(ISSN: 2356 - 9492)

الحماية الجنائية للبيانات في ظل التحول الرقمي

دكتور/ يحيى إبراهيم دهشان
مدرس القانون الجنائي
كلية الحقوق - جامعة الزقازيق

الملخص باللغة العربية:

يعد التحول الرقمي من أهم سمات العصر الحالي، حيث تقوم أغلب الحكومات العربية بهذا التحول في شتى قطاعاتها، ويصاحب هذا التحول مجموعة من المخاطر المتعلقة بتداول البيانات، فطبقاً لأنظمة التحول الرقمي ستكون جميع البيانات والمعاملات متصلة بالشبكة العنكبوتية مما يسهل تعرضها لمخاطر، كالاختراق والاستغلال وغيرها. ولذلك كانت دراسة أوجه الحماية الجنائية لتلك البيانات في ظل التحول الرقمي وانتشار تكنولوجيا الذكاء الاصطناعي ضرورة مُلحة من أجل ضمان أمن وسلامة تلك البيانات.

كما يعد تحديد البيانات التي يجب حمايتها – تحت مظلة القانون الجنائي – على سبيل الحصر درب من الخيال، لأن تلك البيانات لا نستطيع حصرها. فتشعب وتعدد أنواع البيانات يجعل من الصعب تحديدها، وتكمن الصعوبة الأكبر في تحديد ما هو مباح نشره وتداوله وما هو عكس ذلك حيث يحظر نشره أو تداوله، بل يعد من قام بهذا السلوك مرتكباً لجريمة. فعدم تحديد معيار واضح يفرق بين المعلومات المباحة والمعلومات المشمولة بالحماية يجعل الصورة ضبابية وغير واضحة بالنسبة لعموم المواطنين.

وعن أهمية التحول الرقمي فأنه يلعب دورًا مهمًا في القضاء على جرائم غسيل الأموال والتهرب الضريبي. وتكمن خطورته في استغلال هذه البيانات بصوره غير شرعية باستخدام خوارزميات الذكاء الاصطناعي، لتفلتر اهتمامات وميول أصحاب تلك البيانات، فتستطيع الشركات بذلك تقديم منتجات واعلانات تتوافق مع اهتماماتهم، بل ويتطور الأمر إلى تغيير ميولهم توجهاتهم السياسية عن طريق حقن أخبار تتوافق مع اهتماماتهم وتغير توجهاتهم.

وتظهر العديد من الإشكاليات المتعلقة بالموضوع، مثل: هل استعدت الحكومة تقنياً لحماية البيانات في ظل توجهها للتحول الرقمي؟ وما هي التشريعات التي تم سنها من أجل ضمان الحماية الجنائية للبيانات؟

الكلمات الدلالية: التحول الرقمي، البيانات، الذكاء الاصطناعي، الحكومة الالكترونية.

Abstract:

Digital transformation is one of the most important features of the current era, as most Arab governments undertake this transformation in their various sectors, and this transformation is accompanied by a set of risks related to the circulation of data. Therefore, studying aspects of criminal protection for such data in light of digital transformation and the spread of artificial intelligence technology was an urgent necessity in order to ensure the security and safety of such data.

Determining what data should be protected - under the umbrella of criminal law - exclusively is a fantasy, because we cannot limit them. The complexity and multiplicity of types of data makes it difficult to identify, and the greatest difficulty lies in determining what is permissible to publish and circulate, and what is the opposite, as it is prohibited to publish or circulate, but rather the person who has committed this behavior is considered to have committed a crime. Failure to specify a clear standard that differentiates between permitted information and protected information makes the picture blurry and unclear to the general public.

Regarding the importance of digital transformation, it plays an important role in eliminating money laundering and tax evasion crimes. Its danger lies in the illegal exploitation of this data using artificial intelligence algorithms, to filter the interests and tendencies of the owners of that data, so companies can provide products and advertisements that match their interests, and even develop into changing their political tendencies by injecting news that matches their interests and change their orientations.

Many problems arise, such as: Has the government prepared technically to protect data in light of its digital transformation?

(ISSN: 2356 - 9492)

What legislation has been enacted in order to ensure the criminal protection of data?

Keywords: digital transformation, data protection, artificial intelligence, e-government.

مقدمة :

موضوع البحث:

يعد التحول الرقمي من أهم سمات العصر الحالي، حيث تقوم أغلب الحكومات العربية بهذا التحول في شتى قطاعاتها، ويصاحب هذا التحول مجموعة من المخاطر المتعلقة بتداول البيانات، فطبقاً لأنظمة التحول الرقمي ستكون جميع البيانات والمعاملات متصلة بالشبكة العنكبوتية مما يسهل تعرضها لمخاطر، كالاختراق والاستغلال وغيرها. ولذلك كانت دراسة أوجه الحماية الجنائية لتلك البيانات في ظل التحول الرقمي وانتشار تكنولوجيا الذكاء الاصطناعي ضرورة مُلحة من أجل ضمان أمن وسلامة تلك البيانات.

كما يعد تحديد البيانات التي يجب حمايتها – تحت مظلة القانون الجنائي – على سبيل الحصر درب من الخيال، لأن تلك البيانات لا نستطيع حصرها. فتشعب وتعدد أنواع البيانات يجعل من الصعب تحديدها، وتكمن الصعوبة الأكبر في تحديد ما هو مباح نشره وتداوله وما هو عكس ذلك حيث يحظر نشره أو تداوله، بل يعد من قام بهذا السلوك مرتكباً لجريمة. فعدم تحديد معيار واضح يفرق بين المعلومات المباحة والمعلومات المشمولة بالحماية يجعل الصورة ضبابية وغير واضحة بالنسبة لعموم المواطنين.

وفي إطار التحدي الجديد الذي يفرضه التحول الرقمي كوسيط اتصالي وإعلامي بديل لانتشار الحريات، أصبحت ظاهرة جرائم اختراق البيانات تمثل مصدر قلق وتهديد للأنظمة الإعلامية بمختلف مرجعيتها، كما سارعت هذه الأنظمة في التدخل السريع لتنظيم وتجريم الاختراقات الأمنية لأنظمة الإنترنت، متزرعه بالعديد من الحجج فتارة بدعوى حماية الأمن القومي، وتارة ثانية بدعوى حماية الأطفال من المحتوى المعلوماتي

الضار وغير الشرعي ، وتارة ثالثة بزعم مكافحة العنصرية، فأرتفع عدد الدول التي تمارس رقابة كاملة على الإنترنت إلى ما يقارب من ١٠٠ دولة([١]).

حيث منعت الحكومة الأمريكية الآلاف من أجهزة التشفير خوفا من استخدامها من قبل منظمات إرهابية، كما كثفت وكالة المخابرات الأمريكية المركزية جهودها لتعقب نشاطات بعض المنظمات التي تدعى العمل في مجال الدفاع عن حريات التعبير بالتعاون مع مكتب التحقيقات الفيدرالية ([٢])، الأمر الذي يعكس ازدواجية المعايير؛ حيث تواجه الأولى استراتيجيات الرقابة خارج حدودها، وتواجه الثانية تبني استراتيجيات أكثر صرامة وتقدما داخل حدودها ([٣]).

أهمية البحث:

تتعرض البيانات دائما إلى أنواع كثيره من الاعتداء كالأتلاف والاستيلاء أو الجمع غير المشروع لها، وهناك العديد من الأسباب التي دفعت إلى ضرورة حماية البيانات ومن أهمها: زيادة قدرات التقنيات الحديثة، وتدفق البيانات والنقل المتكرر لها بين الجهات، بالإضافة إلى العولمة، ولذلك اصبحت حماية البيانات أمن قومي لأي دولة لما يشكله جمع واستغلال واختراق البيانات بطرق غير مشروعة من خطورة مطلقة على الدولة.

كما يلعب التحول الرقمي دورًا مهمًا في القضاء على جرائم غسيل الأموال والتهرب الضريبي. وتكمن خطورته في استغلال هذه البيانات بصوره غير شرعية باستخدام خوارزميات الذكاء الاصطناعي، لتفلتر اهتمامات وميول أصحاب تلك البيانات، فتستطيع الشركات بذلك تقديم منتجات واعلانات تتوافق مع اهتماماتهم، بل ويتطور

1) Inman, A. James & Inman, R. Ralph Spring. "Responsibility as an Issue in Internet Communication: Reading Flames as Defamation", Journal of Technology Law & Policy, Vol. 11,٢٠٠٦ , No. 35.

٢) طلال محمد داعوس، العرب والعولمة: الظاهرة والتحديات، مجلة الدراسات الدبلوماسية، العدد ١٤٢٠/١٤، ٢٠٠٠، ص١٧٥-١٨٤.

3) Whitfield Diffie and Susan Landau. The Export of Cryptography in the 20th and In Karl de Leeuw, Jan the 21st Centuries Bergstra, ed. The history of information, 2007.

(ISSN: 2356 - 9492)

الأمر إلى تغيير ميولهم توجهاتهم السياسية عن طريق حقن أخبار تتوافق مع اهتماماتهم وتغير توجهاتهم.

إشكالية البحث:

- هل يجوز اختراق موقع الكترونى – كنوع من أنواع الدفاع الشرعي – في حالة قيامه بنشر محتوى يشكل انتهاك لخصوصية شخص ما؟
- هل محو البيانات الشخصية حق مطلق لصاحب الشأن؟
- من المسئول جنائيًا عن الانتهاك الذي يحدث للخصوصية عن طريق المساعد الذكي؟
- مدي إمكانية تطبيق الحق في المحو في أنظمة النسخ الاحتياطي وكذلك النطاق الجغرافي لتطبيق الحكم الصادر بمحو البيانات؟
- هل تتوفر السرية والخصوصية والحماية ضد التلاعب للبيانات الموجودة بالأرشيف الإلكتروني؟
- هل استعدت الحكومة تقنياً لحماية البيانات في ظل توجهها للتحول الرقمي؟
- ما التشريعات التي تم سنها من أجل ضمان الحماية الجنائية للبيانات؟

منهج البحث:

نتبع في دراستنا هذه المنهج التأصيلي التحليلي، حيث نحتاج **المنهج التأصيلي** من أجل رد تلك الوقائع إلى القوانين التي تجرمها، كما نستخدم **المنهج التحليلي** من أجل تحليل ظاهرة جرائم البيانات، بالإضافة إلى الأشكال الجديدة التي تُرتكب من خلالها تلك الجرائم.

خطة البحث:

الفصل الأول: مفهوم البيانات والتحول الرقمي

الفصل الثاني: أنواع البيانات المشمولة بالحماية

الفصل الثالث: جرائم البيانات المرتبطة بالتحول الرقمي

الفصل الأول
مفهوم البيانات والتحول الرقمي

تمهيد وتقسيم:

يصاحب الانتشار الواسع للتحول الرقمي دائما جرائم مرتبطة بالبيانات، لأن هذا الأول قائم على فكرة البيانات وتحويلها من ملموسة وورقية إلى افتراضية غير ورقية، وهذا يتطلب بحث الحماية الجنائية للبيانات والتوسع في دراسة أوجه تلك الحماية من أجل تقليل الجرائم التي قد تقع وتكون مرتبطة بها.

وإذا لم يتخذ المستخدم إجراءات وقائية استثنائية لصون وحماية بياناته، فأنه ينتج عن استخدام التكنولوجيا والتحول الرقمي إنشاء كميات هائلة من البيانات سواء الشخصية أو غيرها، حيث يقوم الأشخاص بتحميل تيرابايت (٤) من البيانات إلى منصات تخزين مثل Dropbox وGoogle Drive ومواقع التواصل الاجتماعي مثل موقع الفيسبوك. بالإضافة إلى محركات بحث مثل Google.

وما يزيد الأمور خطورة هو جمع أنظمة التشغيل الخاصة بالأجهزة الذكية سواء الهواتف المحمول أو الكمبيوتر الشخصي أو غيرها(٥) – والتي اصحبت بحوزة الجميع حاليا – كميات أكبر من البيانات الوصفية ويستخدمون خوارزميات برمجية من أجل تحليلات هذه البيانات واستخدامها في **أغراض سياسية** (مثل معرفة توجهات وميول المواطنين واستغلالها بعرض أفكار تتفق مع ميولهم وتوجهاتهم في الحملات الانتخابية أو تمرير قرارات سياسية)، أو **اجتماعية** (مثل حقن أفكار مغايرة لعادات وتقاليد المجتمع من خلال أكثر المنصات التي يتواجد المواطنين بها)، أو **تجارية** كجني الأرباح من خلال منصات إعلانية مستهدفة مثل Google AdWords.

---

٤) التيرابايت TB كلمة تتكون من مقطعين تيرا وتعني ترليون ١٠٠٠٠٠٠٠٠٠٠٠٠ (١٢ صفر) وبايت، التيرابايت هي وحدة قياس لسعة التخزين في الكمبيوتر..

٥) تتعدد أنظمة التشغيل المستخدمة في أجهزة الحاسوب، والأجهزة الرقمية، والأجهزة الذكية ومنها: نظام دوس DOS، نظام ويندوز Windows، نظام لينكس Linux، نظام ماك Mac، أندرويد Android.

(ISSN: 2356 - 9492)

وبعد هذا التمهيد المختصر سوف نتناول هذا الفصل من خلال مبحثين، أولهما: تعريف البيانات، والثاني: تعريف التحول الرقمي وأهميته.

المبحث الأول

تعريف البيانات

تعددت تعريفات البيانات بين الفقه والقضاء، فمنهم من دمجها مع لفظ المعلومات، ومنهم من اقتصر بتعريف البيانات الشخصية ([٦])؛ وكان حري بنا في البداية التطرق لعرض التعريفات التي ذُكرت بشأن البيانات من أجل إيضاح المصطلح الرئيس في موضوع البحث.

وقد عرف قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ البيانات والمعلومات الإلكترونية بأنها كل ما يمكن إنشاؤه أو تخزينه أو معالجته أو تخليقه أو نقله أو مشاركته أو نسخه، بواسطة تقنية المعلومات، كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات، وما في حكمها ([٧]).

كما عرف قانون نشر وتبادل البيانات في إمارة دبي البيانات بأنها: "مجموعة منظمة أو غير منظمة من المعطيات أو الوقائع أو المفاهيم أو التعليمات أو المشاهدات أو القياسات، تكون على شكل أرقام أو حروف أو رموز أو صور أو غيرها، يتم جمعها وإنتاجها أو معالجتها، عن طريق مزودي البيانات، وتشمل المعلومات أينما وردت في هذا القانون"([٨]).

وعرف قانون حماية البيانات الشخصية البحريني البيانات بأنها: "أية معلومات في أية صورة تخص فردًا معرفًا، أو قابلًا بطريق مباشر أو غير مباشر لأن يعرف، وذلك

6) Yaseen, Humam Khalid, and Ahmed Mahdi Obaid. "Big Data: Definition, Architecture & Applications." JOIV: International Journal on Informatics Visualization 4.1 (2020): 45-51.

