الخصوصية الرقمية خلال الأزمات: الواقع والتحديات (أزمة كورونا نموذجا)

Digital privacy during crises: Reality and challenges Case for Coronavirus pandemic

ط.د/ سليم دحماني *
جامعة الوادي -الجزائر-
dahmani-salim@univ-eloued.com

د/ الصادق جراية
جامعة الوادي –الجزائر-
sssadok83@gmail.com

تاريخ الاستلام:2022/02/23 تاريخ القبول للنشر: 2022/04/08 تاريخ النشر: 2022/05/30

ملخص:

تحاول هذه الورقة البحثية تسليط الضوء على واقع الخصوصية في الفضاء السيبراني في ظل تنامي المراقبة الشاملة خلال جائحة كورونا (كوفيد-19) والتحديات التي تُواجه حماية البيانات الشخصية، فقد كثفت الحكومات (خاصة في الصين) من عمليات جمع ومشاركة البيانات الشخصية للأفراد عبر العالم تحت ذريعة إنقاذ الأرواح، مما يُشكل تهديداً للحق في الخصوصية ويُضعف من حماية البيانات الشخصية. وقد تم الاعتماد في هذه الورقة على المنهج الوصفي الاستكشافي، من خلال القيام بقراءة للإجراءات التي اعتمدتها الدول في تعزيز المراقبة الشاملة أثناء الجائحة، ورصد تحذيرات وتقارير المنظمات والهيئات المدافعة عن الخصوصية. ولقد توصلنا من خلال هذه الورقة إلى أن الخصوصية الرقمية مهددة بشكل كبير، وتواجه تحديات مستقبلية صعبة خاصة في ظل الأزمات.

الكلمات المفتاحية: الخصوصية؛ المراقبة الشاملة؛ الفضاء السيبراني؛ كوفيد-19؛ الأمن.

Abstract:

This paper attempts to highlight the reality of privacy in cyberspace coinciding by the growing of mass-surveillance during the Corona pandemic (covid-19) and challenges facing personal data protection, governments (specially China) have intensified processes of collecting and sharing personal data of individuals across the world for reasons to save lives, starting in China (the source of the virus) and reaching the rest of the world, which threatens the right of privacy and weakens personal data protection.

This paper has been relying on the exploratory descriptive approach, through a reading of the measures adopted by governments to strengthen the mass-surveillance during the Coronavirus pandemic, and monitoring the warnings declared and reports of organizations and bodies defending privacy.

We have concluded through this paper that digital privacy is greatly threatened and confronts difficult challenges in future, especially during international crises.

***key words**: privacy; mass-surveillance; Cyberspace; covid-19; security.*

* المؤلف المراسل

مقدّمة:

يعيش العالم منذ نهاية العام 2019 تحديات كبيرة على عدة مستويات (صحية، اقتصادية، اجتماعية، سياسية وأمنية)، وتُعتبر أزمة فيروس كورونا المستجد (كوفيد 19) المحك الحقيقي لقدرة الدول والمجتمعات على التعامل مع الأزمات في إطار احترام حقوق الإنسان.

من جهة أخرى، تعتبر التهديدات السيبرانية وخاصة التجسس والسطو على البيانات من أبرز التحديات الأمنية في الألفية الثالثة، ذلك أن البيانات هي محور العمليات في الفضاء السيبراني، لذلك لجأت الدول - في اطار سعيها للسيطرة على الفيروس والتقليل من عدد المصابين والوفيات- إلى برامج وأجهزة للمراقبة الشاملة للأفراد، بغرض جمع أكبر قدر من البيانات والمعلومات من أجل وضع الاستراتيجيات والإجراءات الصارمة للحد من تفشي الفيروس.

كانت الصين سباقةً في توظيف التقنيات الحديثة في تحديد وعزل المصابين، إضافة إلى تحول العديد من الموظفين إلى نظام العمل عن بعد، ما مكنها من السيطرة على الفيروس إلى حد كبير، ما جعل بقية دول العالم تتسابق الى توظيف تكنولوجيا جمع البيانات حول مواطنيها بشكل واسع، لكن هذا التهافت على البيانات الشخصية للأفراد أثار مخاوف لدى كل من خبراء الأمن السيبراني، الأفراد والمنظمات المدافعة على حرية الأنترنيت والخصوصية الرقمية، مشككين في قدرة الحكومات والشركات على حماية هذه البيانات من خطر التجسس، أو استعمالها بشكل سيء من طرف أطراف أخرى.

خلقت الخروقات المتتالية والكبيرة للبيانات جواً من عدم الثقة، وأصبحت تُشكل تهديداً فعلياً لخصوصية الأفراد، هذا ما يؤثر على الأعمال والمعاملات التي تتم عبر الفضاء السيبراني، ومن هذا المنطلق نطرح التساؤل التالي: **ما هو واقع الخصوصية الرقمية خلال جائحة كورونا ؟ وماهي أبرز التحديات المستقبلية لحمايتها؟**

منهج البحث:

من أجل معالجة الاشكالية المطروحة، يستخدم البحث المنهج الوصفي الاستكشافي، بهدف وصف واقع الخصوصية الرقمية واستكشاف أهم التحديات التي تواجهها في ظل الأزمات التي يواجهها العالم.

فرضيات البحث:

1. تميل الحكومات عموماً إلى تغليب الجانب الأمني على الحرية والحق في الخصوصية الرقمية ويزداد هذا التفضيل حدة أثناء الأزمات.
2. يتوقف تعزيز الحق في الخصوصية الرقمية على تضافر الجهود بين الحكومات وأصحاب المصلحة في المجالات التشريعي، التنظيمي والتقني.

أهداف البحث:

تهدف الدراسة إلى:

- توضيح مفهوم الخصوصية الرقمية على أنه حق من حقوق الإنسان الأصيلة والتي لا يمكن التنازل عنه، ورصد أهم التشريعات والهيئات التي تدافع عن هذا الحق وتحميه.
- كشف واقع الخصوصية الرقمية عبر دول العالم والطرق والأساليب التي تهدد الحق في الخصوصية خاصة الرقابة الشاملة في ظل أزمة كورونا.
- رصد التحديات التي تواجهها الخصوصية الرقمية، سواء تعلق الامر بالجانب التشريعي والتنظيمي أو بالجانب التقني.

