الجمهورية الجزائرية الديمقراطية الشعبية

People's Democratic Republic of Algeria

وزارة التعليم العالي والبحث العلمي

Ministry of Higher Education and Scientific Research

جامعة البليدة 2

University of Blida 2

كلية الحقوق والعلوم السياسية

قسم القانون العام

حماية الحق في الخصوصية من التأثيرات التكنولوجية وفق مبادئ حقوق الانسان

Protection of the right to privacy from technological influences in accordance with human rights principles

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر في الحقوق

تخصص القانون الدولي

إعدادالطالبة: عمران سارة

إشراف الأستاذة: بن ناصر فايزة

أمام لجنة المناقشة

الاسم	الجامعة	الصفة
حسين حياة	جامعة البليدة 2	رئيسًا
بن ناصر فايزة	جامعة البليدة 2	مشرفًا ومقررًا
بوجمعة شهرزاد	جامعة البليدة 2	مناقشًا

السنة الجامعية: 2025/ 2026

شكر وعرفان

بسم الله الرحمن الرحيم

الحمد لله حمداً كثيراً طيباً مباركاً فيه، حمداً يليق بجلال وجهه وعظيم سلطانه، الذي وفقني وأعانني على إتمام هذا العمل المتواضع.

أتقدّم بخالص الشكر والتقدير إلى الأستاذة المشرفة **بن ناصر فايزة** على توجيهاتها القيّمة ونصائحها السديدة التي كانت عوناً لي في إنجاز هذه المذكرة، وعلى سعة صدرها ومتابعتها المستمرة.

كما أتوجّه بجزيل الشكر إلى جميع أساتذتي الكرام في **الجامعة البليدة 2 قسم الحقوق** على ما قدموه لي من علم ومعرفة طوال مساري الدراسي.

ولا يفوتني أن أشكر كل من ساعدني من قريب أو بعيد في إنجاز هذا العمل، سواء بالدعم أو التشجيع أو النصيحة.

والحمد لله رب العالمين.

إهداء

بكل الحب والامتنان..

إلى من كانوا خلف كل خطوة في دربي،

إلى من غرسوا في قلبي حب العلم والمعرفة،

إلى من تحملوا معي مشقة البحث وسهر الليالي..

إلى والديَّ الكريمين عمران أحمد وبشار نادية هند،

اللذين كان دعاؤهما نبراسًا يضيء طريقي،

وسندهما السند الذي لم يتزعزع..

إلى أخوتي ياسين نائلة لينة الكرام،

رفقاء الدرب وسند الروح،

الذين شاركوني التفاصيل وأحاطوني بالحنان..

أهدي هذا العمل المتواضع،

راجيًا من الله أن يكون نافعًا،

ومعترفًا بأن فضلهم عليَّ لا يُحصى..

شكرًا لكم من أعماق قلبي.

مقدمة

الحق في الخصوصية من الحقوق الأساسية التي تشكل بناء منظومة حقوق الإنسان، لما له من ارتباط وثيق بكرامة الفرد وحريته الشخصية واستقلاليته في تدبير شؤونه الخاصة، فالإنسان بطبيعته يحتاج إلى مجال خاص يحتمي فيه من تدخلات الغير، ويحتفظ من خلاله بأسراره وعلاقاته وخياراته دون رقابة أو تعسف، ومن هذا المنطلق أصبحت الخصوصية تمثل أحد المقومات الجوهرية للشخصية الإنسانية، وعنصرا لا غنى عنه لضمان التوازن بين الفرد والمجتمع.

وقد حظي هذا الحق باهتمام متزايد في الفكر القانوني، حيث لم يعد ينظر إليه على أنه مجرد قيمة أخلاقية أو مطلب اجتماعي، بل أصبح حقا قانونيا مستقلا يجد أساسه في مختلف التشريعات الوطنية والمواثيق الدولية.

ويلاحظ أن تطور مفهوم الخصوصية قد ارتبط بتحولات عميقة شهدتها المجتمعات الإنسانية، سواء على المستوى الاجتماعي أو السياسي أو التكنولوجي، الأمر الذي أدى إلى توسيع نطاق هذا الحق ليشمل مجالات متعددة كالحياة الأسرية والبيانات الشخصية، والمراسلات والهوية الرقمية.

وفي هذا السياق أسهمت المواثيق الدولية لحقوق الإنسان في تكريس الحق في الخصوصية، حيث نص الإعلان العالمي لحقوق الإنسان على حماية الحياة الخاصة للأفراد من أي تدخل تعسفي في المادة 12، كما أكد العهد الدولي الخاص بالحقوق المدنية والسياسية على ذات المبدأ في المادة 17، مع تعزيز الضمانات القانونية المرتبطة به، وقد شكلت هذه النصوص مرجعية أساسية للدول في سن تشريعاتها الوطنية بما يضمن احترام هذا الحق وصيانته من الانتهاكات.

غير أن التطور التكنولوجي المتسارع الذي ميز العصر الحديث قد فرض تأثيره على اغلب مجالات الحياة، وأفرز واقعا جديدا أصبحت فيه المعلومات والبيانات الشخصية من أهم الموارد التي تقوم عليها الأنشطة الاقتصادية والاجتماعية، فقد ساهم انتشار وسائل الاتصال الحديثة

وعلى رأسها شبكة الإنترنت في تسهيل تبادل المعلومات بشكل غير مسبوق، كما أدى بروز تقنيات الذكاء الاصطناعي وتحليل البيانات الضخمة إلى تمكين الجهات المختلفة من جمع ومعالجة كميات هائلة من البيانات المتعلقة بالأفراد.

ورغم ما تحمله هذه التطورات من مزايا وفوائد، إلا أنها في المقابل تطرح تحديات حقيقية أمام حماية الحق في الخصوصية، حيث أصبحت الحدود الفاصلة بين الحياة العامة والخاصة أكثر هشاشة، وأضحى الأفراد عرضة لمختلف أشكال المراقبة الرقمية والتتبع وجمع البيانات دون علمهم أو موافقتهم الصريحة.

كما برزت مخاطر متزايدة تتعلق بانتهاك البيانات الشخصية، سواء من خلال تسريبها أو استغلالها بطرق غير مشروعة، مما يهدد الأمن المعلوماتي للأفراد ويقلل ثقتهم في البيئة الرقمية.

وأمام هذه التحديات تبرز الحاجة إلى إعادة النظر في مدى فعالية الأطر القانونية القائمة، وقدرتها على مواكبة التطورات التكنولوجية المتسارعة، إذ لم يعد كافيا الاكتفاء بالنصوص التقليدية، بل أصبح من الضروري تطوير قواعد قانونية مرنة تستجيب لطبيعة البيئة الرقمية، وتوفر في الوقت ذاته ضمانات حقيقية لحماية الأفراد من أي انتهاك لخصوصيتهم.

كما أن حماية هذا الحق لا تقتصر على الجانب التشريعي فحسب، بل تمتد لتشمل أبعادا مؤسساتية وتوعوية، حيث تلعب الجهات القضائية دورا محوريا في تفسير النصوص القانونية وتطبيقها، كما تساهم المنظمات الدولية وهيئات حماية البيانات في تعزيز ثقافة احترام الخصوصية ونشر الوعي بالمخاطر المرتبطة باستخدام التكنولوجيا الحديثة.

وتبرز أهمية هذا الموضوع كذلك في كونه يرتبط ارتباطا وثيقا بحماية الكرامة الإنسانية وضمان الحريات الفردية، مما يجعله من الركائز الأساسية في منظومة حقوق الإنسان، كما تنبع أهميته من تزايد التحديات التي تفرضها البيئة الرقمية، لاسيما في ظل انتشار وسائل الاتصال الحديثة وتقنيات الذكاء الاصطناعي، وهو ما يطرح إشكالات قانونية تتعلق بمدى كفاية الحماية التشريعية القائمة، وعليه فإن معالجة هذا الموضوع تساهم في فهم أعمق لمختلف الأبعاد القانونية للحق في

الخصوصية، وتساعد في إبراز النقائص التي قد تعتري آليات حمايته، بما يمكن من اقتراح حلول تسهم في تعزيز هذا الحق ومواكبة التطورات الراهنة.

يعود اختيار هذا الموضوع إلى مجموعة من الأسباب الذاتية والموضوعية التي جعلته محل اهتمام ودراسة وهي الاسباب الذاتية تمثلت في ينبع اهتمامي بهذا الموضوع من الرغبة في التعمق في أحد أهم الحقوق الأساسية المرتبطة بحياة الإنسان اليومية، وهو الحق في الخصوصية خاصة في ظل التطور التكنولوجي السريع الذي أصبح يفرض نفسه على مختلف مجالات الحياة.

والاسباب الموضوعية فتتجلى أهمية الموضوع في كونه يعالج إشكالية معاصرة تتمثل في تزايد الانتهاكات التي تمس الحياة الخاصة للأفراد نتيجة الاستخدام الواسع لوسائل الاتصال الحديثة وتطبيقات الذكاء الاصطناعي، وما يترتب عنها من مخاطر تتعلق بجمع البيانات الشخصية واستغلالها، كما أن هذا الموضوع يكتسي أهمية قانونية متزايدة لكونه يطرح تساؤلات حول مدى كفاية القواعد القانونية الحالية في توفير الحماية اللازمة للحق في الخصوصية ومواكبة التحولات الرقمية المتسارعة، الأمر الذي دفع إلى اختياره كمجال للبحث والدراسة.

تهدف هذه الدراسة إلى تسليط الضوء على الحق في الخصوصية من خلال تحديد مفهومه وبيان أبعاده المختلفة في الفكر القانوني مع تتبع تطوره عبر مختلف المراحل التاريخية.

كما تسعى إلى إبراز مكانة هذا الحق في المواثيق الدولية لحقوق الإنسان من خلال تحليل النصوص القانونية ذات الصلة، ومن جهة أخرى ترمي الدراسة إلى الوقوف على تأثير التطور التكنولوجي خاصة في مجال وسائل الاتصال الحديثة والذكاء الاصطناعي على الحق في الخصوصية، مع إبراز أهم الانتهاكات التي قد يتعرض لها في البيئة الرقمية، بالإضافة إلى ذلك تهدف إلى تحليل آليات الحماية القانونية والمؤسساتية المعتمدة لضمان حماية هذا الحق، وتقييم مدى فعاليتها في مواجهة التحديات المعاصرة، وصولا إلى تقديم بعض المقترحات والتوصيات التي من شأنها تعزيز حماية الحق في الخصوصية في ظل التطور التكنولوجي المتسارع.

وعليه تكتسي دراسة الحق في الخصوصية أهمية بالغة في ظل هذا الواقع المتغير، إذ تتيح فهم أبعاده المختلفة، والوقوف على التحديات التي تواجهه، واستكشاف السبل الكفيلة بتعزيز حمايته، ومن هذا المنطلق تسعى هذه الدراسة إلى معالجة الإشكالية التالية:

إلى أي مدى استطاعت القواعد القانونية في ظل التطور التكنولوجي المتسارع توفير حماية فعالة للحق في الخصوصية؟

اعتمدت هذه الدراسة على المنهج الوصفي التحليلي، باعتباره الأنسب لموضوع الحق في الخصوصية، حيث يتيح هذا المنهج وصف مختلف المفاهيم المرتبطة بالموضوع وتحليلها تحليلاً دقيقًا من خلال دراسة النصوص القانونية والمواثيق الدولية ذات الصلة، كما تم الاعتماد على المنهج التحليلي في تفسير وتقييم القواعد القانونية التي تنظم حماية الحق في الخصوصية، ومدى فعاليتها في مواجهة التحديات الناتجة عن التطور التكنولوجي، وتكمن أهمية هذا الاختيار المنهجي في كونه يسمح بالإحاطة بجوانب الموضوع من الناحية النظرية والتطبيقية، بما يضمن معالجة الإشكالية المطروحة بطريقة علمية ومنهجية متكاملة.

ولمعالجة هذه الإشكالية تم تقسيم هذه الدراسة إلى ثلاثة فصول على النحو التالي:

الفصل الأول :الإطار المفاهيمي والقانوني للحق في الخصوصية، ويضم مبحثين:

الأول يتناول مفهوم الحق في الخصوصية من خلال تعريفه وتطوره في الفكر القانوني، والثاني يتناول الحق في الخصوصية في المواثيق الدولية لحقوق الإنسان، من خلال الإعلان العالمي لحقوق الإنسان والعهد الدولي الخاص بالحقوق المدنية والسياسية.

الفصل الثاني :التأثيرات التكنولوجية على الحق في الخصوصية، ويشمل مبحثين:

الأول يعرض مظاهر التطور التكنولوجي من خلال وسائل الاتصال الحديثة والإنترنت، والذكاء الاصطناعي وقواعد البيانات الضخمة، والثاني يتناول انتهاكات الخصوصية الناتجة عن التكنولوجيا، من خلال المراقبة الرقمية وجمع البيانات، وانتهاك البيانات الشخصية والأمن المعلوماتي.

الفصل الثالث :حماية الحق في الخصوصية وفق مبادئ حقوق الإنسان، ويتكون من مبحثين: الأول يخصص للأسس الحقوقية لحماية الخصوصية من خلال مبدأ الكرامة الإنسانية ومبدأ المشروعية وعدم التعسف، والثاني يتناول آليات الحماية القانونية والمؤسساتية، من خلال الحماية التشريعية والقضائية، ودور المنظمات الدولية والتوعية الرقمية.

الفصل الأول:

الإطار المفاهيمي والقانوني للحق في الخصوصية

الفصل الأول: الإطار المفاهيمي والقانوني للحق في الخصوصية

يشكل الحق في الخصوصية محورا إشكاليا في الفكر القانوني المعاصر، ليس فقط بسبب طبيعته المتطورة والمتجددة، بل أيضا نتيجة للصعوبات التي تواجه محاولات ضبطه بمفهوم جامع مانع، فالنظر إلى الخصوصية كمجرد "حق في العزلة" لم يعد كافياً في زمن تتدفق فيه البيانات الشخصية عبر الحدود، وتتداخل فيه الحياة العامة بالخاصة بفعل الثورة الرقمية، من هنا يصبح من الضروري قبل الخوض في آليات الحماية أو دراسة الانتهاكات، العودة إلى جذور هذا المفهوم وتفكيك بنيته القانونية والفلسفية، وهو ما يسعى هذا الفصل إلى إنجازه، ينقسم الفصل إلى مبحثين رئيسيين، يؤسسان معاً للإطار النظري الذي تتبني عليه باقي أجزاء الدراسة.

يتناول **المبحث الأول** مسألة تحديد مفهوم الحق في الخصوصية من منظورين متكاملين: الأول لغوي، والثاني اصطلاحي، كما يعرج هذا المبحث على التطور التاريخي للفكرة، متتبعاً إياها من مرحلتها المادية إلى مرحلتها المعنوية وصولا إلى مرحلتها الرقمية، مع الإشارة إلى الدور المحوري الذي لعبته مقالة وارن وبراندیز عام 1890 في بلورة هذا المفهوم.

أما **المبحث الثاني** فينتقل من المستوى النظري إلى المستوى المعياري، حيث يعرض مكانة الحق في الخصوصية ضمن أبرز المواثيق الدولية لحقوق الإنسان، فيبدأ بالإعلان العالمي لحقوق الإنسان (المادة 12) بوصفه أول إعلان جامع يقر بالحق في الخصوصية، محللاً مضمون هذا النص ونطاق حمايته، ومبينا كيف امتدت هذه الحماية لتشمل التحديات المعاصرة بفضل قراءات المقررين الخاصين وقرارات الأمم المتحدة اللاحقة، ثم ينتقل إلى العهد الدولي الخاص بالحقوق المدنية والسياسية (المادة 17) الذي أضفى الطابع الملزم على هذه الحماية، مع التركيز على التعليق العام رقم 16 الصادر عن لجنة حقوق الإنسان عام 1988، والذي وسع نطاق الحماية ليشمل جمع البيانات وتخزينها إلكترونيا، رغم أنه صدر قبل عصر الإنترنت بسنوات.

المبحث الأول: مفهوم الحق في الخصوصية

يعتبر الحق في الخصوصية من أهم الحقوق الأساسية المرتبطة بشخصية الإنسان وكرامته، إذ يهدف إلى حماية الحياة الخاصة للأفراد ومنع أي تدخل تعسفي أو غير مشروع في شؤونهم الشخصية، والحياة الخاصة تمثل المجال الذي يمارس فيه الفرد حريته بعيدا عن رقابة الآخرين أو تدخلهم، الأمر الذي يجعل احترام هذا الحق شرطاً أساسياً لتحقيق كرامة الإنسان وضمان حرياته الأساسية.

وقد ازداد الاهتمام بهذا الحق في العصر الحديث نتيجة التطورات الاجتماعية والتكنولوجية التي ساهمت في توسيع نطاق التدخل في الحياة الخاصة للأفراد، خاصة مع انتشار وسائل الاتصال والإعلام الحديثة، لذلك سعت التشريعات الوطنية والمواثيق الدولية لحقوق الإنسان إلى تكريس الحق في الخصوصية وتوفير الحماية القانونية اللازمة له.

وبناء على ذلك سيتم في هذا الفصل التطرق إلى الإطار المفاهيمي والقانوني للحق في الخصوصية، من خلال دراسة مفهوم هذا الحق وتطوره في الفكر القانوني، ثم بيان مكانته في أهم المواثيق الدولية لحقوق الإنسان.

المطلب الأول: تعريف الحق في الخصوصية

يعد الحق في الخصوصية من أكثر المفاهيم تعقيدا وتعددا في مجالات القانون والفلسفة والعلوم الاجتماعية، نظرا لتداخل أبعاده الشخصية والاجتماعية والقانونية.

حيث يعتبر مصطلح "الخصوصية" مصطلحا جامعا وكذلك مصطلح "حماية البيانات"، وكلاهما موجودان أخلاقيا باعتبارهما عاملين مساعدين على تنمية شخصية الفرد وهويته والحفاظ عليهما في ظل الاستقلالية؛ أما من الناحية القانونية فهما جانبان من جوانب الكرامة التي تحظى بتقدير كبير في الديمقراطية التي يساهم فيها الأفراد المستقلون.[1]

[1] MARIA GRAZIA PORCEDDA, Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis, HART PUBLISHING, Great Britain, 2023, p. 14

يشمل مفهوم الخصوصية مزيجا من الشخصية والتحفظ والألفة والتفاعل الاجتماعي، بل وحتى المراقبة المجتمعية كآلية لفرض الأعراف وتتجلى أنماط هذا المزيج بأشكال مختلفة في جميع ثقافات العالم على مستوى الفرد والأسرة والمجتمع.

في الواقع تعد الألفة حاجة جوهرية وآلية لتحديد المسافة من أجل العيش والتعلم، وتستخدم بطريقة جدلية مع التفاعل الاجتماعي، الذي يفهم على أنه الرغبة في التفاعل مع الآخرين، ويمكن كل من التحفظ والألفة من تنمية شخصية الفرد من خلال فهم الأدوار المختلفة التي يؤديها في المجتمع، والحفاظ على مكانته الاجتماعية، تساهم الخصوصية والتحفظ اللذان يتمتع بهما الفرد في الحفاظ على اتساق الأدوار التي يؤديها في مواجهة التغيير، مما يضفي معنى على سيرته الذاتية. [1]

ويسبق تقدير المجتمع للخصوصية ظهور تكنولوجيا المعلومات والاتصالات المعاصرة، كما يتضح من مقالة صموئيل وارين ولويس براندیس الشهيرة، المستوحاة من التطفل المستمر الذي مارسه المصورون المتطفلون في ذلك الوقت على حياة وارين العائلية، ومع ظهور تقنية التصوير الفوتوغرافي الناشئة التي أدت إلى الاعتراف القانوني بحق الفرد في صورته، اقترح وارين و براندیس أن تحظى الروايات المكتوبة التي تتسم بالتفاصيل والوضوح مثل الصورة، بحماية القانون بالمثل وتحت غطاء "الحق في أن يترك المرء وشأنه" الذي يندرج تحت قانون المسؤولية التقصيرية، نظر وارين و براندیس إلى الخصوصية على أنها "حق في الشخصية" أو الهوية: أي التعبير عن حياة الفرد مثل المشاعر والأحاسيس وحقائق الحياة والأحداث والأفعال والعلاقات مع الآخرين، لقد تطلب الأمر أهوال الحرب العالمية الثانية لترسيخ المواثيق الوطنية وتطوير المواثيق الدولية التي تحمي الخصوصية كما نعرفها اليوم: مجموعة من الحياة

[1] Anupriya Puri, The Group Right to Mutual Privacy, Ethics and Information Technology, Vol. 2, No. 2, Springer, 2023, page 5.

الخاصة والحياة الأسرية والمنزل والاتصالات.[1]

الفرع الاول: التعريف اللغوي:

تطلق الخصوصية في اللغة من خصه بالشيء خصوصا، وخصوصية والفتح أفصح، واختصه بكذا أي خصه به وأفرده به، والخاصة: خلاف العامة.[2]

لخصوصية لغة مصدر فعل خص يخص خصا وخصوصا وخصوصية، نقيض عم، يقال خصصه بالشيء وخصه خصوصية إذا جعله له دون غيره، ومنه الخاصة والخصوص نقيض العامة والعموم، لذلك يطلق لفظ الخاص بمعنى التفرد، وعبارة خاصة الشيء بمعنى ما يختص به دون غيره، أو دون أية شركة للغير فيه[3]، قال الله تعالى: ﴿وَاتَّقُوا فِتْنَةً لَا تُصِيبَنَّ الَّذِينَ ظَلَمُوا مِنْكُمْ خَاصَّةً وَاعْلَمُوا أَنَّ اللَّهَ شَدِيدُ الْعِقَابِ﴾.[4]

وعليه فإن كلمة الخصوصية تطلق من الناحية اللغوية ويراد بها الدلالات المتناقضة مع معاني فعل عم ومشتقاته، إذ هي بمعنى ما ينفرد به الشخص أو الشيء أو يختص به دون غيره.

يعرف قاموس أكسفورد الخصوصية بأنها حالة يكون فيها الفرد بمنأى عن المراقبة أو التدخل أو الإزعاج من قبل الآخرين، أو وضع يتمتع فيه الشخص بالحماية من أعين العامة والاهتمام غير المرغوب فيه[5]، ومع ذلك لا يوجد تعريف موحد ومتفق عليه عالميا لهذا المفهوم، إذ اختلفت المقاربات العلمية باختلاف الزوايا التي ينظر منها إلى الخصوصية.

الفرع الثاني: التعريف الاصطلاحي:

---

[1] MARIA GRAZIA PORCEDDA, Op.cit page 15

2 ابن منظور، لسان العرب، دار صادر، بيروت، ج 7، ص 24

3 مجمع اللغة العربية، المعجم الوسيط، دار الدعوة، القاهرة، ج 1، ص 251.

4 القرآن الكريم، سورة الأنفال، الآية 25

5 (قاموس أكسفورد، 2015)
https://www.oxfordlearnersdictionaries.com/definition/english/privacy?utm_source=chatgpt.com

يمكن تعريف الحق في الخصوصية بطريقتين أساسيتين، من حيث الوصول أو من حيث التحكم، على الرغم من وجود طرق عديدة لتوضيح معنى كل منهما، إلا أنه يمكن تبسيطها كما يلي:

حق الوصول في الخصوصية: الحق في التمتع بالخصوصية، أي الحق في عدم وصول الآخرين إلى معلومات عن الشخص.

حق التحكم في الخصوصية: الحق في التحكم في مدى تمتع الشخص بالخصوصية، أي الحق في التحكم فيما إذا كان بإمكان الآخرين الوصول إلى معلومات عنه.[1]

كما عرفته المحكمة العليا الكندية بأنه :" النطاق الضيق للاستفادة الشخصية، الذي في إطاره تقرر الاختيارات الخاصة بطبيعتها"، بمعنى الحيز الزماني والمكاني الذي يختاره الشخص للقيام بتصرفات شخصية بعيدا عن أي طارئ قد يخرجها إلى طابع عام، أو الإطار الذي يحدد فيه الصفة الشخصية للمعلومات المتعلقة به.[2]

الخصوصية مفهوم غامض وغير محدد بدقة ولذلك، كتب الكثير في محاولة لتعريف مصطلح "الخصوصية" في عصر المعلومات، تتداخل الخصوصية والتكنولوجيا وتؤثران في بعضهما البعض، وبالتالي لن تنجح آليات حماية الخصوصية ما لم تصمم مع مراعاة التطور التكنولوجي. هذا السياق يوسع تعريف القاضي الأمريكي توماس كولي(Thomas Cooley) البسيط للخصوصية، وهو "الحق في أن تترك وشأنك"، ليشمل المزيد من التعقيدات المتعلقة بالخصوصية وما يرتبط بها من مخاوف اقتصادية واجتماعية وسياسية ونفسية وقانونية، عموما تشير الخصوصية إلى الشرط أو الحق الأخلاقي الذي يفرضه الامتناع عن القيام بأنشطة معينة على الآخرين.

