جامعة عبد الرحمان ميرة _بجاية_
كلية الحقوق والعلوم السياسية
قسم القانون الخاص

السلوك الإجرامي للمجرم المعلوماتي

مذكرة لنيل شهادة الماستر في الحقوق
تخصص: القانون الخاص والعلوم الجنائية

من إعداد الطالبين:

بن منصور صالح
كـــوش أنيـــســـة

إشراف الأستاذ
طباش عز الدين

لجنة المناقشة

-الأستاذ خلفي عبد الرحمان .....رئيسا
-الأستاذ طباش عزالدين.....مشرفا
-الأستاذ شنين صالح.....ممتحنا

السنة الجامعية 2014-2015

"...إنـي رأيـت أنـه لا يكتـب إنسـانًا كتابًـا فـي يومـه، إلا وقـال فـي غـده لـو غيـر هـذا لكـان أحسـن، ولـو زيـد لكـان يستحسـن، ولـو قـدم لكـان أفضـل ولـو تـرك لكـان أجمـل، وهـذا مـن أعظـم العبـر، وهـو دليـل علـى اسـتيلاء الـنقص على جملة البشر"

"عماد الدين الأصفهاني"

إهداء

أهدي هذا العمل المتواضع إلى من أوصاني بهما ربي

برًا وإحسانًا والدي الكريمين أطال الله في عمرهما ومتعهما بالصحة والعافية

إلى كل أشقائي كل باسمه

إلى كل أصدقائي الأعزاء

إلى كل أسرة الحقوق والعلوم السياسية

إلى كل من ساعدني في إعداد هذا العمل ولو بالكلمة الطيبة

وشجعني إلى المضي قدمًا بكل صدق

إلى كل شخص غيور على هذا الوطن الحبيب

صالح

إهداء

أهدي هذا العمل البسيط :

إلى أمي وأبي العزيزين حفظهما الله اللذان سهرا وتعبا على تعليمي، وعلماني معنى الكفاح وأوصلاني إلى ما أنا عليه.

إلى أخي وأخواتي، سندي في الدنيا ولا أحصى لهم فضل.

إلى أساتذتي الذين تتلمذت على أياديهم، وأمدوني بنصائحهم، وتوجيهاتهم.

إلى كل الأصدقاء والأقارب وكل رفقاء الدراسة.

إلى كل أفراد دفعتي دون استثناء.

إلى كل من سقط من قلمي سهوًا.

أنيسة

شكر وتقدير

إنما الشكر الأول إلى الله عز وجل الذي وهبنا الصبر

وحسن التدبير ومكننا من تخطي الصعاب لإتمام هذا البحث

وعملًا بقوله صلى الله عليه وسلم « **من لم يشكر الناس لا يشكر الله** »

نتقدم بالشكر الجزيل وعظيم الامتنان إلى الأستاذ المشرف" **طباش عز الدين**"

على تفضله بقبول الإشراف على هذه المذكرة

والعناية والاهتمام التي أولانا بها

ونتقدم بعظيم التقدير والثناء للسادة الأساتذة أعضاء لجنة المناقشة

كل باسمه على قبولهم مناقشة هذا البحث

إلى كل أساتذة كلية الحقوق والعلوم السياسية لجامعة بجاية

إلى كل من قدم يد المساعدة لإنجاز هذا البحث

صالح/أنيسة

قائمة المختصرات

أولاً:باللغة العربية

ج.ر.ج.ج: جريدة رسمية جمهورية جزائرية.

د.ن.س: دون سنة النشر.

د.ج: دينار جزائري.

ص.ص: من الصفحة إلى الصفحة.

ص: صفحة.

ط: طبعة.

ق. ت.إ: قانون التأمينات الإجتماعية.

ق.ع: قانون العقوبات.

ثانيًا: باللغة الفرنسية

Ed: édition.

INC: incorporée

J.C.P : juris-classeur périodique.

P P: de page a la page.

P: page.

R.I.D.P: revue internationale de droit pénale.

مقدمة

أفرزت العقود الأخيرة ثورة من نوع أخر متعلقة بوسائل الاتصال والمعلومات لعل من أهمها ظهور أجهزة الحاسب الآلي ذات المستوى العالي، وهذا التطور أدى إلى استحداث شبكات ونظم المعلومات حتى بات يطلق على هذه التقنية بالنظام المعلوماتي.

وبعدما كانت الإتصالات تعتمد على الهاتف والفاكس والتلغراف ظهرت الإنترنت وأصبحت الوسيلة المثلى في الإتصالات ونقل المعلومات وتقديمها، فهذه التقنيات كانت لها الأثر الإيجابي على حياة الفرد والمجتمع، إذ بفضل هذه التقنية زالت الحدود الجغرافية بين أفراد المجتمعات المختلفة إذ لم يصبح فقط العالم قرية صغيرة بل أصبح كالبيت من زجاج لما توفره تقنية المعلومات من عنصري السرعة والدقة في نقل وتبادل المعلومة بين الأفراد والمجتمعات.

إلا أنه بالرغم من المزايا الهائلة التي تحققت وتتحقق كل يوم بفضل تقنية المعلومات على جميع الأصعدة وفي شتّى ميادين الحياة، فإنّ هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل جملة من الإنعكاسات السلبية الخطيرة جراء سوء إستخدام هذه التقنية المتطورة، والإنحراف عن الغرض المرجو منها إذ أدت إلى تفشي ظاهرة إجرامية مستحدثة ألا وهي ظاهرة الجريمة المعلوماتية.

هذا ما أدى بالضرورة إلى بروز طائفة جديدة من المجرمين تختلف عن طائفة المجرمين في الجرائم التقليدية، فالمجرم لم يعد يقتصر على من يُشهر سلاحه في وجه ضحيته بل أصبح ينفرد بأسلوب مستحدث في إرتكاب جرائمه باستخدام أخر ما توصلت إليه العلوم التقنية والتكنولوجية واستغلالها لممارسة نشاطاته الإجرامية دون ملاقاة ضحيته.

إذ يستعملون أساليب ناعمة في ارتكاب جرائمهم على خلاف المجرمين التقليدين، فهذا التطور التكنولوجي في عالم التقنية والذي أدى إلى إبراز جرائم مستحدثة انعكست على السلوك الإجرامي للمجرم المعلوماتي.

ومن خلال ما سبق تتضح لنا الأهمية البالغة التي يكتسيها هذا الموضوع، من خلال محاولة تحديد مفهوم الجريمة المعلوماتية باعتبارها من الجرائم المستحدثة نسبيًا، ودراسة السلوك الإجرامي للمجرم المعلوماتي من خلال تحديد دوافعه الإجرامية والسمات التي ينفرد بها، ثم محاولة وضع تصنيف لفئات المجرم المعلوماتي.

وما يزيد من أهمية هذا البحث أن سلوكيات المجرم المعلوماتي تنفرد بأساليب تقنية ومستحدثة من خلال محاولة إرتكابه لأفعاله الإجرامية، وسوف نحاول تحديد أهم هذه السلوكيات من خلال إستعراض أهم الجرائم المستحدثة التي يسعى المجرم المعلوماتي لإرتكابها، واستظهار مدى الحماية القانونية التي وفرها المشرع الجزائري للمعلومات من خطر سلوكيات المجرم المعلوماتي.

ومن خلال ما سبق يقتضي منا محاولة الإجابة على هذا السؤال المحوري المتمثل في **ما هو أثر خصوصية السلوك الإجرامي للمجرم المعلوماتي في التجريم والعقاب؟**

وسنعتمد في بحثنا هذا على المنهج الوصفي التحليلي من أجل محاولة الإجابة على هذه الإشكالية، فهو منهجًا وصفيًا عند وصف الجريمة المعلوماتية والمجرم المعلوماتي من خلال تبيان خصائص هذه الجريمة وفاعلها، وسنعتمد على المنهاج التحليلي عند دراسة سلوكيات المجرم المعلوماتي في كل شكل من أشكال الاعتداءات على المعلومات المجسد لهذا السلوك الإجرامي، ومحاولة تحديد موقف المشرع الجزائري من الحماية التي وفرها للمعلوماتية.

ومن أجل دراسة هذا الموضوع إرتأينا تقسيم بحثنا إلى فصلين، تطرقنا إلى ماهية الجريمة المعلوماتية في الفصل الأول، ثم إلى الأفعال الإجرامية التي تجسد السلوك الإجرامي للمجرم المعلوماتي في الفصل الثاني.

الفصل الأوّل

ماهية الجريمة المعلوماتية

بما أن الجريمة المعلوماتية تعتبر نمطًا مستحدثاً من أنماط الإجرام، وباعتبارها شكلت ثورة على نظم الجريمة المختلفة، فإن كانت تقترب من الجريمة التقليدية في أركانها العامة والخاصة، إذ تحتاج لفاعل ومجني عليه وموضوع للجريمة، إلا أنها تختلف عن الجرائم التقليدية من حيث صفات الفاعل ومميزاته، وطبيعة السلوك الإجرامي المنفرد بخاصية معنوية فريدة، ومسرح للجريمة ذي طابع معنوي، بالإضافة إلى عدم قدرة النصوص الجزائية العقابية التقليدية على الإحاطة بهذه الصور الإجرامية الجديدة التي ابتكرها عقل الجاني[1].

ولهذا سنحاول في هذا الفصل الأول تحديد المقصود من الجريمة المعلوماتية والصعوبات التي تَقف عائقاً في وجه هذا التحديد، كونها تعتبر نمطاً مستحدثاً من أنماط الإجرام، بالإضافة إلى الطبيعة المتميزة التي تنفرد بها هذه الجريمة عن غيرها، مروراً بمحاولة تحديد طبيعة هذه الجريمة كل هذا سنتناوله في(المبحث الأول)؛ أما في (المبحث الثاني) سنتطرق إلى الفاعل(الجاني) في الجريمة المعلوماتية من خلال تبيّان دوافع ارتكاب الجريمة المعلوماتية وسمات وخصائص التي يتميز بها مرتكبُ هذه الجرائم وطوائفهم.

[1]–جلال محمد الزعبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية (دراسة مقارنة)؛ دار الثقافة للنشر والتوزيع، الأُردن، 2010، ص. 62.

المبحث الأول

الجريمة المعلوماتية بين الموضوع والوسيلة

فلما كانت الجريمة المعلوماتية[2] من الأنماط الإجرامية المستحدثة، والتي رافقت التطور التكنولوجي من خلال ظهور وسائل تقنية مستحدثة لارتكاب الجريمة المعلوماتية على خلاف الجرائم التقليدية الأخرى التي قد لا تستلزم توفر وسائل تقنية لاقتراف السلوك غير المشروع من جهة أولى، ومن جهة ثانية فان إستعراض الطبيعة الخاصة للجريمة التقنية وما تثيره من صعوبات، كذلك فان تحديد خصائص هذا النمط المستحدث وتميزه عن الأنماط الأخرى من الإجرام وتحديد دوافع إرتكابه يثير مسائل قانونية على قدر من الأهمية[3]، وعلى هذا سنحاول إستعراض أهم التعريفات الواردة حول الجريمة المعلوماتية مرورًا بدراسة خصوصية هذه الجريمة في (المطلب الأول)؛ أما في (المطلب الثاني) سنحاول تحديد طبيعة هذا النمط المستحدث من الإجرام التقني، وفي (المطلب الثالث) سنبين المقصود بالوسيط الإلكتروني في الجريمة المعلوماتية.

المطلب الأول

مفهوم الجريمة المعلوماتية

إن الجريمة المعلوماتية باعتبارها جريمة مستحدثة أثارت ضجة في الأوساط الفقهية بخصوص تحديد المقصود منها والأفعال الإجرامية التي تدخل في نطاقها ولذلك ارتأينا التعرض لتعريفات المختلفة للجريمة التقنية في (الفرع الأول) والخصائص المميزة لها في (الفرع الثاني).

---

[2]–فالجريمة المعلوماتية ترتكب باستخدام التقنية المعلوماتية، مما يعني أنها ترتكب في مسرح خاص يتمثل في عالم اقتراضي مفرغ **cyberspace** وهو ما يختلف كليا عن المسرح الذي ترتكب فيه الجرائم في صورتها التقليدية.

[3]–محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية؛ دار الثقافة للنشر والتوزيع، الأردن، 2009، ص. 11.

الفرع الأول

تعريف الجريمة المعلوماتية

قبل الخوض في غمار محاولة تعريف الجريمة المعلوماتية يجب الإشارة إلى عدم وجود اتفاق على مصطلح معين للدلالة على هذه الظاهرة الإجرامية المستحدثة[4]، فهناك من يطلق عليها ظاهرة "الغش المعلوماتي"[5]، ومن بين من أطلقوا على الجريمة المعلوماتية هذه التسمية الأستاذ والفقيه الفرنسي Masse ، وهذه الجريمة معروفة أيضاً بسم الاختلاس المعلوماتي، وهناك جانب يرى أن هذه الجريمة ناشئة أساساً من التقدم التكنولوجي ومدى التطور الذي يطرأ عليه، فهو متجدد بصفة دائمة ومستمرة وخاصة في مجال تكنولوجيا المعلومات، إذ يفضل أن يطلق عليها اصطلاح "جرائم التكنولوجيا الحديثة"[6].

أما الرأي الغالب والذي نميل معه نحن من يفضل استعمال مصطلح "الجريمة المعلوماتية" على الجرائم المتعلقة بالحاسب الآلي والإنترنت، فاصطلاح الجرائم المعلوماتية عام ويشمل التقنية الحالية والمستقبلية.

ولقد أحاط بتعريف الجريمة المعلوماتية الكثير من الغموض حيث تعددت الجهود الرامية إلى وضع تعريف جامع مانع لها، لكن الفقه لم يتفق على تعريف محدد ، بل البعض ذهب إلى ترجيح عدم وضع تعريف لها بحجة أن هذا النوع من الإجرام ما هو إلا "**نبيذ قديم في قارورة جديدة**" [7].

في إطار التعريفات الفقهية للجريمة المعلوماتية نجد أن الاتجاهات متباينة في هذا السياق بين موسع لمفهوم الجريمة المعلوماتية ومضيق لها.

---

[4]-chwki(m), la notion de la cybercriminalité ; el iehel, paris, 2006,p.6.

[5]–أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص(الجزء الخاص)؛ الطبعة السادسة عشر، دار هومة، الجزائر، 2013، ص.493.

[6]–علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة(دراسة مقارنة)؛ منشورات زين الحقوقية، لبنان، 2013، ص.85.

[7]–أي أنها جريمة تقليدية ترتكب بأسلوب إلكتروني.

أولاً: التعريف المضيق

ومن التعريفات المضيقة للجريمة المعلوماتية من عرفها بأنها "أي جريمة يكون متطلبًا لاقترافها أن تتوفر لدى فاعلها معرفة بتقنية الحاسب"[8]، وحسب هذا التعريف لإرتكابها يجب أن تتوفر في الفاعل المعرفة الفنية والتقنية باستخدامات الحاسب الآلي، وهو نفس التعريف الذي أوردته وزارة العدل الأمريكية إذ ركزت في تعريفها على أساس سمات شخصية مرتكب الفعل، حيث عرفت الجريمة المعلوماتية على أنها "أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من إرتكابها"، وكذلك عرفها الفقيه دافيد توسون(david thompson) بأنها "أية جريمة يتطلب لاقترافها أن تتوفر لدى فاعلها معرفة بتقنية الحاسوب"[9].

وطبقًا للتعريفات سابقة الذكر فإن جريمة تكنولوجيا المعلومات الحديثة تنحصر في الحالات التي تتطلب قدرًا من المعرفة التقنية في ارتكابها وهو إن تحقق في بعض الأحوال؛ فانه لا يتحقق في كثير منها، ففي كثير من الحالات يُرتكب الفعل بالضغط على زر واحد فقط دون الحاجة إلى هذا القدر من المعرفة التقنية[10].

أما الأستاذ " تريدمان" (tredman) فيرى أنها جرائم تكنولوجية المعلومات تشمل أي جريمة ضد المال، مرتبطة باستخدام المعالجة الآلية للمعلومات[11].

في حين يرى الأستاذ " روزنبلات" (rosenblat) أن الجريمة المعلوماتية عبارة عن نشاط غير مشروع موجه لنسخ أو تغير أو حذف أو الوصول إلى المعلومات المخزنة داخل الكمبيوتر أو تلك التي يتم تحويلها عن طريقه[12].

---

[8]–عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي؛ منشأة المعارف، مصر،2009، ص.22.

[9]–خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنيت؛ دار الثقافة، الأردن،2011، ص.30.

[10]–علي عبود جعفر، المرجع السابق، ص.78.

[11]–نفس المرجع، ص.78.

[12]–محمد أمين الشوابكة، جرائم الحاسوب والإنترنيت (الجريمة المعلوماتية)؛ دار الثقافة للنشر والتوزيع، الأردن، 2009، ص.8–9.

والملاحظ من خلال هذه التعريفات السابقة أن أغلبها ترتكز على معيار موضوع الجريمة، وهو من أهم المعايير وأكثرها قدرة على إيضاح طبيعة ومفهوم الجريمة المعلوماتية، إلا أنهم لم يتجاوزوا المنزلقات التي وقع بها الفقيه (tredman) إذ ضيق هو الأخر من مفهوم جريمة تكنولوجيا المعلومات الحديثة عندما حصر موضوع الجريمة المعلوماتية في الاعتداء على الأموال فقط وأخرج منها جانب كبير من الأفعال غير مشروعة[13].

ثانيًا:التعريف الموسع

ومن جانب أخر فإن هناك تعريفات حاولت التوسيع من مفهوم الجريمة المعلوماتية حيث نجد بعض الفقه يعرفها على أنها" كل سلوك إجرامي يتم بمساعدة الكمبيوتر" أو هي " كل جريمة تتم في محيط أجهزة الكمبيوتر "[14].

أو هي" كل سلوك غير مشروع منافي للأخلاق أو غير مسموح به يرتبط بالمعالجة الآلية للبيانات أو نقلها"[15]، ويعتمد هذا التعريف على معيارين أو لهما وصف السلوك الإجرامي؛ أما الثاني اتصال السلوك بالمعالجة الآلية للبيانات أو نقلها[16].

إذ تم تعريف الجريمة المعلوماتية بحسب هذا الاتجاه على أنها كل سلوك سلبي أو إيجابي يتم بموجبه الاعتداء على البرامج أو المعلومات للإستفادة منها بأي صورة كانت.

فالاتجاه الموسع من مفهوم جرائم المعلومات لا يقيم وزنًا لربط بين إرتكاب الجريمة المعلوماتية وتحقيق نتيجتها وبين إلمام الفاعل أو الشركاء معه بتقنية الحاسب الآلي، وهم لا يقيمون وزنًا لمدى براعة الفاعل وإجادته التقنية أو خبرته ومقدرته، المهم أن تقع الجريمة ولذلك فهم يرون أن جرائم التقنية هي كل فعل غير مشروع يتم بمساعدة الحاسب الآلي[17].

---

[13]–علي عبود جعفر، المرجع السابق، ص.79.

[14]–خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية؛ الدار الجامعية الجديدة، مصر،2008، ص.42.

[15]–عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت(الجرائم)، دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والإنترنت مع الإشارة إلى الجهود مكافحتها محلياً وعربياً ودولياً؛ منشورات الحلبي الحقوقية، لبنان، 2007، ص.16.

[16]–علي عبود جعفر، المرجع السابق، ص.82.

[17]–جلال محمد الزعبي، أسامة أحمد المناعسة، المرجع السابق، ص.67.

ويتبنى الخبير الأمريكي " دون باركر" (don parker) مفهوماً وسعاً للجريمة المعلوماتية، حيث يشير إلى أنها " كل فعل إجرامي متعمد أي كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل"[18].

أما الأساتذة (vivant) و(lestanc) يعرفان الجريمة المعلوماتية بأنها "مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب"[19].

كذلك عُرفَت هذه الجريمة المستحدثة من طرف منظمة الأمم المتحدة من خلال مؤتمرها العاشر لمنع الجريمة ومعاقبة المجرمين فقد تبنت التعريف الأتي للجريمة المعلوماتية " أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية "[20].

ووفقًا لكل ما سبق فالجريمة المعلوماتية يمكن أن نعرفها على أنها كل فعل إيجابي أو سلبي، عمدي مرتبط باستخدام تقنية المعلومات والتي لا يمكن تصور وقوعها إلا بتوفر هذه التقنية، ولا يختلف الأمر سواء أكانت وسيلة تقنية المعلومات أداة لارتكاب النشاط الإجرامي أم كانت محلاً لها أو هدف الاعتداء، ويجب أن نستبعد من الجرائم التقنية الجرائم المرتكبة على مكونات الحاسوب المادية، كذلك يجب أن نستبعد من الجرائم المعلوماتية الجرائم التي يلعب فيها الحاسوب دورا ثانوياً في إرتكاب الجريمة.

الفرع الثاني

خصائص الجريمة المعلوماتية

نظرًا لوقوع هذه الجريمة المستحدثة في غالبية الأحيان في بيئة معلوماتية، حيث تكون المعلومات محل الاعتداء عبارة عن نبضات إلكترونية، فإننا أمام ظاهرة إجرامية ذات طبيعة خاصة وذات صلة بما يعرف بالقانون المعلوماتي[21]، فالجريمة المعلوماتية إفراز ونتاج لتقنية

---

[18]– جلال محمد الزعبي، أسامة أحمد المناعسة، المرجع السابق، ص.66.

[19]–محمد علي العريان، الجرائم المعلوماتية؛ دار الجامعة الجديدة للنشر، مصر، 2004 ، ص.44.

[20]–جلال محمد الزعبي، أسامة أحمد المناعسة، المرجع السابق، ص.69.

[21]–قارة أمال، **الجريمة المعلوماتية**؛ مذكرة ماجستير، كلية الحقوق، جامعة بن عكنون، الجزائر،2001، ص.24.

المعلومات واتساع نطاق تطبيقها في المجتمع، والسياسة الجنائية الحديثة استدعت محاولة حصر خصائص الجريمة المعلوماتية والتي تتسم بلون وطابع قانوني خاص يميزها عن غيرها من الجرائم – سواء المستحدثة منها أو التقليدية – وعلى هذا الأساس يمكن ذكر البعض منها على سبيل المثال فيما يلي:

أولا: الجريمة المعلوماتية جريمة عابرة للحدود

إن الجريمة المعلوماتية غالبًا ما تتسم بالطابع الدولي، وذلك لأن الطابع العالمي لشبكة الإنترنيت وما يرتبه من جعل معظم دول العالم في حالة اتصال دائم على الخط en ligne[22]، وهو ما يؤدي إلى الاستخدام الغير الشرعي لهذه الشبكة وما يترتب عنها من أفعال إجرامية عابرة للقارات، إذ تسهل هذه التقنية إرتكاب الجريمة المعلوماتية من دولة إلى دولة أخرى فهذه الأخيرة لا تعترف بالحدود الجغرافية بين الدول والقارات، ولذلك فهي جريمة عابرة للقارات، وهي كذلك تعتبر شكلًا جديدًا من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة[23].

ولهذا فان جرائم المعلومات تشترك مع غيرها من الجرائم في أنها تتخطى حدود الدول، كتجارة المخدرات مثلًا؛ إلا أنها تتميز عن هذه الأخيرة (تجارة المخدرات) من حيث إمكانية إرتكاب الجريمة المعلوماتية دون الحاجة لمغادرة المقعد المقابل للحاسب الآلي[24]، وبالنقر على زر من أزرار لوحة المفاتيح أو الوسائل التقنية المتصلة بالحاسوب بعكس جرائم المخدرات التي تتطلب حركة مادية بين الدول.

فالجريمة المعلوماتية من نوع الجرائم التي يتم ارتكابها عن بعد، إذ يتصف مسرح الجريمة المعلوماتية بطابعه المعنوي حيث لا يتواجد الفاعل والمجني عليه في هذه الجريمة في مكان واحد، وهو ما يعني أن مساحة مصرح الجريمة لم تعد محلية، أي أنها أصبحت عالمية، ومن الأمثلة

---

[22]–خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية؛ المرجع السابق، ص.44.

[23]–خالد ممدوح إبراهيم، التقاضي الإلكتروني؛ دار الفكر الجامعي، مصر،2008، ص.323.

[24]–محمود أحمد عبابنة، المرجع السابق، ص.34.

الدالة على ذلك، تمكن أحد هواة في أوروبا من حل شفرة أحد مراكز " البنتاغون" ومن ثم أصبح المجال أمامه مفتوحًا للعبث ببيانات هذا المركز[25].

هذا التباعد أدى إلى تشتيت الجهود الدولية في مواجهة هذا النوع من الإجرام من خلال تحديد مكان وقوعها واختصاص المحاكم في النظر فيها وجمع المعلومات والتحريات عنها[26]، إذ أصبح التصدي لهذا النوع من الإجرام أمرًا عسيرًا.

فمن حيث المكان قد يتعدد هذا المكان بين أكثر من دولة، ومن الناحية الزمنية تختلف المواقيت بين الدول الأمر الذي يثير التساؤل حول القانون الواجب التطبيق على هذه الجريمة والإجراءات الجنائية المتبع فيها.

وهذا الأمر يثير أيضًا إشكالية ذات صلة " بالتعارض مع سيادة الدول "، والتعارض مع سيادة الدولة قد يعيق من إمكانية القيام بعمل دولي مشترك للحد من جرائم تقنية المعلومات، بحيث يدفع بتلك الجهود إلى أن ترتكز في الأطر القانونية لكل دولة على حدى.

ثانيًا: الجريمة المعلوماتية من الجرائم الهادئة

تعد الجريمة المعلوماتية أقل عنفًا من الجرائم التقليدية، إذ تمتاز الجريمة المعلوماتية بأنها من الجرائم الناعمة وبعدها عن العنف ، فلا تتطلب لإرتكابها العنف ولا استعمال الأدوات الخطيرة كالأسلحة وغيرها، فنقل بيانات ممنوعة أو التلاعب بأرصدة البنوك مثلًا لا تحتاج إلا إلى لمسات أزرار، بل وتعتمد على الدراسة الذهنية والتفكير العلمي المدروس القائم على معرفة بتقنيات الحاسب الآلي[27].

فلا يوجد في واقع الأمر شعور بعدم الأمان تجاه المجرمين في مجال المعلوماتية باعتبار أن مرتكبيها ليسوا من محترفي الإجرام بصفته المتعارف عليه.

---

[25]–محمود أحمد عبابنة، المرجع السابق، ص.34.

[26]–عبد الله عبد الكريم عبد الله، المرجع السابق، ص.33.

[27]–محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن؛ دار الجامعة الجديدة، مصر، 2007، ص.36.

ذهب البعض من الفقه إلى تشبيه جرائم المعلوماتية بجرائم ذوي **الياقات البيضاء(col blanc)**[28]، وسبب ذلك أن هاته الجرائم تتطلب مقدرة عقلية، وذهنية خاصة لدى الجاني إذ أنها لا تتطلب إجراءات تميل إلى العنف.

كما أنه عادة ما يكون مرتكبو هذه الجرائم من ذوي المراكز المرموقة والتخصصات العالية في أعمالهم، وغالبًا ما يُنظر إلى مرتكبي هذه الجرائم بوصفهم مستخدميهم مثاليين والغالبية العظمى منهم لهم مراكز قيادية ويتمتعون علاوة على ذلك بثقة كبيرة في مجال عملهم ولقد قام فريق من علماء النفس بدراسة عدد من الشخصيات مرتكبي أفعال الغش المعلوماتي ولاحظوا أن هؤلاء لا يعيرون أدنى اهتمام إزاء القيم التي ليست لها أثر مادية ولا يدركون دائمًا أن سلوكهم يستحق العقاب[29].