المبحث الأول

الخصوصية الرقمية: المفهوم وطرق الحماية.

في ظل تصاعد سرعة وحجم تجميع البيانات الشخصية من طرف الشركات والحكومات، تُثار مسألة الحفاظ على الخصوصية الرقمية بالموزاة مع عمليات المراقبة الشاملة التي تقوم بها الدول خاصة في ظل جائحة فيروس كورونا المستجد، يعالج هذا المبحث مفهومي الخصوصية الرقمية والمراقبة الشاملة، كما يقدم أهم القوانين والتشريعات والهيئات التي تسعى لحماية هذا الحق.

المطلب الأول: مطارحة مفاهيمية ثنائية: الخصوصية الرقمية، المراقبة الشاملة.

الفرع الأول: مفهوم الخصوصية الرقمية

تعتبر الخصوصية حق أصيل من الحقوق الأساسية للفرد، ورغم صعوبة تحديد مفهوم موحد للخصوصية إلا أنها في العموم تتعلق بشكلين مهمين، أولاً بالمعلومات والبيانات التي نحتفظ بها في حياتنا، وثانياً بالطريقة التي يتصرف بها الآخرون بمعلوماتنا التي يمتلكونها ومن له الحق في الاطلاع عليها وبأية شروط يمكن معرفتها.

أما في الفضاء السيبراني الذي أصبح يشمل جُل مناحي الحياة الإنسانية، فنجد أن مصطلح "**الخصوصية الرقمية**" يعني نقل ما يتعلق بالخصوصية في الواقع المادي إلى الفضاء الرقمي، حيث يترتب عليه بالضرورة مبدأ "**الحق في الخصوصية الرقمية**".

يُعرف المفكر "**آلان واستن Alen westen**" الخصوصية الرقمية بانها:" **حق الفرد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنه للآخرين**"[1]، فالخصوصية في العصر الرقمي تتعلق بطريقة جديدة لتمثيل البيانات، وتخلق تحديات جديدة في تعقب أو استرجاع أو حتى قابلية محو ونسيان البيانات، كما يقدم القانوني "**ميللر Miller**" تعريفا آخر للخصوصية الرقمية، حيث يقول بأنها:" **قدرة الأفراد على التحكم في دورة المعلومات المتعلقة بهم**"[2]، أي انه يحصر التحكم في البيانات الخاصة على الأفراد المنتجين لها دون غيرهم.

إن الحق في الخصوصية يتعلق بمسألة الاختيار وامتلاك القدرة على التحكم بالطريقة التي تقدم بها نفسك للآخرين في الفضاء السيبراني.

الفرع الثاني: مفهوم المراقبة الشاملة

ورد في تقرير معني بتعزيز وحماية الحق في حرية الرأي والتعبير لـ "**فرانك لارو**" مقدم لمجلس حقوق الإنسان التابع للأمم المتحدة، تعريفا للمراقبة بأنها: "**مراقبة واعتراض وجمع وحفظ واستبقاء المعلومات التي تم نقلها أو الاعتماد عليها أو إنشاؤها عبر شبكات الاتصالات**"[3]، ونركز في دراستنا هذه على المراقبة الشاملة في الفضاء السيبراني التي تقوم بها الدولة ووكالات الاستخبارات ضد الأفراد في جميع أنحاء العالم تحت ذريعة التصدي لفيروس كورونا.

يصف المدير السابق لوكالة الأمن القومي الأمريكية NSA "**كيث ألكسنجر**" في حديثه عن عمل الوكالة للتنبؤ بالعمليات الإرهابية بـ " أنت تحتاج إلى كومة قش للبحث فيها عن إبرة[4]"، وهذا ما يشرح مع مبدأ عمل وكالات الاستخبارات في الفضاء السيبراني "اجمع كل شيء، واستفد من كل شيء".

المطلب الثاني: حماية الخصوصية في الفضاء السيبراني

رغم أن مخاوف الخصوصية وحماية البيانات الشخصية غالبا ما تتداخل مع المخاوف الأمنية إلا أنها ظلت مكفولة كحق أصيل من حقوق الإنسان، واستجابة للتحديات التي فرضها العالم الرقمي والتطورات التقنية الحديثة صدرت العديد من القوانين والتشريعات لحماية

الخصوصية الرقمية، إضافة إلى قيام العديد من المنظمات والهيئات بمهمة الدفاع عن الخصوصية والمطالبة بحماية البيانات في الفضاء السيبراني.

الفرع الأول: القوانين والتشريعات التي تحمي الخصوصية الرقمية

أولاً: على المستوى العالمي

ينص **الاعلان العالمي لحقوق الانسان** وفي المادة 12 منه على أنه: "**لا يجوز تعريضُ أحد لتدخُّل تعسُّفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته، ولا لحملات تمسُّ شرفه وسمعته. ولكلِّ شخص حقٌّ في أن يحميه القانونُ من مثل ذلك التدخُّل أو تلك الحملات**"[5]، كما جاء **العهد الدولي الخاص بالحقوق المدنية والسياسية** للتأكيد على حماية الحق في الخصوصية، وهذا في مادته 17[6].

لكن الطبيعة غير الملزمة لهذه القوانين تبقي تطبيقها رهناً لإرادة الدول، والتي غالبا ما تتذرع بالقانون الداخلي والأمن القومي لانتهاك خصوصية الأفراد.

ثانياً: على المستوى الاقليمي

تعتبر اللائحة العامة لحماية البيانات (***GDPR***) التغيير الأكبر والأبرز في التشريعات الإقليمية والدولية المتعلقة بخصوصية البيانات، فهي تعطي المستخدمين قدراً أكبر من الحرية في تحديد كيفية استخدام معلوماتهم وبياناتهم الشخصية، وهي اتفاقية ملزمة لجميع دول الأعضاء الاتحاد الاوروبي دخلت حيز التنفيذ في 25 ماي 2018.

