جامعة آكلي محند أولحاج –البويرة

كلية الحقوق والعلوم السياسية

قسم : القانون العام

جريمة الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات

مذكرة تخرج لنيل شهادة ماستر في الحقوق

تخصص: قانون جنائي وعلوم جنائية

من إعداد الطالبة:

- حساين ليلية

تحت إشراف الأستاذة:

- د. لوني نصيرة

لجنة المناقشة

الاستاذ: د. لونيسي علي.....جامعة البويرة .....رئيسا

الأستاذة: د. لوني نصيرة.....جامعة البويرة.....مشرفا ومقررا

الأستاذة: د. خليفي سمير .....جامعة البويرة.....ممتحنا

تاريخ المناقشة: 2019/11/13

شكر وعرفان

الحمد لله عظيم فضله وعطائه لأنه وفقني لإتمام هذا العمل

فإنه يشرفني أن أتقدم بخالص شكري وتقديري واحترامي لأستاذتي الفاضلة الدكتورة "لونيي نصيرة" على كل ما قدمته لي من يد المساعدة والعون لإنجاز هذا العمل

عبر تشجيعها وتوجيهاتها القيمة لي

كما لم تبخل علينا بتقديم النصح والإرشاد، فلكي مني ألف تحية وجزاكي الله بكل خير.

كما أتقدم بأسمى عبارات الشكر والعرفان إلى أساتذتي الكرام

أعضاء لجنة المناقشة المحترمين لقبولهم مناقشة هذا العمل

إهداء

أهدي ثمرة عملي المتواضع.....

إلى الوالدين الكريمين أطال الله في عمرهما

إلى أخوتي وأخواتي

وإلى كل من أمد لي يد العون...

مقدمة

مقدمة:

يشهد العالم منذ منتصف القرن العشرين ثورة جديدة اصطلح على تسميتها بالثورة المعلوماتية وذلك إشارة إلى الدور البارز الذي أصبحت تلعبه المعلومات في الوقت الراهن فقد أصبحت قوة لا يستهان بها في أيدي الدول والأفراد وكان التطور الهائل الذي يشهده قطاع تكنولوجيا المعلومات والاتصال المحور الأساسي الذي قامت عليه هذه الثورة.

ومما لا شك فيه أن الثورة المعلوماتية ونتيجة للتقنيات العالية التي تقوم عليها والتي تتمثل في استخدام الحواسيب والشبكات المعلوماتية التي تربط بينها قد تركت آثارًا ايجابية وشكلت قفزة نوعية في حياة الأفراد والدول حيث تعتمد القطاعات المختلفة في الوقت الحالي في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية نظرًا لما تتميز به من عنصري السرعة والدقة في تجميع المعلومات وتخزينها ومعالجتها ومن نقلها وتبادلها بين الأفراد والشركات والمؤسسات المختلفة داخل الدولة الواحدة أو بين عدة دول فأصبحت هذه الأنظمة مستودعا لأسرار الأشخاص المتعلقة بحياتهم الشخصية أو بطبيعة أعمالهم المالية والاقتصادية.

إلاّ أنّ هذا الجانب المشرق الإيجابي لعصر المعلوماتية لا ينفي الانعكاسات السلبية التي أفرزتها هذه التقنية العالية والمتمثلة في إساءة استخدام الأنظمة المعلوماتية واستغلالها على نحو غير مشروع بصورة تضر مصالح الأفراد والجماعات وبالتالي تضر بمصلحة المجتمع ككل، مما أدى إلى تفشي طائفة من الظواهر الإجرامية المستحدثة، ومن بين الجرائم المعلوماتية جريمة الدخول والبقاء غير المشروع إلى نظام المعالجة الآلية للمعطيات وهي جريمة تمس بأنظمة المعالجة، أي المعلومات والبيانات الموجودة داخل أجهزة الإعلام وتكون هذه المعلومات محمية بشفرة حيث أن المجرم يقوم بالدخول إليها وذلك دون الحصول

على تصريح من صاحب النظام ويمكن لهذه الجريمة أن تقوم بصفة مستقلة، أي قيام جريمة الدخول منفصلة عن جريمة البقاء كما يمكن أيضا قيامها بصفة لصقية.

وتكمن أسباب اختيار هذا الموضوع في الرغبة الشخصية لدراسة الجريمة المعلوماتية وبالأخص جريمة الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات كذلك حب الإطلاع على مجال الجرائم التي تقع داخل شبكة المعلومات إضافة إلى معرفة هذه الجريمة بالتفصيل وتسليط الضوء على القوانين التي تحكم هذه الجرائم.

أما الأسباب الموضوعية تتوضح في أنّ هذه الجريمة من الجرائم المستحدثة التي تقع على نظام المعالجة الآلية للمعطيات أي أن المعطيات تكون محمية ومخزنة داخل أجهزة الإعلام الآلي.

والهدف من دراستها هو التعرض لكل جوانبها باعتبارها جريمة معلوماتية مستحدثة فالهدف منها الوقوف على الدور المهم الذي تلعبه الجريمة داخل نظام المعالجة الآلية للمعطيات بالإطلاع عليها وتحديد أهم الأحكام التجريمية من خلال أهم القوانين الدولية.

جريمة الدخول والبقاء من الجرائم التي تستهوي مرتكبيها للإعتداء علي سرية الحياة الخاصة سواء تمس شخص طبيعي أو معنوي، كما أنها لا تزال تثير اهتمام الباحثين في القانون الدولي بحيث نصت عليها الكثير من الاتفاقيات الدولية لمحاربتها ومواجهة العوائق التي تقف في وجه السير الحسن لهذه الأخيرة فإنتشار هذا النوع من الجرائم على المستوى الداخلي والخارجي وارتباطها ببعض الجرائم الأخرى منها جريمة التلاعب بالمعطيات كل ذلك تطلب استحداث قوانين تتولى دراسة مجال الجرائم المعلوماتية.

وتظهر كذلك أهمية هذا الموضوع في دراسة هذه السلوكات التي تقع في مجال الجرائم المعلوماتية وتحديد مجال الإجرام وزوايا مكافحته ولما يشكله من اعتداء على

المعلومات المخزنة، كما تتجلى أهمية هذه الجريمة في كونها جريمة مستحدثة وعابرة للحدود الوطنية، ما استدعى تسليط الضوء عليها وتوضيح ماهيتها القانونية لاسيما في ظل وقوعها في بيئة افتراضية. ومنه نطرح الإشكالية التالي: **ما المقصود بجريمة الدخول والبقاء ؟ وما هو الإطار القانوني لهذه الجريمة؟**

بغرض دراسة هذا الموضوع والإجابة على هذه الإشكالية اعتمدنا في بحثنا على منهجين علميين يتمثل المنهج الأول في المنهج التحليلي وذلك من خلال تحليل ودراسة النصوص القانونية التي تنص على جريمة الدخول والبقاء ومعاقبة مرتكبي هذه الجريمة، وكذلك استعنا في دراستنا هذه بالمنهج المقارن وذلك من خلال تمييز جريمة الدخول عن الأفعال المشابهة لها وأيضا تمييز جريمة الدخول عن جريمة البقاء.

وعليه سيتم دراسة موضوعنا هذا بالاعتماد على تقسيم خطتنا إلى فصلين يندرج تحت كل فصل مبحثين كما مبين:

الفصل الأول: يتمثل في ماهية جريمة الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات، الذي قسمناه إلى مبحثين المبحث الأول تناولنا فيه ماهية جريمة الدخول غير المشروع. والمبحث الثاني تناولنا فيه ماهية جريمة البقاء غير المشروع، في حين خصصنا **الفصل الثاني لدراسة الإطار القانوني لجريمتي الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات،** في المبحث الأول أركان جريمة الدخول والبقاء غير المشروع، أما المبحث الثاني فتطرقنا دوافع ارتكاب جريمة الدخول والبقاء والعقوبات المقررة لها.

الفصل الأول

ماهية جريمة الدخول والبقاء غير المشروع

لنظام المعالجة الآلية للمعطيات

الفصل الأول

ماهية جريمة الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات

يستوجب لقيام جريمة الدخول والبقاء إلى أنظمة المعالجة الآلية للمعطيات توافر معلومات مخزنة داخل النظام المعلوماتي، حيث تقع جريمة الدخول في حالة عدم حصول الجاني على تصريح من صاحب المعلومات ودخوله إليها دون علمه أو دون السماح له بذلك.

وتقعجريمة البقاء في حالة حصول الجاني على التصريح بالدخول وبقاءه داخل هذه المنظومة وتجاوز الوقت المصرح به أو التجاوز إلى أجزاء أخرى.

ولدراسة هذه الجريمة لابد من الإحاطة بالإطار ألمفاهيمي لها وتوضيح صور كل جريمة على حدى وذلك من خلال العناصر التالية:

المبحث الأول: جريمة الدخول غير المشروع لنظام المعالجة الآلية للمعطيات

المبحث الثاني: جريمة البقاء غير المشروع في نظام المعالجة الآلية للمعطيات.

المبحث الأول

جريمة الدخول غير المشروع لنظام المعالجة الآلية للمعطيات

لقد تعرضت الكثير من الأنظمة المعلوماتية إلى الإختراق بواسطة أشخاص غير مصرح لهم بالدخول إليها، وقد أطلق على هؤلاء الذين يدخلون إلى أنظمة الكمبيوتر بدون تصريح بالقراصنة.

وأطلق مصطلح القرصنة[1] في أول الستينات من القرن الماضي على المبرمج الماهر القادر على التعامل مع الحاسب الآلي ومشاكله بخبرة ودراية حيث أنه كان يقدم حلول لمشاكل البرمجة بشكل تطوعي وقد أقر القضاء الفرنسي مجموعة من المبادئ التي يجب إعمالها في حالة دخول أحد الأشخاص للمواقع الإلكترونية والإطلاع على بياناتها وتتلخص في: [2]

- استئذان أو إخطار صاحب الموقع المراد استغلال البيانات أو المعلومات الموجودة في موقعه.
- إحترام القوانين واللوائح التي تحكم حق الملكية الذهنية.

وفي هذا المبحث سنتناول مفهوم جريمة الدخول غير المشروع لنظام المعالجة الآلية للمعطيات (المطلب الأول)، وسنتعرض إلى صور وآليات جريمة الدخول غير المشروع لنظام (المطلب الثاني).

---

[1]- **القرصنة:** كلمة توصف المختص المتمكن من مهارات في مجال الحاسوب وأمن المعلوماتية وأطلقت كلمة هاكر أساسا على مجموعة من المبرمجين الأذكياء الذين كانوا يحاولون اقتحام الأنظمة المختلفة وليس بالضرورة أن تكون في نيتهم ارتكاب جريمة ولكن نجاحهم في الاختراق يعتبر نجاحا لقدراتهم ومهاراتهم، إلا أنّ القانون اعتبرهم دخلاء تمكنوا من دخول مكان افتراضي لا يجب أن يكونوا فيه والقيام بهذه العملية اختيارية يمتحن فيه المبرمج قدراته دون أن يعرف باسمه الحقيقي.

[2]- خالد ممدوح إبراهيم الجريمة المعلوماتية الطبعة الأولى، دار الفكر الجامعي مصر 2009 ص241

المطلب الأول

مفهوم جريمة الدخول غير المشروع لنظام المعالجة الآلية للمعطيات

يقصد بكلمة الدخول في المجال المعلوماتي كافة الأفعال التي تسمح بالولوج إلى نظام معلوماتي والسيطرة على المعطيات التي يتكون منها والخدمات التي يقدمها ومادام الدخول هو الركن المادي لجريمة فعل الدخول عن طريق الغش فلابد أن نتطرق لتعريف جريمة الدخول غير المشروع، أما في الفرع الثاني فسنتناول من خلاله تقنيات ارتكاب جريمة الدخول غير المشروع لنظام المعالجة الآلية للمعطيات.

الفرع الأول: تعريف جريمة الدخول غير المشروع لنظام المعالجة الآلية للمعطيات:

تقوم هذه الجريمة بتحقيق فعل الدخول إلى النظام المعلوماتي ومدلول كلمة الدخول تشير إلى كل الأفعال التي تسمح بالولوج إلى نظام معلوماتي والإحاطة أو السيطرة على المعلومات على المعطيات والمعلومات التي يتكون منها[1].

وكلمة الدخول والتي تقابلها باللغة الفرنسية Accéder والتي تعني النفاذ أو الاختراق لمكان مادي وهو الذي لا يمكن تطبيقه بشأن الدخول إلى أنظمة المعالجة الآلية للمعطيات لأن الدخول إليها هو ظاهرة غير مادية وعليه فالمقصود بالدخول الولوج إلى المعلومات والمعطيات المخزنة داخل نظام الحاسب الآلي بدون رضا المسؤول عن هذا النظام وإساءة استخدام النظام عن طريق شخص غير مرخص له بذلك، ويكفي أن يكون الدخول غير مشروع أو كما عبر عليه المشرع عن طريق الغش فالدخول له طبيعة

1 - نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان 2008، ص158

معنوية غير مادية أي أنه يختلف عن مفهوم الدخول كما هو متصور في العالم المادي وهي الحقيقة التي تتفق مع العالم المعلوماتي[1].

ولم يحدد المشرع الجزائري صفة معينة من يقوم بعملية الدخول هذه إذ أن المادة 394 مكرر من قانون العقوبات جاءت عامة بنصها: " كل من يدخل أو يبقى عن طريق الغش..." سواء كانت لديه القدرة الفنية على الإستفادة من هذا النظام أم لا ويكفي ألا يكون من أولئك الذين لهم حق الدخول إلى هذا النظام[2].

كما أنه لم يشترط أن يتم الدخول بوسيلة أو طريقة معينة فالمادة السابق ذكرها جاءت شاملة لكل طرق الدخول ولو تحدد طريقة يعينها وذلك على غرار ما أتى ذكره المشرع الفرنسي طبقا لنص المادة 123-1 من قانون العقوبات الفرنسي سواء كانت عن طريق كلمة سر أو شفرة أو برنامج ويكفي أن تكون الوسيلة غير مشروعة أو كما عبر عليها المشرع بطريقة الغش خاصة مثل هذا الإجرام المرتبط بتقنيات عالية تتطور وتتغير وسائلها من يوم لآخر وهو ما حرص عليه المشرع عند سنه لمثل هذا القانون.

