتفاق بين الأطراف على تقسيم الأدوار من أجل ارتكاب جنايات ضد الأشخاص أو الأموال، لكن الجريمة المعلوماتية هي دائما حسب الوصف المتفق عليه جنحة وليس جناية إذا سلمنا بظرفية عدم انطباق وصف السرقة الموصوفة عليها، وهو ما سارت عليه مجموعة من القرارات اعتبرت أن ولوج الشبابيك الأوتوماتيكية بواسطة بطائق أداء مزيفة وإدخال القن السري وسحب المبالغ المالية جريمة استعمال وثائق معلوميات مع العلم أنها مزيفة طبقا للفصل 7-607 من ق ج، منها قرار عدد 633 وتاريخ 26-06-2006 ملف عدد 461-05-22 وقرار عدد 364 وتاريخ 17-04-2006 ملف رقم 740-05-22 وقرار عدد 721 وتاريخ 12-09-2006 ملف عدد 600-06-22، الذي اعتبر أفعال المتهم سرقة عادية وليست موصوفة وعدم مؤاخذته من أجل تكوين عصابة إجرامية، ومؤاخذته من أجل تزوير وثائق المعلوميات، والولوج إلى أنظمة المعالجة الآلية للمعطيات عن طريق الاحتيال، وبالتالي فلا مجال للحديث عن جريمة تكوين عصابة إجرامية في الجريمة المعلوماتية على الأقل عندما ترتبط هذه الجريمة بتزوير بطائق الائتمان، وكل القرارات تقريبا ذهبت في نفس الاتجاه بانتفاء جناية تكوين عصابة إجرامية.

الفقرة الثالثة: التحايل في الاستيلاء على مال الغير

إذا كانت بطائق الائتمان تستلزم وجوب حمايتها جنائيا للحيلولة دون وقوع اعتداء عليها، خصوصا أنها تشكل جانبا من المعاملات المالية والتجارية في الوقت الحالي فهل من المتصور أن تكون محلا لجريمة النصب؟

في هذا الصدد، ذهبت محكمة الاستئناف بالرباط في أحد قراراتها إلى أن استعمال المتهمين لأرقام بطائق ائتمانية خاصة بأشخاص آخرين في اقتناء مشتريات عن طريق الإنترنت لا يمكن تكييفه نصبا معللة قراراها كالتالي "...أما جنحة النصب فإن التكييف الذي أعطي لهذه القضية لا ينطبق عليها، وذلك لأن هذه الجريمة يجب أن تتركب وفق ما هو محرر في الفصل 540 من ق ج، ذلك أن المتهمين جميعهم لم يكن لهم أي اتصال مباشر مع الضحايا الذين ارتكبت في حقهم هذه الأفعال ولا معرفة للمتهمين بهم، وكذا الشأن بالنسبة للضحايا، إذ أن القانون الجنائي في الفصل 540 منه، يستدعي بالضرورة أن يقدم الضحية على ارتكاب أفعال معينة تحت تأثير وسائل أو ادعاءات أو غيرها من المسائل المحصورة في الفصل المذكور يقوم الفاعل فينال من ضحيته ويترتب على ذلك ضرر بالضحية، أما وأن تشتغل مصالح هذا الأخير بوسائل تقنية كأرقام البطائق الائتمانية واستعمالها عبر شبكة الإنترنت والاستيلاء له على أمواله ذلك شيء آخر لا يدخل في إطار جريمة النصب[93].

حقيقة لقد كانت الهيئة المصدرة للقرار موفقة في تكييفها، وعللته تعليلا سليما، فمن المسلم به أن الطرق الاحتيالية يجب أن تقع بين شخصين طبيعيين، فالادعاء الكاذب يفترض علاقة مباشرة بينهما وهو ما لم يتوفر في الواقعة المشار إليها أعلاه ، إذ لا معرفة للمتهمين بالضحايا، كما أن التسليم في جريمة النصب المترتب على الطرق الاحتيالية قوامه وأساسه عنصر الرضا الذي بمقتضاه يقوم المجني عليه بتسليم أمواله

[93]- ملف جنائي عدد 971-04-22 وتاريخ 07-05-2007 ص: 10، تم تأييده استئنافيا بقرار عدد 908 وتاريخ 07-11-2007، ملف عدد 690-07-26، غير منشور.

طواعية واختيارا بناء على ما انخدع به، وهو ما لا يمكن تصوره بالنسبة للضحايا الذين لم يعلموا بوقوع الاعتداء على أموالهم إلا بعد حصوله بالفعل.

لكن في حال استعمال بطاقة الائتمان من قبل شخص غير مالكها بعد قيامه بسرقتها أو تزويرها في إجراء عملية سحب للنقود من الموزع الآلي بالبنك هل يعتبر ذلك نصبا؟ وهل يمكن خداع الجهاز الآلي خصوصا وأنه يشرف عليه مستخدم بالبنك وبالتالي إيقاعه في الغلط، مادام أن ساحب النقود بواسطة البطاقة المسروقة أو المزورة يظهر بمظهر مالكها الشرعي؟

إن استعمال شخص آخر غير مالك البطاقة في الاستيلاء على أموال الجهة المصدرة لها بدون وجه حق لا يسمح بانطباق وصف جريمة النصب على سلوك الجاني في هذه الحالة، وإنما يكون جريمتي سرقة وتزوير، وذلك على أساس أن الجاني قد استولى بدون وجه حق على أموال غير مملوكة له وبدون رضاء حائزها الشرعي، وهو ما يدخل في نطاق جريمة السرقة، كما أنه يكون قد حصل على الأموال عن طريق التلاعب في البيانات المخزنة بالبطاقة مما يعد تزويرا لها، ونكون بصدد تعدد مادي للجرائم شريطة أن يكون تزوير البيانات المعالجة آليا معاقبا عليه بنصوص حديثة.

المطلب الثاني: مدى إعمال القواعد العامة في تزوير المحررات لحماية بطائق الائتمان

تخضع بطاقة الائتمان للتزوير المادي بطرقه وأشكاله المختلفة فقد ينصب التزوير على مجرد التغيير في بيانات البطاقة وقد يشمل تصنيع نماذج لبطائق الائتمان على غرار بطائق صحيحة يتم الحصول عليها بطريقة غير مشروعة أو حتى مشروعة (الفقرة الأولى)، ويبقى الهدف الأساسي للمزور هو الحصول على مال الغير، وفي سبيل تحقيق هذا الهدف يلجأ إلى استعمال البطائق المزورة سواء في سحب النقود أو في الوفاء (الفقرة الثانية).

الفقرة الأولى: تزوير بطائق الائتمان

يعد التزوير في مجال بطائق الائتمان من أخطر طرق الغش نظرا لتزايد استخدامها في عمليات الدفع والوفاء وهو ما جعلها عرضة للمزورين، الأمر الذي تطلب ضرورة حمايتها سواء على مستوى القضاء أو القانون.

في هذا الإطار اعتبرت محكمة الاستئناف بالرباط في قرار لها أن قيام مستخدمين أحدهما بمطعم بالرباط والآخر بمحطة بالخطوط الجوية الجهوية بمطار محمد الخامس الدولي بتمرير البطائق البنكية للزبناء بآلة مخصصة لقرصنة هذه البطائق هو تزوير لها معللة قرارها "إن الوقائع المعروضة التي قام بها المتهمان (ض.ح) و(ك.ح) يستشف منها بأنه كانت لهما نية إجرامية تتضح أساسا في مساعدتهم للمتهمين المساهمين عمدا وعن علم حينما أقدموا على تمرير البطائق البنكية للزبناء في الآلة السوداء التي سلمت لهم ويشكل الفعل المنسوب إليهم من حيث الوصف القانوني للتجريم جرائم تقديم مساعدة لعصابة إجرامية والمشاركة في تزوير بطائق الائتمان طبقا للفصل 357 من ق ج[94]".

كما اعتبرت في قرار آخر: "حيث ثبت للمحكمة من خلال المناقشة الشفوية واعتراف (ن.ح) أمام الضابطة القضائية أن المتهمتين (ن.ح) و(ح.ب) تعترفان بأنهما وبإيعاز من المسمى (م ب) الذي سلمهما آلة TPE لتمرير البطائق البنكية لزبناء نزل...الذي يعملون به وقامتا فعلا بتمرير تلك البطائق المزورة بالآلة المذكورة ولحساب (م ب) مقابل مبالغ مالية كان هذا الأخير سلمها لهما وبالتالي يكون العمل الذي قامت به كل من المتهمتين يشكل جريمة مساعدة عصابة إجرامية والمشاركة في تزوير

[94]- قرار عدد 299 وتاريخ 23-03-2006، ملف عدد 736-05-22، ص: 23، تم تأييده استئنافيا بقرار عدد 943 وتاريخ 20-09-2006، ملف عدد 520-06-26، غير منشور.

بطائق بنكية طبقا للفصلين 357 و 129 ق ج وذلك بعد إعادة التكييف وإدانتهما من أجل ذلك[95].

في حين ذهبت نفس المحكمة في واقعة أخرى مشابهة قام فيها مستخدم بمطعم بأكادير بقرصنة حوالي 150 بطاقة بنكية بتمريرها في الآلة المعدة لهذا الغرض على تكييف الفعل طبقا لمقتضيات ف 360 من ق ج [96]، مما يدعو إلى التساؤل حول أسباب هذا التضارب في مواقف العمل القضائي بخصوص تكييف جرم التزوير لبطائق الائتمان.

قبل مناقشة تزوير بطائق الائتمان طبقا لمقتضيات ف 357 من ق ج لابد من الإشارة إلى أنه من غير المنطقي تطبيق ف 360 على واقعة تزوير هذه البطائق، فالبرجوع إلى مقتضياته نجدها تنص على: "من زيف أو زور أو غير في الرخص أو الشهادات أو الكتيبات أو البطاقات أو النشرات أو التواصيل أو جوازات أو أوامر الخدمة أو أوراق الطريق أو جوازات المرور، أو أي وثيقة أخرى تصدرها الإدارات العامة إثباتا لحق أو هوية أو صفة أو منح ترخيص..."

فالبطائق البنكية لا تعد وثيقة إدارية أو شهادة صادرة عن الإدارات العامة، هي عبارة عن عقد يتعهد بموجبه مصدر البطاقة (المؤسسة البنكية) بفتح اعتماد بمبلغ معين لمصلحة شخص آخر هو حامل البطاقة الذي يستطيع بواسطتها الوفاء بمشترياته لدى المحلات التي ترتبط مع مصدر البطاقة بعقد تتعهد فيه بقبولها الوفاء لمشتريات حاملي البطاقة الصادرة عن الطرف الأول، على أن تتم التسوية النهائية بعد كل مدة محددة أو السحب من الشبابيك الأوتوماتيكية، هذا من الناحية القانونية، أما

[95]– قرار عدد 300 وتاريخ 23-03-2006، ملف عدد 999-05-22، ص: 13، تم تأييده استئنافيا بقرار عدد 1134 وتاريخ 17-11-2006، ملف عدد 499-06-26، غير منشور.

[96]– قرار عدد 37 وتاريخ 16-01-2006 ملف عدد 935-05-22، ص: 09-10، تم تأييده استئنافيا بقرار عدد 884 وتاريخ 11-09-2006، ملف عدد 274-06-26، غير منشور.

من الناحية التقنية فهي عبارة عن بطاقة مصنوعة من البلاستيك تقدمها مؤسسة بنكية لزبون يدعى المنخرط تسمح له حسب طرق تقنية أو أوتوماتيكية خاصة بكل بطاقة، أداء ممونيه أو بسحب الأموال من الشبابيك الأوتوماتيكية.

لذا كان حريا تطبيق مقتضيات ف 7-607 من ق ج لأنه الأجدر بالتطبيق من ف 360.

كما أسلفنا كيفت المحكمة تزوير بطائق الائتمان في القرارين الأولين المستدل بهما طبقا لمقتضيات ف 375 من ق ج، الذي ينص على: "من ارتكب.....تزويرا في محرر تجاري أو بنكي أو حاول ذلك...".

فهل يمكن اعتبار بطائق الائتمان محررا؟

يعرف التزوير بأنه تغيير الحقيقة في محرر بإحدى الطرق التي نص عليها القانون تغييرا من شأنه إحداث ضرر ومقترن بنية استعمال المحرر المزور فيما أعد له[97]، ولجريمة التزوير ركنان مادي ومعنوي:

1. الركن المادي في التزوير: يتطلب لقيامه نشاطا يباشره الجاني يتمثل في تغيير الحقيقة في محرر باستخدام وسيلة من الوسائل التي نص عليها القانون، وأن يكون من شأن التغيير إلحاق ضرر بالغير.

أ- تغيير الحقيقة:

أي استبدالها بما يخالفها، فإذا لم يكن هناك تغيير في الحقيقة لا يقوم التزوير[98]، سواء كان هذا التغيير كليا أو جزئيا، وإذا كان تغيير الحقيقة الجزئي يكفي لقيام التزوير كتغيير بيان من بيانات البطاقة فقط إلا أنه يشترط أن يمس تغيير الحقيقة المركز

[97]- **جميل عبد الباقي الصغير**: "القانون الجنائي والتكنولوجيا الحديثة"، مرجع سابق، ص: 162.

[98]- المرجع السابق، ص: 163.

القانوني للغير دون رضائه، وهذا الغير هنا هو حامل البطاقة، وما يقع فيها من تغيير يتم دون رضائه بالطبع.

ب- المحرر:

لا يعد تغيير الحقيقة تزويرا إلا إذا حصل في محرر، فلا يقوم التزوير بتغيير الحقيقة بالقول أو الفعل، والمحرر هو كل كتابة مقروءة تعبر عن معنى معين سواء أكانت حروفا أو أرقاما أو رموزا، بغض النظر عن اللغة التي كتب بها أو مادة هذا المحرر، وهذا ما يتوفر في بطاقات الوفاء كمحرر يعبر عن معنى معين ويستشف هذا المعنى بالقراءة، كما أن رموزه وعلاماته تتصف بالثبات النسبي، ولا ينفي عن البطاقة وصف المحرر ما يدون على أشرطتها الممغنطة أو داخل دوائرها الإلكترونية من رموز وشفرات طالما يمكن فهم الدلالة الكاملة لهذه الرموز بالاستعانة بقارئ للبطاقات سواء للأشرطة الممغنطة أو لدوائرها[99].

ج- طرق التزوير:

لا يكفي أن يقع تغيير الحقيقة في محرر وإنما يتعين أن يكون هذا التغيير بإحدى الطرق التي نص عليها القانون، ويتعين على محكمة الموضوع أن تبين في حكمها الطريقة التي وقع بها التزوير وإلا كان حكمها قاصر البيان[100].

وتتمثل هذه الطرق في:

- **وضع إمضاءات أو أختام مزورة:** يقوم السارق بالتوقيع على البطاقة الخالية من توقيع حاملها ثم يقوم فيما بعد بنسخ هذا التوقيع على فواتير الشراء لدى التجار، وقد يقوم بوضع أي توقيع من نسج خياله ليسهل عليه نسخه فيما بعد

[99]- **كيلاني عبد الراضي محمود:** مرجع سابق، ص: 107.

[100]- **جميل عبد الباقي الصغير:** "القانون الجنائي والتكنولوجيا الحديثة"، مرجع سابق، ص: 169.

على الفواتير، وهذا التوقيع يختلف عن توقيع الحامل الشرعي وأيضا عن توقيع السارق الذي إذا حصل مع البطاقة على تحقيق شخصية يقلد توقيع الحامل المدون في تحقيق شخصيته على البطاقة ونكون هنا حيال طريقة من طرق التزوير وهي التقليد.

- **تغيير المحررات أو الإمضاءات أو الأختام أو زيادة الكلمات** : قد يقتصر عمل المجرم على تعديل أحد بيانات البطاقة، مثل تعديل تاريخ صلاحيتها المدون بحروف بارزة على وجه البطاقة بإطالة صلاحيتها أو تغيير إسم الحامل.
- **وضع أسماء أشخاص آخرين:** قد يقوم الجاني بوضع إسمه مكان إسم حامل البطاقة الشرعي[101].
- **التقليد:** تدوين الجاني محررا أو جزء منه بخط يشبه خط شخص آخر من أجل نسبته إليه.
- **الاصطناع:** يتحقق بخلق محرر لم يكن له وجود من قبل ونسبته كذبا إلى غير مصدره، والاصطناع يصحب غالبا بطريقة أخرى من طرق التزوير وأكثر ما يكون ذلك بالتوقيع بإمضاء مزور[102].
- **الضرر:** يعد عنصرا جوهريا في جريمة التزوير ولا تقوم بدونه ولا يشترط القانون وقوع ضرر بالفعل بل يكتفي باحتمال وقوعه [103]، ويستوي لقيام التزوير أن يكون الضرر ماديا أو أدبيا فرديا أو جماعيا، فالضرر في تزوير بطاقات الائتمان هو ضرر مادي لحامل البطاقة من جراء ما يصيبه في ذمته المالية من وراء استعمال البطاقة للوفاء أو لسحب النقود، وهو أيضا ضرر اجتماعي

[101]– **كيلاني عبد الراضي محمود:** مرجع سابق، ص: 110–111–112.

[102]– **جميل عبد الباقي الصغير:** "القانون الجنائي والتكنولوجيا الحديثة"، مرجع سابق، ص: 174.

[103]– المرجع السابق، ص: 175.

مادي وأدبي لما يصيب المجتمع من اهتزاز الثقة في المعاملات، لاسيما إذا انصبت عمليات التزوير على عدد كبير من البطائق عن طريق التقليد مما قد يؤثر على التعامل بالبطائق البنكية ويصيبها بالشلل التام.

2. الركن المعنوي في التزوير: قوامه القصد الجنائي الذي ينحصر في أمرين ، قصد عام يتمثل في علم الجاني بعناصر الركن المادي، وذلك بأن يدرك أنه يغير الحقيقة في محرر بإحدى الطرق المنصوص عليها في القانون وأن من شأن هذا التغيير حصول ضرر، وأن يقترن هذا العلم بنية الغش أي نية استعمال المحرر المزور فيما زور من أجله وهو القصد الخاص[104].

الفقرة الثانية: استعمال البطائق المزورة

يهدف المزور من ارتكاب التزوير الإثراء غير المشروع وذلك باستعماله للبطائق المزورة، ويعاقب المزور عن تزويره ولو لم يستعملها ولم يصل بذلك إلى تحقيق مصلحة له، كما يعاقب ولو أصبح استعمال البطاقة المزورة مستحيلا لإلغاء البرمجة الخاصة بها من أجهزة السحب النقدي الآلي أو إدراجها على قائمة المعارضة فلا يقبلها التجار، كما أن عدول المزور عن استعمال البطاقة والاحتفاظ بها فقط لا يحول دون عقابه لأن العدول جاء بعد تمام الجريمة، ويسأل المستعمل عن جريمته ولو كان مرتكب التزوير شخصا آخر لا علاقة له به، فلا يتوقف عقاب المستعمل على عقاب المزور، وتتجدد الجريمة بتجدد الاستعمال إذا تنوعت أغراض الجاني من وفاء التجار إلى سحب النقود إلى غير ذلك، إذ يعد كل فعل من هذه الأفعال مكونا لجريمة استعمال قائمة بذاتها.

