تحديات اللغة العربية في تطوير الإدارة الإلكترونية بالجزائر.

د. مولاي امحمد.

أستاذ تكنولوجيا المعلومات والمخطوطات العربية الإسلامية

بجامعة وهران الجزائر.

moulay.m.taha@gmail.com

الملخص:

تسعى الدول إلى تطبيق الإدارة الإلكترونية للتخلص من أساليب الإدارة التقليدية، وذلك بتحويل كافة العمليات الإدارية ذات الطبيعة الورقية إلى عمليات ذات طبيعة إلكترونية، باستخدام مختلف التقنيات الإلكترونية في الإدارة، وبهذا تتحول المؤسسات إلى مؤسسات إلكترونية تستخدم شبكة الانترنت في إنجاز كل معاملاتها وأعمالها الإدارية، من تخطيط وتنظيم وتوجيه ورقابة، بواسطة التبادل غير المادي للبيانات الرقمية فيما بين المرافق الحكومية والعامة، لتسهيل الحصول على البيانات والمعلومات لاتخاذ القرارات المناسبة وتقديم الخدمات للمستفيدين بكفاءة وفاعلية وبأقل تكلفه وبأسرع وقت ممكن، ومن هنا تعد الإدارة الإلكترونية من الركائز الأساسية لتطور الدول في شتى المجالات.

الجريمة ظاهرة اجتماعية توجد بوجود الإنسان في المجتمع وتتطور بتطورهما، والمجرمون اليوم يحاولون الاستفادة من تكنولوجيا المعلومات والاتصال والنقص الحاد في استخدام اللغة العربية في المجال وانعدام انتاج تكنولوجي عربي، مما سهل ارتكاب الجريمة، ولهذا ظهرت أنماط جديدة من الجرائم لم تكن معهودة تتسم بصعوبة اكتشافها وملاحقتها، حيث أنه رغم الفوائد العديدة التي لا تحصى للإدارة الإلكترونية إلا أنه في نفس الوقت زادت أساليب إساءة الاستخدام لمكوناتها في ظل قلة البرمجيات العربية والنظم الآلية العربية، حيث أصبح الحاسب الآلي بشكل عام وشبكة الانترنت على وجه الخصوص أدوات أو محل ارتكاب الجريمة بمفهومها الحديث اتجاه اللغة العربية، كجريمة السرقة عن طريق الحاسب الآلي المتضمن معلومات باللغة العربية، القرصنة الإلكترونية لمواقع المؤسسات العربية، تخريب البيانات باللغة العربية، غسيل الأموال المكتوبة باللغة العربية،..، وهو ما يتسبب في مشاكل قانونية واجتماعية واقتصادية وأمنية معقدة في المجتمع العربي، مما يستدعي بالضرورة إصدار قوانين خاصة بالجريمة الإلكترونية في الدول العربية والتي من بينها الجزائر، تتماشى مع خصوصيات الجريمة الإلكترونية التي تستهدف اللغة العربية، وتضمن أمن المعلومات الالكترونية المكتوبة باللغة العربية داخل إدارة المؤسسات العربية وخارجها.

مقدمة:

تسعى الدول إلى تطبيق الإدارة الإلكترونية للتخلص من أساليب الإدارة التقليدية وذلك بتحويل كافة العمليات الإدارية ذات الطبيعة الورقية إلى عمليات ذات طبيعة إلكترونية باستخدام مختلف التقنيات الإلكترونية في الإدارة، وبهذا تتحول المؤسسات إلى مؤسسات إلكترونية تستخدم شبكة الانترنت في إنجاز كل معاملاتها وأعمالها الإدارية من تخطيط وتنظيم وتوجيه ورقابة، بواسطة التبادل غير المادي للبيانات الرقمية فيما بين المرافق الحكومية والعامة، لتسهيل الحصول على البيانات والمعلومات لاتخاذ القرارات المناسبة وتقديم الخدمات للمستفيدين بكفاءة وفاعلية وبأقل تكلفه وبأسرع وقت ممكن، ومن هنا تعد الإدارة الإلكترونية من الركائز الأساسية لتطور الدول في شتى المجالات.

الجريمة ظاهرة اجتماعية توجد بوجود الإنسان في المجتمع وتتطور بتطورهما، والمجرمون اليوم يحاولون الاستفادة من تكنولوجيا المعلومات والاتصال في ارتكاب الجريمة، ولهذا ظهرت أنماط جديدة من الجرائم لم تكن معهودة تتسم بصعوبة اكتشافها وملاحقتها، حيث أنه رغم الفوائد العديدة التي لا تحصى للإدارة الإلكترونية إلا أنه في نفس الوقت زادت أساليب إساءة الاستخدام لمكوناتها، حيث أصبح الحاسب الآلي بشكل عام وشبكة الانترنت على وجه الخصوص أدوات أو محل ارتكاب الجريمة بمفهومها الحديث، كجريمة السرقة عن طريق الحاسب

الآلي، القرصنة الإلكترونية لمواقع المؤسسات، تخريب البيانات، غسيل الأموال،..، وهو ما يتسبب في مشاكل قانونية واجتماعية واقتصادية وأمنية معقدة، مما يستدعي بالضرورة إصدار قوانين خاصة بالجريمة الإلكترونية تتماشى مع خصوصياتها، وتضمن أمن المعلومات الالكترونية داخل إدارة المؤسسات وخارجها.

إشكالية الدراسة:

أصبحت الجريمة الإلكترونية في المجتمع الجزائري تجد لها مجالا ومناخا خاصة في ظل شبه غياب للتشريعات والقوانين الواضحة في هذا المجال، وفي ظل التحول إلى الحكومة الجزائرية الإلكترونية أصبح لزاما على الجهات المعنية إيجاد حلول لمختلف الصعوبات التي تعوق سير إدارة الحكومة الإلكترونية بالإضافة إلى القوانين التي تكبح المجرمين الإلكترونيين، **و**تتلخص إشكالية هاته الدراسة في تحديد مفهوم الجريمة الالكترونية والمعلوماتية ومختلف أنواعها، مع محاولة تسليط الضوء على صفات وخصائص المجرمين الالكترونيين والمعلوماتيين وأسباب ارتكابهم لهاته الجرائم، ثم مظاهر الجريمة الالكترونية في المجتمع الجزائري وموقف القانون من الجريمة الالكترونية في ظل التحول الذي تشهده الجزائر نحو الحكومة الالكترونية، ومحاولة تسليط الضوء على مختلف الصعوبات التي تواجه الإدارة الإلكترونية في المؤسسات الجزائرية من خلال الجريمة الإلكترونية كأهم محطة يجب الوقوف عندها من أجل إدارة إلكترونية سليمة للمؤسسات بالجزائر وبناء الحكومة الإلكترونية الجزائرية دون صعوبات قانونية، اجتماعية، اقتصادية، أمنية.

تساؤلات الدراسة: تهدف هاته الدراسة إلى الإجابة على التساؤلات التالية:

– ما هي الإدارة الالكترونية، وما إيجابياتها وسلبياتها؟

– ما هي الجريمة الالكترونية، وما هي أنواعها؟

– ما هي أنواع الجرائم الالكترونية المتواجدة بالمجتمع الجزائري والتي تهدد الإدارة الإلكترونية باللغة العربي في المؤسسات الجزائرية؟ وما موقف القانون منها؟

– ما هي علاقة الجريمة الالكترونية باللغة العربية في الإدارة الالكترونية؟

فرضيات الدراسة:

– توجد مجموعة من الجرائم الالكترونية بالمجتمع الجزائري تهدد أمن اللغة العربية تتطلب سن التشريعات القانونية لمكافحتها.

– لإنشاء حكومة جزائرية الكترونية ناجحة ومستمرة لابد من الأخذ بعين الاعتبار الجريمة الالكترونية التي تشكل أهم صعوبة تواجه اللغة العربية في الإدارة الالكترونية الجزائرية.

أهمية الدراسة: تكمن أهمية هاته الدراسة في محاولة تسليط الضوء على مختلف الجرائم الالكترونية التي يعاني منها المجتمع الجزائري، والتي تستهدف الإدارة الإلكترونية، وكيفية محاربتها انطلاقا من القانون الجزائري للجريمة الالكترونية، بهدف ضمان نجاح وأمن الإدارة الالكترونية الجزائرية، إضافة إلى لفت انتباه الباحثين إلى البحث والدراسة في مجال الجريمة الالكترونية على وجه الخصوص، لما لهذا النوع من الجرائم من صفات خاصة تتطلب المتابعة المستمرة والدقيقة حفاظا على أمن اللغة العربية داخل الإدارات الإلكترونية بالجزائر.

مصطلحات الدراسة:

الإدارة الالكترونية (الحكومة الإلكترونية): عملية انجاز التعاملات الكترونيا بواسطة الحاسب الآلي عبر الانترنت في المكتب أو البيت أو خارج البلاد سواء أكان بين إدارتين حكوميتين أو بين مواطن أو شركة وإدارة حكومية أو بين الشركات والمواطنين بأقل تكلفة وبوقت أسرع.

الجريمة الالكترونية: الجريمة التي يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب، أو في بيئة الكترونية.

المجرم المعلوماتي: ويعرف المجرم المعلوماتي (الالكتروني) بأنه المجرم الذي لديه قدرة على تحويل نواياه إلى لغة رقمية باستخدام التقنية الرقمية المعلوماتية، وذلك بأداء فعل أو الامتناع عنه، مما يحدث اضطرابات في المجتمع المحلي أو الدولي نتيجة مخالفته قواعد الضبط الاجتماعي محليا أو دوليا.