تضع اللائحة القواعد المتعلقة بحماية الاشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية والقواعد المتعلقة بحرية حركة البيانات، كما تحمي الحقوق والحريات الأساسية للأشخاص الطبيعيين وخاصة حقهم في حماية بياناتهم[7]، تشمل اللائحة العامة مختلف قضايا الحق في الخصوصية، غير أن مجال تطبيقها المحصور بمواطني دول الاتحاد الاوروبي يحد من أثرها، خاصة أن طبيعة الفضاء السيبراني لا تعترف بالحدود.

ثالثاً: على المستوى الوطني (الدولة)

تلتزم الدول بواجب حماية مواطنيها من التهديدات الداخلية والخارجية في إطار احترام القانون الدولي وحقوق الإنسان، وقد خلق الفضاء السيبراني تحدياً جديداً لحماية الخصوصية، حيث أعطى الدولة ميزة جمع البيانات واختراق خصوصية الأفراد بشكل كبير، وهذا ما دعى إلى وضع تشريعات وطنية لتكريس الحق في الخصوصية، حيث يحصي مؤتمر الأمم المتحدة للتجارة والتنمية أكثر 132 بلدا يمتلك تشريعا خاصا بالخصوصية[8]، من بينها الجزائر التي سنت في جوان 2018 القانون 18-07 لحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، رغم أن بنوده غير مفعلة بالكامل لطبيعة ثقافة الخصوصية الرقمية في المجتمع الجزائري[9]، وفي الغالب جاءت القوانين الوطنية لحماية الخصوصية مقسمة حسب النشاطات (خصوصية مالية، تجارية، طفولة ..)، هذا إضافة إلى مشكلة ضمان تطبيق القانون وقابليته للتعديل بناء على ما قد يَجِدُ من انتهاكات تمس الخصوصية في الفضاء السيبراني.

الفرع الثاني: المنظمات والهيئات الفاعلة في مجال حماية الخصوصية الرقمية

توجد العديد من المنظمات والهيئات الدولية (حكومية وغير حكومية) التي تهتم بقضايا حقوق الانسان عموماً، إضافة إلى مجموعة من المنظمات والهيئات المتخصصة في الدفاع على الحق في الخصوصية نذكر منها:

- **مركز معلومات الخصوصية الإلكترونية**[10] هو مركز أبحاث للمصلحة العامة في واشنطن، أنشأ سنة 1994 لتعزيز اهتمام الأفراد بقضايا الحريات المدنية الناشئة وحماية الخصوصية.

- **منظمة الخصوصية الدولية**[11] هي مجموعة لحقوق الإنسان أنشأت عام 1990 كمراقب للنشاطات المراقبة التي تقوم بها الحكومات والشركات، تهتم بقضايا التنصت، الخصوصية، وحرية المعلومات والتعبير.

- **بريفاتيرا Privaterra**[12] وهي منظمة تقدم الدعم التقني والتكوين لمنظمات المجتمع المدني في مجال خصوصية البيانات والاتصالات الآمنة وأمن المعلومات.

- **مؤسسة الحدود الإلكترونية (EFF)**[13] وهي منظمة تدافع على الحريات في الفضاء السيبراني، كما تعمل على تثقيف واضعي السياسات وعامة الأفراد حول قضايا الحريات المدنية المتعلقة بالتكنولوجيا.

- **Bits of Freedom** [14] هي منظمة للخصوصية والحقوق الرقمية مقرها أمستردام-هولندا، وتهتم بموضوعات حقوق النشر والتوازن بين تطبيق القانون والخصوصية وحرية التعبير.

- **المبادرة الأوروبية للحقوق الرقمية (EDRi)**[15] عبارة عن ائتلاف من المجموعات التي تعمل على الدفاع عن الحقوق المدنية في مجتمع المعلومات، خاصة فيما يتعلق بالإنترنت وحقوق النشر والخصوصية في الاتحاد الأوروبي.

المبحث الثاني

واقع الخصوصية الرقمية في ظل جائحة كورونا

تعد جائحة كورونا فرصة ذهبية للحكومات والشركات لإعادة توظيف سلوك مرفوض في المجتمع (جمع ومعالجة البيانات الشخصية للأفراد) في قالب جديد كإجراء لإنقاذ حياة الناس، لكن في المقابل قد تخلق أزمة حريات مدنية، إذا تم تسريبها أو استغلالها من طرف أطراف أخرى في المستقبل.

المطلب الأول: الخصوصية الرقمية المنتهكة

تزداد درجة توغل التكنولوجيا بتعقيداتها في مختلف مناحي الحياة، تلك التعقيدات جعلت من العصي على الفرد العادي فهم جميع أبعادها ومخاطرها، ولولا التسريبات التي تحدث من حين لآخر لما علمنا شيئا عن أساليب استغلال الحكومات والشركات للبيانات الشخصية للأفراد، وحجم المراقبة الشاملة التي تنتهجها الدول سواء صُنفت على أنها دول ديموقراطية أو كانت ذات نظام حكم شمولي.

الفرع الأول: التسريبات وانتهاك الحق في الخصوصية الرقمية

لعب المبلغون[16] (whistle blower) دورا أساسياً في كشف عمليات الجمع غير المبررة والكثيفة لبيانات المستخدمين، والاستعمال السيء وغير القانوني لها، مما أدى إلى تحفيز تغيير سلوك الأفراد والشركات تجاه الخصوصية وحماية البيانات، ولعل أبرز التسريبات كانت من طرف:

أولاً: ادوارد سنودن

متعاقد سابق مع وكالة الامن القومي الأمريكية (NSA)، قام سنة 2013 بكشف كم هائل من المعلومات حول نشاطات التجسس والمراقبة الشاملة التي تقوم بها الوكالة عبر العالم، حيث تجري عمليات التنصت على المواطنين الأجانب والأمريكيين، بالإضافة إلى عدد كبير من الوثائق التي تتعلق بالاستخبارات الأسترالية والبريطانية والكندية، وعمليات التنصت العالمي واختراق الخصوصية[17].

