Revue de bibliothéconomie مجلة علم المكتبات
المجلد 13 ، العدد 1 ، السنة 2021 ، ص ص . 48 – 67 .
ISSN : 1112-2803
EISSN: 2602-6589

التشريعات المُنظمة للفضاء الرقمي في الجزائر بين تحديات التقنيات والرهانات المستقبلية للبنية التحتية

Digital space legislation in Algeria between the challenges of technologies and stakes of future infrastructure

خروبي أحمد[1] العربي بن حجار ميلود[2] *
[1] كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس سيدي بلعباس (الجزائر)،
khahmed840@gmail.com
[2] كلية العلوم الإنسانية والعلوم الإسلامية، جامعة وهران 1 (الجزائر)، larbibenhadjar.miloud@univ-oran1.dz

تاريخ الاستلام:22 / 2021/04 تاريخ النشر:20 / 2021/12

Abstract
This study aims at exploring the most important legislation and laws taken to organize digital space in Algeria in order to reveal how international community and Algeria in particular deal with cybercrime and information security, and what are the measures taken to prevent cybercrime and threats as well as to cast the light upon cyber threat to the national security.
The study found that in recent years Algeria sees a great progress in developing the infrastructure of the ICT, and we find signs of technological and digital transformation through updating its legal framework and introducing a series of new systems that accompany the growing sector.

Keywords: cyber security; digital space; cybercrime; dangerous data; e-government

المستخلص
الهدف من هذه الدراسة هو الوقوف على أهم التشريعات والقوانين المتخذة من أجل تنظيم الفضاء الرقمي بالجزائر، من أجل الكشف عن كيفية التعامل الدولي والجزائر على وجه الخصوص مع الجرائم الإلكترونية والأمن المعلوماتي، وما هي الإجراءات المتخذة للتصدي للجرائم والتهديدات على الإنترنت، وتوضيح مدى التشابك للأمن الحاسوبي والتهديدات التي يتعرض لها الأمن القومي.
خلصت الدراسة إلى أن الجزائر تشهد تقدما كبيرا في تطوير البنية الرئيسة الأساسية لقطاع تكنولوجيا المعلومات والاتصالات في السنوات الأخيرة، ونجد بوادر السير نحو التحول الرقمي بدأت تتضح شيئا فشيئا من خلال تحديث إطارها القانوني وإدخال سلسلة من الأنظمة الجديدة التي تصاحب نمو القطاع.

كلمات مفتاحية: الأمن المعلوماتي؛ الفضاء الرقمي؛ الجريمة المعلوماتية؛ بيانات خطيرة؛ الحكومة الإلكترونية

المقدمة

المؤلف المراسل *[2]: العربي بن حجار ميلود ، larbibenhadjar.miloud@univ-oran1.dz

إننا نعيش عصر المعلومات الذي يتسم بانتشار الرقمنة، ما يعني ضمنيا تحولاً تكنولوجياً من التقنيات التناظرية والإلكترونية إلى التقنيات الرقمية، أي التكامل المستمر بين الاتصالات الحاسوبية والتكنولوجيات الرقمية التي تدعم كل جوانب الحياة والخدمات الحيوية للمجتمعات الحديثة والاتجاه نحو "ربط كل شيء بكل شيء "، فقد أنشئت العديد من المنصات على شبكة الإنترنت ولها فوائد كبيرة على المستخدمين والإبداع، وساعدت السوق الداخلية في العديد من الدول على اكتساب المزيد من الكفاءة.

نشوء مجتمع المعلومات غير أيضا تعريف المفاهيم التقليدية المتعلقة بالأمن السيبراني أمن البيانات والحواسيب وتقنيات الاتصالات الرقمية، كون التحديات الأكثر خطورة التي تواجهه هو كيفية منع إساءة استخدام اتصالات المعلومات بشكل ضار من قبل المجرمين أو الجماعات الإرهابية، وقد زاد حجم الهجوم بنسبة كبيرة بسبب عدد الأجهزة المتصلة بعضها مؤمّن بشكل ضعيف أو غير مؤمَّن بشكل كامل، وأغلبها يمتلكه مستخدمون غير مطلعين، مما جعل الجريمة السيبرانية أكثر خطورة وفي المقابل أكثر ربحية لبعض المجرمين يمكنهم شن الهجوم من أي مكان في العالم، لهذا فإن معالجة هذه التحديات الأمنية لمجتمع المعلومات أدى إلى ظهور مفهوم جديد يُعرف باسم "الأمن الإلكتروني".

مشكلة الدراسة

أصبحت المعلومات مورداً ثمينا يمكن تداولها وتطبيقها للاستفادة منها، ولكنها في المقابل تؤثر على الأفراد والمجتمعات، واليوم لدينا عدد قليل من الخيارات المتاحة، كما أن شكل تقنيات المراقبة الجديدة المضمنة في أجهزتنا وتطبيقاتنا والمنصات أضحت تشكل مخاطر أكبر من الاستخدام المتعمد والتخريبي غير المقصود لبياناتنا، وفي المقابل فإننا نتحرك نحو تطبيق واسع لنطاق الحوسبة السحابية، وهو ما من شأنه أن يمكن جمع البيانات في المساحات المادية.

إن البيانات الضخمة والذكاء الاصطناعي أداتان رائعتان تم إنشاءهما مع الأخذ بعين الاعتبار الصالح الاجتماعي، فإن المرحلة التالية من الحوسبة السحابية تتهيأ نحو الاندماج في مدننا وبيوتنا، كما أن الفيس بوك لا يزال يستثمر المليارات في الحوسبة السحابية والتقاط البيانات الحيوية والبحوث في مجال علم الأعصاب، لتسويق خدماته وتوسيع نطاقه.

هناك توافقا واسعا في الآراء بشأن فوائد هذا التحول الرقمي، ولكن هناك مشاكل ناشئة تترتب عليها آثار عديدة على مجتمعنا واقتصادنا، بسبب إساءة استخدام الخدمات عبر الإنترنت بواسطة الأنظمة السحابية المتلاعبة لتوسيع نطاق انتشار المعلومات المُضللة ولأغراض الأخرى الضارة، أي أننا ضمن بيئة رقمية عالمية أنشأت فيها وسائل جديدة محلية وإقليمية والأنشطة العالمية، بما في ذلك أنماط جديدة من النشاط السياسي، والتبادلات الثقافية وممارسة حقوق الإنسان.

حيث تعمل البيئة الرقمية العالمية الجديدة أيضاً على إنشاء حيز جديد لقانون السلوك: من أجل محاربة خطاب الكراهية أو المواد الإباحية للأطفال، التحريض إلى العنف، وانتهاكات حقوق النشر ("القرصنة")، والاحتيال، وسرقة الهوية، وغسل الأموال والهجمات على البنية الأساسية للاتصالات الإلكترونية من خلال البرامج الضارة (كفيروسات أحصنة طروادة والفيروسات المتنقلة) أو هجمات "رفض الخدمة"، كون المصطلحين الجرائم الإلكترونية والأمن الإلكتروني أصبح من الشواغل الرئيسة، فقد يقوم المجرمون بتنفيذ الهجمات الإلكترونية، وحتى من قبل الدول لأغراض صناعية والتجسس، وهذا من أجل الحاق الضرر الاقتصادي الناجم عن ممارسة الضغوط وتخريب البنية التحتية.

المؤلف المراسل [2]*: **العربي بن حجار ميلود** ، larbibenhadjar.miloud@univ-oran1.dz

ISSN : 1112-2803
EISSN: 2602-6589

لا تزال هناك فجوات وأعباء قانونية كبيرة يتعين التصدي لها، كما أن بروز وازدياد الشركات الخدماتية سيحتم على الدول أن تدرس وتعيد النظر في تشريعاتها وحماية بياناتها من أجل حماية مواطنيها، وصد البلدان التي تستخدم التكنولوجيا لتحقيق السلطوية الرقمية. مما يحتم على الجزائر أن تضمن تطور التشريع في هذا المجال. **لهذا يتم طرح التساؤل الرئيس التالي:** ما هي التشريعات والتطبيقات التكنولوجية الحديثة التي سنتها واتبعتها الجزائر من أجل تنظيم فضاءها الرقمي؟

منهج الدراسة

من أجل الوصول إلى نتائج مرضية استخدمنا المنهج الاستدلالي من أجل البرهنة والذي بدأناه بقضايا مسلم بها، وسرنا نحو قضايا أخرى نتجت عنها بالضرورة، أي الاتجاه من قضايا بسيطة ثم تركيب بعضها مع بعض حتى يتم الوصول إلى قضايا أكثر تعقيدا، حيث استخدمنا التسلسل المنطقي المنتقل من مبادئ أو قضايا أولية إلى قضايا أخرى تستخلص منها[1].

1. أمن المعلومات الإلكتروني

هو موضوع معقد ويحتوي على عدد من التعريفات تشمل النطاق الكامل للحد من التهديدات، والحد من الضعف، والردع، والمشاركة الدولية، والاستجابة للحوادث، وضمان المعلومات، وإنفاذ القانون، والدبلوماسية، والعسكرية، وبعثات المخابرات فيما يتعلق بأمن واستقرار البنية الأساسية العالمية للمعلومات والاتصالات[2]، أو هو تنظيم وجمع الموارد والعمليات والهياكل المستخدمة لحماية الأنظمة التي تعمل في مجال الفضاء الخارجي والإلكتروني من حالات الحدوث التي تسيء توحيدها بحكم القانون من حقوق الملكية الفعلية[3].

