تحديات الحكومة الإلكترونية في الجزائر _الجريمة الإلكترونية نموذجا_

challenges of e-government in Algeria -cyber-crime model-

نافع زينب[1]، شعباني مجيد[2] .Nafaa Zinab / Madjid Chabani

[1] مخبر بحث السياسات التنموية والدراسات الاستشرافية ،جامعة آكلي محند أولحاج البويرة، z.nafaa@univ-bouira.dz

[2] مخبر بحث مستقبل الاقتصاد الجزائري خارج المحروقات ،جامعة امحمد بوقرة بومرداس، m.chabani@univ-boumerdes.dz

تاريخ الاستلام: 2020/02/16 تاريخ القبول: 2020/07/10 تاريخ النشر: 2020/07/28

ملخص:

تهدف هذه الدراسة إلى عرض واقع الجرائم الإلكترونية في الجزائر، والجهود المبذولة لمكافحتها، باعتبارها أحد تحديات الحكومة الإلكترونية حيث تم توضيح كيفية تأثير هذا النوع من الجرائم على مسار الحكومة الإلكترونية، وقد تم الاعتماد على إحصائيات وطنية وأخرى عالمية، وقد توصلت الدراسة إلى أن الجرائم الإلكترونية من بين أنواع الجرائم الأكثر انتشارا في الجزائر، فبالرغم من الجهود المبذولة في مجال مكافحة هذا النوع من الجرائم من طرف الهيئات الجزائرية المختصة، إلا أنها لا تزال غير كافية.

كلمات مفتاحية: الحكومة الإلكترونية، الجريمة الإلكترونية، الجزائر، إحصائيات، تحديات.

تصنيف JEL : H83 ,K14,O38

Abstract:

This study aims at presenting the reality of cybercrime in Algeria and the efforts exerted to combat it as one of the challenges of e-government, as it clarified how this kind of crime affects the e-government path, and it was based on national and international statistics. The study found that cybercrime was among the most common types of crime in Algeria. Despite efforts to combat such crimes by the competent Algerian authorities, it was still insufficient.

Keywords: : e-government ;cyber-crime; Algeria; statistics; challenges.

Jel Classification Codes: H83 ,K14,O38

Résumé:

Cette étude vise à présenter la réalité de la cybercriminalité en Algérie et les efforts déployés pour la combattre comme l'un des défis de l'e-gouvernement, car elle a clarifié comment ce genre de crime affecte la voie de l'e-gouvernement, et elle était basée sur des statistiques nationales et internationales. L'étude a révélé que la cybercriminalité était l'un des types de crimes les plus courants en Algérie. Malgré les efforts déployés par les autorités algériennes compétentes pour lutter contre ces

Mots-clés: e-gouvernement; e-crime; Algérie; statistiques; défis..

Codes de classification de Jel: H83 ,K14,O38

المؤلف المرسل: نافع زينب، طالبة دكتوراه الإيميل: z.nafaa@univ-bouira.dz

1. مقدمة:

تمثل الحكومة الإلكترونية مشروعا عملاقا يعيد خلق الحكومة من جديد، و ذلك من خلال الاستعانة بوسائل مبتكرة لأداء الأعمال عن طريق تطويع التقنية وتسخيرها لتنفيذ مهام الأجهزة الحكومية، مما يجعل الجودة والتميز شعارها ويحولها إلى مؤسسة اقتصادية تنافس القطاع الخاص في كل ما يتمتع به من مزايا تنافسية وفي مقدمتها الجودة وكسب رضا المستفيد.

لقد لفت مفهوم الحكومة الإلكترونية انتباه أغلب الدول و من بينها الجزائر التي عملت جاهدة من أجل إرسائه في مختلف تعاملاتها، باعتبار أن التقنية تساعد على تنظيم الأعمال و تبسيطها، ولكنها في المقابل قد تفتح أبوابا في وجه القراصنة و المجرمين الإلكترونيين، الذين قد يتحصلون على مختلف البيانات الخاصة بالمواطنين أو المعلومات المتعلقة بتسيير شؤون الدولة بطريقة غير قانونية.

قامت الجزائر باقتناء تجهيزات وأنظمة معلومات متقدمة ومُعقدة لحماية بنيتها التحتية الإلكترونية من الجرائم الإلكترونية، ولكن لا تزال الفرق المُختصة في الأمن المعلوماتي في مختلف القطاعات الأمنية تحصي الآلاف من الجرائم الإلكترونية سنويا، والتي قد تنجح في فك شفرات بعضها وإحباطها قبل حدوثها، وتفشل في صد الكثير منها،حيث تعتبر الجزائر من الدول التي تسجل نسبة استخدام الانترنت فيها نموا مستمرا، وكلما زاد عدد المُستخدمين وتشعبت شبكة الانترنت الوطنية كلما تطورت عصابات الجريمة الإلكترونية فيها ،وأصبحت أكثر خطورة وتأثيرا على الفضاء الافتراضي.

الإشكالية: من خلال ما سبق نطرح الإشكالية التالية:

في ظل توجه الجزائر نحو اعتماد مفهوم الحكومة الإلكترونية، ما هو واقع الجرائم الإلكترونية في الجزائر مقارنة بباقي الدول؟ وما هي الوسائل المسخرة من طرف السلطات لمواجهتها؟

وللإجابة على هذا السؤال ارتأينا تقسيم البحث إلى المحاور التالية:

1. المضامين النظرية للحكومة الإلكترونية والجريمة الإلكترونية.
2. الجريمة الإلكترونية وتأثيرها على مسار الحكومة الإلكترونية.
3. الجريمة الإلكترونية في الجزائر والجهود المبذولة لمواجهتها.

أهمية الدراسة :

تكمن أهمية البحث في كونه محاولة أكاديمية لإلقاء الضوء على مدى خطورة الجرائم الإلكترونية، خصوصا في ظل اعتماد نمط الحكومة الإلكترونية، حيث يعتبر عرض واقع هذا النوع من الجرائم في الجزائر ودول أخرى وفق مؤشرات وإحصائيات وطنية وعالمية مهما جدا لمختلف الباحثين والمهتمين بهذا المجال، من أجل معرفة نقطة الانطلاق للقضاء على هذه الجرائم الإلكترونية .

أهداف الدراسة :

يهدف البحث إلى تحقيق حزمة متكاملة من الأهداف، نذكر منها:

- معرفة كيفية تأثير مختلف الجرائم الإلكترونية على مسار الحكومة الإلكترونية، وكيفية التغلب عليها؛
- التعرف على واقع الجرائم الإلكترونية في الجزائر من خلال إحصائيات وطنية وأخرى دولية؛
- إبراز مختلف الجهود التي بذلتها الجزائر لمواجهة هذا النوع من الجرائم، أوالوقاية منها؛
- إبراز ضرورة مكافحة الجرائم الإلكترونية من أجل إرساء نظام حكومي إلكتروني ناجح؛

منهجية الدراسة:

اتبعت الدراسة الأسلوب الوصفي من أجل وصف الظاهرة محل الدراسة، وقم تم استخدام مختلف المراجع المكتبية من كتب، مقالات، أطروحات، مداخلات علمية، قوانين ومراسيم ...، والأسلوب التحليلي لتحليل مختلف المؤشرات والإحصائيات المتعلقة بواقع الجرائم الإلكترونية في الجزائر.