ويشترط لقيام جريمة الاستعمال إبراز البطاقة والاحتجاج بها على اعتبار أنها صحيحة وأن مقدمها هو حاملها الشرعي، وتعتبر الجريمة تامة ولو لم يبلغ المستعمل

[104]– المرجع السابق، ص: 176.

النتيجة المرجوة من تقديم البطاقة، فإذا قدمها للتاجر وشك في أمره ولم يقبلها للوفاء أو لم تقدم الآلة النقود فيكون فعل الاستعمال تاما[105].

ختاما يثير تحديد الأساس القانوني لتكييف فعل تزوير البطائق البنكية إشكالات متضاربة بالنظر إلى عدم استقرار العمل القضائي على تكييف موحد في القضايا المعروضة على أنظاره من هذا النوع، ولا يسعنا القول سوى أن ذلك راجع لعدم كفاية النصوص المتعلقة بالتزوير لمواجهة التزوير الذي يقع في مجال المعالجة الآلية للمعلومات، ونجد أن المشرع المغربي عاقب على التزوير الذي يقع في وثائق المعلوميات أيا كان شكلها إذا سبب ذلك ضررا للغير، والعقاب على التزوير يشمل التلاعب في المعطيات الذي يكون الغرض منه الحصول على نتائج حقيقية، وبذلك يكون المشرع المغربي بنصه على تجريم تزوير وثائق المعلوميات وضع حدا للاختلافات القضائية بشأن مدى اعتبار جريمة التزوير واقعة في حالة المعلومات والبيانات المخزنة بطريقة إلكترونية، وهو بذلك سن عقوبة لجريمة تزوير بطائق الائتمان واستعمال بطائق مزورة طبقا للفصل 7-607 من ق ج.

المبحث الثاني: المس بالأنظمة المعلوماتية

إن الاستخدام المتزايد لأساليب المعالجة الآلية للمعلومات ليست له دائما آثار إيجابية إذ برزت على مستوى الواقع أشكال مختلفة للاستعمال التعسفي للأنظمة

[105]- **كيلاني عبد الراضي محمود:** مرجع سابق، ص: 117-118-119.

المعلوماتية جراء الاستخدام السيء للكمبيوتر وشبكة الإنترنت (المطلب الأول)، وأدى إلى الكشف عن مخاطر واعتداءات أصبحت عرضة لها (المطلب الثاني).

المطلب الأول: الاستخدام السيء للكمبيوتر وشبكة الإنترنت

ترتب عن التطور الهائل في مجال تكنولوجيا المعلوميات أن أصبح العالم يعيش حياة زاخرة بالاتصالات السريعة ونقل المعلومات عبر المسافات، وكل هذا ما كان له أن يتحقق إلا بوجود حاسوب مرتبط بشبكة الإنترنت، إلا أن ازدياد العمل بهما أدى إلى نشوء جرائم ماسة بالأشخاص (الفقرة الأولى)، وأخرى ماسة بالمصلحة العامة (الفقرة الثانية).

الفقرة الأولى: الاعتداءات الماسة بالأشخاص

التعدي على الأشخاص ليس وليد الآن بل هو قديم قدم الإنسان، إلا أن الثورة المعاصرة في الاتصالات والخدمات الإلكترونية أتاحت للمجرم المعلوماتي تسخيرها لتحقيق أغلب أشكال الاعتداء على الأشخاص بأبسط الأساليب من خلال التلاعب بالبرامج أو برمجة البيانات عن بعد بالضغط على زر واحد [106]، ومن أهم الاعتداءات على الأشخاص عبر الإنترنت، جرائم الأخلاق وجرائم الاعتداء على حرمة الحياة الخاصة.

أ -جرائم الأخلاق:

تشمل هذه الطائفة جرائم التحريض على القتل أو الإيذاء والتهديد، وحض وتحريض القصر على إتيان أنشطة جنسية أو غير مشروعة، إفساد القصر والأحداث

[106]– **محمد أمين أحمد الشوابكة:** "جرائم الحاسوب والإنترنت"، دار الثقافة، عمان، الطبعة الأولى 2004، ص: 28.

بأنشطة جنسية عبر الإنترنت واستخدام هذا الأخير في ترويج الدعارة وممارسة الفجور[107].

إلى جانب هذه الجرائم، هناك جرائم القذف والسب والتشهير والابتزاز التي تعد أكثر الجرائم شيوعا في نطاق شبكة الإنترنت وإن كانت تقليدية إلا أن وقوعها بواسطة هذه الشبكة جعلها تصنف ضمن الجرائم المستحدثة، وتتنوع صور القذف والسب عبر شبكة الإنترنت بتنوع الغرض منها، وغالبا ما يرتكب من خلال إسناد مادة كتابية أو صوتية أو فيديو صوتية تسيء إلى أحد الأشخاص من شأنها أن تنال من شرفه أو كرامته أو تعرضه إلى بغض الناس واحتقارهم.

أما بالنسبة للتشهير فهو الآخر نوع من أنواع القذف، وهو عبارة عن تشويه أو تهديد لسمعة شخص ما بهدف التقليل من قدره في نظر المجتمع والناس أيا كانت نوعية هذه العلاقة[108] أو لابتزازه وبالتالي رضوخه، ومن الأمثلة على ذلك ما قام به مواطن مغربي تمكن من نسخ ومسح محتوى وحدة تخزين المعلومات الخاصة بجهاز مواطن سعودي تعرف عليه عبر موقع في شبكة الإنترنت خاص بالصداقة، وبعد اطلاعه عليه تبين بأنه يحتوي على مجموعة من الصور وتسجيلات بالفيديو لمجموعة من الفتيات المغربيات في وضعية مخلة بالآداب والأخلاق إضافة إلى الأرقام الهاتفية الخاصة بهن، وبعد أن حصل على هذه المعلومات قام بابتزازهن انطلاقا مما حصل عليه من المواطن السعودي، وبدأ يطلب منهن إمداده بمبالغ مالية مقابل سكوته وعدم تشويه سمعتهن عن طريق التشهير بهن عبر شبكة الإنترنت، كما تمكن من خلال مراسلته عبر هذه الشبكة مع العديد من الفتيات بصفته مواطنا لبنانيا

---

[107]– **المواجهة التشريعية للجرائم المتصلة بالكمبيوتر** : ورقة عمل مقدمة من النيابة العامة بمملكة البحرين في إطار الندوة الإقليمية لبرنامج الأمم المتحدة الإنمائي التي أقيمت بالدار البيضاء أيام 19–20 يونيو 2007، غير منشورة.

[108]– **نبيلة هبة هروال:** مرجع سابق، ص: 64–65–66.

من تسجيل عدة فتيات في وضعية منافية للأخلاق وأصبح يستعمل تلك الصور في ابتزازهن[109].

ب – جرائم الاعتداء على حرمة الحياة الخاصة:

حظيت الحياة الخاصة للأفراد بحماية دستورية وقانونية في مختلف تشريعات الدول المتقدمة ولقد لعبت الثورة المعلوماتية وما نتج عنها من تطور تكنولوجي دورا بارزا في تأثيراتها على الحق في الخصوصية بأطوار وأشكال مختلفة، إذ أصبحت تلك الأخيرة تعرف ببنك المعلومات [110]، لكنها في نفس الوقت أصبحت مهددة بالعديد من الانتهاكات والاعتداءات منها:

- استعمال بيانات شخصية غير حقيقية ويتم ذلك سواء بالمحو أو التلاعب في بيانات شخصية من طرف أفراد غير مرخص لهم بالاطلاع أو استعمال هذه البيانات، أو من خلال استعمال بيانات شخصية غير حقيقية من طرف المسموح لهم قانونيا بذلك.
- جمع أو معالجة بيانات حقيقية بدون ترخيص وذلك من طرف جهات غير مسموح لهم بذلك باستعمال أساليب غير مشروعة.
- إنشاء بيانات بصورة غير قانونية وإساءة استعمالها، فقد يتم إنشاء أو إساءة استخدام البيانات المجمعة بصورة مشروعة من قبل القائمين بها[111].

الفقرة الثانية: الجرائم الماسة بالمصلحة العامة

---

[109]– ملف جنحي تلبسي رقم 07/7794 وتاريخ 06–02–2008، تحت عدد 037 صادر عن ابتدائية الدار البيضاء، ص: 1–2، (غير منشور).

[110]– يقصد ببنك المعلومات: تكوين قاعدة بيانات تفيد موضوعا معينا وتهدف لخدمة غرض معين، ومعالجتها بواسطة أجهزة الحاسبات الإلكترونية لإخراجها في صورة معلومات تفيد مستخدمين مختلفين في أغراض متعددة، يراجع: **نبيلة هبة هروال**، مرجع سابق، ص: 71.

[111]– **عفيفي عفيفي كامل:** مرجع سابق، ص: 275 إلى 282.

تتعدد صور الأفعال الإجرامية المتصلة بالكمبيوتر وشبكة الإنترنت التي تستهدف المصلحة العامة، فقد يتم استخدامها في لفظ ونقل وتبادل معلومات وبيانات تتعلق بنشاط إرهابي أو بالعناصر البشرية القائمة عليها أو بمخططاتهم ووسائلهم، ومن ذلك قيام جماعات إرهابية بإنشاء مواقع تتضمن أبوابا دعوية لما تعتنقه من أفكار متطرفة وأخرى استراتيجية تتضمن الخطط والأهداف وتوجيه عناصرها البشرية سواء من خلال تلك المواقع أو بواسطة البريد الإلكتروني[112]، كما استعملت هذه التقنية كذلك استعمالا واسع النطاق من قبل عناصر العصابات المنظمة في تخطيط وتمرير وتوجيه المخططات الإجرامية وتنفيذ وتوجيه العمليات الإجرامية بيسر وسهولة سواء في غسل الأموال غير المشروعة [113] بالنظر للتسهيلات التي منحتها لهم شبكة الإنترنت، منها السرعة الشديدة وتخطي الحواجز الحدودية بين الدول وتفادي القوانين التي قد تضعها بعض الدول وتعيق نشاطهم وكذلك تشفير عملياتهم مما قد يعطيها قدرا كبيرا من السرية[114]، أو في تجارة المخدرات فقد أضحت الإنترنت قناة اتصالية ممتازة ومجالا رحبا للتعامل غير المشروع لمستهلكي المخدرات والمؤثرات العقلية بشكل أكثر أمنا للمروج والمدمن أو المعتمد على المخدرات والمؤثرات العقلية، بل أكثر من ذلك أصبحت هناك مواقع تبين وتشرح التدريب على زراعة المخدرات وطرق وعمليات تحويلها وكذلك كيفية التعاطي لأول مرة[115].

فمن شأن الاستغلال السيء للأنظمة المعلوماتية هز استقرار الأمن بالدولة وزعزعة الاقتصاد الوطني والإضرار بالمواطنين وسلامتهم.

---

[112]– المواجهة التشريعية للجرائم المتصلة بالكمبيوتر: مرجع سابق.

[113]– غسل الأموال عبارة عن معالجة لمصدر الدخل الأول أو الأساسي غير المشروع والناجم عن الجريمة بالقيام بمجموعة تحركات اقتصادية مشروعة تؤدي إلى طبع مصدر الأموال غير المشروع بطابع المشروعية وبطريقة لا يمكن بمقتضاها التعرف على المصدر الأصلي (غير المشروع).

[114]– **محمد محمد الألفي:** مرجع سابق، ص: 53.

[115]– **نبيلة هبة هروال:** مرجع سابق، ص: 76.

إلا أن المعلوماتية لا تكون فقط أداة ووسيلة للاعتداء فقد تكون أيضا موضوعا له.

المطلب الثاني: صور الاعتداء على الأنظمة المعلوماتية

مما لا ريب فيه أن التطور التكنولوجي سهل الكثير من الخدمات على الأفراد بالنظر للتقدم السريع الذي عرفته النظم المعلوماتية، إلا أنه أدى بالمقابل إلى تعرضها لأضرار مختلفة نتيجة الاعتداءات الجرمية التي تطالها والتي قد تأخذ شكل اعتداءات منطقية (الفقرة الأولى)، أو تأتي في صورة اعتداءات مادية (الفقرة الثانية).

الفقرة الأولى: الاعتداءات المنطقية

تشمل الاعتداءات المنطقية أنواعا عديدة إلا أنه سنكتفي بتعداد بعضها:

- **جرائم مهاجمة الشبكة المعلوماتية** : تعتبر من أخطر الجرائم التي تهدد الحواسيب والإنترنت ويلحق بها خسائر كبيرة [116]، ويتم ذلك عن طريق الفيروسات التي تعد برنامجا معلوماتيا يتضمن أهدافا تدميرية لأنظمة المعلومات[117] وأكبر دليل على ذلك المشاكل التقنية التي خلقها فيروس زوطوب للعديد من الأنظمة المعلوماتية الأمريكية الذي عدله المغربي (ف.ص)[118].
- **القناة المخفية:** وهو نوع خطر من الاعتداءات يقوم على مبدأ تهريب المعلومات عبر خرق سياسة الأمن والحماية المعتمدة في الأنظمة المعلوماتية، وتتطلب ذكاء فائقا من المعتدي[119].

---

[116]– المرجع سابق، ص: 57.

[117]– وليد عاكوم: "التحقيق في جرائم الحاسوب"، مقال منشور بالدليل الإلكتروني www.arablaw info.com تاريخ ولوج الموقع يوم السبت 2008/11/22 على الساعة الثالثة زوالا، ص: 3.

[118]– قرار عدد 721 وتاريخ 12–09–2006، ملف عدد 22/06/600، ص: 3–4–5، مشار إليه سابقا.

[119]– **نبيلة هبة هروال:** مرجع سابق، ص: 60.

- **انتحال شخصية الأفراد:** المقصود بانتحال الشخصية ما يعمد إليه المجرم من استخدام شخصية شخص آخر للاستفادة من سمعته أو ماله أو صلاحياته، ومنتحل الشخصية يمكنه استخدام بعض المعلومات التي يمكن الحصول عليها بسهولة من الإنترنت [120] ومن الأمثلة على ذلك انتحال شخص يدعى (ف.م) صفة شخصية سامية بالبلاد بعدما تمكن من الدخول إلى الموقع الإلكتروني "Face Book".

وهو موقع خاص بالتعارف عبر الإنترنت وعمل على إنشاء عنوان إلكتروني منتحلا اسم هذه الشخصية وأرسل رسائل إلكترونية إلى المنخرطين بهذا الموقع بعد أن خلق بطاقة شخصية، ودون بها مجموعة من المعلومات الشخصية الخاصة بها أخذها من موقع "wiki pedia. org" وأرفقها بصورة فوتوغرافية لها حصل عليها من محرك البحث " google"، وكان هدفه من انتحال تلك الشخصية إنشاء علاقات مع الفتيات[121].

بالإضافة إلى انتحال شخصية الأفراد يمكن انتحال شخصية الموقع بمعنى أنه باستطاعة بعض الأشخاص الدخول على موقع ما بغرض حجبه وتفسيره ووضع الموقع الخاص بهم[122].

الفقرة الثانية: الاعتداءات المادية

تعتبر هذه الاعتداءات النوع الثاني من الجرائم التي تكون شبكة المعلوميات محلا لها وتشمل:

---

[120]– **حسن طاهر داود:** مرجع سابق، ص: 84.

[121]– ملف جنحي تلبسي رقم 08/1189 وتاريخ 22-02-2008، صادر عن ابتدائية الدار البيضاء، (غير منشور).

[122]– **نبيلة هبة هروال:** مرجع سابق، ص: 61.

- **الاعتراض المتعمد للبيانات:** يقصد به رصد إشارات إلكترومغناطيسية في الأنظمة المعلوماتية وتحليلها بهدف استرجاع المعلومات المفهومة أو المقروءة منها.
- **التشويش:** يهدف هذا النوع من الاعتداء إلى إعاقة المستوى التشغيلي للأنظمة المعلوماتية وجعلها عاجزة عن العمل.
- **الاكتساح والتفخيخ:** يقصد بالاعتداء الأول منهما إرسال حزمة من المعلومات إلى الشبكة للتوصل إلى تحديد أي من هذه المعلومات هي الصحيحة، أما الاعتداء الثاني فيقصد به إدخال وظائف خفية في مرحلة تصميم أو تصنيع أو نقل أو صيانة النظام المعلوماتي[123].
- **التنصت:** يقوم على التمركز في موقع معين داخل شبكة الاتصالات وتسجيل وحفظ البيانات المتبادلة فيما بين الأنظمة المعلوماتية.

ويضاف إلى هذه الاعتداءات التي لا يمكن تعدادها وحصرها جريمة الاحتيال المعلوماتي، وهي تقوم على اتباع سلوك احتيالي أو خداعي مرتبط بالكمبيوتر يهدف شخص بواسطته إلى كسب فائدة أو مصلحة مالية[124]، ومن ذلك ولوج أحد الأشخاص لشبكة الإنترنت باستعمال الأمن الإلكتروني IP الخاص بالولايات المتحدة الأمريكية كما لو يقطن بها، وقام بالتنقيب على استمارة الزبناء المملوكة لدى الأبناك المتواجدة بها ومن بينها بايبال وإيبال وإيباي ورجيون وقام بتوزيعها لدى جميع المنخرطين بشبكة الإنترنت وطلب منهم ملأها بجميع المعلومات الخاصة بهم للحفاظ على التدابير الأمنية لهم وبعثها له، وعندما توصل صندوق الرسائل الإلكترونية الخاص به بتلك المعلومات شرع في تخزينها بالحاسوب ثم تحول إلى بطائق الشبابيك البنكية بعدما

---

[123]– المرجع السابق، ص: 62.

[124]– **وليد عاكوم:** مرجع سابق، ص: 5.

يحتفظ برقم القن السري بكل واحدة على حدة ويتوجه إلى أي مؤسسة بنكية بأرض الوطن وبواسطة البطائق والقن السري يقوم بسحب المبالغ المالية[125].

[125]– قرار عدد 633 وتاريخ 26–06–2006، ملف عدد 22/05/461، ص: 3، مشار إليه سابقا.

الفصل الثاني:
أوجه التصدي للجرائم الناشئة عن استخدام المعلوميات

الفصل الثاني:
أوجه التصدي للجرائم الناشئة عن استخدام المعلوميات

ساهمت وسائل الاتصال الحديثة في تطوير نظم المعلوميات بشكل ملحوظ، مما جعل العصر الحالي عهد تقنية المعلوميات بامتياز، لاعتماده على المعطيات إما بذاتها أو بما تمثله هذه المعطيات التي تكون مخزنة داخل النظام المعلوماتي أو تكون في طور النقل والتبادل ضمن شبكات الاتصال، الأمر الذي جعل النشاط المعلوماتي

عرضة لمجموعة من المخاطر والاعتداءات التي استوجبت ضرورة التصدي لها من خلال تجريم المس بنظم المعلوميات (الفرع الأول)، مع إيلاء الاهتمام بسبل الحماية من الجرائم الناجمة عنها (الفرع الثاني).

