(ISSN: 2356 – 9492)

البيانات الشخصية بين التهديد والحماية

دراسة في ضوء أحكام القانون رقم ١٥١ لسنة ٢٠٢٠

دكتورة / يارا حافظ الجندي

مدرس القانون بجامعة حورس

مقدمة

من يملك المعلومات يملك مفاتيح المستقبل ، فهي ثروةٌ لا يُستهان بها ، ومصدرُ قوةٍ سياسيةٍ واقتصاديةٍ لمن يُحسِن جمعها واستثمارها وحمايتها كما أنها معيارٌ يُقاسُ بهِ مدى تطور وتحضُّر الشعوب . وهذا ما نص عليه دستور جمهورية مصر العربية الصادره ٢٠١٤ في المادة (٣١) : " أن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد و الأمن القومي ، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، علي النحو الذي ينظمه القانون ".

وقد أضفى تطور الحاسب الآلي ، وبالتالي دخوله في شتى مجالات الحياة السياسية والاقتصادية والاجتماعية ، على المعلومات قيمةً مضافة، ولعب دوراً أساسياً في بزوغِ فجر ثورة تكنولوجيا المعلومات التي يشهدها عصرنا الحالي. إلا أن التطور التقني المعلوماتي بات سلاحاً ذو حدين فعلى الرغم من القفزات النوعية التي حققها ، والتغييرات الإيجابية الكبيرة التي أحدثها سواءٌ على صعيد الدول أو الأفراد، إلا أنه وفي الوقت ذاته أتاحَ الفرصة لظهور أنواعٍ جديدة ومُستحدثة من الجرائم الفنية، والتي تحمل طابع هذه التقنية المعلوماتية وتُساير على الدوام تيار تقدمها،باعتمادها على الحاسب الآلي كأداةٍ لارتكابها. فتكنولوجيا المعلومات، والتي ساعدت الدول على تطوير أجهزتها العدلية ورفع كفاءاتها وقدراتها على التصدي للجريمة المعلوماتية،

ساعدت في الوقت نفسه على تطوّر أساليب وأنماط الجريمة المعلوماتية، خصوصاً مع إقبال المجرمين علي استثمار الوسائل التقنية الحديثة في تنفيذ مشاريعهم الإجرامية.

ومع تزايُد التقنيات الحديثة وتطورها المستمر زادت المخاطر على الخصوصية ، لاسيما مع بداية خضوع المعطيات الشخصية لنظام تحكمٍ مركزي للإدارة العمومية، مما أثار تخوفاتٍ شديدة على حماية البيانات التي تتصل بالأفراد وحياتهم الخاصة[١] .

ولا جدال اليوم في أن الخصوصية تُعدُ من الحقوق الدستورية الأساسية الملازمة للشخص الطبيعي بصفته الانسانية كأصلٍ عام، فهي تُعدُ أساس بنيان كل مجتمعٍ سليم ، وتُعتبر من الحقوق السابقة علي وجود الدولة ذاتها. لذا تحرص المجتمعات خاصة ًالديمقراطية منها على كفالةِ هذا الحق ، وتعتبره حقًا مُستقلاً بذاته، ولا تكتفي بسن القوانين لحمايته بل تسعى إلى ترسيخهِ في الأذهان، وذلك بغرس القيم النبيلة التي تلعب دورًا كبيراً وفعالاً في منع المتطفلين من التدخل في خصوصيات الآخرين وكشف أسرارهم، ولقد حظي هذا الحق باهتمامٍ كبيرٍ سواءٌ من جانب الهيئات والمنظمات الدولية أو من جانب الدساتير أو النظم القانونية.

تهدف هذه الدراسة إلى التعرف علي إشكاليات حماية البيانات الشخصية والجهود الدولية والإقليمية والوطنية لحماية حقوق الفرد وخصوصيته من تأثير المعلوماتية، ومدى جدواها في تحقيق ذلك.

وبناءً على ذلك ، سوف نقوم بتسليط الضوء على أثر التقنية على الحياة الخاصة، وذلك بغية الإجابة على إشكالٍ محوريٍ يتمثل في : ماهية البيانات الشخصية وكيفية معالجتها ، وفيما تتمثل من إشكاليات التعدي علي تلك البيانات ، وإن كانت أغلب دول العالم قد وضعت

(1)La vie privée à l'ère de l'information, Centre de traduction et d'édition Al-Ahram, Le Caire, 1999, p 123 .

(ISSN: 2356 – 9492)

ضماناتٍ قانونيةٍ لحماية هذا الحق فما مدى كفايتها مع تطور استخدامات الانترنت وطرق حمايتها ، وهل التشريع المصري الجديد وفق في معالجة هذا المجال ؟ وللإجابة على هذه الاشكاليات، ارتأينا تقسيم البحث إلى ثلاثة مباحث، يتناول المبحث الأوّل بالدراسة ماهية البيانات الشخصية وكيفية معالجتها التي تواجهها في العصر الرقمي، وذلك في مطلبين، خصصنا الأوّل منه للحديث عن تعريف البيانات الشخصية، وأفردنا الثاني في عرض أنواع البيانات الشخصية وطرق معالجتها. أمّا المبحث الثاني فسيخصص لدراسة إشكاليات حماية البيانات الشخصية، وذلك في مطلبين ، خصصنا الأول منه للحديث عن تحديات حماية خصوصية المعلومات ، و أفردنا في الثاني عن مصادر تهديد خصوصية البيانات الشخصية . بينما نعرض في المبحث ثالث عن المجهودات التشريعية و الدولية وقواعد الاختصاص القضائي لمكافحة جرائم الإعتداء علي الخصوصية المعلوماتية، وذلك في مبحثين ، الأول نستعرض فيه الجهود التشريعية و الدولية لمكافحة جرائم الإعتداء علي الخصوصية المعلوماتية، و خصصنا الثاني لعرض قواعد الإختصاص في الجريمة المعلوماتية.

المبحث الأول

ماهية البيانات الشخصية وكيفية معالجتها

انّ مبدأ الحق في الخصوصية في معناه التقليدي هو: حق الفرد في أن يقرر بنفسه متى وإلى أي حدٍ يمكن أن يطلع الغير على شؤونه الخاصة. وفي إطار الاعتداءات التي أصبحت تطال حياته الخاصة بواسطة التقنيات المعلوماتية، أصبح من الضروري إعادة النظر في هذا المفهوم، بل وقد زاد الاهتمام بهذا الحق نظرًا لما يتعرض له من مخاطرٍ تُحيط به وتهدده أبرزها التقدم التكنولوجي والمعلوماتي الذي كان له دورٌ في اقتحام حصون هذا الحق.

البيانات الخاصة، الخصوصية المعلوماتية، والمعلومات الاسمية[١]، كلها مرادفاتٌ لمعنى واحد وهو حق الشخص في أن يتحكم بالمعلومات التي تخصه. فهذه المعلومات يطلق عليها خاصة كونها تتعلق بالشخص ذاته كإنسان مثل الاسم والعنوان ورقم الهاتف وغيرها من المعلومات التي تأخذ شكل بيانات وثيقة الارتباط والالتصاق بكل شخصٍ طبيعيٍ مُعرَّفٍ أو قابلٍ للتعريف[٢]. بينما يرى البعض أن البيانات الشخصية هي "تلك التي تتعلق بحرمة الحياة الخاصة للإنسان، ومنها ما يسمح برسم صورةٍ لاتجاهاته وميوله ومنها تلك المتعلقة باتجاهاته السياسية ومعتقداته الدينية وتعاملاته المالية والبنكية وكذا جنسيته"[٣]. وهذه النوعية من المعلومات أصبحت في وقتنا الحاضر على درجةٍ كبيرة ٍمن الأهمية في ظِل التطورات التقنية، وتحديدًا إنشاء بنوك

(١) تختلف التسميات التي تُطلق على البيانات الخاصة، حيث يستعمل المشرع الفرنسي مصطلح المعلومات الاسمية، بينما يستخدم الفقه الفرنسي مصطلح المعطيات، أما تسمية المعطيات ذات الطابع الشخصي تطلق من قبل المشرع المغربي من خلال قانون رقم (٠٨-٠٩) المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي– منشور في الجريدة الرسمية، عدد **5711** بتاريخ **23** فبراير **2009** .

(2) Lucas, Jean Devese et Jean Freyssinet, droit de l'informatique et de l'internet, Presses Universitaires de France, Economies, paris, 2001, p76 .

[3] – Ibid., p579

(ISSN: 2356 – 9492)

المعلومات وإجراء عملية المعالجة والتحليل بواسطة الحاسوب، ومن هنا ظهر ما يُعرف بالخصوصية المعلوماتية .[١]

وعليه سنحاول من خلال هذا المبحث الاحاطة بمفهوم البيانات الشخصية و أنواعها وطرق معالجتها من خلال مطلبين و ذلك على النحو التالي:

المطلب الأول

تعريف البيانات الشخصية

عرفت المادة الأولي من القانون رقم ١٥١ لسنة ٢٠٢٠ المصري الخاص بحماية البيانات الشخصية (البيانات الشخصية)[٢] 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."

وفي إطار تحديد مفهوم خصوصية المعلومات، تجدر الإشارة أنه في نهاية الستينات والسبعينات أُثيرَ لأول مرةٍ هذا المصطلح كمفهومٍ مُستقلٍ عن بقية مفاهيم الخصوصية وتحديدًا التدخل المادي والرقابة، وذلك من خلال فقيهين أمريكيين، الأول ألان ويستن Alan Westin سنة 1997 في كتابه الخصوصية والحرية Privacy and Freedom . أما الفقيه الثاني ميلر من خلال كتابه الاعتداء على الخصوصية –The Assault on Privacy 1971 .

[1] Fabien Marchadier, réseaux sociaux sur internet et vie privée, « technique et droit humains », Montchrestien Lex, 2010, p 21

[٢] الجريدة الرسمية ، العدد٢٧ مكرر (ه)، ١٥ يوليو ٢٠٢٠
https://www.scribd.com/document/469505055/%D8%A7%D9%84%D8%AC%D8%B1%D9%8A%D8%AF%D8%A9-%D8%A7%D9%84%D8%B1%D8%B3%D9%85%D9%8A%D8%A9#fullscreen&from_embed

ويقصد بخصوصية المعلومات وفقًا لوينستن: " حق الأفراد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنهم للآخري "في حين عرفها ميلر بأنها: " قدرة الأفراد على التحكم بدورة المعلومات التي تتعلق بهم ".

وكان الغرض من هذه الدراسات الاكاديمية هو منع إساءة استخدام الحكومة للبيانات التي يتم معالجتها آلياً أو إلكترونيًا أو تقييد استخدامها وفقًا القانون فقط، دون حماية الأفراد من مخاطر التقنية التي تتهدد حياتهم الخاصة بصفة عامة[١] .