---

[1] Michael Birnhack , Defense of Privacy-as-Control (Properly Undersrood)" , FORTHCOMING IN JURIMETRICS VOL. 65 ,2026, page 3

[2] FATAH KICHE, Mechanisms for the protection of the right to privacy in Algerian legislation، Adrar University – Algeria ,2019, page 97

المطلب الثاني: تطور الحق في الخصوصية في الفكر القانوني

لقد تطور الحق في الخصوصية في الفكر القانوني من الحماية القديمة للفضاء المادي إلى إطار حديث متطور للتحكم في المعلومات، تاريخيا لم يتم الاعتراف بهذا الحق باعتباره "حقا" قائماً بذاته، ولكنه كان موجودا من خلال تدابير حماية للمنزل والمراسلات.[1]

وقد كان لدى البشر دائما حاجة للخصوصية، اذ يمكن بالفعل رؤية مسألة الخصوصية في كتابات سقراط وغيره من الفلاسفة اليونانيين، عندما كان يتم التمييز بين "الخارجي" و"الداخلي"، بين العام والخاص وبين المجتمع والعزلة، وعلى الرغم من أن الحياة الخاصة كان ينظر إليها أحيانًا على أنها سلوك غير اجتماعي، إلا أنه كان هناك دائما نوع من الصراع بين "الرغبة الذاتية في العزلة والعزلة، والحاجة الموضوعية إلى الاعتماد على الآخرين".

يبدأ جميع المؤلفين حول الخصوصية تقريبا المناقشة بالمقالة الشهيرة "الحق في الخصوصية لصامويل وارن ولويس براندیز" في مجلة هارفارد للقانون الصادرة في 15 ديسمبر 1890، على الرغم من أنه لا يمكن الاستهانة بتأثيرات هذه المقالة، فإن نقطة البداية هذه لا تعني أنه لم تكن هناك مناقشات حول انتهاك الخصوصية قبل عام 1890، وكما يوضح ويستن[2] في منشوراته فقد تم استخدام كلمة "الخصوصية" بالفعل في القرن الخامس عشر في إنجلترا وتظهر الأبحاث التاريخية أن المستعمرين في انجلترا كانوا يحترمون الخصوصية فيما يتعلق بمنزل الفرد وعائلته وحتى التواصل بالمراسلات.

يوضح هيكسون[3] أنه كانت هناك معارضة ضد أول تعداد سكاني للولايات المتحدة في وقت

---

[1] Daniel J. Solove ,A Brief History of Information Privacy Law ,George Washington University Law School,USA, 2006 ,p 36.

[2] آلان ويستن (Alan Westin) هو باحث قانوني وعالم سياسي أمريكي، يُعتبر "الأب الروحي" لقوانين خصوصية البيانات الحديثة.

[3] سي. جيه. هيكسون(C. J. Hickson) ، وهو باحث أو مؤرخ يستشهد بكتاباته عند مناقشة التطور التاريخي لسرية البيانات في التعداد السكاني الأمريكي.

مبكر من عام 1790، على الرغم من أن الحكومة لم تطلب أكثر من مجرد إحصاء الأشخاص سواء العبيد أو الأحرار، أدت هذه المعارضة إلى إصدار تعليمات لمنفذي التعداد في عام 1840 بأن يتم التعامل مع الإقرارات الفردية على أنها سرية، وكان يخشى ألا يكون المواطن محميا بشكل كاف من خطر إفشاء شؤونه الخاصة أو أسرار الأسرة للجيران.[1]

لقد مر تطور الخصوصية بثلاث مراحل تاريخية ظهرت من خلالها فكرة الخصوصية التقليدية الى ان وصل مفهوم الخصوصية الى العصر الرقمي وهذه المراحل هي:

الفرع الأول: مرحلة الخصوصية المادية:

وهي مرحلة الخصوصية المادية ويقصد بها الاعتراف بالخصوصية كحق لحماية الأفراد من مظاهر الاعتداء المادي على حياتهم وممتلكاتهم.

هذه المرحلة هي حجر الأساس في نشأة المفهوم القانوني للخصوصية، حيث تم التركيز فيها على حماية الكيان المادي للفرد ومجاله الحيوي المحسوس، ويقصد بها الاعتراف بالخصوصية كحق لحماية الأفراد من كافة مظاهر الاعتداء المادي التي قد تطال جسدهم، أو ممتلكاتهم، أو الأماكن التي يقيمون فيها[2]، ففي هذه المرحلة لم يكن المفهوم يتجاوز فكرة "الحرمة المادية"، حيث ارتبطت الخصوصية بشكل وثيق بحق الملكية؛ فالمسكن هو "حصن الفرد" الذي لا يجوز اقتحامه أو تفتيشه دون مبرر قانوني، والمراسلات الورقية هي ملكية مادية لا يجوز انتهاك سريتها، إن الحماية في هذا الطور كانت تهدف إلى تأمين "حيز من الانفراد (Seclusion)"

يتيح للشخص ممارسة حياته بعيداً عن أعين المتطفلين أو تدخلات السلطة غير المشروعة.[3]

الفرع الثاني: مرحلة الخصوصية المعنوية والخصوصية كحق عام:

---

[1] Jan Holvast ,History of Privacy ,Holvast & Partner, Privacy Consultants, NL - Landsmeer, The Netherlands, page15

[2]The IT Law Wiki, Definition of physical privacy, Site : https://itlaw.fandom.com/wiki/Physical_privacy#:~:text=Definition,the%20taking%20of%20biometric%20information. 08/03/2026 23:30P.m

[3] خالد عبدالله راشد الزعابي، مفهوم وخصائص و صور الخصوصية "دراسة مقارنة"، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة مصر،2025، ص 05

لم تعد حماية الخصوصية تقتصر على الفضاء المادي للمسكن والمراسلات، إذ سرعان ما تجاوز الفكر القانوني هذه النظرة الضيقة ليشمل الأبعاد المعنوية للشخصية الإنسانية.

أولا: مرحلة الخصوصية المعنوية: وهي انطواء الخصوصية على حماية القيم والعناصر المعنوية للشخص .

شهد الفكر القانوني تحولا جذريا في هذه المرحلة؛ حيث انتقل التركيز من حماية "الجدران والممتلكات" إلى حماية "الكيان المعنوي والشخصية "للفرد، ويقصد بها انطواء الخصوصية على حماية القيم والعناصر المعنوية للشخص، مثل كرامته وسمعته وحقه في السيطرة على صورته واسمه وسيرته الذاتية، في هذه المرحلة لم يعد الاعتداء مشروطا باقتحام مكان مادي، بل أصبح يشمل أي فعل يؤدي إلى كشف أسرار الحياة الخاصة أو استغلال هوية الشخص دون إذنه، مما يتسبب في ضرر أدبي ونفسي، وقد كان للمقالة الشهيرة لـ "وارين وبراندیز" عام 1890 الفضل الأكبر في ترسيخ هذا المفهوم، حيث عرفت الخصوصية بأنها "الحق في أن يترك المرء وشأنه (The right to be let alone) "، وذلك بهدف حماية "السلام الذهني" للفرد من تطفل الوسائل الحديثة آنذاك[1].

ثانيا: المرحلة الخصوصية كحق عام: وهي مرحلة الثالثة ويمتد نطاقه لحماية الشخص من كافة أوجه الاعتداءات والتدخل في حياته اي كان مظهرها او طبيعتها، وفي نطاق المعنى الأخير ولد مفهوم جديد للخصوصية ارتبط بأثار التقنية والتكنولوجيا الحديثة على الحياة الخاصة تمثل بخصوصية المعلومات أو حق الافراد في حماية البيانات الشخصية والسيطرة عليها في ظل تحديات العصر الرقمي، ولقد تأثر الفقه والقضاء بمراحل التطور التاريخي للحياة الخاصة،

[1] Alan F. Westin, Privacy And Freedom, 25 Wash. & Lee L. Rev. Washington and Lee, University School of Law Scholarly Commons (1968). page 166

وبذلك ظهرت لنا تعاريف وأراء فقهية مختلفة على مدى العصور.[1]

ويظهر من خلال دراسة المراحل التاريخية الكبرى لتطور مفهوم الخصوصية من الحماية المادية إلى الحماية المعنوية، وصولا إلى الاعتراف بها كحق عام شامل انبثق عنه في العصر الرقمي مفهوم خصوصية المعلومات أن هذه المراحل لم تكن وليدة الصدفة، بل جاءت نتيجة تراكم تاريخي من الأسس القانونية والفقهية التي أرست دعائم الحق في الخصوصية وهي كالتالي:

1- الأسس الاولية للحق في الخصوصية: يمكن تتبع جذور الحق في الخصوصية في مرحلته المادية إلى أسس أولية تجسدت في عنصرين أساسيين هما:

أ- الحرمة الجسدية: ركزت الأنظمة القانونية القديمة على المنزل حيث كان القانون الروماني وقانون حمورابي ينظمان عمليات اقتحام المساكن الشخصية، وأثبتت القضية الإنجليزية لعام 1604 (قضية سيماين) أن "بيت كل فرد هو بالنسبة له بمثابة قلعته وحصنه[2]."

ب- المراسلات: من القرن الرابع عشر إلى القرن الثامن عشر، غالبًا ما تضمنت النزاعات القانونية التنصت أو فتح الرسائل الشخصية بشكل غير مصرح به .

2- مقالة براندیز ووارن عام 1890 :

تم صياغة المفهوم القانوني الحديث لـ "الحق في الخصوصية" بشكل مشهور من قبل صامويل وارين ولويس براندیز في مقالتهما عام 1890 بعنوان "الحق في الخصوصية" وقد كانوا يستجيبون للتهديدات التكنولوجية وعلى وجه التحديد الكاميرا المحمولة و"الصحافة الصفراء"، والتي اعتقدوا أنها تؤدي إلى تآكل "الحرم المقدس للحياة الخاصة والمنزلية" وبذلك لقد عرفوه

[1] فوزية شريط، التطور التاريخي للحق في الخصوصية بين النصوص الدينية والأحكام الوضعية "دراسة تحليلية"، كلية العلوم الإنسانية والحضارة الإسلامية، جامعة أحمد بن بلة وهران – 1 – الجزائر، مركز جيل البحث العلمي، سلسلة كتاب أعمال المؤتمرات، العدد26، 2019، صفحة 12.

[2] Semayne's Case (1604) ,COURT OF KING'S BENCH, All ER Rep 62, Also reported 5 Co Rep 91 a; Cro Eliz 908; Moore KB 668; Yelv 29; 77 ER 194Michaelmas Term, 1604

بانه "الحق في أن تترك وشأنك".[1]

وجادلوا بأن هذا الحق مضمن بالفعل في مبادئ القانون العام (الملكية والعقود والأضرار) ولكن يجب الاعتراف به كحق متميز لحماية "حرمة الشخصية" بدلا من مجرد الملكية الملموسة.

3-التدوين الدولي للحق في الخصوصية :

في أعقاب الحرب العالمية الثانيـة تم رفع هذا الحـق من مصلحة وطـنية إلى حق إنسـاني دولـي، وذلك عبر مجموعة من المواثيق الدولية والإقليمية:

الإعلان العالمي لحقوق الإنسان (1948): نصت المادة 12 على أنه لا يجوز تعريض أي شخص "لتدخل تعسفي في خصوصياته،[2] العهد الدولي الخاص بالحقوق المدنية والسياسية (1966): قامت المادة 17 بتدوين هذه الحماية في معاهدة ملزمة[3].

الاتفاقية الأوروبية لحقوق الإنسان (1950): تضمن المادة 8 "الحق في احترام الحياة الخاصة والعائلية"، والذي قامت المحكمة الأوروبية لحقوق الإنسان بتوسيع نطاقه منذ ذلك الحين من خلال سوابق قضائية واسعة النطاق[4].

في الوقت الحاضر من المقبول عموما أن كل شخص يحتاج إلى الخصوصية، على الرغم من أن طريقة تقديرها تختلف من ثقافة إلى أخرى ومن شخص لآخر، وفي الوقت نفسه من الواضح أن الحاجة إلى الخصوصية لا يمكن أن تكون مطلقة أبدا ويجب موازنتها مع الاحتياجات الأخرى، على سبيل المثال الحاجة إلى مكافحة الإرهاب والإجرام والاحتيال، وكما سنرى بعد ذلك

---

[1] Warren, S. D., & Brandeis, L. D. (1890). "The Right to Privacy." Harvard Law Review, Vol. 4, No. 5 ,page 193،205

[2] الإعلان العالمي لحقوق الانسان (1948) : الجمعية العامة للأمم المتحدة المادة 12

[3] العهد الدولي الخاص بالحقوق المدنية والسياسية (1966) الصادر عن الجمعية العامة للأمم المتحدة بموجب القرار 2200 ألف (د-21) المؤرخ في 16 ديسمبر 1966، المادة 17.

[4] الاتفاقية الأوروبية لحقوق الانسان (1950) الصادرة عن مجلس أوروبا بموجب المعاهدة الموقعة في روما بتاريخ 4 نوفمبر 1950، والتي دخلت حيز النفاذ في 3 سبتمبر 1953 المادة 8.

فإن المناقشة حول الخصوصية هي في المقام الأول مناقشة سياسية حول الطريقة التي يمكن بها تحقيق التوازن بين المصالح الفردية والمجتمعية المتميزة.

إن تطور الحق في الخصوصية في القانون الدولي عملية معقدة تتطلب تحليلا معمقا لتطورها التاريخي، في البداية لم تكن الخصوصية معترفا بها بوضوح كحق مستقل من حقوق الإنسان ضمن الأنظمة القانونية.

المبحث الثاني: الحق في الخصوصية في المواثيق الدولية لحقوق الإنسان

بعد أن أرست المادة (12) من الإعلان العالمي لحقوق الإنسان لعام 1948 الأساس القانوني الدولي لحماية الخصوصية، جاءت المواثيق الدولية اللاحقة لتحول تلك المبادئ إلى التزامات تعاقدية ملزمة للدول الأطراف، فإذا كان الإعلان العالمي بمثابة وثيقة أخلاقية وسياسية ذات قيمة ارشادية، فإن العهد الدولي الخاص بالحقوق المدنية والسياسية لعام 1966 قد جسد قفزة نوعية عندما أضفى على الحق في الخصوصية صفة الإلزام القانوني، حيث نصت المادة (17) منه على حماية مماثلة مع إخضاع أي تدخل لمعايير القانونية وعدم التعسف[1].

كما تواترت النصوص الدولية الإقليمية والعالمية لتؤكد هذا الحق وتوسع مضمونه لمواكبة التطورات المعاصرة، لاسيما في ظل الثورة الرقمية وتزايد المخاطر المحدقة بالحياة الخاصة.

ويتناول هذا المبحث بالتحليل أبرز هذه المواثيق الدولية العالمية والإقليمية موضحا تطور النصوص القانونية المنظمة للحق في الخصوصية، ونطاق الحماية التي توفرها كل منها، ومدى فعاليتها في تحقيق التوازن بين صيانة هذا الحق وبين متطلبات الأمن العام أو المصالح المشروعة الأخرى.

[1] العهد الدولي الخاص بالحقوق المدنية والسياسية، الصادر عن الجمعية العامة للأمم المتحدة بموجب القرار 2200 ألف (د-21) المؤرخ في 16 ديسمبر 1966، المادة 17.

ويهدف هذا المبحث إلى تقديم إطار شامل للمعايير الدولية التي تشكل اليوم مرجعا أساسيا للمشرعين والقضاء وهيئات حماية حقوق الإنسان في مختلف دول العالم.

المطلب الأول: الحق في الخصوصية في الإعلان العالمي لحقوق الإنسان

يمثل الإعلان العالمي لحقوق الإنسان الصادر عن الأمم المتحدة، أول وثيقة دولية جامعة تكرس مبدأ احترام الحقوق الأساسية للإنسان، ومن أبرزها الحق في الحياة الخاصة، فقد نصت المادة (12) من الإعلان الصادر عام 1948 على أنه:

"لا يجوز إخضاع أي شخص لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته، ولا للمساس بشرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الانتهاكات."

اشتمل الإعلان العالمي على مجموعة من المبادئ التي تدعو إلى احترام حقوق الإنسان عامة، وتولي عناية خاصة بحق الفرد في الخصوصية، مما يرسي حماية أساسية لهذا الحق الذي يعد سمة أصيلة في البشر صونا له من أي تدخل غير مبرر أو غير مشروع. لذا كان لهذه الوثيقة التاريخية أثر بالغ في توجيه اهتمام الدول والشعوب نحو ضرورة صيانة حقوق الإنسان والحريات الأساسية، وعلى رأسها الحق في الخصوصية[1].

الفرع الأول: مضمون ونطاق الحماية بموجب المادة 12

ان الحق في الخصوصية يحمي بطريقتين: أولا إنه يحمي الناس من الدولة من الحكومة نفسها، على سبيل المثال من مداهمة الشرطة دون إذن من القاضي، لذلك لا يجوز للحكومة أن تفعل شيئا، ثانيا يتعين على الحكومة أحيانا أن تفعل شيئا لحماية الخصوصية، على سبيل المثال إذا

[1] عواد حسين ياسين العبيدي الحق في الخصوصية وموقف المواثيق الدولية منه، 2026، المقال على الرابط التالي: https://www.sjc.iq/view.78955/

انتهك مدنيون أو شركات أخرى خصوصية شخص ما مثل منصات التواصل الاجتماعي، في هذه الحالة يتعين على الدولة حماية الخصوصية بشكل فعال، وبذلك أي من جانبي هذا الحق هو الأكثر أهمية يعتمد على الوضع.

وتحدد المادة 12 عددا من عناصر هذه الخصوصية "عدم التدخل في أسرته أو منزله" أمر لا يحتاج إلى شرح بشكل معقول ولكن المراسلات؟ بالنسبة للمراسلات، يمكنك التفكير على غرار التواصل الشفهي والكتابي والإلكتروني مع الآخرين، يمكن أن تكون المحادثات المتعلقة بالعمل مثل المحادثات الخاصة بوظيفتك جزءا من ذلك أيضا، أحد الأمثلة على حماية المراسلات هو البريد التقليدي لكل حرف، وكذلك الرسائل النصية للأصدقاء وغيرها من المعلومات على هاتفك[1].

غالبا ما تتعلق الهجمات على الشرف أو السمعة بتصريحات يمكن أن تضر بشخص أو شركة، في جزء كبير من قضايا المحاكم حول هذا الموضوع، يتعلق الأمر بتصريحات تم الإدلاء بها في مقال في وسائل الإعلام أو أثناء البث التلفزيوني، وغالبا ما يتعارض الحق في الخصوصية مع الحق في حرية التعبير، في مثل هذه الحالة يجب على القاضي أن يوازن بين ما هو أكثر أهمية في هذا الوضع الملموس، على سبيل المثال في قضية الارتباط الخارجي المتعلقة بـ "القائمة السوداء" للأطباء على الإنترنت، تم الحكم على ذلك بأنه غير قانوني، وتغلب حق الأطباء في الشرف والسمعة الطيبة على الحق في حرية التعبير.

وتسمى المادة 12 من الإعلان العالمي لحقوق الإنسان أيضا بالحق في الخصوصية أو الحق في الحياة الخاصة، بعد فترة وجيزة من الحرب العالمية الثانية لم يكن هناك حق واسع النطاق في الخصوصية

[1] OHCHR (United Nations Office of the High Commissioner for Human Rights), Universal Declaration of Human Rights at 70: Article 12 – Right to Privacy, Press Release, 21 November 2018
https://www.ohchr.org/en/press-releases/2018/11/universal-declaration-human-rights-70-30-articles-30-articles-article-12

للجميع والذي يحمي جميع جوانبها حتى الآن، لذا كان يجب وضع المادة 12والتي لا تحمي حياة الناس الخاصة فحسب بل تحمي أيضا حياتهم الأسرية ومنازلهم، واتصالاتهم مع الآخرين

('المراسلات')، وشرفهم وسمعتهم ('السمعة الطيبة').[1]

الفرع الثاني: امتداد الحماية لمواجهة التحديات المعاصرة:

صدر الإعلان العالمي لحقوق الإنسان قبل عقود من ظهور الإنترنت والتقنيات الرقمية الحديثة، ومع ذلك أثبتت صياغته المرنة والمبادئ التي تضمنها قدرتها على استيعاب التحديات المعاصرة، فقد أكدت قرارات الأمم المتحدة المتعاقبة بدءا من القرار 167/68 الصادر عن الجمعية العامة عام 2013، على أن الحقوق التي يتمتع بها الأشخاص خارج الإنترنت يجب أن تحمى أيضا على الإنترنت بما في ذلك الحق في الخصوصية[2].

كما أشارت المفوضية السامية لحقوق الإنسان في تقاريرها إلى أن التطورات التكنولوجية الحديثة مثل الذكاء الاصطناعي وقواعد البيانات الضخمة، تطرح تحديات جديدة للخصوصية. فقد أوضحت أن جمع البيانات وتحليلها على نطاق واسع يمكن أن يؤثر على التمتع بالحق في الخصوصية وغيره من حقوق الإنسان، ودعت الدول إلى ضمان أن أي استخدام لهذه التقنيات يتوافق مع المعايير الدولية لحقوق الإنسان.

وتجدر الإشارة إلى أن المادة (12) من الإعلان العالمي شكلت الأساس المباشر للمادة (17) من العهد الدولي الخاص بالحقوق المدنية والسياسية لعام 1966، والتي أعادت صياغة الحماية نفسها ولكن بصيغة ملزمة قانونا للدول الأطراف[3].

[1] Article 12 :Privacy, https://www.uu.nl/en/education/universal-declaration-of-human-rights-75-years/udhr-in-words-and-images/udhr-articles-1-30/article-12-privacy

[2] United Nations General Assembly, Resolution 68/167 on the right to privacy in the digital age (A/RES/68/167), 18 December 2013

[3] Resolution 68/167 on the right to privacy in the digital age (A/RES/68/167), Op.cit

يمثل الإعلان العالمي لحقوق الإنسان من خلال مادته الثانية عشرة حجر الأساس في البناء القانوني الدولي لحماية الحق في الخصوصية، فهو لم يرس مبدأ حماية الحياة الخاصة فحسب، بل وضع الأسس والمعايير التي لا تزال توجه المشرعين والقضاء وهيئات حماية حقوق الإنسان حتى يومنا هذا وبفضل مرونته وشموليته استطاع الإعلان أن يظل وثيقة حية قادرة على مواكبة التحديات المتجددة التي تفرضها التطورات التكنولوجية، مما يجعله مرجعية أساسية لا غنى عنها في مجال حماية الخصوصية في العصر الرقمي.

المطلب الثاني: الحق في الخصوصية في العهد الدولي الخاص بالحقوق المدنية والسياسية

حاول القانون الدولي اللحاق بالركب لمحاولة تنظيم الاهتمام المتزايد بحماية الخصوصية حيث كان المجتمع الدولي بشكل عام بطيئًا في الاستجابة للتغيرات في التقنيات الحديثة، وخاصة تلك التي تعتمد على الاتصالات وجمع البيانات، ومن بين محاولات تقنين هذا الحق وحمايته جاءت المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية.

الفرع الأول: النص القانوني والتوسع المفاهيمي من خلال التعليق العام رقم 16

وينص العهد الدولي الخاص بالحقوق المدنية والسياسية الذي اعتمدته الجمعية العامة للأمم المتحدة في عام 1966 وصادقت عليه حتى الآن 168 دولة في المادة 17 منه على أنه: "لا يجوز تعريض أي شخص لتدخل تعسفي أو غير قانوني في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته، ولا لحملات غير مشروعة"على شرفه وسمعته"،[1] وينص كذلك على ما يلي:

"لكل فرد الحق في حماية القانون من مثل هذا التدخل أو الاعتداءات."

وفي عام 1988 تم توسيع هذا الأمر بشكل أكبر في التعليق العام رقم 16 بشأن المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية وأوضح هذا التعليق:

[1] العهد الدولي الخاص بالحقوق المدنية والسياسية (1966) المادة 17

أولا: تنص المادة 17 على حق كل شخص في الحماية من التدخل التعسفي أو غير القانوني في حياته الخاصة أو أسرته أو مسكنه أو مرسلاته، وكذلك من الاعتداءات غير القانونية على شرف هو سمعته، وترى اللجنة أن هذا الحق مطلوب ضمانه ضد جميع هذه التدخلات والاعتداءات سواء كانت صادرة عن سلطات الدولة أو من أشخاص طبيعيين أو اعتباريين، وتتطلب الالتزامات التي تفرضها هذه المادة من الدولة اعتماد تدابير تشريعية وغيرها من التدابير لتنفيذ الحظر المفروض على مثل هذه التدخلات والهجمات وكذلك لحماية هذا الحق.

ثانيا: وفي هذا الصدد تود اللجنة الإشارة إلى أن تقارير الدول الأطراف في العهد لا تولي الاهتمام اللازم للمعلومات المتعلقة بالطريقة التي يتم بها ضمان احترام هذا الحق من قبل السلطات التشريعية أو الإدارية أو القضائية، وبشكل عام من قبل الأجهزة المختصة المنشأة في الدولة، وعلى وجه الخصوص لم يتم إيلاء اهتمام كاف لحقيقة أن المادة 17 من العهد تتناول الحماية من التدخل غير المشروع والتعسفي.

وهذا يعني أنه في تشريعات الدولة على وجه التحديد وقبل كل شيء يجب النص على حماية الحق المنصوص عليه في تلك المادة، وفي الوقت الحالي إما أن التقارير لا تذكر شيئًا عن هذا التشريع أو أنها لا تقدم معلومات كافية حول هذا الموضوع[1].

