الحق فى الخصوصية الرقمية فى إطار ثورة البيانات وأنماط التدخلات التشريعية والدولية

د. محمد سعد إبراهيم

أستاذ الصحافة – جامعة المنيا
عميد المعهد الدولى العالى للإعلام بالشروق

مقدمة:

فى إطار ثورة البيانات، وإنترنت الأشياء، وتقنيات الذكاء الإصطناعي، أصبحت الحياة الخاصة للبشر بيئة مباحة للأفراد، ومزودى الخدمة، وشركات الإنترنت والإتصالات العملاقة، والشركات عابرة القارات، والحكومات وأجهزتها المخابراتيه والمعلوماتية، ومن ثم راجت عمليات التجسس الجماعي، وتبادل البيانات وتسويقها، والإنتهاكات الشخصية والإجتماعية والمهنية والتجارية والسياسية للخصوصية الرقمية.

وعلى الرغم من تعدد التشريعات والمواثيق الدولية، والهيئات المعنية بحماية سرية البيانات، وتحذيرات تقارير الشفافية من استباحة الخصوصية، لا يزال الحق فى الخصوصية الرقمية، مجرد حق وشعار غير قابل للإحترام والحماية، شأنه فى ذلك

شأن العديد من القضايا والحقوق الدولية المهدرة والمستباحة، فى نظام دولى يفتقر الى ادنى قواعد الشفافية والعدالة والأنصاف، ولا يتورع فى رفع الشعارات البراقه، وفى الوقت نفسه تتواصل عمليات انتهاك الحقوق والحريات والكرامة الإنسانية، بل ووصلت لحد الاتجار بصحة مليارات البشر.

وفى إطار ما تسمى بثورة البيانات، والبنية التحتية للبيانات، وعمليات المراقبة الشاملة اليومية لأفكار واهتمامات وتفاعلات الأشخاص والمنظمات والقوى والمناطق، تثار العديد من المخاوف والأشكاليات القانونية والأخلاقية والسياسية والإجتماعية، ويصبح من قبيل العبث المطالبة بسن تشريعات جديدة تجعل الأفراد والمجتمعات أكثر أمناً وأماناً وشفافية ومساءلة.

وفى إطار توسيع البيانات الصغيرة داخل البنية التحتية للمعلومات، وإنشاء سوق البيانات الضخمة، وفتح البيانات المؤسسية، وتدفقات البيانات الكبيرة، انتهكت خصوصيات الأفراد فى سوق المصالح السياسية والإقتصادية، وأصبحت المقايضات مقبولة إلى حد ما، حيث يحصل المواطنون على الأمن والأمان مقابل خصوصيتهم، وبعبارة أخرى فأن ثمن الحصول على الأمان من الهجمات الإرهابية هو المراقبة التى تنتهك خصوصيات الأفراد.

وكما تقايض الحكومات مواطنيها بالأمن مقابل الخصوصية، تقابض الشركات عملائها بالخصومات مقابل بياناتهم، حيث يمنحون بطاقات الولاء والخصومات لتؤمن تلك البطاقات قدراً هائلاً من البيانات، يتم استخدامها من أجل بيع المزيد من البضائع وجنى المزيد من الأرباح.

أهداف الدراسة:

تسعى الدراسة لتحقيق الأهداف التالية:

١- تأصيل مفهوم الحق فى الخصوصية الرقمية فى إطار ثورة البيانات والقصور التشريعى وإباحة النفاذ إلى المعلومات واستخدامها.

٢- رصد وتحليل الانتهاكات الشخصية والإجتماعية والمهنية والسياسية والتجارية للخصوصية الرقمية.

٣- رصد وتحليل أنماط التدخل التشريعى لتعزيز وحماية الحق فى الخصوصية الرقمية.

٤- رصد وتحليل الضمانات والمعايير لتحويل الحماية الإفتراضية إلى حماية فعلية.

الخصوصية (privacy):

الخصوصية هى حالة يتوقعها ويقدرها الكثيرمن الناس، وهى تعد حقاً من حقوق الإنسان الأساسية، وهى من الحقوق المقدسة فى الكثير من القوانين الوطنية والدولية والخصوصية مصطلح متعدد الأبعاد فيما يتعلق بمعناه، وهو يستخدم فى غالب الأحيان فى طرق معتمدة على السياق، ولكن على وجه العموم هو يشير إلى الممارسات المقبولة فيما يتعلق بالوصول إلى والإفصاح عن المعلومات الشخصية والحساسة، ومن الوسائل المستخدمة فى إيضاح الأبعاد المتعددة للخصوصية دراسة الوسائل العديدة التى يمكن من خلالها انتهاك الخصوصية والأضرار المرتبطة بهذه الانتهاكات.

فالذى يتضح لنا من خلال هذا التصنيف هو أن انتهاك الخصوصية يمكن أن يكون له العديد من التأثيرات على الرفاهية الجسدية والعاطفية للأفراد، ويجعل هؤلاء الأفراد عرضةً للأنشطة المضرة التى يقوم بها الآخرون، ويجعلهم كذلك عرضة لإختلال توازن السلطات غير المتماثل.(١)

الخصوصية الرقمية:

تعرف "الخصوصية الرقمية" بأنها وصف لحماية البيانات الشخصية للفرد، والتى يتم نشرها وتداولها من خلال وسائط رقمية، وتتمثل البيانات الشخصية فى البريد الإلكتروني، والحسابات البنكية، والصور الشخصية، ومعلومات عن العمل والمسكن، وكل البيانات التى نستخدمها فى تفاعلنا على الإنترنت أثناء استخدامنا للحاسب الآلى أو التليفون المحمول أو أى من وسائل الإتصال الرقمى بالشبكة العنكبوتية.

يقول المحقق الأمريكى ستيف رامبام "الخصوصية ماتت... وعلينا دفنها" واضعاً كل ما يحكى عن إجراءات تقنية وقانونية لحماية حياتنا الشخصية على الشبكة الإلكترونية فى حالة الأساطير، وذلك على خلفية الدعوى القضائية التى رفعتها إحدى المنظمات الحقوقية الأمريكية ضد شركة "غوغل" العملاقة، بعدما تبين خاصية – باز (Buzz) التى أضافتها الشركة على خدمات التواصل الإجتماعي، قد نقلت كل عناوين البريد الإلكترونى الخاصة بمستخدمى خدمة "جى مايل" إلى الشبكة الإلكترونية، مما جعلها متاحة لكل الأعضاء من دون استئذان أصحابها، ولعل هذه الانتهاكات قد تصل حد التسلل إلى ملفاتنا الشخصية.(٢)

الأمان الرقمي

المقصود بالأمان الرقمى هو كيفية استخدام شبكة الإنترنت استخدام فعال، بدون التعرض لأى تهديدات أو مخاطر أو مراقبة تهدد خصوصية وسرية المعلومات.

وفى إطار ثورة التكنولوجيا والمعلومات والتطور المتسارع للتقنيات الرقمية، وبعد أن أصبح أكثر من نصف سكان العالم مستخدمون نشطون للإنترنت ومواقع التواصل الإجتماعي، وأصبحت وسائل التواصل الإجتماعى هى الطريقة الأسهل للتواصل بين الأفراد والمجموعات وتبادل المعلومات، سواء على الصعيد المهنى أو الإنساني، أصبح النشاط الرقمى يحتك بالحريات والحق فى الخصوصية والأمان فى مقابل رغبة

الدول فى السيطرة على الفضاء الرقمى والتجسس على مواطنيها أو التحكم فى نشاطاتهم أو على صعيد آخر المراقبة المخابراتية لرصد نشاط بعض الأفراد أو اختراق حساباتهم، وربما تكون عمليات تهديد السلامة من أفراد وعصابات للوصول إلى معلومات تهدد صاحبها ويمكن استغلالها.(٣)

فى ظل كل تلك الفوضى والإتاحة وصراعات القوى والأنظمة الموضوعة لحماية مع الحقوق والحريات الإنسانية، نشأ مفهوم الأمن الرقمى لحماية الأفراد والجماعات والمنظمات من التهديدات والمخاطر التى قد يواجهونها عند استخدام شبكة الإنترنت.

معايير ضمان المعلومات

هناك ثلاثة معايير أساسية اتفق عليها الخبراء منذ البداية لضمان المعلومات ويشار إليها بمثلث أو ثلاثى CIA وهى السرية والأمانة والتوافر.

ويقصد بالسرية عدم كشف المعلومات لغير أطرافها بما يوفر الخصوصية والسرية للمعلومات المتداولة على الفضاء الرقمي، وتعنى الأمانة عدم التلاعب بالمعلومات أو حذفها أو تعديلها بحيث يضمن المستخدم دقة نقل ما يريد من معلومات دون تدخل فى أثناء النقل أو التخزين أو المعالجة، أما فيما يخص التوافر فهو استمرار توفر المعلومة للشخص أو الجهة التى يسمح لها المستخدم بالإطلاع عليها عند الحاجة.

ودائماً ما يهتم المطورون والعاملون فى مجال الأمن الرقمى والأمن المعلوماتى على ضمان العناصر الثلاثة بشكل أساسى من خلال وسائل تقنية وإجرائية تناسب المستخدمين وتوفر لهم الحماية.(٤)

وقد توسع استخدام الحكومات للتجسس على مواطنيها أو حتى مواطنين دول أخري، مع التطور التقنى الذى مر به العالم، وذلك طبقاً للظروف التى تمر بها هذه الدول وخاصة السياسية منها، فإن كنت تعيش فى غضون منتصف القرن العشرين – فيما

بعد الحرب العالمية الثانية – فإن مراسلاتك التلغرافية يتم مراقبة الصادر والوارد منها، أما إن كنت تعيش فى الفترة ما بين العقد السادس والثامن فى منتصف العقد الأخير من القرن العشرين، من القرن العشرين فإن مكالمتك التى تقوم بها من هاتفك الأرضى ستكون عرضة للتنصت، تبنت الحكومات تقنيات أكثر تطوراً لمجاراة انتشار استخدام الهاتف المحمول والإنترنت.

