

خصوصية البيانات في ظل مجتمع المعلومات

Data Privacy in the information society

شریقي يوسف¹، كريم حرز الله²

¹ طالب دكتوراه، مخبر المؤسسات الدستورية والنظم السياسية، المركز الجامعي تيبازة، الجزائر، cherigui.youcef@cu-tipaza.dz

أ. د، المركز الجامعي تيبازة، الجزائر، Harzallah.karim34@gmail.com

القبول: 2025-04-06

الاستلام: 2025-02-16

11/11/2017 11:11:11 AM

ملخص: أحدثت سرعة التغيرات الاجتماعية مزوجة بالتطورات التكنولوجية التي أصبحت تغطي على المعايير القانونية والأخلاقية تحولا كبيرا في العالم، أدى ذلك بظهور مجتمع المعلومات أو المجتمع الرقمي الذي تدمج فيه تكنولوجيا المعلومات وتتاح فيه الاتصالات العالمية، وتنتج فيه البيانات بكميات ضخمة، كما توزع فيه توزيعا واسعا عبر شبكة الإنترنت، ومع تزايد كمية البيانات الشخصية التي يتم مشاركتها وتخزينها ومعالجتها عبر منصات رقمية مختلفة واسعة النطاق، أصبح من الضروري فهم أهمية الخصوصية واحتمال إساءة استخدام البيانات الشخصية. وعلى هذا النحو، فإن تحقيق التوازن بين فوائد التكنولوجيا الفكرية والحاجة إلى اتخاذ تدابير لازمة لحماية الخصوصية باعتبارها حق إنساني أصيل قضية ملحة.

الكلمات المفتاحية: الحق في الخصوصية، مجتمع المعلومات، العصر الرقمي، البيانات الشخصية، الجرائم الإلكترونية.

Abstract: The rapid pace of social change coupled with technological developments that have come to overwhelm cultural and legal norms has brought about a major transformation in the world, leading to the emergence of the information society or digital society in which information technology is integrated, global communications are made available, and data is produced in huge quantities and widely distributed over the Internet. With the increasing amount of personal data being shared, stored and processed across various large-scale digital platforms, it has become imperative to understand the importance of privacy and the potential for misuse of personal data. As such, balancing the benefits of intellectual technology with the need to take necessary measures to protect privacy as a fundamental human right is an urgent issue.

Keywords: Right to privacy, information society, digital age, personal data, cybercrime.

المؤلف المراسل: شريقي يوسف، الإيميل: cherigui.youcef@cu-tipaza.dz

1. مقدمة:

تعد الخصوصية من الحقوق المتأصلة في طبيعتها، والتي تركز مبادئ وقيم العدالة والحرية والمساواة، وهي أداة جوهرية تكفل للإنسان حماية كرامته من المهانة وصيانة حقوقه وعدم المساس بشخصيته. ولقد حظي هذا الحق اهتماما كبيرا على مر الزمن سواء من جانب الهيئات والمنظمات الدولية أو من جانب الدساتير والنظم القانونية، من خلال البحث عن النصوص والتشريعات الملائمة لتوفير الحماية اللازمة للمعطيات الشخصية من الاعتداء عليها.

ومع تزايد تكنولوجيا المعلومات وتغير بيئة الاتصالات والكم الهائل من البيانات التي يجري إنتاجها وتجميعها من مختلف التطبيقات والمواقع والأنظمة الرقمية زادت المخاطر على أمن وخصوصية بيانات الأفراد التي ترتبط بضرورة احترام الحياة الخاصة عبر شبكات الانترنت والفضاء السيبراني.

فكثيرة هي البيانات الشخصية التي كانت فيما قبل منعزلة متفرقة، والوصول إليها صعبا متعذرا، تصبح في ظل مجتمع المعلومات الذي يعتمد على الذكاء الاصطناعي AI والحوسبة السحابية Cloud computing والبيانات الضخمة Big Data مجموعة متوافرة متكاملة سهلة المنال، ومعظمها متاح من أكثر ذي قبل لاستخدامها في أغراض الرقابة على الأفراد وانتهاك خصوصياتهم وترصد أعمالهم وتتبع حركاتهم بدقة عبر خوارزميات مبرمجة على أساس التمييز والأنظمة الذكية لجمع وتخزين البيانات وتحليلها ومعالجتها آليا. وهي جميعها تشكل تهديدا مباشرا وجديدا على الحياة الخاصة بصورتها المستحدثة والمتمثلة في الخصوصية المعلوماتية. خاصة إذا استغلت المعلومات والبيانات لأغراض دعائية لا سيما التجارية منها أو لأغراض إجرامية مختلفة مع إمكانية وصول الغير إلى بيانات الأفراد والتجسس عليهم دون رضاهم.

إن مجتمع المعلومات وما يشهده من تطور متسارع ومستمر في ظل عصر تكنولوجيا الرقمنة والذكاء الاصطناعي يشكل طفرة كبيرة في عالم المعرفة والتقنية وقاطرة للتطور الإنساني القادم، ولكنه في الوقت ذاته ينطوي على العديد من المخاطر ولا سيما ما يتعلق بالخصوصية التي تتصل بحقوق جوهرية أخرى كحق التعبير وحرية الرأي ومماسة حقوق الإنسان بوجه عام.

إشكالية الدراسة:

إن الإشكالية التي يعالجها موضوع البحث تتمثل في رصد مختلف التأثيرات المرتبطة بمجتمع المعلومات على الحق في الخصوصية المعلوماتية في ظل غياب حماية قانونية دولية ووطنية شاملة.

وتتجسد هذه الإشكالية على وجه الخصوص في المشكلات القانونية الناجمة عن تنامي مظاهر استخدام تكنولوجيا المعلومات التي تأتي كإفرازات للمجتمعات الرقمية المفتوحة، تحت تأثير التقنية والحداثة ومجتمع المعلومات والاتصال. وبناء على ذلك يتسنى لنا طرح الإشكالية التالية:

ما مدى تأثير مجتمع المعلومات على الحق في خصوصية البيانات في ظل عدم توفر تأطير قانوني دولي ملزم؟

أهمية الدراسة:

إن بناء أي مجتمع معلوماتي يتطلب وجود نوعاً من التفاعل الآمن بين توفير فضاء سيرياني يضمن خدمات إلكترونية عالية المستوى وبين أفراد من المجتمع يستفيدون من الخدمات. وهذا لن يتأتى إلا إن أحس الأفراد بنوع من الحماية والأمن والثقة، ومن هنا تأتي أهمية الدراسة في تسليط الضوء على الخصوصية المعلوماتية وأهميتها وكيفية حمايتها من المخاطر التي يمكن أن تواجهها في ظل المجتمعات الرقمية.

