نحو إطار تشريعي لتبني نظام رقمنة الإدارات في الجزائر

Towards a legislative framework to adopt a system of digitization of administrations in Algeria.

عائشة عبد الحميد

Aicha AbdelHamid

جامعة الشادلي بن جديد. الطارف (الجزائر)

الإيميل المهني: draicha614@gmail.com

ملخص:

مع التطور التكنولوجي الكبير، وثورة المعلومات الهائلة ظهر توجه نحو تحويل المدن التقليدية لمدن ذكية، وهو اصطلاح شامل، لوسائل تطوير المدن و إدارتها عبر التقنيات الحديثة. مما يحسن من وجود الحياة فيها، وسيحسن من ظروفها الاجتماعية والمعيشية بشكل عام.

ولا شك أنه كلما زاد الاستخدام التكنولوجي و الارتباط بشبكات الحاسوب و الإنترنت، زاد احتمال حدوث محاولات الاختراق وتخريب وإتلاف البيانات، وبالتالي يكون بحاجة ماسة للأمن السيبراني لحماية تلك الأنظمة الذكية من محاولات الاختراق. فعلى سبيل المثال قد يحدث توقف في نظام المرور الذكي، أو هجوم على شبكات الكهرباء أو شبكات المياه.

حيث تهدف الدراسة إلى إماطة اللثام عن أهمية الأمن الالكتروني الرقمي أو السيبراني للمدن الذكية، وكيف عالج المشرع الجزائري أبعاد الأمن و الدفاع السيبراني.

نسلط الضوء على الموضوع من خلال المنهج التحليلي والمنهج الوصفي.

الكلمات المفتاحية: المدن الذكية؛ الأمن الالكتروني؛ الإجرام السيبراني؛ التجربة الجزائرية؛ الأمن والدفاع السيبراني.

Abstract:

With the great technological development and the massive information revolution, a trend has emerged towards transforming traditional cities into smart cities, which is a comprehensive convention for the means of developing and managing cities through modern technologies. This improves the existence of life in it, which will improve its social and living conditions in general.

There is no doubt that the greater the technological use and connection to computer networks and the Internet, the greater the probability of hacking attempts, sabotage and data destruction, and therefore the urgent need for cyber security to protect those smart systems from hacking attempts.

For example, there may be a breakdown in the smart traffic system, or an attack on electricity or water networks.

The study aims to unveil the importance of cyber security or cyber for smart cities, and how the Algerian legislator addressed the dimensions of cyber security and defense.

We highlight the topic through the analytical and descriptive approach.

key words: Smart cities, electronic security, cybercrime, Algerian experience, cyber security and defense.

المؤلف المرسل: عائشة عبد الحميد، **الإيميل:** draicha614@mail.com

1. مقدمة :

في النصف الثاني من تسعينات القرن العشرين ، بدأت مشاريع إنشاء الحكومة الإلكترونية في العديد من الدول المتقدمة، أما بالنسبة للدول العربية، فقد بدأت تظهر بوادر التجارب الأولى في بداية القرن الحادي والعشرين وهذا في كل من مصر، إمارة دبي، الأردن، وسرعان ما أقنعت الدول العربية بمميزات وفوائد هذا المشروع، مما دفعها إلى تبني الفكرة .

حيث أن الحكومة الإلكترونية هي النسخة الإفتراضية عن الحكومة الحقيقية التقليدية ، مع وجود فارق، أن الأولى تعيض في الشبكات الإلكترونية و أنظمة المعلوماتية ، في حين تحاكي وظائف الثانية التي تتواجد بشكل مادي في أجهزة الدولة، حيث تتميز الحكومة الإلكترونية عن الحكومة الغير الإلكترونية بمجموعة من المميزات وهي:

- إدارة بلا ورق : حيث تتكون من الأرشيف الإلكتروني والبريد الالكتروني والأدلة والمفكرات الالكترونية والرسائل الصوتية ونظم تطبيقات المتابعة الآلية .
- إدارة بالإمكان : وتتمثل في التلفون المحمول والتلفون الدولي الجديد (التليديسك)، والمؤثرات الإلكترونية والعمل عن بعد من خلال المؤسسات التخيلية .
- إدارة بلا زمان : تستمر 24 ساعة متواصلة، وفكرة الليل والنهار والصيف والشتاء، وهي أفكار لم يعدلها مكان في العالم الجديد.
- إدارة بلا تنظيمات جامدة : وهي تعمل من خلال المؤسسات الشبكية والمؤسسات الذكية التي تعتمد على صناعة المعرفة . [1]

في ظل التوجه الدولي نحو الحكومة الالكترونية ، أصبحت قضية الأمن المعلوماتي السيبراني من التحديات الكبرى على الصعيدين الإقليمي و الدولي ، لاسيما مع تزايد التهديدات الأمنية الإلكترونية.

والجزائر كغيرها من الدول سعت من انتهاجها للإدارة الالكترونية حماية منظومتها المعلوماتية من خلال العديد من الأجهزة والخلايا الأمنية.

لقد أضحى الأمن المعلوماتي (السيبراني) ركنا أساسيا ضمن المنظومة الأمنية المعاصرة، والتي تجب على الدفاع الوطني من خلال أجهزته كالدرك الوطني الجزائري، باعتباره مسؤول أمني داخلي في ظل تنامي الجريمة الرقمية.

فرغم الإيجابيات التي حملتها الانترنيت، إلا أنها حملت معها العديد من التهديدات والمخاطر التي ترجمت في شكل جرائم إلكترونية،وهي لا تفرق بين الأشخاص والمؤسسات والدول، بل قد تطال هذه التهديدات أيضا أمن واستقرار الدول فإذا لا أحد ينكر الدور المتعاظم لشبكة الإنترنت في الثورات العربية.

فما هو الإطار القانوني للمدن الذكية طبقا للتشريع الجزائري؟ ومادام الرابط بين المدن الذكية والرقمية هو الأمن الالكتروني وحماية المعطيات الآلية فكيف عالج التشريع الجزائري هذه المعضلة؟

2. التوجه نحو الإدارة الإلكترونية تشريعيا

تعزز المدن الذكية فضاء معرفي يستعين بالتكنولوجيا في كل مجالاته وبهذا خدماته ترضي مواطنيه وتغرز فيهم قيم الانتماء، مواكبة العنصرية والحداثة من خلال التخطيط والاستشراف واليقظة في كل المجالات لتكون فضاء التعايش السلمي.

