

المنظومة التشريعية الموضوعية لمواجهة الجريمة المعلوماتية الماسة

بسلامة وسرية المعلومات في التشريع الجزائري

The Substantive Legislative Framework for Combating Cybercrime Affecting the Integrity and Confidentiality of Information in Algerian Legislation

فرفورجدة*، جامعة محمد بوضياف - المسيلة -

hadda.guergour@univ-msila.dz

تاريخ إرسال المقال: 2026/04/10 تاريخ قبول المقال: 2026/05/01 تاريخ نشر المقال: 2026/05/31

الملخص:

أدى تنوع مجالات استخدام الحاسب الآلي الى تنوع فرص واحتمالات الاعتداء على برامجه والتعرض لها بالإتلاف والتزوير او استخدامهما بغير حق، مشكلا خطرا يهدد امن المجتمع الذي لزاما عليه مواكبة التطور التكنولوجي العالمي في مجال استخدام الوسائل الرقمية، لكن الغموض الذي اكتنف المجال المعلوماتي من الناحية القانونية بسبب تعدد وتنوع تقنيات الاتصال المستحدثة التي استغلها الجناة في أساليب الاعتداء كشف عن فراغ تشريعي لبسط حماية قانونية فعالة للبيانات والنظم المعلوماتية، وتهدف هذه الدراسة الى التطرق لتوجهات المشرع الجزائري للتصدي للجرائم المعلوماتية الماسة بسلامة وسرية المعلومات ومواكبة المستجدات حيث سعى الى تحديث المنظومة التشريعية القائمة وسن قوانين خاصة ذات الصلة على غرار القانون 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال والقانون 07-18 المعدل والمتمم بالقانون 11-25 المتعلق بحماية الاشخاص الطبيعية في معالجة المعطيات الشخصية، على الرغم من هذه التحديثات بقيت هذه القوانين محل جدل من حيث كفايتها في ظل واقع رقمي متغير سريع التطور يتطلب ضرورة اصدار قوانين مرنة ومتكيفة للتعامل مع هذه الجرائم، وتعزيز الفضاء الرقمي باليات متطورة لتحقيق امن المعلومات.

الكلمات المفتاحية: المعلومات السرية، النظام المعلوماتي، التلاعب بالبيانات، الفضاء الرقمي.

Abstract :

The diversification of computer applications has led to a myriad of opportunities and possibilities for assaulting software, whether through destruction, forgery, or unauthorized use. This poses a significant threat to the security of society, which is compelled to keep pace with global technological advancements in the use of digital means. However, the legal ambiguity surrounding the information technology field—due to the multiplicity and diversity of modern communication techniques exploited by perpetrators—has revealed a legislative vacuum in extending effective legal protection to data and information systems.

This study aims to examine the trends of the **algerian legislator** in combating cybercrimes that compromise the integrity and confidentiality of information. In an effort to keep abreast of developments, the legislator has sought to modernize the existing legal framework and enact

specific relevant laws, such as **law no. 04-09** relating to the prevention of crimes connected with information and communication technologies, and **law no. 07-18** (as amended and supplemented by **law no. 11-25**) concerning the protection of natural persons in the processing of personal data. Despite these updates, these laws remain a subject of debate regarding their adequacy within a rapidly evolving digital reality. This necessitates the issuance of flexible and adaptive legislation to tackle such crimes and the reinforcement of the digital space with advanced mechanisms to achieve information security.

Keywords : Confidential Information, Information System, Data Manipulation, Digital Space.

المقدمة:

أحدث التطور العلمي والتكنولوجي ثورة في نظم الاتصالات والمعلومات في العصر الحديث برز فيها الحاسب الآلي كأداة محورية نظرا لتعدد وظائفه وقدرته الفائقة على معالجة البيانات المعقدة، ومع التسارع التقني المتزايد اجتاحت هذه الأنظمة كافة المجالات الاقتصادية والاجتماعية والسياسية والعسكرية، تحولت على اثرها المعلومات الى مصدر للثروة ومقياسا لتقدم الأمم واساسا للقوة السياسية والاقتصادية في النظام العالمي الجديد، رغم ذلك كان لهذا التطور الهائل جانب مظلم ناتج عن سوء استخدام شبكات الحاسب الآلي والمعلومات الالكترونية مفرزا نمطا جديدا من الاجرام يستهدف الفضاء المعلوماتي، وكان من الصعوبة في الكثير من الأحيان بسط النفوذ القانوني على هذا الفضاء وتوفير الحماية الأمنية لبرامج الحاسوب والنظم المعلوماتية لاستخدام الجناة التكنولوجيا المتقدمة في أساليب الاعتداء والاختراق، وبالتفشي الواسع النطاق لهذه الجرائم أصبحت التشريعات الجنائية التقليدية ومن بينها التشريع الجزائري عاجزة عن مجابهة أخطارها، لان نصوصها في الأساس في الأساس تنصب على أفعال تقليدية ومنقولات مادية ذات كيان مادي ملموس لا تتماشى مع طبيعة المعلومات ونظم معالجتها محدثة بذلك فراغا تشريعا لغياب نصوص عقابية خاصة للتصدي لها، رغم محاولة المشرع الجزائري ادراج نصوص ضمن قانون العقوبات بموجب القانون 04-15 المعدل والمتمم بالقانون 24-06 لتجريم هذه الأفعال الا انها لم تكن بالقدر الكافي لردع ومواجهة هذا النمط المستحدث، فنصوصه لم تتضمن جميع الصور والاشكال التي تكون عليها الجريمة المعلوماتية، مما أدت الضرورة إلى سن عدة قوانين خاصة لضمان سلامة المعلومات الإلكترونية وضمان سريتها وتوفير الحماية المتوخاة تماشيا مع ما جاءت به الاتفاقيات الدولية والإقليمية، أهمها القانون 09-04 المنظم للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها والذي يعد ركيزة تشريعية متخصصة لمواجهة الجرائم المعلوماتية. من هنا نطرح الإشكالية حول مدى كفاية الاحكام التشريعية الموضوعية لحماية المعلومات وضمان سلامتها وسريتها؟

تهدف هذه الدراسة الى الوقوف على مدى قدرة الترسانة القانونية الخاصة ذات الصلة بتكنولوجيا الاعلام والاتصال على تنظيم الفضاء الرقمي والحفاظ على سرية وسلامة البيانات والمعلومات وضمان سلامة الأنظمة المعلوماتية من أي استخدام غير مشروع، ومنع استخدام التقنيات الحديثة بما يضر بالأفراد والمجتمع.