ثالثًا: صعوبة اكتشاف وإثبات الجريمة المعلوماتية

نظرًا لطبيعة الخاصة للجريمة المعلوماتية التي تستقل بها عن غيرها من الجرائم، فان إثباتها يحيط به الكثير من الصعوبات، والتي تتمثل في صعوبة اكتشاف هذه الجريمة التقنية المستحدثة، ويرجع السبب في ذلك إلى أنها لا تترك أثارًا خارجية[30].

فكما سبق أن قلنا فان الجريمة المعلوماتية لا عنف فيها، ولا سفك لدماء، وإنما هي أرقام وبيانات تتغيّر أو تمحى من السجلات المخزنة في ذاكرة الحاسبات وليس لها أي أثر خارجي مرئي[31]، وبمعنى أخر فان جرائم المعلومات يسهل إخفاء وطمس معالمها[32] لذلك يصعب اكتشافها.

بالإضافة إلى ذلك إذا تم اكتشاف الجريمة المعلوماتية يكون عادةً بمحض الصدفة، نظرًا لعدم وجود أثر كتابي عند إرتكاب الجريمة، مما يجعل أمر محو الدليل وطمسه آليًا من قبل المجرم، أمرًا في غاية البساطة والسهولة.

---

[28]–قارة أمال، **الجريمة المعلوماتية**؛ المرجع السابق، ص.24.

[29]–علي عبود جعفر، المرجع السابق، ص.107.

[30]–محمود أحمد عبابنة، المرجع السابق،ص.37.

[31] –محمد علي العريان، المرجع السابق، ص.53.

[32] –عبد الله عبد الكريم عبد الله، المرجع السابق، ص.31.

ومما يزيد الأمر تعقيدًا أن الجاني في الجريمة المعلوماتية لا يهاجم من جهاز الحاسوب الخاص به بل يلجئ إلى مقاهي الإنترنيت ويهاجم من خلالها.

ويرجع السبب في عدم وجود إحصائيات دقيقة تحدّد الحجم الحقيقي لهذه الظاهرة إلى عدم تعاون المجني عليه وذلك بعدم التبليغ عنها أصلًا[33]، وإحجامه عن مساعدة السلطات المختصة في إثبات الجريمة والكشف عنها، وحتى في حالة الإبلاغ، فان المجني عليه لا يتعاون مع جهات التحقيق خوفًا من دعاية مغرضة وضياع ثقة العملاء، باعتبار المجني عليه في الجريمة المعلوماتية عادةً ما يكون بنكًا أو مؤسسة مالية أو مشروع صناعي ضخم يهمه المحافظة على ثقة عملائه وعدم اهتزاز سمعته، ومحاولة منع تقليد أساليب ارتكاب هذه الجريمة[34]، لذلك يفضل المجني عليه تقديم ترضية سريعة لعميله وينهي الأمر داخليًا حتى لا يفقده.

رابعًا: الجريمة المعلوماتية تتم عادةً بتعاون أكثر من شخص

تتميز الجريمة المعلوماتية أنها تتم عادةً بأسلوب منظم أي بتعاون أكثر من شخص واحد في ارتكابها، إذ يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والإنترنيت تتوفر فيه الخبرة اللازمة التي تمكنه من تنفيذ جريمته[35]، وشخص أخر من المحيط أو خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه، والاشتراك في إخراج الجريمة المعلوماتية إلى مسرح الوجود قد يكون اشتراك سلبي، وهو الذي يتضح بالصمت من جانب من يعلم بالجريمة في محاولة منه لتسهيل إتمامها، وقد يكون اشتراكًا ايجابيا وهو الغالب في الكثير من الجرائم ويتم في المساعدة الفنية أو المادية[36]، ويظهر ذلك بوضوح في استئجار القراصنة المحترفين للقيام بالأعمال غير المشروعة المتصلة بالحاسب الآلي مقابل مبالغ يُتفق عليها[37].

---

(33)-Ghernauti (s) ,sécurité informatique et réseaux; Dunod, Paris, 4em éd ,2013, p.42.

(34)–محمد علي العريان، المرجع السابق، ص.54.

(35)–منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنيت والحاسب الآلي و وسائل مكافحتها؛ دار الفكر الجامعي، مصر، 2007. ص.15.

(36)–بن عقون حمزة، **السلوك الإجرامي للمجرم المعلوماتي**، مذكرة ماجستير تخصص علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة،2011، ص.25.

(37)–محمود أحمد عبابنة، المرجع السابق، ص.37.

المطلب الثاني

طبيعة المعلومات

لقد نتج عن التطور الهائل في مجال التكنولوجيا والتقنية العالية جرائم مستحدثة من بينها الجريمة المعلوماتية، والتي تتميز بنمط إجرامي يختلف عن النمط التقليدي في الجرائم الأخرى. وتحديد النمط الإجرامي في الجريمة المعلوماتية تكتنفه صعوبات كثيرة ترجع إلى الطبيعة الخاصة لهذا النوع من الإجرام، إذ أن هذا النمط الإجرامي يطال المعلومات التي لا يخفى على أحد أن هناك اتجاهات فقهية متنافرة بخصوص تحديد المقصود بها وبطبيعتها، حيث أن هناك اتجاه الأول، يرى أن المعلومة لها طبيعة من نوع خاص، والاتجاه الثاني الذي يرى أن المعلومة ما هي إلا مجموعة مستحدثة من القيم.

فالمعلومة من حيث اللغة، مشتقة من كلمة "علم"، ودلالتها فيها تدور بوجه عام حول المعرفة التي يمكن نقلها واكتسابها؛ أما من حيث الاصطلاح فيمكن تعريفها بأنها " مجموعة رموز يستخلص منها معنى معين في مجال محدد، وتتمتع بالتحديد، والابتكار، والاستئثار"، وعلى هذا فهي ذات قيمة اقتصادية[38].

وباعتبار أن المعلومات هي الأساس المكون للمعلوماتية وتعرف على أنها علم المعالجة الآلية للبيانات والمعلومات[39]، ومن هنا تتضح العلاقة بين الجريمة المعلوماتية والمعلومات، والتي تدفع لطرح التساؤلات التالية؛ ما هو الوضع القانوني للمعلومة؟ هل يمكن حمايتها من أي اعتداء خاصة إذا اعتبرناها من القيم القابلة للاستئثار؟

---

[38]–سوير سفيان، **جرائم المعلوماتية**؛ مذكرة ماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر،2011، ص.10.

[39]–محمود أحمد عبابنة، المرجع السابق، ص.21.

الفرع الأول

المعلومات لها طبيعة من نوع خاص

يرى الفقه التقليدي أن المعلومة لها طبيعة من نوع خاص وذلك انطلاقا من حقيقة أن وصف القيمة يضفي على الأشياء المادية وحدها وهي القيم القابلة للاستحواذ والاستئثار، وبالنظر للمعلومات كطبيعة معنوية فانه من غير المعقول أن تكون قابلة للاستحواذ وفقًا لهذا المنهاج إلا في ضوء حقوق الملكية الفكرية[40].

إذن فكل معلومة مخزنة لا تنتمي إلى المواد الأدبية أو الصناعية أو الذهنية، لا تندرج ضمن القيم المحمية، غير أن القول بذلك ينفي موقف الفقه والقضاء اللذان يعترفان بوجود اعتداء يجب العقاب عليه عند الاستيلاء غير المشروع على معلومات الغير، ولذلك فقد حاول هذا الاتجاه أن يحمي هذه المعلومات كالتالي:

أولًا: الحماية عن طريق دعوى المنافسة غير المشروعة

يرى أنصار هذا الاتجاه أن أساس العقاب هي المنافسة غير المشروعة التي تتأسس على توفر الخطأ عند الإستلاء على معلومات الغير والتي تتمثل في عدم القدرة على الاستئثار بالشيء وذلك استنادًا إلى منطوق حكم محكمة النقض الفرنسية " إن الغاية من المنافسة غير المشروعة هي تأمين حماية الشخص الذي لا يمكن أن ينتفع بأي حق استثنائي"، رغم أن محكمة النقض رأت عدم توفر الخطأ المستوجب للتعويض لعدم توفر شروط قبول دعوى المنافسة غير المشروعة[41].

ثانيًا: الحماية عن طريق نظرية التصرفات الطفيلية

لقد حاول الأستاذ **ليتورنو letourneau** أن يبرر الخطأ المعترف به وفقًا لهذا الحكم استنادًا إلى تطبيق الواسع لنظرية التصرفات الطفيلية وبالرغم من استبعاد المعلومة من نطاق القيم المالية،

---

[40]–محمد على العريان، المرجع السابق، ص.49.

[41]–نفس المرجع، ص.49.

فهذا لا يمنع من إسباغ الحماية القانونية عليها، بالتوسع في نظرية التصرفات الطفيلية، وهذا لا يتعارض والاعتراف بحق الاستئثار على المعلومة[42].

ثالثًا: الحماية عن طريق نظرية الإثراء بلا سبب

حاول الأستاذ " **لـوكس**" **lucas** تبرير الخطأ على أساس نظرية الإثراء بلا سبب بوصفه تطبيقًا خاصًا لها وبعيدًا عن دعوى المنافسة غير الشرعية.

ربعًا: الحماية عن طريق دعوى المسؤولية التقصيرية

تبنت محكمة النقض الفرنسية فكرة الخطأ لتعريف بالحق على المعلومات في حرمة الحياة الخاصة وهو الخطأ المبني على أساس المسؤولية التقصيرية لا المنافسة غير المشروعة[43].

الفرع الثاني

المعلومات مجموعة من القيم

يرى هذا الاتجاه الحديث أن المعلومات ما هي إلا مجموعة مستحدثة من القيم، ويعود الفضل في ذلك للأستاذين "كتالا" **Catala** و" فيفانت" **vivant** ، إذ يرى الأستاذ " كتالا"، قابلية المعلومة للاستحواذ كقيمة واستقلالًا عن دعامتها المادية، وذلك لأنها تقّوم وفقًا لسعر السوق متى كانت غير محظورة تجاريًا، وإنها ترتبط بمؤلفها عن طريق علاقة قانونية تتمثل في علاقة المالك بالشيء الذي يملكه، وهي تخص مؤلفها بسبب علاقة التبني التي تجمع بينهما[44].

ويلاحظ أن الأستاذ " كتالا" اعتمد على حجيتين لإعطاء وصف القيمة على المعلومة، الأولى قيمة المعلومة الاقتصادية، والثانية وجود علاقة تبني تجمع بينها وبين مؤلفها[45].

---

(42)–معاشي سميرة، " ماهية الجريمة المعلوماتية "؛ مجلة المنتدى القانوني، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، العدد السابع، د.س.ن، ص.279.

(43) –نفس المرجع، ص.279.

(44) –محمد على العريان، المرجع السابق، ص.50.

(45)–قارة أمال، الحماية الجزائية للمعلوماتية في التشريع الجزائري؛ دار هومة، الجزائر، 2006، ص.17.

أولًا: القيمة الاقتصادية للمعلومة

لقد استندا الأستاذ "كتالا" على أن المعلومة تحتوي على قدر كبير من الأهمية في مجال المنفعة الاقتصادية بالمقارنة في مجال البيانات المادية، وإنه من الواضح أن أي قانون يرفض أن يرى قيمة في الشيء له أهمية اقتصادية ويبقيه بمعزل عن الحماية، وباعتبار أن للمعلومة وبالنظر إلى حقيقتها الذاتية واستقلالها، تعد قيمة في حد ذاتها، ولها بالتأكيد مظهر معنوي ولكنها تملك قيمة اقتصادية مؤكدة، وبحيث يمكن عند الاقتضاء أن ترفعها إلى مصاف القيمة القابلة لأن تحاز حيازة غير مشروعة[46].

ومن المقبول إذًا، وفقًا لأهمية المعلومة وعلى نحو ما أشار إليه الأستاذ "كتالا" أن ينطبق وصف القيمة عليها.

ثانيًا: وجود علاقة التبني التي تجمع بينها وبين مؤلفها

لقد أظهرت الاتجاهات المعاصرة أن تحليل حق الملكية، من شأنه حجب وجود صاحب الحق وهو ما أكده الأستاذ "زاناتي" **zanati** هذا الأخير يرى أنه إذا وضع في الاعتبار الرابطة التي تجمع بين المعلومة ومؤلفها، فيجوز إذن الإقرار بإمكانية حيازة المعلومة بوصفها قيمة.

فالمعلومة وإن كانت شيئًا غير مادي، تصلح لأن تكون محل للحقوق العينية وعلى الأخص حق الملكية، فعلى سبيل المثال تقوم وكالات الأنباء ببيع ما تحصل عليه من معلومات أو أخبار[47].

أما الأستاذ " فيفانت" فيؤسس ذلك على حجتين أيضًا، الأولى مستمدة من رأي الفقيهين "بلانيول" **planiol** و "ريبير" **ripert** وهي أن فكرة الشيء أو القيمة لها صورة معنوية وأن أي نوع محل الحق يمكن أن ينتمي إلى قيمة معنوية ذات طابع اقتصادي وتكون جديرة بالحماية القانونية[48].

---

[46]–محمد علي العريان، المرجع السابق، ص.51.

[47]–محمود أحمد عبابنة، المرجع السابق، ص.22.

[48]–محمد علي العريان، المرجع السابق، ص.50.

أما الحجّة الثانية فيرى الأستاذ " فيفانت" أن كل الأشياء المملوكة ملكية معنوية والتي يعترف بها القانون وترتكز على الاعتراف بأن للمعلومة قيمة، عندما تكون من قبيل البراءات والرسومات، والنماذج والتحصيلات الضرورية وحق المؤلف .

فالإنسان الذي يقدم ويكشف ويطلع الجماعة على شيء بصرف النظر عن الشكل أو الفكرة فهو يقدم لهم معلومة بالمعنى الواسع لكنها خاصة به ويجب أن تعامل هذه الأخيرة بوصفها قيمة تصبح محلًا للحق، فلا تكون ملكية معنوية بدون الإقرار بالقيمة المعلوماتية.

ولما كانت البرامج في جوهرها معلومات معالجة بطريقة أليا ولها قيمة اقتصادية، فانه يجب معاملتها معاملة المال أي كون المعلومات مال قابل للتملك أو الاستغلال على أساس قيمته الاقتصادية وليس على أساس كيانه المادي[49].

المطلب الثالث

الوسيط الإلكتروني في جرائم تقنية المعلومات

السلوك الذي تنهض به الجريمة متعدد ومتنوع، والجريمة المعلوماتية لا تخرج عن هذه القاعدة، فكثير من السلوكيات التي تنهض بها الجريمة المعلوماتية ترتكب عن طريق الحاسب الآلي أو تقع عليه بواسطة شبكة الإنترنيت، وهي جريمة ذات ارتباط وثيق بالحاسب الآلي، ولا يمكن وقوعها بمعزل عن الحاسب الآلي– أيًا كانت صورته–[50]؛ إلا أن قسمًا من الجرائم المعلوماتية الحديثة تستخدم فيها أجهزة إلكترونية –محسوبة– تقوم بدور الحاسب الآلي مثل الهواتف الذكية واللوحات الإلكترونية التي يمكن عن طريقها الاتصال بشبكة الإنترنت.

الفرع الأول

الحاسب الآلي (الكومبيوتر)

لقد تطور الحاسوب من آلة حسابية بسيطة إلى جهاز كهربائي يقوم بعدة عمليات فجمع بين الآلة الحاسبة والآلة الكاتبة وآلة تؤدي عدة عمليات، وعرف الحاسوب بأنه " آلة تقوم بأداء

---

[49]–نهلا عبد القادر المومني، الجرائم المعلوماتية؛ دار الثقافة، الطبعة الثانية، الأردن،2010، ص.106.

[50]–عبد الفتاح حجازي بيومي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي؛ المرجع السابق، ص.20.

العمليات الحسابية، واتخاذ القرارات المنطقية على البيانات الرقمية بوسائل إلكترونية، وذلك تحت تحكم البرامج المخزنة فيها"[51]، فالكومبيوتر بهذا الوصف يحتوي على مكونات مادية متمثلة في شاشة الجهاز أو وحدة العرض التي تمكننا من رؤية البيانات أو الأوامر المراد تحقيقها، ولوحة المفاتيح والذي يشبه الطابعة العادية بالإضافة إلى القرص الصلب وكذلك القرص المضغوط وكلاهما يكونان وحدة المعالجة الرئيسية أو وحدة التحكم، وقد تنحصر وظيفتها بعمليات التنسيق بين وحدات الكومبيوتر وضبط العمليات التي يقوم بها المستخدم؛ أما الجانب المعلوماتي في الحاسوب تتمثل في الأنظمة المعالجة والمخزنة في الحاسوب والتي تسمح بتشغيل الفعال للحاسب الآلي.

لكن رغم الإيجابيات التي يزخر بها جهاز الحاسب الآلي له سلبيات كذلك، وتتمثل في إرتكاب مختلف الجرائم المعلوماتية بواسطة جهاز الحاسب الآلي.

فالأشخاص الذين يستخدمون هذا الأجهزة الرقمية منهم الأسوياء، ومنهم دون ذلك[52]، ومجرمي المعلومات يختلفون في ميولهم وأغراضهم، فالشخص الذي يميل إلى الانحراف أو يقع في عالم الجريمة يمارس هذا السلوك بطريقته الخاصة وبوسيلته الخاصة.

فقد يكون الكومبيوتر وسيلة لارتكاب الجريمة المعلوماتية مثل ما هو عليه الحال في الشخص الذي يستهدف المعطيات المعالجة أو المخزنة بواسطة الحاسوب، وقد يكون الحاسوب بيئة لاقتراف الجريمة المعلوماتية.

الفرع الثاني

شبكة الإنترنيت

قد تكون شبكة الإنترنيت داخلية في الدولة الواحدة وقد تكون عالمية، الأولى عبارة عن مجموعة من أجهزة الكومبيوتر ترتبط مع بعضها عن طريق كومبيوتر رئيسي تأخذ منه المعلومة الرئيسية **(server)**أي "ملقم" الشبكة، وهذا معمول به في المؤسسات التجارية والتعليمية، والشركات باختلافها حيث تحتوي هذه الشبكة معلومات رئيسية تزود بها الوحدات الفرعية ويتولى الجهاز

---

[51]–خالد عياد الحلبي، المرجع السابق، ص.39.

[52]–عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في الجريمة والمجرم المعلوماتي؛ المرجع السابق، ص.10.

المركزي مهمة تطوير البيانات وحفظها؛ أما الثانية فهي غير مقيدة بحدود من حيث الامتداد، فهي خيوط عنكبوتية ويرمز لها ب **(www)** ويقصد منها**(Word wide web)**، فهي بحق مكتبة تضم كمًا هائلًا من المعلومات والوصول لها يساعد المستخدم من الاستفادة من تلك المعلومات، وهذه الشبكة تمكن الملايين من الاتصال ببعضهم فيكون من الطبيعي أن تسوء سلوكيات البشر لما تقدمه هذه التقنية من إغراءات خصوصًا إذا ما أخذنا بعين الاعتبار سهولة الاستخدام وضعف الرقابة وعدم وجود قواعد قانونية تفرض أنماطًا معينة من السلوك في هذا المجال، وبذلك أصبح للإجرام في الوقت الحاضر صفة تقنية عندما أقترن بوسائل التطور التكنولوجي هذه.

فأصبحنا اليوم نسمع بالمجرم المعلوماتي، الذي يمارس سلوكه غير المشروع بطريقة خاصة، مما جعل من هذا التقدم بيئة للعصابات الإجرامية، إذ تمكنهم خدمة الإنترنيت من التعبير عن أنفسهم من خلال مواقع خاصة بهم على شبكة الإنترنيت، والتي من خلالها يُروجون لأفكارهم ومبادئهم المتطرفة، وعن طريق هذه المواقع تنتقل هذه الأفكار إلى مستخدمي الشبكة ومتصفحي الموقع التي ستكتسب بالضرورة بعض المتعاطفين معها، ولعل ذلك يظهر في المواقع الإلكترونية التي تروج لمناهضة تجريم تعاطي المخدرات أو الاتجار بها، فيمكن لمستخدم الشبكة الدخول إليها باسم مستعار وليس الحقيقي، وبالتالي يتحدث بكل حرية ويبدي آراءه كيف ما شاء[53].

الفرع الثالث

الأدوات التقنية الأخرى

بادئ ذي بدأ، يجب أن نوضح أن الجريمة المعلوماتية بمفهومها المستحدث لم يعد يقتصر ارتكابها بالضرورة على توفر جهاز الحاسب الآلي، إذ أن التطور التكنولوجي أظهر أجهزة أخرى لا تقل أهمية عن الحاسب الآلي، وتلعب دور في ارتكاب الجريمة المعلوماتية مثل الهواتف النقالة الذكية، إذ أن البعض منها يفوق وبكثير تقنيات الحاسوب، بالإضافة إلى أجهزة إلكترونية أخرى تلعب دور الحاسوب والإنترنيت، مثل خدمة أو شبكة– **المانيتل minitel** – في فرنسا، وتحقق

[53]–عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في الجريمة والمجرم المعلوماتي؛ المرجع السابق، ص.11.

هذه الخدمة عن طريق جهاز يحمل ذات الاسم، حيث شاع استخدامه في فرنسا على نحو واسع منذ منتصف الثمانينات من القرن الماضي.

وتتم هذه الخدمة عن طريق هذا الجهاز الذي يشبه جهاز الحاسب الآلي الشخصي **(pc)** ولكنه صغير الحجم نسبيًا، ويتكون من شاشة صغيرة، ولوحة أزرار تشتمل على الحروف والأرقام مثل تلك الخاصة بالكومبيوتر، وهي وسيلة اتصال مرئية تنقل الكتابة على الشاشة دون الصور، أي أنها وسيلة اتصال بالكتابة، ويكفي لاستعمالها أن يتم إيصاله بخط التليفون، وقد يستعمل هذا الجهاز كذلك في إرتكاب مختلف الجرائم المعلوماتية[54].

ونخلص مما سبق أن الوسيط الإلكتروني في الجريمة المعلوماتية كل ما يتصل بالتكنولوجيا الحديثة، سواء ذو قدرات كهربائية كالحاسوب أو رقمية سلكية أو لا سلكية كالإنترنيت أو أي شبكات إلكترونية أخرى غير معروفة حاليًا قد تظهر في المستقبل وفقًا لمفاهيم التطور العلمي والتكنولوجي.

[54]–عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في الجريمة والمجرم المعلوماتي؛ المرجع السابق، ص.49.

المبحث الثاني

المجرم المعلوماتي

هناك تفرقة تقليدية في دراسات علم الإجرام، تقوم على التمييز بين الإجرام الطبيعي والإجرام الاصطناعي–المكتسب– ونادى بهذه التفرقة عالم الإجرام الإيطالي–جارفالو–، ولقد ثار جدال فقهي يدور حول النوع الذي ينتمي إليه المجرم المعلوماتي[55]، وما يمكن القول في هذا الصدد أن المجرم المعلوماتي يمثل بالنسبة للمجموعات التقليدية أي (الإجرام الطبيعي) شخصية مستقلة قائمة بذاتها، فهو من جهة مثال منفرد " للمجرم الذكي" ومن جهة إنسان اجتماعي بطبعه[56].

ولذلك فإن العقوبة لكي تحقق هدفها في مجال الردع العام أو الخاص، وإذا كنا في مجال الإجرام المعلوماتي فيجب علينا أن ننظر إلى المجرم المعلوماتي من حيث الظروف التي دفعته لارتكاب جريمته وأسبابها وصفاته وذلك حتى يمكن إعادة تأهيله اجتماعيا ويعود إلى حظيرة المجتمع كمواطن صالح ينفع المجتمع ولا يضره، ونظرًا للانتشار ثورة المعلومات وما تبع ذلك من ازدياد عدد الجرائم المعلوماتية سواءً على الصعيد العالمي أو الوطني، فقد حظيت أبحاث علم الإجرام في هذا المجال بالعديد من الدراسات القانونية والتي تحاول كشف النقاب عن فكرة المجرم المعلوماتي[57]، وعلى ذلك سنعرض في المطالب الآتية، صفات المجرم المعلوماتي(مطلب أول)،الدوافع المحفزة لارتكاب الجرائم المعلوماتية(مطلب ثاني)، وأخيرًا سنتطرق إلى تصنيفات المجرم المعلوماتي(مطلب ثالث).

المطلب الأول

السمات الخاصة للمجرم المعلوماتي

ما من شّك أنّ تطور العلوم الجنائية، وما نتج في نطاقها من دراسات وتحديدًا في ميدان علم الإجرام أدى إلا تحديد سمات عامة للمجرمين عمومًا، وسمات خاصة يمكن استظهارها لطائفة

---

[55]–عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في الجريمة و المجرم المعلوماتي؛ المرجع السابق، ص.95.

[56]–محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات؛ الطبعة الثانية، دار النهضة العربية، مصر، 1998، ص.24.

[57]–محمد علي العريان، المرجع السابق، ص.61.

معينة من المجرمين تبعًا للجرائم التي يرتكبونها[58]، فكان من الطبيعي أن يؤدي إرتكاب الجرائم المعلوماتية إلى ظهور وولادة طائفة جديدة من المجرمين، أطلق عليهم جانب من الفقه تسمية "المجرم المعلوماتي".

ولا شك أن الفاعل في الجريمة المعلوماتية يرتكب فعلًا غير مشروع ويعتدي فيه على حق من حقوق الغير، يعد في نظر القانون مجرمًا ويتعرض للعقاب المناسب إذا ما اقترف جريمته.

إذ يقول الخبير الأمريكي "دون باركر" أن المجرم المعلوماتي وإن كان يتميز ببعض السمات الخاصة إلا أنه لا يخرج في النهاية عن كونه مرتكبًا لفعل إجرامي يتطلب توقيع العقاب عليه، فكل ما في الأمر أنه ينتمي إلى طائفة خاصة من المجرمين تقترب في سماتها من جرائم ذوي الياقات البيضاء " الإجرام المكتسب"، من حيث انتماء المجرم في أكثر الحالات إلى وسط اجتماعي، وتميزه بدرجة من العلم والمعرفة، وليس معنى ذلك أنهم أقل خطورة من الناحية الإجرامية من المجرمين ذوي الياقات الزرقاء"المجرم بطبيعته"[59].

باعتبار أن الجريمة المعلوماتية كأي عمل إجرامي أخر، قد ترتكب في شكل اشتراك في جماعة إجرامية فإن هذه الأخيرة تتميز ببعض الخصائص المختلفة عن سمات الفاعل الفرد المستقل في ارتكاب الجريمة المعلوماتية[60]، لذلك سنحاول إستعراض السمات المشتركة بين مرتكبي الجريمة المعلوماتية والسمات التي تنفرد بها الجماعات الإجرامية في جرائم المعلومات.