Shah, S., Vasilis Peristeras, and Ioannis Magnisalis. "Government (Big) data ecosystem: definition, classification of actors, and their roles." International Journal of Computer and Information Engineering 14.4 (2020): 102-114.

٧) مادة رقم (١) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.

٨) المادة ٢ من قانون رقم (٢٦) لسنة ٢٠١٥ بشأن تنظيم نشر وتبادل البيانات في إمارة دبي.

بوجه خاص من خلال رقم هويته الشخصية أو صفة أو أكثر من صفاته الشكلية أو الفسيولوجية أو الذهنية أو الثقافية أو الاقتصادية أو هويته الاجتماعية. ولتقرير ما إذا كان الفرد قابلًا لأن يعرف، تراعى كافة الوسائل التي يستخدمها مدير البيانات أو أي شخص آخر، أو التي قد تكون متاحة له"(٩).

ونعرف البيانات بأنها: مجموعة من الرموز أو الحروف أو الأرقام أو غيرها في صورتها الخام أو بعد معالجتها. أو يمكن اختصار التعريف بأنها: معلومات في صورتها الخام قبل معالجتها.

الفرق بين البيانات والمعلومات والمعرفة (١٠):

على الرغم من التباين بين الألفاظ إلا أنهم لا يحملون نفس المعني فهناك اختلاف، ونحتاج إلى فهم الفرق بين البيانات والمعلومات لأهميتها في صنع القرار وأهميتها في ظل التحول الرقمي.

ويمكن التفرقة بينهم من خلال توضيح تعريف كل منهما، فالبيانات هي الصورة الخام للمحتوى سواء رموز أو أرقام أو حروف أو غيره (١١)، وبعد القيام بعملية المعالجة لهذا المحتوي يصبح معلومات ذات قيمة وأهمية، ونصل للمعرفة بتجميع كم من المعلومات لنصل إلى الخبرة (١٢).

البيانات الضخمة Big Data:

نستعرض تعريف البيانات الضخمة نظرًا لاعتبارها محور الارتكاز في ظل التحول الرقمي، ففي مجال تقنية المعلومات، يطلق مصطلح Big Data على مجموعة من حزم البيانات الضخمة جدا والمعقدة والتي يصعب التعامل معها بواسطة نظم إدارة قواعد

٩) مادة ١ من قانون رقم ٣٠ لسنة ٢٠١٨ بإصدار قانون حماية البيانات الشخصية في البحرين.
١٠) د. يحيى إبراهيم دهشان، الحماية الجنائية لبيانات الشركات المقيدة في سوق الأوراق المالية – دراسة مقارنة، رسالة دكتوراة، كلية الحقوق جامعة الزقازيق ٢٠٢٠، ص ١٧.
١١) د. تامر محمد محمد صالح، الحماية الجنائية للحق في المعلومات الرسمية (دراسة مقارنة)، مجلة القانون والاقتصاد، ملحق خاص العدد الثاني والتسعون، ٢٠١٩، ص ٣٩.
12) Martin Doyle, What Is the Difference Between Data and Information? Online: https://salespop.net/sales-management/difference-between-data-and-information/ site visited on: 20-9-2019.

(ISSN: 2356 - 9492)

البيانات (DBMS) التقليدية من ناحية التخزين، البحث، التمثيل، والتحليل. وفي الواقع فإنه من الصعب تعريف مصطلح Big Data بشكل دقيق، لاختلاف ما يمكن اعتباره بيانات ضخمة من مؤسسة إلى أخرى نظرا إلى اختلاف قدرات كل مؤسسة على حدة، ولكن بشكل عام عندما نذكر Big Data فنحن نتحدث عن بيانات متعددة الأنواع والمصادر بحجم يصل إلى المئات من التيرابايت أو حتى البيتابايت أو حتى أكثر للحزمة ([١٣]) وإجمالا **يمكن تعريفها** وفق عدة مصادر بأنها تنوع كمي ونوعي ضخم من البيانات نتيجة تسارعها وإتاحتها آنيا، ومن ثم تتطلب معالجة واسعة والتنقيب عنها من خلال أدوات تكنولوجية غير تقليدية.

المبحث الثاني

تعريف التحول الرقمي وأهميته

على الرغم من وضوح لفظ التحول الرقمي، إلا أنه توجد صعوبة في توضيح معناه، فبالمعني الدراج يمكن اعتباره التحول في المعاملات من ورقية إلى رقمية ([١٤])، **ويمكننا تعريفة بأنه** اجراء تغييرات جذرية لنموذج العمل والإجراءات والعمليات بحيث تعتمد أكثر على التكنولوجيا والتعامل غير المباشر من خلال العالم الافتراضي.

والتحول الرقمي داخل الحكومة ليس ميكنة فقط، بل تحسين البنية التحتية ثم ميكنة الخدمة داخل الوزارة لتحويلها بعد ذلك لنظام الكترونى، لتقديمها على بوابة الكترونية يستطيع المواطن من خلالها الحصول على الخدمة بشهل أكثر سهولة ويسر ([١٥]).

وننتقل إلى لفظ **المجتمع الرقمي** والذي يعرف بأنه مجتمع تسود فيه استخدام نظم المعلومات والاتصالات في التعامل ما بين الحكومة والأفراد وبين الأفراد وأنفسهم.

13) Santosh K. Vishwakarma, Nirmal K. Gupta, A Big Data Approach for Healthcare Analysis During Covid-19, Springer, Singapore, 2021, p459.
14) Fletcher, Gordon, and Marie Griffiths. "Digital transformation during a lockdown." International Journal of Information Management 55 (2020): 102185.
15) Wessel, Lauri, et al. "Unpacking the difference between digital transformation and IT-enabled organizational transformation." Journal of the Association for Information Systems 22.1 (2021): 102-129.

ففي المجتمع العادي نعتمد إما على المجهود الشخصي والورقي في إنها الخدمات، بالإضافة إلى دفع مبالغ نقدية مقابل الخدمة المقدمة، وتكون كل المعاملات ورقية وملموسة؛ على النقيض في المجتمع الرقمي يتحول التعامل الشخصي والورقي الملموس إلى تعامل افتراضي رقمي غير ملموس متصل بالأنترنت ومتاح في العديد من الأماكن وليس مكان أو أماكن محدودة، بجانب عند طلب الخدمة يحصل الفرد عليها فورًا بملىء استمارات افتراضية غير ورقية وأيضًا دفع مقابل الخدمة الكتروني غير نقدي([١٦]).

ومن أهم مميزات التحول الرقمي، هو انقطاع الاتصال المباشر بين متلقى الخدمة ومقدم الخدمة، وبالتالي اختفاء العديد من الجرائم المتعلقة بالمصلحة العامة مثل الرشوة والاختلاس والاستيلاء، حيث أن تقديم الخدمة ودفع مقابل الخدمة يصبح الكترونيًا.

كما تسارعت وتيرة اهتمام الحكومات بالتحول الرقمي، وزادت المبالغ المنفقة من قبلها لتمكين هذا التحول داخل الأنظمة الحكومية. فوفقًا لآخر دراسة أجرتها جامعة هارفارد بيزنس ريفيو ([١٧])، تم استثمار ما يقرب من ١,٣ تريليون دولار أمريكي في التحول الرقمي في عام ٢٠١٨. ومع ذلك، لا يقتصر التحول الرقمي على استثمار رأس المال فحسب، بل يتعلق بتطوير الاستراتيجيات وتنفيذ ومعالجة التحديات والفرص المرتبطة به. ومع هذا التحول الكبير والخطير، كان لابد من وجود مجموعة من القوانين واللوائح لكي تحد من احتمالات الاستخدام السيء وغير المشروع لبيانات المستخدمين.

الفصل الثاني

أنواع البيانات المشمولة بالحماية

تمهيد وتقسيم:

يعد تحديد البيانات التي يجب حمايتها – تحت مظلة القانون الجنائي – على سبيل الحصر درب من الخيال، لأن تلك البيانات لا نستطع حصرها. فتشعب وتعدد أنواع

16) Porfírio, José António, et al. "Leadership characteristics and digital transformation." Journal of Business Research 124 (2021): 610-619.

17) Behnam Tabrizi, Ed Lam, Kirk Girard, and Vernon Irvin, Digital Transformation Is Not About Technology, harvard business review, 2019. online: https://hbr.org/2019/03/digital-transformation-is-not-about-technology

(ISSN: 2356 - 9492)

البيانات يجعل من الصعب تحديدها، وتكمن الصعوبة الأكبر في تحديد ما هو مباح نشره وتداوله وما هو عكس ذلك حيث يحظر نشره أو تداوله، بل يعد من قام بهذا السلوك مرتكباً لجريمة. فعدم تحديد معيار واضح يفرق بين المعلومات المباحة والمعلومات المشمولة بالحماية، يجعل الصورة ضبابية وغير واضحة بالنسبة لعموم المواطنين.

وطبقًا لتعريف قانون مكافحة جرائم تقنية المعلومات للبيانات (١٨)، سنقوم بتقسيم البيانات طبقاً للتصنيف النوعي، فنحدد أنواع البيانات ونحدد درجة الحماية لك نوع من تلك الأنواع، فسنتحدث عن البيانات الشخصية في مبحث أول، ثم البيانات الحكومية في مبحث ثانٍ.

المبحث الأول
البيانات الشخصية

مفهوم البيانات الشخصية:

تحديد البيانات الشخصية دائما ما يصاحبه صعوبة مطلقة لِما لهذه البيانات من تشعب وتنوع، ولذلك كان وضع مفهوم جامع مانع للبيانات الشخصية محل خلاف في الفقه القانوني.

وقد عرف قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ البيانات **الشخصية بأنها أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى (١٩).**

وعرف قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ البيانات الشخصية بأنها "أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخري كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية".

١٨) مادة رقم (١) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.
١٩) مادة رقم (١) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.

وعرف البيانات الشخصية الحساسة بأنها "البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية، أو بيانات القياسات الحيوية "البيو مترية" أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الحالة الأمنية، وفي جميع الأحوال تعد بيانات الأطفال من البيانات الشخصية الحساسة"([٢٠]).

وعرفت لائحة حماية البيانات الأوروبية GDPR البيانات الشخصية بأنها "أي معلومات تتعلق بشخص طبيعي محدد أو قابل للتحديد"([٢١])

ويمكننا تعريف البيانات الشخصية بأنها أي معلومة مرتبطة بشخص الإنسان سواء حالته المادية أو المعنوية والصحية أو الوظيفية أو الاجتماعية، وقد نتوسع في تعريف البيانات الشخصية – من أجل إصباغ الحماية الجنائية على أكبر قدر من البيانات المرتبطة بالشخص – ونعتبر الاتجاهات والانتماءات الفكرية والمعتقدات بيانات شخصية.

وتعد حماية البيانات الشخصية حقًا أساسيًا للجميع، لكنهم دائمًا ما يشعرون بالسيطرة الكاملة على بياناتهم الشخصية وأنها مستغله دائما وغير مشموله بالحماية الكاملة التي تجعلهم مطمئنين عليها. فأحد النواتج الثانوية لعصر التحول الرقمي هو أن الخصوصية الشخصية تتآكل بطريقة متسارعة. ولقد كشفت قواعد البيانات وشبكات الكمبيوتر وتقنيات التخزين الجماعي عن أفراد حول العالم يتعرضون لتهديدات المراقبة والسيطرة السلبية ([٢٢]).

---

٢٠) مادة رقم (١) من قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠.

21) GDPR, Article 4, Definitions: '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.

٢٢) محمد محمد الألفي، الحماية القانونية لقواعد البيانات في نظم المعلومات، أعمال ندوات: مكافحة الجريمة عبر الانترنت - وورشة عمل: أمن المعلومات والتوقيع الإلكتروني، المنظمة العربية للتنمية الإدارية، ٢٠١٠، ص ١٩٤.

(ISSN: 2356 - 9492)

حيث تحتوي قواعد البيانات حاليًا على عدد لا يحصى من المعلومات حول ملايين الأفراد حول العالم. يتضمن ذلك المعلومات الطبية وبيانات بطاقات الائتمان وعادات الإنفاق الشخصي وطرق السفر والتاريخ الإجرامي وزملاء العمل والممتلكات الشخصية (من سجلات التأمين على سبيل المثال) والتعليم والمعتقدات الدينية ([٢٣]).

وتعد حماية البيانات الشخصية الحساسة، رغم أنها ليست فكرة جديدة، إلا أنها اكتسبت أهمية جوهرية مع التقدم التكنولوجي على مدى السنوات الماضية في العديد من الدول، وقد وضعت تشريعات واسعة النطاق لتجريم إساءة استخدام المعلومات الشخصية من قبل الحكومة أو القطاع الخاص.

أشكال انتهاك الخصوصية واستغلال البيانات الشخصية

تتعدد – في ظل التطور التكنولوجي – أشكال وصور استغلال البيانات الشخصية والتي تشكيل جرائم متعلقة بخصوصية الإنسان، نعرض منها بعض الأمثلة:

- يمكن من خلال مراقبة ماكينات الصراف الآلي (ATM) معرفة أوقات الذروة لاستخدام الأشخاص تلك الماكينات واستغلال تلك الأوقات في إرسال رسائل ترويجية لمنتجات معينة قريبة من هذا المكان. وأيضا معرفة عادات الأنفاق والوجهات التي يتوجهون إليها فور سحب الأموال، واستغلال ذلك في أغراض تجارية.

- تصنيف المنتجات التي تم دفع مقابلها عن طريق الفيزا، ومعرفة اهتمامات هؤلاء العملاء من خلال ذلك، وتوجيه عروض ورسائل ترويجية لهم بمنتجات تتناسب مع اهتماماتهم.

- معرفة العباءة المالية والدخل الثابت للأشخاص من خلال تتبع بيانات دخلهم الشهري وتتبع نفقاتهم، وبالتالي تحديد الطبقة الاجتماعية التي يعيشون فيها، واستغلال ذلك كتوجيه اعلانات عن شركات عقارية أو سياحية لمن يسمح دخلهم الشهري بذلك

كل تلك الأفكار وغيرها تمثل جانب بسيط من الاستغلال الذي يتم للبيانات الشخصية بعد جمعها بطريقة غير مشروعة، واقتحام حياة الأفراد واستغلال ظروفهم

٢٣) دراسة نقدية لقانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، ورشة عمل أعدها مركز بحوث القانون والتكنولوجيا، كلية القانون بالجامعة البريطانية في مصر، اكتوبر ٢٠٢٠، ص ٤٠.

