الخصوصية الرقمية فى القانون الدولى والمواثيق الدولية

محمد حسن عماد مكاوى

مدرس مساعد بكلية القانون بالجامعة البريطانية فى مصر

محاضر بالماجستير المهنى للتحقيق الجنائى فى الجرائم السيبرانية

باحث بالدكتوراه بكلية الحقوق جامعة القاهرة

باحث بمركز القانون والتكنولوجيا

مقدمة

أصبح التقدم التكنولوجى لوسائل الاتصال والمعلومات يشكل تهديدا واضحا لمبدأ الخصوصية كحق من حقوق الإنسان، ولذلك أوجبت المنظومة الأممية على الدول الأطراف احترام حق الخصوصية والالتزام بحمايته من التدخل التعسفى وغير المشروع.

و الجدير بالملاحظة أن الحق في الاعلام يمتد إلى معرفة بعض الوقائع التي ترتبط بشخصية صاحبها، فالجماهير لا تقبل الخدمة العامة من أي شخص ما لم تكن لديه القدرة عليها و الإخلاص في آدائها، ومن هنا فيحق للجماهير أن تطلع على شخصية

من يمارس النشاط العام لأن ذلك النشاط العام هو ثمرة شخصية صاحبه و من حق الجماهير التي يبذل النشاط العام من أجلها أن تعرف جوانب الشخصية التي تفرز هذا النشاط حتى تطلع على مدى قدرته وإخلاصه فى الأداء[١].

لم تعد قضية انتهاك الخصوصية قاصرة على دولة ما، أو مجتمع بعينه، وإنما باتت قضية دولية تشغل اهتمام جميع المجتمعات، حيث ينتج عن الثورة التكنولوجية تغيرات عديدة فى مجالات الخصوصية. لم يعد الاعتداء على الخصوصية يقتصر على الطرق التقليدية فى المراقبة والتلصص، وإنما امتد إلى اختراق البيانات وانتهاك الحرمات فى جميع الأماكن والأوقات.

أتاحت التقنيات الحديثة للدول قدرات غير محدودة فى الرقابة على الأفراد بغرض الحفاظ على أمن المجتمع وسلامته وحماية الأمن القومى، والسيطرة على التهديد المتنام الذى يواجه الدولة من ارتكاب جرائم على أرضها بما يعكس إيجابا على أمن الفرد وسلامته المجتمع برمته.

ينطلق هذا البحث من فكرة التوازن بين مصلحة الفرد فى تحقيق حريته الشخصية وحماية خصوصيته من الانتهاك، ومصلحة المجتمع فى حماية أمنه وسلامته، وبالتالى مراعاه التوازن بين صالح الفرد والصالح العام.

تتحدد مشكلة البحث فى الإجابة على السؤال التالى: ما مدى ملائمة نصوص القانون الدولى والمواثيق الدولية واستجابتها لحماية الخصوصية فى العصر الرقمي؟

[١] أحمد فتحى سرور (١٩٧٦) **الحماية الجنائية للحق في حرمة الحياة الخاصة**، القاهرة، دار النهضة العربية، ص ١٢١

الكلمات المفتاحية:

الخصوصية الرقمية – حقوق الإنسان – القانون الدولى – المراقبة الإلكترونية – المواثيق الدولية – الأمم المتحدة – الذكاء الاصطناعي.

خطة البحث

يتم تقسيم هذا البحث إلى ثلاثه مباحث يتناول أولها ماهية الخصوصية الرقمية من خلال تعريف الخصوصية الرقمية، وتعريف البيانات الشخصية وأنواعها، ونطاق الخصوصية الرقمية، والأثار السلبية والإيجابية لوسائل وتقنيات المعلومات. ويستعرض المبحث الثانى المعاهدات والمواثيق الدولية، وطرح رؤية نقدية للإتفاقية العربية لمكافحة جرائم تقنية المعلومات. ويتناول المبحث الثالث موقف الخصوصية الرقمية فى القانون الدولى وتحديدا إتفاقية بودابست التى باتت تشريعا ملزما للعديد من الدول وأهميتها فى مجال حماية الخصوصية الرقمية، وذلك على النحو التالى:

المبحث الأول: ماهية الخصوصية الرقمية

المطلب الأول: تعريف الخصوصية الرقمية

المطلب الثانى: محل الخصوصية الرقمية

المطلب الثالث: أثر وسائل تقنية المعلومات الحديثة على الخصوصية الرقمية

المبحث الثانى: الخصوصية الرقمية فى المعاهدات والمواثيق الدولية

المطلب الأول: المعاهدات الدولية

المطلب الثانى: الاتفاقيات الإقليمية وأهم المؤتمرات

المطلب الثالث: اللائحة العامة لحماية البيانات GDPR

المبحث الثالث: الخصوصية الرقمية فى القانون الدولى

المطلب الأول: تقارير الجمعية العامة للأمم المتحدة لعام ٢٠١٣

المطلب الثانى: تقارير الجمعية العامة للأمم المتحدة لعام ٢٠١٤

المطلب الثالث: تقارير الجمعية العامة للأمم المتحدة لعام ٢٠١٨

المطلب الرابع: تقارير الجمعية العامة للأمم المتحدة لعام ٢٠٢١

المطلب الخامس: الخصوصية الرقمية فى جمهورية مصر العربية

الخاتمة و التوصيات

المبحث الأول

ماهية الخصوصية الرقمية

ينقسم هذا المبحث الى ثلاثة مطالب، نعرض تعريف الخصوصية الرقمية فى المطلب الأول، ثم محل الخصوصية الرقمية فى المطلب الثانى، ثم أثر وسائل تقنية المعلومات الحديثة على الخصوصية الرقمية فى المطلب الثالث.

المطلب الأول – تعريف الخصوصية الرقمية:

أختلف العديد من الفقهاء فى تعريف الخصوصية، فمنهم من قال أن الخصوصية ترتبط بالحرية وذلك يعنى لدى البعض حق الشخص أن يترك وحيدا، ويعد ذلك من أهم سمات الحرية فى المجتمع الديمقراطى[١]، فى حين ذهب البعض إلى أن الخصوصية هى كل ما لا يعد حياة عامة، والحياة العامة هي ذلك الجانب من حياتنا الذي يجري في حضور أو أمام الكافة أى جميع الناس[٢]، بينما ذهب اتجاه آخر من الفقه إلى تعريفها بأنها الدائرة أو المنطقة السرية من الحياة أو بالأحرى هي المنطقة التي يملك الفرد سلطة إبعاد الآخرين عنها[٣]، كما عرف حق الخصوصية إيضا انه الحق في استبعاد الآخرين من حرمة الحياة الخاصة، وحق الإنسان في احترام طبيعته الشخصية، و الحق في أن يعيش في سلام[٤]، ومن أحدث وأشهر تعريفات الخصوصية

---

[1] Samuel D. Brandeis and Louis D. Warren (1890) **The Right to Privacy**, Harvard Law Review, Page 23

[2] R. Badinter (1974) **Le droit au respect de la vie privee**, JCP, Paris 1968, doct. No. 2136 R. Gassin, L'atteine a la vie privee, Dalloz Penal, P.6

[3] J. Carbonnier Droit Civil. (1995) **Les Personnes. Personnalite, incapacitee, personnes morales** Paris, Coll. Themis Droit pice PUF, P. 254

[٤] أحمد فتحى سرور (١٩٨٤) الحق في حرمة الحياة الخاصة، **مجلة القانون و الإقتصاد**، العدد ٥٤ ،ص ٢٩٠

هو تعريفها عن طريق تعريف المساس بها،[١] فيعتبر مسئولا ومخترقا للخصوصة كل من يقوم بالمساس بشئ خفى لأى أمر لشخص ما وجعلها تصل لعلم الغير، أو جعل صورة الشخص عرضة لأنظار الجمهور دون موافقة هذا الشخص[٢].

تعرف الخصوصية الرقمية بأنها وصف لحماية البيانات الشخصية للفرد، والتي يتم نشرها وتداولها من خلال وسائط رقمية [٣]والتى تتمثل فى البيانات الشخصية مثل البريد الإلكتروني، والحسابات البنكية، والصور الشخصية، ومعلومات عن العمل والمسكن وكل البيانات التي نستخدمها في تفاعلنا على الإنترنت أثناء استخدامنا للحاسب الآلي أو التليفون المحمول أو أي من وسائل الاتصال الرقمي بالشبكة العنكبوتية[٤]

المطلب الثانى – محل الخصوصية الرقمية:

ينقسم محل الخصوصية الرقمية الى فرعين: الفرع الأول تعريف البيانات الشخصية والفرع الثانى أنواع البيانات الشخصية ونستعرض ذلك فى التالى:

---

[١] حسام الدين الاهواني (١٩٧٨) **الحق في احترام الحياة الخاصة**، دراسة مقارنة، القاهرة، دار النهضة العربية، ص ٢٣

[2] Paul M. Schwartz and Daniel J. Solove (2020) **PRINCIPLES OF THE LAW Data Privacy**, The American Law Institute "ALI", Page 121

[3] Michael Iheanyichukwu (2020) Internet Privacy in 2020, Research Gate, available at: https://www.researchgate.net/publication/347362107_INTERNET_PRIVACY_IN_2020 Accessed on 11-1-2022

[4] T. Dinev, and P. Hart (2005). Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact. International Journal of Electronic Commerce [Online]. Vol. 10,No. 2, pp. 7-29. Available at: http://www.jstor.org/stable/27751182. Accessed on 11-1-2022

الفرع الأول: تعريف البيانات الشخصية

نصت المادة الأولى من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨[١] أن البيانات شخصية هى "أى بيانات متعلقة بشخص طبيعى محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى"

وفى هذا التعريف يتم الإشارة إلى أن لا جدوى للبيان فى ذاته الا لو إلتصق بشخص معين، فالرقم القومى على سبيل المثال لا يعبر عن شئ بعينة إلا إذا نسب لصاحب البطاقة، ومن ثم فإن ارتباط المعلومة بالشخص هو ما يجعلها من البيانات الشخصية، فى حين أن بعض البيانات تتعلق بالضرورة للفرد من تلقاء نفسها مثل أسم الشخص، وبالتالى فإن البيانات أو المعلومات لابد أن تكون ملتصقة بشخص معين لكى يتحقق الإستيلاء، اما اذا كان غير متعلق بشخص معين فالاستيلاء على بيان أو معلومة لا يعد خرقا للبيانات الشخصية.

ونصت المادة الأولى من قانون حماية البيانات الشخصية المصرى رقم ١٥١ لسنة ٢٠٢٠[٢] "البيانات الشخصية هى أى بيانات متعلقة بشخص طبيعى محدد او يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذة البيانات وأى بيانات أخرى عن طريق الإسم أو الصوت أو الصورة أو رقم تعريفى او محدد للهوية عبر

[١] قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ متوفر على
https://manshurat.org/node/31487
أخر دخول ١١ يناير ٢٠٢٢

[٢] قانون حماية البيانات الشخصية المصرى رقم ١٥١ لسنة ٢٠٢٠
:https://docs.google.com/viewerng/viewer?url=https://manshurat.org/sites/default/files/287844.pdf
أخر دخول ١١ يناير ٢٠٢٢

الإنترنت أو أى بيانات تحدد الهوية النفسية أو الصحية أو الاقتصادية والثقافية او الاجتماعية.

نخلص من تعريف البيانات الشخصية وفق القانون المصرى لما يلى:

أولا: قصر تعريف القانون المصرى حماية البيانات الشخصية على البيانات المتعلقة بالأشخاص الطبيعيين فقط دون غيرهم أى استبعاد من نطاق الحماية بيانات الأشخاص المعنوية وهو بذلك قد ساير ما جاء به المشرع الاوروبى وكذلك التشريعات العربية المقارنة.

ثانيا:اشترط النص لاستحقاق الحماية القانونية أن تكون البيانات المتعلقة بالشخص الطبيعى محددة او يمكن تحديدها بشكل مباشر أو غير مباشر وبالتالى بمفهوم المخالفة إذا لم يكن تحديد الشخص ممكنا بأي طريقة فإن البيانات لاتعد شخصية ولا تدخل تحت مظلة حماية القانون محل الدراسة.

ثالثا: أورد النص عدد من المسائل التى يمكن من خلالها تحديد هوية الشخص وقد توسع فيها لتمتد إلى النواحى الصحية أو الثقافية أو الاقتصادية أو الاجتماعية وقد جاءت تلك الأمور على سبيل المثال لا الحصر والبيان مما يعنى أن أى بيانات أخرى قد يصدق عليها وصف الشخصية إذا أمكن تحديد هوية صاحبها بشكل مباشر أو غير مباشر

كما عرفتها اللائحة الأوروبية العامة لحماية البيانات[1](GDPR) التى تم اعتمادها في ١٤ أبريل ٢٠١٦ ودخلت حيز التنفيذ اعتبارًا من ٢٥ مايو ٢٠١٨ فى المادة ٤ الفقرة الأولى:

[1] General Data Protection Regulation 2016, Available at https://gdpr-info.eu/art-4-gdpr/ Accessed on 15-1-2022

‘Personal Data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

وترجمته "البيانات الشخصية تعني أي معلومات تتعلق بشخص طبيعي محدد أو قابل للتحديد (موضوع البيانات)؛ الشخص الطبيعي الذي يمكن التعرف عليه هو الشخص الذي يمكن تحديده ، بشكل مباشر أو غير مباشر ، على وجه الخصوص بالإشارة إلى معرّف مثل الإسم أو رقم التعريف أو بيانات الموقع أو المعرّف عبر الإنترنت أو إلى واحد أو أكثر من العوامل المحددة للعوامل المادية والفسيولوجية ، الهوية الجينية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية لهذا الشخص الطبيعي".

وبالنظرة الفاحصة والناقدة يتضح إختلاف نص اللائحة إختلافا جوهريا في تعريف البيانات الشخصية. ويتجلى هذا الاختلاف في استخدام القانون مصطلح "بالربط" واستخدام اللائحة مصطلح" Reference By" والذي يعني "بالإشارة" وليس "بالربط". وتبدو أهمية الفرق بين المصطلحين في أن مصطلح الربط يفهم منه بسهولة أنه لابد من ارتباط بيانين معا لكي يصبح البيان شخصي بالمعنى الذي يقصده ويحميه القانون. بينما استخدام لفظ "بالإشارة" في اللائحة يوسع من نطاق الشخصية التي قد يشملها القانون بحمايته بجعلها قائمة بذاتها كبيان شخصي من دون الحاجة إلى ربطها ببيان أخر[١].

[١] انظر الدراسة النقدية لقانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ (٢٠٢٠)، إعداد مركز بحوث القانون والتكنولوجيا بكلية القانون الجامعة البريطانية بمصر، بالتعاون مع مكتب أندرسن للمحاماه، صفحة ٩١. متوفر فى مكتبة الجامعة البريطانية بمصر

الفرع الثانى: أنواع البيانات الشخصية

هناك عدة اتجاهات يمكننا الذهاب إليها لمعرفة أنواع البيانات الشخصية:

الإتجاه الأول: الناحية الرقمية(التكنولوجية)

تعنى البيانات الشخصية التى يمكن من خلالها تعريف الشخص، التى يتم تداولها عبر وسيط رقمى أو تكنولوجى إلكترونى عبر الإنترنت[١]، لكن تم نقد هذا التعريف لأنه لم يحدد البيانات الشخصية فى ذاتها بل اعتمد فقط على تعريف الوسيط التى يتداول من خلاله تلك البيانات والمعلومات وبالتالى لا يصلح هذا التعريف لوضع معيار يميز بين ما هو بيانات شخصية عن غيرها[٢].

وتجدر الإشارة الى ما ذكرناه من قبل أن البيانات الشخصية تعد فى ذاتها كذلك إن ارتبطت بالشخص معرف أو قابل للتعريف وذلك بدون الحاجة إلى توثيق ذلك سواء كان بشكل رقمى أو غير رقمى.

وأدى تطور مفهوم البيانات الشخصية إلى ضرورة التفرقة بين ثلاث أنواع من البيانات الرقمية الشخصية[٣]:

١- البيانات الطوعية: هى البيانات التى يتركها الشخص اختياريا ويتشاركها مع غيرة عبر مواقع التواصل الاجتماعى بداية من الأسم والبريد الإلكترونى وأخبار حياته وأحداثها، كما يدخل ضمن البيانات الشخصية الطواعية الرقمية

---

[1] Paul M. Schwartz & Daniel J. Solove (2011), "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", 86 N.Y.U. L.REV. 1814 available at http://ssrn.com/abstract1909366 p.11

Accessed on 12-1-2022

[2] Popa, C. (2012) **Managing Personal Information: Insights on Corporate Risk and Opportunity for Privacy-Savvy Leaders**, Carswell p.17

[٣] مروة زين العابدين (٢٠١٤) الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولى الاتفاقي والقانون الوطنى، **رسالة دكتوراه غير منشورة**، جامعة عين شمس، صفحة ٨٦ و ٨٧

الرقم السرى لبطاقة الائتمان والتى تمكن الشخص من شراء المنتجات والدفع online عبر الإنترنت مباشرة.

٢- البيانات المرصودة: هى البيانات التى تنتج عن طريق التتبع للأماكن التى يتم من خلالها إرسال رسائل البريد الإلكترونى.

٣- البيانات الاستدلالية: هى البيانات الناتجة من تحليل البيانات الطوعية والمرصودة

وفى هذا الصدد فإن القوانين والمواثيق الدولية تتفق على تجريم كل أشكال انتهاك الخصوصية المعلوماتية للفرد ولكن تظل الإشكالية فى كيفية تطبيق العقاب على مواقع التواصل الاجتماعى.