1. الإدارة الالكترونية (الحكومة الإلكترونية):

1.1. تعريف الإدارة الالكترونية (الحكومة الإلكترونية): يعد مفهوم الإدارة الالكترونية من المفاهيم الحديثة التي ظهرت نتيجة للتطورات التقنية، وهو مصطلح يغطي أبعادا تقنية وإدارية وتنظيمية واقتصادية وثقافية أيضا،...، وعرفت الإدارة الالكترونية بأنها قدرة القطاعات الحكومية على تبادل المعلومات وتقديم الخدمات فيما بينها وبين المواطن وبين قطاعات الأعمال، بسرعة ودقة عالية وبأقل تكلفة عب شبكة الانترنت، مع ضمان سرية وامن المعلومات المتداولة في إي وقت وأي مكان[1] وتعرف أيضا بأنها تحول الإجراءات الحكومية الداخلية أو الخارجية والمتمركزة حول توفير أو إيصال الخدمات للمتعاملين معها بفاعلية وكفاءة بصورة أفضل من خلال تقنيات المعلومات والاتصالات الحديثة[2]، وهي أيضا ذلك النظام الافتراضي المعلوماتي الذي يمكن الأجهزة الحكومية المختلفة من تقديم خدماتها في إطار تكاملي، لجميع فئات المستفيدين باستخدام التقنية الالكترونية المتطورة، متجاوزة عامل التواصل المكاني أو الزماني مع استهداف تحقيق الجودة والتميز وضمان السرية والأمن المعلوماتي والاستفادة من معطيات التأثير المتبادل[3]، وبالرغم من عدم وجود تعريف موحد ومتفق عليه للحكومة الالكترونية إلا أن أحدا لا يختلف على الهدف الأساسي للحكومة الالكترونية وهو التحسين المستمر لعمليات التفاعل بين ثلاث مجموعات وهي: الحكومة، قطاع الأعمال، والمواطنين وذلك من اجل تحفيز الرقي السياسي، والاقتصادي، والاجتماعي للمجتمع[4]، ومما سبق يمكن تعريف الحكومة الالكترونية على أنها عملية انجاز التعاملات الكترونيا بواسطة الحاسب الآلي عبر الانترنت في المكتب أو البيت أو خارج البلاد سواء أكان بين إدارتين حكوميتين أو بين مواطن أو شركة وإدارة حكومية أو بين الشركات والمواطنين بأقل تكلفة وبوقت أسرع[5].

2.1. خصائص ومميزات الإدارة الالكترونية (الحكومة الإلكترونية): من خلال التعاريف السابقة للإدارة الالكترونية نستنتج الخصائص والمميزات التالية للحكومة الالكترونية:

– الحكومة الالكترونية تمثل نظام معلوماتي افتراضي لا يمكن أن نلمس ونلاحظ كل مكوناته وعملياته، بالرغم من إمكانية معرفة وملاحظة كل نتائجه وآثاره.

– تعتمد في تطبيقاتها على التقنية الرقمية الحديثة من اجل تحقيق أهداف محددة وفي ظل ضمان السرية والأمن المعلوماتي.

– يعتبر المورد المعلوماتي كأحد موارد المنظمات هو المورد الأساسي الذي تقوم عليه تطبيقات الحكومة الالكترونية.

– تضم منظومة الحكومة الالكترونية أطرافا متعددة الطرف الرئيسي الذي يشكل جوهر مشروع الحكومة الالكترونية، وهو مجموع الأجهزة والمصالح الحكومية المعنية بتقديم الخدمات، الأطراف الثانوية المستفيدة من تلك الخدمات كقطاع الأعمال، المنظمات الاجتماعية الغير حكومية كالنقابات والجمعيات المهنية والخيرية، وجمهور المستفيدين بكافة شرائحهم بما ذلك الموظفين الحكوميين.

– مشروع الحكومة الالكترونية يتكون من مجموعة من الخدمات الالكترونية المتكاملة والمترابطة مع بعضها البعض، والتي توجه لخدمة المستفيدين على اختلاف فئاتهم وأنواعهم[6].

3.1. مراحل التحول إلى الإدارة الإلكترونية (الحكومة الالكترونية): تجدر الإشارة إلى أن التطبيق الفوري للحكومة الالكترونية يتطلب موارد مالية كبيرة، وكذلك وجود موارد بشرية ذات تأهيل وتدريب عالي المستوى، وهما آمران لا يتوافران لمعظم البلدان وتحديدا بلدان المنطقة العربية، كما أن التدرج في أسلوب تنفيذ هذا المشروع الرائد هو وسيلة تضمن استمرارية الحكومة الالكترونية على ارض الواقع وتأديتها

لوظائفها على أكمل وجه، كذلك يضمن أسلوب التدرج تقبل المواطنين لهذه الفكرة وتوعيتهم بمضمونها شيئا فشيئا[7]، وهناك خمس مراحل لتطور الحكومة الالكترونية تتمثل فيما يلي:

أولا: مرحلة الوجود: وفيها يكون للدولة موقع واحد أو بضعة مواقع حكومية على الويب يتم عن طريقها نشر المعلومات[8] والبيانات للمستخدمين من المواقع المختلفة للوزارات والوحدات الحكومية دون الحاجة إلى الذهاب الفعلي إليها[9]، وهي مرحلة مبكرة متطورة من مراحل تطور الحكومة الالكترونية تكون فيها المواقع الحكومية عبارة عن وسائل إعلامية[10].

ثانيا: مرحلة تحسن الوجود: وفيها يزداد عدد المواقع الحكومية ويتم توفير بعض الخدمات مثل نماذج طلب الخدمات التي يمكن تنزيلها وطباعتها وروابط بمواقع ذات علاقة[11].

ثالثا: مرحلة التفاعل: وهي أكثر تفاعلا بين الحكومة والمستفيدين[12] حيث يستطيع المواطن أو رجل الأعمال الاتصال المباشر عن طريق البريد الالكتروني مثلا بالمسؤول وتبادل الآراء والملاحظات حول القضايا المختلفة[13].

رابعا: مرحلة تنفيذ العمليات الكترونيا: وهي مرحلة النضج بحيث يستطيع المستفيدون تنفيذ جميع متطلبات الحصول على الخدمة مباشرة من موقع الويب[14]، وهذه المرحلة من أكثر المراحل تعقيدا، حيث إتمام المعاملات المختلفة مع الوحدات الحكومية مباشرة من خلال المواقع الالكترونية للحكومة ووحداتها، بما في ذلك السداد الالكتروني للرسوم والمدفوعات المتنوعة[15].

خامسا: مرحلة التحول النهائي: وهي المرحلة الأخيرة وفيها يتم الاندماج الكامل بن جميع الخدمات التي تقدمها الحكومة على الويب بحيث يتم توفير الخدمات الحكومية من خلال موقع واحد "بوابة" تصنف فيه الخدمات حسب الإدارات والجهات[16]، حيث يصبح استخدام تقنية المعلومات والاتصالات في المعاملات كلها ممارسة يومية عادية ومتوفرة في المناطق كلها[17]، وانطلاقا من استعراض مختلف مرحل تطور الحكومة الالكترونية يمكن القول بان الجمهورية الجزائرية لازالت في المراحل الأولى من تطبيق الحكومة الالكترونية.

4.1. ايجابيات تطبيق الإدارة الإلكترونية (الحكومة الالكترونية): تحقق الحكومة الالكترونية مجموعة من الفوائد للجات التي تتبنى تطبيقها في إطار خدماتها، ومن الفوائد لها اثر حقيقي على الأفراد والمؤسسات ما يلي:

- حفظ وتوفير المعلومات.
- ضبط الإنفاق في مجال تقنية المعلومات على المستوى المؤسسي.
- عدم تكرار آليات العمل والمعاملات.
- تقديم الخدمات بشكل أفضل لمستخدميها من الجمهور وقطاع الأعمال.
- توفير قنوات تواصل بين الأجهزة الحكومية المختلفة.
- زيادة امن المعلومات.
- توفير وسيلة اتصال تساهم في الحفاظ على المعلومات التي تخص الأمن[18].
- توفر المعلومات الغزيرة للمؤسسات بدلا من ندرة المعلومات في المؤسسات التقليدية، ولعل هذا ما أصبح يتجاوز قواعد البيانات إلى مستودع البيانات (يضمن عددا من قواعد البيانات المختلفة في المنظمة).

– توفر إمكانية عظيمة للاتصالات الشبكة وتبادل المعلومات الإلكترونية هنا وفي كل مكان، بما يجعل المؤسسة في كل مستوياتها التنظيمية لا تتجاوز فقط نقص وضعف الاتصالات وبطئها التي تعاني منها جميع المؤسسات التقليدية، وإنما أيضا تحقق الإفراط في الاتصالات داخل المؤسسة وخارجها.

– تعطي المنافسة بعدا عالميا غير مسبوق جراء أنها تمثل مزيجا فريدا وفعالا من تكنولوجيات كثيرة كتكنولوجيا الحاسبات والاتصالات والشبكات وغيرها.

– توفير مجال غير منظور يتمثل في فضاء الأعمال الذي يوجد على نحو مناظر وموازي لكل قطاعات الأعمال المادية ، فالمكان السوقي يقابله الفضاء السوقي وسلسلة توريد القيمة المادية تقابله سلسلة توريد القيمة الافتراضية، وإدارة الأشياء المادية تقابلها الإدارة الإلكترونية بالنقرات على الإنترنت[19] .

5.1. سلبيات الإدارة الإلكترونية (الحكومة الالكترونية): إن الأخذ بالعمل بنظام الحكومة الالكترونية من خلال الإجراءات والتطبيقات الحياتية لا يعني انه الحل الشافي والكافي لجميع مشكلات الحياة، بل له مجموعة من السلبيات تتمثل في:

مشكلة البطالة: وذلك بسبب إحلال الأجهزة مكان العمال والموظفين.

مشكلة التفكك الاجتماعي: حيث أن المستفيد يمكن أن يأخذ خدمته في المنزل أو العمل فلا يحتك في المجتمع حيث أن آماكن الاستفادة بالمؤسسات الحكومية هي سبب من أسباب التواصل والتعارف الاجتماعي.