وارتكاب نوع من أنواع الإكراه المعنوي عليهم في العديد من المغريات التي يقدموها لهم، وهذا يشكل العديد من الجرائم الواردة في قوانين العقوبات بالبلدان المخلفة([٢٤]).

وقد يتم جمع البيانات الشخصية من السلطات المختصة فقط لأغراض محددة وصريحة والأغراض المشروعة في إطار مهامهم ويمكن معالجتها فقط لنفس الغرض الذي تم جمع البيانات من أجله. يجب أن تكون معالجة البيانات قانونية وكافية، ذات صلة وليست مفرطة فيما يتعلق بالأغراض التي تم جمعها من أجلها.

المساعد الذكي:

تقنية المساعد أو الوكيل الذكي([٢٥])؛ مكنت المستخدم من الحصول على المعلومات الملائمة دون عناء البحث في محركات البحث، وأصبحت أكثر دقة وحداثة، بجانب مساعدة تلك التقنية في نمو التجارة الإلكترونية وتوفير حماية أكثر للمستهلكين، من خلال تحقيق رغباتهم في الحصول على السلع وإبرام العقد ومتابعة تنفيذه. ولكن على الجانب الآخر؛ يستطيع الوكيل الذكي أثناء تنفيذ مهامه أن يقوم بجمع ومعالجة وتخزين وتوزيع البيانات، والتي غالبًا ما تكون بيانات حساسة عن الأفراد أو بيانات شخصية، فتصبح مثار تهديد لخصوصية المستخدم.

وتظهر هنا إشكالية متعلقة بتحديد: **من المسئول جنائيًا عن الانتهاك الذي يحدث للخصوصية عن طريق المساعد الذكي؟**

استخدام البيانات الشخصية في ارتكاب جريمة التمييز بين الأفراد:

قد يتم استخدام البيانات الشخصية للتمييز بين الأفراد، فيلي جمع البيانات مرحلة تالية تتمثل في فلترتها بناء على تصنيفات معينة كالجنس والنوع وغيره، ليتم التمييز بين

24) Dib, Omar, Clément Huyart, and Khalifa Toumi. "A novel data exploitation framework based on blockchain." Pervasive and Mobile Computing 61 (2020): 101-104.

٢٥) نظام برمجي حاسوبي قادر على التصرف واتخاذ القرارات بشكل ذاتي لإنجاز هدف محدد والاستجابة للأشخاص أو الأحداث التي تجري في البيئة المحيطة به. يتميز الوكيل الذكي بقدرته على التعلم أثناء أداء المهام المختلفة بالاعتماد على التعلم الآلي، وتشمل وظائفه الأساسية الإدراك واتخاذ الإجراءات. حيث يتم الإدراك بواسطة مجموعة من المستشعرات، بينما يتم اتخاذ الإجراءات بواسطة مجموعة من المحركات أو أجهزة التشغيل.

(ISSN: 2356 - 9492)

الأفراد بناء على النوع أو الديانة أو الأصل العرقي – وهذا مجرم حاليا – فأغلب تشريعات الدول بها نصوص تجرم التمييز بين الأفراد بجميع صورة، وتضع عقوبات مغلظه على مرتكب ذلك السلوك.

فقد نصت المادة (١٦١) مكرر من قانون العقوبات المصري على "يعاقب بالحبس وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه أو بإحدى هاتين العقوبتين كل من قام بعمل أو بالامتناع عن عمل يكون من شأنه إحداث التمييز بين الأفراد أو ضد طائفة من طوائف الناس بسبب الجنس أو الأصل أو اللغة أو الدين أو العقيدة وترتب على هذا التمييز إهدار لمبدأ تكافؤ الفرص أو العدالة الاجتماعية أو تكدير للسلم العام. وتكون العقوبة الحبس مدة لا تقل عن ثلاثة أشهر والغرامة التي لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين إذا ارتكبت الجريمة المشار إليها في الفقرة الأولى من هذه المادة من موظف عام أو مستخدم عمومي أو أي إنسان مكلف بخدمة عمومية"([٢٦]).

وهذا يبين أن التشريعات الحالية بها نصوص استباقية يمكن الاستفادة منها في مكافحة جرائم مستقبليه، ومن جانب آخر هناك جرائم مستمرة، مهما تطور الزمن أو تطور وتغير سلوك ارتكابها.

قيود وأوصاف جريمة التمييز بين الأفراد:

تقيد أوراقها كجنحة بالمادة ١٦١ مكرر من قانون العقوبات. حيث يذكر أنه **قام المتهم بعمل** هو ..... وكان من شأنه التمييز بين الأفراد أو ضد طائفة من طوائف الناس وكان ذلك بسبب الجنس أو الأصل أو اللغة أو الدين أو العقيدة وترتب على هذا التمييز إهدار مبدأ تكافؤ الفرص أو العدالة الاجتماعية أو تكدير السلم العام. أو **امتنع المتهم عن عمل** ..... وكان من شأنه التمييز بين الأفراد أو ضد طائفة من طوائف الناس وكان ذلك بسبب الجنس أو الأصل أو اللغة أو الدين أو العقيدة

٢٦) قانون العقوبات المصري رقم ٥٨ لسنة ١٩٣٧ الوقائع المصرية - العدد ٧١ - في ٥ أغسطس سنة ١٩٣٧، مضافة هذه المادة بالقانون رقم ١٢٦ لسنة ٢٠١١ المنشور بالجريدة الرسمية بتاريخ ١٥ / ١٠ / ٢٠١١.

وترتب على هذا التمييز إهدار مبدأ تكافؤ الفرص أو العدالة الاجتماعية أو تكدير السلم العام. **وتكون العقوبة** الحبس وغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه.

كما تقيد أوراقها كجنحة بالمادة ١٦١ مكرر من قانون العقوبات. حيث يذكر أنه بصفته موظف عام **قام بعمل** هو ..... وكان من شأنه التمييز بين الأفراد أو ضد طائفة من طوائف الناس وكان ذلك بسبب الجنس أو الأصل أو اللغة أو الدين أو العقيدة وترتب على هذا التمييز إهدار مبدأ تكافؤ الفرص أو العدالة الاجتماعية أو تكدير السلم العام. أو بصفته موظف عام **امتنع عن عمل** ..... وكان من شأنه التمييز بين الأفراد أو ضد طائفة من طوائف الناس وكان ذلك بسبب الجنس أو الأصل أو اللغة أو الدين أو العقيدة وترتب على هذا التمييز إهدار مبدأ تكافؤ الفرص أو العدالة الاجتماعية أو تكدير السلم العام. **وتكون العقوبة** الحبس مدة لا تقل عن ثلاثة أشهر والغرامة التي لا تقل خمسين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين.

حماية البيانات الشخصية على مواقع التواصل الاجتماعي:

وهناك إشكالية تتعلق بجمع البيانات الشخصية من خلال مواقع التواصل الاجتماعي، حيث تقوم جميع مواقع التواصل الاجتماعي، مثل: فيسبوك وتويتر وإنستغرام وغيرها، بجمع بيانات شخصية كثيرة عن المستخدمين الذين يمتلكون حسابات شخصية بتلك المواقع، ويتم استغلال تلك البيانات بخوارزميات برمجية معينة في أغراض تجارية بالإضافة إلى إمكانية إعادة بيع البيانات لطرف ثالث، أو السماح لطرف خارج بالوصول لتلك البيانات واستغلالها، كل ذلك يمثل انتهاك صريح للخصوصية وللبيانات الشخصية للمستخدم، حتى ولو وافق المستخدم على استغلال بياناته وذلك من خلال موافقته على بنود سياسة الخصوصية المتعلقة بتلك المواقع، لأنه يتوافر هناك نوع من أنواع الإكراه المعنوي أو الاستخدام غير العادل لتلك البيانات، مما يعصف بالرضاء والموافقة الصادر من المستخدم ويجعلها غير شرعي ([٢٧]).

٢٧) جيهان فقيه، حماية البيانات الشخصية في الإعلام الرقمي، مجلة العلوم الإنسانية، ع٧، ٢٠١٧، ص ١٥٠.

(ISSN: 2356 - 9492)

وهناك إشكالية متعلقة **بالمسئولية الجنائية الواقعة على عاتق الفيس بوك في حالة تسريب بيانات مستخدميه؟**

كما ذكرنا سابقاً، يقوم فيس بوك بجمع بيانات متعلقة بمستخدميه، سواء عن طريق ملفات تعريف الارتباط الخاصة بهم، أو عن طريق خوارزمياته المعقدة التي تستخدم تقنيات الذكاء الاصطناعي، من أجل الحصول على اهتمامات وتفضيلات المستخدمين، ووضحنا أن حصوله على تلك البيانات في أغلب الأحوال يكون صحيحاً قانوناً ولا يشكل جريمة – وذلك بسبب حصوله على موافقة المستخدمين – ولكن هنا الأمر متعلق بتسريب البيانات، وفى الإجابة على هذه النقطة سوف نقسمها إلى جزئيتين:

أولاً: في حال تسريب بيانات المستخدمين بموافقة الفيس بوك

كأن يقوم الفيس بوك ببيع بيانات هؤلاء المستخدمين لشركات أخرى، فيكون هنا مسئولاً مسئولية كاملة، ومرتبكاً لجريمة انتهاك الخصوصية والتي نص عليها القانون

ثانياً: في حال تسريب بيانات المستخدمين عن طريق اختراق أمنى تعرض له الموقع

تكون المسئولية الواقعة على عاتق الفيس بوك مسئولية جزئية وغير كاملة، حيث أن الاختراق تم بدون قصده عن طريق استغلال ثغرات أمنية، وبالتالي المسئولية هنا تقع على من قام بالاختراق والحصول على تلك البيانات([٢٨])، وتقتصر مسئولية الفيس بوك

آلاء بنت سعيد بن ناصر، حماية البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي، رسالة ماجستير، ٢٠١٥، ص ٣٣.

٢٨) لا تزال فضيحة فيسبوك تستحوذ على اهتمام الناس خاصة مع الكشف عن المزيد من الأخبار المقلقة لمستخدمي الموقع؛ آخرها تصريحات لبعض المؤثرين في مجال صناعة التكنولوجيا تعليقا على تسريب بيانات مستخدمي موقع فيس بوك لصالح شركة كامبريدج أناليتيكا وهي شركة استشارية عملت في حملة دونالد ترامب الانتخابية لعام ٢٠١٦. حيث طالب كل من الرئيس التنفيذي لشركة آبل تيم كوك والمديرة التنفيذية لأي بي إم، جيني روميتي طالبا بمزيد من الإجراءات لحماية البيانات الشخصية للمستخدمين. كوك علق على فضيحة فيس بوك قائلا إن الموقف كارثي ومخيف للغاية، واصفا الحدث بالجلل كما شدد على ضرورة وضع لوائح وتنظيمات أكثر صرامة لحماية خصوصية المستخدمين. فيما أكدت المديرة التنفيذية لأي بي إم أن مستخدمي فيس بوك يجب أن يتمتعوا بضمانات أكثر لحمايتهم.
لتفاصيل أكثر راجع:

على مجرد عدم استخدامه أنظمة حماية كافية لحفظ بيانات مستخدميه، حيث يقع على عاتق من يحصل على بيانات متعلقة بخصوصية شخص أن يحافظ عليها ولا يتركها تقع في يد شخص آخر غير مصرح له بالحصول على تلك البيانات(٢٩)، ويطبق عليه القانون المصري رقم (١٧٥) لسنة (٢٠١٨) في شأن مكافحة جرائم تقنية المعلومات لأنه نصَّ في المادة الثالثة المتعلقة بنطاق تطبيق القانون من حيث المكان: " ٢- إذا كان المجنى عليهم أو أحدهم مصرياً"(٣٠).

حماية البيانات الشخصية في عالم التجارة الإلكترونية:

تثير تطبيقات ومواقع التجارة الإلكترونية إشكاليات عديدة بشأن توفير الحماية القانونية للمستهلك عند قيامه بالتعاقد الإلكتروني المتمثل غالبًا في شكل شراء منتجات تباع أون لاين، ومن أهم هذه الإشكاليات تلك المتعلقة بحمايته من الاطلاع على بياناته التي يقدمها قبل أو أثناء عملية الشراء، كما يتم الوصول إلى البيانات الشخصية للمستهلك عن طريق تتبع استخدامه للإنترنت للكشف عن رغباته، ولذلك كان المستهلك في حاجة لتوفير حماية قانونية للبيانات الأسمية أو الشخصية (٣١).

---

١. مقال على موقع epic.org، تحت عنوان "In re Facebook - Cambridge Analytica " على هذا الرابط، https://epic.org/privacy/facebook/cambridge-analytica/ ، تمت زيارته بتاريخ ١ أبريل ٢٠٢١,

2. Margi Murphy, Millions of Facebook user records exposed in data breach, 3 APRIL 2019. https://www.telegraph.co.uk/technology/2019/04/03/millions-facebook-user-records-exposed-data-breach/، تمت زيارته بتاريخ ٤ أبريل ٢٠٢١,

3. Nicholas Confessore, Cambridge Analytica and Facebook: The Scandal and the Fallout So Far, 4 April 2018. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html
، تمت زيارته بتاريخ ٤ أبريل ٢٠٢١.

٢٩) نص القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات في المادة (٢) على التزامات وواجبات مقدم الخدمة: بند (٣) "تأمين البيانات والمعلومات بما يحافظ على سريتها، وعدم اعتراضها أو اختراقها أو تلفها".

٣٠) د. يحيى إبراهيم دهشان، المسئولية الجنائية عن جرائم الذكاء الاصطناعي، مجلة الشريعة والقانون - كلية القانون جامعة الامارات، العدد ٨٢، ابريل ٢٠٢٠، ص ٣٣.

٣١) أمين أعزان، حماية البيانات الشخصية للمستهلك الإلكتروني، مجلة الاقتصاد والمستهلك، ع ٥,٦، ٢٠١٣، ص ٢٠.

(ISSN: 2356 - 9492)

ويستخدم بعض التجار البيانات الأسمية والعناوين الإلكترونية عبر الإنترنت لإغراق المستخدمين بالدعاية لمنتجاتهم، بما قد يؤدي إلى إعاقة شبكة الاتصالات أحياناً. كما يمكن استخدام المعلومات التي تمت معالجتها في غير الأغراض المخصصة لها، مما أدى إلى المطالبة إلى أن تكون المعاملات غير أسمية، وأن تكون عملية تتبع الأثر خاضعة للمراقبة. وخصوصاً أنه ظهرت جهات متخصصة في التعامل والإتجار في البيانات الشخصية المتواجدة على قواعد البيانات الخاصة ببعض الجهات([٣٢]).