الإتجاه الثانى: الناحية الإجتماعية

وفقا للبعض يمكن اعتبار تلك البيانات بيانات شخصية من الناحية الرقمية وهى الإسم بالكامل، عنوان المنزل، عنوان البريد الإلكتروني، رقم الحماية الاجتماعية، رقم جواز السفر، رقم رخصة القيادة، أرقام بطاقات الائتمان، تاريخ الولادة، رقم هاتف. العقارات المملوكة على سبيل المثال، رقم تعريف السيارة، تفاصيل تسجيل الدخول للبريد، الرقم التسلسلي للمعالج أو الجهاز، التحكم في الوصول إلى الوسائط[1]. معلومات التعريف غير الشخصية) وهى بيانات لا يمكن استخدامها بمفردها لتتبع أو تحديد هوية الشخص، ومن الأمثلة على المعلومات التي لا تتعلق بمعلومات التعريف الشخصية، على سبيل المثال لا الحصر: إحصائيات مجمعة عن استخدام المنتج/الخدمة.

ويمكن تحديد الأمثلة فى التالى:

[1] Karolina Matuszewska, Karolina Lubowicka, What is PII, non-PII, and personal data, DATA PRIVACY & SECURITY, Published October 21, 2020, available online at https://piwik.pro/blog/what-is-pii-personal-data/#what-pieces-of-information-are-considered-pii accessed on 15-1-2022

١- الإسم سواء كان إسما مستعارا أو إسم شهرة أو إسم تجارى يستخدمه التاجر فى عمله.

٢- الموطن: هو المكان الذى يعيش فيه الفرد أو يستخدمه فى نشاط معين ويختلف العنوان عن المحل القانونى فى أن الاخير هو المكان الذى يختارة الفرد لتلقى المراسلات والمكان المدرج فى العقود أما العنوان فهو عنوان السكن أو محل العمل.

٣- شهادة الميلاد التى تتضمن السن و تاريخ الميلاد ومحل الميلاد.

٤- أرقام التليفون

٥- القيد العائلى، او الحالة الاجتماعية وكل الشهادات المتعلقة بذلك

٦- بطاقة الرقم القومى أو جواز السفر أو رقم التأمين الاجتماعى.

٧- الدين و الجنس

٨- الانتماء السياسى لدولة بالجنسية سواء بالدم أو الميلاد وكذلك وجهات النظر فى موضوعات عامة.

٩- الصور ومقاطع الفيديو التى يظهر فيها الشخص و أنواع المراسلات الرقمية(مواقع التواصل الاجتماعى وغيرها) وغير الرقمية.

وبالتالي نخلص إلى أن أنواع انتهاك الخصوصية نوعين:

١- **المراقبة** وهى تعقب اتصالات أحد الأفراد وتسجيلها بلا إذن منه أو بلا علم وتقفي أثر تحركاته عبر الانترنت ووسائل التواصل وتسجيل ذلك رقمياً ، ما يمكن من الإطلاع على أسراره الخاصة وإفشائها بلا مسوغ يذكر أو أمر من سلطة مختصة قضائية أو إدارية.

٢- **الاختراق** ويأخذ معنى العدوان على حق الخصوصية عبر تدمير الحواسيب والأجهزة الخاصة بالاتصال أو تخزين المعلومات أو استرجاعها أو تحوير مضمونها أو تغييره بلا اذن

المطلب الثالث – أثر وسائل تقنية المعلومات الحديثة على الخصوصية الرقمية:

مما لا شك فيه أن التطورات الحديثة في تكنولوجيا المعلومات تهدد الخصوصية وقللت من مقدار التحكم في البيانات الشخصية وفتحت إمكانية حدوث مجموعة من النتائج السلبية نتيجة الوصول إلى البيانات الشخصية، لقد أصبح القرن الحادي والعشرون قرن البيانات الضخمة "Big Data"[١] وتكنولوجيا المعلومات المتقدمة[٢]

نظرا الى التطور الهائل فى مجالات التكنولوجيا، والتقدم الكبير به والتحول الرقمي، كان لذلك العديد من الاثار، فالتكنولوجيا سلاح ذو حدين، قد يحسن استخدمه ويكون له أثار إيجابية، وقد يكون له أثار سلبية عديده، والحقيقة أن هذا الموضوع متسع ويحتاج الى بحث مستقل الا اننا سوف نقتصر على بعض المعلومات الاساسية والتى يستنبط منها الاثار الإيجابية والسلبية معا.

أولا: التطورات في تكنولوجيا المعلومات

تشير "تكنولوجيا المعلومات" إلى الأنظمة الآلية لتخزين المعلومات ومعالجتها وتوزيعها، تعتمد كمية المعلومات التي يمكن تخزينها أو معالجتها في نظام معلومات على التكنولوجيا المستخدمة، وزيادة سعة التخزين وسعة المعالجة وعرض النطاق الترددي للإتصالات[٣]،

[1] Big data means data that contains greater variety, arriving in increasing volumes and with more velocity, for more details about the big data, see https://www.oracle.com/big-data/what-is-big-data/ Accessed on 10-1-2022

[2] Stanford Encyclopedia of Philosophy, Privacy and Information Technology, 30 October 2019, available at: https://plato.stanford.edu/entries/it-privacy/ Accessed on 10-1-2022

[3] Turilli, M. & L. Floridi, (2009) **The ethics of information Transparency**", Ethics and Information Technology,p. 105

ومن الاثار الإيجابية لها أن هذه التطورات قد غيرت بشكل جذري ممارساتنا في توفير المعلومات[١]، حتى أن البعض يتحدث عن ثورة رقمية على أنها قفزة تكنولوجية شبيهة بالثورة الصناعية، أو ثورة رقمية باعتبارها ثورة في فهم الطبيعة البشرية والعالم، فأصبح من السهل الوصول الى المعلومات فى ظل الفضاء الرقمى.

ولكن يوجد إيضا اثار سلبية لهذه التطورات فى تكنولوجيا المعلومات، نظرًا لأن الاتصال يزيد من الوصول إلى المعلومات، فإنه يزيد أيضًا من إمكانية تحكم مصادر تلك المعلومات في المستخدمين، فإذا كنت تعتقد أنك تعيش فقط فى المدينة الفاضلة فأنت مخطئ، فإذا حصلت على معلومة رقميا فانت تدفع ثمن ذلك من خلال تنازلك الرضائى عن معلوماتك وبياناتك الشخصية سواء كان هذا المصدر يستخدم "Cookies" او غيرها.

ثانيا: ملفات تعريف الارتباط "Cookies"

يدور موضوع رئيسي في مناقشة خصوصية الإنترنت حول استخدام ملفات تعريف الارتباط أو ما يعرف بإسم "Cookies" وما لها من اثار سلبية على خصوصية المستخدمين

وتعرف بانها: عبارة عن مجموعات صغيرة من البيانات يقوم خادم الويب بتمرير مجموعات البيانات هذه إلى جهاز الكمبيوتر الخاص بك بعد وصولك إلى موقع ويب[٢]،

[1] J. Van Den Hoven and J. Weckert (2008) **Information technology, privacy, and the protection of personal data**, in Information technology and moral philosophy, Cambridge: Cambridge University Press, pp. 301–322.

[2] Robin Langford (2020) Cookie-less countdown: Advertisers fear loss of third-party cookies, while creative see brighter future NETIMPERATIVE Digital intelligence for business, available at: https://www.netimperative.com/2020/03/30/cookie-less-countdown-advertisers-fear-loss-of-third-party-cookies-while-creatives-see-brighter-future/ Accessed on 10-1-2022

وتستخدم بعض ملفات تعريف الارتباط لتتبع المستخدم عبر مواقع ويب متعددة، مما يتيح على سبيل المثال إعلانات لمنتج شاهده المستخدم مؤخرًا على موقع مختلف تمامًا[١]، قد تسمح ميزات مواقع الشبكات الاجتماعية المضمنة في مواقع أخرى (مثل زر "Like") لموقع الشبكة الاجتماعية بتحديد المواقع التي زارها المستخدم[٢].

يقوم جهاز الكمبيوتر الخاص بك بعد ذلك بتخزين البيانات كملفات داخل ذاكرة التخزين المؤقت للمتصفح ويتم عمله من خلال خمس خطوات[٣]:

١- تقوم بزيارة موقع على شبكة الإنترنت
٢- يقوم خادم الويب بتمرير رسالة قصيرة إلى متصفح الويب الخاص بك
٣- يحفظ المتصفح هذه الرسالة في ملف بعنوان شيء مثل"Cookie.Txt"
٤- قمت بالنقر فوق صفحة موقع ويب أخرى
٥- يرسل متصفحك رسالة قصيرة "رجوع" إلى الخادم تكشف المزيد عما تبحث عنه

ولحسن الحظ ، فإن المبادئ هنا واضحة تمامًا. بفضل قوانين الخصوصية الدولية ، بما في ذلك اللوائح العامة[٤] لحماية البيانات(GDPR) للإتحاد الأوروبي وتوجيه

[1] Leenes, R., and E. Kosta (2015) "Taming the cookie monster with dutch law-a tale of regulatory failure", Computer Law & Review p. 317

[2] Krishnamurthy, B. & C.E. Wills (2009) **On the leakage of personally identifiable information via online social networks**, in Proceedings of the 2nd ACM workshop on Online social networks, ACM, pp. 7

[3] Cookie policy | Generate a CCPA and GDPR compliant cookie policy for your website, 2020, COOKIEBOT, available at: https://www.cookiebot.com/en/cookie-policy/Accessed on 10-1-2022

[4] General Data Protection Regulation, GDPR , 2016, available at: https://gdpr-info.eu/ Accessed on 10-1-2022

الخصوصية الإلكترونية ، يجب أن تقوم مواقع الويب بأمرين قبل أن تتمكن من تثبيت ملفات تعريف الارتباط فى أجهزة المستخدمين:

- أخبار المستخدم عن ملفات تعريف الارتباط التي يستخدمونها
- الحصول على موافقه المستخدم على استخدام ملفات تعريف الارتباط هذه.

والحقيقة ان اشتراط القوانين الحصول على موافقة المستخدمين أمر هام جدا لأن الأمر يتعلق بنوع المعلومات التي يمكن أن تجمعها ملفات تعريف الارتباط. يمكن لملفات تعريف الارتباط جمع ما يُعرف باسم "البيانات الشخصية" أو "المعلومات الشخصية". البيانات الشخصية ، بشكل عام ، هي أي معلومات يمكن استخدامها لتحديد هويتك أو تحديد أسرتك. الامثله تشمل: الاسم، عنوان البريد الإلكتروني، التفاصيل المالية، تفاصيل تسجيل الدخول

وتسمح قوانين الخصوصية العالمية للمستهلكين بما يلي:

- تقييد من لديه حق الوصول إلى المعلومات الشخصية
- إلغاء الموافقة على احتفاظ الشركة ببياناتك الشخصية في أي وقت
- رفض قبول ملفات تعريف الارتباط التسويقية وغيرها من ملفات تعريف الارتباط غير الضرورية التي تجمع معلومات التعريف الشخصية.

ثالثا: مواقع التواصل الإجتماعى

مما لا شك فيه أن مواقع التواصل الإجتماعى تعد من الاثار الإيجابية، حيث أصبح يسهل الاتصال و التواصل بين عدد غير محدود من الأفراد، فأصبح الشخص ليس وحيدا أو بعزلة حيث يمكنك التواصل مع الاخرين اينما كنت وفى أى وقت تريده، إلا أن ذلك له أثر بالتأكيد على فكرة العزلة وهو ما نعنية بفكرة انتهاك الخصوصية فى بعض الاحيان، لا يتعلق السؤال بالأسباب الأخلاقية لتقييد الوصول إلى المعلومات

فحسب، بل يتعلق أيضًا بالأسباب الأخلاقية لقصر الدعوات على المستخدمين لتقديم جميع أنواع المعلومات الشخصية.

يميل المستخدمون إلى تبادل بياناتهم الشخصية مقابل فوائد استخدام الخدمات، وتقديم هذه البيانات واهتمامهم مقابل الخدمات، بالإضافة إلى ذلك، قد لا يكون المستخدمون على دراية بالمعلومات التي يميلون إلى تقديمها، كما هو الحال في الحالة المذكورة أعلاه من زر "Like" على مواقع أخرى[١]، ويكمن السؤال الأكثر جوهرية في توجيه سلوك المستخدمين في المشاركة عندما تكون الخدمة مجانية، تكون البيانات مطلوبة كشكل من أشكال الدفع[٢].

رابعا: البيانات العملاقة Big Data

يقول الجنرال الأمريكي مايكل هايدن، الرئيس السابق لوكالة المخابرات المركزية CIA عندما قال "We kill people using Big data" "نحن نقتل الناس بأستخدام البيانات الضخمة".

ينشئ المستخدمون الكثير من البيانات عند الاتصال بالإنترنت. هذه ليست فقط البيانات التي تم إدخالها صراحة من قبل المستخدم ، ولكن أيضًا العديد من الإحصائيات حول سلوك المستخدم: المواقع التي تمت زيارتها ، والنقر فوق الروابط ، ومصطلحات البحث التي تم إدخالها ، وما إلى ذلك[٣].

---

[1] Gürses, S., A. Kundnani, & J. Van Hoboken (2016) **"Crypto and empire: the contradictions of counter-surveillance advocacy"**, Media, Culture & Society, p. 576

[2] Clay Calvert, Dan V. Kozlowski and Derigan Silver (2020) "**Mass Media Law**" 21st edition, MC GRAW HILL, p.299-303

[3] Stanford Encyclopedia of Philosophy, Privacy and Information Technology, 30 October 2019, available at: https://plato.stanford.edu/entries/it-privacy/ Accessed on 10-1-2022

قد تؤثر أيضًا على المستخدم في سياقات مختلفة تمامًا، على وجه الخصوص، يمكن استخدام البيانات الضخمة في تحديد سمات المستخدم وإنشاء أنماط من مجموعات نموذجية لخصائص المستخدم، والتي يمكن استخدامها بعد ذلك للتنبؤ بالاهتمامات والسلوك [١].

واعتمادًا على البيانات المتاحة، قد يتم عمل اشتقاقات أكثر حساسية، مثل التفضيل حسب اللون، كما يمكن أن تؤدي هذه الاشتقاقات بدورها إلى عدم المساواة في المعاملة أو التمييز عندما يمكن تعيين مستخدم إلى مجموعة معينة، حتى من الناحية الاحتمالية فقط، فقد يؤثر ذلك على الإجراءات التي يتخذها الآخرون. يمكن أيضًا استخدام التنميط من قبل المنظمات أو الحكومات المستقبلية المحتملة التي لديها تمييز ضد مجموعات معينة في أجندتها السياسية، من أجل العثور على أهدافها وحرمانها من الوصول إلى الخدمات، أو ما هو أسوأ[٢].

وفقًا لقانون حماية البيانات في الاتحاد الأوروبي ، يلزم الحصول على إذن لمعالجة البيانات الشخصية، ولا يمكن معالجتها إلا للغرض الذي تم الحصول عليها من أجله. وبالتالي ، فإن التحديات المحددة هي (أ) كيفية الحصول على إذن عندما لا يشارك المستخدم صراحة في معاملة (كما في حالة المراقبة)، و (ب) كيفية منع Function Creep "زحف الوظيفة" ، أي استخدام البيانات لأغراض مختلفة بعد جمعها[٣].

[1] Hildebrandt, M. & S. Gutwirth (eds.) (2008) **Profiling the European Citizen: Cross-disciplinary Perspectives**, Dordrecht: Springer Netherlands p.17

[2] Taylor, L., L. Floridi, and B. Van der Sloot (eds.) (2017) G**roup privacy: New challenges of data technologies** (Philosophical Studies Series: Vol. 126), Dordrecht: Springer.

[3] Stanford Encyclopedia of Philosophy, Privacy and Information Technology, 30 October 2019, available at: https://plato.stanford.edu/entries/it-privacy/ Accessed on 10-1-2022

خامسا: أجهزة المحمول

لا يمكن الاستغناء أبدا عن أجهزة المحمول، فوفقا لدراسات فى الولايات المتحدة الأمريكية لعام 2021 وجدت ان نسبة ٤٧% من المواطنين يستخدمون الهاتف المحمول قرابة ٦ ساعات يومية[١]، بينما أظهر برنامج Worldwide Quarterly Mobile Phone Tracker[٢] الذي أصدرته الشركة العالمية لأبحاث التكنولوجيا والخدمات الاستشارية ، أن سوق الهواتف الذكية في مصر نما بنسبة ١٠.٦٪ سنويا في عام ٢٠٢٠ إلى ١١.٩ مليون وحدة[٣].

نظرًا لأن المستخدمين يمتلكون بشكل متزايد أجهزة متصلة بالشبكة مثل الهواتف الذكية ، فإن الأجهزة المحمولة تجمع وترسل المزيد والمزيد من البيانات. تحتوي هذه الأجهزة عادةً على مجموعة من أجهزة استشعار توليد البيانات ، بما في ذلك GPS (الموقع) ، وأجهزة استشعار الحركة ، والكاميرات ، وقد تنقل البيانات الناتجة عبر الإنترنت أو شبكات أخرى، تحتوي العديد من هذه الأجهزة أيضًا على كاميرات يمكن استخدامها لالتقاط الصور[٤].

