

الجريمة الإلكترونية وأثرها على مشروعية أعمال الإدارة القانونية Cybercrime and its impact on the legality of the Department's legal work

د. بن عودة صليحة^(*)

أستاذة محاضرة قسم أ
المركز الجامعي مغنية

الملخص:

تعد الإدارة الإلكترونية من ثمار المنجزات التقنية في الحديث، فهي تقوم على استخدام التقنيات ووسائل الاتصال المتقدمة عن طريق الحاسوب وشبكة الإنترنت لتحسين الخدمة في مجال إصدار الجهة الإدارية للقرار والعقد الإلكتروني. ولكن هذا الاستخدام على الرغم من أن له آثار إيجابية من خلال مساهمته في التطور والرقى فإنه بالمقابل يؤدي إلى آثار سلبية ناتجة تمثلت في الجرائم الإلكترونية التي تؤثر على مشروعية تصرفات الإدارة، ومن ثم مصالح الدولة وكيفية رقابة القاضي الإداري وقاضي العقد على مشروعية كل من القرار والعقد الإداريين غير المشروعين. الكلمات المفتاحية: الجريمة الإلكترونية، آثار، مشروعية، القرار الإداري، العقد الإداري.

Abstract :

Electronic management is one of the fruits of modern technical achievements. It is based on the use of advanced technologies and means of communication via computer and the Internet to improve the service in the field of decision-making and e-contract by the governing body. However, this use, while having positive effects through its contribution to development and advancement, results in negative consequences of cybercrime affecting the legality of the administration's actions, and thus the interests of the State, and how the administrative judge and the contract judge control the lawfulness of both the decision and the illegal administrative contract.

key words : Electronic crime, effects, legality, administrative decision, administrative contract.

* المرسل : د. بن عودة صليحة

مقدمة:

إن التطور الحاصل في تكنولوجيا الإعلام والاتصال وانتشار شبكة الإنترنت وكل ما حملته من تقدم قد وصلت لتوفير معلومات يمكن استخدامها في ما يحقق المصلحة العامة. بالإضافة إلى أهمية الكمبيوتر في شتى مجالات الحياة المعاصرة، فلم يوجد فرع من أي نشاط إلا ويستخدم في معاملاته الكمبيوتر سواء مانت مرافق عمومية أو شركات ومؤسسات خاصة. نظرا لما يتضمنه من برامج وأنظمة يعتمد عليها في عمله، فهو العقل المسير للحاسب الآلي والسبيل الوحيد في تنظيم وتخزين المعلومات وعرضها بشكل منظم. ناهيك عن الشبكة العنكبوتية والتي تشتمل على الكثير من المعلومات المهمة التي تساعد في تسهيل الخدمات والعمليات القانونية، حيث أصبح العالم كله في متناول اليد بفضل هذه الشبكة.

وبغزو هاتين الوسيلتين جميع المجالات نظرا لما تتسم به من الدقة والسرعة، كل ذلك أدى إلى بروز طائفة جديدة من الجرائم، ونوع جديد من المجرمين، وهو الانعكاس السلبي لهذه الثورة العلمية فتطورت الجريمة وأصبحت تمس المعلومات وهو ما يسمى بالجريمة الإلكترونية. وهي تختلف عن الجرائم الأخرى من حيث الضرر الناجم عنها، وطرق وأساليب المجرمون بالتجسس على الوسائل الإلكترونية وسلامة ما يقدمه من معلومات يعتمد عليها في المعرفة للمستفيدين منها. لذلك يجب أن تحاط بالسرية التامة للمحافظة على مصالح البلاد و ما يتعلق بأمنها وسلامة اقتصادها، لذلك يجب أن تتوافر لهذه التقنية الأمن المعلوماتي اللازم لحمايتها من أي اختراق خارجي.

فما مدى مشروعية أعمال الإدارة في ظل الجرائم الإلكترونية ؟

هذا ما سيتم الإجابة عنه من خلال التعرف على الجريمة الإلكترونية من حيث أركانها وخصائصها (القسم الأول) ، ومدى تأثير هذه الجريمة على مشروعية كلا من القرار والعقد الإداريين (القسم الثاني).

القسم الأول: الإطار المفاهيمي والقانوني للجريمة الإلكترونية :

تعد الجريمة الإلكترونية من الجرائم التي استحضرتها الممارسة السيئة لثورة التكنولوجيا المعلوماتية التي تختلف عن الجريمة التقليدية في طبيعتها وأنواعها وأدواتها وحتى في خصوصية وتميز مرتكبها، لهذا لابد من تحديد الإطار المفاهيمي للجريمة (أولا)، ثم نعرض على الإطار القانوني للجريمة الإلكترونية (ثانيا).

أولاً: المقصود بالجرائم الإلكترونية وخصائصها وأركانها:

لقد اختلف الفقهاء حول وضع تعريف موحد للجريمة الإلكترونية، ويعود الاختلاف حول تحديد نطاقها. فالبعض ينظر إليها بمفهوم ضيق (1)، والبعض الآخر ينظر إليها بمفهوم موسع (2).