محو البيانات الشخصية بين الإباحة والتجريم:

يعد الحق في محو البيانات الشخصية من الحقوق المستحدثة في لائحة حماية البيانات الأوروبية GDPR([٣٣])، وإن كان هذا الحق الذي يعرف أيضا بالحق في النسيان كان معروفا في التشريعات الوطنية الأوروبية منذ مدة طويلة عن طريق ما تضمنته هذه التشريعات من إعطاء الفرصة للأشخاص المدانين في جرائم معينة في محو ماضيهم القضائي وإعادة إدماجهم في المجتمع وبدء حياتهم من جديد.

إن الهدف الرئيسي في إقرار الحق في المحو يتمثل في إعطاء الأفراد فرصة للتخلص من بعض الأمور التي تسبب لهم مضايقات وتمنعهم من تطوير شخصيتهم بصورة طبيعية وربما تمنعهم في كثير من الأحوال من تكوين علاقات جديدة أو الحصول على وظيفة معينة أو مسكن خاص بسبب طبيعة الانترنت المعروفة في أنه لا

---

٣٢) في مصر، يستخدم أكثر من ٥٠ مليون مصري الإنترنت وفقا للأرقام المعلنة من وزارة الاتصالات المصرية في ٢٠٢٠ وهو رقم يساوي نصف عدد السكان المصريين تقريبًا، كما قفز حجم التجارة الإلكترونية في مصر في ذات العام الى نحو ملياري دولار، وهي أرقام تؤكد نمو هذه السوق بشكل كبير وتؤكد ضرورة حماية رواد هذه السوق حفاظا على الثقة فيها، وبالتالي ضمان استمرارية ازدهارها .

https://www.idsc.gov.eg/IDSC/DocumentLibrary/View.aspx?id=4589 تمت زيارته بتاريخ ٢٠٢١/٨/٢١.

33) GDPR, Article 17, Right to erasure (‘right to be forgotten’): 1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies.

https://eur-lex.europa.eu/eli/reg/2016/679/oj.٢٠٢١/٧/١٥ تمت زيارته بتاريخ

ينسى أبدا، وبالتالي يعد هذا الحق مظهرا من مظاهر سيطرة الفرد على بياناته الشخصية والتي تعد أحد مظاهر الخصوصية في العصر الرقمي.

ولقد كان لحكم محكمة العدل الأوروبية في قضية GOOGLE SPAIN C-131/12 في ١٣ مايو ٢٠١٤ دور هام وبالغ في الاعتراف بالحق في المحو على مستوي الاتحاد الأوروبي، حيث يعد أول حكم يتضمن الاعتراف قضائيا بالحق في المحو([٣٤]).

ولكن هنا تثار إشكالية متعلقة بـ هل محو البيانات الشخصية حق مطلق لصاحب الشأن؟

إذا كان الحق في المحو يعد أحد مظاهر الخصوصية في العصر الرقمي ([٣٥]) فإن ممارسة هذا الحق تحكمها ضوابط معينة، فالحق في المحو ليس مطلقا كونه يتداخل مع غيره من الحقوق المتعارضة كالحق في حرية التعبير والوصول إلى المعلومات.

وتثار إشكالية أخرى متعلقة بمدي إمكانية تطبيق الحق في المحو في أنظمة النسخ الاحتياطي وكذلك النطاق الجغرافي لتطبيق الحكم الصادر بمحو البيانات والتي كان للآراء الفقهية والأحكام القضائية دور كبير في توضيح كيفية التعامل معها وحلها. وعلى المستوي القضائي لعبت المحكمة الأوروبية لحقوق الإنسان ECTHR ومحكمه العدل الأوروبية والمحاكم المحلية الأوروبية وهيئات حماية البيانات الوطنية دورا هاما في

34) Judgment of the Court (Grand Chamber), 13 May 2014 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González Request for a preliminary ruling from the Audiencia Nacional Personal data — Protection of individuals with regard to the processing of such data — Directive 95/46/EC — Articles 2, 4, 12 and 14 — Material and territorial scope — Internet search engines — Processing of data contained on websites — Searching for, indexing and storage of such data — Responsibility of the operator of the search engine — Establishment on the territory of a Member State — Extent of that operator's obligations and of the data subject's rights — Charter of Fundamental Rights of the European Union — Articles 7 and 8 Case C-131/12

تمت زيارته بتاريخ ٢٠٢١/٧/٢٠ https://curia.europa.eu/juris/liste.jsf?num=C-131/12

٣٥) رضوان اسخيطة، التحقيق الجنائي الرقمي في ضوء قوانين حماية البيانات الشخصية، مجلة الندوة للدراسات القانونية، ع٢٦، ٢٠١٩، ص ٨.

(ISSN: 2356 - 9492)

توضيح المعايير المستخدمة لإجراء التوازن بين الحق في الخصوصية وحرية الجمهور للوصول للمعلومات وحرية التعبير وفقا للمعايير التي وضعتها هذه المحاكم ويتم تطبيقها بدقة إزاء التعامل مع قضايا محو البيانات الشخصية ([٣٦]).

قوانين حماية البيانات الشخصية:

هي تلك القوانين التي تهتم بحماية البيانات الشخصية للأفراد وخصوصيتهم ما يمنع استعمالها بشكل مباشر أو غير مباشر في غير الغرض الذي تم جمعها لأجله. بجانب الحق في محوها أو تحديثها، والوصول إليها، وتتبع كيفية استغلالها، ووقف أو تقييد معالجتها.

وبالطبع توجد في هذا المجال قوانين لها صفة الزامية، منها القوانين العربية والمتمثلة في قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠([٣٧])، وقانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨([٣٨])، وقانون رقم (٢٦) لسنة ٢٠١٥ بشأن تنظيم نشر وتبادل البيانات في إمارة دبي، وقانون رقم ٣٠ لسنة ٢٠١٨ بإصدار قانون حماية البيانات الشخصية في البحرين. ومنها القوانين الأجنبية المتعلقة بحماية البيانات الشخصية قانون حماية البيانات بالمملكة المتحدة

---

٣٦) محمد أحمد سلامة مشعل، الحق في محو البيانات الشخصية: دراسة تحليلية في ضوء لائحة حماية البيانات بالاتحاد الأوروبي GDPR وأحكام المحاكم الأوروبية، مجلة الدراسات القانونية والاقتصادية، مج٣, ع٢، ٢٠١٧، ص ٤١.

٣٧) جاء القانون رقم ١٥١ لسنة ٢٠٢٠ بإصدار قانون حماية البيانات الشخصية المصري متوجا للجهود المصرية الساعية لدفع عجلة التجارة الإلكترونية في البلاد. وقد جاء القانون في ٤٩ مادة بخلاف مواد الإصدار، مقسّمًا إلى أربعة عشر فصلاً تناولت جميع أحكامه وتصنيفات المخاطبين بها وحقوقهم وواجباتهم.

٣٨) يوجد العديد من التشريعات المصرية التي نظمت حماية البيانات الشخصية في بعض موادها ونذكرها بعضًا منها:

- قانون التوقيع الالكتروني رقم ١٥ لسنة ٢٠٠٤ في المادة رقم ٢١.
- قانون البنك المركزي رقم ١٩٤ لسنة ٢٠٢٠ في المادة رقم ١٦.
- قانون الطفل رقم ١٢ لسنة ١٩٩٦ في المادة رقم ١١٦ مكرر.
- قانون العقوبات المصري رقم ٥٨ لسنة ١٩٣٧ في المادة ٣٠٩ مكرر.
- قانون التأمين الصحي رقم ٢ لسنة ٢٠١٨ في المادة رقم ٤٧.
- قانون حماية المستهلك رقم ١٨١ لسنة ٢٠١٨ في المادة رقم ٢٩
- قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣ في المواد رقم ٢٨ و٢٩ و٥٨ و٦٤.
- قانون الأحوال المدنية رقم ٤٤٣ لسنة ١٩٩٤ في المادة رقم ١٣.

الصادر في ٢٠١٨([٣٩])، والذي وضع ضوابط كيفية استخدام المعلومات الشخصية عن طريق المنظمات والشركات أو الحكومة ([٤٠]). وأيضًا لائحة حماية البيانات العامة للاتحاد الأوروبي GDPR ([٤١]). وقانون حماية البيانات الياباني رقم ١١/٢٢ لسنة ٢٠١١، وقانون حماية النظم المعلوماتية والشبكات الياباني رقم ١٧/٧ لسنة ٢٠١٧.

على الطرف الآخر ما تزال التشريعات الخاصة بحماية البيانات الشخصية تقتصر في الكثير من الدول على ما تضمنته الدساتير من قواعد عامة تشمل حماية كل ما يمس بضرر بالإنسان ولا تختص بحماية البيانات بشكل خاص إنما يتم العمل بها حسب القاعدة الشهيرة في القانون المدني "كل خطأ سبب ضرر للغير يلزم فاعله التعويض".

المبحث الثاني
البيانات الحكومية

تعد البيانات الحكومية هي اللاعب الرئيس في التحول الرقمي والانتقال من مفهوم الحكومة التقليدية إلى مفهوم الحكومة الالكترونية والحكومة الذكية، والذي اضحى ضرورة في بلداننا العربية على وجه الخصوص والتي تقوم بإنتاج كمية كبيرة من البيانات يمكن استخدامها في تطوير البنية التحتية وتنمية مختلف القطاعات كالاقتصاد والصحة والتعليم.

وتقوم الجهات الحكومية المختلفة بإنتاج وتجميع كميات ضخمة من البيانات التي تشمل شتى جوانب الحياة فتتنوع البينات ما بين بيانات قانونية وبيانات متعلقة بالصحة والتعليم وبيانات جغرافية وإحصاءات العمالة والتوظيف ... إلخ، وهذه البيانات الحكومية

---

39) Data protection act 2018.

٤٠) بموجب قانون حماية البيانات لعام ٢٠١٨، يحق للشخص معرفة المعلومات التي تخزنها الحكومة والمنظمات الأخرى عنه.

٤١) "GDPR" اختصار لـ"General Data Protection Regulation " وهي مجموعة من القواعد والقوانين تم وضعها من قبل الإتحاد الأوروبي لحماية حقوق جميع مواطني الاتحاد. وتمت الموافقة عليها في ١٤ أبريل ٢٠١٦ من قِبل المفوضية الأوروبية. وطبقت اللائحة في مايو ٢٠١٨ وتمنح اللائحة حق المستخدم بإزالة بياناته، بشكل جزئي أو كامل، من شبكة الإنترنت، ما يعتبر خطوة متقدمة وفقا لـ" يورونيوز" في ٢٧ يناير ٢٠١٧. ووفق اللائحة الأساسية فإنه يجب موافقة المستخدمين أيضا على التعامل مع بياناتهم وفقالـ"DW " في ١٧ مارس ٢٠٢٠.

(ISSN: 2356 - 9492)

قد تكون ذات قيمة كبيرة للمؤسسات غير الحكومية، ومنظمات المجتمع المدني، والقطاع الخاص، والمواطنين الذين يمكنهم استخدامها لأغراض سياسية، وتجارية. وقد اتجهت الحكومات في السنوات الأخيرة لنشر تلك البيانات الحكومية على الإنترنت معتمدة على استثمار التطور في تكنولوجيا المعلومات والاتصالات وبموجب رخصة مفتوحة تسمح لأي شخص أن يقوم باستخدامها، وإعادة استخدامها ومعالجتها، وإعادة توزيعها دون قيود قانونية أو تقنية بشرط الإشارة إلى مصدرها؛ وهذا يعد سلاح ذو حدين (٤٢).

وقد عرف قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ البيانات حكومية بأنها بيانات متعلقة بالدولة أو إحدى سلطاتها، أو أجهزتها أو وحداتها، أو الهيئات العامة، أو الهيئات المستقلة أو الأجهزة الرقابية، أو غيرها من الأشخاص الاعتبارية العامة وما في حكمها، والمتاحة على الشبكة المعلوماتية أو على أي نظام معلوماتي أو على حاسب أو ما في حكمها (٤٣).

البيانات الحكومية بين الافصاح والسرية:

يوجد نوعان من البيانات الحكومية: أولهما البيانات الحكومية المفتوحة، والثاني البيانات الحكومية السرية، نجد أن الأول دائما ما تلتزم الحكومات بالإفصاح عنه على عكس الثاني الذي يغلب عليه طابع السرية لدرجة تجريم الافصاح عنه.

ومع انتشار التحول الرقمي وتوسع الدول في استخدام التكنولوجيا، انتشرت الدعوات المتعلقة بضرورة قيام الحكومة بنشر بيانات ومعلومات في شتى المجالات من أجل تسهيل عملية الرقابة والمتابعة لأنشطة الحكومة بالإضافة إلى تقييم أداء الحكومات، والعديد من المميزات الأخرى المرتبطة بنشر تلك البيانات.

ودفع ذلك الدول إلى انشاء منصات ومواقع الكترونية من أجل عرض تلك البيانات والاحصائيات، على سبيل المثال في مصر يوجد بوابة الحكومة المصرية (٤٤). وفي السعودية يوجد المنصة الوطنية الموحدة (٤٥). وفي الإمارات هناك البوابة الرسمية

٤٢) دراسة نقدية لقانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، مرجع سابق، ص ٦٥.
٤٣) مادة رقم (١) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.
44) https://www.egypt.gov.eg/
45) https://www.my.gov.sa/

لحكومة دولة الإمارات العربية المتحدة ([٤٦]). ومن الجدير بالذكر أيضًا أن تلك المواقع تقوم بتقديم الكثير من الخدمات المرتبطة بالحياة اليومية للمواطنين.

ومن أمثلة البيانات الحكومية المسموح بنشرها وتداولها: الإحصاءات الوطنية والقوانين والبيانات المتعلقة بالموازنة، ومعلومات التعليم والنقل والصحة، والبيانات الجغرافية. ومن أمثلة البيانات الحكومية غير المسموح بنشرها وتداولها: البيانات الشخصية والبيانات السرية المتعلقة بالأمن القومي.

وهناك العديد من التشريعات في كل دولة تنظيم تلك العملية، وتوضح أي من البيانات المسموح بتداولها والافصاح عنها، وأي منها غير المسموح بتداولها وتضفى عليها صفة السرية وتضع عقوبة لمنتهك هذا التحريم ([٤٧]).

فيوجد في أمريكا قانون **حرية المعلومات الأمريكي** (FOIA) وهو قانون فيدرالي ينظم حقوق الأفراد في الاطلاع على البيانات الحكومية، ويحدد أيا منها المسموح بالإفصاح عنها وأيا منها يلتزم فيها بالسرية وعدم الإفصاح، وهذا القانون تمّ إنشاؤه بموجب الأمر التنفيذي ١٣٣٩٢ في ١٤, ديسمبر ٢٠٠٥([٤٨]).