فقدان الأمان: فالتعامل الالكتروني سيؤدي إلى فقدان الأمان على الكثير من التعاملات مثل الصرف وغيرها، وهذا يتطلب جهودا قوية للمحافظة على سرية وامن معلومات الآخرين، وبالرغم من وجود سلبيات للحكومة الالكترونية إلا أن هذه السلبيات لا تؤثر على التطبيق فالحاجة إلى الحكومة الالكترونية ماسة والعالم كله في هذا الاتجاه ويمكن أن تتحول هذه السلبيات إلى ايجابيات[20].

6.1. معوقات تطبيق الإدارة الإلكترونية (الحكومة الالكترونية): يمكن تحديد أهم معوقات تطبيق الحكومة الالكترونية على النحو الآتي:

– عدم وجود هياكل تنظيمية محددة وواضحة للمنظمة.

– ضعف قناعة المسؤولين بالإدارة العليا بأهمية استخدام أسلوب الحكومة الالكترونية.

– نقص التأهيل العاملين ومقاومتهم للتغيير وخوفهم من فقدان وظائفهم.

– عدم التدرج في تطبيق الحكومة الالكترونية ونقص الإمكانيات المادية اللازمة لتطبيقها.

– ضعف برامج التوعية الإعلامية المواكبة لتطبيق الحكومة الالكترونية.

– عدم وجود التشريعات القانونية لاعتماد التوقيع والدفع المالي والتعامل مع البريد الالكتروني والتحقق من شخصية طالب الخدمة.

7.1. وظائف الإدارة الإلكترونية (الحكومة الالكترونية): إن الوظائف المناطة بالحكومة الالكترونية لا تختلف عن وظائف الحكومة العادية التي يمارسها المواطن، فقدت سمحت تقنيات المعلومات الالكترونية بإسقاط كل الوظائف التي كانت تقوم بها الحكومة العادية إلى وظائف الحكومة الالكترونية ويمكن أن نجمل الوظائف الرئيسية للحكومة الالكترونية في:

1.7.1. تزويد المعومات: كتوفير الخرائط والمناسبات والأخبار والخدمات ومعلومات الترفيه والتجارة والتسويق الالكتروني والسياحة والفندقة والحجوزات وخدمات البريد والاتصالات.

2.7.1. الخدمات المباشرة: كتعبئة الطلبات والمعاملات الحكومية الوقتية وتبادلات البريد الالكتروني وتحميل نماذج الطلبات والملفات وبرامج تشغيل من المواقع التي تديرها الحكومة واستطلاعات الرأي والتعليم الافتراضي.

3.7.1. المعلومات الفورية: كالتنبؤات الجوية ومعلومات الازدحام المروري، ومعلومات الإسعاف والإنقاذ والنجدة.

4.7.1. تبادل المعلومات الاجتماعية: كغرف الدردشة بأنواعها، جماعات المواضيع المحددة، مجموعات الحوار، جماعات الرأي السياسي، جماعات حماية الجوار، البيع بالمزاد العلني الالكتروني.

5.7.1. العلاقات بالعالم الخارجي: تبادل الوظائف السابقة مع المدن الأخرى في نفس الدولة ومع بقية دول العالم.

8.1. متطلبات الإدارة الإلكترونية (الحكومة الالكترونية): تتكون منظومة الحكومة الالكترونية من تلاحم القوى بين خمسة عناصر أساسية وهي:

1.8.1. متطلبات تجهيزية: أجهزة خاصة لربط الحومة الالكترونية بشبكة إتصالات داخلية و شبكة الانترنت العالمية، أجهزة تقنية خاصة بتحويل مجموعات الحكومة التقليدية إلى الكترونية، أجهزة الحواسيب و لواحقها المختلفة، طابعات ليزرية متطورة، ماسحات ضوئية، و أجهزة تصوير، نظم وبرامج المعلومات، أوعية ووسائل حفظ وتخزين واسترجاع البيانات والمعلومات، شبكات ووسائل الاتصال[21].

2.8.1. متطلبات برامجية: برمجيات Software و بروتوكولات لربط نظم استرجاع المعلومات على الخط[22].

3.8.1. متطلبات بشرية: كوادر بشرية فنية مؤهلة و قادرة على التعامل مع التقنيات الحديثة بوجهيها المادي و الفكري، و هنا يعتبر هذا العامل أهم عنصر باعتبار الكادر البشري هو الأساس لنجاح أي عملية[23]، وذلك من خلال تدريب الموظفين وتوعيتهم بمفهوم وأهمية الحكومة الالكترونية وترويجها لدى المتعاملين معها[24].

4.8.1. متطلبات مالية: الدعم المالي القوي الذي يساعد على تنفيذ مشروع الحكومة الالكترونية و تشغيله وصيانة الأجهزة والبرامج.

5.8.1. متطلبات قانونية وتشريعية: وهي المتطلبات الأكثر أهمية وخطورة وتنبع أهمية المتطلبات القانونية من كونها تشكل الإطار التنظيمي الوقائي الرادع الذي يحيط بكل متعلقات الحكومة الالكترونية، الأمر الذي يجعل التفكير بالتلاعب بمحتوى هذه الحكومة من قبل العابثين أمرا في غاية الصعوبة، وكذلك يضمن امن المعلومات وسريتها وخصوصيتها خاصة للأفراد الذين يمتلكون الخوف من أن تصبح بياناتهم الخاصة ووثائقهم عرضة لاختراقها، وبالتالي تفقد حرمتها وخصوصيتها، أما خطورة المتطلبات القانونية التشريعية فهي تكمن في أن غيابها سيجعل الباب مفتوحا على مصرعيه أمام المتطفلين والقراصنة ومجرمي المعلوماتية بكل أطيافهم للتطاول على محتوى الحكومة الالكترونية بكل ما تشمله، وقد يصل الأمر إلى حد التلاعب في الأرقام والبيانات خاصة في النواحي الاقتصادية المالية كما هو الحال في حالات الدفع الالكتروني عبر بوابة الحكومة الالكترونية دون وجود إمكانية لمعاقبتهم لعدم وجود نصوص قانونية تسمح بذلك[25].

9.1. الإدارة الإلكترونية (الحكومة الالكترونية) والجريمة الالكترونية: تشكل إستراتيجية الحكومة الالكترونية نهجا شموليا نحو الارتقاء بمختلف جوانب التطبيق والمعرفة في المجال الالكتروني والتواكب مع مختلف معطيات الثورة المعلوماتية، مما يمكن الدولة بمختلف مكوناتها التنظيمية والشعبية من التعامل بكفاءة اكبر مع سلبيات الثورة المعلوماتية والتي من أهمها الجريمة الالكترونية، كون الحكومة الالكترونية تقوم على قاعدة عريضة من الاستخدام واسع النطاق للتقنيات الالكترونية، والذي لا يمكن له أن يتم بمعزل عن وجود الحد المقبول من المعرفة الالكترونية وتقنياتها والإجراءات التي تضمن الأمن والخصوصية المعلوماتية، والتي تفضي جميعها إلى تدعيم قدرة الدولة على التصدي للجريمة الالكترونية على مختلف المستويات ويتضح ذلك من خلال ركني مشروع الحكومة الالكترونية المتمثلان في:

الركن الأول: إيجاد المقومات الرئيسية التي تمثل ركائز مشروع الحكومة الالكترونية كوجود الرؤية الإستراتيجية، وتكوين البنية التحتية المعلوماتية، تحقيق التحول التنظيمي، تهيئة الأنظمة والتشريعات، تحقيق الأمن والموثوقية المعلوماتية، نشر المعرفة المعلوماتية.

الركن الثاني: عملية التحول المرحلي والمتدرج لتطبيقات الحكومة الالكترونية على المستوى الكلي للدولة، بما يضمن سلامة التطبيق والقدرة على استيعاب معطياتها من قبل كل الأطراف المستفيدة منها، مما يعزز تحقيق الأهداف والغايات من وراء تطبيقاتها[26].

2. الجريمة الالكترونية: (المجرم الالكتروني):

1.2. مفهوم الجريمة الالكترونية: استقت كلمة الجريمة في اللغة من الجرم وهو التعدي أو الذنب[27]، والجمع أجرام وجرائم وجروم[28]، والجريمة اصطلاحا هي إتيان فعل محرم معاقب عليه فعله أو ترك فعل محرم الترك معاقب على تركه، والجريمة من الناحية القانونية هي مخالفة القوانين التي ينص عليها النظام، وكما ادخل الحاسوب والانترنت خدمات وتسهيلات ومعارف بل ومصطلحات جديدة فقد أعطيا عالم الجريمة أبعادا جديدة، فصار من الممكن ارتكاب جريمة اختلاس أو سرقة أو تزوير عن بعد، وظهر مصطلح cyber crime الذي يعني الجرائم التي ترتكب باستخدام الحاسوب وشبكة الانترنت[29]، الجريمة الالكترونية أو الجريمة المعلوماتية أو جرائم الانترنت والحاسب الآلي، جرائم السايبر cyber crimes[30] كلها مصطلحات تدل على الجريمة الناشئة عن استغلال تقنية المعلومات واستخدامها وهي جريمة حديثة نسبيا، وذلك لارتباطها بتكنولوجيا متطورة هي تكنولوجيا المعلومات[31]، وتعرف فنيا بأنها ذلك النوع من الجرائم التي تتطلب الماما خاصا بتقنيات الحاسب الآلي ونظم المعلومات، لارتكابها أو التحقيق فيها ومقاضاة فاعليها، وهي أيضا كل عمل غير قانوني يستخدم فيه الحاسب كأداة أو موضوع للجريمة[32]، وقد عرفها مؤتمر الأمم المتحدة في سنة 2000 بأنها الجريمة التي يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب، أو في بيئة الكترونية، وتعرف كذلك بأنها النشاط الإجرامي الذي تستخدم فيه التقنية الالكترونية الرقمية، بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ العمل الإجرامي المستهدف[33]، وتعرف أيضا على أنها الجريمة التي تلعب فيها البيانات الكومبيوترية والبرامج المعلوماتية دورا رئيسيا[34]، ومن هنا فالجريمة الالكترونية نشاط الكتروني يؤدي إلى إلحاق الضرر بالغير ماديا أو معنويا عن طريق استخدام الحاسب من الجاني ضد حاسب المجني عليه، وبناء على ما سبق يمكن أن يكون الحاسب الآلي إما موضع الجريمة كتدمير البيانات، أو التخريب لأجزاء الحاسب وبرامجه، وقد يكون الحاسب أداة لارتكاب الجريمة عن طريق استخدامه للاحتيال والتجسس وسرقة الأموال عن طريق إجراء تحويلات من حساب لحساب آخر أو سرقة أرقام بطاقات الائتمان واستخدامها في الشراء عبر شبكة الانترنت[35]، كما قد يكون الحاسب الآلي هو ضحية للجريمة الالكترونية سواء على الكيان المادي أي كافة الأجهزة المستخدمة في الحاسوب (hardware)أو الكيان المعنوي أي البرامج (software)[36] كتعطيل خادم موقع مؤسسة أو إرسال الفيروسات[37]، وهذه الجرائم لا تعترف بالحدود بين الدول ولا حتى بين القارات حيث تعد من الجرائم الحديثة التي تستخدم فيها شبكة الانترنت باعتبارها أداة لارتكاب الجريمة أو تسهيل ارتكابها[38].