---

[1] How much time on average do you spend on your phone on a daily basis by STATISTA, 2021, available at: https://www.statista.com/statistics/1224510/time-spent-per-day-on-smartphone-us/ Accessed on 10-1-2022

[2] Worldwide Quarterly Mobile Phone Tracker, available at: https://www.idc.com/tracker/showproductinfo.jsp?containerId=IDC_P8397 Accessed on 10-1-2022

[3] Egypt Smartphone Market Records Healthy Growth Despite COVID-19, IDC, 25 May 2021, available at: https://www.idc.com/getdoc.jsp?containerId=prMETA47564421 Accessed on 10-1-2022

[4] Warnier, M., Dechesne, F., and Brazier, F.M.T. (2015) "**Design for the Value of Privacy**", in J. van den Hoven, P. Vermaas, I. van de Poel (eds.), Handbook of Ethics, Values, and Technological Design, Dordrecht: Springer, 431

سادسا: الحكومة الرقمية E Government

تتجه الحكومات والدول الان نحو التحول الرقمي، وهو شئ رائع فى مجال التماشى مع التكنولوجيا المعاصرة، إلا أن ذلك قد يكون له اثار أخرى سلبية على الخصوصية، فإذا نظرنا مثلا إلى خصوصية الناخب فى إجراء الانتخابات، تشترط معظم الدول إجراء الانتخابات بالاقتراع السري، لمنع شراء الأصوات والإكراه، إلا أن تكنولوجيا المعلومات قد تلعب دورًا في مراحل مختلفة من عملية التصويت، والتي قد يكون لها تأثير مختلف على خصوصية الناخب في مراكز الاقتراع، تحرص السلطات على أن يحافظ الناخب على خصوصية التصويت، لكن هذه المراقبة غير ممكنة عند التصويت عن طريق البريد أو عبر الإنترنت، ولا يمكن حتى تنفيذها بالوسائل التكنولوجية، حيث يمكن لأي شخص أن يراقب دائمًا أثناء تصويت الناخب. في هذه الحالة، الخصوصية ليست حقًا فحسب، بل هي أيضًا واجب، وتلعب تطورات تكنولوجيا المعلومات دورًا مهمًا في احتمالات أداء الناخب لهذا الواجب، فضلًا عن إمكانيات السلطات للتحقق من ذلك. بمعنى أوسع، قد تغير مبادرات الديمقراطية الإلكترونية الطريقة التي يُنظر بها إلى الخصوصية في العملية السياسية[1].

سابعا: المراقبة الإلكترونية – التجسس الإلكترونى

تُستخدم تكنولوجيا المعلومات لجميع أنواع مهام المراقبة. يمكن استخدامها لزيادة وتوسيع أنظمة المراقبة التقليدية وأنظمة الكاميرا الأخرى ، على سبيل المثال لتحديد أفراد معينين في الحشود ، باستخدام تقنيات التعرف على الوجوه ، أو لمراقبة أماكن

[1] Delaune, S., S. Kremer, & M. Ryan (2006) "**Coercion-resistance and receipt-freeness in electronic voting**", in the Proceedings of the 19th IEEE Computer Security Foundations Workshop, IEEE Computer Society Press, pages 28–39

معينة للسلوك غير المرغوب فيه. تصبح هذه الأساليب أكثر قوة عند دمجها مع تقنيات أخرى ، مثل مراقبة أجهزة إنترنت الأشياء[١].

إلى جانب زيادة أنظمة المراقبة الحالية ، تُستخدم تقنيات تكنولوجيا المعلومات والاتصالات في الوقت الحاضر بشكل أساسي في المجال الرقمي ، وعادة ما يتم تجميعها معًا تحت مصطلح "رأسمالية المراقبة"[٢]، تُستخدم وسائل التواصل الاجتماعي وأنظمة الإنترنت الأخرى لجمع كميات كبيرة من البيانات حول الأفراد – إما "طوعية" ، لأن المستخدمين يشتركون في خدمة معينة أو غير طوعي من خلال تجميع أنواع البيانات المتعلقة بالمستخدم بطريقة أقل شفافية[٣] . تُستخدم بعد ذلك تقنيات تحليل البيانات والتعلم الآلي لإنشاء نماذج تنبؤ للمستخدمين الفرديين يمكن استخدامها[٤].

[1] Motlagh, N. H., Bagaa, M., & Taleb, T. (2017) "UAV-based IoT platform: A crowd surveillance use case", IEEE Communications Magazine, 55(2): 128–134.

[2] Zuboff, S., (2019) **The age of surveillance capitalism: the fight for the future at the new frontier of power**, London: Profile Books.

[3] Gürses, S., A. Kundnani, & J. Van Hoboken (2016) **Crypto and empire: the contradictions of counter-surveillance advocacy", Media, Culture & Society**, 38(4): 576–590.

[4] Cadwalladr, C., (2019) Facebook's role in Brexit – and the threat to democracy. TED Talk available at:
https://www.ted.com/talks/carole_cadwalladr_facebook_s_role_in_brexit_and_the_threat_to_democracy

Accessed on 10-1-2022

المبحث الثانى

الخصوصية الرقمية فى المعاهدات والمواثيق الدولية

حظيت حقوق الإنسان بالاهتمام اللازم من طرف الدول، وذلك تطبيقا لإرادة شعوب العالم التي سعت بإلحاح للمطالبة بها، وقد تبلور هذا الاهتمام بصدور الإعلان العالمي لحقوق الإنسان عن الأمم المتحدة والذي جاء بجملة من الحقوق من بينها الحق في الخصوصية، واهتمت به جميع المنظمات الدولية عالمية أو إقليمية فعقدت بشأنه الاتفاقيات وكذا المؤتمرات الدولية[١].

إن مجمل المواثيق والاتفاقيات الدولية المتعلقة بحقوق الإنسان تعبر عن التزام الدول باحترامها لخصوصية الأفراد، هذا الالتزام يثبت من خلال مراجعة النصوص الداخلية للدول وتعديلها حسب نصوص المواثيق والاتفاقيات الدولية والتي تكون الدولة طرفا فيها، ولقد أصبح الآن معروفا بأن بعض أحكام المواثيق والاتفاقيات قد ارتقت وأصبحت قواعد عرفية، ما يعني التزام الدول بها حتى ولو كانت غير موقعة عليها[٢].

المطلب الأول – المعاهدات الدولية:

أولا: الإعلان العالمي لحقوق الإنسان[٣]

اهتمت الأمم المتحدة منذ نشأتها بإصدار الإعلانات الدولية و الاتفاقيات المتعلقة بحقوق الإنسان، وقد أسفر اجتماع لجنة حقوق الإنسان التابعة للأمم المتحدة عن اصدارها

[١] أحمد أبو الوفا (١٩٩٨) **الوسيط في القانون الدولي العام**، دار النهضة العربية، القاهرة، ١٩٩٨، ص٥٤٦

[٢] رزق سلمودي وليندا ربايعة وآخرون (٢٠١٧) الموقف المعاصر لقواعد القانون الدولي العام من الحق في الخصوصية في العصر الرقمي، **مجلة الجامعة العربية الأمريكية للبحوث**، مجلد٣، العدد٢، ص٩.

[3] Universal Declaration of Human Rights, 1948, available at: https://www.un.org/ar/universal-declaration-human-rights/ accessed on 22-12-2021

لقائمة دولية للحقوق و الحريات الأساسية للإنسان، أطلق عليها الإعلان العالمي لحقوق الإنسان و هذا بقرارها رقم ٢١٧ في دور الإنعقاد العادي الثالث في ١٠ ديسمبر ١٩٤٨

نصت المادة الخامسة أنه "لا يجوز تعريض أي إنسان للتعذيب أو للعقوبات أو للمعاملات القاسية أو الوحشية الماسة بالكرامة" و في هذه المادة يتضح الاهتمام بحرمة جسد الإنسان و الحفاظ على كرامته و شعوره".

وقد ورد كذلك في المادة التاسعة منه عدم جواز القبض على أي إنسان أو حبسه أو نفيه دون وجه حق، وتبين من هذه المواد اهتمام المجتمع الدولي بحرية الشخص و سلامة جسده[١].

وجاء فى المادة الثانية عشرة: "لا يعرض أى شخص لتدخل تعسفى فى حياته الخاصة أو مسكنه أو اسرته أو مراسلاته، أو شن حملات على سمعته وشرفه، ولكل فرد الحق فى طلب حماية القانون من مثل هذة الحملات والتدخلات"[٢].

يتضح من هذا النص أن الميثاق يهدف إلى اضفاء الحماية اللازمة لحق الإنسان في خصوصياته، و قد شمل الإعلان النص على احترام الحق في الحياة، والحق في الحرية، واحترام الشخص، و حرية التعبير والرأي، و الحق في الراحة و الترويح، و الحق في مستوى كاف للحياة[١].

---

[١] مصطفى فهمى الجوهري (١٩٩٠) **الشرعية الجنائية لقرينة البراءة**، القاهرة، دار الثقافة الجامعية ،ص ١١

[2] Phillips, Melanie (2011) from human rights to the EU, the tide's turning against the liberal thought police". Daily Mail (London). p 72 Available online at: https://www.dailymail.co.uk/debate/article-2010972/From-human-rights-EU-tides-turning-liberal-thought-police.html Accessed on 10-2-2022

[1] Alan Charles Raul, (2014) **The Privacy, Data Protection and Cyber security**, Business Law Research, Page 24, https://www.sidley.com/-

ثانيا: الاتفاقية الأوروبية للحقوق المدنية و السياسية لعام ١٩٦٦[1]

تميزت عن الإعلان العالمي باعتبارها التطبيق الفعلي لحماية حقوق الإنسان المدنية و السياسية، بفرض التزامات قانونية محددة على الدول بضرورة ما تضمنته من حقوق، بخلاف الإعلان الذي يقتصر على فرض التزامات أدبية باحترام ما تناوله من قواعد تتعلق بحقوق الإنسان. بحيث حرصت الاتفاقية على تأكيد كفالة الحريات العامة والأساسية، ولذلك فقد تعهدت الدول آنذاك بحماية الشعوب ضد التجاوزات غير الإنسانية، وأكدت هذه الاتفاقية احترام مبادىء عالمية سامية، منها الحق في الحياة، والحرية و المسكن و حرمة الحياة الخاصة، وحرية التفكير، والديانة، وحرية الرأي والتعبير[2].

تصدت هذه الاتفاقية لتبيان مضمون و حدود الحق في الحياة الخاصة، في مجموعة من النصوص التي عنيت بحماية الحق في الحياة الخاصة، في المادة **الثامنة** منها:

١- أن لكل شخص الحق في احترام حياته الخاصة و حياته العائلية و مسكنه ومراسلاته.

٢- لا يجوز للسلطة العامة التدخل في مباشرة هذا الحق إلا في الحدود التي يفرضها القانون، و بالقدر الضروري للحماية والأمن الوطني والأمن العام

/media/files/publications/2014/11/the-privacy-data-protection-and-cybersecurity-la__/files/united-states/fileattachment/united-states.pdf Accessed on 10-2-2022

[1] International Covenant on Civil and Political Rights, 1966, available at: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx accessed on 22-12-2021

[2] أحمد فتحى سرور (١٩٧٦) **الحماية الجنائية للحق في حرمة الحياة الخاصة**، القاهرة، دار النهضة العربية، ص٥٤٢

والمصلحة الإقتصادية للبلد، و كذا الدفاع عن النظام و الوقاية من الجرائم وحماية الصحة العامة أو الأخلاق أو حماية حقوق و حريات الآخرين[1].

من الملاحظ أن المادة سالفة الذكر قد أقرت احترام حق الخصوصية، و لكن لم تعطي تعريفا له، وقد انتهت لجنة الخبراء الخاصة بحقوق الإنسان في المجلس الأوروبي إلى عدم بيان ماهية الحق في الحياة الخاصة، وكان ذلك مقصودا وهو عدم الدخول في التفاصيل بشأن تحديد مضمون الحياة الخاصة، بحسبان أن ذلك الأمر من المسائل المتحركة، بمعنى أن المسائل قد يختلف مضمونها من دولة إلى أخرى. وحسنا ما فعلت الاتفاقية، حتى يمكن للقضاء و للفقه في كل دولة أن يستقل بتحديد مضمون حق الخصوصية، على أساس كل دولة.

نصت المادة السابعة عشر على:

١- لن يخضع أحد ما للتدخل العشوائي أو غير القانوني في خصوصيته، أو أسرته، أو مراسلاته، ولا يمكن أن يتعرض لهجوم غير قانوني على شرفه أو سمعته.

٢- يتمتع جميع الأفراد بالحق فى الحماية من مثل تلك الهجمات والتدخلات."

فهى ترفض أي تدخل للسلطة العامة في كيفية ممارسة هذا الحق من طرف صاحبه كما لا تجيز للسلطة ذاتها تقييد ممارسته، إلا إذا كانت النصوص التشريعية للدول

[1] (1) «-Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

(2) -Il ne peut y avoir ingérence d'une autorité publique dans l'éxercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui dans une société démocratique est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défence de l'ordre et à -- la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et liberté d'autrui»

المعنية تجيز لها ذلك، وبما لا يتعدى القدر الضروري لتحقيق الأغراض التي من أجلها سمح بالتدخل[١].

والعجيب أن الجمعية العامة للأمم المتحدة[٢] في قرارها رقم (١٦٧/٦٨) بتاريخ ١٩ نوفمبر ٢٠١٤ في الدورة التاسعة والستين بشأن «الحق في الخصوصية في العصر الرقمي» فى التوصية رقم ٩ نصت على "حث الدول الأطراف فى العهد الدولى الخاص بالحقوق المدنية والسياسية لعام ١٩٦٦ التي لا تولى الاهتمام اللازم للمعلومات المتعلقة بالأسلوب الذي تضمن به السلطات التشريعية أو الإدارية أو القضائية والأجهزة المختصة فى الدولة بشكل عام احترام هذا الحق وخاصة المادة ١٧" وجاءت التوصية العاشرة على الرغم من أهمية المادة ١٧ من العهد الدولى الخاص بالحقوق المدنية والسياسية لعام ١٩٦٦ التي تتناول حماية حق الخصوصية ، إلا أن المادة الرابعة من هذا العهد لم تدرج المادة ١٧ من ضمن المواد المحظور تقييدها كما هو الحال للمواد (٦ ، ٧ ، ٨ فقرة ١ و ٢ ، المادة ١١ ، ١٥، ١٦ ، ١٨ ،) مما قد يساهم فى تهميش حماية حق الخصوصية على المستويين الدولى والوطني.

لذلك فقد تعهدت الدول آنذاك بحماية الشعوب ضد التجاوزات غير الإنسانية، و أكدت هذه الاتفاقية احترام مبادىء عالمية سامية، منها الحق في الحياة، والحرية والمسكن وحرمة الحياة الخاصة، وحرية التفكير، والعقيدة، و حرية الرأي و التعبير[١]

---

[١] بارق منتظر عبد الوهاب لامي (٢٠١٧) جريمة انتهاك الخصوصية عبر الوسائل الإلكترونية في التشريع الأردني، **رسالة ماجستير غير منشورة**، جامعة الشرق الأوسط، الأردن، ص٧٦.

[2] General assembly, Human Rights Council , 30 June 2014, Twenty-seventh session, The right to privacy in the digital age Report of the United Nations High Commissioner for Human Rights , United Nations

[١] أحمد فتحى سرور (١٩٨٤) الحق في حرمة الحياة الخاصة، **مجلة القانون و الإقتصاد**، عدد ٥٤، ص٥٤٢

ثالثا: الميثاق العالمى لحقوق الطفل ١٩٨٩[1]

نصت المادة ١٦ على أنه:

١. لا يجوز أن يجرى أي تعرض تعسفي أو غير قانوني للطفل في حياته الخاصة أو أسرته أو منزله أو مراسلاته، ولا أي مساس غير قانوني بشرفه أو سمعته.
٢. للطفل حق في أن يحميه القانون من مثل هذا التعرض أو المساس.

أما عن الحماية الدولية عن طريق المؤتمرات فقد عقدت العديد من المؤتمرات منها ماهو دولي ومنها ماهو إقليمي كلها دعت إلى المحافظة على الخصوصية وحماية حرمة الحياة الخاصة نذكر منها مؤتمر طهران ١٩٦٨ ومؤتمر باريس ١٩٧٠ ومؤتمر هامبورج بألمانيا الغربية سنة ١٩٧٩ .

رابعا: المؤتمر الدولي الثاني عشر الخاص بحماية حقوق الإنسان في الإجراءات الجنائية .

عقدت الجمعية الدولية لقانون العقوبات هذا المؤتمر في هامبورج بألمانيا الغربية في الفترة من ١٢ إلى ٢٢ سبتمبر ١٩٧٩.

وقد تضمنت أعمال القسم الثالث من المؤتمر تحت عنوان حقوق الإنسان في الإجراءات الجنائية العديد من البحوث والتقارير، بحيث تم دراسة مجموعة من القضايا والمشكلات الأساسية في الإجراءات الجنائية، إذ أكد أنه من الضروري أن ترتكز إجراءات ووسائل الإثبات التي من شأنها تعطيل الحقوق الفردية والحريات إلى

[1] Convention on the Rights of the Child, 1989, available at: https://www.unicef.org/child-rights-convention

سند قانوني، وأن الأدلة المتحصلة من جراء التعذيب وإستخدام أساليب القسوة التي تم الحصول عليها بطريقة غير مشروعة تشكل إنتهاكا لحقوق الإنسان بشكل عام[١].

خامسا: اتفاقية حقوق الأشخاص ذوى الإعاقة لسنة ٢٠٠٦[٢]

نصت المادة ٢٢ :احترم الخصوصية

١- لا يجوز تعريض أي شخص ذي إعاقة، بصرف النظر عن مكان إقامته أو ترتيبات معيشته، لتدخل تعسفي أو غير قانوني في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته أو أي نوع آخر من وسائل الاتصال التي يستعملها، ولا للتهجم غير المشروع على شرفه وسمعته. ولجميع الأشخاص ذوي الإعاقة الحق في حماية القانون لهم من أي تدخل أو تهجم من هذا القبيل.

٢- تقوم الدول الأطراف بحماية خصوصية المعلومات المتعلقة بالشؤون الشخصية للأشخاص ذوي الإعاقة وبصحتهم وإعادة تأهيلهم على قدم المساواة مع الآخرين.

---

[١] ممدوح خليل بحر، (2017) **حماية الحياة الخاصة في القانون الجنائي دراسة مقارنة** ،دار النهضة العربية، ص ٩٩ ص إلى ١٠١.

[2] Convention on the Rights of Persons with Disabilities, United Nations, 2006, available at: https://www.ohchr.org/ar/HRBodies/CRPD/Pages/ConventionRightspersonsWithDisabilities.aspx

accessed on 30-12-2021

المطلب الثانى – الخصوصية الرقمية فى المواثيق الإقليمية:

الإتفاقية الأوربية لحقوق الإنسان[١]

قد كانت ومازات الإتفاقية الأوربية لحقوق الإنسان فى ١٩٥٠ مصدر حقوق الإنسان في أوروبا وقد نصت المادة الثامنة من هذه الإتفاقية على:

١. لكل شخص الحق في إحترام حياته الخاصة والعائلية ومسكنه ومراسلاته.
٢. لا يجوز للسلطة العامة التدخل في مباشرة هذا الحق إلا إذا كان هذا التدخل ينص عليه القانون، ويعد إجراءا ضروريا."