أمّا الاتفاقية الأوربية رقم ١٠٨ الصادرة عن مجلس أوربا فقد عرفت البيانات الخاصة من خلال المادة ٢/أ بقولها إنّ: "المعطيات ذات الطابع الشخصي هي كل المعلومات المتعلقة بشخص طبيعي مُعرّف أو قابل للتعرُّف عليه". وبنفس المعنى عرفتها المادة ٢/أ من التوجيه الأوربي رقم ٤٦/٩٥ الصادر بتاريخ ٢٤ أكتوبر١٩٩٥، بقولها إنّ:" المعطيات ذات الطابع الشخصي هي كل معلومة متعلقة بشخص طبيعي مُعرّف أو قابل للتعرُّفِ عليه، ويُعد قابلاً للتعرف عليه [الشخص المعني]، بصفة مباشرة أو غير مباشرة لاسيما بالرجوع الى رقم التعريف أو الى عنصر أو عدة عناصر خاصة مميزة لهويته الطبيعية، الفيسيولوجية النفسية، الاقتصادية، الثقافية أو الاجتماعية" .

هذا وقد شكل هذين التعريفين مصدرين أساسيين لمختلف التشريعات الأوربية لحماية المعطيات الشخصية، حيث عملت هذه التشريعات على ملائمةِ نصوصها مع التوجيه سالف الذكر، مثل التشريع الفرنسي في المادة 2 / 2 من قانون 6 يناير 1978 المتعلق بالمعلوماتية،

(1)Younis Arab, Le rôle de la protection de la vie privée dans la promotion de l'intégration dans la société numérique, document présenté lors du Symposium du club arabe pour l'éthique de l'information, 17 18 octobre 2002, Amman, Jordanie, page 07 .

(ISSN: 2356 – 9492)

وحماية الملفات والحريات، حيث نص علي أنّ : " المعطيات ذات الطابع الشخصي هي كل معلومة متعلقة بشخصٍ طبيعيٍ معُرَّفٍ أو يمكن التعرُّف عليه، بصفةٍ مباشرة أو غير مباشرة، بالرجوع إلى رقم التعريف أو إلى عنصر أو إلى عدة عناصر مميزة له لتحديد ما إذا كان الشخص قابلا للتعرف عليه، هذا ويلزم الأخذ في الاعتبار بمجموع الوسائل التي من شأنها التمكين من تعريفه " .

وكمثال لمعطيات شخصية: المعطيات التي تكون في متناول مصالح الأحوال المدنية المتعلقة بالميلاد كالاسم واللقب، وتاريخ الولادة، وجنس المولود ومحل الاقامة.. الخ. أو المعلومات المتعلقة بالحالة الصحية للأشخاص، حيث تقوم المؤسسات الطبية بتكوين ملفات طبية تضم مجموعة من المعطيات الشخصية عن المريض مثل :أسمه، وجنسه وتاريخ ومكان ميلاده، وعوارض المرض، وتشخيصه ومدة انتشاره .. إلخ .

هذا وتكتسب مختلف هذه المعطيات طابعها الشخصي انطلاقاً من مدي حِرص الأشخاص المعنيين على عدم إفشائها، وأي خطأ بسيط في عنوان البريد الالكتروني أو رقم الفاكس في إرسال معطيات شخصية من قِبَل المستشفى مثلا إلى أشخاص غير مُصرحٍ لهم باستلام هذه المعلومات، تعد سببًا في إفشاء هذه المعلومات لاسيما إذا تعلقت ببعض الحالات المرضية الحرجة، كمرض فقدان المناعة المكتسبة .

وبناء عليه، في القضيه الشهيره قيام فيها أحد المواطنين في إسبانيا بتقديم شكوي أمام محكمة اوروبا العليا ضد شركة جوجل العالمية ، عن قيام الاخيره بعرض محرك البحث بيانات تخص مسكن كان يود بيعه عن طريق نشر إعلان في الجريدة مما جعله يستاء من حفظ هذه البيانات، وحكمت المحكمة علي الشركة بمحو بعض البيانات الشخصية الحساسه من ذاكره

الموقع.[١] وتضمن الحكم إلزم ان محرك البحث هو المسؤول عن معالجة البيانات الشخصية والتي يتم استغلالها من اشخاص آخرين، حيث ألزم شركة جوجل بمحو وتعديل الروابط التي تحتوي علي بيانات قديمه غير محدثة.

الحكم السابق وضع حداً لاستغلال البيانات الشخصية، والتي قد يقع فيها الكثير من الاشخاص عن طريق قيامهم بالافصاح عن بياناتهم الشخصية طواعيه (مثل استخدام تطبيقات برنامجWhat'sApp) وكذلك (Snap chat)، الأمر الذي قد يسبب لهم الكثير من المشاكل القانونية، حيث تتيح لمقدم الخدمه الدخول علي الهاتف الشخصي والاستحواذ علي البيانات الشخصية من أرقام هواتف و صور شخصيه و غيرها من البيانات الخاصة .[٢]

والجدير بالذكر إنتشارما يطلق عليهم (سماسرة البيانات)، حيث ان رأس مال بعض الشركات المتخصصه قائمه علي تجميع البيانات الشخصية للافراد وإعداد قواعد البيانات وتصنيفها وبيعيها والتي تحتوي علي البيانات الشخصية لآلاف العملاء واستخدامها إمام بطريقه مباشره وهي الاتصال بالعميل وإرسال إعلانات دعائية و ترويج السلع أو إستخدامها بهدف دراسة السوق أو تحليل البيانات وإدراج تصنيف عمري و علمي وغيرها من التصنيفات.[٣]

[1] Court of justice of the European Union , Press release No.70/14, Luxembourg, 13 May 2014 , judgment in case c-131/12, Google Spain SL, Google Inc. v Agenecia Espanola de Proteccion de Datos , Mario Costeja Gonzalez.

[2] Shade, L.R. Reconsidering the right to privacy in Canada .Bulletinof science , techonolgy and Society . (2008) P 80-91.

[3] http://icsa.cs.up.ac.za/issa/2004/proceedings/full/078.pdf. Accessed 15 Aug 2019 P.23

(ISSN: 2356 – 9492)

مصطلح البيانات الشخصية يطلق عليها داخل الولايات المتحدة (التعريف الشخص PII) وهي تستخدم في قانون الخصوصية وأمن المعلومات بالولايات المتحدة، حيث يمكن استخدامها بمفردها أو مع غيرها للتعرف أو تحديد الفرد في ساقه .[١]

ورد بمذكرة الإدارة و الميزانية بالبيت الأبيض – بالولايات المتحدة – البيانات الشخصية، هي المعلومات التي يمكن استخدامها لتمييز أو تعقب هوية الفرد، مثل الاسم ورقم الضمان الاجتماعي والسجلات الحيوية وحدها، أو عند دمجها مع المعلومات الشخصية التي ترتبط بشخص معين، مثل تاريخ ومكان ولادته واسم عائلته .[٢]

ووفقاً لتعريف اللائحة التنظيمية EU/2016/679 (اللائحة العامة لحماية البيانات الشخصية المعرفة باسم) اللائحة العامة لحماية البيانات (RGPD) تكون البيانات الشخصية " أي معلومات تتعلق بشخص طبيعي محدد أو يمكن التعرف عليه" (المادة ٤ فقرة ١) شخص طبيعي يمكن التعرف عليه بشكل مباشر أو غير مباشر، وخاصة بالاشارة الي معرف مثل الأسم، أو رقم تعريف، أو بيانات موقع أو معرف عبر الانترنت أو عنصر محدد أو الأكثر حاص بهويته البديعه والفسيولوجية أو الوراثية أو الاقتصادية أو الثقافية أو الاجتماعية.والواقع أن عبور البيانات الضخمة اليوم يسهل عملية هوية الأفراد، لذا فإن النطاق المادي لحماية البيانات الشخصية من المحتم أن يتسع[٣].

[1] Vincent D. Blondel : Unique in the Crowd: the privacy bounds of human mobility . Nature srep 2013, p 78.

[2] http://ww.whitehouse.gov/sites/default/files/omb/assets/legislative_reports/fy14_preview_and_joint_committee_reductions_reports_04102013.Pdf

[3] Le nouveau re'glement sur La protection des donees – Celine castets – Renard- 18/10/2018 Http://actu.dalloz.etudiant.fr/focus-sur

وعليه يمكن القول أن خصوصية المعلومات هي حماية البيانات، فهذه الأخيرة جزء من الخصوصية، وتتعلق بمواجهة الاعتداءات على البيانات الشخصية، في حين أن الخصوصية على إطلاقها تنطوي على خصوصية البيانات، وخصوصية الاتصالات.

المطلب الثاني

أنواع البيانات الشخصية وطرق معالجتها

في ظل التطور البشري، لم تعد البيانات مقصورة علي الاسم والعنوان بل تطور المفهوم ليشمل اكثر من منظور منها وجود وسيط شبكي (من الناحيه التكنولوجيه) ومن الناحية الاجتماعية وكذلك البيانات الصحيه للشخص والمنظور التعليمي والوظيفي والمالي وغيرها من الجوانب الشامله لجميع البيانات الشخصية .

أولاً: البيانات التكنولوجيه :

وهذه البيانات يتم تداولها عن طريق وسيط إلكتروني، أو نشرها عبر شبكة الأنترنت ويمكن من خلالها معرفه الشخص .

ويمكن القول ان جميع البيانات التي يتم تداولها عبر الوسيط الشبكي وتكون متصله بشخص بعينه ويمكنها تعريفه منفردا أو عن طريق إضافتها لبيانات أخري مثل الأسم والحسابات الإلكترونية من بريد إلكتروني بالاضافه الي الارقام السريه، حيث يمكن ان يطلق عليها أيضاً الخصوصية المعلوماتيه.

(ISSN: 2356 – 9492)

وبالتالي فإن أي بيان ارتبط بشخص معرف أو قابل للتعريف يعد بياناً شخصياً، وأية وثائق تثبت تلك البيانات تعد بيانات شخصية، إذن أي معلومه أو شئ يرتبط بالأشخاص من حيث تعريفهم يعتبر بياناً شخصياً.[١]

عرف القانون الالماني البيانات المالية للشخص بأنها البيانات غير العامة، ومن هنا ذهب اتجاه إلي ان البيانات الشخصية هي البيانات غير المنشور والتي لا يمكن الوصول إليها، والغير متاحه في السجلان العامة وبالتالي فلا يعد الاسم والعنوان وغيرها من البيانات التي لا توجد في السجلات الحكومية بيانات خاصة.[٢]

وبالتالي فإن هذا المبدأ لم يقتصر علي ان من يقم بإستغلال البيانات المنشورة يقع تحت طالة القانون فقط ولكن فإن هذا المبدأ أضاف أيضاً أنه يمكم يقع تحت طائله القانون بالاطلاع.

ثانياً : البيانات الاجتماعية

من الناحية الاجتماعية فأن البيانات الشخصية تتمثل في :

- **الاسم** : وهي الوسيله التي تميز الشخص عن غيره . وقد يقصد به اللقب أو اسم العائله

وتجدر الاشاره أن هناك أنواع أخري للاسم يجميها القانون، إذا تم استعمالها بصفه مستمره مثل:

- **اسم الشهرة:** وهو الاسم الذي يشتهر به الشخص بين الناس وهو من صنع الناس ويستحق الحماية القانون.[٣]

[1] Larose, R.,& Rifon, N. J. promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior. Journal Of Consumer Affairs, (2207).127-149

[2] Martin Hilbert and Priscila Lopez. The world's Technological Capacity to Store, Communicate, and Computer Information. Especially Supporting online material, Science (Journal), (2011)P 65.