2.2. المجرم المعلوماتي أو المجرم الالكتروني: أضافت المعلوماتية الكثير من الجوانب الايجابية إلى حياتنا إلا أنها في المقابل جلبت معها نسلا جديدا من المجرمين اصطلح على تسميتهم بمجرمي المعلوماتية آو المجرمين الالكترونيين[39]، ويعرف المجرم المعلوماتي (الالكتروني) بأنه المجرم الذي لديه قدرة على تحويل نواياه إلى لغة رقمية باستخدام التقنية الرقمية المعلوماتية، وذلك بأداء فعل أو الامتناع عنه، مما يحدث اضطرابات في المجتمع المحلي أو الدولي نتيجة مخالفته قواعد الضبط الاجتماعي محليا أو دوليا[40].

3.2. صفات المجرم المعلوماتي (الالكتروني): ليس هناك اتفاق على صفات مرتكبي الجرائم الالكترونية ومنفذيها، ولا يوجد قالب يتضمن الفئات والسمات التي يتسم بها مرتكب الجريمة المعلوماتية، إلا أن هناك صفات ذات دلالة مشتركة يجمع المختصون بأنها توجد في كل الأشخاص الذين تم التحقيق والقبض عليهم في جرائم من هذا النوع، حيث أوردت العديد من الدراسات العربية والغربية في هذا المجال بان متوسط سن مرتكبي هذه الجرائم هم من تقع أعمارهم بين 14 سنة و 38 سنة وهذا يدل بان اغلب مرتكبي الجرائم الالكترونية من فئة الشاب، ويتميز المجرم المعلوماتي بعدد من السمات والخصائص هي:

– المجرم المعلوماتي يتمتع بالمهارة والمعرفة والذكاء. حيث يمكنه التغلب على الكثير من العقبات التي تواجهه أثناء ارتكاب الجريمة[41].

– المجرم المعلوماتي يتمتع بالسلطة اتجاه النظام المعلوماتي، حيث أن المزايا التي يتمتع بها المجرم المعلوماتي تمكنه من ارتكاب جريمته، وقد تتمثل هذه السلطة مثلا في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات والتي تعطي المجرم إمكانية فتح الملفات وقراءتها وكتابتها ومحو المعلومات[42].

– شخص ذو مهارات فنية عالية متخصص في الإجرام المعلوماتي (الالكتروني)، قادر على استخدام خبراته في الاختراقات وتغيير المعلومات.

– قادر على تقليد البرامج وتحويل الأموال، محترف في التعامل مع شبكات الحاسبات، وهو شخص غير عنيف لان تلك الجريمة لا تلجا إلى العنف لارتكابها[43].

4.2. فئات مجرمي المعلوماتية: توصلت الدراسات والأبحاث التي تناولت مجرمي المعلوماتية إلى تصنيف المجرمين الالكترونيين إلى أنماط، لكن لابد من الإشارة إلى أن هاته التصنيفات لا تعني أن كل مجرم معلوماتي يندرج تحت فئة محددة دون غيرها من الفئات المذكورة بل يمكن أن يكون المجرم الواحد مزيجا من أكثر من طائفة أو فئة.

الفئة الأولى: صغار مجرمي المعلوماتية: ويسميهم البعض صغار نوابغ المعلوماتية ويقصد بهم الشباب البالغ المفتون بالمعلوماتية وأنظمتها، ويجب عدم التقليل من خطورة هؤلاء الأشخاص فهذه الفئة قد تتعدى مرحلة الهواية والعبث لتدخل مرحلة متقدمة أكثر في ارتكاب الجرائم المعلوماتية وهي مرحلة الاحتراف لهذه الجرائم، كما انه هناك مخاوف تتمثل في احتضان منظمات الجريمة المنظمة لهذه الفئة للاستفادة من مهاراتهم وتطويرها، حيث أن هاته الفئة أكثر تقبلا لأي أفكار تعرض أو تفرض عليها خاصة إذا كانت تحمل المغامرة والإثارة والتحدي في طياتها.

الفئة الثانية: القراصنة: قراصنة عادة مبرمجون من أصحاب الخبرة يهدفون إلى الدخول إلى الأنظمة المعلوماتية غير المسموح لهم بالدخول إليها وكسر الحواجز الأمنية المحيطة بهذه الأنظمة، وهم نوعين: القراصنة الهواة العابثون أو الهاكرز (Hackers)[44] وهم المتطفلون والمتسللون يتحدون إجراءات امن الشبكات لكن لا تتوفر لديهم في الغالب دوافع التحدي واثبات الذات، وهاته الفئة اغلبها من التلاميذ وطلبة الثانويات والشباب البطال[45]، أما القراصنة المحترفون الكراكرز (Crackers) الكراكرز أو المقتحم هو الشخص الذي يقوم بالتسلل إلى نظام الحاسوب للاطلاع على المعلومات المخزنة فيها أو لإلحاق الضرر أو العبث بها أو سرقتها[46].

الفئة الثالثة: الموظفون العاملون في مجال الأنظمة المعلوماتية: وهذه الفئة من المجرمين يشكل النظام المعلوماتي مجال عملهم الأساسي ولهذا فهم يقترفون جرائم تمكنهم من تحقيق أهدافهم الشخصية، وهناك فئات من الموظفين الحاقدين على مؤسساتهم يسميهم البعض فئة مجرمي المعلوماتية الحاقدين، هؤلاء يعودون إلى مقر عملهم بعد انتهاء الدوام ويعمدون إلى تخريب الجهاز أو إتلافه أو سرقته، وقد يجد الموظف نفسه أحيانا مرتكبا لجريمة الكترونية صدفة ودون تخطيط مسبق لها[47].

الفئة الرابعة: مجرمو المعلوماتية أصحاب الآراء المتطرفة: وتتكون هذه الفئة من الجماعات الإرهابية أو المتطرفة التي تتكون من مجموعة من الأشخاص لديهم معتقدات أو أفكار اجتماعية أو سياسية أو دينية ويرغبون في فرض هذه المعتقدات باللجوء إلى النشاط الإجرامي.

الفئة الخامسة: مجرمو المعلوماتية في إطار الجريمة المنظمة: والجريمة المنظمة هي تعبير عن مجتمع إجرامي يعمل خارج الشعب والحكومة ويضم في طياته الآلاف المجرمين الذين يعملون وفقا لنظام بالغ الدقة والتعقيد يفوق النظم التي تتبعها أكثر المؤسسات تطورا وتقدما، كما يخضع أفرادها إلى لأحكام قانونية سنوها لأنفسهم وتفرض أحكاما بالغة القسوة على من يخرج عن ناموس الجماعة ويلتزمون

في أداء نشاطاتهم الإجرامية بخطط دقيقة ومدروسة يلتزمون بها ويجنون من ورائها الأموال الطائلة[48]، ومثل هاته الجرائم عصابات سرقة السيارات حيث يحددون بواسطة شبكة الانترنت الأماكن التي ترتفع بها أسعار بيع قطع غيار السيارات ومن ثم يبيعون القطع المسروقة في تلك الأماكن ليضمنوا اكبر ربح ممكن[49].

5.2. الأسباب الدافعة إلى ارتكاب الجريمة الالكترونية: لا تختلف الأسباب الدافعة إلى ارتكاب الجريمة الالكترونية عن باقي أنواع الجرائم الأخرى، ومن أبرزها:

الدوافع الذاتية: والتي تجعل من الشخص يقوم بارتكاب عدد من المخالفات نابعة من حب الاستطلاع والتحدي والخوض في المجهول[50]، والمتعة والرغبة في قهر النظام المعلوماتي واثبات الذات[51].

الدوافع النفسية: وتكون من شخص لديه خلل نفسي أو أمراض نفسية تنعكس على السلوك[52] مثل الرغبة في الانتقام والإيذاء وهنا الخطورة[53].

الدوافع الاجتماعية: وتتمثل في الاختراقات للأجهزة الشخصية والتعرف على نقاط الضعف لدى الآخرين وتتبع عوراتهم.

الدوافع المالية (الربح وكسب المال): وذلك بالرغبة في تحقيق مكاسب مادية تكون هائلة أحيانا بزمن قياسي قد يكون من أكثر البواعث التي تؤدي إلى إقدام مجرمي المعلوماتية على اقتراف جرائمهم من اجل تحقيق المكاسب المالية[54]، والغرض الأساسي من الإشارة إلى مختلف الصفات والسمات التي يتصف بها المجرم المعلوماتي هو وضع البرامج العلاجية المبنية على الخصائص النفسية والاجتماعية والمالية في كل مجتمع بما يتماشى مع طبيعة المجتمع وخصائصه ففي المجتمع الجزائري مثلا تختلف دوافع الجرائم الالكترونية والمعلوماتية عن المجتمع الأوروبي.