ثانياً: كريستوفر ويلي

وهو مبرمج كندي، عمل لصالح شركة "كامبريدج انالیتیکا"، وقدم تسريبات حول سوء استعمال البيانات الشخصية في الشركة، حيث قامت بالتعاون مع شركة "فيسبوك" بجمع بيانات 50 مليون مواطن (ناخب) أميركي، وتم استخدامها لتعزيز البرمجيات، التي ساعدت في استهداف الناخبين بإعلانات سياسية مخصصة، ساهمت في فوز "دونالد ترمب" في الانتخابات الرئاسية 2016[18].

إن الهدف (المبرر) الذي تستعمله الحكومات لتفعيل المراقبة الشاملة للأفراد هو إنقاذ الاروح خلال أزمة كورونا، وهو ما يعتبر صفقة جيدة وفرصة ذهبية لتبييض سمعة الجهات الحكومية والشركات بعد الفضائح التي كشفها المبلغون.

الفرع الثاني: الأمن قبل الخصوصية

لايزال الجدل قائما بين المؤيدين للمراقبة الشاملة بدواعي الأمن القومي، والمعارضين لها من أنصار الحق في الخصوصية والحريات العامة، حيث تُسبب جدلية الأمن والخصوصية قلقاً متزايدا على الصعيد العالمي بين الحكومات والأنظمة بصنفيها الديموقراطية والاستبدادية من جهة، والأفراد والهيئات المدافعة على الحق في الخصوصية من جهة أخرى.

ينطلق المدافعون عن الخصوصية الرقمية من نقد لأخلاقيات وفلسفة المراقبة الشاملة التي تنتهجها الحكومات والشركات، حيث يرون أن الفكرة مستمدة من الـ"بانوبتيكون Panopticon"[19] للفيلسوف وعالم الاجتماع الانجليزي "جيريمي بنثام" وهو تصميم لسجن يحتوي على برج مراقبة مركزي ومخفي، يمكن من مراقبة جميع السجناء دون ان يعلموا إن كانوا مراقبين أم لا، هذه الفكرة ألهمت الفيلسوف "ميشال فوكو" للحديث حول سيكولوجية جماعية من الخوف والمراقبة المستمرة سماها "المجتمعات التأديبية"[20]، حيث يفقد الأفراد خصوصيتهم في

ظل المراقبة الشاملة والمستمرة، مايتنج نوعا من الهمينة والتنميط والسيطرة على المجتمعات، أو ما يسميه الفيلسوف جيل دولوز "مجتمعات المراقبة"[21] حيث الكل مراقب والكل تحت السيطرة.

يُقر المدافعون عن الخصوصية بصعوبة عمل رقابة على المراقبة الشاملة (خاصة في الدول المتقدمة تكنولوجياً) حيث تتناقص الشفافية حول عمليات جمع البيانات وكيفية استعمالها، نظراً للتطور التكنولوجي السريع في طرق وأساليب المراقبة، إضافة إلى عدم مواكبة آليات الحماية والرقابة لهذه التطورات، رغم ذلك فهم يدعون إلى خلق توازن بين المراقبة من أجل الأمن والخصوصية بحيث تكون متوافقة مع حقوق الإنسان والحريات العامة.

في الجهة المقابلة، ينظر مؤيدو المراقبة (الحكومات، وكالات الاستخبارات، أصحاب المصلحة) على أنها ضرورة سياسية (أمنية) وتحظى بشعبية انتخابية، في ظل تنامي خطر التهديدات الأمنية الجديدة (الارهاب، الجريمة المنظمة، الجماعات المتطرفة...إلخ)[22]، فإبقاء عمليات جمع البيانات والمراقبة في سرية تامة بعيداً عن أعين الجمهور والأعداء يعتبر من أولويات حماية الأمن القومي، لذلك تسعى الحكومات إلى **مأسسة وشرعنة** المراقبة الشاملة **وأمننة** ما تراه يتوافق مع سياساتها العامة وأهدافها من قضايا مختلفة، ووضعها في إطار قانوني مدفوع بالضرورات الأمنية، حيث سنّت العديد من الدول قوانين تؤطر عمليات المراقبة الشاملة مباشرة عبر الأجهزة الحكومية (مثل: الصين وروسيا) أو عبر شركات التكنولوجيا (الولايات المتحدة الأمريكية).

وعليه، فعمليات المراقبة الشاملة وجمع البيانات تتم بطرق متشابهة في الدول الديمقراطية والاستبدادية على حد سواء، تحت مبررات الأمن القومي، غير أن الديمقراطيات تميل إلى تبرير سياسات المراقبة للحفاظ على المكاسب الانتخابية، أما الدول الاستبدادية فتعطي هامشاً ضيقاً من الخصوصية لتجنب الاضطرابات الاجتماعية.

المطلب الثاني: المراقبة الشاملة في دول العالم أثناء جائحة كورونا

إن القدرة على معرفة **موقع الفرد** والتنبؤ **بسلوكه** لا تقدر بثمن لكل من شركات التكنولوجيا والحكومات (بالأخص في الولايات المتحدة والصين)، لأنها المفتاح في عمليات استهداف الأفراد بالإعلانات التجارية أو بالصواريخ الموجهة.

الفرع الأول: الصين، دمج الصحة العامة والمراقبة الشاملة والأمن

غالبا ما يشعر الوافدون على الصين بأنهم مراقبون، يقول الخبراء بأنه شعور يجب على الفرد التعود عليه، فالصين دأبت منذ بداية الألفية الثالثة على تطوير منظومة المراقبة الأمنية الشاملة، وهي تعتمد استراتيجية "فانغ كونغ" أو "الوقاية والسيطرة"[23] أي: الوقاية من التهديدات مهما كانت طبيعتها عبر السيطرة على الجماهير.

مع بداية جائحة كورونا، حددت الصين رؤيتها لقضايا الصحة، الأمن والخصوصية، حيث اعتبرت فيروس كورونا تهديداً أمنياً من الدرجة الأولى، وسخرت ترسانة تكنولوجية ضخمة لمواجهته، حيث كثفت الحكومة من عمليات جمع البيانات حول درجة حرارة الأفراد، وتحركاتهم، وتواصلهم الاجتماعي.