أهداف الدراسة:

يتسع هذا البحث لبلوغ عدد من الأهداف في طليعتها تبيان التحديات المثارة حول حماية الحق في الخصوصية في ظل تأثيرات تكنولوجيا المعلومات الحديثة في شتى أبعادها وعلاقاتها بالحياة الخاصة للأفراد سيما ونحن نواكب القرن الحادي والعشرين الذي جاء حاملاً معه مجتمعا افتراضياً جديداً يحمل ملامح الابتكار والتغيير والاندماج الرقمي. هذا وكذلك من خلال:

- تسليط الضوء على خصوصية البيانات الشخصية.
- الكشف عن مخاطر المجتمع الرقمي على الحق في الخصوصية.
- بيان الحماية التي تحظى بها الخصوصية.

منهجية الدراسة:

وإجابة على الإشكالية سيتم الاعتماد على التقسيم التالي، مستنداً على المنهج التحليلي والمنهج الاستنباطي.
تقسيم البحث: قصد الإجابة على الإشكالية المطروحة إرتأينا تقسيمها إلى محورين أساسيين وهما:

المحور الأول: أثار مجتمع المعلومات على خصوصية البيانات

المحور الثاني: التحديات التي يفرضها المجتمع المعلوماتي على خصوصية البيانات

2. أثار مجتمع المعلومات على خصوصية البيانات

إن انتشار التكنولوجيا وانتقال نشاط المجتمع من الواقع الفعلي المادي إلى الواقع الافتراضي السيرياني، ساهم بشكل كبير في انفجار كميات كبيرة من البيانات التي يتم توليدها أو جمعها ومشاركتها عبر منصات التواصل ومواقع الويب والانترنت، مما كان له الأثر الإيجابي في إنجاز المعاملات واستحداث المعلومات ونقل المعارف وتعزيز الشفافية والمساءلة، والتقليص من الفجوة الرقمية المتنامية بين الشعوب وتوفير فرص جديدة للاستفادة من التكنولوجيا الحديثة لا سيما في البلدان النامية وبين المجتمعات المهمشة والمتقدمة.

ولا شك أن أثر استخدام تكنولوجيا المعلومات والاتصالات التي تعتمد بالأساس على تراكم المعلومات والنفوذ المفتوح للبيانات المتعلقة بمختلف جوانب حياة الأفراد الخاصة، لم يكن إيجابياً فقط بل أثار مخاوف كبيرة تمتد لتشمل حقوق الإنسان وحياته الأساسية ومن أهمها الحق في الخصوصية وأمن البيانات الشخصية، بحيث يترك كل تفاعل بصمة رقمية يمكن استغلالها، مما أدى ذلك إلى تآكل خصوصية الأفراد والمجموعات وحتى المؤسسات، وأصبحت تتعرض باستمرار لأوجه الاستغلال العديدة من الإعلانات المستهدفة إلى خروقات البيانات.

1.2. أهمية خصوصية البيانات في المجتمع المعلوماتي

يعد الحق في الخصوصية أو الحق في حرمة الحياة الخاصة من أهم حقوق الإنسان، كما يعتبر جوهر الحقوق والحريات الشخصية التي تشكل الإطار الذي يستطيع الإنسان في داخله أن يمارس حقه في حرمة حياته الخاصة (سيد، 2019، ص 01).

وبظهور المجتمعات الرقمية واتساع الفضاء السيبراني وتزايد كمية البيانات أصبحت الخصوصية موضوعاً ذا أهمية قصوى ومصدر قلق كبير للأفراد والدول على حد سواء. ولذلك فإن إدراك أهمية الخصوصية واتخاذ الخطوات اللازمة لاحترامها وحمايتها في إطار مجتمع أمن المعلومات أمر بالغ الأهمية لضمان الكرامة الإنسانية في بيئة رقمية آمنة تعزز حرية التعبير.

ولعل من المفيد تبيان أهمية الخصوصية للبيانات الشخصية في تعزيز عدة حقوق إنسانية رئيسية في ظل مجتمع المعلومات ونذكر منها:

- تعزيز الثقة في استخدام وسائل التكنولوجيا والاتصال: ويشير ذلك إلى وجود علاقة ارتباطية طردية بين الخصوصية ومستوى الثقة في استخدام وسائل تكنولوجيا المعلومات والاتصالات، حيث كلما زادت الخصوصية وسرية البيانات زاد مستوى الثقة في مشاركة الأفراد لتجارهم الشخصية، وكلما ازدادت مشاركة البيانات، ازدادت فرص الحصول والوصول إلى المعلومات عبر الفضاء الرقمي.

- تحسين جودة حياة الأفراد في الفضاء الإلكتروني: تدرك الحكومات في ظل مجتمع المعلومات، أهمية الخصوصية وتأثيرها على الصالح العام، وتتخذ من أجل ذلك خطوات لإتاحة المزيد من الحماية للبيانات وأمن المعلومات، مما يعكس احترام الفرد ككيان مستقل وحر، بحيث يساهم ذلك في بناء بيئة رقمية آمنة تتيح للأفراد حرية التعبير وتبادل الأفكار وإثراء الحوار والتفاعلات الاجتماعية والاقتصادية (Ammon News, 2023).

1.1.2. ارتباط الفرد بالحق في خصوصية البيانات الشخصية

أصبحت البيانات الشخصية في عصر المجتمعات الرقمية جزءاً لا يتجزأ من حياة الأفراد اليومية، ومع تزايد مشاركة البيانات الشخصية عبر الإنترنت، أصبح الأفراد عرضة للكشف عن هوياتهم وبياناتهم الحميمة، فإلى جانب ذلك تتيح الخصوصية للفرد الاستقلالية والفردية في التحكم ببياناته الشخصية دون خوف، وهذا من خلال الحق في الوصول إلى بياناته

وتصحيحها أو حذفها أو تعديلها أو الاعتراض على معالجتها (شافعي، 2022، ص 115)، كما تُعصّد خصوصية البيانات حقوقاً أخرى تتصل بالأفراد وتعتبر أحد مؤشرات قياس حقوق الإنسان مثل حرية التعبير والحصول على المعلومات، وهذا لا يعني أنه وفي مجتمع أصبح فيه كل شيء مترابط بشكل متزايد، يمكن استخدام هذه البيانات للإعلان المستهدف أو سرقة الهوية أو المراقبة. ولذلك، فإن إرباط الفرد ببياناته الشخصية من خلال الحفاظ على الخصوصية أمر بالغ الأهمية لمنع مثل هذه العواقب المدمرة.

علاوة على ذلك، فإن ضمان الخصوصية يخلق بيئة رقمية يشعر فيها الأفراد بالأمان والثقة عند مشاركة التجارب الشخصية والتعبير عن الآراء أو إجراء معاملات تجارية عبر الفضاء السيبراني.