[3] Muench,David " Wisconsin Community Slogans: Their Use and local Impacts", December 1993 .April 10,2007

- **والأسم المستعار:** ويطلقه شخص علي نفسه بعرض إخفاء شخصيته في مناسبة بسبب سياسيا ويعد الشخص حرا في اختيار هذا الاسم، وإذا استخدمه صاحبه بصفه مستمر يستحق الحماية القانونية
- **الاسم التجاري:** وهو الذي يستخدمه التاجر ليمارس تحته تجارته ويكون مميزا لمحله التجاري وهو حق مالي قابل للتصرف فيه.

كما يعد أسم الوالدين من البيانات الشخصية للفرد [1]

- الموطن: وهو غالبا ما يتكون من رقم العقار واسم الشارع والمنطقة والمحافظة، حيث أنه يعد المكان الذي يقطنه الشخص أو يستخدمه لإدارة نشاط معين.

- أرقام الهاتف
- السن وتاريخ الميلاد
- الديانه
- ارقام البطاقات (جواز سفر – رقم تأميني – الرقم القومي)
- الجنس أو النوع
- المراسلات
- الصور والفيديوهات التي يظهر فيها الشخص
- الانتماء السياسي والآراء ووجهات النظر سواء في مواضيع عامه أو خاصة.

ثالثا: البيانات الصحية:

تعرف بأنها أي معلومات تتعلق بالتاريخ الصحي للشخص أو تاريخ التشخيص والتي يمكن استخدامها للتعرف علي شخص بعينه، والتي قد تم استخدامها من قبل لتقديم خدمه طبيه

[1] "Did LuzlzSec, Trick police Into Arresting the wrong Guy? – technology. The Atlantic Wire.2011 P-28 See also " protection of Personal data- Justice". Ec.europa.eu.2011-01-18.23/10/2012

(ISSN: 2356 – 9492)

مثل التشخيص او العلاج، وكذلك بيانات الحمض النووي و غيرها من البيانات مثل التحاليل والفحوصات الخاصة بصحة الشخص .[١]

رابعاً: البيانات التعليمية والمهنية والمالية

تعد البيانات الشخصية التعليمية التي تحدد المستوي الدراسي للشخص والدرجات العلمية. والبيانات التي ترتبط بالتاريخ الوظيفي للشخص والمتعلقة بأدائه الوظيفي ورقم تعريفه في العمل والمرتبات والمستحقات المادية والمعنوية تعتبر بيانات شخصيه، واجراءات الاختيار والتعيين والمراقبه أثناء العمل من خلال المكاتب والموبايلات والبريد الإلكتروني.[٢] كما تعد بيانات شخصيه، الحسابات البنكية وأرقام كروت الائتمان وبيانات القروض والتقارير السنوية للحسابات البنكيه للشخص.[٣]

طرق معالجة البيانات الشخصية:

تسمي أن معالجة البيانات الالكترونية (Electronic data processing)، يشير إلي استخدام الأساليب الآلية لمعالجة البيانات التجارية [٤]. وفي الغالب يكون هذا الاستخدام بسيطا نسبيا لمعالجة الكميات الكبيرة المتشابهة لأنشطة المتكررة. مثل: تطبيق المعاملان المصرفية علي الحسابات والملفات الرئيسية للعملاء، وإجراءات الحجوزات والتذاكر علي نظام الحجز علي خطوط الطيران، تطبيق التحديثات علي جرد المخزون، وفواتير خدمات المرافق.

[1]Narayanan, A.;Shmatikov ,V. " Myths and fallacies of " personally identifiable information"> communications (2010) .P24
See also James W.H. McCord and Sandra L. McCord , Criminal Law and procedure for the paralegal : a system approach ,supra,2000
[2] Bygrave L.Data Protection Law: " Approaching its Rationale, Logic and Limits" coma press (2002) P16
[3] Krishnamurthy B, Wills CE. On the Leakage of Personally Identifiable Information Via Online Social Networks,, US Press, (2009) P 112
[4] Shraddha , Peter J.Lyons &Co.:LEO Computers (2002) P25

تشكل البيانات في جميع الأنظمة هي المادة الخام المستخدمة

في تصنيع المعلومات بعد الخضوع للمعالجة، وحتى يتم معالجة البيانات لتخرج إلينا على هيئة معلومات ذات فائدة؛ لا بد من تتوفر نظام معالجة خاص يؤدي هذا الغرض؛ فظهر نظام معالجة البيانات في الحاسوب الذي يعد البيئة التي تجمع ما بين الأيدي البشرية والآلات التي تعمل على معالجة البيانات أو كما تعرف بالمدخلات لتخرج للمستخدم على هيئة مخرجات أو معلومات أو حقائق، بالاعتماد على مدى علاقة المترجم بالنظام، وتتم عادةً معالجة البيانات من خلال استقطاب البيانات وتسجيلها ثم إخضاعها للمراجعة، والتحقق من مدى التطابق بينها وبين المصادر التي تم تصنيفها إلى مجموعات أو فئات تبعًا لمجموعة من المعايير، وقد يتم تصنيف هذه البيانات وفقًا لمناطق جغرافية أو إقليمية؛ ويطلق على ذلك نظام الترميز الرقمي أو الحرفي، ويُلجأ إلى القيام بخطوة ترتيب البيانات وفقًا لمعيار محدد أيضًا بعد تصنيفها، وتستخدم غالبًا الحسابات المنطقية للخروج بمعلومات جديدة.

المكونات الثابته لنظام معالجة البيانات في الحاسوب، وهي:

- **المكون الأول:** وحدة المعالجة المركزية(Central Processing Unit) ، ويرمز لها اختصارًا بـCPU ، تؤدي دور المفسر الأول والدقيق للبيانات والمعلومات والمعالج لها.
- **المكون الثاني:** الذاكرة (main memory) وتستخدم عادةً لتخزين البيانات المعالجة والأولية فيها، إلا أنها تفقد كل المعلومات فور انقطاع التيار الكهربائي أو إغلاق جهاز الحاسوب، إذ تعرف بأنها عشوائية.

(ISSN: 2356 – 9492)

- **المكون الثالث:** وحدات الإدخال والإخراج :يمكن القول بأنها الوسيلة التي يقوم الإنسان بواسطتها إدخال البيانات المراد معالجتها إلى جهاز الحاسوب؛ ثم يصار إلى معالجتها واستعراضها على وحدات الإخراج كالشاشة مثلًا.
- **المكون الرابع:** وحدة الحساب والمنطق: وهي تلك الوحدة المستخدمة في تخزين البيانات فيها على هيئة أعداد بعد خضوعها للعمليات المنطقية.
- **المكون الخامس:** العنصر البشري :يكمن دور العنصر البشري سواء كان مُصنّع أو مبرمج بأنه معطي الأوامر ومدخل البيانات ليتم معالجتها[١].

أنواع نظام معالجة البيانات في الحاسوب، وهي:

- **النوع الأول:** معالجة البيانات العلمية :يعتمد هذا النوع على العمليات الحسابية بشقيّها سواء كانت حسابية أو مقارنة.
- **النوع الثاني:** معالجة البيانات التجارية :تمتاز بإدخال كميات كبيرة من البيانات وإخراجها؛ إلا أن عدد العمليات الحسابية قليل.
- **النوع الثالث:** حليل البيانات :انتهاج مجموعة من الأساليب للوصول إلى وصف دقيق للحقائق واستنباط الأنماط ووضع أدق التفاسير والتحاليل للبيانات بين يدي متخذ القرار أو من يحتاجها.

عملية المعالجة للبيانات في الحاسوب تمر بعدةِ مراحل، وهي:

- **المرحله الأولي:** إدخال البيانات :حيث تعتبر الخطوة الأولى للبدء بعملية المعالجة لهذه البيانات هي إدخالها بواسطة وحدات الإدخال المتاحة؛ كلوحة المفاتيح أو زر الفأرة وغيرها.

[١] **مراحل عملية معالجة البيانات في الحاسوب**، إيمان الحياري، https://www.mah6at.net/ ١٠ أغسطس ٢٠١٨

- **المرحلة الثانية:** المعالجة :تبدأ مهمة وحدة المعالجة المركزية فورًا بالتزامن مع إعطاء الأوامر من قِبل العنصر البشري في البدء بمعالجة البيانات بعد إدخالها، فيقوم جهاز الحاسوب بإجراء مجموعة من العمليات الحسابية او الاستنتاجية على البيانات، ثم تخزينها وتصنيفها، وترتيبها وأخيرًا مقارنتها لاتخاذ قرار مناسب بشأن قضية ما.
- **المرحلة الثالثة:** الإخراج :تصل البيانات على شكل معلومات بعد الإنتهاء من معالجتها؛ فتصبح جاهزة لأن توضع بين يدي المستخدم بواسطة وحدات الأخراج، وتكون هذه هي النتيجة النهائية[١].

قانون البيانات الشخصية الانجليزي، الصادر في [٢]١٩٩٨ عرف (معالجة البيانات) هي الحصول أو تسجيل أو عقد البيانات أو تنفيذ عملية أو مجموعة من العمليات علي المعلومات والبيانات والمتضمنه:

١- تنظيم وتكيف أو تعديل المعلومات أو البيانات

٢- استرجاع المعلومات أو استخدام المعلومات

٣- الكشف عن المعلوكات عن طريق نقل أو نشر

٤- محاذاة، حظر، الجمع ،محو أو تدمير الملفات أو البيانات .

تم إعتماد النظام الأوروبي العام لحماية البيانات الشخصية بأسم General Data Protection Regulations (GDPR) في ٢٠١٦/٤/١٤ ومر بفترة انتقالية لمدة عامين ليصبح ساري التنفيذ في ٢٠١٨/٥/٢٥، كنظام جديد بدلاً من نظام حماية البيانات المقر في ١٩٩٥.

[١] **مراحل عملية معالجة البيانات في الحاسوب**، إيمان الحياري، https://www.mah6at.net/ ١٠ أغسطس ٢٠١٨

[2] The Data Protection Act 1998 (DPA) is a United Kingdom Act of Parliament which defines UK law on the processing of data on identifiable living people.

(ISSN: 2356 – 9492)

ويختص هذا لنظام (GDPR) بحماية البيانات والخصوصية لجميع الأفراد داخل الإتحاد الأوروبي، ويهتم أيضاً بتصدير البيانات الشخصية خارج الإتحاد الأوروبي. ويهدف في المقام الأول لإعطاء المواطنين والمقيمين قدرة علي التحكم والسيطرة بالبيانات الشخصية وتبسيط بيئة التنظيمات والقوانين للمشاريع التجارية الدولية من خلال توحيد التنظيم داخل الاتحاد الأوروبي .[١]

وقد عرفت النظام (GDPR) المعالجة في المادة (٤) فقرة (٢) ب :

"أي عملية أو مجموعة من العمليات التي يتم إجراؤها علي البيانات الشخصية أو علي مجموعات من البيانات الشخصية، سواء بوسائل آليه أم لا، مثل الجمع أو التسجيل أو التنظيم أو الهيكله أو التخزين أو التكييف أو التغيير أو الاسترداد أو الاستشاره أو الاستخدام أو الكشف عن طريق النقل أو النشر أو الإتاحه أو المحاذاة أو الجمع أو التقييد أو المحو أو التدمير".[٢]

والجدير بالذكر، أن نظام (GDPR) وضع قواعد إلزامية لكيفية استخدام المؤسسات والشركات للبيانات الشخصية بطريقة ذات شفافية.