تتكون هذه الترسانة من[24]:

- **المستشعرات الذكية وتطبيقات الصحة**: جمع كل المعلومات الصحية حول الأفراد.
- **البيانات الضخمة وتقنيات التعرف على الوجوه**: معرفة تحركات الأفراد، تاريخ سفرهم، مكان تواجدهم، توجيههم ..
- **تطبيقات التتبع للهواتف المحمولة**: معرفة أماكن تواجد الأفراد ورسم خريطة تفاعلية لانتشار الوباء وتحديد مواقع المصابين.
- **الروبوتات والدرون** : تقوم بالعمليات اللوجستية، وتوجيه الافراد.

تتكامل كل هذه التقنيات وتشكل قاعدة بيانات مركزية ضخمة، تتحكم فيها الحكومة وتستعملها في تسيير الجماهير، رغم ما تُبديه الشركات التكنولوجية الكبرى في الصين مثل Alibaba وTencent من المقاومة لعمليات مشاركة قواعد بياناتها مع الحكومة لما يشكله من ضرر على سمعتها العالمية.

لقد سيطرت الصين على تفشي الوباء، لكن كان الثمن باهظاً، لأن **أمننة** الوباء تمنح الحكومة الصينية صلاحيات غير محدودة للمراقبة والوصول الى البيانات الشخصية للأفراد ومن ثم تطبيق عمليات الضبط الاجتماعي داخل البلاد، وهذا ما يهدد الخصوصية بشكل كبير.

الفرع الثاني: انتشار تقنيات التتبع عبر الهواتف في العالم

تعتبر الولايات المتحدة مهد الانترنيت، حيث يمكنها الوصول إلى معظم البيانات حول العالم، كما تقوم وكالات الأمن والاستخبارات الامريكية بجمع أكبر قاعدة بيانات حول الأفراد، حسب تسريبات سنودن، لكن هذه العملية تتم بطريقة غير قانونية، نظرا لأن شركات التكنولوجيا هي من تسيطر فعليا على هذه البيانات، وغالبا ما تحدث مشاكل بين وكالات الأمن الحكومية وشركات التكنولوجيا حول شرعية الاطلاع واستعمال هذه البيانات، ومثال ذلك النزاع القانوني بين مكتب التحقيقات الفيدرالي FBI وشركة آبل Apple حول فك شيفرة هواتف أيفون لغرض أمني، إلا أن الشركة بدأت مؤخرا في الرضوخ إلى طلبات المحققين[25].

من جهة أخرى، قدمت كل من شركتي قوقل Google، وآبل Apple منصة مجانية للتتبع عبر الهواتف النقالة لاستخدامها في تطوير تطبيقات خاصة بكورونا[26]، لكن هذا عزز المخاوف من استعمالها من طرف حكومات شمولية في تتبع المعارضين السياسيين والحد من الحريات العامة أو من منظمات إجرامية في تصفية المناوئين لها أو ابتزازهم.

أما بالنسبة لدول الاتحاد الاوروبي، فطريقة التعامل مع الجائحة كانت متفاوتة، وغاب التعاون بين دول الاتحاد، حيث انعكس ذلك على طرق وحجم المراقبة في الفضاء السيبراني حسب الدول، حيث تعددت برامج التتبع عبر الهاتف وانقسمت أهدافها الى:

- تطبيقات لجمع المعلومات حول انتشار الفيروس.
- تطبيقات للتحذير من أشخاص مصابين وتطبيق الحجر الصحي.
- تطبيقات لتشخيص أولي للمصابين بالفيروس وتتبع جهات الاتصال.

تشير الإحصائيات[27] الى ان 53% من التطبيقات في العالم لا تحدد وقت معين للتوقف عن جمع البيانات، و60% منها لا تحتوي على سياسة للخصوصية، إضافة الى أن أوروبا تحتوي على 35 تطبيق على الهواتف تراقب جهات الاتصال للمستخدمين، كما تستعمل الحكومات 13 وسيلة للمراقبة الفيزيائية (كاميرات، درون ..) للمواطنين، وهذا ما يجعل انتهاك الخصوصية أمراً واقعاً.

تتأكد هذه المخاوف في دول أخرى من العالم، حيث تستغل الحكومات ظروف الجائحة لقمع المعارضين وتقليص حرية الرأي، فحسب وكالة "بلومبرغ" للأنباء، مررت كمبوديا قانوناً جديداً يمنح السلطة صلاحيات واسعة لمراقبة الاتصالات وفرض قيود صارمة على حرية التنقل، لتغطية عمليات اعتقال المعارضين[28].

وفي إسرائيل، سمحت الحكومة لجهاز المخابرات باستخدام نظام مصمم لمكافحة الإرهاب في تعقب هواتف ملايين المواطنين خلال الجائحة، وأُرغم الفلسطنيون على تنزيل التطبيق على هواتفهم، ووفقا لتقرير صحيفة "هآرتس" الإسرائيلية، فهذا التطبيق يسمح للجيش الإسرائيلي بتتبع تحركات الفلسطينيين والاطلاع على اتصالاتهم والرسائل التي يتلقونها عبر هواتفهم الخلوية[29].

الحقيقة أن كثيراً من الحكومات قامت بالفعل بتطوير أنظمة مراقبة رقمية واسعة قبل تفشي جائحة كورونا، واستغلت الأزمة لتعزيز هذه الانظمة وزيادة تقبلها لدى الأفراد.

المبحث الثالث

التحديات المستقبلية لحماية الخصوصية في الفضاء السيبراني.