1) الإتجاه المضيق من تعريف الجريمة الإلكترونية:

يعرف أنصار هذا الاتجاه الجريمة المعلوماتية بأنها: " كل فعل غير مشروع يكون بالعلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازم لإرتكابه من جهة، وملاحقته وتحقيقه من جهة أخرى" (1)

حسب هذا التعريف يجب أن تتوفر معرفة كبيرة بتقنيات الحاسوب ليس فقط لإرتكاب الجريمة، بل حتى لملاحقتها والتحقيق فيها (2).

ويعرف الأستاذ Rosenblatt الجريمة الإلكترونية على أنها: " نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو التي تحول عن طريقه" (3).

2) الإتجاه الموسع في تعريف الجريمة الإلكترونية:

يرى فريق آخر من الفقهاء ضرورة التوسيع من مفهوم هذه الجريمة، وبالتالي هي: " كل جريمة تتم بوسيلة إلكترونية كالحاسوب مثلاً، وذلك باستخدام شبكات الإنترنت من خلال غرف الدردشة واختراق البريد الإلكتروني ومختلف وسائل التواصل الإجتماعي بهدف إلحاق الضرر لفرد أو مجموعة من الأفراد، وحتى لدولة من الدول تكون ضمن برنامج الاستهداف الحربي أو الإقتصادي، أو الإضرار بسمعتها أو العكس. ويبقى الهدف واحد وهو الكشف عن قضايا متستر عليها، أو نشر معلومات لفائدة طرف أو أطراف أخرى من باب التسريب" (4).

ثانياً: خصائص الجريمة الإلكترونية:

يعتبر موضوع أو محل الجريمة الإلكترونية أهم خاصية تتميز بها هذه الأخيرة عن الجرائم التقليدية، حيث تكون المعلومات والبرامج هي محل الاعتداء، وهي عبارة عن نبضات إلكترونية وعليه نكون أمام ظاهرة إجرامية مستحدثة ذات طبيعة خاصة كونها إفراز ونتاج لتقنية المعلومات واتساع نطاق تطبيقها في المجتمع.

1) الجريمة المعلوماتية جريمة عابرة للحدود:

يعتبر العالم هو مسرح الجريمة المعلوماتية كونها تقع على شبة الإنترنت العالمية، أي أنها لا تقع بمكان محدد كباقى الجرائم الجنائية. حيث تكون المسافة بين الجاني والمجني عليه آلاف الأميال، وقد تكون أمتارا معدودة، لأنه لا يوجد حائل يقف أمام نقل المعلومات بين الحاسبات الآلية المتواجدة في مختلف دول العالم عبر شبكات الاتصال. حيث نجد أن مستخدم الإنترنت من دولة ومورد أو مقدم خدمة الاشتراك من دولة أخرى وشركة تكنولوجيا معالجة البيانات وإدخالها وتحميلها عبر الشبكة من دولة ثالثة⁽⁵⁾. فيمكن أن تقع الجريمة من الفاعل في دولة على مدني عليه في دولة أخرى في وقت يسير جدا مخلفة أفدح الخسائر خاصة في مجال التجارة الالكترونية وازدياد اعتماد البنوك عليها⁽⁶⁾.

إن الطابع الدولي لهذه الجريمة يثير العديد من الإشكالات والصعوبات لاسيما مشكلة تحديد المحكمة المختصة دوليا بالمنازعات الناشئة، القانون الواجب التطبيق، أدلة الإثبات وقبولها أمام قضاء دولة أخرى، ولهذا فمكافحة هذا النوع من الجرائم يتطلب تعاونا كبيرا بين تشريعاتها⁽⁷⁾.

2) صعوبة تنفيذ العقاب على مرتكبيها:

تتسم الجريمة المعلوماتية بعدم القدرة على منع حدوثها، إذ أن هذا المنع يتطلب وقوع الضرر ووجود متضرر يبلغ الجهات المعنية بالضرر الواقع عليه⁽⁸⁾، وحتى وإن تم التوصل إلى الجاني فيكون من الصعب توقيع العقاب عليه لوجود عدة معوقات يمكن إرجاعها إلى قلة التشريعات التي تواجه هذا النوع من الجرائم. حيث نجد أفعال غير مشروعة التي لا تنطبق عليها أي وصف أو نص من قانون العقوبات خصوصا مع القيود التي ترد على القاضي الجنائي، حيث لا عقوبة ولا جريمة إلا بنص ومبدأ حضر القياس في مجال الجرائم وكذا مبدأ التفسير الضيق للنصوص. إضافة إلى ذلك قلة الخبرة الفنية في التعامل مع الكمبيوتر لدى المشرع والقاضي وبالتالي يظهر ذلك في التأثير على تطبيق العقوبات على هؤلاء الجناة. ويمكن القول بأن الصعوبة ترجع كذلك إلى كل من الجاني والمجني عليه وطبيعة الجريمة في حد ذاتها⁽⁹⁾.

3) الجريمة المعلوماتية جريمة فادحة الأضرار

إن الإقبال المتزايد على الحاسب الآلي والإنترنت في إدارة مختلف الأعمال في شتى المجالات زاد من حدة الأضرار والخسائر التي تخلفها هذه الجرائم، خصوصا بالنسبة

للمؤسسات المالية والبنوك ومختلف الشركات التي تعتمد في خطة عملها على جهاز الحاسوب، وهناك عدة دراسات تشير بأن الأضرار الناجمة عن الجرائم المعلوماتية تفوق الأضرار الناتجة عن الإجرام التقليدي⁽¹⁰⁾.