ويجب علي كل مؤسسة تعالج البيانات الشخصية (وهي كل مؤسسة لديها موظفين وعملاء) التأكد من أن البيانات الشخصية التي تستخدمها تفي بالمتطلبات للنظام العام لحماية البيانات.

وهذه المتطلبات هي كما يلي :[٣]

١- توحيد النظام العام لحماية البيانات في جميع أنحاء أوروبا

يسري النظام العام لحماية البيانات (GDPR) علي جميع الدول الأعضاء في الإتحاد الأوروبي، مما يسهل الأمر علي الشركات و المواطنين علي حد سواء .

[1] Https://eur.lex.europa.eu/legal-content/EN/TXT/?uri=CELEx, See also , GUIDE DE SENSIBILISATION AU RGPD, https://www.cnil.fr/professionnel
[2] https://www.gdprsummary.com/gdpr-definitions/prossing/
[3] https://www.gdprsummary.com/gdpr-definitions/prossing/

٢- يجب أن يتوافق استخدام البيانات الشخصية مع مبدئ الشفافية

يجب أن يكون للافراد الحق في معرفة كيفية استخدام بياناتهم ويجب علي المؤسسات تخزين البيانات الشخصية عندما يكون ذلك ضرورياً فقط .

بالإضافة إلي ذلك، يجب أن تكون المعالجة أمنه ومأمونه، ويجب علي المؤسسات الإمساك والاحتفاظ بالوثائق المناسبة التي توضح إلتزامها بالنظام العام لحماية البيانات .

٣- يجب أن يكون استخدام البيانات الشخصية قانونياً[1]

حدد النظام العام لحماية البيانات الشخصية ستة بدائل للأسس القانونية (علي سبيل المثال: الموافقة أو العقد). إذا كانت المعالجة الخاصه لأي شخص لا تنستند إلي أي من هؤلاء، فهي غير قانونية. قد يكون من الضروري معالجة البيانات الشخصية لأداء العقد. وقد يكون من الضروري أيضاً استخدام البيانات الشخصية لمنع الاحتيال و أداء التسويق .

٤- يجب أن يحترم حقوق الأفراد عند استخدام البيانات الشخصية:

يوفر النظام العام لحماية البيانات الشخصية (GDPR) لكل شخص حقوقاً معينة لبياناته الشخصية، تتمثل في معرفة من لديه الحق في الوصول الي بياناتهم الشخصية و كذا معرفة كيفية استخدام المنظمة للبيانات والإعتراض علي المعالجة .

٥- يجب علي المؤسسات الإبلاغ عن الانتهاكات الشخصية في غضون ٧٢ ساعة :

إذا تم الكشف عن البيانات الشخصية أو الوصول إليها أو تغييرها أو سرقتها، تكون المؤسسة هي المسؤوله عن التصرف، حتي ولو حدث الخرق من أحد الموردين للمؤسسة. في حالة

[1] https://www.gdprsummary.com/gdpr-definitions/prossing/

(ISSN: 2356 – 9492)

فقدان البيانات الحساسة مثل البيانات الصحية أو المالية، يجب الإبلاغ عن الحادث للسلطة وكل فرد متأثر خلال ٧٢ ساعة .

٦- الشركة مسؤولة عن موردیها :[١]

يفرض القانون الجديد GDPR التزامات علي المراقب لتنظيم التزام مورديه تعاقدياً بحماية البيانات. إذا قام المورد بعدم الالتزام او تعرض البيانات للخطر يكون المراقب هو المسؤول.

٧- حجم العقوبات :

قد تواجه المؤسسات التي تنتهك القانون عقوبات تصل إلي ٤% من مبيعاتها العالمه (أخر ١٢ شهر) أو ٢٠ مليون يورو .

وحسناً فعل المشرع المصري، عندما أصدر القانون رقم ١٥١ لسنة٢٠٢٠ المصري الخاص بحماية البيانات الشخصية، حيث عرفت المادة الأولي (المعالجة) [٢]بأنها " أي عملية إلكترونية أو تقنية لكتابة البيانات الشخصية، أو تجميعها، أو تسجيلها، أو حفظها، أو تخزينها، أو دمجها، أو عرضها، أو إرسالها، أو استقبالها، أو تداولها، أو نشرها، أو محوها، أو تغييرها، أو تعديلها، أو استرجاعها أو تحليلها وذلك باستخدام أي وسيط من الوسائط أو الأجهزة الإلكترونية أو التقنية سواء تم ذلك جزئياً أو كليا".

[1] https://www.gdprsummary.com/gdpr-definitions/prossing/

[٢] الجريدة الرسمية ، العدد٢٧ مكرر (ه)، ١٥ يوليو ٢٠٢٠
https://www.scribd.com/document/469505055/%D8%A7%D9%84%D8%AC%D8%B1%D9%8A%D8%AF%D8%A9-%D8%A7%D9%84%D8%B1%D8%B3%D9%85%D9%8A%D8%A9#fullscreen&from_embed

كما حددت المادة (٢) من الفصل الثاني من ذات القانون (شروط الجمع ومعالجة البيانات): بأنها لا يجوز جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشائها بأي وسيلة من الوسائل إلا بموافقة صريحة من الشخص المعني بالبيانات، أو في الأحوال المصرح بها قانونًا.

ويكون للشخص المعني بالبيانات الحقوق الآتية:[١]

١- العلم بالبيانات الشخصية الخاصة به الموجودة لدي أي حائز أو متحكم أو معالج والاطلاع عليها والوصول إليها أو الحصول عليها.

٢- العدول عن الموافقة المسبقة علي الاحتفاظ ببياناته الشخصية أو معالجتها.

٣- التصحيح أو التعديل أو المحو أو الإضافة أو التحديث للبيانات الشخصية.

٤- تخصيص المعالجة في نطاق محدد.

٥- العلم والمعرفة بأي خرق أو انتهاك لبياناته الشخصية.

٦- الاعتراض علي معالجة البيانات الشخصية أو نتائجها متي تعارضت مع الحقوق والحريات الأساسية للشخص المعني بالبيانات. وباستثناء البند (٥) من الفقرة السابقة، يؤدي الشخص المعني بالبيانات مقابل تكلفة الخدمة المقدمة إليه من المتحكم أو المعالج فيما يخص ممارسته لحقوقه، ويتولى المركز إصدار قرارات تحديد هذا المقابل بما لا يجاوز عشرين ألف جنيه.

وكذا نصت المادة (٣) من ذات القانون علي: "يجب لجمع البيانات الشخصية ومعالجتها والاحتفاظ بها ، توافر الشروط الآتية:

١- أن تجمع البيانات الشخصية لأغراض مشروعة ومحددة ومعلنة للشخص المعني.

[١] الجريدة الرسمية ، العدد٢٧ مكرر (ه)، ١٥ يوليو ٢٠٢٠
https://www.scribd.com/document/469505055/%D8%A7%D9%84%D8%AC%D8%B1%D9%8A%D8%AF%D8%A9-%D8%A7%D9%84%D8%B1%D8%B3%D9%85%D9%8A%D8%A9#fullscreen&from_embed

(ISSN: 2356 - 9492)

٢- أن تكون صحيحة وسليمة ومؤمنة.

٣- أن تعالج بطريقة مشروعة وملائمة للأغراض التي تم تجميعها من أجلها.

٤- ألا يتم الاحتفاظ بها لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها.

وتحدد اللائحة التنفيذية لهذا القانون السياسات والإجراءات والضوابط والمعايير القياسية للجمع والمعالجة والحفظ والتأمين لهذه البيانات.

نصت المادة (٦) من قانون حماية البيانات الشخصية علي الشروط المعالجة: "تعد المعالجة الإلكترونية مشروعة وقانونية في حال توفر أي من الحالات الآتية:

١- موافقة الشخص المعني بالبيانات علي إجراء المعالجة من أجل تحقيق غرض محدد أو أكثر.

٢- أن تكون المعالجة لازمة وضرورية تنفيذًا لالتزام تعاقدي أو تصرف قانوني أو لإبرام عقد لصالح الشخص المعني بالبيانات ، أو لمباشرة أي من إجراءات المطالبة بالحقوق القانونية له أو الدفاع عنها.

٣- تنفيذ التزام ينظمه القانون أو أمر من جهات التحقيق المختصة أو بناءً علي حكم قضائي .

٤- تمكين المتحكم من القيام بالتزاماته أو أي ذي صفة من ممارسة حقوقه المشروعة ، ما لم يتعارض ذلك مع الحقوق والحريات الأساسية للشخص المعني بالبيانات.

ومن هنا نستطيع القول، أن التشريع المصري استطاع أن يواكب نظام حماية البيانات الشخصية الصادر من الإتحاد الأوروبي GDPR، بتعرضه لتعريف البيانات والشخصية وضوابط وشروط معالجتها وذلك لحماية خصوصية المعلومات الشخصية.

المبحث الثاني

إشكاليات حماية البيانات الشخصية

في"عصر المعلومات" أصبحت حماية البيانات الشخصية ذات أهمية متزايدة. تلتزم الشركات التي تتعامل مع المعلومات الشخصية للعملاء وتخزينها، بما في ذلك أولئك الذين يستخدمون الوسائل الإلكترونية للقيام بذلك، بحماية هذه البيانات، لاستخدامها فقط لغرض معين والتخلص منها عند الانتهاء من استخدامها للعرض المطلوب مع تزايد الاهتمام بالأمن الإلكتروني، تلتزم الشركات أيضاً بحماية المعلومات الشخصية للأفراد من التهديدات الخارجية، بما فيها الإمتثال للمسئوليات القانونية، إلي جانب زيادة الوعي بين المستهلكين بقضايا الخصوصية، إن حماية البيانات أصبحت قضية تجارية حيوية.[١]

في ظل سياسة إدارة بيانات المؤسسات والإدارات الحكومية والشركات الخاصة التجارية (خدمية أو صحية)، والتي تقوم بتخزين الملايين من سجلات الأفراد (عملاء أو مواطنيين) متضمنه بياناتهم الشخصية و أنشطتهم واهتماماتهم مع القدره الهائلة لتحليل هذه البيانات ومقارنتها ونقلها حول العالم في ثوان معدودة. وتزايد أعداد المخترقين وسارقي الهوية في عمليات إختراق خصوصية البيانات، تؤثر علي حياة الأفراد وجميع تصرفاتهم بشكل لا يمكن تخيله ووفقا لتقرير منظمة Privacy Rights clearinghouse (PRC) ، فإن عدد عمليات الاختراق التي تمت منذ يناير ٢٠٠٥ إلي سبتمبر ٢٠٠٨ علي السجلات التي تحتوي علي معلومات شخصية حساسه في الولايات المتحدة تعدت ٢٣٠,٤١١,٧٣٠ سجل و العدد يزداد يوماً عن الأخر .[٢]

[1] http://ww.localenterprise.ie/Dublincity/sart-or-Grow-your-Business/Knowlegde-centre/eBusiness/Data
[2] Report available at https://www.Privacyrigts.org/speeches.testimeny

(ISSN: 2356 - 9492)

قام الاستشاري و الخبير في خصوصية البيانات والأعمال افلكترونية (روجر كلارك) بتحديد أبعاد الخصوصية، منها :[1]

١- **خصوصية الاتصالات الشخصية:** وهي قدرة الأشخاص علي الاتصال فيما بينهم دون المراقبة الروتينية من قبل أشخاص أخرين أو منظمات وهوما يسمي " بإعتراض الخصوصية".