أما قانون العقوبات الجزائري كأغلب التشريعات لم يقدم تعريفا للدخول فهو ينص على هذه الكلمة دون إعطاء معنى لها.

الفرع الثاني: تقنيات ارتكاب جريمة الدخول والبقاء غير مشروع.

من أكثر التقنيات استخداما لإرتكاب جريمة الدخول غير المشروع لنظام المعالجة نذكر منها:

1- استخدام البرنامج المخصص لتخطي أنظمة الحماية الفنية في الحالات الطارئة وحالات اختلال وظائف الحاسوب أو توقفه عن العمل.

---

[1]- بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير في القانون الجنائي، جامعة وهران، كلية الحقوق والسياسية، 27-06- 2013، 2012-2013، ص 67.

[2]- القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، ص10.

2- تقنية أبواب المصيدة (Traps-doors): يقوم واصفي البرامج بترك فواصل في البرامج أثناء إعدادها تسمى أبواب المصيدة تستخدم في إضافة ما يحلوا لهم من أوجه التلاعب.

3- صناديق القمامة (poubelle) : إعادة استخدام الملحقات الموجودة في كل من أوراق الكربون أو الأوراق العادية التي تحتوي على بيانات التي تم التخلص منها برميها بصندوق القمامة.

4- طريقة المختصر(La raccourci): ويتمثل في استغلال نقاط الضعف الخاصة بالنظام الداخلي للوقاية.

5- طريقة القناع (La déguisement): وذلك بأن يقوم القرصان بإقناع الحاسوب بأنه شخص مرخص له بالدخول وقد يعتمد الشخص إلى كسر إجراءات الحماية التقنية للنظام بتجاوز كلمة السر أو التوصل لنقطة الضعف في نظام حماية البرامج أو النفاذ منها[1].

الفرع الثالث: اختلاف جريمة الدخول عن استعمال النظام

يمكن القول بصفة عامة أن الدخول غير المشروع إلى أنظمة المعالجة الآلية للمعطيات يتحقق بالوصول إلى المعلومات والبيانات المخزنة داخل نظام الحاسب ومنه نجد بأن الدخول يختلف عن بعض الأفعال المشابهة له مثلا اختلاف الدخول عن استعمال النظام ففكرة الدخول تختلف عن استعمال النظام وبالتالي فإن المشرع إذ جرم الدخول فإن ذلك لا يعني أن يقوم الفاعل باستعمال الجهاز فدائرة الدخول أضيق من دائرة الاستعمال، فكل استعمال لنظام دون رضا يشكل دخولا بلا ريب.

[1]- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الأولى، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2006، ص 108.

أما الدخول فإنه لا يعني بالضرورة استعمال النظام فقد يتصل الشخص بالنظام ومن ثم يكون قائما بالدخول ولكنه لا يستعمل إمكانيات النظام، كأن يكتفي بالإطلاع على النظام بوسائل سلكية أو لاسلكية أو باستعمال برامج خاصة بالإقتحام والفاعل يكتفي عندئذ بالإطلاع دون استعمال النظام[1]، لذلك حرصت بعض التشريعات مثل التشريع الكندي على تجريم استعمال النظام بدون رضا صاحبه فينص التشريع الكندي على عقاب:" كل من يسوء نية وبدون وجه حق":

- يحصل بطريق مباشر أو بطريق غير مباشر على خدمة من خدمات الكمبيوتر.

- يستعمل أو يتسبب في استعمال بطريق مباشر أو غير مباشرة نظام الكمبيوتر بنية ارتكاب الجريمة[2].

المطلب الثاني

الصور والآليات جريمة الدخول غير المشروع لنظام المعالجة الآلية للمعطيات

يتحقق فعل الدخول غير المشروع متى كان مخالفا لإدارة صاحب النظام أو من له حق السيطرة عليه كذلك الأنظمة المتعلقة بأسرار الدولة أو دفاعاتها أو تتضمن بيانات شخصية تتعلق بحرمة الحياة الخاصة بحيث لا يجوز الإطلاع عليها[3].

ومن خلال هذا المطلب سنتطرق إلى صور جريمة الدخول في الفرع الأول، كما سنعمل على سنوضح في الفرع الثاني آليات جريمة الدخول غير المشروع.

---

[1]-خالد ممدوح إبراهيم، مرجع سابق، ص ص 250-251.

[2]-غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والأنترنت، دار الفكر والقانون مصر، 2010، ص142.

[3]- أسامة أحمد مناعسة، جلال محمد الزعبني، جرائم تقنية المعلومات الالكترونية الطبعة الثانية، دار الثقافة للنشر والتوزيع الأردن 2014 ص 288.

الفرع الأول: صور وآليات جرائم تقنية نظم المعلومات

يمكن أن تقع جريمة الدخول الغيرمشروع من خلال صورتين وهذا ما يتوضح لنا من خلال الفرع الأول الذي سنتناول فيه حالة عدم وجود التصريح بالدخول إلى نظام المعلوماتية أو تجاوز حدوده (أولا)، وحالة تجاوز حدود التصريح وهذا ما سنتعرض إليه من خلاله (ثانيا).

أولا: حالة عدم وجود التصريح للدخول إلى نظام المعلوماتية

بمعنى أن الشخص الذي أقدم على الدخول إلى النظام المعلوماتي لا يجوز على تصريح يخول له القيام بذلك مطلقا وسواء كان هذا الترخيص يتوقف على سداد مبلغ معين للإشتراك أو يتوقف على العضوية في جهة معينة أو غير ذلك من الشروط أو كان الدخول إلى النظام ممنوعا على الإطلاق.

ويمكن أن نميز بين ثلاثة طوائف من الأشخاص الذين يدخلون نظام المعلوماتية بدون ترخيص:

الطائفة الأولى: وتشمل الأشخاص الذين لا تربطهم بنظام المعلوماتية أية صلة وظيفية بالمؤسسة المسؤولة عن هذا النظام.

الطائفة الثانية:وتشمل الأشخاص المرخص لهم بالدخول إلى هذا النظام. [1]

الطائفة الثالثة: وتشمل الأشخاص الغير مرخص لهم بالدخول إلاّ أنهم بحكم عملهم داخل المؤسسة لديهم من الناحية الفنية نتيجة تواجدهم في موقع أو ظروف تسهل لهم الدخول إلى النظام.[2]

---

[1]- بوخبزة عائشة، مرجع سابق، ص 69.

[2]- بوخبزة عائشة، مرجع سابق، ص70.

ثانيا: حالة تجاوز حدود التصريح

كأن يقوم الشخص الذي خول له التصريح بالدخول للأنظمة المعلوماتية يتجاوز الحدود التي رسمت له بموجبها، وتتم هذه الحالة عموما من طرف العاملين في المؤسسة المسؤولة عن النظام التابع لها، فهم يمتلكون عادة تصريح جزئي بالدخول يشمل مناطق محددة من النظام بحسب الوظيفة التي يؤديها كل عامل وما إذا كان يملك تصريحا بالدخول إلى النظام ككل أو جزء منه.

فتجاوز حدود التصريح يقصد به التجاوز المكاني ليمتد إلى مجالات غير مرخص للفاعل بدخولها، أما التجاوز الزماني فإنه يخرج عن هذا النطاق ويدخل في حالة البقاء الغير مصرح به. [1]

ومن أهم الإشكالات التي تثيرها مسألة تجاوز حدود التصريح هي مسألة التأكد من مدى توافر القصد الجنائي لدى الفاعل في تجاوز حدود التصريح الممنوح له من عدمه لأن هناك حالات يتم فيها الدخول عن طريق الخطأ أو صدفة خصوصا في الحالات التي لم تحدد فيها المؤسسة من له الحق من العمال التابعين لها في الدخول إلى النظام من عدمه أو أنها لم تحدد صلاحية كل عامل تابع لها بدقة.

الجدير بالإشارة أن نص المادة 394 مكرر من قانون العقوبات الجزائري تنص على:"الدخول عن طريق الغش"، أي أن المقصود بها الدخول في حد ذاته الذي يتم بغير وجه حق أو عن طريق الغش وليس ما يحصل بعد هذا الدخول من إلتزام بحدود التصريح أو تجاوزه.[2]

---

[1]- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2005، ص349.

[2]- بوخبزة عائشة، مرجع سابق، ص 70.

الفرع الثاني:آليات جريمة الدخول غير المشروع

من خلال هذا الفرع سنتطرق إلى عنصرين أساسيين هما طرق الدخول غير المشروع ووسائل الدخول الغير المشروع.

أولا: طرق الدخول غير المشروع

تتحقق جرائم الاعتداء أو اختراق جهاز الكمبيوتر أو المواقع في الشبكة المعلوماتية بطريقة غير مباشرة يدخل الجاني لصفحات المواقع الالكتروني والاطلاع على البيانات الموجودة فيها دون أن يكون مصر حاله بذالك ونجد بان هناك طريقتين للدخول : الدخول المباشر والدخول الغير مباشر.[1]

1. **الدخول المباشر:** وفقا لهذه الطريقة فإن الجاني يستطيع الاستيلاء على المعلومات المخزنة داخل الأنظمة المعلوماتية بعدة طرق:
   - باستخدام شاشة النظام و الاطلاع بالقراءة على ما هو مكتوب.
   - باستخدام مكبر الصوت أو سماعات الالتقاط المعلومات والبيانات المعالجة ويعد هذا النوع.
   - باستخدام آلة طباعة لاستخراج المعلومات المكتوبة على الورق.

2- **الدخول الغير مباشر:** أدى ظهور التقنيات الحديثة التي لها صلة بالنظام ألمعلوماتي مثل شبكات الاتصال البعيدة وأيضا المعالجة عن بعد إلى نشؤ مخاطر جديدة نتيجة للإمكانيات المستحدثة للولوج والاستفسار عن بعد من المراكز المعلوماتية إلا أن المعلومات أثناء حركتها أو بثها تكون مهددة في كل لحظة بالالتقاط أو التسجيل غير المباشر[2].

---

[1]-حنان ريحان مبارك المضحكي، الجريمة المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2014، ص 110.

[2]-أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، مصر، 2006، ص ص 190-191.

ثانيا: وسائل الدخول غير المشروع لنظام المعالجة الآلية للمعطيات: هناك عدة وسائل

تختلف الوسائل التي يمكن اللجوء إليها للدخول غير المشروع إلى نظام الكمبيوتر ففي بعض الأحيان لا يتطلب الدخول أكثر من تشغيل جهاز الكمبيوتر أو فتح البرنامج الذي يقوم بتشغيله وقد يتطلب الحصول على الشفرات الخاصة بالدخول باستخدام جهاز لفك الشفرة والدخول عن طريق وسائل أخرى للدخول لأنظمة الحاسبات الآلية على ضعف الأنظمة ذاتها أو على بعض الأخطاء الناجمة عن عملية البرمجة[1].

أ)- تشغيل كمبيوتر مقفول: تتمثل هذه الطريقة في أن المتهم يقوم بفتح جهاز الكمبيوتر وتشغيله بعد أن كان مغلقا فإذا ما بدأ العمل فإن المتهم يعتبر قد دخل النظام بدون وجه حتى، طالما تم ذلك دون موافقة صاحب الحق في ذلك.

ونرى بأن العبرة ليست بتشغيل الجهاز ولكن بالتمكن من الدخول إلى الملفات إذ قد يتمكن المتهم من الدخول إلى الملفات الموجودة داخل الجهاز على الرغم من أن الجهاز مقفل، كما أنه قد يتمكن من تشغيل الجهاز وذلك بإيصال الكهرباء إليه دون أن يتمكن من الدخول إلى الملفات[2].

ب)- استعمال كمبيوتر مفتوح: قد يكون جهاز الكمبيوتر قيد الإستعمال ممن له الحق في ذلك فإذا تغافل عنه أو انشغل وقام شخص آخر باستعماله وذلك بأن فتح ملفات موجودة فيه فإنه بذلك يكون قد دخل في هذا النظام ويقع منه النشاط المعاقب عليه ويختلف هذا الغرض عما لو كان الكمبيوتر قيد الاستعمال واكتفى المتهم بالنظر إلى الملف الذي كان مفتوحا أمام المستخدم[3]، وأن غالبية محاولات اختراق النظر المعلوماتية

---

[1]-خالد ممدوح إبراهيم، مرجع سابق، ص246.

[2]-شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، مصر، 2007، ص107.

[3]-شيماء عبد الغني محمد عطا الله، مرجع نفسه، ص108.

تتم من خلال برامج متوفرة على الأنترنت يمكن لمن له خبرات تقنية متواضعة أن يستخدمها لشن هجماته على أجهزة الغير[1].

ويمكن أن تقوم جريمة الدخول أيضا بعدة وسائل أخرى نذكرها منها:

- الدخول إلى كمبيوتر عن طريق استعمال كارت تشغيل ينتمي إلى شخص آخر.
- الدخول إلى كمبيوتر عن طريق خط تليفوني.
- الدخول من كمبيوتر إلى كمبيوتر آخر.
- الدخول إلى نظام متصل بنفس الكمبيوتر بدائرة واحدة.
- التجسس على النظام بعد اقتحامه.

[1]- خالد ممدوح إبراهيم، مرجع سابق، ص108.

المبحث الثاني

ماهية جريمة البقاء غير المشروع في نظام المعالجة الآلية للمعطيات

يرى البعض أن البقاء الغير مصرح به داخل نظام الحاسب الآلي لا يقتصر فقط في حالة الدخول إلى نظام غير مصرح بالدخول إليه على سبيل الخطأ والبقاء داخل النظام على الرغم من العلم بذلك وإنما ينطبق أيضا على حالة الدخول إلى نظام الحاسب الآلي لموافقة المسؤول عن النظام[1].