6.2. أنواع الجرائم المعلوماتية أو الالكترونية: تصنف الجريمة المعلوماتية (الالكتروني) إلى عدة أصناف فهناك من يصنفها تبعا لمرتكبها، وهناك الجرائم المعلوماتية التي صنفت تبعا لطريقة تنفيذها، وأخرى تبعا لغرض أو هدف الاعتداء[55]، وتم تصنيفها وفق أسس متعددة بغرض تسهيل التعامل معها، ويمكن الإشارة إلى تصنفين رئيسيين:

– التصنيف الشكلي: ويتضح من خلاله الشكل العام للجريمة والتغير الذي طرأ عليها بفعل التقنية المعلوماتية وينقسم إلى نوعين وهما:

– الجرائم الالكترونية التقليدية: وهي الجرائم المعروفة من السابق كالسرقة مثلا، ولكنها أصبحت ترتكب بتسخير قدرات التقنيات المعلوماتية كوسيلة لتنفيذها مما أعطاها مسميات أخرى كالسرقة الالكترونية تتفق وطبيعتها الجديدة.

– الجرائم الالكترونية الجديدة: وهي عبارة عن أشكال إجرامية مستحدثة لم تكن معروفة من السابق، وتعتمد بشكل رئيسي في تنفيذها على التقنيات المعلوماتية أو الالكترونية كونها لم تعرف إلا بعد ظهور التقنيات الرقمية، كنشر الفيروسات الرقمية أو عمليات الاختراق لقواعد البيانات مثلا.

– التصنيف العملي: ويعتمد على الدور الذي تلعبه تقنية المعلومات في الجريمة المنفذة ويندرج تحته ثلاثة أنواع وهي:

– الجرائم التي تستهدف النظام المعلوماتي: وهي الجرائم الالكترونية التي تستهدف احد مكونات النظام المعلوماتي أو الالكتروني كجرائم الاختراق وجرائم إتلاف المعلومات[56].

– الجرائم المنفذة باستخدام النظام المعلوماتي: وهي الجرائم التي يتم ارتكابها بواسطة التقنيات الرقمية، كجرائم التعدي على البيانات وانتهاك الخصوصية.

– الجرائم المنفذة في بيئة النظام المعلوماتي: وتتمثل في الجرائم التي تتم في البيئة الالكترونية دون الإضرار بالبيئة ذاتها، بل يكون الضرر على الأطراف المستخدمة أو المستفيدة من تلك البيئة كجرائم التشهير والجرائم الإباحية والأخلاقية[57].

7.2. خصائص الجريمة المعلوماتية (الالكترونية): تتسم الجرائم بالعديد من السمات والصفات المختلفة التي تؤدي إلى الكشف عن مرتكبيها، إلا أن الجرائم المرتكبة عبر شبكة الانترنت تتصف بخصائص وسمات قد لا توجد في الجرائم العادية[58]، حيث يتضح من خلال التصنيفات السابقة لجرائم المعلوماتية أنها أضحت ذات طابع متجدد ومتغير بشكل مذهل مما يعطيها طبيعة خاصة تميزها عن غيرها من الجرائم التقليدية الأخرى[59]، وتكمن خطورتها في ضعف إيجاد الصلة بين المجرم وبين وسيلة ارتكابه للجريمة، وصعوبة التعرف على شخصيته وبعده أحيانا مسرح الجريمة[60]، ويمكن تلخيص خصائص جرائم المعلوماتية (الحاسب الآلي، المعلوماتية) فيما يلي:

– الجريمة المعلوماتية متعدية الحدود أو جريمة عابرة للقارات[61].

– عدم وضوح الجريمة[62]، أي استتار الجريمة: حيث أن الجرائم الواقعة على الحاسب الآلي أو بواسطته باستخدام شبكة الانترنت تتصف في أكثرها بالاستتار والتخفي، بحيث لا يلاحظها المجني عليه غالبا، أو لا يدري بوقوعها أصلا[63].

– صعوبة إثباتها:[64] حيث تتميز جرائم الانترنت عن سائر الجرائم التقليدية بصعوبة إثباتها ويرجع ذلك إلى عدة أسباب أهمها[65]:

– عدم ترك اثر لها بعد ارتكابها.

– صعوبة الاحتفاظ الفني بها إن وجدت.

– احتياجها إلى خبرة فنية، مما يصعب على المحقق التقليدي التعامل معها.

– اعتمادها على الخديعة في ارتكابها والتضليل في التعرف على مرتكبها.

– اعتمادها على قمة الذكاء في ارتكابها[66].

– سرعة التنفيذ: لا يتطلب تنفيذ الجريمة الالكترونية الوقت، فاستخدام لوحة المفاتيح وأوامر الحاسب الآلي يمكن أن تنقل ملايين الدولارات من مكان إلى آخر، وهو ما يجعلها تتصف بالخاصية الموالية.

– ضخامة الخسائر المادية والمعنوية: المحصلة الاقتصادية لجرائم الحاسب الآلي تكون خسائر عالية في اغلب الأحوال سواء كانت تتصف بسرقة برنامج، أو تدمير قاعدة بيانات، أو سرقة مبالغ نقدية.[67]

– سرعة تطور أساليبها نتيجة التطور المتسارع في تقنية المعلومات ذاتها.

– دقة وسرعة تنفيذها كنتيجة حتمية للتقنيات الرقمية المستخدمة في تنفيذها بصفة سريعة في إصابة الهدف، وتبدأ وتنتهي بسرعة بالغة[68]، حيث لا يحتاج الجاني فيها لأكثر من ضغطة زر لمسح كل آثار الجريمة الأمر الذي قد يفقد هذه الحجة أهميتها[69].

– نقص الخبرة لدى الجهات المعنية بمكافحة الجريمة الالكترونية، وعدم كفاية القوانين الموجودة المتعلقة بمعاقبة مجرمي المعلوماتية والانترنت والحاسب الآلي[70].

– إعاقة الوصول إلي الدليل لإحاطته بوسائل الحماية الفنية كاستخدام كلمات السر حول مواقعهم تمنع الوصول إليها أو ترميزها أو تشفيرها لإعاقة المحاولات الرامية إلي الوصول إليها والإطلاع عليها أو استنساخها[71].

3. الجرائم الالكترونية التي تهدد أمن اللغة العربية في الإدارة الإلكترونية (الحكومة الالكترونية) بالمجتمع الجزائري:

1.3. جرائم المعلوماتية (الالكترونية) المرتكبة ضد اللغة العربية بالمجتمع الجزائري:

– جريمة استنساخ برامج الحاسب الآلي والمتاجرة فيها: وتكون هذه الجريمة إما بنسخ البرامج من مواقع الشركات من أشخاص يعملون فيها ثم يقوم بوضعها في أقراص ممغنطة أو اسطوانات وبيعها، أو من برنامج متداول في السوق فيقوم الشخص بكسر حماية الملكية ومن ثم إنشاء نسخة منه ثم يبدأ بنسخ هذه النسخة نسخا متعددة وبيعها، وكذلك يمكن أن يقوم شخص بأخذ برامج من الانترنت دون إذن من الشركة المنتجة، ويقوم بجمعها ثم نسخها على أقراص وبيعها في السوق بطرق غير مشروعة[72]، وتظهر هاته الجريمة في المجتمع الجزائري من خلال بيع بعض البرمجيات في السوق والتي لا يسمح ببيعها إلا بإذن منتجها الأصلي كبرنامج التشغيل ويندوز اكس بي مثلا windows xp والذي يباع في السوق الجزائرية بما يقارب 50 دج لكن النسخة الأصلية له تبلغ 5 ملايين، وهو ما يسبب أحيانا مشاكل للحواسب المربوطة بشبكة الانترنت حيث تعمل شكة ميكروسوفت إلى إبلاغ المستخدم بان النسخة المثبتة على جهاز الحاسوب ليست أصلية وتطلبه منه تغييرها، وهو نفس المشكل المواجه عند تحميل برمجيات مضادة للفيروسات كبرمجية kaspersky مثلا بمختلف صيحاتها حيث تمنع المؤسسة المنتجة لهاته البرمجية تحديثها بواسطة شبكة الانترنت إذا كانت النسخة غير أصلية ومقرصنة من الانترنت إضافة إلى منع تفعيل البرمجية لان ذلك يتم بواسطة الدفع مع ضمان فعالية وتحديث البرمجية حسب شروط الاشتراك.

– هناك جريمة الكترونية أخرى خسرت شركة mobilis موبيليس وشركة اتصالات الجزائر من ورائها أموالا باهضة حيث أتاحت شركة اتصالات الجزائر إمكانية تعبئة الرصيد بواسطة البطاقة المغناطيسية أو بطاقة الائتمان[73] مع إمكانية مضاعفة الرصيد إلى 50% من الرصيد وكانت عملية التعبئة متاحة بـ 1500.00 دج. فقط وهو ما أتاح لبعض الشباب إمكانية تعبئة هواتفهم النقالة بما يتجاوز 20000.00 دج. والى حد الآن لا توجد آثار تسمح بمتابعة هؤلاء المجرمين لان الخطأ كان تقنيا من المؤسستين وكانت المرحلة للتجريب فقط وهو ما كلفهما خسارة مالية كبيرة.

– قضية سرقة أسئلة الامتحانات للأساتذة من أجهزة الحواسب المتواجدة بالمؤسسات التعليمية حيث يقوم بعض الأساتذة غير المتمكنين من تكنولوجيا المعلومات والاتصال بحذف الأسئلة بعد كتابتها بواسطة الحاسوب لكن دون إفراغ سلة المحذوفات مثلا وهو ما يمكن الطلبة من استرجاعها بسهولة ببرمجيات متخصصة وبدن استخدام هاته البرمجيات خاصة إذا كانت المؤسسة التعليمية لا تفصل بين قاعة التطبيقات للطلبة وأجهزة الحواسيب المخصصة للأساتذة.

– المحادثة الأجنبية مع الأفراد أحيانا جيدة لكن قد يستطيع المجرم المعلوماتي سرقة كل المعلومات المتواجدة في جهاز الحاسوب خاصة إذا كان الحاسوب مربوط بشكة الانترنت بحيث لا يستطيع المستفيد التحكم في فارة الجهاز وهو ما حدث للكثير من الباحثين الذين فقدوا رسائل دكتوراه وماجستير بهاته الطريقة.