الفرع الأول

السمات المشتركة بين جميع فئات مرتكبي الإجرام المعلوماتي

باعتبار أن الفاعل في الجريمة المعلوماتية شخص طبيعي كأصل عام[61] يرتكب أفعاله غير المشروعة تعبيرًا عن إرادته الخاصة المستقلة، ووفقًا لعلم الإجرام المعلوماتي فإن الفاعل الفرد في الجريمة المعلوماتية يتمتع بقدر كبير من الذكاء ويتميز عن غيره من المجرمين، واتصافه بسمات

---

[58]–علي عبود جعفر، المرجع السابق، ص.106.

[59]–نفس المرجع، ص.107.

[60]–خالد ممدوح إبراهيم، الجرائم المعلوماتية؛ المرجع السابق، ص.133.

[61]–خالد عياد الحلبي،المرجع السابق، ص.32.

معينة جعلت منه محلًا للعديد من الأبحاث والدراسات، إذ يتميز المجرم المعلوماتي بعدة سمات أهمها:

أولًا: الذكاء

يعتبر الذكاء من أهم صفات مرتكبي الجرائم المعلوماتية، إذ يقال عادةً أن الإجرام المعلوماتي هو إجرام الأذكياء بالمقارنة مع الإجرام التقليدي الذي يميل إلى العنف[62]، فإذا كان من السهل تصور العنف في الإجرام الموجه ضدّ مكونات النظام المادي للمعلومات والذي يحدث غالبًا في إطار العمليات الإرهابية، فإنّه لا يمكن أن يتصور أي عنف في الإجرام الموجه ضدّ المكونات المنطقية والبيانات، وبالتالي يجب أن يكون المجرم على دراية كافية بأنماط الجريمة فهناك أنماط مختلفة يمكن إستخدامها في التلاعب بهذه البيانات تتمثل في"القنابل المنطقية"[63]، كما أن هناك أنماط أخرى تعرف بالفيروسات المعلوماتية[64].

وتأكيدًا على ذلك فقد أجريت دراسة من طرف وزارة الداخلية البريطانية أنّ الأطفال الذين يقضون وقت أطول أمام ألعاب الكمبيوتر يكونون أكثر ذكاءً مقارنة بغيرهم ممن لا يمارسون ألعاب الكمبيوتر، إذ يتوقع دخولهم مجالات الاستخدامات الغير مشروعة لجهاز الكمبيوتر.

ولقد أجريت الدراسة على مائة وسبعة وعشرون (127) شخصًا من بينهم ثلاثة وستون (63) طفلًا، بمقارنتهم مع صغار آخرين وجد أن هواة الكمبيوتر يعتبرون أشخاص أذكياء للغاية ومتحمسين وساعين للإنجاز، كما أفادت المتابعة لمدة خمسة أعوام على هؤلاء الأطفال أنهم تفوقوا دراسيًا والتحقوا بالجامعة، وبوظائف مرموقة[65].

---

[62]–محمد سامي الشوا، المرجع السابق، ص.35.

[63]–القنابل المنطقية: يمكن للجاني زرع تعليمات في برنامج مزود بعدّاد والذي عندما يصل إلى بداية معينة تنطلق هذه التعليمات لتمحوا البرنامج.

[64]–الفيروسات: هي عبارة عن برامج من الحجم الصغير الذي يصعب اكتشافه ويوضع في الأسطوانة ثم يقوم بنسخ نفسه بداخل النظام لتدميره في فترة وجيزة. أنظر: محمد سامي الشوا، المرجع السابق، ص.35.

[65]–خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص.134.

ثانيًا: الخبرة والمهارة

يرى الخبير" دون باركر" أن المهارة هي أبرز خصائص مجرم تكنولوجيا المعلومات، فتنفيذ الجريمة التقنية يتطلب قدرًا من المهارة يتمتع بها الفاعل والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات الحديثة أو مجرد التفاعل الاجتماعي مع الآخرين[66].

إلا أن ذلك لا يعني بالضرورة أن يكون مرتكب جريمة تكنولوجيا المعلومات الحديثة على قدر كبير من العلم في هذا المجال أو أن تكون لديه خبرة كبيرة، بل إن الواقع العملي قد أثبت أن بعض أنجح مجرمي تكنولوجيا المعلومات الحديثة لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في المجال التقني، كما أننا نرى أن عددًا لابسَ به من صور جرائم المعلومات التي تُرتّكب عبر وسيلة تقنية أي عندما لا يكون نظام المعلومات الإلكترونية هو هدف الجريمة، لا يتطلب سوى الحد الأدنى من المعرفة والمهارة لظهور الجريمة أو إمكانية ظهورها[67] .

ثالثًا: المجرم المعلوماتي عائد للإجرام

يعود الكثير من مجرمي المعلومات إلى إرتكاب جرائم أخرى في مجال الكمبيوتر، انطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم، وأدت إلى تقديمهم إلى المحاكمة في المرة الأولى، ويؤدي ذلك إلى العودة إلى الإجرام، وقد ينتهي بهم الأمر كذلك في المرة الثانية إلى تقديمهم للمحاكمة[68].

تتكون هذه النزعة الإجرامية المتوفرة في المجرم المعلوماتي لتأثره بعوامل عضوية ونفسية صاحبت نشأته، ومع اقتران تلك العوامل بعنصر آخر جديد يساعد على استثارة الحالة الإجرامية

---

[66]–علي عبود جعفر، المرجع السابق، ص.107.

[67]–جلال محمد الزعبي، أسامة أحمد المناعسة، المرجع السابق، ص.71.

[68]–عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والإنترنيت؛ دار الكتب القانونية، مصر،2007، ص.107.

ويزيد من قدرة ضغوط عوامل الإجرام وتفوقها على موانع الإقدام، وهذا العنصر الجديد هو الذي أكسب الشخص للمهارة العلمية والتكنولوجية[69].

ربعًا: الميل إلى التقليد

يبلغ الميل إلى التقليد منتهاه حينما يوجد الفرد وسط الجماعة إذ يكون عندئذ أسهل وأسرع انسياقًا لتأثير الغير عليه، ويظهر ذلك في الجريمة المرتكبة عبر الإنترنيت لأن أغلب الجرائم تتم من خلال محاولة الفرد تقليد غيره بالمهارات الفنية مما يؤدي به الأمر إلى ارتكاب الجرائم[70].

لا شك أن ذلك نتيجة لعدم الاستواء في شخصية الفاعل الفرد الذي يتأثر بخاصية الميل إلى التقليد بسبب عدم وجود ضوابط يؤصلها الفرد في ذاته مما يحجم لديه غريزة التفاعل مع الوسط المحيط، وينتهي به الأمر إلى ارتكاب الجريمة.

الفرع الثاني

السمات التي تنفرد بها الجماعات عن الفرد المستقل في إرتكاب جرائم المعلومات

تتميز المجموعات الإجرامية في الجريمة المعلوماتية بمجموعة من السمات التي تختلف عن المجرم الفرد المستقل في هذا النوع من الجرائم، وسنبرز في هذا الفرع أهم هذه سمات.

أولًا: التخطيط والتنظيم

في عالم الشبكات الإلكترونية وخاصة العالمية للإنترنيت، ترتكب أغلب جرائم المعلومات من مجموعة مكونة من عدة أشخاص يحدد لكل شخص دور معين يتم العمل بينهما وفقًا لتخطيط والتنظيم سابق على إرتكاب الجريمة[71].

---

[69]–خالد ممدوح إبراهيم، الجرائم المعلوماتية؛ المرجع السابق، ص.135.

[70]–خالد ممدوح إبراهيم، الجرائم المعلوماتية؛ نفس المرجع، ص.136.

[71]–خالد ممدوح إبراهيم، الجرائم المعلوماتية، نفس المرجع، ص.136.

فغالبًا ما يكون هذا الإجرام متضمن شخص متخصص في الحسابات يقوم بالجانب الفني من المشروع الإجرامي وشخص أخر يساهم في إرتكاب الجريمة، فمثلًا تحتاج جريمة نسخ برامج الحاسب الآلي إلى شخص يقوم بنسخ تلك البرامج، وتحتاج أيضًا إلى من يقوم بعملية البيع[72].

كذلك هو ما عليه الحال في جريمة زرع الفيروسات إذّ تحتاج إلى مجموعة من الأشخاص منهم المبرمج الذي يقومُ بكتابة البرنامج؛ ومنهم المستخدم الذي يقوم بعملية زرع الفيروسات داخل الأجهزة الأخرى.

ثانيًا: التكيف الاجتماعي

فالتكيف الاجتماعي يحتوي على حقيقتين، فالأولى تتمثل في تكيف المجرمين المعلومتين فيما بينهم وتعتبر هذه الخاصية امتداد لسمة التخطيط والتنظيم، مثل التكيف الاجتماعي بين مجموعة لها صفات مشتركة مثل "نوابغ صغار المعلوماتية" –التي سنتطرق إليها لاحقًا–، ولا شك أنهم يتكيفون في أفكارهم ، وهذه الروابط تتعدى النطاق المحلي إلى المجال الدولي.

أما الحقيقة الثانية تكمن في تكيف المجرم المعلوماتي الذي لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به، بل إنه إنسان متكيف اجتماعيا[73]، وهنا يكمن الاختلاف بين المجرم المعلوماتي والمجرم التقليدي من حيث أن الفاعل في الجريمة المعلوماتية يحيى في وسط اجتماعي، فهو اجتماعي بطبعه [74].

وتكيف المجرم مع مجتمعه يزيده الثقة بأنه خارج إطار الشبهات وهذا الشعور يدفعهُ إلى التمادي في إرتكاب جرائمه.

---

[72]– خالد ممدوح إبراهيم، الجرائم المعلوماتية، ص.136–137.

[73]–عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي؛ المرجع السابق، ص.100.

[74]–محمد علي العريان، المرجع السابق، ص.62.

ثالثًا: التطور في السلوك الإجرامي

تتميز الجريمة المعلوماتية بحقيقة مفادها أن دقة تنفيذ العمليات غير المشروعة يستلزم مشاركة أو مساعدة أشخاص آخرين، وقد يكون هذا الاشتراك سلبيًا، والذي يترجم بالصمت، ولكن غالبًا ما يكون إيجابيًا، يتمثل في مساعدة مادية أو فنية[75].

هذا الاشتراك أو تواجد في جماعة إجرامية يؤدي إلى التطور في السلوك الإجرامي، إذ يستأثر المجرم في قدراته العقلية وسرعة اكتسابه المهارة الفنية التي تؤدي به إلى التمرد على محدودية الدور الذي يقوم به في تنفيذ الجريمة وتمكنه من اكتساب أعلى معدلات التقنية المتمثلة التي تمكنه من إثبات قدرته على القيام بالدور الرئيسي في تنفيذ تلك الجريمة[76].

كذلك فإن وجود الفرد في جماعة إجرامية يشكل خطورة عليه إذ يزيد الملكة الإجرامية والتفوق العلمي لديه مما يجعله يطور أسلوب إرتكابه للجرائم .

المطلب الثاني

الدوافع المحفزة لارتكاب الجريمة المعلوماتية

لا شك أن السلوك الإنساني أيًا كان شرًا أم خيرًا، نبيلًا أم رذيلًا له ما يفسره[77]، وما يبعث على القيام به، وهو الذي يطلق عليه بالدافع.

إلا أن الدافع في قانون العقوبات فكرة تشوبها بعض الغموض وعدم اتفاق من جانب الفقه حول تسميته، ولذلك تعددت الاتجاهات واختلفت، فمنهم من يطلق عليه الغاية، ومنهم من يطلق عليه تسمية الغرض أو الباعث، إلا أننا لا نرى لهذه التسميات المختلفة فائدة تذكر لأنها كلها تؤدى إلى معنى واحد وهو الدافع.

فالدافع هو العامل المحرك للإرادة، والذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغض والانتقام، وهو إذن قوة نفسية تدفع الإرادة إلى الاتجاه نحو إرتكاب الجريمة ابتغاء تحقيق غاية

---

[75]–محمد سامي الشوا، المرجع السابق، ص.46.

[76]–خالد ممدوح إبراهيم، الجرائم المعلوماتية؛ المرجع السابق، ص.137.

[77]–محمد أحمد عبابنة، المرجع السابق، ص.22.

معينة، وهو يختلف من جريمة إلى أخرى تبعًا لاختلاف الناس من حيث السن والجنس ودرجة التعلم[78].

أما بالنسبة لجرائم الكمبيوتر والإنترنيت فثمّة دوافع عديدة تحرك الجناة لارتكاب أفعال الاعتداء المختلفة، فبعضها يرجع إلى دافع شخصي ومنها ما يرجع إلى دافع خارجي ومنها ما يكون خاص بالمنشأة وكل هذه الدوافع قد يكون مصدرها هي الرغبة الإجرامية، وسنستعرض من خلال هذا المطلب لعناصر ثلاثة دافعة لارتكاب الجريمة المعلوماتية[79] إذ في (الفرع الأول) سنتطرق إلى الدوافع الشخصية، وفي (الفرع الثاني) سندرس الدوافع الخارجية، أما في (الفرع الثالث) سنعرض الدوافع الخاصة بالمنشأة.

الفرع الأول

الدوافع الشخصية

إن المجرم المعلوماتي يسعى من خلال اقتراف فعله غير المشروع إلى تحقيق المكسب المادي أو دافع التعلم أو رغبة في إثبات الذات وقهر النظام.

أولًا: الدوافع المادية

تعد الرغبة في تحقيق الثراء من العوامل الرئيسية للارتكاب الجريمة عبر الإنترنيت، وهو من أهم الدوافع وأكثرها تحريكًا للمجرم، نظرًا لربح الكبير الذي يمكن أن يحققه هذا النوع من الأنشطة الإجرامية[80]، وغالبًا ما يقع الجاني بمشاكل مادية تعجز عن سداد ديونه المستحقة، أو مشاكل عائلية تعود إلى عدم توفر الأموال، أو الحاجة للعب القمار أو شراء المخدرات أو المراهنات، وللخروج من هذا المآزق يسعى الجاني إلي التلاعب بالأنظمة المعلوماتية للبنوك والمؤسسات المالية لمحاولة تحقيق المكاسب المادية، إما بسرقة الأموال أو بتحويلها لحسابه الشخصي بحيث يستطيع الجاني بمجرد دخوله على أنظمة البنوك معرفة أرقام الحاسب وسرقتها أو تحويلها، عن

---

[78]–بن عقون حمزة، المرجع السابق، ص.46.

[79]–محمد خليفة الملط، الجريمة المعلوماتية؛ دار الفكر الجامعي، مصر، 2006، ص.88.

[80]–نفس المرجع، ص.89.

طريق إستخدام " الفيزا كارت" أو "الماستر كارت" المستعملة في البيع والشراء عبر شبكة الاتصال الدولية من خلال سرقة تلك الأرقام باستخدام شبكة المعلومات[81].

تجدر الإشارة أنه في حالة نجاح المجرم في إرتكابه جريمته عبر الإنترنيت، فإن ذلك قد يدّر عليه أرباحًا طائلة في زمن قياسي والدليل على ذلك ما حدث في فرنسا في سنة 1976 حيث كانت العائدات من إرتكاب جناية السرقة مع حمل السلاح مقدرة ب70.000 فرنك في حين أن جريمة السرقة في مجال المعالجة الآلية للمعطيات حصل منها على 270.000 فرنك أي ما يعادل 38 مرة ، كما أظهرت دراسة قديمة تعرض إليها الخبير دون "باركر" إذ يقول أن(34%) من حالات الغش المرتبط بالحاسوب المعلن عنها من أجل اختلاس الأموال، و(23%) من أجل سرقة المعلومات، و(19%) من أجل الإتلاف، و(15 %) من أجل سرقة وقت الآلة[82].

ثانيًا: دوافع ذهنية ونمطية

الصورة الذهنية لمرتكبي جرائم الحاسوب والإنترنيت غالبًا هي صورة البطل والذكي الذي يستحق الإعجاب لا صورة المجرم الذي يستوجب محاكمته، فغالبًا ما يكون الدافع لدى مرتكبي جرائم المعلومات هي الرغبة في إثبات الذات وتحقيق انتصار على تقنية المعلومات دون أن يكون لهم دوافع آثمة، ويعود ذلك إلى وجود عجز في التقنية أي تترك فرصة لمشيدي برامج الأنظمة المعلوماتية لارتكاب تلك الجرائم[83]، وهذا ما أدى إلى زيادة الاهتمام بأمن الحاسب الآلي وشبكته عن طريق تطوير طرق جديدة، كبرامج التشفير ومن أمثلة ذلك ما تقوم به وزارة الدفاع الأمريكية التي تقوم بتغير أنظمة الترميز للبيانات المستحدثة يوميًا ودوريًا؛ ومن جانب أخر يقف أصحاب التقنية الالكترونية ويتسابقون لخرق هذه الأنظمة وإظهار تفوقهم عليها، كقيام أحد الهواة في أوروبا بحل شفرة أحد مراكز المعلومات في وزارة الدفاع الأمريكية والعبث ببياناتها[84].

---

(81)–خالد ممدوح إبراهيم، الجرائم المعلوماتية؛ المرجع السابق، ص.139.

(82)–أحمد خليفة الملط، المرجع السابق، ص.89.

(83)–نفس المرجع، ص.90.

(84)–محمود أحمد عبابنة، المرجع السابق، ص.25.

ثالثًا: الرغبة في التعلُم

إنّ الرغبة الشديدة في التعلم في كل ما يتعلق بأنظمة الحاسوب والشبكة الإلكترونية قد يكون الدافع وراء إرتكاب جرائم المعلومات، إذ هناك من يرتكب جرائم الإنترنيت بغية الحصول على الجديد من المعلومات وكشف خفايا هذه التقنية المتسارعة النمو والتطور، وهؤلاء الأشخاص يقومون بالبحث واكتشاف الأنظمة والعمل من خلال الجماعة وتعليم بعضهم البعض، ويفضل هؤلاء القراصنة البقاء مجهولين أكبر وقت ممكن حتى يتمكنوا من الاستمرار في التواجد داخل الأنظمة، ويكرس البعض منهم كل وقته في تعلم كيفية اختراق المواقع الممنوعة، والتقنيات الأمنية للأنظمة الحاسوبية[85].

الفرع الثاني

الدوافع خارجية

الإنسان بطبعه مخلوق هش من الناحية السيكولوجية، حيث يمكن في بعض المواقف أن يستسلم للمؤثرات الخارجية أو أن يحدث سلوكه غير المشروع نتيجة لدوافع عديدة دفعته لارتكاب تلك الجرائم[86].

أولًا: دافع الانتقام

يعد دافع الانتقام من أخطر الدوافع التي يمكن أن تدفع الشخص إلى إرتكاب الجريمة لأنه غالبًا ما يصدر من شخص يملك معلومات كبيرة عن مؤسسة أو الشركة التي يعمل بها، و يقوم بدافع الانتقام إما نتيجة فصله من العمل أو تخطيه في الحوافز أو الترقية، فهذه الأمور تدفعه إلى إرتكاب الجريمة[87].

وسوف نجد في معرض تناولنا للجريمة المعلوماتية أن دافع الانتقام من رب العمل هو المحرك الرئيسي الذي يدفع بالموظفين المستخدَمين في الشركات والمؤسسات لارتكاب جرائمهم عبر الإنترنيت ضد تلك المؤسسات التي قامت بتوظيفهم، وربما تمثل أنشطة زرع الفيروسات في نظم

---

[85]–بن عقون حمزة، المرجع السابق، ص.47.

[86]–محمد سامي الشوا، المرجع السابق، ص.52.

[87]–خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص.140.

الكمبيوتر النشاط الرئيسي والغالب لهذه الفئة من الموظفين[88]، ومن الوقائع التي تؤكد ذلك ما حدث في الولايات المتحدة الأمريكية، إذ قام أحد موظفي بإدخال فيروس لشركة التي كان يعمل فيها مما أدى إلى ضياع 160 سجلًا من سجلات العملاء وذلك انتقاما من تلك الشركة لأنها قامة بفصله من العمل[89].

ثانيًا: دافع التعاون والتواطئ على الإضرار

هذا النوع كثير التكرار في الجرائم المعلوماتية، وغالبًا ما يحدث من شخص متخصص في الأنظمة المعالجة الآلية للمعطيات يقوم بالجانب الفني من الشروع الإجرامي، وشخص أخر من المحيط أو خارج المؤسسة المجني عليها لتغطية عمليات التلاعب، وتحويل المكاسب المادية وعادة ما يمارسون التلصص على الأنظمة وتبادل المعلومات بصفة منتظمة[90].

ثالثًا: دافع التهديد

ينتشر هذا الدافع نتيجة الوقوع تحت تهديد وضغط من الغير في مجالات الأعمال التجارية والخاصة بالتجسس والمنافسة[91]، ونذكر في هذا الخصوص موظف يعمل بإحدى مكاتب شركة مشهورة متعددة الجنسيات والتي مركزها مدينة « Sindelfingen » بألمانيا الغربية–سابقًا– حيث كان يتمتع هذا الموظف بسمعة طيّبة لدى كل المنشآت العمالية، وقد لوحظ عقب اختفائه أن هذا الموظف المثالي كان يعمل في الحقيقة مع مجموعة جواسيس أنشأت خصيصًا في ألمانيا الغربية من أجل مهاجمة أنظمتها المعلوماتية، ولقد نجح الجاسوس في أن ينقل إلى ألمانيا الشرقية معلومات هامة حول منشأة تعمل في ألمانيا الغربية ولكن يجب الاعتراف أن الجاسوس كان ضحية ابتزاز وتهديد[92].

---

[88]–أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية لمكافحة جرائم الكمبيوتر والانترنيت، مكتبة الوفاء القانونية، مصر، 2011، ص.129.

[89]–نفس المرجع، ص.129.

[90]–أحمد خليفة الملط، الرجع السابق، ص.90.

[91]–محمد سامي الشوا، المرجع السابق، ص.53.

[92]–نفس المرجع، ص.53.

الفرع الثالث

الدوافع الخاصة بالمنشأة

من الدوافع التي تؤدي إلى زيادة الإجرام المعلوماتي تلك التي تكون خاصة بالمنشأة، خاصة وأن الشخص المسؤول عن المركز المعلوماتي لدى المنشأة يمكّنه وضعه من إستغلال منصبه إذ ما شاء لمصلحته[93].

ففقط الضعف المحتمل لمركز المعالجة، ومركز الثقة التي يتمتع بها الجاني هي أفضل الأسلحة التي يحوزها لارتكاب أفعال الغش المعلوماتي[94]، هذا ما دفع البعض لتمادي في استخدام الأنظمة بصورة غير مشروعة تصل إلى حد إرتكاب جرائم أكثر خطورة ، ونذكر في هذا الشأن أحد أفعال الغش المعلوماتي الأكثر ربحًا والذي اقترف عن طريق إستخدام غير المشروع للحاسب الآلي وتتلخص وقائعها في أن مستشار لدى أحد البنوك الكبرى ويدعى « Stanley rifking » وكان يتمتع بثقة مطلقة من جانب هذا البنك، وقد سمحت له اختصاصاته بالولوج في مفتاحين إلكترونيين من ثالثة مفاتيح أساسية الخاص بتحويلات الإلكترونية لنقود من بنك إلى أخر، وقد تمكن بفضل قدراته في مجال المعالجة الآلية للمعطيات من الوصول للمفتاح الثالث، وتمكن من تحويل في الحال 10مليون دولار إلى حساب بنكي خاص به في سويسرا، ولقد ألقي القبض عليه وصدر ضده حكم بالسجن لمدة 6 سنوات[95].

المطلب الثالث

تصنيف مرتكبي الجرائم المعلوماتية

تشير أبحاث علم الإجرام إلى أنه من الناحية العملية، فإن كل تقنية مستحدثة ينشأ عنها بالضرورة، وفي أي مرحلة من مراحل تطورها ظاهرة إجرامية خاصة بها[96]، وينطبق ذلك بوجه خاص على تقنية المعلومات نظرًا للإمكانيات التي يقدمها الحاسب الآلي، والتي كان من الطبيعي

---

[93]–أحمد خليفة الملط، المرجع السابق، ص.91.

[94]–محمد سامي الشوا، المرجع السابق، ص.54.

[95]–أحمد خليفة الملط، المرجع السابق، ص.91.

[96]–محمد سامي الشوا، المرجع السابق، ص.37.

أن تحمل ظاهرة إجرامية عبر شبكة الإنترنيت وفي طياتها ولادة طائفة جديدة من المجرمين عُرفوا بسم مجرمي المعلومات.

وهذا ما أدى إلى ظهور العديد من الدراسات التي قامت بمحاولة وضع تصنيف لمرتكبي جرائم المعلومات، وتعد من أهمها دراسة الأستاذ " **دون باركر**" الذي ذهب إلى تصنيف مجرمي التقنية الحديثة إلى سبعة أصناف مختلفة، وهناك دراسة أخرى صنّفت مجرمي المعلومات إلى طائفة صغار السن وطائفة البالغين، غير أننا قد لا نجد لهذه التصنيفات أي فائدة تذكر إذ أن هناك العديد من الأفعال قد تقترف من الصغار والكبار معًا، و بالتالي تتداخل وتتشابك، ولكن مع ذلك يمكن أن نُصنف مجرمي المعلومات إلى ثلاثة طوائف وهم الهواة والمبتدئون(الفرع الأول)، طائفة المخربون(الفرع الثاني)، وطائفة المجرمون المحترفون(الفرع الثالث).

الفرع الأول

الهواة والمبتدئون

يعتبر نمط الهواة والمبتدئون من الأنماط الأقل خطورة من المجرمين الآخرين مرتكبي الجرائم التقنية، نظرًا لانتفاء القصد لديهم في إرتكاب الجرائم، ولكن باعتبار هذه الطائفة لا تتوفر على الخبرة الكافية في استخدام الحاسبات الآلية مما يؤدي للوقوع في الكثير من الأخطاء التي يترتب عنها إرتكاب الجريمة المعلوماتية.

أولًا: صغار نوابغ المعلوماتية

هم فئة من صغار السن مولعون بالثورة المعلوماتية وبسبب انتشار الحاسبات الآلية [97] لذلك كان أولئك الشباب يرتكبون الجرائم المعلوماتية عن طريق إستخدام الحاسبات الآلية الخاصة بهم أو بمدارسهم[98]، وهذه الطبقة من الشباب لديهم قدر لا بأس به من الخبرة المعلوماتية، ومن ثمة فهم يمارسون مواهبهم في استخدام الحاسب الآلي بغرض اللهو أو هواية اللعب من أجل الوصول إلى نظم المعلوماتية سواء الخاصة بالوزارات أو الشركات العملاقة أو الشركات التجارية أو

[97]–خالد عياد الحلبي، المرجع السابق، ص.35.

[98]–عبد الفتاح حجازي بيومي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي؛ المرجع السابق، ص.104.

المؤسسات المصرفية، وقد يتطور الأمر بالنسبة لهذه الفئة من الشباب خاصة إذا كان بينهم من لديه علم ومعرفة بعملية البرمجة، ومع ذلك فهؤلاء الشباب تكون غايتهم في النهاية مجرد التسلية والملاحظة وليس لديهم كأصل عام دوافع لارتكاب أفعال إجرامية، ولكن لا يجب أن نستخف بها لأن خطر انزلاق هذه الفئة إلى احتراف الأفعال غير المشروعة وارتكاب الجرائم المعلوماتية هو احتمال قائم، وعندئذ يتحول من مجرد هاوي صغير للأفعال غير المشروعة إلى محترف لها، ومثال على الجرائم التي تقترفها هذه الطائفة الإجرامية، ما حدث في الولايات المتحدة الأمريكية أين قام أولاد المدرسة الثانوية في مدينة "مانهاتن" عام1980بختراق شبكة اتصالات البيانات الكندية وتدمير ملفات زبائن الشركة[99].