الفرع الأول: تجريم المس بنظم المعلوميات

إن الآثار الخطيرة والمدمرة التي تمس نظام المعالجة الآلية للمعطيات هي التي فرضت وجوب التفكير في حمايتها تشريعيا، وإن خلقت إشكالات بخصوص قدرة القواعد العامة للقانون الجنائي المتعلقة بالأموال على استيعاب وزجر هذه النوعية من الأفعال الإجرامية بصورة فعالة (المبحث الأول)، أم يتعين إنشاء قواعد خاصة تناسب خطورة هذه الأفعال (المبحث الثاني).

المبحث الأول: الجريمة المعلوماتية والتكييف الكلاسيكي

مهما يكن فإن تجريم الاعتداءات التي تتعلق بنظم المعالجة الآلية للمعطيات اعتمادا على النصوص التقليدية يتوقف على إمكانية دخول البرامج والمعلومات المعالجة في إطار الحماية التي تقررها هذه النصوص، سواء منها المتعلقة بالسرقة (المطلب الأول)، أو تلك الخاصة بالنصب وخيانة الأمانة (المطلب الثاني).

المطلب الأول: مدى إمكانية تطبيق نصوص السرقة على نظم المعالجة الآلية للمعطيات

استقر الفقه على تعريف جريمة السرقة بأنها "اختلاس مال منقول مملوك للغير بنية تملكه[126]"، من خلال هذا التعريف يتضح أن أركان جريمة السرقة تتمثل في ركن مادي هو فعل الاختلاس ومحل للجريمة مال منقول مملوك للغير، وركن معنوي القصد الجنائي.

وبالتالي فإن الأمر يقتضي معرفة مدى خضوع المعلومات كمضمون لقواعد البيانات أو المعطيات لجريمة السرقة (الفقرة الأولى)، ثم أن تكون قابلة لوقوع الاختلاس عليها (الفقرة الثاني).

الفقرة الأولى: المعلومات كمحل لجريمة السرقة

تباينت الآراء بشأن إمكانية تطبيق القواعد العامة التقليدية للقانون الجنائي بما فيها أحكام الجرائم ضد الأموال على الجرائم المعلوماتية، كسرقة المعطيات أو المعلومات أو تحويلها وسحب الأموال المودعة في الحسابات البنكية عن طريق التعسف في استعمال البطاقة المغناطيسية وتدمير البرامج المعلوماتية [127]، وقد تم تبني عدة مواقف في هذا الصدد يمكن إجمالها في ثلاث اتجاهات:

اتجاه أول يرى مناصروه أنه من الصعب تطبيق القواعد التقليدية للقانون الجنائي على الجرائم المعلوماتية المستحدثة، على اعتبار أن القصد من أحكام الجرائم التقليدية ضد الأموال هو حماية الأفعال المادية، في حين أن المعلومات تشكل أموالا غير مادية، بل إن المعلومة حالة نادرة في الاقتصاد بحيث لا تفقد قيمتها نتيجة

[126]– **محمد علي العريان:** "الجرائم المعلوماتية"، دار الجامعة الجديدة للنشر، الإسكندرية، طبعة 2004، ص: 107.

[127]– **عبد الكريم غالي:** "قانون المعلوميات، الحماية القانونية للإنسان من مخاطر المعلوميات"، مرجع سابق، ص: 76–77.

استعمالها[128]، وحسب هذا الاتجاه فإن القانون الجنائي لا يتوفر إلا على قواعد تقليدية بالية في الجريمة والعقاب أصبحت متجاوزة وغير متناسبة وخصوصيات الجريمة المعلوماتية ولا تتلاءم مع سائر مظاهر المعلوميات، ورغم الطابع العام لمبدأ شرعية التجريم والعقاب فإن هذا القانون أصبح متجاوزا[129]، وبالتالي فمع غياب النص القانوني لا يمكن المعاقبة على الجرائم المعلوماتية، كما أن الاستناد إلى بعض مقتضيات القانون الجنائي كتلك المتعلقة بالسرقة مثلا حسب الفصلين 505 و 521 المتعلق باختلاس التيار الكهربائي أو أي طائفة أخرى كانت ذات قيمة اقتصادية يتطلب توفر شروط صارمة تقتضي أن يكون المال المختلس شيئا ماديا وهو ما لا يتوفر في المعلومات، كما أن الكهرباء أو أي طائفة أخرى لا يقارن مع المعلوميات ولا بالمعلومة المعالجة[130]، مما يستوجب تدخل المشرع بقواعد تجريمية جديدة [131] تتناسب وخطورة هذه الأفعال الضارة حيث يظهر أنه من الصعب تطبيق القواعد التقليدية للقانون الجنائي على سائر مظاهر الاعتداءات التي تمس المعلوماتية، لذلك فإن تأويل النصوص التقليدية كتلك الخاصة بالسرقة لاحتواء الجرائم المعلوماتية كسرقة المعلومات عبر شبكات الاتصال مرفوض وذلك احتراما لمبدأ التجريم والعقاب[132].

---

[128]– **عبد الكريم غالي:** "المعلوميات القانونية"، خصوصياتها ومدى تطبيقها في المغرب، رسالة لنيل دبلوم الدراسات العليا في القانون الخاص، جامعة محمد الخامس، كلية العلوم القانونية والاقتصادية والاجتماعية بالرباط، السنة الجامعية 1989/1988، ص: 174.

[129] - **Tazi Sadeq Houria** : l'ordinateur, le fraudeur et le juge (observations à propos de l'affaire des manipulations télé phoniques), in revue marocaine de droit de l'économie du développement n° 11-1986 colloque « droit et informatique » Casablanca du 18 au 20 avril 1985, p : 63-64-66-67.

[130]– **عبد الكريم غالي:** محاور في المعلوميات والقانون، البوكيلي للطباعة والنشر والتوزيع، القنيطرة، الطبعة الأولى، 1997 ص: 230–231.

[131]– **بشرى النية:** "حماية برامج الحاسوب عن طريق قواعد القانون الجنائي"، حماية للمصالح الخاصة والنظام العام، المجلة المغربية لقانون الأعمال والمقاولات، العدد 7 يناير 2005، ص: 61.

[132]– **عبد الكريم غالي:** محاور في المعلوميات والقانون، مرجع سابق، ص: 231–232.

فيما ذهب اتجاه ثان إلى أن الأفعال الإجرامية المرتبطة بالمعلوميات أو التيليماتيكا لا تتطلب بالضرورة وجود نصوص خاصة لتجريمها، وإنما يتعين على القضاء اللجوء إلى تأويل النصوص القائمة شريطة أن يكون على معرفة مسبقة بالمبادئ الأولية للوظائف التقنية والعلمية للوسائل المعلوماتية، وذلك درءا للمخاطر التي تشكلها الجرائم المعلوماتية الحديثة على النظام العام بشكل يفوق ضرر الجرائم التقليدية[133].

أما الاتجاه الثالث فينحو أصحابه إلى إمكانية معالجة الجرائم المعلوماتية عن طريق تأويل القواعد الجنائية العامة المتعلقة بالجرائم التقليدية ضد الأموال أو إقرار جرائم جديدة مع تجنب الاصطدام مع مبدأ شرعية الجرائم[134].

وبالرجوع إلى بعض القضايا التي عرضت على القضاء قبل صدور نصوص خاصة لتجريم هذا النوع من الجرائم نلاحظ أن القضاء لم يستقر على اتجاه واحد، إذ استبعد إثر نظره في إحدى القضايا التفسير الواسع للمقتضيات التقليدية للقانون الجنائي والتي يصعب تطبيقها على الحالات والأفعال الإجرامية التي تتولد عن استخدام التقنيات الحديثة، فقد قضى بتبرئة ساحة بعض المتهمين المتابعين من أجل جريمة السرقة وهم مستخدمين بالمكتب الوطني للبريد والمواصلات السلكية واللاسلكية قاموا بتسهيل تحويلات هاتفية لفائدة بعض المشتركين بصورة غير مشروعة، وتمت متابعتهم بمقتضى الفصول 505 و 241 و 248 و 251 و 129 من القانون الجنائي، وأدينوا ابتدائيا وتمت تبرئتهم استئنافيا[135].

---

[133] - **Elhadi Chaibainou** : Revue « informatique juridique et droit de l'informatique » n° 3, casablanca, 1990, p : 41.

[134] - **Mohieddine Amzazi** : « informatique et droit pénal », in revue marocaine de droit de l'économie du développement, op.cit, p : 56.

[135]– ملف جنحي تلبسي عدد 73831/85 وتاريخ 13–11–1985 صادر عن ابتدائية البيضاء أنفا، مشار إليه عند: **الشرقاوي الغزواني نور الدين** : قانون المعلوميات، مطبعة print diffusion، سلا، الطبعة الأولى 1999، ص: 114.

كما اعتبرت الغرفة الجنائية بمحكمة الاستئناف بالدار البيضاء أن الناظمة الآلية (الحاسوب) بمثابة سجل رسمي للإدارة، ذلك أن موظفا بإدارة الجمارك أقر بأنه بتاريخ 1998/05/18 قام باستعمال رمزه السري للولوج إلى قاعدة البيانات المضمنة بالحاسوب لإدارة الجمارك وسجل بها معلومات مخالفة للحقيقة فتمت متابعته من أجل جنحة التزوير في وثيقة إدارية والمشاركة طبقا لمقتضيات الفصول 129 و360 و361 من القانون الجنائي [136]، وما ذهب إليه القضاء يبرز أنه عند الإحالة على المفاهيم التقليدية يتضح عدم قابلية القانون الجنائي للتكييف مع ظاهرة المعلوميات[137].

الفقرة الثانية: المعلومات كموضوع للاختلاس

يعرف الاختلاس بأنه نقل الشيء من حيازة المجني عليه وهو الحائز الشرعي له إلى حيازة الجاني بغير علم المجني عليه أو على غير رضاه [138]، ويستوي في فعل الاختلاس أن يكون الجاني قد استولى على المال خلسة أو عنوة أو تسلمه بناء على يد عارضة فغير نيته واستولى عليه [139]، ويقتضي الاختلاس السيطرة الكاملة للجاني على المال المختلس مما يفترض وقوع هذا الأخير تحت سيطرة واحدة أو حيازة واحدة، وقد تباينت الآراء بخصوص كون الحصول غير المشروع على المعلومات اختلاس أم لا، فهناك من يرى صعوبة التسليم "بالاختلاس المعلوماتي" على اعتبار أن الأمر يتعلق بخدمات وليس بأموال في الحالة التي تكون فيها المعلومات غير محمولة على

---

[136]– قرار عدد 368 وتاريخ 07–04–2000 الملفين الضمومين عدد 410 و99/05/298، مشار إليه عند **صالح خالد:** "جرائم الاتصال الإلكتروني بين التشريع والقضاء"، مجلة المحاكم المغربية عدد 96 شتنبر–أكتوبر 2002.

[137]– **عبد الكريم غالي:** "محاور في المعلوميات والقانون"، مرجع سابق، ص: 230.

[138]– **محمد علي العريان:** مرجع سابق، ص: 107 و108.

[139]– **عبد الفتاح بيومي حجازي** : "الحماية الجنائية لنظام التجارة الإلكترونية"، دار الفكر الجامعي الإسكندرية، ص: 193.

دعامة مادية، وبالتالي انتفاء صفة المنقول عن المعلومات ولو توفرت الحيازة لها من طرف ناشرها الذي قد يسيطر عليها ويشترط للحصول عليها استعمال كلمة سر[140].

فيما ذهب آخرون إلى إمكانية تطبيق أحكام السرقة على اختلاس المعلومات على اعتبار أن الركن المادي لجريمة السرقة يتمثل في فعل الاختلاس الذي يتكون من عنصرين، الأول موضوعي يتمثل في النشاط الإرادي المنتج للاختلاس، فالجاني يمكنه أن يستحوذ على المعلومة بسهولة عبر شبكات الاتصال وبمجرد استحواذه عليها بطريق غير مشروع يتحقق الاختلاس، والحيازة هنا حيازة فكرية وليست مادية، أما العنصر الثاني فهو شخصي ويتجلى في نية الجاني في تملك الشيء وحيازته ويتحقق في الاختلاس المعلوماتي حتى في حالة رضا مالك المعلومات بنقلها لكن على سبيل اليد العارضة وهو ما لا ينفي الاختلاس [141]، ويرى أنصار هذا الرأي أنه يمكن تكييف الحصول غير المشروع على المعلومات اختلاسا وذلك بإدخالها في عداد سرقة المنفعة[142].

من هنا يظهر أن جريمة السرقة لا يمكن إسقاطها على سرقة المعلوميات إلا في حالات محدودة جدا تتمثل في الجانب المادي للمعلوميات لأن تنظيم جريمة السرقة في القانون الجنائي جاء ليحمي الأموال المنقولة المادية.

المطلب الثاني: مدى صلاحية نظم المعالجة الآلية للمعطيات أن تكون محلا للنصب أو خيانة الأمانة

أدى استعمال الأجهزة الإلكترونية بكل مكوناتها في الإدارات والمؤسسات العامة والخاصة في كل القطاعات ومنها البنوك والشركات إلى استخدام الحاسب الآلي من طرف الجناة في تحويل أرصدة الغير أو فوائدها لحسابهم الخاص أو لحساب شخص

[140]– المرجع السابق، ص: 194 و195.

[141]– المرجع السابق، ص: 193 و194.

[142]– المرجع السابق، ص: 194.

آخر وذلك عن طريق التلاعب بالمعلومات وإدخال بيانات مغلوطة إلى الجهاز، وهو ما يستدعي بحث قابلية البيانات لأن تكون موضوعا للنصب (الفقرة الأولى)، أو خيانة الأمانة (الفقرة الثانية).

الفقرة الأولى: جريمة النصب ونظام المعالجة الآلية للمعطيات

ينص الفصل 540 من القانون الجنائي على أنه "يعد مرتكبا لجريمة النصب ويعاقب بالحبس من سنة إلى خمس سنوات وغرامة من خمسمائة إلى خمسة آلاف درهم، من استعمل الاحتيال ليوقع شخصا في الغلط بتأكيدات خادعة أو إخفاء وقائع أو استغلال ماكر لخطأ وقع فيه غيره ويدفعه بذلك إلى أعمال تمس مصالحه أو مصالح الغير المالية بقصد الحصول على منفعة مالية له أو لشخص آخر...".

اعتمادا على هذا الفصل فإن الركن المادي لجريمة النصب يتمثل في إتيان الجاني لفعل الاحتيال، والمشرع لم يعرفه لكن حصر الوسائل التي يتحقق بها في ثلاث: تأكيدات خادعة، إخفاء وقائع صحيحة، استغلال ماكر لخطأ وقع فيه الغير، وفي تحقق الضرر أو نتيجة تتمثل في دفع المجني عليه لارتكاب أفعال تمس بمصالحه أو مصالح غيره المالية، بغض النظر عما إذا كان الجاني قد تسلم المال بالفعل من طرف المجني عليه أو لم يحصل على ذلك، أما الركن المعنوي فيتطلب توفر القصد الجنائي لدى الجاني وذلك بأن يكون عالما بأنه يستعمل وسائل احتيالية لإيقاع المجني عليه في الغلط الذي مس مصالحه أو مصالح غيره مع اتجاه نية الجاني إلى تحقيق منفعة مالية له أو لغيره.

فإلى أي حد يمكن تصور تحقق جريمة النصب المعلوماتي في حالة الاحتيال على الحاسب الآلي وإيقاعه في الغلط للاستيلاء على البيانات المخزنة به خاصة تلك المتعلقة بالذمة المالية للمتعاملين مع الهيئات المستخدمة للحاسوب؟

لقد انقسمت الآراء بهذا الخصوص إلى ثلاث اتجاهات، الأول يرى أن جريمة النصب لا تقوم إلا إذا خدع الجاني شخصا آخر مثله وأن يكون الشخص المخدوع مكلفا بمراقبة البيانات، وعلى ذلك لا يتصور خداع الحاسب الآلي بوصفه آلة ومن تم لا يطبق النص الجنائي الخاص بالنصب والاحتيال لافتقاده أحد العناصر اللازمة لتطبيقه[143].

في حين يرى اتجاه ثان إمكانية وقوع فعل الاحتيال على نظام الحاسب الآلي وإيقاعه في الغلط بقصد سلب المال، لأن هذا الفعل تتوفر فيه الطرق الاحتيالية بمفهومها المستقر ككذب تدعمه أعمال مادية أو وقائع خارجية هي إبراز أو تقديم المستندات أو المعلومات المدخلة إلى الحاسوب، كما تتحقق هذه الطرق كذلك باستخدام المستندات غير الصحيحة التي يخرجها الحاسوب بناء على ما وقع في برامجه أو في البيانات المخزنة داخله من التلاعب كمن يستولي على أموال لا حق له فيها[144].

ومن جهة أخرى، أدرج الاتجاه الثالث الاحتيال الواقع على الحاسب الآلي ضمن القوانين الخاصة بالبريد والاتصالات وبالاحتيال على البنوك والاتفاق الإجرامي بغرض ارتكاب الغش والاحتيال[145].

أما فيما يتعلق بالاستيلاء على مال الغير يتعين أن يترتب على أفعال الاحتيال قيام الجاني بالاستيلاء على أموال الغير دون وجه حق وذلك باستخدام الحاسب الآلي

---

[143]– **محمد سامي الشوا:** مرجع سابق، ص: 132.

[144]– **عفيفي كامل عفيفي:** مرجع سابق، ص: 172.

[145]– **محمد علي العريان:** مرجع سابق، ص: 127.