– قرصنة الأناشيد والأغاني والأفلام والحصص الوثائقية والدروس وإعادة نشرها عن طريق الاستنساخ على الأقراص المضغوطة بأسماء لمؤسسات وطنية ليست المنتج الأصلي ولا تملك إذن بالإنتاج، والاستوديوهات في هذا المجال كثيرة.

– تقنية البلوثوث المستخدمة في نقل المعلومات بسرعة فائقة بين أجهزة الحواسيب حيث أحيانا تدخل إلى جهاز الحاسوب معلومات لا نرغب فيها كالصور الجنسية والمخلة بالحياء.

– ابتزاز الفتيات بواسطة التصوير الرقمي والتغيير في الصور بواسطة برمجيات متخصصة وتهديد الفتيات والأطفال بنشرها إذا امتنعن عن الموفقة على ممارسة الفعل المخل بالحياء[74]، بالاستغلال الغير مشروع للأسرار الشخصية[75].

– الحصول على كلمة السر للدخول لبعض المكتبات الرقمية المتخصصة مثلا في الطب وتحميل المجلات والكتب بدون إذن من المؤسسات المنتجة ولا دفع حقوق التسجيل.

– البرمجيات المتخصصة في فتح البريد الالكتروني والاطلاع على الأمور الشخصية للأفراد والتجسس عليهم، وتزيد الخطورة أحيانا إلى تغيير كلمة المرور إلى البريد الالكتروني ويصبح ملك المجرم المعلوماتي، وهاته يمكن أن نسميها مخاطر الهوية[76].

– الدخول غير المصرح به لشبكة الانترنت المتاحة بواسطة الويفي داخل المؤسسات خاصة المؤسسات التي تهمل مجال وحدود الشبكة، مما يسمح لبعض المجرمين الالكترونيين بالدخول إلى شبكة الانترنت مجانا والأمثلة في هذا كثير ومنها الجامعات.

– التزوير والانتحال في الشهادات بواسطة البرمجيات المتخصصة في ذلك كبرمجية filtrshop و paint مثلا ويكون هذا التزوير مثلا في قوائم امتحانا الطلبة أو في رسائل الاستقبال المتعلقة بتربصات الأساتذة في الخارج وغيرها.

– التجسس واسترجاع المعلومات المتواجدة في الحاسوب عن طريق الدخول إلى قائمة ابدأ وتشغيل فيتحصل المجرم على كل الملفات التي كان صاحب الحاسوب يعالجها وهو ما يمكنه من تدميرها أو سرقتها.

– المواقع الجنسية والممارسات غير الأخلاقية وذلك من خلال المواقع المتاحة على شبكة الانترنت، والتي ترسل صورا وروابط لمواقع مخلة بالحياء عبر البريد الالكتروني، ورغم أننا نسمع من حين لآخر مبادرة وزارة تكنولوجيات المعلومات والاتصال الجزائرية في حجب هاته المواقع التي تشكل خطر كبيرا خاصة على الأطفال والمراهقين والشباب إلا أن التطبيق على ارض الواقع مازال متأخرا.

– المواقع الإرهابية وتعتبر الجزائر من البلدان التي عانت الويلات بما سببه الإرهاب في تدمير مؤسسات البلاد وتعمل شبكة الإرهاب بواسطة الانترنت على استغلال الأطفال في تضليلهم بالفكر التطرفي وإمكانية صنع السلاح بواسطة تقنيات بسيطة متاحة على شبكة الانترنت.

– هناك مجموعة من البرمجيات المتخصصة في التنصت والتجسس على أجهزة الحاسوب حيث تتيح إمكانية تثبيتها على جهاز الحاسوب تسجيل كل الخطوات التي كان المستخدم يقوم بها أثناء عمله على الحاسوب.

– مواقع المؤسسات الحكومية غير مؤمنة إلى درجة كبيرة تضمن عدم إمكانية قرصنتها.

– جريمة غسل الأموال بواسطة الحاسب الآلي[77] حيث من حين لآخر تعثر عناصر الدرك الوطني على شبكات لتزوير الأموال ومن بين أهم الأجهزة المستخدمة في ذلك الحاسب الآلي ولواحقه.

– هناك بعض البرمجيات الوثائقية المنتجة على وطنيا كبرمجية سنجاب مثلا التي تقوم بإنتاجها مركز البحث في الإعلام العلمي والتقني وهي برمجية متخصصة في إدارة نظم المعلومات وخاصة المكتبات، ويتطلب الحصول عليها 60 مليون جزائرية فتلجا بعض المؤسسات إلى تنصيبها على حواسيبها والعمل بها مجانا دون إذن من المنتج الأصلي.

– وهو نفس الشيء الذي نلمسه في قرصنة الكتب الورقية وتحويلها إلى نسخ رقمية وبيعها مجانا دون إذن من مؤلفها أو ناشرها الأصلي، وهذا لا يعني كل الجرائم الالكترونية الموجودة في المجتمع الجزائري بل هناك جرائم الكترونية لم تكتشف بعد، وهذا نظرا لعلاقة هذا النوع من الجرائم بتكنولوجيا المعلومات والاتصالات التي تطور بسرعة كبيرة جدا.

2.3. التشريع الجزائري في مجال الجريمة الالكترونية (المعلوماتية) التي تهدد اللغة العربية: سارعت الجزائر إلى إصدار قانون يتعلق بالجريمة المعلوماتية (الالكترونية) في 05 أوت 2009 تحضيرا للحكومة الالكترونية سنة 2013[78]، والذي تضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال ومكافحتها ويعتبر هذا الإجراء استراتيجيا فكرة جيدة حيث انه قبل التفكير في التحول إلى الحكومة الالكترونية لا بد من وضع القوانين التي تنظم ذلك، وهو ما يضمن السير الحسن للحكومة الالكترونية.

1.2.3. هدف قانون الجريمة الالكترونية الجزائري: يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال ومكافحتها[79].

2.2.3. مفهوم الجريمة الالكترونية في القانون الجزائري: جاء في مصطلحات قانون الجريمة الالكترونية التعريف الموالي للجريمة المعلوماتية: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية[80].

3.2.3. تطبيق قانون الجريمة الالكترونية الجزائري: نصت المادة 03 من هذا القانون مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية قانونية لمراقبة الاتصالات الالكترونية (المراقبة الالكترونية هي التي تتم بواسطة التقنية الالكترونية وعبر شبكة الانترنت[81]) وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية[82].

4.2.3. الحالات التي تسمح باللجوء إلى المراقبة الالكترونية: حددت المادة 04، إجراءات المراقبة الالكترونية والحالات التي يتم اللجوء إليها، وذلك في الحالات الآتية:

– للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

– في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

– لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

– في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[83].

5.2.3. القواعد الإجرائية لقانون الجريمة الالكترونية الجزائري: حيث أفادت المادة الخامسة من القانون بإمكانية تفتيش المنظومات المعلوماتية يجوز للسلطات القضائية المختصة وكذا ضبّاط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 الدخول بغرض التفتيش ولوعن بعد، حيث يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك، إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل، يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها[84].

– ومن بين القواعد الإجرائية التي جاءت في قانون الجريمة الالكترونية الجزائري حجز المعطيات المعلوماتية[85]، الحجز عن طريق منع الوصول إلى المعطيات[86]، المعطيات المحجوزة ذات المحتوى المجرم[87]، حدود استعمال المعطيات المتحصل عيها[88]، وبالإضافة إلى هذا حدد الفصل الرابع من قانون الجريمة الالكترونية الجزائري التزامات مقدمي الخدمة كمساعدة السلطات[89]، وحفظ المعطيات المتعلقة بحركة السير[90]، الالتزامات الخاصة بمقدمي خدمة الانترنت[91].

6.2.3. الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات المعلومات والاتصال ومكافحتها: حيث أفادت المادة 13 بإنشاء هاته الهيئة[92] وتكلف بالمهام الآتية:

– تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات المعلومات والاتصال ومكافحته.

– مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات المعلومات والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

– تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات المعلومات والاتصال وتحديد مكان تواجدهم[93].

7.2.3. تعليق على قانون الجريمة الالكترونية الجزائري: عمد القانون الجزائري إلى سن التشريعات مجال الجريمة الالكترونية وهذه النقطة مهمة جدا قبل الشروع في تطبيق الحكومة الالكترونية.

– حدد أيضا المسرع الجزائري بعض النقاط الأساسية المهمة كالتحري والتحقيق في الجريمة الالكترونية وذلك من خلال التفتيش والمراقبة الالكترونية والاتصالات الالكترونية.

– ولكن رغم هذا لم يعطي المشرع الجزائري أهمية للجرائم الالكترونية التي ترتكب في حق الخواص وركز على الجريمة اتجاه المؤسسات الحكومية والتابعة لقطاع الدولة.

– لم يحدد هذا القانون أنواع الجريمة الالكترونية بمسمياتها، كما لم يتم تحديد مختلف أنواع العقوبات التي تطبق على مرتكبي الجرائم الالكترونية في هذا القانون.

– مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات المعلومات والاتصال ومكافحتها قليلة جدا حيث اقتصرت على ثلاثة ومهام وكما أشرنا سابقا أن الجريمة الالكترونية جد متطورة وهو ما يتطلب الكثير من المهام من اجل التحقيق فيها واكتشافها وهذا بالمقارنة مع قانون الجريمة الالكترونية السعودي والسوداني والإماراتي والفرنسي والأمريكي والبريطاني، التي تحدد الحبس والغرامات المالية لمجرمي المعلوماتية.