ثانيًا: الهاكرز(hackers)

طائفة الهاكرز تقترب إلى حد بعيد مع فئة صغار نوابغ المعلوماتية ولكنها تتفوق عليها علمًا ومعرفة بعملية البرمجة وغايتها أيضًا التسلية والملاحظة والتطفل[100].

" فالهاكرز" هم متطفلون يتحدّون إجراءات أمن النُظم والشبكات لا تتوفر لديهم في الغالب الأعم دوافع حاقدة أو تخريبية، وإنما ينطلقون من دوافع التحدي وإثبات الذات، وتظهر جليًا في اعترافات متهم يبلغ من العمر 17 سنة أمام القضاء الألماني حيث نسب إليه دخوله بطريقة غير مشروعة في نظام "الفيديو تكس"**videotext** الخاص ب**bundaspost** والمعروفة بمصطلح « **btx** » ودافع المتهم عن نفسه قائلا " تملكني إحساس قوي بأن أكون مفيد في كشف عيوب نظام « **btx** »، ولذلك أرسلت في الحال إلى مجموعة عمل « **btx** » كل العناصر التي اكتشفتها بالصدفة والتي أظهرت تشككها فيما يخص حماية البيانات، لاسيما وأن غالبية ملاحظاتي لم تكن معروفة بعد لدى هؤلاء مما أتاح الأمر إلى تلاشي هذه العيوب.

وأضاف كذلك أنه مولع بنظام « **btx** » ويكرس نفسه له صباحًا مساء، ولكنه ليس شريرًا على الإطلاق، كبعض الأشخاص القائمين على نظام « **btx** » الذين لا يملكون أي كفاءة[101] .

---

[99]–محمود أحمد عبابنة،المرجع السابق، ص.41.

[100]–خليفة أحمد الملط، المرجع السابق، ص.117.

[101]–عبد الفتاح حجازي بيومي،نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي؛المرجع السابق، ص.104.

ويجب أن نشير إلى أن أول مرة تم إطلاق على المجرم المعلوماتي مصطلح (hackers) كان في الستينيات القرن الماضي، إذ أُطلق على طلبة الجامعات الأمريكية، ممن يتميزون بقدر عالي من الكفاءة التقنية ويتفاخرون بإلمامهم بعلوم الحاسوب، وبقدرتهم على اختراق شبكات الحاسب الآلي وبجهودهم الذاتية، وبدون الاستعانة بأية تعليمات من أية مصادر.

ومن الأمثلة عن الأفعال التي ارتكبتها طائفة "الهاكرز" ما قامت به **عصابة"414"** الأمريكية والتي نسبت إليها أكثر من ستين(60) فعلًا، وتعديًا، واختراقا لذاكرات الحاسب الآلي مما نتج عنها أضرارًا لحقت بالمنشآت العامة والخاصة[102].

الفرع الثاني

المخربون

إن فئة المجرمون المخربون في الجريمة المعلوماتية لا يرتكبون أفعالهم الإجرامية طمعًا في الإشادة العقلية أو إثبات الذات مثل طائفة الهواة والمبتدئون، وإنما عادةً ما يكونوا مستخدَمين في منشأة أو مؤسسة تساعدهم صفتهم في ارتكاب جرائمهم ضد تلك المنشأة، وقد يكون دافع الحقد والغضب من هيئة معينة يبعث بهم لارتكاب أفعالهم غير المشروعة.

أولًا: المستخدَمون

المجرم في بعض صور جرائم المعلومات هو شخص مستخدَم فقط، تتوافر لديه المعرفة الكافية بآلية عمل الحاسب الآلي ومكوناته، ووظائفه الأساسية، ومعرفة بعض البرامج التي يجري العمل بها في المنشاة كبرامج المحاسبة والتطبيق والتعليمية المختلفة، ولديه أيضًا معرفة كافية بآلية عمل الشبكات المعلوماتية، وهو إذّ يرتكب الجريمة لأنه يتمتع بهذه الصفة فقط فلا علاقة له بالنظام المعلوماتي إلا من ناحية الاستخدام فقط[103].

فهذه الفئة من المجرمين المرتكبين للجريمة المستحدثة في اتساع وازدياد مستمر تبعًا لتطور نظام المعلومات وتقنيات الحاسب الآلي وازدياد انتشارها المتسارع في شتى نواحي الحياة[104].

---

[102]–محمد سامي الشوا، المرجع السابق، ص.40.

[103]–جلال محمد الزعبي، أسامة أحمد المناعسة، المرجع السابق، ص.72.

[104]–خالد عياد الحلبي، المرجع السابق، ص.34.

وطريقة إرتكاب هذه الفئة لجرائم التقنية تتم إما بالدخول إلى مراكز الحاسب الآلي المركزي مباشرة بأي وسيلة، أو باستخدام إحدى وحدات الحاسب الأعلى الفرعية المرتبطة بالحاسب الآلي المركزي، سواءً باستخدام كلمة السر، أو باستخدام البطاقة الممغنطة أو أي وسيلة أخرى تسمح بذلك، بحيث يكون نظام المعلوماتية بالنسبة للمجرمين المستخدمين بمثابة ألعوبة لاقتراف جرائمهم[105].

فهم يملكون المعرفة اللازمة والتقنية الكافية للتلاعب بالحاسبات الآلية وفقًا لهواهم، وهم يشكلون من أجل ذلك خطر كبير.

ثانيًا: الغرباء

وهم أشخاص أجانب عن تلك المؤسسة، ويندرج تحت هذه الطائفة المستخدمون الذين ليس لهم تصريح بالعمل على النظام المعلوماتي الخاص بتلك المؤسسة أو الشركة وفي الغالب يكون التخريب هو هدف هؤلاء الدخلاء أي أنهم يقومون بالدخول على الكمبيوتر بغرض إرتكاب جرائم التخريب أو قد يكون المكسب المادي هو الهدف من عملية الدخول[106].

ولا شك أن عملية الدخول على أنظمة الحاسب الآلي من الغرباء يكون لها تأثير بالغ الضرر وتلك الأفعال التخريبية تكلف المنشأة أو الهيئة ملايين الدولارات لمحاولة إصلاح تلك النظم التقنية التي أفسدتها العمليات التخريبية.

الفرع الثالث

المجرمون المحترفون

ويطلق على المجرمون المحترفون في الجريمة المعلوماتية "الكراكرز"**(crackers)** أو "الهاكرز" ذو النوايا الآثمة لذلك يجب التفرقة بين الصنفين "فالهاكرز" هو شخص متخصص أو خبير في مجال الحاسب الآلي لديه حب التحدي وإثبات الذات والجدارة، ويتمثل ذلك في دخولهم لقواعد الخاصة بالآخرين دون إلحاق الضرر بهم فقط بهدف التحدي، على خلاف "الكراكرز" فهو شخص أيضًا متخصص أو خبير في مجال الحاسب الآلي ولكنه يقوم بأنشطة غير قانونية تتمثل في

---

[105]–محمد سامي الشوا، المرجع السابق، ص.45.

[106]–خالد ممدوح إبراهيم، الجرائم المعلوماتية؛ المرجع السابق، ص.147.

تدمير الأنظمة المعلوماتية، فإن اعتداءاتهم تعكس ميولًا إجراميًا تُنبئ عنها رغباتهم في إحداث الإضرار بالغير وتتراوح أعمارهم من 25 إلى45 سنة[107].

لذلك فإن هذه الطائفة تعد من بين الفئات الأخرى وتهدف اعتداءات أفرادها في الأساس إلى تحقيق الكسب المادي لهم أو الجهة التي كلفتهم لارتكاب جرائم التقنية الحديثة، كما تهدف اعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبير عن مواقف فكرية أو نظرية أو فلسفية، وتبعًا لتخصصهم في نوع معين من الجرائم أو تبعًا للوسيلة المتبعة من قبلهم في إرتكاب الجريمة، فمثلًا نجد طائفة محترفي التجسس بمختلف أنواعه، وطائفة مجرمي الإحتيال والتزوير وهؤلاء هم الطائفة التي تكون أغراضها متجهة إلى تحقيق كسب مادي والإستلاء على أموال الآخرين[108].

إذ تعكس اعتداءاتهم ميولهم الإجرامي والرغبة في الإتلاف والتخزين، والتعديل والتخريب باستخدام الفيروسات أو القنابل المنطقية، باعتبار هم من أصحاب التخصصات العالية، ولهم الهيمنة الكاملة على تقنيات الحاسوب والشبكة المعلوماتية ومثال ذلك ما قام به "الكراكرز" الجزائري المدعو(أنجل) المنحدر من مدينة قسنطينة والذي كرس جل وقته لإتلاف موقع (أرض إسرائيل) وهو أشهر وأكبر موقع إسرائيلي فرانكوفوني على الشبكة العنكبوتية يشرف عليه مهندس في الإلكترونيك يدعى(يوسي طيب) الذي يعمل بوزارة الدفاع الإسرائيلية، ويساهم في تطوير الأسلحة في هذا الكيان... وقد طلب (يوسي) من (أنجل) مرارًا الكف عن اختراق موقعه وتدميره، إلا أن "الكراكرز" الجزائري لم يكف عن ذلك[109]، لذلك يعتبر الكراكرز من أخطر التصنيفات السابقة لما يمثلون من تهديد مباشر وخطير على الأنشطة والمصالح عبر الشبكة العنكبوتية.

---

[107]–خالد عياد الحلبي، المرجع السابق، ص.33.

[108]–علي عبود جعفر، المرجع السابق، ص.116.

[109]–فلالي رشيد، "الشروق تقضي يومًا مع أشهر قراصنة الإنترنت في الجزائر"، عدد صادر في 22 نوفمبر 2008، مقال متوفر على الموقع:
http://www.echoroukonline.com/ara/?news=29084

الفصل الثاني

سلوكيات المجرم في الجرائم المعلوماتية

تختلف سلوكيات المجرم المعلوماتي في إرتكاب الجريمة في مجال المعالجة الآلية للمعطيات باختلاف الجريمة[110]، فمحل هذه الجريمة إمّا أن تكون المعلومة بحد ذاتها ويظهر ذلك بوضوح في جرائم سّرقة المال المعلوماتي، وجرائم الإتلاف والتزوير المعلوماتي ممّا يؤدي إلى توقف أو عرقلة عمل النظام المعلوماتي؛ وإمّا أن يكون محل الجريمة المعلوماتية الذّمة المالية للغير والتعدي عليها كالتحويل الإلكتروني غير المشروع للأموال، أو المساس بالحياة الخاصة للأشخاص عبر الإنترنيت في هذه الحالة تكون تقنية المعلومات وسيلة لارتكاب هذه الجرائم وليست محلاً لها.

في هذّا الفصل سنتطرق إلى تقسيم سلوكيات المجرم المعلوماتي إلى صنفين في المبحث الأول سندرس(سلوكيات المجرم المعلوماتي المرتكبة بواسطة تقنية المعلومات)؛ أما المبحث الثاني سنتناول فيه (سلوكيات المجرم المعلوماتي المرتكبة على تكنولوجيا المعلومات).

[110]–جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول:الجرائم الناشئة عن إستخدام الحاسب الآلي؛ مكتبة دار النهضة العربية، مصر، 1992، ص.18.

المبحث الأول

سلوكيات المجرم المعلوماتي المرتكبة بواسطة تقنية المعلومات

إنّ المجرم المعلوماتي في بعض الأحيان يستعين بتقنية المعلومات لارتكاب أفعاله غير المشروعة، أي باستخدام المعلوماتية كوسيلة لتنفيذ جريمته ففي هذّه الحالة لا تكون المعلومات محلاً للجريمة بل وسيلة لاقترافها[111]، ومن أبرز صور هذه الجرائم، جرائم الأموال كالتحويل غير المشروع للأموال (المطلب الأول)، والجرائم الواقعة على الأشخاص كالجرائم الماسة بالحياة الخاصة (المطلب الثاني)، وجريمتي الدخول والبقاء غير المصرح به في النظام المعلوماتي(المطلب الثالث).

المطلب الأول

جرائم التحويل الإلكتروني غير المشروع للأموال

رافق ظهور الشبكة المعلوماتية وما صاحبها من تطورات كبرى في شتّى المجالات، كتطور نظام المعاملات التجارية حيث أصبحت تتم من خلال الشبكة العنكبوتية، مثل البيع والشراء، ممّا أدى إلى التطور في وسائل الدفع والوفاء وأصبحت جزء لا يتجزأ من هذه المعاملات، ونتيجة هذا التداول المالي عبر الإنترنيت أدى إلى ظهور الكثير من المتسللين للسطو عليها، حيث ابتكرت عدة طرق من أجل ذلك، على غرار التحويل الإلكتروني غير المشروع للأموال، وقرصنة أرقام البطاقات الممغنطة.

الفرع الأول

الإحتيال المعلوماتي

أدى انتشار إستخدام جهاز الكمبيوتر في كافة القطاعات والمجالات ومنها البنوك والشركات إلى ظهور جريمة التحويل الإلكتروني غير المشروع للأموال عن طريق إستخدام طرق احتيالية، إمّا بتحويل الجاني كل أو جزء من أرصدة الغير أو فوائدهم إلى حسابه الخاص ويتم ذلك عن

(111)–محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية؛ دار الثقافة للنشر والتوزيع، الأردن،2005، ص.49.

طريق إدخال بيانات غير صحيحة أو مغلوطة إلى جهاز الكمبيوتر كأن يدعي الجاني كاذباً بوجود فواتير حلّ ميعاد استحقاقها[112].

أولاً: تعريف جريمة الإحتيال المعلوماتي

قبل أن نتطرق إلى تعريف الإحتيال المعلوماتي والأساليب التقنية المستخدمة في إرتكابه، لا بد أن نشير إلى أنّ هناك العديد من الدراسات التي أُجريت لرصد حجم جريمة الإحتيال المعلوماتي والخسائر الناجمة عنها، وقد كشفت إحدى الدراسات التي أُجريت في الولايات المتحدة الأمريكية، بأنّ خسائر المبيعات بسبب الإحتيال المعلوماتي كانت أكثر من (700) مليون دولار في عام2001 [113].

يرى جانب من الفقه أنّ الإحتيال المعلوماتي هو"أيُ سلوك احتيالي ينتهج منهج الحوْسبة بنية الحصول على إمتياز مالي"[114].

كما عرف البعض الإحتيال المعلوماتي بأنه" التلاعب العمدي بمعلومات وبيانات تُمثل قيمًا مادية يختزنها نظام الحاسب الآلي، أو الإدخال غير المصرح به لمعلومات وبيانات صحيحة، أو التلاعب في الأوامر والتعليمات التي تتحكم في عملية البرمجة، أو أية وسيلة أخرى من شأنها التأثير على الحاسب الآلي، حتى يقوم بعملية بناء على هذه البيانات أو الأوامر أو التعليمات، من أجل الحصول على ربح غير مشروع وإلحاق الضرر بالغير[115]، فهذه التعريفات تشمل كل أشكال المساس بنظام الحاسوب، والمتمثلة في الاعتداء على المعطيات المخزنة في نظام المعلومات والمتبادلة عبر قنوات النظام، بما تمثلها من أموال وخدمات بغرض الحصول على منفعة مادية، وعادة ما يكون الجاني في جريمة الإحتيال المعلوماتي من الأشخاص العاملين على إدخال البيانات في ذاكرة الجهاز أو من قبَل المتواجدين على الشبكة أثناء عملية تبادل البيانات[116].

---

[112]–محمد علي العريان، المرجع السابق، ص.77.

[113]–محمد طارق عبد الرؤوف الحق، جريمة الإحتيال عبر الإنترنت(الأحكام الموضوعية والأحكام الإجرائية)؛ منشورات الحلبي الحقوقية، لبنان، 2011، ص.39.

[114]–نفس المرجع، ص.37.

[115]–نفس المرجع، ص.38

[116]–خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية؛ المرجع السابق، ص.76.

ثانيا: وسائل الإحتيال المعلوماتي

وسائل وأساليب إرتكاب جريمة الإحتيال المعلوماتي متنوعة متطورة تبعاً للتطور التكنولوجي الذي تشهده المعلوماتية [117].

1-التلاعب في البيانات المدخلة

التلاعب في البيانات المدخلة إلى جهاز الحاسوب يعد من أكثر حالات الإحتيال المعلوماتي إذ بينت الدراسات أنّ 62% من حالات الإحتيال المعلوماتي في الولايات المتحدة الأمريكية حتّى عام 1984 تنطوي على التلاعب بالبيانات قبل أو أثناء إدخالها إلى جهاز الحاسوب[118]، وعادةً ما تتم هذه الجريمة عندما يكون مرتكبها مدخلاً للبيانات إماّ أثناء إدخالها أو بتعديلها بعد إدخال أو إضافة بيانات وهمية إلى الحاسب الآلي[119].

تتنوع وسائل التلاعب بالبيانات في هذه المرحلة سواءً تم أثناء عملية الإدخال أو أثناء إعدادها أي – قبل الإدخال – ويمكن حصرها في ثلاثة وسائل رئيسية:

أ-الوسيلة الأولى:

تتمثل هذه الوسيلة في تغيير المعلومات المراد إدخالها إلى النظام دون أن يتضمن ذلك حذفًا لجزء أو أجزاء منها، سواءً تم ذلك في مرحلة الإدخال أو قبل ذلك، ويؤدي كل ذلك إلى تغيير معنى المعلومة حيث تصبح غير معبرة عن الحقيقة التي كانت تمثلها .

ب-الوسيلة الثانية:

تتضمن هذه الوسيلة حذف جزء من البيانات في مرحلة الإدخال أو قد يتعدى الأمر إلى حذف المعلومة بأكملها أو عدم إدخالها إلى النظام المعلوماتي، ويترتب على ذلك أيضاً تغيير معنى المعلومة أو عدم وجودها أصلاً.

---

[117]-نهلا عبد القادر المومني، المرجع السابق، ص.190.

[118]-نفس المرجع، ص.190.

[119]-محمود أحمد عبابنة، المرجع السابق، ص.56.

ت-الوسيلة الثالثة:

تتمثل هذه الوسيلة في إعاقة المعلومة من أداء وظيفتها و يتم ذلك عن طريق إدخال المعلومة مع إخفائها، وذلك بأن يتم إدخالها في غير المكان المخصص لها، وهو ما يؤدي إلى إعاقة هذه المعلومة عن أداء الدور الذي كان مقررًا لها[120].

2-التلاعب في البرامج:

تتم هذه الجريمة بعد قيام مرتكبها -عادةً المبرمج- بتعديل البرنامج الذي تعمل به المؤسسة باصطناع برنامج وهمي، ويتم هنا إستغلال هذا التعديل في البرنامج الوهمي الجديد من قبل المبرمجين القادرين على التحكم بنظام تشغيل الحاسب[121].

ويتم التلاعب في البرامج بصفة عامة بوسيلتين:

أ-الوسيلة الأولى:

تهدف هذه الوسيلة إلى تغيير البرامج المطبقة بالفعل داخل المؤسسة المجني عليها، بإدخال تعديلات غير مرخص بها على البرامج المستخدمة، فكثير من البرامج بعد إعدادها واختيارها قد تمر ببعض التعديلات لتصويب أخطاء إكتشفت بعد العمل بها[122]، وهو ما يتيح في هذه الحالة إدخال تغييرات من شأنها أن تساعد الجاني على إتمام جريمته وكذلك إخفائها كما قد يتم إجراء هذا التعديل عن طريق إستخدام البرامج الخبيثة (الفيروسات).

ب-الوسيلة الثانية:

تتمثل هذه الوسيلة في تطبيق برامج إضافية، وهذه البرامج قد يتم كتابتها من طرف الجناة أنفسهم أو قد تكون برامج معدة سلفاً تهدف بشكل أساسي إلى تعديل المعلومات في الحاسوب عن طريق إجراء تعديلات مباشرةً في ذاكرته.

ومن الأمثلة التي تبين ماهية التلاعب بالبرامج كوسيلة من وسائل الإحتيال المعلوماتي، ما قام به مبرمج يعمل في منشأة تجارية بتعديل البرنامج بحيث يقوم باقتطاعات لمبالغ زهيدة على فترات

---

[120]-نهلا عبد القادر المومني، المرجع السابق، ص.191.

[121]-محمود أحمد عبابنة، المرجع السابق، ص.57.

[122]-نهلا عبد القادر المومني، المرجع السابق، ص.193.

مختلفة من خلال الصفقات التي أبرمتها المنشأة مع المنتجين الموزعين[123]، وذلك باستخدام تقنية تدعى تقنية(salami) [124].

الفرع الثاني

الإحتيال باستخدام بطاقة الدفع الإلكتروني

يشمل نظام الدفع الإلكتروني بواسطة البطاقة الممغنطة على عمليات التحويل الإلكتروني من حساب بطاقة العميل بالبنك المصدر للبطاقة إلى رصيد التاجر أو الدائن الذي يوجد به حسابه[125]، وذلك من خلال شبكة التسوية الإلكترونية للهيئات الدولية " هيئة الفيزا كارت" و"هيئة الماستر كارت"، وتعطي بطاقة الدفع الإلكتروني الحق للعميل بالحصول على السلع والخدمات بواسطة شبكة الإنترنت عن طريق تصريح كتابي أو تلفوني، بخصم القيمة على بطاقة الدفع الإلكتروني الخاصة به، وتتم العملية بدخول العميل أو الزبون إلى موقع التّاجر ويختار السلع المراد شرائها ويتم التعاقد بملأ النموذج الإلكتروني ببيانات بطاقة الإئتمان الخاص بالمشتري وعنوانه[126]، وأمام هذا التطور التكنولوجي أصبحت إمكانية خلق مفاتيح البطاقات والحسابات البنكية بالطريق غير المشروع ممكنة عبر قنوات شبكة الإنترنت.

إذ كانت بطاقة الإئتمان بصورتها المادية لا تثير شكوكًا في انطباق وصف الجرائم التقليدية كلإعتداء على الأموال مثل السرقة، فإن ما يثور في هذا الصدد هي مسألة الاعتداء على البيانات السرية الخاصة ببطاقات الدفع الإلكترونية، ومسؤولية الحامل الشرعي لها أو الغير عن فعل الاستخدام غير المشروع للبيانات السرية لبطاقة الإئتمان عبر شبكة الإنترنت.

---

[123]–محمود أحمد عبابنة، المرجع السابق، ص.57.

[124]–**salami**: تقوم هذه التقنية باقتطاع بعض السنتيمات من الحسابات المالية الضخمة وتحويلها أليًا إلى حساب الجاني. متوفر على الموقع: **www.startimes.com/?t=24695044** ، ماي 2015.

[125]–إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان؛ دار الجامعة الجديدة، مصر، 2007، ص.10.

[126]–أمين أحمد الشوابكة، المرجع السابق، ص.193.

أولاً: الغش باستخدام بيانات بطاقة الإئتمان من قبل حاملها الشرعي

تفرض العقود المبرمة بين البنك مصدر بطاقة الإئتمان، وبين العميل حامل البطاقة شروط معينة يتعين هذا الأخير مراعاتها عند استخدامه للبطاقة، وإلاّ كان من حق البنك عدم تجديد مدة البطاقة أو سحبها من العميل قبل إنتهاء مدة صلاحيتها[127]، وقد يستخدم العميل البطاقة بصفة غير مشروعة سواءً أثناء مدة صلاحياتها أو بعد إنتهاء مدة صلاحيتها أو إلغائها.

1-إساءة إستخدام بيانات بطاقة الإئتمان أثناء مدة صلاحيتها

قد يكون العميل سيء النّية فيستغل بطاقته للحصول على السلع والخدمات من التّاجر دون أن يكون بإمكانه بل لا في نيته سداد قيمة ما حصل عليه [128]، ويتم إساءة إستخدام بيانات بطاقة الدفع الإلكترونية من قبل صاحبها عبر شبكة الإنترنت عن طريق دفع ثمن السلع والخدمات التي تقدمها الشبكة –بملأ الاستمارة الإلكترونية – رغم علمه بأن رصيده بالبنك غير كافي لتغطية هذه المبالغ أو أن يقوم بإجراء تحويل إلكتروني من رصيد لأخر متجاوزًا رصيده في البنك مصدر البطاقة[129].

ولعل الفقه والقضاء الفرنسيين هما أول من تطرق للبحث في هذه المسألة، وانقسمت آراء الفقه تبعًا لأحكام القضاء، ففي بادئ الأمر اعتبر هذا السلوك جريمة ولكن لم يتم تحديد وصفها القانوني فيما إذا كانت تشكل سرقة أم احتيالا بالنسبة للفرضين الأول والثاني، اتجهت بعض الأحكام إلى اعتبارها سرقة مؤسسة حكمها على إستلاء حامل البطاقة على مال الغير وحيازته، قضت أحكام أخرى باعتبارها احتيالا لأن العميل قام بأحد الطرق الاحتيالية، ولكن أبرز تلك الأحكام ما قضت به محكمة إستئنافAngers [130] التي قضت بعدم إعتبار هذا السلوك جريمة جنائية بل إخلالاً عقدياً، فهو لا يشكل سرقة لأن العميل حصل على المبلغ من الأجهزة المعدة

---

[127]–جميل عبد الباقي الصغير، المرجع السابق، ص.30.

[128]–نفس المرجع، ص.30.

[129]–أمين أحمد الشوابكة، المرجع السابق، ص.194.

[130]–محمود أحمد عبابنة، المرجع السابق، ص.64.

لتوزيع وتم تسليم المال بصورة إرادية، ولم يتم بطرق احتيالية حتّى يعد احتيالا، ولم يبدد البطاقة حتّى يعد إساءة ائتمان.

وهو الأمر الذي أيدته محكمة النقض الفرنسية 1982 عندما عرض عليها الطعن في حكم محكمة **Angers** وأشارت إلى أنّ الوقائع المنسوبة لا تندرج تحت أي وصف جنائي، ولا تتعدى كونها إخلالاً بالتزام تعاقدي[131].

2-إساءة إستخدام بيانات بطاقة الإئتمان بعد إنتهاء مدّة صلاحيتها أو إلغائها

أ-إستخدام بطاقة انتهت صلاحيتها:

تسلم بطاقة الإئتمان لمدة محدّدة، عادةً ما تكون سنة، فإذا ما حلّ هذا التاريخ يتعين على العميل إعادتها إلى البنك الذي أصدرها ولكن قد يحدث أن يمتنع العميل عن إعادة البطاقة التي انتهت مدّة صلاحيتها إلى مصدرها ويستمر مع ذلك في إستخدامها.

ب-إستخدام بطاقة تم إلغائها:

قد يحدث أن يقوم البنك مصدر البطاقة بإلغائها أثناء مدة صلاحيتها كجزاء لسوء إستخدام البطاقة من طرف العميل، فإذا ما تم إلغاء البطاقة من جانب البنك وتمّ إخطار العميل بذلك، فإنه يتعين على هذا الأخير إعادة البطاقة إلى مصدرها ولكن قد يمتنع العميل-مع ذلك- عن ردها إلى مصدرها ويستمر في إستخدامها[132]، كسحب المال بعد فترة إنتهاء مدة صلاحية البطاقة أو بعد إشعار حاملها بأنه تمّ إلغاء البطاقة ومع ذلك يقوم باستخدامها، وفي هذا الصدّد قضت محكمة **Créteil** بأن قيام حامل البطاقة بالسحب بعد إنتهاء مدّة البطاقة يشكل جريمة إساءة إئتمان[133].