تماشيا مع طبيعة الإشكالية المطروحة اعتمدنا في الدراسة على المنهج الوصفي التحليلي لتوصيف مظاهر الاجرام المعلوماتية وصور الجرائم المعلوماتية التي تمس بسرية المعلومات وتفصيل كل جريمة مع استعراض النصوص القانونية التي رصدها المشرع الجزائري لمواجهتها وتحليلها، بالإضافة الى الاستعانة بالمنهج المقارن في جانب من الموضوع المتعلق بالنظام المعلوماتي ومقارنته بتشريعات بعض الدول والاتفاقية الدولية.

تم تقسيم هذه الدراسة الى محورين رئيسيين تناول المحور الأول الإطار المفاهيمي للجرائم المعلوماتية الماسة بسلامة وسرية المعلومات من خلال تبين اهم المفاهيم المتعلقة بالمعلومات الالكترونية وخصائصها الى جانب ضبط مفهوم الجريمة المعلوماتية، اما المحور الثاني خصصناه للتركيز على اهم التشريعات الوطنية التي رصدها المشرع الجزائري لمواجهة هذه الجرائم.

1 - الإطار المفاهيمي للجرائم المعلوماتية الماسة بسلامة وسرية المعلومات

1.1- مفهوم الجرائم المعلوماتية

لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها، فالبعض يطلق عليها جريمة الغش المعلوماتي والبعض الآخر يطلق عليها جريمة الاحتيال المعلوماتي وآخرون يطلقون عليها تسمية الجريمة المعلوماتية.

كما يطلق جانب من الفقه على جرائم المعلوماتية اصطلاح جرائم التكنولوجيا الحديثة لارتباطها من جهة ارتباطا وثيقا بالتكنولوجيا التي تعتمد أساسا على الحواسيب وغيرها من أجهزة تقنية، ومن جهة أخرى حديثة نظرا لحدائتها النسبية وارتباطها بأجهزة حديثة تكون ذات طاقة تخزينية وسرعة فائقة ومرونة في التشغيل 1.

فمصطلح المعلوماتية يدور في فضاء واسع من الحقول والتخصصات المتنوعة، ويرتبط بأبعاد وعلاقات ومداخل متباينة منها ما هو مرئي واضح، وما هو غير مرئي ومؤثر وحيوي، وهذا ما يجعل مفهوم المعلوماتية غير واضح تماما وغير محدد.

ويكون من الصعوبة الاتفاق على تعريف موحد لسرعة وتيرة تطور التقنية المعلوماتية من جهة، وتباين الدور الذي تلعبه هذه التقنية في الجريمة من جهة أخرى، فالنظام المعلوماتي لهذه التقنية يكون محلا للجريمة تارة، ويكون وسيلة لارتكابها تارة.

فأخرى في هذا السياق تباينت الاتجاهات الفقهية بين المفهوم الموسع والمفهوم المضيق لها.

فمن التعريفات الموسعة لمفهوم الجريمة المعلوماتية تعرف بأنها كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات بهدف الاعتداء على الأموال المادية أو المعنوية.²

وكذلك التعريف الذي جاء به مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاونة المجرمين المنعقد في فيينا سنة 2000 بأنها اية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب³ ويعد هذا التعريف شامل أحاط بجميع الصور الإجرامية المعلوماتية سواء التي تقع بواسطة النظام المعلوماتي أو على المعطيات والبرامج والمعلومات داخل هذا النظام.

في حين أن التعريفات المضيق لمفهوم الجريمة المعلوماتية تعرفها بأنها الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي، أو هي الفعل الإجرامي الذي يستخدم في ارتكابه الحاسوب باعتباره أداة رئيسية⁴، يسند هذا التعريف الجريمة الى وسيلة ارتكابها وهو الحاسوب، وهذا سبب النقد الذي تعرض له لان الجريمة تتجسد بالعمل الأساسي المكون لركنها المادي وليس بالوسيلة المستخدمة لتحقيقها،

كما عرفت أيضا بأنها نشاط غير مشروع موجه لنسخ أو الوصول الى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو الوصول اليها والتي تحول طريقه.

الملاحظ ان تعريفات الاتجاه المضيق ليست جامعة وتتسم بقصور كبير في إعطاء تصور علمي للجرائم المعلوماتية.

1.1.1-المقصود بالمعلومات الإلكترونية

تباين مدلول المعلومات مع بعض المصطلحات كالبيانات والمعطيات غير ان غالبية التشريعات لا تميز بين المعلومات والبيانات في مجال الحماية الجنائية لسرية المعلومات، بل تعتبر كل منهما مرادفا للآخر حيث أن التشريعات التي تبنت مصطلح المعلومات عرفت أنها البيانات، والتشريعات التي تبنت مصطلح البيانات عرفت أنها المعلومات على الرغم من أن التوصية الصادرة عن منظمة التعاون الاقتصادي والتنمية لعام 1992 الخاصة بحماية أنظمة الحاسبات الآلية وشبكات المعلومات وضحت الفرق بينهما، حيث عرفت البيانات بأنها " مجموعة من الحقائق أو المفاهيم والتعليمات تتخذ شكلا محددا يجعلها قابلة للتبادل والتفسير أو المعالجة بواسطة الأفراد أو بوسائل الكترونية، أما المعلومات فهي المعنى المستخلص من هذه البيانات ".⁶

واستعمل المشرع الجزائري في هذا السياق مصطلح المعطيات المعلوماتية عوض البيانات وعرفها بأنها عرض الوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل المنظومة المعلوماتية.⁷

في حين يعرفها التشريع الاماراتي بأنها كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات وبوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والاشارات وغيرها.⁸

وبالرجوع الى الفقه يرى البعض منه ان البيانات هي المعطيات المتصلة بجهة ما والمعلومة هي المعنى المستخلص منها بعد معالجتها، في حين يرى البعض الآخر بأن البيانات هي مدخلات النظام المعلوماتي والمعلومات هي مخرجاته، فالمعلومة هي المعنى المستنتج من البيانات، لأنها في الأصل بيانات ثم تحليلها وتفسيرها ومعالجتها.⁹

ويعد التعريف الفقهي الشامل للمعلومات بأنها "مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال أو للتفسير أو المعالجة بواسطة الأفراد أو الأنظمة الإلكترونية."¹⁰

والمعلومات المستهدفة بالحماية الجنائية محل الدراسة هي المعلومات الإلكترونية المعالجة الكترونيا، أي المعالجة آليا بواسطة نظام معلوماتي أو أحد أجزائه كالحاسب الآلي، بهدف تصنيفها وإعادة انتاجها وبثها او تخزينها وتسجيلها سواء بواسطة أحد الأجزاء الداخلية للنظام المعلوماتي كذاكرة الحاسب مثلا أو على وسائط تخزينا خارجي كالأقراص المرنة، فالفقه القانوني لا يميز بينهما لتحديد نطاق الحماية، لان محل الحماية هي المعلومات بصفة عامة وطالما ان المعلومة هي المعنى المستنتج من البيانات فالحماية تشملهما معا.