بوصفه أداة إيجابية في هذا الاستيلاء، ذلك أن الحاسوب يعد أداة إيجابية في جريمة النصب المعلوماتي متى تم التدخل مباشرة في المعطيات بإدخال معلومات وهمية أو بتعديل البرامج أو خلق برامج صورية، وليس هناك صعوبة في اكتشاف الطرق الاحتيالية في هذه الحالات [146]، علما أنه يلزم أن تتوفر علاقة السببية في جريمة النصب بما فيها النصب المعلوماتي ما بين فعل الاحتيال والنتيجة المتمثلة في تسليم المال[147]، وهو ما ذهب إليه القضاء المغربي في واقعة قام فيها أحد المتهمين بالتنقيب على استمارة الزبناء المملوكة لدى الأبناك المتواجدة بالولايات المتحدة وطلب منهم ملأها بالمعلومات الخاصة بهم حفاظا على التدابير الأمنية لهم وبعثها له، وبعدها قام بتخزين المعلومات بالحاسوب وشرع في سحب أموالهم من الشبابيك البنكية بناء على تلك المعلومات، إذ اعتبرت المحكمة أن فعله يشكل نصبا معللة قرارها بـ: حيث أسفرت المعاينة التقنية التي تم إجراؤها بمصلحة الشرطة عن أن المتهم ومشاركيه سواء بالمغرب أو بالخارج يقومون بإنجاز ملف عبر الإنترنت يوجه إلى زبناء سيتزن بنك وأبناك أخرى أمريكية قصد إخبارهم بأن إدارة بنكهم وضعت رهن إشارتهم وسائل متطورة لحماية حساباتهم البنكية ضد أي تزوير أو قرصنة بطائقهم وذلك شرط تلقي المعلومات المتعلقة بحساباتهم وبطائقهم قصد استفادتهم من برنامج الحماية المذكورة، وهذا الملف في حقيقة الأمر ملف مبرمج على خانات مزورة لتضمين أرقام بطائق الائتمان وكذا القن السري الخاص، حيث يعتقد الزبون أنه يسجل معلوماته الخاصة بقاعدة بيانات بنكية في حين أن الأوامر المعلوماتية التي يملأها الزبون بالصفحة المزورة تتوجه إلى عناوين إلكترونية مصممة لتجميع المعلومات عن الزبائن وبالتالي يتم تحويل مسار هذه المعلومات السرية لتستقر بين أيدي القراصنة مبرمجي هذا الملف المزور الذين يقومون بتزييف البطائق بناء على المعلومات المتوصل بها ويسحبون

---

[146]– **جميل عبد الباقي الصغير**: "الإنترنت والقانون الجنائي"، مرجع سابق ص: 80.

[147]– **أحمد حسام طه تمام**: مرجع سابق، ص: 547.

أموالا من الشبابيك البنكية من مختلف جهات العالم ليتم اقتسامها بينهم، وبالتالي فإنهم استعملوا الاحتيال لتوقيع ضحاياهم في الغلط بتأكيدات خادعة مما يعدون مرتكبين لجريمة النصب طبقا لما ينص عليه الفصل 540 من القانون الجنائي[148].

إن ما ذهبت إليه الهيئة مصدرة القرار مصادف للصواب، ما دامت عناصر الفصل 540 قائمة، فحصول الجاني على المال نجم عن سلوكه طرقا احتيالية على إثرها منحه الضحايا المعلومات الخاصة بأرصدتهم المالية، بعدما انخدعوا بصفته وحسبوه مسؤولا بنكيا مفوضا من قبل البنك الذي يتعاملون معه لحماية حساباتهم البنكية من القرصنة أو التزوير فقام هو باستغلالها لأخذ أموالهم.

الفقرة الثانية: جريمة خيانة الأمانة

نظم المشرع المغربي جريمة خيانة الأمانة بمقتضى الفصول من 547 إلى 550 من القانون الجنائي، وهكذا عاقب الفصل 547 كل من "اختلس عمدا أو بدد بسوء نية إضرارا بالمالك أو واضع اليد أو الحائز أمتعة أو نقودا أو بضائع أو سندات أو وصولات أو أوراقا من أي نوع تتضمن أو تنشئ التزاما أو إبراء كانت سلمت إليه على أن يردها، أو سلمت إليه لاستعمالها أو استخدامها بغرض معين، يعد خائنا للأمانة...".

ويتحدد النشاط المادي في جريمة خيانة الأمانة في ثلاث صور، الاختلاس ويتحقق عند انصراف نية الحائز الذي يحوز المال حيازة مؤقتة إلى حيازته حيازة كاملة دون إخراج المال من حوزته [149]، والتبديد يعني تصرف الأمين في المال الذي أؤتمن عليه تصرفا من شأنه أن يخرجه من حيازته [150]، ثم الاستعمال، وهو استهلاك الأمين

[148]– قرار عدد 23 وتاريخ 7–04–2006، ملف عدد 23/05/50، صادر عن غرفة جنايات الأحداث بمحكمة الاستئناف بالرباط، ص: 14 و15، غير منشور.

[149]– **عفيفي كامل عفيفي:** مرجع سابق، ص: 185.

[150]– **محمد علي العريان:** مرجع سابق، ص: 130.

للمال المسلم إليه استهلاكا يستنفذ قيمته كلها أو بعضها مع بقاء مادته على حالها [151]، وجريمة خيانة الأمانة من الجرائم العمدية تتطلب لقيامها توفر القصد الجنائي العام بعنصريه العلم والإرادة، بالإضافة إلى قصد خاص متمثل في نية تملك المال المنقول من طرف الجاني والذي سلم له على وجه الأمانة.

لا خلاف في تطبيق أحكام جريمة خيانة الأمانة إذا قام الجاني باختلاس قاعدة بيانات سلمت له من طرف المجني عليه محمولة على دعامة مادية على وجه الأمانة، سواء كان الجاني مستخدما لدى المجني عليه أو شخصا آخر، لكن الإشكال المطروح هو ما مدى إمكانية انطباق أحكام جريمة خيانة الأمانة في الحالة التي يقوم فيها أجير لدى منتج لقاعدة بيانات أو لدى مسؤول آخر عن هذه القاعدة بإعطاء نسخة من المعلومات التي هي تحت تصرفه بصفته عاملا إلى شخص آخر من الغير مخالفا بذلك شروط عقد العمل، مع الأخذ بعين الاعتبار أن الفعل انصب على المعلومات في ذاتها بمعزل عن الوسيط المادي الحامل لها، في غياب نص قانوني صريح في التشريع المغربي نجد أن المشرع الفرنسي في المادة 13 من القانون الخاص بالمعلوميات يلزم المعلوماتيين الذين يعملون بمعلومات أو على إدخالها بكتمان أسرار عملهم وإلا عرضوا أنفسهم إلى جريمة إفشاء السر المهني وجريمة خيانة الأمانة[152].

وعموما هناك تفاوت حتى على مستوى القانون المقارن بخصوص صلاحية المعلومات أو البيانات أن تكون موضوعا لخيانة الأمانة لارتباط محل الجريمة بالمنقول المادي ولعدم استيعاب النصوص التقليدية لجميع الحالات التي تفرضها الجرائم المعلوماتية وهو ما فرض سن قوانين حديثة تلائم هذا النمط المستحدث من

[151]– **عفيفي كامل عفيفي:** مرجع سابق، ص: 187.

[152]– **بشرى النية:** مرجع سابق، ص: 54.

الجرائم، والذي يتخذ أشكالا مختلفة قد تبدو معه النصوص الجديدة قاصرة أمامها وهو ما يستدعي وجوب جعلها تشمل الحالات المستجدة حتى يترك للقضاء حيزا مهما عند تطبيقه للنصوص الملائمة لكل حالة جرمية على حدة وإعطائها الوصف القانوني المنطبق عليها وبالتالي تكييفها قانونيا التكييف الصحيح.

المبحث الثاني: الجريمة المعلوماتية وفق المقتضيات والقوانين الحديثة

أمام الصعوبات التي يشكلها تطبيق النصوص التقليدية على الجرائم المعلوماتية المستحدثة، بسبب عدم تماشي القواعد العادية للحماية مع التطور المستمر لهذا النوع من الجرائم وتطور وسائل وطرق الاعتداءات، وسعيا من المشرع لتحقيق حماية أفضل لنظام المعلوميات من قواعد بيانات وبرامج حاسوب ومعطيات لجأ إلى تجريم الإخلال بسير نظم المعالجة الآلية للمعطيات (المطلب الأول)، وحماية قواعد البيانات وبرامج الحاسوب بمقتضى قوانين خاصة (المطلب الثاني).

المطلب الأول: المقتضيات المتممة لنصوص القانون الجنائي

إن وعي المشرع المغربي بخصوصية الإجرام المعلوماتي وانعكاساته على المجتمع بدأ مع صدور القانون المتعلق بالإرهاب الذي وردت فيه إمكانية ارتكاب أفعال إجرامية إرهابية عن طريق نظم المعالجة الآلية للمعطيات، علما أن القانون الجنائي المغربي لا يحتوي على نصوص تخص الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات، مما حذا بالمشرع إلى تبني قانون خاص بهذه العينة من الجرائم وتم ذلك عبر قانون رقم 03-07 المتمم لمجموعة القانون الجنائي.

وهو ما سنح للقضاء بإعطاء تكييفات مناسبة للجرائم الماسة بنظم المعلوميات، ويمكن حصر هذه الجرائم في فئتين: الجرائم التي تستهدف المس بنظم المعالجة الآلية للمعطيات (الفقرة الأولى)، والجرائم التي تستهدف المعطيات ووثائق المعلوميات (الفقرة الثانية).

الفقرة الأولى: الجرائم الماسة بنظم المعالجة الآلية للمعطيات[153]

[153]– اقترح مجلس الشيوخ الفرنسي تعريفا لنظام المعالجة الآلية للمعطيات بأنه: "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط والتي تربط بينها مجموعة من العلاقات التي عن طريقها يتم تحقيق نتيجة معينة وهي معالجة المعطيات، على أن يكون هذا المركب خاضعا لنظام المعالجة الفنية".

تتجلى صور الاعتداء على نظام المعالجة الآلية للمعطيات في الدخول أو البقاء غير المشروع في النظام، وعرقلة سير النظام أو إحداث خلل فيه، ثم الإعداد لارتكاب المس بالنظام.

فبالنسبة للدخول أو البقاء غير المشروع نص الفصل 3-607 "يعاقب بالحبس من شهر إلى ثلاثة أشهر وبالغرامة من 2000 إلى 10.000 درهم أو بإحدى هاتين العقوبتين فقط كل من دخل إلى مجموع أو بعض نظام للمعالجة الآلية للمعطيات عن طريق الاحتيال.

ويعاقب بنفس العقوبة من بقي في نظام المعالجة الآلية للمعطيات أو جزء منه، كان قد دخله عن طريق الخطأ وهو غير مخول له حق دخوله.

تضاعف العقوبة إذا نتج عن ذلك حذف أو تغيير المعطيات المدرجة في نظام للمعالجة الآلية للمعطيات أو اضطراب في سيره".

انطلاقا من هذا النص يتضح أن جريمة الدخول أو البقاء في النظام لا تقوم إذا كان الولوج إليه متاحا للجمهور وإنما تفترض أن يتم ذلك عن طريق الاحتيال، وهو ما ذهب إليه القضاء المغربي إذ اعتبر أن جنحة الدخول إلى نظام المعالجة الآلية عن طريق الاحتيال ثابتة في حق المتهم الذي استطاع الدخول عبر شبكة الإنترنت إلى جهاز الشخص المراسل معه بواسطة ما يدعى بـ PRORAT الذي تمكن من قرصنته، وقام بنسخ جميع المعلومات التي تخصه، كما تمكن من الولوج إلى مواقع إلكترونية عبر شبكة الإنترنت عن طريق قرصنة الأقنان السرية الخاصة بأصحابها[154].

يراجع بهذا الخصوص: **عبد الفتاح بيومي حجازي:** مرجع سابق، ص: 21-22.

[154]- ملف جنحي تلبسي رقم 07/7794، حكم ابتدائي صادر بتاريخ 06-08-2006، تحت عدد 037، مشار إليه سابقا.

ويتكون الركن المادي لهذه الجريمة من فعل الدخول إلى نظام المعالجة الآلية للمعطيات أو جزء منه، وإما في فعل البقاء في هذا النظام أو في جزء منه، هذا ولم يحدد المشرع وسيلة الدخول أو الطريقة التي يتم بها الدخول إلى النظام فقد تقع بأي شكل من الأشكال (برنامج فيروس، قرصنة برامج أو رموز تشفير، تجاوز نظام الحماية)، ويكون الدخول غير مشروع إذا كان من له حق السيطرة على النظام قد وضع بعض القيود للدخول إليه ولم يحترمها الجاني.

كما تقع الجريمة سواء تم الدخول إلى النظام كله أو جزء منه فقط، كالدخول لبعض عناصر النظام أو عنصر واحد منه، أو في الحالة التي يسمح فيها للجاني بالدخول إلى جزء من النظام فينتهز الفرصة ويدخل إلى جزء آخر غير مسموح له الدخول إليه، شرط أن يكون العنصر الذي تم الولوج إليه يدخل في برنامج متكامل قابل للتشغيل[155].

أما فعل البقاء في النظام أو جزء منه فيقصد به التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، وقد يتحقق البقاء المعاقب عليه استقلالا حين يكون الدخول إلى النظام مشروعا، كمن يدخل إلى نظام بالصدفة أو عن طريق الخطأ أو السهو ولا ينسحب أو يبقى فيه بعد المدة المحددة له للبقاء داخله[156].

ونشير إلى أن جريمة الدخول أو البقاء جريمة عمدية بحيث يتخذ الركن المعنوي فيها صورة القصد الجنائي المتكون من علم وإرادة، وذلك بأن تتجه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء، وأن يعلم الجاني أنه ليس له الحق في الدخول إلى النظام أو البقاء فيه.

---

[155]– **نائلة عادل محمد فريد قورة:** مرجع سابق، صفحات متفرقة: 315–352.

[156]– المرجع السابق، ص: 395.

وعليه لا يتوفر الركن المعنوي إذا كان دخول الجاني أو بقائه داخل النظام مسموح به، أو وقع في خطأ في الواقع كجهله وجود حظر للدخول أو البقاء أو يعتقد أنه مسموح له الدخول، فإذا توفر القصد الجرمي بعنصريه العلم والإرادة فلا عبرة بالباعث على الدخول أو البقاء بحيث يظل القصد الجرمي قائما ولو كان الباعث الفضول أو إثبات القدرة على الانتصار على النظام[157].

وبالرجوع إلى الفقرة الأخيرة من الفصل 3-607 نجدها تنص على ظرف مشدد يتحقق عندما ينتج عن الدخول أو البقاء إما محو أو تعديل المعطيات التي يحتويها النظام أو إحداث اضطراب في سيره، ويكفي لتوفر هذا الظرف وجود علاقة سببية بين الدخول أو البقاء غير المشروعين والنتيجة الضارة وذلك بمحو أو تعديل المعطيات التي يحتويها النظام أو تعطيله، ويلاحظ هنا أن المشرع يحمي النظام من خلال حماية المعطيات التي يحتويها.

أما فيما يخص عرقلة سير النظام أو إحداث خلل فيه، فباستقراء الفصل 5-607 من القانون الجنائي [158]، يتبين أن الركن المادي لهذه الجريمة يتمثل في فعل التعطيل الذي يندرج ضمن إعاقة النظام أيا كانت الوسيلة المستخدمة في ذلك، فقد تكون بطريقة مادية كأعمال العنف على أجهزة الحاسوب وشبكة الإنترنت، وقد تكون بطريقة معنوية عندما تقع على الكيانات المنطقية للنظام مثل البرامج والمعطيات [159]،

---

[157]- المرجع السابق، ص: 364.

[158]- ينص الفصل 5-607 على أنه: "يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من 10.000 إلى 200.000 درهم أو بإحدى هاتين العقوبتين كل من عرقل عمدا سير نظام المعالجة الآلية للمعطيات أو أحدث فيه خللا".

[159]- **هدى حامد قشقوش:** "جرائم الحاسب الإلكتروني في التشريع المقارن"، دار النهضة العربية، القاهرة، طبعة 1992، ص: 28.

كما يتمثل أيضا في إحداث الخلل في النظام عن طريق العيب أو الإفساد [160]، أو كل فعل يجعل نظام المعالجة الآلية غير صالح للاستعمال، وإحداث خلل في نظام المعالجة الآلية للمعطيات يتم بعدة وسائل خاصة منها البرامج الخبيثة ذات الأثر التدميري والتي تصيب النظام بالشلل [161]، وهو ما سببه فيروس زوطوب الذي عدله المغربي (ف.ص) للنظم المعلوماتية الأمريكية إذ خلق لها العديد من المشاكل التقنية، مما شكل عرقلة لسير النظام أو إحداث خلل فيه كان على المحكمة أن تأخذه بعين الاعتبار إثر تكييفها للأفعال المنسوبة للمتهم بأن تناقشه في معرض تعليلها للتهم الموجهة إليه بدل الاقتصار على بيان العناصر المكونة لجريمة تكوين عصابة إجرامية وجريمة السرقة والإشارة إلى كون أنه والمتهم الثاني لم ينكرا ولوجهما أنظمة المعالجة الآلية للمعطيات [162]، وذلك حتى يكون للقضاء هامشا كبيرا في تفعيل النصوص القانونية من خلال الوقائع المعروضة عليه.

وغني عن البيان أن جريمة إعاقة سير النظام أو إحداث خلل فيه هي جريمة عمدية تقوم بوجود القصد الجنائي بعنصريه العلم والإرادة.

بقي أن نشير إلى الصورة الثالثة للاعتداء على نظام المعالجة الآلية للمعطيات وهي تلك المتعلقة بالإعداد لارتكاب المس بالنظم من خلال صنع تجهيزات أو أدوات أو أي معطيات تعتمد على ارتكاب جرائم عرقلة سير نظم المعالجة أو تملكها أو حيازتها أو التخلي عنها للغير، أو عرضها أو وضعها رهن إشارته.

الفقرة الثانية: الجرائم التي تستهدف المعطيات والوثائق المعلوماتية

[160]– كاستخدام القنبلة المعلوماتية التي يدخل عن طريقها معلومات تتكاثر داخل النظام فتجعله غير صالح للاستعمال، أو استخدام برنامج يحمل فيروس يقوم بتغيير غير محسوس في البرامج أو المعطيات.

[161]– **هشام محمد فريد رستم:** مرجع سابق، ص: 158.

[162]– قرار عدد 721 وتاريخ 12-09-2006، ملف عدد 600-06-22، مشار إليه سابقا.

عاقب المشرع بمقتضى الفصل 06-607 بالحبس من سنة إلى ثلاث سنوات وبالغرامة من 10.000 إلى 200.000 درهم أو بإحدى هاتين العقوبتين فقط كل من أدخل معطيات في نظام المعالجة الآلية للمعطيات أو أتلفها أو حذفها منه أو غير المعطيات المدرجة فيه أو غير طريقة معالجتها أو طريقة إرسالها عن طريق الاحتيال.

يتكون الركن المادي لهذه الجريمة من الأفعال التالية:

أولا: إدخال معطيات [163] في نظام المعالجة: ويعتبر هذا الفعل أكثر أساليب ارتكاب الاحتيال المعلوماتي بساطة وأمنا وأكثر أشكاله وقوعا، ومن ذلك قيام شخص بإدخال معطيات مصطنعة ببطاقة خاصة به على شبكة الإنترنت ودون بها معلومات متعلقة بشخصية سامية في البلاد أرفقها بصورة لهذه الشخصية واستعملها في موقع Facebook لربط علاقات مع المشاركين بهذا الموقع[164].

ثانيا: إتلاف وحذف المعطيات : يقصد به إزالة جزء من المعطيات الموجودة داخل النظام، ومن أبرز صوره حذف معطيات متعلقة بحسابات بنكية جديدة.

ثالثا: تغيير المعطيات : يتعلق الأمر إما بتغيير المعطيات في حد ذاتها واستبدالها بمعطيات أخرى أو تغيير الطريقة التي تعالج بها أو طريقة إرسالها، وتغيير طريقة المعالجة والإرسال هو في حد ذاته تلاعب بالبرنامج.