وبذلك فإن التعليق العام رقم16 للجنة حقوق الإنسان التابعة للأمم المتحدة بشأن المادة 17 (حقوق إلى الخصوصية) أشارت إلى أنه في رأي اللجنة "يمكن أن تمتد عبارة "التدخل التعسفي" أيضًا لتشمل التدخل المنصوص عليه بموجب القانون"، كما يقدم التعليق العام رقم 16 للجنة حقوق الإنسان التابعة للأمم المتحدة المزيد من الإرشادات بشأن نطاق الحق في الخصوصية المنصوص عليه في المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية فيما يتعلق

[1] Kristian P Humble , Human rights, international law and the right to privacy, University of Greenwich, UK ,2020, page 2

بالتزامات السلطات العامة المشاركة في أنشطة جمع البيانات ومعالجتها[1].

الفرع الثاني: نطاق حماية الخصوصية في العهد الدولي بين النص التقليدي ومتطلبات العصر الرقمي

في عام 1966 لم يكن نطاق العهد الدولي الخاص بالحقوق المدنية والسياسية كافياً للتأكد من التهديد الذي تتعرض له الخصوصية الفردية من التقنيات الرقمية وتكنولوجيات جمع البيانات لأن هذه التقنيات لم تكن موجودة، ولذلك فإن التعريف الوارد في وثيقة عام 1966 يعتبر ضيقا جدا في ظل التقدم التكنولوجي الحالي في مجال الاتصالات وجمع البيانات بحيث لا يمكن أن يكون تعريفا كاملا لحماية الخصوصية[2].

ويذهب التعليق العام لعام 1988 إلى أبعد من ذلك بقليل للتمييز بين التهديد القادم المتمثل في جمع البيانات من قبل الدول وحماية الدول من التدخل في البيانات الخاصة للأفراد، ومع ذلك فإن التقدير الكامل للتكنولوجيات المتعلقة بالاتصالات والمعلومات لم يكن موضع تقدير كامل لأن هذه التكنولوجيات كانت في مهدها فقط[3].

وبذلك تعين على المجتمع الدولي والأمم المتحدة النظر في تحديث التعريف في سياق العصر الرقمي الحديث، وقد تم تعزيز هذه المناقشة العامة من خلال تعيين المقرر الخاص للأمم المتحدة فرانك لارو الذي يتمثل هدفه الوحيد في الإبلاغ عن انتهاك الخصوصية على مستوى الدولة فيما يتعلق بحماية خصوصية الأفراد.

[1] United nations development programme, the impact of digital technology on human rights in Europe and Central Asia, Istanbul regional hub ,2023, page 36

[2] Kristian P Humble, Op.cit , page2

[3] لجنة حقوق الإنسان التابعة للأمم المتحدة، التعليق العام رقم 16: الحق في احترام الحياة الخاصة (المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية)، الدورة الثالثة والثلاثون، 1988، الفقرة 10.

ينص التعليق العام على المادة 17 على أن "جمع المعلومات الشخصية والاحتفاظ بها على أجهزة الكمبيوتر وبنوك البيانات وغيرها من الأجهزة من قبل السلطات العامة أو الهيئات الخاصة يجب أن ينظمه القانون"، كما تمت الموافقة على المبادئ التوجيهية للمادة 17 من قبل لجنة حقوق الإنسان (HRC11) وتم اتباعها في عدد من قرارات المحكمة الأوروبية لحقوق الإنسان (ECtHR).[1]

علاوة على ذلك يؤكد قرار الجمعية العامة للأمم المتحدة المؤرخ 28 ديسمبر 2020 بشأن "الحق في الخصوصية في العصر الرقمي" أيضا على أهمية ضرورة مراعاة المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية فيما يتعلق بمبدأ عدم التمييز (المادة 26 من العهد الدولي الخاص بالحقوق المدنية والسياسية)، والتي تنص على أن "جميع الأشخاص متساوون أمام القانون ويحق لهم دون أي تمييز التمتع بحماية متساوية بموجب القانون"، بالإضافة الى ذلك "في هذا الصدد يجب على القانون أن حظر أي تمييز وضمان لجميع الأشخاص حماية متساوية وفعالة من التمييز على أي أساس مثل العرق أو اللون أو الجنس أو اللغة أو الدين أو الرأي السياسي أو غيره أو الوطني أو الأصل الاجتماعي أو الملكية أو المولد أو أي وضع آخر" ، ويجب قراءة هذه الأحكام مع المادة 17 التي تنص على أنه "لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة" وأن "لكل فرد الحق في حماية القانون من مثل هذا التدخل أو الاعتداءات"، وكذلك مع الفقرة 1 من المادة 2.[2]

[1] Kristian P Humble ,Op.cit, page 2

[2] United nations development programme, the impact of digital technology on human rights in Europe and Central Asia, Istanbul regional hub ,2023 ,page 36.

خلاصة:

يتناول الفصل الأول الإطار المفاهيمي والقانوني للحق في الخصوصية بوصفه أحد الحقوق الأساسية الملازمة لشخصية الإنسان وكرامته، حيث تم التأكيد على أن هذا الحق يهدف إلى حماية الحياة الخاصة للأفراد من أي تدخل تعسفي أو غير مشروع، في ظل ما يشهده العالم من تطورات اجتماعية وتكنولوجية متسارعة.

وقد أبرز الفصل أن مفهوم الخصوصية يعد من المفاهيم المركبة والمتعددة الأبعاد، إذ يجمع بين الجوانب اللغوية التي تشير إلى ما ينفرد به الشخص دون غيره، والجوانب الاصطلاحية التي تعبر عن حق الفرد في العيش بعيدا عن المراقبة أو التدخل، وهو ما يجسد في فكرة "الحق في أن يترك وشأنه"، وقد تطرقنا إلى التطور التاريخي لهذا الحق في الفكر القانوني حيث انتقل من مجرد حماية مادية تقليدية تركز على المسكن والمراسلات إلى حماية معنوية تشمل القيم الشخصية، وصولا إلى مفهوم حديث يرتبط بحماية البيانات الشخصية وخصوصية المعلومات في العصر الرقمي، وفي هذا السياق بين الفصل أن الاعتراف القانوني الصريح بالحق في الخصوصية تبلور مع نهاية القرن التاسع عشر خاصة مع إسهامات الفقه القانوني، قبل أن يتعزز بشكل أكبر بعد الحرب العالمية الثانية من خلال تكريسه ضمن المواثيق الدولية لحقوق الإنسان.

فقد شكل الإعلان العالمي لحقوق الإنسان لسنة 1948 نقطة تحول أساسية بإقراره مبدأ حماية الحياة الخاصة في مادته الثانية عشرة، تلاه العهد الدولي الخاص بالحقوق المدنية والسياسية لسنة 1966 الذي أضفى طابع الإلزام القانوني على هذا الحق، مؤكدا على ضرورة حماية الأفراد من أي تدخل تعسفي في حياتهم الخاصة أو أسرهم أو مراسلاتهم، مع إلزام الدول باتخاذ التدابير التشريعية الكفيلة بضمان ذلك، وأبرز الفصل أن حماية الخصوصية لم تعد تقتصر على مواجهة تدخلات السلطة العامة فحسب، بل امتدت لتشمل حماية الأفراد من انتهاكات الجهات الخاصة، خاصة في ظل التحديات التي فرضها العصر الرقمي وتزايد عمليات جمع ومعالجة البيانات الشخصية، وعليه يخلص الفصل إلى أن الحق في الخصوصية قد شهد تطورا تدريجيا من مفهوم

بسيط إلى منظومة قانونية متكاملة تستدعي تحقيق توازن دقيق بين الحياة الخاصة للأفراد ومتطلبات المصلحة العامة، لاسيما في ظل التحولات التكنولوجية الراهنة.

الفصل الثاني:

التأثيرات التكنولوجية على الحق في الخصوصية

الفصل الثاني: التأثيرات التكنولوجية على الحق في الخصوصية

إذا كانت المواثيق الدولية لحقوق الإنسان قد أرست حماية الحق في الخصوصية بوصفه أحد الحقوق الأساسية للفرد في مواجهة تدخلات السلطة العامة، فإن التحولات التكنولوجية المتسارعة قد فرضت واقعا جديدا أعاد تشكيل مفهوم هذه الخصوصية وتحدياتها، ففي عصر الثورة الرقمية لم تعد الحياة الخاصة مقتصرة على الفضاءات المادية كالمسكن والمراسلات الورقية، بل امتدت لتشمل فضاءات إلكترونية واسعة، تتدفق فيها البيانات الشخصية بلا حدود، وتتقاطع فيها أنماط المراقبة والاستخدام التجاري والحكومي بطرق لم يكن يتخيلها الذين صاغوا الإعلان العالمي لحقوق الإنسان عام 1948[1].

يتناول هذا الفصل أثر التطور التكنولوجي في الحق في الخصوصية من خلال مبحثين رئيسيين : المبحث الأول يتعلق بمظاهر هذا التطور، حيث يستعرض وسائل الاتصال الحديثة والإنترنت التي حولت التواصل الإنساني إلى فضاء مفتوح، ثم الذكاء الاصطناعي وقواعد البيانات الضخمة التي أضفت على جمع البيانات وتحليلها قدرات غير مسبوقة.

أما المبحث الثاني فيتناول الانتهاكات التي رافقت هذه التطورات، متمثلة في المراقبة الرقمية وجمع البيانات على نطاق واسع، وانتهاك البيانات الشخصية وما يرتبط به من تحديات للأمن المعلوماتي.

المبحث الأول: مظاهر التطور التكنولوجي

شهدت العقود الأخيرة تسارعا غير مسبوق في التطور التكنولوجي، طال مختلف نواحي الحياة البشرية، وأحدث تحولات جذرية في أنماط الاتصال، وطرق تخزين المعلومات، وآليات معالجتها. فلم تعد التكنولوجيا مجرد أدوات مساعدة للإنسان، بل أصبحت بيئة افتراضية متكاملة تعكس جوانب واسعة من حياته اليومية من تواصل اجتماعي ومعاملات مصرفية وخدمات صحية إلى أنشطة ترفيهية وعملية، وقد انعكس هذا التحول بصورة مباشرة على مفهوم الحق في الخصوصية،

[1] Geneva International Centre for Justice (GICJ), HRC61: The Global Privacy Gap: When Data Travels Beyond the Law, Report on the 61st Session of the Human Rights Council, 11 March 2026 ; p 2-3

إذ توسعت مجالاته لتشمل فضاءات رقمية لم تكن موجودة من قبل، وتنوعت أشكال التهديدات التي تواجهه بين مراقبة مستمرة وجمع ممنهج للبيانات واستخدامات غير مشروعة للمعلومات الشخصية[1].

يتناول هذا المبحث أبرز مظاهر التطور التكنولوجي ذات التأثير المباشر في الحق في الخصوصية، من خلال تقسيمه إلى مطلبين رئيسيينا :الأول يتعلق بوسائل الاتصال الحديثة والإنترنت، بوصفها البنية التحتية التي غيرت طبيعة التواصل الإنساني وخلقت فضاءات جديدة للحياة الخاصة، والثاني يختص بالذكاء الاصطناعي وقواعد البيانات الضخمة، اللذين يمثلان تغيير نوعي في جمع البيانات وتحليلها واستخدامها، مما أفرز تحديات غير مسبوقة تتطلب إعادة النظر في آليات الحماية التقليدية، ويهدف هذا المبحث إلى تقديم للأسس التقنية التي تقف وراء الانتهاكات الحديثة للخصوصية.

المطلب الأول: وسائل الاتصال الحديثة والإنترنت

تعود أصول الإنترنت إلى حقبة الحرب الباردة في عام 1958، أنشأ الرئيس دوايت د. أيزنهاور وكالة مشاريع الأبحاث المتقدمة(ARPA)[2] ، والتي أعيدت تسميتها فيما بعد بـ DARPA[3]، لتطوير التكنولوجيا العسكرية الأمريكية وكان أحد مشاريع ARPA الطموحة هو إنشاء شبكة كمبيوتر يمكنها مشاركة الموارد بين مرافق البحث المتفرقة جغرافيا.

تم إرسال أول إشارة من كمبيوتر إلى كمبيوتر على ARPANET بين جامعة كاليفورنيا ومعهد ستانفورد للأبحاث في 29 أكتوبر 1969، وكانت هذه الشبكة الناشئة في البداية تربط أربع نقاط فقط في جامعات الأبحاث الكبرى، كان الاختراق هو تقنية تبديل الحزم التي سمحت للبيانات بالانتقال عبر مسارات متعددة بدلا من الاعتماد على اتصال واحد، وهذا يعني أن الشبكة

[1] MDPI Future Internet Journal, Security and Privacy in Physical–Digital Environments: Trends and Opportunities, 2025, p. 1
[2] ARPA : Advanced Research Projects Agency.
[3] DARPA : Defense Advanced Research Projects Agency.

يمكن أن تستمر في العمل حتى لو فشلت العقد الفردية، مع توسع ARPANET خلال السبعينيات ظهر تحدي كبير، لا تستطيع أنظمة الكمبيوتر المختلفة التواصل بشكل فعال مع بعضها البعض.[1]

قام الباحثان فينت سيرف من جامعة ستانفورد وروبرت كان من DARPA، بتطوير بروتوكول التحكم في الإرسال (TCP) وبروتوكول الإنترنت (IP) لحل هذه المشكلة أنشأت هذه البروتوكولات لغة مشتركة لشبكات مختلفة للتواصل.

الفرع الأول: وسائل الاتصال:

الوسيلة لغة :التوصل إلى الشيء برغبة، وهي أخص من الوصلة لتضمنها معنى الرغبة، قال تعالى :وَابْتَغُواْ إِلَيهِ الْوَسِيلَةَ [2](وحقيقة الوسيلة إلى الله تعالى مراعاة سبيله بالعلم والعبادة، وتحري مكارم الشريعة وهي كالقربة، والواسل الراغب إلى الله تعالى).

واصطلاحاً :وسائل الاتصال الحديثة هي أدوات لنشر كافة أنواع المعلومات عن طريق الوسائل الإلكترونية.

الاتصال لغة :وصل بمعنى اتصل، والوصل ضد الهجران، وبينهما وصلة أي :اتصال وذريعة،

وكل شيء اتصل بشيء فما بينهما وصلة، والجمع وصل، والتواصل ضد التقاطع [3].

وقيل :الاتصال لغة: اتخاذ الأشياء بعضها ببعض كاتحاد طرفي الدائرة ويضاد الانفصال

الاتصال اصطلاحاً :له تعاريف كثيرة منها:

---

[1]The Internet: Backbone of modern communication, master of Arts in Distance Education , distance Education Institute, 2025 Available at : **https://distancelearning.institute/educational-communication-technologies/internet-backbone-modern-communication**

[2] سورة المائدة الآية 35

[3] سعيد بن وهف القحطاني، العلاقة المثلى بين الدعاة ووسائل الاتصال الحديثة في ضوء الكتاب والسنة، مطبعة سفير، الرياض الطبعة: الأولى، ١٤٣٢ هـ ، صفحة 9

هو العملية التي بمقتضاها يتفاعل مرسل الرسالة ومستقبلها في مضامين معينة، أو هو تفاعل بين طرفين، وفي هذا التفاعل تنقل أفكار ومعلومات أو وقائع وعواطف وآراء، ومشاركة الصور الذهنية والتوجيه والإقناع.

وسائل الاتصال هي الوسائط والأدوات التي تستخدم لنقل المعلومات والأفكار والرسائل من مرسل إلى مستقبل، بهدف تحقيق التفاهم وتبادل المعارف والخبرات بين الأفراد أو الجماعات، سواء بشكل مباشر أو غير مباشر[1].

أو هو العملية التي ينقل بمقتضاها الفرد القائم بالاتصال منبهات عادة رموز لغوية لكي يعدل سلوك الأفراد الآخرين مستقبلي الرسالة، من خلال مواقع التواصل الاجتماعي، يولد المستخدمون المزيد من البيانات بأنفسهم في مقابل استخدام هذه المواقع، يطلب من المستخدمين الكشف عن بياناتهم الشخصية، وقد لا يدرك المستخدمون المعلومات التي يكشفونها بمجرد إعجابهم بالمنشورات من خلال تفعيل إعدادات خصوصية صارمة افتراضيا، يمكن حماية خصوصية المستخدمين نظرا لجهلهم بالمخاطر، مع ذلك لا يمنع هذا الموقع نفسه من الوصول إلى بياناتهم الشخصية.

الفرع الثاني: الانترنت:

بعد التطرق إلى وسائل الاتصال الحديثة، ينتقل هذا الفرع إلى تناول الإنترنت كأحد أبرز مظاهر التطور التكنولوجي، وذلك من خلال تعريفها وبيان مخاطرها على النحو التالي:

[1] UNESCO, Communication and Information Reports, United Nations Educational, Scientific and Cultural Organization :
https://www.unesco.org/en/communication-information

أولا: تعريف الانترنت: تعرف الإنترنت بأنها "شبكة تتكون من العديد من الحواسيب المرتبطة ببعضها البعض إما عبر الاتصالات السلكية أو اللاسلكية، وتمتد لتشمل مساحات شاسعة من الكرة الأرضية"، وتؤدي الإنترنت خدمات جمة في مجال الحصول على المعلومات بمختلف مجالات الحياة، إذ تمثل خزينة المعرفة ووسيلة للتدفق المعلوماتي.[1]

على الرغم من هذه الأهمية البارزة، فإن الإنترنت تعد أيضاً أداةً متطورة لارتكاب الجرائم، حيث تصبح المعلومات المعالجة إلكترونياً محلاً للتجسس والسرقة والتلاعب بقصد الحصول على أموال أو خدمات غير مستحقة، فالتصفح عبر الإنترنت يترك لدى الموقع المزار كمية هائلة من المعلومات، تتمثل فيما يلي:

1. عنوان بروتوكول الإنترنت (IP) الخاص بالمستخدم، الذي يمكن من خلاله تحديد اسم النطاق، وبالتالي التعرف على اسم الشركة أو الجهة المسجلة للنطاق عبر نظام أسماء النطاقات(DNS) ، وتحديد موقعها الجغرافي.
2. المعلومات الأساسية عن المتصفح ونظام التشغيل، وإعدادات النظام المادية المستخدمة من قبل المستخدم.
3. وقت وتاريخ زيارة الموقع.
4. عناوين الصفحات السابقة التي زارها المستخدم قبل الدخول إلى الصفحة الحالية، وذلك في كل زيارة.
5. معلومات حول محرك البحث الذي استخدمه المستخدم للوصول إلى الصفحة، وقد يظهر عنوان البريد الإلكتروني للمستخدم تبعاً لنوع المتصفح.

كما يمكن أن يحدث التطفل على الحياة الخاصة للغير باستخدام برمجيات خبيثة، مثل: حصان طروادة(Trojan Horse) ، الدودة(Worm) ، والقنابل المنطقية(Logic Bombs) ، أو عبر

[1] أنس الكساسبه وآخرون، دروس في تطبيقات الانترنت وشبكات التواصل الاجتماعي، كلية تكنولوجيا المعلومات، 2025، صفحة 5،6.

وسائل تقنية أخرى كملفات تعريف الارتباط (Cookies) وغيرها من البرامج[1].

ومن أبرز مخاطر الإنترنت قيام الهاكرز بعمليات اختراق أو دخول غير مصرح به، أو البقاء غير المشروع في نظام اتصالي خاص، وجمع المعلومات الخاصة عن الآخرين، ويتم ذلك إما عبر برمجيات ذكية ترسل عبر البريد الإلكتروني، أو من خلال روابط مزيفة قادرة على التجسس على المستخدم، أو حتى ارتكاب جرائم أخرى كالسرقة المعلوماتية والنصب والاحتيال.

أدت التطورات التكنولوجية إلى تأجيج النقاشات حول الخصوصية، وقد استلهمت مقالة وارن وبراندیس الرائدة حول الخصوصية جزئيا من انتهاك الصحفيين للخصوصية عند ظهور الصحف ومنذ ذلك الحين، تركزت نقاشات الخصوصية على حق الأفراد في تحديد مدى وصول الآخرين إليهم، مع مراعاة حق المجتمع في الحصول على المعلومات.

ولذلك يجب أن تأخذ النقاشات حول الخصوصية وحماية البيانات في الحسبان كيفية تطور التطبيقات المختلفة للتقنيات الأساسية، كل تطور تكنولوجي جديد يثير منظورا جديدا حول نقاش الخصوصية، يمكن للمرء أن ينظر على سبيل المثال في تحديات الخصوصية التي تطرحها علم الوراثة والمؤشرات الحيوية وتصوير الدماغ والطائرات بدون طيار وأجهزة الاستشعار القابلة للارتداء وشبكات الاستشعار، ووسائل التواصل الاجتماعي والهواتف الذكية والتلفزيون ذي الدائرة المغلقة، وبرامج الأمن السيبرانية الحكومية، والتسويق المباشر، والبيانات الضخمة، وتقنيات أخرى.[2]

عندما تواجه الخصوصية هذا الهجوم المستمر من قِبل التكنولوجيا الحديثة، يمكن للمرء إما أن يتفاعل بالقبول بأن خصوصيتنا في العصر الرقمي قد انتهت وأننا عاجزون عن حمايتها، أو أن يؤكد أنه نتيجة لهذا التدفق التكنولوجي، باتت حماية الخصوصية أكثر أهمية من أي وقت

[1] بن قارة مصطفى عائشة، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية، كلية الحقوق والعلوم السياسية جامعة عبد الحميد بن باديس، مستغانم، صفحة 42.

[2] بوكر رشيدة، تحديات العصر الرقمي في مواجهة خطط حماية الحق في الخصوصية، مجلة حقوق الإنسان والحريات العامة، المجلد 7، العدد 2، الصفحة 74-75

مضى، كما تؤدي التقنيات الجديدة إلى زيادة الوصول إلى المعلومات الشخصية، مما ينتج عنه زيادة متزامنة في خطر الأذى الشخصي والتمييز، وفقدان الاستقلالية حيث يمكن تحديد موقع الشخص بسهولة، وقد تتعرض فرص العمل والسمعة المهنية للخطر نتيجة للمعلومات الموجودة على الإنترنت. [1]

بالإضافة إلى ذلك بموافقة المستخدمين على مشاركة معلومات شخصية تبدو غير ضارة للوصول إلى مزايا متوقعة عبر الإنترنت، فإنهم يتخلون عن خصوصيتهم، في المقابل تستخدم الأنظمة هذه المعلومات لاستهداف المستخدمين بإعلانات محددة تتناسب مع ملفاتهم الشخصية على الإنترنت.

ثانيا: مخاطر الإنترنت: عندما صمم الإنترنت، لم يكن انتشار شبكة الويب العالمية إلى حالتها الحالية متوقعا، وكذلك إمكانية إساءة استخدامها، كان التوزيع الأولي لمواقع التواصل الاجتماعي ضمن مجموعات من الأشخاص الذين تربطهم معارف في الحياة الواقعية.

لم تصبح الخصوصية مصدر قلق إلا مع توسع شبكات التواصل الاجتماعي، لذا تمت معالجتها كإضافات بدلا من كونها جزءا أساسيا من التصميم[2].

على سبيل المثال تخزن ملفات تعريف الارتباط على جهاز المستخدم للسماح بتخصيص المحتوى، ومع ذلك يمكن لبعض ملفات تعريف الارتباط تتبع المستخدم عبر مواقع ويب متعددة، مما يؤدي إلى عرض إعلانات له لمنتج تصفحه مؤخرا في مكان آخر.

يمكن تضمين أزرار "الإعجاب" من مواقع التواصل الاجتماعي في مواقع ويب أخرى، مما يمكّن شبكة التواصل الاجتماعي من تحديد المواقع التي تمت زيارتها، وبالتالي استهداف الإعلانات وفقا لذلك[3].

---

[1] Sylvana Brannon , Right of privacy Introduction to ICT Law, University of Malta Faculty of Laws, 2018, page 3

[2] OHCHR, The right to privacy in the digital age, A/HRC/39/29, 2018, p. 10-12.

[3] بوكر رشيدة ،المرجع السابق، صفحة 4

نظرا لأن البيانات والبرامج متصلة بالإنترنت، وغالبا ما يكون استخدام البيانات المولدة (من قبل المستخدم والنظام) غير واضح، مما يترك للمستخدم الخيار الوحيد المتاح وهو عدم استخدام الخدمة، علاوة على ذلك ونتيجة لموقع البيانات البعيد ليس من الواضح دائماً أي قانون ينطبق.

المطلب الثاني: الذكاء الاصطناعي وقواعد البيانات الضخمة

لقد أصبح الذكاء الاصطناعي والبيانات الضخمة من أبرز ملامح الثورة الرقمية المعاصرة، حيث يشكلان معا قوة دافعة لإعادة تشكيل مختلف القطاعات الاقتصادية والاجتماعية والأمنية، فبينما يتيح الذكاء الاصطناعي القدرة على تحليل كميات هائلة من البيانات واستخلاص أنماط دقيقة، توفر قواعد البيانات الضخمة المادة الخام التي تغذي هذه الخوارزميات وتمنحها القدرة على التنبؤ واتخاذ القرار[1].