1-1-2 الصفات الواجب توفرها في المعلومات

تختلف المعلومات فيما بينها من حيث النوع، قد تكون نوع من المعرفة أو شكل رسمي هندسي، أو مجموعة من الأوامر والإرشادات، وقد تتعلق بأمور مالية أو ذات طبيعة فنية أو أدبية، ورغم تنوعها يجب أن تتمتع بصفات معينة حتى تحظى بالحماية القانونية وتتمثل هذه الصفات في:

التحديد: سبق أن رأينا انا المعلومات عبارة عن حقائق أو رموز أو مفاهيم يتم تبليغها لإيصال رسالة ما ينبغي أن تكون محددة يمكن حصرها في دائرة أو نطاق خاص بها، فالتحديد عنصر أساسي حتى يمكن اعتبار المعلومات حقا، ومحل الحق يتعين ان يكون محددا لإمكانية اضعاء الحماية الجزائية له في حالة الاعتداء عليه.¹¹

الابتكار: تنصب هذه الصفة على الرسالة التي تحملها المعلومة ما يجعلها ملكا لصاحبها ويوفر الحماية القانونية لها، لأن المعلومة الشائعة متاحة للجميع ويمكن للجميع الوصول اليها ولا يمكن نسبها الى شخص محدد.

السرية: يقصد بها أن المعلومة تدور في نطاق محدود من الأشخاص، وتستمد هذه الصفة إما بإرادة صاحبها كاكشاف في مجال حديث، أو بحسب طبيعتها كاكشاف شيء لم يكن موجودا، أو للسببين معا مثال الرقم السري لبطاقة الائتمان.¹²

الاستثناء: تعد صفة الاستثناء ضرورية، وتعني ان المعلومة تخص شخصا معيناً له السلطة عليها ولا يمكن الحصول او الوصول اليها دون تصريح منه، بمعنى اختصاص الشخص بشيء معين استقلاله به على سبيل التفرد فالمالك في حق الملكية يستأثر بمحل الملكية.¹³

1-3-1 صاحب الحق في سرية المعلومات

إن عماد أمن المعلومات السرية التي تجعل المعلومة خاصة بمالكها أو من له سلطة قانونية عليها سواء كان شخصا طبيعيا أو معنويا، وأن تحفظ من الاطلاع والكشف غير المصرح به من قبل الأشخاص غير المرخص لهم بذلك، وتم تعريفها بواسطة المنظمة الدولية للتوحيد القياسي "ايزو" انها ضمان ان تكون المعلومات متاحة فقط لأولئك الذين يؤذن لهم الاطلاع"¹⁴

فصاحب الحق في سرية المعلومات هو مالكها أو من له سلطة قانونية عليها تخوله الاستثناء بها واستعمالها واستغلالها دون شرط أو قيد، سواء كان شخصا طبيعيا أو شخصا اعتباريا كالمؤسسات البنكية أو الدولة بالنسبة لأسرار الدولة الأمنية أو السياسية، ولا تنتفي صفة السرية عن المعلومات في حالة الاطلاع عليها من شخص معين كما هو الحال بالنسبة لأسرار المصارف والبنوك التي يطلع عليها موظفو البنك لأن كل منهم يتعامل معها في إطار من السرية والكتمان.

كما ان هناك حالة الترخيص ممن له السلطة القانونية على المعلومة، للآخرين للاطلاع عليها واستخدامها مثل القنوات المشفرة.

1-1-4 الفرق بين المعلومات السرية والمعلومات الشخصية

تختلف المعلومات الشخصية عن المعلومات السرية بكونها بيانات تتعلق بشخص معين يمكن استخدامها لتحديد هويته مثل الاسم الكامل، ورقم الهوية تاريخ الميلاد العنوان رقم الهاتف، البيانات البيو مترية، وتستخدم هذه المعلومات عادة في الإجراءات الرسمية، كالتسجيل في المؤسسات التعليمية أو فتح حسابات، الهدف منها تعريف وتحديد هوية الأشخاص، ويمكن مشاركتها مع جهات رسمية بعد موافقة الفرد.

أما المعلومات السرية فهي بيانات تظل محفوظة وسرية لأسباب أمنية أو تجارية، ولا تكشف إلا للأشخاص المسموح لهم بذلك لما قد يؤدي إفشاؤها من خسائر مالية وأضرار قانونية، مثل المعلومات الحكومية أو الأمنية كلمات المرور واسرار الحسابات البنكية، الأسرار التجارية للشركات كخطط الإنتاج، والهدف من سريتها حماية مصالح الأفراد أو المؤسسات من الضرر ولا يمكن مشاركتها إلا مع أشخاص معتمدين أو مخولين بذلك.

1-2- صور الجرائم المعلوماتية الماسة سرية المعلومات

أدى الاعتماد المتزايد على نظم المعلومات في جمع المعلومات الخاصة بالأفراد والشركات ومؤسسات الدولة وتخزينها ومعالجتها وتحليلها والربط بينها واسترجاعها، الى تعرضها الى عدة مخاطر وأفعال إجرامية تمس سلامتها وسريتها عن طريق الوصول إليها بغير تصريح أو إذن.

وتعددت صور هذه الجرائم بحيث تكون دخول أو بقاء أو تلاعب بالبيانات، إلا أن محل الجريمة الذي يعد الركن المفترض فيها واحد وهو النظام المعلوماتي المستهدف بالاعتداء.

1-2-1 محل الجريمة (النظام المعلوماتي)

يقصد بمحل الجريمة النظام المبرمج للبيانات والذي يشمل عدة وحدات المعالجة أو الذاكرة أو البرامج أو البيانات أو وحدات الإدخال والإخراج التي تساعد في الوصول الى نتيجة محددة.