وعن الوضع في مصر فلا يوجد قانون متخصص ينظم هذا الأمر، ونجد أن تنظيمه على المشاع بين نصوص ببعض القوانين العامة أو قرارات جمهورية، مثل قانون العقوبات المصري رقم ٥٨ لسنة ١٩٣٧، والقانون رقم ١٢١ لسنة ١٩٧٥ بشأن المحافظة على الوثائق الرسمية للدولة وتنظيم أسلوب نشرها، وقرار رئيس الجمهورية رقم ٦٢٧ لسنة ١٩٨١ بشأن إنشاء مراكز المعلومات والتوثيق في الأجهزة الإدارية للدولة

46) https://u.ae/

٤٧) **من القوانين التي تنظم ذلك في مصر**: قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨، قانون العقوبات المصري رقم ٥٨ لسنة ١٩٣٧. قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠.

من القوانين التي تنظم ذلك في عمان: قانون المطبوعات والنشر ولائحته التنفيذية، قانون المنشآت الخاصة للإذاعة والتلفزيون ولائحته التنفيذية، قانون مكافحة جرائم تقنية المعلومات، قانون تنظيم التزامات العاملين في كافة مؤسسات الدولة وأعضاء المجالس المعينة والمنتخبة، القانون الإحصائي، قانون الجزاء العماني.

48) Executive Order 13392 of December 14, 2005, Improving Agency Disclosure of Information, online: https://fas.org/irp/offdocs/eo/eo-13392.htm site visited on: 17/1/2021.

(ISSN: 2356 - 9492)

والهيئات العامة وتحديد اختصاصاتها، وقرار رئيس الجمهورية بالقانون رقم ٣١٣ لسنة ١٩٥٦ بحظر نشر أية أخبار عن القوات المسلحة، وقانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨، وقانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠.

ولذا نتمنى صدور قانون متخصص في مصر لتنظيم إتاحة البيانات والمعلومات الحكومية للمواطنين، وهذا حق أكده الدستور المصري في المادة ٦٨ حيث نصت على "المعلومات والبيانات والإحصاءات والوثائق الرسمية ملك للشعب، والإفصاح عنها من مصادرها المختلفة، حق تكفله الدولة لكل مواطن، وتلتزم الدولة بتوفيرها وإتاحتها للمواطنين بشفافية، وينظم القانون ضوابط الحصول عليها وإتاحتها وسريتها، وقواعد إيداعها وحفظها، والتظلم من رفض إعطائها، كما يحدد عقوبة حجب المعلومات أو إعطاء معلومات مغلوطة عمداً. وتلتزم مؤسسات الدولة بإيداع الوثائق الرسمية بعد الانتهاء من فترة العمل بها بدار الوثائق القومية، وحمايتها وتأمينها من الضياع أو التلف، وترميمها ورقمنتها، بجميع الوسائل والأدوات الحديثة، وفقاً للقانون"([٤٩]). وأيضًا أكدته العديد من أحكام المحاكم المصرية ([٥٠]).

<u>الأرشيف الإلكتروني:</u>

يتواجد دائما داخل جميع الهيئات والمصالح الحكومية قسم يسمى الأرشيف، يتم حفظ نسخه من الأوراق والمستندات به، للاستدلال بها مستقبلا والرجوع لها عند الضرورة، ويمثل هذا الأرشيف ركنا جوهريا بالمؤسسة. ومع التحول الرقمي أصبح وجود

٤٩) دستور جمهورية مصر العربية لسنة ٢٠١٤، الجريدة الرسمية - العدد ٣ مكرر (أ) - في ١٨ يناير سنة ٢٠١٤.

٥٠) قضت الدائرة الأولى بمحكمة القضاء الإداري، في الدعوى رقم ٥٩٤٣٩ لسنة ٦٧ قضائية "إن الحق في المعرفة هو حق من حقوق الإنسان التي تمثل أمرًا بالغ الأهمية، وأن تنظيم حق المواطنين في الوصول إلى المعلومات، والبيانات المتعلقة بالتسويات التي تُجرى على المال العام، من شأنه تعزيز مبدأ الشفافية، ويضمن طرقًا أفضل لإتمام هذه التسويات على أحسن وجه، ويقضي على الفساد، ويؤدي إلى اتخاذ قرارات مدروسة من القائمين على أمر هذه التسويات، ويجعل المواطنين مُشاركين فيها، باعتبار أن هذه التسويات تؤثر تأثيرًا مباشرًا في حياتهم وأوضاعهم الاقتصادية، ويضع قادتهم أمام المساءلة، ومن ثم يتعين على الدولة أن تنشئ الأطر القانونية القوية التي تحمي حق الأفراد في الوصول إلى هذه المعلومات –وبما يضمن الحفاظ على سريتها- وبالتالي يؤدي إلى خلق مجتمع مدني نشط قادر على تحقيق رقابة شعبية حقيقية، وفعالة على تصرفات الحكومة في أموال الدولة"

أرشيف ورقى بالمؤسسات غير مقبول وظهر ما يعرف بالأرشيف الالكتروني والذي يعنى تصوير جميع الأوراق الموجودة بالأرشيف ورفعها على الحاسب الآلي (لتكون متاحة بصورة مغلقة)، أو تحميلها على السحابة الإلكترونية (لتكون متاحة بصورة أوسع بجميع فروع المؤسسة على مستوى الدولة) ([٥١]).

وقد ينتج عن هذا التحول إلى الأرشيف الإلكتروني، ظهور العديد من الإشكاليات التي يجب عرضها وتصور حلول لها، ومنها:

- هل تتوفر السرية والخصوصية للبيانات الموجودة بهذا الأرشيف الإلكتروني أم لا؟
- هل تتوافر الحماية الكافية لهذا الأرشيف ضد عمليات القرصنة والاختراق؟
- هل توجد إمكانية لحماية البيانات والملفات الموجودة في الأرشيف من التلاعب سواء بالحذف أو الإضافة أو تغيير لبيانات بها؟

كل هذه الإشكاليات تمثل جوهر حماية البيانات في ظل التحول الرقمي.

اتلاف المستندات الالكترونية:

ومن النقاط التي يلزم توضيحها قبل الانتقال من الحديث عن الأرشيف الالكتروني إلى نقطة آخر، هي أهمية حفظ الملفات والمستندات الحكومية بجودة عالية، فقيام الحكومة بتطبيق نظام الأرشيف الإلكتروني يضم بين طياته إشكاليات جوهرية وأهمها جودة وحجم الصور والمستندات التي يتم حفظها، فهناك علاقة طردية بين حجم الصورة

---

٥١) بدأت الولايات المتحدة الأمريكية مشروع الأرشفة الإلكترونية في محاكم الولايات المتحدة الأمريكية في عام ١٩٨٨، كان الهدف من المشروع هو أرشفة جميع القضايا والمستندات القضائية إلكترونياً بحيث يمكن استرجاعها بسهولة وسير بشكل إلكتروني من خلال الحاسب الآلي واستطاعت الولايات المتحدة الأمريكية أرشفة جميع القضايا والمستندات والآن يتم أرشفة القضايا والمستندات القضائية بشكل يومي من خلال منظومة الأرشفة القضائية. تعد عملية الأرشفة الإلكترونية خطوة هامة في عملية التحول الرقمي وعملية التجهيز للمحكمة الإلكترونية.

25 Years Later, PACER, Electronic Filing Continue to Change Courts, Published on: December 9, 2013, https://www.uscourts.gov/news/2013/12/09/25-years-later-pacer-electronic-filing-continue-change-courts

(ISSN: 2356 - 9492)

وجودتها، حيث كلما قل الحجم قلت الجودة والعكس ([٥٢])، وحفظ المستند بجودة منخفضه قد يترتب عليه طمس أو عدم المقدرة على قراءة البيانات الموجودة بالصورة، وهذا يتشابه مع جريمة اتلاف المستندات.

حيث تعاقب المواد ١٥١ . ١٥٣ من قانون العقوبات المصري على اتلاف الأوراق المودعة في المخازن العامة ولو لم تكن هذه المواد موجودة لكانت هذه الجرائم إذا ارتكبت عن قصد يعاقب عليها بمقتضى النصوص القانونية التي تعاقب على السرقة وخيانة الأمانة وإتلاف الأوراق. ولكن وجود الأوراق المتلفة في مخزن عام يجعل لهذه الأفعال صفة خاصة يبرر إخراجها من الأحكام العامة. ذلك بأن الشارع أعتبر أن المخزن العام هو حرم مقدس وأن كل اختلاس أو اتلاف يرتكب فيه من شأنه الاخلال بالثقة العامة والمساس بالسلطة التي أقامت ذلك المخزن. ومن أجل ذلك نص على هذه الأفعال في نفس الباب الذي يعاقب على فك الأختام. **ولذا يجب تحديث النص بإضافة المستندات المودعة بالأرشيف الالكتروني حتى يتم تطبيق هذا النص عليها، ولا يتم الرجوع للقواعد العامة.**

ويمكننا عرض تصور لعناصر جريمة اتلاف المستندات الالكترونية:

تتكون هذه الجريمة من أربعة عناصر وهي:

(١)حصول إتلاف.

(٢)أن يكون الشيء المتلف أوراقاً أو سندات أو سجلات أو دفاتر متعلقة بالحكومة أو أوراق مرافعة قضائية.

(٣)أن تكون هذه الأشياء محفوظة بطريقة الكترونية معدة لحفظها.

---

٥٢) أدى الانتشار الهائل للرقمنة إلى نمو هائل في حجم البيانات بحيث أنه على الرغم من زيادة السعة، لا تزال هناك اختناقات في نقل البيانات. وتتوقع التقديرات أن حجم البيانات المنتجة عالميًا يمكن أن يتضاعف بمقدار عشرة أضعاف عام 2025، مقارنة بعام ٢٠١٦، والذي صل إلى ١٦٣ زيتابايت، أي ما يعادل ٤١ ألف مليار قرصDVD .

Hippmann S., Klingner R., Leis M., Digitization – Areas of Application and Research Objectives. In: Neugebauer R. (eds) Digital Transformation. Springer Vieweg, Berlin, 2019, p. 11.

(٤)إهمال الجاني أو سوء قصده.

وبعرض هذه العناصر نكون قد شرحنا ضمنيا ركني الجريمة المادي والمعنوي.

أولا – الفعل المادي: والمتمثل في اشتراط حدوث اتلاف

ثانيا – نوع الشيء المتلف: يشترط تحديد الشيء المتلف على سبيل الحصر ويتمثل في الأوراق والسندات والسجلات والدفاتر المتعلقة بالحكومة وأوراق المرافعة القضائية، والمحفوظة بطريقة الكترونية.

فالأوراق والدفاتر المتعلقة بالحكومة هي التي لها صفة عامة. وقد حكم بأن دفاتر قسائم الزواج وشهادات الطلاق المسلمة الى المأذونين هي دفاتر متعلقة بالحكومة لأنها معدة لأمر عام هو اثبات الزواج أو الطلاق (٥٣). وأما أوراق المرافعة القضائية فتشمل كل ورقة يكون وجودها في ملف الدعوى من مستلزمات السير في القضية والمرافعة فيها، وليست قاصرة على أوراق المرافعات كما قد يتبادر إلى الذهن لأول وهلة (٥٤). وقد وقد حكم بأن المقصود بالأوراق المنصوص عليها في المادة ١٥١ عقوبات، هي الأوراق المودعة بالقضايا التي يحصل من سرقتها ضرر لمودعيها لا الأوراق الادارية والقضائية التي يتيسر للإنسان استخراج صور مطابقة لها (٥٥).

ثالثا – الحفظ الالكتروني: يشترط أن يكون الشيء المتلف محفوظاً بطريقة إلكترونية.

رابعا – الاهمال أو سوء القصد: يجب التفرقة في العقاب بين فعل الشخص المعهود اليه بحفظ الشيء وفعل غيره. ويفترض إهمال الشخص المعهود اليه بحفظ الشيء بمجرد عدم تقديمه له. ولكن لهذا الشخص أن يثبت أن سرقة الشيء أو إتلافه لم يكن نتيجة إهماله.

ومن أحكام محكمة النقض المصرية بخصوص مسئولية الموظف عن اتلاف المستندات التي في حوزته قضت بأنه "وكان الحكم قد أثبت أن مندوب الحجز كان

٥٣) حكم صادر عن محكمة فاقوس الجزئية ١٠ مارس سنة ١٩٠٩ مج ١٠ عدد ١١٧.
٥٤) نقض ١٣ فبراير سنة ١٩٣٠ قضية رقم ١١٣ سنة ٤٧ ق
٥٥) نقض ٤ فبراير سنة ١٨٩٩ ـ قضاء ٦ ص ١٣٠.

(ISSN: 2356 - 9492)

مكلفا بتوقيعه وأنه بعد أن وقعه وحرر محضره فعلا أقدم الطاعن على تمزيق هذا المحضر، ولا ريب أن هذا المحضر في يد المندوب المذكور يعد من الأوراق المكلف بحفظها والمشار إليها في المادة ١٥١ من قانون العقوبات، فإن ما انتهى إليه من تطبيق المادتين ١٥١ و١٥٢ على فعلته يكون صحيحا في القانون"([٥٦])

الدفع الإلكتروني:

يعد الدفع الإلكتروني من أحد عناصر التحول الرقمي داخل الحكومة، ويشمل بشقيه المصروفات (كالمرتبات) والنفقات (كمقابل الخدمة التي تقدمها الجهة الحكومية)، وغالبًا ما يثير تطبيق أي نظام جديد العديد من الإشكاليات أثناء التنفيذ، ولا يخفى على أحد أن كل هذا يضم بين طياته بيانات، سواء المتعلقة بالموظفين كرقم حساب بنكي وبيانات شخصية آخري، أو المتعلقة بالعميل الذي يتلقى الخدمة ([٥٧]).

والإشكالية التي تثار هنا هي: **كيف يتم حماية هذه البيانات؟ ومن يكون المسئول عن الخطأ إذا حدث أثناء اتمام هذه المعاملات المالية الالكترونية؟**

ومن الجدير بالذكر أن الدفع الالكتروني في صورته المتقدمة لا يتم عن طريق ماكينة الدفع أمام الموظف ولكن من خلال المواقع الالكترونية عن طريق استخدام العميل لهاتفه أو الكمبيوتر الشخصي الخاص به، وهذا يحتاج في بعض الأحيان أن يقوم العميل بإنشاء حساب شخصي له على الموقع الموجود به الخدمة قبل عملية الدفع، وهذا الحساب يتطلب وسيط كرقم هاتف أو ايميل شخصي من أجل انشاء الحساب([٥٨])، وهنا تظهر إشكاليه جديدة متعلقة بتشعب الخطوات حتى يتم الدفع وتعدد الأطراف المشاركين في اتمام عملية الدفع، فغالبا ما يحدث تعدد لأطراف المسئولين عن الخطأ الذى يحدث، ولذا يجب من الحكومة اللجوء إلى متخصصين لوضع جميع التصورات والاحتمالات التي قد تحدث (وهى ممكنه الحصر) لأنه المهندس الذى يضع نظام

٥٦) الطعن رقم ١٤٧٨ لسنة ٣٠ ق - جلسة ١٤ / ٢ / ١٩٦١ - مكتب فني ١٢ - جزء ١ - صـ ٢١٨.