كما أنشأت هذه الإتفاقية إستنادا إلى أحكام المادة ١٩ منها كل من اللجنة الأوربية لحقوق الإنسان والمحكمة الأوربية لحقوق الإنسان، وكان لهاتين الهيئتين دورا هاما في حماية حق الخصوصية خاصة المحكمة التي أنزلت قرارات كل من الإتفاقية واللجنة الأوربية لحقوق الإنسان بكل جرأة فأضحت مثال يحتدى به في باقي دوب العالم خارج أوروبا.

المجلس الأوروبي: توصيات رقم (99) ٥ حول حماية الخصوصية على الإنترنت [١].

حددت هذه الإرشادات مبادئ ممارسة الخصوصية العادلة للمستخدمين وخدمة الإنترنت لمقدمي الخدمة

قدمت العديد من النصائح للمستخدمين ولمقدمى الخدمة:

---

[1] European convention on human rights, 1920, available at: https://www.echr.coe.int/documents/convention_eng.pdf Accessed on 22-12-2021

[1] Council of Europe, Recommendation No. R (1999)5 on the protection of privacy on the Internet, available at: https://www.coe.int/en/web/cdcj/recommendations-resolutions-guidelines

حيث تناولت نصائح المستخدمين:

١. الإنترنت ليس امنا، وعلى كل مستخدم اتخاذ الطرق والإساليب لحماية بياناته الشخصية.
٢. التذكير على أن كل معاملة يقوم المستخدم بها ، وكل موقع يزوره على الإنترنت يترك آثارا.
٣. يجب على المستخدم ألا يقدم لمزود خدمة الإنترنت الخاص به، أو أي شخص آخر، البيانات التي لا تكون ضرورية للوفاء بالغرض المحدد الذي تم إخطار المستخدم به.
٤. الحذر من المواقع التي تطلب بيانات أكثر مما هو ضروري للوصول إلى الموقع أو من أجل إجراء معاملة.
٥. كما أكدت على أن البريد الإلكترونى يعد من البيانات الشخصية.
٦. يجب الأطلاع على مخاطر الخصوصية والأمان على الإنترنت بالإضافة إلى الطرق المتاحة لتقليل مثل هذه المخاطر.

وتناولت نصائح مقدمى الخدمة استخدام الإجراءات المناسبة والتكنولوجيات المتاحة لحماية خصوصية المستخدمين، وإعلامهم بمخاطر الخصوصية و بالوسائل التقنية التي قد يستخدمونها بشكل قانوني لتقليل المخاطر الأمنية للبيانات والاتصالات، كما أكد على أن مقدم الخدمة يجب ألا يقرأ أو يعدل أو يحذف الرسائل المرسلة للآخرين، والا يجمع أو يعالج أو يخزن البيانات حول المستخدمين فقط عند الضرورة الواضحة والمحددة و أغراض مشروعة، وألا يستخدم البيانات لأغراض ترويجية أو تسويقية خاصة به الا بعد موافقة الشخص المعنى بالبيانات وهو المستخدم.

الاتفاقية الأمريكية لحقوق الإنسان ١٩٦٩[١].

وقعت هذه الاتفاقية في مدينة سان جوزيه بدولة كوستاريكا في شهر نوفمبر سنة ١٩٦٩ أثناء انعقاد مؤتمر حقوق الإنسان، و قد أقرت هذه الاتفاقية حقوق الشخص الأساسية، و أكدت على أن الفرد هو أساس هذه الحقوق، وتهدف هذه الاتفاقية إلى حماية الشخص و تمتعه بالأمن و الآمان.

و من أهم موضوعاتها، ما تناولته في الفصل الأول من القسم الأول مبدأين: أولهما يتعلق بالتزام الدول الأعضاء في الاتفاقية باحترام الحقوق الواردة فيها، و تسهيل ممارسة الأشخاص للحقوق، بغض النظر عن لونهم، و لغتهم، و ديانتهم. أما المبدأ الثاني يتضمن التزام الدولة بتعديل التشريعات والنظام القانوني المعمول به داخلها، حتى يتطابق مع ما جاء في الاتفاقية [١].

نصت المادة الحادية عشرة على أنه "لكل إنسان الحق في أن يحترم شرفه و تصان كرامته" ثم جاء في الفقرة الثانية من نفس المادة "لا يجوز أن يتعرض أحد لتدخل تعسفي في حياته الخاصة أو شؤون أسرته أو منزله أو مراسلاته، و لا أن يتعرض لاعتداءات غير مشروعة على شرفه أو سمعته،" والفقرة الثالثة "لكل إنسان الحق في أن يحميه القانون من مثل ذلك التدخل أو تلك الاعتداءات"

---

[1] American Convention on Human Rights, 1969, available at: https://treaties.un.org/doc/publication/unts/volume%201144/volume-1144-i-17955-english.pdf

Accessed on 22-12-2021

[١] عبدالعزيز محمد سرحان (دون تاريخ نشر) **الاتفاقية الأوروبية لحماية حقوق الإنسان**، القاهرة، دار النهضة العربية، ص ٢٥٥

الميثاق الإفريقي لحقوق الإنسان و الشعوب[١] ١٩٨١

اهتمت الدول الإفريقية هي الأخرى بموضوع حقوق الإنسان، و على هذا دعت منظمة الوحدة الإفريقية إلى عقد دورتها الثامنة عشرة في مدينة نيروبي (كينيا) عام ١٩٨١

وفى هذه الدورة وافقت الدول بالإجماع على الميثاق الإفريقي لحقوق الإنسان و الشعوب[٢].

نصت المادة الرابعة " لا يجوز انتهاك حرمة الإنسان. ومن حقه احترام حياته وسلامة شخصه البدنية والمعنوية. ولا يجوز حرمانه من هذا الحق تعسفا". ونصت المادة الثانية عشرة على أن "للحياة الخاصة لكل إنسان حرمة، و تشمل خصوصيات الأسرة، و حرمة المسكن، و سرية المراسلات، و غيرها من سبل المخابرة الخاصة، و لا يجوز المساس بها إلا في حدود القانون".

ونصت المادة الثامنة على أن حرية العقيدة وممارسة الشعائر الدينية مكفولة، ولا يجوز تعريض أحد لإجراءات تقييد ممارسة هذه الحريات، مع مراعاة القانون والنظام العام.

بعد الاطلاع على الميثاق الأفريقي لحقوق الإنسان والشعوب ، وقعت جمهورية مصر العربية على الميثاق المذكور في ١٦ نوفمبر ١٩٨١ مع تحفظات [١].

---

[1] The African Charter on Human and Peoples' Rights, 1981, available at: http://hrlibrary.umn.edu/arab/a005.html

Accessed on 30-12-2021

[٢] أحمد حلمي السيد، **الحماية الجنائية لحق الإنسان في حرمة حياته الخاصة**، القاهرة، دار النهضة العربية، ١٩٨٣ ،ص ٦١ .

[١] وبعد الموافقة على جميع أحكام الميثاق الأفريقي لحقوق الإنسان والشعوب بموافقة مجلس الشعب مع التحفظ على تطبيق المادة ٨ والفقرة ٣ من المادة ٨ والفقرة ٣ من المادة ١٨ وفق الشريعة الإسلامية و أنه فيما يتعلق بجمهورية مصر العربية ، ينبغي [حصر] حكم الفقرة الأولى من المادة ٩ في المعلومات التي يمكن الحصول عليها في حدود القوانين واللوائح المصرية

الميثاق الأفريقي لحقوق ورفاهية الطفل ١٩٩٠[1]

نصت المادة العاشرة على حماية الخصوصية، لا يجوز تعريض أي طفل لتدخل تعسفي أو غير قانوني في خصوصيته أو منزل أسرته أو مراسلاته ، أو الاعتداء على شرفه أو سمعته ، بشرط أن يكون للوالدين أو الأوصياء القانونيين الحق في ذلك ممارسة الإشراف المعقول على سلوك أطفالهم. للطفل الحق في حماية قانون ضد مثل هذا التدخل أو الهجمات.

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[2] **٢٠١٠.**

صدرت الاتفاقية بالقاهرة في ٢١ ديسمبر ٢٠١٠، دخلت حيز التنفيذ في ٧ فبراير ٢٠١٤، بعد مصادقة ٧ دول، كما تضم الاتفاقية ١١ دولة

والجدير بالذكر أن مصر قد وقعت على الإتفاقية وفقا بالقرار الجمهوري رقم ٢٧٦ لسنة ٢٠١٤[1]

نصت المادة الثالثة على مجالات تطبيق الإتفاقية على جرائم تقنية المعلومات في الحالات الآتية:

١. عندما ترتكب في أكثر من دولة.

---

[1] African Charter on the Rights and Welfare of the Child 1990, available at: https://www.achpr.org/public/Document/file/English/achpr_instr_charterchild_eng.pdf

[2] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات،2010 متوفر على : أخر تاريخ دخول ١١ يناير ٢٠٢٢

https://ar.wikisource.org/wiki/%D8%A7%D9%84%D8%A7%D8%AA%D9%81%D8%A7%D9%82%D9%8A%D8%A9_%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9_%D9%84%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9_%D8%AC%D8%B1%D8%A7%D8%A6%D9%85_%D8%AA%D9%82%D9%86%D9%8A%D8%A9_%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA

[1] الموافقة على انضمام مصر إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، بالقرار الجمهوري رقم ٢٧٦ لسنة ٢٠١٤

٢. عندما ترتكب في دولة ويكون معداً ومخططاً وموجهاً أو تحت إشراف دولة أخرى أو ولايات أخرى.
٣. عند ارتكابها في دولة بتورط جماعة إجرامية منظمة تمارس أنشطتها في أكثر من دولة.
٤. عندما ترتكب في دولة ما وكانت لها عواقب وخيمة في دولة أخرى أو دول أخرى.

نصت الاتفاقية على حماية سيادة الدول من خلال التزام كل دولة طرف بمبدأي المساواة في السيادة الإقليمية للدول وعدم التدخل في الشؤون الداخلية للدول الأخرى. ولا يوجد فى هذه الاتفاقية ما يجيز لدولة طرف أن تمارس في إقليم دولة أخرى الولاية القضائية أو الوظائف التي تعتبر ممارستها حصريًا حقًا لسلطات تلك الدولة الأخرى بموجب قانونها الداخلي.

أسردت الإتفاقية العديد من الجرائم فى الفصل الثانى من المادة الخامسة الى المادة الحادية والعشرون وجاءت الجرائم : جريمة الوصول غير المشروع، جريمة الاعتراض غير المشروع، جريمة إتلاف أو إخفاء أو تعديل بيانات تقنية المعلومات، سوء استخدام تقنية المعلومات، جريمة التزوير، جريمة الاحتيال، جريمة حيازة المواد الإباحية، جريمة القمار، جريمة الاستغلال الجنسي، الجرائم ضد الخصوصية، الجرائم المتعلقة بحق المؤلف والحقوق المجاورة، جريمة الاستخدام غير المشروع لأدوات الدفع الإلكترونية.

وما يهمنا على سبيل الخصوص هو الجرائم ضد الخصوصية حيث نصت المادة الرابعة عشرة: جريمة الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات.

جاء فى المادة الحادية والعشرون: تشديد العقوبات على الجرائم التقليدية المرتكبة بواسطة تقنية المعلومات، والحقيقة أن لنا بعض التحفظات على هذه المادة تشديد غير مفهوم وغامض ولا يقترن فعلياً بالضرر المترتب على الجريمة، بقدر ارتباطه بأداة الجريمة نفسها. المفترض أن الجريمة واحدة حتى وإن اختلفت الأدوات المستخدمة في تنفيذها، ولا يوجد ضرورة لتشديد عقوبة على جريمة واحدة عند اختلاف أداة ارتكابها. وهذا ما قالته المحكمة الدستورية العليا في الطعن رقم ٣٣ لسنة ١٦ قضائي "أن شخصية العقوبة وتناسبها مع الجريمة ، مرتبطتان بالشروط التي يعد بها الشخص قانوناً مسئولاً عن ارتكابها وهو ما يعني أن الأصل في العقوبة هو معقوليتها فلا يكون التدخل فيها إلا بقدر نائياً بها عن أن تكون إيلاماً غير مبرر يؤكد قسوتها في غير ضرورة[١].

وفى المادة ٢٢ احتوت على لفظ غامض تماماً "أية جرائم أخرى" وهو لفظ يمكن من خلاله تجريم أي نشاط رقمي، حيث أن المادة ألزمت الدول الأعضاء بتبني التشريعات والإجراءات الضرورية لتحديد الصلاحيات والإجراءات الواردة بالاتفاقية في قانونها الداخلي،وتطبيقها على الجرائم المنصوص عليها في فصل التجريم، ثم تُزيد المادة نطاق تطبيق الإجراءات لتشمل "أية جرائم أخرى ترتكب بواسطة تقنية المعلومات" وكالعديد من بنود الاتفاقية، لم يتم تعريف أو تحديد أو وضع إطار"للجرائم الأخرى".

إن الاتفاقية تناقض الدستور المصري وما استقرت علية المحكمة الدستورية العليا. على سبيل المثال في الفصل الثاني، تتناول الاتفاقية الأحكام الإجرائية، والتي تحتوي بنود هذا الفصل على ألفاظ غامضة وغير مُحكمة وإجَازة إجراءات واسعة في جمع البيانات والمعلومات، لا تتناسب مع مبادئ حق الخصوصية وسرية البيانات، ولم

[١] المحكمة الدستورية العليا ، الطعن رقم ٣٣ ، لسنة ١٦ قضائية ، تاريخ الجلسة ٣-٢-١٩٩٦ ، مكتب فني ٧ ، رقم الجزء ١ ، رقم الصفحة ٣٩٣

يحتوى على نص واضح ومباشر يُحافظ على حق الفرد في الحفاظ على سرية بياناته الشخصية، وحقه في إعلامه بالإجراءات التي يتم اتخاذها بشأن جمع بيانات ومعلومات حول نشاطه الرقمي، أو يعطيه حقه في الاعتراض على هذه الإجراءات.

وفيما يتعلق بالمادة ٢٣ بإلزام كل دولة بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة، ولم تضع الضمانات الضرورية كاستصدار إذن قضائى مسبب أو تحدد المدة الزمنية لهذا الاحتفاظ.

كما ان الفصل الرابع من الاتفاقية يُنظم التعاون القانوني والقضائي بين الدول أطراف الاتفاقية، واستمراراً لاستخدام المُصطلحات غير المُحكمة والفضفاضة فقد تم استخدام مصطلحي "المصالح العليا للدولة" و"الجرائم السياسية" وهي فعليا لم يتم وضع تعريف واضح لها ضمن الوثيقة، كما أن الفصل بالكامل لم يشترط بشكل واضح وصريح ضرورة حماية البيانات في حالة مشاركة البيانات بين الدول.

وإجمالا يرى الباحث أن بنود الاتفاقية لم تراعي تناسب التجريم مع التطور التكنولوجي في مجال الاتصالات وتكنولوجيا المعلومات

مشروع الميثاق العربي لحقوق الإنسان ٢٠٠٤[١]

بناء على توصية اللجنة العربية الدائمة لحقوق الإنسان في اجتماعها الخامس، أصدر مجلس الجامعة العربية قراره بتاريخ ١٥ سبتمبر ١٩٧٠ الذي دعا فيه الأمانة العامة إلى عقد ندوة من الخبراء لوضع ميثاق عربي لحقوق الإنسان نابعا من الإعلان

[١] الميثاق العربي لحقوق الإنسان، اعتمد من قبل القمة العربية السادسة عشرة التي استضافتها تونس ٢٣ مايو/أيار ٢٠٠٤ http://hrlibrary.umn.edu/arab/a003-2.html اخر تاريخ دخول ١٢-١-٢٠٢٢

العالمي لحقوق الإنسان، يراعي الظروف التاريخية و التراث الحضـــاري و الروحـــي والثقافي للعالم العربي[١].

رغم المراحل العديدة التي مر بها المشروع، لم يدخل الميثاق العربي لحقوق الإنســـان ١٩٩٤ حيز النفاذ حيث لم تصادق عليه أية دولة عربية، وبمقارنته بالاتفاقيات العالمية لحقوق الإنسان، نجد أن هذا الميثاق لم يكن يضيف جديدا، فهو لم يقرر حقوقا جديـــدة أو رقابة مميزة. ومن أهم المراحل التي مر بها هذا المشروع الميثاق هي إعادة النظر فيه و تحديثه، حيث صدر قرار مجلس الجامعة رقم ٦٠٨٩ فـــي ١٢/مـــارس/٢٠٠١ ببدء وضع مشروع حديث[٢].

أما بشأن حق الخصوصية فقد نصت عليه المادة السادسة عشرة فيما يتعلق بضـــمان المتهم خلال إجراءات التحقيق، و هذا في الفقرة الثامنة من المـــادة المـــذكورة[١]. كمـــا نصت المادة الواحدة و العشرون من الميثاق على أنه:

---

[١] قرار مجلس الجامعة العربية، رقم ٢٦٦٨ ،في دور إنعقاده العادي الرابع و الخمسين

[٢] وائل أحمد علام (٢٠٠٥) **الميثاق العربي لحقوق الإنسان، دراسة حول دور الميثاق في تعزيز حقوق الإنسان في جامعة الدول العربية**، دار النهضة العربية،ص ٧ -١٢

[١] كل متهم بريء حتى تثبت إدانته بحكم بات وفقا للقانون، على أن يتمتع خلال إجراءات التحقيق والمحاكمة بالضمانات الآتية:

-1إخطاره فورا وبالتفصيل وبلغة يفهمها بالتهم الموجهة إليه.

-2إعطاؤه الوقت والتسهيلات الكافية لإعداد دفاعه والسماح له بالاتصال بذويه.

