Abhat Journal: Volume. 15, Issue. 1, March 2023

Abhat Journal, Faculty of Arts, Sirte University مجلة أبحاث بكلية الآداب جامعة سرت

Source Homepage: http://journal.su.edu.ly/index.php/ABHAT/index

جرائم التجسس الإلكتروني للمعلومات الشخصية في إطار اتفاقية بودابست بشأن الجريمة الإلكترونية

د. عبير على حسين الورفلي
h19451939@gmail.com
قسم القانون / الجامعة المفتوحة/ ليبيا

الملخّص

تهدف الدراسة إلى تحديد أبرز مجالات وأساليب التجسس الإلكتروني ، وذلك بشرح وتحليل الأحكام العامة لجرائم التجسس الإلكتروني للمعلومات الشخصية وفقًا لنصوص اتفاقية بودبست بشأن الجرائم الإلكترونية. وانطلاقاً من حجم المخاطر الجديدة على سرية المعلومات الإلكترونية ، والارتفاع الهائل والمتزايد لظاهرة اختراق خصوصية المعلومات ، وتأثيرها على الحياة الخاصّة والعامة ، ظهرت عدة تساؤلات حول ماهي أبرز مجالات وأساليب التجسس الإلكتروني للمعلومات الشخصية والتي تشكل خطراً على أمن المعلومات والبيانات الشخصية في إطار اتفاقية بودابست ، وأبرز صورها وأركانها وسُبل مكافحتها. وأمام هذه التساؤلات وباستخدام المنهج التحليلي والاستقرائي توصلت الدراسة إلى عدة نتائج أبرزها: أن جرائم التجسس الإلكتروني والمتعلقة بحماية البيانات الشخصية الإلكترونية تُعدّ صنفاً مستحدثاً من الجرائم التي تتحدى القواعد التقليدية للتجّريم والعقاب، والتي تقضي ضرورة تحقيق أركان الجريمة طبقاً لمبدأ المشروعية للجرائم والعقوبات. كما اشتملت الاتفاقية على جوانب تفصيلية لأنواع جرائم التجسس الإلكتروني بما يكفي أن نستوحي منها الكثير، ونستثمر الجهود المبذولة هناك على أكثر من صعيد.

الكلمات المفتاحية:

الجرائم الإلكترونية، التجسس الإلكتروني، اتفاقية بودابست.

Crimes of Electronic Espionage of Personal Information within the Budapest Convention on Cybercrime

Dr. Abear Ali Hussein Elwarfilee
h19451939@gmail.com
The Open University/ Libya

Abstract

The study aims to identify the most prominent areas and methods of electronic espionage, by explaining and analyzing the general provisions of electronic espionage crimes for personal information in accordance with the provisions of the Budapest Convention on Electronic Crimes. And based on the magnitude of the new risks to electronic information, the huge and increasing phenomenon of information privacy breaches, and its impact on private and public life, several questions arose about what are the most prominent areas and methods of electronic espionage of personal information, which pose a threat to the security of information and personal data within the framework of the Budapest Convention, and What are its most prominent images, pillars, and ways to combat them?. Answering these questions, using the inductive descriptive approach, the study reached several results, the most important of which are:

Cyber espionage crimes related to the protection of electronic personal data are an emerging category of crimes that challenge the traditional rules of criminalization and punishment, which requires that the elements of the crime must be fulfilled in accordance with the principle of legality of crimes and penalties. In this regard, it is necessary for legislative intervention to amend the texts of the Libyan Penal Code or to establish special legislative rules for the protection of electronic personal data.

Keywords

Electronic espionage, Budapest Convention, Electronic Crimes.

المقدمة:

لقد أضحت الحاسبات الآلية ضرورة في كافة المجالات، حيث تعهد مختلف الإدارات والمؤسسات والمنظمات في كل من القطاع الحكومي والقطاعات الخاصة بمعلوماتها الأكثر سرية إلى الحاسبات الإلكترونية، مولية نظم تلك الحاسبات الأمنية ثقتها، وجاهلة أو متناسية أن هذا الجهاز كثيراً ما بدأ وفقاً لوصف بعض الباحثين (1) كخزانة بغير أبواب، وقد أدى هذا الاستخدام المتزايد للحاسبات الآلية في مختلف المجالات إلى تمركز المعلومات بدرجة كبيرة في جميع الدول – المستخدمة لنظم المعلومات – في تلك الأجهزة، كما أدى تخزين هذه البيانات والمعلومات – على هذا النحو – إلى سهولة التجسّس على الأسرار الخاصة، والعامة، ومن ثم أصبحت تلك البيانات والمعلومات المخزنة آليًا في مجالات عديدة تُشكّل الهدف المفضل لأنشطة التجسّس غير المشروع.

أهمية الدراسة:

إن قيام الجاني بالدخول أو الولوج إلى النظام المعلوماتي بقصد الاعتداء على بيانات أو معلومات شخصية غير متاحة للجمهور، أو معلومات تمس الأمن الوطني، أو السلامة العامة، أو الاقتصاد الوطني، من خلال حذفها أو إتلافها أو تدميرها، أم، تعديلها أو تغييرها أو نقلها أو مسحها أو إفشائها يعد جريمة تنال من أسرار الفرد والدولة، واعتداء على حقهم في سرية هذه المعلومات وعدم كشفها.

لذلك فقد بادرت الدول الأوروبية في وضع اتفاقية إقليمية تهدف لحماية خصوصية البيانات الشخصية وحددت في إطارها الانتهاكات التي يمكن أن تطال هذه البيانات، وأوجه الحماية الجنائية المطلوبة.

ولما كانت الجرائم المعلوماتية المرتبطة بخصوصية المعلومات الشخصية تثير كثيراً من الجدل، وتتنوع أساليب ارتكابها وصُورها والتي يصعب الإحاطة بها مجتمعة، لذلك ستقتصر الدراسة على بيان جرائم التجسّس الإلكتروني للمعلومات الشخصية بناءً على ما جاء في الاتفاقية الأوروبية بشأن الجرائم الإلكترونية (بودابست).

أهداف الدراسة:

تهدف الدراسة انطلاقاً من أهميتها إلى ما يلي:

1) تحديد منضبط لأبرز مجالات وأساليب التجسّس الإلكتروني .

2) شرح وتحليل الأحكام العامة لجرائم التجسّس الإلكتروني للمعلومات الشخصية وفقاً لنصوص اتفاقية بودابست بشأن الجرائم الإلكترونية.

إشكالية الدراسة:

تسعى الدراسة إلى فهم وتحليل ظاهرة التجسس الإلكتروني للمعلومات الشخصية والتي جرمتها الاتفاقية الأوروبية بشأن الجرائم الإلكترونية (اتفاقية بودابست) في إطار الإجابة على التساؤلات التالية:

- ما أبرز مجالات وأساليب التجسّس الالكتروني للمعلومات الشخصية؟
- ما هي صور و أركان جرائم التجسّس الالكتروني للمعلومات الشخصية؟

منهج الدراسة:

لاستجلاء مختلف جوانب هذا الموضوع اعتمدت الدراسة بشكل أساسي على المنهج التحليلي، الذي نلمسه بوضوح عند دراسة صور جرائم التجسّس الإلكتروني للمعلومات الشخصية، وبصورة أقل على المنهجين الوصفي والاستقرائي.

خطة الدراسة:

بناء على ما تقدم ستقسم الدراسة إلى مبحثين، يتناول المبحث الأول أساليب ومجالات التجسّس الإلكتروني للمعلومات الشخصية، في حين يتناول المبحث الثاني صور جرائم التجسّس الإلكتروني للمعلومات الشخصية.

المبحث الأول: مجالات وأساليب التجسّس الإلكتروني للمعلومات الشخصية.

إن التطرق لمجالات وأساليب التجسّس الإلكتروني للمعلومات الشخصية يستوجب بداية معرفة المقصود بالمعلومات والتي هي محلّ الجريمة في هذه الدراسة، والتي كثيراً ما كان لها صدى قوي على أسماعنا دون أن يكون لها مفهوم محدد في أذهاننا، لذلك من المفيد أن نضبط هذا المصطلح، وذلك لكي يتسنى لنا الحديث عن تلك المجالات والأساليب في التقسيمات المتقدمة.

ماهية المعلومات: هي "تعبير يستهدف جعل رسالة معينة صادرة من شخص مُعين قابلة للتوصيل إلى شخص آخر، وذلك بفضل علاقة أو إشارة من شأنها أن تُوصِل المعلومة للغير. إذاً هذا التعبير وكيفية

توصيله إلى الغير يُحقق وظيفة المعلومة وهي إمكانية نقل، أو انتقال المعرفة"(2).

كما يعرفها آخرون " بأنها علم التعامل العقلاني على الأخصّ بواسطة آلات أتوماتيكية مع المعلومات باعتبارها دعامة المعارف الإنسانية، وعمادًا للاتصالات في ميادين التقنية والاقتصاد والاجتماع "(3)، ويعرفها آخر " بأنها المعلومات المبرمجة آليًا والتي تُستخدم التقنية الحديثة المتمثلة في الحاسبات الآلية، وأنظمتها والتعامل معها"(4)، أم هي: " نظم وشبكات ووسائل المعلومات، والبرمجيات والحواسيب، والإنترنت، والأنشطة المتعلقة بها "(5).

ومن مجمل ما تقدم ترى الباحثة أن المعلومات هي "جملة البيانات والدلالات والمعارف والمضامين التي تتصل بالشيء أو الموضوع، وتساعد المهتمين بالتعّرف عليه والعلم به. فالمعلومات إذن توضح مفهوم الشئ وتعطيه قدره، وتوضح سماته وخصائصه، وتبيّن استخداماته ووظائفه".

عناصر المعلومة: ويتضح من خلال التعريفات السابقة أن هناك عناصر للمعلومات يمكن حصرها فيما يلي:

1) **كون المعلومة محددة ومبتكرة:** يجب أن تكون المعلومة محددة، ويرجع السبب في ذلك إلى ضرورة حصرها في نطاق معين. ومن أجل ذلك ذهب الأستاذ كاتالا إلى القول: " بأن المعلومة وقبل كل شيء هي تعبير، وصياغة مخصصة من أجل تبليغ رسالة، ويمكن تبليغها عن طريق علامات أو إشارات مختارة لكي تُحمل الرسالة إلى الغير"(6).

ومن ناحية أخرى يجب أن تكون المعلومة مبتكرة، أي أنها تتسم بالأصالة أي لم تكن موجودة من قبل. وبمفهوم المخالفة فإن المعلومة غير المبتكرة لا تعد معلومة بالمعنى الفني الدقيق للكلمة. أي أنها معلومة شائعة يسهل الوصول إليها من قبل أي شخص، وتبعاً لذلك فهذه المعلومة لا ترتبط بشخص معين (7).

2) كون المعلومة سرية: يجب أن تكون المعلومة مُحاطة بجدار من السرية أي ضرورة الاحتفاظ بهذه المعلومة في نطاق محدّد من الأشخاص، وبالتالي فإن المعلومة التي لا تتصف بالسرية هي معلومة عامة وشائعة بين الناس أي أنه لا يمكن في هذه الحالة حصر حركة رسالة ما والتي تحمل المعلومة في دائرة معينة من الأشخاص. إذًا فإن صفة السرّية لازمة للمعلومة، وتكتسب المعلومة هذه الصفة الأخيرة إما بإرادة الشخص أو بحسب طبيعتها كاكتشاف شيئ لم يكن معروفاً من قبل(8).

3)ضرورة توافر الاستئثار في المعلومة: خاصية الاستئثار في مجال المعلومات أمر ضروري حتى تستكمل المعلومة عناصرها القانونية، ويقصد بالاستئثار أن المعلومة يجب أن تكون في حوزة شخص معين أي أنها من قبيل الأسرار الخاصّة طالما كان لهذا الشخص سلطة التصرف في المعلومة التي تخصّه، ولذلك فعندما يحدثْ اعتداء غير مشروع على قيم معينة نجد أن الفاعل في هذه الحالة قد استحوذ أو استأثر بسلطة تخص غيره بصفة مطلقة(9).

واستناداً إلى ما تقدم، ستتوزع الدراسة في هذا المبحث على مطلبين، نتناول في **أولهما** مجالات التجسّس الإلكتروني للمعلومات، ونخصص **ثانيهما** لأساليب التجسّس الإلكتروني للمعلومات.