كما نجده يتمثل في ممارسة الدفاع عن أجهزة الكمبيوتر و الخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الضارة، أي أمن تكنولوجيا المعلومات أو أمن المعلومات الإلكتروني، وهو مصطلح ينطبق في مجموعة متنوعة من السياقات، من الحوسبة في الشركات إلى الحوسبة المتنقلة، ويمكن تقسيمه إلى بعض الفئات الشائعة[4]:

- **أمن الشبكة (Network security)** هو ممارسة تأمين شبكة كمبيوتر من المتطفلين، سواء كانوا مهاجمين مستهدفين أو برامج ضارة انتهازية.
- **أمن التطبيقات (Application security)** يركز على إبقاء البرامج والأجهزة خالية من التهديدات، ويمكن للتطبيق الذي تعرض للاختراق أن يوفر الوصول إلى البيانات التي تم تصميمه لحمايتها، يبدأ الأمان الناجح في مرحلة التصميم قبل نشر البرنامج أو الجهاز بوقت طويل.
- **أمن المعلومات (Information security)** يعنى بسلامة البيانات وخصوصيتها، سواء أثناء التخزين أو أثناء النقل.
- **الأمن التشغيلي ((Operational security** يتضمن العمليات والقرارات المتعلقة بالتعامل مع أصول البيانات وحمايتها، تقع الأذونات التي يتمتع بها المستخدمون عند الوصول إلى الشبكة والإجراءات التي تحدد كيفية ومكان تخزين البيانات أو مشاركتها ضمن هذه المِظلة.
- **استعادة البيانات بعد الكوارث واستمرارية الأعمال (Disaster recovery and business continuity)** كيفية استجابة المؤسسة لحادث أمن إلكتروني أو أي حادث آخر يتسبب في فقدان العمليات أو البيانات، تملي سياسات استرداد البيانات بعد الكوارث كيف تستعيد المؤسسة عملياتها ومعلوماتها للعودة إلى نفس سعة التشغيل التي كانت عليها قبل الحادث، كما أن استمرارية الأعمال هي الخطة التي تتراجع المؤسسة عنها أثناء محاولة العمل بدون موارد معينة، حيث يمكن لأي شخص عن طريق الخطأ إدخال فيروس إلى نظام آمن آخر عن طريق عدم إتباع ممارسات الأمان الجيدة، إن تعليم المستخدمين حذف مرفقات البريد الإلكتروني المشتبه بها،

المؤلف المراسل [2]*: **العربي بن حجار ميلود** ، larbibenhadjar.miloud@univ-oran1.dz

وعدم توصيل محركات أقراص **USB** غير المحددة، والعديد من الدروس الأخرى المهمة أمر حيوي لأمن أي مؤسسة.

يتضمن نطاق عمليات الأمن الإلكتروني حماية المعلومات والأنظمة من التهديدات الإلكترونية الكبرى، وتتخذ هذه التهديدات أشكالاً عديدة، ونتيجة لهذا فإن مواكبة إستراتيجية وعمليات الأمن السيبراني قد تشكل تحدياً كبيرا، خاصة في الحكومة وشبكات المؤسسات، حيث تستهدف التهديدات السيبرانية في أكثر أشكالها إبداعاً في كثير من الأحيان الأصول السرية والسياسية والعسكرية للأمة، ومن بين التهديدات الشائعة [5]:

- **الإرهاب السيبراني** :**(Cyber terrorism)** هو الاستخدام المبدع لتكنولوجيا المعلومات من قِبَل الجماعات الإرهابية لتعزيز أجندتها السياسية، وقد اتخذت شكل هجمات على الشبكات ونظم الحواسيب والهياكل الاساسية للاتصالات السلكية واللاسلكية.
- **حرب الفضاء السيبراني (Cyber warfare)**: تم الاعتراف بالحرب السيبرانية باعتبارها المجال الخامس للحرب، ينفذها في المقام الأول القراصنة الذين يتمتعون بتدريب جيد على استخدام جودة التفاصيل لشبكات الكمبيوتر، وتعمل في ظل مساندة ودعم الدول القومية، فبدلاً من إغلاق شبكات التأمين المستهدفة الرئيسية، قد يضطر هجوم الحرب السيبرانية إلى وضع الشبكات بهدف الإضرار بالبيانات القيمة أو إضعاف الاتصالات، أو إضعاف خدمات البنية الأساسية مثل النقل والخدمات الطبية، أو مقاطعة التجارة.
- **التجسّس الإلكتروني** :**(Cyber Espionage)** هو ممارسة استخدام تكنولوجيا المعلومات للحصول على معلومات سرية بدون إذن من أصحابها، وهي الأكثر استخدامًا لكسب ميزة استراتيجية واقتصادية وعسكرية، ويتم إجراؤها باستخدام تقنيات التشققات **(cracking techniques)** والبرامج الضارة.

أصبح الأمن الإلكتروني عامًا ويهم الجميع: المواطنون، والمهنيون وبشكل أكثر عموماً صانعو القرار، كما أصبح مصدر قلق خطير لمجتمعاتنا التي يتعين عليها أن تحمينا ضد هجمات الأمن الإلكتروني، وذلك من خلال تدابير وقائية وتدابير رد فعل على حد سواء وهذا يعني قدراً كبيراً من المراقبة، ولابد وأن يحافظ في نفس الوقت على حرياتنا أي تجنب المراقبة العامة[6].
يسعى الأمن الإلكتروني إلى ضمان الأمن العام للمعلومات الرقمية، وهو مفهوم يهتم بشكل عام بالمجالات الاجتماعية والقانونية والتنظيمية والتكنولوجية وكذا التدابير التي تضمن النزاهة والسرية للمعلومات الرقمية من أجل تحقيق درجة عالية من الثقة والأمن اللازمين لتطوير مجتمع المعلومات المستدام.

2. الجريمة الإلكترونية

المصطلح لا يعني في واقع الأمر أكثر من مجرد إشارة إلى حدوث سلوك ضار يرتبط بطريقة ما بالكمبيوتر، وليس له أي مرجع محدد في القانون، وبعد مرور أكثر من عشر سنوات، لا تزال هذه الحجة صادقة وبالنسبة للعديد من البلدان التي لا تزال لديها مفاهيم غامضة للغاية في دساتيرها للجرائم على الإنترنت[7].

تُعرَّف الجريمة الإلكترونية بأنها جرائم مرتكبة على الإنترنت باستخدام الكمبيوتر إما كأداة أو ضحية مستهدفة، ومن الصعب للغاية تصنيف الجرائم بصفة عامة إلى مجموعات متميزة نظرا لتطور العديد من الجرائم على أساس يومي، وحتى في العالم الحقيقي، لا ينبغي بالضرورة الفصل بين جرائم مثل الاغتصاب أو القتل أو السرقة. ومع ذلك، فإن جميع الجرائم الإلكترونية تشمل كلاً من الكمبيوتر والشخص الذي يقف وراءه كضحايا، بل يتوقف فقط على أي من الاثنين هو الهدف الرئيسي[8]:

- **الكمبيوتر كأداة**

المؤلف المراسل [2]*: **العربي بن حجار ميلود** ، larbibenhadjar.miloud@univ-oran1.dz

ISSN : 1112-2803
EISSN: 2602-6589

عندما يكون الفرد هو الهدف الرئيس في الجريمة الإلكترونية، يمكن اعتبار الكمبيوتر الأداة وليس الهدف، فالجرائم التي كانت قائمة لقرون في حالة عدم الاتصال بالإنترنت، كالخدع والسرقة وتسجيلات الإعجاب كانت موجودة حتى قبل تطوير المعدات عالية التقنية، ونفس المجرم ببساطة تم إعطائه أداة تزيد من مجموع ضحاياه المحتملين وتجعل من الصعب اقتفاء أثر القبض عليه.

- **الكمبيوتر كهدف**

هذه الجرائم ترتكبها مجموعة مختارة من المجرمين، على عكس الجرائم التي تستخدم الكمبيوتر ككمبيوتر فهذه الأخيرة تتطلب معرفة فنية، هذا ما يفسر عدم استعداد المجتمع والعالم عموما نحو مكافحة هذه الجرائم، إذ هناك العديد من الجرائم يتم اقترافها يوميا على الانترنت.
فالجريمة الإلكترونية هي نشاط غير قانوني يستخدم الكمبيوتر كوسيلة أساسية له مثل شبكة عمليات الاقتحام، ونشر الفيروسات بالحواسيب[9]، التصيد الاحتيالي والتجسس الإلكتروني والتزوير المعلوماتي[10]، بالإضافة إلى جرائم أخرى مثل: سرقة الهوية، التنمّر والإرهاب التي أصبحت مشكلة كبيرة بالنسبة للمجتمع، وهي في تزايد أيضاً جنباً إلى جنب مع تقدم التكنولوجيا[11].
وهي تنطوي على أنشطة مثل النشاط الجنسي؛ والاحتيال في بطاقات الائتمان؛ والملاحقة الإلكترونية؛ وتشويه سمعة أخرى على الإنترنت؛ والحصول على وصول غير مصرح به إلى أنظمة الكمبيوتر؛ وتجاهل حقوق النشر، وترخيص البرامج والعلامات التجارية، والأمان للحماية؛ والتشفير بهدف صنع نسخ غير قانونية؛ والقرصنة على البرامج، وسرقة هوية أخرى تابعة لشركة التأمين، والمجرمون الإلكترونيون هم الذين يرتكبون مثل هذه الأعمال[12].

3. ماهية الأخطار في الفضاء الرقمي

الفضاء الإلكتروني مختلف كونه يحتاج إلى تنظيم السلوك ويشكل مساحة أقل انتظاما من المساحة الحقيقية، كما أن مصدر هذا الاختلاف هو في هندسته وفي الشفرة التي تشكله، فبنيته تجعله غير قابل للتنظيم بشكل أساسي[13].

3 .1. بيانات خطيرة في عصر "البيانات الضخمة"

إن البيئة الرقمية قد تؤدي بطبيعتها إلى تآكل الخصوصية وغير ذلك من الأمور الأساسية وتقوض عملية اتخاذ القرارات التي تخضع للمساءلة، وهناك إمكانات هائلة تقويض سيادة القانون ـ من خلال إضعاف أو تدمير حقوق الخصوصية، وتقييد الحريات حرية الاتصال أو حرية تكوين الجمعيات – والتدخل التعسفي[14].