2. المضامين النظرية للحكومة الإلكترونية والجريمة الإلكترونية

1.2. مدخل إلى الحكومة الإلكترونية:

لقد احتاج ظهور الحكومة الإلكترونية إلى عدة تطورات سياسية واقتصادية واجتماعية وتكنولوجية وغيرها، كانت نماذج الحكم تتطور مع تلك الأحداث وتستفيد من تلك الأساليب والوسائل الإدارية والتقنية المصاحبة لكل مرحلة، حيث توجت المرحلة الأخيرة بميلاد ما يسمى بالحكومة الإلكترونية التي أساسها الحكومة الحقيقية أي التقليدية لكن تؤدي مهامها من خلال نسق رقمي موحد . (بن عيشاوي، 2009، صفحة 288)

1.1.2. **تعريف الحكومة الإلكترونية:** لقد اختلفت آراء الباحثين حول تحديد مفهوم الحكومة الإلكترونية نظرا لأهمية مصطلح الحكومة الإلكترونية واتساع مفهومه، فكل يراها من منظوره، وفيما يلي عرض لبعض هذه التعاريف:

عرفها **البنك الدولي** بأنها: "استخدام تكنولوجيا المعلومات والإتصالات من أجل رفع فعالية وكفاءة الحكومة وهي تشمل: تعزيز المشاركة المدنية من خلا ل تمكين الجمهور من التفاعل مع المسؤولين الحكوميين، جعل عمل الحكومة أكثر شفافية وبالتالي التقليل من فرص الفساد،توفير فرص تطوير خاصة في المجتمعات الريفية. (centre for democracy and tecknology , 2002, p. 1)

عرفتها **الأمم المتحدة** بأنها:" استخدام تكنولوجيا المعلومات والإتصالات، مثل شبكات الإتصالات الخارجية، مواقع الانترنت، ونظم الحاسب الآلي بواسطة الجهات الحكومية لتقديم معلومات وخدمات بين الجهات الحكومية من جانب والمواطنين وأعمالهم من جانب آخر" (فرحي، 2013، صفحة 93)

وعرفها **الإتحاد الأروبي** بأنها " حكومة تستخدم تكنولوجيا المعلومات والاتصال لتقدم للمواطنين وقطاع الأعمال الفرصة للتعامل والتواصل مع الحكومة باستخدام الطرق المختلفة للاتصال مثل: الهواتف، الفاكس، البطاقات الذكية، الأكشاك، البريد الإلكتروني والانترنيت، وهي كيفية تنظيم الحكومة نفسها في الإدارة والقوانين والتنظيم ووضع إطار لتحسين وتنسيق طرق إيصال الخدمات وتحقيق التكامل بين الإجراءات" (براق و كروش، 2013، صفحة 3)

يتضح مما سبق أن الحكومة الإلكترونية كمفهوم يقوم على محورين أساسيين هما: (المناعسة و الزعبي، 2013، الصفحات 13-14)

- **تقديم العمل الإداري باستخدام تطبيقات تقنية نظم المعلومات** : والتي تتيح تقديم الخدمات والمعلومات للإدارات الحكومية المختلفة وللمواطنين وقطاعات العمال في اي مكان وزمان؛
- **تقديم الخدمات عن بعد**: حيث يمكن لمتلقي الخدمة أو الباحث عن المعلومة الحصول عليها دون حاجة إلى القدوم إلى مكان العمل أومكان تقديم تلك الخدمة أوالمعلومة؛

2.1.2. أهداف الحكومة الإلكترونية: للحكومة الإلكترونية عدة أهداف تسعى لتحقيقها نذكر منها:

- تحسين وتطوير الخدمات، وذلك بالتقليل من تنقل المواطن بين المؤسسات المختلفة، والمتباعدة جغرافيا؛
- صحة البيانات المتبادلة والمسترجعة، والتي تزيد من نسبة الثقة بتلك البيانات، ويبعد احتمالات الوقوع في الخطأ، من جراء إعادة كتابة وإدخال البيانات؛ (قنديلجي، 2015، صفحة 33)
- سهولة الوصول للخدمات الإلكترونية من خلال النشر الإلكتروني، وهذا يحقق مبدأ الشفافية والعدالة لكافة شرائح المجتمع وتعزيز الديمقراطي؛ (مجاهد و طويطي، 2016، صفحة 210)
- تحقيق سرعة وفعالية الربط والتنسيق والأداء والإنجاز بين دوائر الحكومة ذاتها، ولكل منها على حدى؛ (يحياوي إ.، 2016، صفحة 20)
- تخفيض التكاليف الحكومية: مما يؤدي إلى انخفاض تكلفة الخدمات الحكومية المقدمة نتيجة لتغيير طريقة تقديم وتنفيذ الخدمات وآليات توصيلها من الشكل التقليدي إلى الشكل الإلكتروني إلى وفرة في ميزانية الدولة؛ (يحياوي م.، 2013، صفحة 21)
- الحد من ظاهرة الفساد الإداري من خلال نشر كافة البيانات والمعلومات المتعلقة بالأداء الحكومي على شبكة الانترنيت وإتاحتها للمواطنين، وإعطائهم حق المساءلة عن القرارات التي يتخذها المسؤولين؛ (زكي، 2009، صفحة 26)
- المساهمة في دعم النمو الاقتصادي من طرف الحكومة الإلكترونية حيث أن مختلف فروعها مثل التجارة الإلكترونية والتسويق الإلكتروني تعمل كأنشطة مساعدة ،مما يوفر حركة اقتصادية أوسع؛ (باري، 2014، صفحة 30)

3.1.2.متطلبات تطبيق الحكومة الإلكترونية: إن تطبيق مشروع الحكومة الإلكترونية يستلزم توفر جملة من الأساسيات التي تشكل البنية الأساسية الضرورية لإقامة هذا المشروع ولعل أهمها:

- **متطلبات تقنية** : وتتمثل في :

- توفير البنية التحتية اللازمة للاتصالات : والتي تقع على عاتق وزارة الاتصال حيث تعمل على توفير وصيانة هذه الشبكات باستمرار، من أجل تسهيل الحصول على مختلف أعمال الحكومة الإلكترونية عبر شبكات الإتصالات؛
- ضرورة انتشار الأنترنيت: والتي بواسطتها يتم تأمين الاتصال بين مستخدمي الشبكة على مستوى جميع القطاعات ؛
- ضرورة اتاحة الحاسب الألي ولواحقه: إذ أن مختلف الخدمات الإلكترونية تقدم بواسطة هذا الجهاز لذا يستلزم استطاعة المواطن على اقتنائه من جهة والإلمام باستخداماته من جهة أخرى؛

- **متطلبات فنية:** وتتمثل في:

- **إعادة هندسة إجراءات العمل في الحكومة**: أي تحويل مختلف أعمال الحكومة للنظام الرقمي وذلك من خلال عدة أمور مثل: وصف كل خدمات الحكومة بالتفصيل ومن يقوم بهذه الخدمات، تحديد علاقة وتداخل الإجراءات بين الوزارات والدوائر بالتفصيل، حذف الاجراءات التي لا تتماشى مع الأسلوب الجديد، نشر تفاصيل الإجراءات الجديدة على موقع الأنترنيت؛ (بن عيشاوي، 2009، الصفحات 289-290)
- **الدعم الإداري**: حيث تشكل قناعة واهتمام ومساندة الإدارة العليا لتطبيق تكنولوجيا المعلومات في المؤسسات كافة، أحد العوامل المساعدة في تحقيق نجاح تطبيق الحكومة الإلكترونية؛

- **متطلبات تشريعية** : لإنجاح الحكومة الإلكترونية فإن الأمر يتطلب الاعتراف بعملياتها تشريعيا، وتحديد متطلبات تطبيقها، والسماح بأطر التعاون بين المؤسسات، والتركيز على الخصوصية والأمن المعلوماتي؛ (جواد و ابو زيد، 2007، صفحة 285)

- **متطلبات بشرية** : حيث يمثل العنصر البشري المحرك الأساسي للحكومة الإلكترونية، وبالتالي فإن الاهتمام بمجالي تطوير وتدريب الأفراد يعتبر أمرا ملحا،وبالمقابل فإن الفرد العادي الذي يتوقع أن يستفيد أو يتعامل مع مشروع الحكومة الإلكترونية يجب أن يمتلك الكفاءة التقنية في التعامل مع التكنولوجيا الحديثة والإلمام بما توفره من فوائد وخدمات؛ (حمزة، 2013، صفحة 3)

وعلاوة على ما تقدم فإن هناك جملة من العناصر ذات الأهمية البالغة لضمان تطبيق الحكومة الإلكترونية مثل الرؤية الواضحة للقائمين على هذا المشروع، وكذا القيادة الفاعلة المتخصصة والماهرة والمتعاونة، والعنصر البشري المؤهل والمتدرب على هذه الاستعمالات وكذا البيئة التنظيمية الملائمة والقادرة على استيعاب هذا التغيير.