كان لهجمات الحادى عشر من سبتمبر – التى استهدفت برجى التجارة العالمى فى الولايات المتحدة الأمريكية – أثراً على تطور الأجهزة الأمنية لأدوات تجسس على جميع الأنشطة الإلكترونية التى تتضمن البريد الإلكتروني، وتصفح الإنترنت، والتعامل البنكى على الإنترنت بالإضافة للمحادثات الهاتفية وذلك بحجة مكافحة الإرهاب، وأما عن ضخامة التجسس فإن التفويض الذى أعطاه الرئيس الأمريكى آنذاك جورج بوش لم يتم إيقاف هذا التفويض حتى الأن (٢٠١٣) بل، بوش لوكالة الأمن القومي، والذى كان محدداً بمدة معينة لمنع أى هجمات إرهابية أخرى تم تطوير آليات أخرى للتجسس، كشف عنها إدوارد سنودن (فنى حاسب سابق بوكالة الاستخبارات الأمريكية) لصحيفة الجارديان فى يونيو ٢٠١٣، يستهدف جمع بيانات جميع مستخدمى خدمات الإنترنت لشركات PRISM برنامج الرقابة المعروف ب Google , Apple , Facebook , Microsoft , yahoo , AOL, PalTalk فى جميع أنحاء العالم من الملاحظ أن هذه الشركات هى الأكثر انتشاراً بين جميع مستخدمى الإنترنت وذلك لتقديمها خدمات متنوعة تلقى اهتمام من العديد من مستخدمى الإنترنت.(٥)

جدول رقم (١) يوضح شركات الإنترنت التى خضعت لبرنـــامج الرقابـــة بالإضـــافة للخدمات التى تقوم بتقديمها، بعض الخانات تحتوى على اسم الخدمة المقدمـــة فـــى حين اكتفيت بوضع علامة (✓) والتى تدل على تقديم هذه الشركة للخدمة مع عدم وجود تسمية لها

مقدم الخدمة	APPLE	Microsoft	facebook	yahoo	AOL	PalTalk	google
البريد الإلكتروني	Icloud	Hotmail (outlook)		Yahoo Mail	AOL Mail		Gmail
متصفح الإنترنت	safari	Internet Explorer					Chrome
التواصل الإجتماعي			✓		About.me		Google+
نظام التشغيل	ios	windows					Android
المحادثة الصوتية والمرئية	iMessage/ iChat	Skype / live Messenger		Yahoo Messenger	AIM	PalTalk Messenger	Hangout (Gtalk)
مشاركات الفيديو/ الصور							Youtube
تخزين الملفات	Apple store	Sky drive					Google Drive

وقد استخدمت عملية التجسس على الأفراد محورين للعمل، الأول عن طريق جمع بيانات ضخمة عن الحياة اليومية لمستخدمى الخدمات الموضحة فى الجدول السابق – سواء كانوا أفراد أو شركات – ويتم بتحليل هذه البيانات والتى تساعد على تحديد اهتماماتهم وتوجهاتهم السياسية بناء على مشاركاتهم أو الصفحات التى يستخدموها أو عمليات البحث التى يقومون بها، ومن الجدول السابق نكتشف حجم البيانات التى يمكن أن يتم جمعها عن المستخدمين، فعلى الأقل معظمنا يقوم يومياً بفحص البريد الإلكترونى بجانب أحد مواقع التواصل الإجتماعى مثل "فيسبوك"، يقوم المحور الآخر

على متابعة أفراد بعينهم معروف مسبقاً عن أنشطتهم ويتم استهدافهم ومتابعتهم ، وقد كشفت تقارير الشفافية التى أصدرتها بعض الشركات الموجودة فى الجدول السابق عن طلبات من العديد من الحكومات منها مصر والولايات المتحدة، طالبت بها الحكومات بتسليم بيانات بعض المستخدمين.

الإتجاهات الدولية لتعزيز ودعم الأمان الرقمي

إن الحديث عن العالم الرقمي، الذى أصبح ملتقى التجمع والوجود الإفتراضى العالمي، هو حديث عن مجمل منظومة الحقوق الإنسانية بنقل تطبيقها على الواقع الطبيعى إلى تطبيقها على الفضاء على الفضاء الرقمي، وبالتالى تخضع معايير الأمن الرقمى لحق الإنسان الأصيل فى الخصوصية وحرية الرأى والتعبير وحرية التنظيم وحرية اعتناق أراء أو عقائد معينة وبعبارة أكثر وضوحاً "كل ما يخضع لمنظومة حماية حقوق الإنسان على الأرض، يخضع لنفس المنظومة على شبكة الإنترنت".

وفى هذا الإطار، تتعدد المواثيق الدولية التى تسعى لتعزيز وحماية الأمن القومي:

- **ميثاق حقوق الإنترنت لجمعية الإتصالات المتقدمة (APC)**[٦]

تم وضع ميثاق حقوق الإنترنت على يد جمعية الإتصالات المتقدمة، فى ورشة عمل حقوق شبكة الإنترنت فى جمعية الإتصالات المتقدمة بأوروبا، والتى تم عقدها فى براغ فى فبراير عام ٢٠٠١، وهذا الميثاق يقوم على ميثاق الإتصالات الشعبي، وهو يهدف إلى تطوير سبع أفكار رئيسية، هي: الوصول إلى الإنترنت للجميع، وحرية التعبير، وحرية التنظيم، والوصول إلى المعارف، والتعليم المشترك والتأليف – البرمجيات مفتوحة المصدر المجانية وتطوير التقنيات، والخصوصية والمراقبة والتشفير، وحوكمة الإنترنت، وحماية الوعى وإعمال الحقوق.

- **قرار الجمعية العمومية للأمم المتحدة بشأن حماية الحق فى الخصوصية الرقمية** (٧)

عندما أصبحت مناقشة الحقوق الرقمية تحتاج إلى تركيز خاص ومساحات مباشرة وليس ربط بحزمة الحقوق الإنسانية الأصيلة التى تم إقرارها دولياً، جاء قرار الجمعية العامة للأمم المتحدة رقم (١٦٦/٦٩) بشأن الحق فى الخصوصية فى العصر الرقمى والذى جاء نصه:

"إن الجمعية العامة، إذ تؤكد من جديد مقاصد ميثاق الأمم المتحدة ومبادئه، وإذ تؤكد من جديد أيضاً حقوق الإنسان والحريات الأساسية بصيغتها المكرسة فى الإعلان العالمى لحقوق الإنسان ومعاهدات حقوق الإنسان الدولية ذات الصلة، بما فى ذلك العهد الدولى الخاص بالحقوق المدنية والسياسية والعهد الدولى الخاص بالحقوق الإقتصادية والإجتماعية والثقافية، وإذ تؤكد من جديد كذلك إعلان وبرنامج عمل فيينا، وإذ تشير إلى قرارها (١٦٧/٦٨) المؤرخ ١٨ كانون الأول / ديسمبر٢٠١٣ بشأن الحق فى الخصوصية فى العصر الرقمي. وإذ ترحب بإتخاذ مجلس حقوق الإنسان القرار (١٣/٢٦) المؤرخ ٢٦ حزيران/يونيه ٢٠١٤. بشأن تعزيز وحماية حقوق الإنسان على الإنترنت والتمتع بها، وإذ ترحب أيضاً بعمل مفوضية الأمم المتحدة لحقوق الإنسان بشأن الحق فى الخصوصية فى العصر الرقمى وإذ تلاحظ مع الإهتمام تقريرها عن هذا الموضوع، وإذ تشير إلى حلقة النقاش بشأن الحق فى الخصوصية فى العصر الرقمى المعقودة خلال الدورة السابعة والعشرين لمجلس حقوق الإنسان، وإذ تلاحظ تقرير المقرر الخاص لمجلس حقوق الإنسان المعنى بتعزيز وحماية حقوق الإنسان والحريات الأساسية فى سياق مكافحة الإرهاب وتقرير المقرر الخاص للمجلس المعنى بتعزيز وحماية الحق فى حرية الرأى والتعبير، وإذ تلاحظ مع التقدير التعليق العام رقم (١٦) الصادر عن اللجنة المعنية بحقوق الإنسان بشأن حق الشخص فى أن تحترم

خصوصياته وشؤون أسرته وبيته ومراسلاته وفى التمتع بالحماية اللازمة لشرفه وسمعته، وإذ تلاحظ أيضاً فى الوقت نفسه القفزات التكنولوجية الواسعة التى حصلت منذ اعتماد التعليق، وإذ تسلم بالحاجة إلى مواصلة القيام، استناداً إلى القانون الدولى لحقوق الإنسان بمناقشة وتحليل المسائل المتصلة بتعزيز وحماية الحق فى الخصوصية فى العصر الرقمي، والضمانات الإجرائية والرقابة وسبل الانتصاف المحلية الفعالة، وأثر المراقبة على الحق فى الخصوصية وغيره من حقوق الإنسان، والحاجة إلى دراسة مبادئ عدم التعسف والمشروعية، وجدوى تقييمات الضرورة والتناسب فيما يتعلق بممارسات المراقبة.

وإذ تلاحظ الاجتماع العالمى لأصحاب المصلحة المتعددين بشأن مستقبل إدارة الإنترنت المعقود فى ساو باولو، البرازيل، فى نيسان/أبريل ٢٠١٤، وإذ تسلم بأن حقوق الإنسان على النحو المجسد فى الإعلان العالمى لحقوق الإنسان والعهد الدولى الخاص بالحقوق الإقتصادية والإجتماعية والثقافية والعهد الدولى الخاص بالحقوق المدنية والسياسية واتفاقية القضاء على جميع أشكال التمييز ضد المرأة.