2.1.2. إرباط الدول بحماية خصوصية البيانات

أدى انتشار التقنية الحديثة والذكاء الاصطناعي في المجتمع المعلوماتي الى تعزيز قدرات الشركات الكبرى وجهات فاعلة أخرى في إمكانية جمع المعلومات وتخزينها وتحليلها، الشيء الذي أفقد نسبياً الحكومات مركزية النفوذ في تنظيم حركة نقل البيانات والتحكم في أمن المعلومات، فهذه الجهات قد يكون هدفها ربحي بامتياز ومن المحتمل أن تتاجر ببيع البيانات الشخصية المخزنة لديها لدول أخرى أو لشركات خاصة، في حين أن الوفاء بالحقوق يقع تحت مسؤولية الدول. لذا حرصت العديد من الأنظمة خاصة الديمقراطية منها على كفالة الحق في الخصوصية، واعتبرته حقاً مستقلاً قائماً بذاته.

غير أنه وبازدياد تقدم التكنولوجيا الفكرية والتضخم في محتوى البيانات الرقمية وانتشار الجرائم السيبرانية العابرة للحدود تزداد فداحة فشل الدول وهذا من جهة لعدم ضمان مدى استيعاب النصوص القانونية التقليدية للجريمة المستحدثة، ومن جهة أخرى عدم ضمان كون القوانين والتنظيمات المتعلقة بحماية الخصوصية متوافقة مع معايير حقوق الإنسان وحرية التعبير على ما ينبغي.

لذا أصبح من الضروري على الدول إيجاد تشريعات وقوانين تحد من انتشار الجرائم الماسة بالخصوصية وتعاقب مرتكبيها، كما تهتم بتعزيز وإحترام المبادئ القانونية حول كيفية حماية الحق في الخصوصية، ويشمل ذلك توفير قوانين واضحة، وتحمل مسؤولية حماية البيانات وتملك تقنيات مجتمع نظم المعلومات وضمان استخدامها والسماح للأفراد بالوصول إلى بياناتهم لأجل تعديلها أو حذفها، والمسائلة عن أي سوء استخدام للبيانات الشخصية بما فيها المعالجة الآلية للبيانات ومراقبة الاتصالات.

كما تظهر الحاجة في سياق بناء مجتمع المعلومات، تحقيق التوازن بين ضرورة اتخاذ الدول تدابير لمنع وتحاشي أي إجراء من جانب واحد لا يتفق مع القانون الدولي وميثاق الأمم المتحدة مما يعرقل التحقيق الكامل للتنمية الاقتصادية

والاجتماعية لفائدة الأفراد ويعوق رفاههم (الاتحاد الدولي للاتصالات، ص7). وتعزيز السيادة الرقمية للدول من خلال قدرة الدول على التحكم في البنية التحتية الرقمية الخاصة بها وبيانات مواطنيها (حميل، 2022، ص51).

2.2. انتهاكات خصوصية البيانات في مجتمع المعلومات

إن انتهاك الحق في الخصوصية في المجتمع المعلوماتي لا يخرج عن أربع صور، وهي: اقتحام عزلة الشخص، والكشف عن أسرار الشخص الخاصة، وادعاء الأكاذيب، والاستخدام غير المصرح به لاسم الشخص أو لصوره (الصانع، 2017، ص 12).

غير أنه ونتيجة لاتساع نطاق استخدام الوسائل التقنية الحديثة على بيانات الأفراد في مجتمع المعلومات، أحدثت تغيرات ومؤثرات اجتماعية وقيمية، أثر ذلك على مفهوم الخصوصية وتحديد نطاق حماية هذا الحق واحترامه، بعدما كان قديما لا يتعدى النطاق العائلي الخاص، بينما في عصرنا الحالي، أصبح النطاق المعلوماتي أوسعاً ثلاثة أضعاف ما كان عليه. إلا أن هذا الاتساع ساهم في تصاعد عدد الجرائم المهددة لخصوصية بيانات الأفراد ومنها التجسس، الاختراق وسرقة البيانات الشخصية وغيرها من الجرائم (القرني، ص 1047).

حيث أصبحت انتهاكات الخصوصية والنفاذ إلى محتوى البيانات ظواهر إجرامية شائعة وبشكل متزايد، مما يمكن أن يؤدي إلى كشف وسرقة وتتبع تفاصيل شديدة الخصوصية سواء تعلق الأمر بالبيانات المالية والحالة الصحية أو الآراء الدينية والسياسية بل الموقع الجغرافي والمحادثات الخاصة، وفي ذات الوقت فإن التفسيرات والفهم الشائعين عن قوانين حقوق الإنسان لم تجار القدرة المعاصرة للمجتمعات الرقمية في النفاذ إلى محتوى البيانات واستخدامها ومعالجتها.

1.2.2. جرائم خصوصية البيانات في المجتمع المعلوماتي

تشكل جرائم الخصوصية مخاطر كبيرة على الأفراد والمجتمع ككل، فكثيرة هي المجتمعات الرقمية التي أصبحت بيئة خصبة لارتكاب الفعل الاجرامي على خصوصية وسرية البيانات، حيث يتم استخدام وبطرق غير مشروعة قواعد البيانات الضخمة وتطبيقات الذكاء الاصطناعي ووسائل معلوماتية أخرى عالية المستوى ومتاحة بشكل كبير لترصد الأفراد والمجموعات في تنقلاتهم وأعمالهم، بحيث تجمع البيانات الشخصية وتخزن وتعالج خارج نطاق القانون، عن طريق استغلال نقاط الضعف في البنية التحتية داخل الشبكة بما في ذلك الأجهزة والبرامج والعوامل البشرية أو المنصات عبر الانترنت للوصول غير المصرح به الى المعلومات الشخصية، وبالتالي تعرض مجتمع المعلومات لخطر فقدان المركزية وآليات السيطرة والتحكم، وعليه يظهر بوضوح اتساع مكامن جدية احتمال وقوع التعدي على البيانات الشخصية فتصبح عرضة للخروقات والهجمات السيبرانية مما يؤثر ذلك على حماية حقوق الأفراد والمجموعات والمؤسسات والحفاظ على الثقة في النظام البيئي الرقمي للمجتمعات المعلوماتية.

فقد رافق الانتشار المتزايد لأنشطة الجهات التخريبية التطورات الهائلة لتقنية نظم المعلومات وثورة الاتصالات الرقمية وانعكست على محاور الجريمة التقليدية من حيث التركيب والأركان والعناصر أو من حيث التكييف القانوني وأساسيات الملاحقة الجزائية والعقاب.

غير أن معظم التشريعات وخاصة العربية منها تأخرت عن استيعاب الجرائم الإلكترونية التي أحدثتها مجتمعات المعلومات الماسة بالحق في الخصوصية، وذلك لاعتمادها على ماديات السلوك السلبي، وعجزها عن فهم الجريمة المستحدثة وتصور أركانها وطبيعتها وخصائصها، ويمكن أن يظهر عجز هذه التشريعات في عدة نقاط من بينها صعوبة فهم السلوك المعنوي التي تقوم عليه الجريمة السيبرانية، ضخامة الآثار السلبية الناتجة عن السلوك الجرمي، وجود بيئة رقمية جديدة مستحدثة للجريمة والسلوك الجرمي تختلف تماما عن البيئة التقليدية للجريمة، وكذلك ضعف قاعدة التكييف وقصورها عن استيعاب القوالب الجرمية المستحدثة (المناعسة، 2022، ص 15).