57) Deng, Xinyang, and Tianhan Gao. "Electronic payment schemes based on blockchain in VANETs." IEEE Access 8 (2020): 38296-38303.

58) Oyelami, Lukman O., Sulaimon O. Adebiyi, and Babatunde S. Adekunle. "Electronic payment adoption and consumers' spending growth: empirical evidence from Nigeria." Future Business Journal 6.1 (2020): 1-14.

الكتروني يكون على علم بجميع عناصره من أجل سد الثغرات – التي قد يتم الولوج للنظام بطريق غير مشروعة – من خلالها.

وأهمية وضع جميع الفرضيات وتوضحيها، تسهل تحديد المسئول عن التقصير أو الضرر الذي يحدث، ويسهل محاسبته عليه، فالمسئولية الجنائية عن أي سلوك يرتكب تحتاج في البداية لخضوعها لمبدأ الشرعية – أي وجود نص جنائي يجرم السلوك المرتكب – ثم ربط النتيجة الاجرامية التي حدثت بالسلوك المرتكب وإظهار أن هذا السلوك هو المحدث لتلك النتيجة – أي وجود علاقة سببيه بينهم – وهذا يمثل عناصر الركن المادي، بخلاف بحث عناصر الركن المعنوي.

الفصل الثالث

جرائم البيانات المرتبطة بالتحول الرقمي

تتعدد وتتنوع صور جرائم البيانات التي ظهرت في عصر التحول الرقمي، ونعرض بعضا منها لتوضيح خطورة هذه الجرائم وأهمية التصدي لها ومكافحتها، وهذا يعد المغذى الحقيقي من وراء الدراسات الاستباقية للتطورات الحديثة وتأثيرها على أشكال ومعدل الجريمة، وذلك من أجل الحد من انتشار الجريمة سواء باتباع اجراءات احترازية معينة أو وضع عقوبات صارمة تحقق الردع العام داخل المجتمع.

ونعرض تباعا عدد من صور جرائم البيانات المرتبطة بالتحول الرقمي، ونصوص القوانين التي تجرمها، والأوصاف القانونية التي تنطبق عليها، وذلك من أجل توضيح أن المشرع دائما ما يكون له نظره مستقبليه، ودائما ما تضم القوانين التي يسوغها، نصوصا تتماشى مع جرائم مستقبليه لم تكن موجودة وقت صياغته للقوانين، بجانب تمهيد الطريق لمن يبحث عن قواعد التجريم والعقاب للجرائم المستحدثة والمرتبطة بالتحول الرقمي.

أولا – جريمة الانتفاع بدون حق بخدمات الاتصالات والمعلومات وتقنيتها:

تتمثل الجريمة في قيام المتهم بالانتفاع بدون وجه حق عن طريق شبكة النظام المعلوماتي أو إحدى وسائل تقنية المعلومات بخدمة اتصالات أو خدمة من خدمات قنوات البث المسموع أو المرئي. و**تقيد الاوراق** جنحة بالمواد ١، ١١، ١٢، ١٣، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

(ISSN: 2356 - 9492)

وتكون العقوبة المقررة الحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين بالإضافة إلى المصادرة. وعلى المحكمة أن تقضي بمصادرة الأدوات والآلات والمعدات والأجهزة مما لا يجوز حيازتها قانونا، أو غيرها مما يكون قد استخدم في ارتكاب الجريمة، أو سهل أو ساهم في ارتكابها.

وفي الحالات التي يتعين لمزاولة النشاط فيها الحصول على ترخيص من إحدى الجهات الحكومية، وكان الشخص الاعتباري المدان بأي جريمة منصوص عليها في هذا القانون لم يحصل على الترخيص فيحكم فضلا عن العقوبات المقررة بالغلق.

ثانيا – جريمة الدخول غير المشروع:

تتمثل الجريمة في أن المتهم دخل عمدا، أو دخل بخطأ غير عمدي وبقي بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه. و**تقيد الاوراق** جنحة بالمواد ١، ١١، ١٢، ١/١٤، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨

وتكون العقوبة المقررة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين بالإضافة إلى مصادرة الأدوات والآلات والمعدات والأجهزة والغلق.

كما تقيد الاوراق جنحة بالمواد ١، ١١، ١٢، ١/١٤-٢، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨

تحت وصف أن المتهم دخل عمدا، أو دخل بخطأ غير عمدي وبقي بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه وقد نتج عن ذلك الدخول إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي.

وتكون العقوبة المقررة الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين بالإضافة إلى مصادرة الأدوات والآلات والمعدات والأجهزة والغلق.

وتثار إشكالية متعلقة بـ: هل يجوز اختراق موقع الكتروني – كنوع من أنواع الدفاع الشرعي – في حالة قيامه بنشر محتوى يشكل انتهاك لخصوصية شخص ما (مثل صور او فيديو أو مؤلف له حقوق ملكية)، فهل يحق لهذا الأخير اختراق الموقع لحذف هذا المحتوي الذي يشكل انتهاك لخصوصيته) – أو لحذف بيانات شخصية منشورة عليه؟

ثالثا – جريمة تجاوز حدود الحق في الدخول:

تتمثل الجريمة في أن المتهم دخل إلى موقع أو حساب خاص أو نظام معلوماتي مستخدما حقا مخولا له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول. و**تقيد الاوراق** جنحة بالمواد ١، ١١، ١٢، ١٥، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨

وتكون العقوبة المقررة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين بالإضافة إلى مصادرة الأدوات والآلات والمعدات والأجهزة والغلق.

رابعا – جريمة الاعتراض غير المشروع:

تتمثل الجريمة في أن المتهم اعترض بدون وجه حق أي معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها. و**تقيد الاوراق** جنحة بالمواد ١، ١١، ١٢، ١٦، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

وتكون العقوبة المقررة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتين وخمسين ألف جنيه، أو بإحدى هاتين العقوبتين بالإضافة إلى مصادرة الأدوات والآلات والمعدات والأجهزة والغلق.

خامسا – جريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية:

تتمثل الجريمة في أن المتهم أتلف أو عطل أو عدل مسار أو ألغى كلياً أو جزئياً، متعمداً وبدون وجه حق البرامج والبيانات أو المعلومات المخزنة أو المعالجة أو المولدة أو المخلقة على أي نظام معلوماتي وما في حكمه، أيا كانت الوسيلة التي استخدمت في

(ISSN: 2356 - 9492)

الجريمة. و**تقيد الاوراق** جنحة بالمواد ١، ١١، ١٢، ١٧، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

وتكون العقوبة المقررة الحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين بالإضافة إلى مصادرة الأدوات والآلات والمعدات والأجهزة والغلق.

سادسا – جريمة الاعتداء على البريد الإلكتروني أو المواقع أو الحسابات الخاصة:

تتمثل الجريمة في أن المتهم أتلف أو عطل أو أبطأ أو اخترق بريدا إلكترونيا أو موقعا أو حسابا خاصا بآحاد الناس. و**تقيد الاوراق** جنحة بالمواد ١، ١١، ١٢، ١٨ /١، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

وتكون العقوبة المقررة الحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين بالإضافة إلى مصادرة الأدوات والآلات والمعدات والأجهزة والغلق.

تقيد الاوراق جنحة بالمواد ١، ١١، ١٢، ١٨ /١– ٢، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

تحت وصف أن المتهم أتلف أو عطل أو أبطأ أو اخترق بريدا إلكترونيا أو موقعا أو حسابا خاصا بأحد الأشخاص الاعتبارية هي.....

وتكون العقوبة المقررة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين. بالإضافة إلى مصادرة الأدوات والآلات والمعدات والأجهزة والغلق.

سابعا – جريمة الاعتداء على تصميم موقع:

تتمثل الجريمة في أن المتهم أتلف أو عطل أو أبطأ أو شوه أو أخفى أو غير تصاميم موقع خاص بشركة أو مؤسسة أو منشأة أو شخص طبيعي بغير وجه حق. و**تقيد الاوراق** جنحة بالمواد ١، ١١، ١٢، ١٩، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

وتكون العقوبة المقررة الحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين بالإضافة إلى مصادرة الأدوات والآلات والمعدات والأجهزة والغلق.

ثامنا – جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة:

تتمثل الجريمة في أن المتهم دخل عمدا، أو بخطأ غير عمدي وبقي بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعا أو بريدا إلكترونيا أو حسابا خاصا أو نظاما معلوماتيا يدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكا لها، أو يخصها. و**تقيد الاوراق** جنحة بالمواد ١، ١١، ١٢، ١/٢٠، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

وتكون العقوبة المقررة الحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.

تقيد الاوراق جناية بالمواد ١، ١١، ١٢، ١/٢٠ – ٢، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

تحت وصف أن المتهم دخل عمدا، أو بخطأ غير عمدي وبقي بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعا أو بريدا إلكترونيا أو حسابا خاصا أو نظاما معلوماتيا يدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكا لها، أو يخصها، وكان ذلك بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية.

وتكون العقوبة المقررة السجن، والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه.

وفي جميع الأحوال، إذا ترتب على أي من الأفعال السابقة إتلاف تلك البيانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي أو البريد الإلكتروني، أو تدميرها أو تشويهها أو تغييرها أو تغيير تصاميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها، أو إلغائها كليا أو جزئيا، بأي وسيلة كانت، تكون العقوبة السجن، والغرامة التي لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه.

(ISSN: 2356 - 9492)

تاسعا – جريمة الاعتداء على سلامة الشبكة المعلوماتية:

تتمثل الجريمة في أن المتهم تسبب متعمدا في إيقاف شبكة معلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها أو التشويش عليها أو إعاقتها أو اعتراض عملها أو أجرى بدون وجه حق معالجة إلكترونية للبيانات الخاصة بها. و**تقيد الاوراق** جنحة بالمواد ١، ١١، ١٢، ٢١ / ١، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

وتكون العقوبة المقررة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين.

تقيد الاوراق جنحة بالمواد ١، ١١، ١٢، ٢١ / ١ – ٢، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

تحت وصف أن المتهم تسبب بخطئه في إيقاف شبكة معلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها أو التشويش عليها أو إعاقتها أو اعتراض عملها أو أجرى بدون وجه حق معالجة إلكترونية للبيانات الخاصة بها.

وتكون العقوبة المقررة الحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.

تقيد الاوراق جناية بالمواد ١، ١١، ١٢، ٢١ / ١–٢–٣، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

تحت وصف أن المتهم تسبب متعمدا – بخطئه في إيقاف شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامة أو تمتلكها أو تدار بمعرفتها عن العمل أو تعطيلها أو الحد من كفاءة عملها أو التشويش عليها أو إعاقتها أو اعتراض عملها أو أجرى بدون وجه حق معالجة إلكترونية للبيانات الخاصة بها.

وتكون العقوبة المقررة السجن المشدد، وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه.

عاشرا – جرائم البرامج والأجهزة والمعدات المستخدمة في ارتكاب جرائم تقنية المعلومات:

تتمثل الجريمة في أن المتهم حاز أو أحرز أو جلب أو باع أو أتاح أو صنع أو أنتج أو استورد أو صدر أو تداول بأي صورة من صور التداول، أي أجهزة أو معدات أو أدوات أو برامج مصممة أو مطورة أو محورة أو أكواد مرور أو شفرات أو رموز أو أي بيانات مماثلة، بدون تصريح من الجهاز أو مسوغ من الواقع أو القانون، وكان ذلك بغرض استخدام أي منها في ارتكاب أو تسهيل ارتكاب أية جريمة من الجرائم المنصوص عليها في هذا القانون، أو إخفاء آثارها أو أدلتها أو ثبت ذلك الاستخدام أو التسهيل أو الإخفاء. و**تقيد الاوراق** جنحة بالمواد ١، ١١، ١٢، ٢٢، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

وتكون العقوبة المقررة الحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين بالإضافة إلى المصادرة والغلق.

حادي عشر – جرائم بواسطة أنظمة وتقنيات المعلومات وجرائم الاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإلكتروني:

تتمثل الجريمة في أن المتهم استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أو بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الإلكترونية. و**تقيد الاوراق** جنحة بالمواد ١، ١١، ١٢، ٢٣ /١، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

وتكون العقوبة المقررة الحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه، ولا تجاوز خمسين ألف جنيه أو بإحدى هاتين العقوبتين.

تقيد الاوراق جنحة بالمواد ١، ١١، ١٢، ٢٣ /١-٢، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨

تحت وصف أن المتهم استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أو بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الإلكترونية. وكان ذلك بقصد استخدامها في الحصول على أموال الغير أو ما تتيحه من خدمات.

(ISSN: 2356 - 9492)

وتكون العقوبة المقررة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين.

وتكون العقوبة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو إحدى هاتين العقوبتين، إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على تلك الخدمات أو مال الغير.

ثاني عشر – الجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإلكتروني:

تتمثل الجريمة في أن المتهم اصطنع بريدا إلكترونيا أو موقعا أو حسابا خاصا ونسبه زورا إلى شخص طبيعي أو اعتباري. و**تقيد الاوراق** جنحة بالمواد ١، ١١، ١٢، ٢٤ /١، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

وتكون العقوبة المقررة الحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز ثلاثين ألف جنيه أو بإحدى هاتين العقوبتين.

تقيد الاوراق جنحة بالمواد ١، ١١، ١٢، ٢٤ /١-٢، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

تحت وصف أن المتهم اصطنع بريدا إلكترونيا أو موقعا أو حسابا خاصا ونسبه زورا إلى شخص طبيعي أو اعتباري واستخدمه في أمر يسئ إلى ما نسب إليه.

وتكون العقوبة المقررة الحبس الذي لا تقل مدته عن سنة، والغرامة التي لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.

وإذا وقعت الجريمة على أحد الأشخاص الاعتبارية العامة، فتكون العقوبة السجن، والغرامة التي لا تقل عن مائة ألف جنيه، ولا تزيد على ثلاثمائة ألف جنيه.

ثالث عشر – الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي غير المشروع:

تتمثل الجريمة في أن المتهم اعتدى على أي من المبادئ أو القيم الأسرية في المجتمع المصري أو انتهك حرمة الحياة الخاصة، أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع

إلكتروني لترويج السلع أو الخدمات دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبارا أو صورا وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة. و**تقيد الاوراق** جنحة بالمواد ١، ١١، ١٢، ٢٥، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

وتكون العقوبة المقررة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين.