2.2. مفهوم الجريمة الإلكترونية:

لقد أصبحت الجريمة الإلكترونية اليوم واقعا مفزعا يهدد الدول والأفراد، ويعود ذلك أساسا إلى الإمكانيات المتاحة للمجرم الإلكتروني الذي يستطيع تعطيل موقع إلكتروني، أو يقرصن حسابا ما، أو يستولي على معلومات شخصية أو أموال غيره، وفيما يلي سيتم التعرف على الجريمة الإلكترونية ومظاهرها .

1.2.2.تعريف الجريمة الإلكترونية

لقد اختلف في تحديد المقصود من الجرائم الإلكترونية، ويعود هذا الاختلاف إلى تباين الزاوية التي ينظر منها ،وفيما يلي عرض لبعض التعاريف: (مطر، 2013، الصفحات 119-120)

- **من حيث موضوع الجريمة:** " هي نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه".
- **من حيث مرتكب الجريمة**: " أي فعل غير مشروع تكون المعرفة بتقنية الكمبيوتر أساسية لارتكابه "
- **من حيث وسيلة ارتكاب الجريمة**: " كل فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية"

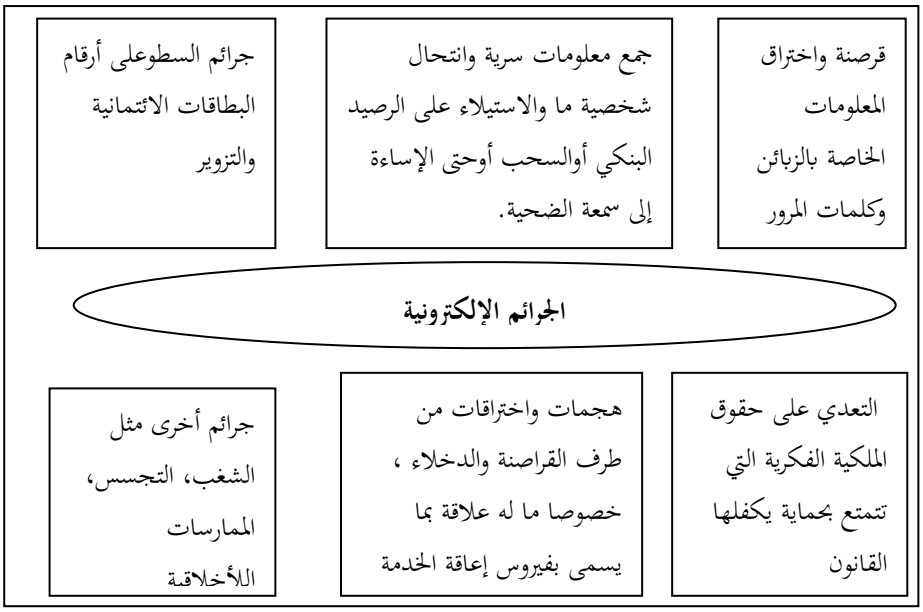
من خلال التعاريف السابقة يمكننا استخلاص بعض السمات الخاصة بالجرائم الإلكترونية :

- سهولة ارتكاب الجريمة الإلكترونية بعيدا عن الرقابة الأمنية؛
- سهولة إتلاف الأدلة من قبل الجناة؛

- صعوبة التحكم في تحديد حجم الضرر الناجم عنها قياسا بالجرائم التقليدية؛
- جريمة عابرة للحدود لا تعترف بعنصر المكان ولا الزمان، فهي لا تعترف بعنصر المكان ولا الزمان، فهي تتميز بالتباعد الجغرافي، واختلاف التوقيت بين الجاني والمجني عليه؛ (بوسيف، 2017، الصفحات 232-233)
- تعتمد على الخداع في ارتكابها، والتضليل في التعرف على مرتكبيها؛
- تعتمد على قمة الذكاء في ارتكابها؛ (بونعارة، 2015، الصفحات 280-281)

2.2.2.مظاهر الجرائم الإلكترونية: تتمثل فيما يلي:

الشكل رقم 01 : مظاهر الجرائم الإلكترونية



المصدر: (قنديلجي، 2015، صفحة 318)

من خلال الشكل رقم1 يمكننا القول أن الجرائم الإلكترونية لها أوجه كثيرة جدا، مما يجعل عملية متابعتها والكشف عنها صعبة جدا، وبالتالي يجب توخي الحيطة والحذر عند استعمال الوسائل التكنولوجية، لتجنب الوقوع فيها.

3 . الجريمة الإلكترونية وتأثيرها على مسار الحكومة الإلكترونية:

لقد شهد العالم خلال العقدين الماضيين ثورة هائلة في مجال تقنية المعلومات و الإتصالات، تميزت اساسا باستخدام الحواسيب الالية والشبكات المتصلة بها، وتزايد بشكل ملفت استخدامات هذه التقنيات مما أدى إلى ظهور الجرائم الإلكترونية، وقد نقلت صحيفة العربي الجديد بأن التكلفة الاجمالية للتهديدات والجرائم الإلكترونية على مستوى العالم ستتجاوز 6 تريليونات دولار عام 2021، ليكون بذلك معدل الجريمة قد سجل ارتفاعا بنحو3 تريليونات دولار عن سنة 2015. (العزي، 2017، صفحة 12)

1.3. الحكومة الإلكترونية والجريمة الإلكترونية

نظرا للدور الكبير الذي تمثله الحكومة الإلكترونية في حياتنا المعاصرة، والتي أصبحت تساهم في كافة المجالات كإبرام العقود إلكترونيا ،الانتخاب الإلكتروني استخراج مختلف الوثائق الإدارية إلكترونيا...، أصبح من الضروري حماية الهيكل الالكتروحكومي من المعطلين وجماعات التخريب، والحفاظ على خصوصية المواطن، كما يجب عدم الاستهانة بمسؤوليات الأمن المعلوماتي في الدولة وأجهزتها الحكومية، واعتبارها أنها مسؤولية من مسؤوليات الحكومة، خصوصا أن التقنيات والأساليب التي يمكن أن يعتمدها المخربون من أجل إلحاق الأذى بالحكومة الإلكترونية متعددة ومتنوعة . (مطر، 2013، صفحة 116)

من جهة أخرى تعتبر مسألة الأمن مكلفة للغاية، وعليه تقتضي الضرورة والأهمية معالجتها خلال مرحلة التصميم، ذلك أن التجاوز على هذه المشكلة قد يفقد ثقة المواطنين بالحكومة الإلكترونية، خصوصا تلك الخدمات التي يتطلب الحصول عليها قيام المواطنين بتزويد الحكومة بمعلومات شخصية . (المبيضين، 2011، صفحة 90)

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

- **الركن الأول** : إيجاد المقومات الرئيسية التي تمثل ركائز مشروع الحكومة الإلكترونية كوجود الرؤية الاستراتيجية، تكوين البنية التحتية المعلوماتية، تحقيق التحول التنظيمي، تهيئة الأنظمة والتشريعات، تحقيق الأمن والموثوقية المعلوماتية، نشر المعرفة المعلوماتية .
- **الركن الثاني**: عملية التحول المرحلي والمندرج لتطبيقات الحكومة الإلكترونية 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. (مولاي، 2013، صفحة 8)

وفي نفس السياق فإن عملية التحول من الحكومة التقليدية إلى الحكومة الإلكترونية تعتبر نقلة نوعية في آليات العمل، الأمر الذي يتطلب التخطيط الجيد والدقيق للتحول من مرحلة إلى مرحلة أخرى، وذلك لتفادي مختلف الأخطار والصعوبات والجرائم التي تحدق بها، وفيما يلي عرض لأهم الأضرار التي قد تحدثها الجريمة الإلكترونية في كل مرحلة من هذه المراحل حسب النموذج المصمم من طرف البنك الدولي :