على الرغم من أن هذه الجريمة الغالب أن تتحقق في حالة الإتصال الذي يقع عن طريق الخطأ فإن ما يبدو لنا أنها تتسع وفق اعتقادنا إلى حالة الإبقاء على الإتصال بعد إنتهاء الوقت المسموح به لإستخدام البرنامج والإستفادة منه[2]، فمجرد الدخول لا يعني أنه يقصد البقاء في النظام والإطلاع على البيانات والمعلومات بصورة غير مشروعة[3].

من خلال المبحث نستعرض لمطلبين: (المطلب الأول) مفهوم جريمة البقاء و(المطلبالثاني) صور وأساليب جريمة البقاء.

---

[1]- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2005، ص147.

[2]- محمد حماد مرهج الهيتي، جرائم الحاسوب ، الطبعة الأولى دار المناهج للنشر والتوزيع ، الأردن 2006، ص190 .

[3]–حنان ريحان مبارك المضحكي، مرجع سابق، ص112.

المطلب الأول

مفهوم جريمة البقاء غير المشروع لنظام المعالجة الآلية للمعطيات

جريمة البقاء نصت عليها المادة 394 مكرر من قانون العقوبات[1]وهي من الجرائم شكلية وهي أيضا جريمة مستمرة لأن المجرم يبقى متواجد داخل النظام ضد إرادة من له حق السيطرة على هذا النظام وبناءًا على هذا سنعرض في الفرع الأول تعريف الجريمة أما في الفرع الثاني فسنتناول اختلافها عن جريمة الدخول.

الفرع الأول: تعريف جريمة البقاء غير المشروع لنظام المعالجة الآلية للمعطيات:

يقصد بحقل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له حق في السيطرة على هذا النظام وقد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول إلى النظام وقد يجتمعان.[2]

وتعتبر جريمة البقاء غير المشروع داخل النظام المعلوماتي بشكل عام من الجرائم التي يصعب تقديم دليل على إثباتها حيث يزعم المتهم في حالة القبض عليه أنه كان على وشك الإنفصال عن النظام المعتدي عليه[3]،وهذه الجريمة لا تترتب إلا على الجريمة السابق ذكرها وهي جريمة الدخول غير المشروع للنظام المعلوماتي [4]،وتعد هذه الجريمة من الجرائم الشكلية كالجريمة السابقة، كما أنها تعد من الجرائم المستمرة فتبقى الجريمة قائمة طالما أن الجاني مازال على اتصال بنظام المعلومات الذي تم دون قصد.[5]

---

[1]- المادة 394 مكرر من قانون العقوبات رقم 04-15 المؤرخ في 10 نوفمبر 2004.

[2]–أمال قارة، مرجع سابق ص110.

[3]–نهلا عبد القادر المومني، مرجع سابق ص 161

[4]–حنان ريحان مبارك المضحكي، مرجع سابق، ص111.

[5]–محمد أمين الرومي، جرائم الكمبيوتر والأنترنت، دار المطبوعات الجامعية، مصر، 2004، ص105

يقصد بمصطلح فعل البقاء غير المشروع في نظام المعلوماتية هو التواجد بداخل النظام بطريقة مخالفة للضوابط والإلتزامات المفروضة على الفاعل وهناك من يتولاه بالتعريف على أنه: "التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام فالبقاء يتمثل في عدم قطع الفاعل للإتصال بالنظام عند إدراكه بأن وجوده فيه غير مشروع".

ومن صور البقاء دخوله إلى النظام صدفة أو سهوا وبالرغم من ذلك بقي ولم ينسحب فورًا فتقوم الجريمة في مواجهة فاعلها بتحقق ركنها المعنوي كذلك، وتقوم أيضا جريمة البقاء في حالة تجاوز المدة المسموح له البقاء داخل النظام وفي هذا الصدد فقد قضت محكمة النقض الفرنسية في قرارها الصادر بتاريخ 2007/10/03 بقيام جريمة البقاء عن طريق الغش في حق شخص قام بالدخول إلى نظام المعالجة الآلية للمعطيات بواسطة كلمة سرية مؤقتة منحت له من قبل المسؤول على النظام لمدة محددة إلاّ أنه قام بتجاوز تلك المدة.

وكذلك الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيها الإطلاع فقط والاستفادة من خدمة الهاتف دون أن يدفع المقابل الواجب دفعه أو يحصل على الخدمة لمدة أطول من المدة التي دفع مقابلها باستخدام عمليات غير مشروع.[1]

يمكن القول بأن جريمة البقاء غير المشروع لنظام المعالجة الآلية للمعطيات تقوم في اللحظة التي يبقى فيها الفاعل يتجول داخل نظام المعالجة الآلية للمعطيات ويستمر في ذلك رغم علمه ودون اشتراطه قيامه بأي عمل لاحق لفعل البقاء أو تحقيق نتيجة معينة فالسلوك الإجرامي في البقاء يستمر معه الاعتداء على المصلحة القانونية بينما الدخول جريمة وقتية سواء كان مجردًا أو أدى إلى نتيجة معينة.[2]

---

[1]–أما قارة، مرجع سابق، ص110.

[2]–بوخبرة عائشة، مرجع سابق، ص73.

الفرع الثاني: اختلاف جريمة البقاء عن جريمة الدخول:

وهذه الجريمة ليست كسابقتها حيث أن الجاني في الجريمة السابقة يسعى بنفسه إلى تحقيق الاتصال مما يتطلب فعلا إيجابيا أي القيام بعمل لذالك قلنا أنها جريمة إيجابية، أما هذه الجريمة فإنها تتطلب الخروج من البرنامج أو النظام الآلي وقطع الاتصال أو عدم الإبقاء عليه ومن ثم الخروج من النظام في حالة تحقق الاتصال مما يعني أن الاتصال على الأغلب لن يكون مقصودا أو إلا تحققت الصورة الأولى أي أن هذه الجريمة يمكن أن تتحقق في الحالات التي يحصل فيها الاتصال عن طريق الخطأ و مع ذالك لا يقوم الجاني بما هو مطلوب منه أو واجب عليه فيبقى في النظام في حين أن المطلوب منه أن يخرج من النظام بقطع الاتصال.[1]

ترجع أهمية ما سبق بيانه إلى أن جريمة الدخول جريمة مؤقتة أما جريمة البقاء فإنها من طبيعة مستمرة وبالتالي فان التقادم تحسب مدته من وقت الدخول بالنسبة لمن قام بالدخول حتى ولو إستمرالبقاء في النظام مادام أن الدخول مشكلا للجريمة،أما إذا كان الدخول غير مقصود تم وعلى علم المتهم بدخوله ففضل البقاء فإنه ينسب إليه جريمة البقاء في النظام و تحتسب مدة التقادم من الوقت الذي فيه انتهاء هذا البقاء.[2]

ومما لا شك فيه أن البقاء داخل نظام الكمبيوتر بعدد دخوله عن طريق الخطأ لا يختلف عن الدخول الغير مصرح به من حيث وجوب التجريم، فاتجاه إرادة الفاعل إلى البقاء داخل هذا النظام على الرغم من معرفته انه غير مصرح له بالدخول لا يختلف عن جوهره عن الدخول الغير مصرح به إلى نظام الكمبيوتر.[3]

---

[1]–محمد حماد مرهج الهيثي، مرجع سابق ص 56.

[2]–شيماء عبد الغني محمد عطا الله، مرجع سابق، ص122.

[3]–مسعود خثير ، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2010، ص116.

المطلب الثاني

صور وأساليب جريمة البقاء غير المشروع

يتمثل نشاط المجرم في بقاء المتهم داخل نظام الكمبيوتر بعد دخوله إليه عن طريق القصد أو بطريق الخطأ، حيث تعد جريمة البقاء جريمة عمدية ففي حالة اكتشاف المتهم دخوله الخطأ ورفضه الخروج من النظام تقوم الجريمة أو في حالة التعدي إلى أجزاء أخرى قد يكون غير مصرح له بدخولها إلا أنه يبقى فيها ومن خلال هذا المطلب سنعالج صورة جريمة البقاء في الفرع الأول في حين سنتعرض في الفرع التالي لأساليب جريمة البقاء.

الفرع الأول: صور جريمة الدخول غير المشروع لنظام المعالجة الآلية للمعطيات:

تختلف صور جريمة الدخول عن صور جريمة البقاء، إلا أنهما يشتركان في تحديد طبيعة الصورة وهي تجاوز حدود التصريح سواء بالتعدي إلى أجزاء أخرى أو تجاوز الوقت المسموح به وهذا ما سنبينه سواء من خلال جريمة البقاء مع تجاوز الوقت المصرح به.

1- جريمة البقاء معتجاوز الوقت المصرح به:

يذهب رأي راجح من الفقه إلى أن جريمة البقاء داخل النظام تبدأ من اللحظة التي يبدأ فيها الجاني التجول داخل النظام أو يستمر في التجول داخله بعد إنتهاء الوقت المحدد أي منذ علم الجاني أنه ليس له حق الدخول فإذا دخل وظل ساكنا تظل الجريمة جريمة الدخول إلى النظام أما إذا بدأ التجول فإن جريمة البقاء داخل النظام تبدأ من تلك

اللحظة لأنه يتجول في نظام يعلم مسبقا أن مبدأ دخوله واستمراره فيه غير مشروع ومنذ تلك اللحظة تبدأ جريمة البقاء داخل النظام.[1]

ولكنه مع ذلك يظل الغموض قائما حول مدة البقاء داخل المنظومة ويطرح صعوبة حول تحديد زمن البقاء ويجب التفرقة هنا بين البقاء الحاصل عن جريمة الدخول غير المشروع وبين البقاء الناتج عن الدخول المسموح به لكون الجاني رفض الدخول بعد استيفاء الوقت المسموح له للدخول فيه للنظام.[2]

وقد يدخل المتهم النظام بطريق مشروع ولكنه يستمر بعد الوقت المحدد لبقائه وكثيرا ما يحدث ذلك إذا كان استعمال النظام محددًا بوقت معين نظير أجر مالي، فيتخطى المتهم هذا الوقت.[3]

يكون البقاء أيضا في الحالة التي يستمر فيها الجاني باقيا داخل النظام بعد المدة المحددة له للبقاء داخله أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيها الرؤية والإطلاع فقط.[4]

2- جريمة البقاء مع التجاوز إلى أشياء أخرى:

يلاحظ أن القانون الأمريكي لم يجرم التوصل غير المشروع كسلوك قائم بحد ذاته بل اشترط وجوب توافر القصد الجنائي خلافا للقانون الفرنسي الذي جاء فيه وينص المادة

---

[1]–مسعود خثير، مرجع سابق ص117

[2]–زيدان زبيحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2011، ص50.

[3]–غنام محمد مرجع سابق، ص142.

[4]–نهلا عبد القادر القهوجي، مرجع سابق، ص133.

323/ 1 على عقاب كل من يصل أو يبقى بطريقة مخادعة في كل أو جزء من نظام المعالجة الآلية للمعطيات[1].

إلاّ أنه من ناحية أخرى قد يجد شخص نفسه داخل نظام حاسب آلي غير مسموح له بالدخول إليه عن طريق الخطأ، كما لو كان في سبيله الدخول إلى نظام له الحق في الدخول إليه ثم يجد نفسه بسبب خطأ ما كإستخدام شفرة خاطئة على سبيل المثال داخل نظام آخر وفي هذه الحالة قد يقوم هذا الشخص بالخروج من هذا النظام بمجرد تنبيهه للخطأ الذي وقع فيه وقد يستمر البقاء داخل النظام على الرغم من معرفته أن هذا الدخول غير مصرح له بالدخول إليه[2].

في كل الحالات يتضح أن المشرع ربط البقاء كتصرف إرادي من قبل الجاني بسوء التية أي عن طريق الغش ويستوي في ذلك أن يكون الدخول أو البقاء في النظام المعلوماتي كله أو حتى في جزء منه ذلك أن الاعتداء قد استهدف جهاز الحاسوب نفسه[3].

الفرع الثاني: أساليب جريمة البقاء غير المشروع لنظام المعالجة الآلية للمعطيات

الفيروسات عبارة عن برامج خبيثة تتسلل إلى البرمجيات بحيث تدخل إليها وتنسخ نفسها على برامج أخرى في الحاسب الآلي.[4]

هناك العديد من الفيروسات التي ضربت حواسيب العديد من الدول وأثرت فيها وقاد ذلك إلى خسائر مادية ضخمة وقد أوضح الباحثون بأن بعض أنواع الفيروس

---

[1]-محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، ص86.

[2]-نائلة عادل محمد قورة، مرجع سابق، ص146.

[3]-زيدان زبيحة، مرجع سابق، ص50.

[4]–محمد أمين، الشوابكة جرائم الحاسوب والأنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2007، ص238.

يستخدم هجمات الـ BRUTE FORCE ATTACKلإستخراج كلمات المرور من أجهزة الكمبيوتر والشبكات الداخلية للمنشآت المصابة بالفيروس، كما حذرت مستخدمي أجهزة الكمبيوتر ومدراء الشبكات من استخدام كلمات مرور ضعيفة ويمكن التنبؤ بها.[1]

الفيروس عبارة عن برنامج يصممه المجرم المعلوماتي بطريقة تعطيه القدرة على ربط نفسه ذاتيا ببرامج أخرى أو بالنظام المعلوماتي حتى يحقق الأهداف المرجوة ويتميز الفيروس بخصائص منها قدرته على التخفي عن مستخدم النظام أو الحاسب والتمويه وأيضا قدرته على التسلل إلى داخل النظم المعلوماتية واختراقها مباشرة أو عن طريق كسر نظم الحماية[2].