3.3. سبل التحقيق في الجرائم المعلوماتية (الجريمة الالكترونية) ومكافحتها:

2.3.3. إجراءات التحقيق في الجريمة الالكترونية: للتحقيق في الجرائم الالكترونية وجب العلم أولا بمجال الحاسب الآلي والانترنت وكيفي استخدامها بكفاءة في التحقيق والتحري واستخلاص الأدلة، ثم معرفة ما يمكم استخدامه كدليل في المحكمة، وأخيرا معرفة الخطوات اللازمة لتجريم المشتبه به من الناحية القانونية[94].

بالإضافة إلى هذا لا بد من توفر مجموعة مختصة في ذلك تتكون من قائد الفريق ويكون له خبرة طويلة في مجال التحقيق وذو معرفة جيدة بالطبيعة الخاصة لجرائم الحاسوب والانترنت، إضافة إلى محقق جنائي وهو شخص لديه خبرة بأساليب التحقيق وإجراءاته، وكيفية التعامل مع الأدلة الجنائية الرقمية ويتولى عملية التفتيش عن الأدلة، خبير في الحاسوب والشبكات، وآخر في تدقيق الحسابات، وخبير في التصوير، والبصمات ثم خبير الرسم التخطيطي[95]، وتساهم الإجراءات السليمة للتحري في مساعدة فريق التحقيق على ما يلي:

– التأكد من وقوع الجريمة.
– تحديد نمط وطبيعة الجريمة المرتكبة.
– التعرف على التقنيات المستخدمة في ارتكابها.
– المساعدة في تحديد الجاني والجناة المحتملين أو المشتبه بهم.
– معرفة الأسباب والدوافع المحتملة لارتكاب الجريمة.
– الاستدلال على الشهود في حالة وجودهم.
– توضيح طبيعة الأدلة الجنائية ومصادرها[96]، وتحتاج فرقة التحقيق في الجرائم المعلوماتية إلى مجموعة من البرمجيات الخاصة بالتحقيق الجنائي في الجرائم المعلوماتية منها: برمجيات النسخ الاحتياطي الجنائي، برمجيات استعادة الملفات المحذوفة، برمجيات كسر كلمات سر بعض المستندات، برمجيات تتبع الاتصال الشبكي، برمجيات استعراض الصور، برمجيات عرض محتوى المفلت المختلفة[97].

3.3.3. سبل مكافحة نماذج من الجرائم المعلوماتية:

أ. بريد الكتروني يحتوي على ذم وتهديد وتحقير: يتم فتح البريد الالكتروني للمشتكي، ثم تحديد رقم المرسل adresse ip، والبحث على مالك هذا الرقم من خلال قواعد المعطيات، بعدها يتم تحديد مزود خدمة الانترنت، وتتم مخاطبتهم بالطرق الرسمية، وبعدها يتم تحديد اسم الشخص ورقم هاتفه المستخدم لهاته الأرقام، ثم يستدعى المشتكي أو التحرك إلى موقعه، فيواجه المشتكي عليه بالأمر واخذ إفادته، وفي الأخير تودع الأطراف إلى الجهات المختصة.

ب. سرقة بريد الكتروني: يتم الاشتراك بأحد المواقع الالكترونية التي تقوم بتتبع البريد الالكتروني للمستقبل، ثم ترسل رسالة الكترونية إلى البريد الالكتروني المسروق من خلال موقع التتبع الالكتروني، وعندما يتم استقبال الرسالة الالكترونية من قبل السارق، يتم إرسال بريد الكتروني للمرسل ليعلمه بمكان ورقم adresse ip للبريد الالكتروني المسروق، ثم البحث عنه، وإيداع الأطراف للجهات المختصة، وهو نفس الشيء في حال اختراق البريد، ولمكافحة الجريمة الالكترونية مهما كان نوعها تتبع مختلف العمليات السابقة في التحقيق التي لا تنتهي إلا باكتشاف المجرمين ومعاقبتهم بما ينص عليه القانون.

الخاتمة: وفي الأخير لابد من التنويه إلى ضرورة التعاون الدولي في مكافحة الجرائم المعلوماتية، وهذا نظرا لخصوصية هاته الجريمة حيث يمكن مهاجمة أجهزة حواسيب في الجزائر مثلا من دولة أخرى، وهذا التعاون يكون في تبادل الخبرات من خلال المؤتمرات والدورات التدريبية المتخصصة في مجال الجريمة الالكترونية، ومواكبة التقنيات الرقمية ومسايرة الركب المعلوماتي والزوال التكنولوجي سواء للبرمجيات أو الأجهزة، وتعتبر التجربة الجزائرية إستراتيجية إلى حد كبير مقارنة بالتجارب العربية، لكن لا بد من الإشارة إلى تكملة نقائص قانون الجريمة الالكترونية، والتحول المرحلي والمتدرج في تطبيق الحكومة الالكترونية الجزائرية من اجل مواجهة مختلف جرائم المعلوماتية المتواجدة في المجتمع الجزائري والتي قد يرتكبها مجرمون إلكترونيون من خارج الجزائر وهو ما يضمن امن وسرية ونجاح الحكومة الالكترونية الجزائرية.

مراجع البحث:

1. بدر بن محمد المالك، الأبعاد الإدارية والأمنية لتطبيقات الإدارة الالكترونية في المصارف السعودية، الرياض: أكاديمية نايف العربية للعلوم الأمنية، 2008، ص.14.
2. نهلا عبد القادر المومني، الجرائم المعلوماتية، عمان: دار الثقافة للنشر والتوزيع، 2008، ص.61.
3. يحي بن محمد أبو مغايض، الأبعاد الإستراتيجية في مواجهة الجريمة الالكترونية، مؤتمر الجرائم المعلوماتية، من 22 إلى 25 شوال 1430 الموافق 12- 14 أكتوبر 2009، الرياض: أكاديمية نايف العربية للعلوم الأمنية، ص. 09.

4. عبد الكريم قاسم السبيق، مدى استفادة الأجهزة الأمنية من خدمات شبكة الانترنت، الرياض: أكاديمية نايف العربية للعلوم الأمنية، 2003، ص.19.
5. صلاح مصطفى قاسم، التحديات الأمنية للحكومة الالكترونية: دراسة مسحية لتجربة دبي في دولة الإمارات العربية المتحدة، الرياض: أكاديمية نايف العربية للعلوم الأمنية، 2003، ص.35.
6. يحي بن محمد أبو مغايض، المرجع السابق، ص. 10.
7. نهلا عبد القادر المومني، المرجع السابق، ص.63.
8. عبد الكريم قاسم السبيق، المرجع السابق، ص.21.
9. نهلا عبد القادر المومني، المرجع نفسه، ص. 63.
10. عبد الكريم المرجع نفسه.
11. عبد الكريم قاسم السبيق، ص.21.
12. عبد الكريم قاسم السبيق، المرجع نفسه.
13. نهلا عبد القادر المومني، ص.24.
14. عبد الكريم قاسم السبيق، المرجع نفسه.
15. نهلا عبد القادر المومني، المرجع نفسه، ص. 64.
16. عبد الكريم قاسم السبيق، المرجع السابق.
17. نهلا عبد القادر المومني، المرجع السابق.
18. صلاح مصطفى قاسم، المرجع السابق، ص.38.
19. موسى بن عبد الله محمد مهدي حمدي، الصعوبات التي تواجه استخدام الإدارة الالكترونية في إدارة المدارس الثانوية: للبنين بمدينة مكة المكرمة، من وجهة نظر مديري المدارس ووكلائها، مكة المكرمة: جامعة أم القرى، 2008.
20. صلاح مصطفى قاسم، المرجع السابق، ص.39.
21. صلاح مصطفى قاسم، المرجع السابق، ص.44.
22. مولاي امحمد، " صعوبات مشاريع رقمنة المخطوطات بالجزائر: مخبر مخطوطات الحضارة الإسلامية في شمال إفريقيا بجامعة وهران نموذجا"، المؤتمر العشرين للاتحاد العربي للمكتبات والمعلومات " نحو جيل جديد من نظم المعلومات والمتخصصين: رؤية مستقبلية " الدار البيضاء من 09 إلى 11 ديسمبر 2009.
23. مولاي امحمد، فوزية ختير، " المتطلبات التقنية لرقمنة الأرصدة الأرشيفية: مشاريع رقمنة الأرشيف بالجزائر نموذجا " المؤتمر العشرين للاتحاد العربي للمكتبات والمعلومات" نحو جيل جديد من نظم المعلومات والمتخصصين: رؤية مستقبلية " الدار البيضاء من 09 إلى 11 ديسمبر 2009.
24. نهلا عبد القادر المومني، المرجع السابق، ص. 65.
25. نهلا عبد القادر المومني، ص.66.
26. يحي بن محمد أبو مغايض، المرجع السابق، ص.22.
27. محمد بن عبد الله بن علي المنشاوي، جرائم الانترنت في المجتمع السعودي، الرياض: أكاديمية نايف العربية للعلوم الأمنية، 2003، ص.53.
28. محسن بن سليمان الخليفة، جرائم الحاسب الآلي وعقوباتها في الفقه والنظام، الرياض: أكاديمية نايف العربية للعلوم الأمنية، 2004، ص. 40.
29. خالد الغثبر، محمد بن عبد الله القحطاني، الجرائم المتعلقة بالمعلومات، منشورات مركز التميز لأمن المعلومات، ص.02.
30. محمد الأمين البشري، الانترنت والإرهاب: تأهيل المحققين في جرائم الحاسب الآلي وشبكات الانترنت، القاهرة: جامعة عين شمس، 2008، ص.07.
31. نهلا عبد القادر المومني، ص.45.
32. محمد بن عبد الله بن علي المنشاوي، المرجع السابق، ص.53.
33. يحي بن محمد أبو مغايض، المرجع السابق، ص. 03.
34. محسن بن سليمان الخليفة، المرجع السابق، ص. 51.
35. محسن بن سليمان الخليفة، المرجع السابق، ص. 51.
36. سرور بن محمد العبد الوهاب، مختصر إجراءات الاستدلال والتحقيق في الجرائم المعلوماتية، مؤتمر الجرائم المعلوماتية، من 22 إلى 25 شوال 1430 الموافق 12- 14 أكتوبر 2009، الرياض: أكاديمية نايف العربية للعلوم الأمنية، ص.07.