ثالثاً: أركان الجريمة الإلكترونية:

يرجع السبب الرئيسي في عدم القدرة على تحديدها إلى صعوبة اكتشاف أركانها، فإضافة إلى الشرط المبدئي في كل جريمة ونقصه به الركن الشرعي، لابد من إثبات ركن مادي ملموس يعبر عن إرادة المجرم المعلوماتي.

أولاً/ الركن الشرعي:

هناك العديد من الجرائم الإلكترونية والتي لا ينطبق عليها أي وصف قانوني، فكان لزاماً على أي مشرع أن يأخذ هذا التقدم التكنولوجي بعين الاعتبار، وأن يقوم بتطوير الوسائل اللازمة، أهمها قواعد التجريم لردع هذا الإجرام المعلوماتي. والذي أخذ بالتزايد والانتشار بشكل مذهل دون معوقات قانونية سواء من المشرع أو المجتمع ككل عن طريق توعية الأفراد بالأضرار التي تخلفها هذه السلوكيات. وفي العديد من الدول تبقى الجهود على المستوى الفردي فقط من قبل أصحاب الأجهزة والمؤسسات المالية والاقتصادية والتي تستخدم أجهزة الحاسوب فتضع بعض أنواع الحماية والشفرة الإلكترونية لردع من يخرق برامجهما ويحاول الاعتداء على معلوماتها وأجهزتها. فكيف تكون محاربة هذا النوع من الإجرام إذ أن العديد من القضايا التي عرضت على القضاء الفرنسي تضاربت فيما الأحكام وحدث الخلاف فيما إذا كانت هذه الأفعال يصدق عليها وصف السرقة وفقاً للمادة 379 من قانون العقوبات الفرنسي، بالمفهوم التقليدي أم أن الفعل يحتاج إلى نص خاص.

فقد كانت الاتجاهات متضاربة فيما يتعلق بتصوير المستندات بالمفهوم التقليدي عن طريق وسائل التصوير المخصصة لذلك، أما الآن فإن جهاز الكمبيوتر نفسه باستطاعته أن يقوم بنسخ المعلومات الموجودة في أي جهاز دون أن ي تلفها. فهل يعد هذا من قبيل السرقة والتصوير التقليدي؟ وإذا قام المجرم المعلوماتي بالإطلاع فقط على المعلومات بالنظر، فهل يمكن أن يحاسب على هذا الفعل وتحت أي تكييف؟ وهناك إشكالية أخرى تتعلق بالمصطلحات المستخدمة والغريبة عن لغة القانون الجنائي مثل القرصنة والتي اعتدنا عليها في المجال البحري، فالعديد من الكتاب عبروا عن فعل السرقة عبر الإنترنت

بالقرصنة، وأطلق هذا المصطلح على عملية نسخ البرامج، ولاشك أنه يعكس مدى خطورة وبشاعة الفعل المرتكب⁽¹¹⁾.

ثانيا/ الركن المادي:

يجب أن يكون الفعل أو السلوك المجرم الذي يقوم به الجاني ملامسا لأرض الواقع حتى يمكن التحقق منه وإثباته، ونحن لا نتكلم عن الركن المادي في الجرائم المعلوماتية التي تكون وسيلة ارتكابها معلوماتية، حيث لا يمكن حصرها تحت تكييف واحد، فقد تشكل واقعة قذف أو سب أو تهديد أو تحريض على أفعال غير مشروعة بشكل مطابق للجريمة التقليدية المقررة في قانون العقوبات ويمكن أن ينطبق التفسير الوارد في النصوص التقليدية على هذه الصور.

بينما الذي يثير صعوبة هو الجرائم التي يكون موضوعها المال المعلوماتي المعنوي، مثل إساءة استخدام البريد الإلكتروني عن طريق الرسائل المفخخة وتعطيل الشبكات عن طريق الفيروسات، التي قد تدمر كلياً أو جزئياً المعلومات المخزنة أو النظام المعلوماتي أو التلاعب ببطاقات الائتمان عبر شبكة الإنترنت⁽¹²⁾. فهذه الجريمة تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والإنترنت، مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة، وذلك لسهولة محو الدليل من قبل الفاعل⁽¹³⁾ عن طريق التلاعب ير المرئي في النبضات الإلكترونية التي يتم تسجيل البيانات عن طريقها، كما أن الوصول إلى المجرم في الوقت الذي يبدأ بالاتصال وارتكابه للجريمة ليس بالأمر السهل لأن الاتصال يمر على العديد من الحواسيب ومن خلال التقنية يمكن الحصول على عناوين الحواسيب المتصلة مباشرة بها، ولكن إن تم معرفة المصدر الأصلي فقد يكون العنوان خاطئاً. ومما يزيد في صعوبة إثباتها هو عدم مساعدة المجني عليهم السلطات فيما لو تم اكتشافها⁽¹⁴⁾.

وأكثر من ذلك فإن أغلب القواعد الجنائية غير كافية لوجود صعوبات أخرى تتمثل في البحث عن الدليل وجمعه ومشكلة قبوله إن وجد ومدى مصداقيته وحجته في إثبات وقائع الجريمة. وعليه فيجب الإسراع في إيجاد منظومة قانونية واستحداث نصوص جديدة تتلاءم والمستحدثات التي فرضتها هذه التكنولوجيا⁽¹⁵⁾.