إن الحديث عن صور الجرائم الماسة بخصوصية البيانات في المجتمع الرقمي لا ينقطع، ولعل من أهم صورها نذكر ما يلي:

أولاً- جرائم نشر البيانات: قد تكون هناك جوانب في الحياة لا يرغب الافراد في مشاركتها مع الآخرين لأسباب بريئة للغاية، غير أنه وفي ظل مجتمع يتميز بسهولة نقل المعلومات، أصبح نشر البيانات على اختلاف أهميتها ودرجة سريتها وطريقة الحصول عليها سواء عن طريق الاختراق لنظم المعلومات أو شبكة الإنترنت سهل المنال، بحيث يتم نشر هذه البيانات على الملأ، كبيانات بطاقات الائتمان البنكية وأرقام الحسابات المصرفية التي تباع علنا على الانترنت.

كما يمكن نشر بيانات مغلوطة وغير صحيحة أو تزويرها، تتعلق بحياة الأشخاص أو معتقداتهم وآرائهم السياسية لترويج الإشاعات أو لأي غرض آخر.

ثانياً: استغلال البيانات الشخصية لنشر دعايات إعلانية أو لأغراض إجرامية: وذلك عن طريق استخدام ملفات تعريف الارتباط (كوكيز)، وتقنيات التتبع، وأدوات التحليل من قبل الشركات وتطبيقات التواصل الاجتماعي التي ترصد البيانات الشخصية لإنشاء سجل التصفح أو سجل البحث الخاص بكل فرد للتوصل الى استنتاجات خاصة به ومن ثم بث إعلانات مستهدفة عبر كلمات وصور وفيديوهات تستغل نقاط الضعف في شخصية أو سلوك الفرد.

كما يمكن أن تستخدم بيانات ائتمانية تصف قدرة الفرد على الحصول على ائتمان أو قدرته على الوفاء به أو تصف حالة زيادة الضغوط الناتجة عن الاقتطاعات الائتمانية التي تمارسها جهة التمويل على الفرد لحرمانه من الوصول إلى خدمات معينة بناء على هذه المعلومات كالتأمين الصحي.

كما يمكن استغلال تلك البيانات لإيذاء بعض الأفراد المستهدفين مثل الصحفيين والناشطين والمدافعين عن حقوق الإنسان، وهو ما ترصده مختلف المنظمات الدولية الحقوقية خاصة منظمة العفو الدولية، التي تنبه من الخطر المتنامي لاستعمالات تقنيات تكنولوجيا المعلومات خاصة في ظل الأنظمة الاستبدادية.

2.2.2. تقييم درجة الانتهاك التي تحدثها تقنيات مجتمع المعلومات

عند تقييم الانتهاكات المحتملة التي يمكن أن تحدثها تقنيات مجتمعات نظم المعلومات اتجاه الحق في خصوصية البيانات وتأثيرها بشكل عام على حقوق الإنسان والحريات الأساسية، من الضروري الأخذ في الاعتبار طبيعة هذه الانتهاكات التي ترتكب في بيئة إلكترونية أو افتراضية، التي تستند إلى اللامادة واللامكان والالزمان (بلعيا، 2022، ص320)، وتتسم بالتغيير والديناميكية والانتشار الجغرافي العابر للحدود (المصري، 2011، ص 217)، فهي تتم في وسط افتراضي يخلق صعوبات بالغة سواء في مجال اكتشافها أو مجال ملاحقة مرتكبيها (بوحليط، 2019، ص 79)، وبذلك فهي تختلف عن البيئة التقليدية المعروفة.

كذلك قدرة هذه المجتمعات على كشف البيانات المحمية، خصوصا مع الفجوة الرقمية وضعف البنية التحتية لتكنولوجيا الاعلام والاتصال، وتعدد صور البيانات بحسب عوامل الزمان والمكان، ويذكر سامح التهامي هذه الصور كالآتي: الاسم واللقب، الصوت والصورة للفرد، الأرقام الشخصية، العنوان، الحالة الاجتماعية، الخصائص الجسمانية، الحالة الصحية، الأصول العرقية، الجنسية، الآراء السياسية والمعتقدات الدينية، نتائج الاختبارات النفسية، البصمة، رقم الحساب البنكي، عنوان البريد الإلكتروني، عنوان الكمبيوتر IP، رقم الهاتف أو السيارة (التهامي، 2018، ص624). كما لا بد من اخذ في الاعتبار الغرض الذي من أجله تسعى هذه المجتمعات إلى الحصول على البيانات.

وبالتالي فإن خرق لخصوصيات الأفراد قد يؤدي إلى إفراغ حقوقا أخرى من مضمونها، بما فيها الحق في حرية التعبير والتنظيم والمشاركة في مختلف المجالات، هذا لأن هذه الحقوق تستوجب قدرة الأفراد والمجموعات على مشاركة بياناتهم بغير تعرض للتدخلات غير المشروعة أو التعسفية.

3. تحديات مجتمع المعلومات على الحق في خصوصية البيانات

أبرزت المجتمعات الرقمية مظاهر جديدة تمثلت في الانفتاح على العالم الافتراضي، وساهمت في الاندماج الرقمي والتكنولوجي والاستفادة من الوسائل الرقمية الحديثة، مما جعلت الحياة أفضل من ذي قبل، غير أنها فرضت العديد من التحديات في مواجهة حماية خصوصية الأفراد والمجموعات، سمحت بظهور صور جديدة من السلوك الإجرامي لم تكن موجودة في الماضي أدت إلى انتكاسات مروعة في مجال حقوق الإنسان، حيث جعلت من السهل من أي وقت مضى جمع واستخدام البيانات الشخصية دون معرفة الفرد أو موافقته، كذلك صعوبة الحفاظ على الخصوصية في مواجهة المراقبة المتزايدة، بالإضافة إلى ذلك، أتاح استخدام الذكاء الاصطناعي تحليل كميات هائلة من البيانات الشخصية وأدى التحيز

الخوارزمي إلى حرمان الكثير من الأشخاص من الخدمات الاجتماعية بسبب البيانات التي تعكس افتراضات عنصرية متجذرة، مما أثار مخاوف بشأن ضرورة حماية استقلالية الفرد وكرامته في ظل مجتمع رقمي آمن.

الأمر الذي يحتم على الدول تكثيف الجهود لمواجهة فعالة للتحديات التي تفرضها المجتمعات المعلوماتية المتصلة بالحق في خصوصية البيانات، وكل ما يمس بحقوق الإنسان.