- **في مرحلة النشر:** أين يتم عرض كم هائل من المعلومات مثل التشريعات والأنظمة والنماذج من خلال الانترنت ووسائل التكنولوجيا المتقدمة، والتي تكون موجهة للمواطنين ومؤسسات الأعمال، (الجوزي و العمري، 2017، صفحة 6) وهي تستهوي صغار المخربين الذين ينبهرون بالتكنولوجيا فيحاولون التغلب عليها من خلال العبث بالمعلومات المعروضة، فيقومون بحذفها أو تغييرها بأخرى، وبالتالي عدم الاستفادة منها من طرف الأطراف الموجهة إليهم، أو قد يقومون بنشر فيروس ما يصيب أي جهاز يلج الموقع الإلكتروني للحكومة، مما يؤدي بالمواطنين ورجال الأعمال إلى العزوف عن ولوج الموقع ،وأحيانا قد يصل الأمر إلى إخفاء الموقع كليا.
- **في مرحلة التفاعل:** أين يتمكن المستخدم من إبداء آرائه وانتقاداته حول التشريعات والسياسات المقترحة (غيشي، 2016، صفحة 49)،نتيجة للاتصال المتبادل بين الحكومة والمواطنين عن طريق البريد الإلكتروني، مما قد يجعل المجرم الإلكتروني يرسل رسائل وهمية بين مختلف المتعاملين وفق هذا النظام، أو قد يغير محتواها أو قد يحذفها ،أو قد يصل الأمر إلى التجسس على مختلف الإتصالات، مما سيجعل التفاعل بين الأطراف غير آمن، ومن جهة أخرى قد يؤثر كذلك على مشاركة المواطن في الحكم الإلكتروني، فيغير مختلف الآراء والأصوات التي تم إبدائها من طرف أصحابها، وبالتالي تزوير المعلومات.
- **في مرحلة التبادل :** أين يتم السماح بإجراء تبادلات بين الأطراف المختلفة للحكومة الإلكترونية (مواطنون، مؤسسات، حكومات..)، حيث يتمكنون من إجراء المعاملات المالية الآمنة وعقد الصفقات على الخط مباشرة (غيشي، 2016، صفحة 49)،مما قد يجعل الحسابات المالية لهذه الأطراف عرضة للسرقة من طرف قراصنة الانترنت، خصوصا بعد تحصلهم على الأرقام السرية للحسابات والتي تعتبر ضرورية الافصاح عنها عند القيام بالشراء وفق التجارة

الإلكترونية، ومن جهة أخرى قد يكون تبادل الوثائق وليس الأموال أين يمكن تخريب هذه الوثائق أو استخدامها في أغراض مشبوهة، مما يعرض صاحبها للعقاب .

2.3.التصدي للجريمة الإلكترونية في ظل الحكومة الإلكترونية:

إن الجريمة الإلكترونية تمثل عائقا كبيرا كفيلا بالإطاحة بمشروع الحكومة الإلكترونية، لأن من أهم الأسس التي يقوم عليها مشروع الحكومة الإلكترونية هو الاستمرارية والسرية والأمن، فلو حدث أي خلل بالجانب الأمني ستنعدم السرية والأمان، ولو تم إختراق موقع من مواقع الحكومة الإلكترونية بشكل كلي أو جزئي سيؤدي بالتالي إلى توقف الموقع عن تقديم الخدمات للمواطنين، وبالتالي إفساد خاصية الحكومة الإلكترونية المتمثلة في تقديم الخدمات على مدار الساعة. (الخمايسة، 2013، صفحة 99)

لا يكفي لحماية نظام الحكومة الإلكترونية تجريم بعض الأعمال العدوانية أو الضارة التي تقع في مجال نظام تقنية المعلومات ووضع العقوبات الرادعة لها، وإنما يلزم وضع نظام وقائي متكامل يهدف إلى تأمين شبكة المعلومات والحيلولة دون وقوع الجرائم الإلكترونية، لأن هذه الجرائم تعد أسهل اقترافا من الجرائم العادية كونها ترتكب دون الحاجة لبذل جهد كبير أو التنقل ... (المبيضين، 2011، الصفحات 19-20)

لذلك على الحكومة أن تبذل جهودا كبيرة لاكتشاف هذه الجرائم ودراستها من عدة جوانب (معرفة النوايا والدوافع، معرفة مصادر الخطر، معرفة وسائل الهجوم الإلكتروني...)، وفيما يلي عرض لأهم المبادئ التي تعتمد عليها الحكومة الإلكترونية للقضاء على الجريمة الإلكترونية:

- **تطوير الاتفاقيات الأمنية الخارجية:** مع دول أخرى من أجل تبادل التجارب والخبرات في مجال التصدي للجرائم الإلكترونية، أو قد تتعاون هذه الدول مع بعضها البعض من أجل التغلب على أي جريمة إلكترونية تهدد أيا منها.
- **إنشاء وحدات خاصة بالأمن الإلكتروني:** إذ لا يجوز أن تمنح مسؤولية الحفاظ على الأمن الإلكتروني ومحاربة الجرائم الإلكترونية في الحكومة الإلكترونية لأطراف ما كجزء إضافي من مهامهم، بل يجب إنشاء وحدات خاصة مهمتها الأساسية هي محاربة الجرائم الإلكترونية.
- **تسجيل الأثر الإلكتروني:** من أجل التدقيق في الأعمال المريبة، ومساءلة الأشخاص المسؤولين عنها، تحتاج الرقابة الإلكترونية إلى معلومات عن الفعل وصاحبه، فعلى سبيل المثال يمكن تسجيل معلومات عن اسم المستخدم، تاريخ ووقت طلب الخدمة، مكان طلبها، عدد مرات الدخول إلى الشبكة..؛ (الخمايسة، 2013، الصفحات 121-124)
- **محاكاة أساليب الهجوم الإلكتروني:** يطلق على هذا الأسلوب أحيانا المناورات الأمنية الإلكترونية وتعمل خلالها أجهزة الأمن الإلكتروني على القيام بهجوم تجريبي غير ضار على أنظمة إدارات الدولة المختلفة للتحقق من صلابتها ومقاومتها، وقد يتم هذا الهجوم بدون سابق إنذار للتأكد من فعالية أجهزة الحماية، ومستوى تطبيق الإدارات الحكومية لمعايير الأمن الإلكتروني؛
- **الحماية المادية للأجهزة والأنظمة:** حيث تحتاج مواقع الحكومة الإلكترونية وأماكن تواجد أنظمتها إلى حماية أمنية للتأكد من عدم تجرأ أطراف عدوة على العبث والتخريب وتدمير المكونات المادية للحكومة الإلكترونية، وقد ينفع من فترة إلى أخرى إجراء مسح راداري لاسلكي للتأكد من عدم وجدود أجهزة تنصت إلكترونية في نطاق الحكومة الإلكترونية؛ (بومروان، 2014، صفحة 95)
- **اعتماد التشفير:** التشفير بكل بساطة نص غير مفهوم إلا من قبل المرسل والمستلم، وتوجد خوارزميات عديدة للتشفير، منها ما يستخدم فيه كل من المرسل والمستلم نفس المفتاح للتشفير وفتح الشيفرة، ومنها ما يستخدم كل من المرسل والمستلم مفتاح خاص به، وللتشفير عدة فوائد مثل: الخصوصية، سلامة الرسالة، عدم الإنكار، التوقيع الرقمي.. (الحمامي و السعدون، 2016، الصفحات 124-125)

- **استخدام برامج رقمية مخصصة للحماية**: أو المساهمة في التصدي للجريمة مثل: البصمة الإلكترونية، البطاقة الذكية، أنظمة المعلومات الجغرافية، فالمؤسسة التي تحوز على أحد هذه البرامج سيكون بمقدورها تحقيق ما يسمى بالموثوقية الإلكترونية، والسير قدما في مكافحة الجريمة الإلكترونية بفعالية أكثر ضمن منظومة الحكومة الإلكترونية. (أبو مغايض، 2009، الصفحات 25-26)

يمكننا القول أنه من الضروري القيام بالتحسين والتطوير الدائم في أساليب الحماية، من أجل التغلب على مختلف الهجومات التي قد تتعرض لها الحكومة الإلكترونية، وذلك باستعمال التقنيات الحديثة، بالإضافة إلى الاستفادة من الأخطاء السابقة.

4. الجريمة الإلكترونية في الجزائر والجهود المبذولة لمواجهتها:

تعرف الجزائر كغيرها من الدول تزايدا مستمرا في عدد الجرائم الالكترونية المرتكبة، و فيما يلي سيتم عرض أهم الإحصائيات الوطنية و العالمية لهذا النوع من الجرائم في الجزائر و دول أخرى، و كذا مختلف الجهود و الإجراءات المتبعة من أجل القضاء عليها أو على الأقل التخفيف من حدتها.