أولا: مجالات التجسّس الإلكتروني للمعلومات:

تتعدد مجالات التجسّس المعلوماتي بتعدد مجالات وأوجه النشاطات المختلفة، فعلى سبيل المثال نجد أنه في مجالات النشاط التجاري ترتكز عمليات التجسّس المعلوماتي على كشف الأسرار التسويقية والتجارية (عناوين العملاء... وغيرها)، وفي مجالات النشاط الصناعي والتقني، تسعى عمليات التجسّس –بصورة كبيرة – إلى كشف نتائج الأبحاث والتطور والبيانات المتعلقة بعمليات الإنتاج، وأسرار تصميمات المنتجات وخاصّة تصميمات الشرائح الصغيرة من أشباه الموصلات، وفي المجالات الأمنية والعسكرية والاستخباراتية والنووية، تُكثف نشاطات التجسّس جل جهودها نحو اختراق النظم الأمنية والعسكرية، والاستخباراتية والنووية للوصول إلى أدق تفاصيل أسرار البيانات والمعلومات المتعلقة بتلك المجالات، بما يكون له من بالغ الأثر على أمن الدولة والحكومات وبقائها(10).

التجسّس المعلوماتي أيضًا في مختلف المجالات وخاصة ما تعلق منها بالمعلومات الشخصية أبعاد خطيرة غير مسبوقة، فالتكثيف المركّز للمعلومات في ذاكرات الحاسبات الآلية يجعلها هدفاً مُغرياً لأي متلصص يملك خبرة كافية وتجهيزات جيدة خاصّة مع إمكانية الاستعانة بالحاسبات الآلية في فرز المعلومات المخزنة، وتصنيفها، ونسخها بسهولة وسرعة فائقة، بغير أن يُخلّف ذلك أي أثر (11).

ثانيا: أساليب التجسّس الإلكتروني للمعلومات:

تتعدد صور وأشكال تخزين البيانات والمعلومات المعالجة إلكترونيًا، فقد تكون تلك البيانات والمعلومات مخزنة على هيئة نبضات كهربائية في دوائر إلكترونية مُجمّعة، أو في وسائط وأوعية معينة

– كالبطاقات الورقية المثقبة، والأشرطة والأقراص المغناطيسية – كما أنها قد تكون في حالة بث وانتقال من نهاية طرفية إلى أخرى، والتوصل غير المشروع إلى تلك البيانات والمعلومات له في كلّ حالة من حالتي تخزين وانتقال البيانات والمعلومات أساليب من أبرزها:

1) **أساليب التجسس والحصول على البيانات والمعلومات المخزنة**: وهذه الأساليب متعددة، ومتدرجة في تعقيدها:

– **أساليب تقليدية**: تتمثل هذه الأساليب في سرقة الأسطوانات التي تخزن فيها البيانات والمعلومات، ورشوة أو تهديد العاملين بالجهة المستهدفة للكشف عن البيانات الشخصية المخزنة داخل حاسباتها، وإلحاق موظفين بالجهة المستهدفة لكي يتولوا مهمة التجسّس من خلال عملهم بها.

– **أساليب فنية**: ومنها دسّ وحدات ناقلة للبيانات داخل أجهزة الحاسب الآلي، وتوصيله كهربائياً بشكل خفي بكابل خارجي، ومعالجة الشرائط، والأسطوانات الممغنطة التي لم تتمكن الجهة المالكة لها من محوها أو إتلافها لإعادة إظهار محتوياتها، واستظهار المعلومات التي تستخدم أوراق الكربون عند تدوينها بمعالجة أوراق الكربون المهملة، وإخفاء برنامج **حصان طروادة** (12) في البرامج التطبيقية بحيث يسمح بالوصول عن بُعْد إلى قاعدة البيانات لقراءتها، أو تعديلها بغير أن يشعر بذلك أحد حيث يتمّ زرعها في جهاز الضحية ؛ ليكون هو حلقة الوصل بين جهاز المخترق وجهاز الضحية، ويطلق على هذا البرنامج أسماء عديدة منها ملف اللاصق أو الصامت أو ملف الباتش وهو الاسم الأشهر في عالم الهاكرز، وهناك طرق عديدة لإرسال هذا البرنامج وزراعته لعلّ أشهرها على الإطلاق هو استخدام البريد الإلكتروني، حيث يقوم المخترق بإرسال رسالة إلى الضحية ويرفق بها ملف حصان طروادة، ونظرًا لعدم إلمام الضحية بمضمون تلك الرسالة فإنه يقوم بفتحها وتحميل الملف المرفق بها اعتقادًا منه أنه يُحمل أحد البرامج المفيدة ثم يكتشف بعد ذلك أن هذا البرنامج لا يعمل فيظنّ أن به عُطل ما فيهمله، وفي ذلك الوقت يكون حصان طروادة قد أخذ مكانه داخل نظام حاسب الضحية وبدأ في مهامه التجسّسية حتى وإن قام الضحية بحذف البرنامج بعد ذلك فلا فائدة من ذلك فملف حصان طروادة يكفيه أن يعمل لمرة واحدة فقط ليقوم بمهامه (13).

كما يمكن أيضًا باستخدام هوائيات متصلة بحاسب خاصّ التقاط وتسجيل ومعالجة الموجات الكهرومغناطيسية التي تنبعث من الحاسب الآلي أثناء تشغيله، وترجمتها إلى بيانات واضحة، وذلك من مسافة تبعُد عن الحاسب المستهدف بما يزيد على الآف الكيلومترات.

كما يمكن كذلك استغلال ما يعرف (بالأبواب الخفية أو الخلفية Back Doors والمعرُوفة أيضًا باسم أبواب المصيدة Trap Doors) (14)، في الوصول غير المشروع وغير المحدّد إلى برامج وملفات بيانات النظام، إذ من المعتاد عند إعداد البرامج ترك ثغرات أو نقاط دخول غير معلن عنها تتجنب إجراءات الأمن العادية، وذلك بهدف السماح بإضافة تعليمات إلى البرامج لتلافي ما قد يظهر فيها من أخطاء، ووجود هذه الثغرات قد لا يكون متعمداً دائمًا حيث يمكن أن توجد عرضاً في بعض الأحيان نتيجة أخطاء في التصميم الكلي للنظام أو نتيجة مواطن ضعف في مجموعة الدارات الإلكترونية للحاسبات الآلية، وعندما يكون تركها مقصودًا فإنها تُلغى في الطبعة النهائية للبرامج، بيد أن هذا الإلغاء قد يتمّ في بعض الأحيان بصورة متعمدة إغفاله وبذلك يكون متاحاً –إذا ما وجدت عمدًا أم عرضًا ثغرات أو نقاط دخول– الوصول إلى أجزاء من النظام غير مصّرح بدخولها، والاطلاع على ملف البيانات المخزنة داخلها(15).

2) أساليب التجسّس والحصول على البيانات والمعلومات المتنقلة:

إذا كانت البيانات والمعلومات في حالة انتقال فيما بين النهايات الطرفية، فإن أساليب التجسّس عليها، والتقاطها تختلف باختلاف الوسيلة الناقلة.

– البيانات التي يجري نقلها عبّر الأسلاك المعدنية، أو خطوط الهاتف المخصّصة لنظم الاتصالات الإلكترونية لا يحتاج معترضها لأكثر من مجرد جهاز التقاط بسيط يمكن تركيبه من وحدات إلكترونية تتوافر في الأسواق، وتثبيته بطريقة خفية داخل صناديق التوزيع التي تنتهي إليها معظم وسائل الاتصال السلكية واللاسلكية، وقد يضاف جهاز بثّ إلى جهاز الالتقاط كي يعمل حسب حال وجود بيانات أو إشارات في السلك أو الخط الذي تجري مراقبته (16).

– المعترض لوصلات الموجة القصيرة المحتوية على حزمة من القنوات المحملة بالبيانات، فإنه يستفيد مما ينتج عن بث هذه الموجات من نتوءات إشعاعية جانبية، وخلفية فيستخدم في مجال أحد هذه النتوءات أجهزة التقاط خاملة لا يصدر عنها أي إشارات لاسلكية، مما يجعل من الصعب اكتشافها (17).

– يمكن اعتراض الاتصالات التي تُبث من المحطات الأرضية في اتجاه الأقمار الصناعية، حيث يمكن أيضًا استغلال ظاهرة التوءات الجانبية والخلفية أما الشعاع الذي يبثه القمر الصناعي إلى الأرض فإنه يُغطي مساحة شاسعة منها تقدر بآلاف الأميال المربعة، ومن أي موقع في نطاق هذه المساحة يمكن – باستخدام أجهزة خاصة – التقاط البيانات والمعلومات المرسلة، حتى أن البيانات التي يتمّ إرسالها بواسطة القمر الصناعي – على سبيل المثال – من ولاية كاليفورنيا جنوب الولايات المتحدة الأمريكية إلى نيويورك بشرقها، يمكن لمعترض في فلوريدا بالجنوب التقاطها(18).

المبحث الثاني: صور جرائم التجسّس الإلكتروني في إطار اتفاقية بودابست.

تناول هذا المطلب بعض صور جرائم التجسّس الإلكتروني والتي يمكن إجمالها في صورتين:

- جريمة الاعتراض غير القانوني لانتقال البيانات.
- جريمة الولوج والبقاء غير المشروع في نظام المعالجة الآلية للبيانات.

أولا: جريمة الاعتراض غير القانوني لانتقال البيانات:

نصتّ المادة الثالثة من اتفاقية بودابست المبرمة في 23 نوفمبر 2001م بشأن الجريمة الإلكترونية، على هذه الجريمة بقولها " يجب على كلّ طرف أن يتبنى الإجراءات التشريعية أو أي إجراءات أخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية وفقاً لقانونه الداخلي واقعة الاعتراض العمدي وبدون حقّ من خلال وسائل فنية للإرسال غير العلني لبيانات الحاسب في مكان الوصول في المنشأة، أو في داخل النظام المعلوماتي بما في ذلك الانبعاثات الكهرومغناطيسية من جهاز حاسب يحمل هذه البيانات.

كما يمكن لأي طرف أن يستلزم أن ترتكب الجريمة عن طريق مخالفة التدابير الأمنية بنية إجرامية أو ترتكب الجريمة في الحواسيب المتصلة عن بعد ببعضها البعض(19).

والهدف من النصّ على هذه الجريمة في سياق المادّة الثالثة من اتفاقية بودابست، هو حماية الحقّ في حرية الاتصالات واحترام نقل البيانات دون التدخل من أطراف أخرى في الحديث، أو المكالمات الهاتفية التقليدية، أو المراسلات البريدية، أو عبر الإنترنت أو بترجمة الانبعاثات الكهرومغناطيسية الصادرة من الحاسب الآلى وصولاً إلى البيانات، وذلك بالنقل أو التسجيل باستعمال أي من الأجهزة الفنية للإرسال غير العلني للمحادثات، أو البيانات أو الملفات أو المراسلات. وسواءً كانت البيانات متداولة عبر الأجهزة الداخلية لنفس الحاسب، أو عن طريق الاتصال عن بعد بالحاسب باستخدام حاسب آخر(20).

كما ينطبق هذا الوصف الإجرامي على كلّ أشكال النقل الإلكتروني للبيانات سواء تمّ عن طريق الهاتف، أو الفاكس، أو البريد الإلكتروني، والخاضع لحماية المادة الثامنة من الاتفاقية الأوروبية لحقوق الإنسان(21).

ومن خلال الاطلاع على نصّ المادة الثالثة من اتفاقية بودابست يتبين أن لهذه الجريمة أركانًا أهمهما: الركن المادي، والركن المعنوي.

– **الركن المادي لجريمة الاعتراض غير القانوني للبيانات:**

يتمثل الركن المادي في جريمة الاعتراض غير القانوني للبيانات في فعل الاعتراض، والذي يقوم به الجاني في الجريمة بدون وجه حقّ وباستخدام الوسائل الفنية غير العلنية.

وهذا يفترض توافر عدة شروط لقيام الركن المادي في جريمة الاعتراض، وقد نصَّت المادة الثالثة من اتفاقية بودابست على عدد من الشروط إلا أنها أجازت للدول الأعضاء إضافة شروط أخرى في حالة تجريمهم لفعل الاعتراض غير القانوني للبيانات في قوانينهم الداخلية، حيث إن الاتفاقية في تناولها لهذا الفعل قد وضعت الإطار العام الذي تستطيع الدول الأعضاء أن تتحرك من خلاله بحرية في وضع وتحديد أركان وشروط هذه الجريمة وما يتلاءم مع كيانها الداخلي.

ولتحديد الركن المادّي لهذه الجريمة وفقاً لنصّ المادة الثالثة من الاتفاقية المشار إليها، وبشيء من الدقة يتطلب الأمر ضبط مصطلح الاعتراض، ومن ثم تفصيل الشروط الواجب توافرها لقيام الركن المادي لهذه الجريمة وفقاً لنصّ المادة الثالثة – المشار إليها –.