وعلى إثر اتساع الجهود المبذولة لمواجهة هذه التحديات، من حيث ضرورة السعي لتكوين أرضية قانونية تعمل على حماية البيانات الشخصية للأفراد في ظل غياب قواعد قانونية تتضمن التزاما مستمرا ومتضافرا وتعاطي مع تطور تقنية مجتمع نظم المعلومات وأثرها على هذا الحق، بذلت هيئات صنع القرار العالمي جهودا كبيرة بسن العديد من التشريعات والقرارات الدولية التي تحمي الحق في خصوصية البيانات، وكانت البداية بإعلان القمة العالمية حول مجتمع المعلومات تحت رعاية الأمم المتحدة سنة 2003، ومن ثم أصدرت الجمعية العامة للأمم المتحدة قرارا بتاريخ 07 نوفمبر 2013 بعنوان "الحق في الحياة الخاصة في العصر الرقمي"، وتبعها القرار رقم 167/68 لعام 2014 بشأن الحق في الخصوصية في العصر الرقمي، وغيرها من العهود والمواثيق الدولية إلى حين صدور تقرير عن الأمم المتحدة بتاريخ 16 سبتمبر 2022 يحذر من أن حق الناس في الخصوصية يتعرض لضغوط متزايدة بسبب استخدام التكنولوجيا الرقمية الحديثة المتصلة بالشبكات، التي حولتها خصائصها إلى أدوات هائلة للمراقبة والسيطرة والقمع (الجمعية العامة، 2022، ص 4).

1.3. الالتزامات الدولية بحماية خصوصية البيانات

مما لا شك فيه أن الحاجة تتزايد إلى الحماية القانونية على المستويين الدولي والإقليمي لتعزيز حقوق الإنسان الرقمية كي تواكب المجتمع المعلوماتي، ومن بينها حماية البيانات الشخصية وأمن المعلومات وخصوصية الأفراد والمجموعات وتوفير الضمانات الأساسية لها، خاصة أن الممارسات العديدة من الدول كشفت عدم وجود تشريعات أو وسائل إنفاذ وطنية كافية، ووجود ضمانات إجرائية ضعيفة، ورقابة غير فعالة (العوضي، 2021، ص 30).

غير أنه إذا كان مفهوم حرمة الحياة الخاصة قد تطور في إطار المجتمعات المعلوماتية الذي أصبحت فيه وقائع الحياة الخاصة تدور في الفضاء السيبراني بواسطة تقنيات تكنولوجيا المعلومات والذكاء الاصطناعي وأنترنت الأشياء، فإن تطور الصكوك الدولية لحقوق الإنسان أثبتت أن احترام الحق في الخصوصية المعلوماتية وحماية حقوق الإنسان تشكل قواعد قانونية ملزمة، ترتب التزامات قانونية واضحة على عاتق الدول، وهي حصيلة توافق عالمي حول قيم إنسانية ذات طابع شامل، وبالتالي يجوز لجميع الدول أن تعتبر بأن لها مصلحة قانونية في حماية هذا الحق الذي أصبح أمر أساسي وضروري لتنمية وأمن المجتمع الدولي.

لا سيما أن الدول المختلفة قد أعربت عن رغبتها في إقامة علاقات دولية تستطيع تحقيق التعاون المشترك لحل مشكلاتها الدولية في إطار مبدأ الالتزام الدولي بحماية الحق في الخصوصية والبيانات الشخصية.

ومما لا شك فيه أن اهتمام الدول بالحق في الخصوصية المعلوماتية بات يمثل قيمة مستهدفة يقرها قانون حقوق الإنسان الدولي، حيث أصبح من الأمور الشائعة تقييم سلوك الحكومات بمدى التزامها بمجموعة من المعايير الدولية التي تحكم سلوكها في مجال إحترام خصوصيات الأفراد، ومدى قانونية إجراءات المراقبة الإلكترونية وجمع البيانات، ومدى التزامها بضرورة إتخاذ جميع التدابير اللازمة لتنفيذ التزاماتها الدولية في مجال حماية هذا الحق. إضافة إلى وجوب ملائمة الدول لتشريعاتها الوطنية وجعلها تتماشى مع المبادئ والنصوص الأساسية لاتفاقيات حقوق الإنسان في هذه المجالات الحقوقية، وأيضاً توفير وسائل التظلم القضائي والإنصاف، لتمكين كل فرد من المطالبة بتوقيع الجزاء على من يعتدي على حقوقه الرقمية أمام المحاكم الوطنية.

وإزاء الأثر السلبي لبعض الممارسات الرقابية على الحق في الخصوصية المعلوماتية، أصدرت الجمعية العامة للأمم المتحدة قرار رقم 179/73 واعتمدته بتاريخ 17 ديسمبر 2018 نص على أن: "الحقوق التي يتمتع بها الأشخاص خارج الإنترنت، بما في ذلك الحق في الخصوصية، يجب أيضاً حمايتها عبر الإنترنت، وإذ نلاحظ على وجه الخصوص أن مراقبة الاتصالات الرقمية يجب أن تكون متسقة مع الالتزامات الدولية لحقوق الإنسان وأن تستند إلى إطار قانوني يمكن للجميع الوصول إليه، بشكل واضح، دقيقة وكاملة وغير تمييزية، وألا يكون أي تقييد للحق في الخصوصية" (الجمعية العامة، ص4). وبالتالي يتعين على الدول أن تمتنع عن التدخل في خصوصية البيانات الشخصية أو تقليص التمتع بها وأن تعمل على توفير آليات قانونية وتقنية تمكنها من حماية الأفراد والمجموعات من انتهاكات الحق في الخصوصية احتراماً لالتزاماتها الدولية.

1.1.3. توفير الحماية القانونية والتقنية

يتوقف تطور المجتمع رقمياً على شعور الأفراد والمجموعات بالأمان في التعامل من خلال فضاء رقمي جدير بالثقة، ويبرز من هذا المنطلق أهمية التدخل بما يضمن تفعيل أمن مجتمع المعلومات حمايةً للحق في الخصوصية المعلوماتية، بما يحقق التوازن بين الاستعانة بقواعد قانونية حافظة لخصوصية البيانات والاستعانة بالتقنيات المعتمدة في أمن وسلامة هذا الحق.

1.1.1.3: الحماية القانونية لخصوصية البيانات: برغم كبر العمق الممكن للانتهاكات التي قد تحدثها مجتمعات تقنية المعلومات في حياة الأفراد الخاصة وعلاقاتهم وأثر ذلك السلبي على بياناتهم الشخصية، فإن معظم التشريعات تضع البيانات الشخصية في درجة أقل جدارة بالحماية ولا تضع قيوداً كافية على كيفية التنقيب فيها وتبادلها وحفظها.

حيث صار اليوم في الإمكان الكشف عن هوية الفرد وسلوكه وعلاقاته وحالته الجسدية والصحية وعرقه ولونه وميوله الجنسية وأصله القومي وآراءه، كما يمكن التعرف على مواضع تواجد الأفراد وتحركاتهم وتفاعلاتهم عبر الزمن.

