جريمة الدخول إلى النظام الآلي لمعالجة المعطيات عن طريق الغش

دراسة في ضوء التشريع الفرنسي

تأليف

الأستاذ المساعد الدكتور محمد حماد مرهج الهيتي

جامعة الأنبار – كلية القانون

أ.م.د. محمد حماد مرهج الهيتي

جامعة الأنبار – كلية القانون

الملخص:

لقد قسمنا البحث إلى أربعة فصول بينا في الأول مدلول النظام الآلي لمعالجة المعطيات باعتبار أن الدخول ينصب عليه فعرضنا معناه في نظر مجلس الشيوخ وبينا النتائج التي تترتب على تبني المدلول الذي رجحناه. وانتهينا في إطار الحماية الفنية أو التقنية للأنظمة إلى أن حجج الاتجاهين تتحطم مع صراحة النص الذي جاء به المشرع. وبينا في الفصل الثاني الوسائل التي تحقق الدخول المعاقب عليه والكيفية التي يتم بها ومعيار الذي يحقق الدخول عن طريق الغش. أما الفصل الثالث الركن المعنوي للجريمة وكون الدخول عن طريق الغش يتم بصورة عمدية مما لا يمكن تصور تحققها في عن طريق الصدفة أو الاعتقاد الخاطيء. وكان لنا أخيرا وفي الفصل الرابع أن نبين أثر الضرر الذي يمكن أن يترتب على الدخول وموقف المشرع منه فوجدنا أن للضرر أثر سواء من حيث طبيعة الجريمة أو من خلال العقاب، حيث اعتبر المشرع الضرر الذي يصيب النظام ظرفاً مشدداً يستوجب تشديد العقاب سواءً بمحو المعلومات والبرامج أو بالتعديل بها أو بالتأثير على تشغيل النظام الآلي وهذا يؤيد منهج المشرع في اعتبار جسامة النتيجة معياراً لتشديد العقاب الأمر الذي استندنا إليه في القول بتأثر طبيعة الجريمة بالضرر، وبعد أن حددنا مدلول كل سلوك انتهينا إلى ان المشرع لم يفرق في العقاب في إطار ذلك مع تفاوت تلك التصرفات في الخطورة.

Illegal access crime by fraud way to the automatic data processing system

The research is divided into four chapters.

The first are deals with meaning of the automatic data processing system according to senate point of view. The results which issue from the definition of the senate within the farm work of " crime consideration " were showed.

The second chapter is assigned to study the criminal act which by means of it a crime is committed.

In the third chapter we discussed the criminal intention. In it we showed that the crime can not be committed by mistake so it is intentional crime.

While in the fourth chapter, we show the circumstances which were considered as aggravating ones by legislator and they are defined as delete or erase information, data and computer software. Or make modification in it, and damage of automatic system operation.

مع ازدياد الاعتماد على الانظمة الآلية لمعالجة المعطيات بعد التطور الذي أصابها سواء في صناعتها أو صناعة البرامج التي تشتغل بها، وكونها الوسيلة الأساسية لمباشرة مجمل الاعمال ومختلفها حتى الشخصية منها أثيرت ولا تزال تثار مشكلة أمنها ومن ثم أمن المعلومات التي تضمها وحمايتها من الاعتداء عليها.

وتعد جريمة الدخول عن طرق الغش سواء الدخول غير المصرح به أو الذي يتجاوز العوائق الفنية والتقنية تطور أساسي في محيط تجريم الاعتداءات التي يتعرض لها النظام الآلي لمعالجة المعطيات وفي محيط ما يمكن أن نسميه بقانون العقوبات المعلوماتي باعتبارها الخطوة الاولى في دراسة الحماية الجنائية للأنظمة الآلية لمعالجة المعطيات. لأنها تعتبر مقدمة لارتكاب اي اعتداء لاحق على النظام الآلي، حيث لا يكون إرتكاب جرائم أخرى كالنسخ غير المشروع والتعديل والمحو في المعلومات والبرامج...الخ من أنماط الاعتداء على الأنظمة الآلية لمعالجة المعلومات ممكناً إلا بعد الدخول إلى النظام الآلي ولا سيما أن الواقع العملي يشهد حالات اختراق متعددة لتلك النظم المحمية بأفضل الوسائل الفنية أو التقنية.

ويكتسب البحث أهميته من خطورة هذه الاعتداءات لما لتلك الأنظمة من دور شمل مجمل أنشطة الحياة المدنية والحربية على حد سواء[١] وأضحت مستودعاً كبيراً للمعلومات والأسرار على مستوى الأفراد والدول والمؤسسات والشركات، ومن تزايد حالات الاختراق الذي تتعرض له والتي يكشف عنها الواقع حيث أعلن معهد أمن المعلومات عن أن ٧٠% من حالات اختراق نظم المعلومات للشركات التي تعتمد على هذا النظام حصلت من نقاط الاتصال الخارجي، أي عبر شبكة المعلومات في حين كانت نسبة الاختراق في عام ٢٠٠٠ تشكل ٥٩%[٢] وكان عدد القضايا التي

---

١. انظر في بيان التطبيقات العملية السلمية والحربية لبرامج الحاسب الآلي
GBREMOND, La Révolution informatique dictionnaire thé matique édition HATIER 1982 p.6.

٢. يونس عرب – جرائم الكومبيوتر والانترنيت – المعنى والخصائص واستراتيجية المواجهة القانونية – الفقرة ١-٣ الموقع على الانترنيت الفقرة ١-٣ ص ١٠
http://www.araplaw.com

فتح فيها مكتب التحقيقات الفدرالي في الولايات المتحدة التحقيق (١١٥٤) قضية خلال عام ١٩٩٩، في حين كان عدد القضايا (٤٥٧) عام ١٩٩٨[٣]. وملاحظة بسيطة للفرق بين عدد القضايا تكشف عن مقدار الزيادة في عدد جرائم اختراق الأنظمة المعلوماتية؛ إذ أنها تزيد على الضعفين وتقترب من الثلاثة أضعاف. وقد كشفت دراسة أجراها معهد أمن المعلومات بالتعاون مع مكتب التحقيقات الفدرالي وبمشاركة ٥٣٨ مؤسسة أمريكية عن أن ٨٥% من المؤسسات التي تم دراستها قد تعرضت لمحاولات اختراق وقد بلغت الخسائر التي تعرضت لها المؤسسات التي استطاعت أن تحصي خسائرها من جراء عمليات الاختراق ٣٧٨ مليون دولار في حين كانت الخسائر لعام ٢٠٠٠ بحدود ٢٦٥ مليون دولار، وأن معدل الخسارة السنوية للأعوام الثلاثة السابقة لعام ٢٠٠٠ بلغت ١٢٠ مليون دولار[٤].

إن هذا البحث يعد محاولة للفت انتباه المشرعين في البلاد العربية بشكل عام خلاف البعض منها[٥] والمشرع العراقي على وجه الخصوص لسن تشريع خاص يعالج تلك الاعتداءات بعد انتشار شبكة المعلومات العالمية (الانترنيت) التي سهلت السبيل للجناة لارتكاب جرائمهم بسبب سعة انتشارها وقدرتها على تجاوز الحدود الجغرافية والسياسية مما أعطى لهذه الجرائم طابعاً دولياً مما ينبغي التكاتف في سبيل مكافحتها أو على الأقل الحد من انتشارها، ولاشك أن انظمتنا المعلوماتية تعاني منها

---

٣. د. عبد الفتاح بيومي حجازي الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنيت. دار الكتب القانونية – ٢٠٠٢ ص٤٩ هامش ١.

٤. أنظر يونس عرب – المرجع السابق – الموقع نفسه

٥. عالج المشرع العماني هذا الموضوع بالمرسوم السلطاني ٢٠٠١/٧٢ الذي أضاف إلى قانون الجزاء الفصل الثاني مكرر لاحظ نص التعديل مقال عبد اللطيف بن عبد الرحمن الهريش – بعيداً عن الاكتفاء بالمعالجة التقليدية: جرائم الحاسب الآلي بحاجة للتنظيم والنصوص القانونية لا تزال قاصرة عن تغطيتها – منشور في مجلة الرياض الأربعاء ١٦ نيسان (أبريل) ٢٠٠٣ الموافق ١٤ صفر ١٤٢٤ هجري العدد ١٢٧١٧ السنة ٣٨ لاحظ موقعها على الانترنيت http://www.alriyadh-np.com

ولاسيما أن أغلبها بدأت تعتمد في تعاملاتها على تلك الأنظمة بشكل يكاد يكون كلياً ولا سبيل رادع لذلك وتفادي أخطارها أمام غياب مثل ذاك التشريع.

النصوص الجنائية

تنص المادة ٢/٤٦٢ من القانون رقم ٨٨-١٩ لسنة ١٩٨٨[٦] الفرنسي التي تقابل المادة ١/٣٢٣ من قانون العقوبات الفرنسي الحالي[٧] على أنه ((كل من دخل بطريق الغش أو مكث في داخل نظام المعالجة الآلية للمعطيات أو في جزء منه يعاقب بالحبس لمدة تتراوح بين شهرين وسنة واحدة وبالغرامة التي تتراوح ما بين ألفين إلى خمسين ألف فرنك أو بإحدى هاتين العقوبتين، فإذا نجم عن هذا الدخول سواء محو أو تعديل في المعطيات المختزنة في النظام أو إتلاف تشغيل هذا النظام تكون العقوبة الحبس لمدة تتراوح ما بين شهرين إلى سنتين والغرامة التي تتراوح ما بين عشرة آلاف إلى مائة ألف فرنك))، ولا يختلف النص الجديد في قانون العقوبات عن نص المادة ٢/٤٦٢ إلا بشأن تعديل العقوبة وإن اختلف قليلا من حيث الصياغة، حيث شدد المشرع العقوبة، وجعلها سنة حبس وغرامة مائة ألف فرنك في حالة الدخول بطريق الغش، وإذا نتج عن الدخول محو أو تعديل في المعلومات الموجودة بالنظام تكون العقوبة الحبس سنتين وغرامة تصل إلى مائتين ألف فرنك حتى يتمكن المشرع من مواجهة ظاهرة الإجرام المعلوماتي[٨]. وسنتناول جريمة الدخول عن طريق الغش بسبب كونها تختلف عن جريمة المكوث أو البقاء بالنظام

---

٦. أدخل المشرع الفرنسي هذه الجريمة أول مرة إلى قانون العقوبات بالقانون رقم ٨٨-١٩- لسنة ١٩٨٨ بشأن الغش المعلوماتي الصادر في الخامس من يناير / كانون الثاني من عام ١٩٨٨ وقد بدأت أول محاولة لاصداره عام ١٩٨٥ حين تقدم وزير العدل بمشروع قانون عقوبات جديد، ولم ترى هذه المحاولة النور حتى العام المذكور.

٧. بدء العمل بقانون العقوبات الفرنسي الجديد في الأول من شهر مارس – آذار – من عام ١٩٩٤ وقد تضمن نصوص المواد التي جاء بها القانون رقم ٨٨-١٩- لسنة ١٩٨٨ بشأن جرائم الغش المعلوماتي وأعاد ترتيبها وأجرى عليها بعض التغييرات.

٨. د. أحمد حسام طه تمام – الجرائم الناشئة عن استخدام الحاسب الآلي – دراسة مقارنة – رسالة دكتوراه – دار النهضة العربية – ٢٠٠٠ ص٢٦٢.

الآلي من حيث الطبيعة ومن حيث النشاط المادي المكون لكل منهما إلى جانب ما يفرضه علينا طبيعة هذه المواضيع التي تتطلب علاج جميع تفاصيلها وما يتعلق بها كونها من الجرائم الحديثة التي فرضها التطور التكنلوجي.

وشأن جريمة الدخول إلى النظام عن طريق الغش شأن الجرائم الأخرى تقوم على ركنين: ركن مادي وركن معنوي حيث تقوم الجريمة على الرأي الغالب في الفقه[٩] على ذلك. وقد يتطلب المشرع إلى جانب ركني الجريمة صفة أو حالة واقعية أو قانونية يحميها القانون ويفترض وجودها وقت وقوع الجريمة ويطلق عليه العنصر المفترض[١٠].

ويعد النظام الآلي ذلك العنصر في الجريمة موضوع البحث.

وقد وجدنا أن السبيل إلى التعرف على جميع دقائق هذه الجريمة يكون من خلال خطة منهجية تعتمد على الأسلوب التحليلي المدعم بالاستنتاج المنطقي المستند للأصول القانونية نستعرض فيها مدلول النظام الآلي باعتباره العنصر المفترض للجريمة والركن المادي والركن المعنوي، وأثر الضرر الذي يتحقق من جراء الدخول على أن يكون كل أمر في فصلٍ مستقلٍ.

---

٩. هناك من الفقهاء من يذهب إلى إضافة ركن آخر للجريمة يصطلح عليه بالركن الشرعي أو بالركن القانوني – لاحظ د. علي حسين الخلف، وسلطان الشاوي – شرح الأحكام العامة في قانون العقوبات – مطابع الرسالة – الكويت – ١٩٨٢ ص١٣٩، د. محمود نجيب حسني – شرح قانون العقوبات اللبناني – القسم العام – دار النهضة العربية – بيروت – ١٩٨٤ ص٧٣ وما بعدها ولاحظ في الاعتراضات التي يثبتها ونحن نؤيده في ذلك د. عوض محمد– الوجيز في قانون العقوبات – القسم العام – الجزء الأول – دار المطبوعات الجامعية – ١٩٧٨ ص٥١.

١٠. وهو العنصر الذي يفترض قيامه وقت مباشرة الفاعل نشاطه كصفة الموظف في جريمة الرشوة – د. محمود نجيب حسني – المرجع السابق – ص٥٧ ويعد العنصر المفترض من الأركان الخاصة في بعض الجرائم د. فخري عبد الرزاق الحديثي – قانون العقوبات – القسم العام – مطبعة الزمان – بغداد ١٩٩٢ ص١٨.

الفصل الأول

المقصود بالنظام الآلي لمعالجة المعطيات ومدى اشتراط حمايته بوسائل فنية

ينبغي الإشارة إلى ان الحاسب الآلي[١١] هو المقصود من عبارة النظام الآلي لمعالجة المعطيات[١٢] لأنه العنصر الأساسي للنظام باعتباره الجزء الذي لا غنى عنه في بناء أي نظام معلوماتي حديث لما له من قدرة، حيث فتح الآفاق بعد الاندماج الذي حصل بين نظامي الاتصال والحوسبة[١٣].

المبحث الأول

مدلول النظام الآلي لمعالجة المعطيات

لم يُحدد المشرع المقصود بالنظام الآلي لمعالجة المعطيات على الرغم من أن مجلس الشيوخ الفرنسي كان قد أدرج مدلوله ضمن التعديلات التي اقترحها على مشروع القانون. وقد آثرنا استعراض مدلوله دفعتنا لذلك ضرورات البحث على الرغم من طابعه الفني على أن نستعرض وفي مطلبين موقف مجلس الشيوخ والفقه من ذلك.

---

١١. أصل تسمية الجهاز الآلي لمعالجة المعلومات هو كلمة كومبيوتر COMPUTER والمشتقة من الفعل COMPUT، الذي تعني باللغة العربية يحسب، وقد عربها مجمع اللغة العربية الأردني بالحاسوب د. عوض منصور محمد أبو النور – مقدمة في علم الحاسب الإلكتروني– وبرمجة بيسك– دار الأمل– أربد– الأردن– ط/ الخامسة ١٩٩٦ ص٢٨ وهي ليست التسمية الوحيدة التي استعملها الفقه لاحظ التسميات المختلفة والأسباب التي تكمن وراء هذا الاختلاف د. محمد حماد مرهج – الهيتي– التكنلوجيا الحديثة والقانون الجنائي– دار الثقافة للطباعة والنشر– الأردن عمان– ٢٠٠٤ ص١٤٣ وما بعدها.

١٢. د. عمر الفاروق الحسيني– المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية– ط/الثانية– ١٩٩٥ ص٥.

١٣. تقوم الحوسبة على أساس استخدام وسائل التقنية لإدارة ومعالجة البيانات وتنفيذ مهام تتعلق بعلمي الحاسب والمنطق– يونس عرب– المرجع السابق فقرة رقم ١ ص١.

المطلب الأول

مدلول النظام الآلي لمعالجة المعطيات في نظر مجلس الشيوخ الفرنسي

حدد مجلس الشيوخ الفرنسي في مشروع قانون غش المعلومات مفهوم النظام الآلي لمعالجة المعطيات بكل مركب يتكون من وحدة أو مجموعة وحدات معالجة. والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الادخال والإخراج وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات التي عن طريقها يمكن تحقيق نتيجة معينة هي معالجة المعطيات أو التي تتظافر فيما بينها نحو تحقيق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضع لنظام الحماية التقنية[١٤]. غير أن إسقاط مدلول النظام الآلي لمعالجة المعلومات من القانون وإن كان قد أفقده عنصر الإلزام الذي للنصوص القانونية إلا أنه لم يفقده كل قيمته القانونية؛ إذ له قيمة قانونية لما للأعمال التحضيرية والمناقشات التي تصاحب وضع القوانين من قيمة مما يمكن الاسترشاد به في إطار بيان مدلول عبارات النص عندما لا تكون واضحة المدلول طبقاً لما تقضي به قواعد التفسير التي غايتها الكشف عن قصد المشرع.

ونشير بصدد الشروط التي وضعها مجلس الشيوخ للنظام التي تحدد جانباً منها عبارة المجلس بأنه عبارة عن (مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط) إلى أن النظام يتكون من عنصرين: الأول عنصر مادي يتكون من وحدة أو مجموعة من وحدات المعالجة، والعنصر الثاني من طبيعة غير مادية أو معنوي يتكون من البرامج والمعطيات تتظافر أو تتآلف فيما بينها من أجل تحقيق غاية محددة هي معالجة المعطيات، أي لابد أن يكون هناك ترابط أو صلة بين

---

١٤. د. علي عبد القادر القهوجي – الحماية الجنائية لبرامج الحاسب الآلي – الدار الجامعية للطباعة والنشر – الاسكندرية – ١٩٩٩ ص١٢٠.