المطلب الأول: ضبط الفضاء السيبراني

تتعدد الرؤى بين الحكومات وأصحاب المصلحة حول الطريقة الفعالة لضبط سلوك الفاعلين في الفضاء السيبراني، فالفوضى تعتبر السمة الرئيسية المميزة له، وهذا ما يجعل من عملية إدارة الفضاء السيبراني وإنفاذ القانون فيه صعبة للغاية، ونرصد في هذا السياق اتجاهين متباينين:

الفرع الأول: الو.م.أ وحلفائها (العيون الخمس)[30]

تعتبر الولايات المتحدة الأمريكية أكبر قوة سيبرانية، حيث تضم معظم شركات التكنولوجيا الكبرى في العالم، كما تنادي دوماً لجعل الفضاء السيبراني فضاءاً حراً، موثوقاً، آمناً ومفتوحاً، هذا خدمة لأهداف أمنها القومي وحماية الحق في الخصوصية لمواطنيها وخاصة الحفاظ على القيم الديمقراطية ضد تدخلات الدول الديكتاتورية مثل الصين وروسيا، كما يصرح بذلك المسؤولون الأمريكيون[31].

لكن منتقديها (على رأسهم الصين وروسيا) يرون أن ممارسات الولايات المتحدة في الفضاء السيبراني لا تعكس هذه التصريحات، فسيطرة الولايات المتحدة على آيكان ICANN الهيئة المسؤولة على تنظيم الانترنيت[32]، والخطط الأمريكية لإبعاد التكنولوجيا الصينية عن الشبكات الأمريكية (الجيل الخامس لهواوي، تطبيقات تيكتوك ووي شات) أو ما يسمى بمبادرة "**الشبكة النظيفة**"[33]، ما هو إلا محاولة من الولايات المتحدة للإبقاء على هيمنتها على الفضاء السيبراني، وهو ما يضمن لها الوصول إلى بيانات الأفراد عبر العالم دون أن يتمكن غيرها من فعل ذلك.

الفرع الثاني: الصين وروسيا وباقي دول البريكس

تدعو كل من الصين وروسيا ومن ورائها دول البريكس إلى توسيع نطاق إدارة الفضاء السيبراني، حيث يشتد الصراع على البيانات والتقنيات مع الولايات المتحدة الأمريكية، ويتبادل الطرفين التهم حول عمليات التجسس السيبراني، ومن أجل كسر هيمنة الولايات المتحدة على الفضاء السيبراني تركز كل من الصين وروسيا على قضيتين رئيستين:

أولاً: السيادة السيبرانية

والتي يقصد بها سيادة كل دولة على فضائها السيبراني، وتطبيق قانونها المحلي فيه، حيث تدافع الصين وحلفائها عن سياسة السيادة السيبرانية وأن من حق كل دولة تبني السياسة المناسبة لها، حيث جاء في الكتاب الأبيض حول الأنترنت في الصين لسنة 2010 أنه "داخل الأراضي الصينية الإنترنت تحت ولاية السيادة الصينية. وينبغي احترام وحماية سيادة الصين على الإنترنت"[34]، كما تسعى كذلك إلى بناء قوة سيبرانية بعيداً عن الهيمنة الأمريكية.

في المقابل، تواجه فكرة السيادة في الفضاء السيبراني انتقادات كبيرة، ويعتبرها المعارضون أنها محاولة لـ"بلقنة الأنترنيت" ذلك أنها تتعارض مع الأساس التي طُورت من أجله الانترنيت وهو الوصول الحر للمعلومة، إضافة إلى أن ممارسة الدولة للسيادة في الفضاء السيبراني يؤجج المخاوف من شرعنة عمليات المراقبة الشاملة للأفراد وانتهاك الخصوصية بحجة الأمن القومي، وأن الدولة أثناء ممارستها لسيادتها على فضائها السيبراني قد تقوم بانتهاك حقوق الانسان والحريات العامة.

ثانياً: الحوكمة الدولية للفضاء السيبراني (الانترنيت)

يسعى أصحاب هذا الطرح (الصين وحلفاؤها) إلى تقديم نموذج جديد لكيفية إدارة الانترنيت إعتماداً على مفهوم السيادة السيبرانية، حيث تبذل هذه الأطراف جهوداً كبيرة في سبيل حوكمة دولية للفضاء السيبراني، غير أن مفهوم الحوكمة عند الصينيين يرتبط بإعطاء الدول الكلمة العليا في تحديد المعايير والقواعد التي تسير الفضاء السيبراني (الانترنيت)، وهذا ما ترفضه الولايات المتحدة والدول الغربية[35]، والذين يرون أن حوكمة الانترنيت تعني مزيداً من مشاركة الاطراف الفاعلة وأصحاب المصلحة والمنظمات الحكومية وغير الحكومية والمجتمع المدني من أجل ضمان تعدد وجهات النظر من جهة، ومحاولة إيجاد حلول ناجعة لمشاكل الانترنيت المتعلقة بالأمن والخصوصية من جهة أخرى.

لذلك فإن التحدي الأكبر هو التقريب بين الرؤيتين، للوصول إلى تعزيز القانون الدولي لحماية الخصوصية في الفضاء السيبراني والسهر على تطبيقه، ووضع استراتيجيات دولية، إقليمية ووطنية لحماية البيانات الشخصية للأفراد، انطلاقا من الاتفاقيات الثنائية والمتعددة الاطراف ووصولا إلى اتفاقيات دولية.

المطلب الثاني: التحديات التقنية لحماية الخصوصية الرقمية

تُعتبر التحديات التقنية للخصوصية وحماية البيانات في جوهرها تحديات للأمن السيبراني، فالتهديدات التي تتعرض لها الخصوصية في الفضاء السيبراني تتطور بسرعة، وقد توسعت لتشمل وسائل التواصل الاجتماعي والهاتف المحمول، وفيما يلي بعض التحديات الناشئة لحماية البيانات والأمن السيبراني[36].

- **تعقيد البيئة المتصلة:** يزداد الفضاء السيبراني تعقيدا في طبيعته (دخول انترنيت الاشياء والمستشعرات الذكية) وإدارته وتزداد صعوبة تأمينه، وهو ما يشكل مخاطر مشتركة على الإنترنت، الأمن والخصوصية.