غير أن هذا التداخل بين الذكاء الاصطناعي والبيانات الضخمة يثير تحديات عميقة تتعلق بـ الخصوصية وحماية البيانات الشخصية، إذ أن جمع البيانات على نطاق واسع وتحليلها باستخدام تقنيات متقدمة قد يؤدي إلى كشف معلومات حساسة عن الأفراد والمجتمعات، بل وقد يستخدم في توجيه السلوك أو التأثير على القرارات.

الفرع الأول: الذكاء الاصطناعي:

يستخدم مصطلح "الذكاء الاصطناعي" على نطاق واسع لوصف التقنيات التي تستخدم البيانات والخوارزميات والأجهزة لتحديد العلاقات، والتنبؤ، أو إنجاز مهام شبه معقدة، ويهدف الذكاء الاصطناعي إلى تطوير آلات وبرامج قادرة على أداء وظائف مشابهة للبشر، مثل التعلم والاستدلال والإبداع. [2]

[1] Schwab Klaus ;The Fourth Industrial Revolution; First U.S. Edition, Crown Business, New York, 2017, page 20-25.

[2] UNESCO, Artificial Intelligence and Human Rights, 2021 , page 3,5

ووفقا للعلماء فإن الذكاء هو القدرة على التفاعل والتعلم والاعتماد على المعلومات المستمدة من التجارب، بالإضافة إلى التكيف مع عدم اليقين، في المقابل يشير مصطلح "اصطناعي" إلى نسخة من صنع البشر، لذا فإن الذكاء الاصطناعي هو قدرة نظام حاسوبي على إظهار ذكاء مشابه للبشر، ويشمل ذلك مهارات أساسية مثل الإدراك والفهم والفعل والتعلم ويعتبر البروفيسور جون مكارثي من كلية دارتموث في نيو هامبشاير، الولايات المتحدة، مؤسس

مصطلح "الذكاء الاصطناعي"، حيث عرفه بأنه "علم وهندسة صناعة الآلات الذكية".[1]

يطرح الذكاء الاصطناعي تحديات وفرصا في مجالات مختلفة من حقوق الإنسان تتجاوز "الحقوق الرقمية" التقليدية، مثل الخصوصية وحماية البيانات وحرية الرأي والتعبير، بما في ذلك حرية التجمع وتكوين الجمعيات، وأكد مجلس حقوق الإنسان التابع للأمم المتحدة والجمعية العامة أن "نفس الحقوق التي يتمتع بها الأشخاص خارج الإنترنت يجب أيضا حمايتها عبر الإنترنت".[2]

ومع ذلك لا تزال هناك أسئلة كثيرة حول العواقب المجتمعية لهذا التحول الرقمي وتأثيره على حقوق الإنسان، مع تزايد اعتماد المجتمعات على التقنيات الرقمية، أصبحت حماية حقوق الإنسان أكثر أهمية من أي وقت مضى كما هو الحال مع استخدام هذه التقنيات لتحقيق الصالح العام.

التقنيات الناشئة مثل الذكاء الاصطناعي (AI) لها تأثير كبير على الخصوصية الرقمية، تتيح معالجة البيانات والقدرات التحليلية التي يتمتع بها الذكاء الاصطناعي تقديم خدمات أكثر كفاءة ورؤى قيمة، ومع ذلك يمكن أيضا استخدام هذه القدرات نفسها لتحليل البيانات الشخصية لتحديد الملفات واتخاذ القرارات تلقائيا دون إشراف بشري كاف، مما قد يتطفل على الخصوصية الفردية دون موافقة، وبالتالي في حين يحمل الذكاء الاصطناعي إمكانات كبيرة، فإنه يشكل أيضا مخاطر

[1] Adel Inezarene- University of MostaganeM ,Challenges of using Artificial Intelligence and Big Data in Public Policymaking ,2024,page 608-609

[2] United nations development programme, the impact of digital technology on human rights in Europe and Central Asia, Istanbul regional hub ,2023, page 04

على الخصوصية الرقمية، مما يسلط الضوء على الحاجة إلى سياسات خصوصية قوية لتوجيه استخدامه.

مع استمرار تطور الخصوصية الرقمية مع تقدم التكنولوجيا، يمكن للأفراد التكيف من خلال البقاء على اطلاع بالتغيرات التكنولوجية وآثارها على الخصوصية، يتضمن ذلك فهم سياسات الخصوصية للخدمات الرقمية، واستخدام أدوات وإعدادات الخصوصية المتاحة، والحفاظ على تحديث الأنظمة لمعالجة الثغرات الأمنية المحتملة.

تمثل التطورات مثل تقنية التعرف على الوجه تحديات كبيرة لمعايير الخصوصية الرقمية الراسخة، وفي حين توفر هذه الأدوات فوائد تحويلية للأمن والتحكم في الوصول، فإنها تثير أيضا أسئلة بالغة الأهمية: هل سيفقد الأشخاص عدم الكشف عن هويتهم في الأماكن العامة؟ كيف يمكننا منع سوء الاستخدام لأغراض المراقبة؟ وتؤكد هذه المخاوف الحاجة إلى أطر قانونية وأخلاقية قوية لتنظيم استخدام مثل هذه التقنيات القوية في وقت يزداد فيه الوعي بالخصوصية[1].

لقد غيرت التكنولوجيات الرقمية طريقة ممارسة حقوق الإنسان والحريات، وقد أصبح الإنترنت عنصرا حاسما في الوصول إلى المعلومات وفي تشكيل المجتمعات السياسية، وفي حين أن الإنترنت أداة لا غنى عنها للاجتماعات والاحتجاجات والمشاركة والحملات عبر الإنترنت، فإن النشاط الرقمي يواجه قيودا على الوصول إلى الإنترنت والاتصالات، والمراقبة الرقمية والتهديدات للخصوصية والأمن، والرقابة على الإنترنت زيادة استخدام التقنيات الرقمية.[2]

ويستمر الذكاء الاصطناعي في إثارة تساؤلات حول حماية الخصوصية، وتهدد زيادة الرقابة والمراقبة على الإنترنت "إعمال مبادئ الشفافية والمساءلة التي تعتبر ضرورية لتعزيز وحماية جميع حقوق الإنسان، لا سيما في البلدان التي تنتقل من الاستبداد إلى الديمقراطية".

---

[1] Varun Pratap Singh Bhakuni & Nalnish Chandr Singh ’HISTORICAL PERSPECTIVE ON PRIVACY RIGHTS AND THEIR EVOLUTION IN THE DIGITAL ERA, AD VALOREM - Journal of Law: Volume 12: Issue I:Part II: January - March 2025 , page 13.

[2] OHCHR : The Right to Privacy in the Digital Age, A/HRC/60/45, 29 August 2025, p. 5

وفي حين أن الفضاء الإلكتروني يسهل التعبير ويوفر تنوعا أكبر في المعلومات المتاحة، فإن بعض أصحاب المصلحة لديهم القدرة على حظر المحتوى عبر الإنترنت أو إزالته أو تشويهه وفقا لمصالحهم، وعلى الرغم من أن الذكاء الاصطناعي يتمتع بإمكانات هائلة غير مستغلة، فإن تصميم الذكاء الاصطناعي واستخدامه بشكل غير منظم قد خلق مخاوف مشتركة على نطاق واسع بشأن انتهاك حقوق الإنسان، وخاصة فيما يتعلق بالتمييز الذي تتعرض له شرائح معينة من المجتمع نتيجة لذلك.

الفرع الثاني: قواعد البيانات الضخمة

إن التعريف الأكثر شيوعا للبيانات الضخمة مستمد من تحليل مجموعة البيانات الوصفية، والذي يشمل موارد المعلومات ذات الحجم الكبير والسرعة العالية والتنوع الواسع للبيانات، مما يتطلب أساليب جديدة ومبتكرة لمعالجة المعلومات وتحسينها وتحسين فهم محتوى البيانات، واتخاذ القرارات بناء على البيانات المعالجة[1].

تم تقديم العديد من التعريفات لمفهوم البيانات الضخمة، ومن خلال دراسة التعريفات الموجودة ومواضيع البحث الرئيسية المرتبطة بها، يمكننا التأكيد على أن جوهر مفهوم البيانات الضخمة يمكن التعبير عنه بالعناصر التالية:

الحجم والسرعة والتنوع: تصف هذه المصطلحات خصائص المعلومات المعنية.

التكنولوجيا والأساليب التحليلية: توضح هذه المصطلحات المتطلبات المحددة اللازمة للتعامل مع هذه المعلومات.

تحويل البيانات الضخمة إلى رؤى وخلق قيمة اقتصادية: يمثل هذا الجانب التأثير الرئيسي للبيانات الضخمة على الشركات والمجتمع.

---

[1] Djuro Klipa, Igor Ristic, Aleksandar Radonjic, Ivan Scepanovic, BIG DATA AND ARTIFICIAL INTELLIGENCE , International Journal of Management Trends: Key Concepts and Research, page 4

لذا يمكن تعريف البيانات الضخمة بأنها أصول معلوماتية تتميز بحجمها وسرعتها وتنوعها الكبير، مما يتطلب تكنولوجيا وأساليب تحليلية محددة لتحويلها إلى قيمة[1].

وغالبا ما تعرف البيانات الضخمة بثلاث خصائص أساسية: الحجم والسرعة والتنوع، يؤكد هذا التعريف أن البيانات الضخمة لا تقتصر على مجموعات البيانات الكبيرة أو المتعددة (الحجم)، بل تشمل أيضا البيانات سريعة التغير واللحظية (السرعة) والتنوع الكبير وبشكل عام تشير البيانات الضخمة إلى الزيادة الهائلة في مصادر البيانات من الفضاء ووسائل التواصل الاجتماعي والقطاعين العام والخاص، والقدرة على دمج هذه البيانات لتوليد رؤى جديدة، عادة لأغراض تجارية، تضيف بعض التعريفات عناصر أخرى مثل المصداقية والقيمة والتصور من منظور تقني، بينما يتبنى مؤلفون آخرون منظورا اجتماعيا وسياسيا، مركزين على البيانات الضخمة و"التصديق" باعتبارهما يحولان حياتنا اليومية إلى بيانات قابلة للقياس والتحكم، مما قد يؤدي إلى أشكال من رأسمالية المراقبة.[2]

أحدثت البيانات الضخمة، التي تشير إلى جمع وتخزين وتحليل كميات هائلة من البيانات، ثورة في قطاعات متنوعة كالأعمال والرعاية الصحية والحكومة، إلا أن استخدامها يثير مخاوف جدية بشأن خصوصية الأفراد، ويمكن ملاحظة التأثير الرئيسي لاستخدام البيانات الضخمة على خصوصية الأفراد من زوايا متعددة، تشمل جمع البيانات وتخزينها وتحليلها واستخدامها وذلك من خلال فيما يتعلق بجمع البيانات، غالبا ما تتضمن البيانات الضخمة استرجاع كميات هائلة من البيانات من مصادر متنوعة، بما في ذلك وسائل التواصل الاجتماعي والمعاملات المالية و إنترنت وغيرها، وتجرى هذه العملية أحيانًا دون علم الأفراد أو موافقتهم الصريحة مما يشكل خطرا على خصوصيتهم، فقد لا يكون الأفراد على دراية بكمية البيانات

[1] Ayoung Yoon, Jihyun Kim ,and Devan Ray Donaldson , Big data curation framework: Curation actions and challenges ,Journal of Information ScienceVolume 51, Issue 1, 2025, Pages 205-206
[2] Adel Inezarene- Op.cit , page 611_610

التي تجمع عنهم وكيفية استخدامها[1].

وايضا ينطوي تخزين كميات كبيرة من البيانات على مخاطره الخاصة، إذ يمكن أن يؤدي التخزين غير الآمن إلى تسريبات هائلة للبيانات عند وصول جهات غير مسؤولة إليها، يمكن أن تؤدي تسريبات البيانات إلى سرقة الهوية والاحتيال ومجموعة متنوعة من الجرائم الإلكترونية الأخرى التي قد تضر بالأفراد ماليا ونفسيا، وكذلك يتيح تحليل البيانات الضخمة للمؤسسات تحديد الأنماط والاتجاهات وسلوك الأفراد بدقة عالية، وبينما يمكن استخدام ذلك لأغراض مفيدة، مثل تفضيلات المستهلكين أو الرعاية الصحية الشخصية، إلا أن هناك أيضا جوانب سلبية إذ يمكن أن تؤدي التحليلات التنبؤية إلى إنشاء ملفات تعريفية مفصلة للغاية للأفراد، والتي يمكن استخدامها للتمييز أو التلاعب أو اتخاذ قرارات غير عادلة.[2]

المبحث الثاني: انتهاكات الخصوصية الناتجة عن التكنولوجيا

في العصر الحديث تعد الخصوصية الرقمية مزيجا معقدا من العوامل بما في ذلك البيانات والخصوصية الفردية، يتضمن حماية المعلومات الشخصية التي يشاركها المستخدمون مع مختلف الكيانات سواء أفراد أو شركات أو مؤسسات عامة عبر المنصات الرقمية، ويشمل ذلك حماية الهوية الرقمية للشخص، وضمان سرية وأمن الاتصالات والمعاملات، والحفاظ على السيطرة على البيانات التي ينشئها المستخدم.

لقد غير العصر الرقمي فهمنا وتوقعاتنا للخصوصية، بعد أن تم تعريفها في المقام الأول على أنها الحق في العزلة، تطورت الخصوصية للتأكيد على السيطرة على البيانات الشخصية،

[1] Gunawan Widjaja ,The impact of big data on individual privacy: legal analysis and protection policies, niversitas 17 Agustus 1946 Jakarta, 2025, page 163,164

[2] Cassandra Crossa and Thomas J. Holt, Beyond fraud and identity theft: assessing the impact of data breaches on individual victims, school of Justice, Queensland University of Technology, Brisbane, Australia; bSchool of Criminal Justice, Michigan State University, Lansing, USA, Journal of crime and justice, 2025, page 3,4

وفي هذا السياق تمثل الخصوصية الرقمية قدرة المستخدمين على امتلاك بياناتهم وإدارتها والتحكم فيها، مع التركيز على كيفية جمع هذه المعلومات ومعالجتها وتخزينها ومشاركتها.

تتكون الخصوصية الرقمية من ثلاث مجالات رئيسية: الخصوصية الفردية، وخصوصية المعلومات وخصوصية الاتصالات، تركز الخصوصية الفردية على حماية المعلومات الشخصية المرتبطة بالأفراد، مثل السجلات الصحية أو البيانات المالية أو أرقام الضمان الاجتماعي، تتضمن خصوصية المعلومات حماية البيانات المجمعة رقميا، وضمان التعامل الأخلاقي والقانوني، تتعلق خصوصية الاتصالات بسرية وأمن الاتصالات الرقمية، مما يمنع الوصول والاعتراض غير المصرح به. [1]

تحمل الخصوصية الرقمية آثارا مهمة لكل من الأفراد والشركات، بالنسبة للأفراد فهي تحمي المعلومات الشخصية من السرقة وسوء الاستخدام والتعرض غير المرغوب فيه، وبالتالي تعزيز الأمن الشخصي وتقليل المخاطر مثل سرقة الهوية والمضايقات عبر الإنترنت، بالنسبة للشركات التي تتعامل مع بيانات العملاء، يعد الحفاظ على معايير صارمة لخصوصية البيانات أمرا ضروريا للحفاظ على ثقة المستهلك وتجنب العواقب القانونية التي قد تنجم عن انتهاكات البيانات[2].

المطلب الأول: المراقبة الرقمية وجمع البيانات:

تعتبر المراقبة الرقمية استثناءا على قاعدة الحق في الخصوصية المعلوماتية، فهو إجراء ينتهك حرمة وسرية المعلومات الشخصية المعالجة اليا، والأصل أن هذا الإجراء استثنائي ولا يلجأ اليه الا في حالات تنفيذ إجراءات وقائية من الجرائم المعلوماتية الماسة بأمن وسلامة الدول، أو في حال تنفيذ الإجراءات القضائية المتعلقة بملاحقة مرتكبي هذه الجرائم، ولا يكون

ذلك الا عن طريق رخصة قانونية تسمح صراحة وحصريا باللجوء الى هذه التقنية.

[1] Inverardi, P. et al. "Privacy categorization: A systematic review". Computer Science Review, Vol. 48, 2023. P 2-3.

[2]Varun Pratap Singh Bhakuni & Nalnish Chandr ,Op.cit page 11.

الفرع الأول: المراقبة الرقمية Digital Surveillance

تعرف المراقبة الرقمية بأنها عملية تتبع وتحليل سلوك الأفراد عبر الوسائل التكنولوجية الحديثة، من خلال تحويل أنشطتهم إلى بيانات رقمية قابلة للمعالجة، وقد ارتبط ظهور هذا المفهوم بالتطور الكبير في تكنولوجيا المعلومات والاتصال، حيث أصبح من الممكن تسجيل وتتبع مختلف الأنشطة البشرية[1].

فالمراقبة الرقمية تقوم أساسًا على ما يعرف بـ "البيانات الأثرية الرقمية(Digital Trace Data) "، وهي البيانات التي يتم إنتاجها نتيجة استخدام الأفراد للأنظمة الرقمية مثل التصفح، الرسائل، أو حتى التفاعل عبر الشبكات الاجتماعية .

ويؤكد الباحث توماس Thomas Grisold أن المراقبة الرقمية ترتبط بتحويل السلوك الإنساني إلى بيانات قابلة للتحليل، مما يجعل الأفراد "مرئيين رقميا" وقابلين للمراقبة بشكل دائم[2].

في السنوات الأخيرة ولد التوسع في تقنيات المراقبة الرقمية جدلا كبيرا حول التوازن بين الأمن القومي وحقوق الخصوصية الفردية تنشر الحكومات والشركات الخاصة بشكل متزايد أنظمة المراقبة الرقمية لمراقبة السلوك وجمع البيانات ومنع التهديدات المحتملة، ومع ذلك في حين أن المراقبة يمكن أن تخدم أغراض أمنية أساسية، فإنها يمكن أن تنتهك أيضا حق الأفراد في الخصوصية، مما يخلق تحديات أخلاقية وقانونية معقدة.

وعلى عكس الكاميرات التقليدية لا تترك المراقبة الرقمية أثراً في أغلب الأحيان، إذ تقوم منصات التواصل الاجتماعي وتطبيقات الهواتف المحمولة، وحتى أجهزة المنازل الذكية بجمع البيانات باستمرار، بدءاً من الموقع الجغرافي وسجل التصفح وصولا إلى أنماط التعرف على الوجوه والأوامر الصوتية، بحسب تقرير صادر عن منظمة العفو الدولية عام 2020 تتزايد استخدامات برامج

[1] Brittyn Davis, Surveillance: The Digital Dark Side, Master's Thesis, Chapman University, Spring 2021, p. 1-2
[2] Grisold, Thomas et al., Op.cit, 2024, p. 401

التعرف على الوجوه من قبل الحكومات لمراقبة الاحتجاجات، وتحديد المعارضين وقمع الحركات الديمقراطية لا سيما في الأنظمة الاستبدادية.[1]

وتعد مراقبة الشركات مصدر قلق بالغ أيضا إذ تمتلك شركات التكنولوجيا العملاقة مثل جوجل وأمازون وميتا وآبل، كميات هائلة من بيانات المستخدمين ومن خلال ما يعرف بـ"رأسمالية المراقبة"، تجني هذه الشركات أرباحا طائلة من تتبع سلوك المستخدمين وتفضيلاتهم الشخصية، غالبا دون علمهم أو موافقتهم الكاملة وبينما تقدّم هذه الشركات خدمات مجانية أو منخفضة التكلفة، فإن الثمن الخفي هو خصوصيتنا.[2]

الفرع الثاني: جمع البيانات Data Collection

يمكن تعريف البيانات بأنها القيمة النوعية أو الكمية لمتغير ما مثل:(الأرقام، الصور، الكلمات، الأشكال، الحقائق)، وهي أصغر وحدة معلومات يمكن من خلالها إجراء قياسات وتحليلات أخرى، وتجمع الحقائق والإحصاءات معا لأغراض مرجعية أو تحليلية كما تجمع الكميات أو الأحرف أو الرموز التي تجرى عليها العمليات بواسطة الحاسوب، والتي قد تخزن وترسل على شكل إشارات كهربائية، وتسجل على وسائط تسجيل مغناطيسية أو ميكانيكية في عملية جمع البيانات الرقمية، ويعد جمع البيانات جزءا أساسيا من البحوث الاجتماعية والسلوكية، ويعتبر جمع البيانات غير المتصل بالإنترنت وجمع البيانات المتصل بالإنترنت النمطين الرئيسيين لجمع البيانات.[3]

يكمن تأثير البيانات الضخمة على الخصوصية في ان البيانات الضخمة تتضمن في كثير من الأحيان معلومات شخصية، وهي أي معلومات مسجلة عن شخص يمكن التعرف عليه مثل الاسم والعنوان والآراء والتاريخ الطبي، وكما هو الحال مع أي مجموعة بيانات تتضمن معلومات

[1] Vinayaka. K, Digital Surveillance Vs. Right To Privacy: A Human Rights Perspective, Journal of Emerging Trends and Novel Research, Volume 3, Issue 6 June 2025 ,page 307 .
[2] Nils Bonfils , An Empirical Inquiry into Surveillance Capitalism: Web Tracking, University of Toronto , Canada, 2025, page 3,4
[3] SANDEEP, G. P. Electronic Data Collection Tools for Social Science Research,AGROBIOS-Textbook on fundamental Entomology, issue 11,2022, page 63

شخصية، تحدد قوانين الخصوصية ضمانات معينة يجب على المؤسسات الحكومية تطبيقها لضمان جمع معلوماتك الشخصية واستخدامها والاحتفاظ بها والإفصاح عنها بشكل مناسب[1].

مع ذلك تثير البيانات الضخمة عددا من قضايا الخصوصية الفريدة نظرا لحجمها وتعقيدها، وأنواع عمليات التحليل المستخدمة فيها.

مثال ذلك يمكن للمعلومات التي تجمعها الحكومات أن توفر قدرا كبيرا من التفاصيل عنا، مثل مكان إقامتنا ومن نتواصل معهم وما هي معتقداتنا السياسية أو الدينية، عندما تتضمن مشاريع البيانات الضخمة جمع ودمج كميات هائلة من البيانات (المتاحة للجمهور والداخلية للمؤسسات)، يصبح من الممكن معرفة الكثير عن الناس وكيف يعيشون حياتهم، عند حدوث هذا ومع مرور الوقت يتحول إلى مراقبة، وهي أي نشاط يرصد السلوكيات أو الأفعال أو الاتصالات هذه المراقبة لها استخدامات عديدة مسموح مثل الأمن العام وأبحاث الرعاية الصحية، مع ذلك قد تؤدي البيانات الضخمة عند استخدامها بشكل غير مسؤول إلى أنشطة مراقبة غير مبررة، عندما تقرر الحكومات الانخراط في أنشطة البيانات الضخمة التي تتضمن

معلومات شخصية، يجب أن تفوق فوائد هذه الأنشطة أي مخاطر محتملة على الخصوصية.[2]

عندما تقدم المعلومات الشخصية للحكومة، أو أي مؤسسة خاضعة لقوانين الخصوصية، يجب ان يتم الإبلاغ عن كيفية استخدام هذه المعلومات وسبب ذلك، إلا أن مشاريع البيانات الضخمة تعقّد الأمور، فقد تدمج المعلومات التي جمعت لغرض ما مع معلومات جمعت لغرض آخر، وقد تكون نتائج هذا الدمج وأي تحليلات تجرى على البيانات المدمجة جزءا من دراسة أو برنامج لم يسمع به الأشخاص الذين قدموا معلوماتهم، وبشكل عام تنص قوانين الخصوصية على أنه لا

[1] UN General Assembly (2018) , Report of the Special Rapporteur on the right to privacy (A/73/438). Page 10

[2] Privacy Fact Sheet: BIG DATA AND YOUR PRIVACY RIGHTS, Information and privacy commissioner of ontario,2017, page 2

يجوز استخدام المعلومات الشخصية إلا وفقا للغرض الذي جمعت من أجله في الأصل أو لغرض مصرح به قانونا، وإذا لم تدار مجموعات البيانات الضخمة بشكل سليم، فقد يخالف جمعها واستخدامها والإفصاح عنها قوانين الخصوصية.[1]

المطلب الثاني: انتهاك البيانات الشخصية والأمن المعلوماتي

إذا كانت المراقبة الرقمية وجمع البيانات تمثلان الوجه الأول لتهديد الخصوصية في العصر الرقمي، فإن انتهاك البيانات الشخصية واختلال الأمن المعلوماتي يشكلان الوجه الآخر الأكثر خطورة وفداحة، فمع التوسع الهائل في تخزين البيانات ومعالجتها عبر الأنظمة السحابية وقواعد البيانات الضخمة، برزت إشكالية جديدة تتمثل في هشاشة هذه البيانات أمام الاختراق والتسريب والاستغلال غير المشروع، فلم تعد خروقات البيانات تقتصر على الأفراد العاديين، بل طالت أكبر الشركات والمؤسسات الحكومية، مما أسفر عن تسريب ملايين من السجلات الشخصية والحساسة.[2]

وتتفاقم هذه المعضلة في ظل غياب آليات أمنية فعالة، وضعف التشريعات المنظمة لحماية البيانات، وتزايد الهجمات الإلكترونية المتطورة التي تستهدف البنى التحتية المعلوماتية، لذا يتطلب هذا المطلب تسليط الضوء على طبيعة انتهاكات البيانات الشخصية وأبرز أشكالها، والأسباب المؤدية إليها، وسبل تعزيز الأمن المعلوماتي للحد من هذه المخاطر المتصاعدة.