وحدات النظام توحدها أو تحاول توحيد جهدودها نحو تحقيق الهدف المقصود. فالوحدة التي لا تتوفر فيها تلك الصفات فلم تكن مرتبطة بغيرها ولم يكن لها دور في تحقيق المقصود وهو معالجة المعطيات تخرج من نطاق مدلول النظام الآلي وبالتالي تخرج من نطاق الحماية. ولهذا التحديد أهمية سنكشف عنها عند بياننا للنتائج التي تترتب على تبني هذا التعريف.

المطلب الثاني

مدلول النظام الآلي لمعالجة المعطيات في نظر الفقه

يرى جانب من الفقه بأن النظام الآلي لمعالجة المعطيات هو كل وحدة أو مجموعة من الوحدات القادرة على معالجة أو تخزين البرامج والمعلومات أو أجراء الدخول أو الخروج أو الاتباط والتي تهدف الى نتيجة محددة في هذه المجموعة وتكون موضوعاً للحماية بنظام الأمن[١٥].

وهذا التعريف لايختلف فيما يتعلق بشرط الحماية الأمنية: الفنية أو التقنية عن سابقة ولا غرابة في ذلك لأنه يعكس وجهة نظر تيار آخر في مجلس الشيوخ. غير أنه إلى جانب كونه لم يحدد النتيجة التي ينبغي أن يسعى النظام إلى تحقيقها اشتراط في وحدات النظام التي يتكون منها أن تكون قادرة أما على معالجة أو على تخزين البرامج والمعلومات فقد دون أن يتطلب الارتباط بينها. مما يفيد أنه أي وحدة يمكن استخدامها لخزن البرامج والمعلومات أو لمعالجتها تعد جزء من النظام الآلي لمعالجة المعطيات، فالأقراص الممغنطة و أجهزة الحاسب غير المستخدمة تعد من مكونات النظام الآلي. لأنها – وطبقا للتعريف – وحدات قادرة على تخزين البرامج والمعلومات بالنسبة للأقراص ووحدات قادرة على معالجة وتخزين البرامج والمعلومات

---

١٥. قال بهذا التعريف العضو Thyraud أمام مجلس الشيوخ في جلسة مناقشة مشروع القانون لاحظ في عرض هذا الاتجاه وتقييمه أيضا د.أحمد حسام طه تمام – المرجع السابق – ص٢٨٣.

بالنسبة لأجهزة الحاسب. في حين أنها تخرج من عداد ذلك طبقاً للتعريف الذي قدمه مجلس الشيوخ الذي اشترط الاتباط بين تلك الأجزاء فكان اكثر وضوحاً وتحديداً، بشأن اشتراط ان تكون الأجزاء التي يتكون منها النظام قادرة على الاتصال فيما بينها من أجل الغاية التي وجدت من أجلها الأمر الذي لم يدر بخلد الفقه والذي تتضح نتائجه فيما بعد.

ويصف البعض[١٦] هذا التعريف بالسعة ونحن نؤيده في هذا الوصف ونختلف معه فيما اعتبره توسعة في مدلوله حيث يرى أن هذا المدلول واسع لأنه يشمل شبكة المعلومات العالمية وبطاقات الائتمان الممغنطة.

والحق أن سعة هذا المدلول لم تكن بضمه شبكة المعلومات العالمية التي هي عبارة عن مجموعة من الأجهزة والأدوات المختلفة التي تساعد على تخزين المعلومات في صيغة يمكن استعادتها[١٧]، ومن ثم تبادلها. إنما السعة التي نقول بها بالنسبة جاءت من الصفات التي اشترطها أصحاب هذا التعريف في وحدات النظام والتي تشمل كل وحدة يمكنها أن تقوم بإحدى عمليتين: المعالجة أو الخزن، وهذا من شأنه أن يمد الحماية إلى أي جهاز طالما أنه له القدرة على المعالجة أو القدرة على الخزن الأمر الذي يعد من صميم عمل شبكة المعلومات العالمية (الانترنيت). أما بالنسبة لبطاقات الائتمان فإنها أيضاً لا تخرج عن مدلول النظام الذي يقول به الفقه عند تطبيقه عليها مما لا يجعله تعريفاً واسعاً في هذا المجال لأنها، أي بطاقات الائتمان، تعد من وحدات الارتباط أو الاتصال أو من وحدات الإدخال إذا أخذنا بنظر الاعتبار الدور الذي تقوم به.

غير أن صاحب هذا الاتجاه إذا كان قد اعتمد على كون شبكة المعلومات وبطاقات الائتمان الممغنطة لها القدرة على معالجة وخزن المعطيات مما يعد توسعاً

---

١٦. من هذا الرأي د. أحمد حسام طه تمام – المرجع السابق ص٢٨٣.

١٧. كرستان كروملش، روبرت كورت وآخرين– الانترنيت بدون خبرة– إعداد د. خالد العامري– قسم الترجمة بدار الفاروق– مصر– القاهرة ط/الثانية ٢٠٠٠ ص٢٠.

في رأيه فإن هذا لا ينطبق وبشكل خاص على بطاقات الائتمان[١٨]؛ إذ أنها ليس لها القدرة على معالجة المعلومات ولا حتى خزنها بالشكل الذي هي عليه وحدات الخزن الداخلية أو الخارجية التي يتكون منها النظام الآلي كالأقراص الصلبة أو المرنة[١٩] وإذا كان يستند على قدرة البطاقة في خزن المعلومات التي تزود بها الأشرطة الممغنطة التي تثبت في جسمها المادي في القول بقدرتها على الخزن. فإن هذا غير مقبول لأن هذا الكيان هو الذي ترتبط به البطاقات الممغنطة بالحاسب الآلي فهو حلقة الوصل التي تسمح لحامل البطاقة بالاتصال بالحاسب الآلي للجهة المصدرة للبطاقة، ويتكون من معلومات وبيانات يتم تثبيتها أو بالأحرى يتم دمجها في الأشرطة الممغنطة بطريقة إلكترونية، ولا يتم قراءتها إلا من قبل الحاسب الآلي أو من جهاز يرتبط به يسمى قارئ البطاقات الأمر الذي يجعلها من وحدات الاتصال أكثر من كونها وحدة من وحدات خزن المعلومات، بل أن هذه البيانات والمعلومات هي التي تمكن البطاقة بالاتصال بالنظام الآلي، أي هي الجزء الذي يجعل البطاقة قادرة على أداء وظائفها.

وما نؤيد به وصفها هذا هو أن الوفاء عن طريقها إذا تم آلياً، أي وفق الطريقة الإلكترونية، فعن طريقها أو من خلالها يرتبط التاجر مع المصرف الذي أصدر

---

١٨. بطاقات الوفاء الإلكترونية هي بطاقات بلاستيكية أو من الورق الصلب تصدر بواسطة مؤسسة مالية بإسم أحد الأشخاص وتقوم بوظيفتي الوفاء والائتمان د. فايز نعيم رضوان بطاقات الوفاء- مكتبة الجلاء الجديدة- المنصورة- ١٩٩٠ ص٧١، ولاحظ في بطاقات الإئتمان على وجه الخصوص التعاريف المختلفة لها فداء يحيى أحمد الحمود- النظام القانوني لبطاقة الائتمان- دار الثقافة للطباعة والنشر- الأردن- عمان-١٩٩٩ ص١٤ وما بعدها ولاحظ في أنواعها والجرائم التي ترتكب عن طريقها القانون الجنائي والتكنلوجيا الحديثة- الجرائم الناشئة عن استخدام الحاسب الآلي- دار النهضة العربية القاهرة ١٩٩٢ ص٣٤ وما بعدها.

١٩. ولا يمكن اعتبار بطاقات الوفاء من وحدات الخزن لأن المعلومات التي تتضمنها الأشرطة الممغنطة معلومات بسيطة وخاصة تتعلق ببيانات تخص حامل البطاقة والجهة التي أصدرتها إلى جانب، وهو الأهم، لا يمكن معاملتها كالمعلومات الموجودة على الأقراص من حيث نسخها أو التعديل بها، بل أن التغيير فيها غير ممكن إلا من قبل الجهة المصدرة للبطاقة.

البطاقة بواسطة جهاز معد خصيصاً لهذه الغاية يسمى بجهاز التحويل عند نقط البيع Point of sale transaction terminal، ومهمة هذا الجهاز التأكد من صحة البطاقة المقدمة من العميل إلى التاجر، حيث يتبادل هذا الجهاز المعلومات والبيانات المشفرة إلكترونياً على البطاقة مع البيانات والمعلومات المخزنة على جهاز الحاسب الآلي لدى المصرف[٢٠]، ولذلك فهي إن لم تكن من وحدات الاتصال فهي تعد من وسائل الدخول أو الارتباط وليست من وحدات المعالجة والخزن الأمر الذي ينفي عن التعريف السعة بهذا الاتجاه لأنه اعتبر وحدات الإدخال من ضمن وحدات النظام وهي منها كما انتهينا.

خلاصة الأمر إن من حسنات التعريفين أنهما جعلا وحدات الاتصال بالنظام الآلي من ضمن الوحدات التي يتكون منها، ويتأكد ذلك من خلال شمولهما لبطاقات الوفاء الممغنطة لأنه لولا ذلك لما كان بالإمكان شمول تلك البطاقات بالحماية بحيث من يستعملها بصورة غير مشروعة يعد مرتكباً لجريمة الدخول إلى النظام الآلي عن طريق الغش إلى جانب مسئوليته عن جرائم أخرى حيث يتوقف ذلك على نوع البطاقة والطريقة التي استخدمها للوفاء بمشترياته وطريقة الحصول عليها. وهذا من شأنه أن يجعل التعريف يساير التقدم الذي يصيب تقنية المعلومات لأن اعتبار وحدات الاتصال بالنظام من ضمن مدلول النظام وقدرتها على الاتصال يُمّكنُ هذا التعريف من أن يكون حياً يستطيع أن يواكب التقدم في هذا المجال كما هو الأمر بالنسبة لشموله شبكات الهاتف الخلوي باعتبارها نظاماً وفقاً للمدلول الذي بيناه، وتجدر الإشارة هنا إلى ضرورة تحديد المقصود بالنظام بنص إن شاء لمشرعنا أن يجرم ذلك، حيث أننا مع الاتجاه الذي يرى بضرورة ذلك حفاظاً على قدسية مبدأ شرعية التجريم والعقاب.

المبحث الثاني

---

٢٠. عماد علي الخليل– الحماية الجزائية لبطاقات الوفاء– دار وائل للنشر– الأردن عمان – ط الأولى– ٢٠٠٠ ص١١.

النتائج التي تترتب على الأخذ بالتعريف الذي قدمه مجلس الشيوخ

إن أي وحدة حتى تدخل في مكونات النظام طبقاً لمفهوم مجلس الشيوخ ينبغي أن يتم التحقق من أمرين: ارتباطها بالنظام أو قدرتها على ذلك وأن يكون لها دور في تحقيق الغاية الأساسية وهي معالجة المعلومات بحيث أن الوحدة غير المتصلة بالنظام ولا يكون لها القدرة على تعضيد الوحدات الأخرى في إطار الغاية الأساسية وهي معالجة المعلومات لا يمكن أن تكون من مكونات النظام خلاف الأمر بالنسبة لموقف الفقه من مدلول النظام ولهذا آثار يمكن بيانها من خلال الإجابة على الأسئلة الآتية:- مدى اشتراط ارتباط الوحدة أو الوحدات بالنظام؟ ومدى اشتراط تشغيلها؟ ومدى شموله لأجزاء الارتباط والدخول والخروج؟ لتحقق جريمة الدخول.

وفي صدد الإجابة على التساؤل الأول يمكن القول بأن الأخذ بتعريف الفقه للنظام الآلي يجعل الدخول أو الاتصال بأي وحدة من وحدات الخزن أو المعالجة محققاً للجريمة سواء كانت تلك الوحدة متصلة أو مرتبطة أو غير مرتبطة قادرة أن تساند أو تتظافر مع غيرها على تحقيق مهمتها أو غير قادرة على ذلك؛ إذ يكفي لتحقق جريمة الدخول في ضوء مدلول الفقه للنظام أن تكون الوحدة التي تم الاتصال بها من وحدات الخزن أو المعالجة. بمعنى آخر أن جريمة الدخول تتحقق بمجرد الاتصال بأي وحدة من تلك الوحدات سواء كانت من الوحدات القادرة على خزن المعلومات أو القادرة على معالجتها وبغض النظر عن ارتباطها أو عن قدرتها لأن تحقق ذلك، أي تدخل الوحدة في مدلول النظام حتى ولو لم تكن متصلة به أو لم تكن قابلة للارتباط أو للإتصال.

أما الأخذ بتعريف مجلس الشيوخ فمن شأنه أن يؤدي إلى أن الدخول لا يتحقق في أي من هذه الوحدات مالم تكن متصلة بالنظام أو على الأقل أن ترتبط فيما بينها بعلاقات تمكنها من إنجاز مهمتها في معالجة المعطيات أو أن تتظافر في سبيل ذلك بمعنى أن يكون لها دور مباشر في معالجة المعلومات أو تكون لها القدرة مع غيرها على ذلك بحيث تكون مقام الوحدة المساندة لعمل الوحدات الأخرى أو لوحدة

منها، أي تعتبر الوحدة من مكونات النظام ويعد الدخول إليها أو اختراقها محققاً للجريمة حتى ولو أنها تقوم بدور غير مباشر.

أما بالنسبة لمدى اشتراط تشغيل الوحدة فإن النتيجة المنطقية التي تترتب على الأخذ بمفهوم النظام ذاته، أي بالدخول يقول به الفقه وأستناداً إلى النتائج التي توصلنا إليها بالفقرة السابقة فإن الوحدة التي يتحقق الدخول إليها لا ينبغي أن تكون من الوحدات التي قد تم تشغيلها أو حتى التي تم تهيئتها، بحيث تكون قابلة للاشتعال ضمن وحدات النظام. لأن جل ما يشترط في مكونات النظام أن تكون الوحدة من الوحدات القادرة على خزن أو معالجة المعطيات دون أن يشترط فيها أن تكون على علاقة ببقية الوحدات الأمر الذي يشترطه مجلس الشيوخ والذي لا يجعلها كذلك إلا من خلال تشغيلها أو على الأقل قدرتها على الاشتغال حتى تكون قادرة على تحقيق نتيجة معينة هي معالجة المعطيات أو أن تتظافر نحو تحقيق تلك النتيجة فيما بينها أو بينها وبين وحدة من وحدات النظام وليس بتهيئتها. وبمعنى أخص أن مفهموم الفقه للنظام لا يشترط في الوحدة حتى تكون من ضمن مدلول النظام إلا أن تكون من وحدات الخزن حتى ولو لم يتم تشغيلها بل يكفي تهيئتها لذلك وهذا وجه التوسع الذي ينسب للتعريف الذي يأخذ به الفقه الأمر الذي لايمكن التوصل إليه لو تم الأخذ بمفهوم مجلس الشيوخ الذي يشترط في الوحدة لكي تعد من مكونات النظام أن تكون في حالة تشغيل أو اشتغال باعتباره السبيل إلى إتصالها مما يترتب عليه أن الدخول لا يمكن أن يتحقق إلا في حالة أن تكون هذه الوحدات مرتبطة ولا تكون كذلك إلا عند تشغيلها أو أن تكون قادرة على ذلك، أي عند تهيئتها للاتصال بوحدات النظام الأخرى. وعلى أساس ذلك بتحقيق الدخول حتى في الوحدات التي قد تم إيقافها عن العمل بصورة غير نهائية لعطل أصابها يمكن إصلاحه أو تم توقيفها كالاعتداء الذي يقع خارج ساعات التشغيل والذي يعالجه البعض تحت جريمة سرقة ساعات العمل[٢١]. المهم ان تكون الوحدة التي تم

---

٢١. د.هدى حامد قشقوش جرائم الحاسب الآلي في التشريع المقارن دار النهضة العربية – القاهرة – ١٩٩٢ – ص١٠٢ ويرى البعض أن سرقة ساعات العمل تقع مع عامل أو موظف

الاتصال بها أو التي تحقق الدخول اليها لا ينبغي أن تكون قد فقدت قدرتها على العمل والاتصال بالنظام بصورة نهائية. مما يترتب عليه أن النشاط المادي المكون لجريمة الدخول لا يمكن أن يتحقق إذا تم الاتصال بوحدة قد تم استعمالها نهائياً من النظام كالوحدة التي يتم إخراجها من الخدمة بسبب أو تقني كأن تكون من الأجيال القديمة. على خلاف مايؤدي اليه الأخذ بتعريف الفقه. حيث يتحقق الدخول المجرم حتى بالاتصال بحاسب آلي لم يدخل الخدمة ولم يتم تشغيله بعد لمجرد أنه من الوحدات القادرة على معالجة المعلومات.

أي أن الأخذ بمدلول النظام الذي طرحه مجلس الشيوخ من شأنه أن يؤدي إلى عدم تحقيق جريمة الدخول إن تم الاتصال بوحدة لاتشكل جزء من هذا النظام سواء كانت خارجة عنه سبب خروجها من الخدمة أو ما زالت في مرحلة التجربة وعلى العكس تقع الجريمة حتى لو كان الدخول قد وقع على أحد وحدات النظام وهي في حالة عطل أو توقف طالما أنها تعد جزءً من النظام، بل حتى لو وقع النشاط على النظام وهو في حالة إيقاف كان يقع الاعتداء خارج ساعات تشغيله الاعتيادية[٢٢] طالما أن الوحدة التي وقع عليها النشاط متصلة بالنظام أو مرتبطة به.

إذن نخلص من ذلك إلى أهمية شرط الاتصال بين الوحدات أو تظافرها على إنجاز مهمتها الذي جاء به تعريف مجلس الشيوخ الذي أن يحقق الحماية الجنائية المطلوبة والحقيقية للنظام، وعدم إضفاء الحماية على مكونات مادية كونها تنتسب إلى مكونات التي يتكون منها النظام، والتي من الممكن أن تكون لها علاقة مستقبلية بالنظام. وبمعنى أدق أن الأخذ بالمفهوم الذي يقول به الفقه من شأنه أن يمد الحماية حتى إلى أجهزة الحاسب الآلي والأقراص التي يتم عرضها للبيع، والتي يتم تشغيلها أو ربطها بالنظام لمجرد أنها قادرة على معالجة المعلومات وقادرة على خزنها، وهذه

يتصل بحكم عمله بهذه الآلة، ومن ثم فمن غير الممكن أن يجد نفسه في اتصال مع هذا النظام الذي يفترض بأنه يعرف الكثير عن الكثير. د.عمر الفاروق الحسيني – المرجع السابق – ص١٢٨.