٢- **خصوصية البيانات الشخصية:** وهي قدرة الأشخاص بأن لا تكون البيانات الخاصة بهم متوفره بشكل تلقائي لغيرهم سواء أفراد أو منظمات، وبناء عليه يكون لهم قدر كبير من السيطرة والتحكم علي تلك البيانات وطريقة استخدامها حتي في حالة أن تكون هذه البيانات تحت يد طرف أخر .

قامت مؤسسة (AMR) للبحوث بإستطلاع حوالي ١٥٤ متخذ قرار في كبري شركات تقنية المعلومات في الولايات المتحدة المريكية، وانتهي البحث إلي أن أكثر ثلاث صعوبات في إدارة خصوصية البيانات، هي :[2]

١- اختلاف وتعدد سياسات الخصوصية المناطق المختلفة جغرافيا

٢- مواكبة التغييرات المستمره في الأنظمة والسياسات

٣- إجبار الأفراد و المنشأت الحكومية لإتباع هذه القوانين والأنظمة المستحدثة.

٤- كما انتهي أيضاً إلي أن أكثر ما يخشاه أصحاب الشركات في قضايا خصوصية البيانات هي :

١- خسارة ثقة العملاء والموظفين والمستثمرين والعلامات التجارية،

[1] Roger Clarker's Privacy and Social Media: An Analytical Framwork, " Data Surveillance and Information Privacy" (2013) P.126.

[2] http://www.gartner.com/technologhy/supply-chain-professionals.JSP

٢- الخوف من التلاعب بالحسابات المالية للمنشأت.

في عام ٢٠٠٩ بناء علي ما انتهي إليه هذا البحث، اتجهت أكثر من ٥٥% من الشركات المشاركة في هذا البحث لزيادة قيمة الاستثمار الداخلي في قضايا حفظ خصوصية البيانات عما أنفقته في العام الأسبق، وذلك عن طريق إستخدام التقينيات والسياسات الحديثة مثل :

١- أم الشبكات (من مضادات الفيروسات والشبكات الإفتراضية الخاصة)

٢- أدوات مراقبة أنشطة قواعد البيانات.

٣- المن الاحترازي (أنظمة كشف التلاعب ونقاط ضعف الشبكات والتطبيقات) وغيرها من الأنظمة الأخري التي تساعد الشركات في حماية خصوصية بياناتها.

المطلب الأول

تحديات حماية خصوصية البيانات

في ظل عدم توفر القدر الكافي من الحماية القانونية عبر شبكة الإنترنت، فإن كافة المعلومات المعلنه من الأفراد تكون بمثابة تنازل ضمني عن تلك المعلومات، ووجود ضمانات مثل وسائل حماية رسائل التأكيد وسياسات الخصوصية لا توفر القدر الكافي من حماية خصوصية البيانات المعلن عنها من قبل الافراد.[1]

ولإرساء نظام لحماية الخصوصية، يجب مراعاة طبيعة التهديدات الخاصة التي تتعرض لها الخصوصية عبر سبكة الانترنت، وذلك لأن الانترنت يستحدث سلسلة من التحديات في مواجهة حقوق حماية المستهلك والطفولة وحماية الخصوصية بشكل عام.

[1] Hunton& Williams LLP, New Requirements for online Privacy Policie, Basic Books, 2004, p.22

(ISSN: 2356 – 9492)

وفي هذا المطلب سنتناول هذه التحديات والتي تتمثل في :

الفرع الأول: تزايد كمية البيانات المجمعة والمعالجة غير الانترنت

الفرع الثاني: عولمة البيانات وفقان المركزية وأليات السيطرة والتحكم

الفرع الأول

تزايد كمية البيانات المجمعة والمعالجة عبر الانترنت

ورد في مؤلف ل جيري بيرن وديردري موليغان الأتي :

"تخيل أنك تسير في أحد السواق بين مخازن عديدة لا تعرف أي منها، فتوضع علي ظهرك إشارات تبين كل محل زرته وما الذي قمت به من شراء لمنتج أو أكثر، ان هذا يتشابه لما يحدث في بيئة الانترنت " .[1]

شهد التطور الهائل للتكنولوجيا وتقنية المعلومات عبر الانترنت تزايد التوجه نحو جمع البيانات المتوفره في العالم الحقيقي بسهوله من حيث قدرة الوصول إليها، وسهولة التبادل وأكثر ملائمة للتبويب بسبب تقنيات الحوسبة، وذلك كله عن طريق برمجيات التصفح والتبادل والنقل. إلا أن هذا يعد سلاحا ذا حدين، فسهولة الوصول للبيانات وإمكانية معالجتها والاستفاده منها من جانب، ومن جانب أخر عدم توفير الحماية اللازمة لخصوصية تلك المعلومات. وبالتالي، يجب الموازنة بين الاستفاده من الإفصاح عن المعلومات أو البيانات وتوفير الحماية اللازمة لخصوصياتها.

[1] Jerry Berman & Deirdre Mulligan , Privacy in the Dighital age: work in progress, Nova Law Review, volume 23, Number 2, the Internetand Law , (winter 1999), P.4

قد تم ابتكار أدوات لجمع أنواع مختلفة من المعلومات كان يستحيل الوصول إليها في الماضي، حيث يختص كل جهاز كمبيوتر أو هاتف نقال أو أي جهاز أخر متصل بالانترنت بعنوان بروتوكول إنترنت IP يوفر لتحديد هوية كل جهاز، والذي يتيح تتبع هذا الجهاز وتحديد موقعه، الأمر الذي ينشأ عن طريقها تحديات كثيره من حيث الخصوصية. فزيادة القدرة الحاسوبية تعني أنه يمكن تخزين كميات هائله من المعلومات ودمجها وتحليلها بمجرد جمعها بدون تكلفة وبشكل فعال. ويسمح التقدم التكنولوجي الربط بين قواعد البيانات مع بعضها البعض، الأمر الذي يتيح زيادة كميات البيانات التي يمكن معالجتها، ويهيئ الفرص للاستخدام التجاري للبيانات الشخصية. حيث أن أغلب الخدمات التي تقدمها هذه الشركات هي خدمات مجانية ويعتمد نشاطها علي جمع معلومات المستخدم وإعادة إستخدامها في أغراض تسويقية.[١]

ما تنامي حديثاً من شبكات التواصل الاجتماعي والتي تنازل الفرد فيها طواعية عن بياناته الشخصية للتسجيل في الموقع أو الحصول علي حساب خاص به، وفقاً لسياسات الخصوصية التي لا يقرأها عادة المستخدم، تكون تنازل صريح للفرد عن بياناته، فضلاً عن الإفصاح اليومي عن حاله المزاجيه، وصوره الشخصية وآرائه وأماكن تواجده وزياراته والأشخاص المقربين منه، وغيرها من المعلومات التي لا يجوز للغير الإطلاع عليها إلا بموافقة صاحب هذه البيانات. ونظراً لعدم الوعي القانوني للمستخدمين وعدم قراءة سياسات الخصوصية، ينتج عن ذلك إستغلال البيانات الشخصية للمستخدمين.[٢]

[1] Eneken Tikk, IP,address subject to personal data regulation , out Law, 2013, P.34
[2] Lori Andrews, Social Networks and the Death of Privacy, Free Press, 2011, P.121

(ISSN: 2356 – 9492)

الفرع الثاني

عولمة البيانات وفقدان المركزية وآلية السيطرة والتحكم

تنتقل المعلومات والإتصالات عبرالحدود دون أي إعتبار للجغرافيا والسيادة، حيث أن الأفراد يعطون معلوماتهم لجهات خارجية وداخليه، وقد لا تكون لها مكان معروف، الأمر الذي يثير مخاطر إساءة إستخدام هذه البيانات خاصة في الدول التي لا تتمتع بمستويات الحماية القانونية.

قد لا تستطيع القوانين الوطنية أن تخدم كثيراً في هذا الغرض وتضمنها نصوص بشأن السيطرة علي نقل البيانات، وقد لا يكون فاعلاً في ظل غياب التنسيق (الدولي) الذي يضمن أن تكون البيانات محكومه بإتفاقيات حماية مماثلة في الدولة المنقول لها البيانات.

وتنشا المخاطر في وجود ملاجئ لا تقيد عمليات المعالجة بأي قيد ولا توجد لديها أي قيد يمنع من جمع ومعالجة البيانات، وهي الملاجئ التي تهرب إليها المؤسسات في بيئة الانترنت للإفلات من القيود القانونية مثل (الضرائب، أو إتاحة تداول الأموال دون رقابة مثلما يحدث في تداول النقود الإفتراضية Bitcoin وغيرها) الأمر الذي يشكل تحديا عالميا وليس مجرد تحديا وطنياً، بخصوص حماية البيانات الشخصية عبر الحدود وهو الأمر الذي دفع إلي ضرورة إيجاد الأدوات العقدية التي تفرض علي المؤسسات متلقية البيانات أو الوسيطه في تلقيها وإرسالها إلي الطرف الثالث بإلتزامات قانونية معينه وذلك لحماية الخصوصية ومنع إساءة استخدام بيانات الأفراد الخاصة وممارسه النشطة الاحتيالية والمساس بخصوصية المستهلك عبر الانترنت .[1]

وضع قانون وطني ملائم لحماية الخصوصية المعلوماتية، قد يكون فاعلاً ويرجع ذلك لعنصر السيطرة والسيادة وتوفير جهات رقابية لمنع الاعتداء أو الاستمرار فيه، وكذا يتيح التعويض

[1] Anne Blise, PHD, Technology and Privacy in the new Milliennium, Ethica Publishing , 2004, P 163-199

الناتج عن اضرار هذا التعدي ولاحقة المخالفين. ولكن المر الكثر صعوبة، هو كيف يتم ذلك في ظل الانترنت الذي يملكه كل شخص وغير مملوك لأحد، ولا يتوافر فيه سلطة المركزية ولا جهة سيادة توفر الحماية من حدوث افعتداءات علي الخصوصية المعلوماتيه.