-3حقه في أن يحاكم حضوريا أمام قاضيه الطبيعي وحقه في الدفاع عن نفسه شخصيا أو بواسطة محام يختاره بنفسه ويتصل به بحرية وفي سرية.

-4حقه في الاستعانة مجاناً بمحام يدافع عنه إذا تعذر عليه القيام بذلك بنفسه أو إذا اقتضت مصلحة العدالة ذلك، وحقه إذا كان لا يفهم أو لا يتكلم لغة المحكمة في الاستعانة بمترجم من دون مقابل.

-5حقه في أن يناقش شهود الاتهام بنفسه أو بواسطة دفاعه، وحقه في استحضار شهود النفي بالشروط المطبقة في استحضار شهود الاتهام.

-6حقه في ألا يجبر على الشهادة ضد نفسه أو أن يعترف بالذنب.

-7حقه إذا أدين بارتكاب جريمة في الطعن وفقاً للقانون أمام درجة قضائية أعلى.

١. لا يجوز تعريض أي شخص على نحو تعسفي أو غير قانوني للتدخل في خصوصياته أو مراسلاته أو شؤون أسرته أو بيته أو التشهير بمس شرفه أو سمعته.
٢. من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس

كما نصت فى المادة ٣٠

١. لكل شخص الحق في حرية الفكر والعقيدة والدين ولا يجوز فرض أية قيود عليها إلا بما ينص عليه التشريع النافذ.
٢. لا يجوز إخضاع حرية الإنسان في إظهار دينه أو معتقده أو ممارسة شعائره الدينية بمفرده أو مع غيره إلا للقيود التي ينص عليها القانون والتي تكون ضرورية في مجتمع متسامح يحترم الحريات وحقوق الإنسان لحماية السلامة العامة أو النظام العام أو الصحة العامة أو الآداب العامة أو لحماية حقوق الآخرين وحرياتهم الأساسية

إعلان القاهرة لحقوق الإنسان في الإسلام ١٩٩٠[١].

أصدر المؤتمر الإسلامي التاسع عشر لوزراء الخارجية في القاهرة في الفترة ما بين ٣١ يوليو إلى ٤ أغسطس ١٩٩٠ قراره بالموافقة على إعلان القاهرة عن حقوق الإنسان في الإسلام.

٨- وفي جميع الأحوال للمتهم الحق في أن تحترم سلامته الشخصية وحياته الخاصة.

[١] إعلان القاهرة لحقوق الإنسان في الإسلام ، القاهرة، ٥ أغسطس ١٩٩٠، متوفر على

https://www.nhrc-qa.org/wp-content/uploads/2014/01/%D8%A5%D8%B9%D9%84%D8%A7%D9%86-%D8%A7%D9%84%D9%82%D8%A7%D9%87%D8%B1%D8%A9-%D9%84%D8%AD%D9%82%D9%88%D9%82-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86-%D9%81%D9%8A-%D8%A7%D9%84%D8%A5%D8%B3%D9%84%D8%A7%D9%85.pdf

وصف قرار الإعلان بأنه يشكل إرشادات عامة للدول الأعضاء في مجال حقوق الإنسان، و كان هذا القرار قد صدر بعد أن إطلع المؤتمر على مراحل إعداد مشروع ميثاق الدول العربية و على تقرير اجتماع لجنة الخبراء القانونيين [١].

ورد حق الخصوصية فى المادة الثامنة عشرة على الوجه التالى:

١- لكل إنسان الحق في أن يعيش آمنا على نفسه ودينه وأهله وعرضه وماله.
٢- للإنسان الحق في الاستقلال بشؤون حياته الخاصة في مسكنه وأسرته وماله واتصالاته، ولا يجوز التجسس أو الرقابة عليه أو الإساءة إلي سمعته ويجب حمايته من كل تدخل تعسفي.
٣- للمسكن حرمته في كل الأحوال ولا يجوز دخوله بغير إذن أهله أو بصورة غير مشروعة، ولا يجوز هدمه أو مصادرته أو تشريد أهله منه.

المبحث الثالث – اللائحة العامة لحماية البيانات (GDPR) وإتفاقية بودابست:

الفرع الأول: اللائحة العامة لحماية البيانات[١] GDPR General Data Protection Regulation

دخلت اللائحة العامة لحماية البيانات GDPR حيز التنفيذ يوم ٢٥ مايو2018 وتنطبق على جميع المؤسسات داخل وخارج الاتحاد الأوروبي التي تتعامل مع بيانات سكان منطقة الاتحاد الأوروبي وتعالجها. ويكمن الغرض من اللائحة في تقوية حماية البيانات ومنح الأشخاص قدرا أكبر من التحكم في الطريقة التى يتم بها استخدام

[١] يوسف الشيخ يوسف، (١٩٩٣) **حماية الحق في حرمة الأحاديث الخاصة**، القاهرة، دار النهضة العربية،ص ٧٦-٧٧

[1] General Data Protection Regulation, European Parliament and Council of the European Union, L119, 4 May 2016, available at: https://gdpr-info.eu/Accessed on 14-1-2022

وتخزين ومشاركة معلوماتهم الشخصية من قبل المؤسسات إلى الشركات التي لها حق الوصول إليها، بدءا من أصحاب العمل ووصولا إلى الشركات التى يشترى هؤلاء الأشخاص أو يستخدمون منتجاتها وخدماتها. كما تفرض GDPR على المؤسسات تصميم وتنفيذ عناصر فنية وتنظيمية للتحكم في أمن المعلومات لتفادي فقدان البيانات، أو تسريبها، أو الاستخدامات الأخرى غير المصرح بها للبيانات.

اللائحة العامة لحماية البيانات (GDPR) هى أحد قوانين الاتحاد الأوروبي مع قواعد إلزامية لكيفية استخدام المؤسسات والشركات للبيانات الشخصية بطريقة نزيهة. وتعني البيانات الشخصية أي معلومات يمكن أن تحدد بشكل مباشر أو غير مباشر شخصًا على قيد الحياة. الاسم ورقم الهاتف والعنوان أمثلة في الكتاب المدرسي للبيانات الشخصية. الاهتمامات والمعلومات حول عمليات الشراء السابقة والصحة والسلوك عبر الإنترنت تعتبر أيضًا بيانات شخصية لأنها قد تحدد هوية الشخص. تعني معالجة البيانات جمع البيانات وهيكلتها وتنظيمها واستخدامها وتخزينها ومشاركتها والكشف عنها ومحوها وإتلافها. يجب على كل مؤسسة تعالج البيانات الشخصية (وهي كل مؤسسة لديها موظفين وعملاء) التأكد من أن البيانات الشخصية التي تستخدمها تفي بمتطلبات اللائحة العامة لحماية البيانات (GDPR). المتطلبات الرئيسية للائحة العامة لحماية البيانات هي كما يلي:

- يسري القانون العام لحماية البيانات (GDPR) في جميع الدول الأعضاء في الاتحاد الأوروبي
- يجب أن يتوافق استخدام البيانات الشخصية مع المبادئ الصديقة للنزاهة
- يجب أن يكون استخدام البيانات الشخصية قانونيًا
- يجب أن يحترم استخدام البيانات الشخصية حقوق الأفراد
- يجب الإبلاغ عن انتهاكات البيانات الشخصية في غضون ٧٢ ساعة

- الشركات مسؤولة عن مورديها
- حجم العقوبات كبير. قد تواجه المنظمات التي تنتهك القانون عقوبات تصل إلى المبلغ الأعلى البالغ ٤٪ من مبيعاتها العالمية (آخر ١٢ شهرًا) أو ٢٠ مليون يورو.

الفرع الثانى: إتفاقية بودابست[1] لعام ٢٠٠١

اتفاقية بودابست هي المعاهدة الدولية الوحيدة الملزمة بشأن الجرائم السيبرانية، وقد صادقت ٦٥ دولة على الاتفاقية، تعمل اتفاقية بودابست على مواءمة قوانين الدول الأعضاء بشأن الجرائم السيبرانية من خلال تعاون الحوار الدولى، مما يسهل عليهم التعاون في التحقيقات الجنائية التي تنطوي على أدلة إلكترونية. تحدد الاتفاقية السياسات الأساسية ، والأمر متروك لكل دولة لتقرر بنفسها كيفية تنفيذها لتمكين استجابة فعالة في سياق الترتيبات الدستورية الخاصة بها ، وإعدادات الخصوصية والسياسات الأمنية.

كما تتطلب الاتفاقية من الدول الأعضاء أن يكون لديها قوانين محلية تحمي حقوق الإنسان والحريات ، وأن يكون لها إشراف قضائي أو غيره من الإشراف المستقل على استخدام الإجراءات والسلطات، يتم التعاون في تحقيقات محددة من خلال النظام الراسخ للمساعدة القانونية المتبادلة باستخدام الصلاحيات والإجراءات المنسقة المنصوص عليها في اتفاقية بودابست. تلتزم الدول الأعضاء بالتعاون إلى أقصى حد ممكن في التحقيقات ، وتوفير نقطة اتصال على مدار الساعة طوال أيام الأسبوع لطلبات التعاون العاجلة

[1] Convention on Cybercrime, Budapest, 23.XI.2001, European Treaty Series - No. 185, available at: https://rm.coe.int/1680081561 Accessed on 14-1-2022

ميزت الاتفاقية بين نوعين من الجرائم السيبرانية:

١. **الجريمة السيبرانية البحتة** Pure Cybercrime: فعل إجرامي يُرتكب من خلال استخدام تقنيات المعلومات والاتصالات أو الإنترنت ، حيث يكون الكمبيوتر أو الشبكة هدفًا للجريمة. من الأمثلة على الجرائم الإلكترونية البحتة نشر برامج ضارة مثل الفيروسات.
٢. **الجرائم الإلكترونية** Cyber-enabled Crime: أي عمل إجرامي يمكن أن يُرتكب بدون تكنولوجيا أو الإنترنت ، ولكن يتم دعمه أو تسهيله أو تصعيده على نطاق واسع باستخدام التكنولوجيا. وهذا يشمل مجموعة من الجرائم الخطيرة والمنظمة ، مثل الاحتيال عبر الإنترنت ، وتوزيع مواد استغلال الأطفال ، والإرهاب

تعمل الاتفاقية أيضًا على مواءمة السلطات القانونية التي تستخدمها الدول الأعضاء لتأمين الأدلة الإلكترونية للجرائم الخطيرة بما في ذلك جرائم القتل واستغلال الأطفال والاعتداءات الجنسية وجميع الجرائم الخطيرة الأخرى

المبحث الثالث:

الخصوصية الرقمية فى القانون الدولى

يقوم النظام الدولي أساسا على احترام و تعزيز حقوق الإنسان و الحريات الأساسية لجميع الناس دون تمييز بسبب الجنس، أو اللغة، أو الدين، ولا فرق بين الرجال و النساء. ومن أهم مبادئه الاستقرار و السلام والعدل والأمن[١].

هناك كثير من الدول يربطون مفهوم الخصوصية بمفهوم حماية البيانات وهو ما يضع الخصوصية ضمن اطار الحق في حماية البيانات الخاصة، وفي خارج نطاق هذا المفهوم، فإن الخصوصية ظهرت كوسيلة لتحديد الخطوط الفاصلة بين حق الفرد المطلق وبين حق المجتمع بالتعرض لشؤونه، وفى أنظمة قانونية أخرى كانت الخصوصية هي الحرية في مواجهة كل اعتداء أو انتهاك[٢].

في يونيو عام ٢٠١٣ فجر إدوارد سنودن Edward Snowden[٣] ،وهو متعاقد تقنى سابق مع وكالة الأمن القومي الأمريكى، فضيحة التنصت العالمى واختراق الخصوصية،حيث قام بتسريب وثائق سرية للغاية لوكالة الأمن القومي الأمريكى وشركائها الدوليين، ونشرتها جريدة الجارديان ,والتى أجرت معه الحوار فى هونج

---

[١] طارق عزت رخا (٢٠٠٥) **قانون حقوق الإنسان**، القاهرة، دار النهضة العربية للطباعة و النشر، ط1 ، ص٦

[٢] أسامة عبد الله قايد، (١٩٩٢) **الحماية الجنائية للحياة الخاصة وبنوك المعلومات**، دار النهضة العربية، القاهرة، ط٢، ص١١

[3] Glenn Greenwald, Ewen MacAskill and Laura Poitras, Edward Snowden: the whistleblower behind the NSA surveillance revelations, The Guardian Newspaper, Tue 11 Jun 2013, available at: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Accessed on 30-12-2021

كونج، وجريدة الواشنطن بوست وغيرها من الصحف العالمية،والتى كشفت عن تدخلهم بصورة واسعة النطاق فى التنصت من خلال الإنترنت، ومراقبة الهواتف على نطاق عالمي عبر برنامج التجسس بريسم PRISM[١] وقد أثارت هذه التسريبات النقاش بشأن القيود المفروضة على المراقبة الشاملة وعما إذا كانت قوانين الخصوصية تواكب التقدم التكنولوجي، وخاصة وأن القواعد الدولية لحقوق الإنسان والتى تحمي حق الخصوصية قد صيغت قبل ظهور الإنترنت[٢].

المطلب الأول – تقارير الجمعية العامة للأمم المتحدة لعام ٢٠١٣:

ونظرا لهذه المخاوف، في ديسمبر ٢٠١٣ قد اعتمدت الجمعية العامة[٣] وبدون تصويت القرار (١٦٧/٦٨) بشأن حق الخصوصية في العصر الرقمي وفي هذا القرار، أكدت الجمعية العامة فى المادة ٣ للمرة الأولى أن الحقوق المكفولة للناس حاليا يجب أن تكون محمية ومحفوظة ودعت جميع الدول إلى الالتزام بواجباتهم في احترام وحماية حق الخصوصية، كما نصت فى المادة الرابعة على الحفاظ على الخصوصية في الاتصالات الرقمية عبر الانترنت،متضمنا ذلك مراجعة الاجراءات و الممارسات الحالية والتشريعات الوطنية.

---

[١] برنامج الرقابة المعروف ب - PRISM والذي كشف عنه سنودن يستهدف جمع بيانات جميع مستخدمي خدمات الإنترنت لشركات PalTalk, AOL, Yahoo, Microsoft, Facebook, Apple, Google : في جميع أنحاء العالم. من الملاحظ أن هذه بين جميع مستخدمي الإنترنت وذلك لتقديمها خدمات متنوعة تلقي اهتمام من العديد من مستخدمي الإنترنت

[2] Alan Rusbridger and Ewen MacAskill, Edward Snowden interview - the edited transcript, The Guardian Newspaper, Friday 18 July 2014, available at: https://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript Accessed on 30-12-2021

[3] General Assembly backs right to privacy in digital age,13 December 2013 , available at: https://news.un.org/en/story/2013/12/458232-general-assembly-backs-right-privacy-digital-age

Accessed on 30-12-2021

اعتمدت الجمعية العامة للأمم المتحدة القرار ١٦٧/٦٨ الذي يعرب عن القلق البالغ إزاء الأثر السلبي الذي يمكن أن تخلفه مراقبة الاتصالات واعتراضها على حقوق الإنسان، وأكدت الجمعية العامة أن حقوق الأشخاص خارج الفضاء الإلكتروني يجب أن تحظى بالحماية أيضاً فى الفضاء الإلكتروني، وأهابت بجميع الدول أن تحترم وتحمي حق الخصوصية في الاتصالات الرقمية ، كما أهابت الجمعية العامة بجميع الدول أن تعيد النظر في إجراءاتها وممارساتها وتشريعاتها المتعلقة بمراقبة الاتصالات واعتراضها وجمع البيانات الشخصية، وشددت على ضرورة أن تضمن الدول تنفيذ التزاماتها بموجب القانون الدولي لحقوق الإنسان تنفيذاً كاملاً وفعالاً.

المطلب الثانى – تقارير الجمعية العامة للأمم المتحدة لعام ٢٠١٤:

أكدت الجمعية العامة للأمم المتحدة في قرارها رقم (١٦٧/٦٨) بتاريخ ١٩ نوفمبر ٢٠١٤ في الدورة التاسعة والستين بشأن «الحق في الخصوصية في العصر الرقمي» على أن:

- حق الإنسان في الخصوصية الذي لا يسمح بتعريض أي شخص لتدخل تعسفي، أو غير قانوني في خصوصياته، أو في شؤون أسرته أو بيته أو مراسلاته، وحقه في التمتع بحماية القانون من مثل هذا التدخل.
- أهمية الاحترام التام لحرية الحصول على المعلومات وتلقيها ونقلها للغير، بما في ذلك الأهمية الأساسية للوصول إلى المعلومات والمشاركة الديمقراطية.
- التشديد على أن مراقبة الاتصالات أو اعتراضها على نحو غير قانوني أو تعسفي، وجمع البيانات الشخصية على نحو غير قانوني أو تعسفي، أمور تنتهك حق الخصوصية ، ويمكن أن تمس بالحق في حرية التعبير، وقد تتعارض مع مبادئ المجتمع الديمقراطي باعتبارها أعمالًا تدخلية بدرجة كبيرة ولا سيما عند الاضطلاع بها على نطاق واسع.