٢٢. د.جميل عبد الباقي الصغير – المرجع السابق ص١٢١.

توسعة لا مبرر لها. أما اعتماد المدلول الذي يقول به مجلس الشيوخ فمن شأنه ان لاتكون مثل هذه الحالة داخل إطار تجريم المشرع إذا تم الدخول إليها. وبمعنى أخص لا يشترط أن تكون الوحدة في حالة تشغيل إنما يكفي أن تكون في حالة اشتغال. ولا يكفي أن تكون مهيئة لذلك وقادرة عليه فلا ينبغي أن تمتد الحماية استناداً إلى ذلك لوحدة غير قادرة على الاتصال بالنظام وإن كان قد تمت تهيئتها كتهيئة جهاز جديد وتزويده ببرامج التشغيل بحيث أصبحت بإمكانها القيام بمهامها قالاتصال بهذه الواحدات أن يحقق الوصف المطلوب.

إن هذه الحسنات التي تثبت للتعريف الذي يقول به مجلس الشيوخ من شأنها أن ترجع مدلوله على المدلول الذي يقول به الفقه ناهيك عما يمكن أن يؤدي إليه تبنيه من قدرته على مواكبة التطورات في مجال تقنية المعلومات كشموله للإختراق الذي تتعرض له شبكة الهاتف الخلوي بحيث أصبح هناك هكرز للخلوي كما هناك هكرز للانترنيت[٢٣].

---

٢٣. أنظر يونس عرب – الخصوصية وأمن المعلومات في الأعمال اللاسلكية بواسطة الهاتف الخلوي – ورقة عمل مقدمة إلى منتدى العمل الالكتروني بواسطة الهاتف الخلوي الذي عقدت برعاية اتحاد المصارف العربية من ٢٠ – ٢٢ أيار ٢٠٠١ في الأردن عمان – فندق المرديان – ص١٦ لاحظ الموقع على الانترنيت

http://www.arablaw.com

والهكرز هم قراصنة برامج النظام الآلي الهواة الفضوليين الذين يجعلون من أنظمة الحاسب الآلي، ومن الاعتداء عليها بمثابة التسلية، ولا يشكلون خطورة على الأنظمة المعلوماتية باستثناء ما يمكن أن تؤدي إليه أفعالهم من إتلاف في الأنظمة بسبب العبث وتكمن الخطورة في القراصنة المخادعين (Crackers) لأنهم يؤلفون نوادي لتبادل المعلومات فيما بينهم ويقسمون على أساس جرائمهم إلى:- المخادعون Frudeurs والجواسيس، وهؤلاء مهمتهم استخبارية تقتصر على جمع المعلومات ومن مقتضيات عملهم الا يتركو أي دليل عن عملهم، لذلك فهم أشخاص من أصحاب الكفاءات، ويتمتعون بقدرة عالية على التعامل مع الحاسب الآلي، إلى جانب قدرتهم على طمس الأدلة التي تتختلف عن جرائمهم وللمزيد عن خصائصهم لاحظ د.عبد الفتاح بيومي حجازي – المرجع السابق – ص٣٣.

والذي يمكن أن ينتظم تحت مدلول النظام باعتباره شبكة من شبكات المعلوماتية لا سيما بعد تعدد استخداماته وتعديها إلى إمكان إجراء مختلف العمليات الإلكترونية وبضمنها العمليات المصرفية عن طريق مايعرف بالتجارة الإلكترونية بسبب قدرته على الاتصال بشبكة المعلومات العالمية (الانترنيت) واستقبال وإرسال الأوامر فهو إن لم يكن نظاماً، ونحن لا نشك به، فهو من أجوات الدخول ومن قبل م أدوات الاتصال حيث يمكن استخدامه لهذا الغرض.

المبحث الثالث

مدى لزوم حماية النظام الآلي بوسائل فنية

أو تقنية لتحقق جريمة الدخول عن طريق الغش

لا يدخر مستخدموا النظام الآلي ومنتجوا البرامج وسعاً في الحفاظ على مكوناتهم من برامج ومعلومات من القرصنة أو النسخ غير المشروع أو من التصرفات غير المشروعة الأخرى، وذلك باتباع وسائل فنية أو تقنية متعددة تمنع اختراق هذه الأنظمة أو الإطلاع عليها أو التلاعب بها أو تغييرها[٢٤]. أما لما تمثله من قيمة أو لما تمثله من خصوصية، بل حتى صناديق البريد الإلكتروني التي ينشؤها أي منا على شبكة المعلومات لا يمكن الدخول إليها إلا من خلال معرفة مفاتيح الحماية الأمنية الرقم السري أو مايسمى بكلمة المرور (Pass Word) أو أي وسائل أخرى.

ولكن قد لا يلجأ الكثيرون ممن يستخدم تلك الأنظمة إلى تلك الوسائل، وقد توجد مواقع على شبكة المعلومات تقدم خدماتها بشكل مجاني بحيث يمكن لجميع

---

٢٤. كالتشفير أو التحقق من الشخصية باستخدام التوقيع الإلكتروني لاحظ في مدى فاعلية هذه الوسائل في حماية البرامج د. محمد حماد مرهج– مبررات الحماية الجنائية لبرامج الحاسب الآلي– مجلة العلوم الإنسانية والاقتصادية– جامعة الأنبار– العدد السادس نيسان/٢٠٠٥ ص٥٣٥ وما بعدها.

الأفراد الاستفادة من خدماتها من غير حاجة إلى إدخال الرقم السري وهو رقم السماح أو الإذن بالدخول، فهل يعد الدخول إلى هذه المواقع دخولاً غير مشروع أم ينبغي لتحقق جريمة الدخول عن طريق الغش أن يكون النظام محمي بوسائل فنية بحيث لا يعد الدخول إلى هذه الانظمة تم بطريق الغش؟

إن الإجابة على ذلك ستكون في مطلبين الأول نبين فيه موقف الفقه الفرنسي والثاني نبين فيه موقفنا من ذلك.

المطلب الأول

موقف الفقه الفرنسي من مسألة حماية النظام الآلي بوسائل أمن فنية أو تقنية

إن خلافاً في الفقه الفرنسي[٢٥] ظهر بشأن ضرورة أو عدم ضرورة أن يكون النظام مؤمناً بوسائل حماية فنية أو تقنية. ويرى الاتجاه الغالب في الفقه بضرورة أن يكون النظام محمي بمثل تلك الوسائل باعتبار ذلك عنصراً مفترضاً ينبغي تحققه إلى جانب ركني جريمة الدخول بطريق الغش المادي والمعنوي. فجريمة الدخول على رأي في الفقه تقتضي أن يكون الجهاز قد تمت حمايته بنظام أمني فيكون الاتصال بالنظام الذي تتوافر فيه تلك الوسائل دخولاً تم عن طريق الغش، وهذا يعني من وجهة نظر أخرى أن الدخول بنظام آلي غير محمي بتلك الوسائل لا يحقق الدخول بطريق الغش حتى ولو كان دخوله رغماً عن إرادة من له الحق في السيطرة على النظام. ومبررات هذا الاتجاه هي: أن وجود نظام حماية التزام قانوني مفروض بنص القانون على كل من يقوم بإدارة نظام معلوماتي، حيث يلزم المشرع كل شخص أو منشئ أوامر يعمل بالمعالجة الآلية للمعلومات الشخصية ضرورة إتخاذ الاحتياطات اللازمة لحفظ وحماية هذه المعلومات وخاصة بمنع تشويهها أو تعديلها أو الحصول

---

٢٥. أنظر في عرض هذا الخلاف د. أحمد حسام طه تمام- المرجع السابق- ص٢٦٤ وما بعدها.

عليها بواسطة أشخاص غير مرخص لهم الاطلاع عليها[٢٦] بل إن الاخلال بالألتزام المفروض على كل من يدير نظاماً آلياً من شأنه أن يعرضه للعقاب المنصوص عليه بالمادة ٤٢ من قانون العقوبات والتي تصل فيها العقوبة إلى الحبس لمدة خمس سنوات. وهذا يعني أن يعاقب من يخل بهذا الالتزام بعقوبة أشد ممن يدخل إلى النظام الآلي. فمن يرتكب مجرد الامتناع عن وضع نظام أمني يعاقب بعقوبة أجسم ممن يباشر نشاطاً إيجابياً فيدخل إلى النظام الآلي أو بدون ترخيص لمجرد أن يكون الأخير غير محمي بوسائل فنية[٢٧]، وفي هذا مفارقة من شأنها أن تكشف عن ضرورة الحماية الفنية للأنظمة التي يعول عليها المشرع.

وإلى جانب ما تقدم فإن الحماية الفنية أمر تقتضيه العدالة والمنطق، حيث أن القانون الجنائي لا ينبغي أن يقوم بحماية الأشخاص الذين لا يأخذون الاحتياط اللازم المتطلب من الإنسان متوسط الذكاء. لأن القانون الجنائي لا يحمي إلا الأشخاص الذين لديهم الحرص على أموالهم ولا يحمي من ليس لديه هذا الحرص أو من يهمل منهم في توفير الحد الأدنى لحماية أمواله؛ إذ من الطبيعي أن من يقوم باستغلال نظام للمعالجة الآلية للمعطيات أن يوفر الوسائل الفنية لمنع الغش طالما أنه يستغل هذه التقنية ويحقق من ورائها أرباحاً إلى جانب أن يكون دور القانون الجنائي في حالة تطلب وجود حماية فنية دور وقائي؛ إذ سيدفع تطلب هذا الشرط

---

٢٦. منصوص عليه بالمادة ٢٩ من القانون الصادر في ٦ يناير/كانون الثاني عام ١٩٧٨ المتعلق بالحريات في مواجهة نظم المعلومات د. أحمد حسام طه تمام- المرجع السابق- ص٢٦٥ وما بعدها. ولمزيد عن هذا القانون وشرح ما جاء به من قواعد خاصة بحماية الحريات راجع د. عمر أحمد حسبو- حماية الحريات في مواجهة نظم المعلومات- دراسة مقارنة- دار النهضة العربية- القاهرة- ٢٠٠٠ ص١٠٢ وما بعدها.

٢٧. حيث يعاقب مستخدم الجهاز الآلي الذي لم يرتكب إلا سلوك سلبي بأن امتنع أن يحمي نظامه الآلي بوسائل فنية بعقوبة الحبس الذي يصل إلى خمس سنوات في حين يعاقب الشخص الداخل إلى النظام من دون ترخيص والذي يباشر نشاطاً إيجابياً بالحبس الذي لا يتجاوز الحبس لمدة سنة واحدة د. أحمد حسام طه تمام- المرجع السابق- ص٢٦٨.

مستغلي تلك الأنظمة إلى حمايتها بوسائل فنية[٢٨]. وأخيراً فإن نية العقاب على مجرد الدخول قول غير مقبول به إن لم يكن بطريق غير مشروع، ولا يكون الدخول بهذا الوصف إلا إذا كان عن طريق الغش، ولا يكون الأخير بهذا الوصف إلا إذا وجد نظام حماية باعتباره الطريقة الوحيدة للتمييز بين الدخول المشروع وغير المشروع[٢٩].

أما الاتجاه الثاني الذي لا يرى ضرورة في وجود نظام الحماية فيستند في تبرير مذهبه على أساس أن انتهاك نظام الحماية الفني للنظام الآلي أمر غير ضروري لعدم النص عليه في القانون فإذا كان المشرع قد رفض صراحة النص على هذا الشرط وفي ذات الوقت تطلب القصد الجنائي فإن الرأي الذي ينادي بضرورة وجود نظام أمني قد وسع من مدلول النص فالنظام الأمني لا يكون له إلا دور واحد وهو إثبات سوء نية من قام بانتهاك النظام والدخول فيه بطريقة غير مشروعة[٣٠]، ذلك الأمر الذي استلزمه المشرع في الركن المعنوي لهذه الجريمة. بل أن اشتراط أن يكون النظام الذي تم الدخول إليه محمي بأجهزة حماية فنية من شأنه أن يؤدي إلى قصر نطاق الحماية الجنائية التي جاء بها المشرع على الأنظمة المحمية فقط دون الأنظمة المفتوحة للجمهور مثل الدليل الإلكتروني أو الخدمات التي تقدم من خلال جهاز (Minitel)[٣١]، الذي هو دليل إلكتروني متصل بخط التلفون، وهو مستخدم في الشركات والبنوك، بل وحتى المنازل.

يبدو لنا أن هذا الرأي محل نظر وبالذات فيما يتعلق بفكرة الأنظمة المفتوحة للجمهور ومسألة الاستناد إليها والتذرع بها من أجل رفض فكرة الحماية الفنية لأن القول بأن الدخول إلى الأنظمة المفتوحة للجمهور يمكن أن يتم عن طريق الغش قول

---

٢٨. د. علي عبد القادر القهوجي– المرجع السابق– ص١٢٣.

٢٩. د. أحمد حسام طه تمام– المرجع السابق– ص٢٩٣.

٣٠. د. أحمد حسام طه تمام– المرجع السابق– ص٢٦٤–٢٦٦.

٣١. د. جميل عبد الباقي الصغير ص١٥١، وكان قد أشار في ذلك إلى
Chmaux (F), La loi sur la fraude informatique de nouvelle incriminations, J.CP.I. NO.6.

مرفوض لأنه يتعارض ومفهوم تلك الأنظمة فلا يمكن أن يتم الدخول إليها عن طريق الغش فكونها مفتوحة للجمهور يتعارض وفرض القيود على الدخول إليها، حيث يؤدي ذلك إلى نزع الصفة التي تتصف بها عنها. وعلى أساس ذلك يبدو لنا أن هناك عدم انسجام في الأفكار وبشكل دقيق فيما يخص مفهوم الأنظمة المفتوحة للجمهور وتحقق الدخول عن طريق الغش، فكيف يا ترى يتم التوفيق بين أن يكون الدخول إلى هذه المواقع قد تم عن طريق الغش على أساس إنعدام حق الشخص في الدخول وبالتالي أن يكون الاتصال بمثل هذه المواقع اتصال غير مشروع، وبين أن تكون هذه الانظمة مفتوحة للجمهور؛ إذ كونها تتصف بالصفة الأخيرة، من شأنه أن يؤدي إلى أن يكون الدخول أو الإتصال بها من أية جهة كانت ومهما كان لا يمكن أن يكون قد تم عن طريق الغش. فمن غير الممكن أن يأخذ الاتصال بها أو الدخول إليها صفة عدم المشروعية طالما أن لها هذه الصفة، وأقصد كونها مفتوحة للجمهور، الأمر الذي يجعل من الاتصال بمثل هذه المواقع اتصالاً مشروعاً في كل الظروف والأحوال. مما يترتب عليه عدم إمكان الاستناد إليها كحجة لدعم الاتجاه الذي يرى عدم ضرورة الحماية الفنية كون تلك الحماية تخرجها من نطاق الأنظمة التي تحميها نصوص هذه الجريمة لأنها تخرج من نطاق الأنظمة المفتوحة لتدخل في إطار الأنظمة التي يقيد فيها الدخول، أو التي يقيد فيها حق الأشخاص في الدخول. ففرض الحماية الفنية على الأنظمة المفتوحة للجمهور يفقدها صفتها تلك إلى جانب أن حق الدخول مكفول للجميع ولا يمكن تقييده مما يتعارض وما تقوم عليه فكرة جريمة الدخول بطريق الغش لأنه إذا كان الغش يفسر على أساس عدم وجود حق للشخص بالاتصال وليس وجود نظام حماية فإن كون الجميع لهم الحق بالاتصال بهذه الانظمة يجعل هذا الشرط لا وجود له ولا يمكن تحققه بحق من يدخل إلى هذه المواقع أياً كان وصفه أو كانت صفته. بل أن هذا الإتجاه في مذهبه هذا قد ألقى الحجة على نفسه فكيف يتطلب ألا تكون هناك حماية فنية للقول بتحقق جريمة الدخول عن طريق الغش والذي على أساسه استنتج أن تطلبها يؤدي إلى أخراجها من الحماية، والحق أنها تفقد طبيعتها تلك بكل قيد يفرض على حق الدخول إليها سواء بالحماية الفنية أو بتقييد حق الدخول إليها. بل أن جريمة الدخول لا يمكن أن

تتحقق حتى في فرض عدم وجود تلك الحماية لأن عدم تطلب الحماية ليس من شأنه أن يحقق الحماية لمثل هذه الانظمة لعدم إمكان اعتبار الدخول إليها دخولاً غير مشروع في كل الظروف والأحوال. بل ولا يمكن حمايتها حتى فيما لو ترتب على الدخول إليها ضرر في أنظمتها أو معلوماتها كالمحو والتعديل لأن جريمة الدخول حتى على وفق رأي الاتجاه الذي لا يتطلب وجود نظام حماية والتي تتحقق في حالة تحقق الاتصال بنظام ليس للشخص حق الاتصال به لا يمكن إعماله كون هذا الشرط غير متحقق فيها حتى يمكن إعمال الظروف المشددة التي تتطلب أصلاً أن يكون الدخول غير مشروع والأمر كذلك حتى في حالة أن يكون النظام محمي بوسائل فنية فإن هذا الشرط لا يمكن أن يتحقق في حالة كون النظام مفتوح للجمهور، لأن وضع مثل تلك الوسائل ينفي عن تلك الأنظمة صفتها ويغيير من طبيعتها بكونه نظاماً مخصصاً لاستخدام الجمهور، أو نظاماً عاماً، حيث تتعارض تلك القيود وطبيعته. مما لا ينبغي على ضوئه الحديث عن قصور الحماية عن هذه الأنظمة.

نستنتج مما تقدم هو ألا يكون مثل هذا السلوك تحت طائلة التجريم ومن ثم العقاب لأنه لا يمكن أن يأخذ الوصف المطلوب في الدخول وأقصد عدم المشروعية. وإذا يمكن أن يكون محلاً للعقاب فذلك يتحقق عندما يتجاوز السلوك عن صفة الدخول أو الاتصال إلى غاية أخرى كالتخريب والإتلاف، وهذا شأن آخر لا علاقة له بالجريمة موضوع البحث، بل أن المنطق يقضي بعدم محاسبته حتى عن المحو والتعديل إذا كان نتيجة للدخول استناداً إلى الصورة الجسيمة لهذه الجريمة لأن تطبيق الظروف المشددة أو إعمالها يتطلب أن يكون الدخول قد تم بصورة غير مشروعة الأمر الذي لا وجود له في الفرض الذي بين أيدينا، أي في الدخول إلى المواقع المخصصة للجمهور. مما يقتضي علاجه بنص مستقل.