1) المقصود بالاعتراض: يقصد بالاعتراض في نصّ المادة الثالثة من الاتفاقية الدولية بشأن حماية البيانات الشخصية (التصنت أو نقل البيانات التي تتمّ داخل جهاز الحاسوب أو التي تتمّ عبر الأجهزة المرتبطة بشبكة المعلومات– المحلية والدولية – أو بترجمة الانبعاثات الكهرومغناطيسية الصادرة من الحاسب إلى بيانات، أو التي تتمّ عبر الأجهزة اللاسلكية، وذلك عن طريق أي من الوسائل الفنية غير المعلنة)(22).

ومن هذا التعريف يتّضح أنّ نصّ المادة الثالثة يشمل وسائل الاتصالات التقليدية فضلاً عن وسائل الاتصال الحديثة في إطار المعالجة الآلية للبيانات. ففعل الاعتراض غير القانوني يشمل التصنت ، ونقل وتسجيل المحادثات الهاتفية بين الأشخاص ، ويمتد ليشمل علاوة على ذلك كلّ أشكال النقل التي تتمّ من خلال التعامل مع الأجهزة الآلية المعالجة للبيانات مثل نقل البيانات ،والملفات التي تكون موجودة بداخل الحاسب الإلكتروني، أو عن طريق نقل البيانات التي تتمّ عبر الاتصالات، والمراسلات الإلكترونية (البريد الإلكتروني) من خلال شبكة المعلومات، أو التي تكون عبر الاتصالات اللاسلكية المتطورة التي نعرفها في العصر الحاضر كالفاكس، أو عن طريق قيام الجاني في هذه الجريمة باستعمال أجهزة معدة لاستقبال الانبعاثات الكهرومغناطيسية التي تنبعث من أجهزة الحاسب الآلي، ثم فك رموزها وشفرتها لتحويلها إلى البيانات التي يرغب في نقلها أو تسجيلها، أو التصنت عليها لتحقيق غايته الإجرامية(23).

2) يشترط أن يكون فعل الاعتراض باستخدام وسائل فنية غير علنية: يتطلب لقيام الركن المادي لجريمة الاعتراض أن يكون فعل الاعتراض باستخدام وسائل فنية معينة، وغير علنية معدة للتصنت أو نقل البيانات وتسجيلها، أو التحكم والحصول على المحتويات بصورة مباشرة عن طريق الولوج إلى نُظم المعالجة الآلية للبيانات واستخدامها، أو بشكل غير مباشر عن طريق استخدام أجهزة التصنت أو بتسجيل البيانات على أي من الأشرطة أو الدعامات المغناطيسية المعدة للتسجيل، أو الأوراق، أو البطاقات المثقبة(24).

كما يمكن أن يمتد نطاق هذه الوسائل إلى الأجهزة الفنية المتصلة بخطوط النقل، أو الاتصال مثل أجهزة تجميع وتسجيل الاتصالات اللاسلكية، ويمتدّ إطارها ؛ ليشمل الكيانات المنطقية كالبرامج المعلوماتية، وكذلك كلمات المرور والكودات السرية أو الشفرات، ووسائل الاعتراض غير القانوني للنظم والبيانات المعلوماتية وهي وسائل توصف بأنها غير علنية، وهذه الصفة تلحق الوسيلة نفسها من أجهزة، ومعدات، وأدوات معدة للتسجيل، أو النقل، أو التصنت، أو للالتقاط البيانات، وليس للبيانات المرسلة في حدّ ذاتها والتي قد تكون متاحة للغير وعامة لكلّ الناس(25).

فأطراف المحادثة الهاتفية أو المراسلة قد يرغبون في الاتصال بصورة سرية إما لاعتبارات شخصية، أم سياسية، أم تجارية عبر الشبكات المعلوماتية الداخلية، أم الدولية –الإنترنت–، ولكن وبالرغم من ذلك فإن مصطلح غير العلنية لا يستبعد الاتصالات في حدّ ذاتها التي تكون متاحة لأي من الأشخاص الذين يرغبون في استعمال هذه الشبكات لهذه الغاية.

ومما تجدر الإشارة إليه أن الاتصال بنقل البيانات قد يكون في حدود ذات الحاسوب كالذي يكون في حالة الدورة المعلوماتية بين وحدات الحاسب المختلفة من وحدة المعالجة المركزية ووحدة الإدخال والإخراج، وأيضًا يمكن أن يتمّ الاتصال عبر جهازين أو أكثر من الحاسبات الآلية المتصلة ببعض عن طريق نظام معلوماتي واحد داخل المنشأة، أو المؤسسة كالاتصالات التي تتمّ بين العاملين والمستخدمين(26).

كما يمكن أن يكون الاتصال عبّر الشبكات المحلية التي ترتبط بنشاط واحد كالشبكة المصرفية، أو الشبكات العسكرية، أو الاقتصادية داخل حدود الدولة الواحدة، هذا ويمكن أن يحدث الاتصال أيضاً من خلال الشبكات الدولية والتي تتعلق بكافة الأنشطة والمجالات المختلفة، والتي تُغطي معظم أرجاء الكرة الأرضية.

ونظراً للثورة المعلوماتية الجامحة وما يلازمها من ثورة تكنولوجية في جميع الاتجاهات العلمية ،وما قد أدى إليه من ارتباط واضح بينها وبين التقدم في وسائل الاتصالات السلكية واللاسلكية، فإن عبارة النظام المعلوماتي الذي يقوم عليه بُنيان الحاسبات الآلية يمكن أن يمتدّ مفهومه ؛ ليشمل الاتصالات اللاسلكية استناداً إلى أن معظم الاتصالات التي تتمّ حاليًا من خلال الأنظمة المعلوماتية تكون عبر الشبكات والأجهزة التي تعتمد على أجهزة الاتصالات اللاسلكية في إتمام وإجراء هذه الاتصالات، وبالتالي فإن من شأن اعتراضها ونقل أو تسجيل بياناتها أو التصنت عليها أن يقع تحت طائلة المادة الثالثة المشار إليها(27).

3) يجب أن يكون الاعتراض بدون حقّ: يشترط في فعل الاعتراض المكون لجريمة الاعتراض غير القانوني أن يكون بدون وجه حقّ، أما إذا كان المتهم بالقيام بفعل التصنت على المحادثات الشخصية للأطراف المعنية، أو بنقل وتسجيل البيانات المعلوماتية قد أوجد من الأسانيد والأدلّة على أن قيامه بذلك قد تمّ بناءً على ما له من حقّ استمده من أطراف المكالمة، أو الحديث الشخصي أو البثّ حيث سبق وأن صرحا له بذلك، أو أنه قد تصرف بناءً على أمر قد صدر له منهما، أو من السلطة المعنية بمراقبة الاتصالات، أو بناءً على تصريح من الأطراف المعنية باختبار أجهزة الاتصالات والحاسبات الشخصية

والنظم المعلوماتية الخاصّة بالمنشأة، أو بالشركة أو الإدارة، والتي عن طريقها قد تمكن من الاستماع إلى الأحاديث والمكالمات الشخصية أو الاطلاع على البيانات ونقلها وتسجيلها لأغراض تتعلق بتجربة واختبار الأجهزة والمعدات لوضع أفضل السبل الأمنية ؛ لحماية هذه البيانات والمعلومات من الانتهاكات التي يمكن أن تتعرض إليها بدون أنظمة أمان، أو أنه قد قام بالمراقبة بناءً على تصريح من السلطات المختصَّة لاعتبارات تتعلق بالأمن القومي للبلاد التي ينتمي إليها، أو لأغراض مخابراتية للبحث والتنقيب عن الأفعال الإجرامية، وأعمال الجاسوسية، أو مكافحة الإرهاب بتعقب مراسلاته واتصالاته عبر الشبكات المختلفة والمستترة في الغالب تحت أقنعة مزيفة تبث عبر المقالات والمنشورات، والمراسلات، والمجلات التي لا تحمل في مضمونها سوى الدفع بالمستمع إليها أو قارئها إلى هوة الفكر الأعمى، والمتعصب نحو مبادئ مجهولة الهوية لا أساس لها من الشرع، أو قواعد المنطق والعدالة(28). ففي كلّ هذه الحالات وما يماثلها فإن هذا الشخص يكون قد لجأ إلى ارتكاب الفعل بحقّ وبناءً على سند من الاتفاق، أو القانون، وبالتالي فإن فعله لا يُعدّ جريمة اعتراض غير القانوني، والمنصوص عليها في المادة الثالثة المشار إليها.

– الركن المعنوي لجريمة الاعتراض:

جريمة الاعتراض غير القانوني للمحادثات الشخصية، ولنقل البيانات المعلوماتية من الجرائم العمدية التي يتطلب فيها القصد الجنائي بشقيه العلم والإرادة. فلابد أن يعلم الجاني أنه يقوم بالتصنت على المكالمات والأحاديث الشخصية وتسجيل، ونقل البيانات المعلوماتية بغير رضا من أطراف الاتصال، أو سند من القانون، أما إذا لم يتوافر لديه هذا العلم كما لو اعتقد على خلاف الحقيقة بأن الأطراف قد صرحا له بذلك، أو أن من سلطته مراقبة هذه الاتصالات على نحو فيه خطأ في تفسير حدود سلطاته واختصاصه، أو أنه قد دخل إلى نطاق الاتصال على سبيل المصادفة، وتوقف نشاطه عند هذا الحدّ دون أن يتعداه، فإنه في هذه الحالات يكون عنصر العلم قد انتفى لديه، وبالتالي لا قيام للركن المعنوي(29).

كذلك لا بد أن تتجه إرادة الجاني إلى إتيان السلوك المادي الذي يشكل جريمة الاعتراض، وهو التصنت، أو النقل، أو التسجيل للبيانات والمحادثات فإذا ما أكره على ذلك من قبل آخرين لما لديه من خبرة، ومهارة في استخدام أجهزة التصنت أو التسجيل، أو لديه من التقنية في استخدام الحاسبات الآلية، ومهارة اختراق الشبكات المعلوماتية وأجهزة الاتصالات اللاسلكية، أو كان دخوله غير إرادي عن طريق المصادفة المحضة، أو تحت تأثير أي من وسائل الدفع والإكراه المعنوي والمادي الأخرى نحو الجريمة فإنه لا قيام للقصد الجنائي، وبالتالي لا جريمة.

ثانيا: جريمة الدخول في نظام المعالجة الآلية للبيانات:

نَصَّت المادة الثانية من اتفاقية بودابست على هذه الجريمة، وأشارت بدورها إلى أنه "يجب على كلّ طرف أن يتبنى الإجراءات التشريعية أو أي إجراءات يرى أنها ضرورية من أجل اعتبارها جريمة جنائية، وفقاً لقانونها الداخلي للولوج العمدي لكلّ جزء من جهاز الحاسب الآلي بدون حقّ، كما يمكن لها أن تشترط أن ترتكب الجريمة من خلال انتهاك إجراءات الأمن بنية الحصول على بيانات الحاسب أو أي نية إجرامية أخري، أو ترتكب الجريمة في الحاسب الذي يكون متصلا عن بعد بحاسب أخر"(30).

وبناءً على ذلك عُرّفت جريمة الولوج غير المشروع في أنظمة المعالجة الآلية للبيانات "بأنها الاختراق الذي يحدث للنظام المعلوماتي بأكمله أو لجزء منه أيًا كان سواء كان جزءاً مادياً، أو برامج جزئية، أو مجرد بيانات مختزنة في نظام التنصيب عن طريق التوصل إلى الأرقام، أو الكلمات، أو الشفرات، أو الحروف، أو المعلومات السرية التي تكون بمثابة النظام الأمني لجهاز الحاسب الآلي، أو البرامج والنظم المعلوماتية مع توافر القصد الجنائي لدى مرتكب الفعل، وأياً كان الباعث عليه "(31).

يتبين من خلال ما تقدم أنه يتطلب لقيام هذه الجريمة توافر أركان وشروط، ومن أهمّ أركانها الركن المادي المتمثل في فعلي الولوج داخل النظم المعلوماتية، والركن المعنوي المتمثل في القصد الجنائي. وفيما يلي بيان ذلك:

– علة التجريم والشروط المفترضة لقيام جريمة الدخول غير المشروع :

لقد أشارت المادة الثانية من الاتفاقية – السالف بيانها – لخطورة هذه الجريمة باعتبارها تشكل تهديداً لأمن وسرية وسلامة النظم والبيانات والمعلومات، خاصة وأن هناك حاجة ضرورية لتوفير حماية ملائمة لمصالح المنظمات، وبالأخصّ لرجال الإدارة حتي يكون بمقدورهم أن يُديروا ويستثمروا، ويتحكّموا في أنظمتهم بدون تشويش أوعقبة من أي نوع (32).