1.4. الإحصائيات الوطنية (المحلية) للجرائم الإلكترونية في الجزائر:

في حقيقة الأمر لا توجد إحصائيات دقيقة عن عدد الجرائم الإلكترونية في الجزائر، فما هو موجود لا يتعدى بعض التصريحات لهيئات وطنية مسؤولة عن محاربة هذا النوع من الجرائم، أو بعض التقارير الصادرة عن هذه الهيئات، والجدول التالي يبين عدد الجرائم الإلكترونية في الجزائر المسجلة من طرف الأمن الوطني، خلال الفترة 2017-2019 ، حسب أنواعها:

الجدول رقم 01: الجرائم الإلكترونية في الجزائر في الفترة 2017–2019

نوع الجريمة / السنة	2017	2018	2019
جرائم المساس بالأشخاص عبر الأنترنيت	1511	2410	225
جرائم المساس بأنظمة المعالجة الآلية للمعطيات	28	189	1152
جرائم الاحتيال عبر الأنترنيت	47	149	68
جرائم الإخلال بالنظام العام	/	383	225
جرائم بيع السلع المحضورة على شبكة الانترنيت	/	203	90
جرائم أخرى	544	188	13
مجموع القضايا المسجلة	**2130**	**3522**	**1773**
مجموع القضايا المعالجة	**1570**	**2677**	**1402**
نسبة القضايا المعالجة	**73.71**	**74.95**	**79.05**

المصدر: من إعداد الباحثان اعتمادا على: (زكري، 2019، صفحة 33) (جوزي، 2018، صفحة 128)

من خلال الجدول رقم 01 نلاحظ أن:

- عدد الجرائم الإلكترونية في الجزائر، في تزايد مستمر من سنة لأخرى، فبعدما تم تسجيل 2130 جريمة إلكترونية في سنة 2017، ارتفع عددها في 2018 ب 1392 جريمة إلكترونية، ليصل بذلك عدد الجرائم المسجلة في 2018 إلى 3522 جريمة، أما خلال السداسي الأول من 2019 فقد تم تسجيل 1773 جريمة إلكترونية، وهو ليس بالعدد القليل.
- بالنسبة لسنتي 2017 و 2018، تتصدر جرائم المساس بالأشخاص عبر الانترنت قائمة الجرائم المرتكبة، بنسب تقدر ب71%، 68% على التوالي من مجموع الجرائم المسجلة، بينما تمثل باقي الأنواع الأخرى نسب ضعيفة مقارنة بها.
- بالنسبة للسداسي الأول من سنة 2019، تتصدر جرائم المساس بأنظمة المعالجة الآلية للمعطيات قائمة الجرائم المرتكبة ، بنسبة تقدر بحوالي 65%، و هي نسبة كبيرة مقارنة بباقي الأنواع الأخرى.

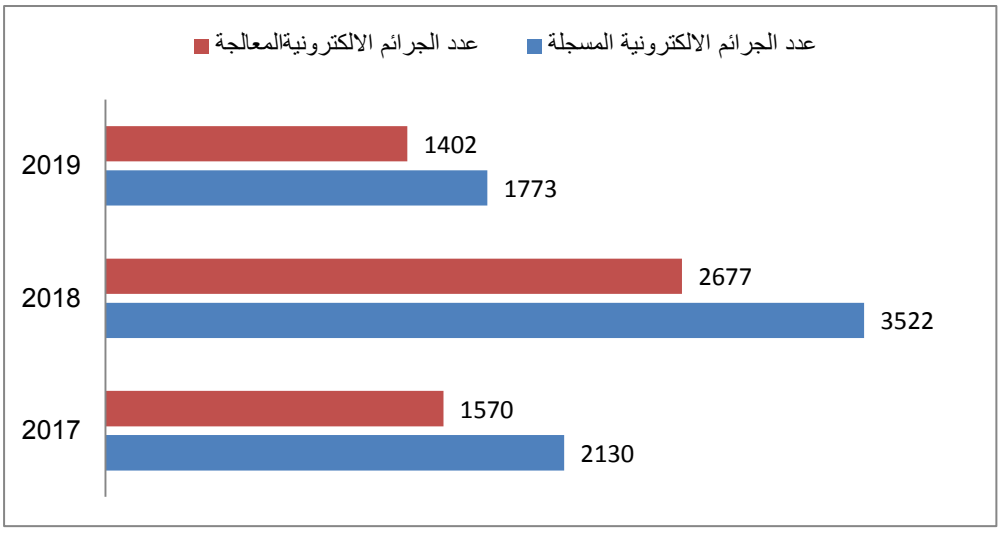
- يحتوي الجدول على الجرائم الإلكترونية المسجلة لدى مصالح الأمن فقط، أي تلك الجرائم التي قدم أصحابها شكوى، أو الجرائم التي تم اكتشافها من طرف فرق الأمن المختصة بهذا النوع من الجرائم، بينما العدد الفعلي لهذا النوع من الجرائم أكبر من ذلك بكثير، باعتبار أن بعض الأشخاص لا يصرحون بالجرائم الإلكترونية التي مستهم بسبب الخوف، أو الخجل أو أسباب أخرى.

و لعل أهم أسباب تزايد عدد الجرائم الإلكترونية في الجزائر مؤخرا نجد:

- تزايد إستخدام الانترنت في الجزائر في السنوات الأخيرة، حيث ارتفعت نسبة مستخدمي الانترنت ارتفعت إلى 49.2% من عدد السكان سنة 2018 بعدما كانت 45.2 % سنة 2017، لترتفع مرة أخرى إلى 59.6% سنة 2019، و هذا ما سيفتح المجال أمام المجرمين الذين يجدون أنفسهم متصلين بالانترنت الذي سيساعدهم في القيام بجرائمهم دون أدنى تعب، فيحاولون الحصول على معلومات و أموال الآخرين دون وجه حق؛
- نقص القوانين و التشريعات الردعية التي تضبط مختلف التعاملات الإلكترونية في ظل اعتماد مفهوم الحكومة الالكترونية؛
- ضعف نظام الأمن و الحماية الإلكترونية في الجزائر، و الذي يؤدي إلى سهولة اختراق بعض المواقع المهمة في البلاد؛
- تكتم بعض الضحايا عن الابلاغ عن الجرائم الإلكترونية المرتكبة في حقهم خوفا من المجتمع أو العادات و التقاليد، جعل المجرمين الإلكترونيين يتمادون في ارتكاب هذا النوع من الجرائم؛

و لتوضيح عدد القضايا المعالجة مقارنة بتلك المسجلة خلال الفترة 2017-2019، تم تمثيل المعطيات المتعلقة بذلك من الجدول السابق في الرسم البياني التالي:

الشكل رقم 02: عدد الجرائم الإلكترونية المسجلة والمعالجة خلال الفترة 2017-2019



المصدر: من اعداد الباحثان اعتمادا على معطيات الجدول رقم 01

من الشكل رقم 02 نلاحظ أن:

- خلال الفترة 2017-2019 تم معالجة عدد معتبر من الجرائم الإلكترونية من طرف الأمن الوطني الجزائري؛
- في سنة 2017 تم معالجة 1570 جريمة إلكترونية من مجموع 2130 جريمة، بنسبة تقدر ب 73.71 %، وكذلك الحال بالنسبة لسنتي 2018 و2019، فقد بلغت نسبة الجرائم الإلكترونية المعالجة 74.95 و79.05 على التوالي، و هي نسب مرتفعة جدا ،وهذا إن دل على شيء فإنما يدل على أن السلطات الجزائرية تولي أهمية كبيرة لهذا النوع من الجرائم، فهي تعمل على متابعته و محاربته باستمرار .