- **القمة العالمية حول مجتمع المعلومات (wsis) ٢٠٠٣ :-** [٨]

فى ديسمبر عام ٢٠٠٣، تم عقد القمة العالمية حول مجتمع المعلومات (wsis) تحت رعاية الأمم المتحدة . وبعد مفاوضات طويلة بين الحكومات والشركات وممثلى المجتمع المدنى ، تم إعلان مباديء القمة العالمية حول مجتمع المعلومات ، والذى يعيد التأكيد على حقوق الإنسان :

" إننا نعيد تأكيدنا على شمولية كل حقوق الإنسان والحريات الأساسية وعدم تجزئتها والترابط بينها ، بما فى ذلك حق التطوير على النحو الموضح فى إعلان فيينا . كما أننا نعيد تأكيدنا كذلك على أن الديمقراطية والتطوير المستدام واحترام حقوق الإنسان والحريات الأساسية بالإضافة إلى الحكومة الرشيدة على كل المستويات هى عوامل

مترابطة ويقوى بعضها بعضا . كما أننا نعقد العزم كذلك على تقوية سيادة القانون فى الشئون الدولية وكذلك الشئون القومية ".

كما يشير إعلان القمة العالمية حول مجتمع المعلومات بشكل خاص إلى أهمية حق حرية التعبير فى مجتمع المعلومات ":

" نحن نؤكد مجدداً على أن للجميع الحق فى حرية الرأى والتعبير ، كأساس ضرورى لمجتمع المعلومات ، وكما هو موضح فى البند (١٩) من الإعلان العالمى لحقوق الإنسان ، وأن هذا الحق يشتمل على الحرية فى تبنى الآراء بدون تدخل ، بالإضافة إلى الحق فى البحث عن المعلومات والأفكار وتلقيها ونقلها عبر أية وسيط بغض النظر عن الحدود . ويعد الاتصال عملية اجتماعية جوهرية ، وحاجة بشرية أساسية ، كما أنها تعد بمثابة الأساس لكل المنظمات الاجتماعية . وهو أمر مركزى فى مجتمع المعلومات . ويجب أن تتاح الفرصة للجميع فى كل مكان للمشاركة ، ويجب ألا يتم استثناء أى شخص من الامتيازات التى يوفرها مجتمع المعلومات " .

كما أقر إعلان مبادىء القمة العالمية حول مجتمع المعلومات كذلك " بأنه من الضرورى منع استخدام موارد وتقنيات المعلومات للأغراض الجنائية والإرهابية مع احترام حقوق الإنسان".

وتوفر ١٣٠ دولة حماية دستورية للحق فى الخصوصية وهناك مائة دولة لديها تشريعات خاصة بحماية البيانات علاوة على وجود (١٢) مادة فى المواثيق الدولية تتعلق بحماية الخصوصية وسرية البيانات وحرية الانترنت هى [٩]

- المادة (١٢) من الإعلان العالمى لحقوق الانسان لعام ١٩٤٨ .
- المادة (١٧) من الميثاق الدولى للحقوق المدنية والسياسية لعام ١٩٦٦.
- المادة (١٤) من ميثاق الامم المتحدة لحقوق العمال المهاجرين .
- المادة (١٠) من الميثاق الافريقى لحقوق الطفل .

- المادة (١٤) من مبادىء الاتحاد الافريقى لحرية التعبير.
- المادة (١٦) و(٢١) من الميثاق العربى لحقوق الانسان .
- المادة (١٦) من الميثاق العالمى لحقوق الطفل .
- المادة (١٨) من ميثاق حماية حقوق الانسان والحريات الانسانية.
- قرار الجمعية العامة للامم المتحدة حول ملفات البيانات الشخصية المؤتمنة.
- قرارات اللجنة الوزارية للاتحاد الاوربي.
- إرشادات منظمة التعاون الاقتصادى والتنموى حول السياسة والممارسة فيما يتعلق بالخصوصية على الانترنت .
- إرشادات منظمة التعاون الدولى والتنموى حول تطبيق القانون فيما يتعلق بالخصوصية عبر الحدود
- ارشادات منظمة التعاون الاقتصادى والتنمولى حول أنظمة المعلومات والشبكات : نحو ثقافة الأمن ٢٠٠٢ .
- المادة الثامنة من إعلان القاهرة حول حقوق الانسان فى الاسلام لعام ١٩٩٠ .
- المادة (٣٠٤) من الإعلان والمباديء الخاصة بحرية التعبير فى أفريقيا لعام ٢٠٠٢.
- المادة (٥) من الإعلان الامريكى حول حقوق وواجبات الانسان .

ويلاحظ أن الدساتير الحديثة لبعض الدول مثل جنوب أفريقيا وهنغاريا تتضمن مواداً خاصة تتعلق بخصوصية البيانات الشخصية والوصول اليها والتحكم بها .

وعلى الرغم من حرص كثير من الدول على تعديل تشريعاتها لمواكبة العصر الرقمى الا ان المراقبة الشاملة للبيانات تفوق بكثير الحماية الدستورية والقانونية للحق فى الخصوصية.

وإذا كانت تلك المواثيق الدولية تضفى الشرعية الدولية على الحق فى الخصوصية الرقمية، وتوفر إطار أخلاقياً دولياً لمراقبة عمليات التجسس والمراقبة والتصيد، فأنها لا توفر حماية دولية حقيقية وفاعلة فى غياب تفعيل القانون الدولى لحقوق الإنسان، وتجاهل شركات الإنترنت والإتصالات العملاقة لتقارير الشفافية والدعاوى القضائية للمنظمات الحقوقية الدولية.

أنماط التدخل التشريعى لحماية الخصوصية الرقمية:

نظراً لحداثة موضوع الخصوصية الرقمية تختلف الأطر التشريعية من دولة لأخرى طبقاً للمستجدات التى مرت بها كل دولة، وفلسفتها التشريعية، وكيفية تطبيقها للقوانين والتحولات التى يمر بها المجتمع، ومقدرة كل دولة على تبنى تعديل لقوانيها بناء على قضايا جديدة تكون خارج اطارها التشريعي.

تهتم قوانين الخصوصية بحماية وسائط نقل المعلومات إما عبر الإنترنت أو الهواتف أو حتى البريد، كما تتضمن الحفاظ على سرية المعلومات الخاصة للأفراد الموجودة فى سجلاتهم مثل المعلومات المالية أو الصحية، كما يجب أن تضمن بياناتهم الخاصة التى يتم تداولها من خلال التصفح والتواصل على الإنترنت.

و تختلف أنواع القوانين المتعلقة بالخصوصية فى الفضاء الرقمى فهى تتراوح بين حماية البريد الإلكتروني، وفرض قيود على نشر بيانات التواصل الإجتماعي، ومتابعة نشاط متصفح الإنترنت والمخالفات للبيانات المحفوظة، وفيما يلى الأنواع المختلفة لقوانين الخصوصية الرقمية:(١٠)

- **قانون حماية البيانات:** تفرض على الشركات المقدمة لخدمات الإنترنت والتى تقوم بتخزين معلومات رقمية لعملائها من نشر هذه المعلومات أو مشاركتها مع أطراف أخرى دون إفادة من العميل.

- **قانون مراقبة الإتصالات:** تقيد مراقبة وسائل الإتصال بالإنترنت، والتى تكون فى مجال العمل أو الموجودة فى الأماكن العامة أو حتى المنزل.
- **قانون الحماية من جرائم الإنترنت:** تمنع الاستيلاء على الهوية أو سرقة البريد الإلكترونى وكل ما يخص حماية البيانات الشخصية التى يشاركها الفرد أثناء استخدامه للإنترنت.

ولقد ساهمت الدول الأعضاء بالاتحاد الأوروبى فى تشريع قوانينها الخاصة لحماية الخصوصية الرقمية فى إطار بعض المعايير التى تضمنتها الإتفاقية الأوروبية لحقوق الإنسان والتى نصت فى المادة الثامنة الخاصة بأنه:

١- من حق أى شخص أن يحصل على احترام لحياته الشخصية والعائلية بالإضافة لمنزله ومراسلاته.

٢- لا يحق للدولة التدخل فى هذا الحق إلا بموجب القانون وما تمليه الضرورة فى المجتمع الديمقراطي، وما يمس الأمن القومى أو السلامة العامة أو الإقتصادية للبلاد أو لمنع الفوضى وما قد يضر الصحة والأداب العامة أو لحماية حقوق وحريات الآخرين.(١١)

وقد أدى ذلك لتوسع مفهوم الخصوصية بالرغم من اختلافات تطبيق القانون من دولة لأخري، فنجد لدى كل من أسبانيا وألمانيا أشد القوانين حزماً، فى حين أن أسبانيا أكثر الدول الأوروبية التى تسجل شكاوى ضد انتهاك حماية البيانات والأكثر تحصيلاً لغرامات ضد انتهاكات البيانات الشخصية.