وقد اعتبرت ابتدائية الدار البيضاء في الواقعة المستدل بها أعلاه أن فعل المتهم يشكل جنحة إدخال معطيات في نظام المعالجة الآلية للمعطيات وتغييرها وتزييف

---

[163]- تعني المعطيات أو ما يصطلح عليه بالبيانات شيء معطى أو مسلم به وبصحته كحقيقة وكواقعة، وهي عبارة عن الأرقام والكلمات أو الرموز أو الحقائق والإحصاءات الخام التي لم تخضع بعد لعملية تقسيم أو تجهيز للاستخدام وهي بشكل أوضح البيانات الأولية التي تتعلق بقطاع أو نشاط ما قبل أن يتم تنظيمها ومعالجتها بطريقة تسمح باستخلاص النتائج المتمثلة في المعلومات.
يراجع: **الحسين القمري**: "القيمة القانونية للوثائق الصادرة عن الحاسوب"، مجلة الدفاع عدد 4، 2003، ص: 59.

[164]- ملف جنحي تلبسي رقم 2008/1189 وتاريخ 08/02/22، صادر عن ابتدائية البيضاء، (غير منشور).

وثائق المعلوميات وإعداد معطيات معلوماتية غير صحيحة وتملكها وعرضها معللة حكمها: "حيث إن النظام المعلوماتي يشكل بيانات ومعلومات تمت معالجتها بعد اتباع طرق وإجراءات إلكترونية معينة لتصير برنامجا تطبيقيا يشمل معلومات مخزنة يتم الرجوع إليها عند الحاجة...

وإن دخول الظنين غير المشروع لموقع فايس بوك عن طريق انتحال شخصية (...) باستعمال صورته وجميع المعلومات الشخصية الخاصة به يعتبر دخولا مزورا في الصفحة الإلكترونية التي استعملها الظنين في استقطاب مراسليه كما أن إقدام الظنين على نشر صورة (...) والمعلومات الخاصة به ونسبتها لنفسه يعد دخولا لنظام معلوماتي عن طريق تزوير إلكتروني رغم علمه بذلك خاصة وأنه مهندس دولة له تكوين في الميدان[165]".

وتعتبر جريمة التلاعب في المعطيات جريمة عمدية لذلك يلزم أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل كما يجب أن يكون على علم أن ما يقوم به هو تلاعب بالمعطيات وأن لا حق له في القيام بذلك.

هذا وقد عاقب المشرع المغربي على تزوير أو تزييف وثائق المعلوميات أيا كان شكلها إذا كان من شأن التزوير أو التزييف إلحاق ضرر بالغير وكذا استعمال هذه الوثائق المعلوماتية مع العلم أنها مزورة أو مزيفة طبقا للفصل 7-607 من القانون الجنائي، غير أنه لم يضع تعريفا لوثائق المعلوميات[166].

أما التزوير فهو أي تغيير للحقيقة يرد على مخرجات الحاسب الآلي سواء تمثلت في مخرجات ورقية مكتوبة أو كانت مرسومة، كما قد يتم في مخرجات غير ورقية

---

[165]- نفس الحكم: ص: 8-9-10.

[166]- هي كل جسم منفصل أو يمكن فصله عن نظام المعالجة الآلية للمعطيات وقد سجلت عليه معلومات معينة سواء أكان معدا للاستخدام بواسطة نظام المعالجة الآلية للمعطيات أو يكون مشتقا عنها.
يراجع: **عبد الفتاح حجازي بيومي**، مرجع سابق، ص: 308.

شرط أن تكون محفوظة على دعامة كبرنامج منسوخ على أسطوانة، كما يتحقق التزوير بتقليد الوثائق المعلوماتية أو التوقيع الإلكتروني، ويكتمل الركن المادي لهذه الجريمة بتوفر عنصر إلحاق الضرر بالغير، أما بالنسبة لاستعمال وثائق المعلوميات مع العلم أنها مزورة فمن ذلك استعمال توقيع إلكتروني مزور أو بطاقة وفاء مزورة.

وقد ذهبت بعض القرارات الصادرة عن محكمة الاستئناف بالرباط إلى اعتبار قرصنة البطائق البنكية من قبل مجموعة من الأشخاص بمثابة تزوير في وثائق المعلوميات ومن هذه القرارات، قرار عدد 364 الذي جاء فيه: "بالنسبة للمتهم (ع.ص)، حيث اعترف المتهم بأنه كان يقوم بسحب المبالغ المالية من شبابيك إلكترونية بواسطة بطائق ائتمان مزيفة عن طريق قرصنة الحسابات البنكية لزبناء أبناك أجنبية...

وحيث إن المحكمة اقتنعت بثبوت الفعل المنسوب للمتهم ويشكل من حيث الوصف القانوني للتجريم جريمة تزوير وثائق المعلوميات واستعمالها طبقا للفصل 7-607 بعد إعادة التكييف لجريمة تزوير بطائق الائتمان واستعمالها مما يتعين معه التصريح بإدانته من أجل ذلك".

- "بالنسبة للمتهم ب ك:

حيث اعترف المتهم بأنه لقن كيفية قرصنة الحسابات البنكية عن طريق المتهم (ع.ص) وحدد الطريقة التي تتم بها قرصنة الحسابات البنكية...

وحيث إن الوقائع المعروضة تشكل من حيث الوصف القانوني للتجريم جريمة المشاركة في تزوير وثائق المعلوميات واستعمالها طبقا للفصلين 129 و 7-607 بعد إعادة التكييف لجريمة تزوير بطائق الائتمان واستعمالها مما يتعين معه التصريح بمؤاخذته من أجلها"[167].

[167]- ملف عدد 22/05/740، ص: 11-12، مشار إليه سابقا.

وفي قرار آخر تحت عدد 633 اعتبرت أن: "حيث ثبت للمحكمة أن المتهم كان يعلم أن البطائق البنكية التي تسلمها من المتهم (ح.ك) مزيفة وأنه ولج الشبابيك الأوتوماتيكية البنكية واستعملها في سحب المبالغ المالية لفائدته ولفائدة غيره دون وجه حق...

وحيث ثبت للمحكمة أن الأفعال المنسوبة إلى المتهم توصف بجريمة استعمال وثائق المعلوميات (بطاقة بنكية) وهو يعلم أنها مزيفة حسب الفقرة الثانية من الفصل 607-7"[168].

إن تعليل الهيئتين مصدرتي القرار تعليل منطقي وفيه انسجام مع النصوص المستحدثة التي سنها المشرع لزجر جرائم المعلوميات، وإعادة تكييف جريمة تزوير بطائق الائتمان واستعمالها لتزوير وثائق المعلوميات لهو تكييف قانوني سليم يتماشى مع ضرورة إعمال النصوص في مواضعها عوض إهمالها.

المطلب الثاني: القوانين الجنائية الخاصة

عمل المشرع المغربي على حماية برامج الحاسوب وقواعد البيانات من الاعتداءات التي تكون عرضة لها، وذلك بمقتضى قانون حماية حقوق المؤلف والحقوق المجاورة، لذلك سنعرض لنطاق مبدأ حماية برامج الحاسوب في ظل هذا القانون (الفقرة الأولى)، دون أن نغفل الحماية التي يكفلها لقواعد البيانات كذلك (الفقرة الثانية).

الفقرة الأولى: حماية برامج الحاسوب طبقا لقانون حماية حقوق المؤلف

يتكون الحاسوب من جزئين رئيسيين: المكونات المادية التي يتكون منها، والمكونات اللامادية وهي البرامج، والبرنامج له أهمية كبرى في استخدام الحاسوب، لأنه هو القادر على تحقيق ما يطلب منه هذا الأخير وغيابه عن الحاسوب يجعله

[168]- ملف عدد 08/09/461، ص: 11-12، مشار إليه سابقا.

قطعة من البلاستيك لا قيمة لها، وتتسم البرامج بالتعدد والتنوع بحسب مجالات استعمالها وتطبيقها في الحياة العملية.

ويمكن تعريف برامج الحاسوب بأنها مجموعة من الأوامر والتعليمات مكتوبة بلغة ما لتنفيذ عمليات محددة للوصول إلى نتائج تتماثل مع إجراء نفس العمليات بالطرق اليدوية، ذلك أن البرامج هي تعليمات مكتوبة موجهة إلى جهاز تقني يسمى الحاسوب بغرض الوصول إلى نتيجة محددة، وهذا المفهوم الواسع يشمل التعليمات الموجهة إلى الحاسوب وملحقات البرنامج مما يجعل الحماية منصرفة إليهما معا، وهو ما أخذ به المشرع الذي عرف برامج الحاسوب في البند 23 من المادة الأولى من قانون حماية حقوق المؤلف، "بأنه كل مجموعة من التعليمات المعبر عنها بكلمات أو رموز أو برسم أو بأي طريقة أخرى تمكن حينما تدمج في دعامة قابلة لفك رموزها بواسطة آلة، أن تنجز أو تحقق مهمة محددة أو تحصل على نتيجة بواسطة حاسوب أو بأي طريقة إلكترونية قادرة على معالجة المعلومات"[169].

وقد نص هذا القانون صراحة في الفقرة الثانية من المادة الثالثة على استفادة برامج الحاسوب من الحماية المقررة للمصنفات الأدبية والفنية، وبذلك فحماية برامج الحاسوب في القانون المغربي أصبحت بمقتضى نص القانون حسما لمختلف التأويلات الفقهية والاجتهادات القضائية [170]، وليس المقصود بالحماية برامج التشغيل والتي يطلق عليها عادة برامج الاستغلال التي تمكن الحاسوب من أداء وظيفته المحددة له والتي تعتبر بالتالي جزءا من هذا الجهاز، بل يتعلق الأمر ببرامج التطبيق التي تستهدف تحقيق نتيجة معينة [171]، وتبدأ حماية الحقوق التي تترتب عن هذا العمل

---

[169]– **محمد بوشيبة:** "حماية برامج الحاسوب طبقا لقانون 00–2 المنظم لحقوق المؤلف والحقوق المجاورة"، مجلة القضاء والقانون، العدد 150، ص: 85–86.

[170]– المرجع السابق، ص: 87.

[171]– **عبد الكريم غالي:** "إشكالية حماية البرامج المعلوماتية على ضوء القانون المتعلق بحقوق التأليف والحقوق المجاورة الصادر في 15 فبراير 2000"، مجلة كتابة الضبط العدد 9، الطبعة 2001، ص: 12–13.

المصنف بمجرد إنجاز البرنامج ولمدة 25 سنة والحقوق المترتبة عن هذا العمل أي إنجاز البرنامج تنقسم إلى حقوق معنوية وحقوق مادية، ومن ضمن الحقوق المعنوية للمؤلف المطالبة بانتساب العمل إليه، ومن الحقوق المادية نشره أو إعادة نشره أو بيعه أو إجارته أو إعادته إلا إذا كان برنامج الحاسوب ليس الموضوع الأساسي في التأجير أو الإعارة.

واستنساخ برنامج الحاسوب غير مسموح به إلا في حالات ضيقة، فلا يمكن للمالك الشرعي لنسخة من البرنامج إنجاز نسخة من هذا الأخير والاقتباس منه إلا بشرط أن يكون ذلك ضروريا وحصرا من أجل استعمال برنامج الحاسوب للأغراض التي تم اقتناؤه من أجلها ولأغراض توثيقية بأخذ الاحتياط لتعويض النسخة في حالة الضياع أو التلف[172].

لذلك فالحصول على برامج الحاسوب بطريقة غير شرعية واستنساخها أو الحصول على معلومات سرية حول طريقة إنشائها يعد عملا مجرما قانونا، وإن كان التطور التكنولوجي لأجهزة ومعدات النسخ أدى إلى ظهور صناعة نشطة متخصصة في استنساخ برامج الحاسوب، ناهيك عن أن الثورة الحاصلة في مجال المعلوميات أدت إلى تنامي إفشاء معلومات برامج الحاسوب والاعتداء عليها بالقرصنة أو الاستغلال غير المشروع، وهو ما يعد مساسا ليس فقط بحقوق مبتكريها الخاصة بل وأيضا مسا بالاقتصاد الوطني.

لذلك عمد المشرع إلى تشديد العقوبات فيما يخص الخروقات التي تطال المصنفات الأدبية والفنية (التقليد، القرصنة) بما فيها برامج الحاسوب، فبعد أن كانت العقوبات في هذه الجريمة عبارة عن غرامة تتراوح بين مائة وعشرين وعشرة آلاف درهم (الفصل 575 ق ج)، أصبحت حسب المادة 64 من قانون حماية حقوق المؤلف

[172]– المرجع السابق، ص: 13–14.

الجديد المعدل سنة 2006، عقوبات حبسية ومالية تتجلى في الحبس من شهرين إلى ستة أشهر وغرامة بين عشرة آلاف ومائة ألف درهم وذلك سعيا منه لتوفير حماية أكثر فعالية لها.

الفقرة الثانية: حماية القانون المتعلق بحقوق المؤلف لقواعد البيانات

إن قواعد البيانات باعتبارها من أنظمة المعالجة الآلية للبيانات، نتاج للتقدم العلمي في مجال أنظمة المعلومات ووسائل الاتصال، فهي مظهر من مظاهر ارتباط تكنولوجيا الحواسيب الآلية والمعلوماتية بتكنولوجيا الاتصال.

وقد عرفت المادة الأولى من قانون حماية حقوق المؤلف والحقوق المجاورة في فقرتها الرابعة عشر قواعد البيانات بأنها: "مجموعة من الإنتاجات والمعطيات أو عناصر أخرى مستقلة مرتبطة بطريقة ممنهجة ومصنفة يسهل الوصول إليها ذاتيا بواسطة الوسائل الإلكترونية أو كل الوسائل الأخرى".

وقد نص المشرع المغربي صراحة ومباشرة على حماية قواعد البيانات وأعطاها صفة المصنف في المادة الخامسة من نفس القانون وتتمتع بنفس الحماية المنصوص عليها بالنسبة للمصنفات الأصلية الواردة في المادة الثالثة.

لذا ففي حالة خرق متعمد للحقوق المعنوية والمادية لمؤلف قاعدة بيانات بطريقة غير مشروعة وبأي وسيلة كانت بقصد الاستغلال التجاري، يعاقب المعتدي بالحبس من شهرين إلى ستة أشهر وبغرامة تتراوح بين 10.000 و100.000 درهم أو بإحدى هاتين العقوبتين حسب ما تنص عليها المادة 64 من قانون حماية حقوق المؤلف لسنة 2000 المعدل بمقتضى القانون رقم 05- 34 الصادر في 14 فبراير 2006، وقد عرفت نفس المادة "الخروقات المعتمدة بقصد الاستغلال التجاري" بكونها كل اعتداء متعمد على حقوق المؤلف أو الحقوق المجاورة، ليس دافعه بصورة مباشرة أو غير مباشرة الربح المادي، أو كل اعتداء متعمد ارتكب من أجل الحصول على امتياز

تجاري أو على كسب مالي خاص [173]، كما نصت نفس المادة على التدابير الوقائية والعقوبات الإضافية، إذا ما تم اقتران الجرائم الأخرى الملحقة بجرائم خرق حق من حقوق المؤلف، ويتعلق الأمر فيما يخص قواعد البيانات استيراد وتصدير نسخ من قبل شخص ذاتي لأغراض شخصية دون إذن المؤلف أو أي مالك آخر بحوزته حقوق المؤلف، وقد شددت المادة 64-2 العقوبات في حالة اقتراف فعل آخر يعد خرقا لحقوق المؤلف والحقوق المجاورة داخل الخمس سنوات التي تلي صدور حكم أول صار نهائيا على إثر ارتكاب أحد الأفعال المشار إليها في المادة 64، حيث يعاقب المخالف بالحبس من سنة إلى أربع سنوات وبغرامة تتراوح بين 60.000 و600.000 درهم أو بإحدى هاتين العقوبتين فقط[174].

هذا ويجوز للنيابة العامة طبقا للمادة 65-2 ودون تقديم أي شكاية من جهة خاصة أو من صاحب الحقوق أن تأمر تلقائيا بمتابعات ضد كل من مس بحقوق مؤلف قاعدة بيانات أصلية تخضع لحماية القانون المتعلق بحماية حقوق المؤلف.

والملاحظ أن المشرع المغربي من خلال قانون سنة 2000 المعدل سنة 2006 لم يحل فيما يخص عقوبات جريمة التقليد وجريمة القرصنة التي تخضع لها الخروقات التي تمس حقوق مؤلفي قواعد البيانات على فصول القانون الجنائي، بل نص لأول مرة ضمن نصوص قانون حماية حقوق المؤلف على عقوبات سالبة للحرية وجزاءات مالية وأخرى إضافية محددة (المواد 64 و64-1 و64-2 و64-3)، وقد كانت المادة 56 من ظهير 1970 تحيل على فصول القانون الجنائي (الفصول من 575 إلى 579) فيما يخص جريمة التقليد، وكانت العقوبات عبارة عن غرامة محددة قانونا في

---

[173]- **تيسير الغمري**: "الإطار القانوني لقواعد البيانات الإكترونية"، رسالة لنيل دبلوم الدراسات العليا المعمقة في القانون الخاص، جامعة محمد الخامس أكدال، كلية العلوم القانونية والاقتصادية والاجتماعية بالرباط، السنة الجامعية 2007/2006، ص: 211.

[174]- المرجع السابق، ص: 212.

حالة جريمة التقليد طبقا للمادة 56 من الظهير والفصل 575 و 576 من القانون الجنائي، كما أن قانون 15 فبراير 2000 أحال على العقوبات المنصوص عليها في القانون الجنائي دون التقيد بنصوص معينة في حالة خرق لحق محمي يتم اقترافه عن قصد أو نتيجة إهمال بهدف الربح مع ترك تحديد مبلغ الغرامة لتقدير المحكمة التي لها سلطة تحديد القدر بالنظر للأرباح التي حصل عليها المعتدي من الخرق.

وبذلك تتجسد إرادة المشرع في إعطاء مفهوم أوسع لجرائم خرق حقوق المؤلف أو القرصنة، مما يجعل العقوبات المنصوص عليها لهذه الجرائم خصوصا فيما يتعلق بقواعد البيانات الإلكترونية أكثر جدوى في توفير حماية فعالة لهذه المصنفات والحد من الخروقات التي تتعرض لها من طرف كل المتدخلين عبر شبكات الاتصال، كما أن إدراجه لقواعد البيانات ضمن المصنفات المحمية بقانون حماية حقوق المؤلف وإخضاعها لمقتضيات جريمة القرصنة في حالة مخالفة النصوص الحامية لها هو محاولة لتوفير الأمن للبيانات المعالجة آليا ولأنظمتها، بالنظر للتطور السريع للجريمة في مجال المعلوماتية والمصاحب لتطور مهم في وسائل ارتكاب هذه الأفعال الإجرامية.