ولكي تفي الدول حقاً بالتزاماتها الدولية اتجاه حقوق الإنسان فيما يتعلق بحماية خصوصية البيانات في المجتمع الافتراضي وجب عليها حمايتها وتعزيزها بذات القدر وذات الالتزام اللذين تجري بهما حماية حقوق الإنسان في العالم المادي (OHCHR, 2013)، كذلك لا بد من أخذ سرعة التطور التقني في الحسبان، وهذا الأمر يتحقق من خلال مراجعة

القوانين التي تحمي الخصوصية بشكل دوري وبصيرورة منتظمة، فما يميز القاعدة القانونية أنها قابلة للتطبيق من حيث طبيعة المكان والزمان وأحوال الأشخاص، وأنها تنشأ في نطاق بيئة اجتماعية تجعل منها تتطور معها في تقدمها وفقاً لقواعد مضبوطة وعملية سهلة التطبيق، وكل هذا يأهلها لاستيعاب وقائع الحياة المستمرة والتطورات التكنولوجية السريعة وتحويلها إلى قوالب تشريعية تساعد على تطبيق القانون في تحقيق الغرض الذي ينشده الأفراد في أن تحترم حياتهم الخاصة والعائلية ومراسلاتهم أو الحق في الاعتراف بكرامتهم أو سلامتهم الشخصية أو سمعتهم واحترامها.

وفي السياق ذاته، ينبغي على الدول إصدار قوانين تجرم المعالجة الآلية غير المشروعة للبيانات الشخصية، باعتبار أن الخصوصية الرقمية هي حقوق قانونية بامتياز وأن دور القانون لا يقتصر على إنشاء هذه الحقوق بل هو إقرارها وأن تدخل القانون يكون في إطار تنظيمي وحماي لهذه الحقوق (السعدي، 2020، ص 354).

هذا وقد كفلت العديد من اتفاقيات حقوق الإنسان العالمية حماية هذا الحق واعترفت به، على غرار الإعلان العالمي لحقوق الإنسان (المادة 12 منه) والعهد الدولي للحقوق المدنية والسياسية (المادة 17 منه). وبعبارة أخرى، هناك اعتراف عالمي بالأهمية الأساسية والصلة الوطيدة للحق في الخصوصية والحاجة إلى ضمان حماية هذا الحق في القانون والممارسة (HRC, 2014).

2.1.1.3. الحماية التقنية للبيانات الشخصية: نظراً لأهمية البيانات ودورها في الحياة اليومية للأفراد، كان لا بد من تصميم وتنفيذ تقنيات تدرج ضمن أمن مجتمع المعلومات يمكن من خلال بسط الحماية القصوى لخصوصية البيانات والحد من المخاطر التي تهددها، وذلك من خلال توفير مجموعة من المعايير التقنية مثل التشفير واستخدام الأسماء المستعارة وإخفاء الهوية، كما سنبين ذلك على سبيل المثال:

- تشفير البيانات باستخدام شبكة افتراضية خاصة (VPN): حيث تساعد هذه التقنية على تشفير حركة البيانات الخاصة بالمستخدم من خلالها تشفير البيانات المرسل والمستلمة بأمان وسرية، وإخفاء هويته الإلكترونية. وهذا أمر مهم خاصة عند إجراء المعاملات المالية أو منح التفويضات على المواقع الإلكترونية أو نقل المعلومات السرية، لأنه في مثل تلك الحالات قد يتسبب اعتراض حركة مرور البيانات من قبل أي متطفل بإحداث خسائر فادحة (kaspersky, 2024).

- تثبيت برامج موثوقة لمكافحة الفيروسات والبرامج الضارة: سيضمن برنامج مكافحة الاختراق حماية البيانات الخاصة من التهديدات الشائعة، مثل برامج تسجيل ضغطات لوحة المفاتيح وبرامج الفدية والتصيد الاحتيالي وفيروسات حصان طروادة.

- التحقق من بعض التطبيقات: تشكل بعض التطبيقات تهديدا قويا للبيانات، حيث تتطلب عند تنزيلها الإذن للوصول إلى الكاميرا والميكروفون وخدمات الموقع والاذن للاطلاع على سجل تصفح مواقع الويب وجهات الاتصال وحسابات الوسائط الاجتماعية.

وبالتالي فمن الضروري اعتماد هذه الأدوات واستخدامها لتعزيز الحق في الخصوصية وحماية البيانات الحساسة والسرية، ومع ذلك هذا لا يعني من أن تبقى الخطة والحذر أهم من كل ذلك، فليس على الأفراد وضع كل شيء على الانترنت، فكثير من المعلومات كالاسم واللقب، تاريخ ومكان الميلاد، ورقم الهاتف، غالبا ما يستخدمها الأفراد كمعرف لمواقع التواصل الاجتماعي، يحتاجها المجرمون كمدخل لسرقة الهوية وتنفيذ هجمات سيبرانية واختراق حسابات مصرفية أو بنكية.

2.1.3. القدرة على التحكم في المعلومات الشخصية

ويظهر ذلك من خلال قدرة الجهة المختصة في الدولة على اتخاذ ما يلزم من إجراءات قانونية ووسائل تنظيمية وإدارية وتقنية تضمن حماية البيانات الشخصية للأفراد وكفالة حقوقهم في نطاق تطبيق القانون.

وعلى وجه التحديد فإن الدول إذا ما سعت إلى النفاذ أو إلى استخدام بيانات محمية من شأنها أن تؤدي إلى معرفة الفرد على وجه التحديد، أو تجعل التعرف عليه ممكنا بصفة مباشرة أو غير مباشرة، حيزت بطريقة المعالجة الآلية أو المراقبة لغرض لن يعرض فردا لخطر الملاحقة الجنائية ولا التحري ولا التمييز ولا لانتهاك حقوق الإنسان، فإنه وجب عليها أن تبرهن لسلطة نزيهة كفاء أن أساليب المعالجة الأخرى الأقل انتهاكا قد استنفذت بلا جدوى وأن البيانات الشخصية المتحصل عليها ستقتصر على ما يتعلق بالغرض المطلوب وكل ما يزيد منها عن ذلك سيتلف أو يعاد إلى الشخص المعني بالمعالجة، والبيانات المتحصل عليها لن تنفذ إليها غير الهيئة المعنية ولن تستخدم في غير الغرض الذي لأجله أعطي الإذن. وفي نفس السياق فإنه وفقا لمعايير ومتطلبات محددة تنبع من حقيقة أن حماية الخصوصية المعلوماتية مسألة تنظيمية، الغرض منها حماية البيانات وحقوق الأفراد من التجاوزات والانتهاكات غير القانونية وتعزيز الثقة في التداولات والمعاملات الإلكترونية من خلال رفع مستوى تحكم الجهات المسؤولة في الدولة عن معالجة البيانات الشخصية ونقلها، يتم توفير آليات لتمكين الأفراد من ممارسة حقوقهم عند معالجة بياناتهم الشخصية، ومن بين هذه الآليات نذكر ما يلي:

- حق الأفراد بالعلم: ويشمل ذلك إحاطة الأفراد بالمسوغ القانوني لغرض المعالجة الآلية لبياناتهم الشخصية، والجهة المسؤول عن ذلك، سواء تعلق الأمر بعمليات الجمع، التسجيل، التخزين، الاسترجاع، النقل، النشر.