المطلب الثاني

موقفنا من موضوع الحماية الأمنية التقنية أو الفنية للنظام الآلي لمعالجة المعطيات

إن الرأي الذي ننتهي إليه بعد هذا والذي يجنبنا هذا الجدل والنتائج غير العادلة التي تترتب عليه والذي نستند فيه إلى المنطق القانوني هو أن النظام الأمني الفني أو التقني إذا كان يعد أمراً ضرورياً في نطاق المشرع الفرنسي، حيث هناك إلزام قانوني فإنه مفروض فقط على من يدير نظاماً معلوماتياً وليس على كل من يستخدم ذلك. ةالفرق واضح بين الإدارة والاستخدام، وإذا جئنا إلى حقيقة النص موضوع البحث فإن كل الحجج التي قيلت مهما كانت وجاهتها فإنها تتحطم أمام صراحة النص فإن هذا النص لم يتضمن أي شرط يفيد ذلك، وليس من المنطق القانوني السليم أن يضاف شرط لم ينص عليه القانون وعدم النص من قبل المشروع على شرط الحماية الفنية يعني أن المشروع أراد استبعاده ولا يجوز لنا حينئذٍ أن نخالف إرادة المشروع الصريحة أمام تأويل لا يمكن أن نجني من ورائه إلا توسيع في نطاق التجريم بما يجاوز قصد المشرع حتى لوكان مجلس الشيوخ قد أوصى في مناقشته للمشروع بضرورة إقراره. إن الأخذ بغير ذلك يشكل هدماً ومخالفة صريحة للمبدأ الذي يقوم عليه القانون الجنائي ونقصد بذلك مبدأ شرعية التجريم والعقاب ولا نظن أن المشرع الفرنسي يسمح بالتجاوز عليه أو التغاضي عنه. إلى جانب أن ذلك يعد مخالفة لأصول وقواعد التفسير التي ينبغي للمفسر أياً كان أن يلتزم بها وأقصد بذلك غاية المشرع من النص وعدم تجاوز إرادته التي عبر عنها في مجمل عبارات النص، ولاسيما أن النص خلا من إيراد مثل هذا القيد ولو كان المشرع يريد ذلك لقال لأن المشرع إذا أراد قال. ونؤيد ما نقول به بما يذهب إليه القضاء الفرنسي الذي أيد عدم ضرورة الحماية الفنية أو التقنية للبرامج، حيث قضى بأنه لا يشترط لوجود الجريمة أن يكون الدخول إلى النظام مقيد بوجود حماية فنية[٣٢].

---

٣٢. د. علي عبد القادر القهوجي- المرجع السابق- ص١٢٤ ولاحظ قرار المحكمة المشار له في الهامش رقم (١).

إلى جانب ذلك كله فإن الإصرار على هذه التفرقة يكشف عن قلة أهميتها الواقع العملي، حيث أن نطاق الأنظمة غير المحمية نطاق ضيق فشبكة المعلومات العالمية التي هي عبارة عن مجموعة من الأجهزة والأدوات المختلفة التي تساعد على تخزين المعلومات في صيغة يمكن استعادتها[٣٣] فإلى جانب كونها شبكة اتصال لأجهزة الحاسب الآلي يتم ربطها باستخدام أنظمة الاتصال ويمكن من خلالها تبادل المعلومات فإنها تضم إلى جانب ذلك أنظمة برمجية لإدارتها[٣٤]. الأمر الذي يجعل من انظمة الحماية الفنية أمر ضروري تكشف عنه علة تجريم الدخول إلى هذه الأنظمة؛ فكونها شبكة لتبادل المعلومات مكونة من مجموعة ضخمة من أجهزة الحاسب الآلي المنتشرة حول العالم والمرتبطة ببنوك المعلومات ومختلف المراكز العلمية والبحثية. وكون المعلومات التيس هي كل ما يمكن إرساله عبر خطوط الاتصال الإلكترونية ومن رسائل وتقارير وكتب ومقالات وصور أو أرقام أو كلمات عبارة عن معلومات لها قيمة اقتصادية عالية، يجعل مايوجد على شبكة الانترنيت كمبدأ عام لاينتهي أن يتم الحصول عليه إلا بترخيص، لذلك برزت الحاجة إلى حماية ذلك من الاستخدام غير المشروع، أي غير المرخص به ولذلك كان الدخول إليها بشكل عام، وإلى أغلب مواقعها بشكل خاص بترخيص يتمثل بالرقم الذي يتم من خلاله الدخول إليها أو بالأحرى الاتصال بها. ومن أساليب الحماية التي يمكن اتخاذها سواء لحماية المعلومات الموجودة على الشبكة أو لحماية الشبكة من الاختراق، ومن ثم الاستخدام غير المرخص هو أسلوب كلمة المرور (Pass Word) المدعم ببرتوكول خاص مسؤول عن التأكد من صحة كلمة المرور، يسمى (Pass Word authentication)[٣٥] ومن ثم السماح للمستخدم بالدخول إلى الموقع المعلومات، بل حتى أن الدليل الإلكتروني الذي يوفر خدماته الجهاز (Minitel) والذي عده البعض من الأنظمة المخصصة للجمهور فأن كل مشترك

---

٣٣. كرستان كروملش، روبرت كورت وآخرين- المرجع السابق- ص٢٠.

٣٤. مراد شلباية- علي فاروق- مقدمة إلى الانترنيت- دار المسيرة للنشر والتوزيع- الأردن- عمان ط/الأولى ٢٠٠١ ص١٩.

٣٥. مراد شلباية- علي فاروق- المرجع السابق- ص٣٠.

فيه يخصص رقم سري للدخول إلى المعلومات التي يرغب في الحصول عليها مما يجعله يفقد طبيعته.

الفصل الثاني

الركن المادي لجريمة الدخول عن طريق الغش

سنقسم هذا الفصل إلى مبحثين في الأول ماهية الدخول على أن يكون الثاني مخصصاً لبيان أو تحديد الوسائل التي يمكن أن يرتكب بها.

المبحث الأول

ماهية الدخول عن طريق الغش

يقتضي البحث ماهية الدخول عن طريق الغش أن نبين مدلوله أو المقصود به ومن ثم المعيار الذي ضوئه يتحقق الغش، وقد خصصنا لكل أمر مطلباً مستقلاً.

المطلب الأول

مدلول الدخول

الدخول في النظام الآلي يقوم على عنصرين: عنصر مكاني، وعنصر زماني، والعنصر المكاني يحدد مدلول النظام الآلي الذي سبق أن بيناه بحيث ينبغي لتحقق الدخول أن يكون في وحدة من وحدات النظام الآلي بالمعنى الذي تم تحديده، ورجحناه في إطار المدلول الذي طرحه مجلس الشيوخ الفرنسي أما العنصر الزماني فيتكون من جانبين: الأول يحدده الحالة التي عليها النظام الآلي والتي على ضوئها

يتحقق الدخول، والجانب الثاني يحدده الزمن الذي يستغرقه فعل الدخول وينتهي عنده. وبخصوص الجانب الأول فإن الدخول يتحقق عندما يكون النظام الآلي في حالة تشغيل أو اشتغال. ولا يمنع ذلك أن يتم الدخول و الوحدة في حالة إيقاف فيقوم الجاني بتشغيلها ومن ثم الدخول إليها أو إلى النظام من خلالها أو عن طريقها. ولا يمكن أن يتم الدخول والنظام في حالة إطفاء. وخاصة بالنسبة للدخول في غير شبكة المعلومات العالمية لأنها في حالة اشتغال على مدار الساعة. ولكن هذا لايعني أن جميع الوحدات المتصلة بها يمكن الدخول فيها؛ إذ لابد أن تكون الوحدة في حالة اشتغال حتى لو كانت الشبكة بنفس الحالة، بمعنى آخر اشتغال شبكة المعلومات العالمية ومن ثم الدخول بها لا يعني تحقق الدخول إلى الوحدات المرتبطة بالشبكة إلا إذا كانت تلك الوحدات في حالة اشتغال ذلك المبدأ الذي يقوم عليه العمل بفايروسات الحاسب الآلي، حيث يصيب جميع الوحدات المرتبطة والتي كانت في حالة اشتغال. لذلك ينبغي التفريق بين تشغيل الوحدة وتشغيل النظام بأكلمه الأمر الذي لا تلازم بينهما. أما فيما يتعلق بالجانب الثاني والذي يتعلق بالزمن الذي يستغرقه فعل الدخول وينتهي عنده فإن هذا يعتمد على جملة عوامل منها قدرات الشخص والأجهزة التي يستخدمها وطبيعة النظام الآلي وكفاءة أنظمة الحماية، ولكن بشكل عام فإن الدخول يتحقق وينتهي عند تحقق الاتصال بالنظام بحيث يكون النظام أو الجزء الذي تم الاتصال به مفتوحاً أمامه وهذا هو مظهر النتيجة في جريمة الدخول بحيث أن تحقق الاتصال يعكس من جانب حالة شاهدة للعيان بحيث تحقق التغير في العلم الخارجي المتطلب لتحقق النتيجة الجرمية بمدلولها المادي بحيث أصبحت الوحدة التي استخدمها الجاني في فعله متصلة بالنظام بعد أن كانت غير ذلك، وهذا من شأنه أن يجعل النظام مفتوحاً بعد أن كان مغلقاً أمامه هذا من جانب.

ومن جانب آخر فإن الدخول إلى النظام الآلي كما يمكن أن يكون منطقياً يمكن أن يكون مادياً ويتحقق الأخير بإدخال وحدة ما داخل النظام بطريقة غير مشروعة أو ربط أي وحدة بوسائل إتصال مادية كالأسلاك خلاف الأمر بالنسبة

للدخول المنطقي الذي يكون من خلال الاستخدام غير المشروع لأحدى وحدات النظام أو خطوط الجهاز أو بانتحال صفة شخص له حق الدخول وذلك من خلال استخدام كلمة المرور أو الرقم السري الذي يسمح له بالدخول إلى النظام أو بلأحرى الاتصال به على المعنى الذي قدمناه؛ إذ لا يشترط في الدخول أن يكون الاتصال بوسائل مادية، ولا يشترط من قبل أن يكون الدخول مادياً وأن كان ذلكأبسط صور الدخول عندما يقوم الجاني بربط وحدة بالنظام ربطاً مادياً سواء بربط أو بوصل الوحدة بأي وحدة من وحدات النظام أو بالوحدة الرئيسية له. إذ كما يمكن أن يكون الدخول كذلك يمكن أن يكون عن طريق الاتصال عن بعد وذلك بتمكين الاتصال بين الوحدة التي يعدها الجاني والنظام بوسائل الاتصال اللاسلكية. لذلك ينبغي في إطار إعتماد مدلول الدخول عدم فهمه على أن المقصود به هو الدخول المادي كالذي يتحقق عند الدخول إلى منزل إنما ينبغي فهمه على أنه ظاهرة معنوية تتحقق في الوصول إلى العلميات المنطقية التي يقوم بها أو عليها النظام الآلي لمعالجة المعطيات بمختلف الوسائل والسبل، والذي كما يمكن بوسائل اتصال مادية، أي سلكية، يمكن أن يكون بوسائل اتصال عن بعد أي بوسائل لا سلكية وهو الأسلوب الأحدث في هذا المجال.

كما لا ينبغي لتحقق الدخول أن يتحقق الاتصال بكل أجزاء النظام، أي أن يتم الدخول إلى النظام كله إنما يكفي لتحقق الدخول الاتصال بجزء أو بعنصر منه، أي يكفي لتحقق الجريمة أن يتم الدخول إلى جزء من الشبكة أو النظام حتى ولو كان ذلك الجزء ضيقاً ولا يتضمن المعلومات التي يسعى الجاني للوصول إليها كأن يقوم أحد الموظفين في مؤسسة ما المسموح له بالاتصال بالجزء (C) بالاتصال بالجزء (D) في النظام المعمول به في المؤسسة. وتكمن خطورة الدخول إلى النظام الآلي فيما يترتب عليه من أضرار بالنظام أو بالمعلومات التي يتضمنها أو فيما يرتكب من أفعال بعد تضر بالنظام؛ إذ يمكن بعد ذلك أن يقوم الجاني بالنسخ والإتلاف وإفشاء السر والحذف أو التعديل والتعطيل والإفساد..الخ من الافعال التي تتناسب وطبيعة النظام.

وبشأن طبيعة فعل الدخول يذهب جانب من الفقه إلى القول بأن الدخول من الممكن أن يقع بوسائل إيجابية وبوسائل سلبية[٣٦]. غير أن هذه الجريمة حيث أنها تتحقق عندما يتحقق الدخول، ويتحقق الأخير عند تحقق الاتصال بالنظام أو أحد وحداته، أي عندما يباشر الجاني نشاطاً يمكن من خلاله الاتصال بالنظام فإن النشاط في هذه الجريمة هو نشاط إيجابي، ولا يمكن أن يتخذ صورة النشاط السلبي.

وعلى أساس ما تقدم فإن الدخول هنا يجب أن يحمل على أنه إجراء الاتصال بالنظام أو بجزء منه بأي طريقة من الطرق اللازمة لذلك والوصول إلى العمليات المنطقية التي يقوم عليها النظام. فالدخول من الممكن أن يتحقق سواء استخدم الجاني قرصاً أو جهازاً تلفونياً أو استخدم كارتاً ممغنطاً أو ضرب حروف الرقم السري أو ما يصطلح عليه بكلمة المرور الذي يستخدم كطريقة تقنية لحماية البرامج[٣٧]، أو أي جهاز آخر لديه يمكن من خلاله أن يتحقق الاتصال بالنظام.

ولنا أن نتساءل بعد أن بينا مدلول الدخول عن مدى تحقق الدخول غير المشروع فيما لو استخدم شخص حق غيره بالدخول؟ ومدى تحقق الدخول بطريق الغش بحق من يملك حق الاتصال بجزء من النظام فيتصل بالنظام؟ هل يعد فعله أيضاً دخولاً غير مشروع بالنسبة للجزء الممنوع من الدخول به أم يمكن أن يستند على حق الاتصال بجزء من النظام ليدفع المسئولية عنه؟

في إطار الإجابة على ذلك لا ينبغي لنا أن نضع في الاعتبار استخدام النظام الآلي لمعالجة المعلومات من قبل شخص لا يملك حق الدخول إليه ولكنه يدخل إليه أو يستخدمه بموافقة ورضا من له حق الدخول إليه أو إلى جزء منه. أصلاً فمن يستخدم حق الغير بالدخول وبموافقته ورضاه لا ينبغي التوقف عنده لأن من نافلة القول بأن الدخول إلى النظام بموافقة من له الحق في السيطرة عليه يمنع تحقق جريمة الدخول؛ إذ أنه دخول مشروع ولا يمكن أن يوصف بعدم المشروعية إلا إذا

---

٣٦. د. أحمد حسام طه تمام- المرجع السابق- ص٣٠٦.

٣٧. د. عمر الفاروق الحسيني- المرجع السابق- ١٢٧.

كان قد تعدى الحدود المسموح بالدخول إليها بحيث كان قد قيد دخوله بجزء منه فتجاوز ذلك إلى الجزء الآخر كما هو الأمر بالنسبة لبعض المؤسسات أو المنشآت عندما تسمح لموظفيها بالدخول إلى النظام ولكن ضمن حدود معينة كأن تسمح لموظف الإدارية الإطلاع على البريد الوارد والصادر والذي يخزن بجزء من النظام ولكنها لا تسمح له بالدخول إلى النظام المالي أو المحاسبي لها والذي يخزن بجزء آخر من النظام أو حتى إلى ملف مهما كان حجمه في نفس الجزء فدخوله إلى هذه الأجزاء لاشك يقع تحت طائلة الدخول غير المشروع لأنه دخول غير مصرح به حتى ولو أن تلك المنشأة لم تقم بحماية الجزء بوسائل فنية تمنع الدخول إلى تلك الأجزاء.

غير أن ما ينبغي الوقوف عنده هو حالة من يستعمل حق غيره بالدخول ممن يتمكن من الحصول على رقم الدخول إلى النظام عن طريق ما فيستخدمه في حالة أن يكون النظام محمي بوسائل أمن فنية أو تقنية؟

مثل هذا الفرض يثير أمرين: الأول لا علاقة لبحثنا فيه ألا وهو الوسيلة التي تم الحصول بها على الرقم السري أو كلمة المرور الذي تمكن من خلالها الدخول إلى النظام الأمر الذي من الممكن أن يثير المسئولية الجنائية عن طريقة حصوله على ذلك ومدى تحقق جريمة السرقة بحقه فيما لو تمكن من الاستيلاء على الأرقام التي تمكنه من الدخول دون البطاقة الأمر الذي تواجهه صعوبات ومشاكل عدة لا تتعلق ببحثنا مما لا يجعلنا نتعرض إليها لأنها مدار بحث مستقل[٣٨]. أما الأمر الثاني التي يثيره هذا الفرض والذي يتعلق بحق الغير في استخدام النظام، فيتعلق بظهوره بمظهر من له الحق في استخدامه الأمر الذي على ما نعتقد يحقق الغش

---

٣٨. لاحظ في عرض الصعوبات التي تواجه تطبيق نصوص جريمة السرقة على برامج الحاسب الآلي بشكل عام وعلى الأموال ذات الطبيعة غير المادية د. محمد حماد مرهج الهيتي – الصعوبات التي تعترض تطبيق نصوص جريمة السرقة على برامج الحاسب الآلي – مجلة الشريعة والقانون – تصدر عن مجلس النشر العلمي جامعة الإمارات العربية – العدد العشرون – ذو القعدة ١٤٢٤ هـ يناير ٢٠٠٤م.

المتطلب لتحقق جريمة الدخول غير المشروع وإن كان دخوله قد يبدو في ظاهره مشروعاً، حيث استخدم كلمة المرور التي تعود لغيره في خداع النظام ومن ثم الدخول إليه.

ويؤكد هذا ما سبق أن أكدنا عليه من أن الغش يتحقق في كل حالة يستطيع فيها الشخص الدخول إلى النظام دون أن يكون له الحق في ذلك، ولم يصرح له من يملك حق السيطرة على النظام بذلك حتى ولو لم يباشر الجاني أي نشاط من شأنه أن يحقق الغش باتجاه الحماية الفنية.