الفرع الثاني: الحماية من جرائم المعلوميات

نظرا للتقدم الذي عرفته وسائل الاتصال وتكنولوجيا المعلوميات أصبحت الجرائم المعلوماتية من أشد الجرائم التي تمارس على الأنظمة المعلوماتية وبواسطتها، لذا كانت سبل الحماية التقنية أهم الوسائل التي لجأت إليها جل القطاعات لحماية أنظمتها

المعلوماتية، وبرزت تقنيات جديدة للحد من الأخطار التي تتعرض لها وللحيلولة دون الوصول إلى الأنظمة الخاصة لمختلف القطاعات.

إلا أن هذه الوسائل تصبح هشة وهزيلة إذا لم تقترن بحماية قانونية داخلية تكفل لمختلف هذه القطاعات مواجهة الانتهاكات التي تقع على برامجها وأنظمتها المعلوماتية (المبحث الأول)، علما أن الجهود المبذولة بصفة انفرادية من طرف الدول لمواجهة التطور الذي تعرفه الجرائم المعلوماتية تبقى غير كافية إذا لم تتضافر جهود المنتظم الدولي للتصدي لها خاصة وأنها تتخطى حدود الدول (المبحث الثاني).

المبحث الأول: دور المصالح الوطنية في رصد وقمع الجريمة المعلوماتية

إذا كان المشرع عمل على تطوير القوانين الداخلية بهدف تأسيس حماية قانونية للنظم المعلوماتية، وعيا منه بأوجه الخلل والقصور في هذه القوانين، فإرساء دعائم هذه الحماية رهين بتوفر كوادر أمنية وقضائية متخصصة في ضبط جرائم المعلوميات

(المطلب الأول)، وإشراك المؤسسات ذات الطابع الاقتصادي في الاستراتيجية الأمنية المعتمدة لرصد هذه الجرائم المستحدثة (المطلب الثاني).

المطلب الأول: الأجهزة ذات الطابع الزجري

يختلف قمع ومكافحة الجرائم المعلوماتية عن ضبط الجرائم التقليدية، على اعتبار أن هذه الجرائم ذات طبيعة خاصة لتعلقها ببيانات معالجة إلكترونيا وكيانات منطقية غير مادية، لذا فهي تحتاج لأجل مواجهتها لفرق خاصة بتتبع هذه الجرائم (الفقرة الأولى)، ومتخصصة في التدخل والبحث الجنائي لتحقيق الزجر والردع العام عن طريق ضبط الأنشطة الإجرامية وتقديم فاعليها إلى العدالة (الفقرة الثانية).

الفقرة الأولى: وحدات الشرطة القضائية المكلفة بضبط جرائم المعلوميات

تتميز الجرائم المعلوماتية بكونها جرائم تقنية تنشأ في الخفاء يرتكبها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية التي توجه للنيل من الحق في المعلومات وتطال اعتداءاتها معطيات الحاسوب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات، لذا فالتصدي لها يقتضي وجود عناصر خاصة من الضابطة القضائية لها من التكوين العلمي والمعرفي في ميدان المعلوميات ما يكفي لمكافحة هذا النشاط الإجرامي الحديث، وهذا لا يتحقق إلا بعد تلقيها التعليم والتدريب الكافيين على استخدام شبكات الاتصال واستخدام الأجهزة الفنية الحديثة والمعرفة الكافية باللغات الأجنبية، مما يسمح لها بالقيام بإجراءات التفتيش والضبط والتحفظ على الأدلة التي تساعد على إثبات الجريمة.

وقد يعتقد البعض أن الإنترنت وشبكات المعلومات يصعب فيها تطبيق القانون لغياب نقاط المراقبة على الشبكات وتقنيات إرسال الرسائل والتحقق من هوية المعتدين وتشفير التوقيعات، وهي خصائص يتميز بها الإنترنت تجعل من الصعب تحديد

وملاحقة مرتكب الأفعال المجرمة، مما يعقد عمل الشرطة التي قد تبقى مكتوفة الأيدي[175].

إلا أن ذلك غير صحيح فهذه الأفعال المجرمة ترتكب في بادئ الأمر داخل حدود الدولة يستطيع المحققون أن يتصرفوا حيالها دون مصاعب أو تعقيدات، كما أن معرفة شخصية الفاعل التي يتستر وراءها المجرم المعلوماتي هو أمر نسبي، إذ يترك آثارا أثناء تنقله في شبكة المعلومات تسمح للمحققين بالوصول إليه، علما أن الطابع الدولي للجريمة لا يمثل عقبة تمنع إجراء التحقيق والملاحقة [176]، وإن كان الطابع اللامادي لشبكة الإنترنت باعتبارها ملتقى لمختلف الأصناف والمتعاملين القادمين من مختلف الأوساط، يقتضي لتفعيل دور مصالح الأمن خلق خلية للرصد والمتابعة 7 أيام /7 و 24 ساعة/24، تكون مهمتها الإبحار عبر الشبكة وبطريقة موجهة وهادفة لمعرفة التطورات التي تشهدها ومتابعة نوع المضامين المتداولة في مختلف مجالات استخدام هذه الشبكة [177]، ويبقى دور الأجهزة الأمنية مهما في ضبط معالم الجريمة المعلوماتية خاصة وأنها تتوفر على عناصر متخصصة في الميدان المعلوماتي فقد ساعدت مصلحة المعلوميات التابعة لقيادة الدرك الملكي بالرباط بتنسيق مع المصالح والمؤسسات المختصة في التعرف على أسماء وعناوين مجموعة من الضحايا تمت قرصنة بطائقهم البنكية، وجميع المعلومات المتعلقة بهذه البطائق المقرصنة وكذا الأشخاص المتورطين في ذلك مع التوصل لكيفية قيامهم بعمليات القرصنة ومعالجتهم للمعلومات المضمنة بالبطائق وتزويرها، كما أن تحليلها للمعطيات المستخرجة من الحاسوب المستعمل من قبل المتورطين مكنها من معرفة بعض أسماء الأبناك التي تم

---

[175]– **صالح أحمد البربري** : "دور الشرطة في مكافحة جرائم الإنترنت في إطار الاتفاقية الأوروبية الموقعة في بودابست في 2001/11/23"، مقال منشور بالدليل الإلكتروني www.arablawinfo.com، تاريخ ولوج الموقع يوم السبت 22–11–2008 على الساعة الثالثة زوالا، صفحات متفرقة: 2–4.

[176]– المرجع السابق: ص: 4.

[177]– **أحمد آيت الطالب:** مرجع سابق، ص: 25.

سحب النقود منها ورموز البطائق المقرصنة واكتشاف خزائن مختلفة مسجلة بالحاسوب تحتوي أرقام عدة بطائق بنكية لزبناء تمت قرصنتها تحمل أسماء المتورطين الذين ألقي القبض عليهم[178].

وفي هذا الإطار كذلك تمكنت مصلحة الإعلاميات إثر استخدامها للمعلومات الموجودة في القرص الصلب لأحد الحواسيب ودراسة محتوياته من التوصل إلى عدد البطائق المقرصنة من طرف عناصر شبكة متخصصة في القرصنة ومعرفة الأماكن التي تمت بها عمليات هذه القرصنة[179].

من هنا تبدو أهمية الدور المنوط بوحدات الأمن في مواجهة هذه الظاهرة المستحدثة والمعقدة من الإجرام، فوجود شرطة تقنية وعلمية على درجة كبيرة من المعرفة بأنظمة الحاسب الآلي وكيفية تشغيلها وأساليب ارتكاب الجرائم عليها أو بواسطتها، مع القدرة على كشف غموض هذه الجرائم وسرعة التصرف بشأنها من حيث كشفها وضبط الأدوات التي استخدمت في ارتكابها والتحفظ على البيانات والأجهزة المستخدمة في ذلك أو تلك التي تكون محلا للجريمة، يبقى أمرا ضروريا في ضبط الجرائم ذات الصلة بالأنظمة المعلوماتية، والتي تتسم بحداثة أساليب ارتكابها وسرعة تنفيذها وسهولة إخفائها ودقة سرعة محو أثارها، الأمر الذي يقتضي الوقوف على آليات البحث والتحقيق المعتمدة في مواجهة هذه النوعية من الجرائم.

الفقرة الثانية: تقنيات البحث والتحقيق المعتمدة في مواجهة جرائم المعلوميات

تتميز إجراءات البحث والتحقيق في جرائم المعلوميات بنوع من الخصوصية وتشمل هذه التقنيات:

[178]– قرار عدد 299 وتاريخ 23–03–2006، ص: 5–6، مشار إليه سابقا.

[179]- قرار عدد 37 وتاريخ 16–01–2006، ص: 3، مشار إليه سابقا.

- **معاينة مسرح الجريمة المعلوماتية:** ويقصد بالمعاينة فحص مكان أو أي شيء أو شخص له علاقة بالجريمة وإثبات حالته، ولا تتمتع المعاينة في مجال كشف غموض الجريمة المعلوماتية بنفس الدرجة من الخصوصية التي تكتسيها في مجال الجريمة التقليدية ومرد ذلك لاعتبارين، الأول أن الجرائم التي تقع على نظم المعلومات والشبكات قلما يترتب على ارتكابها آثار مادية، والثاني أن عددا كبيرا من الأشخاص قد يترددون على مكان أو مسرح الجريمة خلال الفترة الزمنية الفاصلة بين ارتكاب الجريمة واكتشافها، مما يهيء الفرصة لحدوث تغيير أو إتلاف أو عبث بالآثار المادية أو زوال بعضها، وهو ما يثير الشك في الدليل المستمد من المعاينة.

وحتى تصبح معاينة مسرح الجريمة المعلوماتية لها فائدة في كشف الحقيقة عنها وعن مرتكبيها ينبغي مراعاة عدة قواعد وإرشادات أبرزها، تصوير الحاسوب والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه، مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسوب وملحقاته ويراعى تسجيل وقت وتاريخ ومكان التقاط الصورة، كذلك يجب الاهتمام بملاحظة الطريقة التي تم بها إعداد النظام والآثار الإلكترونية وبوجه خاص السجلات الإلكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الولوج إلى النظام أو الموقع، مع ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل حين عرض الأمر فيما بعد على القضاء، ويتعين عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسوب من أي مجالات لقوى مغناطيسية يمكن أن تتسبب في محو البيانات المسجلة، وأخيرا التحفظ على محتويات سلة المهملات من الأوراق الملقاة أو الممزقة والمستعملة والشرائط والأقراص الممغنطة

وغير السليمة أو المحطمة، وفحصها ورفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة[180].

- **التفتيش:** هو البحث عن شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها، وقد يقتضي التفتيش إجراء البحث في محل له حرمة خاصة، وقد أحاط القانون التفتيش بضمانات عديدة ومحل التفتيش قد يكون مسكنا أو شخصا.

مع مراعاة الضوابط التي يرسمها قانون المسطرة الجنائية للدخول إلى المنازل لتفتيشها بحثا عن أشياء تؤدي إلى إظهار الحقيقة، يمكن لضابط الشرطة القضائية اعتماد هذا الإجراء لضبط أدلة لها علاقة بجريمة من الجرائم المرتبطة بالمعلومات، وبصرف النظر عن المعيقات التي قد تحول دون بلوغ الأهداف المتوخاة من هذه العملية، فإن القيام بالتفتيش في منزل شخص وفقا للشروط والإجراءات المنصوص عليها في القانون قد يساعد في ضبط الآلة المشبوهة وحجزها تمهيدا لفحصها وإجراء التحليلات التقنية عليها بحثا عما تتضمنه من معطيات أو أدلة رقمية، وأيضا الأدلة التقليدية ذات العلاقة بأنظمة وبرامج وتجهيزات الحاسبات الآلية ومعدات التشغيل والأوراق والمستندات وآلات الطباعة إلى غير ذلك[181].

غير أن عملية البحث في أطراف الحاسبات أو وحدات التشغيل أو ملحقاتها، قد تدفع الباحث الجنائي إلى توسيع دائرة التحريات إلى حاسب آلي أو مركزي موجود في محل آخر يشغله المشتبه فيه أو شخص آخر، كما قد يجد نفسه مضطرا للدخول إلى معطيات آلية أو قواعد بيانات أو مواقع محمية ومؤمنة، وهو ما يثير إشكالا بخصوص إمكانية الولوج إليها بناء على الإذن المحصل عليه أصلا عند الدخول إلى

---

[180]– **عبد الله حسين علي محمود:** "إجراءات جمع الأدلة في مجال سرقة المعلومات"، مقال منشور بالدليل الإلكتروني: comwww.Arablawinfo.، تاريخ ولوج الموقع يوم السبت 2008/11/22، على الساعة الثالثة زوالا.

[181]– **أحمد آيت الطالب:** مرجع سابق، ص: 29-30.

المنزل الذي قام فيه بتحرياته الأولى، أم أن هذا الإذن لا يجزأ للقيام بعمليات تحري في وسط معلوماتي، باعتبار أن الأنظمة المعلوماتية المحمية لا تعتبر منازل في مفهوم القانون، وإذا كان الأمر كذلك فما هي المبررات القانونية الوجيهة التي يمكن اعتمادها لاقتحام أنظمة المعلومات المحمية وإجراء الأبحاث أو التحريات فيها بدون علم المكلفين بها أو أصحابها الشرعيين؟

في غياب إطار قانوني خاص يسمح بالولوج إلى هذه الأنظمة، يمكن القول أن قانون المسطرة الجنائية المغربي رغم حداثته، لا يتضمن استجابة صريحة لمتطلبات البحث وتفتيش قواعد المعطيات الآلية باستعمال الشبكة[182].

- **الشهادة في الجريمة المعلوماتية:** الشهادة هي الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق بشأن جريمة وقعت، سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى متهم أو براءته منها، والشاهد في الجريمة المعلوماتية هو الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي، والذي لديه معلومات جوهرية أو هامة لازمة للولوج في نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله، ويطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتي تمييزا له عن الشاهد التقليدي، ويشمل الشاهد المعلوماتي عدة طوائف من أهمها القائم على تشغيل الحاسب الآلي، وهو المسؤول عن تشغيله والمعدات المتصلة به ويجب أن تكون لديه خبرة كبيرة في هذا المجال، ثم المبرمجون وهم الأشخاص المتخصصون في كتابة البرامج، ويمكن تقسيمهم إلى فئتين: الأولى تشمل مخططي برامج التطبيقات والثانية مخططي برامج النظم.

هناك أيضا المحللون، يتجلى دورهم في تجميع بيانات نظام معين ودراسته ثم تحليله أي تقسيمه إلى وحدات منفصلة، ثم مهندسوا الصيانة والاتصالات، هم

[182]– المرجع السابق، ص: 30.

المسؤولين عن أعمال الصيانة الخاصة بتقنيات الحاسوب بمكوناته وشبكات الاتصال المتعلقة به، بالإضافة إلى مديري النظم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية[183].

ويتعين على الشاهد المعلوماتي أن يقدم لسلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات للكشف عن أدلة الجريمة[184].

عموما هناك صعوبات مختلفة تعترض سلطات البحث والتحقيق في ضبط الجريمة المعلوماتية وهو ما يقتضي من المشرع مراجعة قانون المسطرة الجنائية ليتلاءم مع خصوصية هذه الجريمة، الأمر الذي تنبهت له الكثير من التشريعات الأجنبية التي قررت بعد سنها للقوانين المتعلقة بنظم المعالجة الآلية للمعطيات تنظيم مسطرة خاصة للبحث، على غرار مسطرة التقاط المكالمات الهاتفية أو وسائل الاتصال الإلكترونية عن بعد، وخولت للسلطة القضائية – قاضي التحقيق– صلاحية مراقبة هذه العمليات، الذي يؤهل وحده من حيث المبدأ بالترخيص بإجرائها في الحالات وضمن الشروط المنصوص عليها في القانون[185].

المطلب الثاني: المؤسسات ذات الطابع الاقتصادي

تتميز الجريمة المعلوماتية بكونها جريمة تقنية يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية توجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسوب المخزنة والمعلومات المنقولة عبر نظم وشبكات الاتصال، واعتبارا لطابعها التقني ظهرت أهمية بعض المؤسسات التنظيمية كعامل حاسم في التصدي لهذه

---

[183]– **عبد الله حسين علي محمود:** مرجع سابق، ص: 14–15–16

[184]– المرجع السابق، ص: 16.

[185]– **أحمد آيت الطالب:** مرجع سابق، ص: 31.

الجريمة، عن طريق استعانة عناصر البحث والتحقيق وهيئة الحكم بها من أجل الوصول لمرتكبيها.

ولعل أهم هذه المؤسسات مركز النقديات والبنوك (الفقرة الأولى)، وشركات الاتصال (الفقرة الثانية).

الفقرة الأولى: مركز النقديات والبنوك

يوجد بالمغرب حاليا مجموعة من الشبكات الخاصة بالبطائق البنكية مسيرة من طرف العديد من الأبناك (التجاري وفابنك، البنك المغربي للتجارة الخارجية، مجموعة البنك الشعبي...)، ولضمان الاتصال بين مختلف هذه الشبكات أنشأت المجموعة المهنية للأبناك بالمغرب مركز النقديات والبنوك، المعروف اختصارا بـ CMI [186]، الذي أحدث قانونيا كشركة مجهولة الإسم في 15 فبراير 2001 وبدأ عمليا في ممارسة مهامه بداية فبراير 2004[187]، وإنشاء هذا المركز يدخل في إطار المجهودات المبذولة من طرف البنوك الرامية إلى تطوير وتوسيع مجال استعمال البطائق البنكية، خصوصا عبر إحداث مركز متخصص في إدارة الصفقات النقدية وضمان سيرورتها، مع تأمين استخدام البطائق البنكية وتشجيع عمليات الأداء بواسطتها [188]، وتتمثل مهام هذا المركز في إدارة النشاط النقدي (الدفع بالبطائق البنكية)، كما ينظم عمليات المقاصة بين البنوك الوطنية وكذلك الأجنبية فيما يتعلق بسحب الأموال عبر الشبابيك الأوتوماتيكية، ويسعى هذا المركز إلى خلق طريقة مضمونة للأداء عبر الإنترنت

[186]- voir le site web : www.ubm.org.tn,upload/pdf/s1/cmi.pdf, date d'accés le22/11/2008, à 20 h00.

[187] -voir le site web : http://doc.abhatoo.net.ma/doc/img/ pdf/syspai100602.pdf, date d'accés le 22/11/2008, à 20 h00.

[188] - www.ubm.org. tn, upload/ pdf/s1/cmi.pdf.

تساهم في تطوير الصفقات عبر التجارة الإلكترونية وإنشاء موقع إنقاذ عن بعد للمعلومات البنكية المخزنة لديه ومحاربة الجرائم الماسة بالبطائق البنكية[189].