37. ناصر بن زيد المشاري، الجرائم المعلوماتية وإجراءات التحقيق: المفاهيم، التحديات، التوجهات، مؤتمر الجرائم المعلوماتية، من 22 إلى 25 شوال 1430 الموافق 12- 14 أكتوبر 2009، الرياض: أكاديمية نايف العربية للعلوم الأمنية، ص.07.

38. محمد بن عبد الله بن علي المنشاوي، المرجع السابق، ص.54.

39. نهلا عبد القادر المومني، المرجع السابق، ص.76.

40. يحي بن محمد أبو مغايض، المرجع السابق، ص. 04.

41. منصور بن مصلح الجهني، أنواع الجرائم المعلوماتية وصفات مرتكبيها، مؤتمر الجرائم المعلوماتية، من 22 إلى 25 شوال 1430 الموافق 12- 14 أكتوبر 2009، الرياض: أكاديمية نايف العربية للعلوم الأمنية، ص. 04.

42. نهلا عبد القادر المومني، المرجع السابق، ص.80.

43. يحي بن محمد أبو مغايض، المرجع السابق، ص. 04.

44. نهلا عبد القادر المومني، المرجع السابق، ص.84.

45. منصور بن مصلح الجهني، المرجع السابق، ص. 05.

46. منصور بن مصلح الجهني، المرجع السابق، ص.

47. محمد بن عبد الله بن علي المنشاوي، المرجع السابق، ص.38.

48. نهلا عبد القادر المومني، ص.87.

49. محمد بن عبد الله بن علي المنشاوي، المرجع السابق، ص.38.

50. منصور بن مصلح الجهني، المرجع السابق، ص. 05.

51. نهلا عبد القادر المومني، المرجع السابق، ص.92.

52. منصور بن مصلح الجهني، المرجع السابق، ص. 05.

53. نهلا عبد القادر المومني، ص.92.

54. نهلا عبد القادر المومني، ص.90.

55. منصور بن مصلح الجهني، المرجع السابق، ص. 06.

56. أسامة بن غانم العبيدي، جريمة إتلاف المعلومات، مجلة دراسات المعلومات، ع.04، يناير 2009، ص.ص. 93-123.

57. يحي بن محمد أبو مغايض، المرجع السابق، ص.06.

58. محمد عبد الرحيم سلطان العلماء، جرائم الانترنت والاحتساب عليها، المجلة العربية للدراسات الأمنية والتدريب، س.18، ع.36، مج.18، رجب 1424 هـ. ص.ص. 05-58.

59. يحي بن محمد أبو مغايض، المرجع السابق، ص.06.

60. محسن بن سليمان الخليفة، المرجع السابق، ص.44.

61. نهلا عبد القادر المومني، المرجع السابق، ، ص.58.

62. محسن بن سليمان الخليفة، المرجع السابق، ص.44.

63. محمد عبد الرحيم سلطان العلماء، المرجع السابق.

64. محسن بن سليمان الخليفة، المرجع السابق، ص.45.

65. محمد عبد الرحيم سلطان العلماء، المرجع السابق.

66. جرائم الانترنت في المجتمع السعودي، ص. 38.

67. محسن بن سليمان الخليفة، المرجع السابق، ص.45.

68. يحي بن محمد أبو مغايض، المرجع السابق، ص.06.

69. عبد الرحمان مطهر أبو طالب، الصعوبات والعوائق أمام اكتشاف جرائم الحاسوب، منشورات مركز التميز لأمن المعلومات، ص.02.

70. مجلة العلوم الأمنية س.18، ع.36، مج.18، ص.ص.5-58.

71. خالد ممدوح إبراهيم، إجراءات التحقيق في الجرائم المعلوماتية، مؤتمر الجرائم المعلوماتية، من 22 إلى 25 شوال 1430 الموافق 12- 14 أكتوبر 2009، الرياض: أكاديمية نايف العربية للعلوم الأمنية، ص. 04.

72. محمد بن عبد الله بن علي المنشاوي، المرجع السابق، ص.47.

73. محمد أمين احمد الشوابكة، جرائم الحاسوب والانترنت: الجريمة المعلوماتية، عمان: دار الثقافة للنشر والتوزيع، 2004، ص.200.

74. إبراهيم بن سليمان الهويمل، جرائم ابتزاز الفتيات وطرق اكتشافها والتحقيق فيها، مؤتمر الجرائم المعلوماتية، من 22 إلى 25 شوال 1430 الموافق 12- 14 أكتوبر 2009، الرياض: أكاديمية نايف العربية للعلوم الأمنية، ص. 08.

75. أسامة بن غانم العبيدي، حماية الحق في الحياة الخاصة في مواجهة جرائم الحاسب الآلي والانترنت، المجلة العربية للدراسات الأمنية والتدريب، مج. 23، ع. 46، س. 23، ربيع الآخر 1429- ابريل 2008، ص-ص. 51-90.

76. سلطان الديحاني، التحديات الجديدة في مجال الجرائم المعلوماتية، مؤتمر الجرائم المعلوماتية، من 22 إلى 25 شوال 1430 الموافق 12- 14 أكتوبر 2009، الرياض: أكاديمية نايف العربية للعلوم الأمنية، ص.10.

77. عبد الله عبد الكريم عبد الله، توظيف تطبيقات الحاسب الآلي في غسل الأموال، مؤتمر الجرائم المعلوماتية، من 22 إلى 25 شوال 1430 الموافق 12- 14 أكتوبر 2009، الرياض: أكاديمية نايف العربية للعلوم الأمنية ، ص.01.

78. قانون رقم 09-04 مؤرخ في 14 شعبان 1430هـ الموافق لـ 05 أوت 2009، الجريدة الرسمية الجزائرية ع. 47، س. 46، ص.05.

79. المادة 01، قانون رقم 09-04 مؤرخ في 14 شعبان 1430هـ الموافق لـ 05 آوت 2009، الجريدة الرسمية الجزائرية ع. 47، س. 46، ص.05.

80. المادة 02، قانون رقم 09-04 مؤرخ في 14 شعبان 1430هـ الموافق لـ 05 أوت 2009، الجريدة الرسمية الجزائرية ع. 47، س. 46، ص.05.

81. مصطفى محمد موسى، المراقبة الالكترونية عبر شبكة الانترنت: دراسة مقارنة بين المراقبة الأمنية التقليدية والالكترونية ماهيتها- مفاهيمها- نظم معلوماتها- تحليلها- النظرية- التدريب- التطبيق، القاهرة: دار الكتب القانونية، 2005، ص.27.

82. المادة 03، قانون رقم 09-04 مؤرخ في 14 شعبان 1430هـ الموافق لـ 05 أوت 2009، الجريدة الرسمية الجزائرية ع. 47، س. 46، ص.05.

83. المادة 04، قانون رقم 09-04 مؤرخ في 14 شعبان 1430هـ الموافق لـ 05 أوت 2009، الجريدة الرسمية الجزائرية ع. 47، س. 46، ص.05.

84. المادة 05، قانون رقم 09-04 مؤرخ في 14 شعبان 1430هـ الموافق لـ 05 أوت 2009، الجريدة الرسمية الجزائرية ع. 47، س. 46، ص.06.

85. المادة 06، قانون رقم 09-04 مؤرخ في 14 شعبان 1430هـ الموافق لـ 05 أوت 2009، الجريدة الرسمية الجزائرية ع. 47، س. 46، ص.07.

86. المادة 07، قانون رقم 09-04 مؤرخ في 14 شعبان 1430هـ الموافق لـ 05 أوت 2009، الجريدة الرسمية الجزائرية ع. 47، س. 46، ص.07.

87. المادة 08، قانون رقم 09-04 مؤرخ في 14 شعبان 1430هـ الموافق لـ 05 أوت 2009، الجريدة الرسمية الجزائرية ع. 47، س. 46، ص.07.

88. المادة 09، قانون رقم 09-04 مؤرخ في 14 شعبان 1430هـ الموافق لـ 05 أوت 2009، الجريدة الرسمية الجزائرية ع. 47، س. 46، ص.07.

89. المادة 10، قانون رقم 09-04 مؤرخ في 14 شعبان 1430هـ الموافق لـ 05 أوت 2009، الجريدة الرسمية الجزائرية ع. 47، س. 46، ص.07.

90. المادة 11، قانون رقم 09-04 مؤرخ في 14 شعبان 1430هـ الموافق لـ 05 أوت 2009، الجريدة الرسمية الجزائرية ع. 47، س. 46، ص.07.

91. المادة 12، قانون رقم 09-04 مؤرخ في 14 شعبان 1430هـ الموافق لـ 05 أوت 2009، الجريدة الرسمية الجزائرية ع. 47، س. 46، ص.08.

92. المادة 13، قانون رقم 09-04 مؤرخ في 14 شعبان 1430هـ الموافق لـ 05 أوت 2009، الجريدة الرسمية الجزائرية ع. 47، س. 46، ص.08.

93. المادة 14، قانون رقم 09-04 مؤرخ في 14 شعبان 1430هـ الموافق لـ 05 أوت 2009، الجريدة الرسمية الجزائرية ع. 47، س. 46، ص.08.

94. ناصر بن زيد المشاري، المرجع السابق، ص.10.

95. احمد إبراهيم الكفاوين، إجراءات التحقيق في الجرائم المعلوماتية، مؤتمر الجرائم المعلوماتية، من 22 إلى 25 شوال 1430 الموافق 12- 14 أكتوبر 2009، الرياض: أكاديمية نايف العربية للعلوم الأمنية، ص.05.

96. تركي بن عبد الرحمان المويشير، التحقيق في الجرائم المعلوماتي، مؤتمر الجرائم المعلوماتية، من 22 إلى 25 شوال 1430 الموافق 12- 14 أكتوبر 2009، الرياض: أكاديمية نايف العربية للعلوم الأمنية، ص. 30.

97. تركي بن عبد الرحمان المويشير، المرجع السابق، ص. 31.