ثانياً: الغش باستخدام بيانات بطاقة الإئتمان من قبل الغير

إنّ عملية نقل وتبادل البيانات عبر شبكة الإنترنت، ومنها البيانات المتعلقة ببطاقة الإئتمان (كالرقم السّري) يجعلها عرضةً للإلتقاط من قبل الغير سيء النّية، وبالتالي إستخدامها بطرق غير

---

[131]-أمين أحمد الشوابكة، المرجع السابق، ص.195.

[132]-جميل عبد الباقي الصغير، المرجع السابق، ص.30.

[133]-محمود أحمد عبابنة، المرجع السابق، ص.65.

مشروعة في سحب النقود الرقمية أو الوفاء بها، ولذلك فإن التقنية الحديثة سمحت بإمكانية خرق أرقام بطاقات الإئتمانية أو إستغلال الأرقام الخاصة بالغير واستخدامها بصورة غير مشروعة.

1-حالة سرقة البطاقة أو فقدانها:

تعد سرقة البطاقة أو ضياعها من أهم المشكلات القانونية التّي يثيرها التعامل بنظام بطاقة الإئتمان، ذلك أنّ السّارق أو من وجد البطاقة قد يستخدمها للحصول على السلع أو الخدمات من التّاجر، أو قد يسحب مبالغ بموجبها من أجهزة التوزيع الآلي للنقود[134].

2- حالة السحب باستخدام بطاقة مزورة:

ظهرت فكرة تزييف البطاقات الممغنطة كوسيلة يتحايل بها الجاني على أجهزة التفتيش الآلي للمواصلات حتّى يمكنه المرور منها بدون دفع الأجرة، كما قد يستخدمها الجاني للدخول بها إلى أجهزة التوزيع الآلي، وهو ما أكدّته **محكمة النّقض الفرنسية** في حكمها الصادر في 19 ماي 1987 حيث أيدت الحكم القاضي باعتبار المتهم مرتكباً لجريمة الإحتيال بعد سرقته لبطاقة الإئتمان العائدة لأحد الأشخاص، والشراء بواسطتها[135]، وكذلك يمكن اعتباره مرتكباً لجريمة التزوير إذّا قام هذا الأخير بالتوقيع تحت إسم مالك البطاقة الأصلي[136].

الفرع الثالث

موقف المشرع الجزائري من حماية المجني عليه في جرائم الإحتيال المعلوماتي

إنّ المشّرع الجزائري كفل حماية قانونية للمجني عليه في جرائم الإحتيال المعلوماتي، ويظهر ذلك جلياً في مجموعة من القوانين سواءً العامة منها أو الخاصة، وذلك بموجب تعديل ق.ع الجزائري بالقانون 04_15 المؤرخ في 10 نوفمبر 2004، والّذي أورد في قسمه السابع مكرّر المادة 394 مكرّر2 والتّي يمكن تفصيل الجرائم الواردة فيها على النحو التالي:

- ❖ جريمة تصميم أو بحث في معطيات مخزنة أو معالجة آليًا.
- ❖ جريمة تجميع أو توفير لبيانات مخزنة أو معالجة آليًا.

---

(134)-جميل عبد الباقي الصغير، المرجع السابق، ص.32.

(135)-محمود أحمد عبابنة، المرجع السابق، ص.66.

(136)-محمد أمين الشوابكة، المرجع السابق، ص.202.

❖ جريمة نشر للمعطيات وإفشائها.

❖ جريمة إعاقة سير المعلومات المرسلة عن طريق منظومة معلوماتية.

❖ جريمة الاتجار في المعطيات[137].

ومن خلال هذّا يتضح لنا أنّ المشرع الجزائري لم يبقى مكتوف الأيدي إزاء هذه الظاهرة الإجرامية الخطيرة، والمتمثلة في الإحتيال المعلوماتي هذّا من جهة؛ ومن جهة أخرى وفرّ المشرع الجزائري حماية للمجني عليه في جرائم الإحتيال المعلوماتي بموجب نصوص خاصة من بينها ما جاء في المادة 6 مكرر 1 من القانون رقم 08-01 المؤرخ في2008/01/23 المتمم للقانون رقم 83-11 المتعلق بالتأمينات الإجتماعية، إذ نص المشرع صراحةً أن صفة المؤمن له اجتماعيا تثبت ببطاقة إلكترونية وتسّلم للمؤمن له اجتماعيا مجانًا من طرف هيئة الضمان الاجتماعي وهي صالحة في كل التراب الوطني وهي تُقَدَمْ لكل مقدم علاج أو مقدم خدمات مرتبطة بالعلاج يزود بمفتاح إلكتروني يسمى"المفتاح الإلكتروني لهيكل العلاج " حسب نّص م65 مكرّر من نفس القانون[138].

ونظرًا لكون البطاقة الإلكترونية شخصية فإن القانون نفسه أضفى عليها حمايته إذْ نصّ في المادة 93 مكرر2 من ق.ت.إ على معاقبة كل من يستلمها أو يسلمها-أي البطاقة الإلكترونية- بغرض استعمالها بطريقة غير مشروعة وجاءت المادة كما يلي:"...**دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به، يعاقب بالحبس من سنتين(2) إلى خمسة سنوات(5) وبغرامة من مئة ألف دج إلى مائتين ألف دج**"، فكل من يستعمل أو يتسلم أو يسلم بهدف الاستعمال الغير المشروع للبطاقة الخاصة بالمؤمن له اجتماعيا أو المفتاح الإلكتروني لهيكل العلاج، وتتضاعف العقوبة حسب نص المادة 93 مكرر3 على كل من يقوم عن طريق الغش بتعديل أو حذف كل أو جزء للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا، أو في المفتاح الإلكتروني لهيكل العلاج، وهي نفس العقوبة التّي تطبق كذلك على من قام بتعديل أو نسخ وبطرق غير مشروعة البرمجيات التي تسمح باستعمال المعطيات المدرجة في

---

[137]-زيبح زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي؛ دار الهدى، الجزائر،2011، ص.56.

[138]-قانون رقم08-01 مؤرخ في2008/01/23، يتمم القانون رقم 83-11 المؤرخ في1983/05/02، المتعلق بالتأمينات الإجتماعية، ج.ر.ج.ج.عدد04، الصادرة في 2008/01/27.

البطاقة الإلكترونية للمؤمن له اجتماعيا ويعاقب المشرع الجزائري كل شخص حاول إرتكاب هذه الجريمة [139].

نستخلص إذن أنّ المشرع الجزائري لم يفوت الفرصة وهو بصدّد إعداد قانون خاص أنْ يُشّدد العقوبة على كل تلاعب في المعطيات أو البيانات المدرجة في البطاقة الإلكترونية كما أضفى حماية على البرمجيات وذلك بتشديد العقوبة على كل من قام بنسخ أو بتعديلها بطريقة غير مشروعة.

المطلب الثاني

الجرائم المعلوماتية الماسة بحرمة الحياة الخاصة

يعد الهدف الأول والأسمى لوضع القوانين وسّن التشريعات، حمايةً سلامة الأشخاص من مختلف الانتهاكات التي قد يتعرضون لها، سواءً في أبدانهم أو في حياتهم الخاصة، أو في سمعتهم وشرفهم.

تطور الأمر بعد ذلك مع ظهور شبكة الإنترنت، فرغم الفوائد التي جاءت بها هذه التقنية، والتسهيلات التي قدمتها في الحياة اليومية للفرد والمجتمع على حد سواء، إلاّ أنّها أصبحت سلاح فتّاك في يد المجرمين، بالإضافة إلى ذلك فإنّ المعلومات المتعلقة بالأفراد متداولة بكثرة عبر هذه التقنية، مما يجعلها عرضةً للانتهاك والاستعمال من طرف هؤلاء المجرمين، إذ جعلت سمعة وشرّف الأفراد مستباحة.

الفرع الأول

الحياة الخاصة في مواجهة المعلوماتية

للحياة الشخصية خصوصيتها بمّا تحويه من أسرار، والمحافظة على هذه الأسرار يحظى بحماية دستورية وقانونية في كافة دساتير الدول وقوانينها، وقد اهتم المشرع الجزائري بإضفاء

[139]–زيبح زيدان، المرجع السابق، ص.77.

الحماية على الحياة الخاصة سواءً في الدستور وفقًا لنّص المادة 39 منه[140]، أو في القانون وفقاً لنّص المادة 303 مكرّر من قانون العقوبات.

ولكن قد يستخدم النظام المعلوماتي كما سبق وأن أشرنا في الاعتداء على حرمة الحياة الخاصة، كما لو قام شخص يعمل بالنظام المعلوماتي بإعداد ملف يحتوي على معلومات تخص شخص أخر بدون علمه ودون إذن منه، أو أن يكون تجميع هذه المعلومات بموجب موافقة من صاحبها ولكن قام الشخص المكلف بحفظها بإطلاع الغير عليها بدون إذن صاحبها[141]، كما في حالة الأسرار المودعة لدى المحاسبين أو المحامين أو الأطباء، فكل هذه الأسرار يحميها القانون ويُجرم إفشائها بالطرق غير المشروعة وبدون موافقة صاحبها.

وجريمة التعدي على الحياة الخاصة والإطلاع على الأسرار أو إفشائها، قدْ تتم بتخزين المعلومات وفتح السجلات الإلكترونية والإطلاع عليها من خلال شاشة الكمبيوتر.

الفرع الثاني

صور التهديد المعلوماتي للحياة الخاصة

إنّ صور سلوك الاعتداء على الحياة الخاصة يصعب حصرها، لأنها متطورة نتيجة تطور تكنولوجيا المعلومات باستمرار، إلاّ أنّه يمكن أن نشير إلى أبرز الانتهاكات التّي تمس بحق الأفراد في حرمة حياتهم الخاصة نتيجة لاستخدام الأنظمة المعلوماتية بصورة غير مشروعة.

أولاً: الذّم والقدح والتحقير عبر الإنترنيت

تعد جرائم الذم والقدح أو القذف (كما سماه المشرع الجزائري) والتحقير من أهم الجرائم انتشارًا على شبكة الإنترنيت، باعتبار أنّ هذّه التقنية توفر للمجرم إمكانية إستخدامها لنيل من شرف الغير أو كرامته أو اعتباره[142] أو تعريضه إلى بغّض النّاس واحتقارهم له، سواءً تم ذلك

---

[140]–دستور الجمهورية الجزائرية الديمقراطية الشعبية، المنشور بموجب المرسوم الرئاسي رقم96–438، مؤرخ في 7 ديسمبر1996 يتعلق بنشر نص تعديل الدستور الموافق لاستفتاء 28 نوفمبر1996، ج.ر.ج.ج. عدد76، صادر في 8 ديسمبر 1996، المعدل والمتمم.

[141]–خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية؛ المرجع السابق، ص.72.

[142]–محمد أمين الشوابكة، المرجع السابق، ص.30.

وجاهيًا عبر خطوط الاتصال المباشر أو قد يكون كتابيًا أو غيابيًا، أو قد يكون بواسطة المطبوعات، وجميع هذّه الصور ترتكب عبر الإنترنيت من خلال المبادلات الإلكترونية الكتابية أو الصوتية أو البصرية[143]، التي توفرها خدمة البريد الإلكتروني أو شبكة الويب العالمية وغرفة الدّردشة[144] فهذه الأخيرة تمّكن الأشخاص من التخاطب عن بعد عن طريق الكتابة باستخدام لوحة المفاتيح الخاصة بهم،حيث يمكن لآخرين رؤية ما يكتبه المخاطب فإنه عادةً ما يكون الذّم والقدح والتحقير الذي يرتكب بواسطة غرفة الدّردشة يكون بصفة خطئية وغير مقصودة[145] كالخطأ في الضّغط على زر ما أو إرسال صورة غير مقصودة.

كما يتحقق شرط العلنية لهذه الجريمة في إمكانية إطلاع العامة على الكتابات أو الصور أو الفيديوهات التّي تتضمن الذم والقدح والتحقيق عن طريق الدخول إلى الموقع الذي تمّ فيه نشرها.

ثانياً: التسجيل غير المشروع للبيانات الاسمية

يتمثل فعل الانتهاك للحق في الحياة الخاصة للأفراد في عملية تسجيل بيانات صحيحة عنهم لكن على نحو غير مشروع، ومخالف لأحكام القانون09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[146]، عن طريق استعمال الغش والطرق التدليسية[147].

وتظهر هذه الأساليب الغير المشروعة في الاعتداء على وسائل تشكل انتهاكًا واضحًا للخصوصية من أجل تسجيل البيانات الاسمية للأفراد ومن ضمن هذه الأساليب القيام بالتقاط

---

[143]-محمد أمين الشوابكة، المرجع السابق، ص.31.

[144]-**غرفة الدّردشة:** تستخدم لدّردشة أو المحادثة عن طريق وسائل الإعلام لوصف أي شكل من أشكال المقابلات عبر الإنترنيت إمّا أن تكون متزامنة أي(التحدث و المناقشة في نفس الوقت) وأحيانًا غير متزامنة (كما في المنتديات).
تعريف موجود على الرابط التالي:

http://ar.wikipedia.org.avril, 2015.

[145]-محمد أمين الشوابكة، المرجع السابق، ص.45.

[146]-قانون رقم 09-04 مؤرخ في5 أوت 2009، يتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،ج.ر.ج.ج.عدد47، بتاريخ 2009.

[147]-محمد أمين الشوابكة، المرجع السابق، ص.93.

الارتجاجات التّي قدْ تحدثها الأصوات في الجدران الإسمنتية للغرف وترجمتها إلى عبارات وكلمات بواسطة حاسوب مزود ببرنامج خاص، وكذلك قدْ يتم مراقبة الرسائل المتبادلة واعتراضها والتقاطها عن طريق البريد الإلكتروني أو توصيل أسلاك بطريقة خفية إلى الحاسوب الذي تخزن بداخله البيانات أو التوصل بطريق غير مشروع إلى ملفات تخص بيانات الآخرين، أو أية وسيلة أخرى غير مشروعة كالتدليس والغش أو التصنت على المكالمات التّي تتم عن طريق شبكة الإنترنيت[148].

ثالثًا: انتحال الشخصية والتغرير والاستدراج

تعتبر عملية انتحال الشخصية من الجرائم المعاقب عليها قانونًا، فهي من الجرائم القديمة لذلك يمكن أن تطبق عليها القوانين التقليدية دون الحاجة إلى تعديلها، فأصبحت تتم بأسلوب متطور تكنولوجيًا مغايرًا للأسلوب التقليدي[149]، وتتخذ جريمة انتحال الشخصية عبر الإنترنيت شكلين؛ الشكل الأول يتمثل في انتحال شخصية الفرد، إذْ يقصد به إستخدام الجاني لشخصية شخص آخر للإستفادة من سمعته أو ماله أو سلطاته[150]؛ والشكل الثاني يقوم على انتحال شخصية الموقع المراد منها إمكانية بعض الأشخاص الدخول على الموقع إمّا أن يحجبه ويضع الموقع الخاص به بدلاً عنه، أو أن يغير هذا الموقع كما يحلوا له، وفي غالب ما يحدث هذّا في المواقع السّياسية أو الدّينية ومثال ذلك دخول بعض الإسرائيليين إلى بعض المواقع الفلسطينية ويحاولون إلغاء الموقع ووضع بدلاً منه صورة العلم والنشيد الوطني الإسرائيلي والعكس صحيح[151].

---

[148]–حمزة بن عقون، المرجع السابق، ص.103.

[149]–منير محمد الجنبيهي، ممدوح أحمد الجبنيهي، المرجع السابق، ص.44.

[150] –مزغيش سمية، **جرائم المساس بالأنظمة المعلوماتية**؛ مذكرة الماستر، كلية الحقوق، جامعة محمد خيضر، بسكرة 2013–2014، ص.28.

[151]–منير محمد الجنبيهي، ممدوح أحمد الجنبيهي، المرجع السابق، ص.45.

الفرع الثالث

موقف المشّرع الجزائري من حماية الحياة الخاصة في مواجهة سلوكيات المجرم المعلوماتي

إنّ المشرع الجزائري على غرار التشريعات الأخرى قد نّص في القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 المتعلق بقانون العقوبات على عقوبة الحبس من ستّة(6) أشهر إلى ثلاثة(3) سنوات وبغرامة من 50.000 دج إلى3000.000 دج، على أي شخص تعمدا المساس بحرمة الحياة الخاصة وبأية تقنية كانت، وذلك عن طريق الالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة وسّرية، دون إذن صاحبها أو رضاه أو بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذنه.

كما تنص المادة 303 مكرّر 1 من نفس القانون على معاقبة أي شخص احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير، واستخدام في ذلك أية وسيلة كانت من التسجيلات أو من الصور أو الوثائق.

فالملاحظ هنا أنّ المشرع الجزائري لم يبين بصورة دقيقة الأساليب المستخدمة بل استخدم عبارة "... **بأية تقنية كانت** ...".

أمّا القسم الخاص بالمساس بالأنظمة المعالجة الآلية للمعطيات الواردة في قانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 فتضمن صور أخرى للغش المعلوماتي، في حين أبقى خارج دائرة التجريم بعض الأفعال لنذكر منها المساس بحقوق الأشخاص عن طريق المعلوماتية ومنها جمع المعلومات حول الشخص.

المطلب الثالث

جريمتي الدخول والبقاء غير المصرح به في النظام المعلوماتي

تعتبر جريمتي الدخول والبقاء غير المصرح بهما من أبرز وأخطر الجرائم التي يمكن أن تستهدف النظام المعلوماتي فهي تنقسم إلى جريمتين، جريمة الدخول غير المشروع لنظام

المعلوماتي، وجريمة البقاء غير المصرح به في النظام المعلوماتي، لذلك كرس المشرع الجزائري حماية لها بتجريم الاعتداء عليها سواءً بصورتها البسيطة أو المشدّدة.

الفرع الأول

الدخول غير المشروع لنظام المعلوماتي

لا يقصد بالدخول إلى نظام المعالجة الآلية للمعطيات الدخول إلى مكان أو منزل بل هو عبارة عن دخول معنوي إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات[152]، ويقصد به توجيه هجمات إلى معلومات الكمبيوتر بقصد المسّاس بالسرية، أو المسّاس بسّلامة المحتوى أو تعطيل القدرة للأنظمة للقيام بعملها بصفة غير مشروعة، والذي يشكل فعل الاختراق وهي عبارة عن"عملية دخول غير مصرّح به إلى أجهزة الغير وشبكاتهم الإلكترونية، ويتم هذّا الاختراق بواسطة برامج متطوّرة يستخدمها كل من يملك خبرة في استعمالها[153].

لكن لم يحدد المشرع الجزائري وسيلة الدخول ويستوي أن يتم الدخول مباشرة أو بطريقة غير مباشرة، بحيث أنّ هذه الجريمة لا تتحقق إلاّ عندما يتم الدخول سواء استخدم الجاني قرصا أو جهاز تليفونيا أو جهاز الحاسب الآلي أو بطاقة ممغنطة أو إدخال الرقم السّري الذي يحمي البرنامج...إلخ [154]، ومثال ذلك تمكن أحد قراصنة الإنترنيت في الجزائر الذي يطلق على نفسه إسم "**صدام 213**" إذْ قام بعدة اعتداءات على الأنظمة المعلوماتية للعديد من المواقع الخاصة ببعض مؤسسات الدولة، وتمكن من الدخول بطريقة غير قانونية للمنظومة المعالجة الآلية للمعطيات لوزارة التعليم العالي والبحث العلمي وبريد الجزائر وجامعتي بومرداس وتلمسان، وتمكنت فرقة الدرك الوطني لولاية الجزائر العاصمة من توقيفه وتقديمه أمام النيابة العامة "لبئر مراد

---

[152]–قارة آمال، **الجريمة المعلوماتية**؛ المرجع السابق، ص.42.

[153]–خالد ممدوح إبراهيم، الجرائم المعلوماتية؛ المرجع السابق ، ص.242.

[154]–محمد حمّاد مرهج الهيتي، جرائم الحاسوب، ماهيتها موضوعها أهم صورها والصعوبات التي تواجهها، دراسة تحليلية (لواقع الاعتداءات التي يتعرض لها الحاسوب وموقف التشريعات الجنائية منها)؛ دار المناهج للنشر والتوزيع، الأردن، 2006، ص.182.

رايس"[155]، ومثال آخر دخول الجاني بطريقة غير مشروعة إلى نظام المعلوماتي للمستخدم من أجل الحصول على امتيازات[156]، وعليه فإن النّشاط الإجرامي لهذه الجريمة يتحقق في حالة الاتصال ومن ثم الدخول بغير حق إلى النظام الآلي لمعالجة المعلومات إذْ كانّ هذّا النظام محمياً بتجهيزات أمنية، والسؤال المطروح فهل يمكن أن تتحقق الجريمة إذا كانّ النظام مفتوح للجمهور[157]؟ وهذّا ما أدى إلى ظهور جدال فقهي حول مدى أحقية النظم المعلوماتية الغير المزودة بأنظمة أمنية للإستفادة من الحماية الجنائية ضد الولوج غير المشروع، وظهر رأيان، الأول يرى أنه من غير المعقول توفير حماية جنائية للمعلومات على درجة من الأهمية دون تزويدها بتجهيزات أمنية، إذْ أنّ القانون الجنائي لا يحمي الأشخاص الذين لا يأخذون واجب الحيطة والحذر التي يتخذها الرجل العادي[158].

أما الرأي الثاني، ناد إلى ضرورة حماية الأنظمة المعلوماتية سواءً كان النظام محميًا أو مفتوح للجمهور إذ أن عدم وجود نظام الحماية سوف يؤدي إلى حرمان بعض النظم الغير المزودة بتجهيزات أمنية من الحماية الجنائية من جهة؛ ومن جهة أخرى توسيع دائرة الإفلات من العقاب لذلك اكتفت غالبية التشريعات باشتراط أن يتم الدخول بالغش فقط وهذا ما أخذ به المشرع الجزائري.

وتعتبر جريمة الدخول غير المشروع إلى النظام المعالجة الآلية للمعطيات من الجرائم الوقتية وليست من الجرائم المستمرة، ولا يعتد بصفة الجاني في هذه الجريمة فقد يكون الفاعل شخص مسؤول عن الجهاز، كما قد يكون الفاعل شخص أجنبي عن ذلك النظام استطاع اقتحام النظام المعلوماتي عن طريق استخدام وسائل احتيالية[159].

---

[155]–جريدة النهار الجديد،"توقيف متهم قام بعدة اعتداءات على الأنظمة المعلوماتية الخاصة ببعض مؤسسات الدولة"، عدد صادر في 2014/01/30، مقال متوفر على الموقع:
http://www.ennaharonline.com/ar/algeria_news/195696.html, mars 2015

[156]-LARGUIER(J),CONTE(PH), FOURNIER(S),Droit pénal spécial, Dalloz, Paris, 15em éd, 2013, P.251.

[157]-Idem, P.251.

[158]–محمد أمين الرومي، المرجع السابق، ص.103.

[159]–محمد أمين الرومي، المرجع السابق، ص.102.

الفرع الثاني

البقاء غير المصرح به في النظام المعلوماتي

إنّ هذّه الجريمة ليست كسابقتها حيث أنّ الجاني في جريمة الدخول غير المشروع لنظام المعلوماتي يسعى بنفسه إلى تحقيق الاتصال مما يتطلب منه فعلاً إيجابياً؛ أما جريمة البقاء غير المصرح به في النظام المعلوماتي فإنها تتطلب الخروج من البرنامج وعدم البقاء فيه، وتتحقق في الحالات التي يكون فيها الاتصال عن طريق الخطأ، لذلك على الجاني إتيان فعل إيجابي وهو قطع الاتصال والخروج من النظام[160]، ويتمثل السلوك الإجرامي لهذه الجريمة في فعل البقاء، ويقصد به التواجد داخل نظام المعالجة الآلية للمعطيات دون إرادة صاحب الموقع أو النظام[161]، وجريمة البقاء غير المصرح به في النظام المعلوماتي لها صورتان؛ صورة إيجابية وصورة سلبية، فالصورة الأولى تشمل الفعل الإيجابي المتمثل في البقاء، والصورة الثانية، تتمثل في الفعل السلبي أي الامتناع عن الخروج[162]، ولم نجد في القانون المقارن رأيًا يحدد بدقة زمن إنتهاء جريمة الدخول وبداية جريمة البقاء في كل المنظومة أو جزء منها، غير أنّ البعض اعتبر بدايتها منذ اللّحظة التي يبدأ فيها الجاني التجول داخل النظام المعلوماتي، ومع ذلك فإنه يطرح صعوبة في تحديد زمن البقاء إذْ يجب التفرقة هنا بين البقاء الحاصل عن جريمة الدخول غير المشروع، وبين جريمة البقاء الناتجة عن الدخول المسموح به لكون الجاني رفض الخروج بعد إنتهاء الوقت المسموح له بالدخول إلى النظام[163]، وفي نطاق موضوعنا فالمشرع يأمر الجاني بعدم الإبقاء على اتصال، فامتناع الجاني عن الانسحاب يشكل إخلال بالواجب، وهو علة العقاب على إبقاء الاتصال قائما[164]، فالعبرة في هذه الحالة هو الاستمرارية والبقاء داخل النظام، حتى ولو كان الدخول مصادفة، إذ يتحقق ذلك بالنسبة للخدمات المفتوحة للجمهور كالخدمات الهاتفية، التي

---

[160]–قارة آمال، الحماية الجنائية للمعلوماتية في التشريع الجزائري؛ المرجع السابق، ص.110.

[161]–قارة آمال، **الجريمة المعلوماتية**؛ المرجع السابق، ص.44.

[162]–محمد حمّاد مرهج الهيتي، المرجع السابق، ص.191.

[163]–زيبح زيدان، المرجع السابق، ص.50.

[164]–محمد حمّاد مرهج الهيتي،المرجع السابق،ص.192.

يستطيع الجاني فيها الحصول على الخدمة دون أن يدفع مقابل أو يحصل على مدة أطول من المدة التي دفع مقابلها[165].

تعتبر جريمة البقاء غير المشروع داخل النظام المعلوماتي من الجرائم الشكلية التي لا يشترط فيها حدوث نتيجة إجرامية[166]، فيكفي البقاء غير المصرح به داخل النظام المعلوماتي لقيام هذه الجريمة على خلاف جريمة الدخول إلى نظام المعالجة الآلية للمعطيات فإن جريمة البقاء تعتبر من الجرائم المستمرة[167].

الفرع الثالث

موقف المشرع الجزائري من جريمتي الدخول والبقاء

لقد تدارك المشرع الجزائري الفراغ القانوني في مجال الإجرام المعلوماتي من خلال تكريسه لحماية المواقع من الاعتداء بالدخول أو البقاء الغير المصرح به في النظام المعلوماتي، ونجد غالبية القوانين المنظمة لمسألة الحماية الجنائية للمواقع الإلكترونية قد جرمته وعاقبت عليه، إذ جعل المشرع الجزائري نص المادة 394 مكرّر من قانون العقوبات متطابقة مع نّصت عليه المادة 323-1 من قانون العقوبات الفرنسي ومنه استمد المشرع الجزائري محتواه في تعديل قانون العقوبات[168] بموجب قانون رقم 04-15 المؤرخ في 2004/11/10، والتي عدلت وتممت بخصوص شق العقوبة، بموجب المادة 60 من قانون رقم 06-23، المؤرخ في 2006/12/20 المعدل والمتمم لقانون العقوبات، والمشرع الجزائري فرض عقوبات صارمة ضدّ المعتدين على المعطيات المعلوماتية وذهب إلى تجريم بعض الأفعال المتصلة بالمعالجة الآلية للمعطيات منها جريمة الدخول غير المصرح به عن طريق الغش سواء كان الدخول أو البقاء في كل المنظومة أو

---

(165)-قارة آمال، **الجريمة المعلوماتية**؛ المرجع السابق، ص.44.