– **تنامي تعقيد التهديد:** دخولنا للفضاء السيبراني دائما يترك بصمات، وكلما زاد التشبيك بين الأفراد، زاد حجم البيانات التي نعهد بها لأطراف ثالثة لا نملك أي سلطة عليها، والمنافسة بين الشركات من أجل الربح تحفزها على التستر على الخروقات التي تتعرض لها وإخفاء فشلها في حماية البيانات الشخصية للأفراد.

– **انتقال التهديدات إلى الهواتف النقالة:** يستعمل الهواتف النقالة أكثر من 5.19 مليار شخص في العالم[37]، وهي تحتوي على تقنيات وتطبيقات تتبع للمعلومات الشخصية وتسجيلها وتخزينها وتحميل قوائم الاتصال والاتصالات والمعاملات، وهو ما يهدد الخصوصية بشكل خطير.

– **البيانات الضخمة:** يزداد حجم البينات المجمعة بازدياد عدد الأجهزة والمستشعرات[38]، وتعمل الشركات على تحليل هذه البيانات لحل مشكلات معينة، وهذا التحليل بدوره يولد بيانات إضافية، وكل هذا يشكل تحديا لحمايتها والحفاظ على سريتها.

– **الاستعداد المبدئي لانتهاك الخصوصية:** لا تبدي الكثير من الشركات والحكومات أولوية لمجابهة خروقات البيانات الشخصية، وعليه فإن التحدي الذي يواجه المؤسسات يتمثل في فهم أن الأمن ليس مجرد مسألة تلبية الحد الأدنى من معايير الامتثال، بل هو مسألة الانخراط في إدارة فعالة للمخاطر والتنفيذ الديناميكي للأمن.

الخاتمة

من خلال هذه الدراسة التي تطرقنا فيها إلى واقع الخصوصية الرقمية في العالم خلال جائحة كورونا، ثم عرجنا على أهم التحديات المستقبلية التي تواجه الحفاظ على هذا الحق الإنساني الأصيل، نخلص إلى أن الخصوصية في العالم الرقمي منتهكة، خاصة أن أبرز المنتهكين هي الحكومات ووكالات الاستخبارات، وهذا ما يجعل الأفراد والمجتمعات أمام تحديات كبيرة تشريعية وتنظيمية وتقنية للحفاظ على خصوصيتهم وحمايتها، وقد توصلت الدراسة إلى نتائج وتوصيات نوجزها فيما يلي:

النتائج:

– تمنح المراقبة الشاملة الحكومات قدرة تنبؤية كبيرة من خلال بيانات الافراد، وقد يكون استعمال أساليب مستوحاة من استراتيجيات الحرب (المراقبة الشاملة) بهدف إنقاذ الارواح فكرة مقبولة في المجتمع.

– تأتي الحكومات ووكالات الاستخبارات على رأس مهددات الخصوصية الرقمية والبيانات الفردية، مما يجعلنا أمام موازنة صعبة للتوفيق بين الخصوصية والأمن.

– قدمت الصين نموذجاً مغرياً (لبقية الدول) في استعمال التكنولوجيا لمحاربة فيروس كورونا، لكن الثمن كان الانتهاك الصارخ لخصوصية المواطنين الصينيين.

– لا يمكن للدول ببساطة أن تنتهك الحق في الخصوصية وحرية التعبير، بدعوى مواجهة أزمة صحية عامة، لأن دروس التاريخ تخبرنا أن الحكومات فرضت بعد احداث 11 سبتمبر أنظمة مراقبة شاملة على الأفراد بحجة الأمن فلا الأمن تحقق ولا أنظمة المراقبة زالت.

التوصيات:

– بما أن الأزمة صحية فيتوجب على مسؤولي الصحة تولي قيادة القرارات المتعلقة بإدارة البيانات وتحديد ما يجب جمعه منها وكيفية استعمالها.

– وضع مجال زمني محدد لانتهاء صلاحية البيانات، حيث يجب إلغاء إجراءات المراقبة وتدمير البيانات مع انتهاء الأزمة.

– اتخاذ تدابير وقائية لضمان الأمن السيبراني، وإبلاغ المستهلكين بالمخاطر المحتملة وكيف تم تخفيفها مما يؤدي إلى تعزيز الثقة لدى مستخدمي الإنترنت.

– إلزام شركات التكنولوجيا وصناعة الهواتف ومطورو التطبيقات بتحمل مسؤولية ضمان سلامة الأنظمة الأساسية وأنظمة الواجهة الخلفية، والبيانات الشخصية للمستخدمين.

– عدم التركيز فقط على التكنولوجيا فهناك عدة أساليب أخرى لمحاربة الجائحة.

الهوامش:

[1] توبي مندل وآخرون: **دراسة استقصائية عالمية حول خصوصية الانترنت وحرية التعبير**، الأمم المتحدة، منشورات 1 اليونسكو، فرنسا، 2013م، ص13

[2] المرجع نفسه، ص 13

[3] Frank La Rue, **Report of the Special Rapporteur on the Promotion and Protection of the Right to the Freedom of Opinion and Expression**, UN Doc A/HRC/23/40,17 April 2013, p.3.

[4] بروس شناير، **المعلومات وجالوت المعارك الخفية لتجميع بياناتك والسيطرة على عالمك**، ترجمة : أحمد مغربي،ط1، منتدى العلاقات العربية والدولية، 2017، ص 213.

[5] **الإعلان العالمي لحقوق الإنسان**، الامم المتحدة ، المادة رقم 12، على الرابط :
https://www.un.org/ar/udhrbook/pdf/UNH_AR_TXT.pdf

[6] **العهد الدولي الخاص بالحقوق المدنية والسياسي**، الأمم المتحدة، المادة رقم 17، على الرابط :
https://www.ohchr.org/AR/ProfessionalInterest/Pages/CCPR.aspx

[7] **General Data Protection Regulation**, Official Journal of the European Union, 27 April 2016, accessed: 20/05/2021, at: https://gdpr-info.eu/

[8] **مؤتمر الأمم المتحدة للتجارة والتنمية**، على الرابط: https://bit.ly/3CNAndp

[9] بهلول سمية، رمازنية سفيان. **الإطار القانوني لحماية المعطيات الشخصية للأشخاص الطبيعية في البيئة الإفتراضية في التشريع الجزائري**، المجلة الدولية للبحوث القانونية والسياسية، الجزائر، المجلد 05، العدد01، ماي2021، ص43-59.