و من أجل تسهيل عمل المصالح الأمنية و مساعدتها للحد من هذه الجرائم، هناك إجراءات و تعليمات وجب اتباعها نذكر منها:

- التوعية الدائمة عن طريق وسائل الإعلام بمدى خطورة هذا النوع من الجرائم، و كيفية التعامل معها؛
- تجنب نشر أي معلومات أو صور شخصية على مواقع التواصل الاجتماعي، لتفادي الابتزاز أو السرقة...
- تجنب استخدام أي برنامج مجهول المصدر، أو إدخال كلمات مرور مجهولة من أجل تجنب القرصنة...
- تثبيت برامج حماية من الفيروسات و الاختراقات من أجل الحفاظ على سلام الجهاز و سرية المعلومات؛
- عدم كشف كلمات المرور لأي حساب خصوصا تلك المتعلقة بالحسابات البنكية او البريدية؛
- التبليغ عن مثل هذه الجرائم عند حدوثها، و بالتالي المساهمة في ردع مثل هذه التصرفات غير القانونية؛

2.4. الجريمة الإلكترونية في الجزائر حسب دراسات و مؤشرات عالمية:

لقد حاولت عدة هيئات عالمية دراسة مدى انتشار الجرائم الإلكترونية في العالم، و لعل أهمها:

1.2.4. دراسة الموقع العالمي comparitech.com :

من أجل التعرف على مدى خطورة الوضع فيما يخص الجرائم الإلكترونية في الجزائر، ارتأينا عرض مقارنة بسيطة لمدى استفحال هذا النوع من الجرائم في الجزائر و بعض الدول الأخرى، و قد إعتمدنا على دراسة مقارنة قام بها موقع comparitech.com في سنة 2019، حول مدى توفر الأمن الإلكتروني في دول العالم، حيث شملت الدراسة 60 دولة من بينهم دول عربية وأخرى أجنبية، وقد اعتمد على دراسة كانت قد قامت بها شركة kespersky حول نفس الموضوع، حيث الدول التي تحصل على أكبر نسبة فإنها دولة تملك أضعف أمن إلكتروني وبالتالي تكون أكثر عرضة للجرائم الإلكترونية، أما الدول التي تتحصل على أصغر معدل فهي الدولة التي تمتلك أقوى أمن إلكتروني، والجدول التالي يوضح بعض الدول التي شملتها الدراسة، والتي من بينها الجزائر:

الجدول رقم 02: معدل انتشار الجرائم الإلكترونية في الجزائر ودول أخرى

المرتبة	البلد	معدل انتشار الجريمة الإلكترونية
1	الجزائر	55.75
20	مصر	38.03
23	الإمارات العربية المتحدة	36.88
25	المغرب	36.47
27	تونس	35.57
32	المملكة العربية السعودية	32.99
60	اليابان	8.81

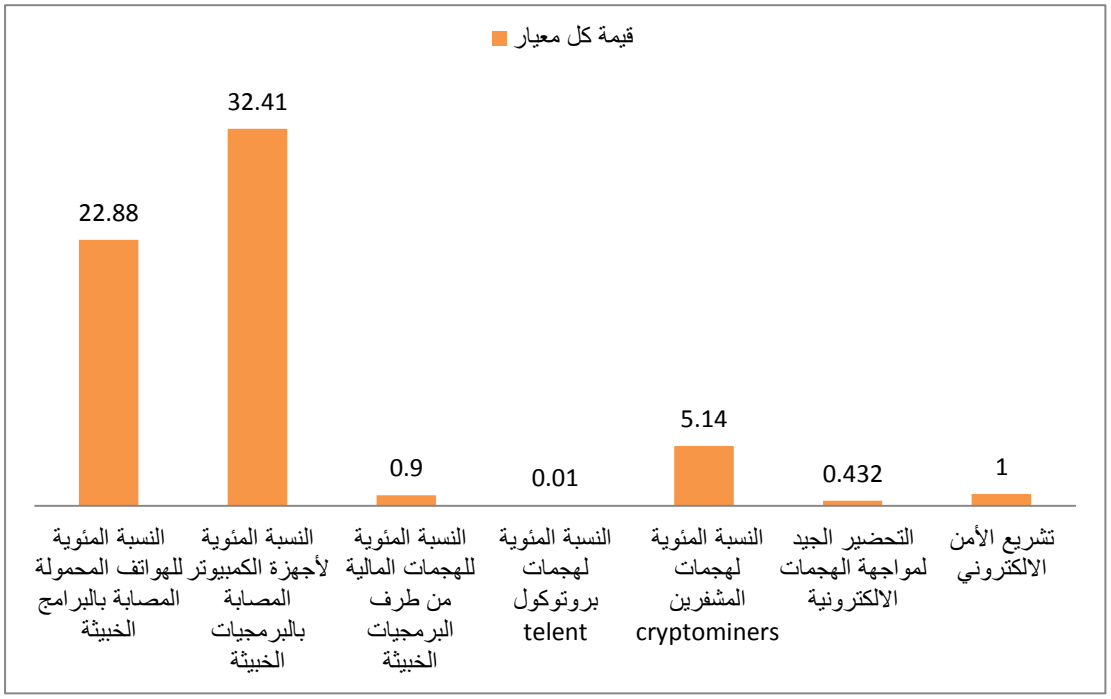
المصدر: من اعداد الباحثان اعتمادا على (Mody, 2019)

من خلال الجدول أعلاه نلاحظ أن:

- من بين 60 دولة شملتهم الدراسة، احتلت الجزائر المركز الأول في معدل انعدام الأمن الإلكتروني،بمعدل يقدر ب 55.75 %، بما يعني أنها الدولة الأقل حماية لوسائلها الإلكترونية من بين 60 دولة؛
- بالنسبة للدول العربية الأخرى، تنخفض معدلات انتشار الجرائم الإلكترونية، فنجده 35.57% في تونس، و 36.47 % في المغرب و32.99 % في المملكة العربية السعودية؛
- تتصدر اليابان جميع الدول التي شملتهم الدراسة بمعدل 8.81 وتكون بذلك الأكثر أمنا إلكترونيا من الدول 59 الأخرى.

و تعتمد الدراسة على عدة معايير للحصول على النسبة المئوية المطلوبة، والشكل التالي يوضح مختلف القيم التي تحصلت عليهم الجزائر في هذه المعايير :

الشكل رقم 03: قيم المعايير التي تحصلت عليهم الجزائر في الدراسة المقارنة



المصدر: من إعداد الباحثان اعتمادا على: (Rebecca mody , 2019)

من خلال الشكل أعلاه نلاحظ أن:

- تحصلت الجزائر على نسب مرتفعة بالنسبة لأجهزة الهواتف النقالة وأجهزة الكمبيوتر المصابة بالبرامج الخبيثة، حيث بلغت النسب 22.88 % و32.41% على التوالي، من مجموع الأجهزة المستعملة، في حين حصلت على نسب منخفضة في 3 معايير أخرى؛
- لم تتعدى النسبة المئوية للهجمات المالية من طرف البرمجيات الخبيثة في الجزائر 0.9 %، في حين كانت النسبة المئوية لهجمات المشفرين cryptominers 5.14 %، بينما تحصلت على أدنى نسبة في هجمات بروتوكول telent ب 0.01 %؛
- فيما يخص معيار التحضير الجيد لمواجهة الهجمات الإلكترونية فقد تحصلت الجزائر على 0.432 من 1، أي أقل من النصف،و هو غير كاف لمجابهة مختلف الهجمات التي قد تتعرض لها مختلف الأجهزة أو البرامج، أو المواقع الالكترونية، لذا وجب عليها إعادة النظر و بجدية في كيفية جديدة من أجل إصلاح ذلك؛
- تحصلت الجزائر على 1 من 10 في معيار تشريع الأمن الإلكتروني، و هذا راجع إلى قلة عدد التشريعات التي تعالج و تنظم الجرائم الإلكترونية بمختلف أنواعها؛

2.2.4. مؤشر الاتحاد الدولي للاتصالات للأمن الإلكتروني:

يعد مؤ شر الأمن الإلكتروني العالمي مؤشرًا مركبًا يجمع بين 25 مؤشرًا في مقياس مرجعي واحد لرصد التزامات الأمن الإلكتروني لدى الدول الأعضاء في الاتحاد الدولي للاتصالات البالغ عددها 193 دولة، وهو يدور حول خطة الأمن الإلكتروني العالمي، وهي إطار للتعاون الدولي أطلقه الاتحاد الدولي للاتصالات في عام 2007 لتعزيز الثقة والأمن في مجتمع المعلومات، (united nations, 2018, p. 69)والجدول التالي يوضح ترتيب الدول العربية وفق هذا المؤشر:

الجدول رقم 3: ترتيب الدول العربية وفق مؤشر الأمن الإلكتروني

المرتبة عربيا	الدولة	قيمة المؤشر	المرتبة عالميا
1	المملكة العربية السعودية	0.881	13
2	عمان	0.868	16
3	قطر	0.860	17
4	مصر	0.842	23
5	الإمارات العربية المتحدة	0.807	33
6	الكويت	0.600	67
7	البحرين	0.585	68
8	الأردن	0.556	74
9	تونس	0.536	76
10	المغرب	0.429	93
11	فلسطين	0.307	101
12	السودان	0.294	103
13	العراق	0.263	107
14	الجزائر	0.262	108
15	سوريا	0.237	114
16	ليبيا	0.206	117
17	لبنان	0.186	124
18	موريطانيا	0.107	145
19	صوماليا	0.070	156
20	جيبوتي	0.063	159
21	اليمن	0.019	172
22	جزر القمر	0.015	173

Source : (the International Telecommunication Union , 2018, pp. 57-58)

من الشكل رقم 4 نلاحظ أنه:

- من بين 193 دولة التي شملها التقرير، احتلت بعض الدول العربية على غرار السعودية(13 عالميا)، وعمان (16 عالميا)، قطر (17 عالميا)، مراتب عالمية جيدة جعلتها تنافس أكبر الدول المتطورة .
- تحصلت الجزائر على قيمة 0.262 في مؤشر الأمن الإلكتروني العالمي، وهي قيمة أقل ما يقال عنها أنها ضعيفة جدا، باعتبار أن القيمة الأعلى هي 1، وهذا يدل على أن الجزائر لا تزال بعيدة في مجال مكافحة الجرائم الإلكترونية، و تطوير أمنها الإلكتروني.
- احتلت الجزائر المرتبة 14 عربيا و108 عالميا في مؤشر الأمن الإلكتروني العالمي، وهي مراتب جد متأخرة ، فبالنسبة للترتيب العربي ، تقدمت عليها 13 دولة عربية أي أكثر من النصف، أما بالنسبة للترتيب العالمي فقد احتلت ذيل الترتيب أيضا.

3.4.جهود الجزائر لمواجهة الجريمة الإلكترونية:

لقد أصبحت الجريمة الإلكترونية خطرا كبيرا على الدول، لذا كان لزاما عليها ان تواكب تطور هذا النوع من الجرائم للحد من أخطاره، والجزائر كغيرها من الدول سخرت الوسائل وبذلت جهودا من أجل مواجهتها، لعل أهمها:

1.3.4. إصدار القوانين والتشريعات المنظمة لأشكال الجريمة الإلكترونية:

رغم صعوبة ضبط ومكافحة جرائم الانترنيت على الصعيد الوطني إلا أن هناك جهودا معتبرة قام بها المشرع الجزائري لمحاربة قراصنة الانترنت وإحالتهم قانونيا على المحاكم، متأثرا بجل الدول العربية التي وضعت قوانين لمكافحة الجريمة الإلكترونية، منذ بداية الألفية الثالثة وعلى الأخص منذ منتصف العشرية الأولى منها، ومن أهم الأمور التي أعطاها المشرع الجزائري أهمية قصوى هي أمن الدولة والحفاظ على النظام العام. (عاقلي، 2017، صفحة 12)

حيث ذهبت الجزائر إلى صياغة مشروع قانون مكافحة الجرائم الإلكترونية الذي ينص على جملة من الإجراءات التي تحدد آليات الرقابة على الانترنت ومحاربة الجنح المرتبطة بالشبكة الافتراضية، حيث قام المشرع الجزائري بإحداث قسم في قانون العقوبات في القسم السابع مكرر من الفص الثالث الخاص بالجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات ويتضمن القسم ثمانية مواد من المادة 394 مكرر إلى المادة 397 مكرر 7، وفي عام 2006 أدخل المشرع الجزائري تعديلا آخر على قانون العقوبات بموجب قانون رقم 23-06، حيث تم تشديد العقوبة المقررة لمختلف الجرائم الإلكترونية دون المساس بالنصوص في حد ذاتها. (بلفكرات و بنزعمة، 2019، صفحة 517)

كما صادقت الجزائر سنة 2014 على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والتي تهدف إلى تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم المعلومات، لدرء أخطار هذه الجرائم حفاظا على الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها. (المرسوم الرئاسي رقم 14-252، 2014، صفحة 4)

ولم يكتف المشرع الجزائري عند هذا الحد، بل وسع مجال التعامل في البيئة الرقمية، ليشمل مجالات غير القطاع القضائي، من خلال القانون رقم 15-04 الذي يهدف إلى تحديد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، أين عالج آليات التوقيع الإلكتروني، وكذا السلطات التي تشرف عليه إلى جانب النظام القانوني لتأدية خدمات التصديق الإلكتروني. (مزاولي، 2017، صفحة 312)

2.3.4. إنشاء الهيئات لمواجهة الجريمة الإلكترونية :

قامت السلطات الجزائرية بإنشاء العديد من الهيئات والهياكل التي تهتم بقضايا الجرائم الإلكترونية، نذكر منها:

- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال : حيث نصت على إنشائها المادة 13 من القانون 04/09 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ؛
- المعهد الوطني للأدلة الجنائية على الإجرام: والذي يتكون من احدى عشر دائرة متخصصة في مجالات مختلفة، جميعها تضمن إنجاز الخبرة، فدائرة الإعلام الآلي والإلكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة ؛
- الهيئات القضائية الجزائية المتخصصة: حيث أن السلطة القضائية ستتعامل تأكيدا في قضايا الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ولاسيما بعد الانتشار الواسع والمتزايد إلى الشبكات الرقمية في حياة المواطنين، ومنذ 2003 قامت وزارة العدل باطلاق برنامج تكوين خاص بالقضاة هدفه رفع مستوى أداء القضاة، ليواكب التطور الخاص بجرائم المعلوماتية ؛ (بوضياف، 2018، الصفحات 368-370)

5. خاتمة:

للجريمة الإلكترونية صدى كبير جدا في جميع دول العالم، حيث أصبحت تشكل تهديدا خطيرا لاقتصادها ونموها، فالجريمة الإلكترونية أصبحت أمرا مرعبا خصوصا لدى الدول العربية، لما تسببه من أضرار كثيرة على مختلف الأصعدة، لذلك لابد من وضع قوانين وأنظمة صارمة لردع مرتكبي الجرائم الإلكترونية بأسرع وقت ممكن.

لذلك كان لزاما على الجزائر أن تساير هذه الثورة المعلوماتية بإيجاد حلول سريعة ومراجعة تشريعاتها في هذا المجال بما يواكب التطور الحاصل، فانضمت للاتفاقيات الدولية لسد فراغها التشريعي وقامت بتجريم الأفعال الماسة بالنظم المعلوماتية ومتابعة المجرمين، إلا أنها لا تزال تعرف ارتفاعا كبيرا في الجرائم الإلكترونية .