الانترنت يتصف باللامركزية وغياب السلطة التحكيمية، علي الرغم من وجود نشاط مضاد لجهة منع الاحتكار المعلوماتي وتباين المصالح بسن أمريكا وأوروبا وشرق آسيا، وليس لدعوات إنشاء حكومة الانترنت أو سياسات التنظيم الذاتي للالتزامات إلا وسائل إفتراضية، الأمر الذي تقضي التوجه للأهمية بعض مسائل التعاون الدولي، أبرزها الاتفاق في مسائل الاختصاص القضائي والقانون واجب التطبيق في بيئة منازعات الانترنت. وعلي الرغم من وجود توجهات للتعاون والتنظيم الدولي لدي منظمة التعاون الاقتصادي والتنمية و الاتحاد الأوروبي في هيئات عامله في بيئة الانترنت، إلا أنها حتي الآن لم تقدم حلولاً لجهة حل مشكلات عدم وجود تنظيم مقبول يحكم الانترنت في كل مسائله، ويعطي ذلك انطباعات أن الانترنت سيبقي خارج سيطرة الحكومات في اتحاد تنظيم قانوني تحكمه و تسيطر علي شؤونه.[1]

لم يعد إرادة القوي هي حجر الزاوية، حيث أن البيانات يتم نقلها عبر الانترنت من دوله إلي دولة أخري ومن منظمه إلي أخري ومن فرد إلي مؤسسه دون قيود وبجميع اللغات وفي رحلتها تزور العديد من مناطق الاختصاص القضائي ومناطق السيادة، قد لا تكون بين تلك المناطق تعاون أو روابط. ومن هنا وفي مثل هذه البيئة يوجد حاجه ملحه لجهد اشتثنائي علي النطاق الدولي أهمها الخروج من المفاهيم التقليدية للسيطرة. فقد يكون لفرد القدرة لتحدي أعظم القوي، لذا فإن عدالة

[1] Jason Angiulo and Graut Kleinwachter Privacy in a Transparent world , Ethica Publishing , 2010 , P.30

(ISSN: 2356 – 9492)

التعامل مع المعرفة وانتهاء عهد الاحتكار والسيطرة، هي أسس يتعين التفكير فيها بشكل يراعي السمات التقنية لمسائل الانترنت.[١]

المطلب الثاني

مصادر تهديد خصوصية البيانات الشخصية عبر الإنترنت

تختلف المصادر التي تهدد خصوصية المعلومات في الفضاء المعلوماتي لإسيما في البنية الرقمية، ولذلك سنتناول تهديدات الخصوصية علي النحو التالي

الفرع الأول: تحديد هوية المستخدم والاتجار بالبيانات

الفرع الثاني: تقنية إصطياد البيانات (وتقنيات ال Cookies)

الفرع الأول

تحديد هوية المستخدم والاتجار بالبيانات

في فرنسا، في مارس ١٩٧٤ ، تم وضع خطة لإنشاء نظام آلي للملفات الإدارية ودليل للأفراد (Système automatisé pour les fichiers Administrativeatifs et le répertoire des individus، or SAFARI). كان الهدف من المشروع هو ربط الخدمات العامة المختلفة باستخدام رقم هوية واحد. كان رفض هذا القانون هو السبب الجذري لقانون تكنولوجيا المعلومات والملفات والحريات (Loi “Informatique، fichiers et libertés”)

[١] عبد الله علي الشنبري ، التحولات المعرفيه الكبري منذ العصر الحجري وحتي جوجل ، مدارك للنشر ، ٢٠١١ ، ص ٣٢٠

الصادر في ٦ يناير ١٩٧٨. كان هذا بداية نقاش مستمر حول المشاركة الإدارية لقانون أكثر شمولاً. معلومات عن الأفراد في إطار الإدارة الرقمية.[١]

من نهاية التسعينيات إلى أوائل القرن الحادي والعشرين، بدأت قضية "الخصوصية الشخصية" في الظهور باعتبارها جهات فاعلة رئيسية على الويب (France Télécom وCisco وSun وeBay) انعكست على "المعايير العالمية لإدارة البيانات الشخصية وإجراءات المصادقة ٢ ". من عام ٢٠٠٣ فصاعدًا، تم إطلاق شبكات اجتماعية كبيرة، بما في ذلك MySpace و Friendster (معلق الآن) و3 LinkedIn في هذا الوقت أيضًا، أصبحت Google الأداة التي لا مفر منها التي نعرفها اليوم بالإضافة إلى مرآة الهوية العامة البارزة، مع أكثر من ثلاثة مليارات صفحة مفهرسة بحلول نهاية عام ٢٠٠٢. ظهرت أول آثار مجتمعية لمشكلة الهوية الرقمية من عام ٢٠٠٥ فصاعدًا، أي بعد عامين من إطلاق الشبكات الاجتماعية وفي الوقت الذي أصبح فيه استخدام هذه الشبكات أمرًا روتينيًا وواسع الانتشار.[٢]

تتكون الهوية الرقمية من مجموع الآثار الرقمية المتعلقة بفرد أو مجتمع: آثار "الملف الشخصي" المقابلة لما أقوله عن نفسي (من أنا)؛ تتبعات "التصفح" توضح المواقع التي أزورها

[1] Pierre Truche, Jean-Paul Faugère, Patrice Flichy, *Administration électronique et protection des données personnelles – Livre Blanc*, http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/024000100/0000.pdf,

[2] The "Do Not Track" standard, developed for browsers by W3C (http://www.w3.org/TR/tracking-dnt/), is starting to be adopted, notably by Microsoft, which unlike Firefox has chosen to activate it by default. But this move has failed to win unanimous support: "By blocking advertisers who would like to install their cookies in the user's browser, it seems Microsoft is banking on the fact that users will accept an exception being added to DNT to access its own services. Yet once Microsoft's exception is accepted, all the targeted adverts managed by Microsoft will be accepted." (Guillaume Champeau, "Do Not Track pourquoi Microsoft vous veut du bien", *Numérama*, 11 June 2012, http://www.numerama.com/magazine/22853-donot-track-pourquoi-microsoft-vous-veut-du-bien.html,

(ISSN: 2356 – 9492)

أو أعلق عليها أو أشتري منها (كيف أتصرف)؛ وأخيرًا، آثار مكتوبة أو توضيحية – ما أنشره على مدونتي، على سبيل المثال – والتي تعكس بشكل مباشر أفكاري وآرائي (ما أعتقده).[١]

بتعبير أدق، يمكن تعريف الهوية الرقمية على أنها مجموعة من الآثار (الكتابات، ومحتوى الصوت/ الفيديو، ورسائل المنتدى، وتفاصيل تسجيل الدخول، وما إلى ذلك) التي نتركها وراءنا، بوعي أو بغير وعي، أثناء تصفحنا للشبكة، وانعكاس هذه الكتلة من الآثار كما تظهر بعد "إعادة مزجها" بواسطة محركات البحث.[٢]

تتضمن هويتي الرقمية ما يلي: عنوان IP؛ رسائل البريد الإلكتروني. الاسم الاول؛ لقب؛ أسماء المستخدمين التفاصيل الشخصية والإدارية والمصرفية والمهنية والاجتماعية؛ الصور؛ الآلهة والشعارات. العلامات. الروابط. أشرطة فيديو؛ مقالات؛ تعليقات المنتدى. البيانات المحلية الجغرافية، إلخ.[٣]

مع انتشار الخدمات عبر الإنترنت، يأتي النمو الهائل في تفاصيل تسجيل الدخول، أي اسم مستخدم وكلمة مرور مقترنين يوفران الوصول إلى تلك الخدمات. ليس من غير المعتاد أن يمتلك فرد واحد عشرات من أسماء المستخدمين وكلمات المرور المختلفة. لقد شهدنا بالفعل ظهور العديد من البرامج المصممة خصيصًا لإدارة تفاصيل تسجيل الدخول المتعدد هذه.[٤]

اليوم، اختار المزيد والمزيد من الخدمات واللاعبين على الويب تبسيط الأمور لمستخدميهم من خلال الاشتراك في نقطة وصول واحدة تُعرف باسم OpenID ، حيث يتيح اسم

[1] John Battelle's searchblog, http://battellemedia.com.
[2] Sigmund Freud, "Three Essays on the Theory of Sexuality" (1905), trans. and ed. James Strachey, *The Standard Edition of the Complete Psychological Works of Sigmund Freud*, vii, 24 vols. (London: Hogarth Press, 1974), pp. 123–231
[3] Blanchette,J.f.& Johnson, D.G.Data retention and the panoptic society: the social benefits of forgetfulness.
[4] For example, see http://www.laviedapres.com.

مستخدم واحد وكلمة مرور واحدة للمستخدمين الوصول إلى رسائل البريد الإلكتروني الخاصة بهم أو لوحة معلومات المدونة الخاصة بهم أو حساب Facebook أو Twitter.[١]

تعمل المتصفحات الرائدة (Firefox و Google Chrome و Internet Explorer) على تطوير إدارة مباشرة و"أصلية" لتفاصيل تسجيل الدخول من واجهاتهم الخاصة. حرصًا منهم، على الأقل في الظاهر، على إبراز كيفية حماية خصوصية مستخدميهم، كما يقدمون أوضاع تصفح خاصة لا تخزن بيانات الاتصال المعتادة .[٢]

التهويل وشفافية الهوية الزائفة

يعطينا إجراء بحث على Google وهم صفحة فارغة لا تحتوي إلا على حقل البحث. ومع ذلك، في الحياة اليومية، يبدأ الكثير منا يوم عملنا عن طريق التحقق من رسائل البريد الإلكتروني، غالبًا على نفس منصة Google Gmail. من الآن فصاعدًا، وحتى عندما ننتقل مرة أخرى إلى محرك البحث، يعرف Google من نحن وما هو اسمنا، وبالتالي يأمر برؤية شفافة تمامًا لجميع طلبات البحث لدينا والوصول إلى كل رسالة أرسلناها أو تلقيناها. مثل: Gamil

عندما أطلقت Google خدمة البريد الإلكتروني عبر الإنترنت (Gmail) في ١ أبريل ٢٠٠٤، زادت بشكل كبير من مقدار مساحة تخزين محرك الأقراص المقدمة لمستخدمي الإنترنت، والأهم من ذلك، دمجت في Gmail نفس المنطق والصيغة المطبقة على جناحها

[١] رشاد عبد الله ، افنترنت في مصر و العالم العربي ، طذ ، أفاق للنشر و التوزيع ، ٢٠٠٥ ، ص ١٦.

[2] The Commission nationale de l'informatique et des libertés (CNIL) website provides information on case law dating from 2011: http://www.cnil.fr/la-cnil/actu-cnil/article/article/maitriser-les-informations-publiees-sur-les-reseaux-sociaux/, accessed 30 October 2012; Christelle Dardant's article, "Incertitudes autour de la jurisprudence 'Licenciements Facebook'", *Institut de recherche et d'études en droit de l'information et de la communication* (IREDIC), 31 January 2012, http://junon.univ-cezanne.fr/u3iredic/?p=8378, .