- الحق في الوصول إلى البيانات الشخصية.

- الحق في طلب تعديل أو إتمام أو تحديث البيانات الشخصية.

- الحق في طلب حذف أو إتلاف البيانات الشخصية فور انتهاء جهة التحكم من معالجتها.

- الحق للأفراد في الرجوع عن الموافقة على معالجة بياناتهم الشخصية، إلا إذا كانت المعالجة مطلوبة لأغراض أمنية أو لاستيفاء متطلبات قضائية.

2.3. المبادئ الأساسية لحماية البيانات في مجتمع المعلومات

إن التحديات التي يفرضها مجتمع المعلومات من شأنها أن تؤدي إلى درجة من الانتهاكات تستوجب حماية قوية من الدول تتوافق مع المبادئ القانونية التي أقرتها معايير حقوق الإنسان. تلك المبادئ التي لا ينبغي اعتبارها مجرد توصيات، بل هي أعلى من ذلك وبأنها تشكل جزءاً هيكلياً من النظم القانونية ذات الصلة بالموضوع، وتلزم هذه المبادئ المتحكمين في المعلومات ومعالجي البيانات بالتصرف على النحول الملائم لدى معالجة البيانات الشخصية، ومواجهة مخاطر إساءة استخدام تكنولوجيا المعلومات والاتصالات والذكاء الاصطناعي، وهذا ما يسمح بدوره لأصحاب البيانات بعدم فقدان تحكمهم في معلوماتهم الشخصية (الجمعية العامة، 2022، ص3).

وعلى هذا الأساس، استدعى الأمر تدخل الهيئات الفاعلة على المستوى الدولي، خاصة تلك المتعلقة بحقوق الإنسان وتبني مبادئ أساسية مشتركة، تولي العناية وتحقق الحماية الكفيلة عند معالجة البيانات الشخصية للأفراد ومحاولة منع إساءة استخدامها غير المشروع، نذكر منها ما جاءت به الأمم المتحدة في المقرر الخاص بالحق في الخصوصية (A/77/196, 2022)، بالإضافة إلى منظمة العفو الدولية (UNESCO, 2018).

أولاً_ مبدأ القانونية: إن أي استخدام للتكنولوجيا الحديثة فيما يخص المعالجة الآلية للبيانات الشخصية وتحليلها ونقلها ومشاركتها يجب أن يكون منصوصاً عليه في القانون ويتوافق مع حقوق الإنسان المعترف بها دولياً. فليس لمجتمع المعلومات أن يعتمد أو يطبق برامج معلوماتية من شأنها تقييد هذا الحق في غياب تشريع علني معلوم للكافة، يتصف بالوضوح والدقة الكافيين لضمان علم الأفراد المسبق به وقدرتهم على استشراف تطبيقاته.

ثانياً_ مشروعية الغرض: ينبغي ألا تسمح القوانين بمعالجة البيانات الشخصية إلا بواسطة مؤسسات حكومية بعينها ولتحقيق أهداف مشروعية ذات صلة بغرض قانوني ثابت وضروري في المجتمع المعلوماتي.

وبالتالي ينبغي ألا تطبق التقنيات الحديثة بما فيها استغلال البيانات الشخصية على نحو يكون فيها تمييز على أساس أصل الفرد العرقي أو أصله الإثني، أو معتقده الديني أو الفكري أو السياسي، أو استغلال البيانات الأمنية والجنائية، أو بيانات السمات الحيوية التي تحدد الهوية، أو البيانات الوراثية أو الصحية التي تتعلق بحالة الفرد الجسدية أو العقلية أو النفسية.

ثالثاً_ الضرورة: القوانين التي تسمح بالمعالجة الآلية للبيانات من قبل كيانات أخرى كالشركات التجارية يجب أن تقصّر المعالجة على القدر الأدنى بيان ضرورته لتحقيق غرض مشروع، فمعالجة البيانات يجب ألا تجرى إلا عندما تكون هي الوسيلة الوحيدة لتحقيق غرض مشروع أو في حال وجود أكثر من وسيلة، عند كونها الوسيلة الأقل انتهاكاً لحقوق الإنسان، ويقع على الدولة عبء إثبات ذلك المبرر أمام القضاء وعند التشريع.

رابعاً_ الملاءمة: أي حالة من حالات المعالجة الآلية للبيانات الشخصية المسموح بها قانوناً يجب أن تتناسب مع الغرض المشروع الذي تمارس من أجله.

خامساً_ التناسب: القرارات بشأن معالجة البيانات الشخصية آلياً يجب اتخاذها بموازنة المكاسب المنشود تحقيقها في ظل مجتمع معلوماتي، وبالضرر الذي ستحدثه في حقوق الفرد، وكذلك بالأهداف الأخرى المتعارضة مع أهداف المعالجة، وينبغي أن تؤخذ في الحسبان حساسية البيانات ودرجة فداحة الانتهاكات الواقعة على الخصوصية وحرية التعبير.

4. خاتمة:

أصبحت مسألة حقوق الإنسان والحريات العامة في تلامس مباشر مع تقنيات مجتمع نظم المعلومات، وبالتالي باتت الخصوصية وبيانات الأفراد مهددة في ظل أطر قانونية تجاوزها الزمن، خاصة وقد تم رصد من قبل منظمات حقوقية بعض الممارسات الخطيرة كشفت عن عدم وجود تشريعات أو وسائل إنفاذ وطنية كافية لتجريم الأفعال الماسة بالخصوصية وسلامة البيانات، وأصبح من الضروري ترسيخ حماية هذا الحق في صميم المجتمع المعلوماتي الذي عكس نفسه على الواقع الافتراضي لحياة الأفراد وأثر بشكل كبير وسلب على خصوصياتهم، مما بات من الضروري إيجاد تشريع خاص يقرر آليات قانونية إجرائية ووقائية لحماية البيانات الشخصية في إطار الموازنة بين حق الأفراد في الخصوصية وبين حاجات المجتمع لتكنولوجيا المعلومات والاتصالات.

1.4. نتائج الدراسة:

- للمجتمع المعلوماتي دور كبير في حياة الأفراد، من خلال تسخير إمكانيات تكنولوجيا المعلومات والاتصالات في إزالة الفجوة المعرفية والنهوض بأهداف التنمية المستدامة.
- اعتبار الحق في خصوصية البيانات حق جوهرية يعزز العديد من حقوق الإنسان وحياته التي تعتمد بشكل متزايد على تقنيات المعلومات والاتصالات كالحق في حرية الرأي والتعبير.
- تشكل انتهاكات خصوصية البيانات تهديداً لأمن مجتمع المعلومات، ويحول دون وقوعها، حماية هذا الحق، بوضع ضوابط قانونية للحد من هذه الانتهاكات، إذ تشكل المعالجة الآلية للبيانات الشخصية دون موافقة صاحبها وعلمه أبرز ما يمكن أن تكون عليه هذه الانتهاكات من صور.
- تتميز جرائم الخصوصية في مجتمع نظم المعلومات بعدة خصائص لا توجد في الجرائم التقليدية، مثل الطابع التقني، وكونها جرائم عابرة للحدود.
- وجود قصور تشريعي في القواعد والإجراءات الواجب اتباعها ضد جرائم الخصوصية.
- إن حماية البيانات مرهون بالتشريعات الوطنية والالتزامات الدولية.