وبينت المذكرة التفسيرية في تعليقها على المادة 2 من اتفاقية بودابست المقصود بالنظام المعلوماتي الدخول الى أحد الكيانات المادية أو المعنوية مثل البرامج أو بيانات مخزنة في نظام التنصيب أو بيانات تتعلق بالمرور والمحتوى.¹⁵

وتناولت تعريفه التشريعات العربية والغربية منها التشريع الجزائري حيث جاء في القانون 04-09 بالمنظومة المعلوماتية هو " أي نظام منفصل او مجموعة من الأنظمة المتصلة أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات لتنفيذ لبرنامج معين "¹⁶

وعرفه التشريع الإماراتي بأنه " مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات أو المعلومات أو الرسائل الإلكترونية أو غير ذلك. "¹⁷

وجاء في التشريع الفرنسي المقصود بنظام المعالجة الآلية للمعلومات بأنه مجموعة وحدات المعالجة أو الذاكرة أو البيانات أو نظام الدخول أو الخروج أو وحدات الاتصال التي تساعد على تحقيق النتيجة المطلوبة وتكون موضوعة للحماية بنظام الأمن.¹⁸

وتعرف كذلك نظم المعلومات على انها البرامج التي تستخدم في ارشفة وإدارة وتنظيم البيانات والحصول على المخرجات من خلال إجراءات معينة يتم انشاؤها وفق الية سير العمل في أي مؤسسة.¹⁹

1-2-2 جريمة الدخول غير القانوني للنظام المعلوماتي

يمثل الدخول غير المشروع الى النظام المعلوماتي من الجهة التقنية الفعل الأول لأنشطة جرائم الحاسوب والأنترنت، فقد يتوقف نشاط الجاني عند هذا الحد وقد يمتد الى ابعد من ذلك، وهذا ما اثار الجدل حول ما إذا كان مجرد الدخول في حد ذاته يشكل جريمة، أم يجب ان يقترن بأفعال أخرى لاحقه كتعديل معلومات أو

حيازتها أو إتلافها، كما أثار أيضا خلافا في الفقه الجنائي حول مدى اعتباره جريمة تامة أم اعتباره عملا تحضيريا لأفعال أخرى ومدى انطباق وصف جريمة تقنية المعلومات عليه.

1-2-2-1 السلوك المحدد لجريمة الدخول غير المشروع

لم تفرض اتفاقية بودابست أسلوبا محددا لتجريم الدخول الى النظام المعلوماتي، وتركت الخيار للدول لاختيار الأسلوب الأنسب لها لتجريم الدخول غير القانوني، وتأثرت العديد من التشريعات الداخلية بهذه الاتفاقية حتى بالنسبة للدول غير المصادقة عليها فيكفي ان يكون الدخول غير مصرح به أو تم عن طريق الغش كما جاء في قانون العقوبات الجزائري بعبارة " كل من يدخل أو يبقى عن طريق الغش "²⁰

وعادة يتم النشاط في هذه الجريمة بالاتصال بالنظام المعلوماتي بأي طريقة كانت ولا عبء بالوسيلة التي اتبعتها الجاني في الدخول إلى النظام، وفي الغالب يتم باستخدام وسائل تقنية أو إلكترونية لأنها أساس الجريمة بشرط أن يتم بدون تصريح أو ترخيص، أي انعدام سلطة الجاني في الدخول مع علمه بذلك.

لأن الدخول بحد ذاته لا يشكل سلوكا غير مشروع، وإنما يتخذ الوصف الجرمي إذا تم دون وجه حق بدون رضا مالك النظام كما وصفه المشرع الجزائري عن طريق الغش أو دون الحصول على تصريح منه أو بدون إذن من السلطة المختصة، ويأخذ نفس الحكم إذا تجاوز الجاني التصريح الممنوح له بأن كان مصرح له بالدخول الى جزء من النظام إلا أنه تجاوز هذا التصريح وقام بالدخول الى كامل النظام أو إلى أجزاء أخرى يحظر عليه الدخول اليها وهذا بما جاء في المادة 394 مكرر الدخول في كل جزء من منظومة المعالجة الآلية للمعطيات، والعلة في ذلك أن التصريح يخول له صلاحيات الاطلاع على معلومات أو بيانات محددة، ما عدا ذلك من المعلومات والبيانات يسري عليه حكم السرية، ويتعين بذلك وجوب تحديد مسبق للتصريح بالدخول إلى النظام المعلوماتي، يحدد فيه اختصاص كل عامل بالنظام وحدود اختصاصه،²¹ وكذلك الحالة التي يكون فيها الدخول مشروطا بدفع ثمن محدود وبالرغم من ذلك ينفذ الجاني الى النظام دون تسديد ثمن.²²

1-2-2-2 وسائل الدخول غير القانوني

على اعتبار أن القانون لم يحدد الوسيلة التي يتم بها الدخول يمكن أن نتناول بعض الوسائل يلجأ إليها الجاني:

- تشغيل كمبيوتر مقفول وهنا ليس تشغيل الجهاز فقط وإنما التمكن من النفاذ الى الملفات والاطلاع على ما تحتويه من معلومات.

- الدخول الى الكمبيوتر عن طريق خط تلفوني.

- الدخول الى الكمبيوتر من كمبيوتر آخر، ويتم باستعمال الجاني جهاز الكمبيوتر بطريقة قانونية ويدخل الى معلومات في كمبيوتر آخر كإجراء توصل بدون موافقة صاحب الجهاز الثاني.

-النفاذ الى نظام متصل بنفس الكمبيوتر يكون النفاذ الى الأنظمة المتصلة بهذا الجهاز متاح الدخول اليها نظير اشتراك مالي معين.²³

1-2-2-3 صاحب السلطة في التصريح بالدخول

كل شخص طبيعي أو معنوي، أو كل سلطة عامة أو مؤسسة أو جهاز يكون له سلطة التصرف في نظام الحاسب الآلي التابع له وتقرير مضمونه أو محتواه وكيفية تنظيمه، والهدف منه حسب ما جاء في الاتفاقية الخاصة بحماية الأفراد في مواجهة نظم المعالجة الآلية للمعطيات التفرقة بين مالك النظام والمستخدم، فمالك النظام المعلوماتي كل شخص له سلطات على النظام المعلوماتي بحيث يحق له استعماله واستغلاله والتصرف فيه وهذا مستمد من تعريف حق الملكية سواء كان شخص طبيعي أو شخص معنوي كالمؤسسات والشركات والهيئات والدول، أما المستخدم أو المرخص له فهو من منحه مالك النظام الرخصة لاستخدام إما بحكم عمله لديه أو مقابل مادي.²⁴

1-2-3 جريمة البقاء غير المرخص به في النظام المعلوماتي

تعد جريمة الدخول الى النظام المعلوماتي جريمة عمدية تتم بسلوك إيجابي، وهذا ما يجعل مجرد الدخول الخاطئ أو العرضي غير معاقب عليه قانونا، لكن يعاقب على البقاء في هذا النظام بعد أن يتبين للجاني أن دخوله خاطئ ويصبح فعله بذلك جريمة عمدية وهي من الجرائم الشكلية التي لا تشترط حدوث نتيجة جرمية معينة، ولم تتطرق غالبية التشريعات ومن بينها التشريع الجزائري الى تحديد المقصود بالبقاء وتولي الفقه تحديده.