وعلى ذلك فإن الولوج بأي شكل من الأشكال في هذه الانظمة قد يترتب عليه الوصول إلى بيانات ومعلومات في غاية السرية والخصوصية، وقد يشكل تهديداً للأمن القومي في بلدان العالم التي تعتمد في كيانها على الحاسبات الآلية بشكل كبير، أو المساس باقتصاديات المؤسسات، والشركات الكبرى (33).

كما أن من شأن الولوج غير المشروع في أنظمة المعالجة الآلية للبيانات عن طريق استخدام الأرقام السرية الخاصّة بالمرور إلى المواقع المعلوماتية التي يتمّ التوصل إليها في أغلب الحالات إما بمحض الصدفة أو بتكرار استخدام رموز وأرقام وشفرات على سبيل التجربة للوصول إلى الموقع المراد، أو باستعمال معلومات عن النظام، أن يؤدي إلى استخدام الشبكات المعلوماتية بشكل غير قانوني. وفي بعض الأحوال يتمّ الاستفادة من بعض المواقع المعلوماتية بصورة مجانية على غير رغبة من الشركة، أو المؤسسة المنتجة للبرامج، أو النظم، أو الناشرة للمعلومات، أو المعروضات، أو السلع والخدمات، وفي كلّ هذه الحالات تتكبد هذه الشركات والمؤسسات مبالغ طائلة نتاج هذا الولوج غير المشروع (**34**).

كما ينسب لهذه الجريمة أيضاً أنها تُعد المدخل الذي من خلاله يتمّ ارتكاب كافة أشكال الإجرام المعلوماتي، وجرائم نظم المعالجة الآلية للبيانات.

الشروط المفترضة في الجريمة:

يلزم لقيام جريمة الولوج والبقاء غير المشروع في أنظمة المعالجة الآلية للبيانات شروط ثلاثة مفترضة قبل الحديث عن أركان هذه الجريمة، وتتمثل هذه الشروط في التالي:

– ضرورة وجود نظام معالجة آلية للبيانات.

– أن يكون هذا النظام مشمولاً بنظام حماية.

– أن يكون الولوج بدون حقّ أو سند من القانون أو بناء على عقد أو اتفاق. وفيما يلي بيان ذلك:–

الشرط الأول: وجود نظام معالجة آلية للبيانات:

للتوصل إلى المقصود بنظام المعالجة الآلية للبيانات نذكر بعض المصطلحات الفنية المستخدمة في مجال المعلوماتية فهناك مصطلح المعالجة الميكانيكية Mechanical treatment وتتمّ هذه المعالجة للبيانات عن طريق بعض الأجهزة الأقل تطوراً من الناحية الفنية والتقنية، والتي سبقت ظهور الحاسب الآلي أساس الثورة المعلوماتية الحالية مثل الآلة الكاتبة والتي كانت تستخدم في الكتابة إلى وقت قريب، وأجهزة المحاسبة اليدوية التي كانت تستخدم في المحلات التجارية والتي تعمل بصورة يدوية.

وهناك مصطلح المعالجة الآلية للبيانات Automatic data processing وهو ما يقوم به الحاسب الآلي من معالجة البيانات وحفظها وتخزينها وإخراجها عن طريق مجموعة من الوحدات، والأجهزة التي تعمل بصورة مجتمعة لهذه الغاية. ويوجد مصطلح المعالجة المختلطة Combined treatment وهذه المعالجة تتمّ عن طريق جيل من الآلات الكاتبة المتطورة، والتي تتمتع بميزتي المعالجة الآلية واليدوية في آن واحد، وهي عبارة عن آلات كاتبة لها ذاكرة معلوماتية تستطيع بها الاحتفاظ بالمعلومات التي تمّ كتابتها، وكذلك تعديلها، وإخراجها عند الحاجة.

واستناداً لأرجح الأقوال الفقهية(35) فإن المعالجة الآلية للبيانات تشمل كلّ من المعالجة الآلية والمعالجة المختلطة، وبالتالي فإن كلمة الآلية Automatic ذاتها تدخل في مصطلح المعلوماتية Information أو المعالجة الآلية للبيانات الذي يتكون من شقين الشق الأول هو كلمة معلومة Information، والشق الثاني هو كلمة آلي أو Automatic.

ومما تقدم نخلص إلى أن نظام المعالجة الآلية للبيانات يتضمن كلا النوعين السابقين من المعالجة الآلية والمختلطة، وبالتالي يمكن القول بأن كلمة الآلية تجعلنا نفكر في النظام المعلوماتي ذاته بوصفه نظاماً حركياً يتحرك بديناميكية محددة، أما كلمة المعلوماتية فتبّين لنا نِتاج عمل هذا النظام المتمثل في الوثائق المعلوماتية بأنواعها المختلفة، ولهذا فلا غنى لأحدهما عن الآخر، وكلاهما يكمل الآخر.

الشرط الثاني: وجود نظام أمان لحماية البيانات:

إن اشتراط وجود نظام أمان لحماية محتويات الحاسب من الولوج إليها، والبقاء فيها بغير سند قانوني ليس محل اتفاق بين الفقهاء، حيث اختلفت الآراء بين موسع للحماية لتشمل كلّ الأنظمة، وبين من يحصرها في تلك المحمية فقط بأجهزة أمان، وسنتناول فيما يلي حجج كلا الفريقين:

– الاتجاه المقيد للحماية الجنائية:

يرى أصحاب هذا الاتجاه ضرورة قصر الحماية الجنائية على تلك الأنظمة التي تتمتع بالحماية الفنية فحسب، ويستندون في تبرير رأيهم هذا إلى عدة حجج أهمها مايلي:

1) إن المنطق السليم والعدالة يقتضيان قصر الحماية الجنائية على الأنظمة المحمية بأنظمة أمان فحسب، ذلك لأن القانون الجنائي لا يساعد إلا الأشخاص المجتهدين، ومن غير المعقول حماية معلومات مهمة تركها المسؤولون عنها دون أي إجراءات تكفل لها الحماية، ولا ينبغي حماية حقّ لم يتحوط له صاحبه، وهذا يجعل الأشخاص لا يلجأون إلى القانون الجنائي إلا عندما تعجز تلك التدابير الوقائية عن حماية أنظمتهم. وقد قاس أصحاب هذا الرأى جريمة الدخول غير المصرح به على جريمة انتهاك حرمة المسكن، حيث أن هذه الأخيرة لا تقوم بمجرد دخول المسكن بغير رضا صاحبه، وإنما يجب لقيامها أن يصحب ذلك الدخول استعمال وسائل تدلّ على عدم رضا صاحب المسكن، كالتهديد، أو الاحتيال(36).

2) إن أنظمة الحاسبات تتميز بالانفتاح على الخارج عبر شبكات المعلومات، وهذه المعلومات قد تكون من الأهمية بحيث يصبح من الواجب حمايتها، وإلا أصبح الدخول إليها سهلاً، فهذه الأنظمة لها القابلية للتعرض لهجمات، ولهذا وجبت حمايتها(37).

3) إن النظام الأمني للنظم المعلوماتية يشكل أهمية كبرى بالنسبة إلى شركات التأمين والتي تضع حداً أدنى من الحماية التي لايمكن النزول عنها من قبل مستخدمي النظام المعلوماتي، حيث يؤدي التقصير في ذلك إلى تحمل شركات التأمين خسائر فادحة، وتعويضات جمَّة نتيجة المطالبات القضائية التي تتعلق بتعويض الخسائر الناشئة عن الاعتداء على الأنظمة المعلوماتية، وبالتالي كان من الأولى أن يعطي القانون الجنائي حماية أكثر وجوداً من تلك التي توليها شركات التأمين للأنظمة المعلوماتية، ولا يتسنى ذلك إلا باشتراط أن تكون هذه النظم مشمولة بالحماية من قبل أصحابها ضدّ التسلل إليها أو الولوج إلى محتوياتها أو ارتكاب أي من الأفعال الإجرامية المعلوماتية الأخرى، ولهذا كان على القانون الجنائي أن يُلزم مُستخدمي أو مالكي النظم المعلوماتية بوضع أي من وسائل الحماية لأنظمة المعالجة الآلية للبيانات الخاصّة بهم، والتي تتناسب مع قدر وأهمية ما تحتويه من معلومات وأسرار(38).

4) إن إقامة الدليل على قيام الركن المادي للجريمة والتحقق من توافر القصد الجنائي لدى فاعلها يتطلب وجود أنظمة الأمان، فالولوج إلى أنظمة الأمان يُسهل عملية الكشف عن الجريمة لأنه يترك في العادة أثراً يدلّ عليه، كما أن هذا الولوج يساعد على التحقق من وجود القصد الجنائي لدى الفاعل، وعليه فإن التفسير السليم لنصّ تجريم الولوج غير المصرح به يقتضي قصره على اختراق الأنظمة المحمية دون سواها(39).

– الاتجاه الموسع للحماية الجنائية:

رغم قوة حجج المنادين بتضييق الحماية الجنائية وحصرها في الأنظمة المحمية فقط، فإن هناك اتجاهاً آخر يرى بأن أنظمة الحاسبات الآلية، وما تحويه من معطيات لابد أن تحظى بالحماية بغض النظر عن احتوائها على أنظمة أمان أو عدم احتوائها. ولهم في ذلك حجج، وفيما يلي بيان ذلك:

1) إن تمتع المال المسروق بحماية صاحبه، أو عدم تمتعه لايؤثر في قيام جريمة السرقة كما لا يؤثر فيها مقدار الصعوبة التي واجهها الجاني في ارتكابه لجريمته(40).

2) إن اشتراط وجود أجهزة أمان من شأنه أن يضّيق كثيراً من مجال تطبيق النصّ القانوني.

3) هذا الشرط يتجاهل الحالات التي يتمّ فيها الدخول إلى النظام نتيجة خطأ قام به المبرمجون أو المسؤولون عن أمن النظام(41).

4) إن نظام الحماية لا يكون له دور إلا في إثبات القصد الجنائي لدى مرتكب الولوج في النظام المعلوماتي، والذي يمكن إثباته بأي من طرق الإثبات الأخرى التي يقتنع بها القاضي الجنائي.

5) كما أن الأخذ بفكرة نظام الأمان يضعنا أمام مشكلة تحديد متى يصلح نظام ما لأن يكون نظام أمان ؟ وما هو الحّد الأدنى من الأمان ؟ أي كيف نحدد نوع الأمان وكمه ؟(42). ولكن إذا نظرنا للواقع نلاحظ أن غالبية أنظمة المعالجة الآلية للبيانات تتمتع بنظام حماية فنية، بالإضافة إلى أن وجود مثل تلك الحماية يساعد – كما سبق القول – على إثبات أركان الجريمة، وبصفة خاصة الركن المعنوي.

الشرط الثالث: أن يكون الدخول في نظام المعالجة الآلية للبيانات بدون حقّ:

يلزم لقيام جريمة الولوج داخل النظم المعلوماتية أن يكون الولوج بدون حقّ أي ألا يكون مشروعًا، أو حقًا للشخص مرتكب فعل الولوج، وبالتالي فإنه بمفهوم المخالفة لا جريمة ولا عقاب إذا كان هذا الولوج مصرحًا به، ولكن من هو المسؤول عن إعطاء هذا التصريح ؟ إن تحديد الشخص أو الهيئة التي تصرح بالدخول أمر بالغ الأهمية، إذ تتوقف الجريمة على إرادة ذلك الشخص أو الهيئة، لأنهما يملكان السيطرة على النظام، ويملكان التصرف في تنظيمه والتصريح بالدخول إليه، أو عدم التصريح بذلك.

وإذا كان الأصل أنه لا يكون للنظام أكثر من مسؤول واحد له سلطة التصرف فيه، فقد ثار التساؤل حول إمكانية أن يكون للنظام الواحد أكثر من مسؤول، بحيث يقرر أحدهم مضمون النظام ويشرف الثاني على تنظيمه. نظرياً على الأقل، ويمكن أن يحصل ذلك فيكون للجميع سلطة التصريح بدخول هذا النظام، لكن عملياً تكون سلطة تقرير مضمون النظام وسلطة تنظيمه متداخلتين ويصعب الفصل بينهما بحيث يكون لكلّ منهما مسؤول خاصّ به(43).

ولكن حالة التعدد هذه قد تثور فعلاً في الأنظمة المشتركة، أو الأنظمة الناتجة عن أكثر من نظام " subsystems " – النظم الفرعية –، ويثور في إطار ذلك مشكلة تحديد المسؤول عن هذه الأنظمة، وهل جميع مسؤولي الأنظمة الأصلية مسؤولون عن هذا النظام المشترك ؟

في الواقع إن هذه الحالة تتطلب تحديد المسؤول عن النظام المشترك – وهو ما يجري العمل به عادة – وإذا لم يحدد هذا المسؤول فإن الجميع سيكونون مسؤولين عن هذا النظام إضافة إلى مسؤولية كلّ واحد عن نظامه.