- من المهم التأكيد على أن الانتقال من المفهوم الضيق للحياة الخاصة، باعتباره حقا في ترك الفرد شأنه، إلى المجال الموسع للخصوصية كوسيلة ضرورية لحماية البيانات الخاصة في ظل مجتمع المعلومات، يؤدي إلى تغيير حجم الالتزامات المتزايدة على الدول، حيث قد تكون هناك حاجة إلى ضمان التحكم في البيانات الشخصية وما إلى ذلك.

2.4. اقتراحات الدراسة:

- من خلال منطلقات وأهداف البحث، ومن خلاصة ما توصلنا إليه يمكن تصنيف جملة من الاقتراحات العامة التي قد تساهم في التقليل من الآثار السلبية من التحديات المصاحبة لتقنيات مجتمع المعلومات:
- من الضروري سد الفراغ التشريعي في مجال مكافحة الجريمة السيبرانية، على أن يكون شاملا للقواعد الموضوعية والإجرائية.
- ضرورة مواكبة تطورات تكنولوجيا المعلومات واستحداث قوانين وإجراءات خاصة بما يتلاءم مع طبيعة مجتمع المعلومات، وجعلها أكثر فاعلية في تحقيق حماية خصوصية البيانات من الانتهاكات.
- ضرورة تفعيل التعاون الدولي والانخراط في الاتفاقيات الدولية في التعامل مع الجرائم السيبرانية.
- ضرورة إقامة التوازن بين حق الأفراد في حماية بياناتهم الشخصية واحترام خصوصياتهم، وبين حاجات المجتمع لتكنولوجيا الاتصالات للوصول إلى المعلومات وتسهيل حياتهم اليومية.

5. قائمة المراجع:

النصوص القانون:

- الاتفاقيات وقرارات الأمم المتحدة:
- الإعلان العالمي لحقوق الإنسان 1948.
- العهد الدولي الخاص بالحقوق المدنية والسياسية لعام 1966.
- قرار الجمعية العامة، (سبتمبر، 2022)، الحق في الخصوصية في العصر الرقمي، رقم 179/73، الدورة 51.
- قرار الجمعية العامة، (ديسمبر، 2018)، الحق في الخصوصية في العصر الرقمي، رقم 179/73، الدورة 73.

المؤلفات:

- محمد نور الدين سيد، (2019)، أثر جائحة فيروس كورونا على الحق في الخصوصية، ملتقى دولي حول الجوانب القانونية الموضوعية والإجرائية لجائحة كورونا، كلية القانون، جامعة الشارقة.
- أحمد المناعسة، (2022)، جلال محمد الزعبي، جرائم تقنية نظم المعلومات، دار الثقافة للنشر والتوزيع، عمان.
- يوسف المصري، (2011)، الجرائم المعلوماتية والرقمية للحاسوب والإنترنت، دار العدالة، القاهرة، مصر، ط1.
- يزيد بوحليط، (2019)، الجرائم الالكترونية والوقاية منها في القانون الجزائري، دار الجامعة الجديدة، مصر.

المقالات:

- بدرية عبد الله العوضي، (2021)، الضمانات الدولية والإقليمية لحماية الحق في الخصوصية، مجلة كلية القانون الكويتية العالمية، العدد 10.
- مصطفى حميل، (ديسمبر، 2022)، السيادة الرقمية والتحول الرقمي: التحديات والحلول الهيكلية، مجلة الدراسات الإعلامية والاتصالية، المجلد 02، العدد 03.
- شافعي أمال، شافعي أم السعد، (مارس، 2022)، التأسيس للحق في حماية البيانات الشخصية كحق مستقل عن الحق في الخصوصية في تشريع الإتحاد الأوروبي، مجلة الباحث القانوني، المجلد 01، العدد 02.
- رؤى سعد القرني (2021)، الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)، مجلة كلية الدراسات الإسلامية والعربية للبيانات، الجزء 1، الإصدار 2، العدد 6.
- الزهرة بلعيا، (سبتمبر، 2022)، أثر البيئة الافتراضية على الحقوق والحريات الخاصة قراءة في التشريعات الإعلامية لحماية الحق في الخصوصية، مجلة الرسالة للدراسات الإعلامية، المجلد 06، العدد 03.
- سامح التهامي، (ديسمبر، 2018)، نطاق الحماية القانونية للبيانات الشخصية والمسؤولية التقصيرية عن معالجتها: دراسة في القانون الاماراتي، مجلة البحوث القانونية والاقتصادية، العدد 67.
- إبراهيم السعدي، (2020)، الحقوق الرقمية وآليات الحماية الدولية المقررة لها في إطار ق. الدولي لحقوق الإنسان، على الرابط التالي: <https://portal.arid.my/Publications/57339a35-9f98-44f7-aba0-cb37648b7f43.pdf>
- الاتحاد الدولي للاتصالات، (جينيف، 2014)، القمة العالمية لمجتمع المعلومات، الوثيقة الختامية للحدث الرفيع المستوى (WSIS+10)، متوفر على الرابط التالي:
- <https://www.itu.int/net/wsis/implementation/2014/forum/inc/doc/outcome/362828V2A.DOCX>

مواقع الانترنت:

- الجمعية العامة للأمم المتحدة، مجلس حقوق الإنسان: <http://undocs.org/A/HRC/27/37>، تاريخ التصفح: 2024/10/02.
- موقع kaspersky : <https://me.kaspersky.com/> ، تاريخ التصفح: 2024/10/06.
- مفوضية الأمم المتحدة السامية لحقوق الإنسان: <https://www.ohchr.org/ar/stories/2013/11/right-privacy-digital-age> ، تاريخ التصفح: 2024/09/23.

- موقع kaspersky : <https://me.kaspersky.com/resource-center/threats/internet-and-individual-privacy-protection> ، تاريخ التصفح: 2024/10/06.
- عمون نيوز، أهمية الخصوصية، <https://www.ammonnews.net/article/733572> ، تاريخ التصفح: 2025/01/23.
- الجمعية العامة للأمم المتحدة، <https://docs.un.org/A/77/196> ، تاريخ التصفح: 2025/01/30.
- منظمة الأمم المتحدة للتربية والعلم والثقافة، <https://www.unesco.org/ar/privacy-policy> ، تاريخ التصفح: 2025/01/30.