وكانت دولة الإمارات العربية المتحدة سباقة للتخطيط لصناعة مدينة ذكية تنافس المدن العالمية الأخرى وأولى مبادراتها كانت في دبي سنة 2007 لتليها بعض الدول العربية.[2]على العموم تستشرف المدن الذكية مستقبلها على كل الأصعدة و غايتها توفير بيئة رقمية محفزة للإبداع والتعلم.

إن أول من استخدم مصطلح المدينة الرقمية أو الذكية في المؤتمر الأوربي للمدينة الرقمية في عام 1994، وفي عام 1996 دشن الأوروبيون مشروع المدينة الرقمية الأوروبية في عدد من المدن الأوروبية، و التي لاقت نجاحا متواضعا، ثم تبنت السلطات الأوروبية بشكل أساسي مدينة أمستردام كمدينة رقمية ثم تلتها مدينة هلسنكي و في الولايات المتحدة الأمريكية برزت عدة محاولات لإعلان بعض المدن كمدينة رقمية إلا أن معظمها أخذ الطابع التجاري و ليس الطابع المدني الشامل للمدينة.[3]

حيث بعد دولة الإمارات العربية المتحدة أحد الدول التي حفر اسمها في تاريخ تطبيقات تقنية الحاسوب المتقدمة وتحديدا في مجالات الذكاء الاصطناعي، فقد اعتمدت عدم انتظار المستقبل بل الدخول إليه والتنافس على تقنياته واستباق تحدياته ووضع الحلول الناجحة لها وهذا ما يفسر توجه الدولة الحديثة نحو الاستثمار في تفعيل تقنيات الجيل الرابع من الثورة الاصطناعية وعلى رأسها الذكاء الاصطناعي.[4]

1.2 المقصود بالمدن الذكية:

المدينة الذكية يبدأ قوامها من الشبكات المعلوماتية أولا ومن المباني الذكية التي تستخدم التكنولوجيا القائمة على استخدام المشغلات الذاتية المصغرة في نظم التحكم والسيطرة، وهي تشمل على تكنولوجيا الاستخدام الكفء للطاقة من خلال التحكم.[5]

ويقصد بالمدينة الرقمية الذكية تلك التي تقوم على معاملات شبكية بسيطة، يعيش فيها الأفراد رفاهية اجتماعية واقتصادية وتنمية محلية في جميع المجالات من نقل وصحة وتعليم وترفيه، بالاعتماد على معاملات رقمية مبتكرة، وهذا من خلال تكنولوجيا المعلومات والاتصالات كأداة لتحسين المدينة وجعل الخدمات الحضرية والتنقل للمدينة أكثر فعالية وكفاءة.[6]

إن تطور مفهوم ومصطلح المدينة، بالموازاة مع هذا التطور التكنولوجي الحاصل، بحيث ظهرت تسميات مختلفة لها فسميت بالمدن الرقمية والمدن الذكية والمدن الإلكترونية وكذلك بالمدن الإفتراضية والمدن المعرفية وتتميز عن غيرها كونها تتصف بمجموعة من المميزات كالإبداع والابتكار والقدرة على معالجة المشاكل.[7]

لقد وردت عدت تعريفات للمدينة الذكية Smart cities و يرجع ذلك بالدرجة الأولى إلى المفهوم المستحدث لهذا النوع من المدن، و لكن يمكن القول أن المدينة الذكية هي المدينة التي تعتمد في خدماتها على البنية التحتية لتكنولوجيا المعلومات و الاتصالات كأدلة المرور الذكية التي تدار آليا و خدمات إدارة الأمن المتطورة، و أنظمة سير المباني، واستخدام التسهيل الآلي في المنازل و مكاتب العمل.[8]

يجب التنويه على هذا الصدد إلى وجوب التفرقة بين المصطلحات:

هناك مصطلح المدينة الذكية يشترك فيه مصطلحين باللغة الإنجليزية هما: Smart city يركز على التقنيات المستخدمة أو أجهزة الاستشعار و وسائل الإعلام التفاعلية. أما مصطلح Intelligent city فهو يعني الذكاء الجماعي والتعاوني والأنظمة الإبداعية.[9]

2.2 التجربة الجزائرية:

لن تتخلف الدولة الجزائرية عن ركب التطور التكنولوجي الذي اجتاح العالم، بحيث أطلقت مشروعا جديدا عرف باسم: "الجزائر مدينة ذكية" و يهدف المشروع إلى تحسين إدارة العاصمة اشتراك مختلف الجهات و المصالح، كمصالح النقل و الطاقة و العمران، و الأمن و الصحة و غيرها...[10] فمن خلال هذا المشروع تسعى الدولة الجزائرية إلى تحسين إدارات مدنها و ذلك عن طريق استعمال و استغلال التكنولوجيا بهدف تطوير الخدمات المقدمة لمواطنيها.[11]

و في هذا الصدد عقدت يومي 27 و 28 جوان 2018، قمة دولية بالجزائر العاصمة، حول مشروع: "الجزائر، مدينة ذكية" و كانت بعنوان: "مدينة ذكية" بحيث شارك فيها أزيد من 4000 مشارك من ضمنهم 900 طالب أجنبي و 15 مؤسسة دولية.[12]

لقد أصبحت المدن الذكية تجربة رائدة في العالم الواقعي والإفتراضي لما جاءت به من تقنيات ووسائل متطورة جدا في المجال التكنولوجي، و لما أسهمت من خلاله في تحقيق الأهداف التي لم تستطيع الوصول إليها المدن التقليدية في جميع المجالات الاقتصادية والاجتماعية و الثقافية بل و حتى على مستوى الجانب الأمني.