- التزام الدولة بأن تكون مراقبة الاتصالات الرقمية متسقة مع الالتزامات الدولية المتصلة بحقوق الإنسان، وأن تتم بالاستناد إلى إطار قانوني متاح للعموم، وواضح ودقيق ومستفيض وخال من التمييز، وأن أي مساس بحق الخصوصية يجب ألا يكون تعسفياً، أو غير قانوني، مع مراعاة ما هو معقول لتحقيق أهداف مشروعه.
- على الدول الأطراف في العهد الدولي الخاص بالحقوق المدنية والسياسية وعددها حتى الآن (١٦٨) دولة، أن تتخذ الخطوات اللازمة لاعتماد القوانين، أو التدابير اللازمة لإعمال الحقوق المعترف بها في العهد الدولي لسنة ١٩٦٦، وفي الإعلان العالمي لحقوق الإنسان لسنة ١٩٤٨، وفي إعلان القاهرة حول حقوق الإنسان في الإسلام لسنة ١٩٩٠. مع مراعاة القيود القانونية التي ينص عليها القانون، والضرورية لحماية الأمن القومي، والنظام العام، أو الصحة العامة، أو الأخلاق العامة، أو احترام حقوق وحرية الآخرين

وقد وضعت لجمعية العامة للأمم المتحدة في قرارها رقم (١٦٧/٦٨) العديد من التوصيات بشأن حماية الخصوصية فى العصر الرقمى ونستعرضها فى التالى:

١- العمل على جمع المعلومات عن المراقبة الإلكترونية وجمع البيانات الشخصية وتخزينها وتقييم أثرها على حقوق الإنسان.
٢- معاجلة قصور الشفافية الحكومية المرتبطة بسياسات وقوانين وممارسات الرقابة الذي يعيق أي جهد لتقييم اتساقها مع القانون الدولى لحقوق الإنسان، ولضمان المسائلة القانونية عن انتهاك الحقوق والحريات العامة
٣- المواجهة الفعالة للتحديات المتصلة بحق الخصوصية فى سياق تقنية الاتصالات الحديثة مما يرتب التزاماً مستمراً ومتضافراً ومتعدداً لأصحاب المصلحة.

٤- ينبغي أن تتضمن هذه العملية حوارا يشمل جميع أصحاب المصلحة المعنيين، بمن فيهم الدول الأعضاء والمجتمع المدنى والأوساط العلمية والتقنية، وقطاع الأعمال والأوساط الأكاديمية وخبراء حقوق الإنسان ومع استمرار تطور تكنولوجيا الاتصالات، سيكون للقيادة دور حاسم لضمان استخدام هذه التكنولوجيات وتسخير إمكانياتها من أجل تحسين التمتع بحقوق الإنسان المعتمدة فى الإطار القانونى الإقليمي والدولى.

٥- الحاجة إلى اليقظة فى ضمان امتثال أي سياسة أو ممارسة فى مجال المراقبة للقانون الدولى لحقوق الإنسان، بما فيه حق الخصوصية، من خلال وضع ضمانات فعالة ضد التجاوزات. وكتدبير فوري، ينبغي أن تستعرض الدول قوانينها وسياساتها وممارساتها الوطنية الخاصة لضمان مطابقتها للقانون الدولى لحقوق الإنسان. مع الأخذ فى الاعتبار القيم الأخلاقية والدينية لجميع دول العالم على قدم المساواة دون تمييز.

٦- لمواجهة أوجه القصور فى الأنظمة القانونية الوطنية، ينبغي على الدول أن تتخذ خطوات لمعالجتها بوسائل متنوعة منها اعتماد إطار تشريعي واضح وشامل وغير تمييزي، وينبغي اتخاذ خطوات لضمان وجود نظم وممارسات رقابة فعالة ومستقلة، مع الاهتمام بحق ضحايا الاعتداءات على الحقوق الأساسية للإنسان ومنها حق الخصوصية لتحقيق الإنصاف والعدالة.

٧- الحاجة إلى تحليل إضافى من قبل كيانات الأعمال للوفاء بمسؤولياتها لاحترام حقوق الإنسان،وحق الخصوصية ، بما فى ذلك بذل العناية الواجبة وضمانات إدارة المخاطر، كما سيساعد فى دورها المتعلق بتوفير سبل فاعلة للعدالة والإنصاف.

٨- مراجعة النصوص المتعلقة بحق الخصوصية الواردة فى الدساتير العربية وفى بعض التشريعات الوطنية ذات العلاقة بحق الخصوصية لتعزيز وحماية هذا الحق لمواكبة مخاطر العصر الرقمي.

٩- حث الدول الأطراف فى العهد الدولى الخاص بالحقوق المدنية والسياسية لعام ١٩٦٦ التي لا تولى الاهتمام اللازم للمعلومات المتعلقة بالأسلوب الذي تضمن به السلطات التشريعية أو الإدارية أو القضائية والأجهزة المختصة المؤسسة فى الدولة بشكل عام احترام هذا الحق وخاصة المادة ١٧

١٠- على الرغم من أهمية المادة ١٧ من العهد الدولى الخاص بالحقوق المدنية والسياسية لعام ١٩٦٦ التي تتناول حماية حق الخصوصية ، إلا أن المادة الرابعة من هذا العهد لم تدرج المادة ١٧ من ضمن المواد المحظور تقييدها كما هو الحال للمواد (٦ ، ٧ ، ٨ فقرة ١ و ٢ ، المادة ١١ ، ١٥، ١٦ ، ١٨ ،) مما قد يساهم فى تهميش حماية حق الخصوصية على المستويين الدولى والوطني.

١١- مراجعة القيود الواردة فى المادة ١٩ من العهد الدولى الخاص بالحقوق المدنية والتي تجيز للدولة إخضاع بعض الحقوق والحريات العامة للضرورة أو لاحترام حقوق الآخرين أو سمعتهم أو لحماية الأمن القومي أو النظام العام أو الصحة العامة أو الآداب العامة.

المطلب الثالث – تقارير الجمعية العامة للأمم المتحدة لعام ٢٠١٨:

الجمعية العامة للأمم المتحدة في قرارها رقم ٧/٣٤ بتاريخ ٣ اغستطس ٢٠١٨ في الدورة التاسعة والثلاثون بشأن «الحق في الخصوصية في العصر الرقمي»[١]

اكد التقرير أن الحاجة إلى مواجهة التحديات التي يفرضها عالم التكنولوجيا الرقمية على حق الخصوصية أكثر إلحاحاً من أي وقت مضى. فالتكنولوجيا الرقمية، التي تستغل باستمرار البيانات المرتبطة بحياة الأشخاص، تتغلغل تدريجياً في النسيج الاجتماعي والثقافي والاقتصادي والسياسي للمجتمعات الحديثة، مدفوعةً في الغالب من القطاع الخاص. وثمة تهديد ناجم عن التكنولوجيات التي تستخدم البيانات استخداماً كثيفاً، وهي تحتل موقعاً متنامياً باستمرار من قبيل البيانات الضخمة والذكاء الاصطناعي، ألا وهو إقامة بيئة رقمية تدخّلية تتيح للدول ومؤسسات الأعمال ممارسة المراقبة، وتحليل سلوك الناس والتنبؤ به، بل والتلاعب به أيضاً إلى حد غير مسبوق. وإذا كان لا يسعنا إنكار إمكانية توظيف التكنولوجيات القائمة على البيانات في استخدامات مفيدة للغاية، فإن هذه التطورات التكنولوجية تنطوي على مخاطر كبيرة بالنسبة إلى الكرامة الإنسانية، والخصوصية والاستقلالية ، وممارسة حقوق الإنسان بوجه عام[٢].

وأصدر التقرير مجموعة من التوصيات بعضها للدول وبعضها لمؤسسات الأعمال ونستعرضها فى التالى:

---

[1] General assembly, Human Rights Council , The right to privacy in the digital age, Report of the United Nations High Commissioner for Human Rights ,3 August 2018, United Nations, available at: https://undocs.org/ar/A/HRC/39/29 Accessed on 30-12-2021

[٢] قرارات الجمعية العامة ١٦٧/٦٨ و١٦٦/٦٩ و١٩٩/٧١ وقراري مجلس حقوق الإنسان ١٦/٢٨ و٧/٣٤ والمقرر ١١٧/٢٥

توصيات الى الدول:

١- الاعتراف بالتبعات الكاملة الناجمة عن التكنولوجيات الجديدة، ولا سيما التكنولوجيات المستنِدة إلى البيانات، إزاء الحق في الخصوصية وجميع حقوق الإنسان الأخرى.

٢- اعتماد تشريعات قوية الأثر ومُحكمة وشاملة في مجال الخصوصية، بما في ذلك خصوصية البيانات، وبما يمتثل للقانون الدولي لحقوق الإنسان من حيث الضمانات والرقابة من أجل حماية حق الخصوصية على نحو فعال.

٣- كفالة عدم نشر النُظم القائمة على الاستخدام الكثيف للبيانات، بما في ذلك النُظم التي تشمل جمع البيانات البيومترية والاحتفاظ بها، إلا عندما يمكن للدول أن تُبيِّن أنها ضرورية وتناسبية لتحقيق هدف مشروع.

٤- إنشاء هيئات مستقلة وتزويدها بالصلاحيات اللازمة لمراقبة ممارسات الدولة والقطاع الخاص فيما يتعلق بخصوصية البيانات، والتحقيق في الانتهاكات، وتلقي الشكاوى من الأفراد والمنظمات، وإصدار غرامات وعقوبات فعالة أخرى على معالجة البيانات الشخصية بشكل غير قانوني من جانب الهيئات العامة والخاصة.

٥- سنّ التشريعات المناسبة واللجوء إلى الوسائل الأخرى المتاحة لكفالة امتثال أي تدخل في حق الخصوصية ، بما في ذلك عن طريق مراقبة الاتصالات وتبادل المعلومات الاستخبارية، لإحكام القانون الدولي لحقوق الإنسان، بما يشمل مبادئ المشروعية والضرورة والتناسب، وتحقيق هدف مشروع، وبصرف النظر عن جنسية الأفراد المتضررين أو مكان وجودهم، والتوضيح بأن منح الإذن باتخاذ تدابير المراقبة يتطلب وجود سبب كافٍ يدعو إلى

الافتراض أن فرداً معيناً قد ارتكب أو أنه يرتكب جرماً، أو أنه يشارك في أعمال يمكن اعتبارها تهديداً محدداً للأمن القومي.

٦- تعزيز الآليات المستقلة لإصدار الإذن بممارسة أنشطة المراقبة من جانب الدولة وتطبيق رقابة على تلك الأنشطة، وكفالة أن تكون تلك الآليات مختصة ومجهزة بموارد كافية لرصد وإنفاذ مشروعية تدابير المراقبة وضرورتها وتناسبها.

٧- استعراض القوانين لكفالة أنها لا تفرض شرط الاحتفاظ الشامل والعشوائي ببيانات الاتصالات على شركات الاتصالات وغيرها من الشركات.

٨- اتخاذ خطوات من أجل تعزيز الشفافية والمساءلة في اقتناء الدول لتكنولوجيات المراقبة.

٩- تنفيذ الواجبات الواقعة على عاتق الدول بالكامل للحماية من انتهاكات حق الخصوصية من جانب مؤسسات الأعمال في جميع القطاعات ذات الصلة، بما في ذلك قطاع تكنولوجيا المعلومات والاتصالات، عن طريق اتخاذ الخطوات المناسبة لمنع هذه الانتهاكات والتحقيق فيها والمعاقبة عليها والانتصاف منها باعتماد السياسات والتشريعات والأنظمة والأحكام القضائية الفعالة.

١٠- كفالة حصول جميع ضحايا الانتهاكات والتجاوزات في حق الخصوصية على سبل إنصاف فعالة، بما في ذلك في القضايا العابرة للحدود.

توصيات الى مؤسسات الأعمال:

١- بذل كل الجهود الممكنة للوفاء بمسؤوليتها عن احترام حق الخصوصية وجميع حقوق الإنسان الأخرى. وكحد أدنى، ينبغي أن تعمل مؤسسات الأعمال على تنفيذ المبادئ التوجيهية بشأن الأعمال التجارية وحقوق الإنسان تنفيذاً كاملاً، مما ينطوي على بذل العناية الواجبة في مراعاة حقوق الإنسان

على نحو فعال في جميع عملياتها وفيما يتعلق بجميع حقوق الإنسان، بما في ذلك حق الخصوصية ، واتخاذ الإجراءات المناسبة لمنع الآثار ذات الصلة سواء كانت فعلية أو محتملة، والتخفيف منها ومعالجتها.

٢- السعي إلى كفالة مستوى عالٍ من الأمان والسرية لأي اتصالات تقوم مؤسسات الأعمال بإحالتها ولأي بيانات شخصية تقوم بجمعها أو تخزينها أو معالجتها بطريقة أخرى. وإجراء تقييمات بشأن أفضل السبل المتاحة لتصميم وتحديث أمن المنتجات والخدمات على أساس مستمر.

٣- الامتثال لمبادئ الخصوصية الرئيسية المشار إليها في الفقرات من ٢٩ إلى ٣١ من هذا التقرير وكفالة أكبر قدر ممكن من الشفافية في سياساتها وممارساتها الداخلية التي تؤثر على الحق في خصوصية مستخدميها وعملائها.

٤- إتاحة الإنصاف عن طريق عمليات مشروعة، أو التعاون مع الجهات الأخرى من أجل إتاحة الإنصاف، عندما تتسبب مؤسسات الأعمال في آثار ضارة أو تسهم في حدوثها، بما في ذلك من خلال آليات فعالة للتظلم على المستوى التنفيذي.

٥- الإسهام في عمل مشروع المساءلة والانصاف التابع لمفوضية الأمم المتحدة السامية لحقوق الإنسان، الهادف إلى وضع توجيهات وتوصيات لتعزيز فعالية آليات التظلم غير التابعة للدولة فيما يتعلق بانتهاكات حق الخصوصية في الفضاء الرقمي.

المطلب الرابع – تقارير الجمعية العامة للأمم المتحدة لعام ٢٠٢١:

تقرير الجمعية العامة للأمم المتحدة رقم ١٥/٤٢ بتاريخ ١ اكتوبر ٢٠٢١ في الدورة الثامنة والأربعون بشأن «الحق في الخصوصية في العصر الرقمي[١]

يتحدث التقرير عن الذكاء الإصطناعى[٢] بما في ذلك تكنولوجيات التنميط وصنع القرار الآلي والتعلم الآلي،وتأثيره في غياب ضمانات مناسبة على التمتع بحق الخصوصية[٣]، حيث يستخدم الذكاء الاصطناعي المعلومات الشخصية ويتخذ في كثير من الأحيان قرارات لها آثار ملموسة على حياة الناس. غير أن مسألة الخصوصية مسألة متشابكة تشابكاً عميقاً مع آثار مختلفة على التمتع بحقوق أخرى، مثل الحق في الصحة والتعليم وحرية التنقل وحرية التجمع السلمي وحرية تكوين الجمعيات وحرية التعبير.

وعادة ما تعتمد أنظمة الذكاء الاصطناعي على مجموعات كبيرة من البيانات التي تتضمن في غالب الأحيان بيانات شخصية. ويحفز ذلك على جمع البيانات وتخزينها ومعالجتها على نطاق واسع. وتقوم العديد من مؤسسات الأعمال بتحسين الخدمات لجمع أكبر قدر ممكن من البيانات[٤]فعلى سبيل المثال، تعتمد مؤسسات الأعمال الشبكية مثل

---

[1] General assembly, Human Rights Council , The right to privacy in the digital age Report of the United Nations High Commissioner for Human Rights ,13 September 2021, United Nations, available at: https://undocs.org/a/hrc/48/l.9.rev.1 Accessed on 1-1-2022

[٢] لا يوجد تعريف لمصطلح "الذكاء الاصطناعي" يحظى بقبول عام. وهو يُستخدَم في هذا التقرير للإشارة إلى مجموعة من العمليات والتكنولوجيات التي تُمكن الحواسيب من تكميل عمل الإنسان أو الحلول محله في مهام محددة يؤديها هو في ظروف أخرى، مثل اتخاذ القرارات وحلّ المشاكل) وتشمل، على سبيل المثال لا الحصر، التعلم الآلي والتعلم العميق

[٣] انظر A/HRC/45/26 و A/HRC/47/61.

[4] Wolflie Christl, (2017) Corporate surveillance in everyday life How Companies Collect, Combine, Analyze,

Trade, and Use Personal Data on Billions (Vienna, Cracked Lab – Institute for Critical Digital Culture, page 48, available as a pdf file at: https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

Accessed on 1-1-2022

شركات وسائل التواصل الاجتماعي على جمع وتسييل كميات هائلة من البيانات المتعلقة بمستخدمي الإنترنت ،ويشكل ما يسمى إنترنت الأشياء مصدراً سريع النمو للبيانات التي تستغلها الشركات والدول على حد سواء. ويحدث جمع البيانات في الأماكن الحميمة والخاصة والعامة [١]،ويحصل الوسطاء على البيانات الشخصية ويدمجونها ويحللونها ويشاركونها مع عدد لا يحصى من المستلمين. وتحظى صفقات البيانات هذه بحماية كبيرة من التدقيق العام ولا تعوقها الأطر القانونية القائمة إلا قليلاً[٢]، وتأتي مجموعات البيانات الناتجة عن ذلك بأحجام كبيرة وتتخذ المعلومات المجمعة أبعاداً غير مسبوقة.

وتتسم عمليات صنع القرار في العديد من نظم الذكاء الاصطناعي بعدم الشفافية، فضلاً عن السرية التي تتعمدها الجهات الفاعلة الحكومية والخاصة، وتضيف نظم التعلم الآلي عنصراً هاماً من عناصر التعتيم؛ فيمكن أن تكون قادرة على تحديد أنماط ووضع مقترحات يصعب أو يستحيل تفسيرها وغالبا ما يُشار إلى ذلك باسم مشكلة "الصندوق الأسود"[٣]. والتعتيم يجعل من الصعب التدقيق بطريقة مجدية في نظام الذكاء الاصطناعي ويمكن أن يشكل عقبة أمام المساءلة الفعالة في الحالات التي تسبب فيها نظم الذكاء

[1] Submissions by Centre for Communication Governance at National Law University Delhi, Derechos Digitales, Digital Rights Watch, Global Partners Digital, International Center for Not-for-Profit Law and Universidade Federal de Uberlândia

[2] Aaron Rieke and others (2016) Data brokers in an open society (London, Open Society Foundation, 2016).page 46, available as a pdf file at: https://www.opensocietyfoundations.org/uploads/42d529c7-a351-412e-a065-53770cf1d35e/data-brokers-in-an-open-society-20161121.pdf Accessed on 1-1-2022

[3] Ariel Bleicher, Demystifying the Black Box That Is AI, August 9, 2017, Scientific American, available at: https://www.scientificamerican.com/article/demystifying-the-black-box-that-is-ai/

Accessed on 1-1-2022

الاصطناعي ضرراً[1] ومع ذلك، تجدر الإشارة إلى أن هذه النظم لا يجب أن تكون مبهمة بالكامل.