(ISSN: 2356 – 9492)

الإعلاني AdSense: جميع الرسائل سيتم التعامل مع تكوين مراسلاتنا الخاصة كصفحات ويب، وعلى هذا النحو، يتم فحصها وفهرستها بواسطة خوارزميات Google وبرامج الزحف.[١] والغايه من ذلك إقران الكلمات الرئيسية المميزة لمحادثاتنا بالإعلانات الأكثر استهدافًا والسياق الممكنة. لذلك تتم فهرسة كل رسالة، ولكن Gmail قادر أيضًا على تحليل موضوعات أو موضوعات المحادثة التي نتحدث عنها غالبًا، والأشخاص الذين نتواصل معهم بشكل منتظم، والمواضيع التي نناقشها، مما يجعل اهتمامه الإعلاني أكثر فعالية. بينما اعتمد مقدمو بريد الويب المتنافسون النموذج الاقتصادي لعرض لافتات إعلانية، كانت Google أول من قام بفهرسة مراسلاتنا الخاصة بنفس التقنيات وبهدف نشر نموذج اقتصادي كان محجوزًا حتى الآن لصفحات الويب العامة. وعلى الرغم من أنه من الممكن إخفاء هذه الإعلانات المستهدفة بمساعدة موفري خدمات الطرف الثالث، إلا أنه من المستحيل مع ذلك منع فهرسة رسائل البريد الإلكتروني الخاصة بنا.[٢]

ما هو الثمن الذي يجب دفعه؟

غالبًا ما يؤدي تسجيل الدخول إلى إحدى الخدمات قبل استخدام خدمة أخرى، وخاصة محرك البحث، إلى خذلاننا أثناء التصفح. هذا هو السبب في أن الآثار التي نتركها دون وعي أو عن غير قصد على الشبكة تعتبر أساسية في تعريف الهوية الرقمية: فهي تلخص أدوات تسجيل الدخول المستخدمة في هندسة شفافية الهوية.[٣]

[1] Deighton, J.A The Presentatio of self in the Information age Harvard Business SchoolWorking Knowledge. (2006) P.66

[2]Maslow's hierarchy of needs", *Wikipedia*, http://en.wikipedia.org/wiki/Maslow's_hierarchy_of_needs.

[3] Amazon recommendations are one example. Recommendations are based on users' buying history and what they have viewed on the site, as well as on overall statistics about sales on the platform.

هل هذا هو الثمن الذي يتعين علينا دفعه مقابل تجربة تصفح سلسة ونتائج بحث أكثر صلة؟ تدافع معظم شركات الإنترنت عن ممارسة التعرف على المستخدمين وتعقبهم باعتبارها الطريقة الوحيدة لتوفير تجربة تصفح ثرية وإضفاء الطابع الشخصي على الخدمة المقدمة. في حين أن هذه الحجة يمكن تبريرها من الناحية الفنية، فإنها لا تعفي تلك الشركات نفسها من تقديم ضمانات فيما يتعلق بطول الفترة الزمنية التي تحتفظ فيها بهذه البيانات الشخصية، وكيفية استخدامها.[1]

تسير الدائرة الفاضلة للهوية الرقمية على النحو التالي: قبل التمكن من الوصول إلى موارد النظام (التفويض)، يجب أن أقول أولاً من أنا (تحديد الهوية)، ويجب التحقق من ذلك إما عن طريق إجراء تقني –على الأقل كلمة مرور (المصادقة)–أو بواسطة طرف ثالث مثل بروتوكول OpenID (شهادة).[2]

ومع ذلك، غالبًا ما تتحول هذه العملية إلى حلقة مفرغة يكون فيها النظام نفسه مخولًا للوصول إلى مواردي (المستندات، ورسائل البريد الإلكتروني، والأصدقاء، وما إلى ذلك)، أو في الواقع الكتابة على مساحات الإنترنت الخاصة بي (حسابات Facebook أو Twitter).

التعريف مستمر وشفاف في كثير من الأحيان (انظر أعلاه)، بينما تصبح المصادقة مشكلة بسبب انتشار أسماء المستخدمين. تصبح الشهادة في النهاية نوعًا من حصان طروادة يسمح للأطراف الثالثة (سواء اخترناهم أم لا) بالوصول إلى بعض بياناتنا الشخصية. هذا هو الحال مع بعض تطبيقات Facebook التي لاقت نجاحًا شعبيًا بفضل قيمتها الترفيهية و"سهولة

[1] See the debates on the Loppsi and Hadopi laws, the Edwige file, etc

[2] Roger Clarke, The suprevisor's Dilemma: Reconcilition possible between , the Candidate's Nedds and the supervisor's Integrity, Sloenia (June2013) P.231

(ISSN: 2356 – 9492)

استخدامها". عندما نضيف هذه التطبيقات إلى ملفنا الشخصي، يمكن للمعلنين التعرف على تفضيلاتنا وأذواقنا، في الواقع حول جزء كامل من حياتنا الخاصة .[١]

الجهات الفاعلة في السوق

بالنسبة للاعبين في سوق الهوية الرقمية (محركات البحث والشبكات الاجتماعية) ، فإن الأمر الأكثر أهمية هو تعزيز نموذجهم الاقتصادي: خدمة مجانية يتم تمويلها عن طريق الإعلانات. من أجل ذلك يحتاجون إلى خريطة محدثة باستمرار لجميع المحتويات التي يتم الوصول إليها على الويب، ولكن أيضًا –وكان هذا هو الأصل العظيم للشبكات الاجتماعية – خريطة لعلاقاتنا الاجتماعية واهتماماتنا. لأن الجمع بين الاثنين هو الذي يحافظ على دوران عجلة اهتماماتهم الإعلانية ويسمح لهم ببيع بيانات ثمينة للغاية للمعلنين مستخرجة من عينات تمثيلية هائلة ولكن أكثر من أي وقت مضى. في عالم اقتصاد يكون فيه الاهتمام، انتباهنا، هو أندر الموارد وبالتالي أغلى ثمناً، يسود التنميط وتجزئة السوق.[٢]

ومن الوقائع الفاضحه في هذا المجال، ما قامت به شركة إنتل، كبري شركات صناعة المعالجات، من تحديد أحد منتجاتها من الكمبيوترات وتمييزه بحيث كلما استخدم الشخص هذا الكمبيوتر الموسوم فإن البيانات الخاصة به تظهر ويميزه عن غيره من المستخدمين. ومن الوقائع الشهيرة أيضاً، ما أعلن في١٩٩٨ من قيام أحد أكبر مواقع الانترنت التجارية (Double Click)، ستزود معلومات زبائنه – بخصوص قراراتهم وتسويقهم وعادات التسلية الخاصه بهم – إلي نظام أنشأته إحدي شركان ولاية ماسشيوسيتش التي كانت تتبع أكثر من ٣٠ مليون مستخدم

[1] See Janna Quitney Anderson, Lee Rainie, "The Future of The Internet", *Pew Internet*, http://www.pewinternet.org/2014/03/11/digital-life-in-2025/,
[2] Clay Shirky", *Wikipedia*, https://en.wikipedia.org/?title=Clay_Shirky.

وتسجل ما يقومون به، وما يقرؤون بدوم علم المستخدمين.[١] وفي ٢٠٠٩ تم بيع بيع كمبيوترات لا تزيد أسعارها عن ١٠٠٠دولار تتيح تتبع مسالك المستخدمين وكذلك كافة البيانات عنهم وعن أسرهم، وذلك علي سبيل ممارسة البيع التي تستهدف الخصوصية.[٢]

عثر الباحثون في دراسة أجريت علي مستخدمين في أميركا الشمالية وأوروبا وآسيا، حيث تم تحليل البيانات المتداولة علي الشبكة العنكبوتية العامة، ووجدوا نحو ١٠٠ مليار غيغابايت من البيانات المقرصنة المتداولة، وهو ما يشكل ٢٣.٨% من إجمالي البيانات التي تم تداولها في تلك الفترة، علما بأن النطاق المخصص لهذه النوعيه من عمليات نقل وتبادل البيانات جاوز نسبة ١٦٠% في الفترة من ٢٠١٠ و حتي ٢٠١٢.[٣]

الفرع الثاني

تقنية إصطياد البيانات (وتقنيات ال Cookies)

هل تلقيت يومًا بريدًا إلكترونيًا يبدو أنه من البنك الذي تتعامل معه يحذرك من أنه سيجمد حسابك الجاري ما لم تتحقق من معلوماتك الشخصية؟ قد يحتوي البريد الإلكتروني على ارتباط. وإذا نقرت؟ ربما تكون قد وصلت إلى موقع ويب يطلب منك ملء معلومات شخصية مثل رقم الضمان الاجتماعي وأرقام الحساب المصرفي.

[1] Saul Hansell, "Big Web Sites to Track Steps of Their Users" , N.Y. TIMES ABSTRACT , Aug.16,1998, at 1, available in 1998 WL5422846. P21

[2] Karen Kaplan, In Giveawayof 10.000 Pcs, the price is Users' Privacy Marketing : Recipients Must agree to Let Pasadena Firm Monitors Where They Go on Internet and What They Buy , L.A. TiMES, (Feb,8,2009), at A1 P.51

[3] David Price New Study: The Size and Scope of Global Internet Piracy is on the rise (VIDEO) of NetNamws retriveted , http://cretivefuture.org/new-study-the-size-and-scope-of-global-internet-priracy-is-on-the-rise-video/16/6/2014

(ISSN: 2356 – 9492)

المشكلة لا تأتي رسائل البريد الإلكتروني هذه من مصرفك الفعلي. بدلاً من ذلك، فهي جزء من أداة احتيال تسمى التصيد الاحتيالي الذي يستخدمه مجرمو الإنترنت وتشكل تهديدًا لأمنك الإلكتروني.

ما هو التصيد؟

التصيد الاحتيالي هو جريمة إلكترونية يحاول فيها المحتالون استدراج معلومات أو بيانات حساسة منك، من خلال التنكر كمصدر جدير بالثقة. يستخدم المخادعون منصات متعددة.[1]

الهدف النهائي بغض النظر عن الطريقة التي يستخدمها المحتالون؟ إنهم يريدون معلوماتك الشخصية حتى يتمكنوا من استخدامها للوصول إلى حساباتك المصرفية أو بطاقات الائتمان الخاصة بك. وسيقومون بإرسال عدد لا يحصى من رسائل البريد الإلكتروني والرسائل النصية المزيفة في جميع أنحاء العالم على أمل أن يخدعوا عددًا كافيًا من الأشخاص لتسليم هذه المعلومات الحساسة.قد تبدو بعض رسائل البريد الإلكتروني أو النصوص المخادعة غير مهنية بالنسبة لك، وذلك باستخدام قواعد نحوية سيئة أو تطلب منك النقر على روابط ذات عناوين URL غريبة المظهر. لكن لا يجب أن يكون المخادعون متطورين. يعمل مجرمو الإنترنت هؤلاء في الحجم، ويحتاجون فقط لخداع عدد صغير من الضحايا لاعتبار عملهم ناجحًا.