(166)-نهلا عبد القادر المومني، المرجع السابق، ص.161.

(167)-**الجرائم المستمرة délits continu:** هي تلك الجريمة التي لا ترتكب في لحظة واحدة بل يفترض فيها استمرارية الحالة الإجرامية ومثال ذلك جريمة حمل غير الشرعي للسلاح الناري أو إخفاء أشياء مسروقة أو استعمال وثائق مزورة، أنظر: بن شيخ لحسن، مبادئ القانون الجزائي العام، (النظرية العامة للجريمة، العقوبات وتدابير الأمن، أعمال تطبيقية، القانون العرفي الجزائي لقرية تاسلنت"منطقة أقبو")؛ دار هومه، الجزائر،2005، ص.63.

(168)-حمودي ناصر،"التنظيم القانوني لظاهرة المعلوماتية في الجزائر(الإنجازات والتحديات)؛ المجلة النقدية والعلوم السياسية، كلية الحقوق، جامعة مولود معمري_ تيزي وزو، الجزائر، العدد2، 2012، ص. ص.(208-209).

جزء منها فقط، وهو ما أشارت إليه المادة **394 مكرّر** من قانون العقوبات الجزائري "**يعاقب بالحبس من ثلاثة (3)أشهر إلى سنة (1) وغرامة مالية من 500.00 إلى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.**

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة... "[169].

ونلاحظ من خلال هذّا النّص أنّ المشرع الجزائري في حقيقة الأمر يعاقب على جريمتين، الأولى هي الدخول بطريق الغش إلى نظام المعالجة الآلية؛ أما الجريمة الثانية تتمثل في البقاء غير المصرح به برغم من علم الجاني بعدم مشروعية البقاء، كما تجدر الإشارة أنّ المشرع الجزائري أقر للجريمتين عقاب واحد الأمر الذي يستوجب التفريق بينهما في نطاق العقوبة، كما يعاقب أيضًا على الشروع فيهما.

[169]–القانون رقم 14–01 مؤرخ في 4 فيفري 2014، يتمم ويعدل الأمر رقم 66–156 المؤرخ في8جوان 1966، والمتضمن قانون العقوبات، ج.ر.ج.ج.عدد.07، بتاريخ 2014.

المبحث الثاني

سلوكيات المجرم المعلوماتي الواقعة على تكنولوجيا المعلومات

بالإضافة للسلوك الإجرامي للمجرم في الجرائم المعلوماتية التي يعتمد فيها على النظام المعلوماتي لارتكاب جرائمه؛ هناك نوع أخر لسلوكيات المجرم في الجرائم الواقعة على النظام المعلوماتي بحد ذاته وهي المتمثلة في الجرائم التي تستهدف إما المكونات المادية للنظام المعلوماتي؛ أو المكونات المنطقية الموجودة داخل النظام المعلوماتي.

المطلب الأول

سّرقة المال المعلوماتي المعنوي

إنّ السّرقة التقليدية كما استقر عليه الفقه الجنائي يشترط في محلها أن يكون مال مادي مملوك للغير مما يمكن نقله وتغيير الحيازة فيه[170]، فهل يمكن تطبيق هذّا النّص على السّرقة المستحدثة والمتمثلة في سرقة المال المعلوماتي المعنوي؟ باعتبار أنّ هذه الأخيرة لها قيمة غير تقليدية وبسبب إستخدامها في شتّى المجالات أدى إلى إضفاء عليها قيمة اقتصادية جديرة بالحماية من كل اعتداء غير مشروع عليها.

الفرع الأول

محل جريمة السرقة المعلوماتية

إذا كانّ المال المعلوماتي ينقسم إلى مال معلوماتي طبيعي أي مكونات العناصر المادية للنظام المعلوماتي والتي تحتوي على المعلومات التي لها كيان مادي ملموس وهي المتمثلة في وحدات العرض والتسجيل والشاشة والملحقات التي تمكن من إدخال وإخراج المعلومة، كما للمال المعلوماتي جانب آخر لا مادي وهو ما يطلق عليه بالمال المعلوماتي المنطقي[171].

---

[170]–بن شيخ لحسن، مذكرات في القانون الجزائي الخاص(جرائم ضد الأشخاص، جرائم ضد الأموال، أعمال تطبيقية)؛ دار هومة، الجزائر، 2004، ص127.

[171]–أحمد خليفة الملط، المرجع السابق، ص.234.

وبما أن أي اعتداء أو بالأحرى أي سّرقة تمس الجانب المادي للمال المعلوماتي لا تثير أي مشكل لأنّ السّرقة هنا تنصرف إلى مال منقول مادي يمكن إخراجه من حيازة مالكه، ويحدث هذّا عندما تكون المعلومة مخزنة على أدوات التخزين ذات الكيان المادي، كأسطوانات الحاسب الآلي[172]، ولكن يثور الخلاف عندما يتم سرقة المال المعلوماتي المعنوي أو المنطقي، فهل يصلح هذّا المال ليكون محلاً لسّرقة؟ وهل يمكن تطبيق القواعد العامة لسّرقة على سّرقة المعلومات؟[173].

أولاً: طبيعة المال المعلوماتي المعنوي

لقد ثار جدالاً فقهيًا حول إمكانية إعتبار المال المعلوماتي المعنوي يمكن أن يكون محل لجريمة السّرقة المعلوماتية، فلقد انقسم الفقه بين مؤيد لاعتباره محل لجريمة سّرقة المال المعلوماتية المعنوية، وهناك اتجاه آخر رافض لأن تخضع المعلوماتية للسرقة.

1-إعتبار المعلوماتية مالاً يمكن سّرقتها:

هناك جانب من الفقه من اعتبر أنّ للمعلوماتية قيمة مالية يمكن أن تخضع للسّرقة، باعتبار أنّ المعلومة عبارة عن نتاج ذهني وابتكار، مما يترتب على ذلك وجود علاقة تبني بين المعلومة ومؤلفها وتشبه العلاقة التي تنشأ بين المالك والشيء الذي يملكه، فيكون له حق نقلها أو إيداعها وحفظها وبيعها، فالمعلوماتية من قبيل الأموال باعتبار أنّ لها قيمة اقتصادية، حيث أنّه يمكن طرحها في السّوق للتداول مثل أي سلعة أخرى[174]، ويعتبر هذا الاتجاه الفقهي "الشيء" مالاً ليس بالنظر إلى ما إذا كان له كيان مادي محسوس، وإنّما بالنظر إلى قيمته الاقتصادية، وهذّا ما ذهب إليه الأستاذ **(Carbonnier)** إذ يقول: " **إنّ القانون يرفض أن يرى قيمة في الشيء له أهمية اقتصادية ولا يتدخل لإقرار حماية له** "[175].

---

[172]-محمود أحمد عبابنة، المرجع السابق، ص.93.

[173]-أحمد خليفة الملط، المرجع السابق، ص.236.

[174]-نفس المرجع، ص.239.

[175]-نهلا عبد القادر المومني، المرجع السابق، ص.106.

وهناك جانب آخر يرى أنّ المال المعلوماتي المعنوي يمكن أن يكون له كيان مادي حيث يمكن رؤية تلك المعلومات على شاشة الحاسب مترجمة إلى أفكار ويمكن بالتالي سرقة تلك المعلومات المعروضة على شاشة الحاسوب[176].

أما المشرع الجزائري حينما نّص على السّرقة في المادة **350** من قانون العقوبات الجزائري استعمل لفظ "الشيء" الذي يشمل كل حقيقة ملموسة مادية أو مجردة[177]، واعتبره محل لجريمة السّرقة، وقد تطور مفهوم الشيء الذي لا ينحصر فقط في الأشياء المادية بل يشمل الأشياء ذات الطابع المعنوي بشرط أن تكون لها قيمة مالية[178].

2-المعلوماتية ليست بمال ولا يمكن أن تكون محلاً لسّرقة:

لقد تعددت الآراء الفقهية التّي ترى أنّ المعلوماتية ليست بمال ولا يمكن أن تكون محلاً لجريمة السّرقة، وقد ساد هذا الاتجاه لمدّة زمنية طويلة نسبيًا إذْ كانّ يعترف فقط بالأشياء المادية لاعتبارها من قبيل الأموال، أما الأشياء المعنوية أو اللامادية لا تتمتع من وجهة نظرهم بصفة المال فكان ينظر إلى الأشياء المعنوية إما باعتبارها عديمة القيمة أو ذات قيمة زهيدة[179].

فذهب جانب فقهي يرى نكران صفة المال على المعلوماتية فالقابلية للاستغلال المالي لن يضفي عليها وصف المال بحد ذاته، ولهذّا لا يمكن أن تكون المعلوماتية محلاً لجريمة السرقة باعتبار أنّ أي برنامج حاسوبي ينطوي على الإبداع والابتكار إذْ يتضمن اعتداء على حق المؤلف في إستغلال مصنفه، ولا تشكل هذّه الأفعال جريمة السّرقة [180].

---

[176]-أحمد خليفة الملط، المرجع السابق، ص.240.

[177]-**la chose : « toute sorte d'objet matériel ou d'abstraction »,** Larousse De poche, Les éditions françaises Inc, paris, 1996, P.17.

[178]-عمر الفاروق الحسيني،" لمحة عن جرائم السرقة من حيث اتصالها بنظم المعالجة الآلية للمعطيات"؛ مؤتمر القانون والكمبيوتر والإنترنيت، المنعقد بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، أيام 01-03 ماي2000، المجلد الأول، ص.331.

[179]-نهلا عبد القادر المومني، المرجع السابق، ص.105.

[180]-أحمد خليفة الملط، المرجع السابق ، ص.137.

ثانيًا: طبيعة المنقول في جريمة السّرقة المعلوماتية

من المبادئ العامة في علم العقاب أنّ جريمة السرقة تنصب على مال منقول أما العقارات فلا تصلح أن تكون محلاً للسرقة، وإنّما القانون يحميها بنصوص أخرى[181]، ولكن يثور جدال فقهي وقانوني فيما يخص إعتبار المعلوماتية من الأموال المنقولة التّي تكون محل لجريمة السرقة المعلوماتية، فهناك رأي يعتبر أنّ المعلوماتية ليست بمنقول ولا يمكن لها أن تصلح لسرقة، ورأي الآخر معارض للأول يعتبرها من الأموال المنقولة التّي تصلح لأن تكون محل لجريمة السرقة.

1- إعتبار المعلوماتية منقولا تصلح كمحل لجريمة السرقة:

ويرى هذا الجانب من الفقه أنّ كلمة "الشيء" تشمل على الأشياء المادية وغير المادية، كما سبق الإشارة إليه سابقًا وإذْ كانّ من الممكن حيازة الأشياء غير المادية كحق الانتفاع والدين فإنه من الممكن كذلك حيازة وسلب حيازة المعلومات وبذلك تكون محل لجريمة السرقة[182].

واتجه جانب ثاني من الفقه إلى القول بإمكانية الإستلاء والسرقة الذهنية للمعلومات التي تم عرضها عليه سواء عن طريق شاشة الحاسب الآلي أو قدْ تم سماعها من خلال جهاز الحاسب الآلي، فالمعلومة في هذّه الحالة يمكن أن تنتقل من عقل إلى آخر، ويمكن وضع وتخزينها بعد ذلك في كيان مادي إذْ يمكن بعد ذلك للشخص الذي إلتقط المعلومة عن طريق المشاهدة أو السمع أن يقوم بتدوينها وتخزينها في دعامة شأنها شأن الكهرباء فمادامت المعلومة لها كيان مادي يمكن نقلها من مكان لأخر والتصرف فيها كبيعها مثلاً والقدرة على التحكم فيها فهي بهذا الشكل تحمل خصائص الشيء ذات الطابع المادي[183].

2- المعلوماتية ليست منقولاً ولا تصلح كمحل للجريمة:

هذّا الاتجاه يعتبر المعلومات ليست من قبيل الأشياء إذْ يمكن الحصول عليها، بالمشاهدة أو القراءة أو السمع من جهاز الحاسب ولا تقع عليها جريمة السرقة، باعتبار أنّ هذّه الأخيرة تقع فقط على الأشياء والمعلومات بحسب هذا الموقف لا تعد من قبيل الأشياء، ولقد ذهب رأي ثاني

---

(181)-عمر الفاروق الحسيني، المرجع السابق، ص.333.

(182)-أحمد خليفة الملط، المرجع السابق ، ص.243.

(183)-محمد أمين الشوابكة، المرجع السابق، ص.150.

لاعتبار أنّ المعلومات لا يمكن لها أن تكون محل في جريمة السرقة باعتبار أنّ عدم إمكانية انتزاعها وحيازتها يحول دون ذلك، أما المستندات المثبتة لها والتّي تكون وسيلة لتسجيل عليها هي التّي تصلح لأنّ تكون محل لجريمة السرقة بما أنّ لها كيان مادي[184].

ثالثًا: ملكية الغير للمال المعلوماتي

يشترط أن يكون المال المسروق غير مملوك للجاني أي أنّ المال محل السرقة مملوك للغير، وكل إستغلال أو نقل حيازة بدون رضا صاحبها يشكل جريمة السرقة، ولذلك ظهر اتجاه فقهي يرى أنّ المعلومات في حالتها المجردة لا تصلح أن تكون قابلة لتملك والاستئثار وأن تداولها من حق العامة دون تمييز، ولا يمكن أن تكون محل للملكية[185]، في حين ذهب الفقه الفرنسي الحديث إلى إعتبار المعلومات محل لحق الملكية وإمكانية نقلها وحيازتها من ذمة شخص إلى آخر بصفة غير مشروعة لذا يمكن أن تكون محل لجريمة السرقة، إذ يرى هذّا الجانب الفقهي أنّ جوهر الاختلاس في السرقة هو إمكانية نقل حيازة الشيء محل السرقة وإدخاله في الذمة المالية للجاني ويتحقق ذلك في السرقة المعلوماتية عن طريق سلب المعلومات المملوكة للغير والمنسوخ على الدعامة لأنّ الدعامات بلا معلومات لا قيمة لها، وبالتالي في حالة السرقة ينتقل المال المعلوماتي من حيازة مالكه إلى حيازة الغير[186].

الفرع الثاني

أنماط وطرق سرقة المال المعلوماتي المعنوي

إنّ الأموال المعلوماتية المعنوية اللامادية المخزنة في قواعد البيانات والمتبادلة عبر خطوط الشبكة، عادةً ما تكون هدف وغاية الجاني في الجرائم المعلوماتية.

ويأخذ السلوك الإجرامي للجاني في جرائم السرقة المعلوماتية أحد الصورتين إما الالتقاط غير المشروع للبيانات عن طريق التجسس الإلكتروني وإما أن يقوم الجاني باستخدام وسرقة وقت الحاسب الآلي بصفة غير قانونية.

---

[184]–أحمد خليفة الملط، المرجع السابق، ص.243.

[185]–محمد علي العريان، المرجع السابق، ص.117.

[186]–أحمد خليفة الملط، المرجع السابق، ص.247.

أولا: الالتقاط غير المشروع للمعلومات

تقنية الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات تمكن المخترق من الوصول إلى محتويات النظام من المعلومات والبيانات وإمكانية التقاطها وسرقتها بعد ذلك[187]، ويتمكن المجرم المعلوماتي من التقاط المعلومات إما عن طريق التجسس المعلوماتي أو عن طريق إستخدام أساليب تظليلية أو عن طريق تفجير الموقع المستهدف.

1- أسلوب التجسس المعلوماتي:

يعتبر التجسس من أقدم الأساليب التي اعتمد عليها الإنسان أثناء الحروب والنزاعات، إذ كان الإنسان يتجسس على أعدائه لمعرفة أخبارهم والخطط التي يعدّها لمهاجمته، ويبرز عصر العولمة وما ترتب عنها من تطور وازدهار في الإتصالات تحول التجسس من صفته التقليدية إلى ما يعرف بالتجسس المعلوماتي أو التقني[188]، ويتحقق السلوك الإجرامي في جريمة التجسس المعلوماتي باستخدام البرامج التي تمكنه من الإطلاع على المواد والبيانات المرسلة عن طريق الشبكة المعلوماتية أو أحد أجهزة الكمبيوتر دون سبب مشروع، والتجسس المعلوماتي يأخذ أنواع عدة من بينها التجسس العسكري، أو التجسس التجاري، أو التجسس الشخصي، ولقد ازدادت في الآونة الأخيرة أساليب التجسس التجاري خاصة مع توسع التجارة الإلكترونية عبر الشبكة العنكبوتية ففي إستفتاء الذي أجري لمستوردي الأمن الصناعي في الولايات المتحدة الأمريكية عام 1996 حيث تم من التأكد على حصول الكثير من الدول وبشكل غير قانوني على بيانات سرية لأنشطة تجارية وصناعية في الولايات المتحدة الأمريكية[189] وهذّا ما أدى بالمشرع الأمريكي إلى إصدار تشريع يجرم سرقة الأسرار التجارية لشركات ويعتبرها جريمة فيدرالية[190].

---

[187]-محمود أحمد عبابنة، المرجع السابق، ص.86.

[188]-خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية؛ المرجع السابق، ص.338.

[189]-خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية؛ المرجع السابق، ص.341.

[190]-حسن طاهر داود، جرائم نظم المعلومات؛ أكاديمية نايف العربية للعلوم الأمنية، السعودية، 2000، ص.26.

2-استعمال أساليب تضليلية:

كقيام أحد الأشخاص بإنشاء موقع وهمي مشابه لموقع إلكتروني مشهور يقدم خدمات ممتازة لعملائه، فإنشاء هذا الموقع الوهمي سيؤدي إلى تظليل عملاء الموقع الأصلي المشهور ويتجهوا إلى التعامل مع الموقع الوهمي مما يسمح لهذا الموقع الوهمي من الاستفادة من المعلومات السرية للعملاء كالبيانات الاسمية مثل بطاقات الدفع الإلكتروني وبعد ذلك يتم إستغلال تلك المعلومات بأسلوب غير مشروع.

ويعتبر أول حكم قضائي في فرنسا صادر عن محكمة "كليرمون فيران" Clermont-Ferrand يجرم السرقة المعلوماتية باستعمال أساليب تظليلية في قضية تتلخص وقائعها أن هناك سيدة موظفة لدى إحدى الشركات التجارية حيث قامت هذه الموظفة بنقل البيانات الخاصة بعملاء الشركة وحفظها داخل دعامة رقميةUSB [191] واستغلت البيانات المحفوظة فيه، لإنشاء شركة وهمية من أجل منافسة الشركة التي كانت تعمل لحسابها، وفي 17 فيفري 2009 قامت محكمة"كليرمون فيران" بإدانة هذه الموظفة بجريمة السرقة لأن هذه الأخيرة قامت باختلاس ملفات الكمبيوتر ذات طابع سري[192].

3-تقنية الموقع المستهدف:

تتم هذه الجريمة عن طريق وصول عدد ضخم من رسائل الإلكترونية مجهولة المصدر[193]من جهاز الحاسب الآلي للجاني إلى جهاز المستهدف، ويستخدم في إرسالها برامج محظورة بقصد التأثير على السعة التخزينية[194] حيث يجد صاحب البريد الإلكتروني نفسه أمام كم هائل من الرسائل عديمة الفائدة وقد يصاحبها فيروسات أو صور أو ملفات كبيرة الحجم يترتب

---

[191]-**USB**:هو ناقل متسلسل عام يقوم بنقل البيانات يسمح بوصل أغلب الملحقات الطرفية والأجهزة المرتبطة بجهاز الحاسوب لنقل المعلومات بينهما، أنظر: الرابط الإلكتروني

http://ar.wikipedia.org ، ماي 2015.

[192]-Le figaro, **«Première sanction d'un vol de données numériques par un tribunal »,** article du 3 octobre 2011: http://blog.lefigaro.fr/crequy/2011/10/premiere-sanction-dun-vol-de-donnees-numeriques-par-un-tribunal.html .Vu mars 2015.

[193]-خالد ممدوح إبراهيم، أمن المستندات الإلكترونية؛ المرجع السابق، ص.158.

[194]-بن عقون حمزة، المرجع السابق، ص141.

عليه تعطيل نظام الحماية مما يسمح للجاني بالدخول إلى النظام وسرقة كل ما يحتاج إليه من معلومات وبيانات مملوكة للغير[195].

ثانيا: سرقة منفعة الحاسب

يطلق على هذّه التقنية العديد من التسميات، فهناك من الفقه من سماها بإساءة إستخدام وقت الحاسب أو الخدمات التي يؤديها[196]، واستعمل بعضهم الأخر للدلالة عليه سرقة وقت الحاسوب، أو تشغيل الحاسوب دون مقابل[197]، وترتكب هذّه الجريمة باستخدام غير المشروع للحاسب الآلي لتحقيق أغراض شخصية[198] أو تجارية دون علم مالكه فغالبًا ما ترتكب من قبل العاملين في القطاع العام أو الخاص، ويرتكز الاستخدام غير المشروع لنظام الحاسوب بصورة رئيسية على الخدمات التي يوفرها هذا النظام، وهي تتعلق بمعالجة وإرسال المعطيات، ولاسيما تلك التي تتم عن طريق المكونات المادية للحاسوب أو عن طريق استخدام برامج الحاسوب والبيانات المخزنة فيه[199]، قد ترتكب جريمة سرقة وقت الحاسب الآلي من قبل أشخاص مشتركين في موقع ما من مواقع الشبكة العنكبوتية عن طريق دفع الاشتراك نظيرة ما يوفره الموقع من خدمات وامتيازات لعملائه الّذين دفعوا قيمة الاشتراك ومن خلاله يمكن لعملائه من الدخول إلى الموقع في أوقات محدّدة في اليوم وتقوم جريمة سرقة الخدمة في هذّه الحالة بدخول الجاني إلى الموقع باستخدامه كلمة المرور التي تحصل عليها نظير اشتراكه في الفترات الزمنية غير المصرح بها للدخول.

ولقد رفض القضاء الفرنسي إضفاء وصف السرقة على الاستغلال غير المشروع لوقت الحاسب في حكم صادر عن محكمة جنح **Lille** في قضية تتلخص وقائعها في قيام اثنين من المختلسين لديهم شغف بالمعلوماتية بإنشاء خط بريدي في النظام المعلوماتي الخاص بشركة

---

[195]–عبد الفاتح بيومي حجازي، النظم القانونية لحماية التجارة الإلكترونية؛ دار الفكر الجامعي، مصر، 2002، ص.132.

[196]-Deveze(j), attentes aux systèmes de traitement automatisé de donnée; J.C.P, N°44, p.p 140-180.

[197]–محمد أحمد عبابنة، المرجع السابق، ص.88.

[198]–محمد علي العريان، المرجع السابق، ص.119.

[199]-Sieber(v),les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique; R.I.d.P,1993,p.18.

فرنسية، إذ تحملت الشركة تكاليف إنشاء ذلك الخط البريدي، اكتشفت الجريمة عندما لاحظ المسؤول عن هذه الشركة وجود 927 **Email** في الصندوق البريد الخاص بها لا يخص الشركاء وتم التعرف على شخصية مرتكبي هذا الفعل، فتم تقديمهما أمام محكمة **Lille** بتهمة السرقة بوصفهما قد استعملا بدون وجه حق حاسبًا آليًا خاصًا بالغير، إلا أن المحكمة برأتهما إستنادًا إلى عدة أسباب لعلا أهمها يتمثل في أن المشرع الفرنسي لا يعاقب على سرقة المنفعة كما لا يمكن وصف البرنامج الذي تم انتهاك سريته بأنه محمي طبقًا لقانون حماية المؤلف لأنه لا يحتوي على أي عنصر ابتكار، ومن جهة أخرى لم يمنع المتهمان مستخدمي الشركة المدعية من استخدام جهاز الكمبيوتر[200].

الفرع الثالث

موقف المشرع الجزائري من السرقة المعلوماتية

ما يعاب على المشرع الجزائري أنّه لم يتضمن نص صريح يجرم فعل سرقة المال المعلوماتي المعنوي، فيخضعها إلى نّص المادة **350** من قانون العقوبات الجزائري ولعلّ السبب في ذلك ورود هذه المادة بصفة فضفاضة حيث نلاحظ أنّ المشرع الجزائري استعمل كلمة "شيئًا" والشيء بالمعنى الاصطلاحي قدْ يتضمن الأشياء المادية والمعنوية، بالإضافة إلى ذلك فالمشرع الجزائري في إطار القوانين والجرائم التقليدية ساير التشريعات المقارنة كالتشريع الفرنسي الذي نص في المادة **311** من قانون العقوبات الفرنسي على أن: "**السرقة هي اختلاس الشيء المملوك للغير...**" والملاحظ أن هذه المادة تتطابق مع نّص المادة **350** من قانون العقوبات الجزائري إذْ أنّ المشرع الجزائري استعمل عبارة "الشيء " الذي قد يقصد بها المال المعنوي أيضًا[201].

كذلك فجريمة سرقة المعلومات تقوم كالسّرقة التقليدية على شرط إمكانية المال للحيازة والانتفاع به، حتى ولو كانت الحيازة معنوية، وهذّا ما يمكن استخلاصه من نص المادة **2/394** من قانون العقوبات الجزائري والتي قد تسمح بتطبيق أحكام المادة **350** من نفس القانون إذا ما اعتبرنا كلمة "الشيء" قد تنصرف إلى المال المعلوماتي المعنوي.

---

[200]–محمد أمين الرومي، المرجع السابق، ص.50.

[201]–زيبح زيدان، المرجع السابق، ص.85.

المطلب الثاني

إتلاف المال المعلوماتي

يعاقب المشرع الجزائري على الآثار المترتبة عن جريمتي الدخول والبقاء غير المصرح به في النظام المعلوماتي، والتّي تشمل كل حذف، أو تعديل للمعطيات، أو تعطيل نظام عمل المنظومة، أو إتلاف المال المعلوماتي الذي له صورتان فالصورة الأولى، تتمثل في إتلاف المكونات المادية للنظام المعلوماتي؛ أما الصورة الثانية، تشمل إتلاف المكونات المعنوية للنظام المعلوماتي[202].

الفرع الأول

إتلاف المكونات المادية للنظام المعلوماتي

يقصد بالإتلاف الإنقاص من الشيء وجعله في حالة غير الحالة التي هو عليه بحيث لا يمكن الاستفادة منه وفقًا للغرض الذي أعد من أجله[203]، وتتعدد أسباب إتلاف المعدات المادية فقد يكون مصدرها الطبيعة كالزلازل والفيضانات...إلخ، وقد يكون مصدرها فعل الإنسان سواءً بكسر أو حرق أو إتلاف الأشرطة والأقراص الممغنطة وشاشات العرض[204] ولم يجد المشرع الجزائري إشكالاً في إخضاعه لنصوص التقليدية، إذ تنص المادة**407** من ق.ع الجزائري: "**كل من خرب أو أتلف عمدًا أموال الغير المنصوص عليها في المادة 396 بأية وسيلة أخرى كليًا أو جزئيًا يعاقب بالحبس من سنتين(2)إلى خمس(5) سنوات وبغرامة من 500 إلى5.000دج دون الإخلال بأحكام المواد 395 إلى 404... إلخ**".