فالتطور التكنولوجي و بالرغم من كل ما جاء به من إيجابيات و مزايا سهلت حياة الأفراد بشكل خاص، وعززت حقوق الإنسان و حرياته الأساسية بشكل عام، إلا أنه انطوى على عدة جوانب سلبيته أثرت بشكل أساسي، ومباشر على الحرية الشخصية إذ أظهرت جراثيم لم تكن مألوفة فيما مضى، ارتبطت بالأساس بوسائل التكنولوجيا المعاصرة والتي انتهكت الحقوق الأساسية للمواطنين بشكل صارخ كحق سرية المعلومات الشخصية، ورغبة منها في التصدي لظاهرة الإجرام الإلكتروني و ما يصاحبها من أضرار جسيمة على الأفراد والمؤسسات، عمدت الدولة الجزائرية إلى وضع العديد من الآليات والقوانين الوطنية والتشريعات العقابية.[13]

ويعد التوجه نحو تبني مدن ذكية في المجتمع الجزائري أحد أهم الآليات التي تعتمد من خلالها الدولة الجزائرية لحماية حقوق مواطنيها من أخطار الجرائم المعلوماتية.[14]

حيث يعد الأمن المعلوماتي أحد الركائز الأساسية التي هي من المبادئ الرئيسية في أمن المعلومات وبالتالي يصبح من الضروري في قيام المدن الذكية هو حمايتها في مواجهة الجرائم الالكترونية أو الجرائم السيبرانية [15]

وتشمل هذه الطائفة من الجرائم قطاعا واسعا بحيث تضم كافة جرائم تعطيل الأعمال الحكومية. أو تعطيل تنفيذ القانون أو تهديد السلامة العامة ويشمل ذلك، الإرهاب الالكتروني، أنشطة التدمير والاختراق الالكتروني[16]

تعد فكرة المدينة الذكية مصطلح فريد ولذلك نجد عدة مصطلحات إما تدل عليه أو تتقاطع معه منها:

- **تعريف المدينة الرقمية:** أول ما استخدم مصطلح المدينة الرقمية في المؤتمر الأوربي للمدينة الرقمية وفي عام 1996، دشن الأوروبيون مدينة أمستردام كمدينة رقمية و تلتها مدينة هلسنكي.[17]

وتعرف المدينة الرقمية على أنها: محاكاة شاملة تعتمد على تقنية الشبكة العنكبوتية لتنفيذ الوظائف الاعتيادية لقاطني المدن بطريقة الكترونية وينفذها أشخاص طبيعيون على مدينة عادية.[18]

- **المدينة الالكترونية:** هي المدينة التي تقدم الخدمات والمعلومات الكترونيا وبكل شفافية ومساواة وسرعة متناهية.[19]
- **المدينة الافتراضية:** نظير افتراضي للمدينة الاعتيادية، يؤدي فيها كل من السكان والهيئات نشاطاتهم بشكل غير مباشر، عبر تقنيات الوسائط الرقمية افتراضيا، و من دون الحاجة إلى التواجد الشخصي، وتكون المدن الافتراضية على شكل مواقع الكترونية.[20]

3.2 تكييف المنظومة التشريعية الجزائرية مع متطلبات المدينة الذكية:

يتطلب الإنتقال إلى المدن الذكية توفير الأسس القانونية، التي تتمثل في إصدار القوانين و التشريعات الضرورية لمواكبة هذه التطورات، حيث يتطلب الاعتماد المتزايد على التقنيات و نمو التعاملات الالكترونية، وضع عدد من القوانين الخاصة بإتمام عمليات التجارة إلكترونيا تساعد على المساواة بين التعاملات الورقية و التعاملات الالكترونية، بالإضافة إلى قوانين حماية الخصوصية، حيث تظهر ضرورة سن قوانين حماية أمن و سرية المعاملات، بالإضافة إلى القوانين المنظمة لحماية الملكية الفكرية و القوانين المنظمة للتوقيع الالكتروني.[21]

وقد صدرت عدة قوانين و مراسيم تواكب هذا الانتقال وهي:

- القانون رقم 18-04 المؤرخ في 10 ماي 2018،[22]الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية.
- القانون رقم 18-05 المؤرخ في 10 ماي 2018، [23]المتعلق بالتجارة الالكترونية.
- القانون رقم 18-07 المؤرخ في 10 جوان 2018،[24]المتعلق بحماية الأشخاص الطبيعية في مجال معالجة المعطيات ذات الطابع الشخصي.
- القانون رقم 18-08 المؤرخ في 10 جوان 2018، و الذي يعدل القانون رقم 04-08 [25] المتعلق بشروط ممارسة الأنشطة التجارية.
- القانون رقم 15-03 المؤرخ في 01 فيفري 2018 يتعلق بعصرنة العدالة.[26]
- القانون رقم 15-04 المؤرخ في 01 فيفري 2018 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني.[27]
- القانون رقم 09-04 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.[28]
- القانون رقم 04-09 المؤرخ في 14 أوت 2014 يتعلق بترقية الطاقات المتجددة في اطار التنمية المستدامة.[29]

أما من مشروع البلدية الالكترونية، فقد دشنت أول بلدية الكترونية جزائرية يوم 14 مارس 2011، بالمقر الفرعي الإداري حي 500 مسكن بباتنة، أصدرت أول شهادة ميلاد (12 خ) في بضع ثوان على مستوى الشباك الالكتروني، كما تم أيضا إصدار الوثائق البيومترية في إطار تحسين الخدمة الالكترونية المقدمة للمواطن، وأعلنت وزارة الداخلية الجزائرية عن إنطلاق إصدار الوثائق الالكترونية المتمثلة في جواز السفر البيومتري وبطاقة التعريف البيومترية.[30]

3. تطور نظام الدفاع السيبراني للمعطيات الإلكترونية

لقد وضعت قيادة الدفاع الوطني الأمن السيبراني أحد أولوياتها على غرار باقي دول العالم التي سارعت إلى مراجعة سياستها الأمنية، وإدراجها لآليات وميكانيزمات جديدة تعني بهذه الوسائل، حيث يفرض الأمن مضاعفة أنظمة الرقابة التي تشكل تهديدا ممكنا للحريات الفردية، ولهذا وجب مرافقة كل المقاربات الأمنية في مجال الأمن الرقمي للأطر القانونية والتكنولوجية الملائمة، وتأخذ بعين الاعتبار الهجمات الالكترونية وتعقيباتها والتي يزداد خطرها مع التطور التكنولوجي واستخداماتها اليومية.[31]