ويترتب على هذا أن التصريح بالدخول الذي يصدر من أحد هؤلاء يلزم الباقين ويُعتبر كأنه صادر منهم جميعاً(44).

– حالات عدم التصريح:

يتحقق الولوج غير المصرح به إلى أنظمة المعالجة الآلية للبيانات بأحد أمرين: أولهما ألا يكون هناك تصريح بالدخول بتاتًا لدى من يقوم بالولوج، وثانيهما أن يوجد تصريح بالولوج، ولكن المصرح له يقوم بتجاوز الحدود التي رُسمت له في هذا التصريح، وسنتعرض فيما يلي لكلتا الحالتين:

أ) حالة عدم وجود تصريح مطلقاً:

وهي الحالة التي لا يكون فيها للشخص الذي يدخل النظام أي علاقة بهذا الأخير، وذلك لأنه من غير العاملين لدى الجهة التي يتبعها النظام، أو رغم كونه من العاملين فلا علاقة له بالنظام، ولا تخوله وظيفته الاتصال به، وفي كلتا الحالتين لا يحوز هذا الشخص ترخيصًا بالدخول للنظام، سواءً كان هذا الترخيص بالدخول يتوقف على سداد مبلغ معين، أو يتوقف على العضوية في جهة معينة أو على غير ذلك من الشروط، أو كان الولوج إلى النظام ممنوعًا على الإطلاق.

وهناك من يرى أن جريمة الولوج غير المصرح به لا تقوم في حالة الولوج إلى نظام معين دون دفع ثمن الاشتراك، ويبرر ذلك بأن الحكمة من تجريم الفعل هو حماية المعلومة من الوصول إليها من قبل أشخاص ليس لهم الحقّ في الاطلاع عليها، أي حماية خصوصية المعلومة في مواجهة هؤلاء، ويرى أن ذلك لا يتحقق في حالة الولوج مع سداد قيمة الاشتراك لأن هذا الشرط إنما هو شرط تنظيمي للولوج إلى نظام الحاسب الآلي الذي يُعَدُّ في هذه الحالة مصرحًا بالولوج إليه من قبل أي شخص يُسدد قيمة الاشتراك المطلوبة مقابل هذا الولوج، والمعلومات التي يحتويها هذا النظام لا تتمتع بالسرية في مواجهة بعضهم، وهو ما يشكل المصلحة التي تحميها جريمة الولوج غير المصرح به(45).

ومن وجهة نظر الباحثة أن هذا الرأي لم يحالفه الصواب ؛ لأنه يُضيّق من مجال تطبيق النصّ، خاصّة وأن هذا الأخير جاء عاماً، ومطلقًا لكلّ حالات الولوج إلى أنظمة الحاسب الآلي، وهو ما يتحقق في حالة الولوج بدون دفع قيمة الاشتراك. وأما حجة انعدام سرية المعطيات في مواجهة بعضهم، فليس هناك معطيات تتمتع بالسرية في مواجهة الجميع، إذ لابد لطائفة من الأشخاص أن تطلع على المعطيات عند استفاء شروط معينة، سواء كانت هذه الشروط تتعلق بصفة وظيفية معينة كالانتماء لجهة معينة، أو كانت متعلقة بدفع قيمة معينة. وذلك أن مصلحة صاحب النظام أن تبقى المعطيات سرية في مواجهة من لم يدفع قيمة الاشتراك، فمصلحة سرية المعطيات قائمة على الأقل في مواجهة هؤلاء.

ب) حالات تجاوز حُدود التصريح:

لا تُثير حالة عدم التصريح إشكالاً بقدر ما تثيره حالة وجود هذا التصريح، ففي هذه الأخيرة يكون مصرحاً بالولوج لنظام الحاسب الآلي في حدود معينة، لكن الفاعل يقوم بتجاوز هذه

الحدود، والفاعل في أغلب الأحوال يكون من العاملين لدى الجهة التي تمّ الولوج إلى نظامها الآلي، ويقوم بتجاوز السلطة المخولة له بالدخول إلى هذا النظام في غير الحالات المرخص له فيها بذلك. ويصعب في كثير من الحالات تحديد ما إذا كان العامل قد تجاوز اختصاصه بالفعل، وما إذا كان قد تجاوزه بعمد أو بغير عمد، لهذا يكون من الواجب تحديد اختصاصات كلّ عامل بدقّة، والمجالات التي يمكن لكلّ واحد الدخول فيها(46).

وعلى هذا الأساس نجد أن بعض القوانين تنصّ صراحة على وجوب أن تكون هناك تعليمات واضحة داخل المؤسسات تحدد من له الحقّ من العمال في الولوج إلى النظام ومن ليس له الحقّ في ذلك. وإذا كان تجاوز التصريح يتعلق بنطاق هذا الأخير والمجالات التي يحددها، فإن هناك من يرى أن التجاوز يتعلق أيضاً بالغرض الذي منح الترخيص من أجله(47).

1–ب– تجاوز المجال الذي حدده التصريح:

في هذه الحالة يملك الشخص الذي يدخل النظام تصريحاً بالدخول إليه، لكن هذا التصريح غير عام، أي أنه غير شامل لكلّ النظام، وإنما هو قاصر على بعض المناطق فيه دون مناطق أخرى، بحيث يكون الدخول إلى المناطق المصرح بها مشروعاً، ويكون غير مشروع في تلك المناطق غير المصرح بها.

ويتمّ هذا النوع من الدخول عموماً من طرف العاملين في المؤسسات الضخمة، لأن هؤلاء هم الذين يملكون في العادة تصريحاً بالدخول، ولكنه تصريح جزئي يشمل مناطق محددة من النظام بحسب الوظيفة التي يؤديها كلّ عامل. لهذا نجد بعض التشريعات تجعل من توافر صفة العامل فيمن يقوم بالدخول غير المصرح به ظرفاً مشدداً(48)، لأن هذا العامل إنما خان بدخوله الأمانة والثقة التي وضعها فيه ربّ العمل، واستغلّ سهولة اتصاله بالنظام ؛ ليتسلل إلى أجزاء منه لا يجوز له الدخول إليها. وتثير هذه المسألة إشكالاً فيما يخص الأنظمة المشتركة التي سبق الحديث عنها، والتي تتكون إثر ارتباط أكثر من نظام، فهل يُعتبر العاملون في الأنظمة الأصلية عاملين أيضاً في النظام المشترك ؟

والإجابة عن هذا التساؤل تكون بالإيجاب إذا كانت ثمة علاقة بين العامل والنظام المشترك، أي أنه يملك تصريحاً بالدخول إلى هذا النظام أو إلى جزء منه ؛ لأن الظرف المشدد – في القوانين التي تأخذ به – لا ينطبق على كلّ العاملين في المؤسسة الضحية، وإنما ينطبق على أولئك الذين يصرح لهم بالدخول إلى النظام، وكذلك العمال الذين لهم علاقة بالنظام، بحيث يمكنهم الدخول إليه بحكم عملهم وعلاقتهم هذه، ولا ينطبق هذا الظرف المشدد على العمال الذين لا تربطهم بالنظام أي علاقة عمل، لأن هؤلاء في حكم من هم خارج المؤسسة التي تحوي النظام، ولأن الحكمة من التشديد هنا هي كون العامل قد خان الثقة الموضوعة فيه، وكذلك سهولة هذا الدخول بالنسبة إليه(49)، وهو ما يتحقق بخصوص من لا تربطه بالنظام أي علاقة تصرح له بالدخول أو تسهل له ذلك.

وجدير بالذكر أن تجاوز التصريح الذي نقصده هنا هو التجاوز في المكان لا في الزمان أي تجاوز الفاعل للمناطق و المجال المكاني المصرح به إلى غيره من المجالات غير المرخص له بدخولها، أما تجاوز الزمان أو وقت المصرح به فهو إنما يدخل في حالة البقاء غير المصرح به. ويثير تجاوز التصريح في الدخول إلى أنظمة الحاسبات مشكلات عملية عديدة، خاصة المتعلقة بمسالة إثبات القصد الجنائي لدى الفاعل الذي يتمتع بتصريح محدود، لأن هناك حالات يتمّ فيها الدخول عن طريق الخطأ أو الصدفة، وخاصّة إذا لم تحدد صلاحيات كلّ عامل بدقّة، كما أن أنظمة الحاسبات تمتاز بأن مناطقها مفتوحة بعضها على بعض، وتمتاز بتشعب نوافذها، لهذا يجب التأكد من توافر القصد الجنائي لدى الفاعل في تجاوز التصريح الممنوح له.

وإذا كان تجاوز التصريح يقع كثيراً من العاملين في المؤسسات الضحية، فإنه قد يقع من غير العاملين أيضاً. لكن الذي يحكم على الفاعل هنا بأنه قد تجاوز التصريح هو ما يمكن أن نسميه العرف المعلوماتي، ذلك أن هناك معايير اجتماعية تسود مجتمع استخدام الحاسوب، وهذه المعايير تقضي بأن مصممي برامج الحاسوب يقومون بتصميمها لتأدية عدة مهام، وأن مزودي خدمات الشبكة يسمحون بوجود هذه البرامج فيُجيزون للمستخدمين القيام بهذه المهام، إذ إن مزودي الخدمة يصرحون ضمناً للمستخدمين بذلك، لكنهم لا يصرحون في المقابل بنشر الضعف في البرامج التي تسمح لهم بإنجاز وظائف غير مقصودة، فاستغلال مستخدم البرامج لنقاط الضعف فيها قد يؤدي على توظيفها بشكل غير مشروع للدخول إلى الحاسوب(50).

2–ب– تجاوز الغرض الذي منح من أجله الترخيص:

هل يُعد من قبيل تجاوز التصريح إذا ما كان الدخول قد استُخدم لغرض آخر غير الغرض الذي مُنح من أجله التصريح ؟

اختلفت مواقف القضاء المقارن في هذا الشأن، حيث يرى القضاء الأمريكي أن السلوك يُعَدُّ جريمة لأن الحقّ في هذا الدخول يجب أن يكون مقيداً بالغرض الذي أُعطي من أجله، فإذا تعارض معه أصبح دخولاً غير مشروع(51).

وفي رأي الباحثة أن جريمة الدخول غير المصرح به لا تتحقق بتجاوز الغرض الذي منح من أجله الترخيص أو التصريح، لأن الجريمة تقوم بالدخول أو الولوج وليس ما يحصل بعد هذا الدخول من التزام بحدود التصريح أو تجاوزه، ومن المعروف أن مبادئ التفسير في القانون الجنائي لا تسمح بهذا التوسع أو القياس.

– الركن المادي لجريمة الدخول غير المشروع في نظام المعالجة الآلية للبيانات:

يُعد السلوك الإجرامي من أهمّ عناصر الركن المادي، لأنه يمثل القاسم المشترك بين جميع أنواع الجرائم، سواء التي يكفي لقيامها ارتكاب السلوك الإجرامي فقط أم تلك التي يلزم لقيامها ضرورة تحقق نتيجة إجرامية معينة إلى جانب السلوك الإجرامي، وسواء كانت الجريمة تامة أو ناقصة، أي وقفت عند حدّ الشروع، فلا قيام للركن المادي ولا قيام للجريمة بالتالي إذا تخلف هذا السلوك. إذن القاعدة أنه "لا جريمة بغير سلوك"(52). وعليه لا تقوم جريمة الدخول غير المصرح به إلا بسلوك الولوج.

والسلوك في جريمة الولوج غير المصرح به سلوك إيجابي أو ما يطلق عليه بالفعل وهو الذي يتمثل في فعل الدخول، والسلوك الإيجابي عبارة عن حركات إرادية من شأنها أن تحدث تغييراً في العالم الخارجي، وهذا التغيير يكون ملموساً في العالم المعلوماتي بالنسبة لجريمة الدخول.

وفيما يلي بيان صور السلوك الإجرامي لجريمة الولوج غير المصرح به في نظام المعالجة الآلية للبيانات:

1) فعل الدخول:

لقد نصّت المادة الثانية من اتفاقية بودابست إلى فعل الدخول(53) والذي يمكن تعريفه بأنه (الولوج إلى المعلومات والمعطيات المخزنة داخل نظام الحاسب الآلي بدون رضا المسؤول عن هذا النظام)(54).

أو أنه وفقاً لوجهة نظر الباحثة "هو إساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مرخص له باستخدامه والدخول إليه، للوصول إلى المعلومات والمعطيات المخزنة بداخله، للاطلاع عليها أو لمجرد التسلية، أو لإشباع الشعور بالنجاح في اختراق الحاسب الآلي".