أما عن دول القارة الأسيوية، فقد قامت سنغافورة فى عام ٢٠١٢ بتشريع قانون لحماية البيانات الشخصية يمنح حماية مدتها عشر سنوات بعد وفاة الشخص، كما يعتبر قانون كوريا الجنوبية من أفضل التشريعات فى آسيا حيث نصت أحد البنود القانون على حماية صورة وصوت الفرد.(١٢)

أما بالنسبة للولايات المتحدة الأمريكية فإن قوانين الخصوصية بها غير مكتملة وتعانى من فقر تشريعي، فهناك قوانين تغطى البيانات المالية مثل الحسابات البنكية والعناوين، وآخر خاص بالرعاية الصحية، كما يوجد لديها أيضاً تشريع يلزم المواقع التى تقوم بجمع معلومات عن الأطفال تحت سن ١٣ سنة بوضع سياسة خصوصية عن كيفية التحقق من موافقة الوالدين أو المسئول عن الطفل عند نشر الأطفال لبياناتهم و المتاجر الأمريكية لها سياسة ذاتية لحماية عملائها لكن المقاضاة فى حالة الإنتهاك لن يقابلها أى عقوبة قانونية والمستهلك لن يجد حلاً إلا بعدم الشراء من المتجر.(١٣)

تبنت بعض المؤسسات الأمريكية صياغة مشاريع قوانين للخصوصية الرقمية طبقاً للتطورات التى تمر بها الخصوصية الرقمية، ففى عام ٢٠١٠ تم تقديم مشروع قانون يكشف عن أحقية المستهلكين فى منع المواقع الإلكترونية من متابعة سلوكهم من خلال لجنة التجارة الفيدرالية الأمريكية التى تعتبر النقطة المحورية فى مشروع هذا القانون حيث يقيد برامج تصفح الإنترنت بإدراج وظيفة لعدم التتبع، كما يقترح بأن تكشف الإنترنت الكيانات التجارية عن الوضع الحالى للبيانات الشخصية التى قامت بجمعها ومع من قامت بمشاركتها.

وتتطرق بعض القوانين الفيدرالية الأمريكية ومنها قانون التأمين الصحي، وقانون المحاسبة لعام ١٩٦٦ الذى يتعلق بالبيانات الصحيحة، وقانون حماية خصوصية الأطفال على الإنترنت إلى حماية البيانات الشخصية للأفراد، وتمتلك بعض الولايات قوانين أكثر جرامة فيما يتعلق بالخصوصية منها قانون حماية الخصوصية فى ولاية كاليفورنيا الذى يفرض على مواقع الإنترنت حتى لو كانت خارج الولاية طالما كانت تستخدم من قبل مواطنيها بوجوب وضع سياسة للخصوصية وعلى أن تتضمن هذه السياسة ما يلي:

- نوع البيانات الشخصية التى يتم جمعها.

- الأطراف الأخرى التى تتم مشاركة البيانات معها.
- كيف يمكن للمستخدم مراجعة وتعديل بياناته التى تم جمعها.
- كيف يتم إعلان المستخدمين بالتغيرات التى تطرأ على سياسة الخصوصية.
- تاريخ دخول السياسة ضد التنفيذ.

وفى يناير ٢٠١٢ اقترحت المفوضية الأوربية تشريعاً لحماية البيانات والذى يجعل من حق الفرد أن يطلب من مقدمى خدمات الإنترنت بمسح بياناته الشخصية التى يمكن أن تظهر فى محركات البحث وسمى التشريع ب Right to Be Forgotten، ويحاول القانون المقترح السماح للمستخدمين أن يطالبوا شركات مثل تويتر وفيسبوك بحذف بياناتهم الخاصة وكذلك جوجل بأن تمنع ظهور هذه البيانات فى محركات البحث لديها.

وفى الدنمارك تم إقرار قانون معالجة البيانات الشخصية عام ٢٠٠٠ وتقوم وكالة حماية البيانات بالإشراف على تطبيق قوانين الخصوصية، وتمتلك الوكالة صلاحيات إصدار تنبيه أو منع بحق المخالفين، أو إعلام الشرطة الشخصية فى حالة موافقة الشخص فقط، ولا يحق للشركة أن تشارك المعلومات مع طرف ثالث دون موافقة الشخص.

وفى العديد من دول أمريكا اللاتينيه، تم تشريع قوانين لحماية الخصوصية، استرشاداً بتجربة الإتحاد الأوروبى وذلك سعياً لفتح السوق التجارية معها، حيث قامت الأرجنتين فى عام ٢٠٠٠ بوضع قانون جديد وفق معايير الإتحاد الأوروبي.

وفى كندا، ينظم قانون حماية المعلومات والبيانات الإلكترونية كيفية جمع وتخزين واستخدام المعلومات من المستخدمين كما يوجد مفوض خاص للخصوصية مسئوليته متابعة تنفيذ القانون.

نخلص مما سبق إلى أنه هناك ثلاثة أنماط للتدخل التشريعى لتعزيز الخصوصية الرقمية وحماية البيانات هي:

أولاً: النموذج التشريعى الشامل الذى يتبناه الإتحاد الأوروبى وكندا، حيث قام الإتحاد الأوروبى بإصدار مرسوماً يضمن لمواطنيه الحق فى حماية أوسع لبياناتهم المرسوم هو المعيار لوضع تشريعات محلية فى دول الإتحاد.

ووفق النموذج التشريعى الشامل، تنشئ الدولة منصباً خاصاً بموظف كبير مسئول عن الخصوصية وتطبيق القوانين التى تحميها، ويسمى عادة مفتش أو مفوض أو مسئول الخصوصية ويختص بالتحقيق فى الإنتهاكات وإدارة العلاقات مع الدول الأخرى فيما يتعلق بالموضوع.

ثانياً: النموذج التشريعى القطاعى كما هو الحال فى الولايات المتحدة الأمريكية، حيث تصدر الولايات قوانين تنظم الخصوصية فى قطاعات معينة مثل الخصوصية المصرفية، وخصوصية البيانات الصحية، وحماية بيانات الأطفال، ولكن لا يوجد إطار قانونى شامل لحماية الحق فى الخصوصية الأمر الذى يترك ثغرات عديدة لا تستطيع تلك القوانين الجزئية سدها.

ثالثاُ: نموذج التشريعات العامة وهو النموذج السائد فى معظم الدول ويتمثل فى قوانين الحماية من جرائم الإنترنت أو حماية البيانات أو قوانين الصحافة والعقوبات.

المبادئ السبعة العالمية للخصوصية الرقمية:

إن تشريعات الخصوصية الرقمية مبنية حول الحقوق الشخصية، والموافقة المتعلقة بإنشاء واستخدام والإفصاح عن البيانات الشخصية، وهى تتكون من سبعة مبادئ عالمية للخصوصية، وفى إطارهذه المبادئ فإن الأفراد، من الناحية النظرية، يتم منحهم الحق للتحكم فى بياناتهم الشخصية ومنح موافقتهم للآخرين فيما يتعلق بهذه البيانات، وعلاوة على ذلك، فإنه يتعين على مقتنيى البيانات الالتزام بقوانين حماية البيانات التى تقيد الإفصاح عن المعلومات الشخصية المعرفة (Personally Identifiable Information-PLL)، والمعلومات الحساسة، والبيانات الأخرى التى يمكن استخدامها للاستدلال على الشخصية، وتؤيد تقليص البيانات بحيث يقتصر إنشاء

البيانات الضرورية لتحقيق غرض معين، وعلى وجه العموم، فإن الحل لاشتراطات المعلومات الشخصية المعرفة (PLL) هو استخدام أساليب إخفاء الهوية مثل عدم تحديد الهوية (إخفاء المعلومات الشخصية المعرفة)، والأسماء المستعارة، والتجميع، بالإضافة إلى التشفير، والتخزين الآمن، والقيود الخاصة بالوصول إلى المعلومات.[١٥]

جدول رقم (٢) يوضح المبادئ السبعة الأساسية للخصوصية من خلال التصميم

المبدأ	الوصف
استباقية وليست تفاعلية: الوقاية وليس العلاج	ينبغى أن تسعى نظم تكنولوجيا المعلومات لتوقع الخصوصية تحديد المخاوف المتعلقة بالخصوصية وتجنبها بدلاً من السعى إلى حل المشاكل الناتجة عن مخالفات الخصوصية بعد حدوثها
الخصوصية هى الوضع الافتراضي	الخصوصية محمية تلقائياً ولا تتطلب أى عمل من جانب الأفراد
الخصوصية مدمجة فى التصميم	حماية الخصوصية هى سمة أساسية للتصميم والهندسة الهيكلية لأنظمة تقنية المعلومات وليست ميزة إضافية متدنية الأهمية
الفعالية الكاملة – عائد إيجابى وليس محصلة صفرية	جميع المصالح والأهداف المشروعة يتم استيعابها، بدلا من أن يكون هناك مقايضات بين الخصوصية واعتبارات أخرى مثل الأمن
الأمن من النهاية للنهاية – حماية كاملة طوال دورة حياة النظام	تكون الخصوصية جزءاً لا يتجزأ من النظام من بداية إطلاقه إلى حين التخلص منه
الوضوح والشفافية – فلتكن مفتوحة على الدوام	تكون جميع الأجزاء المكونة للنظام وعملياته واضحة وشفافة للمستخدمين والشركات الموفرة على السواء وتخضع لتدقيق مستقل
احترام خصوصية المستخدم - أى جعلها تتمحور حول المستخدم	يجب أن يبنى النظام حول الأفراد، وأن يحمى مصالحهم، وأن يكون ممكناً لهم

- المصدر : (Cavoukian 2009) [١٦]

جدول رقم (٣) يوضح مبادئ الممارسة العادلة للمعلومات

المبدأ	الوصف
الإخطار (Notice)	يتم إخطار الأفراد بأن بياناتهم يتم إنشاؤها ويتم إعلامهم بالغرض الذى سيتم استخدام هذه البيانات فيه.
الإختيار (choice)	يتمتع الأفراد بحرية اختيار المشاركة أو يؤثرون عدم المشاركة وذلك فيما يتعلق بما إذا كانوا يرغبون فى استخدام بياناتهم أو الإفصاح عنها وكيفية القيام بذلك.
الموافقة (consent)	يتم إنشاء البيانات والإفصاح عنها فحسب بعد موافقة الأفراد المعنيين.
الأمن (security)	يتم حماية البيانات من الفقد، وإساءة الإستخدام، والوصول غير المصرح به، والإفصاح عنها، وتعديلها أو تدميرها.
التكامل (Integrity)	تكون البيانات موثوقة ودقيقة وكاملة وحالية.
الوصول (Access)	يمكن للأفراد الوصول إلى بياناتهم الشخصية والتحقق منها والتثبت منها.
المساءلة (Accountability)	يكون مقتنى البيانات مسئولاً عن ضمان تحقق المبادئ السابق ذكرها وأن يكون لديه الوسائل اللازمة من أجل ضمان الإلتزام بهذه المبادئ.