وتجسيدا لذلك باشرت الدولة الجزائرية و في مقدمتها مؤسسة الدفاع الوطني إلى إعداد برامج خاصة لمجابهة الجريمة الالكترونية و الحد من انتشارها، و إنشاء أجهزة جديدة تنسجم في أدائها مع المتغيرات الحاصلة في هذا المجال، إذ أصبحت الحماية السيبرانية جزءا مهما في أي منظومة دفاع، و قد استطاع الجيش الوطني الشعبي المضي قدما و مسايرة التطورات التكنولوجية و الإعلامية الحاصلة في العالم،و من ثم تأمين و حماية نطاقه المعلوماتي، وتأمين الفضاء المعلوماتي.[32]

1.3 النصوص القانونية:

- **قانون العقوبات 04-15:**[33]

استدرك المشروع الجزائري في السنوات الأخيرة و لو متأخرا الفراغ القانوني في مجال الجريمة الالكترونية، و ذلك لما أصدر القانون رقم 04-15 الذي يتضمن تعديل قانون العقوبات، حيث خصص قسمه السابع مكرر للمساس بأنظمة المعالجة الآلية

للمعطيات وتضمن ثمانية مواد، إذ تتعلق المادة 394 مكرر بمعاقبة كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، أما المادة 394 مكرر ، فتنص على معاقبة كل من أدخل بطريق الغش معطيات في نظام المعالجة أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها، كما قامت المادة 394 مكرر 2 على معاقبة كل من يقوم عمدا بالغش الالكتروني.

أما المادة 394 مكرر 3 فإنها تعاقب بعقوبة مضاعفة، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد.

- **قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها: وهو القانون 09-04:**[34]

وقد استهل بالهدف الأسمى منه وهو الوقاية من الجريمة المعلوماتية، وقامت المادة 02 منه بتوضيح المفاهيم التالية:

- الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: وهي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو سهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.
- منظومة معلوماتية: هي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض، يقوم بها واحد منها أو أكثر لمعالجة المعطيات.
- معطيات معلوماتية: أي عملية عرض الوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية
- مقدمو الخدمات: أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و / أو نظام الاتصالات.
- الاتصالات الالكترونية:أي تراسل أو إرسال أو استقبال أو علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة باسطة أي وسيلة الكترونية.[35]

2.3 الأمن السيبراني و الدفاع السيبراني:

إن مفهوم الأمن السيبراني هو مفهوم شامل يشمل مجموعة من الوسائل و الآليات التقنية و التنظيمية و الإدارية التي يتم استخدامها لمنع أي تدخل أو عمليات غير مصرح بها و استعادة البيانات و نظم المعلومات الإلكترونية التي تحتويها و حمايتها و ضمان توافرها و استمرارية عملها. تجدر الإشارة إلى أنه لا يوجد لحد اليوم أداة قانونية دولية في إطار منظمة الأمم المتحدة خاصة بمكافحة الجرائم السيبرانية، بحيث تبقى اتفاقية بودابيست (23 نوفمبر 2001) و التي دخلت حيز التنفيذ في جويلية 2004، الإطار القانوني الدولي الوحيد لمكافحة هذا النوع من الجريمة بعد أن حظيت بمصادقة أغلبية حول المجلس الأوروبي، مع العلم أنه يتم صياغة بروتوكول تكميلي ثان ليلحق بهذه الاتفاقية منذ سبتمبر 2017، و من المتوقع أن يصدر سنة 2019.

بالإضافة إلى اتفاقية الإتحاد الإفريقي حول الأمن السيبراني بتاريخ 27 جوان 2014 وفي إطار مسار الرقمنة الإفريقية تجسد ذلك خلال قمته الـ 23 التي انعقدت بمالابو بجمهورية غينيا الاستوائية، اتفاقية حول الأمن السيبراني حيث تعكس معاهدة "مالابو" درجة الوعي الدول الإفريقية بالخطر الذي يهددها، بحيث حرصت دول الاتحاد الإفريقي على تحسين قوانينها وتشريعاتها الإقليمية في مجال الأمن السيبراني ومن أهمها:

- القرار شأن تكنولوجيا الإعلام والاتصال في إفريقيا، التحديات والآفاق (2010)
- إعلان "أليفرتامبو" بجوهانسبورغ بتاريخ 09 نوفمبر 2019.
- إعلان أبيذجان بتاريخ 22 فيفري 2012.
- إعلان أديس أبابا الصادر في 22 جوان 2012. [36]

كما نجد أن المشرع الجزائري قد اتخذ جملة من الإجراءات اللازمة من أجل مقاومة الجريمة الإلكترونية، المنصوص عليها في الاتفاقية الأورو متوسطية المبرمة في 22 أفريل 2002.[37] و التي كانت تهدف إلى ربط الجهود بين مجموعة الوحدة الأوروبية، و الدول الأعضاء فيها من جهة، و ما بين الحكومة الجزائرية منت جهة أخرى، و قد صادقت

الجزائر على إتفاقية مع فرنسا في مجال مكافحة الإجرام المنظم و ذلك بتاريخ 2003/10/25، و قد دخلت حيز التنفيذ بموجب المرسوم الرئاسي رقم 08-375 .[38]

حيث تواجه البشرية تهديدات رقمية جديدة أكثر تعقيدا، و أشد فتكا و ضررا، تتسبب في إتلاف منظومات شبكات الكمبيوتر لمؤسسات كبيرة و حساسة داخل الدول التي لا زالت غير أمنة، فقد أصبح التجسس الصناعي والتجاري على مواقعها الإستراتيجية و سرقة بياناتها الحساسة و الموضوعة، في خانة "سري للغاية"، أمرا شائعا، حيث نشأ جيل جديد من الهجمات الالكترونية الموجهة و المعقدة حيث يمتد الدفاع السيبراني إلى أبعد من مجرد العمل على سلامة و أمن الحواسيب، ليصل إلى الحد الذي يكون له تأثير مباشر على الأمن القومي وبالتالي العمل عن الدفاع على مختلف النظم الالكترونية الخاصة بالدولة، وما تواجهه من حرب الكترونية، كما يسمح الدفاع السيبراني بالتصدي للتهديدات المتصلة بالشبكات و الأجهزة الرقمية الحساسة للمؤسسات الكبرى حيث يرتكز الدفاع السيبراني على الحماية و الدفاع الفعال لمنظومة المعلومات إلى جانب اعتمادها على قدرتها على إدارة الأزمات السيبرانية ودعم الالتزامات الدولية فيما يخص الأمن الالكتروني.[39]