2.3 التقنية العالمية و الخصوصية

نظرًا للطبيعة المفتوحة للإنترنت (التي تعد أكبر قوة لها)، يمكن لأي نقطة نهاية على الشبكة الاتصال أن ترتبط بأي نقطة نهاية أخرى تقريبًا، تتدفق البيانات عبر كافة أنواع المحولات وأجهزة التوجيه والكابلات، كونها البنية الأساسية المادية للإنترنت، التي تتألف من كابلات الألياف البصرية عالية السعة تعمل تحت محيطات العالم وبحاره، فضلاً عن الكابلات وأجهزة التوجيه المرتبطة بالأرض، وأهم كابلات أوروبا هي تلك التي تمتد من أوروبا القارية إلى المملكة المتحدة ومن هناك تحت المحيط الأطلسي إلى الولايات المتحدة، ونظراً لهيمنة الشركات الأميركية على الإنترنت والسحابة، فإن هذه الكابلات تحمل في طياتها نسبة كبيرة من جميع بيانات حركة المرور على الإنترنت والاتصالات القائمة على الإنترنت، بما في ذلك كل البيانات تقريباً من أوروبا وإليها. وفي الوقت

المؤلف المراسل *2: العربي بن حجار ميلود ، larbibenhadjar.miloud@univ-oran1.dz

الحالي، فإن العديد من هذه المكونات المادية توجد في الولايات المتحدة الأمريكية والعديد منها تدار وتسيطر عليها كيانات خاصة، وليس كيانات حكومية[15].

4. تحديات التشريع الدولي المُنظم للفضاء الرقمي

إن فكرة تنظيم الفضاء الرقمي بالقانون الدولي ليست جديدة بشكل لافت للنظر وإنما يعود لعام 1996 حيث بذلت جهود كبيرة، وتم بالفعل اقتراح صياغة القانون الدولي بشأنه من قبل خبراء القانون، والجهات الفاعلة في مجال الأعمال، وكانت هناك ثلاث أفكار مهيمنة حول الكيفية التي ينبغي بها تنظيمه بواسطة القانون الدولي، على الرغم من وجود المدافعين عن الحريات السيبرانية مثل جون بارلو (**John Barlow** 1996) كونه من أنصار فكرة أن يظل الفضاء الرقمي حراً من طغيان وأي حكم قمعي قد يعوق حرية الإنترنت، ويعتقد جيمس لويس (**James Lewis** 2010)، أنها مسؤولية تقع على عاتق الدول في صياغة القانون الوطني والدولي لتنظيمه، وكانت تدور المناقشات حول ثلاث نقاط رئيسية ترتبط بالتحديات التي تواجه صياغة القانون الدولي بشأنه بأساس المبادئ والخصائص التي يتسم بها القانون العام الدولي: الاختصاص القضائي والتحكيم والصكوك القانونية والفقهية[16].

إن موضوع التشريع الدولي المنظم للفضاء الرقمي صعب ضبطه كون الجهات الفاعلة في هذا الفضاء متنوعة على نطاق واسع، حيث إنه يمتد من الجهات الفاعلة في الدولة إلى شركات الإنترنت الكبيرة والمؤسسات الصغيرة والمتوسطة، والمتطفلين و الأفراد، إن التعقيدات والتحديات التي يفرضها القانون الدولي على الفضاء الإلكتروني أصبحت محرومة على نحو متزايد من خلال الاتجاه الأخير نحو الترويج للسيادة الرقمية والتي أصبحت فكرة التحكم في الوصول للمعلومات والاتصالات والشبكات والبنية التحتية في العالم الرقمي، والتحكم فيها من قبل جهات فاعلة دولية في السنوات الأخيرة: الصين والتحالف السيبراني الروسي حول السيادة الرقمية؛ وقضايا سنودن وويكيليكس **(Snowden and Wikileaks)**؛ وصعود التحالف السيبراني العالمي **(GAFA Google-Apple Facebook-Amazon)** ، كون التحالف السيبراني بين **الصين وروسيا** بشأن السيادة الرقمية هو من اجل تعزيز فكرة حماية مصالحها الوطنية التي ترتبط في معظمها بالاقتصاد والمخاوف الأمنية، وكل من البلدين تطالب بقدر أعظم من السيطرة على الفضاء السيبراني من خلال دعم مبدأ عدم التدخل في الإدارة العالمية المتعددة للإنترنت مثل الاتحاد الدولي للاتصالات (**ITU**)، و **ICANN**، و **IANA**، ومنتدى حوكمة الإنترنت[17].

تطبق المجتمعات المختلفة أدوات وأساليب أخلاقية مختلفة تجاه المواطنة الرقمية والحقوق، ولعل الصين وروسيا هما البلدان الأكثر شهرة في مجال تطبيق تكنولوجيات المراقبة الرقمية والتأثير على الأدوات ضد مواطنيهما (بل وربما على مواطني البلدان الأجنبية) ، رغم أن **روسيا** كانت معروفة بتنفيذ تكنولوجيات المراقبة ضد مواطنيها منذ عام 1995، فإنها كانت متهمة أيضاً بمحاولة التأثير على السياسات الخارجية، وكانت أحدث هذه الاتهامات في ما يتصل بالدعاية الآلية وإكراه وسائل الإعلام الاجتماعية، حيث اتهمت تقارير أميركية رسمية روسيا بالتدخل في انتخابات الولايات المتحدة الأمريكية عام 2016، كما أن طموحها يصل إلى مناطق أخرى بما في ذلك ممارسة نفوذها في أفريقيا[18].

يسمح التعديل الرئاسي لقانون المعلومات الروسي (**The Law on Information (FL 398)**) لمكتب المدعي العام بوضع أي موقع على الشبكة العالمية يسمعه بأنه "دعاية متطرفة"، مع احتمال التحريض على أعمال الشغب المناهضة للحكومة في القائمة السوداء ومن دون أمر من المحكمة، وتجرم روسيا أيضاً مشاركة المحتوى "المتطرف" على الشبكات الاجتماعية[19].

المؤلف المراسل [2]*: **العربي بن حجار ميلود** ، larbibenhadjar.miloud@univ-oran1.dz

ISSN : 1112-2803
EISSN: 2602-6589

كما تعتبر **الصين** واحدة من أقل المساحات الرقمية حرية في العالم، إن سور الصين الناري العظيم**The Great Firewall of China (GFW)** عبارة عن مصطلح يستخدم لوصف سلسلة من التنظيمات على شبكة الإنترنت، وسياسات الرقابة، وأدوات المراقبة المستخدمة لتنظيم ومنع الوصول إلى خدمات الاتصالات على شبكة الإنترنت والأجهزة المحمولة غير المعتمدة من قِبَل الحكومة، وقد تجاوز هذا ما هو أبعد من الشاشات اللامعة وفي الشوارع[20]، كما تنص المادة الخامسة عشرة من "التدابير الخاصة بإدارة خدمات المعلومات على شبكة الإنترنت"، التي أصدرها مجلس الدولة في عام 2000، على ما أصبح يعرف باسم "فئات المحتوى المحظورة التسع" **(Nine for bidden content categories)** للخدمات الصينية على شبكة الإنترنت، ومن بين هذه الفئات الخطاب الذي "يضر بكرامة الدولة أو مصالحها"، أو "يروج عن المعاهد الدينية، ويعكر النظام الاجتماعي أو يعطل الاستقرار الاجتماعي"، أو "تحري السياسة الدينية للدولة أو تروج لتعاليم هرطقة أو الخرافات الإقطاعية."[21]

تحد **مصر** من الخطاب المفتن، فضلاً عن الهجوم الكلامي على السلطات الحكومية المحلية والأجنبية، ويفكر البرلمان المصري في قانون لمكافحة الإرهاب يسمح لشركات الإنترنت والمنصات بأن تمنع من دخول البلاد "تعريض النظام العام للخطر، كما تسمح **الهند** بتقييد المحتوى على شبكة الإنترنت من قِبَل الحكومة المركزية أو السلطات المخولة لأسباب تتعلق بالأمن القومي، بما في ذلك: وحرصا على سيادة الهند وسلامتها، أو الدفاع عن الهند، أو أمن الدولة، أو العلاقات الودية مع الدول الأجنبية، أو النظام العام، أو منع التحريض على ارتكاب أي جريمة يمكن ارتكابها فيما يتصل بما سبق[22].

تحظر **الولايات المتحدة الأمريكية** التحريض على "العمل الوشيك غير المشروع" مصادر مسؤولة لمنظمة إرهابية أجنبية، وتتجه في نفس سياق حليفتها **المملكة المتحدة** حيث تحظر كل انتهاكات الأسرار الرسمية، وتعبير يشجع الإرهاب أو ينشر منشورات إرهابية. وفي عام 2010 أنشأت المملكة المتحدة وحدة إحالة مكافحة الإرهاب على شبكة الإنترنت، التي تستعرض محتوى "المتطرف العنيف أو الإرهابي" الذي يقدمه الجمهور من خلال أداة إبلاغ مجهولة على الإنترنت، وتفحص الشبكة بشكل استباقي بحثاً عن محتوى يروّج للإرهاب أو يمجده، ثم تعمل مع الوسطاء لإزالة المحتوى المنتهك[23]، كما أن الطموح في الحفاظ على الزعامة في اقتصاد البيانات وسباق التكنولوجيا الفائقة، فإن بلدان مثل الولايات المتحدة وكندا من الممكن أن تستفيد من تطوير وتطبيق تنظيمات أفضل وحماية إلكترونية لمواطنيها، في حين تفرض غرامات كبيرة على انتهاكات التنظيمات في الاتحاد الأوروبي من قِبَل منصات التكنولوجيا، فإن سياسات الحقوق الرقمية لا تطبق بشكل كبير – على الأقل ليس في اتجاه عمالقة التكنولوجيا في أميركا الشمالية[24].

أما في **أستراليا** فإننا نجد المشرعين الأستراليين اتخذوا نهجاً مختلفاً في التعامل مع الخصوصية، كون أن استخدام البيانات الشخصية ليست مجرد مسألة خصوصية وأمان و ثقة، لهذا نجد لجنة المنافسة والمستهلكين الأسترالية وحدة تحليل البيانات **(The Australian Competition & Consumer Commission)** تهدف بشكل خاص إلى ضمان الاستخدام القانوني للبيانات والخوارزميات الضخمة .أطلقت مشروع يبحث في منصات رقمية (محركات البحث ووسائل التواصل الاجتماعي) في المنافسة، بما في ذلك أهمية قوانين الخصوصية، زيادة ترسيخ الصلة الوثيقة بين قوانين المنافسة و الخصوصية، فإن "حق بيانات المستهلك" الجديد الذي اقترحته وزارة الخزانة الأسترالية سوف يمنح المستهلكين حق الوصول بأمان إلى بعض البيانات الخاصة بها والتي تحتفظ بها الشركات، وسوف يكون بوسعهم أيضاً أن يتمكّنوا من طلب نقل هذه المعلومات إلى أطراف ثالثة معتمدة وموثوق بها من اختيارهم، في البداية سوف ينطبق حق بيانات المستهلك على القطاع المصرفي فقط، ولكن سيتم تطبيقه على كل القطاعات الأخرى لاحقا[25].