1-3-2-1 السلوك الإجرامي المحقق للبقاء غير المرخص به

يقصد بالبقاء التواجد داخل نظام معلوماتي ضد إرادة من له الحق في السيطرة عليه ويمكن ان يتحقق مستقلا عن الدخول أو يجتمعان معا، ويكون البقاء معاقب عليه استقلا إذا فضل الجاني البقاء في النظام الذي دخله عن طريق الخطأ أو الصدفة على الرغم من علمه بأنه غير مرخص له بدخوله، فالنتيجة هي الوصول إلى نظام غير مصرح له الدخول إليه والمساس بالمصلحة التي يحميها القانون وهي المعطيات.²⁵

التساؤل هل يأخذ نفس الحكم دخول الجاني إلى النظام بطريقة مشروعة ولكنه يستمر بعد الوقت المحدد لبقائه فيه ويحدث ذلك إذا كان استعمال النظام محددا بوقت معين نظير أجر مالي فيتخطى الجاني هذا الوقت ويحصل على الخدمة مدة أطول من المدة التي دفع مقابلها نتيجة استخدام وسائل أو عمليات غير مشروعة، الملاحظ أن المشرع الجزائري لم يشير إلى هذه النقطة بل اكتفى بالنص على البقاء عن طريق الغش والمفترض أنها تنطبق كذلك على حالة الدخول صدفة أو خطأ، أما الدخول المرخص به لوقت محدد وتجاوز الجاني المدة المحددة في التصريح لا يسري عليها نفس الحكم بل تحتل وصفا آخر وهو الاستعمال غير المشروع للنظام

المعلوماتي، وتعتبر جريمة البقاء في النظام المعلوماتي من الجرائم المستمرة نظرا لاستمرار الاعتداء على المصلحة المحمية قانونا باستمرار البقاء غير المصرح به.²⁶

1-2-3-2 القصد الجنائي في جرمتي الدخول والبقاء عن طريق الغش

لا يكفي لتقرير المسؤولية الجزائية أن يصدر عن الجاني سلوك إجرامي ذو مظهر مادي بل يلزم توافر قصد جنائي، وذهبت اتفاقية بودابست المتعلقة بالجريمة الإلكترونية وغالبية التشريعات الى اعتبار جريمة الدخول أو البقاء من الجرائم العمدية التي يقترفها الجاني وهو عالما بحقيقتها وعناصرها القانونية، غير انه تباينت التشريعات لتجريم الدخول أو البقاء حول ضرورة توافر قصدا خاصا لدى الفاعل وهو نية التأثير على البيانات أو على نظام الكمبيوتر نفسه، ام تجريم مجرد الدخول بشكل مطلق دون استلزام توافر قصدا خاصا، تبنت غالبية التشريعات ومن ضمنها التشريع الجزائري الرأي الأخير فالقصد الجنائي المطلوب هو القصد العام ويراد به أن يكون الفاعل على علم بأن دخوله غير مشروع لا يستند إلى حق قانوني أو تصريح من مسؤول النظام يخوله النفاذ إلى النظام أو الاطلاع على ما يحتويه من معلومات أو بيانات أو برامج، وأن تتصرف إرادته الى اتيان السلوك وتحقيق النتيجة ويجب ان يعاصر القصد الجنائي النشاط الإجرامي فإذا لم يتحقق وقت الدخول ولكنه تحقق فيما بعد اعتبر فعله جريمة بقاء غير مشروع، والتساؤل المطروح هل يسأل الجاني في حالة ما ترتب عن الدخول أو البقاء تخريب النظام المعلوماتي أو تم حذف وتغيير معطياته والبيانات المخزنة فيه عن جريمة مستقلة قائمة بذاتها أم يؤخذ بقصد احتمالي متوقع منه عن فعلي الدخول والبقاء غير المشروع؟ هذا ما اشارت اليه المادة 394 مكرر من قانون العقوبات في حالة تجاوز مجرد الدخول او البقاء إلى إلحاق أضرار أو تخريب النظام المعلوماتي أو إحداث تغيير أو إزالة بيانات ومعطيات مخزنة به لا يسأل عن جريمة مستقلة بل كظروف مشددة لجريمة الدخول او البقاء غير المشروع.

1-2-4 جريمة التلاعب بالبيانات المبرمجة

لم يعرف المشرع الجزائري جريمة العبث أو التلاعب عن طريق الغش في المعطيات المبرمجة في النظام المعلوماتي، بل أورد لها صور سنوضحها بعد الإجابة على السؤال الجدير بالطرح هل يشترط القانون لقيام جريمة التلاعب أن يكون الدخول إلى النظام المعلوماتي غير مشروع؟

يستوي الأمر لقيام الجريمة أن يكون دخولا مشروعا أو غير مشروع رغم أنه في الحالة الأخيرة نكون أمام جريمتين الدخول غير المشروع والتلاعب بالمعطيات، فهل يسأل الجاني عن الجريمتين طالما أن المشرع أفرد لكل جريمة نصا خاصا، أم يؤخذ بالوصف الأشد وهو في هذه الحالة العبث بالمعطيات لأنه لا يتصور التلاعب دون دخول.

ويقصد بالتلاعب بالبيانات المبرمجة إدخال معطيات غير مصرح بها في النظام المعلوماتي أو تعديل بيانات موجودة أو إلغائها،²⁷ وهنا يكمن الفرق بين إدخال معطيات أو حذفها أو تغييرها كنتيجة عن جريمة

الدخول والإدخال والتغيير والإزالة كصورة لجريمة التلاعب بالمعطيات ففي هذه الحالة يكون الفعل مقصودا في حد ذاته كسلوك وليس كنتيجة.