3.3 مجالات إجازة الخرق الالكتروني للمعلومات:

لقد جاءت المادة 03 من القانون رقم: 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها: لتوضح مجال تطبيق القانون، كيف؟ لقد أشارت إلى أنه ومع مراعاة الأحكام القانونية التي تتضمن سرية المراسلات والاتصالات، إلا أنه ووفقا لمقتضيات الأمن العام وحماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية وفقا لقواعد المنصوص عليها في قانون الإجراءات الجزائية الجزائري.[40] يمكن وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية و تجميع وتسجيل محتواها في حينها و القيام بإجراءات التفتيش و المعاينة و الحجز داخل المنظومة المعلوماتية و قد بين المشرع الجزائري في المادة الرابعة من هذا القانون الحالات التي يسمح فيها باللجوء إلى المراقبة الالكترونية و حددها كما يلي:

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب 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 الالكترونية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة وقد أكد المشرع الجزائري على أنه لا يمكن إجراء عمليات المراقبة في الحالات المذكورة سابقا إلا بإذن مكتوب من السلطة القضائية المختصة.

وقد حدد أنه في الحالة الواردة في البند – أ –فإن الإذن يكون من النائب العام لدى مجلس قضاء الجزائر.

كما أجازت المادة الخامسة من نفس القانون الدخول للتفتيش،ولو عن بعد إلى منظومة معلوماتية أو جزء منها والمعطيات المعلوماتية المخزنة فيها.

كما نصت المادة السادسة على حجز المعطيات التي تخدم التحقق وضرورة السهر على سلامتها، مع التشديد على ضرورة استعمالها في الحدود الضرورية للتحريات والتحقيقات القضائية.

وقد عدل قانون الإجراءات الجزائية بموجب القانون رقم 19-10 المعدل للأمر 66-155 والذي يعزز أداء الشرطة القضائية، حيث يوسع صلاحيات ومهام ضباط الشرطة القضائية، التابعين للمصالح العسكرية للأمن خلال إلغاء المادة 15 مكرر من قانون الإجراءات الجزائية التي حصرت مهام المصالح العسكرية للأمن في جرائم المساس بأمن الدولة حيث تنص المادة 02 من القانون الصادر بالجريدة الرسمية إلى تعديل المواد 15 و19 و207، من الأمر 66-155 المؤرخ في 08 يونيو 1966.

4.3 الأجهزة المخولة بضبط جرائم الأمن الالكتروني: أو الأجهزة العملياتية:

ويتمثل في المركز والوحدات التي أنشأت لغرض مواجهة الجريمة الالكترونية ومدى استعدادها لأدائها والمتمثلة في:

4.3.1 الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته:

تضمنها الفصل الخامس من القانون رقم 09-04، و قد تشكلت الهيئة بموجب المرسوم الرئاسي 15- 2016 [(41)] وهي سلطة إدارية مستقلة لدى وزير العدل، تعمل تحت إشراف و مراقبة لجنة مديرة يترأسها وزير العدل، وتضم أعضاء من الحكومة معينين بالموضوع و مسئولي مصالح الأمن وقاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

وتضم الهيئة قضاة وضباط وأعوان من الشرطة القضائية العسكرية والدرك الوطني والأمن الوطني وفقا لأحكام قانون الإجراءات الجزائية.

حيث تعمل على التنسيق بين مختلف الأجهزة على الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ومكافحتها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة هذه الجرائم، وضمان المراقبة الوقائية للاتصالات الإلكترونية، قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة.

4.3.2 مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني:

لقد أنشأ سنة 2008، ويعتبر الجهاز الوحيد المختص بهذا الصدد في الجزائر، ويهدف إلى تأمين منظومة المعلومات لخدمة الأمن العمومي، واعتبر بمثابة مركز توثيق ومقره يوجد في بئر مراد رايس بالجزائر العاصمة ويهدف هذا المركز إلى تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة وتحديد هوية أصحابها. سواء كانوا أفرادا أو جماعات، كما يهدف الى مساعدة باحث الأجهزة الأمنية الأخرى في أداء مهامها، واستطاعت قيادة الدرك الوطني من خلال التكوين المستمر والمتميز لأفرادها وتبادل الخبرات مع دول أخرى.

4.3.3 الهيئات القضائية الجزائية المتخصصة:[42]

والمتمثلة في الأقطاب القضائية الجزائية المتخصصة و التي تم إنشاؤها بموجب القانون [43] 14/04 كما تختص بالنظر في القضايا المتعلقة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد 37-40-329، و من قانون الإجراءات الجزائية الجزائري، هذه من جهة أما في ما يتعلق بالاختصاص الإقليمي للأقطاب المتخصصة [44]فانه يمكن النظر في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال، و المرتكبة خارج الوطن و حتى و لو كان مرتكبها أجنبيا، لكن في حالة ما إذا كانت تستهدف مؤسسات الدولة أو مؤسسات الدفاع الوطني.

4.3.4 المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:[45]

هو مؤسسة عمومية ذات طابع إداري تحت الوصاية المباشرة الوزير الدفاع الوطني فهو مكلف بالبحث والتحري في مجال الإجرام و الأدلة الجنائية على الصعيدين الوطني والدولي، و لأداء مهامه على أكمل وجه فإن المعهد الوطني للأدلة الجنائية و علم الإجرام يحتوي على العديد من المصالح المختصة من أهمها:

- مصلحة البصمات: يتم على مستوى هذه المصلحة مقارنة البصمات للتعرف على الجثث، وتجدر الإشارة إلى أن الدرك الجزائري مجهز بأنظمة التعرف الآلي على البصمات
(AFIS : The Automated Fingerprint Identification System)
- مصلحة الوثائق في هذه المصلحة يتم التأكد من صحة الوثائق والإمضاءات والتحقق من النقود وكذلك التأكد من صحة الوثائق السرية.
- مصلحة الإعلام الآلي: على مستوى هذه المصلحة تم رصد و مراقبة و تتبع عمليات الإختراق والقرصنة المعلوماتية، و كذا اكتشاف المعلومات المسروقة، وتفكيك البرامج المعلوماتية.