في الأخير نقدم بعض الأسباب التي قام بجمعها محمد محمد شتا⁽¹⁶⁾ والتي تعد مظاهر لصعوبة الجريمة المعلوماتية وهي خمس:

- أنها جريمة لا تترك أثرا ماديا ملموسا.
- أنها جريمة يصعب فنيا الاحتفاظ بأثارها إن وجدت.
- أنها جريمة يصعب على المحقق التقليدي أن يفهم حدودها الإجرامية وما تخلفه من آثار غير مرئية.
- أنها جريمة تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبها
- أنها جريمة بيضاء تعتمد على قمة الذكاء في ارتكابها.

ثالثا/ الركن المعنوي:

لقد أثر استخدام الوسائل التقنية الحديثة في ارتكاب الجريمة على الفكرة أو التصور القديم المتعارف عليه بشأن الانحطاط الثقافي والفكري للمجرم والظروف الاجتماعية القاسية لهذا الشخص المبرز لخطورته الإجرامية على نحو ملفت للانتباه يستدعي الخوف وأخذ الحيطة والحذر منه. فالوضع اليوم مختلف حيث أصبح المجرم المعلوماتي يتمتع بقدر من الفطنة والذكاء ونصيب وافر من التعليم والاختصاص، فبالنسبة للجرائم المعلوماتية لا بد من توافر قدر كبير من المعرفة في مجال تقنية المعلومات والحاسوب حيث أصبحت أصابع الاتهام موجهة للمتعلمين وذوي الاختصاص⁽¹⁷⁾.

ومن المتصور غالبا أن لا تقع الجريمة المعلوماتية إلا بصورة عمدية سبقها التفكير في الحصول على المعلومة أو اختراق الشبكة. والأصل في الجرائم هو العمدية إلا ما استثنى بنص، وهناك من الجرائم ما يتطلب المشرع إرادة ارتكاب السلوك وتحقيق النتيجة، حيث يكفي بتوافر القصد الجنائي العام بصورتيه العلم والإرادة كالدخول إلى أنظمة المعلومات وتدمير المعلومات الموجودة بها أو تدمير ذاكرة الحاسب بعد نسخ ونقل المعلومات التي كانت عليها من أجل طمس الدليل.

لكن قد يتطلب المشرع إضافة إلى القصد الجنائي العام قصدا جنائيا خاصا كضرورة توافرية التملك للأموال المتحصل عليها من سرقة بطاقات الائتمان وتحويلها إلى حسابه الخاص.

إلا أن هذا لا يعني أن هذه الجريمة لا تتحقق بطريقة غير عمدية عن طريق الخطأ أو الصدفة، كتدمير أجهزة المؤسسة نتيجة إفراط الموظف المسؤول الذي استخدم الجهاز العائد لها في عمليات لحسابه الخاص معتمدا على قدرته ومهارته، أو استخدام القرص المرن الخاص به في أجهزة المؤسسة ونقل الفيروسات لها والدخول له ميزة غير مادية فقد

يعلم الشخص أنه دخل بمحض الصدفة أو عن طريق الخطأ إلا أن هذه الجرائم هي جرائم امتناع يصعب تقديم الدليل لإثباتها، فقد يزعم الجاني أنه كان على وشك الانفصال أو يدعي بأنه يتجول في جزء ضيق من النظام. وعمليا لا يمكن التحقق من هذا الإدعاء. كذلك تثير حالة تجاوز مجال التصريح مشكلة الإثبات حيث أن إثبات القصد الجنائي للفاعل الذي يتمتع بتصريح محدد صعب، إضافة إلى أن أنظمة الحاسبات مفتوحة على بعضها⁽¹⁸⁾.

القسم الثاني: مدى تأثير الجريمة الإلكترونية على مشروعية أعمال الإدارة:

يثور التساؤل في هذا القسم عن مدى مشروعية كلا من العقد الإداري الناتج من جرائم غير مشروعة عبر شبكة الإنترنت، أي أن الجريمة الإلكترونية تسبق صدور القرار بإبرام العقد الإداري، وبذلك سوف يتم دراسة كيفية الحكم بعدم المشروعية للعقد أو القرار الإداري وذلك من خلال تجريم المشرع للجرائم الإلكترونية (أولا)، وتقيد سلطة القاضي الإداري بالتكليف الجنائي للجريمة الإلكترونية للحكم بعدم المشروعية (ثانيا).

أولا: تجريم المشرع للجرائم الإلكترونية:

احتراما لمبدأ الشرعية الجنائية الذي يعوز عدم جواز التجريم والعقاب عند انتفاء النص الأمر الذي يمنع مجازاة مرتكب السلوك الضار أو الخطير على المجتمع بواسطة الحاسوب أو الإنترنت طالما المشرع الجنائي لم يقرم بسن التشريعات اللازمة لإدخال هذا السلوك ضمن دائرة التجريم والعقاب بسبب انعدام وجود تصور واضح المعالم للقانون والقضاء اتجاه جرائم الإنترنت كونها من الجرائم الحديثة، ومزالت مكافحة الجرائم المعلوماتية في الدول العربية لا غطاء تشريعي يحددها ويجرم كافة صورها، بالإضافة إلى وجود قصور تشريعي في عدة جوانب منها وسائل الإثبات التقنية وتنظيم الصور الإجرامية في ميدان الحاسب أو الإنترنت. وإذا كان المحقق مهنته البحث عن الحقيقة، وإذا كان القاضي مهمته هي الفصل فيما يعرض عليه من قضايا ومنازعات، فإن عمل كل من المحقق والقاضي يحتاج إلى بيئة قانونية تساعدتهما على أداء وظائفهما، وهذه البيئة مازالت غامضة وإما قاصرة.