1-4-2-1 السلوك المحقق لجريمة التلاعب

يتحقق السلوك الاجرامي بإدخال بيانات غير مصرح بها اي بيانات جديدة غير موجودة في النظام ينتج عنها تعديل المحتوى المادي للبيانات المبرمجة ويتخذ عدة صور :

- الصورة الأولى: تتجسد بإدخال بيانات غير مصرح بها، أي إضافة معطيات غير موجودة في النظام.
- الصورة الثانية: حالة تعديل واستبدال المعلومات التي يحتويها النظام، فهنا تظل المعلومة موجودة لكن لها معنى مغاير للمعنى الأصلي الذي كانت عليه قبل فعل التغيير فتؤدي إلى نتائج مغايرة عن تلك التي صمم البرنامج لأجلها.

- الصورة الثالثة: وهي الحذف أو الإزالة لمعطيات موجودة في المنظومة يسري عليها نفس حكم التعديل تتجسد بمحو جزء من البيانات المسجلة على الدعامة والموجودة داخل نظام المعالجة الآلية أو نقل وتخزين جزء من المعلومات إلى المنطقة الخاصة بالذاكرة.

وعلة تجريم هذه الأفعال هي حماية البيانات المبرمجة التي أصبحت محل البيانات المكتوبة في الملف الورقي وتصلح أن تكون محررات مرتبة لآثار قانونية في حالة التمسك بها، يشكل العبث بها جريمة تزوير محررات إدارية أو عرفية أو مصرفية، ويوفر القانون حماية أكثر للبيانات داخل الكمبيوتر تتسحب إلى كافة البيانات ذات القيمة حتى ولو لم ترتب آثارا قانونية فتصبح جريمة إتلاف مستند.

1-4-2-2 الركن المعنوي في جريمة التلاعب

يثار التساؤل حول شكل الركن المعنوي، أي مدى تطلب القصد الجنائي أم الخطأ غير العمدى في جريمة التلاعب، لم يحدد النص الجنائي في قانون العقوبات شكل الركن المعنوي بصورة واضحة واكتفى بإدراج صور السلوك، والأصل أنه إذا لم يحدد النص العقابي صورة الركن المعنوي تكون الجريمة عمدية تقوم على القصد الجنائي العام يكون الجاني قاصد إحداث تغيير أو إزالة أو إضافة بيانات إلى النظام.

2-آليات المواجهة التشريعية للجرائم المعلوماتية الماسة بسرية وسلامة المعلومات

عمل المشرع على حماية الفضاء الرقمي ومستخدميه بالتصديق على الاتفاقيات الدولية والإقليمية مع ادراج تعديلات على القوانين القائمة تماشيا مع هذه الاتفاقيات، ونظرا لعدم كفايتها للإلزام بهذا الجرائم المستحدثة توجب ضرورة إصدار قوانين خاصة من أجل إقرار منظومة تشريعية متكاملة وفعالة للتصدي لهذا النوع من الإجرام.

1.2- آليات المواجهة ضمن احكام قانون العقوبات

يتسم الفضاء المعلوماتي بضبابية قانونية ناتجة عن تسارع وتيرة التقنيات المستحدثة، مما أدى الى بروز فجوة تشريعية عجزت النصوص التقليدية عم استيعابها. ورغم الجهود المبكرة للمشرع الجزائري في تطوير قانون العقوبات، إلا أن القصور ظل قائما أمام تنوع صور الجريمة المعلوماتية و يشكل القانون 04-15²⁸ نقطة تحول جوهريّة بجنوحه نحو تجريم المساس بأنظمة المعالجة الآلية للمعطيات، لا سيما الدخول الاحتياطي و التلاعب بالبيانات، وتلا ذلك تعزيز السياسة الجنائية بموجب القانون 06-23²⁹ الذي بسط الحماية القانونية لتشمل حرمة الحياة الخاصة ومواجهة إفشاء الأسرار عبر الوسائط الرقمية، باستعمال الحاسوب وشبكة الأنترنت والهاتف النقال لالتقاط أو تسجيل ونقل مكالمات أو أحاديث خاصة وسرية بغير إذن صاحبها ورضائه، وصولا الى القانون 06-24³⁰ الذي جاء بتعديلات حاسمة شددت العقوبات في المادتين 394 مكرر و 394 مكرر 1، استجابة للمنحنى التصاعدي لهذه الجرائم التي مست القيم المعنوية المتمثلة في المعلومات والبيانات مما جعل نصوص قانون العقوبات عاجزة عن مواجهة هذه الصور الأمر الذي دفع المشرع إلى إخضاعها لنصوص مباشرة دقيقة وشاملة لكل صور الإجرام المعلوماتي.

2.2- آليات المواجهة في القوانين الخاصة

أدى عجز قانون العقوبات على مواجهة الواقع المعلوماتي بكل ما فيه من سلبيات وإيجابيات وعدم إمكانية النصوص التقليدية من الإحاطة بصور الجريمة المعلوماتية إلى وجوب الاتجاه نحو إصدار قوانين خاصة يجرم من خلالها جميع صور وأشكال هذه الجريمة تماشيا مع جاءت به الاتفاقيات الدولية والاقليمية، وتم إصدار العديد من القوانين القطاعية التي تنظم أي قطاع خاص يكون محلا لإجرام إلكتروني تهدف قواعده إلى تطوير الفضاء الرقمي مع ضمان المصلحة العامة والفردية وإضفاء حماية وقائية وردعية من الجرائم المتصلة به ونحاول تناول أهم القوانين الخاصة ذات الصلة في التشريع الجزائري.

2-2-1 القانون المتعلق بحماية الاشخاص الطبيعية في مجال معالجة المعطيات الشخصية

نظم قانون معالجة المعطيات ذات الطابع الشخصي بطريقة تراعي فيها عدم المساس بحقوق الأشخاص وشرفهم وسمعتهم وأن تتم في إطار حماية الحياة الخاصة والحريات العامة ،مع إخضاع كل عملية منجزة بوسائل آلية كجمع أو تسجيل أو تنظيم أو حفظ أو تغيير أو استخراج أو الاطلاع أو الاستعمال وكذا التشفير والاعلاق والمسح والاتلاف أو الربط البيني لها ،للموافقة المسبقة الصريحة للشخص المعني أو ممثله الشرعي إذا كان الشخص المعني عديم أو ناقص الأهلية ، وبالنسبة للطفل موافقة ممثله الشرعي أو بترخيص من القاضي المختص عند الاقتضاء³¹، كما قيد عملية معالجة المعطيات لتصريح مسبق لدى السلطة الوطنية التي أنشأت بموجب هذا القانون والتي تعتبر سلطة إدارية مستقلة مشكلة من مختصين قانونيين وتقنيين، تكلف بالسهر على مطابقة المعالجة لأحكام القانون، وضمان عدم انطواء استعمال تكنولوجيا الإعلام والاتصال على أي أخطار على الحقوق والحريات العامة والحياة الخاصة³² مع تزويد هذه السلطة بأقطاب جهوية تتكفل بمهام