- مصلحة البيئة: تهدف هذه المصلحة على عمليات البحث في أسباب التلوث المياه والتربة و كذا الكشف عن المواد السامة المتواجدة في المحيط.
- المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني (DGSN) استجابة لطلب الأمن المعلوماتي و محاربة التهديدات الأمنية الناجم عن الجرائم الالكترونية قامت مصالح الأمن الجزائري بإنشاء المصلحة المركزية للجرعة الالكترونية، التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية، وقد أنشأت سنة 2011، ليتم بعدها إنشاء المصلحة المركزية بقرار من المدير العام للأمن الوطني و أضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015.

وقد صادقت الجزائر على اتفاقية عربية لمكافحة الجرائم المعلوماتية سنة 2014.[46]

حيث تصدت المديرية العامة للأمن الوطني لمختلف أنواع الجرائم الالكترونية والمتمثلة في:

- **الجانب القانوني:** و يتمثل في جملة من القوانين من بينها: القانون 06-22 المعدل و المتمم لقانون الإجراءات الجزائية. و القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و لاتصال ومكافحتها، و قانون العقوبات بموجب المواد من 394 مكرر إلى 394 مكرر 7.
- **الجانب التنظيمي:** يتمثل في: التكوين المتواصل و تدعيم مخابر الشرطة العلمية.[47]

4.3.5 مصلحة الدفاع السيبراني و مراقبة الأنظمة:

قررت القيادة العليا للجيش الوطني الشعبي، استحداث مصلحة "الدفاع السيبراني" ومراقبة أمن الأنظمة على مستوى دائرة الاستعمال و التجهيز لأركان الجيش بهدف تأمين وحماية المنظومات والمنشآت الحيوية للبلاد، ضد التهديدات و الإرهاب الالكتروني والجوسسة على أسرار الدولة الجزائرية[48]. حيث نبهت المؤسسة العسكرية إلى

ضرورة إيلاء أهمية مختلف القطاعات أو ما يعرف بالأمن السيبراني وحذرت مختلف القطاعات في الجزائر من التهديدات التي يمثلها، التطور المتسارع للتكنولوجيا الجديدة والإعلام والاتصال، بعد النجاحات التي حققها ذات الجهاز الأمني في محاربة الإرهاب على الميدان وتشديد الخناق على عصابات الجريمة المنظمة على الحدود، جاء الدور على الفضاء الافتراضي، فمن واجب الدولة اتخاذ الإجراءات اللازمة لإحباط أي هجوم من شأنه تهديد أمنها وسيادتها و مؤسساتها و أمن مواطنيها، وأضافت أن التطور المتسارع الذي تشهده الجزائر في مجال التكنولوجيا الجديدة للأعلام و الاتصال والاستخدام المتنامي للتطبيقات المتصلة بالأنترنت والوسائط الالكترونية والرقمية الجديدة لحفظ الملفات و الصور وغيرها، يستدعي إرساء قاعدة قانونية وتوفير الأجهزة والهياكل الضرورية لمكافحة الجريمة السيبرانية العابرة للأوطان.[49] حيث تعد مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة هي تركيبة ملحقة بدائرة التحضير و الاستعمال لأركان الجيش الوطني الشعبي، فاستحداثها في نوفمبر 2015، يندرج ضمن نهج إرساء السياسة الشاملة المسطرة من قبل القيادة العليا و الهادفة إلى حماية مؤسساتها ضد المخاطر و التهديدات السيبرانية، باعتبارها جهاز للتوجيه و الخبرة على المستوى الاستراتيجي، حيث تحرص هذه المصلحة أساسا على وضع و تطبيق السياسة العامة للدفاع السيبراني في الجيش الوطني الشعبي و أيضا إلى تقييم و تعزيز مستوى آمن الأنظمة المستغلة و كذا إلى تحسين و تطبيق الإطار التنظيمي المسير مجال الدفاع السيبراني.

حيث تساهم هذه المصلحة في تعزيز السياسة الوطنية المتعلقة بالدفاع السيبراني، مع ضمان التنسيق مع مختلف الهيئات في مجال تأمين المنشآت الرقمية الحساسة.[50]

إن الأمن الوطني مفهوم شامل يتعدى الحفاظ على السياسة الإقليمية، و الاستقرار الداخلي في ظل بيئة أمنية معقدة و متشابكة، فالأمن الوطني يواجه العديد من التهديدات غير التقليدية، مثل الأوبئة، التغير المناخي، و هو ما يتطلب تشكيل الأمن الحدودي كرهان استراتيجي للسياسة الدفاع الوطني الجزائري خاصة مع طول مساحة الحدود الجزائرية. وظهور دول فاشلة أمنيا في الجوار الإقليمي للجزائر، (مالي، ليبيا، و تونس) و لحماية

المصالح الوطنية، يجب رسم إستراتيجية و أولويات و أهداف لحماية الأمن الالكتروني الجزائري ضد كل التهديدات.[51]

4. خاتمة:

تستخدم المدينة الذكية التقنيات الرقمية لتعزيز جودة وأداء الخدمات الحضرية والحد من التكاليف واستهلاك الموارد والتفاعل بشكل أكثر فعالية و نشاط مع مواطنيها، حيث يمكن تحقيق مصطلح المدينة الذكية من خلال عملية إرسال واستقبال مستمرة لأهم الأعمال والبيانات الشخصية الحيوية في مختلف المحاور والوحدات. مثل النقل الذكي، الرعاية الصحية المتصلة والسلامة العامة والأمن وخدمات الطوارئ وإدارة النفايات وقياس الشبكات الذكية بما يعزز الكفاءة والذكاء في الزمن العقلي.

يعد مفهوم المدينة الذكية مفهوم حديث للغاية، حيث تعمل العديد من المؤسسات على وضع حلول ذكية لجعل المناطق الحضرية ذات الكفاءة في استخدام الطاقة ومرعية وصديقة للبيئة ومحمية من الجرائم.

ولذلك فمن أهم الأولويات في تنفيذ مفهوم المدينة الذكية ضمان اعتماد إستراتيجية أمنية للأرضية الرقمية ومزودو الخدمات، وفي حال لم تؤخذ هذه الخطوات بجدية أثناء بناء المدينة الذكية، يمكن أن تكون العواقب وخيمة و مدمرة.