1) أسباب الفراغ التشريعي:

- استخدام المجرم المعلوماتي وسائل متطورة بدل الوسائل التقليدية كالحاسوب والإنترنت مما أدى إلى تطور الجريمة الإلكترونية تبعا لتطور الوسائل لدى المجرم ولدى المختصين في القبض عليه، حيث يتم ارتكاب الجريمة بضغطة زر، وصعوبة تحديد الفاعل أو عدم

إمكانية معرفة مكانه، لذلك نجد الاحتيال على شكل رسائل إلكترونية مجهولة المصدر توهم المستقبل بأنها رسالة رسمية من إحدى الجهات الحكومية، وبمجرد تنزيله لدى المستقبل إما أن تمنح للمجرم صلاحيات الدخول إلى الإيميل أو يدخل لجهاز الضحية لسرقة ملفاته المهمة أو تخريبها، وهناك من المجرمين من يستغل التوقيع الإلكتروني فيرسل باسم شخص آخر استغل توقيع الإللكتروني .

- صعوبة تحديد وصف مادي للجريمة الإلكترونية حيث لا يوجد حراس فالمجال مفتوح لكل أنواع الجرائم الإلكترونية التي يصعب حصرها أو تعدادها بسبب عمليات القرصنة الإلكترونية وبذلك فإن الإنترنت ساحة إجرام مثالية تتحدى الأجهزة الأمنية و القضائية بثغرات قانونية.

(2) صور التجريم في التشريع الجزائري:

لقد استحدث المشرع الجزائري في تعديله لقانون العقوبات بمقتضى القانون رقم 04-15، المؤرخ في 10/11/2004⁽¹⁹⁾ بإدراج القسم السابع مكرر وخصصه للإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات حيث جرم بعض الأفعال وحدد لها عقوبات.

أ) جريمة الدخول والبقاء الغير مشروع إلى نظام المعالجة الآلية :

نص المشرع على فعل الدخول في المادة 394 مكرر⁽²⁰⁾، ويقصد بالدخول ذلك النشاط المتمثل في الإتصال بنظام الكمبيوتر بهدف الإطلاع على المعلومات التي يحتويها النظام، وحسب نص المادة فهي لا تشترط أن يقع الدخول على كامل النظام، بل يكفي أن يقع على جزء منه، واشترط كذلك أن يكون الدخول عن غش غير أنه لم يحدد وسائل وطرق الغش.

أما البقاء فهو مكوث الفاعل واستمراره داخل نظام الكمبيوتر بعد دخوله ولو عرضا أو تجاوز الوقت المسموح به للبقاء. كما نصت الفقرة الثانية من نفس المادة على مضاعفة العقوبة إذا ترتب على ذلك حذف لمعطيات المنظومة . أما إذا تم تخريبها فتكون العقوبة من ستة (6) إلى سنتين (2) والغرامة من 50.000 دج إلى 300.000 دج⁽²¹⁾.

(ب) جريمة التلاعب بأنظمة المعالجة الآلية للمعطيات:

وتتمثل هذه الجريمة في الدخول بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها. فقد تختلف أسباب الإختراق باختلاف أهداف المخترق، فمنهم من يخترق لمجرد الفضول، والبعض الآخر لسرقة المعلومات من حواسيب الغير قد يكونوا عرضوها مقابل بدل مالي للإطلاع عليها. أما سبب الإختراق الذي أشار إليه المشرع فيمكن في نية المخترق في تبديل أو تحريف أو إزالة المعلومات في أجهزة الغير، وهذا أخطر أنواع الإختراق⁽²²⁾.

(ج) جريمة الاستعمال غير المشروع لأنظمة المعالجة الآلية للمعطيات:

وتتمثل هذه الصورة في تصميم أو بحث أو توفير أو نشر أو إتجار في معطيات مخزنة أو فعالة أو عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجريمة المذكورة سابقا. وأيضا حيازة أو إفشاء أو نشر أو استعمال لأي غرض كل المعطيات المتحصل من إحدى الجرائم السالفة الذكر⁽²³⁾. وعليه يعد مرتكبا لهذه الجريمة كل من يستخدم البرامج المخزنة آليا بقصد الحصول على منفعة غير مشروعة. بمعنى الاستخدام غير المصرح به. كما نصت المادة 394 مكرر3 على مضاعفة العقوبة في حالة المساس بالمصالح العليا للوطن.