ويتحقق الدخول غير المصرح به متى كان مخالفًا لإرادة صاحب النظام أو من له حقّ السيطرة عليه، سواء كانت الأنظمة التي تمّ الدخول إليها متعلقة بأسرار الدولة أو دفاعها، أو تتضمن معطيات شخصية تتعلق بحرمة الحياة الخاصّة، أو غير ذلك من المعطيات التي لا يجوز الاطلاع عليها(55).

ولا يشترط توافر صفة معينة فيمن يقوم بعملية الدخول هذه، فجريمة الدخول غير المصرح به وجرائم المعطيات عموماً يقوم بها كلّ الأشخاص رجالاً ونساءً، محترفين وغير محترفين، عمالاً في المؤسسات المجني عليه أو غير عمال فيها، سواء كانوا يستطيعون الاستفادة من الأنظمة أو لا يستطيعون، إذ يكفي فقط ألا يكونوا من أولئك الذين لهم حقّ الدخول إلى هذه الأنظمة(56).

ولا يشترط أن يتمّ الدخول كذلك بطريقة معينة، فالدخول يتحقق بكلّ وسيلة تصلح لذلك، سواء كانت عن طريق كلمة سرّ، أو شفرة، أو برنامج، أو عن طريق شبكات الاتصال الهاتفية، أو عن طريق الشبكات المحلية أو العالمية. أي أن جريمة الولوج جريمة غير محددة الوسيلة أو جريمة ذات قالب حر.

والمعنى اللُّغَوي لكلمة الدخول هى النفاد والاختراق إلى مكان مادي، كالدخول مثلاً إلى قاعة المحاضرات، وهذا المعنى لا يمكن تطبيقه بشأن الدخول إلى أنظمة المعالجة الآلية للبيانات، لأنه لا يمكن الدخول إلى هذه الأنظمة بالطريقة ذاتها التي يدخل بها إلى مكان ما في العالم المادي، لأن الدخول إلى تلك الأنظمة هو ظاهرة غير مادية، وهو يشبه إلى حدّ كبير الدخول في القدرة على التفكير لدى شخص ما. فالدخول إذن له طبيعة معنوية وليست مادية، هذه الطبيعة تشبه الدخول في ذاكرة الإنسان أو في قدرته على التفكير، ووفقاً لهذا التصور المعنوي لفكرة الدخول فإنه يتحقق بأي صورة من صور التعدي المباشر أو غير المباشر(57).

غير أن الدخول يكون بصورة غير مباشرة أكثر من أن تكون مباشرة، لأنه ليس دخولاً إلى مكان ما في العالم المادي إنما هو دخول في القدرة على تحقيق عمليات ذهنية وفكرية، هذا ما يجعله غير مباشر. وذلك أن المقاييس والمعايير التي تحكم العالم المادي لا يمكن تطبيقها على العالم الافتراضي أو المعلوماتي، فما قد يُعَدُّ دخولاً في الأول قد لا يُعَدُّ كذلك في الثاني، فالحاسبات الآلية من وجهة

نظر العالم المادي هو عبارة عن آلات تتولى عملية الاتصال بينها بإرسال واستقبال المعلومات. ولنتخيل مستخدماً يحاول الدخول إلى حاسب محمي بكلمة عبور، فيرسل طلباً إلى هذا الحاسب يسأله؛ ليرسل له الصفحة التي تدعو المستخدم للدخول بوضع الاسم الصحيح وكلمة العبور، ويُذعن الحاسب كما لو كان الأمر يتشابه مع السير إلى باب مغلق(58).

من منظور العالم المادي، فإن الطلب يمكن أن يكون الدخول، فقد أرسل المستخدم أمراً إلى الحاسب وتلقي الإجابة المرغوبة. وكذلك الأمر إذا كان الإرسال بمراسلة إلكترونية ليدخل إلى حاسبات مزود خدمات الإنترنت الذي يتبعه المرسل إليه، فمن وجهة نظر العالم المعلوماتي فإن الإجابة يمكن أن تكون النفي، فالمستخدم الذي يرسل بريداً إلكترونياً إلى مزود خدمات الإنترنت لا يفهم نفسه بأنه دخل إلى مزود خدمات الإنترنت، ومن المنظور المادي يمكن أن تكون الإجابة بالإيجاب، حيث إن المستخدم في الحقيقة قام بإرسال اتصال إلى مزود خدمات الإنترنت الذي تقوم خدماته على الاستقبال، والاستمرار في الإجراء (59). فالدخول إذن له طبيعة معنوية غير مادية، أي أنه يختلف عن مفهوم الدخول كما هو متصور في العالم المادي، والحقيقة أن هذه النظرة هي التي تتفق مع العالم المعلوماتي، ومكوناته غير المادية.

الجمع بين الدخول و البقاء:

لقد ثار تساؤل مهم حول إمكانية أن يشكل سلوك واحد جريمتي الدخول والبقاء في الوقت نفسه، أي إمكانية اجتماع الدخول والبقاء، وبمعنى آخر هل يمكن أن يحصل بقاء بعد دخول غير مصرح به –خاصّة–وأن الدخول والبقاء يجمعهما نصّ واحد ؟

لقد ثار الخلاف حول هذه المسألة: فهناك من يرى إمكانية الجمع بين الدخول والبقاء، وهناك من يرى عكس ذلك، **فأما الرأي الأول** فيرى أن البقاء لا يكون فقط عندما يكون الدخول مشروعاً، ذلك أنه بعد كلّ دخول غير مشروع هناك بقاء غير مشروع، أي هناك دائماً جمع بينهما، إذ أن الدخول جريمة وقتية تعقبها جريمة مستمرة هي البقاء، ويرى أصحاب هذا الرأي أنه ليس من العدالة أن يتساوى من دخل النظام، ثم خرج مع من دخله ثم بقي فيه، أي بين من ارتكب جريمة واحدة ومن ارتكب جريمتين وإن الأخذ بهذا الرأي يشجع على العدول عن جريمة البقاء لمن ارتكب جريمة الدخول(60).

أما الرأي الثاني – والذي تؤيده الباحثة – فيرى أن كلّ جريمة تقع مستقلة عن الجريمة الأخرى، أي أن لكلّ جريمة سلوكها الإجرامي الخاصّ بها دون الأخرى، ويعتمد هذا الرأي على حجتين: الأولى استقاها من المبادئ التي تحكم تفسير القانون، وهي تقضي بأن المشّرع عندما يستخدم كلمتين أو مصطلحين مختلفين فلا بدّ أن يكون لكلّ مصطلح معناه ومدلوله المختلف عن المصطلح الآخر، فمصطلح البقاء لا يحتوي على مصطلح الدخول، والعكس صحيح، ولأن نصّ المادة الثانية لم يتطرق إلا إلى مصطلح واحد، وهو الدخول فلا يجوز مدّ مدلول هذا المصطلح إلى المصطلح الأخر وهو البقاء. أما الحجة الثانية، فسندها المنطق، وهي أن جريمة الدخول ذات طبيعة وقتية وإن كانت ذات آثار مستمرة، فالاستمرار هنا هو من آثار الدخول، وليس هو البقاء(61).

2) طبيعة الجريمة:

الأصل أن يتطلب المشرع لقيام جريمة ما وجود ما يسمى بالنتيجة الإجرامية التي يُرتّبها أو يُحدّثها السلوك الإجرامي، لكن هناك جرائم يكتفي فيها بالسلوك الإجرامي لكي يعاقب عليها، ويسمى النوع الأول جرائم ذات نتيجة بينما يسمَّى النوع الثاني بالجرائم ذات القالب الحر، أو جرائم السلوك المحض، ووجوب تحقق النتيجة الإجرامية هو الذي يفرق بين هذين النوعين من الجرائم، ولهذه النتيجة مدلولان أحدهما مادي والآخر قانوني، فأما المدلول المادي فهو الذي يتحقق بالنظر إلى النتيجة باعتبارها ظاهرة مادية وهي التغيير الذي يحدث في العالم الخارجي كأثر للنشاط الإجرامي، أما المدلول القانوني للنتيجة فهو الاعتداء على الحقّ الذي يحميه القانون والذي يتضمنه النصّ التشريعي، وبهذا تكون النتيجة بمدلولها القانوني عنصرًا في كلّ جريمة، لأن المشرع في كلّ جريمة يجرم الاعتداء على حقّ أو مصلحة يراها جديرة بالحماية، أما النتيجة بمدلولها المادي فلا تظهر في كلّ الجرائم بوضوح، وتبعاً لهذا قسم الفقه الجرائم إلى نوعين: جرائم مادية أو الجرائم ذات النتيجة، وجرائم شكلية أو جرائم السلوك المحض(62)، وجريمة الدخول غير المصرح به تنتمي لكلا النوعين وفيما يلي تفسير ذلك:

2.1) جريمة الدخول غير المشروع من جرائم القالب الحرّ:

من خلال الاطلاع على الفقرة الأولى من المادة الثانية من اتفاقية بودابست نجدها تنصّ على تجريم فعل الدخول غير المصرح به، ولا تتطلب تحقق نتيجة معينة كالوصول إلى المعطيات والبرامج، أو

التلاعب بها، بل تكتفي أن يبدأ الفاعل بتشغيل الحاسب الآلي ومنذُ هذه اللحظة يبدأ هذا الأخير بالعمل، إذ يتمّ إرسال إشارة كهربائية نحو وحدة المعالجة المركزية، وتقوم هي بدورها بإرسال البرامج المسؤولة عن تشغيل ذاكرة القراءة، وتقوم هذه الذاكرة بالبحث عن المعطيات التي تسمح بتشغيل النظام المسؤول عن البحث، ثم تقوم بتسجيلها في ذاكرة القراءة والكتابة التي تقوم بمتابعة المراحل اللاحقة، وحتى هذه اللحظة لا يمكن القول بوجود وصول إلى معلومات محددة، لكن مما لا شك فيه أنه قد تمّ الدخول إلى نظام الحاسب الآلي، وهذا كاف لقيام جريمة الدخول غير المصرح به وفقاً لنصّ المادة الثانية المشار إليها(63).

2.2) جريمة الدخول غير المشروع من جرائم المادية:

أسلفنا أن نصّ المادة الثانية وفي فقرتها الأولى اكتفت لقيام جريمة الدخول غير المصرح به مجرد الدخول، دون أن يتطلب حدوث نتيجة معينة، ولكن السؤال الذي يطرح نفسه ما الوضع إذا نجم عن الدخول نتيجة معينة ؟ هل يترتب على ذلك أثر قانوني ؟

في الواقع لقد تفادت المادة الثانية إمكانية حدوث ذلك، ونصّت في فقرتها الثانية على أنه إذا كان الدخول بقصد الحصول على بيانات الحاسب الآلي، أو بقصد آخر غير أمين يُعد هذا السلوك جريمة، والمقصود من عبارة الحصول على بيانات الحاسب الآلي هو الاطلاع غير المشروع على تلك البيانات وسرقتها، أما ما يتعلق بعبارة "بقصداً آخر غير أمين" قد يدخل في طيات هذه العبارة العديد من المعاني كالحذف، أو تغيير البيانات، أو تخريب النظام، وهذا ما ذهبت إليه العديد من القوانين التي جرمت فعل الدخول غير المصرح به في قوانينها الوضعية(64).

– **الركن المعنوي في جريمة الدخول غير المشروع به لنظام المعالجة الآلية للبيانات:** إن جريمة الدخول هي من الجرائم العمدية التي يتطلب لقيامها القصد الجنائي بعنصريه العلم والإرادة، العلم بمكونات الجريمة والإرادة المتجهة إلى ارتكاب السلوك الإجرامي لهذه الجريمة.

والحقيقة أن المنطق يُحتم أن تكون هذه الجريمة عمدية، لأن عمليات الدخول إلى أنظمة الحاسبات الآلية هي عمليات تتكرر بشكل مذهل في اليوم الواحد، وتقع من عدد هائل من المستخدمين خاصّة مع ارتفاع عدد مرتادي شبكة الإنترنت، وليس من المستبعد في ظلّ كلّ هذه الحركة دخولاً وخروجاً أن تكون هناك عمليات دخول غير مشروعة لكنها غير عمدية، ولو كانت جريمة الدخول غير عمدية لوقع الكثير من مستعملي هذه الشبكة والحاسب الآلي تحت طائلة العقاب، وعلى هذا كان من الضروري أن تكون هذه الجريمة عمدية وذلك من أجل الموازنة بين حماية خصوصية الأنظمة المعلوماتية، وحماية حرية الأفراد في استخدام الإنترنت.