الفرع الأول: انتهاكات البيانات الشخصية

تعد الجرائم الإلكترونية انتهاكا صارخا للخصوصية، وتتجلى في صورٍ عديدة، منها: سرقة الهوية والاحتيال المصرفي وإنشاء الفيروسات والاختراق وفرض الديون، كما تتضمن هذه

[1] Privacy Fact Sheet. Op.cit, page 03

[2] Cassandra Cross & Thomas J. Holt, Beyond fraud and identity theft: assessing the impact of data breaches on individual victims, School of Justice, Queensland University of Technology & School of Criminal Justice, Michigan State University, Journal of Crime and Justice, 2025, p. 3-4

الجرائم انتهاكات مباشرة لخصوصية الأفراد على سبيل المثال في صورة: المطاردة الإلكترونية، والتنمر الإلكتروني، والمضايقة عبر الإنترنت[1].

يدرك الممارسون القانونيون وغير القانونيين على حد سواء قيمة البيانات، مما يجعل الوصول إليها ممكنا ماديا وافتراضيا، على سبيل المثال تعد البيانات هدفا رئيسيا للمخترقين نظرا لأهميتها في ارتكاب مختلف الجرائم الإلكترونية، ويرجع ذلك عادة إلى أن البيانات غير محمية بشكل كاف، مما يسهل الوصول غير القانوني إليها[2].

وتتمثل الأسباب الرئيسية لانتهاكات البيانات في عدم كفاية أمن النظام والبيانات، وفقدان أو سرقة وحدات التخزين المحمولة المشفرة أو أجهزة الكمبيوتر المحمولة أو الهواتف الذكية؛ والوصول غير المنضبط إلى قاعدة البيانات؛ والكشف غير المقصود عن البيانات أو نشرها أو تسريبها، ومن الأمثلة الشهيرة على انتهاكات البيانات ما يلي:

خلال حادثة عام 2018 تعرضت البيانات البيومترية في الهند للهجوم وخطر الاختراق من قبل قراصنة، فقد تم اختراق أسماء وأرقام هواتف وعناوين بريد إلكتروني وهويات الأفراد المتضررين، حيث استهدفوا قاعدة بيانات الهوية الوطنية المركزية في الهند "آدهار"، والتي تخزن البيانات البيومترية والديموغرافية لـ 1.2 مليار هندي، وتستخدم للتحقق من هويات الناخبين للخدمات المالية والعامة وغيرها.

في عام 2017 تعرض نظام تسجيل العقارات والأراضي في جنوب أفريقيا للاختراق، مما أدى إلى كشف أسماء وجنس ورواتب وتاريخ عمل وأرقام هوية وأرقام هواتف وعناوين منازل ما يقرب من 30 مليون جنوب أفريقي.

---

[1] Vinayaka. K, Digital Surveillance Vs. Right To Privacy: A Human Rights Perspective, Journal of Emerging Trends and Novel Research, Volume 3, Issue 6, June 2025, p.306, 307

[2] UNODC ،الوحدة التعليمية رقم 10 الجرائم الإلكترونية التي تؤثر على الخصوصية. برنامج التعليم من أجل العدالة 2026_03_22 من الرابط :

https://www.unodc.org/e4j/ar/cybercrime/module-10/key-issues/cybercrime-that-compromises-privacy.html

في عام 2013 وفي اختراق شركة ياهو الامريكية Yahoo تضرر أكثر من 3 مليارات مستهلك عندما تم اختراق هوياتهم وعناوين بريدهم الإلكتروني وكلمات مرورهم (التي كانت مخزنة بتشفير ضعيف)، بالإضافة إلى تواريخ ميلادهم.

وقد تعرض أكثر من 350 عميلا لشركة الاستشارات الدولية ديلويت Deloitte لتسريب أسماء المستخدمين ومعلومات الهوية الخاصة بهم بسبب ملف غير محمي داخل الشركة.[1]

في عام 2016 تم الكشف عن واحدة من أكبر وأخطر حوادث انتهاك البيانات الشخصية في تاريخ الإنترنت، وذلك عندما ظهرت قاعدة بيانات قابلة للبحث تحتوي على معلومات حساسة تعود لأكثر من 49 مليون شخص في تركيا، لم تقتصر البيانات المسربة على المعلومات الأساسية مثل الاسم وتاريخ ومكان الميلاد والعنوان فحسب، بل شملت أيضاً تفاصيل دقيقة تهدد الخصوصية الفردية بشكل خطير.

وفي نفس العام 2016، تعرضت بيانات أكثر من 55 مليون ناخب فلبيني (26) الشخصية البيومترية للاختراق عندما تم اختراق موقع لجنة الانتخابات الالكتروني(COMELEC).

وتؤكد الإحصاءات الحديثة خطورة هذه الظاهرة، حيث كشف تقرير صادر عن Experian أن النصف الأول من عام 2025 وحده شهد أكثر من 8,000 خرق بيانات عالمي، كشف ما يقارب 345 مليون سجل شخصي، مما يعكس تصاعد المخاطر التي تهدد خصوصية الأفراد وأمنهم المعلوماتي على نطاق غير مسبوق.[2]

الفرع الثاني: صور انتهاك البيانات والأمن المعلوماتي:

بينما تقدم التقنيات الحديثة فوائد كثيرة تسهل حياة الأفراد، فإنها تشكل أيضا مخاطر كبيرة نظرا للكم الهائل من المعلومات الشخصية المخزنة إلكترونيا، ويتطلب وضع إطار لحماية

[1] Sabah HAOUES, University of Batna1 Legal protection of the right to privacy in the digital era, ELBAHITH for Academic Studies ,2025, page85-86

[2] Experian هي شركة عالمية رائدة في مجال تقارير الائتمان وتحليلات البيانات، وتصدر تقارير دورية حول أمن المعلومات وخرق البيانات، تقاريرها تستخدم كمصادر موثوقة في الأبحاث الأكاديمية والأمنية.

الخصوصية في العصر الرقمي معالجة التهديدات المحددة التي تشكلها هذه التقنيات.

وقد أدى تطور تكنولوجيا المعلومات ولا سيما الإنترنت، إلى ظهور سلسلة من التحديات الجديدة لحماية الخصوصية، فقد زادت الإنترنت بشكل كبير من حجم البيانات التي يتم جمعها ومعالجتها وإنشاؤها، كما سهلت عولمة المعلومات والاتصالات وقد أدى ذلك إلى اللامركزية وفقدان آليات الرقابة، مما قلل من دور الدولة في مراقبة البيانات وحمايتها، وتتبع هذه التحديات من إساءة استخدام تكنولوجيا المعلومات وتطبيقاتها، كما يتضح من الصور التالية:

أولا انتهاك سرية البيانات الشخصية: بما أن البيانات الشخصية تشكل أساس الحق في الخصوصية إذ تتضمن معلومات وتفاصيل عن الفرد تتسم بالسرية بطبيعتها فإن معالجتها غير القانونية تعد من أخطر أشكال انتهاكات الخصوصية، وتحدث هذه الانتهاكات عندما لا يلتزم معالجو البيانات بالمتطلبات والإجراءات القانونية المحددة على المستوى الوطني.

ثانيا الكشف غير المصرح به عن البيانات الشخصية: يعد الكشف غير القانوني عن البيانات الشخصية، لا سيما في المعاملات الإلكترونية شكلا آخر من أشكال انتهاك الخصوصية، وتثير هذه المسألة قلقا بالغا في المهن التي تعتمد على سرية البيانات، كالبنوك والمحاماة.

ثالثا التجسس الإلكتروني: يعد التجسس الإلكتروني من أخطر انتهاكات الخصوصية في التفاعلات الرقمية، وترتبط هذه الممارسة ارتباطاً مباشرا بالاعتراض غير المصرح به للمحادثات والمراسلات والمعاملات الخاصة التي تجرى عبر الإنترنت.[1]

ويعرف التجسس الإلكتروني في سياق الاتصالات الشخصية بأنه "التنصت أو اعتراض البيانات المنقولة بين جهازين عبر الإنترنت" أو "استخراج الانبعاثات الكهرومغناطيسية من جهاز كمبيوتر وتحويلها إلى بيانات قابلة للقراءة باستخدام الوسائل التقنية"، ومن المهم الإشارة إلى أن المراقبة الإلكترونية غير المصرح بها التي تجريها سلطات الدولة عندما تتم خارج إطار القانون تشكل

[1] Chahrazed Aouabed, PROTECTION OF THE RIGHT TO INFORMATIONAL PRIVACY IN ALGERIAN LEGISLATIONDR, Faculty of Law and Political Science, Mohamed Lamine Debaghine University -Sétif 2, Algeria, page2139،2140.

انتهاكا للمعايير القانونية الدولية والمحلية التي تحمي حقوق الأفراد، إذا حدثت مثل هذه المراقبة دون إذن قضائي مسبق، فإنها تعتبر إساءة استخدام لسلطة الدولة بذريعة حماية الأمن القومي أو العام. [1]

تزايدت مخاطر التجسس الإلكتروني بشكل ملحوظ مقارنة بالماضي، لا سيما في عصر العولمة والتقنيات الحديثة، لم يعد التجسس مقتصرا على السلطات الحكومية أو أجهزة الاستخبارات؛ فقد أصبحت أدوات المراقبة متاحة بشكل متزايد للأفراد العاديين، خاصةً في الدول المتقدمة، في المقابل لا تزال الدول العربية تفرض قيوداً صارمة على تسويق وتوزيع معدات المراقبة، مما يجعل الحصول على هذه الأدوات بحرية أمراً صعباً.[2]

تختلف أساليب التجسس الإلكتروني باختلاف الثقافة التقنية للمستخدمين، ومن أكثر التقنيات شيوعاً اعتراض الشبكة، الذي يعتمد على برامج متخصصة لتنفيذ العملية تسمح هذه الطريقة لطرف ثالث غير مصرح له بالتجسس على اتصالات الشبكة التي تجرى عبر الإنترنت، سواء كانت رسائل نصية أو مكالمات صوتية أو مؤتمرات فيديو من خلال اعتراض الشبكة، يمكن التقاط البيانات واسترجاع الصور، ومراقبة المحادثات الصوتية، واعتراض الاتصالات السمعية والبصرية عبر الكاميرات أثناء التفاعلات عبر الإنترنت.[3]

يشكل التنصت والاعتراض والتسجيل العناصر الأساسية لجريمة انتهاك خصوصية الاتصالات، يقصد بالتنصت الاستماع سرا بأي وسيلة كانت إلى محادثة ذات طبيعة سرية أو خاصة دون موافقة الشخص المعني، أما اعتراض المكالمات أو المحادثات فيشمل الحصول على محتوى نقاش بين أفراد أو تسجيل ما قاله شخص ما سرا دون علمه بغض النظر عن التقنية المستخدمة،

---

[1] OHCHR. (n.d.), The right to privacy in the digital age. United Nations Office of the High Commissioner for Human Rights, page 6.
https://docs.un.org/en/A/HRC/39/29
https://www.ohchr.org/en/privacy-in-the-digital-age

[2] Dr. Abeba Birhane & al, Pervasive Surveillance in Computer Vision Research Nature Magazine, 2025, page 75

[3] CHAHRAZED AOUABED,Op.cit, page 2139_2140

ويتضمن التسجيل تخزين المحادثات على جهاز مصمم خصيصا لهذا الغرض، بقصد إعادة تشغيلها لاحقا، أما الإرسال فيشير إلى نقل محادثة أو مكالمة تم الاستماع إليها أو تسجيلها من موقعها الأصلي إلى مكان آخر بأي وسيلة أو تقنية، علاوة على ذلك لا يقل اختراق أجهزة الكمبيوتر وحسابات البريد الإلكتروني خطورة عن أشكال انتهاكات الخصوصية المذكورة آنفا، فقد أصبح الحاسوب الشخصي أحد أهم أدوات التواصل الحديث بين الأفراد إذ يعد وسيلة أساسية للمراسلات والمعاملات الإلكترونية.[1]

وبالتالي يعد اختراق الحاسوب الشخصي انتهاكا جوهريا لخصوصية وسرية المعاملات، واستغلالها لأغراض غير مشروعة، مما قد يلحق ضررا ماليا ومعنويا كبيرا بالأفراد.[2]

وقد ربط بعض الباحثين الاختراق بالمعالجة غير المصرح بها للبيانات، معرفين إياه بأنه: "الوصول غير المصرح به إلى نظام معالجة البيانات باستخدام الحاسوب"

رابعا اختراق البريد الالكتروني: وفيما يتعلق باختراق البريد الإلكتروني، يعد البريد الإلكتروني أحد الأدوات الحديثة المستخدمة في المعاملات الإلكترونية التي يسهلها الإنترنت، فهو يتيح تبادل الرسائل الفورية، مما يبسط التواصل الإلكتروني، ونتيجة لذلك يشكل اختراق البريد الإلكتروني تهديدا كبيرا للحق في الخصوصية، معرضا الأفراد لانتهاكات سرية المعاملات والمراسلات عبر مختلف المجالات، وبناء على ذلك تلزم المبادئ القانونية العامة بوضع ضمانات لحماية سرية الاتصالات، ضمن حدود ولوائح محددة، بغض النظر عما إذا كانت الأساليب المستخدمة تقليدية أم حديثة. [3]

[1]Office of the High Commissioner for Human Rights. Spyware and Surveillance: Threats to Privacy and Human Rights Growing. Geneva: United Nations Human Rights Office, September 16, 2022.
https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing

[2] Spyware and Surveillance: Threats to Privacy and Human Rights Growing . Op.cit 2022

[3] European Union Agency for Cybersecurity (ENISA). Threat Landscape 2021: Email Security and Privacy Risks. Athens: ENISA Publications, 2021. Page 56,57

خلاصة:

يهدف هذا الفصل إلى رصد وتحليل التأثيرات المترتبة على التطور التكنولوجي المتسارع فيما يتعلق بالحق في الخصوصية، وذلك من خلال التمييز بين مظاهر هذا التطور من جهة، وانتهاكات الخصوصية الناتجة عنه من جهة أخرى.

تناول المبحث الأول مظاهر التطور التكنولوجي وتم تقسيمه إلى مطلبين أساسيين: تناول المطلب الأول وسائل الاتصال الحديثة والإنترنت، حيث تبين أن هذه الوسائل قد أعادت تشكيل مفهوم التواصل الإنساني، ولكنها في المقابل أفضت إلى خلق بيئة رقمية دائمة القابلية للمراقبة والتتبع، تجعل الفرد في موقع "المكشوف رقميا" دونما إدراك كاف لتبعات ذلك.

كما ناقش المطلب الثاني الذكاء الاصطناعي وقواعد البيانات الضخمة، وخلص إلى أن قدرة هذه التقنيات على المعالجة الآلية للبيانات والتنبؤ بالسلوك ورسم الملفات الرقمية للأفراد تمثل تحولا نوعيا في طبيعة التهديد الموجه للخصوصية، إذ لم يعد الخطر قاصرا على جمع البيانات بل تجاوزه إلى استخلاص معلومات وأحكام غير معلنة عنها مسبقا.

أما المبحث الثاني فقد خصص لدراسة انتهاكات الخصوصية الناتجة عن التكنولوجيا، واشتمل على مطلبين: كان الأول منها المراقبة الرقمية وجمع البيانات، حيث أظهر التحليل أن هذه المراقبة لم تعد حكرا على أجهزة السيادة الوطنية، وإنما امتدت لتشمل قطاع التكنولوجيا الخاص، منصات التواصل الاجتماعي، وتطبيقات الهواتف الذكية، في مشهد معقد تختلط فيه أغراض الأمن القومي بالتسويق التجاري والدراسة السلوكية، في حين اختص المطلب الثاني بانتهاك البيانات الشخصية وأمن المعلومات، وخلص إلى أن خروقات البيانات قد تحولت إلى ظاهرة هيكلية، تعكس قصورا في أنظمة الحماية التقنية والقانونية على حد سواء، وتؤدي إلى آثار خطيرة تتراوح بين سرقة الهوية الرقمية والابتزاز الإلكتروني، ووصولا إلى التأثير على الحقوق السياسية والاقتصادية للأفراد.

وكخلاصة جوهرية تستمد من هذا الفصل بأكمله، هي أن التكنولوجيا الحديثة تمتلك وجهين متناقضين، فهي من ناحية أداة فعالة للتقدم والتطور وتحسين جودة الحياة، لكنها من ناحية أخرى أصبحت أداة خطيرة لانتهاك الحقوق الإنسانية وأهمها الخصوصية.

كما أن الضرر لا يأتي فقط من التكنولوجيا بحد ذاتها، بل أيضا من غياب الوعي الكافي لدى الأفراد حول كيفية حماية أنفسهم، ومن عدم وجود تشريعات رادعة وشفافة تحد من تجاوزات القطاعين العام والخاص في هذا المجال.

الفصل الثالث:

حماية الحق في الخصوصية وفق مبادئ حقوق الإنسان

الفصل الثالث: حماية الحق في الخصوصية وفق مبادئ حقوق الإنسان

يشكل الحق في الخصوصية أحد الركائز الأساسية في منظومة حقوق الإنسان، إذ يتضمن الضمانة الأساسية التي تتيح للفرد مجالا من الاستقلال والحرية بعيدا عن تدخلات السلطة العامة أو الخاصة غير المبررة، ومع التطور المتسارع لتكنولوجيا المعلومات وظهور أنظمة المراقبة الرقمية وجمع البيانات الضخمة والذكاء الاصطناعي، باتت حماية هذا الحق تواجه تحديات غير مسبوقة تتجاوز قدرة الوسائل القانونية التقليدية على مواكبتها، لذلك أصبح من الضروري تجاوز المقاربات التقنية الضيقة والولوج إلى تأسيس حماية الحق في الخصوصية على مبادئ حقوق الإنسان الجامعة، والتي تستمد شرعيتها من المرجعيات الدولية والدستورية وتجمع بين الثبات الأخلاقي والمرونة في مواجهة مستجدات العصر.[1]

ويتناول هذا الفصل الأسس الحقوقية التي ترتكز عليها حماية الخصوصية، من خلال بداية مبدأ الكرامة الإنسانية باعتباره المنطلق القيمي، ومبدأ المشروعية وعدم التعسف باعتبارهما الضابطين الإجرائيين، ثم الانتقال لاحقا إلى تحليل الآليات القانونية والمؤسساتية الكفيلة بترجمة هذه المبادئ إلى حماية فعالة على أرض الواقع.

المبحث الأول: مبادئ حماية الحق في الخصوصية

لا يمكن فهم حماية الخصوصية على نحو سليم بمعزل عن الأسس الحقوقية التي تنبثق منها، إذ إن فعالية أي نظام قانوني في هذا المجال تتوقف على مدى رسوخ تلك الأسس في الفكر القانوني والسياسي، وعلى قدرتها على استيعاب المتغيرات التكنولوجية دون فصل المحتوى الحقوقي للخصوصية من مضمونه، وفي هذا السياق تستمد حماية الخصوصية مشروعيتها من مبدأين رئيسيين متكاملين: الأول، مبدأ الكرامة الإنسانية، الذي يعد المصدر الأسمى للحقوق والحريات، ويجعل من احترام الفرد وحرمته غاية في ذاتها لا يجوز المساس بها إلا في حدود

[1] The Right to Privacy in the Digital Age, Report A/HRC/39/29, 2018, p3,4.

ضيقة، والثاني مبدأ المشروعية وعدم التعسف، الذي يشكّل الضمانة الإجرائية والموضوعية لضبط أي تدخل في الخصوصية، سواء كان هذا التدخل صادرا عن السلطة العامة أو عن فاعلين من القطاع الخاص، ويهدف هذا المبحث دراسة هاذين المبدأين وتحديد دور كل منهما في بناء إطار حقوقي قادر على تحقيق التوازن بين متطلبات التقدم التكنولوجي وحماية الحقوق الأساسية للأفراد.

المطلب الأول: مبدأ الكرامة الإنسانية

تعد الكرامة الإنسانية إحدى الركائز الأخلاقية للنظام الدولي، إلا أنه لم يظهر مفهوم الكرامة كمفهوم قانوني قبل نهاية الحرب العالمية الثانية وكرد فعل على فظائع الحرب أدرج هذا المفهوم في العديد من قوائم حقوق الإنسان الوطنية والدولية التي وضعت في فترة ما بعد الحرب.[1]

الكرامة الإنسانية مفهوم قانوني بامتياز، يظهر من خلال التكريس الواسع الذي حظيت به على مستوى النصوص القانونية الداخلية أو الدولية، على رأسها الإعلان العالمي لحقوق الإنسان، والذي أدى إلى انتهاج معظم دول العالم هذا المنهاج بتكريسها لهذا الحق في دساتيرها وقوانينها الداخلية.

الفرع الأول: الكرامة في الإعلان العالمي لحقوق الإنسان

من المؤكد أن أهم الأدوات لتحديد مفهوم عام للكرامة الإنسانية هما الوثيقتان التأسيسيتان للنظام الدولي الحديث، وهما ميثاق الأمم المتحدة والإعلان العالمي لحقوق الإنسان، كان ميثاق الأمم المتحدة أول وثيقة قانونية دولية تذكر الكرامة في ديباجتها، وكان الإعلان العالمي لحقوق الإنسان أول وثيقة لحقوق الإنسان تذكر الكرامة، وتشير العديد من صكوك حقوق الإنسان اللاحقة إلى إشارة الإعلان العالمي لحقوق الإنسان إلى الكرامة الإنسانية في ديباجاتها[2].

[1] McCrudden, Christopher. "Human Dignity and Judicial Interpretation of Human Rights". European Journal of International Law, Vol. 19, No. 4, 2008, pp. 655-724.

[2] Niels Petersen, Human Dignity, International Protection, the Max Planck Institute for Comparative Public Law and International Law. 2020.page 3

ورد مصطلح الكرامة مرتين في ديباجة الإعلان العالمي لحقوق الإنسان، في الفقرة الأولى من الديباجة أن "الكرامة المتأصلة" هي "أساس الحرية والعدالة والسلام في العالم"، وتشير الفقرة الخامسة إلى ديباجة ميثاق الأمم المتحدة وتستشهد بها من خلال إعادة تأكيد الإيمان بـ "كرامة الإنسان وقيمته"

ومع ذلك لا يستخدم مصطلح الكرامة في الديباجة فحسب، بل يستخدم أيضا في الجزء التنفيذي من الإعلان العالمي لحقوق الإنسان وبشكل بارز في المادة 1، حيث تنص المادة 1 من الإعلان العالمي لحقوق الإنسان على أن " جميع البشر يولدون أحرارا متساوين في الكرامة والحقوق".

تقترب صياغة المادة 1 من الإعلان العالمي لحقوق الإنسان من المفهوم كانط للكرامة فالتركيز على الحرية والمساواة يذكرنا بالحق الأصلي في الفلسفة الكانطية[1]، علاوة على ذلك تشير الإشارة إلى القيمة في الديباجة إلى تمييز كانط بين القيمة والثمن، مع ذلك تجنب واضعو الإعلان الالتزام صراحة بتقاليد فلسفية محددة لجعل الإعلان مقبولا عالميا، فبدلا من كرامة الشخص تستخدم المادة 1 من الإعلان العالمي لحقوق الإنسان مصطلحا أكثر حيادية «الإنسان»[2]، ولا يقصد بالعقل المجرد البسيط بل «العقل والضمير» ما فطر عليه الإنسان[3].

ذكرت الكرامة أيضا في المادتين 22 و23 من الإعلان العالمي لحقوق الإنسان، واللتين تعلنان حقوقا اجتماعية معينة، تنص المادة 22 من الإعلان العالمي لحقوق الإنسان على أن «لكل إنسان الحق في التمتع بالحقوق الاقتصادية والاجتماعية والثقافية التي لا غنى عنها لكرامته ولنمو شخصيته بحرية»، وبالتالي ترتبط الكرامة بنمو الشخصية بحرية وتضمن المادة 23 من

---

[1] الفلسفة الكانطية هي المدرسة الفلسفية التي أسسها الفيلسوف الألماني إيمانويل كانط.

[2] Hansa Mehta مندوبة الهند: غيرت صياغة "All men" إلى "All human beings" لضمان الحيادية بين الجنسين.

[3] Peng Chun Chang المندوب الصيني فأضاف "الضمير (conscience) "إلى "العقل" ليعبر عن المفهوم الكونفوشيوسي الذي يعني الإحساس بالآخرين.

الإعلان العالمي لحقوق الإنسان لكل إنسان الحق في أجر يمكنه من عيش حياة " تستحق الكرامة الإنسانية ".