[10] موقع مركز معلومات الخصوصية الإلكترونية https://epic.org

[11] موقع منظمة الخصوصية الدولية https://privacyinternational.org

[12] موقع منظمة بريفاتيرا https://www.prevatira.org

[13] موقع مؤسسة الحدود الإلكترونية https://www.eff.org/about

[14] موقع منظمة بيت الحرية https://www.bitsoffreedom.nl

[15] موقع المبادرة الأوروبية للحقوق الرقمية https://edri.org

[16] **المبلغ** هو الذي يقوم بالافصاح والكشف عن معلومات متعلقة بأنشطة فاسدة، أو غير قانونية، أو منطوية على مخاطر يتم ارتكابها في/ أو بواسطة منظمات في القطاع العام أو القطاع الخاص، وتثير مخاوف أو تمثل تهديدا للأفراد أو المؤسسات (منظمة الشفافية الدولية).

[17] Dominika Popielec**, From Edward Snowden to Christopher Wylie: The Face of the Second Generation Whistleblowing**, Zeszyty-Prasoznawcze, Kraków 2019, t. 62, nr 3(239), s. 39–51, p 46,47
DOI: 10.4467/22996362PZ.19.037.10739.

[18] Ibid, p 43,44,45.

[19] Bentham, Jeremy, and Miran Božovič, **The panopticon writings**, Verso Trade, 1995, p43.

[20] Foucault, Michel, **Discipline and punish: The birth of the prison**, Duke University Press, 2007.

[21] Deleuze, Gilles, **Les sociétés de contrôle**, EcoRev' 2018/1 (N° 46), 2018, p5-12.

[22]Ünver, H. Akın, **Politics of digital surveillance, national security and privacy,** Centre for Economics and Foreign Policy Studies., 2018.

[23] فرح عصام، **جاذبية الصين تتضاعف. لماذا يعد نجاح الصين في ملف "كورونا" خطرا على الديمقراطية؟**، موقع الجزيرة، تاريخ النشر: 2020/07/22، تاريخ الإطلاع: 2021/05/30 على الرابط: https://bit.ly/3kDy7ev.

[24] Aditya chaturvedi, **The China way: Use of technology to combat Covid-19**, geospatialworld, accessed: 30/05/2021, at: https://bit.ly/3f6N1sm.

[25] Joseph menn, **Apple dropped plan for encrypting backups after FBI complained**, Reuters, JANUARY 21, 2020, at: https://reut.rs/3lHMRKD.

[26] Apple & Google, **Privacy-Preserving Contact Tracing**, accessed: 02/06/2021, at: https://covid19.apple.com/contacttracing

[27] Samuel Woodhams, **COVID-19 Digital Rights Tracker**, accessed: 04/06/2021, At : https://bit.ly/3CI7dMR

[28] .....، **الرقابة بسبب كورونا قد تتحول إلى رقابة أمنية دائمة** ، موقع DW ، تاريخ النشر: 2020/06/03، تاريخ الإطلاع: 2021/06/30 ، على الرابط : https://bit.ly/35Bios0

[29] إيهاب خليفة، **المواجهة القبلية: المقاربة الذكية في مكافحة "كورونا"**، مركز المستقبل للدراسات والأبحاث المتقدمة، تاريخ النشر: 2020/03/25، تاريخ الإطلاع: 2021/05/25، على الرابط: https://bit.ly/36IvenJ.

[30] العيون الخمس (Five eyes) مصطلح يشير إلى التحالف الاستخباراتي بين: الولايات المتحدة الأمريكية، المملكة المتحدة، كندا، نيوزيلاندا واستراليا، حيث تلتزم هذه بتبادل المعلومات والبيانات الاستخباراتية فيما بينها بموجب المعاهدة البريطانية الامريكية المتعددة الأطراف سنة 1946.

[31] تصريح لوزير الخارجية الأمريكي **أنتوني ج. بلينكين** في القمة العالمية للتكنولوجيا الناشئة التي تنظمها لجنة الأمن القومي للذكاء الاصطناعي (NSCAI)، تاريخ النشر: 2021/07/13، تاريخ الاطلاع: 2021/08/10، على الرابط: https://bit.ly/3myrBKC

[32] **الآيكان** ICANN منظمة غير ربحية يقع مقرها في كاليفورنيا، مهمتها إدارة عناوين الإنترنت وأسماء المجال وتخصيص أسماء المواقع في العالم، كما تدير الموارد الرئيسية للبنية التحتية للشبكة.

[33] الشبكة النظيفة Clean Network مبادرة دعى إليها وزير الخارجية الأمريكي الأسبق **مايك بومبيو** وتتضمن استبعاد كل ما له علاقة بالتكنولوجيا الصينية عبر خمس محاور رئيسية: النواقل، متاجر التطبيقات، السحابة، الكوابل. للمزيد من المعلومات يرجى الاطلاع على الرابط: https://bit.ly/38a9t1p

[34] Xinhua, **Full Text: White paper on the Internet in China**, June 2010, accessed: 20/08/2021, at: https://bit.ly/3j9t8oh

[35] Zeng Jinghan, Tim Stevens, and Yaru Chen. **China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty**, Politics & Policy 45.3 ,2017, p432-464.

[36] Research Group**, Privacy and Cyber Security Emphasizing privacy protection in cyber security activities**, office of the Privacy Commissioner of Canada, December 2014, accessed: 25/06/2021, at: https://bit.ly/38XtjOG

[37] Simon Kemp, **Digital 2020: 3.8 billion people use social media**, wearesocial.com, accessed: 20/06/2021, at: https://bit.ly/3f5dQ0a.

[38] للاطلاع على حجم البيانات عبر المواقع والتطبيقات لسنة 2021 يرجى زيارة موقع: https://bit.ly/3g6peKS