وقد لعب هذا المركز بالفعل دورا مهما في التصدي للجريمة الإلكترونية ومعرفة مرتكبيها، فقد تم انتدابه للاتصال بمختلف البنوك على الصعيد الوطني بغية الإفادة عن جميع عمليات السحب عبر الشبابيك البنكية بواسطة بطائق الائتمان المزيفة وخصوصا التي تم ابتلاعها من طرف هذه الشبابيك، فوردت إفادة من البنك الشعبي بكل من القنيطرة والرباط ومن بينها شبابيك مزودة بكاميرات تصوير التقطت صورا عديدة لشخص وهو يقوم بعمليات سحب بواسطة بطائق مزيفة تم ابتلاعها من طرف الشباك[190].

كما أنه في إطار عمليات البحث التي تنجزها الضابطة القضائية للكشف عن مزوري بطائق الائتمان انتقلت إلى مركز النقديات فأفادهم المسؤول عن المركز بأنه توصل بعدة شكايات من مؤسسة Master card مفادها أن حوالي ستة بطائق ائتمان مزورة تم الأداء بواسطتها لمطعم بالرباط، وسلمهم نسخة من التقرير الذي تم إنجازه من طرف هذه المؤسسة حول ظاهرة قرصنة البطائق البنكية، وأضاف بأن مركز النقديات يستقبل جميع الشكايات الواردة عليه من طرف المؤسسات البنكية والتجارية، كما سلمهم صورة شمسية بالألوان لبطاقة هوية مسلمة من طرف السلطات البلجيكية ببروكسيل في إسم أحد الأشخاص، وفي أسفل الوثيقة صورة فوتوغرافية لصاحبها تبين لعناصر الضابطة القضائية أنها لأحد المتهمين بقرصنة البطائق البنكية، وقد أعلمهم المسؤول عن مركز النقديات بأن الجناة يستعملون بالمغرب ثلاث آلات لقرصنة البطائق البنكية وهي MSR 500 و TA 90، TA 48، وسلمهم جرد لجميع العمليات

[189] - htt p://doc. Abhatoo. net.ma/doc/img/pdf/syspai 100602. pdf.

[190]– قرار عدد 364، وتاريخ 17–04–2006، ملف عدد 22/05/740، ص: 3، مشار إليه سابقا.

التي تمت عبر البطائق البنكية المقرصنة ومكان قرصنتها مما ساعدهم في الوصول إلى أحد الجناة[191].

فالتنسيق مع مركز النقديات ساعد الضابطة القضائية في التحريات التي تجريها والتي بمقتضاها تتوصل إلى قراصنة بطائق الائتمان وتقديمهم أمام العدالة، وهو ما يبرز دور هذا المركز في رصد الجريمة المعلوماتية، بل إن المجموعة المهنية لبنوك المغرب المنشئة له وعيا منها بخطورة هذا النمط المستحدث من الإجرام في مجال الأنشطة البنكية، تعد عنصرا محوريا في الندوات المنعقدة للتعريف بخطورة الجرائم المعلوماتية، وقد وضحت في إحداها أن أنماط هذه الجرائم تتجلى في التلاعب في المعلومات والبرامج والمعطيات واعتماد القرصنة بواسطة الكمبيوتر سواء بسرقة البرامج أو المعلومات واستعمالها بشكل تعسفي وأيضا تخريب الحاسوب وإتلاف المعطيات المخزنة به وسرقة وقته، واعتبرت أن الجريمة المعلوماتية في المجال البنكي متطورة في الأبناك مع سهولة تعرض زبنائها كمستعلمين للخدمات البنكية والتجارة الإلكترونية ووسائل الأداء للاعتداء، إلا أن واقع هذه الجريمة في القطاع البنكي يبرز ندرة الاعتداءات المباشرة على الأنظمة المعلوماتية للبنوك وأن زبناءها هم الذين يتعرضون للاعتداء من خلال الاحتيال عليهم والحصول على معلومات خاصة بهم تمكن المعتدين من استعمال أقنانهم السرية أو أرقام بطائقهم البنكية ومن تم تقليدها واستعمالها في سحب أموالهم، لذا فالجريمة المعلوماتية حسب المجموعة المهنية للبنوك تتميز بنوع من الخصوصية بالنظر لطابعها اللامادي وصعوبة إثباتها، وهو ما يقتضي ضرورة سن تشريع خاص بها لعدم كفاية النصوص الجنائية التقليدية كالسرقة والنصب وخيانة الأمانة والتزوير للإحاطة بها، مع وجوب ملاءمة الجهاز القضائي

[191]– قرار عدد 299 وتاريخ 23-03-2006، ملف عدد 22/05/736، ص: 6-7، مشار إليه سابقا.

وتكوين القضاة حول مجال محاربة الجريمة المعلوماتية وتنمية التعاون الدولي في هذا الإطار، بالإضافة إلى ضرورة التوعية في هذا المجال عبر تحسيس زبناء الأبناك[192].

الفقرة الثانية: شركات الاتصال

شهد قطاع شبكات الاتصال اللاسلكية المتنقلة تطورات تكنولوجية متسارعة وخاصة على صعيد الأنظمة وشبكات الخدمة المرتبطة به، وإذا كان تحديد هوية المعتدي على المعلوميات لم يعد وهما، فإن الكشف عن الشخصية الحقيقية للشخص الذي ارتكب الجريمة مازال يواجه الكثير من الصعاب، لذا فمن الضروري تحسين أسلوب تتبع "أثار الرسائل" وتحديد هوية المستخدمين حتى يمكن تحريك دعوى المسؤولية، وهنا تظهر أهمية دور مؤدي الخدمة كهمزة وصل ضرورية بالنسبة لنقل المعلومات[193]، ونقصد هنا بمؤدي الخدمة شركات الاتصال، باعتبارها تقدم خدمات للجمهور ويبرز دورها في أن تحدد على مواقعها هوية ناشر الرسالة وبياناته، وقد دخل هذا الالتزام حيز التطبيق منذ زمن بالنسبة لخدمات جهاز télématique بموجب المادة 43من قانون 30 شتنبر 1986 في فرنسا، ويعاقب على عدم الالتزام بها بالمادة 2/76 من نفس القانون بغرامة تتراوح ما بين عشرة آلاف إلى أربعين ألف فرنك، ومن شأن هذا الإجراء أن يقدم الكثير من الشفافية بالنسبة للخدمات الموضوعة تحت تصرف الجمهور، ويساعد على تحديد هوية الشخص المسؤول جنائيا، ومن الضروري تحديد هوية المشتركين بشبكة الاتصالات لتسهيل عمل الشرطة في حال وقوع أي مخالفة حيث يجب على مؤدي الخدمة – شركة الاتصال– أن يكون قادرا على تقديم بيانات شخصية عن زبائنه، في إطار التحقيقات التي تتم بواسطة الشرطة عندما

[192] - **El hadi chaibainou** -directeur général du groupent professionnel des banques au maroc- : « les crimes informatiques commis dans les activités bancaires », document communiqué au séminaire régional sur le théme, « les infration liées à l'utilisation de l'ordinateur », organisé par le PNUD et le ministére de la justice au maroc, le 19 et 20 juin 2007 à casablanca, non publié.

[193]– **صالح أحمد البربري**: مرجع سابق، ص: 5.

يطلب منه ذلك، وفي فرنسا يتم التعاون بين مؤدي الخدمة ورجال الشرطة استنادا إلى المادة 1/462 من قانون العقوبات التي دخلت حيز التطبيق أول مارس 1994، وهنا تثار مشكلة جديدة بالنسبة للاشتراكات المجانية التي تتم دون تحديد هوية المشترك، هذه الاشتراكات هي التي تسهل ارتكاب الجرائم في ظل غياب أي تحديد لهوية أو مكان المستخدم، وهو ما يصعب منعه أو إلغاؤه[194].

وتعد البيانات التي تتعلق بالاتصال التي يقوم مؤدي الخدمة بتجميعها أتوماتيكيا عند توصيل المستخدم بالشبكة ذات قيمة كبرى للمكلفين بالتحقيق، إذ يظهر فيها المستخدم ووقت بداية ونهاية الاتصال، والرقم الكودي للمتصل، والمواقع التي زارها والمعلومات التي طلبها والبيانات التي حصل عليها، فهذه المعلومات وغيرها بمثابة الآثار التي يتركها المستخدم.

وتحفظ هذه البيانات بواسطة مؤدي الخدمة لفترات متغيرة حسب أهمية وكثافة تردد العملاء ومن المهم الاحتفاظ بهذه المعلومات لفترة كافية، حتى يمكن تسهيل عمل شرطة البحث في متابعة وإقامة الدليل على المخالفات المرتكبة[195].

وفي هذا الإطار تمكنت الضابطة القضائية في إطار تنسيقها مع شركة اتصالات المغرب التي زودتهم بمعلومات حول أحد قراصنة البطائق البنكية من التوصل إليه[196].

لذا فدور مؤدي خدمات الاتصال مهم في الكشف عن خيوط الجريمة، وإن كان هذا الدور قد يبقى محدودا أحيانا بالنظر للسرعة التي تنتقل بها المعلومات عبر شبكات الاتصال.

---

[194]– المرجع السابق، ص: 5–6.

[195]– المرجع السابق، ص: 6.

[196]– قرار عدد 37 وتاريخ 16–01–2006، ملف عدد 935–05–22، ص: 3، مشار إليه سابقا.

المبحث الثاني: دور التعاون الدولي في مكافحة الجريمة المعلوماتية

قد ترتكب الجرائم المعلوماتية في دولة معينة ويتحقق الفعل الإجرامي في دولة أخرى فهي تتميز بالتباعد الجغرافي بين الفاعل والمجني عليه، هذا التباعد قد يكون ضمن دائرة الحدود الوطنية للدولة، لكن بفعل سيادة شبكة الإنترنت يمتد خارج هذه الحدود ليطال دولة أخرى، مما جعلها بحق جريمة عابرة للحدود (المطلب الأول)، والحقيقة أن مسألة التباعد الجغرافي بين الفعل وتحقق النتيجة من أكثر المسائل التي تثير إشكالات في مجال الجرائم المعلوماتية وبشكل خاص الإجراءات الجنائية، والاختصاص والقانون الواجب التطبيق، مما يشكل عاملا رئيسيا في ضرورة تظافر الجهود الدولية لمكافحة هذه الجرائم (المطلب الثاني).

المطلب الأول: الجريمة المعلوماتية جريمة عابرة للحدود

تشكل الجريمة المعلوماتية صورة من صور العولمة إذ يمكن ارتكاب هذه الجريمة عن بعد وقد يتعدد مكان ارتكابها بين أكثر من دولة، فهي لا تعترف بالحدود القائمة بين الدول سواء الجغرافية أو السياسية، وهذا ما أدى إلى اعتبار الجريمة المعلوماتية من الجرائم الدولية، وكذا من الجرائم ذات البعد الدولي، وتأخذ بعدا دوليا من حيث إمكانية وقوع الفعل الإجرامي داخل دولة معينة إلا أنها تمتد إلى خارج إقليمها، مما يعني خضوعها لأكثر من قانون جنائي كما هو الشأن في جرائم المخدرات والإرهاب وغسل الأموال، وتعتبر جريمة دولية في الحالة التي يكون أحد أطرافها شخصا دوليا، كما يمكن أن تكون في مقابل ذلك جريمة وطنية إذ أن لها أثرا إقليميا فحجم الأثر المكاني يحتويها كأي جريمة ثانية إذ ينبغي أن تبدأ في نطاق إقليمي معين، ومن تم ينعقد الاختصاص للتشريع الجنائي لذلك الإقليم[197].

[197]– **نبيلة هبة هروال:** مرجع سابق، ص: 38–39–40.

وقد ساهمت شبكة الإنترنت بشكل كبير في إلغاء أي حدود جغرافية فيما بين الدول، إذ يمكن التحدث بين أشخاص في بلدان مختلفة في نفس الوقت على هذه الشبكة من خلال الدردشة (Chat) وقد يتبادلون المعلومات فيما بينهم حول تقنيات قرصنة الحسابات البنكية، ويوزعون الأدوار بينهم بشكل منظم بخصوص سحب الأموال من الشبابيك الأوتوماتيكية، فقد تعرف أحد المتهمين بتزوير بطائق الائتمان وهو مواطن مغربي عن طريق ما يعرف (بالشات) على أجانب تعلم منهم كيفية قرصنة الحسابات البنكية، ونظرا لعدم توفره على آلة (MSR) وبطائق لإتمام العمليات داخل المغرب اضطر إلى تحويل المبالغ المختلسة إلى بعض أفراد عائلته بالخارج حيث توصل بنصيبه من ذلك عبر وكالة وسترن يونيون، كما تعامل مع أجانب عبر الإنترنت أحدهما إسباني والآخر أمريكي في هذا المجال[198].

ومن الجرائم العابرة للحدود أيضا، جريمة ارتكبت في فرنسا تتعلق بتعرض حسابات بنكية لبعض الفرنسيين لاقتطاعات من أبناكهم، وذلك لأداء ثمن مشتريات عن طريق شبكة الإنترنت دون أن يكون أصحاب هذه الحسابات البنكية قد أقدموا على تلك العمليات، وبعد البحث تبين أن إحدى المشتريات التي تمت عن طريق الإنترنت تسلمها مواطن مغربي بالرباط، وأن طلبات التزود بالمشتريات تمت انطلاقا من نفس المدينة عبر أجهزة حواسيب في حوزة معهد دولي للدراسات العليا[199].

كما قام مغربي بولوج شبكة الإنترنت باستعمال الأمن الإلكتروني IP الخاص بالولايات المتحدة الأمريكية كما لو كان يقطن بها، وقام بالتنقيب على استمارة الزبناء المملوكة لدى الأبناك المتواجدة بها ومن بينها بايبال وإيباي وريجيون ووزعها لدى جميع المنخرطين بشبكة الإنترنت، وطلب منهم ملأها بجميع المعلومات الخاصة بهم للحفاظ على التدابير الأمنية لهم وبعثها له، وعندما توصل صندوق الرسائل

[198]– قرار عدد 364 وتاريخ 17–04–2006، ملف عدد 22/05/740، ص: 4، مشار إليه سابقا.

[199]– ملف جنائي عدد 971–04–22 وتاريخ 07–05–2007، ص: 3، مشار إليه سابقا.

الإلكترونية الخاص به شرع في تخزين تلك المعلومات بالحاسوب ثم حولها إلى بطائق الشبابيك البنكية بعدما يحتفظ برقم القن السري بكل واحدة على حدة ويتوجه إلى أي مؤسسة بنكية بالمغرب وبواسطة البطائق والقن السري يقوم بسحب المبالغ المالية التي بلغ مجموعها 30 مليون سنتيم وذلك في غضون فترة وجيزة لا تتجاوز مدة 15 يوما[200].

أكثر من هذا، هناك مجرمون يقومون بسحب مبالغ مالية مهمة من أرصدة الضحايا من دول مختلفة، كدول الشرق الأوسط خاصة مصر والإمارات العربية المتحدة والكويت، والدول الأوربية خاصة إسبانيا بواسطة بطائق بنكية تمت قرصنتها بالمغرب[201].

ومنهم من يقوم بتحويل مبالغ مالية من وكالات بنكية بالولايات المتحدة الأمريكية لفائدة بعض الأشخاص بالمغرب باستخدام تقنيات الحاسوب والإنترنت والمس بالنظم المعلوماتية الخاصة ببعض الشركات المتواجدة بالولايات المتحدة الأمريكية بواسطة فيروسات[202].

من هنا تبرز خطورة الجريمة المعلوماتية التي لا تتطلب ضرورة تواجد مرتكبها بمسرح وقوعها بل يمكنه تحقيق نتائجها من أي مكان بالعالم، الأمر الذي يقتضي تكثيف الجهود لأجل مكافحتها.

المطلب الثاني: التعاون الدولي في مواجهة الجرائم المعلوماتية

إن المخاطر التي تتعرض لها البرامج والنظم المعلوماتية على حد سواء باتت تهدد مختلف الأنشطة والقطاعات مما جعل الجهود الدولية تصب كلها في اتجاه التصدي لهذه المخاطر سواء منها تلك المستهدفة للبرامج أو البيانات المدرجة في هذه

[200]– قرار عدد 633 وتاريخ 26–06–2006، ملف عدد 22/05/461، ص: 3، مشار إليه سابقا.

[201]– قرار عدد 299 وتاريخ 23–03–2006، ملف عدد 22/05/736، ص: 6، مشار إليه سابقا.

[202]– قرار عدد 721 وتاريخ 12–09–2006، ملف عدد 22/06/600، ص: 2–3–4، مشار إليه سابقا.

البرامج أيا كان نوعها أو مضمونها، فبالرغم من مختلف الجهود المبذولة بصفة انفرادية من طرف الدول، فإن التصدي للتطور الذي تعرفه الجرائم المعلوماتية أمر صعب المنال، بالتالي اتسمت قدرتها على مواكبة الانتهاكات المتعددة بالمحدودية، خاصة وأن المجرمين المعلوماتيين قادرين على تحديد الحلقات الضعيفة من سلسلة المنظومة الجزائية في مجال الإجرام المعلوماتي، إذ بوسعهم استغلالها بهدف الحيلولة دون تتبعهم وتقديمهم للمحاكم، لذلك ما انفكت الجهود الدولية تتآزر في سبيل إرساء الآليات والإجراءات الملائمة لمكافحة هذا الصنف المستحدث من الجرائم.

ففي إطار التعاون القضائي المغربي الفرنسي تم التوصل إلى بعض المجرمين المختصين بقرصنة الحسابات البنكية وذلك بناء على إنابة قضائية صادرة عن السيدة كاركولو قاضية التحقيق بالمحكمة الكبرى بمارموند بفرنسا بتاريخ 28-04-2000 رقم 600 ضد مجهول، وكذا الانتداب القضائي الصادر عن السيد قاضي التحقيق بتاريخ 19-06-2000 في ملف الانتداب الدولي عدد 51 م.ع 2000[203].

كما أن التوصل إلى معدل أحد الفيروسات التي مست بالأنظمة المعلوماتية الأمريكية جاء بناء على معلومات واردة عن مكتب التحقيقات الأمريكية زودت بها الإدارة العامة للأمن الوطني[204].

لذلك فإن تكوين المحققين في مجال البحث عن الأدلة في الجرائم المعلوماتية لا يؤتي ثماره على المستوى الوطني فحسب وإنما يؤهلهم لبلوغ مستوى الخبرة المطلوب وفقا للمعايير الدولية حتى يكون التعاون الدولي منتجا في مكافحة الإجرام

[203]- ملف جنائي عدد 971-04-22 وتاريخ 07-05-2007، ص: 2-3، مشار إليه سابقا.

[204]- قرار عدد 721 وتاريخ 12-09-2006، ملف عدد 22/06/600، مشار إليه سابقا.

المعلوماتي وذلك لمعالجة وسائل الإثبات الرقمية بذات النجاعة والفاعلية باعتبار أن الجريمة المعلوماتية لا تقف عند الحدود الجغرافية[205].