تكون هذه الفيروسات مرفقة ومخزنة على البرامج التطبيقية وبرامج التشغيل وتنشط في حالة نسخ البرامج من جهاز لآخر أو عن طريق المباشر من شبكة لأخرى وخاصة عبر الأنترنت بحيث تكون مختبئة داخل رسائل البريد الإلكتروني.[3]

فالفيروس يمكن أن يتسلل إلى حاسب آلي معين دون أن تتجه إرادة مستخدمه إلى ذلك زمن ناحية أخرى فإن تجريم الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات لا يغني عن تجريم استخدام البرامج الخبيثة كما أنه لا يعد شرطا لهذا التجريم حيث أنه قد يتم استخدام الفيروس داخل نظام دون أن يسبقه دخول الفاعل إلى هذا النظام ويرجع ذلك إلى القدرة الفائقة للفيروسات على الانتشار والانتقال من نظام إلى آخر دون تدخل الفاعل بل وأحيانا دون علمه بذلك.[4]

---

[1]–عبد الحليم موسى يعقوب، الإعلام الجديد والجريمة الإلكترونية، الطبعة الأولى، الدار العالمية للنشر والتوزيع، السعودية، 2014، ص205.

[2]–فؤاد حسين العزيزي، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، مصر 2014، ص ص 371-372.

[3]–نائلة عادل، محمد فريد قورة، مرجع سابق، ص 296.

[4]–فؤاد حسين العزيزي، مرجع سابق، ص 372.

ولهذا فإن الفيروس يعتبر شديد الصلة بالجريمة المعلوماتية بشكل عام يلجأ إليه المجرم المعلوماتي لإرتكاب الجرائم في مجال المعالجة الآلية للمعطيات فقد يؤدي الفيروس بالنظام المعلوماتي يؤثره وقد يختص ببرنامج معين وفي هذه الحالة ينشط الفيروس ويمارس نشاطه التخريبي عند تشغيل البرنامج حيث ينتقل من برنامج إلى آخر إلى أن يصل إلى القرص الصلب ويدمره فيتوقف النظام عن العمل[1].

وأما عن بدء عملها فبدأ عملها يتحدد طبقا لأسلوب تصميمها فتبدأ تلك الفيروسات العمل بمجرد فتح الرسالة الموجودة بها والتي وصلت عن طريق البريد الإلكتروني وقد تبدأ العمل بمجرد تشغيل البرنامج الموجودة عليه في الجهاز[2].

[1]– بلال أمين زين الدين، الجريمة المعلوماتية في التشريع المقارن والتشريعية الإسلامية، دار الفكر الجامعي، مصر، 2014، ص373.

[2]–منير محمد الجنبيهي، ممدوح محمد الجنبيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي، مصر، ص47.

خلاصة الفصل الأول :

تعد جريمة الدخول والبقاء من الجرائم المعلوماتية التي تصيب نظام المعالجة الآلية للمعطيات وهي تمس المعلومات المخزنة داخل النظام فجريمة الدخول تعني قيام الجاني بالولوج إلى نظام المعالجة الآلية للمعطيات والاطلاع عليها دون علم صاحبها أي دون الحصول على تصريح بذالك وهي جريمة وقتية أي أنها تقوم بالاطلاع على المعلومات وهذا النوع من الجرائم يختلف عن عدة أفعال مشابهة له و لهذه الجريمة صور تقوم غليها فقد تقوم هذه الجريمة بتجاوز الوقت وهو يملك تصريح حول أي ما تضمنه الدخول هو فترة زمنية إلا انه تعدى ذالك الوقت المصرح به ويمكن أيضا قيامها بالتجاوز إلى أجزاء أخرى أي أن التصريح يتضمن جزء معين إلى أن الجاني يتعدى إلى أجزاء أخرى غير مصرح بها وهناك وسائل لقيام بهذه الجريمة فمنها تشغيل كمبيوتر مقفول وإستعماله مفتوح وهناك عدة وسائل أخرى لقيام ذالك و هذا بتباع طريقتين لذالك الدخول المباشر وغير المباشر إلى نظام المعالجةالآلية للمعطيات

أما جريمة البقاء فهي جريمة مستمرة قد تكون مستقلة عن جريمة الدخول أيأن الجاني قد يحصل على تصريح بالدخول غير انه يرتكب جريمة البقاء وهذه الجريمة قد تتجاوز هي الأخرى الوقت المصرح به أو تتعدى أيضا إلى أجزاء أخرى غير مصرح بها ومن جهة أخرى قد تقوم جريمة الدخول والبقاء معا ولقيام هذا النوع من الجرائم هناك طرق مستحدثة لقيامها وذالك بنشر الفيروسات داخ أنظمة المعالجة الآلية للمعطيات.

يظهر الاختلاف بين جريمة الدخول الغير مصرح به إلى نظام الحاسب الآلي و جريمة البقاء داخل هذا النظام بعد دخوله عن طريق الخطأ يكمن في أن الأولى جريمة إيجابية من ناحية روتينية من ناحية أخرى في حين أن الثانية جريمة سلبية ومستمرة من ناحية أخرى.[1]

[1]–نائلة عادل محمد فريد قورة مرجع سابق ص384.

Nom du document : الفصل الأول المعدل
Répertoire : C:\Users\fathi\Documents
Modèle : C:\Users\fathi\AppData\Roaming\Microsoft\Templates\Normal.dotm
Titre : الفصل الأول: ماهية جريمة الدخول والبقاء الغير مشروع لنظام المعالجة الآلية للمعطيات
Sujet :
Auteur : admin
Mots clés :
Commentaires :
Date de création : ص 09:11:00 2019/10/12
N° de révision : 26
Dernier enregistr. le : ص 11:51:00 2020/02/22
Dernier enregistrement par : fathi
Temps total d'édition : 386 Minutes
Dernière impression sur : ص 11:51:00 2020/02/22
Tel qu'à la dernière impression
Nombre de pages : 22
Nombre de mots : 3 902 (approx.)
Nombre de caractères : 22 243 (approx.)

الفصل الثاني

الإطار القانوني لجريمتي الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات

الفصل الثاني

الإطار القانوني لجريمتي الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات

تقوم الجريمة بشكل عام على توافر الأركان الأساسية المكونة لها وهو ما يطبق أيضا على الجرائم المعلوماتية ففي هذا الصدد نقوم بدراسة جريمة الدخول والبقاء إلى أنظمة المعالجة الآلية للمعطيات وهذا من خلال توضيح ما جاء في نصوص القانون من ركن شرعي، إضافة إلى قيام الركن المفترض الذي يعني أساسا وجود نظام معالجة آلية وتوافر الحماية لهذا النظام إلى جانب الركن المادي والركن المعنوي الذي يظهر بأن هناك نية لدى الجاني لإرتكاب هذا النوع من الجرائم ذلك لأن الجريمة لا تقوم إلاّ بتوافر القصد العام لإرتكابها وهذا ما ينطوي عليه الركن المعنوي.

وقد صادقت الكثير من الدول العربية والغربية على اتفاقية بوداسبت لمكافحة الجريمة المعلوماتية وأصدرت هذه الدول عقوبات مختلفة لها ولكي يتضح لنا المجال القانوني الذي تدور فيه جريمة الدخول والبقاء لابد من دراسة محتواه من خلال الأركان والعقوبات وهذا ما سنتطرق من خلال:

المبحث الأول: أركان جريمة الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات.

المبحث الثاني: دوافع ارتكاب جريمة الدخول والبقاء غير المشروع والعقوبات المقررة لها.

المبحث الأول

أركان جريمة الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات

يعتبر قانون العقوبات الجزائري من القوانين العربية السابقة إلى هذا الموضوع وخطى المشرع الجزائري هذه الخطوة من خلال تعديل قانون العقوبات بمقتضى القانون رقم 04- 15[1] المؤرخ في 10 نوفمبر 2004 بإدراج القسم السابع مكرر 3 بمحتوى المادة 394 مكرر إلى المادة 394 مكرر 7 المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات وسنتعرض من خلال هذا المبحث لأركان جريمة الدخول والبقاء غير المشروع ويكون ذلك في مطالبين المطلب الأول نتناول فيه: الركن المادي والمعنوي والمطلب الثاني نتناول فيه: الركن الشرعي والركن المفترض.

المطلب الأول

الركن الشرعي والركن المفترض لجريمة الدخول والبقاء غير المشروع

جريمة الدخول والبقاء غير المشروع مثلهما مثل باقي الجرائم الأخرى تستوجب توافر الركن الشرعي فيها ليتم اعتبارها جريمة معاقب عليها في القانون وهو ما سنعرضه من خلال الفرع الأول كما سنوضح في الفرع الثاني ضرورة توافر الركن المفترض في هذه الجريمة إذ تتطلب توافر الحماية القانونية لنظام المعالجة الآلية للمعطيات فقيام هذه الجريمة يكون بالإعتداء على المعلومات التي تخضع لحماية قانونية داخل الحاسب الآلي.

[1]- قانون 15/04 المؤرخ في 27 رمضان 1425 هـ الموافق لـ 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 156/66 المؤرخ في 18 صفر 1386 الموافق لـ 8 يونيو 1966 المتضمن قانون العقوبات، جريدة رسمية عدد 71 بتاريخ 2004.

الفرع الأول: الركن الشرعيلجريمة الدخول والبقاء غير المشروع

يقصد بالركن الشرعي للجريمة وجود نص يجرم الفعل ويوضح العقاب المترتب عليه وقت وقوع هذا الفعل فمبدأ الشرعية الجنائية يمنع المساءلة الجنائية ما لم يتوفر النص القانوني فلا جريمة ولا عقوبة إلا بنص قانوني ومتى انتفى النص على تجريم مثل هذه الأفعال التي لا تطالها النصوص القائمة امتنعت المسؤولية وتحقيق القصور في مكافحة جرائم من هذا النوع، غير أنّ السؤال المطروح هو مدى تطبيق مبدأ الشرعية على الجرائم التي ترتكب عبر الأنترنت[1].

ونجد بأن المشرع الجزائري قد تدارك مؤخرًا ولو نسبيا الفراغ القانوني في مجال الإجرام المعلوماتي وذلك باستحداث نصوص تجريمية لقمع الإعتداءات الواردة على المعلوماتية بموجب القانون رقم 15/04 المتضمن تعديل قانون العقوبات لكن تجدر الإشارة إلى أن المشرع الجزائري قد ركز على الإعتداءات الماسة بالأنظمة المعلوماتية وأغفل الإعتداءات الماسة بمنتوجات الإعلام الآلي والمتمثلة في التزوير المعلوماتي[2].

وهذا ما جاء ذكره في نص المادة 394 مكرر من قانون العقوبات على أنه يعاقب بالحبس من 3 أشهر إلى سنة وبغرامة من 50.000 دج إلى 200.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك[3].

---

[1]- يوسف صغير، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، جامعة مولود معمري كلية الحقوق والعلوم السياسية، 06-03-2014/2013، ص ص 59-60.

[2]- أمال قارة، مرجع سابق، ص99.

[3]- قانون رقم 06-23 المؤرخ في29 ذو القعدة 1427 الموافق لـ 20 ديسمبر 2006. يعدل ويتمم الأمر 66/ 156 المؤرخ في 18 صفر 1386 الموافق لـ 8 يونيو 1966، المتضمن العقوبات، جريدة رسمية عدد 84، بتاريخ 24 ديسمبر 2006.

وبالإطلاع على العديد من القوانين نجد بأن هناك الكثير من الدول التي جرمت وعاقبت على الدخول والبقاء إلى أنظمة المعالجة الآلية للمعطيات دون تصريح كما جرمت عدة اتفاقيات دولية ذلك ومنها الاتفاقية الدولية للإجرام المعلوماتي التي نصت في المادتين 05 و08 منها على الإعتداء العمدي على سير نظام المعالجة الآلية للمعطيات.

الفرع الثاني: الركن المفترضلجريمة الدخول والبقاء غير المشروع

يتمثل الركن المفترض لقيام هذه الجريمة في تواجد نظام معالجة آلية للمعطيات (أولا) إضافة إلى ضرورة توافر حماية للمعطيات (ثانيا).

أولا: وجود نظام معالجة آلية للمعطيات

هو عبارة عن مجموعة من الوحدات والأجهزة والبرامج التي تعمل مجتمعة بغية التوصل إلى معالجة المعطيات آليا وإخراجها أو تخزينها واسترجاعها عند الحاجة[1].

فنظام المعالجة الآلية للمعطيات هو عبارة عن مجموعة العمليات التي تتم آليا أي باستخدام الحاسب الآلي وتتعلق بالتجميع والتسجيل والإعداد والتعديل والإسترجاع والإحتفاظ ومحو المعلومات الاسمية ومجموعة العمليات التي تتم آليا بغرض استغلال المعلومات وخصوصا عمليات الربط والتقريب وانتقال المعلومات الإسمية ودمجها مع بيانات أخرى أو تحليلها للحصول على معلومات ذات دلالة[2].

ثانيا: خضوع النظام للحماية

يسعى المخصصون بأمن المعلومات للحفاظ على خصوصية المعطيات المتنقلة عبر الأنترنت بالأخص شبكة الأنترنت فهم يسعون لتأمين سرية الرسائل الإلكترونية

[1]- بلال أمين زين الدين، مرجع سابق، ص264.

[2]- محمود أحمد عبابنة، مرجع سابق، ص83.

وسرية المعطيات المتناقلة خاصة بأعمال التجارة الرقمية ويمثل التشفير أفضل وسيلة للحفاظ على سرية المعطيات المتناقلة ويرى الخبراء ضرورة استخدام أسلوب التشفير لمنع الآخرين من الإطلاع على الرسائل الإلكترونية[1].

ويستوي في ذلك النظام أن يكون محميا بأسلوب معين مثل كلمة السر أو غير محمي وذلك في غالبية التشريعات المقارنة مثل القانون الإنجليزي القانون الكندي والقانون الفرنسي وهذا ما تتجه إليه القوانين المقارنة[2].

ففي نص المادتين 62 2/3 و 23 1/3 من القانون الفرنسي لم تشترطا هذا الشرط في جريمة الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات كما يستند إلى الأعمال التحضيرية[3].

ولقد انتقد هذا الرأي من جانب آخر من الفقه على أساس أن النظام الأمني للنظم المعلوماتية هو مهم جدا بالنسبة للشركات التأمين والتي تضح حد أدنى من الحماية الذي لا يمكن النزول عنه من قبل مستخدمي النظام المعلوماتي حيث يؤدي التقصير في ذلك إلى تحميل شركات التأميم خسائر فادحة وتعويضات جمة نتيجة المطالبات القضائية التي تتعلق بتعويض الخسائر الناشئة عن الإعتداء على الأنظمة المعلوماتية[4].