ولكون الجريمة عمدية فلابدّ أن يُلمَّ الجاني بكلّ واقعة يتطلبها القانون لبناء أركان الجريمة، واستكمال عناصرها، فضلاً عن ذلك لابدَّ أن يشمل العلم أيضًا التكيّيف الذي تتصف به بعض هذه الوقائع وتكتسب به أهميتها في نظر القانون، حيث إن عددًا من الوقائع التي تقوم بها الجريمة لا يمثل أهمية في نظر القانون إلا إذا اكتسب وصفًا معينًا فإذ تجرّد من هذا الوصف فقد تجرّد من الأهمية القانونية، ولم يعد صالحاً لتقوم به الجريمة(65).

وعلى هذا يجب أن يشمل علم الجاني كلّ واقعة تدخل في تكوين جريمة الدخول، وأول ما يجب أن ينصرف إليه علمه هو موضوع الحقّ المعتدى عليه، فلابد أن يعلم الجاني أن فعله ينصب على نظام للمعالجة الآلية للبيانات وليس على شيء آخر، فإذا كان الجاني يعتقد بناءً على أسباب معقولة أنه يقوم مثلاً بإجراء بعض العمليات الحسابية عن طريق الحاسب الآلي، ولا يعلم أنه دخل في نظام للمعالجة الآلية للبيانات بما يحويه من بيانات فإن الجريمة لا تقوم لعدم توافر القصد لديه (66).

وكذلك لابدَّ أن يعلم الجاني أنه يقوم بالدخول إلى هذا النظام من غير تصريح أي بصفة غير مشروعة، فإذا كان يعتقد أن له تصريحًا بالدخول، أو أن الموقع مفتوح للجمهور لم يقم القصد الجنائي لديه، وكذلك الأمر إذا كان الدخول عن طريق الصدفة، أو السهو، أو الخطأ، ولكن في المقابل لابدَّ عليه أن يخرج فوراً من النظام عند علمه بأن دخوله غير مصرح به، فإذا لم يفعل ذلك توافر لديه القصد الجنائي منذُ اللحظة التي تحقق فيها العلم وعُد مرتكباً لجريمة الدخول غير المشروع(67).

وفضلاً عن ذلك لابدَّ أن يعلم الجاني بخطورة الفعل الذي يقوم به على المصلحة التي يحميها القانون، كأن يعلم أنه ينتهك سرية هذا النظام وأن فعله قد يؤدي إلى تخريب هذا النظام، أو الإضرار بالبيانات الموجودة فيه. وهناك بعض العناصر لا يتطلب القانون توقعها ؛ لتقوم الجريمة، فالقانون مثلاً لا يحدد في حمايته نظاماً بعينه، فإذا قصد الجاني الدخول إلى نظام معين ثم وجد نفسه داخل نظام آخر فإنَّ الجريمة تتحقق، ولا يُغير هذا من أمر القصد شيئاً. فالجريمة

تتحقق مادام الجاني قد قصد الدخول إلى النظام الأول، وحتى ولو لم يقصد الجاني الدخول إلى نظام معين أو محدد بذاته، كأن يكون باعثه الاستكشاف، وغرضه الدخول إلى أي نظام يمكنه الدخول إليه، فالقصد يتحقق.

كما يتطلب في القصد الجنائي لجريمة الدخول غير المشروع لنظم المعالجة الآلية للبيانات أن تتجه إرادة الجاني إلى فعل الدخول، وإلى النتيجة الإجرامية، وهي الاطلاع أو التجول خلال المواقع والمعلومات والأسرار المعلوماتية بدون حقّ، فإذا لم تتجه إرادة الجاني إلى فعل الدخول، ولكنه وجد نفسه في إطار النظام المعلوماتي بمحض الصدفة، ولم يتعّد سلوكه ذلك أو وقف عند هذا الحد دون أن يتعداه إلى التجول، أو إبداء الرغبة في الاطلاع أو استراق المعلومات أو البيانات أو غير ذلك، أو أُكّره على فعل الدخول بأي من وسائل الإكراه المادي أو المعنوي على هذا الفعل كما لو قامت إحدى عصابات قرصنة المعلومات على إجباره على ذلك نظراً لما لديه من مهارات ودرية بفنون وتقنيات الحاسبات الآلية والنظم المعلوماتية الأمر الذي جعله ينساق وفق إرادتهم، لا إرادته هو فإنه في هذه الحالة لا يتوافر القصد الجنائي لديه، وبالتالي لا قيام للركن المعنوي في جريمة الدخول، ولا عقاب على فعله.

الخـاتمـة:

نخلص مما تقدم إلى ما يلي :

1) إن جرائم التجسس الإلكتروني والمتعلقة بحماية البيانات الشخصية الإلكترونية تُعدّ صنفًا مستحدثاً من الجرائم التي تتحدى القواعد التقليدية للتجّريم والعقاب، والتي تقضي ضرورة تحقيق أركان الجريمة طبقًا لمبدأ المشروعية للجرائم والعقوبات.

2) تشمل الاتفاقية على جوانب تفصيلية لأنواع جرائم التجسّس الإلكتروني بما يكفي أن نستوحي منها الكثير، ونستثمر الجهود المبذولة هناك على أكثر من صعيد.

3) إن نظام المعالجة الآلية للبيانات، والذي شملته الاتفاقية بالحماية هو نظام يتحرك بديناميكة محددةً، وأن المعلومات الإلكترونية ما هي إلا شطر من نظام المعالجة الآلية وكلاهما يُكمّل الآخر.

4) جعلت الاتفاقية التجسّس على البيانات في إطار مفهوم الجرائم التي تستهدف السرّية و السلامة وتوافر المعلومات ، وهذا بدوره أمكنها من إدخال الانماط المختلفة لجرائم البريد الإلكتروني و التراسل الإلكتروني، كما ابتعدت عن الوصف الفرعي أو التفصيلي لانماط السلوك الإجرامي أو الصور التي تتخذها الجريمة الواحدة أو التي تندرج في نطاق الجريمة الواحدة، وهذا مسلك محمود باعتبار أن تُوصّيف السلوك في الغالب يتصل بالوسائل الإلكترونية المتبعة في ارتكاب الجريمة .

5) كما لم تميز الاتفاقية وفي إطار الجرائم التي تستهدف البيانات الشخصية في مراحل الجمع والمعالجة والاستخدام والنقل ، نوعية المعطيات و ما إذا كانت بيانات تتصل بالشخص أم بمصالح اقتصادية أم مالية أم مسائل أمنية أم غير ذلك ، ولعل مرد هذا الاتجاه السعي لتعميم حماية المعطيات بكافة أنواعها .

التوصـيات :

1) تعزيز وتفعيل دور التعاون الدولي من أجل مكافحة التجسّس الإلكتروني، بما فيه تكريس مبدأ الاختصاص الجنائي العالمي ..

2) تطويع قواعد الاتفاقيات الدولية الخاصة بالجرائم الإلكترونية وتفعيلها في كل دولة لخصوصية الجرائم المعلوماتية من حيث صعوبة إثباتها ومتابعة مرتكبيها وسهولة إتلاف أدلتها ولكونها لا تترك آثارًا مادية في مسرح ارتكابها.

3) حماية الحياة الخاصة للأفراد من أعمال التطفل والتجسّس ، وذلك بإضافة مواد قانونية في قانون العقوبات أو بموجب قوانين خاصة.

4) إعداد كوادر متخصصة فنياً تابعة لوزارة الداخلية لمتابعة هذه الجرائم لأنها تتطلب قدراً عالياً من الخبرة في مجال البحث والتحري وإجراءات التحقيق والمتابعة.

5) إنشاء هيئة وطنية تتولى مراقبة المواقع الالكترونية عبر شبكة الإنترنيت لحجب المواقع المشبوهة والتي تهدد أمن واستقرار المجتمع .

الهوامش:

(1) وفي ذلك يقول Kennth Weiss رئيس قسم الحاسبات الآلية لدى شركة أمريكية، أنه " لو أدرك كبار المسؤولين الإداريين حقيقة المسؤولية والمخاطر المحتملة التي تهدد أصول الشركات وسمعتها، لأغلقوا جميع شبكات ومراكز الحاسبات الآلية ". انظر: محمد عبد الله أبو بكر، جرائم الكمبيوتر والإنترنت، الإسكندرية: منشأة المعارف، 2006م، ص 145.

(2) محمد علي العريان، الجرائم المعلوماتية، الإسكندرية: دار الجامعة الجديدة، 2011، ص 39.

(3) أحمد خليفة الملط، جرائم المعلوماتية، الإسكندرية: دار الفكر الجامعي، 2006م، ص 167.

(4) نائلة معوض، جرائم الحاسب الآلي الاقتصادية، لبنان: منشورات الحلبي الحقوقية، 2005م، ص 98 وما بعدها. انظر: عواطف محمد عثمان عبد

الحليم، جرائم المعلوماتية تعريفها صورها جهود مكافحتها دولياً إقليمياً، ووطنياً، مجلة العدل، العدد 24، السنة العاشرة، ص 58.

(5) انون مكافحة الجرائم الإلكترونية، رقم 13 لسنة 2007م، موقع وزارة العدل لجمهورية السودان، لمزيد من التفصيل انظر: الموقع الإلكتروني: http://www.moj.gov.sd/home_ar.htm

(6) حسام الدين كامل الاهواني، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الآلي، مجلة العلوم القانونية والاقتصادية، العدد الأول والثاني، السنة 32، ص 100. انظر: محمد حماد مرهج الهيتي، الحماية الجنائية للبيانات والمعلومات الشخصية المخزنة في الحاسب الآلي، مجلة الشريعة والقانون، العدد السابع والعشرون، ص 403.

(7) ينظر المرجع السابق، ص 101.

(8) ينظر محمد على العريان، مرجع سابق، ص 40.

(9) ينظر محمد حماد مرهج الهيتي، مرجع سابق، ص 404 وما بعدها.

(10) ينظر هشام محمد رستم، الحماية الجنائية لحق الإنسان في صورته، أسيوط: مكتبة الآلات الحديثة، (د.ت)، ص138.

(11) ينظر المرجع السابق.

(12) برنامج حصان طروادة " هو برنامج خادع يخفي وراءه غرضاً غير مشروع، حيث يظهر كبرنامج عادي يؤدي بعض المهام المفيدة والمألوفة لمستخدمه بينما الحقيقة على النقيض من ذلك تماماً. حيث يخفي هذا البرنامج داخله بعض الأوامر والتعليمات التي تؤدي عند تشغيله مهام ضارة غير متوقعة تمثل أغراضه الحقيقية المدمرة، وهكذا فقد =يبدو البرنامج كما لو كان مُعداً لتنظيم البيانات بالملفات أو تكثيفها بينما الهدف الحقيقي من وراء تشغيله قد يكون محو هذه البيانات من ذاكرة الحاسب الآلي أو التهديد بذلك لابتزاز مستخدمه، أو الاستيلاء على المال بتحريف البيانات المدخلة أو المخزنة، وعادة ما توجد برامج أحصنة طروادة في برامج الأعمال (كبرامج معالجة النصوص، و برامج إدارة قواعد البيانات)، وغالباً ما تكون مختفية في منتصف البرنامج في مكان غير مستعمل منه، والبرنامج الذي يتضمنها قد يعمل بطريقة صحيحة لعدة شهور قبل أن تظهر أعراض أو أمر غير متوقعة وغير مشروعة، وقد تظهر هذه الأوامر و تنفذ مباشرة عند تشغيله، وبرامج أحصنة طروادة – وعلى خلاف ما يسمى بفيروسات الحاسب الآلي – لاتنسخ نفسها، واكتشافها بالغ الصعوبة، وكذلك أيضاً محاولة اقتفاء أثر مُعديها، وقد تم نعت تلك البرامج ب(حصان طروادة)، نظراً لخطورتها وآثارها المدمرة وقدرتها على الخداع والمفاجأة والتضليل مثلما فعل حصان طروادة الخشبي الكبير الذي ضم بداخله مجموعة من الجنود حينما أحكم خداع جيش طروادة الذي كان يدافع عن أرضه حيال غزو إسبرطة لتلك المدينة، فعندما رآه أهل المدينة فرحو به وقاموا بإدخاله داخل مدينة طروادة وحينما استقر به الحال قام الغزاة بالخروج منه واستولوا على تلك المدينة، وذلك وفقاً لما جاء بقصص الحرب التي رواها الشاعر الإغريقي القديم هوميروس في ملحمتي الإلياذة والأوديسة. ينظر: في ذلك أحمد حسن خميس، الهاكروز والكراكرز، الإسكندرية: دار البراء، 2003م، ص36.

(13) المرجع السابق، ص 37 وما بعدها.