المؤلف المراسل *2: **العربي بن حجار ميلود** ، larbibenhadjar.miloud@univ-oran1.dz

يسعى **الاتحاد الأوروبي** جاهداً إلى إنشاء سوق موحدة للبيانات والتنظيمات في عام 2020، وسوف يكافأ المواطنون أو يعاقبون وفقاً لسلوكهم، حيث أن العديد من البلدان تتسابق نحو سوق رقمية متكاملة، إذ تهدف مبادرة السوق الرقمية الموحدة في أوروبا إلى تعزيز الصناعة الرقمية الأوروبية وبناء اقتصاد بيانات أوروبي موحد، ولكن مثل هذه الطموحات العالية تنطوي أيضاً على مخاطر كبيرة، لقد كان الاتحاد الأوروبي رائداً في وضع قواعد ولوائح حماية البيانات، حيث أطلق اللائحة العامة لحماية البيانات (**General Data Protection Regulations**) في الاتحاد الأوروبي، إذ تم تصميم هذه اللوائح بحيث تتوافق مع قوانين خصوصية البيانات في جميع أنحاء أوروبا، وحماية مواطنيها الاتحاد الأوربي وتمكينهم من ملكية البيانات، فضلاً عن التحكم في التنقيب عن البيانات واستخدامها من قبل المؤسسات العامة والخاصة[26].
حيث اقترحت المفوضية الأوروبية إصلاحاً طموحاً للفضاء الرقمي، ومجموعة شاملة من القواعد الجديدة لكل الخدمات الرقمية، بما في ذلك وسائل الإعلام الاجتماعية، وأماكن السوق على شبكة الإنترنت، وغير ذلك من المنصات التي تعمل في الاتحاد الأوروبي: قانون الخدمات الرقمية وقانون الأسواق الرقمية[27].

بموجب قانون الخدمات الرقمية، هناك التزامات على مستوى الاتحاد الأوروبي بالكامل على كل الخدمات الرقمية التي تربط المستهلكين بالسلع أو الخدمات أو المحتوى، بما في ذلك الإجراءات الجديدة لإزالة المحتوى غير القانوني بشكل أسرع فضلاً عن الحماية الشاملة للحقوق الأساسية للمستخدمين على الإنترنت، وسوف يعمل الإطار الجديد على إعادة التوازن إلى حقوق ومسؤوليات المستخدمين والمنصات الوسيطة، والسلطات العامة، وهو يقوم على القيم الأوروبية، بما في ذلك احترام حقوق الإنسان، والحرية، والديمقراطية، والمساواة وسيادة القانون، ويكمل الاقتراح خطة العمل الأوروبية من أجل الديمقراطية والتي تهدف إلى جعل الديمقراطيات أكثر مرونة وقدرة على الصمود، وعلى نحو ملموس سوف يقدم قانون الخدمات الرقمية سلسلة من الالتزامات الجديدة المنسقة على مستوى الاتحاد الأوروبي فيما يتصل بالخدمات الرقمية، والتي يتم تدرجها بعناية على أساس حجم هذه الخدمات وتأثيرها، مثل :[28]:

- قواعد لإزالة السلع أو الخدمات أو المحتوى غير القانوني عبر الإنترنت؛
- ضمانات للمستخدمين الذين حذفت المنصات محتوياتها خطأ؛
- التزامات جديدة لمنصات العمل الكبيرة للغاية باتخاذ إجراءات قائمة على المخاطر لمنع إساءة استخدام أنظمتها؛
- تدابير واسعة النطاق للشفافية، بما في ذلك بشأن الإعلانات على الإنترنت والخوارزميات المستخدمة لتوصية المستخدمين بالمحتوى؛
- سلطات جديدة لفحص كيفية عمل المنصات، بما في ذلك تسهيل وصول الباحثين إلى بيانات المنصات الرئيسية؛
- قواعد جديدة بشأن إمكانية تعقب مستخدمي الأعمال التجارية في الأسواق على الإنترنت، للمساعدة في تعقب بائعي السلع أو الخدمات غير المشروعة؛
- عملية تعاون مبتكرة بين السلطات العامة لضمان الإنفاذ الفعال في السوق الموحدة.

يحدد الإعلان العالمي لحقوق الإنسان والعهد الدولي الخاص بالحقوق المدنية والسياسية وغير ذلك من المنظمات الدولية لحقوق الإنسان القيود المفروضة على الحق في حرية التعبير من أجل حماية حقوق الإنسان الأخرى، ولكن كما أكد المقرر الخاص للأمم المتحدة في تقريره لعام 2011، فإن القيود لا تتوافق إلا مع معايير حقوق الإنسان الدولية عندما تلبي ثلاثة شروط[29]:

- يجب أن يكون التقييد قائماً على القواعد، ويوفره القانون وينفذ بطريقة شفافة ويمكن التنبؤ به؛
- يجب أن يكون التقييد ضرورياً ومتناسباً، باستخدام أقل الوسائل تقييداً لتحقيق الهدف؛

المؤلف المراسل [2]*: **العربي بن حجار ميلود** ، larbibenhadjar.miloud@univ-oran1.dz

ISSN : 1112-2803
EISSN: 2602-6589

- يجب أن يكون التقييد متوافقاً مع الأغراض المذكورة في العهد الدولي الخاص بالحقوق المدنية والسياسية: حماية حقوق الآخرين أو سمعتهم، أو الأمن القومي أو النظام العام، أو الصحة العامة أو الآداب العامة.

4. 1. الأهداف الرئيسة لقانون الخدمات الرقمية[30]:

- تعزيز الإبداع والنمو والقدرة التنافسية، وتيسير توسيع المنصات والمشاريع الأصغر والمتوسطة حجماً والمشاريع البادئة؛
- حماية المستهلكين وحقوقهم الأساسية على الإنترنت بشكل أفضل؛
- تأسيس شفافية قوية وإطار واضح للمساءلة فيما يتصل بالمنصات على شبكة الإنترنت؛
- تعزيز الابتكار والنمو والقدرة التنافسية في السوق المشتركة.

5. المحيط التشريعي للفضاء الرقمي في ظل التوجه نحو الحكومة الإلكترونية بالجزائر

انطلاقا من عدد السكان الذين بلغ عددهم جانفي 2020، 43.45 مليون نسمة، نسبة 73 بالمائة يتمركزون في المدن، فإن البنية التحتية للبيئة الرقمية تتمثل في : عدد مستعملي الهاتف النقال 49.48 مليون مقابل 114 بالمائة من السكان، وعدد مستخدمي الإنترنت 22.71 مليون، عدد مستخدمي الشبكات الاجتماعية 22 مليون[31].

و وفقاً لدراسة أجرتها شركة **(Comparitech)** والتي تمت على 60 دولة وتضمنت عدداً من التصنيفات لمعدلات البرامج الضارة وإلى التشريعات المتعلقة بالأمن الإلكتروني، فإن الجزائر هي الدولة الأقل أماناً على مستوى العالم، وكانت الأعلى بسبب نقص التشريعات ومعدلات البرامج الضارة بالحواسيب، كما حصل على درجة عالية في فئة البرامج الضارة المستهدِفة للهواتف المحمولة وعلى واحدة من أدنى الدرجات استعدادًا للهجمات الإلكترونية، ونظرت الدراسة في سبعة معايير:[32]

- نسبة الهواتف المحمولة المصابة بالبرامج الضارة – بنغلادش – 35.91% من المستخدمين.
- نسبة الحواسيب المصابة بالبرامج الضارة – الجزائر 32.41%.
- عدد هجمات البرامج الضارة المالية – ألمانيا – 3% من المستخدمين.
- النسبة المئوية لهجمات telnet (حسب البلد الأصلي) – الصين – 27,15%.
- نسبة الهجمات التي يقوم بها خبراء التشفير - أوزباكستان - 14. 23% من المستخدمين.
- البلدان الأقل استعداداً للهجمات السيبرانية – فيتنام 0.245 نقطة.
- أسوأ تشريع حديث للأمن الإلكتروني – الجزائر – فئة رئيسية واحدة.

إذ سجل مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها، التابع لقيادة الدرك الوطني، 1140 جريمة إلكترونية في الفترة الممتدة بين 12 جانفي و25 نوفمبر 2018 والرقم مرشح للارتفاع، حيث وقع عدد من الوزراء وإطارات عليا في الدولة للابتزاز والتهديد والتشهير والمساس بحريتهم الشخصية عبر مواقع التواصل الاجتماعي، كما تم تسجيل عدد كبير من القضايا المتعلقة باختراق مختلف المواقع من بينها مؤسسات رسمية ووزارات سيادية والبنوك والشبكات الاجتماعية، بما فيها جرائم القرصنة أو الابتزاز أو التشهير أو التحرش الإلكتروني أو حتى الاحتيال[33].

يحمي الدستور الجزائري حقوق وحريات المواطنين من خلال ضمان حقوق الإنسان والحريات؛ وحرية العقيدة والرأي؛ وحرية التجارة والصناعة؛ وحرية الإبداع الفكري والفني والعلمي، كما ينص على أنه لا يمكن مصادرة أي منشور دون أمر قضائي، وتضمن خصوصية المراسلات والاتصالات، وحرية التعبير، والمساواة في الحصول على التعليم والتدريب المهني[34].

المؤلف المراسل [2]*: العربي بن حجار ميلود ، larbibenhadjar.miloud@univ-oran1.dz

تستند الإستراتيجية الإلكترونية الجزائرية إلى عدة أهداف: تعزيز استخدام تكنولوجيا المعلومات والاتصالات في الإدارة العامة والأعمال التجارية؛ تطوير آليات وتدابير تشجيعية لمنح المواطنين إمكانية الوصول إلى معدات وشبكات تكنولوجيا المعلومات والاتصالات؛ وتحفيز تطوير الاقتصاد الرقمي مع تعزيز القدرات والهياكل الأساسية العالية السرعة للاتصالات السلكية واللاسلكية وتنمية القدرات البشرية؛ تعزيز البحث والتطوير والابتكار؛ وتحديث الإطار القانوني الوطني؛ واعترافا بقيمة التعاون الدولي؛ و إنشاء آليات للرصد والتقييم الإلكتروني[35].