وعلى ما يبدو لنا أن هذا كان سبباً في اتجاه البعض للقول بإمكان تطبيق هذا النص في نطاق جريمة سرقة وقت الآلة باعتباره تطبيقاً للاستخدام بطريق التحايل [٣٩] وذلك بالنسبة للموظف أو العامل أو غيرهما حين يسرق وقت الماكنة ضد إرادة من له الحق في السيطرة على النظام فيقوم بطبع ونسخ بعض المعلومات[٤٠] مع تحفظنا على عبارة سرقة وقت الآلة لأسباب تتعلق بالعقبات القانونية التي تعترض تطبيق تلك النصوص في التشريعات التي تعرف هذه الجريمة. هذا إلى جانب أن سرقة ساعات العمل تقع من عامل أو موظف يتصل بحكم عمله بهذه الآلة، ومن ثم فمن غير الممكن أن يجد نفسه في اتصال مع هذا النظام الذي يفترض بأنه يعرف عنه الكثير[٤١].

أما بالنسبة لمن يملك حق التجوال في جزء من النظام لكنه يستخدم هذا الحق في التجوال في جزء آخر غير الجزء المسموح به وحالة من ينتهي حقه في الاتصال بالنظام ويظل مستمراً به رغم ذلك؟

إن الأمر في اعتقادنا واضح بالنسبة لهذا الفرض أي أن اتصال الشخص ومن ثم دخوله يعتبر قد تم عن طريق الغش وأصبح غير مشروع وإن كان يملك حق

---

٣٩. من هذا الرأي د. هدى حامد قشقوش – المرجع السابق – ص١٠٢.

٤٠. د. علي عبد القادر القهوجي – المرجع السابق – ص١٣٥.

٤١. د. عمر الفاروق الحسيني – المرجع السابق – ص١٢٨.

الاتصال بجزء من النظام لأنه لا يملك الاتصال بكل أجزاء النظام، ولا يمكن الاستناد على حق الاتصال بجزء من البرنامج لدفع المسئولية عنه ومن ثم لإباحة فعله طبقاً لمدلول الدخول الذي جوهره إنعدام حق الشخص بالاتصال بالنظام أو بجزء منه. هذا من جانب.

ومن جانب آخر فإن هذا ينطبق أيضاً على انتهاء الفترة المخصصة للاتصال ويظهر هذا بشكل جلي في الاتصال بشبكة المعلومات العالمية، لأن الجاني أصبح في مركز من ليس له حق الاتصال بانتهاء الوقت المخصص للاتصال[٤٢]. ذلك لأن حق الاتصال يكون محدداً بفترة زمنية معينة يعلمها الشخص أو على الأقل ينبغي عليه أن يعلمها. وهذا القول لا ينطبق طبعاً على من يعتقد خطأً أنه ما زال لديه الوقت الذي يستطيع استغلاله في الاتصال بالنظام في حين أن الواقع غير ذلك لأن الغلط الذي وقع فيه يتعلق بالقصد فيؤثر عليه، ومن ثم على قيام الجريمة لأنها جريمة عمدية.

المطلب الثاني

معيار الدخول عن طريق الغش

يذهب البعض في إطار ذلك إلى القول بأن المعيار الذي على أساسه يعتبر الدخول قد ارتكب عن طريق الغش هو مدى أن يكون النظام محمي بوسائل فنية أو تقنية بحيث أن التغلب على تلك الوسائل يحقق الغش المطلوب لتحقق الجريمة بل هو المعيار المفضل باعتباره يمكن ان يبين الحد الفاصل بين الدخول المشروع وغير المشروع[٤٣]. ولكننا حيث انتهينا في الفصل الأول من هذا البحث وبأدلة قانونية إلى عدم ضرورة أن يكون النظام محمي بوسائل فنية ولاسيما أن المشرع قد أغفله ولم ينص عليه فإن ذلك يحتم علينا البحث عن معيار آخر لاسيما أن الأخذ بمعيار

---

٤٢. أنظر خلاف هذا الرأي د. علي عبد القادر القهوجي – المرجع السابق – ص١٣٣.

٤٣. د. أحمد حسام طه تمام – المرجع السابق – ص٢٩٢.

الحماية الفنية من شأنه أن يخرج طائفة الأنظمة التي لا تستخدم تلك الوسائل من دائرة الحماية بحيث يعد الدخول فيها دخولاً مشروعاً الأمر الذي يؤكد عدم صلاحيته؛ إذ ينبغي في المعيار الذي يتم تبنيه ألا يؤدي إلى إستبعاد أي طائفة من تلك الأنظمة، حيث ينبغي أن يتمتع بالشمولية.

ويبدو لنا أن المعيار الذي يتحقق على ضوئه الغش يرسمه الجواب على السؤال الآتي إذا كان الدخول إلى البرنامج يتحقق بالاتصال فمتى يكون الاتصال قد تم بطريق الغش؟

إن الاتصال حتى يكون قد تم بطريق الغش ينبغي أن يكون غير مشروع، ويكون الاتصال غير مشروع عندما يكون قد تم من قبل شخص ليس له حق الاتصال بالنظام بشكل عام أو بجزء منه.

بمعنى أن الجريمة أو الدخول المكون للجريمة يتحقق حتى ولو كان الاتصال قد تم بجزء من النظام.

ويكون كذلك، أي لا يكون للشخص حق الاتصال، متى كان لا يحق له إجراء هذا الاتصال لأي سبب من الأسباب، بل حتى ولو كان مخالفاً لشروط الدخول التي ينص عليها القانون أو الاتفاق أي يعد الاتصال غير مشروع وبالتالي قد تم عن طريق الغش حتى ولو كان مخالفاً لإرادة من له حق السيطرة على النظام فيكون الدخول غير مشروع إذا كان من له حق السيطرة على النظام قد وضع بعض القيود للدخول ولم يحترم الشخص تلك القيود.

ويتحقق الدخول غير المشروع أيضاً فيما لو كان هناك قيد قانوني على المعلومات التي يمكن الاطلاع عليها والتي يتضمنها النظام أي المخزنة فيه. كما هو الأمر بالنسبة للقيود التي يفرضها المشرع بشأن سرية بعض المعلومات الاسمية منها أو الشخصية كأسرار الأشخاص وما يتعلق بحياتهم الخاصة والمعلومات المتعلقة بأسرار الدولة[٤٤]. وإذا شئنا بتعبير أعم يجمع ذلك فنقول بان كل معلومات

---

٤٤. د. علي عبد القادر القهوجي – المرجع السابق – ص١٣٢.

يتم جمعها في نظام آلي من قبل شخص طبيعي أو معنوي حكومي أو غير حكومي ولا يترك الإطلاع عليها مسموحاً به لأي إنسان يكون الاتصال بها اتصالاً غير مشروع الأمر الذي يحقق الدخول غير المصرح به أو غير المشروع ومن ثم الدخول عن طريق الغش.

وعلى العموم فإن الضابط أو المعيار الذي على ضوئه يمكن تحديد كون الاتصال كان قد تم بطريق الغش، ومن ثم على ضوئه يمكن تحديد كونه قد تم بصورة مشروعة أو غير مشروعة هو انعدام حق الشخص في الاتصال بهذا النظام سواء كان هذا الانعدام يتعلق بكل النظام أو ببعضه[٤٥] وأياً كان السبب الذي يجعل الشخص لا يحق له إجراء هذا الاتصال. فيكون الاتصال غير مشروع سواء كان الاتصال مخالفاً للقانون أو الاتفاق أو إرادة من له حق السيطرة على النظام أو لطبيعة محتويات النظام.

المبحث الثاني

الوسائل التي يتحقق بها الدخول إلى النظام الآلي

لم يحدد المشرع وسيلة معينة لتحقق الدخول، وهذا ما يجعلنا نقول بأن الدخول يقع بأي وسيلة يتوسل بها الجاني ويتم من خلالها الوصول إلى الكيان المعنوي أو إلى العمليات المنطقية التي يقوم بها النظام الآلي، والذي يتحقق بالاتصال. سواء كان قد تم الاتصال عن طريق فعل ينصب على مكونات الكيان المادي كاستبدال الجزء المسئول عن أمن أو عمل الجهاز بآخر أو بفعل من شأنه تحقق الاتصال السلكي كربط الجهاز بمنظومة تستقبل المعلومات التي تبثها الشبكة كاستخدام الهاتف أو أي وسيلة أخرى تمكنه من الاتصال كالتلاعب بعناصر النظام (المادية) كربط جهاز تصنت يستطيع من خلاله اختراق الشبكة أو استقبال المعلومات التي تبث عن طريقها، أو تحقق الاتصال اللاسلكي عن طريق تهيئة جهاز بإمكانه التقاط

---

٤٥. د. عمر الفاروق الحسيني – المرجع السابق – ص١٢٧.

المعلومات التي تبثها شبكة المعلومات أو أي وسيلة أخرى يمكن أن يحقق الجاني هدفه عن طريقها حتى ولو كان عن طريق برنامج فايروسي حيث يتولى هذا البرنامج التغلب على أجهزة الحماية أو أن يقوم باختراق الموقع عن طريق تقنية تفجير موقع الهدف بقصد كشف كافة البيانات والمعلومات التي قد تكون مركزة في موقع التاجر أو موقع المشتري في إطار الوفاء عن طريق بطاقات الوفاء[٤٦].

وبذلك فإن تعبير الدخول يتسع لاستعمال كل الوسائل المتاحة للاتصال بالنظام، فالدخول يتحقق إذا استخدم الجاني كارت مصطنع أو قام بالدخول نتيجة التجربة عن طريق ضرب أرقام أو حروف استطاع من خلالها التعرف على الرقم السري الذي مكنه من تحقيق الاتصال بالنظام. لأن الدخول المحقق لهذه الجريمة يتطلب أن يكون الاتصال قد تحقق مع نظام مشتغل أو قابل للاشتغال ولا يشترط أن يكون الجاني قد تمكن من تشغيله أو لم يتمكن كما لا يشترط أن يكون قد استفاد من دخوله أو لم يتمكن من ذلك. فالمشرع لم يشترط لتحقق هذه الجريمة أن يكون بمقدور الجاني الاستفادة من دخوله لأنه جرم مجرد الدخول إلى النظام ولم يتطلب أي نتيجة تترتب على ذلك، ولم يشترط لتحقق الدخول المجرم أن يتمكن الجاني من إلتقاط المعلومات التي يحتويها النظام كلها أو بعضها، ولم يشترط أيضاً أن يكون الجاني قادراً على استعمال النظام. فيكفي لتحقق الجريمة أن يحصل إتصال بالنظام. فالجريمة تتحقق بحق من يقوم بالدخول حتى ولو كان عاجزاً من حيث القدرة الفنية على القيام بالعمليات التي يتطلبها النظام. فضرورة استعمال النظام أمر غير متطلب أو غير مشروط تحققه لتحقق الدخول المعاقب عليه المهم أن يُحقق الجاني الاتصال بالنظام أو بجزء منه أو بوحدة لها صلة بعمل النظام، أي متصلة به. وعليه لا يتحقق فعل الدخول المحقق لهذه الجريمة إذا دخل الجاني في جزء لا علاقة له بالنظام الآلي كالدخول إلى عنصر أو وحدة لم يكن لها دور مباشر، أي متصلة بعمل النظام ولها دور أساسي، أو حتى دور غير مباشر، أي تساند الوحدات الأخرى المتصلة بالنظام أو تعضدها على إنجاز مهمتها.

---

٤٦. لاحظ – عماد علي الخليل – المرجع السابق – ص١٠٢.

أما بالنسبة لما قد يقال بالنسبة إلى ضرورة توافر صفات معينة بمرتكبي هذه الجريمة كضرورة الإلمام بتقنية النظم الآلية على درجة معينة. فإن هذه الجريمة تقع من كل إنسان أياً كانت صفته أو درجة تعلمه أو معلوماته فهي ليست من الجرائم التي يشترط أن يكون مرتكبها ذا صفة معينة على الرغم مما يشترطه البعض من أن هذه الجرائم ترتكب من أشخاص ينبغي أن تتوافر فيهم درجة معينة من الإلمام بتقنية الحاسب الآلي[٤٧] فإن اشتراط البعض لذلك لا يعني أنها أصبحت من الجرائم ذات الصفة الخاصة، أي ليست من الجرائم التي يطلق عليها جرائم ذوي الصفة كالرشوة والاختلاس إنما هي جريمة يصح ارتكابها من أي شخص سواء كان يعمل أو لا يعمل في مجال النظام الآلي وسواء كان يفهم أم لا يفهم أسلوب تشغيل النظام المهم أن يكون الجاني ممن ليس لهم الحق في الدخول مطلقاً أو من الذين ليس لهم الحق في الدخول بالطريقة التي دخلوا فيها[٤٨]، وما اشتراط تلك الصفات إلا لبيان القدرة على ارتكابها ممن هم لهم الدراية في ذلك أكثر من غيرهم. ويؤيد ذلك الاحصائيات في هذا المجال، حيث يقف في مقدمة مرتكبي هذه الجرائم المحللون، حيث يقترفون ما مجموعه ٢٥% من مجمل جرائم المعلوماتية، ومن ثم يليهم بعد ذلك، أي في المرتبة الثانية، مصممي النظم حيث يرتكبون الجرائم بنسبة ١٨%، ثم يأتي مستخدميها الذين لديهم خبرة معلوماتية، ونسبتهم في نطاق ذلك ١٧%، من ثم يأتي الصيارفة، ونسبتهم ١٦%، ثم الأشخاص غير العاملين بالمنشأة التي تتعرض للاعتداء، ونسبتهم ١٢% وأخيراً مشغلي الحاسب الآلي ونسبتهم ١١%[٤٩] دون أن يعني ذلك عدم إمكان ارتكابها من غير هؤلاء، أي ممن لا توافر لديهم المؤهلات

---

٤٧. حيث يذهب أنصار هذا الاتجاه إلى أن جرائم الحاسب الآلي هي أية جريمة يكون متطلباً لإقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب لاحظ في عرض هذا الرأي وتقديره محمد أحمد عبابنة – جرائم الحاسب الآلي وأبعادها الدولية – دار الثقافة للنشر والتوزيع – الأردن – عمان – ٢٠٠٥ ص١٦، ١٨.

٤٨. د. علي عبد القادر القهوجي – المرجع السابق – ص١٣١.

٤٩. د. عبد الفتاح بيومي حجازي – المرجع السابق – ص٤٣.

العلمية كأن يكونوا من الهواة وهم طائفة من المجرمين يصطلح عليهم بالهكرز (Hikers).

الفصل الثالث

الركن المعنوي لجريمة الدخول عن طريق الغش وإثباته

من المتصور أن يكون الدخول إلى النظام الآلي بصورة عمدية كما هو متصور أن يكون بصورة غير عمدية كأن يجد الشخص نفسه عن طريق الخطأ أو الصدفة في النظام. فهل يحقق ذلك جريمة الدخول غير المشروع؟ هذا لن يكون إلا من خلال بيان صورة الركن المعنوي في المبحث الأول ثم نتعرض في المبحث الثاني إلى دور الحماية الفنية وذلك من خلال إثباته.

المبحث الأول

صورة الركن المعنوي لجريمة الدخول بطريق الغش

صورة الركن المعنوي للجريمة كشف عنها المشرع في سياق نص المادة موضوع الدراسة باستعماله عبارة (بطريق الغش) تلك العبارة التي لا تجعل مجالا للشك من أن الجريمة عمدية لأن معرفة الركن المعنوي للجريمة تحدده النصوص الجزائية التي تكون كلفة ببيان نوع الجريمة والعناصر المتطلبة فيها ومن ضمنها طبعاً الركن المعنوي الذي يستشف بصورة عامة من استخدام المشرع لعبارات محددة كالغش أو سوء النية أو الحيلة أو مع علمه...[٥٠] مما ينبغي أن يتوافر القصد الجنائي في جريمة الدخول.

---

٥٠. D.W Elliot. J.C Wood A Case book in criminal law third edition Maxwel 1974 P88.

غير أن جانباً من الفقه الفرنسي ينظر إلى هذه العبارة بمنظر الريبة والشك فيذهب إلى أنها عبارة منتقدة ووجه انتقاده لها أن المشرع باستخدامه لها قد يوحي من أنه يتطلب في النظام أن يكون محمي بوسائل فنية، أي بضرورة توفير نوع من الحماية التقنية للنظام حتى يمكن الاستفادة من هذا النص[٥١]. ويعكس هذا وجهة نظر الفقه الذي لا يشترط في النظام أن يكون محمي بوسائل فنية. الذي انتهينا إلى تأييده وعدم ضرورته استناداً إلى قواعد المنطق القانوني وعدم استلزام وجوده أو تطلب ذلك مستخلص من النص فحينئذٍ يكون هذا الاعتراض مبني على مجرد التخوف مما لا يمكن الركون إليه.

خلاصة الأمر أن جريمة الدخول إلى النظام الآلي بطريق الغش من الجرائم العمدية وهذا مستفاد من عدة أمور أولها فعل الدخول الذي يغلب أن يكون بصورة يقترن فيها العلم بالإرادة – وبوجه خاص فيما لو كان النظام محمي بوسائل أمن فنية – علم الشخص بما يفعل وإرادة متجه إلى ذلك، وثاني هذه الأمور هو أن الغش هو الصفة الملازمة لفعل الدخول فيكون الدخول إلى النظام الآلي في أغلب الأحوال قد تم بوسائل وأساليب مارسها الشخص لكي يصل إليه ويدخل في مكوناته المعنوية، أي البرامج والمعلومات. وأهمها أنه لا يملك حق الدخول فتظاهر على خلاف الحقيقة بأنه يملك هذا الحق. إلى جانب أن هذه الجريمة تقتضي طبيعتها أن تنتسب إلى الجرائم العمدية لما ينبغي على الشخص القيام به لتحقيق الاتصال وخاصة عندما يكون النظام في حالة سبات أو عدم اشتغال، حيث يتطلب منه ذلك أن يقوم بتشغيل النظام أو الوحدة التي يريد الدخول عن طريقها. لذلك فإن الركن المعنوي لجريمة الدخول عن طريق الغش هو القصد الجنائي الذي يقوم على العلم والإرادة

وكذلك العبارات الأخرى التي أشار إليها

ANTHONY, HOOPER, Harriss criminal law, twenty First edition, 1968, sweet MAXWELL London. P.46

٥١. د. جميل عبد الباقي الصغير – المرجع السابق – ص١٥١.