و تجدر الإشارة إلى وجود العديد من المشاكل الإدراكية والبنيوية المرتبطة بتشريعات الخصوصية الحالية، حيث تحاول الدول بصورة روتينية التحايل على قوانين الخصوصية، وذلك من أجل أغراض الأمن وجمع المعلومات الإستخباراتية، بحسب ما تم الكشف عنه مؤخراً بواسطة برامج تحليل وجمع البيانات السرية فى الولايات المتحدة الأمريكية، والمملكة المتحدة، والعديد من الحكومات الأخري، كما أن الكثير من الشركات لا تشعر بأنها مجبرة على تقديم سياسة الخصوصية، للأفراد وذلك لأن هذه الشركات تدعى أنها تجمع معلومات مجهولة المصدر، ومن ثم فهى لا تقع تحت

طائلة ممارسات المعلومات العادلة، أو ربما تقدم هذه الشركات سياسة الخصوصية، وذلك عند الاستهلال الأولى للالتزامات (على سبيل المثال، عند تثبيت برنامج ما أو الاشتراك فى خدمة ما) وتكون هذه السياسة مصاغة بلغة معقدة وغامضة، وعادة ما تشتمل على الاحتفاظ بالحق فى تعديل هذه السياسة فى وقت لاحق دون تشاور إضافى مع الشخص.(١٨)

أشكال انتهاكات الخصوصية الرقمية:

تسعى الدول والهيئات والمؤسسات والشركات بشكل فعال للحصول على البيانات المتعلقة بمواطنيها وعملائها، ومن الصعوبة بمكان أن يمارس الفرد حياته اليومية بمنجى من المراقبة والتعقب والإنتهاك فى إطار تنامى وتوحش دور التقنيات الرقمية، فحتى لو استخدمت اسم مستعار على وسائل التواصل الإجتماعي، فإنه يتم تسجيل عنوان وبروتوكول الإنترنت (IP Address) وعنوان التحكم بالوصول للوسائط (MAC Address)، ولو لم تقم بإستخدام بطاقتك الإئتمانية، فإن كاميرات المراقبة تلاحقك وتسجل نشاطك.(١٩)

وهكذا، فإن الفرد يترك آثار بياناته بشكل روتينى أينما ذهب، ومن ثم فإنه من الصعب أن يشعر بالأمن والأمان.

وطبقاً لهيئة حماية البيانات الهولندية، فإن المواطن الهولندى مندرج فى نحو ٢٥٠-٥٠٠ قاعدة بيانات فى حين ان المواطن النشط اجتماعياً وسياسياً مندرج فى نحو ألف قاعدة بيانات. (٢٠)

وتوفر قواعد البيانات عملية تعقب للبيانات الخاصة بالمواقع والتفاعلات والممارسات عبر الزمان والمكان، وتخزن النسخ الرقمية للأثار الرقمية والصور التخيلية للبيانات فى قواعد البيانات لفترة غير محدودة الأمر الذى يتيح تفتيتها وتقسيمها ونشرها عبر الكثير من المنظمات والخوادم.(٢١)

وهكذا، يمكن القول أن هناك سجلاً مفصلاً بحياة الفرد اليومية وأنماط استهلاكه وعمله وسفره واتصالاته وأفكاره واهتماماته وتفاعلاته. وأن هذه السجلات متاحة من خلال أسواق البيانات والبنى التحتيه للبيانات ومبادرات البيانات المفتوحه، وهذه المراقبة الشاملة تشمل الأفراد والمؤسسات والمنظمات والأحزاب والقوى السياسية والإجتماعية والمناطق.

لقد أصبحت عملية المراقبة للشخصيات والمنظمات والقوى والمناطق سهلة من خلال استعراض سجلات الأجهزة الرقمية كالهواتف الخلوية، وبرامج تصفح الإنترنت، وبرامج الملاحة بالأقمار الصناعية فى السيارة، علاوة على دور سماسرة البيانات الذين يبحثون دراسة تواريخ الأشخاص وسجلاتهم المالية والإجتماعية والوظيفية والجنائية.

إن طوفان البيانات مكشوفة للمراقبة والفرز والتدقيق والتتبع والتنظيم والتنبؤ والتوجيه، حيث يتم تحويل تلك الكميات الكبيرة من الأفكار والمعتقدات والإهتمامات والتفاعلات لصورة واضحة ومقروءة ونماذج واضحة للحكم على الموضوعات والقضايا وهى مكون أساسى من الأشكال الحديثة للحوكمة.[٢٢]

الأساليب المتغيرة للحوكمة:

جدول رقم (٤) يوضح تصنيف الخصوصية

النطاق	انتهاك الخصوصية	الوصف
جمع المعلومات Information collection	المراقبة	مشاهدة أو الإستماع إلي، أو تسجيل الأنشطة التى يقوم بها الشخص
	الاستجواب	الأشكال المتعددة من الإستجواب أو التقصى من أجل الحصول على المعلومات
معالجة المعلومات Information Processing	التجميع	تجميع أجزاء مختلفة من البيانات عن شخص ما
	التعريف	ربط المعلومات بأشخاص معينين
	عدم الأمان	الإهمال فى حماية المعلومات المخزنة من التسريبات والوصول إليها بطريقة غير ملائمة
	الإستخدام الثانوي	يتم استخدام المعلومات التى تم تجميعها لغرض معين فى أغراض أخرى دون الحصول على موافقة الشخص موضوع البيانات
	الاستبعاد	الإخفاق فى السماح للشخص موضوع البيانات بمعرفة البيانات التى يمتلكها الآخرون عنه والمشاركة فى معالجة واستخدام هذه البيانات، وهذا يشمل الإقصاء والمنع من التمتع بالمقدرة على الوصول إلى هذه البيانات وتصحيح الأخطاء الواردة فيها.
نشر المعلومات Information Dissemination	انتهاك السرية	إخلاف الوعد فى المحافظة على سرية بيانات الشخص
	الإفصاح	الكشف عن المعلومات عن شخص ما والتى تؤثر فى الطرق التى يحكم بها الأخرون على شخصيته
	الكشف	الكشف عن عرى أو حزن أو الوظائف الجسدية لشخص ما

نشر المعلومات Information Dissemination	زيادة إمكانية الوصول	زيادة إمكانية الوصول إلى المعلومات
	الابتزاز	التهديد بالكشف عن معلومات شخص ما
	الاستيلاء	استخدام هوية الشخص موضوع البيانات من أجل خدمة أهداف أو مصالح شخص آخر
	التشويه	نشر معلومات خاطئه أو مضللة عن شخص ما
الإنتهاك Invasiom	التطفل	الأعمال الانتهاكية التى تزعج هدوء أو انعزال شخص ما
	التدخل المتعلق بالقرارات	التدخل فى قرارات الشخص موضوع البيانات التى تتعلق بشئونه الخاصة

- المصدر: تم تجميعه من (٢٠٠٦) Solove [٢٣]

اننا نعيش فى عالم أكثر انفتاحاً وشفافية بكثير عما اعتدنا عليه سابقاً، فالمعلومات التى كانت تعد خاصة فى السابق يتم مشاركتها الآن بشكل أكثر حرية كالسير الذاتية من خلال موقع لينكد إن (LinkedIn)، والصور والفيديوهات العائلية من خلال مواقع فليكر (Flickr) وإنستجرام (Instagram) ويوتيوب (YouTube)، والقصص الشخصية والعائلية من خلال موقع فيسبوك (Facebook) والمونات، والأفكار والمعتقدات الشخصية من خلال تويتر(Twitter) وغرف الدردشة والتعليقات على الإنترنت، فما كان يتم مشاركته فى السابق مع عدد لا يتجاوز أصابع اليد الواحدة من الأشخاص كأفراد العائلة، والأصدقاء المقربين، وأرباب العمل فى المنزل أو المقهى المحلى أو مكتب للموارد البشرية يتم نشره الآن على المستوى العالمى مما يسمح لأى شخص بمشاهدته وتعديله (Minelli et al.2013).[٢٤]

وكشفت صحيفة وول ستريت جورنال (Wall Street Journal) فى اختبار أجرى على ١٠١ تطبيق للهواتف الذكية، أن ٥٦ تطبيقاً نقلت معرف الجهاز المتفرد للهاتف

إلى شركات أخرى وذلك دون معرفة المستخدم أو الحصول على موافقته، وأن ٤٧ تطبيقاً أرسلت موقع الهاتف، وأن ٥ تطبيقات أرسلت البيانات الشخصية للمستخدمين . وأن ٤٥ تطبيقاً لم يكن بها أى ارتباط مع سياسات حماية الخصوصية التى يمكن للمستخدمين مشاهدتها، كما وجدت شركة الثقة الإلكترونية (TRUSTe) أن ١٩% فقط من أعلى ٣٣٤٠ تطبيقاً مرتبطون بسياسة الخصوصية وأن متاجر شركتى أبل وجوجل يشترطان ضرورة اشتمال التطبيقات على هذه السياسة، ومع ذلك يمكن للتطبيقات أن تتبع وتنقل "عاداتك على الشبكة، وأن تبحث فى قائمة جهات الاتصال لديك، وأن تجرى مكالمات هاتفية دون أن تعرف، وأن تتبع موقعك، وأن تفحص ملفاتك، وغير ذلك الكثير".(٢٥)

إن مشهد الخصوصية الآن فى حالة تغير مستمر، وهو يخيب التوقعات القانونية والإجتماعية، وهكذا، يتضح أن مفهوم الخصوصية قد تعطل بشكل كبير ، ويرى البعض أنه من الصعوبة بمكان المحافظة على الخصوصية فى التطبيق العملي، كونها تحجب وتخفى تجربة المستخدم، وهى معوق اقتصادي، ولا يبدو أن معظم الناس يعارضون أن يتم التنقيب فى بياناتهم، وإذا لم يكن هناك شئ لتخفيه، فما المشكلة فى أن يتم معرفة بياناتك، والنسبة للبعض الآخر، فإن الخصوصية حق يتعين حمايته لأن من الحقوق التأسيسية ل"المواطنة المطلعة والمتأملة" وهو مكون أساسى أيضاً لحرية التعبير.