النتائج:

- ارتفاع كبير للجرائم الإلكترونية في الجزائر في السنوات الأخيرة؛
- عدم الاهتمام بتأمين مختلف الأجهزة الإلكترونية المستخدمة مما يعرضها للاصابة بالبرمجيات الخبيثة؛
- تعمل الهيئات المنشأة لمواجهة هذا النوع من الجرائم على معالجة أكبر عدد منها؛
- رغم الجهود المبذولة من طرف المشرع الجزائري للتصدي للجرائم الإلكترونية، إلا أنه لم يخصها بقانون قائم بذاته للتحكم فيها بصرامة؛
- التباين الكبير بين دول العالم في مكافحة الجريمة الإلكترونية ؛

التوصيات:

- ضرورة إبرام اتفاقيات عربية ودولية في مجال مكافحة الجرائم الإلكترونية؛
- على الدول الراغبة في إرساء حكومة إلكترونية ناجحة أن تعمل على التصدي لمختلف التحديات والمعيقات التي تواجهها، مثل الجرائم الإلكترونية؛
- على الجزائر اقتناء برامج حماية متطورة من أجل مواجهة مختلف التهديدات التي تمس بنيتها التحتية؛
- ضرورة مراجعة التشريعات واصدار تشريعات جديدة تشدد العقوبات على مرتكبي الجريمة الإلكترونية؛
- تفعيل اسلوب التوعية لدى مستخدمي مختلف شبكات الإتصالات العالمية ؛

6.قائمة المراجع:

- the International Telecommunication Union .(2018) . *the global cybersecurity index 2018* . switzerland.
- centre for democracy and tecknology .(2002) . *the e-government handbook for developing countries* . washington.
- rebecca Mody 6) .february, 2019 .(*Which countries have the worst (and best) cybersecurity* ؟ تم الاسترداد من comparitech: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/
- united nations .(2018) .*e-government survey2018* .new york.
- أحمد بن عيشاوي. (جوان، 2009). أثر تطبيق الحكومة الإلكترونية على مؤسسات الأعمال. *مجلة الباحث، 7* (7)، الصفحات 287-294.
- أسامة المناعسة، و جلال محمد الزعبي. (2013). *الحكومة الإلكترونية بين النظرية و التطبيق*. الأردن: دار الثقافة للنشر و التوزيع.
- اسمهان بوضياف. (سبتمبر، 2018). الجريمة الإلكترونية و الإجراءات التشريعية لمواجهتها. *مجلة الأستاذ الباحث للدراسات القانونية و السياسية، 3*(3)، الصفحات 348-375.
- المرسوم الرئاسي رقم 14-252 المرسوم الرئاسي رقم 14-252. (8 سبتمبر، 2014). المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. الجريدة الرسمية رقم 57 الصادرة بتاريخ 28 سبتمبر 2014.
- إلهام يحياوي. (2016). الحكومة الإلكترونية في الجزائر بين الواقع و التحديات. *مجلة العلوم الاقتصادية و علوم التسير، 16*(16)، الصفحات 15-45.
- امحمد مولاي. (2013). صعوبات الحكومة الإلكترونية : الجريمة الإلكترونية نموذجا. *مقدمة من الملتقى الدولي حول متطلبات إرساء الحكومة الإلكترونية في الجزائر: تجارب بعض الدول*. البليدة: جامعة سعد دحلب.
- إيمان عبد المحسن زكي. (2009). *الحكومة الإلكترونية : مدخل إداري متكامل*. مصر: المنظمة العربية للتنمية الإدارية .
- خالد ممدوح العزي. (2017). الجرائم المالية الإلكترونية : الجرائم المصرفية نموذجا. *المؤتمر الدولي حول الجرائم الإلكترونية*. لبنان: مركز جيل البحث العلمي.

- رشيد بلفكرات، و عبد القادر بنزعمة. (مارس، 2019). الجريمة الإلكترونية كتهديد للأمن الوطني الجزائري. *مجلة العلوم القانونية و الاجتماعية، 4*(1)، الصفحات 510-522.
- سمية بومروان. (2014). *الحكومة الإلكترونية و دورها في تحسين اداء الإدارات الحكومية: دراسة مقارنة*. السعودية: مكتبة القانون و الاقتصاد.
- شعيب حمزة. (2013). تطوير المركز الوطني للسجل التجاري كأحد متطلبات إرساء الحكومة الإلكترونية في الجزائر. *الملتقى الدولي حول متطلبات إرساء الحكومة الإلكترونية في الجزائر : تجارب بعض الدول* . البليدة : جامعة سعد دحلب.
- شوقي ناجي جواد، و سليم ابو زيد. (سبتمبر، 2007). الأبعاد المستقبلية للحكومة الإلكترونية في الأردن. *المجلة الأردنية في إدارة الأعمال، 3*(3)، الصفحات 278-295.
- صدام الحمايسة. (2013). *الحكومة الإلكترونية الطريق نحو الإصلاح الإداري*. الأردن: عالم الكتب للنشر و التوزيع.
- صفوان المبيضين. (2011). *الحكومة الإلكترونية: النماذج و التطبيقات و التجارب الدولية*. الأردن: دار اليازوري للنشر و التوزيع.
- صليحة جوزي. (مارس، 2018). الجرائم المستخدمة نقمة التطور التكنولوجي. *مجلة الشرطة*(140)، 124-132.
- عامر ابراهيم قنديلجي. (2015). *الحكومة الإلكترونية*. الأردن: دار المسيرة للنشر و التوزيع.
- عبد العالي غيشي. (2016). تقييم جودة خدمات الحكومة الإلكترونية من منظور تسويقي(أطروحة دكتوراه). كلية العلوم الاقتصادية و العلوم التجارية و علوم التسيير، الجزائر: جامعة الجزائر3.
- عبد اللطيف باري. (2014). دور مكانة الحكومة الإلكترونية في الأنظمة السياسية المقارنة(اطروحة دكتوراه). كلية الحقوق و العلوم السياسية، بسكرة: جامعة محمد خيضر.
- عصام عبد الفتاح مطر. (2013). *الحكومة الإلكترونية بين النظرية و التطبيق*. مصر: دار الجامعة الجديدة.
- علاء الحمامي، و غصون السعدون. (2016). *تطبيقات تكنولوجيا المعلومات في الأعمال الإلكترونية المتطورة*. الأردن: دار وائل للنشر و التوزيع.
- فتيحة الجوزي، و صفية العمري. (2017). استراتيجيات التحول الناجح نحو الحكومة الإلكترونية في الدول العربية بين واقع التحقيق و تحديات التطبيق. *الملتقى الدولي حول متطلبات و تحديات إرساء الحكومة الإلكترونية في الجزائر على ضوء التجارب العالمية*. خميس مليانة: جامعة الجيلالي بونعامة.
- فضيلة عاقلي. (2017). الجريمة الإلكترونية و إجراءات مواجهتها من خلال التشريع الجزائري. *المؤتمر الدولي حول الجرائم الإلكترونية*. لبنان: مركز جيل البحث العلمي.
- كريمة فرحي. (ديسمبر، 2013). الحكومة الإلكترونية في الوطن العربي بين التطبيق و التحديات. *مجلة معارف، 8*(15)، الصفحات 91-120.
- ليندة بوسيف. (جوان، 2017). آليات و سبل مكافحة الجريمة الإلكترونية. *مجلة الاتصال و الصحافة، 4*(2)، الصفحات 228-240.
- محمد براق، و نور الدين كروش. (2013). الحكومة الإلكترونية: المفاهيم و آليات التطبيق على أرض الواقع. *الملتقى الدولي حول متطلبات إرساء الحكومة الإلكترونية في الجزائر: تجارب بعض الدول* (صفحة 3). البليدة: جامعة سعد دحلب.
- محمد زكري. (2019). نشاة الجريمة المعلوماتية من بداية الستينات إلى القرن 21. *مجلة الشرطة العلمية و التقنية*، 6-9.
- محمد مزاولي. (جوان، 2017). المعالجة التشريعية للجريمة الرقمية في القانون الجزائري. *مجلة الحقيقة، 16*(43)، الصفحات 311-348.
- محمد يحياوي. (ماي، 2013). الحكومة الإلكترونية كأداة لتبسيط الإجراءات الإدارية : الجزائر نموذجا(أطروحة دكتوراه). كلية العلوم الاقتصادية و علوم التسيير، الجزائر: جامعة الجزائر 3.
- نسيمة لعرج مجاهد، و مصطفى طويطي. (جوان، 2016). استراتيجية إقامة الحكومة الإلكترونية : المحاولة الجزائرية. *مجلة ميلاف للبحوث و الدراسات، 1*(1)، الصفحات 205-226.
- ياسمينة بونعارة. (جوان، 2015). الجريمة الإلكترونية. *مجلة المعيار، 20*(39)، الصفحات 273-314.
- يحي بن محمد أبو مغايض. (2009). رؤية مستقبلية لدور الحكومة الإلكترونية في مواجهة الجريمة المعاصرة. *الملتقى الدولي حول الجريمة الإلكترونية : التحديات الأمنية*. الرياض: كلية الملك فهد الأمنية.