أما فيما يتعلق باستخدام أدوات **Web 2.0**، فلا يزال هذا الأمر يعتبر ظاهرة جديدة في الجزائر، كون عالم المدونات هو صغير ومتشكل من أصحاب المدونات الذين يعيشون في فرنسا وأماكن أخرى من أوروبا، يُعتبر **You Tube** أكثر شعبية، ويُستخدم للتعبير عن الآراء الفردية بشأن القضايا السياسية و وصف القضايا الاجتماعية أو تناولها، الشباب الجزائري يستخدم الهواتف المحمولة لتسجيل مقاطع فيديو ومن تم نشرها على **YouTube**، ثم يتم تشجيع الأصدقاء على زيارة موقع الويب، وهناك اتجاه جديد آخر يشجع على الوصول إلى المعلومات استخدام الهواتف المحمولة للوصول إلى الإنترنت[36].

قد اتجهت بحوث الحكومة الإلكترونية إلى التركيز على تقديم الخدمات، وليس على استخدام تكنولوجيا المعلومات والاتصالات في إطار العملية التنظيمية، ولكن هذا يأخذ نظرة ضيقة للغاية حول الغرض من التنظيم وتطبيقه[37]. تحاول السلطات الجزائرية بذل جهود كبيرة لتحسين وتأمين مناخ الأعمال والاستثمار، ولا سيما من خلال التدابير التالية[38] :

- تنفيذ تشريع جديد للتجارة الإلكترونية، بما في ذلك الإعلان الإلكتروني، من خلال القانون رقم 18-05 الصادر في 10 ماي 2018[39] بشأن التجارة الإلكترونية، مما يدل على خطوة كبرى إلى الأمام من خلال تقديم نظام قانوني إلى مجال لم يكن منظماً في السابق.

إن الشركات الجزائرية اليوم تؤدي دورا مهما على المسرح العالمي، ولكي تنافس تلك البلدان فيتعين عليها أن تتحسن بشكل مستمر الإنتاجية والكفاءة على حد سواء، النبأ السار هنا أنهم يستطيعون الآن الاستفادة من هذه الزيادة وإمكانية الوصول إلى التقنيات المبتكرة[40].

1.5 تنفيذ إطار عمل لحماية البيانات القانونية

في عام 2015، أنشأت الحكومة الجزائرية رسمياً الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهو مركز منع جرائم الكمبيوتر والجرائم الإلكترونية ومكافحتها، وفقًا لمرسوم منشور في الجريدة الرسمية بتاريخ 8 أكتوبر 2015، تم وضع هذه السلطة الجديدة تحت مسؤولية وزارة العدل[41]، ليأتي بعدها المرسوم الرئاسي تحت رقم 19-172 المؤرخ في 06 جوان 2019، والذي يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، حيث حددت المادة 2 من المرسوم على كونها هيئة ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية توضع تحت سلطة وزارة الدفاع[42].

- في عام 2018، نفذت الجزائر إطاراً قانونياً لحماية البيانات الشخصية بموجب القانون رقم 18-07 الصادر في 10 جوان 2018 والمتعلق بحماية الأفراد في معالجة البيانات الشخصية، ويعرف القانون 18-07 البيانات الشخصية بأنها أي معلومات، بغض النظر عن الدعم، تتعلق بشكل مباشر أو غير مباشر بشخص محدد أو يمكن التعرف عليه (يسمى "الشخص المعني"). على سبيل المثال، رقم تعريف أو أي عناصر فيزيولوجية أو وراثية أو اقتصادية أو حيوية، ينطبق هذا القانون عندما[43]:

المؤلف المراسل [*2]: **العربي بن حجار ميلود** ، larbibenhadjar.miloud@univ-oran1.dz

ISSN : 1112-2803
EISSN: 2602-6589

- تتم معالجة البيانات الشخصية بواسطة مواطن جزائري أو كيان قانوني يتم تأسيس الممثل له على أرض الجزائر؛
- تتم معالجة البيانات الشخصية بواسطة فرد أو كيان قانوني يتم تأسيس الممثل له على أراضي دولة لديها قواعد قانونية مماثلة للقانون الجزائري؛ ويتم تأسيس ممثل الكيان القانوني خارج الجزائر، ولكن استخداماته لوسائل معالجة البيانات الشخصية يتم تمركز في الأراضي الجزائرية (باستثناء الوسائل المستخدمة في النقل البسيط للبيانات).

أي عملية أو مجموعة من العمليات تقوم بها وسائل آلية أو غير تلقائية أو تتم من الباطن لمعالجة البيانات الشخصية (على سبيل المثال، التجميع أو التسجيل أو تعديل الاستبقاء أو التكيف)، ويتعين على الطرف المسؤول عن هذه المعالجة أن يبلغ الأفراد بتجهيز بياناتهم الشخصية، وأن يضمن لهم أيضاً الحق في الوصول إلى بياناتهم وتصحيحها، فضلاً عن حق المعارضة في هذه العملية، ويتطلب الامتثال لهذه اللائحة الجديدة إنجاز الإجراءات الشكلية أمام السلطة الجزائرية لحماية البيانات الشخصية، فضلا عن تنفيذ التدابير التقنية والتنظيمية لحماية هذه البيانات، وعلى نطاق أوسع سوف تسيطر الهيئة الجزائرية لحماية البيانات الشخصية على تنفيذ هذه اللائحة الجديدة، ويعاقب انتهاك هذه القواعد بفرض عقوبات إدارية وجنائية بغرامات وسجن[44].

6. الأفاق المستقبلية للمحيط التشريعي المنظم للفضاء الرقمي بالجزائر

لا بد على الجزائر أن تتجه نحو التحول الرقمي الذي يجمع بين نماذج الحوكمة وآليات التفاعل بين الابتكار والخدمات والبرامج من خلال الاستفادة من التقنيات الرقمية، وهو يشير إلى عملية تغيير أساسي تتطلب نهجاً شاملاً في التحول الحكومي الرقمي من خلال دعم التغيير المرغوب داخل وخارج القطاع العام من أجل توليد القيمة العامة[45]، علما أن الجزائر شهدت تقدما كبيرا في تطوير البنية الرئيسية الأساسية لقطاع تكنولوجيا المعلومات والاتصالات في السنوات الأخيرة، لهذا نجد أن هناك بوادر السير نحو التحول الرقمي بدأت تتضح شيئا فشيئا من خلال تحديث إطارها القانوني وإدخال سلسلة من الأنظمة الجديدة التي تصاحب نمو القطاع، ونجد منها على سبيل المثال لا الحصر:

- القانون رقم 05 -10 المؤرخ في 20 جوان 2005 المعدل والمتمم للأمر رقم 75 – 58 المتضمن القانون المدني. الاعتراف بالكتابة الإلكترونية كوسيلة إثبات[46].
- 05 أوت 2009، صدور القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[47].
- المرسوم تنفيذي رقم 09 – 410 المؤرخ في 10 ديسمبر 2009 الذي يحدد قواعد الأمن المطبقة على النشاطات المتصلة بالتجهيزات الحساسة[48].
- القانون رقم 15 - 04 المؤرخ في 01 فيفري 2015 المتضمن تحديد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[49].
- **جوان 2018:** اعتمد البرلمان القانون رقم 18-04[50]، وهو قانون رئيسي آخر لخدمات البريد والاتصالات، وكان هذا الإجراء هو فصل البنية التحتية للإنترنت التي تجلب احتكار شركة الاتصالات والسماح لأي شركة اتصالات بطلب ترخيص من الهيئة التنظيمية للمنشورات والاتصالات الإلكترونية واستخدامها في البنية التحتية لتقديم خدمات الإنترنت للعملاء، وهناك جانب رئيسي آخر من القانون رقم 18-04 يتعلق بالالتزام المزدوج المفروض على أصحاب التجارة الإلكترونية لتسجيل أعمالهم التجارية في السجل التجاري ولاستضافة موقعهم على شبكة الإنترنت في خوادم جزائرية تحمل اسم النطاق extension.com.dz، ويمنح القانون المتعاملين في هذا القطاع ستة أشهر للامتثال، ويؤدي عدم القيام بذلك إلى رسوم تتراوح بين (363 يورو) إلى (14520 يورو)[51] .

المؤلف المراسل [2]*: العربي بن حجار ميلود ، larbibenhadjar.miloud@univ-oran1.dz

- المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، كترسانة تشريعية لمواجهة الحوادث السيبرانية التي تستهدف المؤسسات الوطنية، حيث حددت المادة 02 دورها في كونها أداة الدولة ضمن مجال أمن الأنظمة المعلوماتية، وتشكل الإطار التنظيمي لإعداد الإستراتيجية الوطنية لأمن الأنظمة وتنسيق تنفيذها[52].
- **حق الخصوصية**

نجده يتأقلم مع التغيرات التكنولوجية والبيئة الرقيمة منذ صدور أحكام الدستور 1996 والذي ينص في مادته 39 أنه: " ...سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة"[53]، ليتم تعديله في أحكام الدستور لسنة 2016، حسب المادة 77 التي نص على: "....احترام الحق في الشرف وستر الحياة الخاصة" [54]، ليضيف الدستور 2020 في المادة 47 " حماية كل الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي"[55].

- **شبكة الألياف البصرية**

وفقًا لوزارة البريد والاتصالات السلكية واللاسلكية والتقنيات الرقمية، تم تركيب 123000 كم من الألياف الضوئية في الجزائر في عام 2017 مما يجعلها أكبر شبكة في أفريقيا، كما تم تخطيط 7000 كم إضافية لربط ولايات الجنوب، تهدف هذه الخطة إلى تحسين سعة عرض النطاق الترددي العريض للإنترنت في الجزائر بمقدار عشرة أضعاف إلى 6,4 تيرابايت[56].

- فتح دورات تدريبية للمؤسسات حول الأمن الإلكتروني بالجزائر، لمعرفة كيفية تجنب تهديدات الأمن الإلكتروني وحمايتها منه من أجل ضمان أفضل لأمن المؤسسة[57].
- التعاون مع شركة (Trend Micro)، تنظم شركة (Cyber Talents)الجزائرية للأمن الإلكتروني للمرة الثانية على التوالي مسابقة حول الامن الإلكتروني، حيث يستطيع المشاركون إظهار قدراتهم التقنية ضمن فئات مختلفة مثل: الهندسة العكسية للمعلومات وأمن الويب والتحاليل الرقمية وأمن الشبكة وغيرها[58].