ولهذه الأنشطة آثارا واسعة النطاق على الخصوصية وحقوق الإنسان بشكل عامم.

أولاً: تتضمن مجموعات البيانات المستخدمة معلومات عن أعداد كبيرة من الأفراد، مما يمس ضمنياً حقهم في الخصوصية.

ثانياً: يمكن أن تؤدي إلى تدخلات الدولة، مثل عمليات التفتيش والاستجواب والاعتقال والملاحقة القضائية،وتشمل الحقوق المتأثرة حق الخصوصية ، والحق في محاكمة عادلة، والحق في عدم التعرض للاعتقال والاحتجاز التعسفي، والحق في الحياة.

ثالثاً، يثير التعتيم المتأصل في القرارات القائمة على الذكاء الاصطناعي أسئلة ملحة بشكل خاص فيما يتعلق بقابلية خضوع الدولة للمساءلة عندما تسترشد بالذكاء الاصطناعي في اتخاذ تدابير قسرية، بل تكون هذه الأسئلة أكثر إلحاحاً في المجالات التي تعاني عادة من انعدام الشفافية بشكل عام، مثل أنشطة قوى مكافحة الإرهاب [2] .

---

[1] Lorna McGregor, Daragh Murray and Vivian Ng, INTERNATIONAL HUMAN RIGHTS LAW AS A FRAMEWORK FOR ALGORITHMIC ACCOUNTABILITY, Cambridge University Press: 17 April 2019, available as a pdf file at: https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/international-human-rights-law-as-a-framework-for-algorithmic-accountability/1D6D0A456B36BA7512A6AFF17F16E9B6

Accessed on 1-1-2022

[2] Submission by Tech Hive Advisory Limited. See also Committee on the Elimination of Racial Discrimination, general recommendation No. 36 (2020), para. 33; and the conference room paper of the United Nations High Commissioner for Human Rights on promotion and protection of the human rights and fundamental freedoms of Africans and of people of African descent against excessive use of force and other human rights violations by law enforcement officers (A/HRC/47/CRP.1), available at www.ohchr.org/Documents/Issues/Racism/A_HRC_47_CRP_1.pdf, paras. 15 and 19. Accessed on 1-1-2022

رابعاً، تنطوي الأدوات التنبؤية على مخاطر كامنة تتسبب في إدامة التمييز أو حتى تعزيزه، مما يعكس التحيز العرقي والإثني التاريخي المدمج في مجموعات البيانات المستخدمة، مثل التركيز غير المتناسب على ضبط الأمن بين بعض الأقليات

وأصدر التقرير مجموعة من التوصيات بعضها للدول وبعضها لمؤسسات الأعمال ونستعرضها فى التالى:

أولا: التوصيات للدول

١- الاعتراف الكامل بالحاجة إلى حماية جميع حقوق الإنسان وتعزيزها عند استحداث الذكاء الاصطناعي واستخدامه وإدارته باعتبار ذلك هدفاً من أهدافها المحورية، وضمان احترام جميع حقوق الإنسان وإنفاذها بالتساوي على شبكة الإنترنت وخارجها.

٢- ضمان أن استخدام الذكاء الاصطناعي يمتثل لجميع حقوق الإنسان، وأن أي تدخل في حق الخصوصية وحقوق الإنسان الأخرى من خلال استخدام الذكاء الاصطناعي منصوص عليه في القانون، ويسعى إلى تحقيق هدف مشروع، ويمتثل لمبادئ الضرورة والتناسب، ولا يخل بجوهر الحقوق المعنية.

٣- الإعلان عن حظر صريح لتطبيقات الذكاء الاصطناعي التي لا يمكن تشغيلها وفقاً للقانون الدولي لحقوق الإنسان وفرض وقف اختياري على بيع واستخدام نظم الذكاء الاصطناعي التي تنطوي على مخاطر كبيرة على التمتع بحقوق الإنسان، ما لم تتوفر ضمانات كافية لحماية حقوق الإنسان وإلى أن تتوفر هذه الضمانات.

٤- فرض وقف اختياري لاستخدام تكنولوجيا التعرف البيومتري عن بعد في الأماكن العامة، على الأقل ريثما تتمكن السلطات المسؤولة من إثبات امتثالها

لمعايير حماية الخصوصية والبيانات، وعدم وجود عوائق كبيرة تتعلق بالدقة وآثار تمييزية، وريثما تُنفَّذ جميع التوصيات الواردة في الفقرة ٥٣(ي)('١'-'٥') من الوثيقةA/HRC/44/24 .

٥- اعتماد وإنفاذ تشريعات خصوصية البيانات بطريقة فعالة للقطاعين العام والخاص، من خلال سلطات مستقلة ومحايدة، كشرط أساسي لحماية حق الخصوصية في سياق الذكاء الاصطناعي.

٦- اعتماد أطر تشريعية وتنظيمية تمنع وتخفف بشكل كاف الآثار السلبية المتعددة الأوجه لحقوق الإنسان المرتبطة باستخدام الذكاء الاصطناعي من جانب القطاعين العام والخاص.

٧- ضمان حصول ضحايا انتهاكات حقوق الإنسان والتجاوزات المرتبطة باستخدام نظم الذكاء الاصطناعي على سبل إنصاف فعالة.

٨- المطالبة بإمكانية تقديم تفسير كافٍ لجميع القرارات المدعومة بالذكاء الاصطناعي التي يمكن أن تؤثر تأثيراً كبيراً على حقوق الإنسان، ولا سيما في القطاع العام.

٩- تعزيز الجهود الرامية إلى مكافحة التمييز المرتبط باستخدام نظم الذكاء الاصطناعي من جانب الدول ومؤسسات الأعمال، بما في ذلك عن طريق إجراء واشتراط ودعم تقييمات منهجية ورصد نواتج نظم الذكاء الاصطناعي وآثار نشرها.

١٠- ضمان أن الشراكات بين القطاعين العام والخاص في توفير واستخدام تكنولوجيات الذكاء الاصطناعي شفافة وخاضعة لرقابة مستقلة في مجال حقوق الإنسان ولا تؤدي إلى التخلي عن مساءلة الحكومة عن حقوق الإنسان.

ثانيا: التوصيات التى يتعين على الدول ومؤسسات الاعمال القيام بها:

١- بذل العناية الواجبة في مجال حقوق الإنسان بشكل منهجي طوال دورة حياة نظم الذكاء الاصطناعي التي تطورها أو تنشرها أو تبيعها أو تحصل عليها أو تشغلها. وينبغي أن يكون من العناصر الرئيسية في بذلها العناية الواجبة في مجال حقوق الإنسان إجراء تقييمات منتظمة وشاملة للأثر على حقوق الإنسان.

٢- زيادة شفافية استخدامها للذكاء الاصطناعي بشكل كبير، بما في ذلك من خلال إعلام الجمهور والأفراد المتأثرين بشكل كافٍ وتمكين تدقيق مستقل وخارجي للنظم الآلية. وكلما كانت الآثار المحتملة أو الفعلية على حقوق الإنسان المرتبطة باستخدام الذكاء الاصطناعي أكثر رجحاناً وجدية، كلما كانت هناك حاجة إلى مزيد من الشفافية.

٣- ضمان مشاركة جميع أصحاب المصلحة المعنيين في اتخاذ القرارات المتعلقة بتطوير الذكاء الاصطناعي ونشره واستخدامه، ولا سيما المتأثرين من أفراد وجماعات.

٤- النهوض بقابلية تفسير القرارات القائمة على الذكاء الاصطناعي، بما في ذلك عن طريق التمويل وإجراء البحوث لتحقيق هذا الهدف.

ثالثا: توصيات مؤسسات الأعمال:

١- بذل كل الجهود للوفاء بمسؤوليتها عن احترام جميع حقوق الإنسان، بما في ذلك من خلال التفعيل الكامل للمبادئ التوجيهية المتعلقة بالأعمال التجارية وحقوق الإنسان.

٢- تعزيز جهودها لمكافحة التمييز المرتبط بتطويرها أو بيعها أو تشغيلها لنظم الذكاء الاصطناعي، بما في ذلك عن طريق إجراء تقييمات منهجية ورصد نواتج نظم الذكاء الاصطناعي وآثار نشرها.
٣- اتخاذ خطوات حاسمة لضمان تنوع القوى العاملة المسؤولة عن تطوير الذكاء الاصطناعي.
٤- إتاحة الإنصاف أو التعاون عن طريق عمليات مشروعة عندما تتسبب في آثار ضارة بحقوق الإنسان أو تسهم في حدوثها، بما في ذلك من خلال آليات فعالة للتظلم على المستوى التنفيذي.

المطلب الخامس – الوضع فى جمهورية مصر العربية:

يستعرض هذا المطلب وضع الخصوصية الرقمية فى التشريعات المصرية من خلال الدستور المصرى لسنة ٢٠١٤ المعدل فى ٢٠١٩، ثم إلقاء الضوء على بعض الأحكام القضائية المصرية ثم النظر بتمعن فى النصوص المنظمة للخصوصية فى القوانين المصرية ومدى مواكبتها للعصر الرقمي من عدمه.

أولا الحماية الدستورية

وضع الدستور المصري حدودا تحفظ حق الخصوصية حيث نصت المادة ٥٧ على "للحياة الخاصة حرمة، وهى مصونة لا تمس. وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفى الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين

في استخدام وسائل الاتصال العامة بكافة أشكالها ، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك".

مادة ٥٨ "للمنازل حرمة، وفيما عدا حالات الخطر، أوالاستغاثة لا يجوز دخولها، ولا تفتيشها، ولا مراقبتها أو التنصت عليها إلا بأمر قضائى مسبب، يحدد المكان، والتوقيت، والغرض منه، وذلك كله فى الأحوال المبينة فى القانون، وبالكيفية التي ينص عليها، ويجب تنبيه من فى المنازل عند دخولها أو تفتيشها، وإطلاعهم على الأمر الصادر فى هذا الشأن".

المادة ٥٩ "الحياة الآمنة حق لكل إنسان، وتلتزم الدولة بتوفير الأمن والطمأنينة لمواطنيها ولكل مقيم على أرضها".

ثانيا: القوانين المصرية

قانون العقوبات المصري[١]

مادة رقم ٣٠٩ مكرر يعاقب بالحبس مدة لا تزيد على سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجني عليه: (أ) استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه محادثات جرت في مكان خاص أو عن طريق التليفون. (ب) التقط أو نقل بجهاز من الأجهزة أياً كان نوعه صورة شخص في مكان خاص. فإذا صدرت الأفعال المشار إليها في الفقرتين السابقتين أثناء اجتماع على

[١] قانون العقوبات رقم ٥٨ لسنة ١٩٣٧، متوفر على

https://www.cc.gov.eg/legislation_single?id=404680https://manshurat.org/search?keys=%D9%82%D8%A7%D9%86%D9%88%D9%86+175+%D9%84%D8%B3%D9%86%D8%A9+2018 تاريخ الدخول ١٤-١-٢٠٢٢

مسمع أو مرأى من الحاضرين في ذلك الاجتماع، فإن رضاء هؤلاء يكون مفترضاً. ويعاقب بالحبس الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتماداً على سلطة وظيفته. ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة، كما تحكم بمحو التسجيلات المتحصلة عنها أو إعدامها.

مادة رقم ٣٠٩ مكرر (أ) يعاقب بالحبس كل من أذاع أو سهل إذاعة أو استعمل ولو في غير علانية تسجيلاً أو مستنداً متحصلاً عليه بإحدى الطرق المبينة بالمادة السابقة أو كان بغير رضاء صاحب الشأن. ويعاقب بالسجن مدة لا تزيد على خمس سنوات كل من هدد بإفشاء أمر من الأمور التي تم التحصل عليها بإحدى الطرق المشار إليها لحمل شخص على القيام بعمل أو الامتناع عنه. ويعاقب بالسجن الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتماداً على سلطة وظيفته. ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة أو تحصل عنها، كما يحكم بمحو التسجيلات المتحصلة عن الجريمة أو إعدامها.

قانون رقم ١٨٠ لسنة ٢٠١٨ باصدار قانون تنظيم الصحافة و الإعلام و المجلس الاعلي لتنظيم الإعلام

يتضح لنا أنه لا يوجد تشريع مستقل ينظم الإعلام الرقمي، أما عن الخصوصية الرقمية فهى تتواجد من خلال النصوص التالية:

المادة ١٩ "يحظر علي الصحيفة أو الوسيلة الإعلامية أو الموقع الالكتروني نشر او بث اخبار كاذبة، أو ما يدعو أو يحرض علي مخالفة القانون أو الي العنف أو الكراهية أو ينطوي علي تمييز بين المواطنين، أو يدعو الي العنصرية أو يتضمن طعنا في أعراض الأفراد أو سبا أو قذفا لهم أو امتهانا للاديان السماوية أو للعقائد الدينية.

ويلتزم بأحكام الفقرة السابقة كل موقع الكتروني شخصي أو مدونة الكترونية شخصية أو حساب الكتروني شخصي يبلغ عدد متابعيه خمسة الاف متابع أو اكثر"

المادة ٢٠ " يحظر في أي وسيلة من وسائل النشر أو البث التعرض للحياة الخاصة للمواطنين كما يحظر في أي وسيلة من وسائل النشر او البث تناول مسلك المشتغل بالعمل العام أو الشخص ذي الصفة النيابية العامة أو المكلف بخدمة عامة الا اذا كان التناول وثيق الصله بأعمالهم".

بالنظر الى اتفاقية بودابست التى قد تناولناها، نجد أن مصر لم تنضم إليها حتى الأن والحقيقة أنه لا يوجد تبرير لذلك، فإتجاه الدول فى الإنضمام للمعاهدة الأوسع نطاقا ولمكافحة جرائم تقنية المعلومات، فمازال المشرع المصرى يحتفظ بقانون تنظيم الاتصالات الصادر عام ٢٠٠٣ و قام بإصدار قانون رقم ١٧٥ لسنة ٢٠١٨ والذى نص على العديد من الجرائم المشابهة تماما للإتفاقية.

اتجه المشرع الفكر العقابى فى قانون[١] رقم 175 لسنة 2018 فى شأن مكافحة جرائم تقنية المعلومات، فجاء الباب الثالث بعنوان الجرائم والعقوبات وفيها جريمة الانتفاع بدون حق بخدمات الاتصالات والمعلومات وتقنيتها مادة (13)، جريمة الدخول غير المشروع مادة (14)، جريمة تجاوز حدود الحق فى الدخول مادة (15)، جريمة الاعتراض غير المشروع مادة (16)، جريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية مادة (17)، جريمة الاعتداء على البريد الإلكترونى أو المواقع أو الحسابات الخاصة مادة (18)، جريمة الاعتداء على تصميم موقع مادة (19)، جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة مادة (20)، جريمة

[١] قانون رقم ١٧٥ لسنة ٢٠١٨ فى شأن مكافحة جرائم تقنية المعلومات، متوفر على
https://manshurat.org/search?keys=%D9%82%D8%A7%D9%86%D9%88%D9%86+175+%D9%84%D8%B3%D9%86%D8%A9+2018 تاريخ الدخول ١٤-١-٢٠٢٢

الاعتداء على سلامة الشبكة المعلوماتية مادة (21)، البرامج والأجهزة والمعدات المستخدمة فى ارتكاب جرائم تقنية المعلومات مادة (22)، جرائم الاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإلكترونى مادة (23)، الجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإلكترونى مادة (24)، وخصص ثلاث مواد للجرائم المرتكبة من مدير الموقع فى المواد مادة (27) (28) (29).

اما ما يخصنا هو الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتى غير المشروع مادة (٢٥) ونستعرض المادة فى التالى:

"يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعتدى على أى من المبادئ أو القيم الأسرية فى المجتمع المصرى، أو انتهك حرمة الحياة الخاصة أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكترونى لترويج السلع أو الخدمات دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبارًا أو صورًا وما فى حكمها، تنتهك خصوصية أى شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة".

ومما لا شك فيه أن النص ينظم فكرة مكافحة الإبتزاز الإلكترونى و يعالج فكرة التسوق غير الإرادى وتبادل المعلومات، وانتهاك الخصوصية، وقد استخدم هذا النص للإدانة فى العديد من الجرائم التى تعرف بأسم قضايا التيك توك، ولكن إن جاز لنا التعليق فإننا نجد أن النص العقابى يجب أن يكون ضيق ولا يقبل القياس أو التأويل، وهنا نطرح سؤالا: ما هو تعريف قيم المجتمع المصرى؟ وبالرجوع للقضايا ومبادئ محكمة النقض والقوانين، لم نجد تعريف لقيم الأسرة المصرية، بل هناك تعريف فقط للأسرة، فالسؤال هنا هو ماذا يعنى بقيم الأسرة المصرية؟ وهذا يخلق نوع من أنواع

الجدل حيث وأننا الأن فى ٢٠٢٢ ولم يصدر تعريف فى أى حكم قضائى لقيم الأسرة، فذلك يثير الشكوك، كما أن المبدأ الأساسى فى تطبيق العقاب ينص على أن التوسع فى الإعفاء أفضل من التوسع فى التشديد، وبذلك الشكل يجعل النص قبيل تفسير كل قاضى على حدى فقد يفسره قاضى بشكل معين و يفسره أخر بشكل مخالف وهو شئ غير مقبول فى نص عقابى يشترط فيه الوضوح والتفسير الضيق وعدم وجود قياس أو تأويل.

أما عن قانون رقم ١٥١ لسنة ٢٠٢٠ قانون حماية البيانات الشخصية[١]، فأنه جاء وفقا للائحة العامة لحماية البيانات وساير نفس الفكر والتعريفات الأساسية.