وعلى ضوء ذلك نلخص ما يلي:

1- إن المدن الذكية تعتمد بشكل أساسي و رئيسي على النظام الرقمي و الذي يقودنا مباشرة إلى ضرورة ضمان ما يعرف بالأمن السيبراني و الدفاع السيبراني.
2- حاولت الدولة الجزائرية إعطاء الأولوية بالغة للدفاع السيبراني من خلال مؤسسة الدفاع الوطني وهي القيادة العامة للجيش الوطني الشعبي.
3- تقتضي المدن الذكية الإعداد المسبق لنظام مراقباتي آلي متميز قائم على الحد والتصدي للإختراق الرقمي (الالكتروني).

ونقدم الاقتراحات التالية:

1- ترى الباحثة أن التجربة الجزائرية في مجال المدن الرقمية هي تجربة أولية من خلال ما قام به المشرع الجزائري، وقد أوجد أرضية قانونية لمختلف الجرائم الرقمية و لكن الأمر ما زال قاصرا على أنواع معينة من الاختراقات الرقمية.

2- إن المنظومة الدفاعية الجزائرية القائمة على الدفاع السيبراني هي جاءت أصلا وخصيصا لحماية السياسة العامة والمؤسسات العليا للدولة والتصدي للإرهاب الالكتروني والاختراق الرقمي للوزارات ذات الطابع السياسي مثل الداخلية والدفاع والخارجية فما مدى ضرورة امتداد هذا النظام الدفاعي إلى باقي الإدارات؟

3- نرى من وجهة نظرنا أن ضرورة الإعداد المسبق للنظم الأمنية (الأمن الالكتروني) قبل التوجه إلى المدن الالكترونية، لأن كل ما هو رقمي يتعرض للقرصنة الالكترونية.

5. التهميش:

(1) لعرج مجاهد نسيمة ، طويطلي مصطفى ، إستراتيجية إقامة الحكومة الالكترونية ، المحاولة الجزائرية ، مجلة ميلاف للبحوث والدراسات ، المركز الجامعي ، ميلة ، العدد 3 جوان 2016 ، ص209 .

(2) نصر الدين لبال، دور حوكمة في إرساء المدن المستدامة، رسالة الماجستير، جامعة قاصدي مرباح ورقلة، الجزائر، 2011-2012، ص 55.

(3)بن الطيب علي، مهلول زكرياء، تطبيقات الذكاء الاصطناعي و دورها في تعزيز رقمنة المجتمعات و التحول نحو المدن الذكية، دراسة الإمارات العربية المتحدة نموذجا، المركز الديمقراطي العربي للدراسات الإستراتيجية، و السياسة الاقتصادية، برلين، ألمانيا، ص 90.

(4)شعيب قمار، عبد العزيز صحراوي، الحكومة الالكترونية ومساعي تحقيق الأمن المعلوماتي، الإمارات العربية المتحدة نموذجا، مجلة الحقوق والعلوم السياسية، جامعة عباس لعزور، خنشلة، الجزائر، العدد 11، جانفي 2019، ص287.

(5)إبراهيم جواد آل يوسف، محمد مهدي حسين، المدن الذكية المستدامة آفاق و تطلعات على خطى مدن القرن الحادي و العشرين، جامعة التكنولوجيا، العراق، بدون س ن، ص 10.

(6)نعيمة مدان، قسول سفيان، الجزائر العاصمة مدينة ذكية كنموذج مدن الدول النامية، المركز الديمقراطي العربي للدراسات الإستراتيجية و السياسة و الاقتصادية، برلين ألمانيا 2019، ص 119.

(7)محفوظ برجماني، المدينة الذكية بين الحتمية الإدارية و الضرورة البيئية، مجلة الحقوق و العلوم الإنسانية جامعة زيان عاشور، الجلفة الجزائر، المجلد العاشر، الجزء 2 ،العدد 2، بسكرة، ص 113

(8)نعمة مدان، قسول سفيان، مقال سابق، ص 122.

(9)خلود رياض الصادق، مناهج تخطيط المدن الذكية، حالة دراسية: دمشق رسالة ماجستير، كلية الهندسة المعمارية، طبعة دمشق، الجمهورية العربية الثورية، 2013، ص 1.

(10)موقع جريدة الجزائر (eldjazair) مقال بعنوان، انطلاق مشروع، الجزائر مدينة ذكية، تاريخ الاطلاع، (20 أفريل 2020) https://eldjazair365.com

(11)موقع جريدة الجزائر، مقال بعنوان، "ولاية الجزائر تدعو الأطراف الفاعلة للاشتراك مشروع الجزائر مدينة ذكية يدخل مرحلة التنفيذ، تاريخ التصفح 01 ماي 2020. https://eldjazair365.com

(12)موقع جريدة الجزائر، مقال بعنوان، سينظم يومي 27 و 28 جوان 2018، بالعاصمة مشاركة في قصة المدينة الذكية، تاريخ التصفح، 2020/04/13.https://eldjazair365.com

(13)براهيمي جمال، مكافحة الجرائم الالكترونية، في التشريع الجزائري، المجلة النقدية، كلية الحقوق والعلوم السياسية جامعة تيزي وزو، الجزائر، العدد 2-2016، ص 2.

(14)بن حدة باديس، إستراتيجية المجلة الالكترونية في التوجه نحو تفعيل المدن الذكية، مجلة الرسالة للدراسات والبحوث والبحوث الإنسانية، جامعة العربي التبسي، تبسة، الجزائر، المجلد 1، العدد 4-2017، ص 61.

(15)منصور الصالح، أمن المعلومات على المدن الذكية، مجلة العلوم والتقنيات، الملك عبد العزيز للعلوم التقنية، الرياض، المملكة العربية السعودية، العدد 111، 2014، ص 35.

(16)عنتر أسماء، حتيالة معمر، الحماية القانونية للمدن الذكية من الجرائم الذكية، المركز الديموغرافي العربي للدراسات الإستراتيجية والسياسة والاقتصادية، برلين، ألمانيا، 2019، ص 261.

(17)نصر الدين حبال، الحوكمة المحلية في إرساء المدن المستدامة، مذكرة ماجستير، جامعة ورقلة، الجزائر، 2012، ص 460.

(18)خلود رياض صادق، مناهج تخطيط المدن الذكية حالة دراسية، دمشق، رسالة ماجستير، ص 13.