(14) ويذكر عفيفي كامل عفيفي أن هذه التقنية قد تم استخدامها من قبل أحد المبرمجين حيث قام بإعداد باب خفي في البرنامج الذي تستخدمه إحدى الشركات التي تستخدم حاسب للمشاركة الزمنية ما سمح له بالحصول على برامج وبيانات مستخدمين آخرين للنظام. انظر عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون (دراسة مقارنة)، الإسكندرية: منشأة المعارف، (د.ت)، ص 314. ينظر أيضاً هشام محمد فريد رستم، مرجع سابق، ص 142.

(15) ينظر المرجع السابق، ص 139. ينظر أيضاً محمد عبد الله ابو بكر سلامة، جرائم الكمبيوتر والإنترنت، الإسكندرية: منشأة المعارف، 2006م، ص 147 وما بعدها.

(16) ينظر عفيفي كامل عفيفي، مرجع سابق، ص 314.

(17) ينظر محمد عبد الله أبو بكر سلامة، مرجع سابق، ص 150.

(18) ينظر هشام رستم، مرجع سابق، ص 140 وما بعدها.

(19) اتفاقية بودابست للجريمة الإلكترونية، منشورات مجلس أوروبا، مجموعة المعاهدات الأوربية، رقم 185، 2001م، ص 5.

(20) ينظر: بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات، القاهرة: دار الفكر الجامعي، 2008م، ص 305.

(21) ينظر: المرجع السابق، ص 306.

(22) اتفاقية بودابست للجريمة الإلكترونية، مرجع سابق، ص 5.

(23) ينظر: محمد علي العريان، مرجع سابق، ص 75 وما بعدها. انظر: جمعة سعيد سرور، ملامح الجريمة الإلكترونية العابرة للحدود، مجلة المحامي، العدد 77-78، السنة 20 (2009م)، ص 15 وما بعدها.

(24) ينظر: محمد عبد الله أبو بكر سلامة، مرجع سابق، ص 156.

(25) ينظر: حسن طاهر داود، جرائم نظم المعلومات، الرياض: أكاديمية نايف العربية للعلوم الأمنية، 2002م، ص 205.

(26) ينظر: مجلة عالم الكمبيوتر والإنترنت، العدد 92، يونيو 2007م، ص 98 وما بعدها.

(27) ينظر: بلال أمين زين الدين، مرجع سابق، ص 308 وما بعدها.

(28) المرجع سابق، ص 309.

(29) المرجع السابق، ص 310.

(30) المذكرة التفسيرية لاتفاقية بودابست باللغة العربية المبرمة في 8 نوفمبر 2001م، والخاصة بحماية المعلوماتية ومنع وقمع الإجرام المعلوماتي، ص 4.

(31) ينظر: أيمن عبد الله فكري، جرائم نظم المعلومات (دراسة مقارنة)، الإسكندرية: دار الجامعة الجديدة، 2009م، ص 260.

(32) ينظر: المذكرة التفسيرية لاتفاقية بودابست، مرجع سابق، ص 5.

(33) ينظر: عفيفي كامل عفيفي، مرجع سابق، ص 311. ومن ذلك ما تعرضت له وكالة ناسا الفضائية، ووزارة الدفاع الأمريكيتين من ولوج وتجول غير مشروع بل خطير في أنظمتها المعلوماتية وقد أكدت إحصاءات صادرة من مكتب التحقيقات الفيدرالي الأمريكي FBI بأن 80% من الثغرات الأمنية في

النظم المعلوماتية الأمريكية تحدث عن طريق شبكة الإنترنت. ينظر المرجع السابق، ص 312.

(34) راجع هشام رستم، مرجع سابق، ص 138 ومن الأمثلة التي يمكن ضربها في هذا الصدد عندما تمكن الجاني من دس برنامج يحمل تعليمات خفية من شأنها منع تشغيل بعض برامج الحاسب بعض الوقت حتى يتاح له نسخ البيانات المخزنة بداخله بعد جمعها على قرص ممغنط خاص بالجاني. ينظر المرجع السابق، هامش 3 ص 139 ومابعدها.

(35) ينظر: بلال أمين زين الدين، مرجع سابق، ص 263.

(36) ينظر: نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، دراسة نظرية وتطبيقية، القاهرة: دار النهضة العربية، 2004م، ص 366.

(37) ينظر: المرجع السابق.

(38) ينظر: بلال أمين زين الدين، مرجع سابق، ص 266.

(39) ينظر: نائلة قورة، مرجع سابق، ص 367.

(40) ينظر: المرجع السابق، ص 368.

(41) ينظر: محمد خليفه، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، الإسكندرية: دار الجامعة الجديدة، 2007م، ص 136 وما بعدها.

(42) ينظر: على عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، منشورات كلية الشريعة والقانون، جامعة الإمارات، المجلد الثاني، الطبعة الثانية، 2004م، ص 595.

(43) ينظر: بلال أمين زين الدين، مرجع سابق، ص 269.

(44) ينظر: على عبد القادر القهوجي، مرجع سابق، 560.

(45) ينظر: نائلة قوره، مرجع سابق، ص 346.

(46) ينظر: محمد خليفه، مرجع سابق، ص 149.

(47) ينظر: المرجع السابق.

48 ينظر: محمود أحمد عبابنه، جرائم الحاسوب وأبعادها الدولية، عمان: دار الثقافة للنشر والتوزيع، 2005 م، ص150.

(49) ينظر: بلال أمين زين الدين، مرجع سابق، ص 270.

(50) ينظر: محمود أحمد عبابنه، مرجع سابق، ص 153.

(51) ينظر: على عبد القادر القهوجي، مرجع سابق، ص 587.

(52) ينظر: فتوح عبد الله الشاذلي، علي عبد القادر القهوجي، شرح قانون العقوبات، القسم العام، القاهرة: مطابع السعدني، 2006م، ص 261.

(53) ينظر: المذكرة التفسيرية لاتفاقية بودابست، مرجع سابق، ص 4.

(54) محمد خليفة، مرجع سابق، ص 139.

(55) ينظر: علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، مرجع سابق، ص 592.

(56) ينظر: محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، القاهرة: دار النهظة العربية، 1998م، ص 71.

(57) ينظر: محمد خليفه، مرجع سابق، ص 142 وما بعدها.

(58) ينظر: أورين كير، ترجمة، عمر بن يونس، نطاق الجريمة الافتراضية تفسير الدخول والتصريح به في إطار تشريعات الإساءة إلى الحاسوب، مجلة القانون، جامعة نيويورك، العدد 78 نوفمبير 2003م، ص 67.

(59) ينظر: المرجع السابق، ص 68.

(60) ينظر: محمد خليفة، مرجع سابق، ص 157.

(61) ينظر: المرجع السابق، ص 158.

(62) ينظر: عفيفي كامل عفيفي، مرجع سابق، ص 282.

(63) وفي الولايات المتحدة الأمريكية تعاقب المادة 1030(أ) (3) على الدخول المجرد، لكن ليس لكلّ الحاسبات، بل لتلك التي تعمل داخل الحكومة الفيدرالية أو التي ترتبط بها مصالح هذه الأخيرة، وغير هذه من الحاسبات لا يعاقب على الدخول المجرد إليها، بل يعاقب على الدخول بغية الحصول على معلومات معينة، وذلك وفق ما تنصّ عليه المادة 1030 (أ) (3) والمادة 1030 (أ) (2)، والأمر هذا نفسه نجده في قانون إساءة استخدام الحاسبات الآلية في المملكة المتحدة. ينظر نائلة قورة، مرجع سابق، ص 356.

(64) ينظر الأمانة العامة للحكومة الجزائرية، قانون العقوبات الجزائري، الجزائر: منشورات الأمانة العامة للحكومة 2009م، المادة 394 مكرر، ص 119. قانون العقوبات الفرنسي 1810، الباب الثاني " الجنايات والجنح ضد الافراد، الفصل الأول " الجنايات والجنح ضد الأشخاص، المادة 323. لمزيد من التفصيل انظر الموقع الإلكتروني: www.napoleon-series.org

(65) ينظر محمود نجيب حسني، النظرية العامة للقصد الجنائي " دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية"، القاهرة: دار النهضة العربية، د. ت، ص 51.

(66) ينظر نائلة قوره، مرجع سابق، ص 379.

(67) ينظر منير محمد الجنبيهي، مرجع سابق، ص 52.

قائمة المصادر المراجع:

أولا: الكتب

- الملط، أحمد خليفة، (2006)، جرائم المعلوماتية، الإسكندرية: دار الفكر الجامعي.
- الشاذلي، فتوح عبد الله وعلي عبد القادر القهوجي، (2006)، شرح قانون العقوبات، القسم العام، القاهرة: مطابع السعدني.
- العريان، محمد علي، (2011). الجرائم المعلوماتية، الإسكندرية: دار الجامعة الجديدة.
- الشوا، محمد سامي، (1999). ثورة المعلومات وانعكاساتها على قانون العقوبات، القاهرة: دار النهضة العربية.
- أبو بكر، محمد عبد الله، (2006). جرائم الكمبيوتر والإنترنت، الإسكندرية: منشأة المعارف.

– حسني، محمود نجيب، (د.ت). النظرية العامة للقصد الجنائي " دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية"، القاهرة: دار النهضة العربية.

– خميس، أحمد حسن، (2003)، الهاكروز والكراكرز، الإسكندرية: دار البراء.

– خليفه، محمد (2007م). الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، الاسكندرية: دار الجامعة الجديدة.

– داود، حسن طاهر، (2002م). جرائم نظم المعلومات، الرياض: اكاديمية نايف العربية للعلوم الآمنية.

– رستم، هشام محمد فريد. (د.ت). الحماية الجنائية لحقّ الإنسان في صورته، أسيوط: مكتبة الآلات الحديثة.

– زين الدين، بلال أمين، (2008). جرائم نظم المعالجة الآلية للبيانات، القاهرة: دار الفكر الجامعي.

– سلامة، محمد عبد الله ابو بكر، (2006)، جرائم الكمبيوتر والانترنت، الإسكندرية: منشأة المعارف.

– عفيفي، عفيفي كامل، (د.ت). جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون (دراسة مقارنة)، الإسكندرية: منشأة المعارف.

– عبانية، محمود أحمد، (2005)، جرائم الحاسوب وأبعادها الدولية، عمان: دار الثقافة للنشر والتوزيع.

– فكري، أيمن عبد الله، (2009م). جرائم نظم المعلومات (دراسة مقارنة)، الإسكندرية: دار الجامعة الجديدة.

– قورة، نائلة عادل محمد فريد، (2004). جرائم الحاسب الاقتصادية، دراسة نظرية وتطبيقية، القاهرة: دار النهضة العربية.

– معوض، نائلة، (2005). جرائم الحاسب الآلي الاقتصادية، لبنان: منشورات الحلبي الحقوقية.

ثانيا – الدوريات

– الاهواني، حسام الدين كامل (د.ت). الحماية القانونية للحياة الخاصة في مواجهة الحاسب الآلي، مجلة العلوم القانونية والاقتصادية، العدد الأول والثاني، السنة 32.

– الهيتي، محمد حماد مرهج (د.ت). الحماية الجنائية للبيانات والمعلومات الشخصية المخزنة في الحاسب الآلي، مجلة الشريعة والقانون، العدد السابع والعشرون.

– بن يونس، أورين كير، ترجمة، عمر (2003). نطاق الجريمة الافتراضية تفسير الدخول والتصريح به في إطار تشريعات الإساءة إلى الحاسوب، مجلة القانون، جامعة نيويورك، العدد 78.

– سرور، جمعة سعيد (2009م). ملامح الجريمة الالكترونية العابرة للحدود، مجلة المحامي، العدد 77–78، السنة 20.

– عبد الحليم، عواطف محمد عثمان (د.ت). جرائم المعلوماتية تعريفها صورها جهود مكافحتها دولياً إقليمياً، ووطنياً، مجلة العدل، العدد 24، السنة العاشرة.

ثالثا: الرسائل والبحوث العلمية:

– القهوجي، على عبد القادر (2004). الحماية الجنائية للبيانات المعالجة إلكترونيا، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، منشورات كلية الشريعة والقانون، جامعة الإمارات، المجلد الثاني، الطبعة الثانية.

رابعا – القوانين والاتفاقيات الدولية:

– الأمانة العامة للحكومة الجزائرية، قانون العقوبات الجزائري، الجزائر: منشورات الأمانة العامة للحكومة 2009م،

– مجلس أوروبا، اتفاقية بودابست للجريمة الإلكترونية، منشورات مجلس أوروبا، مجموعة المعاهدات الأوربية، رقم 185، 2001م.