علم بأن الداخل في النظام ليس له الحق في الدخول وأتجاه الإرادة مع ذلك إلى تحقيقه وذلك بالسعي إلى تحقيق الاتصال بالنظام أو بأحد مكوناته.

ولكن من المتصور واستناداً إلى طبيعة النظام الآلي الذي يعمل بأوامر إلكترونية ولجهل الكثيرين في استخدامه بالشكل الذي ينبغي. أن يتم الدخول إليه أو إلى جزء منه عن طريق الخطأ فهل يحقق ذلك جريمة الدخول غير المشروع؟

إذا كنا قد إنتهينا إلى أن جريمة الدخول جريمة عمدية فإن النتيجة المنطقية التي تترتب على ذلك هي عدم إمكان تحققها ولا تحقق المسئولية الجنائية عنها إذا تم الدخول عن طريق الخطأ لإنتفاء القصد الجنائي. غير أن هناك من يرى بأمكان مساءلة من يدخل إلى النظام المعلوماتي بالصدفة أو معتقداً بمشروعية فعله ثم يبقى به بعد معرفته بعدم مشروعية فعله عن جريمة الدخول وهذا من شأنه أن يجعل جريمة الدخول جريمة مستمرة[٥٢].

ولكن هذا الرأي محل نظر من حيث فكرة الدخول إلى النظام الآلي وكيفية تحققه وموقف المشرع الفرنسي من جريمة الدخول وجريمة المكوث أو البقاء في النظام الآلي، ومن حيث فكرة القصد الجنائي ووقت تحققه على أن نرجيء مناقشة موقفه من طبيعة الجريمة وكونها جريمة وقتية أم مستمرة إلى الموقع المخصص في الفصل الرابع من هذا البحث.

فبالنسبة لموقفه من حيث فكرة الدخول فإن المشرع يشترط وبصريح النص أن يحصل الدخول بطريق الغش الأمر الذي لا يمكن أن يتحقق عندما يكون الدخول بالصدفة أو مع الاعتقاد بمشروعية الفعل؛ إذ ثمة تعارض بين الدخول بطريق الغش والدخول بطريق الصدفة يؤدي بنا إلى عدم قبول هذا الرأي وعدم تصور أن يكون الداخل بطريق الخطأ أو بالصدفة محلاً للمساءلة عن جريمة الدخول بطريق الغش. كما أن بقاء الشخص بعد تحقق الاتصال عن طريق الخطأ أو الصدفة وعدم قطع الاتصال والخروج منه من شأنه أن يحقق جريمة أخرى هي جريمة البقاء أو المكوث

---

٥٢. د. أحمد حسام طه تمام – المرجع السابق – ص٢٨٠.

في النظام التي عالجها المشرع أيضاً ولها من الأركان ما تختلف به اختلافاً جذرياً مع جريمة الدخول وأهمها طريقة الدخول حيث يتطلب الدخول فيها ألا يكون بصورة متعمدة لأن ذلك وجه اختلافها عن جريمة الدخول بطريق الغش بمعنى، حيث يتطلب المشرع في الدخول أن يكون عن طريق الغش في جريمة الدخول يتطلب في جريمة البقاء أو المكوث أن يتم الدخول عن طريق الخطأ، أي أن يكون متجرداً من القصد. ويكشف هذا الاتجاه بتحقق جريمة الدخول عند البقاء بعد الدخول عن طريق الصدفة الخلط الذي وقع فيه، بين جريمتين مستقلتين في الطبيعة والسلوك وشروط تحقق الدخول، وأعتباره جريمة البقاء كنتيجة تترتب على جريمة الدخول.

أما فيما يتعلق بتعارض ما يقول به وفكرة القصد الجنائي فالقول بتحقق جريمة الدخول بعد اكتشاف الشخص بأن دخوله غير مشروع من شأنه أن يطيح بنظرية القصد الجنائي التي من قواعدها أن يكون القصد معاصراً للفعل وليس بوقت لاحق عليه. فالدخول إن تم عن طريق الصدفة أو الاعتقاد بمشروعية الفعل من شأنه أن ينفي القصد الجنائي لجريمة الدخول طبقاً للقواعد العامة والذي تنتفي الجريمة بانتفائه، فتخلف القصد الجنائي لحظة بدء النشاط ينفي ركن من أركان الجريمة وهو الركن المعنوي ومن ثم المسئولية عنها. والقول بغير ذلك فيه مغالطة للمبادئ الأساسية التي يقوم عليها القصد الجنائي. فالدخول إلى النظام عن طريق الخطأ ينفي المسئولية الجنائية العمدية لانتفاء القصد الجنائي الذي لا تقوم بدونه جريمة الدخول طبقاً للقواعد العامة. أما بقائه على هذا الوضع فمن شأنه ان يحقق القصد الجنائي لجريمة أخرى هي جريمة البقاء أو المكوث في النظام الآلي التي عاقب عليها المشرع بنفس المادة وبذات العقوبة المقررة لجريمة الدخول، وهذا يعد من احتياطات المشرع الفرنسي وحمايته لمختلف جوانب النظام الآلي سواء من الداخل بصورة متعمدة فعاقب على الدخول بطريق الغش ومن الداخل بصورة غير متعمدة فأوجب على من يجد نفسه في النظام عن طريق الصدفة أو الخطأ أن يخرج من النظام أو من الموقع الذي لا يسمح له بالتواجد فيه، وجعل هذه الصورة جريمة

مستقلة. وقد بينا الأسباب التي دعتنا إلى عدم تناولنا لجريمة المكوث في النظام الآلي في بداية بحثنا؛ إذ ينبغي بحثها بشكل مستقل.

المبحث الثاني

إثبات القصد الجنائي

ينبغي إلى جانب إثبات فعل الدخول مع صعوبة ذلك لطبيعة الأنشطة التي يتعرض لها النظام الآلي كونها أنشطة غير مادية تأخذ شكل النبضات الإلكترونية وهي منتشرة في الفضاء ومن حولنا ومتجردة في أغلب الأحوال من الآثار المادية كالدماء وغيرها. إثبات القصد الجنائي ومدى توافره لإثبات مسئولية الجاني عن جريمة الدخول إلى النظام المعلوماتي. وإثبات القصد الجنائي بشكل عام هو مسألة موضوعية يرجع إلى تقدير محكمة الموضوع تستخلصه من الواقع تبعاً لنوع الجريمة ذلك لأنه أمر نفسي باطني يجوش في صدر الجاني ولا يمكن استخلاصه إلا من إمارات أو دلائل تكشف عنه.

ولاشك في إطار ذلك من أن الدخول إلى النظام الآلي لمعالجة المعلومات وكون هذ النظام محمي بأنظمة حماية تقنية أو فنية يشكل دليلاً أو قرينة على وجود القصد وسوء نية مرتكب الفعل ذلك لأنه لم يتمكن من الدخول إلى النظام إلا بعد أن تغلب على تلك الوسائل، وهذا لوحده في اعتقادنا كاف لإثبات قصده وسوء نيته. بحيث أن المحكمة تستطيع أن تستظهر القصد الجنائي من خلال كون النظام محمي بوسائل تقنية فتقر بوجود القصد الجنائي من مجرد كون الدخول قد تم والنظام الآلي محمي بوسائل فنية. بحيث تعتبر تلك الوسائل دليلاً عليه دون أن يعني هذا اشتراط وجود تلك الوسائل لتحقق الجريمة. فوجود نظام حماية له جوانب إيجابية من الناحيتين: القانونية والواقعية فمن الناحية الواقعية يسمح للشخص المتواجد في الشبكة أو النظام المعلوماتي بمعرفة الحدود التي لا ينبغي أن يتجاوزها فمثلاً الذي يملك حق الاتصال الجزئي مع وجود نظام الحماية الأمنية: التقنية أو الفنية من شأنه أن يحذره عند محاولة الدخول إلى الجزء غير المسموح به وينبهه إلى عدم جواز إجراء

هذا الاتصال، ولاشك أن إصراره على الدخول إلى هذا الجزء مع وجود هذا التحذير يكشف عن إرادته المصممة على ارتكاب الفعل الأمر الذي يكشف عن فائدة الحماية التقنية أو الفنية في الجانب القانوني، حيث يكشف الاتصال بالجزء المحمي إصرار الجاني على إجراء الاتصال والدخول الأمر الذي يمكن على ضوئه استخلاص القصد الجنائي منه، بحيث يعد القصد الجنائي لجريمة الدخول متوافراً بمجرد الدخول في النظام عند وجود نظام حماية(٥٣).

ويعتبر نظام الحماية من الأهمية في الجانب القانوني أيضاً فيما يتعلق بصلة النظام المحمي بتحقق عناصر القصد الجنائي وأهمها العلم، حيث أن وجود النظام الأمني من شأنه أن ينبه الأشخاص الراغبين في الدخول إلى النظام بأنهم ليس لهم الحق في إجراء هذا الاتصال وأن الموقع ليس للعامة وليس مسموح الدخول إليه من غير موافقة من له الحق في منح التراخيص. التي غالباً ما تكون على شكل رقم سري تحمله بطاقة الاشتراك يتوجب إدخاله أو كلمة مرور ينبغي إدخالها حتى يتحقق الاتصال أو موافقة شفهية يحددها من يتولى السيطرة على النظام كالدخول إلى شبكة المعلومات في مقاهي الانترنيت مع الأخذ بنظر الاعتبار القيود التي يفرضها الغرض الذي من أجله مُنح الإذن فلن يستطيع من أخذ الإذن باستخدام الوحدة المرتبطة بشبكة المعلومات الاستناد إلى هذا الإذن لفتح المواقع المحمية ولا حتى بالنسبة لما تضمه الوحدة التي يستخدمها ودفع المسئولية عنه استناداً إلى ذلك الإذن؛ إذ أن دخوله للنظام تنظمه القيود التي يفرضها غرض الإذن بالاستخدام وما دور من قدم الوحدة إلا أن هيء له السبيل لاستخدام الوحدة استخداماً يتوافق مع الغرض من الاستخدام والقواعد التي تفرضها أصول أستخدام الأنظمة الآلية لمعالجة المعطيات.

فالتنبيه إلى أن الدخول يتطلب موافقة الغير من شأنه أن يحقق العلم وإصرار الشخص على الدخول على الرغم من هذا التنبيه من شأنه أن يبدد القرينة التي يمكن أن يستند إليها الجاني وينشئ قرينة في صالح الإثبات بعلمه بعدم وجود حق

---

٥٣. د. أحمد حسام طه تمام – المرجع السابق – ص٢٧٥.

بالاتصال الأمر الذي له أهميته في نطاق عناصر القصد الجنائي. مع الإقرار بارتباط الإرادة بالعلم لأن الإرادة الواعية هي الإرادة المحيطة أي العالمة بحقيقة التصرف وما يترتب عليه من نتائج. وعلى أساس ذلك يبدو لنا أن ما يقوم به نظام الحماية يتعدى كونه وسيلة إعلام لمن يحاول الاتصال بالنظام بضرورة القيام بما ينبغي عمله للدخول إلى كونه بمثابة الدليل الذي يمكن للجهة القائمة على الدعوى الجنائية الاعتماد عليه لإثبات العلم الأمر المتطلب لقيام القصد الجنائي.

أما عن السبب الذي يؤدي بنا لتأييد أن القصد الجنائي متوافر بمجرد تحقق الدخول في نظام معلوماتي محمي بوسائل فنية أو تقنية فهو أن الدخول إلى مثل هذا النظام يتطلب نشاطاً من شأنه التغلب على تلك الوسائل والذي في كثير من الأحيان يرتبط بمحاولات متعددة تصدر عن الجاني وهذه المحاولات تكشف عن قصده، بل عن إصراره في الدخول مستغلاً في ذلك قدرة الحاسب الآلي من جانب ونقاط الضعف الموجودة في نظام الحماية من جانب آخر لاسيما أن وسائل الحماية الفنية أو التقنية يمكن التغلب عليها ممن لهم الخبرة والدراية بتصميم البرامج وتحليلها[٥٤] وهي، أي وسائل الحماية، تتفاوت من برنامج إلى آخر وهي في كل الأحوال غير مستعصية على من له الخبرة في ذلك، حيث يكشف لنا الواقع عما يؤيد ذلك[٥٥].

ولكن ما ينبغي أخذه بنظر الاعتبار هو أن ما يقال بصدد ذلك ما هو إلا وسيلة من وسائل إثبات القصد الجنائي مثلها في ذلك مثل باقي الوسائل. ويعني هذا من جانب آخر أن هذه الوسيلة هي ليست الوحيدة لإثبات القصد الجنائي فلا يعني

---

٥٤. راجع في الاحصائيات التي تؤيد ذلك – د. عبد الفتاح بيومي حجازي – المرجع السابق ص٤٣ وراجع في الوقائع التي تؤيد ذلك د. جميل عبد الباقي الصغير – المرجع السابق – ص٣١ وما بعدها.

٥٥. ومن الظريف في هذا السياق أن أعلنت شركة أمريكية عن توصلها إلى برنامج غير قابل للنسخ بفضل ما استخدمت فيه من تقنية متقدمة في تحصينه من القرصنة إلا أنها فوجئت بخطاب مرفق به نسخة من برنامجها الحصين! وقد أعلن صاحب الخطاب أن عملية النسخ لم تستغرق أكثر من ست ساعات فقط د. محمد حسام محمود لطفي – الحماية القانونية لبرامج الحاسب الإلكتروني – دار الثقافة للطباعة والنشر – القاهرة – ١٩٨٧ ص٣٢-٣٣.

هذا أن الجهة القائمة على نسبة الفعل إلى الشخص لا تملك وسيلة أخرى غيرها لإثبات قصده، فمن الناحية القانونية ليس هناك ما يمنع من استخلاص القصد من غير ذلك؛ إذ ليس ثمة قاعدة ينبغي تطبيقها عند إثبات القصد الجنائي. مما يعني جواز إثباته بطريقة أخرى كتكرار الاتصال وتعدد المحاولات...الخ ولاسيما أن الحماية التقنية ليست بركن او عنصر في الجريمة إلى جانب أن هناك أنظمة لا تستعمل تلك الوسائل.

الفصل الرابع

أثر الضرر الناتج عن الدخول إلى النظام الآلي عن طريق الغش

يعاقب المشرع على الجريمة بشكل عام أما لأنها تسبب ضرراً أو تهدد بخطر؛ إذ هما معيارا التجريم عند المشرع وتقسم الجرائم على أساس ذلك إلى جرائم ضرر وجرائم خطر. فالمشرع لا يعاقب على الأفعال التي لا ينتج عنها ضرر عام أو خاص ولا تهدد المصالح العامة أو الخاصة بخطر. وينبغي لنا أن نحدد جريمة الدخول إلى أي طائفة تنتمي وإذا تحقق الضرر ما تأثير ذلك على طبيعتها وعلى العقاب المقرر لها على أن يكون كل أمر في مبحث مستقل.

المبحث الأول

أثر الضرر على طبيعة جريمة الدخول إلى النظام الآلي عن طريق الغش

يذهب جانب من الفقه إلى القول بأن الركن المادي لهذه الجريمة يكتمل بالنشاط الإيجابي الذي يصدر من الجاني دون أن يتطلب تحقق نتيجة مادية منفصلة عنه، وبذلك تكون هذه الجريمة من الجرائم الشكلية التي لا يلزم لتحققها تحقق نتيجة معينة منظوراً لها وفق مدلولها المادي[٥٦].

هذا القول إن صدق على وصف جريمة الدخول إلى النظام الآلي بطريق الغش فله نتائج قانونية تتعارض وما يأخذ به المشرع الفرنسي وبوجه خاص على ما يبنى على التفرقة بين الجرائم الشكلية والمادية، بمعنى إن صدق أن جريمة الدخول جريمة شكلية لا يستلزم لتحققها تحقق نتيجة معينة، فلهذا القول أهميته من حيث التفرقة التي تبنى عليه بين الجرائم المادية والجرائم الشكلية بشكل عام، وأهم هذه

---

٥٦. الذي يعني التغيير الناتج عن السلوك الإجرامي في العالم الخارجي. علي حسين الخلف، سلطان الشاوي – المرجع السابق ص١٠٤.

الفوارق هو عدم تصور الشروع في الجرائم الشكلية، وتصوره في الجرائم المادية. ذلك لأن الشروع يعني تخلف النتيجة الجرمية بسبب لا دخل لإرادة الفاعل فيه، الأمر الذي تفتقد إليه الجرائم الشكلية، حيث أنها جرائم من غير نتيجة بمدلولها المادي[٥٧].

ولكننا سبق أن أشرنا إلى أن الدخول في هذه الجريمة يتحقق عند تحقق الاتصال بالنظام، ويمثل الاتصال الفعلي السلوك الإجرامي المتطلب لقيام الجريمة غير أن الجريمة حتى تقوم ينبغي أن تتحقق النتيجة الجرمية التي تتمثل بضرر يصيب المصالح المحمية أو بخطر يتهددها، والنتيجة الجرمية المادية في الجريمة بشكل عام هي التغيير في العالم الخارجي الذي يحدثه النشاط الإجرامي ولو لم يصل إلى حد الضرر[٥٨] والنتيجة المجرمة في الجريمة موضوع البحث هي ليست الإخلال بالنظام الأمني للنظام حتى يكون القول بأنها من جرائم الخطر مقبولاً لعدم ضرورته كما أسلفنا. إنما النتيجة المجرمة تتمثل بالتغيير الذي يحدث في العالم الخارجي والذي يتحقق بمظهر الاتصال بالنظام والذي يجسده اشتغال النظام الآلي بعد أن كان في حالة سبات أو فتح النظام أو جزء منه أو إنفتاحه أمام الجاني بعد أن كان غير متاح له ذلك، بحيث يستطيع التجوال والاطلاع على مكنونات لا يجوز الاطلاع عليها أو بشكل عام الاطلاع على ما لا يجوز له الاطلاع عليه. فيكفي لتحقق الجريمة إتصال الشخص بالنظام الآلي لكي يكون الطريق للإطلاع على ما فيه مفتوحاً دون أن يعني ذلك اشتراط وجود المعلومات المطلوبة. المهم أن الجريمة تكتمل عند تحقق الاتصال بأي صورة وبأي وسيلة سواء باستخدام كارت غير حقيقي أو بضرب كلمات المرور أو الرقم السري الذي حصل عليه بطريقة ما أو أن يستعمل جهاز الهاتف...الخ من الوسائل المتاحة للاتصال بالنظام بحيث يكون

---

٥٧. لأن الجريمة لا يمكن تصور وقوعها من غير نتيجة وإن كانت بمدلولها المعنوي، حيث أن للنتيجة مدلولان مادي ومعنوي، وحيث يمثل الأول التغيير الذي يحدث في العالم الخارجي يمثل الثاني العدوان على المصلحة المحمية راجع في ذلك د. فخري عبد الرزاق الحديثي – المرجع السابق ص٩٨.