[1]- أمال قارة، مرجع سابق، ص103.

[2]- شيماء عبد الغني محمد عطا الله، مرجع سابق، ص101.

[3]- بلال أمين زين الدين، مرجع سابق، ص 265.

[4]- بلال أمين زين الدين، مرجع سابق، ص 271.

المطلب الثاني:

الركن المادي والركن المعنوي

يلزم لقيام جريمة الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات أن يقوم الجاني بنشاط خارجي ملموس أو فعل مادي يعبر به عن إرادته في انتهاك نظم الحماية الأمنية التي تضعها المؤسسات أو الإدارات أو الشركات لحماية نظمها المعلوماتية من محاولات العبث بها أو تعديلها أو إتلافها أو الإطلاع عليها أو إفشاءها أو ما يعبر عنه عن إرادته في البقاء داخل النظم المعلوماتية وبدون حق لتحقيق أي من الأهداف الإجرامية عادة[1].

ويمكن القول أنه لقيام هذه الجريمة لا بد من اشتمالها على ركنين ألا وهما الركن المادي الذي سنعرضه في الفرع الأول والركن نورده في الفرع الثاني.

الفرع الأول: الركن المادي لجريمة الدخول والبقاء الغير المشروع

يقصد بالركن المادي ذلك السلوك أو العمل أو الفعل المحظور الذي يصيب المصالح الدولية بضرر أو يعرضها للخطر فالركن المادي للجريمة هو نشاط يتمثل في حركة عضوية صادرة عن إنسان لها مظهرها الملموس في العالم الخارجي وتحدث أثرا أو تهدد بالخطر مصالح معنية بالحماية الجنائية.

وبالرجوع إلى النصوص التشريعية نجدها قد تضمنت صورتين للركن المادي لهذه الجريمة فهناك الصورة البسيطة لفعل الدخول أو البقاء غير المشروع وهناك الصورة

[1]- بلال أمين زين الدين، المرجع السابق، ص271.

المشددة لفعل الدخول والبقاء غير المشروع وهذا ما سنوضحه من خلال العنصرين التاليين:

أولا: الصورة البسيطة

يتكون الركن المادي في هذه الجريمة من نشاط إجرامي يتمثل إما في فعل الدخول إلى نظام المعالجة الآلية للمعطيات أو جزء منه وإما في فعل البقاء في هذا النظام أو في جزء منه يعرضه للخطر[1]، فالركن المادي للجريمة هو نشاط يتمثل في حركة عضوية صادرة عن إنسان، لها مظهرها الملموس في العالم الخارجي تحدث أثرا أو تهدد بالخطر مصالح معنية بالحماية الجنائية، وبهذه الأوصاف يختلف الركن المادي عن مجرد النوايا التي لا يعاقب عليها وذلك أن القانون لا يعتد بالنوايا ولو كانت خبيثة، قبل تتجسد في أفعال مادية موجهة لإرتكاب الجرائم[2].

وتفترض هذه الجريمة أن هناك إتصال شرعي بنظام المعلومات لم يسعى الجاني للدخول فيه، ولكن تم دخول الجاني فيه بطريق الصدفة، ويتحقق الركن المادي للجريمة منذ اللحظة التي يقرر فيها الجاني الإبقاء على ذلك الاتصال وعدم الخروج منه، فهذه الجريمة من جرائم الإمتناع، ويتمثل السلوك المجرم في الإمتناع عن قطع الاتصال مع النظام[3].

---

[1]- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، لبنان، 1999، ص130.

[2]- عبد الله سليمان سليمان، المقدمات الأساسية في القانون الدولي الجنائي، ديوان المطبوعات الجامعية: الجزائر، ص113.

[3]- محمد أمين الرومي، مرجع سابق، ص105.

لا يشترط في هذه الجريمة أن يكون البقاء على الاتصال غير المسموح به قد تم بطريق الغش، حيث أن اشتراط استمرارية البقاء في النظام عن طريقالغش يعد شرط لم ينص عليه المشرع، كما أن الاستمرارية في البقاء على الاتصال بالنظام بطريق الغش يتنافى مع القول بأن الاتصال بنظام المعلومات قد تم بطريق الصادقة البحتة، ودون أن يسعى إليه الجاني، لذلك ليس صحيحا ما يشترطه البعض من البقاء على الاتصال بالنظام لابد أن يكون عن طريق الغش[1].

كما أن من يدخل إلى النظام المعلوماتي بمحض الصدفة ثم يبقى داخل النظام مع علمه بعدم مشروعية فعله فإنه أيضا يعاقب على فعل الولوج غير المشروع في أنظمة المعالجة الآلية للمعطيات[2].

غير أنه لا يشترط في هذه الجريمة حدوث أي نتيجة إجرامية فيكفي البقاء في نظام للمعلومات غير مسموح بدخوله، ولا يغير من ذلك كون المشرع قد شدد العقوبة في حالة ما إذا ترتب على الدخول نتائج أخرى أشد خطورة مثل محو أو تعديل المعلومات أو تعطيل تشغيل النظام، وإنما تعد هذه الحالات ظروف مشددة للعقاب[3].

ثانيا: الصورة المشددة

أيا كانت طبيعة فعلي الولوج والبقاء غير المشروعين فإنهما لابد وأن يردا على نظام معلوماتي بمكوناته المتعددة والمتكاملة مع بعضها البعض بهدف واحد وهو معالجة المعطيات آليا[4].

[1]- محمد أمين الرومي، مرجع سابق، ص 106.

[2]- فؤاد حسين العزيز، مرجع سابق، ص273.

[3]- محمد أمين الرومي، مرجع سابق، ص105.

[4]- فؤاد حسين العزيز، مرجع سابق، ص273.

وقد نصت المادة394 مكرر 2 و3 قانون العقوبات الجزائري على ظرفين تشدد بهما عقوبة جريمة الدخول والبقاء داخل النظام، ويتحقق الظرفان عندما ينتج عن الدخول أو البقاء إما محو أو تعديل المعطيات التي يحتويها النظام، وإما عدم صلاحية النظام لأداء وظائفه[1].

ويكفي لتوافر هذا الظرف وجود علاقة سببية بين الدخول غير المشروع أو البقاء غير المشروع وتلك النتيجة الضارة سواء محو أو تعديل المعطيات التي يحتويها النظام، ويلاحظ هنا أن المشرع إنما يحمي النظام من خلال حماية المعطيات التي يحتويها، أما عدم صلاحية هذا النظام للقيام بوظائفه، فإنه يعني عدم قدرته على تنفيذ المعالجة الآلية للمعطيات[2].

الفرع الثاني: الركن المعنوي لجريمة الدخول والبقاء غير المشروع

الركن المعنوي هو ذلك الجانب الشخصي أو النفسي في الجريمة، فلا تقوم الجريمة بمجرد قيام الواقعة المادية إذ لابد من أن تصدر هذه الواقعة عن إرادة فاعلها وترتبط به إرتباطا معنويا أو أدبيا، فالركن المعنوي للجريمة يتمثل في قيام هذه الرابطة المعنوية، أو الصلة النفسية أو العلاقة الأدبية التي تربط ماديات الجريمة بنفسية الفاعل بحيث يمكن أن يقال بأن الفعل المقترف هو نتيجة إرادة الفاعل[3].

لا يتطلب توافر القصد الجنائي الخاص لتحقيق جريمة الدخول والبقاء غير المصرح بهما، فيكفي توافر القصد العام بعنصرية المتمثل في عنصر العلم وذلك بأن يعلم الجاني أنه يتجول في نظام آلي للمعطيات دون أن يكون له الحق في ذلك، والعنصر الثاني وهو

[1]- أمل قارة، مرجع سابق، ص273.

[2]- علي عبد القادر القهوجي، مرجع سابق، ص137.

[3]- عبد الله سليمان سليمان، مرجع سابق، ص122.

عنصر الإرادة وذلك بأن يريد الجاني الذي دخل هذا النظام الإمتناع عن وقف الاتصال بنظام المعلومات[1].

تعتبر جريمة الدخول والبقاء من الجرائم العمدية بحيث يكفي فيها القصد العام، فيكفي لتوافر هاته الجريمة أن يعلم الجاني أنه قد دخل إلى نظام ليس له حق الدخول فيه، أو تعتمد البقاء فيه رغم إنتهاء مدة حقه بالبقاء فيه، ولو كان الدخول مشروعا، أما إذا إنتفى علمه فإنه لا تتوافر الجريمة كأن يجهل وجود خطر الدخول أو كان خطأ أنه مسموح له الدخول فيه[2].

أولا: المقصود بالقصد الجنائي العام

هو القصد في أبسط صوره وهو اتجاه الإرادة الإجرامية لإرتكاب الجريمة مع علم الجاني بعناصرها أي أنه قصد يقوم على عنصري الإرادة والعلم وهو قصد يجب توافره في جميع أنواع الجرائم العمدية.

جريمة الدخول والبقاء غير المشروع في صورتها البسيطة هي من الجرائم الشكلية التي لم يتطلب المشرع لقيامها حصول نتيجة إجرامية معينة فالقصد الجنائي فيها يشترط ضرورة العلم بماهية السلوك الإجرامي وتتصرف معه إرادة الجاني إلى هذا السلوك[3].

1- العلم: يقوم القصد الجنائي على العلم بجميع الظروف والوقائع التي تعطي للفعل دلالته الإجرامية فعلم الجاني في جريمة الدخول والبقاء يجب أن ينصرف إلى كل واقعة

[1]- محمد أمين الرومي، مرجع سابق، ص106.

[2]- مسعود خثير، مرجع سابق، ص118.

[3]- عبد الله أوهايبية، شرح قانون العقوبات الجزائري، القسم العام المؤسسة الوطنية للفنون المطبعية الموفم للنشر، الجزائر، 2009، ص ص 334-355.

تدخل في تكوينهما، فلابد أن يعلم الجاني بأن فعله ينصب على نظام المعالجة الآلية للمعطيات وليس لشيء آخر وأنه يعلم بأن لاحق له في الدخول إلى النظام والبقاء فيه فلا يقوم القصد الجنائي لديه إذا كان يعتقد بأن الموقع مفتوح للجمهور أو إذا كان دخوله إليه بمحض الصدفة أو الخطأ، أو إذا كان الدخول إلى النظام يتم بموجب اشتراك وكان قد سبق للشخص الدخول بوجه مشروع غير أنه قد انتهت مدة اشتراكه وكان يجهل ذلك ولكن في المقابل عليه أن يخرج فورًا من النظام عند علمه بأن دخوله أو بقاؤه غير مصرح به وأن يفعل ذلك بتوافر القصد الجنائي منذ اللحظة التي تحقق فيها العلم وعدّ مرتكبا لجريمة الدخول والبقاء غير المشروع لنظام المعالجة الآلية.

2- **الإرادة:** الإرادة الآثمة قد توجه نحو ارتكاب السلوك المجرم وإحداث نتيجة[1] فهي التي تبين الموقف النفسي للفاعل من سلوكه والنتيجة المترتبة عنه ولكون جريمة الدخول أو البقاء جريمة شكلية فإن الإرادة تقتصر على السلوك الإجرامي لتستغرقه بكل مقوماته ولا تمتد معه لأي نتيجة أخرى[2].

ومن القرائن الدالة على توافر الجنائي هي استخدام وسائل خداعية في تحقيق الدخول أو البقاء في النظام المعلوماتي إذا كان الدخول يتطلب شفرة أو بطاقة معينة فقام الفاعل بسرقة هذه البطاقة أو اختراق الشفرة.

وإذا توفر القصد الجنائي بعنصريه العلم والإرادة فإنه لا عبرة بعد ذلك بالباعث على الدخول أو البقاء داخل نظم المعلوماتية فيظل معه القصد قائما حتى ولو كان ذلك

[1]- عبد اللهأوهايبية، مرجع سابق، ص334.

[2]- محمد خليفة، مرجع سابق، ص166.

الباعث الفضول أوجب الاستطلاع أو إثبات القدرة على التفوق والتغلب على قيود النظام أو أن يكون الغرض هو الاستفادة من المعلومات والبيانات التي يحتويها النظام.

فهذه الجريمة عمدية، يتعين لقيامها توافر القصد الجنائي العام لدى الجاني بعنصريه العلم والإدارة، فإذا أثبت الجاني إنتفاء العلاقة السببية بين السلوك والنتيجة التي هي ذات الظروف المشدد في الجريمة، كأن يثبت أن تعديل أو محو المعطيات، أو أن عدم صلاحية النظام للقيام بوظائفه يرجع إلى القوة القاهرة، أو الحادث المفاجئ، إنتفى السلوك الإجرامي، وإنتفى بذلك معه القصد الجنائي[1].

ونظرا للصعوبات التي تعتري التحقق من التوافر القصد الجنائي في عملية الدخول والبقاء غير المشروع للمواقع الإلكترونية فإنها تبقى مسألة موضوعية ينفرد بتحديدها قاضي الموضوع، حيث يبحث في الموضوع من عدة جوانب من حيث توافر القصد ومن عدمه[2].

ثانيا: إمكانية توافر القصد الجنائي الخاص في جريمة الدخول والبقاء عن طريق الغش لنظام المعلوماتية

يقصد بالقصد الجنائي الخاص الإرادة لوقائع إضافية تدخل في تكوين الجريمة بالإضافة إلى عنصري العلم والإدارة[3]، وباستقراء نص المادة 394 مكرر من قانون العقوبات نستشف من خلالها أن غاية المشرع الجزائري لا تتطلب وجود نية خاصة لدى

[1]- مسعود خثير، المرجعسابق، ص119.

[2]- حنان ريحان مبارك المضحي، مرجع سابق، ص107.

[3]- عبد الله أوهايبية، مرجع سابق، ص335.

الجاني حتى تقوم ضده جريمة الدخول والبقاء عن طريق الغش لنظام المعلوماتية وهو الموقف الذي كرسه كذلك المشرع الفرنسي بنص المادة 1/323 من قانون الفرنسي.