ونستخلص من خلال المادة المذكورة أعلاه لقيام جريمة الإتلاف يجب أن يكون موضوعها مالاً وأن يكون هذا المال مملوك للغير، وتجدر الإشارة أنّ الحماية الجنائية للمعطيات تنصب على تلك التي توجد داخل نظام المعالجة أو تلك التي تكون في طريقها لدخول إليه، أو تلك التي خرجت منه بعد دخولها، وعليه فلا تقوم الجريمة إذا وقع النشاط الإجرامي على المعطيات خارج النظام

---

[202]–أحمد خليفة الملط، المرجع السابق، ص.527.

[203]–محمد حمّاد مرهج الهيتي، المرجع السابق، ص.197.

[204]–أحمد خليفة الملط، المرجع السابق، ص.527.

كما لو كانت هذه المعطيات مفرغة على قرص أو شريط ممغنط خارج النظام، على خلاف إتلاف المال المعلوماتي المعنوي على شبكة الإنترنيت وما يترتب عنه من اعتداء على نظام المعالجة الآلية للمعطيات سواءً كان بالدخول أو البقاء غير مشروع فتطبق عليه أحكام المادة **394 مكرر1** من قانون العقوبات الجزائري " **يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3)سنوات و بغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها** "، ومن خلال المادة **394 مكرر1** نستخلص منها النشاط الإجرامي في إتلاف المال المعلوماتي الذي يتجسد في إحدى الصور الثلاث: الإدخال، المحو، التعديل، ولا يشترط اجتماع الصور الثلاث معًا بل يكفي أن يصدر من الجاني أحد منهما فقط لكي يتوافر الركن المادي[205] وإنما في اعتقادنا أن هذه الصور الثلاث وردت على سبيل المثال وليس الحصر.

الفرع الثاني

إتلاف المكونات المعنوية للنظام المعلوماتي

يطلق على إتلاف المكونات المنطقية لنظم المعلوماتية تعبير لدى بعض الفقهاء يسمى "تدمير المعلومات" ويأخذ فعل إتلاف المكونات المنطقية لنظام المعلوماتي إحدى الصورتين، الصورة الأولى متمثلة في إتلاف البيانات المنسوخة على الدعامات والشرائط الممغنطة، فيحدث الاعتداء بإتلاف البيانات والبرامج والمعلومات المنسوخة على الدعامات المادية كالأسطوانات أو الشرائط الممغنطة بأي طريقة من طرق الإتلاف مما يجعلها غير صالحة للاستعمال[206]، أما الصورة الثانية تكون بإتلاف البيانات والمعلومات الموجودة داخل النظام المعلوماتي.

ويحدث تدمير النظم المعلوماتية بعدة أساليب مستخدمة في إتلاف البيانات والبرامج، بدءًا من فيروس الحاسب الآلي ومرورا ببرامج الدودة وانتهاءً القنبلة المنطقية والزمنية وسنتعرض لكل منها بالتوضيح الموجز على الوجه التالي:

---

[205]–محمد حمّاد مرهج الهيتي، المرجع السابق، ص.199.

[206]–أحمد خليفة الملط، المرجع السابق، ص.(528–529).

أولاً: فيروسات الحاسب الآلي

هو عبارة عن برنامج يتم زرعه على الأقراص والأسطوانات الخاصة بالحاسب الآلي ويظل خامدًا كالبركان لفترة محددة من الزمن ثم ينشط فجأةً بهدف تدمير البرنامج والبيانات المسجلة فيه[207]، وهذا الأسلوب يشبه إلى حد كبير أسلوب الفيروسات الحيوية التي تصيب الإنسان[208]، وتكمن خطورة الفيروس في أنه يجعل البرنامج المصاب ينتج برامج جديدة هي الأخرى مصابة بذات الفيروس مما يساعد على انتشاره بصورة أكبر، كما يرسل عن بعد وهذا ما يؤدي إلى صعوبة اكتشافه فهو يؤثر على برامج التشغيل ويمتد أثره إلى الأنظمة الأخرى الملحقة به، ويؤدي إلى الإستلاء على الذاكرة ويصبح من غير الممكن التعامل مع هذه المعلومات باستخراجها مثلاً أو استرجاعها والسبب في ذلك أنّ البرنامج الدخيل جعل برامج الحاسب الآلي لا يستجيب للأوامر التي توجه إليه، وللفيروسات عدّة أنواع منها، فيروس عام العدوى، فيروس عام الهدف، الفيروسات النائمة، الفيروسات القاتلة، فيروس حصان طروادة...إلخ[209].

ثانيًا: برامج الدودة

ينتقل هذا النوع من البرامج من حاسب لآخر وأثناء عملية الانتقال تتكاثر كالبكتيريا باستنساخ نسخ منها، ومن أهدافها شغل أكبر مجال من سعة الشبكة، وتتعدى أهدافها بعد التكاثر والانتشار إلى تخريب الملفات وأنظمة التشغيل[210]، وتم إطلاقها من طرف طالب أمريكي سنة 1988 يدعى "روبرت موريس" طالب في قسم علوم الكمبيوتر وتعتبر من أبرز القضايا المشهورة في هذا الشأن وأطلق عليها تسمية« Le ver de Morris » [211].

ثالثا:القنابل المنطقية والزمنية

هي برامج تهدف إلى تدمير المعلومات كوسيلة لارتكاب جريمة الإتلاف وعلى ذلك يتضح أنّ القنابل المنطقية، تظل ساكنة تبقى غير مكتشفة لمدة قد تصل إلى عدة أعوام يحددها مؤشر

---

[207]–محمد حمّاد مرهج الهيتي، المرجع السابق، ص.203.

[208]–أحمد خليفة الملط، المرجع السابق، ص.540.

[209]–محمد أمين الشوابكة، المرجع السابق، ص.239.

[210]–أحمد خليفة الملط، المرجع السابق، ص.544.

[211]-Filiol(e), Les virus informatiques : théorie, pratique et applications, Springer, 2em éd, France, 2009,P. 283.

موجود في برنامج القنبلة؛ أما القنبلة الزمنية تقوم بوظيفتها التخريبية خلال وقت محدد مسبقًا ويتم إدخالها في برامج بطريقة متخفية مع برامج أخرى تهدف إلى تدمير معلومات النظام[212] ومن أمثلة عن ذلك قيام مبرمج فرنسي بدافع الانتقام إثر فصله من العمل، بوضع قنبلة زمنية على شبكة المعلومات الخاصة بالمنشأة، بحيث انفجرت بعد مضي 6 أشهر من رحيله عن المنشأة[213].

الفرع الثالث

موقف المشرع الجزائري من إتلاف المال المعلوماتي

لقد عالج المشرع الجزائري جريمة الإتلاف المعلوماتي في صورتين، الأول عندما يكون الإتلاف نتيجة الدخول والبقاء غير المصرح به في منظومة معلوماتية وهذا ما تضمنته المادة **394مكرر** فقرة**(2)** ق ع، والمشرع الجزائري شدد العقوبة وجعلها تبدأ من ستة(6) أشهر إلى سنتين(2) حبس وغرامة مالية تبدأ من 50.000 دج إلى 150.000 دج.

ونلاحظ من خلال المادة المذكورة أعلاه فالمشرع الجزائري نص على الإتلاف المعلوماتي وجعله كظرف مشدّد لجريمتي الدخول والبقاء غير مشروع في منظومة معلوماتية إذا ترتب عن الدخول أو البقاء حذف أو محو أو تعديل لمعطيات المنظومة.

كما أقر المشرع الجزائري في قانون العقوبات عقوبة على جريمة الإتلاف باعتبارها جريمة قائمة في حد ذاتها وذلك في نص المادة **394 مكرر1** ق ع إذ تنص على أنه:" **يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات و بغرامة من500.000دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.**"

والملاحظ أيضًا أن المشرع في هذه المادة بادر بتشديد العقوبة وجعلها تبدأ من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من500.000دج إلى2.000.000 دج على خلاف ما نصت عليه المادة **394مكرر** فقرة**2** من ق.ع السالفة الذكر، كما تأثر المشرع الجزائري بالمشرع الفرنسي في تعريفه للأفعال الإجرامية المشكلة لجريمة الإتلاف المعلوماتي والمتمثلة في إدخال المعطيات

---

[212]–أحمد خليفة الملط، المرجع السابق، ص.545.

[213]–بن عقون حمزة، المرجع السابق، ص.106.

بطريقة غير مشروعة أو إزالتها أو تعديلها[214]، إذ هناك فقط اختلاف بسيط في العقوبة المقررة وهذا ما يظهر جليًا في نص المادة**323-3** من قانون العقوبات الفرنسي والتي تنص على أن:" **إدخال البيانات بطريق الغش في نظام المعالجة الآلية أو محوها أو تعديلها بطريق الغش للمعطيات التي يحتوي عليها يعاقب فيها بالحبس لمدة خمس (5) سنوات وبغرامة مقدرة ب75.000 أورو...**"[215].

كما تفطن المشرع الجزائري في تقرير الحماية الجنائية للمنظومة المعلوماتية من خلال فرض عقوبات تكميلية المنصوص عليها في المادة **394 مكرر 6** إلى جانب العقوبات الأصلية، وهذا ما يؤكد أن المشرع الجزائري قد حقق خطوة إيجابية في مجال التجريم المعلوماتي من خلال المواد القانونية التي كرسها لحماية مؤسسات الدولة ومحتوى شبكة نظام المعلومات[216].

المطلب الثالث

التزوير المعلوماتي

التزوير هو تغير الحقيقة بقصد الغش في محرر رسميًا كان أو عرفيًا وفق لطرق التي حددها القانون من شأن هذا السلوك الإجرامي أن يمس بمصالح الغير، ويكون الهدف من تزوير المحرر لغرض استعماله فيما أعد من أجله[217].

غير أن التزوير في عصرنا هذا لم يعد محصورًا في المحررات العرفية والرسمية والتجارية إذ أصبحنا نسمع عن التزوير الإلكتروني وهو الذي يرد على قاعدة البيانات والبرامج والملفات، بتغيير الحقيقة على الدعامات التي تحمل تلك المعلومات والبيانات التي تمثل مخرجات الحاسب الآلي،

---

[214]–زيبح زيدان، المرجع السابق، ص.59.

[215] -**Article 323-3**: **«La fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende… »** code pénal francais : http://droit-finances.commentcamarche.net/download/telecharger-199-code-penal-2015-pdf-en-ligne .Vu mai 2015.

[216]–زيبح زيدان، المرجع السابق، ص.53.

[217]–بوسقيعة أحسن، الوجيز في القانون الجزائي الخاص، الجزء الثاني: الجرائم الاقتصادية وبعض الجرائم الخاصة(طبعة منقحة ومتممة في ضوء النصوص الجديدة)؛ ط.2، دار هومة، الجزائر،2006.

سواء تمثلت في مخرجات ورقية كالتي تتم بواسطة الطابعة الرقمية؛ أو سندات مخزنة في دعامات إلكترونية[218].

بالرجوع إلى المادة **214** وما يليها من ق.ع الجزائري نجد المشرع قد جرم كل شخص يزور محررًا رسميًا كان أو عرفيًا أو محررًا تجاريًا.

لعل التساؤل الذّي يمكن إثارته في هذّا المقام هل نّص المادة **394مكرّر1** يمكن لها أن تستوعب التزوير المعلوماتي الواقع داخل نظام المعالجة الآلية للمعطيات والتزوير المخرجات الحاسب الآلي باعتبارها محررات إلكترونية؟ وهل النصوص الخاصة بالتزوير التقليدي يمكن إسقاطها على التزوير المعلوماتي في صورتيه؟

الفرع الأول

التعريف بطرق التزوير المعلوماتي

لقد حددت المواد **214** إلى **229** من ق ع طرق التزوير في المحررات الرسمية والعرفية والتجارية، إذْ حصرتها في ثمانية طرق ثلاثة منها تدخل في طرق التزوير المادي بينما تقع خمس منها في طرق التزوير المعنوي[219]، فطرق التزوير نوعان إما تزويرًا ماديًا؛ أو تزويرًا معنويًا.

أولاً: التزوير المادي

هو ذلك التزوير الذي يترك أثرًا ماديًا يدل على العبث بالمحرر سواء بالزيادة أم بالحذف أو بالتعديل أو باصطناع محرر لا وجود له في الأصل، ويقع التزوير المادي بالطرق المحددة وهي ثلاث:

1-وضع توقيع مزور:

ترتكب جريمة التزوير عندما يقوم الجاني بوضع إمضاء ليس له في المحرر، فإذا استلم شخص تحويلاً مرسلاً إلى شخص آخر يشاركه في الإسم وأمضى هو التحويل اعتبر هذّا تزويرًا بوضع إمضاء مزور، وقد يعد أيضًا تزويرًا بانتحال شخصية الغير، ويستوي أن يكون هذاّ

---

[218]-خريت علي محرز، التحقيق في جرائم الحاسب الآلي؛ دار الكتاب الحديث، مصر، 2012، ص.140.

[219]-بوسقيعة أحسن، الوجيز في القانون الجزائي الخاص، الجزء الثاني: الجرائم الاقتصادية وبعض الجرائم الخاصة، المرجع السابق، ص.317.

الإمضاء لشخص موجود أو لشخص وهمي، ويتحقق التزوير حتّى ولو كان الإمضاء صحيحًا في حد ذاته وصادرًا من صاحبه إذا كان الجاني قد حصل عليه بطريق الإكراه[220].

فيمكن تصور وقوع تزوير التوقيعات في المحررات الإلكترونية إذْ يكون من السهل إدخال ذلك التوقيع المزور لتعويض التوقيع الصحيح على المحرر الموجود في الحاسب الآلي عن طريق جهاز الماسح الضوئي المرتبط بالحاسوب فهذه الوسيلة التقنية تمكن الحاسب الآلي من استقبال الصور والتوقيعات والنصوص المطلوب ظهورها على شاشته دون الحاجة إلى إستخدام الكتابة القلمية إن صح التعبير[221].

2- حذف أو إضافة أو تغيير مضمون المحرر:

قد يحصل التزوير بالحذف في محرر بشتّى الطرق، فقد يحصل بشطب جملة أو عبارة أو كلمة من المحرر، أو بمحوها وبطمسها أو قطع وتمزيق جزء من المحرر، أما التزوير بالإضافة فقد يحدث بتحشير العبارات والكلمات بين السطور أو بتعليتها على الهامش أو بإضافتها في مواضيع متروكة على بياض، في حين التزوير بالتغيير يكون باستبدال عبارة بعبارة أخرى [222] ومثال الذي يمكن استحضاره في هذّا الصدد ما قام به أحد قراصنة الهواة (hacker) بالدخول إلى الحاسب الرئيسي وقام على سبيل المزاح بتغيير رقم واحد في قيمة للوحدة الدولية للأبحاث الفيزياء النووي بسويسرا للنسبة التقريبية π 3.142857 حيث جعلها 3.143857، وقد نتج عن هذا التغيير البسيط الذي لم يلاحظه الباحثون خسارة ملايين من الدولارات بسبب النتائج غير الصحيحة للأبحاث[223].

---

[220]-جندي عبد المالك، الموسوعة الجنائية، الجزء الثاني: إضراب- تهديد، دار إحياء التراث العربي، لبنان، 2008، ص.373.

[221]-خريت علي محرز، المرجع السابق، ص.184.

[222]-جندي عبد المالك، المرجع السابق، ص. 376.

[223]-حسن طاهر داود، المرجع السابق، ص. 30.

[224]-عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون(دراسة مقارنة)؛ ط2، منشورات الحلبي الحقوقية، لبنان، 2007، ص.253.

[225]-خريت علي محرز، المرجع السابق، ص.200.

3-اصطناع محرر:

يقصد به خلق محرر بأكمله ونسبته إلى غير محرره فهو إما أن يتضمن إنشاء محرر بتقليد الخط المنسوب إليه ذلك المحرر أو بدون تقليد خطه، ومن أمثلة ذلك إنشاء سند دين ونسبته زورًا إلى الغير أو اصطناع شهادة إدارية بالوفاة ونسبتها لضابط عمومي[224].

عادةً ما يقع التزوير بالاصطناع في المحررات الإلكترونية بواسطة التقنيات التي وفرتها الثورة المعلوماتية وقد يكون في تقليد العلامات التجارية أو النقود سواء كان محل التقليد شيئًا مكتوبًا أو مرسومًا كالعلامات التجارية[225].

ثانيًا:التزوير المعنوي

التزوير المعنوي هو كل تغيير للحقيقة في مضمون المحرر ومعناه وظروفه وملابساته تغييرًا لا يمكن إدراك أثره، ويتم هذا النوع من التزوير وقت تحرير المحرر من طرف محرره فيكون صحيحًا في شكله، غير أنه يتضمن بيانات غير صحيحة أو غير مطابقة للواقع، وهذا إما بكتابة اتفاقات على خلاف ما أملاه عليه الأطراف، أو جعل واقعة مزورة في صورة واقعة صحيحة أو جعل واقعة غير معترف بها أو تغيير إقرار أولى الشأن أو انتحال شخصية الغير[226].

1-تغير إقرار أولى الشأن:

يتحقق التزوير بهذه الطريقة عندما يكلف الجاني بكتابة المحرر، وفقًا للبيانات والشروط التي طالب أصحاب الشأن إثباتها بالمحرر، فيكتب بيانات أو شروطًا أخرى مغايرة لما طُلبَ منه، ويقع التزوير بهذه الطريقة في محررات رسمية من طرف موظف عمومي كأصل عام ويتحقق ذلك عند قيام كاتب قاضي التحقيق مثلًا بتغيير ما أفاد به المتهم أو الشاهد أو طلب إثباته في محضر التحقيق أو في الجلسة، كما قد يقع هذا التزوير في محرر عرفي فمثلًا إذا كلف مترجم بترجمة

---

[226]-بوسقيعة أحسن، الوجيز في القانون الجزائي الخاص، الجزء الثاني: الجرائم الاقتصادية وبعض الجرائم الخاصة؛ المرجع السابق، ص.317.

[227]-جندي عبد المالك، المرجع السابق، ص.386.

محرر عرفي من لغة إلى لغة أخرى فأثبت في الترجمة بيانات مخالفة لما تضمنه المحرر الأصلي فان هذا الفعل يعد تزويرًا معنويًا بتغيير إقرار أولى الشأن[227].

وعليه فتغيير إقرار أولى الشأن كطريقة من طرق التزوير المعنوي، يمكن وقوعه في التزوير المعلوماتي سواءً كان ذلك التزوير في محرر رسمي حرر من طرف موظف عمومي أو في محرر عرفي[228]، خاصةً مع تنامي ظاهرة إبرام العقود الإلكترونية وتبني معظم الدول نظام الحكومة الإلكترونية[229].

2-جعل واقعة مزورة في صورة واقعة صحيحة:

يدخل في هذه الصورة كل إثبات لواقعة في محرر على غير حقيقتها، فهذه الطريقة من طرق التزوير المعنوي ليست مرادفة لعبارة تغيير إقرار أولى الشأن بل هي تشير إلى طريقة أخرى لارتكاب التزوير، فلا يشترط أن تكون الواقعة التي قررها المتعاقدان قد كتبت محرفة في العقد بل يتحقق التزوير ولو دونت الوقائع كما قررها المتعاقدان بالضبط متى أقر المتعاقدان أمام كاتب المحرر واقعة مزورة في صورة واقعة صحيحة فأثبتها بحسن نية في محرره[230]، ومن الأمثلة حول هذا النوع من التزوير المعنوي كأن يثبت موثق في عقد بيع أن المشتري قد دفع نصف الثمن في حين أنه لم يدفع شيئًا أو يذكر للعقد تاريخ آخر أو مكان آخر، أو أن يثبت المحضر كذبًا في محضر حجز أنه لم يجد أي منقول في منزل المدين.

3-جعل واقعة غير معترف بها في صورة واقعة معترف بها:

هذه الطريقة تعتبر من أوسع طرق التزوير وأكثرها عمومية، ويقصد بها إثبات واقعة على غير حقيقتها، وبهذه العمومية فان طريقة جعل واقعة غير معترف بها في صورة واقعة معترف بها تشمل الطريقة الأولى للتزوير المعنوي المتمثلة في تغيير إقرار أولى الشأن، فكل تغيير إقرار أولى

---

[228]-خريت علي محرز، المرجع السابق، ص.(204،207).

[229]-**الحكومة الإلكترونية:**هو نظام تتبناه الحكومات باستخدام الشبكة العنكبوتية العالمية في ربط مؤسساتها ببعضها البعض، ووضع المعلومة في متناول الأفراد لتقريب المواطن من الإدارة. تعريف متوفر على هذا الرابط:
http://ar.wikipedia.org ماي 2015.

[230]-جندي عبد المالك، المرجع السابق، ص.386.

الشأن يعتبر بمثابة جعل واقعة غير معترف بها في صورة واقعة معترف بها، ومن أمثلة عن هذا التزوير أن يثبت القاضي أن المتهم قد اعترف بالجريمة في حين أنه لم يعترف بها، أو أن يثبت موثق أن البائع قد تسلم الثمن كاملًا في حين أنه لم يقر بذلك[231].

4-انتحال شخصية الغير:

يتحقق السلوك الإجرامي في هذه الطريقة حينما يقوم الجاني بانتحال شخصية الغير أو التسمية باسمه سواءً كانت هذه الشخصية موجودة في الواقع أو غير موجودة[232].

وغالبًا ما يكون المنتحل في مثل هذا التزوير مساهمًا مع المكلف بتحرير المحرر سواء كان هذا الأخير حسن النية أو سيئ النية وهو الذي يكون الفاعل المادي في هذه الجريمة، كأن يتقدم شخص إلى المحكمة بصفته شاهدًا ويتسمى باسم الشاهد الحقيقي ويدلي بشهاداته في الجلسة باعتباره شاهدًا حقيقيًا، أو يتسمى الجاني باسم طالب ما ويتقدم للامتحان بدلًا منه[233]، بالإضافة إلى ذلك عادةً ما يتم انتحال شخصية الغير عن طريق انتزاع صورة شخص من مستند مثبت لشخصيته كجواز السفر الإلكتروني ووضع عن طريق الغش صورة الجاني أو صورة شخص آخر ويتم ذلك عن طريق جهاز"سكانير" الذي يمكن الجاني من رسم صورة ضوئية ونقلها إلى جهاز الحاسب الآلي، فكل هذه الوسائل التقنية تجعل من إمكانية وقوع التزوير المعلوماتي أمرًا في غاية البساطة[234].

---

[231]-بوسقيعة أحسن، الوجيز في القانون الجزائي الخاص، الجزء الثاني: الجرائم الاقتصادية وبعض الجرائم الخاصة؛ المرجع السابق، ص.321.

[232]-عفيفي كامل عفيفي، المرجع السابق، ص.253.

[233]-بوسقيعة أحسن، الوجيز في القانون الجزائي الخاص، الجزء الثاني: الجرائم الاقتصادية وبعض الجرائم الخاصة؛ المرجع السابق، ص.322.

[234]-خريت علي محرز، المرجع السابق، ص.196.

الفرع الثاني

موقف المشرع الجزائري من جريمة التزوير المعلوماتي

رغم أنّ جريمة التزوير المعلوماتي من أخطر صور الغش المعلوماتي نظرًا للدور الهام والخطير الذي أصبح يقوم به الحاسب الآلي حاليا والذي اقتحم كافة المجالات من خلال استخدامه لكم هائل من المعلومات التي كثيرا ما تكون عرضة للتزوير.

إلا أن المشرع الجزائري نص فقط في المواد **214**إلى**229** من ق.ع على التزوير التقليدي دون التزوير المعلوماتي، واكتفى المشرع فقط بنص واحد يتناول صورة من التزوير المعلوماتي في نص المادة **394مكرر1** ق.ع إذ استعمل المشرع في هذه المادة عبارة "تعديل" التي تعتبر شكل من أشكال التزوير، فالتعديل يقصد به تغيير المعطيات الموجودة داخل النظام المعالج الآلي للمعطيات واستبدالها بمعطيات أخرى[235].

إن التزوير المعلوماتي وفقًا للمشرع الجزائري يقع على المعطيات الموجودة في النظام المعالج الآلي للمعطيات، في حين أن تغيير الحقيقة في المعطيات الموجودة خارج النظام والمحملة على الدعامات والأشرطة الممغنطة لم يشملها المشرع الجزائري بالحماية من خلال نص المادة **394مكرر1** ق.ع إذ تنص:" **يعاقب بالحبس من ستة(6)أشهر إلى ثلاث(3)سنوات وبغرامة من500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها**"، فهل يعني هذا أن المعلومات الموجودة على الدعامات والتي قد تمثل محررات الحاسب الآلي يمكن إخضاعها في حالة تعديلها للنصوص الخاصة بالتزوير العادي؟

إن الإجابة على هذا التساؤل ستكون حتمًا بالنفي، باعتبار أن السندات المعالجة أليًا[236] والتي تعتبر بمثابة محررات الحاسب الآلي لا يمكن أن تخضع للنصوص الخاصة بالتزوير إذ يشترط المشرع في التزوير أن يكون المحرر محل الجريمة مكتوب وهذا ما لا يتحقق مع التغير في الوعاء

---

[235]–قارة أمال، **الجريمة المعلوماتية**، المرجع السابق، ص.53.

[236]–**السندات المعالجة أليًا:** هي كل شيء مادي متميز(قرص أو شريط ممغنط)، يصلح لأن يكون دعامة أو محلًا لتسجيل المعلومات المعالجة بواسطة نظام معلوماتي. أنظر: قارة أمال، **الجريمة المعلوماتية**، المرجع السابق، ص.56.

المعلوماتي، فالمعلومات المدونة على الدعامات ليست مكتوبة بل هي على هيئة نبضات إلكترونية بشكل يسمح فقط للحاسب الآلي بقراءتها، أو بمعنى آخر فإن هذه البيانات لا تنطوي تحت النصوص التقليدية ولا تصلح لأن تكون بمثابة محرر مكتوب، في حين أن المستندات الورقية المستخرجة من الحاسب الآلي فإنها مشمولة بالنصوص التقليدية الخاصة بالتزوير الواردة في ق.ع الجزائري بما أنها تحمل وصف المحرر المكتوب.

من خلال كل ما سبق، نستخلص أن المشرع الجزائري أشار فقط إلى التزوير الإلكتروني في المستندات المعالجة آليًا الموجودة في النظام وهذا ما نصت عليه المادة **394مكرر1**؛ أما المستندات المعالجة أليًا الموجودة خارج النظام أي المحمولة على الدعامات فهي غير مشمولة بالحماية سواءً كانت هذه الحماية في نصوص خاصة كنص المادة **394مكرر1**، أو بالرجوع إلى النصوص العامة المتعلقة بالتزوير والتي تأتي قاصرةً هي الأخرى على أن تشملها،على خلاف المشرع الفرنسي الذي ميز بين التزوير في البيانات المسجلة في ذاكرة النظام المعالج الآلي للمعطيات وبين تغييرها في محررات الحاسب الآلي[237].