٥٨. د. احمد فتحي سرور – الوسيط في قانون العقوبات – الجزء الأول – القسم العام – دار النهضة العربية ١٩٨١ ص٤٣٣.

النظام مفتوحاً وقابلاً لاستقبال الأوامر وهذه هي النتيجة التي يجرمها المشرع في الدخول فغاية المشرع حماية النظام الآلي من الاختراق، الأمر الذي يترتب عليه أن المشرع لا يتطلب تحقق نتيجة معينة جراء الدخول إلى النظام الآلي غير الاتصال به لما يتضمنه هذا السلوك من مخاطر حيث جعل النظام في حالة اتصال مع الوحدة التي أعدها الجاني بعد أن كان هذا غير متاح له مع أن الضرر متحقق ومندمج بالنشاط لما يمثله من انتهاك لحرمة النظام.

ويبدو لنا أن هذا الوضع والخلط الذي يجري بين النتيجة بمدلولها المادي والضرر جعل البعض يذهب إلى أن هذه الجريمة تعد من الجرائم الشكلية أو جرائم السلوك المجرد[٥٩] على خلاف حقيقتها. ونؤيد ما نقول به بأمرين: الأول يتعلق بحقيقة الجريمة الشكلية، حيث أنها الجريمة التي لا تتوافر فيها نتيجة مادية، أي هي الجريمة التي لا يترتب عليها تغيير في العالم الخارجي كأثر للنشاط الإجرامي[٦٠]، وقد بينا هذا الأثر في نطاق الجريمة موضوع البحث. أما الأمر الثاني فيتعلق بما أعطاه القانون للنتيجة بمدلولها المادي من أهمية ومن دور، حيث اعتبرها من جانب كشرط لتمام الجريمة وبتخلفها تتخلف الجريمة التامة أو الكاملة وتتحقق الجريمة الناقصة، أي تتحقق الشروع الذي يتحقق بتخلفها. ومن جانب آخر اعتبرها أيضاً كمعيار لتحديد جسامة العقاب أو مقداره الأمر الذي يظهر بشكل جلي في إطار موضوعنا فما دام نشاط الجاني لا يترتب عليه أي ضرر يصيب مضمون النظام الآلي من محو وتعديل في المعطيات التي يتضمنها من معلومات وبيانات وبرامج فالجريمة تأخذ وصفها البسيط، أي الدخول غير المشدد، ولكن ما أن يترتب على نشاط الجاني ضرر، أي شيء من قبيل ما ذكرناه إنقلب وصف الجريمة إلى جريمة

---

٥٩. من هذا الرأي د. عمر الفاروق الحسيني – المرجع السابق – ص١٢٥، د. جميل عبد الباقي الصغير – المرجع السابق – ص١٥٠.

٦٠. لاحظ في النتائج التي يرتبها جانب من الفقه على التعريف القانوني للجرائم الشكلية د. أحمد فتحي سرور – المرجع السابق – ص٤٣٣ وما بعدها.

الدخول المشددة، حيث ينبغي تشديد العقاب باعتباره أثراً لاحقاً للنشاط، أو نتيجة جسيمة ترتبت كأثر لاحق له.

وبذلك نصل إلى نتيجة هي أن هذه الجريمة من طبيعة يمكن أن يتحقق فيها الشروع، فلو كانت من الجرائم ذات السلوك المجرد كما يذهب أصحاب هذا الاتجاه فإن فعل هذا الشخص يخرج من نطاق المساءلة لكون جرائم السلوك المجرد لا يشترط لتحققها أو لقيامها تحقق نتيجة معينة، أي لو أنها كانت من الجرائم الشكلية تلك الجرائم المجردة من النتيجة بمدلولها المادي، لما أمكن تصور الشروع فيها لأن المعلوم أن الشروع غير متصور في تلك الجرائم لأنه يعني تخلف النتيجة بمدلولها المادي لسبب خارج عن إرادة الجاني، والنتيجة بمدلولها المادي غير متصور وجودها في الجرائم المتجردة منها. مما يعني أن الجريمة لو كانت من الجرائم الشكلية فإنها لا تقوم إن حاول الجاني الاتصال ففشل هذا هو حكم المنطق القانوني فهل يا ترى تعامل المشرع الفرنسي مع هذه الجريمة على هذا الأساس؟

إن ما يؤيد ما نقول به هو أن المشرع الفرنسي لم يتعامل مع طائفة الجرائم ضد النظام الآلي وبضمنها جريمة الدخول إلى النظام الآلي على أساس تجردها من النتيجة بمدلولها المادي الأمر الذي يمكن قبول النتيجة التي توصل إليها جانب من الفقه إنما عاقب على الشروع بذات العقوبة المقررة للجريمة[٦١]. وهذا ما نستند إليه في تأييد وجهة نظرنا بشأن طبيعة جريمة الدخول؛ إذ أن المشرع الفرنسي يكون قد خرج عما هو معمول عليه في إطار جرائم السلوك المجرد لو أنه اعتبر جريمة الدخول من ذات الطبيعة عندما يعاقب على الشروع فيها. لأن الشروع أمر خارج عن التصور في إطار تلك الجرائم. فعقاب المشرع على الشروع في جريمة الدخول ومساواته بالجريمة التامة لا يمكن أن يستفاد منه إلا أن جريمة الدخول من طبيعة الجرائم التي يتصور أن يقع فيها، أي من الجرائم المادية التي من المتصور أن يقع

---

٦١. لاحظ المادة ٧/٣٢٣ من قانون العقوبات الفرنسي الجديد التي تقابل المادة ٧/٤٦٢ من القانون رقم لسنة ١٩٨٨ التي تنص على أنه (يعاقب على الشروع في الجرائم المنصوص عليها في المواد ٢/٤٦٢ إلى ٦/٤٦٢ بنفس عقوبات الجرائم).

فيها وليست من الجرائم الشكلية، وإلا ما كان ليعاقب عليه استناداً إلى المنطق القانوني الذي ينبغي أن يحكم الجرائم الشكلية فيما لو أنه يعتبرها من تلك الطائفة.

وقد أثار هذا الوضع وأقصد طبيعة النشاط المادي المكون لجريمة الدخول والخلاف الفقهي الذي برز بشأن انتسابها إلى الجرائم الشكلية أم إلى الجرائم المادية في أذهان البعض إشكالاً يتعلق بالوصف القانوني الذي يمكن أن تأخذه الجريمة استناداً إلى طبيعة نشاط الجاني وما يمكن أن يثيره الدخول من إشكال باعتباره واقعة ليست محددة بزمن، حيث اختلف بشأن وقت انتهاء جريمة الدخول وبداية جريمة البقاء وفقاً للإتجاه الذي يرى بأن الجريمة الأخيرة ما هي إلا امتداد للجريمة الأولى ونحن لسنا منه. فكان علينا أن نوضح إلى أي طائفة من الجرائم يمكن ان تنسب جريمة الدخول هل إلى طائفة الجرائم الوقتية أم إلى طائفة الجرائم المستمرة؟

ابتداءً لابد من الإشارة إلى أن الاختلاف في تحديد طبيعة هذه الجريمة ناشئ من مدى تحقق جريمة البقاء بعد تحقق جريمة الدخول فالاتجاه الذي يرى بأن جريمة البقاء هي امتدادا لجريمة الدخول غير المشروع بحيث يمكن مساءلة الجاني عن جريمة البقاء أو المكوث في النظام الآلي بعد تحقق الدخول اعتبر جريمة الدخول جريمة مستمرة كما هي الحال بالنسبة لجريمة البقاء، والذي اعتبرها جريمتين منفصلتين اعتبر جريمة الدخول جريمة وقتية وجريمة البقاء جريمة مستمرة.

واستجلاء حقيقة هذا الوضع يكون من خلال بيان مدلول الجريمتين: فالجريمة الوقتية هي التي تتم وتنتهي في لحظة واحدة ولا يستمر بعدها النشاط الاجرامي الذي ساهم في اتمامها، والجريمة المستمرة هي تلك التي يلزم فيها بقاء حالة الاستمرار، أي هي التي يكون فيها السلوك الاجرامي متجدد بحيث يتكون من حالة جنائية تقبل بطبيعتها الاستمرار ولا تنتهي إلا بانتهاء هذه الحالة[٦٢] حيث يتطلب ركنها المادي نشاط متجدد يمتد لفترة زمنية، ولا ينبغي الاكتفاء بإمتداد السلوك الإجرامي إنما لابد

---

٦٢. د. فخري الحديثي – المرجع السابق – ١٨٦. د. علي حسين الخلف، سلطان الشاوي – المرجع السابق ص٣١٤.

أن يعاصره إمتداد معنوي إن صح التعبير فالجريمة المستمرة في المدلول القانوني هي ما امتدت مادياتها ومعنوياتها خلال وقت طويل أما الجريمة التي تمتد مادياتها دون معنوياتها فلا يكفي ذلك لقيام جريمة مستمرة[٦٣] أي أن الجريمة المستمرة تفترض استمرار ركنها المادي والمعنوي بعد لحظة تمامها.

ولكن أن تستمر آثار النشاط الإجرامي بعد إتمام الجريمة، فهذا في حقيقة الأمر جوهر الإشكال بين الجريمة المستمرة والجريمة ذات الآثار المستمرة التي تعتبر جريمة سرقة الطاقة الكهربائية لها مثلاً[٦٤]. حيث لا يكون النشاط الإجرامي فيها قادر بحسب طبيعته على الاستمرار إنما آثاره هي التي تستمر. وبما أن العبرة في الوصف الذي تأخذه الجريمة هو ليس بالفترة التي يستمر فيها تنفيذ الجريمة قبل إتمامها إنما بالفترة التي يستمر فيها النشاط الإجرامي بعد تمامها فإنه بالاعتماد على ذلك يكون التمييز بين الجريمة الوقتية والمستمرة واضحاً.

ويؤدي بنا هذا إلى القول بأن من يعتبر جريمة الدخول جريمة مستمرة[٦٥] مثلها مثل جريمة البقاء يكون قد جانب الصواب بسبب الخلط بين النشاط الإجرامي المكون للركن المادي للجريمة وآثاره يؤيدنا في ذلك مذهب المشرع الفرنسي الذي عاقب على فعل البقاء في النظام الآلي بحد ذاته واعتباره البقاء أو المكوث في النظام جريمة مستقلة، ومن هذا يمكن الاستدلال على أن المشرع أراد اعتبار الدخول إلى النظام جريمة وقتية وليست جريمة مستمرة. فالوصف القانوني الذي تأخذه جريمة الدخول استناداً إلى التصور الذي طرحناه بشأن طبيعة النشاط الاجرامي وكونه ينتمي إلى النشاط الإيجابي الذي يترتب عليه نتيجة بمدلولها المادي يجعلها تنتسب إلى طائفة الجرائم الوقتية أما ما يترتب على سلوك الجاني بحيث تبقى مظاهره لفترة بحيث يبقى النظام بحالة اشتغال أو أن يكون النظام مفتوحاً بعد تحقق الاتصال فلا

---

٦٣. د. محمود نجيب حيني – المرجع السابق – ص٣١٨.

٦٤. د. أحمد فتحي سرور – المرجع السابق – ص٤٢٦.

٦٥. لاحظ د. جميل عبد الباقي الصغير – المرجع السابق – ص١٥٠ الذي يرى نسبة هذه الجريمة إلى طائفة الجرائم المستمرة سواء تعلق الأمر بالدخول إلى النظام أو البقاء فيه.

ينبغي أن يؤدي ذلك إلى إمكان نسبتها إلى طائفة الجرائم المستمرة؛ إذ ينبغي عدم الخلط بين النشاط وآثاره، أي بين الجريمة المستمرة والجرائم الوقتية التي ترتب آثاراً مستمرة من حيث الزمان[٦٦] كون آثار نشاط الجاني ظل مستمراً بعد تحقق الدخول، وليس سلوك الجاني هو الذي ظل كما يذهب البعض[٦٧]، بل ان طبيعة النشاط في جريمة الدخول واستمرار بقاء الجاني في النظام وعدم خروجه منه لا يمكن أن يستنتج منه أن الجريمة ذات طبيعة مستمرة إنما هو أثر للنشاط الذي تحقق به الدخول، أي الاتصال.

المبحث الثاني

أثر الضرر على العقاب المقرر لجريمة الدخول إلى النظام الآلي عن طريق الغش

من المتصور أن يترتب على الدخول إلى النظام الآلي لمعالجة المعطيات إحداث أضرار بسبب العبث سواء بالبرامج التي يعمل بها أو بالمعلومات التي

---

٦٦. لاحظ في عرض هذا الرأي د. أحمد حسام طه تمام – المرجع السابق – ص٢٩٨.

٦٧. د. جميل عبد الباقي الصغير – المرجع السابق – ص١٥٠.

يختزنها مما يحدث أضراراً بالنظام بحد ذاته أو بمحتوياته، ولاسيما عندما يمس النظم أو البرامج التي يعمل بها سواء بمحوها أو حتى تعديلها، وسواء كان هذا الأمر مقصود أي من بين اهداف الجاني أو ناتج عن جهل الجاني بأصول التعامل مع النظام فتؤدي الأوامر التي يصدرها والحركات التي يقوم بها إلى ذلك.

ومن ملاحظة المادة ١/٣٢٣ عقوبات التي تنص في شقها الأخير على أنه (... ... فإذا نجم عن هذا الدخول أو البقاء محو أو تعديل في المعطيات المختزنة في النظام أو إتلاف تشغيل هذا النظام تكون العقوبة الحبس لمدة تتروح ما بين شهرين إلى سنتين والغرامة التي تتراوح ما بين عشرة آلاف إلى مائتي ألف فرنك). يتبين أن المشرع قد شدد العقاب بالنسبة لجريمة الدخول إذا ترتب على الدخول محو، أو تعديل في المعطيات المخزنة في الحاسب الآلي، أو ترتب على ذلك إتلاف تشغيل النظام، ولخصوصية الموضوع ارتأينا أن نبين مدلول هذه المصطلحات وفقاً لفهمنا للموضوع ولما هو متعارف عليه في الفقه باعتبارها صور النتائج التي يقتضي تحققها تشديد العقاب.

وابتداءً لابد من التنويه إلى أن النشاط الذي يباشره الجاني في هذه الأحوال يكتسب خصوصية تتأتى من أنه نشاط ينصب على محتويات ومضمون النظام الآلي فبعد أن كان هدف الجاني الوصول إلى النظام أصبح موضوع النشاط أمر آخر هو محتوياته بما يتضمنه من معلومات وبيانات وبرامج مع التأكيد على أن هذه النتائج من شأنها أن تؤثر على عمل النظام فتشوهه أو ربما تعطله إذا ما أنصب المحو والتعديل على الحلقات الأساسية التي يشتغل بها النظام كبرامج التشغيل. ويعرف البعض المحو بأنه إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل أو تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة في حين يعرف التعديل بأنه (تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى)[٦٨].

---

٦٨. د. علي عبد القادر القهوجي – المرجع السابق – ص١٤٤.

والحقيقة أن المحو إذا كان يعني بمفهومه العام بأنه إزالة أو طمس المعطيات على أي دعامة فإن مفهومه الخاص في موضوع دراستنا ينبغي أن يفهم على أساس أنه إزالة أو طمس نهائي للمعطيات الموجودة داخل النظام الآلي أو أي وحدة من الوحدات المتصلة به طبقاً لمدلول النظام الذي بيناه في هذا البحث، بصورة كلية أو جزئية؛ إذ كما يمكن أن يكون المحو جزئياً يمكن أن يكون كلياً. مع الأخذ بنظر الاعتبار أن من شأن المحو الكلي أن يؤدي إلى إتلاف أو تعطيل النظام الآلي وعدم اشتغاله أو تأديته لوظائفه بصورة كلية متى ما انصب على الحلقات الأساسية التي يتكون منها النظام كمحو برامج التشغيل التي يعمل بها النظام أو ربما يؤدي إلى عدم أدائه لوظائفه إذا انصب على المحو على برامج التطبيق أو التنفيذ خلاف المحو الجزئي الذي ربما يؤدي فقط إلى تغيير في وظائف البرنامج أو تعديلها أو ربما إلى تعطيل بعض أجزائه بإلغاء عملها أو بإلغاء بعض مهامها. إلى جانب ان المحو كما يتحقق بالازالة يمكن أن يتحقق بالإضافة أو الاستبدال لذلك يمكن أن نعرف المحو بأنه كل طمس نهائي بالإزالة أو الإضافة أو الاستبدال من شأنه أن يعيق عمل النظام بصورة كلية أو جزئية أو يوقفه عن العمل أو أدائه لوظائفه التي رصد لإنجازها بحيث لا يمكنه أن يؤدي وظائفه بالشكل المطلوب.

أما التدقيق بتعريف التعديل فيكشف عن تناقض وقع فيه صاحبه، ولاسيما إذا أخذنا بنظر الاعتبار التعريف الذي قدمه للمحو. فإذا كان التعديل يتم بتغيير المعطيات الموجودة داخل النظام فإن التغيير وفقاً لخصائص البرامج التي يعمل بها النظام الآلي لا تشترط الاستبدال؛ إذ كما يحدث التعديل بتغيير المعطيات يحدث بحذف فقرات منها، إلى جانب أنه يحدث أيضاً بإضافة فقرات أو بيانات أو برامج يقوم الجاني بإدخالها، سواء كان ذلك في نطاق برامج التشغيل أو برامج التطبيق أم في نطاق المعلومات المخزنة في وحدات الخزن الداخلية[٦٩] وبسبب ما يتصف به

---

٦٩. هي وحدات مسئولة عن تخزين البيانات والتعليمات، ومن قبل البرامج اللازمة لتشغيل الحاسب الآلي وتقوم إلى جانب ذلك بإرسال أوامر وتعليمات البرنامج إلى وحدة التحكم لتفسيرها وتنفيذها، كما أنها ترسل البيانات التي يتم إدخالها إلى وحدة الحساب والمنطق من أجل

عمل النظام الآلي وما تتصف به البرامج من صفات فإن التعديل يحصل حتى في المناقلة لكل أو بعض فقرات البرامج أو المعلومات، دون أن يكون من وراء ذلك إحداث حذف للمعلومات أو للبرامج، ذلك لأن المناقلة تعني إعادة صياغة أو ترتيب البرنامج أو المعلومات بأسلوب يختلف عن أصله مما يؤدي إلى حصول التعديل تبعاً لنوع وطبيعة البرنامج أو المعلومات التي تمت منها أو إليها المناقلة.