فلفظ الغش وغن حمل معنى الاحتيال فهو لا يدل إلاّ على معنى واحد هو أن الجريمة عمدية لا أكثر أي أنه يكفي لقيامها توافر القصد الجنائي العام فحسب[1].

ويشكل الركن المعنوي أهمية بالغة في قيام جريمة الدخول والبقاء غير المصرح بهما إلى نظام الكمبيوتر فالأفعال التي تقوم بها هذه الجريمة يقو بها كل يوم مستخدمو الكمبيوتر، ومن بين هذه الأفعال لا يمكن تجريم سوى تلك التي يتحقق بشأنها القصد الجنائي[2]، فلابد أن يحيط الجاني علما بأنه يأتي فعلا غير مشروع يتمثل في الولوج والبقاء في النظام المعلوماتي المملوك لغيره والغير مصرح له بدخوله أو بالتجول في محتوياته من معلومات وأسرار وبرامج ونظم[3].

ولقد عبرت جميع النصوص القانونية التي تناولت جريمة الدخول والبقاء إلى نظام الكمبيوتر عن القصد العام المتطلب في هذه الجريمة، وذلك على الرغم من الإختلاف في العبارات المستخدمة لهذا الغرض، ويتطلب القصد العام أن يحيط علم الجاني بكل واقعة ذات أهمية قانونية في تكوين الجريمة، فكل مليتطلبه القانون من وقائع لبناء أركان الجريمة واستكمال عناصرها يتعين أن يشمله علم الجاني، ولكن علم الجاني يقتصر نطاقه على الوقائع التي تدخل في تكوين الجريمة، وإنما يتعين أن يحيط أيضا بالتكيف الذي تتصف به بعض هذه الوقائع وتكتسب بها أهميتها في نظر القانون[4].

---

[1]- علي عبد القادر قهوجي، مرجع سابق، ص107.

[2]- خالد ممدوح إبراهيم، مرجع سابق، ص259.

[3]- بلال أمين زين الدين، مرجع سابق، ص277.

[4]- خالد ممدوح إبراهيم، مرجع سابق، ص ص 259-260.

كما يجب في القصد الجنائي في الجريمة الولوج والبقاء غير المشروع داخل أنظمة المعالجة للمعطيات أن تتجه إرادة الجاني إلى فعلي الولوج والبقاء وإلى النتيجة الإجرامية وهي الإطلاع و التجول خلال المواقع والمعلومات والأسرار المعلوماتية بدون حق[1].

ولا يتوافر الركن المعنوي إذا كان دخول الجاني أو بقائه داخل النظام مسموح به أي مشروع، كما لا يتوافر هذا الركن إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء أو في نطاق هذا الحق[2].

فللركن معنوي أهمية كبيرة في تحقق جريمة الدخول والبقاء غير المصرح بهما إلى نظام الحاسب الآلي، فالأفعال التي تقوم بها هذه الجريمة يقو بها كل يوم مستخدمو الحاسبات الآلية، ومن بين هذه الأفعال لا يمكن تجريم سوى تلك التي يتحقق بشأنها القصد الجنائي، فالركن المعنوي لجريمة الدخول والبقاء في التشريعات التي تناولتها يتخذ صورة القصد الجنائي بإعتبارها من الجرائم العمدية[3].

[1]- فؤاد حسن العزيزي، مرجع سابق، ص278.

[2]- علي عبد القادر القهوجي، مرجع سابق، ص 136.

[3]- نائلة عادل محمد فريد قورة، مرجع سابق، ص346.

المبحث الثاني

دوافع ارتكاب جريمة الدخول والبقاء غير المشروع والعقوبات المقررة لها

شددت التشريعات القانونية في عقوبة جريمة الدخول والبقاء وجعلتها مضاعفة إذ ترتب عنها حذف أو تغيير لمعطيات المنظومة ويعد تغيير أو تخريب المنظومة من أبرز صور الجريمة لكونها تجسد الركن المادي للجريمة وتعطي انطباعا على بلوغ المجرم لمبتغا ويجسد الركن المادي هنا بإحداث تغيير في المعطيات وذلك بمحوها كليا أو جزئيا بحيث تصبح غير صالحة للإستعمال في ذات الوقت بتحقق الركن المعنوي لهذه الجريمة بتوافر العلم بأن تتجه إدارة الجاني لتحقيق نتيجة تصرفه ومن ثم فإن الإتلاف والتخريب جريمة عمدية وهي لا تقتصر على تغيير في المعطيات بل قد تصل إلى تخريب نظام أشغال المنظومة كليا كما يصورها نص المادة 394 مكرر من قانون العقوبات وبصدد ذلك ضاعف المشرع الجزائري العقوبة[1].

ومن خلال هذا المبحث سنعالج مطلبين الأول يتمثل في تبيان دوافع ارتكاب جريمة الدخول والبقاء والثاني يوضح العقوبات المقررة لجريمة الدخول والبقاء.

[1]– ريدان ربيحة، مرجع سابق، ص ص 51-52.

المطلب الأول

دوافع ارتكاب جريمة الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات

عملت الدول عبر الزمن إلى سن التشريعات والقوانين من أجل مواجهة كل من مواجهة الجرائم ومن ذلك الجرائم المرتكبة عبر الأنترنت فالبرغم من قلتها إلا أنها تعتبر محاولات هامة وملموسة في هذا المجال وتتمثل هذه الجهود على المستوى الدولي والداخلي وتعتبر الجهود الدولية داعمة للجهود التي تبذلها مختلف الدول في تشريعاتها الداخلية فهي بمثابة قوانين استر شادية تأخذ بها الدول لمواجهة الجرائم المستحدثة بما فيها تلك المرتكبة عبر الأنترنت[1].

وتختلف الجريمة المرتكبة عبر الأنترنت عن الجريمة التقليدية من حيث الدوافع حيث أن مجرمي الأنترنت يسعون من خلال ارتكابها إلى تحقيق الكسب المادي أو أعراض أخرى مثل التعلم أو اللعب أو المزاح أو الإنتقام[2] وتحصر هذه الدوافع من خلال دوافع شخصية (الفرع الأول) ودوافع مادية (الفرع الثاني).

الفرع الأول: الدوافع الشخصية

تتمثل الدوافع الشخصية لدى المجرم المعلوماتي في تحقيق أغراضه الخاصة وهذا بالرجوع إلى الحالة النفسية له سواء كانت حالات ذهنية أو بغرض الإنتقام ونبين هذه الدوافع من خلال الدوافع الذهنية (أولا) ودوافع الإنتقام (ثانيا).

---

[1]– يوسف صغير، مرجع سابق، ص92.

[2]– يوسف صغير، مرجع نفسه، ص38.

أولا: الدوافع الذهنية

تعتبر الدوافع الذهنية تلك العوامل اللصيقة بالمجرم المعلوماتي والتي تدفعه إلى ارتكاب الجريمة المعلوماتية بهدف الرغبة في اثبات الذات وتحقيق انتصار على تقنية الأنظمة المعلوماتية والتفوق على تعقيد وسائل التقنية دون أن يكون له نوايا خبيثة[1].

ففي الوقت الذي يزداد فيه الاهتمام بأمن الحاسب الآلي وشبكاته عن طريق تطوير طرق جديدة وصعبة لإختراقه كبرمجيات التشفير التي تمكن مستقبلها وحده من فهمه فمن جهة أخرى هناك أصحاب الشغف الإلكتروني الذي يتسابقون لخرق هذه الأنظمة واظهار تفوقهم عليها والدليل على ذلك قيام أحد الهواة في أوربا بحل شفرة أحد مراكز المعلومات في وزارة الدفاع الأمريكي وتمكنه من العبث في بيانات هذا المركز[2].

ثانيا: دافع الإنتقام

يكون دافع الإنتقام مؤثرا في ارتكاب هذه الجريمة حيث يعد من أخطر الدوافع التي يمكن أن تدفع شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل فيها لأنه غالبا ما يكون أحد موظفيها ويقوم بهذا الدافع نتيجة إما لفصله أو تخطيه في الترقية فهذه الأمور تجعله يُقْدِمُ على ارتكاب جريمته[3].

---

[1]– سفيان سوير، الجرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، محمد بن عمار، جامعة أبو بكر بلقايد، كلية الحقوق والعلوم السياسية، 2010، ص27.

[2]– محمود أحمد عبابنة، مرجع سابق، ص25.

[3]– يوسف صغير، مرجع سابق، ص42.

الفرع الثاني: الدوافع المادية

الجرائم المعلوماتية مثلها مثل الجرائم التقليدية غايتها أو رغبة الجاني فيها تتجه إلى تحقيق منفعة مادية إذ أن الجاني لا يرتكب الجريمة دون هدف يرجو الوصول إلى تحقيقه إذ أنه يحقق مكسب مادي (أولا) أو يحقق متعة شخصية بغرض التسلية (ثانيا).

أولا: تحقيق مكسب مادي

تعد الرغبة في تحقيق الثراء من العوامل الرئيسية لإرتكاب الجريمة عبر الأنترنت وهو من أهم الدوافع وأكثرها تحريكا للمجرم نظرًا للربح الكبير الذي يمكن أن يحققه هذا من النشاط الإجرامي وغالبا ما يكون الدافع لإرتكاب هذه الجرائم وقوع الجاني في مشاكل مادية تعجزه عن سداد ديونه المستحقة أو لوجود مشاكل عائلية تعود لعدم توفر الأموال أو الحاجة لها[1].

فيعتبر السعي إلى تحقيق الكسب المالي غاية الفاعل وهو من بين أكثر الدوافع تحريكا للنجاة لإقتراف الجرائم المعلوماتية ذلك أن خصائص هذه الجرائم وحجم الربح الكبير الممكن تحقيقه من بعضها خاصة غش الحاسوب أو الاحتيال المرتبط بالحاسوب يتيح تعزيز هذا الدافع بما يحقق من ثراء فاحش[2].

ثانيا: دافع التسلية

يعتبر دافع المزاح والتسلية من الدوافع التي تجعل الشخص يقوم بتصرفات وإن كان لا يقصد من ورائها إحداث جرائم وإنما بغرض المزاح فقط ولكن هذه التصرفات قد تنتج عنها نتائج ترقى إلى درجة الجريمة[3].

---

[1]– يوسف صغير، المرجع نفسه، ص ص 38-39.

[2]– سفيان سوير، مرجع سابق، ص26.

[3]– يوسف صغير، مرجع سابق، ص 41.

فقد يكون دافع الشخص مجرد اللعب مع أشخاص يكون له معهم صلة إذ أن هذا المزاح قد يتجاوز الحدود المعروفة إذ تصير هذه التصرفات مبالغ فيها إذ تتحول إلى جريمة مرتكبة دون قصد.

المطلب الثاني

العقوبات المقررة لجريمة الدخول والبقاء

تعاقب غالبية التشريعات الحديثة على الدخول والبقاء في نظام الكمبيوتر غير أن موقف التشريعات الحديثة يتباين في تجريم الدخول الغير مصرح به، من بين هذه التشريعات ما يقيد تجريم الدخول بقيد يتولق بالركن المعنوي فيشترط توافر قصد خاص لدى المتهم وهو قصد التأثير في البيانات أو التأثير في نظام الكمبيوتر نفسه للعقاب على هذا الدخول والبقاء ومن هذه القوانين القانون الألماني الكندي والقانون الياباني[1].

ولقد حاولت قوانين العقوبات مواجهة الجرائم المرتكبة عبر الأنترنت بطرق تقليدية كتلك المقررة في جرائم الأموال إلاّ أنه يتبين قصور هذه الرسائل التقليدية عن مواجهة العديد من الأفعال التي تهدد مصالح اجتماعية والتي ارتبطت بظهور وانتشار أجهزة الكمبيوتر[2].

ففي هذا المطلب سنتعرض لفرعين نتناول في الفرع الأول العقوبات المقرر في الدول العربية أما الفرع الثاني سنوضح العقوبات المقررة في الدول الغربية.

[1]– خالد ممدوح إبراهيم، مرجع سابق، ص278.

[2]– يوسف صغير، مرجع سابق، ص60.

الفرع الأول: العقوبات المقررة في الدول العربية

من الدول العربية التي جرمت الدخول والبقاء غير المشروع للنظام المعلوماتي بنصوص صريحة دولة سلطنة عمان، التي نص قانون العقوبات فيها على أنه يعاقب الفاعل لهذا النوع من الجرائم بالسجن لمدة لا تقل عن ثلاثة أشهر وات تزيد عن سنتين وبغرامة مالية تقدر بـ 1000 ريال إلى 5 000 ريال أو بإحدى هاتين العقوبتين[1].

ولقد أورد المشرع السوداني من خلال قانون الجرائم المعلوماتية لسنة 2007 من خلال المادة الرابعة منه المنظمة لعملية دخول المواقع وأنظمة المعلومات المملوكة لغير عقوبة السجن لمدة لا تزيد عن السنتين أو بغرامة مالية أو بالعقوبتين معا وأيضا كل من قام بإلغاء بيانات أو معلومات ملكا للغير أو حذفها أو تغييرها أو تدميرها أو إفشائها أو إتلافها أو إعادة نشرها أو تغير تصاميم الموقع أو إلغاء أو شغل عنوانه يعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بغرامة أو بالعقوبتين معا[2].

ويعاقب بالحبس مدة لا تزيد عن ثلاث سنوات وبغرامة لا تتجاوز عشرة آلاف ريال أو بإحدى العقوبتين كل من توصل بطريق الإحتيال إلى نظام المعالجة الآلية للمعطيات المحفوظة في جهاز حساب آلي، أو ضبطه داخله، أو في جزء منه بدون زجه حق، هذا ما نص عليه المشرع القطري من خلال قانون العقوبات رقم 11 لسنة 2004 من خلال نص المادة 1/378.[3]

ومن هذه التشريعات أيضا القانون السعودي بشأن مكافحة جرائم المعلوماتية لسنة 2007 حيث جرم هذا القانون الدخول والبقاء غير المشروع بطريقة متعمدة غلى الكمبيوتر أو موقع إلكتروني أو نظام معلوماتي أو شبكة حاسبات آلية غير مصرح لذلك

---

[1]– نهلا عبد القادر المومني، مرجع سابق، ص 162.