على الرغم من كل هذا إلا أنه يمكن أن تطفو بعض القضايا فوق السطح منها:[59]

- **قضايا الخصوصية**

إن الخصوصية مشكلة في تنفيذ خدمات الحكومة الإلكترونية وهذا من حيث عدم قدرة شبكات الإتصال على توفير أمان مطلق وكامل السرية عبر ما ينقل بواسطة البيانات[60]، وسيقلق المواطنون بشأن خصوصية حياتهم وأمنهم وسرية معلوماتهم المقدمة من أجل الحصول على الخدمات الحكومية.

- **مشاكل أمنية**

الأمن شرط مطلق لا سيما في معاملات الدفع مثل الضرائب،الخ.

- **التحديات التي تواجه حقوق الملكية**

مع التقارب بين العالمين الرقمي والفعلي بدأ التوتر بين حقوق الملكية وحرية التعبير ينشأ الآن في ظل العالم الرقمي، وهو ما أدى بالفعل إلى العديد من النزاعات القانونية، من بينها: تصوير مساحة مادية بشكل مختلف، إلحاق الضرر بالممتلكات العامة والخاصة، أدت هذه الأمور كلها إلى معارك قانونية، غير أن المحكمة لا توفر حلا دائما لجميع المنازعات، فإن الحلول المستقبلية ستثير العديد من التحديات الاخلاقية الجديدة حول الملكية الفكرية والخصوصية والسلامة التي ستتطلب حلولا أوسع[61].

لا تزال حماية براءات الاختراع والعلامات التجارية في الجزائر مشمولة بسلسلة من القوانين التي يرجع تاريخها إلى عامي 2003 و2005، وأفاد ممثلو الشركات الأميركية العاملة في الجزائر بأن هذه القوانين كانت مرضية من حيث نطاق ما تشمله والعقوبات التي تطبق على الانتهاكات، وقد أدى مرسوم حكومي صدر في عام 2015 إلى زيادة التنسيق بين الديوان الوطني

المؤلف المراسل [*2]: **العربي بن حجار ميلود** ، larbibenhadjar.miloud@univ-oran1.dz

ISSN : 1112-2803
EISSN: 2602-6589

لحقوق المؤلف والحقوق المجاورة (The National Office of Copyrights and Related Rights ONDA) والمعهد الوطني للملكية الصناعية (The National Institute for Industrial Property INAPI) لإنفاذ القانون من أجل ملاحقة انتهاكات براءات الاختراع والعلامات التجارية[62].

يغطي الديوان الوطني حقوق المؤلف والحقوق المجاورة فضلاً عن حقوق البرامج الرقمية، وعلى الرغم من الجهود المعززة المبذولة والتي شهدت اختفاء العديد من المنتجات للسلع المقرصنة أو المزيفة منذ عام 2011، فإن السلع المزيفة المستوردة منتشرة ويسهل الحصول عليها، لهذا تصادر سنويا العديد من الأجهزة، حيث دمرت مؤسسة (ONDA) أكثر من 100000 نسخة من وسائل الإعلام المقرصنة للاحتفال باليوم العالمي للملكية الفكرية في عام 2017، ولكن شركات البرمجيات تقدر أن أكثر من 85 في المائة من البرامج المستخدمة في الجزائر، ونسبة مماثلة من العناوين التي تستخدمها المؤسسات الحكومية والشركات المملوكة للدولة غير مرخصة[63].

الخاتمة

من الواضح أن الحقوق الرقمية ليست امتيازات أو مصالح شخصية، بل هي عنصر حيوي للحصول على الحرية الشخصية والاجتماعية والسياسية، وسوف يكمن التحدي دوماً في إيجاد التوازن بين الحقوق المدنية وإنشاء ممارسات الحماية الخاضعة للرقابة أو التدخل، إن الأمر متروك لصناع القرار السياسي، ومقدمي الخدمات، وبناة المنصات، وأنفسنا لإنشاء مجتمعات رقمية مستدامة.

خطوات العمل التي ينبغي توافرها في الجزائر، هي إنشاء هيئة وطنية للأمن السيبراني لتشجيع القطاع الخاص مع توفير المزيد من الخدمات الافتراضية مثل الخدمات المصرفية الإلكترونية، التجارة الإلكترونية.
هذا إذا علمنا أن الشركات والإدارات الأفريقية تتطور من خلال استخدام التكنولوجيا الرقمية إلى حد كبير كعامل تنافسي، الأمر الذي يعرض نظام الكمبيوتر لديها للهجمات السيبرانية، لهذا عليها في مثل هذا الموقف أن تتوخى الحذر من التهديدات السيبرانية، من خلال تعلم استكشاف وتحديد مثل هذا الهجوم[64].

كما يجب الإقرار بحجم صعوبة تحقيق الأمن السيبراني ولا ينبغي التغاضي عن الشكل المطلق بسبب التعقيد الذي يتسم به هذا المجال مع تعدد الجهات الفاعلة، ومن الجدير بالملاحظة أن الوقت قد حان لتعزيز جيل من الموارد البشرية بأقصى قدر من الكفاءة ذو مستوى عالٍ في أنظمة المعلومات وتكنولوجيا المجال الإلكتروني[65]، كون الإنترنت من خلال التصميم عبارة عن نظام موزع لا يتمتع بقلب مركزي أو نقطة تحكم مركزية، بل إن أمن الإنترنت يتحقق من خلال التعاون حيث تتخذ شركات ومنظمات وحكومات وأفراد متعددة الإجراءات اللازمة لتحسين أمن الإنترنت وجدارتها بالثقة بحيث تصبح مفتوحة وآمنة ومتاحة للجميع[66].

قائمة المراجع

1- الجمهورية الجزائرية الديمقراطية الشعبية. الجريدة الرسمية. قانون رقم 05-10 المؤرخ في 20 جوان 2005، ع44.

المؤلف المراسل [2]*: **العربي بن حجار ميلود** ، larbibenhadjar.miloud@univ-oran1.dz

2- الجمهورية الجزائرية الديمقراطية الشعبية. الجريدة الرسمية. قانون رقم 09-04 المؤرخ في 05 اوت 2009، ع 47.

3- الجمهورية الجزائرية الديمقراطية الشعبية. الجريدة الرسمية. المرسوم التنفيذي رقم 09-410 المؤرخ في 10ديسمبر 2009، ع 73.

4- الجمهورية الجزائرية الديمقراطية الشعبية. الجريدة الرسمية. مرسوم رئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015، ع 53.

5- الجمهورية الجزائرية الديمقراطية الشعبية. الجريدة الرسمية. قانون رقم 18-04 المؤرخ في 10 ماي 2018، ع 27.

6- الجمهورية الجزائرية الديمقراطية الشعبية. الجريدة الرسمية. قانون رقم 18-05 المؤرخ في 10 ماي 2018، ع 28.

7- الجمهورية الجزائرية الديمقراطية الشعبية. الجريدة الرسمية. قانون رقم 18-07 المؤرخ في 10 جوان 2018. ع 34.

8- الجمهورية الجزائرية الديمقراطية الشعبية. الجريدة الرسمية. مرسوم رئاسي رقم 19-172 المؤرخ في 06 جوان 2019، ع37.

9- الجمهورية الجزائرية الديمقراطية الشعبية. الجريدة الرسمية. مرسوم رئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، ع04.

10- الجمهورية الجزائرية الديمقراطية الشعبية. الجريدة الرسمية. مرسوم رئاسي رقم 20-442 المؤرخ في 30 ديسمبر 2020، ع82.

11- كريكط عائشة (2019) . **حق الخصوصية لمستخدم الفضاء الرقمي: المخاطر والتحديات**. في: *مجلة الحقيقة للعلوم الإجتماعية والإنسانية*، مج 18، ع02، ص ص 253-279 [على الخط] https://www.asjp.cerist.dz/en/article/95229

12- نوارة باشوش. 1140 جريمة "فايسبوكية" استهدفت نساء ووزراء ونوابا ومسؤولين. في: جريدة الشروق، 2018/11/28 [على الخط] https://www.echoroukonline.com/1140

13- ربيعي حسن (2016). **المراقبة الإلكترونية وحق الفرد في الخصوصية داخل الفضاء الرقمي**. في: *المجلة الاكاديمية للبحث والقانون*، مج 13، ع1، ص ص 409-428 [على الخط] www.asjp.cerist.dz/en/article/4991

14- مريم لوكال (2019). **الحماية القانونية الدولية والوطنية للمعطيات ذات الشخصي في الفضاء الرقمي في ضوء القانون حماية المعطيات رقم 18-07**. في: *مجلة العلوم القانونية والسياسية*، مج 10، ع1، ص ص 1304-1325 [على الخط] https://www.asjp.cerist.dz/en/article/91438

15- مرينز فاطمة (2016). **المراقبة الإلكترونية كإجراء إستدلالي في مواجهة الحق في الخصوصية**. في: *مجلة الحقيقة*، ع38، ص ص 102-115 [على الخط] https://www.asjp.cerist.dz/en/article/9236

16- عبد الرحمن بدوي (1977). منهاج البحث العلمي. ط3. الكويت. وكالة المطبوعات. ص82.