الخصوصية الرقمية فى التشريع المصري:

تأثرت الخصوصية الرقمية فى مصر بالفراغ التشريعى الذى يخص قضايا الإنترنت وتداول المعلومات – شأنها شأن دول كثيرة – وعدم وضوح الأطر التى تحمى الحريات الرقمية بصفة عامة والخصوصية الرقمية بصفة خاصة.

يعتقد البعض أنه طالما لم يقم بأى جريمة ولم ينتهك القانون، فإنه يتمتع بخصوصية وسرية على حياته الشخصية، ذلك أن تجسس الحكومات على الأفراد طالما تم تبريره بأنه بغرض ملاحقة المجرمين والخارجين عن القانون، وعدم وجود تشريع يحافظ على خصوصية الأفراد، سهل ذلك اتباع ممارسات التجسس بدعوى الحفاظ على الأمن القومى وحمايته.

فى مارس ٢٠١١، حصل المتظاهرون الذين قاموا بإقتحام مبنى أمن الدولة المصرى على وثائق، كان من بينها عروض أسعار لبرنامج بالرغم من أن شركة جاما صرحت بأنها لم تكن قد سلمت البرنامج أو قامت شركة جاما لجهاز أمن الدولة المصرى FinFisher بأية تدريبات عليه للجهاز، وأفادت الوثائق فى مخاطبات داخلية لجهاز أمن الدولة بأن يلتزم الجهاز بعد التصريح لأى جهة أجنبية أو محلية بإستخدامهم للبرنامج.

ووفقاً للمدير العام لمجموعة جاما – المنتجة لهذا البرنامج – فإن مثل هذه الحلول Skype التى تقدمها الشركة للحكومات هى فقط من أجل مراقبة الإرهابين والتنظيمات الإجرامية التى تهدد المجتمع، إلا أنه من تحليل الظروف التى تمر بها الدول التى قامت بإستخدام هذه التقنيات فقد وجد أنها دول تعانى من تأزم سياسى وترتيب متدنى فى الحفاظ على حقوق الإنسان.(٢٧)

ولا تتضمن التشريعات المصرية قانوناً خاصاً لحماية الخصوصية الرقمية، لكن رغم أن هناك بعض المواد الدستورية التى جاءت على ذكر الخصوصية، والتى تحدثت بصورة غير صريحة عن الأنشطة الإلكترونية إلا أن ذلك حتى الأن لم ينتج عنه قانون، فما جاء ذكره أنه "لحياة المواطنين الخاصة حرمة، وسريتها مكفولة، ولا يجوز مصادرة المراسلات البريدية والبرقية والإلكترونية والمحادثات الهاتفية وغيرها من لقطات لشاشات الحاسبات المستهدفة، وتسجيل المحادثات النصية، أو محادثات الصوت

والصورة التى تقوم بها برامج المراسلة الفورية مثل والتحكم بالأجهزة المخترقة ونسخ محتوياتها.

ويتضمن الدستور المصرى أربعة مواد تتعلق بحماية الحق فى الخصوصية هى المواد (٥٧ – ٦٥ – ٧٠ – ٩٩):

(مادة ٥٧)

للحياة الخاصة حرمة، وهى مصونة لا تمس وللمراسلات البريدية، والبرقية والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الإتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الإطلاع عليها، أو رقابتها إلا بأمر قضائى مسبب، ولمدة محددة، وفى الأحوال التى يبينها القانون، كما تلتزم الدولة بحماية حق المواطنين فى استخدام وسائل الإتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك.

(مادة ٦٥)

حرية الفكر والرأى مكفولة، ولكل إنسان حق التعبير عن رأيه بالقول، أو الكتابة، أو التصوير، أو غير ذلك من وسائل التعبير والنشر.

(مادة ٧٠)

حرية الصحافة والطباعة والنشر الورقى والمرئى والمسموع والإلكترونى مكفولة، وللمصريين من أشخاص طبيعية أو اعتبارية، عامة أو خاصة، حق ملكية وإصدار الصحف وإنشاء وسائل الإعلام المرئية والمسموعة، ووسائط الإعلام الرقمي.

وتصدر الصحف بمجرد الإخطار على النحو الذى ينظمه القانون، وينظم القانون إجراءات إنشاء وتملك محطات البث الإذاعى والمرئى والصحف الإلكترونية.

(مادة ٩٩)

كل اعتداء على الحرية الشخصية أو حرمة الحياة الخاصة للمواطنين، وغيرها من الحقوق والحريات العامة التى يكفلها الدستور والقانون، جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم، وللمضرور إقامة الدعوى الجنائية بالطريق المباشر.

وتكفل الدولة تعويضاً عادلاً لمن وقع عليه الإعتداء، وللمجلس القومى لحقوق الإنسان إبلاغ النيابة العامة عن أى انتهاك لهذه الحقوق، وله أن يتدخل فى الدعوى المدنية منضماً إلى المضرور بناء على طلبه، وذلك كله على الوجه المبين بالقانون.

لم يول المشروع المصرى اهتماماً بالخصوصية وحماية البيانات الشخصية، حيث جاءت النصوص والقوانين التشريعية خالية من قانون يوفر الحماية للبيانات الشخصية من الاعتداء عليها.

والأمر على خلاف ذلك بالنسبة إلى الدستور المصري، حيث حظيت البيانات الشخصية للأفراد الطبيعين فى البيئة الرقمية بحماية الدستور المصري، الذى يعتبرها حقاً أساسياً من حقوق الإنسان، طالما أنها ترتبط بحرمة الحياة الخاصة للمواطنين، وهذا هو ما نصت عليه المادة (٥٧) من الدستور المصري، كما تداول هذه البيانات الشخصية عبر شبكة الإنترنت يتطلب مزيداً من الإحتياطات والإجراءات الخاصة اللازم اتباعها خلال تدفقها بين دول العالم من أجل الحفاظ على خصوصية هذه البيانات. (٢٨)

ويتضمن قانون العقوبات فى بابه الخامس المادة (٧٩) وتنص علي:

مع عدم الإخلال بأية عقوبات أشد منصوص عليها فى أى قانون آخر يعاقب بالغرامة التى لا تقل عن مائة ألف جنية ولا تزيد عن خمسمائة ألف جنية كل من خالف أحكام المواد "٢١ ، ٥١ ، ٧٦" من هذا القانون.

ويتضمن القانون الموحد لتنظيم الصحافة والإعلام خمس مواد تتعلق بحماية الخصوصية هى المواد (٣ – ٤ – ٢١ – ٥١ – ٧٦) كما يتضمن قانون الأحوال المدنية رقم ٢٦٠ لسنة ١٩٦٠ وتعديلاته مادة تحظر إنشاء البيانات التى تحويها سجلات الأحوال المدنية.

وبالنظر للقانون رقم ٧٥ لسنة ٢٠١٨ فى شأن مكافحة جرائم تقنية المعلومات يمكننا تسجيل عدداً من الملاحظات تتمثل على النحو التالي:

أولاً: عدم التزام القانون بالضمانات الدستورية والحقوقية للحق فى الخصوصية، وكذلك المواد ذات الصلة من مواثيق وعهود حقوق الإنسان الدولية التى صدقت عليها مصر وأصبحت ملزمة.

ثانياً:تعريض خصوصية المواطنين للخطر من خلال تقنين التدخل غير المشروع فى البيانات والأنظمة المعلوماتية وإلزام مقدمى الخدمة بمنح الجهاز القومى للإتصالات ووزارة الداخلية ومجلس الأمن ورئاسة الجمهورية والمخابرات العامة وهيئة الرقابة الإدارية حق النفاذ الكامل إلى أنظمتها المعلوماتية تحت أى ظرف وبدون الحصول على أمر قضائي.

تنص المادة (٢) على أن يلتزم مقدمو الخدمة أى الشركات مقدمة خدمات الإتصالات والإنترنت بعدة أمور منها:

١- حفظ وتخزين سجل النظام المعلوماتى أو أى وسيلة لتقنية المعلومات لمدة مائة وثمانون يوماً متصلة، وتتمثل البيانات الواجب حفظها وتخزينها فيما يأتي:

أ) البيانات التى تمكن من التعرف على مستخدم الخدمة.

ب) البيانات المتعلقة بمحتوى ومضمون النظام المعلوماتى المتعامل، متكانت تحت سيطرة مقدم الخدمة.

ج) البيانات المتعلقة بحركة الإتصال.

د) البيانات المتعلقة بالأجهزة الطرفية للإتصال.

ه) أى بيانات أخرى يصدر بتحديدها قرار من مجلس إدارة الجهاز.