وإزاء تنامي ظاهرة الإجرام المعلوماتي لم تجد دول الاتحاد الأوربي غير سبيل مجانسة قوانينها الإجرائية والموضوعية تمهيدا للتعاون القضائي فيما بينها كآلية حتمية لمكافحة هذه الظاهرة، فبادرت بإجراء المفاوضات والمشاورات في هذا الشأن طوال أربع سنوات، توجت بمصادقة المجلس الأوربي على اتفاقية "بودابست" المتعلقة بالإجرام السيبيري بتاريخ 23 نونبر 2001، وخلال المؤتمر السادس للمنظمة الدولية للشرطة الجنائية "إنتربول" المنعقد بالقاهرة من 13 إلى 15 أبريل 2005، تم الوقوف على المخاطر المحدقة بالهياكل الوطنية والدولية نتيجة تنامي الجرائم السيبيرية بسرعة فائقة، والتوصل إلى ضرورة تحسيس الجهات المسؤولة عن العدالة الجزائية والإدارات العمومية والمؤسسات الخاصة للعمل على دعم مواردها بما يضمن التحدي لتلك الجرائم والحرص على ضمان سرعة وأمان تبادل المعلومات بشأن الاستعمال غير المشروع لتكنولوجيا الاتصال، ووجوب توحيد القوانين الجزائية بفرعيها الإجرائي والموضوعي[206].

وبالرغم من الغياب الواضح لأي تنسيق رسمي عربي ملموس في إطار اتفاقية أو تنظيم إقليمي فيما يخص مكافحة الجرائم المعلوماتية، إلا أن الجهود العلمية والأمنية بشكل خاص واضحة ومتوالية في مجال رصد هذه الجرائم ومنها:

---

[205]– **محمد العسكري**: "خصوصيات الإثبات في الجرائم المعلوماتية"، مجلة القضاء والتشريع، يوليوز 2007، العدد 7 السنة 47،ص: 168.

[206]– المرجع السابق، ص: 169–170.

- ندوة حول الجرائم الناجمة عن التطور التكنولوجي نظمتها الجمعية الوطنية للدفاع الاجتماعي بنادي ضباط الأمن عمان، الأردن، خلال الفترة من 28-1998/10/29؛
- ندوة المواجهة الأمنية للجرائم المعلوماتية 1999 مركز البحوث والدراسات لشرطة دبي؛
- مؤتمر جرائم الإنترنت بأكاديمية اتصالات دبي في الفترة 22-23 أكتوبر 2000؛
- ندوة دراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، نظمتها أكاديمية نايف العربية للعلوم الأمنية، تونس 2000؛
- المؤتمر الخليجي الثاني لأمن الإنترنت بمسقط في الفترة من 24-25 أبريل 2001[207]؛
- الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر بالدار البيضاء، المغرب في الفترة 19-20 يونيو 2007[208].

ورغم ذلك فإن مواجهة الجرائم المعلوماتية تكتنفه عدة عراقيل لصعوبة تتبع هذه الجريمة أحيانا في شبكة الإنترنت وكذا تتبع حركة شبكات الاتصال العالمية المتصلة بالشبكة، كما أن الاختلافات في النظرة التشريعية لبعض الجرائم التقنية تحول دون

---

[207]- **فايز بن عبد الله الشهري** : "التحديات الأمنية المصاحبة لوسائل الاتصال الجديدة"، دراسة وصفية تأصيلية للظاهرة الإجرامية على شبكة الإنترنت، منشور بالدليل الإلكترون ي www.arablawinfo.com، تاريخ ولوج الموقع يوم السبت 22 نونبر 2008 على الساعة الثالثة زوالا.

[208]- هذه الندوة أقيمت بدعم من برنامج الأمم المتحدة الإنمائي ووزارة العدل بالمملكة المغربية، في إطار برنامج تعزيز حكم القانون في بعض الدول العربية، مشروع تحديث النيابات العامة، غير منشورة.

الوصول إلى اتفاقيات عالمية محددة، لاختلاف الثقافات وتباين الرؤى حول التهديدات التي يخشاها كل مجتمع ويرى إيلاءها الأولوية قبل سواها، إضافة إلى تفاقم أعدادها بشكل يربك الأجهزة الأمنية والقضائية.

خـاتـمة:

لا حاجة للتذكير بأن الجريمة المعلوماتية ظاهرة إجرامية مستجدة تحمل في طياتها العديد من المخاطر وتكلف ضحاياها خسائر جسيمة، إنما لابد من القول بأنها نتيجة حتمية للتطور العملي والتقني الذي شهده عصر المعلوميات، تستهدف المال والأشخاص وحتى القطاعات الحيوية داخل المجتمع، لذا فالتصدي لهذا النمط المستحدث من الإجرام لا يتحقق بتفسير النصوص التقليدية على اختلافها على نحو لا تحتمله، أو التوسع في تحديد مفهوم الأموال بإدخال المعلومات المعالجة آليا في نطاقها، بل على المشرع تطوير ترسانته القانونية وعدم الاقتصار على القوانين التي سنها لمواجهة بعض الصعوبات الطارئة والتي همت تجريم الأنشطة الماسة بنظم

المعالجة الآلية للمعطيات والاعتداءات الإرهابية التي تستخدم هذه الأنظمة، إلى جانب المساس بحقوق المؤلف والحقوق المجاورة المرتبطة ببرامج الحاسوب وقواعد المعطيات الآلية، وكذا تجريم توظيف وسائل الاتصال ومنها الإنترنت لتحريض القاصرين على الدعارة أو البغاء أو تشجيعهم عليها أو تسهيلها لهم أو في استغلال صورهم في مواد إباحية، لأنها مع ذلك تبقى قاصرة عن الإحاطة بمختلف مظاهر هذه الجريمة، وذلك من أجل ضمان حسن معالجة القضاء للقضايا المعروضة عليه وتكييفها قانونيا التكييف الصحيح، بفتح المجال أمامه لتطبيق النصوص القانونية المناسبة لكل واقعة خاصة مع تنوع أشكال الجريمة، ولتوحيد الرؤى وتفادي تضارب العمل القضائي في إعطاء أوصاف قانونية مختلفة لنفس الفعل المجرم، بالنظر لدور القضاء في التصدي للجريمة المعلوماتية وزجر مرتكبيها الذين يعدون مجرمين متمرسين يلجأون دائما لتطهير المحيط الذي يعملون فيه، مما يصعب معه اكتشافهم أو تحديد هوياتهم، وهو ما يستدعي إيلاء الاهتمام بآليات البحث المعتمدة في رصد الجريمة التي تبقى محدودة لاحتواء مظاهر إساءة المعلومات، فالقدرة الفائقة التي تنتقل بها المعلومات والآثار المدمرة التي تخلفها الهجمات الواقعة على الأنظمة المعلوماتية والمواقع باستعمال الفيروسات وضلوع تقنيين وخبراء في ذلك، يحد من التدخلات الزجرية خاصة على شبكة الإنترنت مما يقتضي مراجعة قانون المسطرة الجنائية حتى يستجيب لمتطلبات البحث وتفتيش قواعد المعطيات الآلية باستعمال الشبكة، دون أن ننسى أهمية تأهيل وإعداد الشرطة التقنية وسلطات التحقيق في جمع الأدلة باستعمال التقنيات العلمية، حتى يتم استخلاص الدليل في إطار قانوني يضمن سلامة هذا الاستخلاص لأغراض قضائية، فالوسائل العلمية وإن كانت تفيد في مهمة الكشف عن الحقيقة إلا أنها قد تعصف أحيانا بحريات وحقوق الأفراد إذا لم يحسن استخدامها، مع وجوب التفكير في تطوير التعاون العربي والدولي من خلال عقد اتفاقيات مشتركة أو المصادقة على الاتفاقيات المنظمة لعمليات مكافحة جرائم المعلوميات.

قائمة المراجع

المراجع المعتمدة باللغة العربية:

الكتب:

- **محمد سامي الشوا:** "ثورة المعلومات انعكاساتها على قانون العقوبات"، دار النهضة العربية، طبعة 1998.
- **علي كحلون:** "الجوانب القانونية لقنوات الاتصال الحديثة والتجارة الالكترونية"، دار إسهامات في أدبيات المؤسسة، تونس، طبعة 2002.
- **نائلة عادل محمد فريد قورة:** "جرائم الحاسب الآلي الاقتصادية"، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى 2005.

- **عبد الكريم غالي:** محاور في المعلوميات والقانون، البوكيلي للطباعة والنشر والتوزيع، القنيطرة، الطبعة الأولى، 1997.
- **محمد السعيد خشبة:** "مقدمة في التجهيز الإلكتروني للبيانات"، جامعة الأزهر القاهرة، طبعة 1984.
- **محمد محمد شتا:** "الحماية الجنائية لبرامج الحاسب الآلي" دار الجامعة الجديدة للنشر، الإسكندرية، طبعة 2001.
- **أحمد خليفة الملط:** "الجرائم المعلوماتية"، دار الفكر الجامعي، الإسكندرية، طبعة 2005.
- **هشام محمد فريد رستم :** "قانون العقوبات ومخاطر تقنية المعلومات"، مكتبة الآلات الحديثة أسيوط، طبعة 1994.
- **أحمد المناعسة:** "جرائم الحاسب الآلي والإنترنت"، دراسة مقارنة، دار وائل للنشر والتوزيع، عمان.
- **الشرقاوي الغزواني نور الدين:** "قانون المعلوميات"، مطبعة Print diffusion، سلا، الطبعة الأولى 1999.
- **جميل عبد الباقي الصغير :** "الانترنت والقانون الجنائي" الأحكام الموضوعية للجرائم المتعلقة بالانترنت، دار النهضة العربية القاهرة، طبعة 2001.
- **جميل عبد الباقي الصغير:** "القانون الجنائي والتكنولوجيا الحديثة" الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، الطبعة الأولى 1992.
- **انتصار نوري الغريب:** "أمن الكمبيوتر والقانون"، دار الراتب الجامعية، بيروت، طبعة 1994.
- **محمد عبد الله أبو بكر سلامة :** "جرائم الكمبيوتر والانترنت" منشأة المعارف الإسكندرية، طبعة 2006.

- **محمد محمد الألفي** :" المسؤولية الجنائية عن الجرائم الأخلاقية عبر الانترنت"، المكتب المصري الحديث، القاهرة، الطبعة الأولى: 2005.
- **فاروق حسين:** "الإنترنت الشبكة الدولية للمعلومات"، دار الراتب الجامعية، بيروت، طبعة 1997.
- **أبو العلا علي أبو العلا النمر:** "الحماية الوطنية للملكية الفكرية"، دار النهضة العربية، القاهرة، طبعة 1998.
- **منير محمد الجنبيهي وممدوح الجنبيهي :** "جرائم الإنترنت"، دار الفكر الجامعي الإسكندرية، طبعة 2004.
- **وليد الزيدي:** "القرصنة على الإنترنت والحاسوب"، دار أسامة للنشر والتوزيع، الأردن، الطبعة الأولى 2003.
- **نبيلة هبة هروال:** "الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات"، دار الفكر الجامعي الإسكندرية، طبعة 2007.
- **محمد الأمين البشري:** "التحقيق في الجرائم المستحدثة"، جامعة نايف للعلوم الأمنية الرياض، الطبعة الأولى 2004.
- **عفيفي كامل عفيفي** : "جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون– دراسة مقارنة– منشورات الحلبي الحقوقية، بيروت، طبعة 2003.
- **هلالي عبد الإله أحمد:** "التزام الشاهد بالإعلام في الجرائم المعلوماتية"، –دراسة مقارنة– دار النهضة العربية، الطبعة الأولى 2000.
- **يونس عرب:** "موسوعة القانون وتقنية المعلومات"، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والإنترنت، الجزء الأول، منشورات اتحاد المعارف العربية، الطبعة الأولى.

- **أبو اليزيد المنبت** : "الحقوق على المصنفات الأدبية والفنية والعلمية"، منشأة المعارف الإسكندرية، الطبعة الأولى 1967.
- **طارق بن عبد الله الشدي** : "مقدمة في الحاسب الآلي وتقنية المعلومات"، دار الوطن، الرياض، الطبعة الأولى 1995.
- **عبد الله حسين علي محمود** : "سرقة المعلومات المخزنة في الحاسب الآلي"، دار النهضة العربية، القاهرة، الطبعة الأولى 2001.
- **محمد فهمي طلبة:** "فيروسات الحاسب الآلي وأمن البيانات"، موسوعة دلتا، مطابع المكتب المصري الحديث، القاهرة، طبعة 1992.
- **حسن طاهر داود:** "جرائم نظم المعلومات"، أكاديمية نايف للعلوم الأمنية، مركز الدراسات والبحوث، الرياض، طبعة 2000.
- **محمد علي العريان:** "الجرائم المعلوماتية"، دار الجامعة الجديدة للنشر، الإسكندرية، طبعة 2004.
- **عبد الفتاح بيومي حجازي** : "الحماية الجنائية لنظام التجارة الإلكترونية"، دار الفكر الجامعي الإسكندرية.
- **هدى حامد قشقوش:** جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، طبعة 1992.
- **كيلاني عبد الراضي محمود** : "المسؤولية عن الاستعمال غير المشروع لبطاقات الوفاء والضمان"، دار النهضة العربية، القاهرة، طبعة 2001.
- **طوني عيسى:** "حول الدفع الإلكتروني بالبطاقة الائتمانية في شبكة الإنترنت"، بحث تمت المشاركة به في أعمال المؤتمر العملي السنوي لكلية الحقوق بجامعة بيروت العربية منشور بكتاب تحت عنوان الجديد في أعمال المصارف من الوجهتين القانونية والاقتصادية الجزء

الأول: الجديد في التقنيات المصرفية، منشورات الحلبي الحقوقية، بيروت الطبعة الأولى 2002.

الرسائل والأطروحات:

- **عبد الكريم غالي:** "المعلوميات القانونية"،، خصوصياتها ومدى تطبيقها في المغرب، رسالة لنيل دبلوم الدراسات العليا في القانون الخاص، جامعة محمد الخامس، كلية العلوم القانونية والاقتصادية والاجتماعية بالرباط، السنة الجامعية 1988 و1989.
- **عبد الكريم غالي:** "قانون المعلوميات، الحماية القانونية للإنسان من مخاطر المعلوميات"، أطروحة لنيل دكتوراه الدولة في القانون الخاص، جامعة محمد الخامس، كلية العلوم القانونية والاقتصادية والاجتماعية بالرباط، السنة الجامعية: 1994-1995.
- **طارق عبد الرحمان ناجي كميل:** التعاقد عبر الإنترنت وآثاره، دراسة مقارنة، رسالة لنيل دبلوم الدراسات العليا المعمقة في القانون الخاص، جامعة محمد الخامس، كلية العلوم القانونية والاقتصادية والاجتماعية بالرباط، السنة الجامعية 2003-2004.
- **عبد الرحيم زروق:** "حماية المعلوميات من الجرائم المرتكبة عبر الانترنت"، رسالة لنيل دبلوم الدراسات العليا المعمقة في القانون الخاص، جامعة محمد الأول، كلية العلوم القانونية والاقتصادية والاجتماعية بوجدة، السنة الجامعية 2006-2007.
- **أحمد البختي:** "استعمال الوسائل الإلكترونية في المعاملات التجارية"، رسالة لنيل دبلوم الدراسات العليا المعمقة في القانون الخاص، جامعة محمد الخامس، كلية العلوم القانونية والاقتصادية والاجتماعية السويسي بالرباط، السنة الجامعية 2003-2004.
- **تيسير الغمري:** "الإطار القانوني لقواعد البيانات الإلكترونيةِ"، بحث لنيل دبلوم الدراسات العليا المعمقة في القانون الخاص، جامعة محمد الخامس أكدال-الرباط.

المجلات:

- **عبد الله العلوي البلغيتي:** "الإجرام المعاصر أسبابه وأساليب معالجته"، مقال مقدم في إطار سلسلة الندوات والأيام الدراسية لوزارة العدل، العدد 3، 2004 تحت عنوان السياسة الجنائية بالمغرب، واقع وآفاق، المجلد الأول، الأعمال التحضيرية أيام، 9 و 10 و 11 دجنبر 2004 بمكناس، منشورات جمعية المعلومة القانونية والقضائية.
- **عبد الكريم غالي:** "الحماية الجنائية للمعلوميات على ضوء القانون المغربي"، مجلة الملحق القضائي، العدد 34، مارس 2002.
- **عبد الكريم غالي:** إشكالية حماية البرامج المعلوماتية على ضوء القانون المتعلق بحقوق التأليف والحقوق المجاورة الصادر في 15 فبراير 2000، مجلة كتابة الضبط العدد 9، الطبعة 2001.
- **محمد الشافعي:** "بطاقات الأداء والائتمان بالمغرب"، سلسلة البحوث القانونية 5، مراكش الطبعة الأولى، 2002.
- **بشرى النية:** "حماية برامج الحاسوب عن طريق قواعد القانون الجنائي"، حماية للمصالح الخاصة والنظام العام، المجلة المغربية لقانون الأعمال والمقاولات، العدد 7 يناير 2005.
- **محمد بوشيبة:** حماية برامج الحاسوب طبقا لقانون 00-2 المنظم لحقوق المؤلف والحقوق المجاورة، مجلة القضاء والقانون، العدد 150.
- **محمد العسكري :** "خصوصيات الإثبات في الجرائم المعلوماتية"، مجلة القضاء والتشريع، يوليوز 2007، العدد 7 السنة 47.
- **محمد عبد الرحيم:** "جرائم الانترنت والاحتساب عليها"، بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت، المجلد الثالث، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة. الطبعة الثالثة 2004.
- **محمد كرام:** "صعوبة إثبات الجرائم المرتكبة عن طريق التقنيات الحديثة"، مجلة المحامي العدد 44-45.
- **أحمد آيت الطالب :** تقنيات البحث وإجراءات المسطرة المتبعة في جرائم الانترنت المعلوميات مجلة الملف، العدد 9 نونبر 2006.

✍ **الحسين القمري:** "القيمة القانونية للوثائق الصادرة عن الحاسوب"، مجلة الدفاع عدد 4، 2003.

المراجع المعتمدة باللغة الفرنسية:

Ouvrages et périodiques :

- **GAVALDA (Christian) & Stoufflet (jean) :** « effets de commerce chéque cartes de paiement et de crédit », troisiéme édition, litec 1998.
- **Tazi Sadeq Houria** : l'ordinateur, le fraudeur et le juge (observations à propos de l'affaire des manipulations télé phoniques), in revue marocaine de droit de l'économie du développement n° 11-1986 colloque « droit et informatique » Casablanca du 18 au 20 avril 1985.
- **Elhadi Chaibainou** : Revue « informatique juridique et droit de l'informatique » n° 3, casablanca, 1990.
- **Frédérique touboul**, le logiciel, analyse juridique, FEDUCI. LGD. J, 1986.
- **Mohieddine Amzazi** : « informatique et droit pénal », in revue marocaine de droit de l'économie du développement

Les sites éléctroniques :

- www.arablawinfo.com
- www.ubm.org..tn,upload/Pdf/si/CMI.Pdf.
- http://doc.abhatoo.net.ma/doc/img/ pdf/syspai100602.pdf.
- www.google.com.

الفهرس