ينبغي فهم الكرامة الإنسانية في المقام الأول باعتبارها أساسا رسميا والأساس المبرر لحقوق الإنسان، ويتم التعبير عن ذلك من خلال استخدام الكرامة كسبب إما لضمانات محددة أو حتى لنظام حقوق الإنسان برمته، ومن خلال إرساء حقوق الإنسان على الكرامة المتأصلة، توضح صكوك حقوق الإنسان أن حقوق الإنسان ليست مستمدة من إرادة الدول أو تعتمد عليها، إن حقوق الإنسان غير موجودة لأن الدول اتفقت عليها ولكنها جزء مستقل من النظام القانوني الدولي مما يجعل حماية الحقوق الفردية أحد أهدافه الرئيسية.[1]

الفرع الثاني: العلاقة بين الكرامة الإنسانية والحق في الخصوصية

تعتبر الكرامة الإنسانية من المفاهيم المركزية التي يقوم عليها بناء الحقوق والحريات الأساسية، حيث تمثل الإطار المرجعي الذي تفسر في ضوئه مختلف الحقوق، ومن بينها الحق في الخصوصية، فالخصوصية لا تعتبر مجرد حق ثانوي أو وسيلة لحماية مصالح فردية، بل هي تعبير مباشر عن كرامة الإنسان، إذ إن احترام الحياة الخاصة يعكس الاعتراف بقيمة الفرد كغاية في ذاته وليس مجرد وسيلة.[2]

كما ترتبط الخصوصية ارتباطا وثيقا بالهوية الشخصية، ذلك أن المعطيات الشخصية لا تعتبر مجرد ممتلكات مادية خارجية، بل هي جزء لا يتجزأ من تكوين الإنسان وكيانه، وعليه فإن الاعتداء على هذه المعطيات يمثل مساسا مباشرا بهوية الفرد، ومن ثم انتهاكا لكرامته الإنسانية، ومن هذا المنطلق فإن حماية الخصوصية تعد في جوهرها حماية للذات الإنسانية في بعدها المعنوي.

وفي سياق التطور التكنولوجي والمجتمعات الرقمية، ازدادت أهمية هذا الترابط بين الكرامة

[1] Niels Petersen. Op.cit. page 7

[2] Weber, Olaf. " Human Dignity and the Commercial Appropriation of Personality: Towards a Cosmopolitan Consensus in Publicity Rights?". SCRIPT-ed: A Journal of Law, Technology and Society, Vol. 1, No. 1, 2004, pp. 168-171

والخصوصية، حيث أفرزت تقنيات المراقبة ومعالجة البيانات الشخصية تحديات جديدة تهدد استقلالية الأفراد وتخل بتوازن القوى بينهم وبين المؤسسات، لذلك أصبحت حماية الخصوصية ضرورة لضمان صون الكرامة الإنسانية في مواجهة هذه المخاطر خاصة في ظل اتساع نطاق جمع البيانات وتحليلها[1].

إضافة إلى ذلك ينظر إلى الخصوصية باعتبارها شرطا أساسيا لتحقيق إنسانية الإنسان، حيث تتيح له بناء ذاته وتطوير شخصيته بحرية، فالإنسان كائن في حالة تشكل دائم، والخصوصية تمنحه المساحة اللازمة للحفاظ على هذا الانفتاح، في حين أن انتهاكها يؤدي إلى تقييد هذا المسار وتحويل الفرد إلى موضوع ثابت للمراقبة، مما يفقده جزءا من إنسانيته.

ولا تقتصر هذه العلاقة على الجانب الحقوقي فحسب بل تمتد إلى البعد الأخلاقي، إذ يقابل حق الفرد في الخصوصية واجب احترام خصوصية الآخرين، ومن ثم فإن حماية الخصوصية تسهم في بناء مجتمع قائم على الاحترام المتبادل والمسؤولية، حيث تتكامل الحقوق والواجبات في إطار صون الكرامة الإنسانية[2].

لكل فرد الحق المتساوي في الحقوق الطبيعية ولا يجوز حرمان أي شخص منها، ومن بين هذه الحقوق الحق في الخصوصية، الذي يرتكز بلا شك على كرامة الإنسان وعند المقارنة بين كرامة الإنسان والخصوصية، نجد أن الكرامة هي المجال غير الملموس والشخصي للفرد الذي يضفي الشرعية على الحق في الخصوصية، وتندرج الخصوصية بمفهومها الواسع ضمن نطاق ضمان حقوق الفرد وحرياته ففي نهاية المطاف، لا جدال في أن هذه الحقوق تستند إلى الكرامة المتأصلة للإنسان وغير القابلة للانتهاك. [3]

المطلب الثاني: مبدأ المشروعية وعدم التعسف

[1]Zuboff, Shoshana.The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Public Affairs, New York, 2019, pp. 8-15.

[2]Luciano Floridi, On Human Dignity as a Foundation for the Right to Privacy, Springer, 2016 page 1,2,3,4.

[3] Marcin Wielec ,The Right to Privacy in the Digital Age : Perspectives on Analysis of Certain Central European Countries' Legislation and Practice , page 13.

مبدأ الشرعية أحد أهم مبادئ سيادة القانون، فهو أساس أي نظام قضائي، ولا يمكن تصور وجود سيادة القانون بدونه، وكما هو مبين بوضوح فإن "سيادة القانون" بمعناها الواسع، أي مجموعة السلطات العامة، بغض النظر عن موقعها لا تستحق اسم سيادة القانون ما لم تقدم بنفسها مثالا على الشرعية الدائمة".

وقد ترسخ هذا المبدأ كمبدأ لتنظيم وعمل السلطات العامة للدولة مع ثورة 1789 في فرنسا، وشكل الاعتراف به في قانون ذي قيمة دستورية لحظة تأسيس الدولة القائمة على مبادئ القانون، ومثل شرطا أساسيا لإنشاء إدارة عامة حديثة.

وفي سياق التدخل المتزايد للسلطة القضائية في تنظيم تفاصيل الحياة الاجتماعية، يسهم مبدأ الشرعية إسهاماً حاسماً في الحفاظ على النظام والتوازن في عمل النظام الاجتماعي، من بين الآثار العديدة التي ينطوي عليها هذا المبدأ في القانون ككل، فإن أهمها يتعلق بتطبيقه في القانون العام.

الفرع الأول: علاقة مبدأ الشرعية بمبادئ القانون الأخرى:

يندرج مبدأ الشرعية ضمن المبادئ الدستورية الأخرى التي تضمن سيادة القانون، ومنها: مبدأ الفصل بين السلطات في الدولة، ومبدأ حماية حقوق الإنسان وحرياته، ومبدأ المساواة في الحقوق والواجبات بين جميع المواطنين ومبدأ التعددية السياسية، ومبدأ حرية اللجوء إلى القضاء ومبدأ استقلال القضاء.[1]

توجد مبادئ توجيهية تتعلق بالخصوصية وحماية البيانات، تشكل هذه المبادئ إرشادات للتفسير، وتساعد في سد الثغرات القانونية، وهي ضرورية لتحديد سبل معالجة المشكلات التي تنشأ عند معالجة البيانات الشخصية باستخدام تكنولوجيا المعلومات والاتصالات.

[1] Alexandru STOIAN et Teodora DRĂGHICI, The Principle Of Legality, Principle Of Public Law "Nicolae Balcescu" Land Forces Academy, Sibiu, Romania, 2015, page 512.

يتطلب مبدأ الشرعية في إطار حماية الخصوصية، بالإضافة إلى وجود نص قانوني، أن يكون التدخل متناسباً مع الهدف المراد تحقيقه، وهذا ما يعرف بـ "مبدأ التناسب" أو "الضرورة"، وهو مبدأ مكمل لمبدأ الشرعية، فليس كافياً أن يستند التدخل في الخصوصية إلى نص قانوني، بل يجب أن يكون هذا التدخل ضرورياً في مجتمع ديمقراطي لتحقيق هدف مشروع، كحماية الأمن الوطني أو النظام العام أو الصحة العامة أو حقوق الآخرين.[1]

وتنص المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان على أنه "لا يجوز لأي سلطة عامة التدخل في حق أي شخص في احترام حياته الخاصة... إلا إذا كان هذا التدخل منصوصاً عليه في القانون، وكان ضرورياً في مجتمع ديمقراطي"، كما تنص المبادئ التوجيهية الصادرة عن منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو) للجهات القضائية على أن "أي تدخل في الحق في الخصوصية يجب أن يكون متسقاً مع مبادئ المشروعية والضرورة والتناسب"، وتؤكد منظمة Privacy International أن "مبدأ التناسب يتطلب أن يكون التدخل في الخصوصية متناسبا مع الهدف وأن يكون الخيار الأقل تقييدا المتاح"

الفرع الثاني: علاقة مبدأ المشروعية مع الحق في الخصوصية:

وفقا لمبدأ المشروعية يجب على الجهة المسؤولة معالجة البيانات الشخصية طوال دورة حياتها، بما يتوافق مع القوانين ذات الصلة ومع احترام حقوق الإنسان المعترف بها دوليا، وهذا يعني أنه من خلال المعالجة المناسبة وبالتالي القانونية للبيانات الشخصية، سيتم ضمان احترام الخصوصية والحقوق الأخرى فضلًا عن كرامة صاحب البيانات.

إن دعم الحق في حماية البيانات الشخصية المعترف به كحق يمكن من حماية الحقوق الأخرى، سيضمن أن المعالجة السليمة للبيانات المتعلقة بالفرد ستضمن بدورها احترام حقوقه الأساسية

[1] Privacy International, Legality, Necessity and Proportionality, 2023
https://privacyinternational.org/our-demands/legality-necessity-and-proportionality

الأخرى[1].

على الرغم من أن الشرعية يجب أن تكون أساسا لجميع أنشطة المعالجة طوال دورة حياة البيانات الشخصية من جمعها إلى حذفها، إلا أنه يتم التركيز عادة على نشاط المعالجة الأول وهو جمع البيانات، لأنه إذا تم تنفيذ هذا النشاط بشكل غير قانوني، فسيؤثر ذلك على شرعية أنشطة المعالجة الأخرى الناشئة عنه.

تنص الاتفاقية 108[2] المحدثة على أن معالجة البيانات يجب أن تسعى إلى تحقيق غرض مشروع في جميع المراحل، ويجب أن تتم وفقا للقانون المادة 1.5.

بموجب مبادئ الأمم المتحدة التوجيهية، ووفقا لمبدأ الشرعية والإنصاف، يجب جمع المعلومات الشخصية ومعالجتها بطرق قانونية وعادلة، حيث تعمل الوثائق التنظيمية الدولية المختلفة على توسيع نطاقها وإدراج مبادئ أخرى لحماية البيانات ترتبط بمبدأ الشرعية وتكمله، وفي هذا الصدد تنص المادة 6 والفقرتان 39 و40 من اللائحة العامة لحماية البيانات على أن المعالجة قانونية عند إجرائها وفقا لأساس قانوني منصوص عليه في القانون، وبموجب المعايير الأمريكية ووفقا لمبدأ الشرعية لا يجوز معالجة البيانات الشخصية إلا في ظل الشروط المنصوص عليها في القانون[3].

وتماشيا مع مبادئ منظمة التعاون الاقتصادي والتنمية التوجيهية، يجب جمع البيانات بوسائل

---

[1] Ana Brian Nougreres, Principles underpinning privacy and the protection of personal data, report on the right to privacy, General assembly 77, 2022, page 4

[2] اتفاقية 108: اتفاقية حماية الأشخاص تجاه معالجة المعطيات ذات الطابع الشخصي، وهي إطار قانوني دولي يهدف إلى ضمان حماية الأفراد فيما يتعلق بمعالجة بياناتهم الشخصية.

[3] OECD, Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD Publishing, C(80)58/FINAL, 2013, pp 11,12

قانونية وعادلة وبمعرفة أو موافقة صاحب البيانات، وتستند شرعية معالجة البيانات الشخصية إلى وجود أسس مشروعة كما هو منصوص عليه في اللوائح المعمول بها[1].

المبحث الثاني: آليات الحماية القانونية والمؤسساتية

بعد أن تم التطرق في الفصول السابقة لمفهوم الحق في الخصوصية وبيان أسسه الفلسفية والتاريخية والقضائية، يتناول هذا المبحث الجانب التطبيقي ألا وهو آليات حماية هذا الحق على المستويات التشريعية والقضائية والدولية والتوعوية.

فالحق في الخصوصية رغم كونه من الحقوق الأساسية الملازمة للشخصية الإنسانية، يظل الأكثر تعرضاً للانتهاك في عصر الثورة الرقمية، حيث اتسعت قدرة الدول والشركات والأفراد على جمع البيانات وتحليلها وتداولها بطرق غير مسبوقة، ومن هنا تنبثق أهمية دراسة الآليات التي تحول هذا الحق من كونه مجرد مبدأ نظري إلى حماية عملية فعالة.

تتنوع آليات حماية الخصوصية وتختلف، ويمكن تصنيفها ضمن مستويين رئيسيين هما:

آليات الحماية التشريعية والقضائية وتشمل الإطار القانوني الذي يرسي قواعد حماية البيانات الشخصية، بدءا من النصوص الدستورية التي تقر الحق في الخصوصية كحق أساسي، مرورا بقوانين حماية البيانات العامة والقطاعية، وانتهاء بالسبل القضائية حيث تمثل دور القضاء في تفسير النصوص القانونية، وإنزالها على وقائع النزاعات المستجدة، وموازنة الحق في الخصوصية مع حقوق أخرى كحرية التعبير والحق في المعلومة[2].

آليات الحماية عبر المنظمات الدولية والتوعية الرقمية، وتتمثل في الجهود الدولية الرامية إلى وضع معايير موحدة لحماية الخصوصية، كتوجيهات الاتحاد الأوروبي وإعلانات الأمم المتحدة، وقرارات محكمة العدل الدولية، كما تشمل هذه الآليات دور منظمات المجتمع المدني، ومبادرات

[1] Ana Brian Nougreres, Op.cit, page 5.

[2] Graham Greenleaf, The new data protection convention 108+ and its importance for Asia, International Journal of Law and Information Technology, Volume 34, Oxford Academic, 2026 , Page 09,10

التوعية الرقمية التي تستهدف تعزيز ثقافة الخصوصية لدى الأفراد والمؤسسات، وتمكينهم من أدوات حماية أنفسهم من انتهاكات الخصوصية في الفضاء الرقمي.

المطلب الأول: الحماية التشريعية والقضائية

تعد الحماية التشريعية والقضائية الركيزة الأساسية في منظومة حماية الحق في الخصوصية، إذ تمثل الإطار القانوني الملزم الذي يحدد الحقوق والالتزامات، والآليات القضائية القادرة على إنزال الجزاء على المخالفين وإعادة الحق إلى أصحابه، ويتناول هذا المطلب مستويين مترابطين من الحماية: المستوى التشريعي الذي يرسي القواعد المجردة، والمستوى القضائي الذي يطبق هذه القواعد على النزاعات الواقعية ويضفي عليها الحيوية والفعالية.

الفرع الأول: الحماية التشريعية للحق في الخصوصية

تعتمد الحماية الفعالة للحق في الخصوصية في البيئة الرقمية بشكل أساس على وجود أطر قانونية وتنظيمية سليمة تضعها الدول، وفي هذا السياق تشدد قرارات الأمم المتحدة الصادرة في هذا الشأن على ضرورة أن تتوافق هذه التشريعات مع التزامات الدول في مجال حقوق الإنسان، وأن تتضمن جزاءات رادعة لكل مساس بهذا الحق.[1]

وقد أكد قرار الجمعية العامة للأمم المتحدة رقم 167/68 على ضرورة أن تعمل الدول على تهيئة الظروف الكفيلة بمنع انتهاكات الخصوصية الرقمية، ومن بين هذه السبل ضمان توافق تشريعاتها الوطنية مع التزاماتها بموجب القانون الدولي لحقوق الإنسان[2].

كما تناول القرار رقم 179/73 الأمر ذاته، حيث شدد على ضرورة اعتماد الدول لتشريعات ولوائح وسياسات لحماية البيانات، بما في ذلك تلك المتعلقة ببيانات الاتصالات الرقمية، على أن تمثل

[1] قرار الجمعية العامة للأمم المتحدة رقم 167/68، "الحق في الخصوصية في العصر الرقمي"، 18 ديسمبر 2013.

[2] قرار الجمعية العامة للأمم المتحدة رقم 167/68، مرجع سابق .

هذه الالتزامات الدولية في مجال حقوق الإنسان. ونص القرار نفسه على أن لوائح حماية البيانات ينبغي أن تتضمن جزاءات فعالة[1]

كما أوصى تقرير صادر عن مجلس حقوق الإنسان التابع للأمم المتحدة عام 2021، الدول إلى اعتماد وتنفيذ تشريعات فعالة لخصوصية البيانات في كل من القطاعين العام والخاص، وذلك من خلال سلطات مستقلة وآليات رقابية قوية، باعتبار ذلك شرطاً أساسياً لحماية الحق في الخصوصية في سياق تطبيقات الذكاء الاصطناعي.[2]

وبمراجعة القوانين الوطنية، نجد أن العديد من الدول أدرجت في منظومتها التشريعية نصوصاً قانونية تحمي الخصوصية الرقمية؛ فالجزائر على سبيل المثال، أوجدت حماية قانونية للمعطيات الشخصية بمقتضى القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين إزاء معالجة المعطيات ذات الطابع الشخصي، حيث تنص المادة الثانية منه على أن معالجة هذه المعطيات، مهما كان شكلها أو مصدرها، لا يجوز أن تمس بالحق في الخصوصية، أو الكرامة الإنسانية، أو السمعة، أو الشرف.

أولاً: الحماية الدستورية :تتجه العديد من الدول إلى النص على الحق في الخصوصية ضمن وثائقها الدستورية، مما يمنحه مرتبة عليا تجعله مقيدا للسلطة التشريعية والتنفيذية والقضائية على حد سواء، فالدستور الجزائري لعام 2020 على سبيل المثال ينص في المادة 47 منه على أن "الدولة تضمن حرمة الحياة الخاصة للمواطن وحرمة الأسرة، ولا يمكن المساس بالأسرار الخاصة إلا في الأحوال التي يقررها القانون"[3].

كما ينص الدستور التونسي لعام 2014 في الفصل 24 على أن "الدولة تحمي الحق في الخصوصية وحرمة الحياة الخاصة". [4]

---

[1] قرار الجمعية العامة للأمم المتحدة رقم 179/73، "الحق في الخصوصية في العصر الرقمي"، 17 ديسمبر 2018.

[2] مجلس حقوق الإنسان التابع للأمم المتحدة، تقرير عن "الحق في الخصوصية في العصر الرقمي" 2021 .

[3] المادة 47 من الدستور الجزائري لسنة 2020.

[4] الفصل 24 من الدستور التونسي لسنة 2014.

أما على المستوى المقارن فإن التعديل الرابع للدستور الأمريكي يحمي الأشخاص من التفتيش والمصادرة غير المعقولة، وهو ما فسره القضاء الأمريكي على نطاق واسع ليشمل حماية الخصوصية، وفي ألمانيا قضت المحكمة الدستورية الاتحادية عام 1983 بأن الحق في "تقرير المصير المعلوماتي" يعد حقاً أساسياً مستمداً من الكرامة الإنسانية والحق في حرية تنمية الشخصية.

ثانياً: الحماية عبر قوانين حماية البيانات الشخصية :إلى جانب الحماية الدستورية تسن الدول قوانين خاصة بحماية البيانات الشخصية، وهي تشريعات مفصلة تنظم كيفية جمع البيانات الشخصية ومعالجتها وتخزينها ونقلها، وتعتبر اللائحة العامة لحماية البيانات (GDPR) للاتحاد الأوروبي الصادرة عام 2016 والنافذة عام 2018 النموذج الأكثر تأثيرا على المستوى العالمي، وتقوم هذه اللائحة على مبادئ أساسية منها: مبدأ المشروعية والشفافية وتحديد الهدف، ومبدأ تقليل البيانات، ومبدأ الدقة ومبدأ تحديد مدة التخزين، ومبدأ السلامة والسرية[1].

وعلى المستوى الوطني أصدرت الجزائر القانون رقم 18-07 المؤرخ في 10 يونيو 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، والذي أنشأ أيضاً السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي.

وينص هذا القانون في مادته الأولى على أن "يهدف هذا القانون إلى ضمان حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي"[2].

الفرع الثاني: الحماية القضائية للحق في الخصوصية

إذا كانت النصوص التشريعية تمثل الإطار النظري للحماية، فإن الحماية القضائية تمثل الجانب التطبيقي، إذ يقوم القضاء بتفسير النصوص القانونية وإنزالها على وقائع النزاعات المستجدة، وسد

[1] The EU General Data Protection Regulation (GDPR): A Practical Guide, Springer, 2017, p. 2.

[2] القانون رقم 18-07 المؤرخ في 10 يونيو 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

الثغرات التي قد تتركها النصوص التشريعية، وتحقيق التوازن بين الحق في الخصوصية والحقوق الأخرى المتعارضة معه، وتتجلى أهمية الحماية القضائية في كون القضاء يمثل حماية للحقوق والحريات، حيث يلجأ إليه الأفراد طلباً للانتصاف من أي اعتداء يمس بحياتهم الخاصة سواء أكان صادراً عن أفراد أم عن الدولة نفسه.

لقد تطور تفسير النصوص الدستورية بشكل كبير عبر الزمن لمواكبة التغيرات التكنولوجية، وأبرز مثال على ذلك ما قامت به المحكمة العليا الأمريكية بخصوص التعديل الرابع لدستور الولايات المتحدة الأمريكية، الذي ينص على أن "حق الشعب في أن تكون أشخاصهم ومنازلهم وأوراقهم وممتلكاتهم آمنة من عمليات التفتيش والضبط غير المعقولة، ولا يجوز انتهاكه"[1].

ففي قضية Katz v. United States (1967)، وسعت المحكمة العليا الأمريكية مفهوم الخصوصية ليشمل ما يتجاوز الأماكن المادية، حيث قضت بأن التعديل الرابع يحمي الأشخاص وليس الأماكن فقط، وقدمت مفهوم "التوقع المعقول في الخصوصية ".

وقد مثل هذا القرار نقلة نوعية في الفقه القضائي الأمريكي، حيث انتقل بالحماية من النطاق المادي إلى النطاق المعنوي[2].

وفي قضية Riley v. California (2014)، واجهت المحكمة العليا الأمريكية تحديا جديدا يتمثل في محتوى الهواتف المحمولة، قضت المحكمة بالإجماع أن إنفاذ القانون يحتاج عموما إلى أمر قضائي لتفتيش المحتويات الرقمية للهاتف الخلوي المضبوط من شخص أثناء عملية التوقيف، معتبرة أن الهواتف المحمولة تحمل كميات هائلة من المعلومات الشخصية التي تستحق حماية خصوصية معززة[3].

[1] Ana Dhamo & Iris Dhamo, *Right to Privacy and Constitution: An In-Depth Analysis*, Journal of Rights and Democracy, Vol. 1, Issue 1, 2024, p. 1991.
[2] Katz v. United States, 389 U.S. 347 (1967).
[3] Riley v. California, 573 U.S. 373 (2014).

على الجانب الآخر لعب القضاء الأوروبي دورا رائدا في حماية الحق في الخصوصية، مستندا إلى المادة 8 من الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية، التي تنص على أن "لكل شخص الحق في احترام حياته الخاصة والعائلية ومسكنه ومراسلاته".

ففي قضية S. and Marper v. the United Kingdom (2008) نظرت المحكمة الأوروبية لحقوق الإنسان في سياسة الاحتفاظ بالعينات الوراثية (DNA) للأشخاص المتهمين الذين تمت تبرئتهم، قضت المحكمة بأن الاحتفاظ الدائم بالبصمات الوراثية وعينات الحمض النووي للأشخاص المتهمين ولكن لم تتم إدانتهم يشكل انتهاكاً للمادة 8 من الاتفاقية الأوروبية.[1]

وأكدت المحكمة أن "سياسة الاحتفاظ غير التمييزية بالعينات الوراثية للأشخاص المتهمين ولكن غير المدانين تمثل تدخلاً غير متناسب في حقهم في احترام حياتهم الخاصة".

أما على المستوى الوطني فقد لعبت المحاكم العليا في بعض الدول دورا محوريا في حماية الحق في الخصوصية، ففي نيبال على سبيل المثال أصدرت المحكمة العليا في قضية Advocate Sapana Pradhan Malla v. Government of Nepal أمرا توجيهيا للحكومة بوضع قانون مناسب لحماية الخصوصية في الإجراءات القضائية، ووضعت مبادئ توجيهية إجرائية لحماية الخصوصية في القضايا ذات الطبيعة الخاصة، كقضايا الاغتصاب والاتجار بالأطفال وزنا المحارم، وأكدت المحكمة أن "الحق في الخصوصية هو أساس ضمان كرامة الإنسان" وأن "حماية الحق في الخصوصية تشكل جزءاً مهماً من الوصول إلى العدالة"[2]

المطلب الثاني: دور المنظمات الدولية والتوعية الرقمي

إذا كانت الحماية التشريعية والقضائية تمثل الإطار الداخلي لحماية الخصوصية، فإن المنظمات الدولية ومبادرات التوعية الرقمية تشكل البعد الخارجي والتكميلي لهذه الحماية، فالتحديات العابرة

[1] UNESCO, *Guidelines for Judicial Actors on Privacy and Data Protection*, UNESCO Publishing, 2022, p. 9.

[2] Barsha Jha, *Role of Judiciary in Protection and Promotion of Right to Privacy*, Nepal Law Review, Vol. 57, Issue 68, p. 64-65.