وهكذا يلاحظ التدخل غير المشروع وتعريض الخصوصية للخطر لعدة أسباب هي:[٢٩]

- إلزام مقدمى الخدمة بالإحتفاظ ببيانات تتخطى ما تحتاجه فى إتمام عملها بشكل كفؤ، علماً بأن هذه البيانات لا تخص مقدمى الخدمة وليست مملوكة لها بأى شكل، وإنما هى خاصة بمستخدمى الخدمة ومملوكة لهم بشكل كامل.
- إلزام مقدمى الخدمة بالإحتفاظ بهذه البيانات لمدة طويلة، وكلما طالت هذه المدة، كانت هذه البيانات عرضة لأن يصل إليها من لا يحق له الإطلاع عليها، أو التعامل معها بشكل تجارى أو خارج القانونى مما ينتهك خصوصية المواطنين، وبشكل يصعب معه تحديد المنتهك، سواء كان من القائمين على النظام المعلوماتى التابع لمقدم الخدمة، أو كان من خارجه وتمكن من اختراقه بأية وسيلة.
- تسمح لجهة إدارية غير تشريعية أو قضائية بتحديد أنواع إضافية غير معلومة وغير محددة ودون ضوابط من البيانات التى تلزم مقدمى الخدمة بالإحتفاظ

بها، وفى هذا إخلال جسيم مستخدم أى خدمة من معرفة البيانات الخاصة به والتى سيحتفظ بها مقدم الخدمة، مقدماً وعلى وجه التفصيل.

ثالثاً: عدم تحديد ماهية البيانات التى يلتزم مقدمو الخدمة بالإحتفاظ بها وعدم تحديد مدة زمنية لذلك، وعدم تحديد عقوبة فى حالة تخطى مقدمى الخدمة للبيانات المطلوبة لأداء وظيفتها.

رابعاً: غياب الرقابة القضائية فى حال حاجة التحريات والتحقيقات فى جرائم بعينها، ومن ثم ينبغى النص صراحة على عدم جواز النفاذ للبيانات إلا من خلال التقدم إلى جهة قضائية مستقلة والنص على ضوابط الطلب من خلال النص صراحة على الشخص أو الأشخاص المطلوب النفاذ إلى بياناتهم ومبررات ذلك.

خامساً: ترهيب مقدمى الخدمة، حيث وضع القانون مسئولية جنائية على عاتق مقدمى الخدمة، فإذا امتنع أى منها عن تنفيذ القرار الصادر بتسليم ما لديها من بيانات أو معلومات أو ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات أو تتبعها فى أى مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه لأجهزة الأمن القومي، أو لم تسمح لأجهزة الأمن القومى بالبحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية، تعاقب الجهة مقدمة الخدمة بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن عشرين ألف جنية، ولا تجاوز مائة جنية أو بإحدى هاتين العقوبتين.

سادساً: التوسع فى حماية الأشخاص الإعتبارية العامة مقارنة بالأشخاص الإعتبارية الخاصة والأشخاص الطبيعية، ويتضح ذلك من خلال زيادة العقوبة إن ارتكبت الجريمة ذاتها فى حق الأشخاص الإعتبارية العامة (مثل الحكومة أو الهيئات العامة) عن تلك التى ترتكب فى حق الأشخاص الإعتبارية الخاصة (مثل

الشركات) عن تلك التى ترتكب فى حق الأشخاص الطبيعيين (الأفراد من الناس)، يفرض القانون عقوبات قاسية على الجرائم التى ترتكب فى حق الأفراد، وقاسية جداً على الجرائم التى ترتكب فى حق الشركات، وشديدة القسوة على الجرائم التى ترتكب فى حق الدولة والمؤسسات العامة، أى أنه يميل إلى حماية مصالح الأقوي.

سابعاً: توسع المشروع فى منح الصلاحيات لأجهزة الأمن القومى فى غياب رقابة قضائية، فعلى الرغم من أن القانون ألزم الشركات مقدمة الخدمة بالحفاظ على سرية تلك البيانات التى تم حفظها وتخزينها، وألزمهم بعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة، إلا أن ذات القانون جعل لأجهزة "الأمن القومي" التى عرفها وحددها القانون بأنها رئاسة الجمهورية، ووزارة الدفاع، ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الإدارية، الحق فى الإستفادة من ذلك القرار القضائى المسبب فأصبح من حقهم الآتي:

- ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات أو تتبعها فى أى مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه.
- البحث والتفتيش والدخول والنفاذ إلى برنامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقاً لغرض الضبط.
- أن تأمر مقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتى أو جهاز تقنى موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمى خدمته وحركة الإتصالات التى تمت على ذلك النظام أو الجهاز التقني.

ويعيب مواد القانون فيما يخص هذه الصلاحيات عدة أمور أساسية:

- عدم الإتساق، فبعض المواد تلزم أن يكون النفاذ إلى البيانات بأمر قضائي، والبعض يمنح صلاحية تقديرية لجهة تحقيق لم يعرفها، والآخر يمنح صلاحيات لأجهزة الأمن القومى نفسها دون اشتراطات الحصول على أمر قضائى أو من جهة تحقيق.
- لم يبين القانون أية ضوابط فيما يتعلق أو لا، بالأسباب والظروف التى يمكن فى ظلها إصدار أمر قضائى بالنفاذ إلى بيانات مستخدمى نظام معلوماتي، ثانياً، ماهية البيانات التى يمكن أن يشملها مثل هذا الأمر القضائي، فى المطلق أو فيما يتعلق بالحالة التى يسمح فيها بالنفاذ إليها.
- منح القانون جهة مجهولة الحق فى التظلم من الأمر القضائي، مع أنه لم يلزم بإخطار صاحب الشأن (المستخدم) بصدور الأمر القضائي، ولو يحدد فترة زمنية تسمح بالتظلم من الأمر قبل تنفيذه فعلياً، كما لم ينص القانون على أية سبل لجبر الضرر أو التعويض فى حال كانت أسباب طلب النفاذ إلى البيانات غير كافية أو غير صحيحة، وترتب عليها الإضرار بمصالح صاحبها أو غيره أو سلامتهم بأى شكل.
- الأخطر هو أن المواد المذكورة تسمح لأجهزة الأمن القومى بالنفاذ إلى كامل البيانات الموجودة على النظام المعلوماتى ولا تقصرها أصلا على تلك الخاصة بمستخدم أو مستخدمين بعينهم يتعلق بهم الأمر القضائى (حين تشترط الحصول عليه)، وبالتالى فإن بيانات جميع مستخدمى النظام المعلومات تصبح مباحة دون أى مبرر أو مسوغ قانونى ودون أية ضوابط.

نحو إصلاح تشريعى لحماية الخصوصية الرقمية:

نتيجة لهذه المخاوف، يدرس الإتحاد الأوروبى منذ فترة سياسات حماية البيانات وتشمل اقتراحات أن تكون الموافقة صريحة وليست ضمنية أو مفترضة، وأن يكون وصول الأفراد إلى البيانات الخاصة بهم سهلاً وشاملاً، وأن يكون للأفراد الحق فى قابلية النقل للبيانات بمعنى المقدرة على نقل البيانات الشخصية من مزود خدمة إلى مزود آخر، والحق فى أن يتم نسيان الشخص، حيث يمكن للأفراد أن يطلبوا حذف بياناتهم إذا لم تكن هناك أى أسس مشروعة للإحتفاظ بهذه البيانات، وأن تنطبق هذه القواعد أيضاً على الشركات خارج الإتحاد الأوروبى إذا كانت هذه الشركات عامة فى سوق الإتحاد الأوروبى وتقدم خدماتها لمواطنى دول الإتحاد الأوروبي.

وبالمثل، تقدمت مفوضية التجارة الفيدرالية فى الولايات المتحدة الأمريكية بإقتراح يتضمن ثلاثة تعديلات من أجل توفير حماية أكثر فعالية للخصوصية: الخصوصية من خلال التصميم، حيث يتم تأسيس الخصوصية بشكل متأصل فى كل مرحلة من مراحل تطوير المنتج، منح الشركات والمستهلكين خياراً مبسطاً يمنحهم المقدرة على اتخاذ القرارات بشأن بياناتهم الخاصة، وهذا يشمل تطبيق آلية لعدم التتبع والحصول على الموافقة الصريحة فيما يتعلق بالبيانات الحساسة، أو الحصول على موافقة قبل استخدام البيانات فى عرض مختلف بشكل مادى عن الغرض الذى تم من أجله تكوين هذه البيانات، وشفافية أكثر فيما يتعلق بالبيانات وجمعها واستخدامها.(٣١)

لقد اقترح العديد من العلماء المتخصصين فى الخصوصية، وأيضاً العديد من مجموعات الضغط الصناعية مناهج متعددة لكيفية التعامل مع قضية الخصوصية، فالعلماء المختصون بموضوع الخصوصية سبق لهم التطرق للمواضيع التالية: الإصلاح التشريعى المصمم من أجل حماية حقوق المواطنين، والذى يشمل بعض القضايا كالحق فى الصفحة البيضاء، وتواريخ الإنتهاء للبيانات، ومن الذى يكون

مسئولاً عن ضمان الخصوصية، المطورون أم الوكالات أم المستخدمون، وعن الوسائل التقنية والإدارية لتنفيذ هذه الأمور، وما الذى يشكل المعلومات الخاصة، وكيفية تأطير الخصوصية حول المخاطر، ومدى الضرر بدلاً من تأطيرها حول تعريف المحتوي.(٣٢)

واقترح هؤلاء العلماء أيضاً دخول الأفراد فى شراكات مع المطورين، حيث يكون بإمكانهم أن يختاروا بشكل أكثر استباقية ما البيانات التى يرغبون فى نشرها، ولمن تنشر هذه البيانات، وتحت أى ظروف تنشر هذه البيانات، كما اقترحوا أن تتيح الشركات للمستخدمين الوصول إلى بياناتهم الشخصية بصيغة قابلة للإستخدام وذلك من أجل مصلحتهم الشخصية، و أن تقوم الشركات بمشاركة الثروات الناتجة عن تحويل البيانات الشخصية إلى أموال، وكمثال على هذه المشاركة المفيدة لكلا الطرفين فى الثروات المتحصلة من بيع بيانات الشبكات الذكية حيث يتم استخدام البيانات التى تم تكوينها من خلال العدادات الذكية والمتعلقة بإستهلاك أفراد الأسرة للكهرباء من قبل شركة الكهرباء.(٣٣)

نحو أساس قانونى لمعالجة البيانات:

ينبغى أن تكون هناك أسس قانونية لجمع البيانات الشخصية وتخزينها ومعالجتها واستخدامها، ويمكننا أن نستخلص الأسس الأربعة التالية من قوانين خصوصية البيانات: (٣٤)

١- فى حالة موافقة الشخص ذاته.