وما يؤكد أن التعديل من الممكن أن يحصل دون حذف أي فقرة أو حتى استبدالها ما قام به واضع برامج لإحدى الشركات، حيث تم الكشف عن أنه قد أعد برنامجاً يتيح له إدخال مرتبات أشخاص وهميين، ومن ثم تحويل هذه المرتبات إلى حسابه الخاص، وبسبب أن هذه الطريقة باتت معروفة، ومن السهل اكتشافها لأنها أصبحت طريقة شائعة تعرضت لها أكثر من شركة، مما أضطره إلى إجراء تعديل في تصميم برنامج دفع المرتبات يكون من شأنه عدم طبع حوافظ مرتبات الموظفين الوهميين عند طبع حوافظ مرتبات الموظفين، ومن ثم لا تظهر مدفوعات رواتب الموظفين الوهميين في قوائم المراجعة التي يعدها الحاسب الآلي والشيكات التي يتم صرفها[٧٠]. وبذلك يكون قد نجح الجاني في تحقيق التعديل المطلوب دون أن يقوم بحذف أو حتى استبدال أي مكونة من مكونات النظام.

المهم في إطار موضوعنا هو أن المشرع الفرنسي جعل من النتيجة التي من الممكن أن تترتب على الدخول إلى النظام الآلي عن طريق الغش ظرفاً يشدد العقاب متى ما ترتب على نشاط الجاني محواً بالمعنى الذي قدمناه، أو تعديلاً، أو إتلافاً لنظم التشغيل، وما يمكن أن يذكر بشأن إتلاف نظام التشغيل، فإن هذا الأمر يتحقق

معالجتها، كما أنها تقوم باستقبال نتائج اشتغال الحاسب الآلي، وما قام به من عمليات على البيانات المدخلة تمهيداً لإخراجها، لذلك توصف هذه الوحدة، وبالذات وحدة الذاكرة منها بأنها همزة الوصل بين وحدات الحاسب المختلفة د. يحيى مصطفى حلمي – الحاسبات الإلكترونية – مكتبة عين شمس – ١٩٩٦.

٧٠. راجع في تفصيل هذه الواقعة د. عبد الفتاح بيومي حجازي – المرجع السابق – ص٣٠ هامش رقم (١).

ليس بشأن إتلاف الأنظمة التي يشتغل بها الحاسب الآلي، فحسب، بل إنما من الممكن أن يشمل إتلاف النتائج التي توصل إليها الحاسب الآلي أو التي من الممكن أن يتوصل إليها، أي حتى التي لم يتم استخراجها، على شكل مخرجات ورقية، أو إلكترونية.

ومما تقدم يمكن استنتاج أن غاية المشرع الأخرى من التجريم هي ضمان سلامة النظام الآلي من كل عبث وتلاعب، لذلك فإن الدخول الذي يصاحبه ضرر بإحدى الصور التي حددها المشرع بالمحو أو التعديل أو تعطيل نظام التشغيل ينبغي أن يتم التعامل معه على أساس تشديد العقاب، وفقاً لما حدده المشرع بالمادة موضوع البحث.

ولكن ما يلاحظ على مذهب المشرع الفرنسي هو أنه لم يفرق في العقاب بين المحو والتعديل وتعطيل النظام مع اختلاف خطورة كل فعل، حيث شدد العقاب بتحقق أي من تلك الصور وترك الأمر بيد القضاء في ضوء سطته التقديرية للعقاب إذا تحققت إحدى تلك الصور لاسيما أنه جعل العقاب بين حدين وإن كان هذا يمكن أن يعد معياراً لتشديد العقاب في إطار كل صورة حسب جسامة التعديل أو المحو أو تعطيل نظام التشغيل وإن كانت الصورة الأخيرة أخطر وأشد جسامة من الصور الأخرى مع التأكيد على أن المحو أو التعديل قد يؤدي إلى تحققه الأمر الذي يبرر للمشرع جمع هذه الصور بنص واحد.

وما ينبغي التنويه إليه هو أن هذه الأفعال إذا كان التصور الغالب فيها هي أن تكون من جراء فعل المتهم نتيجة للدخول وبشكل خاص عندما يباشر نشاطاً من شأنه أن يؤدي إلى ذلك بأمر من الأوامر التي يمكن أن يوجهها للنظام، حيث أن الاتصال بالنظام يكون من خلال أوامر فإن هذه المهمة من الممكن أن يقوم بها الجاني ويحقق أغراضه من خلال برنامج فايروسي[٧١] يتم بثه بعد تحقق الاتصال

---

٧١. الفايروس عبارة عن أمر مضلل يدخله الجاني إلى النظام من شأنه كف منفعة النظام وبرامجه فيما أعد لها من خلال تكرار كتابة المعلومات ذاتها إلى آلية إدارة القرص مما يؤدي إلى إيقاف الحاسب الآلي عند حد معين، ويسبب أعباء إضافية على القرص ويزيد من حرارته نتيجة

الأمر الذي تعاني منه الأنظمة الآلية ولاسيما بعد إرتباطها بشبكة المعلومات وللخصائص التي تتمتع بها فايروسات الحاسب الآلي وأهمها قدرتها على إصابة الأجهزة السليمة بسبب قدرتها على الانتقال.

الخاتمة

فرضت علينا طبيعة البحث أن ننتهج نهجاً ربما يبدو فيه شيء من الغرابة على الدراسات القانونية وبالذات التطرق والتوسع نوعا ما في بعض المواضيع التي لها علاقة بموضوعات علم تقنية الحاسب الآلي ونتلمس لمذهبنا هذا العذر في حداثة هذا الموضوع من جهة وإعطاء الإطار الواضح والمحدد لمحل الجريمة باعتبار أن الدخول ينصب على النظام الآلي مما اقتضى منا أن نتعرض إلى معناه في نظر جانب من الفقه ومجلس الشيوخ وبينا الأسباب التي استندنا إليها في ترجيح المدلول الأخير عند تطبيق تلك النصوص وذلك من خلال بياننا للنتائج التي تترتب على تبني هذا المدلول والأخذ به. واستكمالاً لوجهة النظر هذه كان علينا أن نبين

للتشغيل المستمر أنظر في هذا المعنى سرحان سليمان داود، ومحمود عبد المنعم المشهداني – أمن الحاسوب والمعلومات – دار وائل للطباعة والنشر – الأردن – عمان – ٢٠٠١ – ص١٣٢.

مدى ضرورة الحماية الفنية أو التقنية للأنظمة الآلية لكي تتحقق الجريمة وبعد أن عرضنا الاتجاهين: الاتجاه الذي يرى ضرورة ذلك لتحقق الغش المتطلب في الدخول، والاتجاه الذي يرى بعدم ضرورته. انتهينا إلى أن حجج الاتجاهين تتحطم مع صراحة النص الذي جاء به المشرع فالأخير لم يتطلب في النظام صفة معينة الأمر الذي ينبغي على ضوئه عدم إضافة شرط لم يتضمنه النص ولم يفصح عنه المشرع، وإذا كان هناك من يدفع بهذا الاتجاه فإن الأخذ به يعني مخالفة لإرادة المشرع الصريحة ولقواعد وأصول التفسير الذي ينبغي أن يلتزم بها المفسر أياً كان، وأهمها الإلتزام بإرادة المشرع التي عبرت عنها عبارات النصوص وعدم إضافة قيود لم ينص عليها فلا ينبغي تقييد مطلق أو تخصيص عموم نص من غير سند قانوني لأن المشرع إذا أراد قال.

وفي إطار بياننا النشاط الذي يحقق الدخول والوسائل التي يمكن أن يتوسل بها الجاني في سبيل ذلك وجدنا أن الدخول في النظام يتحقق بالاتصال به بأي وسيلة من الوسائل المتاحة والتي تمكن الجاني من ذلك مما يعني عدم تقييد ارتكاب الجريمة بوسائل معينة غير ما تقتضيه طبيعة النظام وإمكان الاتصال به بحيث يكون النظام أو الجزء الذي تعرض للنشاط المجرم مفتوحاً بعد أن كان مغلقاً أو أن يكون قد تم تشغيله بعد أن كان مطفأً لأن الدخول للنظام لا يمكن أن يكون إلا والنظام في حالة اشتغال حتى ولو استخدم الجاني وسائل الاتصال عن بعد الأمر الذي بينا من خلاله ضرورة أن يقوم الجاني بتشغيل النظام إذا ما كان الأخير في حالة سبات. كما وجدنا أن الدخول يتم عن طريق الغش عندما يكون من شخص ليس له الحق في إجرائه بعد أن رفضنا اعتبار الوسائل الفنية والتقنية المعيار الذي يمكن الاستناد إليه لتحقق الاتصال بطريق الغش وقدمنا المبررات لرفضنا ذلك.

وانتهينا أيضاً إلى أن جريمة الدخول جريمة عمدية ورفضنا الاتجاه الذي ينادي بإمكان تحقق جريمة الدخول عن طريق الغش في حالة أن يكون الدخول تم عن طريق الصدفة أو الاعتقاد الخاطيء وبينا الأسانيد القانونية التي تدعم رأينا من حيث قواعد القصد وما تقتضيه من معاصرة القصد للحظة ارتكاب السلوك المجرم أو من

حيث مخالفة ذلك لطبيعة الجريمة وكان لنا أن نبحث في أثر الضرر الذي يمكن أن يترتب على الدخول وموقف المشرع منه فوجدنا أن للضرر أثر سواء من حيث طبيعة الجريمة أو من خلال العقاب، حيث اعتبر المشرع الضرر الذي يصيب النظام ظرفاً مشدداً يستوجب تشديد العقاب سواءً بمحو المعلومات والبرامج أو بالتعديل بها أو بالتأثير على تشغيل النظام الآلي وهذا يؤيد منهج المشرع في اعتبار جسامة النتيجة معياراً لتشديد العقاب الأمر الذي استندنا إليه في القول بتأثر طبيعة الجريمة بالضرر، وبعد أن حددنا مدلول كل سلوك انتهينا إلى أن المشرع لم يفرق في العقاب في إطار ذلك مع تفاوت تلك التصرفات في الخطورة.

وفي خاتمة المطاف لا ننكر أن النص الذي جاء به المشرع الفرنسي بصدد جريمة الدخول بشكل خاص والجرائم الأخرى التي توجه للنظام الآلي بشكل عام يمكن أن تكون نموذجاً يحتذى به في هذا المجال ولكننا من الممكن أن نضع تصورنا لهذه الجريمة في حالة نهج المشرع العراقي هذا النهج بحيث يكون نصنا المقترح كالآتي:(يعاقب بالحبس لمدة لا تزيد عن سنتين وبالغرامة أو بإحدى هاتين العقوبتين كل من دخل إلى نظام آلي مع علمه بإنعدام حقه بالدخول، وتكون العقوبة الحبس بما لا يقل عن سنتين وبغرامة تعادل ثلاثة أمثال الضرر إذا نشأ عن الدخول ضرر، وتكون العقوبة السجن إذا أدى الدخول إلى تعطيل نظام تشغيل مؤسسة أو مصلحة حكومية أو تساهم الحكومة بنصيب فيها وتكون العقوبة السجن بما لا يقل عن سبع سنوات إذا أدى تعطيل النظام الآلي إلى تعطيل عمل المؤسسة أو المصلحة أو التأثير على اشتغالها).

مراجع البحث

١. د. أحمد حسام طه تمام – الجرائم الناشئة عن استخدام الحاسب الآلي – دراسة مقارنة – رسالة دكتوراه – دار النهضة العربية – ٢٠٠٠.

٢. د. أحمد فتحي سرور – الوسيط في قانون العقوبات – الجزء الأول – القسم العام – دار النهضة العربية ١٩٨١.

٣. جميل عبد الباقي الصغير القانون الجنائي والتكنلوجيا الحديثة – الجرائم الناشئة عن استخدام الحاسب الآلي – دار النهضة العربية القاهرة ١٩٩٢.

٤. سرحان سليمان داود، ومحمود عبد المنعم المشهداني – أمن الحاسوب والمعلومات – دار وائل للطباعة والنشر – الأردن – ٢٠٠١.

٥. د. عبد الفتاح بيومي حجازي الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنيت. دار الكتب القانونية – ٢٠٠٢.

٦. عبد اللطيف بن عبد الرحمن الهريش – بعيداً عن الاكتفاء بالمعالجة التقليدية: جرائم الحاسب الآلي بحاجة للتنظيم والنصوص القانونية لا تزال قاصرة عن تغطيتها – منشور في مجلة الرياض الأربعاء ١٦ نيسان (أبريل) ٢٠٠٣ الموافق ١٤ صفر ١٤٢٤ هجري العدد ١٢٧١٧ السنة ٣٨ لاحظ موقعها على الانترنيت http://www.alriyadh-np.com

٧. عماد علي الخليل – الحماية الجزائية لبطاقات الوفاء – دار وائل للنشر – الأردن عمان – ط الأولى – ٢٠٠٠.

٨. د. عمر أحمد حسبو – حماية الحريات في مواجهة نظم المعلومات – دراسة مقارنة – دار النهضة العربية – القاهرة – ٢٠٠٠.

٩. د. عمر الفاروق الحسيني – المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية – ط/الثانية – ١٩٩٥.

١٠. علي حسين الخلف، وسلطان الشاوي – شرح الأحكام العامة في قانون العقوبات – مطابع الرسالة – الكويت – ١٩٨٢.

١١. د. علي عبد القادر القهوجي – الحماية الجنائية لبرامج الحاسب الآلي – الدار الجامعية للطباعة والنشر – الاسكندرية – ١٩٩٩.

١٢. د. عوض محمد – الوجيز في قانون العقوبات – القسم العام – الجزء الأول – دار المطبوعات الجامعية – ١٩٧٨.

١٣. د. عوض منصور محمد أبو النور – مقدمة في علم الحاسب الإلكتروني – وبرمجة بيسك – دار الأمل – أربد – الأردن ط/الخامسة ١٩٩٦.

١٤. د. فايز نعيم رضوان – بطاقات الوفاء – مكتبة الجلاء الجديدة – المنصورة – ١٩٩٠.

١٥.د. فخري عبد الرزاق الحديثي – قانون العقوبات – القسم العام – مطبعة الزمان – بغداد ١٩٩٢.

١٦.فداء يحيى أحمد الحمود – النظام القانوني لبطاقة الأئتمان – دار الثقافة للطباعة والنشر – الأردن – عمان – ١٩٩٩.

١٧.كرستان كروملش، روبرت كورت وآخرين – الانترنيت بدون خبرة – إعداد د. خالد العامري – قسم الترجمة بدار الفاروق – مصر – القاهرة ط/الثانية ٢٠٠٠.

١٨.محمد أحمد عبابنة – جرائم الحاسب الآلي وأبعادها الدولية – دار الثقافة للنشر والتوزيع – الأردن – عمان – ٢٠٠٥.

١٩.د. محمد حسام محمود لطفي – الحماية القانونية لبرامج الحاسب الإلكتروني – دار الثقافة للطباعة والنشر – القاهرة – ١٩٨٧.

٢٠.محمد حماد مرهج

- الخطأ المفترض في المسئولية الجنائية رسالة دكتوراه مقدمة إلى كلية القانون – جامعة بغداد – ١٩٩٦ – مسحوبة على الرونيو

- التكنلوجيا الحديثة والقانون الجنائي – دار الثقافة للطباعة والنشر – الأردن عمان – ٢٠٠٤ ص١٤٣ وما بعدها.

- الصعوبات التي تعترض تطبيق نصوص جريمة السرقة على برامج الحاسب الآلي – مجلة الشريعة والقانون – تصدر عن مجلس النشر العلمي جامعة الإمارات العربية – العدد العشرون – ذو القعدة ١٤٢٤هـ يناير ٢٠٠٤م.

- مبررات الحماية الجنائية لبرامج الحاسب الآلي – مجلة العلوم الإنسانية والاقتصادية – جامعة الأنبار – العدد السادس نيسان / ٢٠٠٥.

٢١.د. محمود نجيب حسني – شرح قانون العقوبات اللبناني – القسم العام – دار النهضة العربية – بيروت – ١٩٨٤.

٢٢.مراد شلباية – علي فاروق – مقدمة إلى الانترنيت – دار المسيرة للنشر والتوزيع – الأردن – عمان ط/الأولى ٢٠٠١.

٢٣.د. هدى حماد قشقوش جرائم الحاسب الآلي في التشريع المقارن دار النهضة العربية – القاهرة – ١٩٩٢.

٢٤.يونس عرب – الخصوصية وأمن المعلومات في الأعمال اللاسلكية بواسطة الهاتف الخلوي – ورقة عمل مقدمة إلى منتدى العمل الإلكتروني بواسطة الهاتف الخلوي الذي عقدت برعاية اتحاد المصارف العربية للفترة من ٢٠ – ٢٢ أيار ٢٠٠١ في الأردن عمان – فندق المرديان – ص١٦ لاحظ الموقع على الانترنيت http://www.arablaw.com

٢٥.يونس عرب – جرائم الكومبيوتر والانترنيت – المعنى والخصائص واستراتيجية المواجهة القانونية – الفقرة ١–٣ الموقع على الانترنيت

http://www.araplaw.com.

26. ANTHONY, HOOPER, Harriss criminal law sweet MAXWELL, twenty First edition London 1968.

27. D.W Elliot. J.C Wood A Case book in criminal law third edition Maxwel 1974.

28. GBREMOND, LA REVOLUTION INFORMATIQUE DICITIONNAIRE. The matique edition HATIER 1982.