17- ABID A. ADONIS (2020). **International Law on Cyber Security in the Age of Digital Sovereignty**. In: *E-International Relations*, MAR. 14, PP1-5 [in line]https://www.e-ir.info/pdf/82169

18- Allan V. Cook, Joe Mariani, Pankaj Kishnani [et al.](July 2019). **How to begin regulating a digital reality world :Businesses and governments should guide augmented reality development**. In: *Deloitte review*, Issue 25, PP 136-145 [in line]https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-regulation.html

19- BUREAU OF ECONOMIC AND BUSINESS AFFAIRS. **Custom Report Excerpts: Algeria, Sudan, Uganda**. In: *U.S department of state* [in line] https://www.state.gov/report/custom/34cd2d0ab6/

20- Claire Vishik, Mihoko Matsubara, Audrey Plonk (2016). **Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms**, CHAPTER 11. In: Anna-Maria Osula and Henry Rõigas. *International Cyber Norms: Legal, Policy & Industry Perspectives*, NATO CCD COE Publications, Tallinn, PP 221-222 [in line] https://www.ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch11.pdf

المؤلف المراسل [*2]: **العربي بن حجار ميلود** ، **larbibenhadjar.miloud@univ-oran1.dz**

21- Dan Craigen, Nadia Diakun-Thibault, and Randy Purse (Oct. 2014). **Defining Cybersecurity**. In : *Technology Innovation Management Review*, PP 13-21 [in line] https://www.researchgate.net/publication/267631801_Defining_Cybersecurity

22- European Commission (2020). **Europe fit for the Digital Age: Commission proposes new rules for digital platforms**. 15 Dec. [in line]https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347

23- European Commission. **The Digital Services Act: ensuring a safe and accountable online environment**.[in line]https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347

24- European Commission. **The Digital Markets Act: ensuring fair and open digital markets**[in line]https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347 (consulted in 18/12/2020).

25- Jack N. and Lillian R. Berkman (1998). **The Laws of Cyberspace**. April 3, P06 [in line] https://web.cs.dal.ca/~abrodsky/7301/readings/Le04.pdf

26- Joseph Aghatise. Cybercrime definition. [in line] https://www.researchgate.net/publication/265350281_Cybercrime_definition

27- Hamid Jahankhani, A. Al-Nemrat, Amin Hosseinian-Far. **Cyber-crime Classification and Characteristics**. In book: *Cyber Crime and Cyber Terrorism Investigator's Handbook,* PP 149-164, Chapter: 12, Publisher: Elsevier, DOI: 10.1016/B978-0-12-800743-3.00012-8

28- INRIA (Jan.2019). Cybersecurity Current challenges and Inria's research directions. France: Le Chesnay Cedex, N° 03, P13 [in line] https://www.inria.fr/sites/default/files/2019-10/LB_cybersecurity_WEB.pdf

29- International Telecommunication Union (2018). Powering the digital economy: Regulatory approaches to securing consumer privacy, trust and security. In: Thematic reports : Regulatory & market environment. Switzerland: Telecommunication Development Bureau, P10 [in line]https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.POW_ECO-2018-PDF-E.pdf

30- G. NIKHITA REDDY, G.J. UGANDER REDDY. **A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGNING TRENDS ON LATEST TECHNOLOGIES** [in line] https://arxiv.org/ftp/arxiv/papers/1402/1402.1842.pdf

31- GALIT Ariel(2019). **Digitalands: Law and order in digital societies**. In: Futur-what-mic, October 11[in line]https://www.futurithmic.com/2019/10/11/digitalands-law-and-order-in-digital-societies/

32- Khaled Koubaa (*2009*.). **Global Information Society Watch**. In: *Global Information Society Watch* Uruguay : APC and Hivos, P84 [in line]https://giswatch.org/sites/default/files/algeria.pdf

33- Kaspersky Lab. What is Cyber Security?[in line] https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

34- NOURREDINE BESSADI (2019). **Cyber security in Algeria**. in: Algiers herald, MARCH 19, [in line]https://www.algiersherald.com/cybersecurity-in-algeria/

35- OSAC. **Algeria 2020 Crime & Safety Report.** in: *Country Security Report*, 6/9/2020 [in line]https://www.osac.gov/Country/Algeria/Content/Detail/Report/aceef5ea-f045-453b-8fc9-18e3d2222273

المؤلف المراسل *2: العربي بن حجار ميلود ، larbibenhadjar.miloud@univ-oran1.dz

36- OXFORD BUSINESS GROUP (2018). **Summary of relevant laws and regulations for investors in Algeria**. In: The Report Algeria [in line]https://oxfordbusinessgroup.com/overview/legal-landscape-summary-laws-and-regulations-investors-algeria
37- P.S. Seemma, S. Nandhini, M. Sowmiya. **Overview of Cyber Security**. In: *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 7, Issue 11, Nov. , PP125-128 [in line] https://www.researchgate.net/publication/329678338_Overview_of_Cyber_Security
38- Rónán Kennedy (Feb. 2016). E-**regulation and the rule of law: Smart government, institutional information infrastructures, and fundamental values**. In*: Information Polity*, vol. 21, N°01, PP 77-98 [in line]https://www.researchgate.net/publication/295834023_E-regulation_and_the_rule_of_law_Smart_government_institutional_information_infrastructures_and_fundamental_values
39- STEVE Tzikakis (2018). **Wiring the future**. In. *The Report Algeria 2018*. Algeria: oxford business group, P162.
40- The Council of Europe Commissioner for Human Rights (2014). **The rule of law on the Internet and in the wider digital world**. Paris: The Council of Europe, P08 [in line]https://rm.coe.int/16806da51c
41- UNESCO, MacKinnon, Rebecca, Hickok, Elonnai , Bar, Allon[et al.](2014). **Fostering freedom online: the role of Internet intermediaries.** France: UNESCO, P30 [in line]https://unesdoc.unesco.org/ark:/48223/pf0000231162
42- we are social. digital 2020 Algeria [in line]https://datareportal.com/reports/digital-2020-algeria

الهوامش

[1] - عبد الرحمن بدوي. منهاج البحث العلمي. ط3. الكويت. وكالة المطبوعات،1977. ص82.

[2] - Claire Vishik, Mihoko Matsubara, Audrey Plonk. **Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms**, CHAPTER 11. In: Anna-Maria Osula and Henry Rõigas. *International Cyber Norms: Legal, Policy & Industry Perspectives*, NATO CCD COE Publications, Tallinn 2016, PP 221-222 [in line] https://www.ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch11.pdf (consulted in 20/12/2020).

[3] - Dan Craigen, Nadia Diakun-Thibault, and Randy Purse. **Defining Cybersecurity**. In : *Technology Innovation Management Review*, Oct. 2014, PP 13-21 [in line] https://www.researchgate.net/publication/267631801_Defining_Cybersecurity(consulted in 20/12/2020).

[4] - Kaspersky Lab. **What is Cyber Security ?**[in line] https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security (consulted in 20/12/2020).

[5] - P.S.Seemma, S.Nandhini, M.Sowmiya. **Overview of Cyber Security**. In: *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 7, Issue 11, Nov. 2018, PP 125-128 [in line] https://www.researchgate.net/publication/329678338_Overview_of_Cyber_Security(consulted in 20/12/2020).

[6] - INRIA. Cybersecurity Current challenges and Inria's research directions. France: Le Chesnay Cedex, : January 2019, N° 03, P13 [in line] https://www.inria.fr/sites/default/files/2019-10/LB_cybersecurity_WEB.pdf (consulted in 20/12/2020).

[7] - Hamid Jahankhani, A. Al-Nemrat, Amin Hosseinian-Far. **Cyber-crime Classification and Characteristics**. In book: *Cyber Crime and Cyber Terrorism Investigator's Handbook,* PP 149-164, Chapter: 12, Publisher: Elsevier, DOI: 10.1016/B978-0-12-800743-3.00012-8

المؤلف المراسل [*2]: **العربي بن حجار ميلود** ، larbibenhadjar.miloud@univ-oran1.dz

ISSN : 1112-2803
EISSN: 2602-6589

[8] - Joseph Aghatise. Cybercrime definition. [in line] https://www.researchgate.net/publication/265350281_Cybercrime_definition (consulted in 27/12/2020).
[9] - G. NIKHITA REDDY, G.J. UGANDER REDDY. **A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGNING TRENDS ON LATEST TECHNOLOGIES** [in line] https://arxiv.org/ftp/arxiv/papers/1402/1402.1842.pdf (consulted in 20/12/2020).
[10] - كريكط عائشة. **حق الخصوصية لمستخدم الفضاء الرقمي: المخاطر والتحديات**. في: *مجلة الحقيقة للعلوم الإجتماعية والإنسانية*، مج 18، ع02، ص ص 253-279 [على الخط] https://www.asjp.cerist.dz/en/article/95229 (تاريخ الإطلاع يوم 2021/01/05).
[11] - G. NIKHITA REDDY, G.J. UGANDER REDDY. **Op. Cit.**
[12] - P.S.Seemma, S.Nandhini, M.Sowmiya. Op. Cit. PP 125-128.
[13] - Jack N. and Lillian R. Berkman. **The Laws of Cyberspace**. April 3, 1998, P06 [in line] https://web.cs.dal.ca/~abrodsky/7301/readings/Le04.pdf (consulted in 18/12/2020
[14] - The Council of Europe Commissioner for Human Rights. **The rule of law on the Internet and in the wider digital world**. Paris: The Council of Europe, 2014. P08 [in line]https://rm.coe.int/16806da51c(consulted in 19/12/2020).
[15]- The Council of Europe Commissioner for Human Rights. Op. Cit. P08.
[16] - ABID A. ADONIS. **International Law on Cyber Security in the Age of Digital Sovereignty**. In: E-International Relations, MAR. 14, 2020, PP1-5 [in line]https://www.e-ir.info/pdf/82169 (consulted in 18/12/2020).
[17] - UNESCO, MacKinnon, Rebecca, Hickok, Elonnai , Bar, Allon[et al.]. Op. Cit. P30.
[18] - GALIT Ariel. **Digitalands: Law and order in digital societies**. In: Futur-what-mic, October 11, 2019 [in line]https://www.futurithmic.com/2019/10/11/digitalands-law-and-order-in-digital-societies/ (consulted in 17/12/2020)
[19] - UNESCO, MacKinnon, Rebecca, Hickok, Elonnai , Bar, Allon[et al.].Op. Cit. P32.
[20] - GALIT Ariel. Op. Cit.
[21] - UNESCO, MacKinnon, Rebecca, Hickok, Elonnai , Bar, Allon[et al.].Op. Cit. P32.
[22] - UNESCO, MacKinnon, Rebecca, Hickok, Elonnai , Bar, Allon[et al.].Op. Cit. P32.
[23] - Ibid. PP32-33
[24] - GALIT Ariel. Op. Cit.
[25] - International Telecommunication Union. Powering the digital economy: Regulatory approaches to securing consumer privacy, trust and security. In: Thematic reports: Regulatory & market environment. Switzerland: Telecommunication Development Bureau, 2018. P10 [in line]https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.POW_ECO-2018-PDF-E.pdf (consulted in 17/12/2020).
[26] - GALIT Ariel. Op. Cit.
[27] - European Commission. **Europe fit for the Digital Age: Commission proposes new rules for digital platforms**. 15 Dec. 2020 [in line]https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347 (consulted in 18/12/2020).
[28] - European Commission. **Europe fit for the Digital Age: Commission proposes new rules for digital platforms**. Op. Cit.
[29] - UNESCO, MacKinnon, Rebecca, Hickok, Elonnai , Bar, Allon[et al.]. **Fostering freedom online: the role of Internet intermediaries.** France: UNESCO, 2014, P30 [in line]https://unesdoc.unesco.org/ark:/48223/pf0000231162 (consulted in 18/12/2020).
[30] - European Commission. **The Digital Services Act: ensuring a safe and accountable online environment**.[in line]https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347 (consulted in 18/12/2020).
[31] - we are social. digital 2020 Algeria [in line]https://datareportal.com/reports/digital-2020-algeria (consulted in 19/12/2020).
[32] - NOURREDINE BESSADI. **Cyber security in Algeria**. in: Algiers herald, MARCH 19, 2019 [in line]https://www.algiersherald.com/cybersecurity-in-algeria/ (consulted in 19/12/2020).
[33] - نوارة باشوش. 1140 جريمة "فايسبوكية" استهدفت نساء ووزراء ونوابا ومسؤولين. في: جريدة الشروق، 2018/11/28 [على الخط] https://www.echoroukonline.com/1140 تاريخ الاطلاع يوم 2021/01/03
[34] - Khaled Koubaa. **Global Information Society Watch**. In: *Global Information Society Watch 2009*. Uruguay: APC and Hivos, 2009. P84 [in line]https://giswatch.org/sites/default/files/algeria.pdf (consulted in 19/12/2020).
[35] - Khaled Koubaa.Op. Cit. P84.