[2]- حنان ريحان مبارك المضحي، مرجع سابق، ص117.

[3]- حنان ريحان مبارك المضحي، المرجع نفسه، ص118.

الشخص بالدخول إليها فيعاقب بالحبس مدة لا تزيد على أربع سنوات وبغرامة لا تزيد عن ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين.[1]

أما المشرع الإماراتي فقد نص المادة الثانية من قانون مكافحة تقنية المعلومات كل فعل عمدي يتوصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو يتجاوز مدخل مصرح به، يعاقب عليه بالحبس وبالغرامة أو بإحدى هاتين العقوبتين وإذا ترتب على الفعل إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات فيعاقب بالحبس مدة لا تقل ستة أشهر أو بالغرامة أو بإحدى عاتين العقوبتين.[2]

كما استحدث المشرع الجزائري بدوره نصوصا عقابية لقمع الاعتداءات المعلوماتية بتعديل قانون العقوبات فقد جرم المشرع الجزائري في هذا التشريع فعل الدخول والبقاء غير المشروع بعقوبة الحبس أو الغرامة(، وتضاعف العقوبة إذ ترتب على ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة من سنة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج[3].

وقد أقر المشرع الجزائري مبدأ مسائلة الشخص المعنوي في القانون 04-15 المؤرخ في 2004/11/10 المعدل والمتمم للأمر 66-156 المؤرخ في 1966/06/08 المتضمن قانون العقوبات وذلك بنص المادة 51 مكرر من هذا التعديل، كما حددت ثلاثة شروط لإمكان مسائلة الشخص المعنوي جنائيا والتي حددها كالتالي:

---

[1]- حنان ريحان مبارك المضحي، مرجع سايق، ص ص 278-279.

[2]- حنان ريحان مبارك المضحي، المرجع نفسه، ص118.

[3]– زيدان زبيحة، مرجع سابق، ص49.

1- أن يرتكب إحدى الجرائم المنصوص عليها قانونا.

2- أن تكون بواسطة أعضاء أو ممثلي الشخص المعنوي.

3- أن ترتكب الجريمة لحساب الشخص المعنوي. [1]

كما نصت المادة 18 مكرر من قانون العقوبات على مايلي: العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات والجنح هي:

1- الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

2- واحدة أو أكثر من العقوبات التالية:

- حل الشخص المعنوي.
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس سنوات.
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات.
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر نهائيا.
- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.
- نشر تعليق حكم الإدانة.
- الوضع تحت الحراسة القضائية لمدة لا تزيد عن 5 سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكب الجريمة بمناسبته.

ومن هذا المنطق فقد عاقب المشرع الجزائري في المادة 394 مكرر الشخص المعنوي في حالة ارتكابه إحدى جرائم الإعتداء على نظام المعالجة الآلية للمعطيات بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي[1].

[1]–مسعود خثير، مرجع سابق، ص127.

إضافة إلى جانب العقوبات الأصلية هناك عقوبات تكميلية ورد ذكرها في نص المادة 394 مكرره وهي مصادر الأجهزة والبرامج والوسائل المستخدمة لإرتكاب الجرائم الماسة بالنظام وذلك ببيعها أو حجزها مع مراعاة حقوق الغير.

مما ينتج عنه إلى إغلاق المواقع أي موقع الأنترنت أو المواقع الإلكترونية بصفة عامة والتي كانت وسيلة لارتكاب هذه الجرائم أو المساهمة في ارتكابها [2]، أدى رواج المعلومات في كل الدول العربية إلى ظهور عدة ممارسات إجرامية في مجال الجرائم المعلوماتية مما حذا بهذه الدول إلى المحاولة لإيجاد سبل تشريعية وإجرائية ناجمة لمواجهة هذا النوع من الجرائم المستحدثة ونجد من تلك الجهود القرار الصادر عن مجلس وزراء العدل العرب الخاص بإصدار القانون الجزائي الموحد كقانون عربي نموذجي أين نجد الباب السابع خاص بالجرائم ضد الأشخاص.[3]

ولقد دفع القصور الذي عرفه القانون رقم 04-15 المعدل لقانون العقوبات الجزائري الذي ينص على حماية جزائية نسبية لأنظمة المعلومات من خلال تجريم مختلف أنواع الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات بالمشرع الجزائري إلى سد الفراغ التشريعي الذي يعرفه مجال الجرائم المتعلقة بوسائل الإعلام والإتصال وخاصة الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت خاصة في ظل الثورة التي تعرفها في مجال استخدام الأنترنت وذلك بوضع هذا القانون من أجل تعزيز القواعد السابقة من خلال وضع إطار قانوني أكثر ملائمة مع خصوصية الجريمة المرتكبة عبر الأنترنت.[4]

---

[1]– مسعود خثير، مرجع سابق، ص ص 128-129.

[2]– مسعود خثير، المرجع نفسه، ص ص130-131.

[3]–يوسف صغير، مرجع سابق، ص101.

[4]– يوسف صغير ، مرجع سابق، ص102.

ومن ناحية أخرى قام المشرع المصري برصد ومتابعة جرائم التطور التكنولوجي وتتبع مرتكبيها من خلال أحداث النظم الفنية والتقنية الحديثة ويتم تقنين الإجراءات بعد عملية التتبع الفني وضبط القائم بإرتكاب الجريمة التي يكون تكييفها القانوني من خلال قانون العقوبات والجريمة التي تتعامل معها الإرادة تتمثل في الأنشطة الغير قانونية التي يكون فيها الكمبيوتر وسيلة أو غاية أو كليهما وتتخذ أشكالا متعددة بما فيها الدخول إلى أجهزة الحاسب الآلي للغير وسرقة المعلومات التي تمثل سرية خاصة لبعض الأشخاص أو المؤسسات.[1]

الفرع الثاني: العقوبات المقررة في الدول الغربية

لقد نصت العديد من الدول الغربية على ضرورة مكافحة الجرائم المعلوماتية بحيث أوردت نصوص صريحة بخصوص جريمة الدخول والبقاء فقد كان المشرع الأمريكي سباق في تقرير العقاب على هذا النوع من الجرائم فمنذ عام 1984 تمّ إصدار قانون تزيين آليات الدخول والإساءة و الاحتيال عبر الكمبيوتر الذي يعد أول تشريع عالمي في هذا الإطار وبالتالي تم اعتبار كل دخول غير مشروع إلى معلومات مصنفة في حاسوب جنحة، أما إذا كان الدخول غير المشروع قاصدا سجلات مالية أو سجلات ائتمان في المؤسسة المالية أو انتهاك حرمة كمبيوتر الحكومة الفيدرالية فإن الجريمة تأخذ شكل جناية.

وقد مر القانون الأمريكي بعدة تعديلات كان أو لها في 1986 وثانيها في 1994 أما التعديل الثالث فقد جاء سنة 1996[2].

[1]– عبد العال الديري، محمد صادق إسماعيل، الجرائم الإلكترونية، ط1، المركز القومي، مصر، 2012، ص115.

[2]– خالد ممدوح إبراهيم، مرجع سابق، ص264.

وفي فرنسا صدر قانون 05 يناير 1988 بشأن جرائم الغش المعلوماتي المرتكبة ضد النظم المعلوماتية، وتضمن هذا القانون عدة مواد منها نص المادة 2/362 والتي تجرم الدخول والبقاء غير المشروع في كل أو جزء من نظام المعالجة الآلية للمعطيات وذلك بعقوبة الحبس الذي لا يقل عن شهرين ولا يزيد عن خمسين ألف فرنك أو بإحدى هاتين العقوبتين.

وإذا نتج عن الدخول أو البقاء غير المشروع محو أو تعديل في المعطيات المخزنة في النظام تكون العقوبة بالحبس لمدة تتراوح ما بين شهرين إلى سنتين والغرامة التي تتراوح ما بين عشرة آلاف إلى مائة ألف فرنك، وبعد تعديل القانون لعام 1994 بالمادة 1/323 طبق عقوبة الحبس لمدة سنة ومائة ألف فرنك فرنسي وفي حالة ما إذا نتج عن الدخول غير المشروع محو أو تعديل في المعلومات الموجودة بالنظام تكون العقوبة الحبس سنتين ومائتين ألف فرنك فرنسي غرامة[1].

وإذا وقعت تلك الجريمة من شخص معنوي سواء باعتباره فاعلا أو مساهما فيها توقع عليه عقوبة الغرامة فقط التي تصل إلى خمسة أضعاف الغرامة التي يحكم بها الشخص الطبيعي كما توقع على المحكوم عليه العقوبة الإضافية المنصوص عليها في المادة 6/323 إذا كان المحكوم عليه شخص معنويا[2].

ومن بين التشريعات الغربية التي أشارت إلى جرائم الإعتداء على نظم المعالجة الآلية للمعطيات التشريع الجنائي البلجيكي بعد تعديله بالقانون الصادر بتاريخ 2000/11/28 وذلك من خلال نص المادة 550 حيث جاء من خلالها عقوبة الحبس

[1]– خالد ممدوح إبراهيم، مرجع سابق، ص ص 266-267.

[2]– علي عبد القادر القهوجي، مرجع سابق، ص138.

من ثلاثة أشهر إلى سنة أو بغرامة أو بإحدى هاتين العقوبتين فقط وكل من يتجاوز المسموح به في الدخول إلى نظام معلوماتي بنية الإحتيال أو إلحاق ضرر يعاقب بالحبس من ستة أشهر إلى سنتين وبالغرامة من 26 فرنك إلى 5000 2 فرنك أو بإحدى هاتين العقوبتين فقط[1].

وقد نصت اتفاقية بودابست لسنة 2001 بشأن مكافحة جرائم القضاء المعلوماتي في المادة الثانية منها والمتعلقة بالدخول غير المشروع للنظام المعلوماتي بأنه يجب على كل طرف أي الدول الموقعة أن تتبنى الإجراءات التي تنص عليها الاتفاقية.

وعليه فإن مجرد الدخول الغير مصرح به بمعنى القرصنة أو السطو أو الدخول غير المشروع في النظام المعلوماتي يعتبر في حد ذاته غير قانوني وذلك على أساس أن هذه الأفعال يمكن أن يترتب عليه الدخول إلى بيانات سرية كذلك فإن هذا الدخول غير مشروع يساعد القراصنة على ارتكاب جرائم معلوماتية أخرى[2].

لا تعتبر اتفاقية بودابست المشروع الأول الذي بذله المجلس الأوربي في هذا المجال بل بذل جهود عديدة من قبل، نذكر منها على سبيل المثال اتفاقية تتعلق بحماية الأشخاص في مواجهة المعالجة الإلكترونية للمعطيات ذات الصبغة الشخصية وذلك في 28 يناير 1981 لكن تبقى اتفاقية بودابست الحيز الأمثل لمواجهة الجريمة المرتكبة عبر الأنترنت[3].

---

[1]– خالد ممدوح إبراهيم، مرجع سابق، ص ص 270-271.

[2]–خالد ممدوح إبراهيم، المرجع نفسه، ص ص 277-278

[3]– محمود أحمد عبابنة، مرجع سابق، ص 164.

وتتطلب الوقاية نوعية فردية وأسرية ومؤسساتية ومجتمعية بالذات مع التقنية السريعة الأداء والدقيقة في الإستخدام والماهرة في الوصول إلى الأهداف والممارسة في أجراء مجهولة في الإتصال والكثافة في الإستعمال والتنوع في الأغراض والأهداف، إذ تم ابتكار الأجهزة الإلكترونية (الحاسوب والهاتف المحمول) من أجل استخدامها في العلاقات والعمليات التجارية والصناعية.

خلاصة الفصل الثاني:

اختلف موقف التشريعات المقارنة في تصنيف جريمة الدخول والبقاء بين جنح وجنايات ويرجع الإختلاف في هذه الدول إلى السياسة الجنائية التي تنتجها كل دولة بالإضافة إلى نوع أو درجة التعامل بالشبكة المعلوماتية في كل دولة غير أنه عند تقييم هذه التشريعات نرى أن الجرائم المعلوماتية بشكل عام تشكل جنحا لكون عقوبتها توصف بالحبس أو الغرامة أو الحكم بالعقوبتين معا آخرين في الإعتبار طبيعة هذه الجرائم فيمكن أن تنص التشريعات على هذه العقوبة ولكنها ترفع من الحد الأقصى أو الأدنى للغرامة .

غير أن هناك من الدول من تصنف جرية الدخول والبقاء بالجناية نظرا إلى المحل الذي تقع عليه والمصلحة التي تهددها كان تمس بالحياة الخاصة أو بأمن الدولة الداخلي أو الخارجي فتوصف الجريمة في هذه الحالة على أنها جناية وتقررها عقوبة الحبس.

Nom du document : الفصل الثاني حسين
Répertoire : H:\memoire droit lila
Modèle : C:\Users\fathi\AppData\Roaming\Microsoft\Templates\Normal.dotm
Titre : الفصل الثاني: الإطار القانوني لجريمتي الدخول والبقاء الغير مشروع لنظام المعالجة الآلية للمعطيات
Sujet :
Auteur : ets
Mots clés :
Commentaires :
Date de création : ص 02:58:00 2019/10/21
N° de révision : 21
Dernier enregistr. le : ص 10:51:00 2020/02/22
Dernier enregistrement par : fathi
Temps total d'édition : 405 Minutes
Dernière impression sur : ص 11:06:00 2020/02/22
Tel qu'à la dernière impression
Nombre de pages : 29
Nombre de mots : 4 958 (approx.)
Nombre de caractères : 28 263 (approx.)

خاتمة

خاتمة:

أصبحت المعلوماتية سمة العصر وبات استخدام الأنظمة المعلوماتية من قبل الدول والأفراد المقياس الذي يحدد مدى تطور الشعوب وتقدمها فتكنولوجيا المعلومات تساهم في تسريع إنجاز الأعمال، الأمر الذي يعني تنفيذ الأهداف والخطط التي ترسمها الدول لتحقيق التنمية الاقتصادية والاجتماعية في وقت قياسي ومن هنا أصبح لزاما على الدول من أجل ضمان نهضتها وتماشيا مع عصر المعلوماتية الذي لا ينتظر أحدا أن يعل على مواكبة التطور التكنولوجي الذي نجم عن تحول العديد من المجتمعات إلى مجتمعات معلوماتية تعتمد على التقنية الرقمية في أداء أعمالها.