المراقبة والتدقيق على مستوى الهيئات والأشخاص المعالجين للمعطيات، و إخضاع كل خرق للإجراءات المنصوص عليها في المادة 07 من القانون 07-18 للعقاب ومسؤولية المسؤول عن المعالجة عن أي خرق للالتزامات السرية وسلامة المعالجة المنصوص عليها في المادتين 38 و39 التي تفرض عليه وضع تدابير تقنية كانت أو تنظيمية لمنع المساس بسلامة المعطيات أو الولوج غير المرخص به الى النظام المعلوماتي الذي يحوي معطيات شخصية³³

2-2-2 القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحة

نظم القانون 04-09 القواعد الخاصة للوقاية ومكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بصورة أكثر وضوحا، حيث أعطى تعريفا للمصطلحات القانونية التي تبين الجريمة بطريقة لا تترك مجالا للتفسير القضائي الموسع الذي ينتهك قاعدة الشرعية الجنائية، وركز على وضع قواعد إجرائية خاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاتصال بمنع الوصول غير المشروع الى الأنظمة المعلوماتية، والتلاعب بالبيانات، وضمان حماية البيانات الشخصية مع وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش و الحجز داخل المنظومة المعلوماتية،³⁴ يعتبر القانون 04-09 قانون ذا طابع وقائي إجرائي سعى المشرع من خلاله الى وضع قواعد إجرائية مستحدثة في البحث والتحري عن الجرائم المتصلة بتكنولوجيا المعلومات، و فرض التزامات على مقدمي خدمة الأنترنت، مع إنشاء هيئة وطنية للوقاية من هذه الجرائم مهمتها تنسيق عمليات الوقاية من هذه الجرائم ومساعدة السلطات القضائية ومصالح الضبطية القضائية في التحريات التي تجريها بشأنها وتبادل المعلومات مع نظيراتها في الخارج لجمع المعطيات المفيدة والتعرف على مرتكبي الجرائم وتحديد مكان تواجدهم.³⁵

2-2-3 القانون المتعلق بالتأمينات الاجتماعية

لتعميم رقمه التأمينات أخضع القانون 01-08 إثبات صفة المؤمن له اجتماعيا ببطاقة الكترونية تحمل الهوية الكاملة له بياناته الشخصية ورقم التأمين، تقدم وجوبا لكل مقدم علاج أو هيكل علاج أو مقدم خدمات مرتبطة بالعلاج، وزود هؤلاء بمفتاح إلكتروني يسمى بالمفتاح الإلكتروني لهيكل العلاج، وأحاط البطاقة بحماية قانونية تحدد صلاحيات مقدمي العلاج أو هيكل العلاج أو الخدمات المرتبطة بالعلاج بالتدخل في حدود مجال اختصاص كل منهم، بقراءة وإدخال كل عمل وخدمة علاج مقدمة للمؤمن اجتماعيا أو ذويه مع إعداد وإرسال الفواتير الإلكترونية الى الضمان الاجتماعي بغرض التعويض، ويتم الاستعمال بواسطة برمجيات يعتمد عليها ويقدمها مجانا صندوق الضمان الاجتماعي،³⁶ يتبين أن القانون اشترط أن يكون الدخول الى البيانات المدرجة في البطاقة الإلكترونية مشروعا وبالقدر المرخص له، وكل مخالفة لهذه الإجراءات ترتب مسؤولية جزائية للفاعل سواء بتعديل عن طريق الغش أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج يترتب عليها مسؤولية الفاعل جزائيا.³⁷

2-2-4- قانون حماية حق المؤلف والحقوق المجاورة

أدرج المشرع ضمن القانون 03-05 برامج الحاسوب كمصنفات تحظى بالحماية القانونية، كما أضاف البيانات كمصنفات محمية سواء كانت مستنسخة على دعامة قابلة للاستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى، واعتبر كل من ينتهك الحقوق المحمية بموجب هذا الأمر جنحة التقليد التي تتم بالوصول الى المصنف بأي طريقة كانت منها التوزيع بواسطة الكابل أو بأي وسيلة نقل أخرى لإشارات تحمل أصواتا أو صورا أو بأي منظومة معالجة معلوماتية، يحمي قانون حماية العلامة التجارية وإجراءات الإفراغ.

2-2-5 قانون حماية المعلومات والوثائق الادارية

اضفى المشرع الجزائري من خلال القانون 21-09 حماية قانونية للمعلومات والوثائق الادارية حيث اعطى مفهوما للوثائق محل الحماية على أنها كل مكتوب ورقي أو إلكتروني أو أي سند مادي³⁹، ثم عمل على تصنيفها حسب درجة حساسيتها الى وثيقة سرية وسرية جدا، وثيقة واجب الكتمان ووثيقة توزيع محدودا وألزم السلطات المعنية بتأمين سلامتها وحماية المعلومات التي تحتويها وعزز الحماية بأحكام عقابية على الموظف الذي يطلع الغير أو ينشر أو يفشي وثيقة مصنفة سواء بصورة عمدية او بعدم مراعاة الاحكام التشريعية أو التنظيمية أو التدابير الاحترازية المرتبطة بطبيعة وظيفته وجرم الدخول بدون ترخيص الى منظومة معلوماتية أو شبكة إلكترونية بغرض الحصول بغير وجه حق على معلومات أو وثائق مصنفة⁴⁰ ويسري التجريم ايضا على كل شخص يقوم بنشر أو بث عن طريق منظومة معلوماتية أو وثيقة مصنفة بغرض المساس بالنظام العام والسكينة العمومية.