ثالثا: أحكام المحاكم المصرية

وضحت المحكمة الدستورية العليا حدوداً لعدم جواز استخدام القوانين في فرض قيود على حقوق الإنسان " كان منطقياً وضرورياً أن تعمل الدول المتمدينة على أن تقيم تشريعاتها الجزائية وفق أسس ثابتة تكفل بذاتها انتهاج الوسائل القانونية السليمة في جوانبها الموضوعية و الإجرائية لضمان ألا تكون العقوبة أداة قامعة للحرية عاصفة بها بالمخالفة للقيم التي تؤمن بها الجماعة في تفاعلها مع الأمم المتحضرة و اتصالها بها، و كان لازماً – في مجال دعم هذا الاتجاه و تثبيته – أن تقرر الدساتير المعاصرة القيود التي ارتأتها على سلطان المشرع في مجال التجريم تعبيراً عن إيمانها بأن حقوق الإنسان و حرياته لا يجوز التضحية بها في غير ضرورة تمليها مصلحة

[١] قانون رقم ١٥١ لسنة ٢٠٢٠ قانون حماية البيانات الشخصية، متوفر على https://manshurat.org/node/66932 تاريخ الدخول ١٤-١-٢٠٢٢

اجتماعية لها اعتبارها، و اعترافا منها بأن الحرية في أبعادها الكاملة لا تنفصل عن حرمة الحياة" [١].

كما أكدت محكمة القضاء الإداري على أهمية حق الخصوصية "أن الحق في الخصوصية هو حق أصيل سواء نصّ عليه الدستور أو أغفَلَه"[٢].

خاتمة

إنطلاقاً مما تقدم فإن التحدي الأكبر الذي يواجه حق الخصوصية في ظل هذه الثورة الرقمية يتمثل في وضع قواعد قانونية سواء دولية أو وطنية في هذا المجال، والطريق اليسير للحصول على المعلومات الشخصية بكافة أشكالها أصبح من أكبر المشكلات التي يواجهها الأفراد في مختلف المجتمعات، لذلك نجد أن العديد من الدول سعت ولازالت نحو إبراز نصوص قانونية تحد من انتهاك الخصوصية والعمل على حمايتها، كما نجد أنَ الجمعية العامة للأمم المتحدة والمجتمع الدولي عامة يحاول جاهداً إنتاج الاتفاقيات والمعاهدات التي تلزم كافة الدول للسعي نحو ضبط المعايير الخاصة بحق الخصوصية والعمل على تطويرها لما للعصر الرقمي من نمو يفوق الجهود الدولية كثيراً.

[١] المحكمة الدستورية العليا – الطعن رقم ٣ – لسنة ١٠ قضائية – تاريخ الجلسة ٢-١-١٩٩٣ – مكتب فني ٥ – رقم الجزء ٢ – رقم الصفحة ١٠٣

[٢] حكم محكمة القضاء الإداري في الدعوى رقم ١٤٣٠ لسنة ٦٥ قضائية

النتائج

١. يسعى المجتمع الدولي للحد من توسع وسائل المعلوماتية ووضع إطار لحماية الخصوصية للأفراد ، حيث ان التحدي الأكبر الذي يواجه حق الخصوصية في العصر الرقمي يتمثل في غياب واضح لقواعد قانونية ملزمة في هذا المجال، في هذا الإطار يمكننا القول أن قواعد القانون الدولي بشأن حق الخصوصية، والتي قد أسس لها في المواثيق الدولية المختلفة، قد وفرت الحماية للخصوصية بشكل عريض ولم تتعاط مع إشكالية التطور التكنولوجي وأثرها في هذا الحق.

٢. إن التطور الهائل لتكنولوجيا المعلومات والتحول الرقمي كان له أثر سلبى فيما يخص انتهاك الخصوصية الرقمية بشكل واسع ومتزايد.

٣. إن النصوص القانونية المصرية لا زالت رغم وجود قانون رقم ١٧٥ لسنة ٢٠١٨ فى شأن مكافحة جرائم تقنية المعلومات، و قانون رقم ١٨٠ لسنة ٢٠١٨ باصدار قانون تنظيم الصحافة و الإعلام و المجلس الاعلي لتنظيم الإعلام، وقانون ١٥١ لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية بعيدة عن الواقع المتطور لتكنولوجيا المعلومات والتحول الرقمي وما تفرضه من خطر على اقتحام الخصوصية الفردية، ومن خلال ما سبق يتضح أنه لا يوجد قوانين أو تشريعات في مصر تحمي حق الخصوصية من الانتهاك بشكل مستقل.

٤. لا نمتلك فى مصر مفوضية للخصوصية تستطيع الفصل في كافة قضايا انتهاكات حُرمة الحياة الخاصة للمواطنين بأي وسيلة من وسائل النشر.

٥. لا يوجد ميثاق شرف إعلامي يحوز رضا وموافقة غالبية الجماعة الصحفية والإعلامية.

التوصيات

١. ضرورة قيام المجتمع الدولي من خلال منظماته الدولية بالاتفاقيات التي توسع من السلطة الدولية إلى حدٍ ما للحفاظ على حق الخصوصية، والعمل على فرض عقوبات دولية صارمة وموحدة للحد من التدخلات عبر الإنترنت، وحث الدول على فرض العقوبات على المخالف بهدف التقليل من توسعها.

٢. إن المواجهة الفعالة للتحديات المتصلة بحق الخصوصية في سياق تكنولوجيا الاتصالات الحديثة ينبغي أن تتضمن حوارا يشمل جميع أصحاب المصلحة المعنية، ويجب أن تشمل الدول الأعضاء والمجتمع المدني و الأوساط العلمية والتقنية وقطاع الأعمال و الأوساط الأكاديمية وخبراء حقوق الإنسان، ومع استمرار تطور تكنولوجيا الاتصالات، سيكون للدولة دور حاسم لضمان استخدام هذه التكنولوجيات، و لتسخير إمكانياتها من أجل تحسين التمتع بحقوق الإنسان المكرسة في الإطار القانوني الدولي.

٣. حتمية سن القواعد القانونية لحماية الخصوصية الرقمية والتماشي من خلالها مع تحديات العصر الحديث ووضعها ضمن إطار قانوني سليم.

٤. يجب على المشرع المصرى الإنتباه الى مخاطر الذكاء الاصطناعى، حيث لا ينص أى قانون فى مصر حتى اللحظة على ما يتعلق بالثورة الصناعية الرابعة، فيجب معرفة أبعادها و أثارها وكيفيه توافر حماية قانونية جنائية ومدنية للحفاظ من خلالها على الخصوصية الرقمية

٥. ضرورة نشر الوعي الثقافي لحق الخصوصية الرقمي من خلال إقامة دورات وورش تطلق هذا المفهوم وتبين مدى الأضرار الناتجة عن العبث فيه، وحث المجتمع على احترامه

٦. سرعة إصدار اللائحة التنفيذية لقانون ١٥١ لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

قائمة المراجع

أولا: المراجع العربية

١. أحمد أبو الوفا (١٩٩٨) **الوسيط في القانون الدولي العام**، القاهرة: دار النهضة العربية.

٢. أحمد حلمي السيد (١٩٨٣) **الحماية الجنائية لحق الإنسان في حرمة حياته الخاصة**، القاهرة: دار النهضة العربية.

٣. أحمد فتحى سرور (١٩٧٦) **الحماية الجنائية للحق في حرمة الحياة الخاصة**، القاهرة: دار النهضة العربية.

٤. أحمد فتحى سرور (١٩٨٤) الحق في حرمة الحياة الخاصة، مجلة القانون و الإقتصاد، القاهرة: العدد ٥٤

٥. أسامة عبد الله قايد (١٩٩٢) **الحماية الجنائية للحياة الخاصة وبنوك المعلومات**، ط٢ القاهرة: دار النهضة العربية.

٦. الدراسة النقدية لقانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، (٢٠٢٠) إعداد مركز بحوث القانون والتكنولوجيا بكلية القانون الجامعة البريطانية بمصر، بالتعاون مع مكتب أندرسن للمحاماه.

٧. بارق منتظر عبد الوهاب لامي (٢٠١٧) جريمة انتهاك الخصوصية عبر الوسائل الإلكترونية في التشريع الأردني، **رسالة ماجستير غير منشورة**، جامعة الشرق الأوسط، الأردن.

٨. زينب محمد جميل الضناوي (٢٠١٩) أعمال مؤتمر الخصوصية في مجتمع المعلوماتية، لبنان.
٩. حسام الدين الاهواني (١٩٧٨) **الحق في احترام الحياة الخاصة، دراسة مقارنة**، القاهرة: دار النهضة العربية.
١٠.رزق سلمودي وليندا ربايعة وآخرون (٢٠١٤) الموقف المعاصر لقواعد القانون الدولي العام من الحق في الخصوصية في العصر الرقمي، مجلة الجامعة العربية الأمريكية للبحوث، مجلد٣، العدد٢.
١١.طارق عزت رخا (٢٠٠٥) **قانون حقوق الإنسان**، ط ١ القاهرة: دار النهضة العربية للطباعة و النشر.
١٢.عبدالعزيز محمد سرحان (دون تاريخ نشر) **الاتفاقية الأوروبية لحماية حقوق الإنسان**، القاهرة: دار النهضة العربية.
١٣.مروة زين العابدين (٢٠١٤) الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولى الاتفاقيى والقانون الوطنى، **رسالة دكتوراه غير منشورة**، جامعة عين شمس.
١٤.مصطفى فهمى الجوهري (١٩٩٠) **الشرعية الجنائية لقرينة البراءة**، القاهرة: دار الثقافة الجامعية.
١٥.ممدوح خليل بحر (٢٠١٧) **حماية الحياة الخاصة في القانون الجنائي دراسة مقارنة** ، القاهرة: دار النهضة العربية.
١٦.وائل أحمد علام (٢٠٠٥) **الميثاق العربي لحقوق الإنسان، دراسة حول دور الميثاق في تعزيز حقوق الإنسان في جامعة الدول العربية**، القاهرة: دار النهضة العربية.
١٧.يوسف الشيخ يوسف (١٩٩٣) **حماية الحق في حرمة الأحاديث الخاصة**، القاهرة: دار النهضة العربية.

التشريعات

- الدستور المصرى لسنة ٢٠١٤ المعدل فى ٢٠١٩
- قانون العقوبات رقم ٥٨ لسنة ١٩٣٧

- قانون رقم ١٧٥ لسنة ٢٠١٨ فى شأن مكافحة جرائم تقنية المعلومات،
- قانون تنظيم الصحافة والإعلام رقم ١٨٠ لسنة ٢٠٢٠
- قانون حماية البيانات الشخصية المصرى رقم ١٥١ لسنة ٢٠٢٠
- US. Patriot Act 2001

أحكام قضائية

- المحكمة الدستورية العليا ، الطعن رقم ٣٣ ، لسنة ١٦ قضائية ، تاريخ الجلسة ٣-٢-١٩٩٦ ، مكتب فني ٧ ، رقم الجزء ١ ، رقم الصفحة ٣٩٣
- المحكمة الدستورية العليا ، الطعن رقم ٣ ، لسنة ١٠ قضائية ، تاريخ الجلسة ٢-١-١٩٩٣ – مكتب فني ٥ ، رقم الجزء ٢ ، رقم الصفحة ١٠٣
- حكم محكمة القضاء الإداري في الدعوى رقم ١٤٣٠ لسنة ٦٥ قضائية

ثانيا: المراجع الأجنبية

1. Alan Charles Raul (2014) **The Privacy, Data Protection and Cyber security**, November , Business Law Research
2. Carbonnier Droit Civil. (1995) Les Personnes. Personnalite, incapacitee, personnes morales Paris
3. Clay Calvert, Dan V. Kozlowski and Derigan Silver (2020) "**Mass Media Law**" 21st edition, MC GRAW HILL
4. Cookie policy | (2020) Generate a CCPA and GDPR compliant cookie policy for your website COOKIEBOT
5. Delaune, S., S. Kremer, & M. Ryan (2006) "**Coercion-resistance and receipt-freeness in electronic voting**", in the Proceedings of the 19th IEEE Computer Security Foundations Workshop, IEEE Computer Society Press
6. Gürses, S., A. Kundnani, & J. Van Hoboken (2016) "**Crypto and empire: the contradictions of counter-surveillance advocacy**", Media, Culture & Society

7. Hildebrandt, M. & S. Gutwirth (eds.) (2008) **Profiling the European Citizen**: **Cross-disciplinary Perspectives**, Dordrecht: Springer Netherlands
8. J. Van Den Hoven and J. Weckert (2008) "**Information technology, privacy, and the protection of personal data**", in Information technology and moral philosophy, Cambridge: Cambridge University Press
9. Karolina Matuszewska, Karolina Lubowicka, (2020) What is PII, non-PII, and personal data, DATA PRIVACY & SECURITY, Published October 21, 2020
10. Krishnamurthy, B. & C.E. Wills (2009) "On the leakage of personally identifiable information via online social networks", in Proceedings of the 2nd ACM workshop on Online social networks, ACM
11. Leenes, R., and E. Kosta (2015) "**Taming the cookie monster with dutch law-a tale of regulatory failure**", Computer Law & Security Review
12. Michael Iheanyichukwu, (2020) Internet Privacy in 2020, Research Gate
13. Motlagh, N. H., Bagaa, M., & Taleb, T. (2017) "UAV-based IoT platform: A crowd surveillance use case", IEEE Communications Magazine
14. Paul M. Schwartz and Daniel J. Solove, (2020) **PRINCIPLES OF THE LAW Data Privacy**, the American Law Institute "ALI",
15. Paul M. Schwartz & Daniel J. Solove, (2011), "The PII Problem: **Privacy and a New Concept of Personally Identifiable Information**", 86 N.Y.U. L.REV
16. Popa, C., (2012) "**Managing Personal Information: Insights on Corporate Risk and Opportunity for Privacy-Savvy Leaders**", Carswell
17. Robin Langford, (2020) Cookie-less countdown: Advertisers fear loss of third-party cookies, while creative see brighter future NETIMPERATIVE Digital intelligence for business

18. R. Badinter, (1968), Le droit au respect de la vie privee, JCP, Paris doct. No. 2136
19. R. Gassin, (1974) **L'atteine a la vie privee**, Dalloz Penal, Paris
20. Samuel D. Brandeis, Louis D. Warren, (1890) **The Right to Privacy**, Harvard Law Review
21. Stanford Encyclopedia of Philosophy, (2019) Privacy and Information Technology, 30 October 2019
22. Taylor, L., L. Floridi, and B. Van der Sloot (eds.), (2017) Group privacy: **New challenges of data technologies** (Philosophical Studies Series: Vol. 126), Dordrecht: Springer
23. Turilli, M. & L. Floridi, (2009) "**The ethics of information transparency**", Ethics and Information Technology
24. Warnier, M., Dechesne, F., and Brazier, F.M.T. (2015) "**Design for the Value of Privacy**", in J. van den Hoven, P. Vermaas, I. van de Poel (eds.), Handbook of Ethics, Values, and Technological Design, Dordrecht: Springer
25. Wolflie Christl, (2017) Corporate surveillance in everyday life How Companies Collect, Combine, Analyze,Trade, and Use Personal Data on Billions (Vienna, Cracked Lab – Institute for Critical Digital Culture
26. Zuboff, S., (2019), **The age of surveillance capitalism: the fight for the future at the new frontier of power**, London: Profile Books.

Articles

1. Aaron Rieke and others, (2016) Data brokers in an open society (London, Open Society Foundation
2. Alan Rusbridger and Ewen MacAskill, (2014) Edward Snowden interview - the edited transcript, The Guardian Newspaper, Friday 18 July 2014,
3. Ariel Bleicher,(2017) Demystifying the Black Box That Is AI, August 9, 2017, Scientific American
4. Big data means data that contains greater variety, arriving in increasing volumes and with more velocity, for more details about the big data

5. Cadwalladr, C.(2019), Facebook's role in Brexit – and the threat to democracy.
6. Egypt Smartphone Market Records Healthy Growth Despite COVID-19, IDC, 25 May 2021
7. Glenn Greenwald, Ewen MacAskill and Laura Poitras, Edward Snowden: the whistleblower behind the NSA surveillance revelations, The Guardian Newspaper, Tue 11 Jun 2013
8. How much time on average do you spend on your phone on a daily basis by STATISTA, 2021
9. Lorna McGregor, Daragh Murray and Vivian Ng, INTERNATIONAL HUMAN RIGHTS LAW AS A FRAMEWORK FOR ALGORITHMIC ACCOUNTABILITY, Cambridge University Press: 17 April 2019
10. Phillips, Melanie "From human rights to the EU, the tide's turning against the liberal thought police". Daily Mail (London). (4 July 2011).
11. Worldwide Quarterly Mobile Phone Tracker

International and Regional conventions

1. The African Charter on Human and Peoples' Rights, 1981
2. African Charter on the Rights and Welfare of the Child 1990
3. American Convention on Human Rights, 1969
4. Arab Charter on Human Rights, adopted by the 16th Arab Summit hosted by Tunis on May 23, 2004
5. Arab Convention on combating Information Technology offences ،2010
6. Cairo Declaration of Human Rights in Islam, Cairo, August 5, 1990
7. Convention on Cybercrime, Budapest, 23.XI.2001, European Treaty Series - No. 185
8. Convention on the Rights of the Child, 1989
9. Convention on the Rights of Persons with Disabilities, United Nations, 2006

10. Council of Europe, Recommendation No. R (1999)5 on the protection of privacy on the Internet
11. European convention on human rights, 1920
12. International Covenant on Civil and Political Rights, 1966
13. General Data Protection Regulation, European Parliament and Council of the European Union, L119, 4 May 2016Universal Declaration of Human Rights, 1948
14. General Assembly backs right to privacy in digital age, 13 December 2013
15. General assembly, Human Rights Council ,Twenty-seventh session, The right to privacy in the digital age
16. Report of the United Nations High Commissioner for Human Rights ,30 June 2014, United Nations
17. General assembly, Human Rights Council, The right to privacy in the digital age
18. Report of the United Nations High Commissioner for Human Rights, 3 August 2018, United Nations
19. General assembly, Human Rights Council , The right to privacy in the digital age
20. Report of the United Nations High Commissioner for Human Rights ,13 September 2021, United Nations

تم بحمد الله