ويظهر ذلك جليًا بالرجوع إلى نصوص المواد**323-3** و**411-1**ق.ع الفرنسي، إذ نجد المادة **323-3** تتضمن التزوير المنصب على البيانات المسجلة في ذاكرة النظام المعالجة الآلية للمعطيات وتنص على أنه:"**كل من أدخل عن طريق الغش بيانات في نظام المعالجة الآلية للمعطيات، أو ألغى أو عدل المعطيات التي يحتويها النظام يعاقب بخمس(5)سنوات حبس وبغرامة75.000 أورو...**"، فهذه المادة تقابلها المادة 394مكرر1 من ق.ع الجزائري؛ أما تغيير البيانات الموجودة على الدعامات والتي تمثل محررات النظام الآلي لمعالجة المعطيات تضمنتها المادة 441-1 ق.ع الفرنسي حيث تنص على أن:" **التزوير هو تغيير تدليسي للحقيقة بسوء نية من شأنه الإضرار بالغير أيًا كانت الوسيلة المنتهجة في مستند مكتوب أو في دعامة من دعائم التعبير عن الفكر التي لها شأن في إثبات حق أو واقعة لها أثار قانونية...**"[238]، فالمشرع الفرنسي بتعديله لقانون العقوبات سنة 1994 وسع في طرق التزوير فلم تعد محصورة على سبيل الحصر كما فعل المشرع الجزائري.

---

[237]-عفيفي كامل عفيفي، المرجع السابق، ص.250.

[238]-**article 441-1: « constitue un faux tout altération frauduleuse de vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établer la preuve d'un droit ou d'un fait ayant des**. **Conséquences juridiques… »** Code pénal français.

خاتمة

تعتبر الجريمة المعلوماتية من أكبر السلبيات التي خلفتها الثورة الرقمية حيث اختلف الفقه في وضع تعريف موحد لها لعل ذلك يعود إلى غياب تعريف تشريعي من جهة، والسبب الثاني طبيعة الجريمة المعلوماتية والتي تمتاز بطابع فني وتقني معقد يصعب على رجال القانون فهمها والإحاطة بجوانبها هذا ما أدى إلى تباين تعريفات الفقهية لهذه الظاهرة الإجرامية المستحدثة بين التعريف الموسع والمضيق.

وبما أن الجريمة المعلوماتية متميزة عن الجرائم التقليدية بعدة خصائص لعل أهمها طابعها العابر للحدود وإنفرادها بخاصية الجرائم الهادئة التي لا تحتاج لاستخدام العنف عند ارتكابها هذا ما أدى إلى انعدام أو صعوبة اكتشاف أثار هذه الجريمة المستحدثة بما أنها ترتكب في عالم افتراضي لا مادي.

بظهور هذه الظاهرة الإجرامية ترتب عنها بروز طائفة جديدة من المجرمين الذين يمتازون بذكاء وبالخبرة والمهارة التي اكتسبوها إما من الدراسة المتخصصة أو من خلال العمل في المجال التقني أو باحتكاكهم وتفاعلهم مع أشخاص آخرين لهم معرفة بتكنولوجيا المعلومات، والمجرم المعلوماتي عند تنفيذه للجريمة عادةً ما يعتمد على التخطيط والتنظيم إذ يشترط لتحقيق النتيجة الإجرامية في الجرائم المعلوماتية تحلي الفاعل بالدقة عند تنفيذ أفعاله الإجرامية.

إن الجريمة المعلوماتية تتمثل في كل فعل أو سلوك غير مشروع مرتبط بتقنيات المعلومات، قد يتسبب في تحميل المجني عليه خسارة، والحصول أو إمكانية الحصول على غاية مادية أو غير مادية، وغالبًا ما تكون تقنية المعلومات وسيلة لارتكاب جرائم تقليدية كالاحتيال المعلوماتي أو الجرائم الماسة بالحياة الخاصة للأفراد أو الجرائم الشكلية التي يكفي فيها الدخول إلى النظام المعلوماتي أو البقاء فيه بصفة مخالفة للقانون، وإما أن تكون المعلوماتية غاية من الجريمة إذ تهدف إلى سرقة المعلومات الموجودة في الحاسبات الآلية أو الموجودة في الوسائط الإلكترونية، ويتخذ شكل الاعتداء على المعلوماتية صورة الإتلاف أو التزوير المعلوماتي.

ومن خلال دراستنا لهذا الموضوع توصلنا إلى استخلاص مجموعة من النتائج لعل أهمها يتمثل في غياب تعريف موحد للجريمة المعلوماتية لحداثتها وطبيعتها التقنية، ونحن بدورنا نقترح التعريف القائل بأنّ الجريمة المعلوماتية هي كل فعل إيجابي أو سلبي، عمدي مرتبط باستخدام تقنية المعلومات سواءً كانت هذه التقنية أداة لارتكاب النشاط الإجرامي أو محلاً للجريمة، ويجب

استبعاد من الجرائم المعلوماتية جرائم المرتكبة على المكونات المادية للحاسوب باعتبار أنها مشمولة بالحماية بموجب نصوص تقليدية.

ومن خلال دراسة السلوك الإجرامي للمجرم المعلوماتي لاحظنا أنّ المجرم المعلوماتي ينفرد عن المجرم التقليدي سواءً من خلال سمات والدوافع الإجرامية التي دفعت المجرم المعلوماتي إلى عالم الجريمة أو بالنظر إلى السلوك الإجرامي للمجرم المعلوماتي الذي يأخذ من تقنية المعلومات إمّا كأداة مساعدة لارتكاب أفعاله المجرمة إذْ يظهر ذلك جليًا في جرائم المساس بحرمة الحياة الخاصة للأشخاص، وتظهر سلوكيات المجرم المعلوماتي أيضًا عندما تطال أفعاله أو يكون الهدف منها الاعتداء على المعلومات بحد ذاتها إما بسرقتها أو تغيير من حقيقتها سواءً بالتزوير أو بالإتلاف.

صعوبة تحديد وتقسيم الجرائم المعلوماتية والسبب في ذلك تعدد السلوكيات المجسدة لركن المادي في مختلف الجرائم المعلوماتية ولعل السبب في ذلك التطور المستمر لتقنية المعلومات التي انعكست على السلوك الإجرامي للمجرم المعلوماتي الذي يستعين بأهم التطورات التي حققتها وستحققها التكنولوجيا.

تطرح الجريمة المعلوماتية صعوبة بالغة في اكتشاف مرتكب الجريمة ومتابعته مع العلم أن معظم الجرائم المعلوماتية ترتكب في عالم افتراضي متمثل في الشبكة العنكبوتية، كما إنّ هذا النمط المستحدث من الإجرام يطرح إشكالية متابعة المتهم خاصةً إذا كان قد اقترف فعله الإجرامي في دولة أجنبية.

ومن النتائج المتوصل إليها أيضًا، برغم من أنّ بعض الجرائم المعلوماتية قابلة لتطبيق عليها بعض النصوص القانونية التقليدية كالمتعلقة بجرائم النصب وخيانة الأمانة، إلا أنّ هذّا لا يعني إمكانية تطبيق النصوص القانونية التقليدية على جميع الجرائم المعلوماتية إذ يستلزم تجريمها بموجب نصوص خاصة كما هو عليه الحال بنسبة لجريمة المساس بأنظمة المعالجة الآلية للمعطيات فهنا الأمر يختلف فلولا تخصيص المشرع الجزائري نصوص عقابية خاصة بمثل هذه الأفعال لما كانّ بإمكان العدالة الجزائرية من متابعة وإدانة مرتكبي الجرائم المعلوماتية.

إن المشرع الجزائري من خلال المادة 02 من قانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ومكافحتها لم يتضمن تحديد لصور

السلوك الإجرامي للمجرم المعلوماتي ودور المنظومة المعلوماتية في النشاط الإجرامي، والسبب في ذلك تبني المشرع الجزائري للتعريف الموسع للجرائم المعلوماتية.

إنّ المشرع الجزائري حاول مجابهة هذه الظاهرة الإجرامية المستحدثة من خلال سنه مجموعة من القوانين لعل أهمها تعديل قانون العقوبات سنة 2004، إذ استحدث الفصل السابع مكرر والذي يتضمن قانون المساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون رقم 04-15، وأعقب هذا التعديل إصدار المشرع الجزائري قانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ومحاولة المشرع تفعيل الحماية من الجرائم المعلوماتية إذْ نص هذّا القانون في المادة 13منه على استحداث هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

إنّ المشرع الجزائري رغما استحداثه لهذه القوانين السابقة الذكر إلا أنها غير كافية لمواجهة جميع الجرائم المعلوماتية.

ونتيجة لذلك فإنّنا نقترح على المشرع الجزائري أن يصدر نصوص قانونية أو يعدل من النصوص القانونية القائمة وذلك بتحديد أنماط السلوك الإجرامي للمجرم في الجرائم المعلوماتية، وتجنب التعبيرات الغامضة التي تحمل أكثر من معنى لتفادي الوقوع في المحظور والمساس بمبدأ الشرعية الجنائية التي تقتضي من القاضي عدم إخضاع النّص القانوني لتفسير الواسع، فكان من الأجدر على المشرع الجزائري أن يتدخل لتعديل النصوص المتعلقة بالأموال لكي تشمل المال المعلوماتي المعنوي.

بالإضافة إلى ما سبق فإننا نقترح أيضًا، تفعيل دور الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته في مجال مكافحة الجريمة المعلوماتية.

بما أن الجريمة المعلوماتية من الجرائم العابرة للقارات هذا ما أدى بالضرورة إلى صعوبات ضبط الجاني وبروز ما يعرف بالتنازع في القانون الواجب التطبيق لذلك كان من اللازم ضرورة توحيد القوانين على المستوى الدولي كما هو معمول به في دول العالم المتقدمة بالإضافة إلى عقد اتفاقيات دولية للحد والتصدي للإجرام المعلوماتي؛ أمّا على المستوى الداخلي فتظهر الحماية من الجرائم المعلوماتية من خلال العمل على سن القوانين الملائمة لمكافحة هذه الظاهرة الإجرامية المستحدثة، والمشرع الجزائري على المستوى الداخلي حقيقتًا نرى أنه تدخل من خلال تعديله قانون

العقوبات بالقانون 04-15وسنه لقانون 09-04 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال؛ في حين على مستوى الدولي لم يبادر بالانضمام إلى أهم الاتفاقيات الدولية لمكافحة الجرائم المعلوماتية.

يجب على مؤسسة اتصالات الجزائر نشر المواد القانونية الخاصة بالعقوبات المقررة على جرائم الكمبيوتر على ظهر فواتير الهاتف لتوعية بمخاطر هذا النوع من الجرائم.

كما نطالب من المسؤولين والمشرفين على المواقع الإلكترونية بتطوير المنظومة الأمنية وذلك بتحديثها تفاديًا للاختراق وهجمات القراصنة.

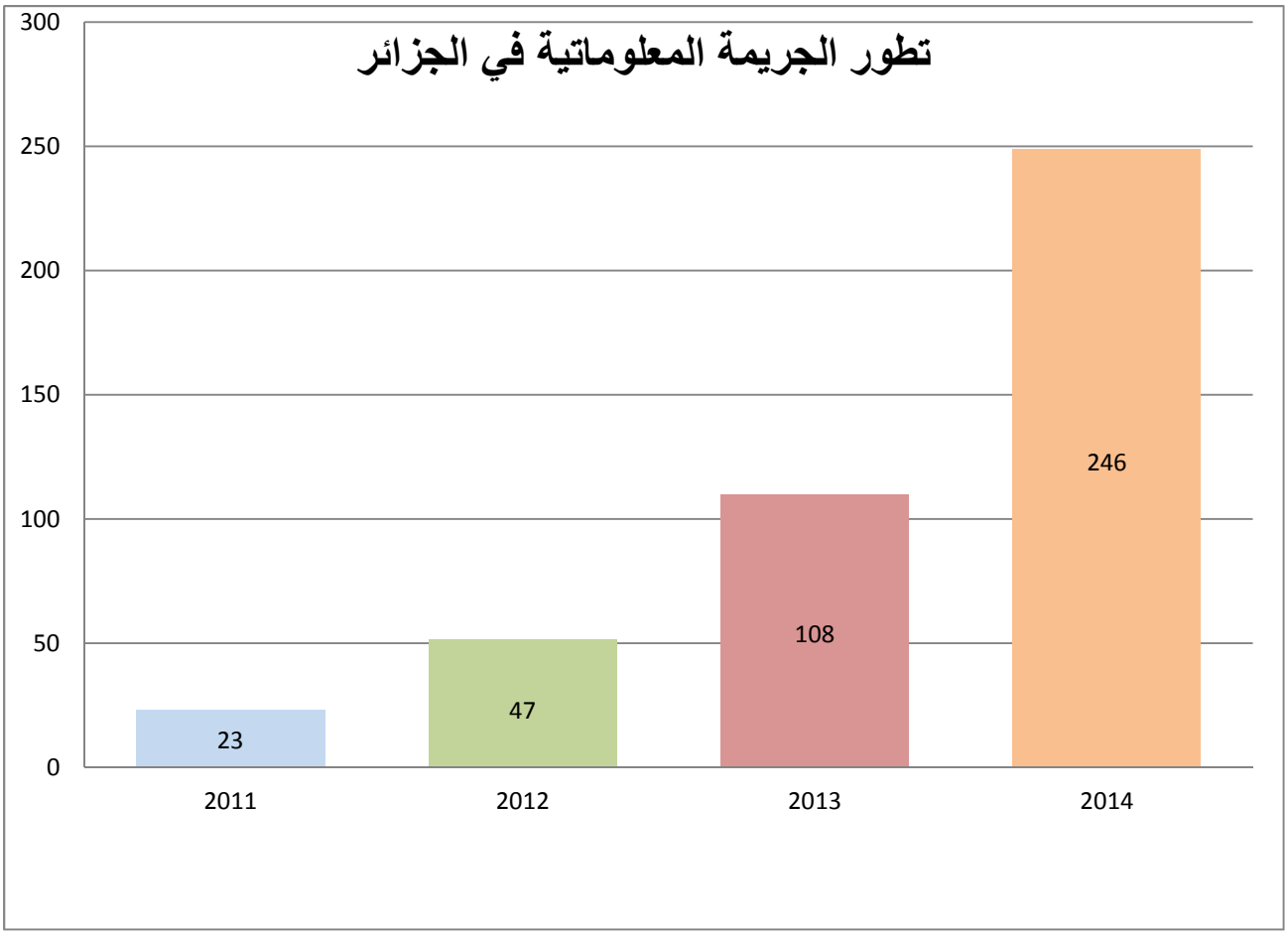
بالرغم من الجهود التي بذلها المشرع الجزائري لسد الفراغ التشريعي لمواجهة هذه الظاهرة الإجرامية وذلك بإنشاء مركز لمكافحة الجريمة المعلوماتية على مستوى القطاع الأمني(الدرك الوطني) هذا ما يدل على المتابعة الجادة والجهود المبذولة من طرفه، إلا أن هذه الجهود لا تقضي على ظاهرة الإجرام المعلوماتي نهائيًا بل التقليص منها فقط، وهذا ما يستدعي تدخل الفقه الجنائي لوضع نظرية عامة للجريمة وللمجرم المعلوماتي وذلك لتفادي المعالجة المبسترة والوصفية الخالية من أي دقة.

ملحق

عيساتي عبلة«الأمن الوطني يدق ناقوس الخطر»، جريدة أخبار اليوم، العدد الصادر في 13 ماي 2015، مقال متوفر على:

الموقع:**http://www.akhbarelyoum.dz/ar/200235/142876**

24 ماي 2015، على الساعة 23:15.



2011	2012	2013	2014
23 قضية	47 قضية	108 قضية	246 قضية
9 أشخاص متورطين	48 شخص متورط	91 شخص متورط	296 شخص متورط

قائمة المصادر والمراجع

أولاً: باللّغة العربية

1- الكتب:

أ- كتب عامة:

01-بن شيخ لحسن، مذكرات في القانون الجزائي الخاص(جرائم ضد الأشخاص، جرائم ضد الأموال، أعمال تطبيقية)، دار هومة، الجزائر، 2004.

02-بن شيخ لحسن، مبادئ القانون الجزائي العام(النظرية العامة للجريمة، العقوبات والتدابير الأمن، أعمال تطبيقية، القانون العرفي الجزائي لقرية تاسلنت "منطقة أقبو")، دار هومة، الجزائر، 2005.

03-بوسقيعة أحسن، الوجيز في القانون الجزائي الخاص، الجزء الثاني: الجرائم الاقتصادية وبعض الجرائم الخاصة(طبعة منقحة ومتممة في ضوء النصوص الجديدة)، ط.2، دار هومة، الجزائر، 2006.

04-بوسقيعة أحسن، الوجيز في القانون الجزائي الخاص، الجزء الخاص، ط.16، دار هومة، الجزائر، 2013.

05-جندي عبد الملك، الموسوعة الجنائية، الجزء الثاني: إضراب-تهديد، دار إحياء التراث العربي، لبنان، 2008.

ب- كتب متخصصة:

06-أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية لمكافحة جرائم الكمبيوتر والإنترنيت، مكتبة الوفاء القانونية، مصر، 2011.

07-إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الإئتمان، دار الجامعة الجديدة، مصر،2007.

08-جلال محمد الزعبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية(دراسة مقارنة)، دار الثقافة للنشر والتوزيع، الأردن، 2010.

09-جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول:الجرائم الناشئة عن إستخدام الحاسب الآلي، مكتبة دار النهضة العربية، مصر، 1992.

10-حسن طاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، السعودية،2000.

11-خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنيت، دار الثقافة، الأردن،2011.

12-خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، مصر، 2009.

13-خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، مصر، 2009.

14-خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية الجديدة، مصر،2008.

15-خالد ممدوح إبراهيم، التقاضي الإلكتروني، دار الفكر الجامعي، مصر، 2008.

16-خالد ممدوح إبراهيم، أمن المستندات الإلكترونية، الدار الجامعية الجديدة، مصر،2008.

17-خريت علي محرز، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، مصر، 2012.

18-زيبح زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، 2011.

19-عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، منشأة المعارف، مصر، 2009.

20-عبد الفاتح بيومي حجازي، التزوير في جرائم الكمبيوتر والانترنيت، دار الكتب القانونية، مصر، 2007.

21-عبد الفتاح بيومي حجازي، النظم القانونية لحماية التجارة الإلكترونية، دار الفكر الجامعي، مصر،2002 .

22-عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنيت(الجرائم)، دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلومات والإنترنيت مع الإشارة إلى الجهود مكافحتها محليًا وعربيًا ودوليًا، منشورات الحلبي الحقوقية، لبنان،2007.

23-عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون(دراسة مقارنة)، ط.2، منشورات الحلبي الحقوقية، لبنان، 2007.

24-علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة(دراسة مقارنة)، منشورات زين الحقوقية، لبنان، 2013.

25-قارة آمال، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر،2006.

26-محمد أمين الشوابكة، جرائم الحاسوب والإنترنيت(الجريمة المعلوماتية)، دار الثقافة للنشر والتوزيع، الأردن، 2009.

27-محمد حماد مرهج الهيتي، جرائم الحاسوب، ماهيتها موضوعها أهم صورها والصعوبات التي تواجهها، دراسة تحليلية(لواقع الاعتداءات التي يتعرض لها الحاسوب وموقف التشريعات الجنائية منها)، دار المناهج للنشر والتوزيع، الأردن، 2006.

28-محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، مصر،2007.

29-محمد خليفة الملط، الجريمة المعلوماتية، دار الفكر الجامعي، مصر،2006.

30-محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الثانية، دار النهضة العربية، مصر،1998.

31-محمد طارق عبد الرؤوف الحق، جريمة الإحتيال عبر الإنترنيت(الأحكام الموضوعية والأحكام الإجرائية)، منشورات الحلبي الحقوقية، لبنان، 2011.

32-محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، مصر، 2004.

33-محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن،2009.

34-محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن،2005.

35-منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنيت والحاسب الآلي و وسائل مكافحتها، دار الفكر الجامعي، مصر،2007.

36-نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، الطبعة الثانية، الأردن، 2010.

2- الرسائل والمذكرات:

01- بن عقون حمزة، السلوك الإجرامي للمجرم المعلوماتي، مذكرة ماجستير تخصص علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2011.

02-سوير سفيان، جرائم المعلوماتية، مذكرة ماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان،2011.

03-قارة آمال، الجريمة المعلوماتية، مذكرة ماجستير، كلية الحقوق، جامعة بن عكنون، الجزائر، 2001.

04-مزغيش سمية، جرائم المساس بالأنظمة المعلوماتية، مذكرة الماستر، كلية الحقوق، جامعة محمد خيضر، بسكرة، 2013-2014.

3-المقالات العلمية:

01-حمودي ناصر، "التنظيم القانوني لظاهرة المعلوماتية في الجزائر(الإنجازات والتحديات)"، المجلة النقدية والعلوم السياسية، كلية الحقوق، جامعة مولود معمري- تيزي وزو، الجزائر، العدد الثاني،2012، ص.ص.179-242.

02-عمر الفاروق الحسيني، "لمحة عن جرائم السرقة من حيث اتصالها بنظام المعالجة الآلية للمعطيات"، مؤتمر القانون والكمبيوتر والإنترنيت، والمنعقد في جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، أيام01-03 ماي 2000، المجلد الأول، ص.ص.329-354.

03-معاشي سميرة، "ماهية الجريمة المعلوماتية"، مجلة المنتدى القانوني، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، العدد السابع، دون سنة نشر، ص.ص.276-285.

4-النّصوص القانونية:

01-دستور الجمهورية الجزائرية الديمقراطية الشعبية، المنشور بموجب المرسوم الرئاسي رقم96-438، مؤرخ في 7 ديسمبر1996 يتعلق بنشر نص تعديل الدستور الموافق لاستفتاء 28 نوفمبر1996، ج.ر.ج.ج. عدد76، صادر في 8 ديسمبر 1996، المعدل والمتمم.

02-قانون رقم14-01 مؤرخ في04 فيفري2014، يتمم ويعدل الأمر رقم66-156 المؤرخ في08 جوان1966، والمتضمن قانون العقوبات، ج.ر.ج.ج، عدد07، بتاريخ2014.

03-قانون رقم09-04 مؤرخ في 05 أوت2009، يتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج، عدد47، 16أوت2009.

04-قانون رقم08-01 مؤرخ في 23 جانفي2008، يتمم القانون رقم 83-11 المؤرخ في 02 ماي1993، المتعلق بالتأمينات الإجتماعية، ج.ر.ج.ج، عدد04،الصادرة في 27 جانفي 2008.

5-مواقع الإنترنيت:

01-***USB:*** متوفر على الموقع: http://ar.wikipedia.org

تم الإطلاع عليه في: 10 ماي 2015، على الساعة 17:20.

02-غرفة الدردشة: متوفر على الموقع:

http://ar.wikipedia.org

تم الإطلاع عليه في: 18 أفريل 2015، على الساعة 21:05.

03-جريدة النهار الجديد،"توقيف متهم قام بعدة اعتداءات على الأنظمة المعلوماتية الخاصة ببعض مؤسسات الدولة"، عدد صادر في 2014/01/30، مقال متوفر على الموقع:
http://www.ennaharonline.com/ar/algeria_news/195696.html

تم الإطلاع عليه في: 13مارس 2015،على الساعة 19:30.

04-تقنية salami: متوفر على الموقع:

www.startimes.com/?t=24695044 ، تم الإطلاع عليه في 8 ماي 2015، على الساعة 10:40.

05-الحكومة الإلكترونية: متوفر على الموقع:

http://ar.wikipedia.org ، تم الإطلاع عليه في: 8 ماي 2015 ، على الساعة 11:00.

06-فلالي رشيد، "الشروق تقضي يومًا مع أشهر قراصنة الإنترنت في الجزائر"، عدد صادر في 22 نوفمبر 2008، مقال متوفر على الموقع:
http://www.echoroukonline.com/ara/?news=29084

تم الإطلاع عليه في: 27 ماي 2015، على الساعة 15:30.

ثانيًا: باللغة الفرنسية

1-Ouvrages:

01-CHAWKI(M), La notion de la cyber criminalité; Iehei, Paris, 2006.

02-GHEMAUTI(S), Sécurité informatique et Réseaux; Dunod, Paris, 4éme édition, 2013.

03-LARGUIER(J), CONTE(PH), FOURNIER(S), Droit pénal spécial; Dalloz, Paris, 15éme édition, 2013.

04-FILIOL(E), Les virus informatique: théorie, pratique et applications, Springer, 2em éd, France, 2009.

05-Larousse De poche, Les éditions françaises Inc, paris, 1996.

2-articles:

01-DEVEZE(J), Attentes aux systèmes de traitement automatisé de donnée; J.C.P, P.P.140-180.

02-SIEBER(V), Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatiques; R.I.D.P, 1993, P.P.18-60.

3-Sites internet:

01-code pénal français:
http://droit-finances.commentcamarche.net/download/telecharger-199-code-penal-2015-pdf-en-ligne .Vu mai 2015.

02-Le figaro, **«Première sanction d'un vol de données numériques par un tribunal »,** article du 3 octobre,2011:
http://blog.lefigaro.fr/crequy/2011/10/premiere-sanction-dun-vol-de-donnees-numeriques-par-un-tribunal.html .Vu mars 2015.

فهرس المحتويات

ملخص المذكرة باللغة العربية:

صاحب التطور التكنولوجي الذي عرفه عصرنا الحاضر مجموعة من الآثار السلبية لعل أهمها ما يعرف بالجريمة المعلوماتية، والتي أدت بدورها إلى استحداث نوع جديد من المجرمين يعرف بإسم المجرم المعلوماتي، إذ يختلف عن المجرم التقليدي سواءً من حيث الوسيلة الإجرامية أو السلوك أو فئاته أو الدوافع التي تؤدي به لارتكاب الجريمة.

وتهدف هذه الدّراسة إلى إبراز السلوكيات الإجرامية للمجرم المعلوماتي باعتبارها تأخذ إحدى الصورتين، إمّا المرتكبة بواسطة تقنية المعلومات، أو المرتكبة على تقنية المعلومات بحد ذاتها.

وإظهار مدى صمود النصوص التشريعية العقابية لمواجهة تلك التطورات التي تشهدها المعلوماتية وكذلك قدرتها على استيعاب الأشكال الحديثة لارتكاب بعض الجرائم خاصة تلك المتعلقة بالأموال.

Le résumé du mémoire en langue française :

Le développement technologique qu'a connu notre siècle présent a été marqué par un ensemble d'effets négatifs dont le cyber crime, ce qui a, à son tour, créé un nouveau type de délinquant connu sous le nom du criminel informatique, Ce dernier diffère du criminel traditionnel, que ce soit par le moyen de l'infraction, le comportement, les catégories ou les facteurs l'ayant poussé à commettre le crime.

La présente étude a pour but de faire apparaître les comportements du criminel informatique, étant donné qu'ils prennent deux aspects, soit les crimes commis par le moyen d'une technique informatique ou ceux commis sur une technique informatique en elle - même.

Par ailleurs, l'étude vise à savoir dans quelle mesure les textes législatifs répressifs peuvent faire face à l'évolution informatique et s'ils sont adaptés aux nouvelles formes d'infractions, notamment celles relatives aux biens.