للحدود التي تفرضها العولمة وتكنولوجيا المعلومات جعلت من المستحيل على الدول وحدها حماية خصوصية مواطنيها بشكل كامل، مما استدعى تدخلاً دولياً وتوعية جماهيرية تعزز ثقافة الخصوصية وتمكن الأفراد من حماية أنفسهم. ويتناول هذا المطلب محورين رئيسيين: دور المنظمات الدولية في وضع المعايير والرقابة، ودور التوعية الرقمية في تمكين الأفراد والمجتمع المدني.

الفرع الأول: دور المنظمات الدولية في حماية الحق في الخصوصية

لعبت المنظمات الدولية سواء الحكومية منها أو غير الحكومية دورا محوريا في وضع المعايير الدولية لحماية الخصوصية وتنسيق الجهود بين الدول ومراقبة الانتهاكات وتقديم الدعم الفني والقانوني للضحايا، وتتعدد هذه المنظمات وتتنوع أهدافها غير أنها تتفق جميعها على أن الحق في الخصوصية يمثل قيمة إنسانية عليا تستحق الحماية على الصعيدين الداخلي والدولي[1].

أولا الأمم المتحدة :اهتمت الأمم المتحدة بالحق في الخصوصية منذ وقت مبكر، حيث نصت المادة 12 من الإعلان العالمي لحقوق الإنسان (1948) على أن "لا يجوز تعريض أي شخص لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلته، ولا لحملات تمس بشرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات"،[2] كما أكدت المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية (1966) على نفس المبدأ بشكل ملزم قانوناً للدول الأطراف[3].

وفي العصر الرقمي أصدرت الجمعية العامة للأمم المتحدة عدة قرارات تؤكد على الحق في الخصوصية في سياق العصر الرقمي، أبرزها القرار 167/68 الصادر في 18 ديسمبر 2013،

---

[1] عبد اللطيف دحية، أحمد بن بلقاسم، "الدور الجديد لمنظمة الأمم المتحدة في حماية الحق في الخصوصية في ظل العصر الرقمي"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 2، العدد 4، 2017، ص 498-509 .

[2] المادة 12 من الإعلان العالمي لحقوق الإنسان، الصادر عن الجمعية العامة للأمم المتحدة في 10 ديسمبر 1948.

[3] المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية، الصادر عن الأمم المتحدة عام 1966

الذي أعرب عن القلق البالغ إزاء أعمال المراقبة الجماعية والتنصت التي تجريها الدول[1]، كما عينت الأمم المتحدة مقرراً خاصاً للحق في الخصوصية يقوم برصد انتهاكات الخصوصية حول العالم وتقديم تقارير إلى مجلس حقوق الإنسان، وقد أكدت هذه التقارير على أن "التقدم التكنولوجي وإن كان يحمل فوائد جمة إلا أنه يخلق مخاطر جديدة على الحق في الخصوصية، لا سيما في مجال المراقبة الرقمية وجمع البيانات الشخصية على نطاق واسع".

ثانيا الاتحاد الأوروبي :يعد الاتحاد الأوروبي أكثر المنظمات الإقليمية تقدما في مجال حماية الخصوصية، وذلك من خلال لائحته العامة لحماية البيانات (GDPR) الصادرة عام 2016 والنافذة عام 2018، ولا تقتصر أهمية هذه اللائحة على كونها تطبق داخل دول الاتحاد الأوروبي فقط بل تمتد إلى أي شركة أو مؤسسة تتعامل مع بيانات مواطني الاتحاد، أينما كانت مقرها وذلك بفضل مبدأ "التبعية الإقليمية (territorial scope)[2] "وقد أصبحت اللائحة نموذجا تحتذي به العديد من الدول خارج أوروبا، كالبرازيل واليابان وكاليفورنيا.

كما أنشأ الاتحاد الأوروبي المجلس الأوروبي لحماية البيانات(EDPB) ، وهي هيئة مستقلة تعنى بضمان التطبيق المتسق للائحة عبر الدول الأعضاء، وتقديم التوجيهات والآراء الملزمة في القضايا العابرة للحدود.

وتقوم اللائحة العامة لحماية البيانات على مبادئ أساسية، منها: مبدأ المشروعية والشفافية وتحديد الهدف، ومبدأ تقليل البيانات ومبدأ الدقة ومبدأ تحديد مدة التخزين ومبدأ السلامة والسرية، ومبدأ المساءلة، كما تمنح اللائحة أصحاب البيانات حقوقاً عديدة من أبرزها: الحق في الوصول إلى البيانات والحق في تصحيحها والحق في محوها (الحق في النسيان)، والحق في تقييد المعالجة، والحق في نقل البيانات، والحق في الاعتراض على المعالجة[3].

---

[1] قرار الجمعية العامة للأمم المتحدة رقم 167/68 بتاريخ 18 ديسمبر 2013

[2] Federico Fabbrini, The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court, iCourts Working Paper Series, No. 19, 2015,page 05

[3] Regulation (EU) 2016/679 (General Data Protection Regulation).

ثالثا مجلس أوروبا واتفاقية 108 :يعد مجلس أوروبا أول منظمة إقليمية تتبنى معاهدة دولية ملزمة قانوناً في مجال حماية البيانات، وذلك من خلال "اتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية" (المعروفة بالاتفاقية 108) الصادرة عام 1981 ، وقد تم تحديث هذه الاتفاقية عام 2018 من خلال "الاتفاقية 108+"، والتي أضافت متطلبات جديدة تتوافق مع تطورات العصر الرقمي كتعزيز مبدأ الشفافية وتنظيم تدفق البيانات عبر الحدود، وتوفير حماية أقوى للبيانات الحساسة[1]، وتتميز هذه الاتفاقية بأنها مفتوحة للانضمام من قبل أي دولة في العالم وليس فقط أعضاء مجلس أوروبا مما يوسع نطاق تأثيرها العالمي.

رابعا منظمة التعاون الاقتصادي والتنمية :(OECD) أصدرت منظمة التعاون الاقتصادي والتنمية عام 1980 "المبادئ التوجيهية لحماية الخصوصية وتدفق البيانات عبر الحدود"، والتي شكلت الأساس الذي قامت عليه معظم تشريعات حماية البيانات لاحقا، وقد تم تحديث هذه المبادئ عام 2013 لتواكب التغيرات التكنولوجية وأصبحت مرجعاً أساسياً للدول التي تسن قوانين حماية البيانات لأول مرة، وتقوم هذه المبادئ على ثمانية مبادئ أساسية: مبدأ تقييد الجمع (Collection Limitation)، ومبدأ جودة البيانات(Data Quality) ، ومبدأ تحديد الغرض (Purpose Specification)، ومبدأ تقييد الاستخدام(Use Limitation) ، ومبدأ الضمانات الأمنية (Security Safeguards)، ومبدأ الانفتاح(Openness) ، ومبدأ مشاركة الفرد (Individual Participation)، ومبدأ المساءلة[2](Accountability) .

خامسا المنظمات غير الحكومية :(NGOs) لعبت المنظمات غير الحكومية دورا حاسما في رصد انتهاكات الخصوصية والدفاع عن ضحاياها، لا سيما في المجالات التي تقصر فيها الحكومات أو تعجز عن التحرك، وتشمل أبرز هذه المنظمات: منظمة Privacy"

[1] UNESCO**,** *Guidelines for Judicial Actors on Privacy and Data Protection*, UNESCO Publishing, 2022, p. 16.

[2] OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980, p. 39.40.41.42.43

"International"التي تأسست عام 1990 وتعمل على رصد انتهاكات الخصوصية من قبل الحكومات والشركات حول العالم[1]؛ ومؤسسة "Electronic Frontier Foundation" (EFF) التي تأسست عام 1990 وتدافع عن الحقوق الرقمية في الفضاء الإلكتروني، وتقدم أدلة ونشرات توعوية مبسطة حول مواضيع الخصوصية المعقدة؛[2] ومنظمة "Access Now" التي تركز على حماية خصوصية الناشطين والصحفيين والفئات المعرضة للخطر، كما أن منظمات مثل "منظمة العفو الدولية" و"هيومن رايتس ووتش" باتت تخصص أقساماً للحقوق الرقمية وتوثق انتهاكات الخصوصية في سياق المراقبة الحكومية والرقابة على الإنترنت.

سادسا الجامعة العربية والمنظمات الإقليمية العربية :على المستوى العربي تبنت جامعة الدول العربية "الاتفاقية العربية لمكافحة جرائم تقنية المعلومات" في 21 ديسمبر 2010، والتي تسعى إلى تعزيز التعاون والدعم بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، ودرء أخطار هذه الجرائم حفاظاً على أمن الدول العربية في هذا المجال، وقد أقرت الاتفاقية في فصلها الثاني تجريم الدخول غير المشروع والاعتراض غير القانوني للبيانات الشخصية والاعتداء على سلامتها، كما نصت المادة 14 منها بشكل مباشر على تجريم الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات[3]،غير أنه يؤخذ على هذه الاتفاقية أنها "تسير بخطوات متواضعة وبطيئة في مجال التصدي لاختراق وسرقة البيانات الشخصية وعمليات التجسس على الحياة الخاصة للأفراد"، مقارنة بالتطورات التشريعية في الاتحاد الأوروبي.

الفرع الثاني: دور التوعية الرقمية في حماية الحق في الخصوصية

[1] Privacy International تأسست عام 1990، ومقرها لندن، تعمل كجهة رقابية دولية على انتهاكات الخصوصية، رغم أن موقعها الرسمي يعود لعام 2005، إلا أن المنظمة لا تزال نشطة حتى اليوم.

[2] Electronic Frontier Foundation (EFF) تأسست عام 1990، وهي منظمة غير ربحية رائدة في مجال الحريات المدنية الرقمية، توثق الرسالة الأولى للمؤسس John Perry Barlow (1990) المبادئ التأسيسية للمنظمة.

[3] *الدهبي خدوجة*، حق الخصوصية في مواجهة الاعتداءات الإليكترونية (دراسة مقارنة)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة أحمد دراية – أدرار، العدد الثامن، المجلد الأول، 2017، *ص* 154

إلى جانب الحماية القانونية والمؤسساتية تبرز التوعية الرقمية كآلية أساسية وقائية تهدف إلى تمكين الأفراد والمؤسسات من المعرفة والمهارات اللازمة لحماية خصوصيتهم بأنفسهم، فلا يمكن لأي نظام حماية مهما كان متقدما أن يكون فعالا إذا كان الأفراد يجهلون حقوقهم أو لا يعرفون كيفية ممارستها.

أولاً: مفهوم التوعية الرقمية وأهميتها :تعني التوعية الرقمية في مجال الخصوصية مجموعة الجهود والبرامج التي تهدف إلى رفع مستوى المعرفة لدى الأفراد حول مخاطر انتهاك الخصوصية وكيفية تجنبها وكيفية التصرف في حالة حدوث انتهاك، وتكمن أهمية التوعية الرقمية في أنها تحول الفرد من مجرد "ضحية محتملة" إلى "فاعل قادر على حماية نفسه"، كما تساهم في خلق ثقافة مجتمعية تحترم الخصوصية وتستنكر انتهاكاتها، وقد أظهرت الدراسات أن نقص الوعي هو أحد الأسباب الرئيسية وراء الوقوع ضحية لانتهاكات الخصوصية، حيث يشارك الأفراد بياناتهم الحساسة مع تطبيقات ومواقع غير موثوقة دون أن يدركوا العواقب المحتملة[1].

وفي هذا السياق أشارت إحدى الدراسات إلى أن "المستخدمين العاديين لشبكة الإنترنت يجهلون في الغالب كيفية عمل التقنيات التي يستخدمونها، كما يجهلون المخاطر المحتملة التي تهدد خصوصيتهم، مما يجعلهم فريسة سهلة للمعتدين الإلكترونيين"، كما لوحظ أن "الكثير من مستخدمي وسائل التواصل الاجتماعي لا يحسنون ضبط إعدادات الخصوصية، إما لجهلهم بكيفية القيام بذلك، أو لاعتقادهم أن ما ينشرونه ليس ذا أهمية أو لرغبتهم في نشر صورهم وتعليقاتهم للجمهور".[2]

ثانياً: أشكال وآليات التوعية الرقمية :تتعدد أشكال التوعية الرقمية لتشمل:

---

[1] توبي مندل وآخرون، دراسة استقصائية عالمية حول خصوصية الإنترنت وحرية التعبير، الأمم المتحدة، منشورات اليونسكو، فرنسا، 2013، ص24،25

[2] وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، المركز العربي للبحوث القانونية والقضائية، مجلس وزارة العدل العرب، جامعة الدول العربية، ط1، بيروت، 2017، ص46،47.

أ _ **الحملات الإعلامية والتوعوية** :تنظم الحكومات والمنظمات غير الحكومية حملات توعية عبر وسائل الإعلام التقليدية والجديدة، تهدف إلى نشر المعرفة الأساسية حول حماية الخصوصية كأهمية استخدام كلمات مرور قوية وتفعيل المصادقة الثنائية، وتجنب مشاركة البيانات الحساسة عبر وسائل التواصل الاجتماعي[1]، وفي الجزائر تقوم السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي (ANPDP) بنشر أدلة وإرشادات للمواطنين حول كيفية حماية بياناتهم الشخصية، كما تنظم حملات توعوية في المؤسسات التعليمية والجامعات.

ب _ **إدماج التوعية في المناهج التعليمية** :بدأت العديد من الدول في إدراج مواضيع الخصوصية والأمن الرقمي ضمن المناهج الدراسية من المراحل المبكرة، بهدف ترسيخ ثقافة رقمية سليمة لدى الأجيال الجديدة[2]، ويعد هذا الأمر ضروريا في ظل تزايد اعتماد الأطفال والمراهقين على الإنترنت في الدراسة والتواصل والترفيه.

ج _ **برامج تدريبية للمؤسسات** :تقدم جهات حكومية وخاصة برامج تدريبية للموظفين في المؤسسات حول كيفية التعامل مع البيانات الشخصية وفق أحكام القانون، وكيفية الإبلاغ عن خروقات البيانات وتكتسي هذه البرامج أهمية خاصة في المؤسسات التي تتعامل مع كميات كبيرة من البيانات الشخصية، كالبنوك وشركات الاتصالات والمستشفيات.

د _ **أدوات التوعية التفاعلية** :تم تطوير أدوات تفاعلية كالألعاب التعليمية والمحاكاة، التي تساعد الأفراد على فهم مخاطر الخصوصية بطريقة جذابة وسهلة.

هـ _ **منصات التوعية الرقمية** :أنشأت العديد من هيئات حماية البيانات حول العالم منصات إلكترونية متخصصة تقدم نصائح وإرشادات وأدوات مجانية للمواطنين، كموقع "Have I Been[3] Pwned" الذي يتيح للمستخدمين التحقق مما إذا كانت بياناتهم قد تسربت في خروقات

---

[1] مندل وآخرون، المرجع السابق، ص 26

[2] Sandra Cortesi & Andres Lombana-Bermudez, Digital Citizenship and Privacy in K-12 Education, Berkman Klein Center for Internet & Society, Harvard University, 2019, p31

[3] Have I Been Pwned: https://haveibeenpwned.com/

بيانات سابقة.

ثالثاً: دور المجتمع المدني في التوعية الرقمية :يقوم المجتمع المدني بدور رائد في التوعية الرقمية، لا سيما في المجالات التي لا تستطيع أو لا ترغب الحكومات في تغطيتها، فمنظمات مثل "Electronic Frontier Foundation"[1] تقدم أدلة ونشرات توعوية مبسطة حول مواضيع الخصوصية المعقدة كما تنظم ورش عمل وندوات مجانية، ومنظمة "Privacy International" [2] تنشر تقارير وأدلة حول كيفية حماية الخصوصية في مواجهة المراقبة الحكومية ومراقبة الشركات، وفي العالم العربي برزت مبادرات مجتمع مدني مثل "مؤسسة سورا Sora) Foundation) [3]" المتخصصة في الأمن الرقمي للناشطين والصحفيين، ومشروع "سمسم" لتعزيز الثقافة الرقمية في شمال إفريقيا.

رابعاً: علاقة التوعية الرقمية بالحماية القانونية والمؤسساتية :لا يمكن النظر إلى التوعية الرقمية على أنها بديل عن الحماية القانونية والمؤسساتية بل هي مكمل ضروري لها، فالحماية القانونية توفر الإطار والضمانات والجزاءات، أما التوعية فتمكن الأفراد من الاستفادة من هذه الضمانات والجزاءات، فقد لا يعرف المواطن أن له حق تقديم شكوى إلى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي أو لا يعرف كيفية تقديمها، أو لا يدرك أن ما تعرض له يشكل انتهاكاً يستوجب الشكوى أصلاً وهنا يأتي دور التوعية في سد هذه الفجوة المعرفية[4].

كما أن التوعية تساهم في تعزيز فعالية الحماية المؤسساتية، لأنها تزيد من عدد الشكاوى المقدمة وتنوعها، مما يمنح الهيئات الرقابية صورة أوضح عن حجم ونوع الانتهاكات الجارية، ويمكنها من تحديد أولويات عملها بشكل أفضل، وقد أكدت الدراسات الجزائرية أن "توعية المواطنين بحقوقهم

---

[1] EFF: https://www.eff.org/issues/privacy

[2] Privacy International: https://privacyinternational.org/learn

[3] : موقع مؤسسة سورا: https://sora.foundation/

[4] عمراوي مارية – حجاج مليكة، حماية الحق في الخصوصية عبر الانترنيت دراسة وصفية تحليلية وفق قانون العقوبات الجزائري، دراسات وأبحاث المجلة العربية للأبحاث والدراسات في العلوم الإنسانية والاجتماعية، مجلد 12، عدد 3، جويلية *2020، ص329، 330*

في الخصوصية الرقمية تعتبر خطوة أساسية لتفعيل آليات الحماية القانونية، فكثير من الانتهاكات تمر دون متابعة قضائية لمجرد أن الضحية لا تعلم أن ما تعرض له يشكل

جريمة يعاقب عليها القانون".

خلاصة الفصل الثالث:

تناولنا في هذا الفصل حماية الحق في الخصوصية في ضوء مبادئ حقوق الإنسان، حيث قسمناه إلى مبحثين رئيسيين: الأول تناول الأسس الحقوقية لحماية الخصوصية، والثاني تناول آليات الحماية القانونية والمؤسساتية.

في المبحث الأول فقد بينا أن الحق في الخصوصية يقوم على ركيزتين أساسيتين، الأولى مبدأ الكرامة الإنسانية الذي يُعد الأساس الفلسفي والقيمي لهذا الحق، فهو الذي يمنحه قدسيته وأهميته، و أن الخصوصية إنما هي تجسيد للكرامة الإنسانية في الحياة اليومية، حيث تحمي الإنسان من التدخلات التعسفية في شؤونه الخاصة، وتصون أسراره وحرمات مسكنه ومراسلاته، والثانية مبدأ المشروعية وعدم التعسف الذي يمثل الضمانة الأساسية لحماية الخصوصية من تجاوزات السلطات العامة والأفراد، حيث يقتضي أن أي تدخل في هذا الحق لا يكون مشروعاً إلا إذا استند إلى نص قانوني واضح، وكان ضرورياً في مجتمع ديمقراطي لتحقيق هدف مشروع مع مراعاة مبدأ التناسب.

أما في المبحث الثاني فقد استعرضنا فيه آليات الحماية العملية للحق في الخصوصية، وقسمناها إلى مستويين، المستوى الأول الحماية التشريعية والقضائية، حيث تبين أن الحماية التشريعية تتمثل في النصوص الدستورية التي تكرس الحق في الخصوصية، وقوانين حماية البيانات الشخصية كاللائحة العامة لحماية البيانات (GDPR) للاتحاد الأوروبي والقانون الجزائري 18-07، أما الحماية القضائية فقد تجسدت في دور القضاء في تفسير النصوص القانونية وتطويرها لمواكبة التطورات التكنولوجية والمستوى الثاني فقد خصصناه لدور المنظمات الدولية والتوعية الرقمية، فتبين أن المنظمات الدولية لعبت دوراً محورياً في وضع المعايير وتنسيق الجهود،

وفي مقدمتها الأمم المتحدة من خلال الإعلان العالمي لحقوق الإنسان والعهد الدولي الخاص بالحقوق المدنية والسياسية، وقرارات الجمعية العامة والمقرر الخاص للحق في الخصوصية، والاتحاد الأوروبي من خلال لائحته العامة لحماية البيانات، ومجلس أوروبا من خلال الاتفاقية 108 المعدلة ، كما يظهر أن المنظمات غير الحكومية كـ Privacy International و Electronic Frontier Foundationو Access Now تساهم بشكل فعال في رصد الانتهاكات والدفاع عن الضحايا.

أما التوعية الرقمية فأنها تمثل آلية وقائية أساسية تهدف إلى رفع مستوى المعرفة لدى الأفراد حول مخاطر انتهاك الخصوصية، وتحول الفرد من ضحية محتملة إلى فاعل قادر على حماية نفسه، وتساهم في خلق ثقافة مجتمعية تحترم الخصوصية، كما تواجه جهود التوعية تحديات عديدة، أبرزها الفجوة الرقمية، وسرعة تطور التقنيات، ومحدودية الموارد.

نخلص إلى أن حماية الحق في الخصوصية وفق مبادئ حقوق الإنسان تتطلب مقاربة متكاملة تقوم على ثلاث ركائز، التأسيس القيمي من خلال ترسيخ مبدأ الكرامة الإنسانية والمشروعية، والإطار القانوني من خلال تشريعات وازنة وقضاء فعال، والدعم المؤسساتي والتوعوي من خلال انخراط المنظمات الدولية وبرامج التوعية المستدامة.

الخاتمة:

بعد التطرق في الفصول الثلاثة من هذه المذكرة إلى مختلف جوانب الحق في الخصوصية، بدءا من الإطار المفاهيمي والقانوني الذي يحدد ماهية هذا الحق وأسسه وتطوره التاريخي، مروراً بالتأثيرات التكنولوجية المتسارعة التي أفرزتها الثورة الرقمية وتداعياتها على الحياة الخاصة للأفراد في عصر الذكاء الاصطناعي والبيانات الضخمة، وصولا إلى آليات الحماية القانونية والمؤسساتية وفق مبادئ حقوق الإنسان التي تشكل الضمانة الأساسية لصون هذا الحق في مواجهة التحديات الراهنة والمستجدة، نصل في هذا المقام إلى استخلاص جملة من النتائج التي توصلنا إليها من

خلال هذه الدراسة التحليلية، ورصد بعض الاقتراحات التي نرى أنها تساهم في تعزيز حماية الحق في الخصوصية في البيئة الرقمية، وذلك من منظور متكامل يجمع بين الجوانب التشريعية والقضائية والمؤسساتية والتوعوية.

وبناء على ما سبق من تحليل نظري وتطبيقي لمختلف جوانب الحق في الخصوصية، فإننا ننتقل فيما يلي إلى استخلاص أهم النتائج التي أسفرت عنها هذه الدراسة والتي تمثلت في تأصيل الحق في الخصوصية حيث تبين من خلال الدراسة أن الحق في الخصوصية ليس وليد العصر الحديث، بل هو حق راسخ في الفكر القانوني، شهد تطورا تاريخيا من حماية مادية تركز على المسكن والمراسلات إلى حماية معنوية تشمل القيم الشخصية، وصولا إلى مفهوم حديث يرتبط بحماية البيانات الشخصية وخصوصية المعلومات في العصر الرقمي.

والأسس الحقوقية للحماية يبرز الحق في الخصوصية كأحد الحقوق الأساسية المرتبطة بكرامة الإنسان، حيث توجد علاقة وثيقة بين الكرامة الإنسانية والخصوصية، فالخصوصية تجسيد مباشر للكرامة في الحياة اليومية، كما أن مبدأ المشروعية وعدم التعسف يشكل الضمانة الإجرائية لأي تدخل في الحياة الخاصة.

التحديات التكنولوجية حيث أفرز التطور التكنولوجي المتسارع تأثيرات مباشرة على الحق في الخصوصية، فوسائل الاتصال الحديثة والإنترنت حولت التواصل الإنساني إلى فضاء مفتوح، كما أن الذكاء الاصطناعي وقواعد البيانات الضخمة أضفت على جمع البيانات وتحليلها قدرات غير مسبوقة، تقنيات المراقبة الرقمية لم تعد حكرا على أجهزة السيادة الوطنية بل امتدت إلى قطاع التكنولوجيا الخاص ووسائل التواصل الاجتماعي.

وانتهاكات الخصوصية إذ كشفت الدراسة أن انتهاك البيانات الشخصية تحول إلى ظاهرة هيكلية، تتجلى في خروقات كبيرة طالت ملايين السجلات الشخصية، مما يهدد الأمن المعلوماتي للأفراد ويقلل ثقتهم في البيئة الرقمية.

والحماية التشريعية إذ تتفاوت التشريعات الوطنية في قدرتها على حماية الخصوصية الرقمية، فالجزائر مثلاً أصدرت القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي وأنشأت السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي غير أن هذه النصوص تبقى بحاجة إلى تفعيل وتطوير.