تقيد الاوراق جنحة بالمواد ١، ١١، ١٢، ٢٦، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨

تحت وصف أن المتهم تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى مناف للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه.

وتكون العقوبة المقررة الحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين.

<u>رابع عشر – الجرائم المرتكبة من مدير الموقع:</u>

تتمثل الجريمة في أن المتهم أنشا أو أدار أو استخدم موقعا أو حسابا خاصا على شبكة معلوماتية يهدف إلى ارتكاب أو تسهيل ارتكاب جريمة معاقب عليها قانوناً. و**تقيد الاوراق** جنحة بالمواد ١، ١١، ١٢، ٢٧، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

وتكون العقوبة المقررة الحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن مائة ألف جنيه، ولا تزيد عن ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين.

تقيد الاوراق جنحة بالمواد ١، ١١، ١٢، ٢٨، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

تحت وصف أن المتهم بصفته مسئول عن إدارة موقع أو حساب خاص أو بريد إلكتروني أو نظام معلوماتي أخفى أو عبث بالأدلة الرقمية لإحدى الجرائم المنصوص

(ISSN: 2356 - 9492)

عليها في هذا القانون والتي وقعت على موقع أو حساب أو بريد إلكتروني بقصد إعاقة عمل الجهات الرسمية المختصة.

وتكون العقوبة المقررة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.

تقيد الاوراق جنحة بالمواد ١، ١١، ١٢، ٢٩ /١، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨

تحت وصف أن المتهم بصفته مسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإلكتروني أو النظام المعلوماتي عرض أيا منها لإحدى الجرائم المنصوص عليها في هذا القانون – تحدد الجريمة –.

وتكون العقوبة المقررة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.

تقيد الاوراق جنحة بالمواد ١، ١١، ١٢، ٢٩ /٢، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

تحت وصف أن المتهم بصفته مسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإلكتروني أو النظام المعلوماتي تسبب بإهماله في تعرض أي منها لإحدى الجرائم المنصوص عليها في هذا القانون، وكان ذلك بعدم اتخاذه التدابير والاحتياطيات التأمينية الواردة في اللائحة التنفيذية لهذا القانون.

وتكون العقوبة المقررة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين.

خامس عشر – جرائم مقدمي الخدمة:

تتمثل الجريمة في أن المتهم بصفته مقدم خدمة امتنع عن تنفيذ القرار الصادر من المحكمة الجنائية المختصة بحجب أحد المواقع أو الروابط أو المحتوى المُشار إليه في الفقرة الأولى من المادة (٧) من هذا القانون. و**تقيد الاوراق** جنحة بالمواد ١، ١١، ١٢، ٣٠ /١، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

وطبقا للفقرة الاولي من المادة السابعة المقصود هو اي موقع يبث داخل الدولة أو خارجها، بوضع أي عبارات أو أرقام أو صور أو أفلام أو أي مواد دعائية أو ما في حكمها، بما يعد جريمة من الجرائم المنصوص عليها في هذا القانون، ويشكل تهديدا للأمن القومي أو يعرض أمن البلاد أو اقتصادها القومي للخطر، أن تأمر بحجب الموقع أو المواقع محل البث، كلما أمكن تحقيق ذلك فنيا.

وتكون العقوبة المقررة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه، أو بإحدى هاتين العقوبتين.

تقيد الاوراق جناية بالمواد ١، ١١، ١٢، ٣٠ / ١ – ٢، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

تحت وصف أن المتهم بصفته مقدم خدمة امتنع عن تنفيذ القرار الصادر من المحكمة الجنائية المختصة بحجب أحد المواقع أو الروابط أو المحتوى المُشار إليه في الفقرة الأولى من المادة (٧) من هذا القانون، وقد ترتب على ذلك وفاة شخص أو أكثر، أو الإضرار بالأمن القومي.

وتكون العقوبة المقررة السجن المشدد، والغرامة التي لا تقل عن ثلاثة ملايين جنيه ولا تجاوز عشرين مليون جنيه، وتقضي المحكمة فضلا عن ذلك بإلغاء ترخيص مزاولة النشاط.

تقيد الاوراق جناية بالمواد ١، ١١، ١٢، ٣١، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

تحت وصف أن المتهم بصفته مقدم خدمة لم يلتزم بالمحافظة على سرية البيانات التي تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة.

ويشمل ذلك البيانات الشخصية لأي من مستخدمي خدمته، أو أي بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التي يتواصلون معها.

(ISSN: 2356 - 9492)

وتكون العقوبة المقررة الحبس مدة لا تقل سنة، وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز عشرين ألف جنيه، أو بإحدى هاتين العقوبتين، وتتعدد عقوبة الغرامة بتعدد المجني عليهم من مستخدمي الخدمة.

تقيد الاوراق جنحة بالمواد ١، ٦، ١١، ١٢، ٣٢، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨

تحت وصف أن المتهم بصفته مقدم خدمة امتنع عن تنفيذ القرار الصادر من جهة التحقيق المختصة بتسليم ما لديه من البيانات أو المعلومات المشار إليها في المادة (٦) من هذا القانون.

وتكون العقوبة المقررة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين.

تقيد الاوراق جنحة بالمواد ١، ٢ فقرة اولا / ١، ١١، ١٢، ٣٣ / ١، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨

تحت وصف أن المتهم بصفته مقدم لم يلتزم بحفظ وتخزين سجل النظام المعلوماتي أو أي وسيلة لتقنية المعلومات، لمدة مائة وثمانين يوما متصلة.

كما يجب مراعاة الملاحظات الآتية: تتمثل البيانات الواجب حفظها وتخزينها:

(أ) البيانات التي تمكن من التعرف على مستخدم الخدمة.

(ب) البيانات المتعلقة بمحتوى ومضمون النظام المعلوماتي المتعامل فيه متى كانت تحت سيطرة مقدم الخدمة.

(ج) البيانات المتعلقة بحركة الاتصال.

(د) البيانات المتعلقة بالأجهزة الطرفية للاتصال.

(هـ) أي بيانات أخرى يصدر بتحديدها قرار من مجلس إدارة الجهاز.

وتكون العقوبة المقررة غرامة لا تقل عن خمسة ملايين جنيه ولا تجاوز عشرة ملايين جنيه. وتضاعف عقوبة الغرامة في حالة العود، وللمحكمة أن تقضي بإلغاء الترخيص.

تقيد الاوراق جنحة بالمواد ١، ٢ فقرة / ثانيا، ١١، ١٢، ٣٣ / ٢، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨

تحت وصف أن المتهم بصفته مقدم خدمة لم يوفر لمستخدمي خدماته او لأي جهة حكومية مختصة، بالشكل والطريقة التي يمكن الوصول إليها بصورة ميسرة ومباشرة ومستمرة.

كما يجب مراعاة الملاحظات الآتية: البيانات والمعلومات الواجب توافرها هي:

١- اسم مقدم الخدمة وعنوانه.

٢- معلومات الاتصال المتعلقة بمقدم الخدمة، بما في ذلك عنوان الاتصال الإلكتروني.

٣- بيانات الترخيص لتحديد هوية مقدم الخدمة، وتحديد الجهة المختصة التي يخضع لإشرافها.

٤- أي معلومات أخرى يقدر الجهاز أهميتها لحماية مستخدمي الخدمة، ويصدر بتحديدها قرار من الوزير المختص.

وتكون العقوبة المقررة غرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه.

تقيد الاوراق جنحة بالمواد ١، ٢ فقرة / رابعا، ١١، ١٢، ٣٣ / ٢، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨

تحت وصف أن المتهم بصفته مقدم خدمة تقنية المعلومات لم يلتزموا حال تسويق تلك الخدمات بالحصول على بيانات المستخدمين.

أو **تحت وصف** أن المتهم قام بالحصول على بيانات المستخدمين حال تسويقه خدمة تقنية المعلومات حال كونه ليس من مقدمي الخدمات أو أحد وكلائه او موزعينه المعتمدين.

وتكون العقوبة المقررة غرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه.

(ISSN: 2356 - 9492)

تقيد الاوراق جنحة بالمواد ١، ٢ فقرة / ثالثا، ١١، ١٢، ٣٣ / ٣، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨

تحت وصف أن المتهم بصفته مقدم خدمة لم يلتزم أن يوفر كافة الإمكانيات الفنية التي تتيح لجهات الأمن القومي ووفقا لاحتياجاتها ممارسة اختصاصاتها وفقا للقانون.

وتكون العقوبة المقررة الحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليون جنيه.

سادس عشر – المسئولية الجنائية للشخص الاعتباري:

فضلنا عرض المسئولية الجنائية للشخص الاعتباري في النهاية، لأنها تشكل أهمية ذات طبيعة خاصة، نظرًا لطبيعة التحول الرقمي والكيانات التي تنظم ويدار بها هذا التحول. فغير متصور حاليًا مسئولية الألة جنائيًا – حتى ولو كانت تعمل بالذكاء الاصطناعي – لذلك كان لزامًا تصور من تقع عليه تلك المسئولية؟ والتي إجاب عنها القانون بإسناد المسئولية للمسئول عن الإدارة الفعلية.

تتمثل الجريمة في أن المتهم بصفته مسئول عن الإدارة الفعلية لأي شخص اعتباري لم يبلغ الجهات الرسمية المختصة بتعرض الموقع أو الحساب الخاص أو البريد الإلكتروني أو النظام المعلوماتي المخصص للكيان الذي يديره لأي جريمة من الجرائم المنصوص عليها في هذا القانون وقت علمه بالجريمة. **وتقيد الاوراق** جنحة بالمواد ١، ١١، ١٢، ٣٥، ٣٨ من القانون رقم ١٧٥ لسنة ٢٠١٨.

وتكون العقوبة المقررة الحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تزيد عن مائة ألف جنيه، أو بإحدى هاتين العقوبتين.

كما يجب مراعاة الملاحظات الآتية:

١- طبقا لنص المادة ٣٤ من القانون الخاصة بالظروف المشددة في الجريمة فانه إذا وقعت أي جريمة من الجرائم المنصوص عليها في هذا القانون بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر أو الإضرار بالأمن القومي للبلاد أو بمركزها الاقتصادي أو منع أو عرقلة ممارسة السلطات العامة لأعمالها أو تعطيل

أحكام الدستور أو القوانين أو اللوائح أو الإضرار بالوحدة الوطنية والسلام الاجتماعي، تكون العقوبة السجن المشدد.

٢- طبقا لنص المادة ٣٦ من القانون في الأحوال التي ترتكب فيها أي من الجرائم المنصوص عليها في هذا القانون باسم ولحساب الشخص الاعتباري، يعاقب المسئول عن الإدارة الفعلية إذا ثبت علمه بالجريمة أو سهل ارتكابها تحقيقا لمصلحة له أو لغيره بذات عقوبة الفاعل الأصلي.

وللمحكمة أن تقضي بإيقاف ترخيص مزاولة الشخص الاعتباري للنشاط مدة لا تزيد على سنة، ولها في حالة العود أن تحكم بإلغاء الترخيص أو حل الشخص الاعتباري بحسب الأحوال، ويتم نشر الحكم في جريدتين يوميتين واسعتي الانتشار على نفقة الشخص الاعتباري.

٣- طبقا لنص المادة ٣٧ من القانون فانه في تطبيق أحكام هذا القانون، لا يترتب على تقرير مسئولية الإدارة الفعلية للشخص الاعتباري استبعاد المسئولية الجنائية للأشخاص الطبيعيين الفاعلين الأصليين أو الشركاء عن ذات الوقائع التي تقوم بها الجريمة.

٤- طبقا لنص المادة ٣٩ من القانون فانه إذا قضت المحكمة بالإدانة على أحد الموظفين العموميين، لارتكابه جريمة من الجرائم المنصوص عليها في هذا القانون، أثناء وبسبب تأديته لوظيفته، أن تقضي بعزله مؤقتا من وظيفته مؤقتا، إلا في الحالات المشار إليها في المادة (٣٤) من هذا القانون فيكون العزل وجوبيا.

٥ - طبقا لنص المادة ٤٠ من القانون فانه يعاقب كل من شرع في ارتكاب الجنح المنصوص عليها في هذا القانون بما لا يجاوز نصف الحد الأقصى للعقوبة المقررة للجريمة.

٦- طبقا لنص المادة ٤١ من القانون فانه يعفى من العقوبات المقررة للجرائم المنصوص عليها في هذا القانون كل من بادر من الجناة أو الشركاء إلى إبلاغ السلطات القضائية أو السلطات العامة بما يعلمه عنها قبل البدء في تنفيذ الجريمة وقبل كشفها.

(ISSN: 2356 - 9492)

ويجوز للمحكمة الإعفاء من العقوبة أو التخفيف منها إذا حصل البلاغ بعد كشف الجريمة وقبل التصرف في التحقيق فيها إذا مكن الجاني أو الشريك، في أثناء التحقيق، السلطات المختصة من القبض على مرتكبي الجريمة الآخرين، أو على ضبط الأموال موضوع الجريمة، أو أعان أثناء البحث والتحقيق على كشف الحقيقة فيها، أو على القبض على مرتكبي جريمة أخرى مماثلة لها في النوع والخطورة. ولا يخل حكم هذه المادة، بوجوب القضاء برد المال المتحصل من الجرائم المنصوص عليها في هذا القانون.

٧- طبقا لنص المادة ٤٢ من القانون الخاصة بالصلح أو التصالح فانه يجوز للمتهم في أي حالة كانت عليها الدعوى الجنائية، وقبل صيرورة الحكم باتا، إثبات الصلح مع المجني عليه أو وكيله الخاص أو خلفه العام، أمام النيابة العامة أو المحكمة المختصة بحسب الأحوال، وذلك في الجنح المنصوص عليها في المواد (١٤، ١٥، ١٦، ١٧، ١٨، ١٩، ٢٣، ٢٦، ٢٨، ٣٠، ٣١) من هذا القانون.

ولا ينتج إقرار المجني عليه بالصلح المنصوص عليه بالفقرة السابقة أثره إلا باعتماده من الجهاز بالنسبة للجنح المنصوص عليها بالمواد (١٤، ١٧، ١٨، ٢٣) من هذا القانون.

كما لا يقبل التصالح إلا من خلال الجهاز في الجنح المنصوص عليها بالمادتين (٢٩، ٣٥) من هذا القانون.

ولا يسقط حق المتهم في التصالح برفع الدعوى الجنائية إلى المحكمة المختصة إذا دفع ثلثي الحد الأقصى للغرامة المقررة للجريمة أو قيمة الحد الأدنى أيهما أكثر، وذلك قبل صدور حكم نهائي في الموضوع.