ثانيا : تقييد سلطة القاضي الإداري بالتكليف الجنائي للجريمة الإلكترونية للحكم بعدم المشروعية:

من المبادئ المقررة في القانون الإداري أن للإدارة سلطة تقديرية في اختيار وقت إصدار القرار من عدمه وتقدير خطورة الوقائع ووزن مناسبة إصداره حتى يكون متناسبا مع الظروف والملابسات المحيطة به ولا يحد من سلطتها التقديرية إلا إساءة استعمال السلطة، بمعنى أنه يجب أن تتغير تحقيق المصلحة العامة وحسن أداء الخدمة وإلا شاب تصرفها الانحراف بالسلطة، وبذلك فإن الإدارة تستقل دون تدخل القضاء بتقدير ملائمة إصدار القرار الإداري وتقدير المناسبات التي تدعوها إلى ذلك ما دام التقدير قد استخلص استخلاصا سائغا من الوقائع الثابتة في الأوراق، أي أن رقابة القاضي الإداري

تقف عند حد المشروعية أو عدمها في مجال القرارات الإدارية، فلا يجاوزها إلى تقدير مناسبة إصدار التصرف القانوني مما يدخل في نطاق الملاءمة التقديرية التي تملكها الإدارة دون معقب عليها، وذلك استناداً إلى مبدأ الفصل بين السلطات واستقلال كل منهما عن الأخرى، حيث أن تقدير الملاءمة من الأمور التي تخرج من ولاية القاضي الإداري، فهو قاضي مشروعية وليس قاضي ملاءمة⁽²⁴⁾.

1) تأثير الجريمة الإلكترونية على مشروعية القرار الإداري:

إن رقابة القاضي تقف عند التحقق من الوجود المادي للوقائع والتكييف القانوني لها حتى تحكم بعدم مشروعية القرار الإداري، ولكن إذا كانت هذه الوقائع التي تدعيها الإدارة كسبب لإصدار القرار تمثل في جريمة إلكترونية وبناء على ذلك أصدرت القرار، فإن القرار غير مشروع، لأن ما بني على باطل فهو باطل، ومثال ذلك القرار الإداري الصادر بتعيين أو ترقية شخص انتحل شخصية آخر تتوافر فيه شروط تولي الوظيفة أو ترقيته، وذلك من خلال سرقة المعلومات الواردة بالبريد الإلكتروني للشخص الحقيقي، ففي هذه الحالة فإن صدور القرار بتعيين هذا الشخص المحتال أو ترقيته يعتبر قرار غير مشروع⁽²⁵⁾.

وأيضاً حينما يتم تزوير التوقيع الإلكتروني الخاص بالجهة الإدارية من خلال موظفيها مقابل التبرع واستغلال الوظيفة، ففي هذه الحالة أي قرار صادر من الجهة الإدارية بتوقيع مزور يعتبر صادر من غير مختص وغير مشروع قابل للإلغاء.

2) تأثير الجريمة الإلكترونية على مشروعية العقد الإداري:

إذا كان انعقاد العقد الإداري قائماً على وقائع وهمية وغير حقيقية فإنه يكون غير مشروع، ومثال ذلك تزوير التوقيع الإلكتروني للجهة الإدارية المتعاقدة، أو للشخص المتعاقد معها، حيث أن التوقيع شرط لمشروعية التصرف الإداري، وأي عيب في التوقيع لأحد الطرفين يؤدي إلى إبطال العقد ويمثل عيب في الشكل.

كذلك حينما يظهر المجرم رغبته في شراء سلعة من خلال مزايمة معلنة من جانب الجهة الإدارية فينتحل شخصية شخص آخر حيث يقوم باستغلال البيانات المعلنة لشخص ما عبر شبكة الإنترنت فيبرم العقد الإداري باسم هذا الشخص ولا يدفع مقابل العقد بعد تسلمه السلعة المعروضة من جانب الجهة الإدارية⁽²⁶⁾.

وعليه فإن العقد الإداري المبرم على أساس وقائع تمثل جريمة إلكترونية فإن العقد يكون غير مشروع تطبيقاً لمبدأ ما بني على باطل فهو باطل. وبناء على ذلك عدم مشروعية جميع القرارات الإدارية السابقة واللاحقة للعقد الإداري باستثناء قرار الإعلان عن المناقصة أو المزايدة، أي جميع القرارات الصادرة عن اللجان المنعقدة لرسو العطاء على الشخص المحتال قبل إبرام العقد، وبذلك يوجد أمام القاضي الإداري عند الحكم بعدم مشروعية قرار إداري أو قاضي العقد جريمة إلكترونية تمثل جريمة جنائية معاقب عليها بموجب قانون العقوبات، وتطبيقاً لمبدأ لا جريمة ولا عقوبة إلا بنص فإن القاعدة العامة هو تطبيق قانون العقوبات في حالة عدم وجود قانون يعاقب على الجرائم الإلكترونية حيث أن الخاص يقيد العام، غير لابد من التمييز بين نوعين من المجرمين:

(أ) المجرم الأول قد يكون موظف عام ارتكب خطأ يمثل جريمة إلكترونية وبناء على ذلك أصدر قرار إداري أو أبرم عقد إداري مثال ذلك تزوير التوقيع الإلكتروني للجهة الإدارية أو إفشاء أسرار مناقصة أو مزايدة معينة، مما أدى إلى كشف سريتها ورسو المزايدة على شخص ما مما أخل بمبدأ المساواة والعدالة بين المتنافسين وبناء على ذلك تم إبرام العقد الإداري، وكان الموظف العام هو السبب الرئيسي في الجرائم السابقة، ففي هذه الحالة يتم الحكم بعدم مشروعية العقد الإداري أو القرار الإداري حينما يتم الطعن فيه من جانب الغير المتضرر من إبرام العقد أو إصدار القرار.