والدور الدولي حيث ساهمت المنظمات الدولية سواء الحكومية منها أو غير الحكومية بشكل فعال في وضع المعايير الدولية لحماية الخصوصية. فالاتحاد الأوروبي يعد نموذجاً رائداً من خلال لائحته العامة لحماية البيانات(GDPR) ، كما أن الأمم المتحدة ومجلس أوروبا ومنظمة التعاون الاقتصادي والتنمية ساهمت في ترسيخ المبادئ الأساسية لحماية البيانات الشخصية.

ثم أهمية التوعية الرقميةحيث أثبتت الدراسة أن التوعية الرقمية تشكل خط الدفاع الأول في مواجهة انتهاكات الخصوصية، إذ تحول الفرد من مجرد ضحية محتملة إلى فاعل قادر على حماية نفسه، كما تساهم في تعزيز فعالية الحماية القانونية والمؤسساتية إلى حد كبير، وتخفض من عدد الانتهاكات المترتبة أساسا عن الجهل.

استنادا إلى النتائج المتوصل إليها، نقترح جملة من الاقتراحات التي نأمل أن تساهم في تعزيز حماية الحق في الخصوصية في البيئة الرقمية:

1. تطوير الإطار القانوني الدولي:

_ صياغة صك دولي ملزم (اتفاقية او بروتوكول) خاص بحماية الخصوصية في العصر الرقمي، يسد الفراغ القانوني القائم حالياً.

_ توسيع الانضمام إلى الاتفاقية 108 لمجلس أوروبا والاتفاقية العربية لمكافحة جرائم تقنية المعلومات مع تحديثهما.

ـ **إدراج الحق في حماية البيانات الشخصية** كحق مستقل في الصكوك الدولية، مثل المادة 8 من ميثاق الحقوق الأساسي للاتحاد الأوروبي.

2. تعزيز آليات الرقابة الدولية:

ـ **تعزيز ولاية المقرر الخاص** للأمم المتحدة المعني بالحق في الخصوصية بالموارد اللازمة وتوسيع اختصاصه.

ـ **إنشاء لجنة دولية** لحماية البيانات الشخصية على غرار لجنة حقوق الإنسان، تختص بمراقبة تنفيذ الدول لالتزاماتها والنظر في الشكاوى الفردية.

ـ **تفعيل آليات الإنذار المبكر** للتدخل السريع في حالات الانتهاكات الجسيمة للخصوصية.

3. تعزيز التعاون الدولي:

ـ **توسيع التعاون القضائي الدولي** في مكافحة الجرائم الإلكترونية العابرة للحدود، من خلال تبادل المعلومات وتسليم المجرمين.

ـ **تنسيق التشريعات الوطنية** عبر الحدود لتجنب تضارب القوانين وتسهيل تدفق البيانات بشكل آمن.

ـ **إنشاء آليات عربية مشتركة** كمركز عربي للاستجابة السريعة لانتهاكات البيانات، وآلية للتعاون القضائي في الجرائم الإلكترونية.

4. مواجهة التحديات التكنولوجية:

ـ **وضع معايير دولية ملزمة** لتنظيم استخدام تقنيات الذكاء الاصطناعي، خاصة أنظمة التعرف على الوجه والتنميط الآلي.

ـ **تنظيم تدفق البيانات عبر الحدود** (Cross-Border Data Flows)وفق آليات واضحة تحقق التوازن بين حماية الخصوصية وحرية التجارة.

_ حظر تصدير تقنيات المراقبة الجماعية إلى الدول التي قد تستخدمها في انتهاك جسيم لحقوق الإنسان.

5. التوعية وبناء القدرات:

_ إطلاق برنامج دولي للتوعية بالخصوصية الرقمية تحت إشراف الأمم المتحدة واليونسكو، خاصة في البلدان النامية.

_ إدماج حقوق الخصوصية الرقمية في مناهج التربية على حقوق الإنسان على المستوى العالمي.

_ **بناء قدرات القضاة وأعضاء النيابة** في الدول النامية من خلال دورات تدريبية دولية متخصصة.

6. اقتراحات خاصة بالدول العربية والجزائر

_ تعزيز المشاركة العربية في صياغة المعايير الدولية لحماية الخصوصية، لضمان مراعاة الخصوصيات الثقافية والقانونية للدول العربية.

_ تحديث الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (2010)لتتماشى مع المعايير الدولية المتقدمة.

_ إنشاء محكمة عربية متخصصة في الجرائم المعلوماتية العابرة للحدود.

_ انضمام الجزائر إلى الاتفاقية 108 لمجلس أوروبا، والتفاعل مع آليات الأمم المتحدة المعنية بحماية الخصوصية.

قائمة المصادر والمراجع:

أولا: المصادر باللغة العربية:

- ابن منظور، **لسان العرب**، دار صادر، بيروت، ج 7.
- مجمع اللغة العربية، **المعجم الوسيط**، دار الدعوة، القاهرة، ج 1.

ثانيا: المراجع باللغة العربية:

- وسيم شفيق الحجار، **النظام القانوني لوسائل التواصل الاجتماعي**، المركز العربي للبحوث القانونية والقضائية، مجلس وزارة العدل العرب، جامعة الدول العربية، ط1، بيروت، 2017.

- سعيد بن وهف القحطاني، **العلاقة المثلى بين الدعاة ووسائل الاتصال الحديثة في ضوء الكتاب والسنة**، مطبعة سفير، الرياض، الطبعة الأولى، 1432 هـ.
- أنس الكساسبة وآخرون، **دروس في تطبيقات الانترنت وشبكات التواصل الاجتماعي**، كلية تكنولوجيا المعلومات، 2025.
- توبي مندل وآخرون، **دراسة استقصائية عالمية حول خصوصية الإنترنت وحرية التعبير**، الأمم المتحدة، منشورات اليونسكو، فرنسا، 2013.

ثالثا: المواثيق والقوانين الدولية

- **الإعلان العالمي لحقوق الإنسان**، الصادر عن الجمعية العامة للأمم المتحدة بتاريخ 10 ديسمبر 1948، المادة 12.
- **العهد الدولي الخاص بالحقوق المدنية والسياسية**، الصادر عن الأمم المتحدة عام 1966، المادة 17.
- **الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية**، الصادرة عام 1950، المادة 8.
- **الاتفاقية 108 لمجلس أوروبا**)اتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية) الصادرة عام 1981 والمحدثة عام 2018 (الاتفاقية 108+)
- **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات**، جامعة الدول العربية، 21 ديسمبر 2010.
- **اللائحة العامة لحماية البيانات(GDPR)** ، Regulation (EU) 2016/679الصادرة عن الاتحاد الأوروبي.
- **مبادئ منظمة التعاون الاقتصادي والتنمية (OECD) التوجيهية** لحماية الخصوصية وتدفق البيانات عبر الحدود، 1980 (المحدثة 2013).

رابعا: القوانين الوطنية الجزائرية

- **الدستور الجزائري لسنة 2020**، المادة 47.
- **القانون رقم 18-07** المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 34، المؤرخة في 10 يونيو 2018.

خامسا: قرارات الأمم المتحدة وتقاريرها

- **قرار الجمعية العامة للأمم المتحدة رقم 167/68**، "الحق في الخصوصية في العصر الرقمي"، 18 ديسمبر 2013.
- **قرار الجمعية العامة للأمم المتحدة رقم 179/73**، "الحق في الخصوصية في العصر الرقمي"، 17 ديسمبر 2018.

- **قرار الجمعية العامة للأمم المتحدة رقم 166/69**، "الحق في الخصوصية في العصر الرقمي"، 18 ديسمبر 2014.
- **تقرير مفوض الأمم المتحدة السامي لحقوق الإنسان** حول الحق في الخصوصية في العصر الرقمي، المؤرخ في 13 سبتمبر 2021، الملحق رقم.A/HRC/48/31
- **تقرير مجلس حقوق الإنسان التابع للأمم المتحدة**، "الحق في الخصوصية في العصر الرقمي"، 2021.
- **تقرير المقرر الخاص المعني بالحق في الخصوصية**، الجمعية العامة للأمم المتحدة، A/73/438، 2018.
- **تقرير مجلس حقوق الإنسان**، "الحق في الخصوصية في العصر الرقمي"، A/HRC/39/29، 2018.
- **التعليق العام رقم 16 للجنة حقوق الإنسان** التابعة للأمم المتحدة بشأن المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية، 1988.

سادسا: المجلات العلمية والأبحاث الأكاديمية باللغة العربية:

- عبد اللطيف دحية، أحمد بن بلقاسم، "الدور الجديد لمنظمة الأمم المتحدة في حماية الحق في الخصوصية في ظل العصر الرقمي"، **مجلة الأستاذ الباحث للدراسات القانونية والسياسية**، المجلد 2، العدد 4، 2017.
- الدهبي خدوجة، "حق الخصوصية في مواجهة الاعتداءات الإليكترونية (دراسة مقارنة"(، **مجلة الأستاذ الباحث للدراسات القانونية والسياسية**، جامعة أحمد دراية – أدرار، العدد الثامن، المجلد الأول، 2017.
- عمراوي مارية – حجاج مليكة، "حماية الحق في الخصوصية عبر الانترنيت: دراسة وصفية تحليلية وفق قانون العقوبات الجزائري"، **دراسات وأبحاث: المجلة العربية للأبحاث والدراسات في العلوم الإنسانية والاجتماعية**، مجلد 12، عدد 3، جويلية 2020.
- خالد عبد الله راشد الزعابي، "مفهوم وخصائص وصور الخصوصية (دراسة مقارنة"(، **مجلة البحوث القانونية والاقتصادية**، جامعة المنصورة، 2025.
- فوزية شريط، "التطور التاريخي للحق في الخصوصية بين النصوص الدينية والأحكام الوضعية (دراسة تحليلية)"، كلية العلوم الإنسانية والحضارة الإسلامية، جامعة أحمد بن بلة وهران –1– الجزائر، مركز جيل البحث العلمي، سلسلة كتاب أعمال المؤتمرات، العدد 26، 2019.
- بوكر رشيدة، "تحديات العصر الرقمي في مواجهة خطط حماية الحق في الخصوصية"، **مجلة حقوق الإنسان والحريات العامة**، المجلد 7، العدد 2.

- بن قارة مصطفى عائشة، "الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية"، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم.

سابعا: المراجع باللغات الأجنبية:

- **Bonfils, Nils.** *An Empirical Inquiry into Surveillance Capitalism: Web Tracking*. University of Toronto, Canada, 2025.
- **Brannon, Sylvana.** *Right of Privacy: Introduction to ICT Law*. University of Malta, Faculty of Laws, 2018.
- **Davis, Brittyn.** *Surveillance: The Digital Dark Side*. Master's Thesis, Chapman University, Spring 2021.
- **Floridi, Luciano.** *On Human Dignity as a Foundation for the Right to Privacy*. Springer, 2016.
- **Holvast, Jan.** *History of Privacy*. Holvast & Partner, Privacy Consultants, NL - Landsmeer, The Netherlands.
- **Humble, Kristian P.** *Human Rights, International Law and the Right to Privacy*. University of Greenwich, UK, 2020.
- **Petersen, Niels.** *Human Dignity, International Protection*. Max Planck Encyclopedia of Public International Law, Oxford Public International Law, 2020.
- **Porcedda, Maria Grazia.** *Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis*. HART PUBLISHING, Great Britain, 2023.
- **Solove, Daniel J.** *A Brief History of Information Privacy Law*. George Washington University Law School, 2006.
- **Westin, Alan F.** *Privacy And Freedom*. 25 Wash. & Lee L. Rev., Washington and Lee University School of Law Scholarly Commons, 1968.
- **Wielec, Marcin.** *The Right to Privacy in the Digital Age: Perspectives on Analysis of Certain Central European Countries' Legislation and Practice*.
- **United Nations Development Programme**, *The Impact of Digital Technology on Human Rights in Europe and Central Asia*, Istanbul Regional Hub, 2023.
- **UNESCO**, *Guidelines for Judicial Actors on Privacy and Data Protection*, UNESCO Publishing, 2022.
- **UNESCO**, *Artificial Intelligence and Human Rights*, 2021.

- **UNODC** الوحدة التعليمية رقم 10: الجرائم الإلكترونية التي تؤثر على الخصوصية، برنامج التعليم من أجل العدالة
- **Office of the High Commissioner for Human Rights**, *Spyware and Surveillance: Threats to Privacy and Human Rights Growing*, Geneva, September 16, 2022.

ثامنا: الأحكام القضائية

- **Semayne's Case (1604)** ،COURT OF KING'S BENCH ،All ER Rep 62.
- **Katz v. United States**389 ، U.S. 347 (1967).
- **Riley v. California**573 ، U.S. 373 (2014).
- **S. and Marper v. the United Kingdom** (2008) المحكمة الأوروبية لحقوق الإنسان.
- **Advocate Sapana Pradhan Malla v. Government of Nepal** المحكمة العليا النيبالية.

تاسعا: المجلات العلمية والأبحاث الأكاديمية باللغة الاجنبية:

- **AOUABED, CHAHRAZED.** "Protection of the right to informational privacy in Algerian legislation". Faculty of Law and Political Science, Mohamed Lamine Debaghine University - Sétif 2, Algeria.
- **Bhakuni, Varun Pratap Singh & Singh, Nalnish Chandr.** "Historical Perspective on Privacy Rights and Their Evolution in the Digital Era". *AD VALOREM - Journal of Law*, Volume 12, Issue I, Part II, January - March 2025.
- **Birhane, Abeba (Dr.) et al.** "Pervasive Surveillance in Computer Vision Research". *Nature Magazine*, 2025.
- **Birnhack, Michael.** "Defense of Privacy-as-Control (Properly Understood)". *Forthcoming in Jurimetrics*, Vol. 65, 2026.
- **Brian Nougreres, Ana.** "Principles underpinning privacy and the protection of personal data". *Report on the Right to Privacy*, General Assembly 77, 2022.
- **Cross, Cassandra & Holt, Thomas J.** "Beyond fraud and identity theft: assessing the impact of data breaches on individual victims". *Journal of Crime and Justice*, School of Justice, Queensland University of Technology & School of Criminal Justice, Michigan State University, 2025.
- **Fabbrini, Federico.** "The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court". *iCourts Working Paper Series*, No. 19, 2015.
- **Greenleaf, Graham.** "The New Data Protection Convention 108+ and its Importance for Asia". *International Journal of Law and Information Technology*, Volume 34, Oxford Academic, 2026.
- **Grisold, Thomas; Seidel, Stefan; Heck, Markus; & Berente, Nicholas.** "Digital Surveillance in Organizations". *Business & Information Systems Engineering*, Volume 66, Issue 3, June 2024.
- **Grisold, Thomas; Heck, Markus; Seidel, Stefan; & Berente, Nicholas.** "How Behavioral Visibility Leads to Disempowerment and

Empowerment in Organizations: Evidence from Manufacturing". *SaudiCIS 2024 Proceedings*, 2024.

- **HAOUES, Sabah.** "Legal protection of the right to privacy in the digital era". *ELBAHITH for Academic Studies*, University of Batna 1, 2025.
- **Inezarene, Adel.** "Challenges of using Artificial Intelligence and Big Data in Public Policymaking". University of Mostaganem, 2024.
- **Jha, Barsha.** "Role of Judiciary in Protection and Promotion of Right to Privacy". *Nepal Law Review*, Vol. 57, Issue 68.
- **KICHE, FATAH.** "Mechanisms for the protection of the right to privacy in Algerian legislation". Adrar University - Algeria, 2019.
- **Klipa, Djuro; Ristic, Igor; Radonjic, Aleksandar; Scepanovic, Ivan.** "Big Data and Artificial Intelligence". *International Journal of Management Trends: Key Concepts and Research* (ISSN: 2956-0772), Publisher: Fakultet za menadžment, Univerzitet Union Nikola Tesla, Sremski Karlovci, Serbia.
- **MDPI Future Internet Journal.** "Security and Privacy in Physical-Digital Environments: Trends and Opportunities", 2025.
- **Puri, Anupriya.** "The Group Right to Mutual Privacy". *Ethics and Information Technology*, Vol. 2, No. 2, Springer, 2023.
- **Sandeep, G. P.** "Electronic Data Collection Tools for Social Science Research". *AGROBIOS-Textbook on Fundamental Entomology*, Issue 11, 2022.
- **Stoian, Alexandru & Drăghici, Teodora.** "The Principle of Legality, Principle of Public Law". *International Conference KNOWLEDGE-BASED ORGANIZATION*, Vol. XXI No 2, "Nicolae Balcescu" Land Forces Academy, Sibiu, Romania, 2015.
- **Vinayaka K.** "Digital Surveillance Vs. Right To Privacy: A Human Rights Perspective". *Journal of Emerging Trends and Novel Research (JETNR)*, ISSN: 2984-9276, Volume 3, Issue 6, June 2025.
- **Widjaja, Gunawan.** "The Impact of Big Data on Individual Privacy: Legal Analysis and Protection Policies". Universitas 17 Agustus 1946 Jakarta, 2025.
- **Yoon, Ayoung; Kim, Jihyun; Donaldson, Devan Ray.** "Big data curation framework: Curation actions and challenges". *Journal of Information Science*, Volume 51, Issue 1, 2025.

عاشرا: المواقع الإلكترونية والتقارير الإلكترونية

- **Privacy International**: https://privacyinternational.org/
- **Electronic Frontier Foundation (EFF)**: https://www.eff.org/
- **مؤسسة سورا**: https://sora.foundation/
- **Have I Been Pwned**: https://haveibeenpwned.com/
- **OHCHR** (United Nations Office of the High Commissioner for Human Rights): https://www.ohchr.org/

- **The IT Law Wiki**: Definition of physical privacy.
- **The Internet: Backbone of modern communication**, Master of Arts in Distance Education, Distance Education Institute, 2025.
- **European Union Agency for Cybersecurity (ENISA)**, *Threat Landscape 2021: Email Security and Privacy Risks*, Athens, 2021.
- **Information and Privacy Commissioner of Ontario**, *Privacy Fact Sheet: Big Data and Your Privacy Rights*, 2017.
- **Experian** (تقارير دورية حول أمن المعلومات وخرق البيانات).

الفهرس:

شكر وعرفان..... أ

إهداء..... ب

مقدمة.....01

الفصل الأول: الإطار المفاهيمي والقانوني للحق في الخصوصية.....06

المبحث الأول: مفهوم الحق في الخصوصية.....07

المطلب الأول: تعريف الحق في الخصوصية.....07
الفرع الأول: التعريف اللغوي.....09
الفرع الثاني: التعريف الاصطلاحي.....09
المطلب الثاني: تطور الحق في الخصوصية في الفكر القانوني.....11
الفرع الأول: مرحلة الخصوصية المادية.....12
الفرع الثاني: مرحلة الخصوصية المعنوية والخصوصية كحق عام.....13
المبحث الثاني: الحق في الخصوصية في المواثيق الدولية لحقوق الإنسان.....16
المطلب الأول: الحق في الخصوصية في الإعلان العالمي لحقوق الإنسان.....17
الفرع الأول: مضمون ونطاق الحماية بموجب المادة 12.....17
الفرع الثاني: امتداد الحماية لمواجهة التحديات المعاصرة 19
المطلب الثاني: الحق في الخصوصية في العهد الدولي الخاص بالحقوق المدنية والسياسية20
الفرع الأول: النص القانوني والتوسع المفاهيمي من خلال التعليق العام رقم 16.....20
الفرع الثاني: نطاق حماية الخصوصية في العهد الدولي بين النص التقليدي ومتطلبات العصر الرقمي.....22
خلاصة الفصل الأول.....24
الفصل الثاني: التأثيرات التكنولوجية على الحق في الخصوصية.....26
المبحث الأول: مظاهر التطور التكنولوجي.....26
المطلب الأول: وسائل الاتصال الحديثة والإنترنت.....27
الفرع الأول: وسائل الاتصال.....28
الفرع الثاني: الانترنت.....29
المطلب الثاني: الذكاء الاصطناعي وقواعد البيانات الضخمة.....33
الفرع الأول: الذكاء الاصطناعي.....33

الفرع الثاني: قواعد البيانات الضخمة 36
المبحث الثاني: انتهاكات الخصوصية الناتجة عن التكنولوجيا.....38
المطلب الأول: المراقبة الرقمية وجمع البيانات.....39
الفرع الأول: المراقبة الرقمية.....40
الفرع الثاني: جمع البيانات.....41
المطلب الثاني: انتهاك البيانات الشخصية والأمن المعلوماتي.....43
الفرع الأول: انتهاكات البيانات الشخصية.....43
الفرع الثاني: صور انتهاك البيانات والأمن المعلوماتي.....45
خلاصة الفصل الثاني.....49
الفصل الثالث: حماية الحق في الخصوصية وفق مبادئ حقوق الإنسان.....51
المبحث الأول: الأسس الحقوقية لحماية الخصوصية.....51
المطلب الأول: مبدأ الكرامة الإنسانية.....52
الفرع الأول: الكرامة في الإعلان العالمي لحقوق الإنسان.....52
الفرع الثاني: العلاقة بين الكرامة الإنسانية والحق في الخصوصية.....54
المطلب الثاني: مبدأ المشروعية وعدم التعسف.....56
الفرع الأول: علاقة مبدأ الشرعية بمبادئ القانون الأخرى.....56
الفرع الثاني: علاقة مبدأ المشروعية مع الحق في الخصوصية.....57
المبحث الثاني: آليات الحماية القانونية والمؤسساتية.....59
المطلب الأول: الحماية التشريعية والقضائية.....60
الفرع الأول: الحماية التشريعية للحق في الخصوصية.....60
الفرع الثاني: الحماية القضائية للحق في الخصوصية.....62
المطلب الثاني: دور المنظمات الدولية والتوعية الرقمية.....64

الفرع الأول: دور المنظمات الدولية في حماية الحق في الخصوصية.....65
الفرع الثاني: دور التوعية الرقمية في حماية الحق في الخصوصية.....68
خلاصة الفصل الثالث.....72
الخاتمة.....74
قائمة المصادر والمراجع.....78
الفهرس.....84
الملخص.....87

الملخص:

تناولت هذه المذكرة موضوع "الحق في الخصوصية في ظل التطور التكنولوجي"، وذلك في إطار دراسة قانونية تحليلية تهدف إلى بيان مفهوم هذا الحق وأسسه القانونية وتطوره التاريخي، ثم رصد التأثيرات التي أحدثتها التكنولوجيا الحديثة لاسيما وسائل الاتصال الحديثة والإنترنت والذكاء الاصطناعي وقواعد البيانات الضخمة على خصوصية الأفراد، إلى جانب تحليل مختلف الانتهاكات التي تمس الحياة الخاصة في البيئة الرقمية كالمراقبة الرقمية وجمع البيانات واختراق الحسابات الشخصية، كما هدفت الدراسة إلى استعراض آليات الحماية القانونية والمؤسساتية المكرسة لهذا الحق على المستوى الدولي والوطني، بدءاً من بعض النصوص الدستورية والتشريعية مروراً بالحماية القضائية، وانتهاء بدور المنظمات الدولية والتوعية الرقمية. اعتمدت الدراسة على المنهج الوصفي التحليلي، وذلك من خلال وصف المفاهيم والنصوص القانونية وتحليلها، ثم استخلاص النتائج وتقديم التوصيات، وقد خلصت الدراسة إلى أن الحق في الخصوصية حق أساسي مستمد من كرامة الإنسان، وأن التطور التكنولوجي المتسارع قد أفرز تحديات غير مسبوقة تهدد هذا الحق، كما أظهرت أن الحماية الفعالة تتطلب مقاربة متكاملة تجمع بين تشريعات وازنة

وقضاء فعال ومؤسسات مستقلة وتوعية مستدامة وتعاون دولي، مع ضرورة مواكبة التشريعات الوطنية والمواثيق الدولية للتطورات التكنولوجية، وتفعيل دور الهيئات الوطنية و الدولية لحماية البيانات، وإطلاق حملات توعية واسعة النطاق.

الكلمات المفتاحية :الحق في الخصوصية، التطور التكنولوجي، حماية البيانات الشخصية، المواثيق الدولية، المراقبة الرقمية، الذكاء الاصطناعي، الحماية التشريعية، الحماية القضائية، التوعية الرقمية

Abstract

This thesis examines the "Right to Privacy in Light of Technological Development" through a legal analytical study aimed at clarifying the concept of this right, its legal foundations, and its historical evolution, It then monitors the impacts of modern technology particularly modern means of communication the Internet artificial intelligence and big data on individuals' privacy, while analyzing various violations affecting private life in the digital environment, such as digital surveillance, data collection, and personal account hacking, The study also aims to review the legal and institutional protection mechanisms established for this right at both international and national levels, starting from constitutional and legislative texts, through judicial protection, to the role of international organizations and digital awareness, The study adopted a descriptive analytical approach, describing and analyzing concepts and legal texts, then drawing conclusions and providing recommendations, The study concluded that the right to privacy is a fundamental right derived from human dignity, and that rapid technological development has created unprecedented challenges threatening this right, It also showed that effective protection requires an integrated approach combining robust legislation, effective judiciary, independent institutions, sustainable awareness, and international cooperation, while emphasizing the need for national legislation to keep pace with technological developments, activating the role of national data protection authorities, and launching large-scale awareness campaigns.

Keywords: Right to Privacy, Technological Development, Personal Data Protection, International Charters, Digital Surveillance, Artificial Intelligence, Legislative Protection, Judicial Protection, Digital Awareness.