وفي جميع الأحوال، يجب على المتهم الذي يرغب في التصالح أن يسدد قبل رفع الدعوى الجنائية مبلغا يعادل ضعف الحد الأقصى للغرامة المقرر للجريمة. ويكون السداد إلى خزانة المحكمة المختصة أو النيابة العامة، بحسب الأحوال.

ويترتب على الصلح انقضاء الدعوى الجنائية، ولا أثر للصلح على حقوق المضرور من الجريمة أو على الدعوى المدنية.

٨- طبقا لنص المادة ٤٣ من القانون فانه يلتزم مقدمو الخدمة والمخاطبون، بأحكام القانون والتزاماته باتخاذ الإجراءات اللازمة لتقنين أوضاعهم خلال سنة من تاريخ العمل بأحكامه(15 / 8 / 2018) .

الخاتمة

أمن البيانات هو قضية غاية في الأهمية ونحن بحاجة إلى تبادل المعلومات مع إجراء بحث أو تقديم خدمات مخصصة، ولكن البيانات تحتاج أيضًا إلى الحماية من الوصول غير المصرح به ولا تكمن المشكلة في سرقة البيانات فحسب، بل في تزوير البيانات أيضًا، وكلما ازدادت العمليات التي تعتمد على البيانات، زادت خطورة إثارة الخطأ وتزوير البيانات.

واستعرضنا من خلال دراستنا تعريف البيانات والتحول الرقمي بالإضافة إلى أنواع البيانات المشمولة بالحماية وتعمقنا في توضيح البيانات الشخصية والحكومية وأوجه الاعتداء عليها، وختمنا دراستنا بعرض عدد لجرائم البيانات المرتبطة بالتحول الرقمي وأوجه الحماية الجنائية لها في ظل القوانين الحالية.

وننتقل إلى عرض أهم النتائج والتوصيات التي استخلصناها من دراستنا.

النتائج:

- تتعرض البيانات دائما إلى أنواع كثيره من الاعتداء كالأتلاف والاستيلاء أو الجمع غير المشروع لها.
- اصبحت حماية البيانات أمن قومي لأي دولة لما يشكله جمع واستغلال واختراق البيانات بطرق غير مشروعة من خطورة مطلقة على الدولة.
- يلعب التحول الرقمي دورًا مهمًا في القضاء على جرائم غسيل الأموال والتهرب الضريبي.
- يصاحب الانتشار الواسع للتحول الرقمي دائما جرائم مرتبطة بالبيانات، لأن هذا الأول قائم على فكرة البيانات وتحويلها من ملموسة وورقية إلى افتراضية غير ورقية.

(ISSN: 2356 - 9492)

- التحول الرقمي يمنع الاتصال المباشر بين متلقى الخدمة ومقدم الخدمة، وبالتالي يختفي العديد من الجرائم المتعلقة بالمصلحة العامة مثل الرشوة والاختلاس والاستيلاء، حيث أن تقديم الخدمة ودفع مقابل الخدمة يصبح الكترونيا.

- تحديد البيانات الشخصية – على سبيل الحصر – دائما ما يصاحبه صعوبة مطلقة لما لهذه البيانات من تشعب وتنوع.

- قد يتم استخدام البيانات الشخصية للتمييز بين الأفراد، فيلي جمع البيانات مرحلة تالية تتمثل في فلترتها بناء على تصنيفات معينة كالجنس والنوع وغيره، ليتم التمييز بين الأفراد بناء على النوع أو الديانة أو الأصل العرقي.

- يعد الحق في محو البيانات الشخصية من الحقوق المستحدثة في لائحة حماية البيانات الأوروبية GDPR، وهو ليس مطلقا كونه يتداخل مع غيره من الحقوق المتعارضة كالحق في حرية التعبير والوصول إلى المعلومات.

- ما تزال التشريعات الخاصة بحماية البيانات الشخصية تقتصر في الكثير من الدول على ما تضمنته الدساتير من قواعد عامة تشمل حماية كل ما يمس بضرر بالإنسان ولا تختص بحماية البيانات بشكل خاص إنما يتم العمل بها حسب القاعدة الشهيرة في القانون المدني "كل خطأ سبب ضرر للغير يلزم فاعله التعويض".

- يوجد نوعان من البيانات الحكومي ة: أولهما البيانات الحكومية المفتوحة، والثاني البيانات الحكومية السرية، نجد أن الأول دائما ما تلتزم الحكومات بالإفصاح عنه على عكس الثاني الذي يغلب عليه طابع السرية لدرجة تجريم الافصاح عنه.

- الدفع الإلكتروني من أحد عناصر التحول الرقمي داخل الحكومة، ويشمل بشقيه المصروفات والنفقات، ولا يخفى على أحد أن كل هذا يضم بين طياته بيانات، سواء المتعلقة بالموظفين كرقم حساب بنكي وبيانات شخصية آخري، أو المتعلقة بالعميل الذي يتلقى الخدمة.

التوصيات:

- نوصي بإصدار قانون متخصص في مصر لتنظيم إتاحة البيانات والمعلومات الحكومية للمواطنين، وهذا حق أكده الدستور المصري في المادة ٦٨ منه.

- نوصي بوضع ضوابط ونصوص تجريم، تحمي المستخدمين من استغلال مواقع التواصل الاجتماعي والمتاجر الالكترونية لبياناتهم.

- نوصي بتنظيم الحق في محو البيانات الشخصية، بما لا يتعارض مع حق حرية التعبير والوصول إلى المعلومة.

- نوصي بالبحث عن آليه للمحاسبة عن الانتهاك والتعدي على البيانات الشخصية من قبل الذكاء الاصطناعي نفسه، والكيانات غير البشرية.

- نوصي بتعديل صور الجرائم بمواد العقوبات في القوانين المختلفة والمتعلقة بالبيانات بما يتناسب مع التحول الرقمي والبيانات الرقمية، وعدم قصرها على البيانات الورقية فقط.

- يجب تنظيم آليه عمل الأرشيف الإلكتروني من جميع جوانبه، بحكم أنه محور ارتكاز البيانات الحكومية؛ وذلك حتى نضمن توافر السرية والخصوصية للبيانات المخزنة به، وكذلك الحماية الكافية ضد القرصنة والاختراق، وأيضا حماية البيانات من التلاعب بالحذف أو التغيير.

المراجع

المراجع العربية:

أولًا- مراجع عامة ومتخصصة:

- آلاء بنت سعيد بن ناصر، حماية البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي، رسالة ماجستير، ٢٠١٥.

- أمين أعزان، حماية البيانات الشخصية للمستهلك الإلكتروني، مجلة الاقتصاد والمستهلك، ع ٥,٦، ٢٠١٣.

- جيهان فقيه، حماية البيانات الشخصية في الإعلام الرقمي، مجلة العلوم الإنسانية، ع٧، ٢٠١٧.

- د. تامر محمد محمد صالح، الحماية الجنائية للحق في المعلومات الرسمية (دراسة مقارنة)، مجلة القانون والاقتصاد، ملحق خاص العدد الثاني والتسعون، ٢٠١٩.

(ISSN: 2356 - 9492)

- د. حسن صادق المرصفاوى، الإجرام والعقاب في مصر، منشأة المعارف بالإسكندرية، بدون سنه نشر.

- د. رمسيس بهنام، الإجرام والعقاب علم الجريمة وعلم الوقاية والتقويم، منشأة المعارف بالإسكندرية، ١٩٧٨.

- د. غنام محمد غنام، د. شيماء عبدالغنى عطا الله، مبادئ علم الإجرام، كلية الحقوق جامعة الزقازيق، ٢٠١٧.

- د. هيثم أحمد محمود سلامة، الحماية الجنائية لسوق الأوراق المالية: دراسة مقارنة، رسالة دكتوراة، جامعة القاهرة، ٢٠١١.

- د. يحيى إبراهيم دهشان، الحماية الجنائية لبيانات الشركات المقيدة في سوق الأوراق المالية – دراسة مقارنة، رسالة دكتوراة، كلية الحقوق جامعة الزقازيق ٢٠٢٠.

- د. يحيى إبراهيم دهشان، المسئولية الجنائية عن جرائم الذكاء الاصطناعي، مجلة الشريعة والقانون – كلية القانون جامعة الامارات، العدد ٨٢، ابريل ٢٠٢٠.

- دراسة نقدية لقانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، ورشة عمل أعدها مركز بحوث القانون والتكنولوجيا، كلية القانون بالجامعة البريطانية في مصر، اكتوبر ٢٠٢٠.

- رضوان اسخيطة، التحقيق الجنائي الرقمي في ضوء قوانين حماية البيانات الشخصية، مجلة الندوة للدراسات القانونية، ع٢٦، ٢٠١٩.

- طلال محمد داعوس، العرب والعولمة: الظاهرة والتحديات، مجلة الدراسات الدبلوماسية، العدد ١٤٢٠/١٤، ٢٠٠٠.

- محمد أحمد سلامة مشعل، الحق في محو البيانات الشخصية: دراسة تحليلية في ضوء لائحة حماية البيانات بالاتحاد الأوروبي GDPR وأحكام المحاكم الأوروبية، مجلة الدراسات القانونية والاقتصادية، مج٣, ع٢، ٢٠١٧.

- محمد محمد الألفي، الحماية القانونية لقواعد البيانات في نظم المعلومات، أعمال ندوات: مكافحة الجريمة عبر الانترنت – وورشة عمل: أمن المعلومات والتوقيع الإلكتروني، المنظمة العربية للتنمية الإدارية، ٢٠١٠.

ثانيا – قوانين وأحكام محاكم:

- حكم صادر عن محكمة فاقوس الجزئية ١٠ مارس ١٩٠٩ مج ١٠ عدد ١١٧.
- الدائرة الأولى بمحكمة القضاء الإداري، الدعوى رقم ٥٩٤٣٩ لسنة ٦٧ قضائية.
- دستور جمهورية مصر العربية لسنة ٢٠١٤.
- الطعن رقم ١٤٧٨ لسنة ٣٠ ق – جلسة ١٤/2/ ١٩٦١ – مكتب فني ١٢ – جزء ١ – صـ٢١٨.
- قانون العقوبات المصري رقم ٥٨ لسنة ١٩٣٧.
- قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠.
- قانون رقم (٢٦) لسنة ٢٠١٥ بشأن تنظيم نشر وتبادل البيانات في إمارة دبي.
- القانون رقم ١٢٦ لسنة ٢٠١١.
- قانون رقم ٣٠ لسنة ٢٠١٨ بإصدار قانون حماية البيانات الشخصية في البحرين.
- قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.
- نقض ١٣ فبراير سنة ١٩٣٠ قضية رقم ١١٣ سنة ٤٧ ق
- نقض ٤ فبراير سنة ١٨٩٩ . قضاء ٦ ص ١٣٠.

المراجع الأجنبية:

- Inman, A. James & Inman, R. Ralph Spring. "Responsibility as an Issue in Internet Communication: Reading Flames as Defamation", Journal of Technology Law & Policy, Vol. 11,٢٠٠٦ .
- Porfirio, José António, et al. "Leadership characteristics and digital transformation." Journal of Business Research 124 (2021): 610-619.
- Yaseen, Humam Khalid, and Ahmed Mahdi Obaid. "Big Data: Definition, Architecture & Applications." JOIV: International Journal on Informatics Visualization 4.1 (2020): 45-51.
- Shah, S., Vasilis Peristeras, and Ioannis Magnisalis. "Government (Big) data ecosystem: definition, classification of actors, and their roles." International Journal of Computer and Information Engineering 14.4 (2020): 102-114.

(ISSN: 2356 - 9492)

- Whitfield Diffie and Susan Landau. The Export of Cryptography in the 20th and In Karl de Leeuw, Jan the 21st Centuries Bergstra, ed. The history of information, 2007.
- Martin Doyle, What Is the Difference Between Data and Information? Online: https://salespop.net/sales-management/difference-between-data-and-information/
- Fletcher, Gordon, and Marie Griffiths. "Digital transformation during a lockdown." International Journal of Information Management 55 (2020): 102185.
- Behnam Tabrizi, Ed Lam, Kirk Girard, and Vernon Irvin, Digital Transformation Is Not About Technology, harvard business review, 2019. online: https://hbr.org/2019/03/digital-transformation-is-not-about-technology
- Deng, Xinyang, and Tianhan Gao. "Electronic payment schemes based on blockchain in VANETs." IEEE Access 8 (2020): 38296-38303.
- Dib, Omar, Clément Huyart, and Khalifa Toumi. "A novel data exploitation framework based on blockchain." Pervasive and Mobile Computing 61 (2020): 101-104.
- Oyelami, Lukman O., Sulaimon O. Adebiyi, and Babatunde S. Adekunle. "Electronic payment adoption and consumers' spending growth: empirical evidence from Nigeria." Future Business Journal 6.1 (2020): 1-14.
- Santosh K. Vishwakarma, Nirmal K. Gupta, A Big Data Approach for Healthcare Analysis During Covid-19, Springer, Singapore, 2021.
- Hippmann S., Klingner R., Leis M., Digitization – Areas of Application and Research Objectives. In: Neugebauer R. (eds) Digital Transformation. Springer Vieweg, Berlin, 2019.
- Wessel, Lauri, et al. "Unpacking the difference between digital transformation and IT-enabled organizational transformation." Journal of the Association for Information Systems 22.1 (2021): 102-129.
- Iwona Seredyńska, Insider Dealing and Criminal Law, Springer, Berlin, Heidelberg, 2012.
- General Data Protection Regulation (GDPR).

- data protection act 2018.
- In re Facebook - Cambridge Analytica - Online:
- https://epic.org/privacy/facebook/cambridge-analytica/
- Margi Murphy, Millions of Facebook user records exposed in data breach, 3 APRIL 2019 - Online:
- https://www.telegraph.co.uk/technology/2019/04/03/millions-facebook-user-records-exposed-data-breach/
- Nicholas Confessore, Cambridge Analytica and Facebook: The Scandal and the Fallout So Far, 4 April 2018 - Online:
- https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html
- Judgment of the Court (Grand Chamber) - Online:
- https://curia.europa.eu/juris/liste.jsf?num=C-131/12
- Executive Order 13392 of December 14, 2005, Improving Agency Disclosure of Information - online: https://fas.org/irp/offdocs/eo/eo-13392.htm
- 25 Years Later, PACER, Electronic Filing Continue to Change Courts, Published on: December 9, 2013 - online: https://www.uscourts.gov/news/2013/12/09/25-years-later-pacer-electronic-filing-continue-change-courts

المواقع الإلكترونية:

- https://curia.europa.eu
- https://epic.org
- https://eur-lex.europa.eu
- https://fas.org
- https://salespop.net
- https://u.ae/
- https://www.cc.gov.eg/
- https://www.egypt.gov.eg/
- https://www.idsc.gov.eg
- https://www.my.gov.sa/
- https://www.nytimes.com
- https://www.telegraph.co.uk
- https://www.uscourts.gov