٢- فى حال إذا دعت الضرورة للإمتثال لالتزام قانونى لحماية الأمن القومي.

٣- فى حال إذا دعت الضرورة من أجل تنفيذ عقد يكون الفرد طرفاً فيه.

٤- فى حال إذا كانت هناك مصلحة مشروعة طالما المعالجة عادلة وآمنة وشفافة ولا تؤثر فى حقوق الشخص.

وينبغى أن يكون هناك مدى زمن للإحتفاظ بالبيانات الشخصية، للوفاء بأى متطلبات قانونية أو محاسبية أو تعاقدية، وتختلف الفترة الزمنية وفق تلك المتطلبات والأسباب التى يتم معالجة البيانات بشأنها.

ووفق المؤسسات الدولية الخيرية العاملة فى هذا المجال المتعلق بحماية البيانات يبلغ المدى الزمنى للمؤسسة الملكية لدوق ودوقة كمبريدج (٦ سنوات)، وهى مؤسسة خيرية تتبادل المعلومات الشخصية وفق سياسة خصوصية معلنة بالتعاون مع عدد من الجمعيات والمؤسسات الخيرية العاملة فى مجال رفع الوعى وتقديم المساعدة للأشخاص الذين يواجهون تحديات الصحة النفسية والمحافظة على الحياة اليومية ومكافحة التنمر على الإنترنت والمصابين بالجروح والإصابات الرياضية والمرضى العاملين فى الجيش. (٣٥)

الحقوق القانونية المتعلقة بإستخدام البيانات الشخصية:

ينبغى أن يحتفظ الفرد بسبعة حقوق أساسية لحماية بياناته الشخصية هي: (٣٦)

١- الحق فى الإعتراض: فللشخص الحق فى الإعتراض على المعالجة فى حال إذا كانت المعالجة لإلتزام قانونى أو مالى أو تعاقدى أو إحصائى أو تسويقي.

٢- الحق فى سحب الموافقة فى حالة إذا تم استخدام البيانات الشخصية على أساس موافقة الشخص.

٣- حق الإطلاع: يجوز للشخص أن يطلب التأكد من ماهية المعلومات التى يتم حفظها وتخزينها ويطلب نسخة منها.

٤- حق المحو: فى بعض الحالات يمكن للشخص أن يطلب محو البيانات الشخصية من السجلات المحفوظة.

٥- حق التصحيح: للشخص أن يطلب تصحيح وتحديث البيانات إذا كانت غير دقيقة.

٦- حق تقييد نطاق المعالجة: فى بعض المواقف من حق الشخص أن يطلب تقييد نطاق المعالجة إذا كان هناك خلاف حول دقتها أو استخدامها المشروع.

٧- الحق فى نقل البيانات: للشخص أن يطلب نقل البيانات من مزود خدمة إلى أخر.

المراجع

١) روب كينشن، ثورة البيانات: البيانات الكبيرة والبيانات المفتوحة والبنيه التحتيه للبيانات والنتائج المترتبة عليها، ترجمة محمد بن أحمد نمرودي، الطبعة الأولى (السعودية، مركز البحوث والدراسات بمعهد الإدارة العامة، ٢٠١٨) ص٢٨٧.

٢) مركز هردو لدعم التعبير الرقمي، إنتهاك الخصوصية الرقمية فى الصحافة.. المهنية الصحفية والحياة الشخصية، القاهرة، ٢٠١٧ [www.hardoegypt.org] at.

٣) مركز هردو لدعم التعبير الرقمي، الأمن القومى وحماية المعلومات.. الحق فى استخدام شبكة آمنة، القاهرة، ٢٠١٧، ص ٦-٧ [www.hardoegypt.org] at.

٤) الأمن الرقمى كأداة لحماية المدافعات والمدافعين عن حقوق الإنسان، سبتمبر ٢٠١٤، [https://goo.gl//ffA4mm].

٥) تقرير شفافية الصادر عن فيس بوك عن النصف الأول من سنة ٢٠١٣.

٦) ميثاق حقوق الإنترنت لجمعية الإتصالات المتقدمة فى أوروبا، براغ، تشيكيا، فبراير عام ٢٠١.

٧) قرار الجمعية العامة للأمم المتحدة بشأن حماية الحق فى الخصوصية الرقمية رقم (١٦٦/٦٩) الصادر فى ١٨ ديسمبر ٢٠١٣.

٨) لمزيد من التفاصيل يمكن الرجوع إلي:

- القمة العالمية لمجتمع المعلومات، الوسيط، ١٦ نوفمبر ٢٠٠٥.

[https://goo.gl/BCf7qb].

- الوثائق الصادرة عن القمة العالمية لمجتمع المعلومات، ديسمبر ٢٠٠٥.

[https://goo.gl/ShH4eY].

٩) تقرير منظمة سلامتك، الخصوصية من منظور حقوق الإنسان at [www.salamtek.org].

10) Boundless informate, the NAS's secret tool to track global surveillance data.

11) convention for the protection of Human Rights and Fundamental freedom.

12) FTC staff Issues Privacy Report, offers Framework for consumers Businessmen and Policy makers.

13) Children's online Privacy Protectiom Act of 1998.

١٤) مركز دعم لتقنية المعلومات SITC، الخصوصية الرقمية بين الإنتهاك والغياب التشريعي، سلسلة أوراق الحق فى المعرفة، ٢٨ أكتوبر ٢٠١٣.[https://siteegypt.org] at .

١٥) روب كينشن، مرجع سابق، ص ٩١،٩٢.

16) Cavoukian, A,(2009) Privacy by Design: A Primer . [http://www.privacybydesign.ca/content/uploads/201310//pbd-primer.bdf], p32.

17) Minelli,M, and Dhiraj. A. (2013) Big Data ,Big Analytics. Wiley, Hoboken,Nj. p156.

18) Rubinstein, I.S (2013) 'Big date: the end of privacy or a new beginning?', International Date Privacy Law, online first, [http://idpl.oxfordjournals.org/content/early/201324/01//idpl].

١٩) روب كينشن، مرجع سابق، ص ٢٩.

20) Koops, B.J. (2011), 'forgetting footprints, shunning shadows: a critical analysis of the ''right to be forgotten'' in big data practice' ,SCRYPTED, 8(3): P56.

21) Raley, R. (2013), 'Dataveillance and countervailance' , in L. Gitelman (ed.) 'Raw Data' is an Oxymoron. MIT Press, Cambridge, MA,pp. 121-46.

22) Curry, M.R., Philips, D.J. and Regan, P.M. (2004), 'Emergency response systems and the creeping legibility of people and places', The Information Society. P 239.

23) solove, D.J. (2006), 'A taxonomy of privacy', University of Pennsylvania Law Review,154(3): 477-560.

24) Minelli,M,Chambers and Dhiraj (2013)/ op cit, pp 151-152.

25) Gralla, p. sacco, A . and fass, R. (2011), 'Smartphone apps: is your privacy protected?' Computerworld [http://www.Computerworld.com/s/ article/9218163 /Smartphone_apps_protected , Pp 11-12.

26) Raley,R.(2013), op.cit, p126.

٢٧) مركز دعم لتقنية المعلومات SITC، الخصوصية الرقمية بين الإنتهاك والغياب التشريعي، سلسلة أوراق الحق فى المعرفة، ٢٨ أكتوبر ٢٠١٣. [https://siteggpt.org] at

٢٨) محمد أحمد المعداوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الإجتماعي.. دراسة مقارنة، العدد الثالث والثلاثون، الجزء الرابع، ص ١٩٥٤ – ١٩٥٦.

٢٩) وحدة الدعم القانوني، استباحة الحياة الخاصة بإسم القانون.. قانون مكافحة جرائم المعلومات واستباحة خصوصية مستخدمى الإتصالات والإنترنت، ٧ سبتمبر ٢٠٢٠.

٣٠) مركز هردو لدعم التعبير الرقمي، انتهاك الخصوصية الرقمية فى الصحافة.. المهنية الصحفية والحياة الشخصية مرجع سابق.

٣١) روب كينشن، مرجع سابق ص ٢٩٤.

32) Coterill, C. (2011), 'Location privacy: who protects?', URISA, 23 (2). PP 49 – 59

33) Tene,O.and Polonetsky, J.(2012) 'Big date for all: privacy and user control in the age of analytics', Social Sciences R esearch Network, [http://ssrn.com/abstract=2149364].

34) Royal foundation of the Duke and the Duchess of Cambridge, the Earthshot Prize,2020, at (earthshotprize.org) [www.royalfoundation.co.uk]

٣٥) المؤسسات المشاركة مع مؤسسة دوق كمبريدج

- حملة Heads Together لرفع الوعى وتقديم المساعدة للأشخاص الذين يواجهون تحديات الصحة النفسية.
- حملة united for wildlife للمحافظة على الحياة البرية.
- جائزة إيرث شوت.
- حملة مكافحة التنمر على الإنترنت.

- صندوق أنديفور Endeavour found لتمويل التحديات الرياضية والمغامرة للمصابين ومرضى الجيش.
- برنامج coach core لإلهام الشباب ومساعدتهم لبناء حياتهم المهنية فى التدريب الرياضي.
- مؤسسة استديو للتسجيل المجتمعى community Recording Studio لدعم الشباب المعرض للمخاطر والمتضرر من العنف الشبابى فى نوتنجهام.

36) Royal foundation of the Duke, op cit.