(ب) وقد يكون المجرم شخص عادي قام بالاحتيال على الجهة الإدارية إما بتزوير التوقيع الإلكتروني الخاص بالشخص الذي يتعامل مع الجهة الإدارية، وقد ينتحل شخصية شخص آخر تحت اسم مستعار غير حقيقي ليستفيد من إبرام العقد، ففي الحالات السابقة يلتزم القاضي الإداري بالتكييف والوصف الجنائي بهذه الأفعال وفقاً لقانون العقوبات⁽²⁷⁾.

(3) استعراض بعض الفروض في هذا الشأن:

- الفرض الأول: إذا أصدرت النيابة العامة قرار بتجريم الأفعال المرتكبة من جانب المجرم وأحالت المتهم إلى المحاكمة الجنائية فيلتزم كلا من القاضي الإداري وقاضي

العقد بالحكم الصادر من جانب القاضي الجنائي، حيث يتقيد القاضي الإداري بالوصف الجنائي للأفعال حتى يصدر حكمه بعدم مشروعية القرار أو العقد الإداري.

- الفرض الثاني: إذا صدر حكم بالبراءة ينفي الوجود المادي للوقائع فإن القاضي الإداري يتقيد بالحكم.
- إذا كان الحكم مبني على بطلان إجراءات التفتيش أو التلبس ولكن لا ينفي اعتراف الأفعال المجرمة فإن القاضي الإداري لا يتقيد بذلك الحكم لأنه لا ينفي ارتكاب الوقائع المجرمة وإنما يبني على البطلان في الإجراءات.
- الفرض الرابع: إذا صدر حكم بالإدانة على أساس تجريم الأفعال المقترفة من الجاني وإثبات ارتكاب الوقائع المجرمة فإنه وتطبيقاً لمبدأ حجية الحكم النهائي يتقيد القاضي الإداري أو قاضي العقد بهذا الحكم دون مناقشة الواقعة التي سبق بشأنها الحكم الجنائي وفصل فيها بإثبات ارتكابها لأن في ذلك مساس بقوة الشيء المقضي به. وعليه فإن القاضي الإداري لا يرتبط بالحكم الجنائي إلا في الوقائع التي فصل فيها الحكم وكان فصله ضرورياً للفصل في الدعوى المنظورة أمامه، أي يتقيد بما أثبتته القاضي الجنائي في حكمه من وقائع كان الفصل فيها لازماً.

الخاتمة:

من خلال ما سبق فإن الجزائر كغيرها من الدول قد تبنت الإدارة الإلكترونية باستخدام الأدوات التكنولوجية في جميع أجهزة الدولة الحديثة مما يسهل عملية التعامل مع المواطنين خاصة في تقديم الخدمات. ولكن هذا المشروع يتطلب بيئة مناسبة لكي يتمكن من تنفيذ ما هو مطلوب.

النتائج:

- عدم توافر وسائل الكترونية بأسعار معقولة متاحة لجميع أفراد الشعب لكي يتم التعامل بها بدلاً من الوثائق الورقية. بالإضافة إلى انتشار الأمية الإلكترونية.
- عدم توفر الموارد المالية اللازمة لتطبيق الإدارة الإلكترونية، حيث تتكبد الدول نفقات باهضة لتوفير الوسائل الإلكترونية بأسعار معقولة.

- عدم استطاعة الدول النامية مواكبة التطور التكنولوجي لمواجهة الجرائم الإلكترونية، والتي تمثل إعاقة حقيقية للمجتمع الإلكتروني مما يؤثر على مشروعية القرار والعقد الإلكتروني.

وختاما من الضروري:

- توفير الأمن الإلكتروني والسرية الإلكترونية على مستوى عالي لحماية المعلومات الوطنية والشخصية ولصون الأرشيف الإلكتروني من أي عبث مثل الفيروسات والسرقة وأعمال التخريب المعتمدة.

إعداد قانون ينظم المعاملات الحكومية الإلكترونية بما يتلاءم مع مشروع الإدارة الإلكترونية مع إعادة صياغة التشريعات الجنائية وذلك لتوقيع العقوبات الرادعة لجرائم السرقة المعلوماتية والتخريب المعتمدة، لذلك لا بد من تناسق وانسجام القوانين والتشريعات المرتبطة بنظم المعلومات مع نظام الإدارة الإلكترونية.

المواش المعتمدة:

¹ - حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، رسالة ماجستير في العلوم القانونية، تخصص علم الإجرام والعقاب، جامعة باتنة، 2011-2012، ص 13.