الخاتمة:

اعتمد المشرع الجزائري مقاربة واسعة لحماية الأنظمة المعلوماتية من الاعتداء على سرية وسلامة البيانات والمعلومات المخزنة أو المعالجة أو المتداولة عبر نظم المعلومات دون ترخيص، بهدف تحقيق حماية وأمن المعلومات وضمان الثقة في استعمال الوسائل الرقمية من خلال نصوص قانون العقوبات والقوانين القطاعية ذات الصلة بتكنولوجيا الإعلام والاتصال ولإرساء حماية جزائية موضوعية فعالة جابهت هذه المجهودات عدة تحديات فرضها التطور التكنولوجي وخصوصية الجريمة المعلوماتية وتوصلنا الى جملة من النتائج:

- عدم تجميع النصوص العقابية المنظمة للجرائم المعلوماتية الماسة بسلامة وسرية المعلومات في قانون موحد -غموض وعدم دقة القوانين الخاصة بالجرائم المعلوماتية وافتقارها الى اليات تقنية تتماشى مع طبيعة الجرائم.
- قصور نصوص قانون العقوبات على مواجهة الجرائم المعلوماتية لكونها وضعت أساسا لحماية أموال ذات كيان مادي.

- عدم قدرة المشرع الإحاطة عند صياغة القانون بجميع أنماط الجرائم المعلوماتية لتطور التقنية الإلكترونية

-وجود فجوة قانونية بين التطور التكنولوجي والنصوص التشريعية الحالية

التوصيات

- ضرورة إصدار قوانين مرنة ومتكيفة للتعامل مع الجرائم المعلوماتية
- تعزيز الفضاء الرقمي بآليات متطورة لتحقيق أمن المعلومات
- الاهتمام بالتأهيل والتكوين المعمق لإطارات الأجهزة القضائية لجعلها قادرة على التعامل مع هذا النوع من الاجرام.
- نشر الوعي الثقافي والقانوني عن طريق المجتمع المدني بكيفية التعامل مع الفضاء المعلوماتي.

الهوامش:

1. عفيفي، عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية الطبعة 1 بدون نشر 2000 ص 20
2. سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات ط1 دار النهضة العربية القاهرة 1994 ص 170
3. محمد امين الشوابكة، جرائم الحاسوب والانترنت الجريمة المعلوماتية دار الثقافة عمان الأردن 2004، ص 10
4. أحمد هلالى عبد الله، إلزام الشاهد بالإعلام في الجرائم المعلوماتية ط1 دار النهضة العربية القاهرة 1997 ص 13
5. يونس عرب، دليل امن المعلومات والخصوصية، الجزء الأول، جرائم الكمبيوتر والانترنت ط1 اتحاد المصارف العربية، 2002، ص 2013
6. نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، دراسة نظرية وتطبيقية، دار النهضة العربية، القاهرة، 2003، ص 94
7. القانون 04-09 المؤرخ في 05 غشت سنة 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها الجريدة الرسمية الجزائرية، عدد 47 لسنة 2009
8. القانون الاتحادي الاماراتي رقم 2 في شأن مكافحة جرائم تقنية المعلومات الامارات العربية المتحدة الصادر بتاريخ 2006/01/03
9. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الكاتبة، أسيوط، مصر 1995، ص 26 -
10. نائلة عادل إبراهيم قورة، المرجع السابق، ص 93
11. سامي الشوا، المرجع السابق، ص 175
12. نائلة عادل محمد قورة، المرجع السابق ص 109
13. سامي الشوا، المرجع السابق، ص 176

14. إبراهيم حامد طنطاوي، الحماية الجنائية لسرية معلومات البنوك عن عملاتها في ضوء القانون رقم 88 لسنة 2003، دراسة مقارنة دار النهضة العربية، مصر، 2005 ص 18
15. غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، در الفكر والقانون، المنصورة، مصر 2017، ص 142
16. هلاي عبد الله أحمد، الجوانب الموضوعية والاجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست، دار النهضة العربية القاهرة مصر 2003 ص 68
17. انظر المادة 02 من القانون 04-09 المؤرخ في 5 غشت سنة 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها ج.ر الجزائر، العدد 47 لسنة 2009
18. المادة 01 من القانون الاتحادي رقم 2 الصادر بتاريخ 3-01-2006 الموافق لـ 3 ذي الحجة 1426 في شأن مكافحة جرائم تقنية المعلومات المارات العربية المتحدة
19. ايمن عبد الله فكري، جرائم نظم المعلومات، دراسة مقارنة دار الجديدة للنشر الإسكندرية، 2007، ص 223
20. غنام محمد غنام، مرجع سابق ص 136
21. ايمن عبد الله فكري، مرجع سابق، ص 80
22. نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع عمان، الأردن، 2010، ص 159
23. بوبكر رشيدة، جرائم الاعتداء على نظم المعالجة الآلية للمعطيات في التشريع الجزائري والمقارن، منشورات الحلبي الحقوقية، 2012، ص 191
24. نائلة عادل محمد قورة، مرجع سابق، ص 358
25. غنام محمد غنام، مرجع سابق، ص 142
26. سامي الشوا، مرجع سابق، ص 83
27. انظر المادة 394 مكرر من القانون 04-15 المؤرخ في 10-11-2004 المعدل والمتمم للأمر 66-155 المتضمن قانون العقوبات، الجريدة الرسمية الجزائرية عدد 71 لسنة 2004
28. القانون 06-24
29. انظر المادة 07 من القانون 07-18 المؤرخ في 10 يوليو 2018، المتضمن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية الجزائرية العدد 14 لسنة 2018
30. انظر المادة 25 من القانون 07-18 مرجع نفسه
31. انظر المادة 54 مرجع نفسه
32. طباش عزالدين، الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري، دراسة في ظل القانون 07-18 المجلة الاكاديمية للبحث القانون، مجلد 09 العدد 2 سنة 17-12-2018، ص 26-60
33. انظر المادة 3 من القانون 04-09 المؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحة ج ر الجزائر عدد 47 سنة 2009
34. القانون 01-08 المؤرخ في 23 يناير 2008، المتمم للقانون 83-11 المتعلق بالتأمينات الاجتماعية الجريدة الرسمية الجزائرية عدد 04 الصادرة بتاريخ 27-01-2008

35. انظر المادة 65 مكرر من القانون 08-01، مرجع نفسه

36. انظر المادة 93 مكرر، مرجع نفسه

37. الامر 03 - 05 المؤرخ في 19-07-2003 المتعلق بحق المؤلف والحقوق المجاورة الجريدة الرسمية الجزائرية.

ر ج عدد 44 الصادرة بتاريخ 23-07-2003

38. انظر المادة 153 من القانون 03-05 مرجع نفسه

39. المادة 3 من الامر 21-09 المؤرخ في 8 يونيو 2021 المتعلق بحماية المعلومات والوثائق الإدارية الجريدة الرسمية

الجزائرية العدد 45 الصادرة بتاريخ 9 جوان 2021

40. المادة 37 ،مرجع نفسه.