المؤلف المراسل [*2]: **العربي بن حجار ميلود** ، larbibenhadjar.miloud@univ-oran1.dz

[36] - Ibid.

[37] - Rónán Kennedy. E-**regulation and the rule of law: Smart government, institutional information infrastructures, and fundamental values**. In*: Information Polity*, Feb. 2016, vol. 21, N°01, PP 77-98 [in line]https://www.researchgate.net/publication/295834023_E-regulation_and_the_rule_of_law_Smart_government_institutional_information_infrastructures_and_fundamental_values (consulted in 18/12/2020).

[38] - OXFORD BUSINESS GROUP. **Summary of relevant laws and regulations for investors in Algeria**. In: The Report Algeria 2018 [in line]https://oxfordbusinessgroup.com/overview/legal-landscape-summary-laws-and-regulations-investors-algeria (consulted in 19/12/2020).

[39] - الجمهورية الجزائرية الديمقراطية الشعبية. الجريدة الرسمية. قانون رقم 18-05 المؤرخ في 10 ماي 2018. ع 28، ص ص 04-10.

[40] - STEVE Tzikakis. **Wiring the future**. In. *The Report Algeria 2018*. Algeria: oxford business group, 2018. P162.

[41] - الجمهورية الجزائرية الديمقراطية الشعبية. الجريدة الرسمية. مرسوم رئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015، ع 53، ص ص 16-20.

[42] - الجمهورية الجزائرية الديمقراطية الشعبية. الجريدة الرسمية. مرسوم رئاسي رقم 19-172 المؤرخ في 06 جوان 2019، ع37، ص 05.

[43] - الجمهورية الجزائرية الديمقراطية الشعبية. الجريدة الرسمية. قانون رقم 18-07 المؤرخ في 10 جوان 2018. ع 34، ص ص 11-23.

[44] - OXFORD BUSINESS GROUP.Op. Cit.

[45] - UNITED NATIONS. **E-GOVERNMENT SURVEY 2020: DIGITAL GOVERNMENT IN THE DECADE OF ACTION FOR SUSTAINABLE DEVELOPMENT**. New York : UNITED NATIONS, 2020, P180 [in line]https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf (consulted on 02/01/2021).

[46] - الجمهورية الجزائرية الديمقراطية الشعبية. الجريدة الرسمية. قانون رقم 05-10 المؤرخ في 20 جوان 2005، ع44، ص17.

[47] - الجمهورية الجزائرية الديمقراطية الشعبية. الجريدة الرسمية. قانون رقم 09-04 المؤرخ في 05 اوت 2009، ع 47، ص5.

[48] - الجمهورية الجزائرية الديمقراطية الشعبية. الجريدة الرسمية. المرسوم التنفيذي رقم 09-410 المؤرخ في 10 ديسمبر 2009، ع 73، ص4.

[49] - الجمهورية الجزائرية الديمقراطية الشعبية. الجريدة الرسمية. قانون رقم 15-04 المؤرخ في 01 فيفري 2015، ع 06، ص6.

[50] - الجمهورية الجزائرية الديمقراطية الشعبية. الجريدة الرسمية. قانون رقم 18-04 المؤرخ في 10 ماي 2018، ع 27، ص ص 03-33.

[51] - Oxford business group. Algerian ICT expands on digitisation and cyber security. In: This article is from the ICT chapter of The Report: Algeria 2018 [in line]https://oxfordbusinessgroup.com/overview/increased-competition-alongside-digitisation-and-cybersecurity-efforts-arrival-new-players-has(consulted on 03/01/2021).

[52] - الجمهورية الجزائرية الديمقراطية الشعبية. الجريدة الرسمية. مرسوم رئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، ع04، ص06.

[53] - ربيعي حسن. **المراقبة الإلكترونية وحق الفرد في الخصوصية داخل الفضاء الرقمي**. في: *المجلة الاكاديمية للبحث والقانون*، 2016، مج 13، ع1، ص ص 409-428 [على الخط] www.asjp.cerist.dz/en/article/4991 (تاريخ الإطلاع يوم 2021/01/05).

[54] - مريم لوكال. **الحماية القانونية الدولية والوطنية للمعطيات ذات الشخصي في الفضاء الرقمي في ضوء القانون حماية المعطيات رقم 18-07**. في: *مجلة العلوم القانونية والسياسية*، 2019، مج 10، ع1، ص ص 1304-1325 [على الخط] https://www.asjp.cerist.dz/en/article/91438 (تاريخ الإطلاع يوم 2021/01/05).

[55] - الجمهورية الجزائرية الديمقراطية الشعبية. الجريدة الرسمية. مرسوم رئاسي رقم 20-442 المؤرخ في 30 ديسمبر 2020، ع82، ص13.

[56] - Oxford business group. **Algerian ICT expands on digitisation and cyber security**. In: *This article is from the ICT chapter of The Report: Algeria 2018* [in line]https://oxfordbusinessgroup.com/overview/increased-competition-alongside-digitisation-and-cybersecurity-efforts-arrival-new-players-has(consulted on 03/01/2021).

المؤلف المراسل [*2]: **العربي بن حجار ميلود** ، **larbibenhadjar.miloud@univ-oran1.dz**

[57] - The knowledge academy. Cyber Security Training – Algeria [in line]https://www.theknowledgeacademy.com/dz/courses/cyber-security-training/(consulted on 03/01/2021).

[58] - Cyber Talents. Algeria National Cybersecurity CTF 2020. 22 August 2020 [in line]https://cybertalents.com/competitions/algeria-national-cybersecurity-ctf-2020 (consulted on 03/01/2021).

[59] - Djilali Idoughi. **TOWORDS AN ALGERIAN E-GOVERNMENT STRATEGY AND ACHIEVEMENTS**. in : *INTERNATIONAL JOURNAL OF eBUSINESS AND eGOVERNMENT STUDIES* Vol 5, No 1, 2013, PP 88-97 [in line]https://www.researchgate.net/publication/264436569_TOWORDS_AN_ALGERIAN_E-GOVERNMENT_STRATEGY_AND_ACHIEVEMENTS (consulted on 02/01/2021).

[60] - مرينز فاطمة. **المراقبة الإلكترونية كإجراء إستدلالي في مواجهة الحق في الخصوصية**. في: *مجلة الحقيقة*، ع38، ص ص 102-115 [على الخط] https://www.asjp.cerist.dz/en/article/9236 (تاريخ الإطلاع يوم 2021/01/05).

[61] - Allan V. Cook, Joe Mariani, Pankaj Kishnani [et al.]. **How to begin regulating a digital reality world: Businesses and governments should guide augmented reality development**. In: *Deloitte review*, Issue 25, july 2019, PP 136-145 [in line]https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-regulation.html (consulted in 19/12/2020).

[62] - BUREAU OF ECONOMIC AND BUSINESS AFFAIRS. **Custom Report Excerpts: Algeria, Sudan, Uganda**. In: *U.S department of state* [in line] https://www.state.gov/report/custom/34cd2d0ab6/(consulted in 19/12/2020).

[63] - BUREAU OF ECONOMIC AND BUSINESS AFFAIRS. Op. Cit.

[64] - Hana Saada. Cyber security in Africa highlighted in Algiers. In: DZ breaking, June 11, 2019 [in line]https://www.dzbreaking.com/2019/06/11/cyber-security-in-africa-highlighted-in-algiers/(consulted on 03/01/2021).

[65] - Youcef Bougherara. **Cybernitic Security: the Algerian Strategy of Security and Defence in the Cyber Space**. In: *Journal of Afro Asian Studies*, April 2020 [in line]https://www.politics-dz.com/en/cybernitic-security-the-algerian-strategy-of-security-and-defence-in-the-cyber/ (consulted on 03/01/2021).

[66] - Olaf Kolkman. Major Initiatives in Cyber security' Shows Everyone Can Contribute to Trust. In: Internet society, 10 January 2020[in line]https://www.internetsociety.org/blog/2020/01/major-initiatives-in-cybersecurity-shows-everyone-can-contribute-to-trust/?gclid=Cj0KCQiA88X_BRDUARIsACVMYD-vMdWLBoe1-zbSvgCwgypwTCtWDoZH5lD-qZ_DAwJ5Utc_XXaOijQaAndMEALw_wcB (consulted on 03/01/2021).

المؤلف المراسل [*2]: **العربي بن حجار ميلود** ، larbibenhadjar.miloud@univ-oran1.dz