إلاّ أن عصر المعلوماتية خلف ورائه آثارًا سلبية نجمت عن استغلال بعض الأفراد والجهات للتقنيات المعلوماتية في غير الفرض الذي خلقت من أجله الأمر الذي أثر على حقوق الأفراد وحرياتهم.

وتعد جريمة الدخول والبقاء الغير مشروع من الجرائم المعلوماتية التي تقع على أنظمة المعالجة الآلية للمعطيات وتعني قيام الجاني بالدخول والإطلاع على المعلومات المخزنة حيث يقوم المجرم المعلوماتي بالاعتداء على المعطيات مع عدم حصوله على ترخيص للدخول أو البقاء في أنظمة المعالجة، ولردع هذا النوع من الجرائم لابد من النص على عقوبات لها للحد منها وأيضا لحل الغموض الكامن في الجرائم المعلوماتية.

من خلال ما تعرضنا إليه نستخلص أهم النتائج:

- رغم أهمية برامج الحماية التقنية للأنظمة ودورها الفعال في صد مختلف الاعتداءات على تلك الأنظمة، لاسيما إذا كانت تحوي معطيات مهمة وحساسة، ورغم أن المنطق السليم يقتضي عدم الاستغناء عن تلك الحماية، خاصة عند الربط بشبكة الأنترنت وما يشكله من

مخاطر الاعتداء على تلك الأنظمة، رغم ذلك فإن المشرع الجزائري لم يشر إلى ضرورة أن يكون نظام المعالجة الآلية للمعطيات محميًّا ببرامج أمان، وإنما جاءت الحماية الجنائية عامة ، لتشمل كل الأنظمة، سواء كانت محمية من الناحية التقنية أو غير محميّة.

انطلاقا من ذلك يتضح لنا أن جريمة والبقاء صورة من صور الجريمة المعلوماتية حيث سهلت هذه التقنية ارتكاب الكثير من الجرائم وقد ازدادت هذه المخاطر تفاقما في البيئة الإفتراضية.

ولمكافحة هذا النوع من الجرائم لابد من:

- نقترح توحيد المصطلح بين مختلف القوانين ذات الصلة، وإستخدام مصطلح "النظام المعلوماتي"، في عنوان الفصل المتضمن لصور الجرائم المعلوماتية في قانون العقوبات وحتى على مستوى مضامين النصوص القانونية الاجرائية المرتبطة بها ، بوصفه المصطلح الأكثر شمولا للمعنى والأوسع إستخداما من قبل القوانين المقارنة، فضلا عن أنه المصطلح المستخدم من طرف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 والتي صادقت عليها الجزائر في الثامن من سبتمبر 2014.
- تطوير أساليب حماية المعلومات مسبقا كإجراء وقائي وذلك بتحديث أساليب تخزين وحماية المعلومات بوسائل متطورة.
- ضرورة استغلال الأجهزة المعنية لمكافحة هذه الجريمة قصد استغلال التطور التكنولوجي الحاصل في هذا المجال لمكافحة هذه الأفعال.
- تشجيع أصحاب الأنظمة المعلوماتية لحماية أنظمتهم ببرامج الحماية التقنية لاسيما في ظل انفتاحها على الأنترنت، فإننا نقترح على المشرع الجزائري تشديد العقوبة (ظرف تشديد) إذا تعلق الاعتداء بنظام محمي تقنيا، في مقابل كون الجريمة مجردة إذا كان النظام المعتدى عليه غير محمي من الناحية التقنية.

- تكوين الأجهزة المكلفة بمكافحة وتتبع هذه الجرائم في المجال المعلوماتي حتى يكونوا في مستوى التطور الذي تعرفه هذه الجريمة.
- يجب على المشرع الجزائري توفير حماية أكبر للأنظمة المعلوماتية، ولاسيما في مواجهة الأشخاص المنوط بهم التعامل مع هذه الأنظمة أو العاملين والموظفين الذين يملكون هذه الصلاحية، لأن بعضا من هؤلاء قد يستغل هذه الصلاحية للاعتداء على النظام ومحتوياته، وعليه نقترح تشديد العقوبة إذا تم الاعتداء على النظام من طرف عامل أو موظف له علاقة بالنظام وسهلت له وظيفته القيام بالجريمة.

Nom du document : خاتمة
Répertoire : H:\memoire droit lila
Modèle : C:\Users\fathi\AppData\Roaming\Microsoft\Templates\Normal.dotm
Titre : خاتمة
Sujet :
Auteur : ets
Mots clés :
Commentaires :
Date de création : م 01:20:00 2019/11/02
N° de révision : 5
Dernier enregistr. le : ص 11:01:00 2020/02/22
Dernier enregistrement par : fathi
Temps total d'édition : 11 Minutes
Dernière impression sur : ص 11:06:00 2020/02/22
Tel qu'à la dernière impression
Nombre de pages : 4
Nombre de mots : 487 (approx.)
Nombre de caractères : 2 778 (approx.)

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أ- الكتب:

1- أحمد خليفة الملط، الجرائم المعلوماتية، طبعة الثانية، دار الفكر الجامعي، مصر، 2006.

2- أسامة أحمد مناعسة، جلال محمد الزعبني، جرائم تقنية المعلومات الالكترونية طبعة الثانية، دار الثقافة للنشر والتوزيع الأردن 2014 .

3-أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، طبعة الأولى، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2006.

4- بلال أمين زين الدين، الجريمة المعلوماتية في التشريع المقارن والتشريعية الإسلامية، دار الفكر الجامعي، مصر، 2014.

5- حنان ريحان مبارك المضحكي، الجريمة المعلوماتية، طبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2014.

6- خالد ممدوح إبراهيم الجريمة المعلوماتية طبعة الأولى، دار الفكر الجامعي مصر 2009.

7- زيدان زبيحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2011.

8- شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، مصر، 2007.

9- عبد الحليم موسى يعقوب، الإعلام الجديد والجريمة الإلكترونية، طبعة الأولى، الدار العالمية للنشر والتوزيع، السعودية، 2014.

10- عبد العال الديري، محمد صادق إسماعيل، الجرائم الإلكترونية، طبعة الأولى، المركز القومي، مصر، 2012.

11- عبد الله أوهايبية، شرح قانون العقوبات الجزائري، القسم العام المؤسسة الوطنية للفنون المطبعية الموفم للنشر، الجزائر، 2009

12- عبد الله سليمان سليمان، المقدمات الأساسية في القانون الدولي الجنائي، ديوان المطبوعات الجامعية: الجزائر.

13- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، لبنان، 1999.

14- غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والأنترنت، دار الفكر والقانون مصر، 2010.

15- فؤاد حسين العزيزي، الجرائم المعلوماتية، طبعة الأولى، دار الفكر الجامعي، مصر 2014.

16- محمد أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، طبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2009.

17- محمد أمين الرومي، جرائم الكمبيوتر والأنترنت، دار المطبوعات الجامعية، مصر، 2004.

18- محمد أمين، الشوابكة جرائم الحاسوب والأنترنت، طبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2007.

19- محمد حماد مرهج الهيتي، جرائم الحاسوب ، طبعة الأولى، دار المناهج للنشر والتوزيع ، الأردن 2006.

20- مسعود خثير ، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2010

21- مصطفى محمد موسى، التحقيق في الجرائم الإلكترونية طبعة الأولى، مطابع الشرطة مصر 2009.

22- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي، مصر.

23- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، طبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2005.

24- نهلا عبد القادر المومني، الجرائم المعلوماتية، طبعة الأولى، دار الثقافة للنشر والتوزيع، عمان 2008.

ب- الرسائل العلمية:

1- بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير في القانون الجنائي، زهدور محمد، جامعة وهران، كلية الحقوق والساسية، 27-06- 2013، 2012-2013.

2- سفيان سوير، الجرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، محمد بن عمار، جامعة أبو بكر بلقايد، كلية الحقوق والعلوم السياسية، 2010.

3- يوسف صغير، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، محمد إقلولي، جامعة مولود نعمري، كلية الحقوق والعلوم السياسية، 2013/03/06، 20134-2014.

ج- نصوص قانونية

1- قانون 15/04 المؤرخ في 27 رمضان 1425 هـ الموافق لـ 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 155/06 المؤرخ في 18 صفر 1386 الموافق لـ 8 يونيو 1966 المتضمن قانون العقوبات، جريدة رسمية عدد 71 بتاريخ 2004.

2- قانون رقم 06-23 المؤرخ في29 ذو القعدة 1427 الموافق لـ 20 ديسمبر 2006. يعدل ويتمم الأمر 66/ 156 المؤرخ في 18 صفر 1386 الموافق لـ 8 يونيو 1966، المتضمن العقوبات، جريدة رسمية عدد 84، بتاريخ 24 ديسمبر 2006.

Nom du document : المراجع
Répertoire : C:\Users\fathi\Documents
Modèle : C:\Users\fathi\AppData\Roaming\Microsoft\Templates\Normal.dotm
Titre : قائمة المصادر والمراجع
Sujet :
Auteur : ets
Mots clés :
Commentaires :
Date de création : ص 05:19:00 2019/10/24
N° de révision : 13
Dernier enregistr. le : ص 11:07:00 2020/02/22
Dernier enregistrement par : fathi
Temps total d'édition : 47 Minutes
Dernière impression sur : ص 11:07:00 2020/02/22
Tel qu'à la dernière impression
Nombre de pages : 5
Nombre de mots : 534 (approx.)
Nombre de caractères : 3 049 (approx.)

فهرس المحتويات

فهرس المحتويات

شكر وعرفان...../

إهداء...../

مقدمة.....2

الفصل الأول: ماهية جريمة الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات

المبحث الأول: ماهية جريمة الدخول غير المشروع لنظام المعالجة الآلية للمعطيات....7

المطلب الأول: مفهوم جريمة الدخول غير المشروع لنظام المعالجة الآلية للمعطيات...8

الفرع الأول: تعريف جريمة الدخول غير المشروع لنظام المعالجة الآلية للمعطيات.....8

الفرع الثاني: تقنيات ارتكاب جريمة الدخول والبقاء غير مشروع.....9

الفرع الثالث: اختلاف جريمة الدخول عن استعمال النظام.....10

المطلب الثاني: صور وآليات جريمة الدخول غير المشروع لنظام المعالجة الآلية للمعطيات.....11

الفرع الأول: صور وآليات جريمة الدخول غير المشروع لنظام المعالجة الآلية للمعطيات12

أولا: حالة عدم وجود التصريح للدخول إلى نظام المعلوماتية.....12

ثانيا: حالة تجاوز حدود التصريح.....13

الفرع الثاني:آليات جريمة الدخول غير المشروع لطرق و وسائل الدخول غير المشروع.14

أولا: طرق الدخول غير المشروع 14

ثانيا: وسائل الدخول غير المشروع لنظام المعالجة الآلية للمعطيات.....15

المبحث الثاني: ماهية جريمة البقاء غير المشروع في نظام المعالجة الآلية للمعطيات..17

المطلب الأول: مفهوم جريمة البقاء غير المشروع لنظام المعالجة الآلية للمعطيات....18

الفرع الأوّل: تعريف جريمة البقاء غير المشروع لنظام المعالجة الآلية للمعطيات.....18

الفرع الثاني: اختلاف جريمة البقاء عن جريمة الدخول.....20

المطلب الثاني: صور وأساليب جريمة البقاء غير المشروع.....21

الفرع الأول: صور جريمة الدخول غير المشروع لنظام المعالجة الآلية للمعطيات....21

أولا: جريمة البقاء مع تجاوز الوقت المصرح به.....21

ثانيا:جريمة البقاء مع التجاوز إلى أشياء أخرى.....22

الفرع الثاني: أساليب جريمة البقاء غير المشروع لنظام المعالجة الآلية للمعطيات.....23

خلاصة الفصل الأول:..... 26

الفصل الثاني: الإطار القانوني لجريمتي الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات

المبحث الأول: أركان جريمة الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات.....29

المطلب الأول: الركن الشرعي والركن المفترض لجريمة الدخول والبقاء الغير مشرع.....29

الفرع الأول: الركن الشرعي لجريمة الدخول والبقاء الغير مشرع.....30

الفرع الثاني: الركن المفترض.....31

أولا: وجود نظام معالجة آلية للمعطيات.....31

ثانيا: خضوع النظام للحماية.....31

المطلب الثاني: الركن المادي والركن المعنوي.....33

الفرع الأول: الركن المادي.....33

أولا: الصورة البسيطة.....34

ثانيا: الصورة المشددة 35

الفرع الثاني: الركن المعنوي لجريمة الدخول والبقاء الغير مشرع.....36

أولا: المقصود بالقصد الجنائي العام.....37

ثانيا: إمكانية توافر القصد الجنائي الخاص في جريمة الدخول والبقاء عن طريق الغش لنظام المعلوماتية.....39

المبحث الثاني: دوافع ارتكاب جريمة الدخول والبقاء غير المشروع والعقوبات المقررة لها...42

المطلب الأول: دوافع ارتكاب جريمة الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات.....43

الفرع الأول: الدوافع الشخصية..... 43

أولا: الدوافع الذهنية.....44

ثانيا: دافع الإنتقام.....44

الفرع الثاني: الدوافع المادية.....45

أولا: تحقيق مكسب مادي.....45

ثانيا: دافع التسلية.....45

المطلب الثاني: العقوبات المقررة لجريمة الدخول والبقاء.....46

الفرع الأول: العقوبات المقررة في الدول العربية.....47

الفرع الثاني: العقوبات المقررة في الدول الغربية.....51

خلاصة الفصل الثاني: 55

خاتمة.....57

قائمة المصادر والمراجع.....61

فهرس المحتويات.....65