(19)بهجت رشاد شاهين و محسن جبار عودة، دور البيئة المعلوماتية في بناء المدن الذكية، مجلة الهندسة، جامعة بغداد، العدد 22-2016، ص 04.

(20)مصطفاوي عايدة، شريف هنية، إستراتيجية الانتقال إلى المدن الذكية في الجزائر، المركز الديمقراطي العربي، للدراسات الإستراتيجية و السياسية و الاقتصادية، برلين، ألمانيا، 2018، ص 159.

(21)حنان نحاس، المدن الذكية، دراسة في المفهوم و الأساس مجلة مغرب القانون، مقال منشور على الموقع التالي: https://www.mzroclaw.com ، تاريخ اطلاع 2020/06/01)

(22)القانون رقم 18-04 المؤرخ في 10 ماي 2018، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد17.

(23)القانون رقم 18-05 المؤرخ في 10 ماي 2018، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد28.

(24)القانون رقم 18-07 المؤرخ في 10 جوان 2018، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد34.

(25)القانون رقم 18-07: المؤرخ في 10 جوان 2018،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد35.

(26)القانون رقم 15-03: المؤرخ في 01 فيفري 2015،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد 06.

(27)القانون رقم 15-04: المؤرخ في 01 فيفري 2015،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد 06.

(28)القانون رقم 09-04 المؤرخ في 05 أوت 2009،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد47.

(29)القانون رقم 04-09 المؤرخ في 14 أوت 2004،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد52.

(30)حزر الله حسن، الحكومة الالكترونية في الجزائر، دراسة إمكانية التطبيق، مذكرة ماستر في السياسة، جامعة بسكرة، الجزائر، 2013، ص 104.

(31)بارة سمير، الأمن السيبراني (cyber security) في الجزائر، المجلة الجزائرية للأمن الإنساني، جامعة باتنة، الجزائر، العدد الرابع، جويلية 2017، ص264.

(32)ج. رضوان، الأمن السيبراني، أولوية في إستراتيجية الدفاع ، مجلة الجيش، العدد 630 سنة 2016، يصدرها المركز الوطني للمنشورات العسكرية، ص ص ، 40 41.

(33)قانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 يعدل الأمر رقم 66-1516 المخصص قانون العقوبات الجزائري، جريدة رسمية عدد 74 الصادرة بتاريخ 10 نوفمبر 2004، ص ص، 11 12.

(34)القانون رقم 09-15 المؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية – العدد 47-الصادرة 16 سبتمبر 2009، ص ص، 5 8.

(35)إلهام غازي، الوقاية ومكافحته الجريمة المعلوماتية في التشريع الجزائري، مجلة الجيش، العدد 630، جانفي 2016 يصدرها المركز الوطني للمنشورات العسكرية، ص 44 على الموقع الالكتروني: www.mdn.dz

(36)إسماعيل جنادي، الأمن السيبراني، التحدي القائم للاتحاد الإفريقي، مجلة الجيش العدد 663، أكتوبر 2018 ص44.

(37)الاتفاقية الأورو متوسطية المبرمة في 22 أفريل 2002.

(38)المرسوم الرئاسي 08-375 المؤرخ في 1 ديسمبر 2008، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد 77.

(39)إلهام غازي الدفاع السيبراني، مجلة الجيش، العدد 663، أكتوبر 2018 يصدرها المركز الوطني للمنشورات العسكرية، ص 47.

(40)الأمر رقم 66 – 155 المؤرخ في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية الجزائري، المعدل والمتمم.

(41)المرسوم الرئاسي، رقم 15-216، المؤرخ في 8 أكتوبر 2015، يحدد تشكيلة و تنظيم و كيفيات سر الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، جريدة رسمية عدد 53 الصادرة في 8 أكتوبر 2015، ص ص 16-20.

(42)سالم عبد الرزاق، ملتقى حول المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية بمحكمة سيدي امحمد،

القانون 14/04 المؤرخ في 2004/11/10 المعدل لقانون الإجراءات الجزائية، ص ص، 12، 14.

(43)هواري عياش، مداخلة، حول المسار التحقيقات الجزائية في مجال الجرعة المعلوماتية، المعهد الوطني للأدلة الجنائية و على الإجرام، جامع بسكرة، كلية الحقوق؟، 2016، ص 03.

(44)عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائر / الجزء الأول والجزء الثاني، دار هومة، الجزائر، 2018، ص 80.

(45)مؤسسة عمومية ذات طابع إداري تم إنشاؤه بموجب مرسوم رئاسي 04-183 المؤرخ في 26 جوان 2004، مقره مدينة بوشاوي في العاصمة الجزائر...المزيد حول الموضوع نضع تحت تصرفكم الموقع الالكتروني الآتي: https://www.mdn.dz و قد عدل نظامه الأساسي بموجب المرسوم الرئاسي 09-118 المؤرخ في 14 أفريل 2009

(46)مقال: المصلحة المركزية للجريمة الالكترونية في مواجهة مجرمي العالم الافتراضي، تشكيل أمني مختص للردع و الوقاية، نشر بواسطة: منشور في جريدة السلام اليوم يوم 2016/02/13 على الموقع الالكتروني:https://www.djazairess.com

(47)حملاوي عبد الرحمان، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجريمة الالكترونية جامعة محمد خيضر، بسكرة، الجزائر، 2016، ص 02.

(48)مقال الجيش يدخل حرب القضاء الالكتروني و محاربة الجوسسة على الموقع الآتي: https://army-tech.net

(49)بوكبشة محمد، الأمن و الدفاع السيبراني، مجلة الجيش، العدد 651، أكتوبر 2017،يصدرها المركز الوطني للمنشورات العسكرية، ص 40، على الموقع www.mdn.dz

(50)غرارمي عبد الغني، الفريق أحمد قايد صالح يدشن المركز الوطني للإشارة، الحروب المستقبلية هي بالأساس حروب الكترونية، مجلة الجيش، العدد 676، نوفمبر 2019،يصدرها المركز الوطني للمنشورات العسكرية،ص 03.

(51)فيروز مزياني، إستراتيجية الدفاع الوطني الجزائري في ظل التهديدات الأمنية الجديدة، مجلة العلوم القانونية و السياسية، المجلد -10 العدد 03 ديسمبر 2019 ، ص 954.