² - لقد اعتمد الفقهاء في تعريف الجريمة الإلكترونية على مفهوم ضيق، فمنهم من اعتمد على معيار وسيلة ارتكاب الجريمة المتمثل في الحاسب الآلي، وعليه فيعتبر الجهاز كوسيلة عندما ما ننظر إلى العلاقة بين الجاني والضحية، ويعتبر الجهاز كمسهل للجريمة عندما ننظر إلى العلاقة بين الجاني والجاني من خلال تبادل الاتصالات عبر الخط بين المجرمين. وهناك من يعتمد على معيار توفر المعرفة بتقنية المعلوماتية فيستندون في تعريفهم على الشخص الجالس أمام الحاسب الآلي الذي يكون على دراية ومعرفة بتقنية المعلوماتية. ووفريق آخر يعتمد في تعريفه للجريمة الإلكترونية على موضوع الجريمة والمتمثل في المال المعلوماتي المعنوي، كالقرصنة والاستعمال غير المشروع الأنظمة المعلوماتية وخلق الفيروسات المعلوماتية، فهي أيضا تقع على حق الملكية، أو الحق في سلامة الشرف والاعتبار، أو الحق في حماية حقوق الملكية الفكرية، الحق في الحفاظ على حرمة الحياة الخاصة. بل يمكن الذهاب إلى أكثر من ذلك إمكانية تصور وقوع اعتداء على حرمة السلامة الجسدية عن طريق أجهزة الحاسب الآلي، كإيقاع الخلل في أجهزة الحاسب التابعة لوسائل النقل، كالطيران أو السكك الحديدية أو النقل البحري، إذا كان الهدف منه إلحاق الضرر بالسلامة الجسدية للركاب وإزهاق أرواحهم. ينظر في ذلك، غنية باطلي، الجريمة الإلكترونية (دراسة مقارنة)، الدار الجزائرية للنشر والتوزيع، الجزائر، 2016، ص 15.16.17.

- ³ - مأخوذ عن حمزة بن عقون، نفس المرجع، ص 14.
- ⁴ - سميرة بيسطام، الجريمة الإلكترونية وتقنية الإجرام المستحدث، ص4، Culture/net. Alukah.www//http/br 30/11/2016
- ⁵ - محمد الصديقي، الضبط في الجريمة الإلكترونية، العدد 23، وكالة الأهرام للتوزيع، 2004، ص09.
- ⁶ - M.QUEMENER et J.FERRY, cybercriminalité, defé mondial, 2éme édition, Economica, Paris, 2009,p 67.
- ⁷ - محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الاسكندرية، 2007، ص 78
- ⁸ - محمد الصديقي، نفس المرجع السابق، ص9
- ⁹ - غنية باطلي، المرجع السابق، ص51.
- ¹⁰ - محمد خليفة، المرجع السابق، ص38.
- ¹¹ - غنية باطلي، المرجع السابق، ص44-45
- ¹² - غنية باطلي، مرجع سابق، ص45
- ¹³ - نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008، ص56.
- ¹⁴ - محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، الإسكندرية، 2001، ص46
- ¹⁵ - Mohamed BOZABAR, La criminalité informatique sur l'internet, Journal Of Law Academic, N:01, volume 26, Faculté de droit, université du Koweit, 2002, p73
- ¹⁶ - محمد محمد شتا، نفس المرجع، ص103.
- ¹⁷ - فايز الظفيري، الأحكام العامة للجريمة الإلكترونية، مجلة العلوم القانونية والاقتصادية، العدد الثاني، كلية الحقوق، جامعة عين شمس، 2002، ص520.
- ¹⁸ - JEAN FRANCOIS CASILE, le code pénal à l'épreuve de la délinquance informatique, presse universitaires D'AIX, marseille, PUAM, 2002, p97.
- ¹⁹ - يعدل ويتمم الأمر رقم 156-66، المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، ج.ر عدد 71.
- ²⁰ - من القانون رقم 23-06، مؤرخ في 20 ديسمبر 2006، يعدل ويتمم الأمر رقم 156-66، المتضمن قانون العقوبات، ج.ر عدد 84.
- ²¹ - المادة 394 مكرر 2، من القانون 23-06، سالف الذكر.

- ²² - حوالف حليلة، مهاجي فاطمة الزهراء، معالم الجريمة المعلوماتية في القانون الجزائري، مجلة البحوث القانونية والسياسية، المجلد 3، عدد 16، تصدر عن جامعة مولاي الطاهر، سعيدة، 2021، ص 147.
- ²³ - المادة 394 مكرر 2 من القانون 23-06، المرجع السابق.
- ²⁴ - أمل لطفي حسن جاب الله، أثر الوسائل الإلكترونية على مشروعية تصرفات الإدارة القانونية - دراسة مقارنة-، دار الفكر الجامعي، الاسكندرية، مصر، 2013، 158-159.
- ²⁵ - أمل لطفي حسن جاب الله، المرجع السابق، ص 159.
- ²⁶ - في مثال آخر إذا أبرم المجرم الإلكتروني عقد إداري مع الجهة الإدارية بمناسبة مناقصة معلنة من جانبها لشراء سلعة ما فيعرض المجرم سلعة وهمية من خلال شبكة الإنترنت، ولا يسلم الجهة الإدارية شيء أو يسلم سلعة غير متوافر فيها جميع الشروط المحددة في المناقصة، ولكن يوهم المجرم الجهة الإدارية بتوافر جميع المواصفات المطلوبة في السلطة مما يؤدي إلى وجود إرادة معيبة مشوبة بالتدليس تبطل العقد الإداري وتجعله غير مشروع. ينظر في ذلك، أمل لطفي حسن جاب الله، نفس المرجع، ص 160.
- ²⁷ - أمل لطفي حسن جاب الله، المرجع السابق، ص 161.