كمثال، في عام ٢٠١٨، أشارت لجنة التجارة الفيدرالية إلى هجوم تصيد استهدف مستخدمي Netflix. رسالة البريد الإلكتروني المخادعة التي يُزعم أنها مرسلة من Netflix وحذرت المستلمين من أن شركة البث "تواجه بعض المشاكل" في الوصول إلى معلومات الفواتير

[1]What is phishing? How to recognize and avoid phishing scams
https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html

الخاصة بالعميل. طلبت الرسالة من الضحايا النقر على رابط لتحديث طريقة الدفع الخاصة بهم. هذا الرابط، بالطبع، لم يأخذ المستخدمين إلى Netflix ولكن بدلاً من ذلك إلى موقع ويب مزيف أنشأه المحتالون.[1]

كيف تتأكد من أنك لست من هؤلاء الضحايا غير المحظوظين؟ يتعلق الأمر برمته بتعلم كيفية التعرف على عمليات التصيد الاحتيالي والعزم على عدم النقر مطلقًا على رابط في نص أو رسالة بريد إلكتروني يفترض أنها مرسلة من بنك أو مزود بطاقة ائتمان أو شركة أخرى معروفة. وهذا لا يشمل جميع رسائل البريد الإلكتروني المخادعة التي يتم اكتشافها في عامل تصفية البريد العشوائي.

كيف يعمل التصيد؟

يبدأ المخادع بتحديد هوية الضحايا المستهدفين (سواء على مستوى المؤسسة أو الفرد) ويضع استراتيجيات لجمع البيانات التي يمكنهم استخدامها للهجوم.بعد ذلك ، سينشئ المخادع طرقًا مثل رسائل البريد الإلكتروني المزيفة أو صفحات الويب المزيفة لإرسال رسائل تجذب البيانات من ضحاياهم ثم يرسل المخادعون رسائل تبدو جديرة بالثقة للضحايا ويبدأون الهجوم. بمجرد نشر الهجوم، سيقوم المحتالون بمراقبة وجمع البيانات التي يقدمها الضحايا على صفحات الويب المزيفة. أخيرًا، يستخدم المخادعون البيانات التي تم جمعها لإجراء عمليات شراء غير قانونية أو ارتكاب أعمال احتيالية.

[1] https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html

(ISSN: 2356 – 9492)

ومع ذلك، عند تحديد ما هو التصيد الاحتيالي، لا تبدو كل الهجمات وتعمل بالطريقة نفسها. يمكن أن تتخذ عمليات التصيد الاحتيالي أشكالًا متنوعة ويمكن أن يكون لها أهداف مختلفة في نشرها.

أنواع هجمات التصيد وأمثلة عليها[1]

يمكن أن تتخذ عمليات التصيد الاحتيالي عدة أشكال. ستطلب منك بعض رسائل البريد الإلكتروني المخادعة النقر فوق ارتباط لمنع إغلاق حسابك المصرفي أو بطاقة الائتمان الخاصة بك. عند النقر فوق الارتباط، سيتم نقلك إلى موقع ويب يطلب معلوماتك المالية الشخصية. يمكن أن يفتح الباب أمام سرقة الهوية.

تطلب الأنواع الأخرى من هجمات التصيد الاحتيالي النقر فوق ارتباط للتحقق من أن بطاقة الائتمان أو الحساب المصرفي ملكك. مرة أخرى، سينقلك هذا الرابط إلى موقع ويب احتيالي سيطلب منك تقديم معلومات شخصية أو مالية من المحتمل أن يلتقطها المحتالون.

قد تتلقى رسالة بريد إلكتروني للتصيد الاحتيالي تحذرك من أن حساب بريدك الإلكتروني ممتلئ ومعرض لخطر الإغلاق. ما لم تنقر على رابط، يحذر البريد الإلكتروني، ستفقد الوصول إلى رسائل البريد الإلكتروني الخاصة بك. مرة أخرى، قد تطلب روابط كهذه معلوماتك الشخصية وتلتقطها أو قد تثبت برامج ضارة أو برامج إعلانية على جهاز الكمبيوتر الخاص بك.

[1] The Center For Democracy and Technonlogy 's noop Demonstration att://snoop.cdt.org/ for example of information that can be easily captured by sites on the World Wide Web

كيفية الإبلاغ عن التصيد

إذا كنت ضحية عملية احتيال تصيد، فيجب عليك تنبيه السلطات المختصة. يمكنك الإبلاغ عن محاولة التصيد أو الجريمة إلى لجنة التجارة الفيدرالية على صفحة مساعد الشكاوى. يمكنك أيضًا الإبلاغ عن الهجوم إلى مجموعة عمل مكافحة الخداع أو إعادة توجيه رسالة البريد الإلكتروني المخادعة على reportphishing@apwg.org. إذا تلقيت رسالة نصية تصيد احتيالي، قم بإعادة توجيهها إلى (SPAM 7726).[١]

Cookies

تنتشر ملفات تعريف الارتباط على الإنترنت على نطاق واسع، لكن العديد من مستخدمي الإنترنت لا يدركون وجودها. ومع ذلك، إذا سبق لك استخدام عربة تسوق افتراضية لإجراء عملية شراء من متجرك المفضل عبر الإنترنت، فلا شك أنك واجهت ملفات تعريف ارتباط الإنترنت. بينما تُستخدم ملفات تعريف الارتباط بشكل متكرر لوظائف موقع الويب غير الضارة، إلا أنها تُستخدم أيضًا في أنشطة أكثر إثارة للجدل مثل تتبع أنشطة المستخدم. ولكن ما هي ملفات تعريف الارتباط على الإنترنت بالضبط، ولماذا هي مهمة؟ في مقال اليوم، سنجيب على هذين السؤالين المهمين ونلقي الضوء على المعلومات الأساسية التي يجب أن يعرفها كل مستخدم للإنترنت حول ملفات تعريف الارتباط على الإنترنت.[٢]

[1] What is phishing? How to recognize and avoid phishing scams, https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html

[2] Peng,Weihnong: Cisna, Jennifer HTTp cookies-" A Prromissing technology" , (2000) P.74

(ISSN: 2356 – 9492)

ما هي ملفات تعريف الارتباط على الإنترنت بالضبط؟

ملفات تعريف الارتباط على الإنترنت هي أجزاء صغيرة من البيانات يتم تخزينها كملفات نصية على المستعرض. باختصار، تعمل ملفات تعريف الارتباط على الإنترنت لربط أجزاء البيانات هذه بمستخدمين محددين. لتحقيق ذلك، يجب أن تحتوي على جزأين على الأقل من البيانات: معرف مستخدم فريد وبعض المعلومات حول هذا المستخدم الفريد. الأنواع الأربعة الشائعة من ملفات تعريف الارتباط هي:

الكوكيز المؤقته Session Cookies

تعريف الارتباط الخاصة بالجلسة لا تجمع ملفات تعريف الارتباط الخاصة بجلسات العمل معلومات من كمبيوتر المستخدم. ملفات تعريف الارتباط هذه مؤقتة ويتم مسحها بمجرد أن يغلق المستخدم متصفحه. تسمح ملفات تعريف الارتباط للجلسة بالتعرف على المستخدمين داخل موقع الويب بحيث يتم تذكر أي اختيارات أو تغييرات من صفحة إلى أخرى، ولا يُطلب من المستخدمين مرارًا وتكرارًا نفس المعلومات. تعتبر ميزات سلة التسوق مثالًا شائعًا على ذلك، حيث تسمح ملفات تعريف ارتباط الجلسة لسلة التسوق "بتذكر" العناصر التي تضعها في سلة التسوق الخاصة بك واختيارها للشراء.[1]

الكوكيز المستمرة (Persistent Cookies)

هذه الملفات يمكن أن توفر المواقع مع تفضيلات المستخدم. تم تصميمها لتوفير وصول سريع ومريح إلى الكائنات المألوفة لتحسين تجربة المستخدم. يمكن أن تساعد ملفات تعريف

[1] Peneberg,Adam;CookiesMonsters,Slate , (November 7, 2005) P.43

الارتباط الدائمة موقع الويب على تذكر إعدادات اللغة أو معلومات تسجيل الدخول، على سبيل المثال، بحيث لا يُطلب منك إدخالها عند كل زيارة.

تعريف ارتباط الطرف الأول هذه هي ملفات تعريف الارتباط التي يتم إنشاؤها بواسطة الموقع الذي تزوره وحفظها على جهاز الكمبيوتر الخاص بك.تعريف ارتباط الطرف الثالث بخلاف ملفات تعريف ارتباط الطرف الأول، لا يتم إنشاء ملفات تعريف الارتباط هذه بواسطة المجال الذي تزوره. تقوم الأطراف الأخرى بإنشاء ملفات تعريف الارتباط هذه لتتبع المستخدمين الذين ينقرون على الإعلانات. غالبًا ما تكون ملفات تعريف الارتباط للجهات الخارجية موضوعًا للتدقيق لأنها تشكل المزيد من المخاطر الأمنية وتثير أسئلة حول انتهاك الخصوصية.[1]

مخاوف أمنية[2]

بصفتك مستخدمًا للإنترنت، من الحكمة فهم مخاطر ملفات تعريف الارتباط بحيث يمكنك عرضها وحذفها عند الضرورة. انتهاك الخصوصية بالنسبة لمعظم مستخدمي الإنترنت، الخصوصية هي شاغلهم الأساسي عندما يتعلق الأمر بملفات تعريف الارتباط على الإنترنت. تتعقب محركات البحث المهمة وغيرها من الأنظمة الأساسية الإعلانية المستخدمين وتستخدم المعلومات لتقديم إعلانات مستهدفة. بطبيعة الحال، يشعر العديد من المستخدمين أن هذا يعد انتهاكًا صارخًا للخصوصية. ويكمن الاحتيال هنا في أن: ملفات تعريف الارتباط باستخدام ملفات تعريف الارتباط الاحتيالية عبر الإنترنت، تُستخدم ملفات تعريف الارتباط إما لتزوير هوية المستخدمين الشرعيين أو استخدام هوية المستخدمين الشرعيين للقيام بأعمال ضارة.

[1] Rouse, Margaret, " Transient Cookies Session Cookie", (September 2005) P.63
[2] What are cookies ?, https://us.norton.com/internetsecurity-privacy-what-are-cookies.html

(ISSN: 2356 – 9492)

المبحث الثالث

المجهودات التشريعية والدولية وقواعد الإختصاص القضائي لحماية الخصوصية المعلوماتية

بالرغم من المنافع الكبيرة التي أنتجتها تكنولوجيا المعلومات وشبكات المعلومات العالمية فقد أوجدت أيضًا سلبياتٍ عديدة تتمثل في امكانية جمع المعلومات وتخزينها واستخدامها على نحوٍ غير مشروع وبدون عِلم صاحبها، وذلك ما سنحاول بيانه من خلال مطلبين علي النحو التالي:

المطلب الأول: الجهود التشريعية والدولية لحماية الخصوصية المعلوماتية

المطلب الثاني: قواعد الاختصاص القضائي في الجريمة المعلوماتية

المطلب الأول

الجهود التشريعية والدولية لحماية الخصوصية المعلوماتية

في بداية حديثنا عن تعريف "الجريمة المعلوماتية" لابد من الإشارةِ إلى أنّ هذه الجريمة تكاد تستعصي على التعريف، ذلك أن الأبحاث والدراسات التي تتعلق بها قد أوردت لها تعريفاتٍ مختلفة ومتنوعة بحيث اتفقت جميعها على ألا تتفق على تعريف محدد لهذه الجريمة.

وفي هذا المطلب سنتناول الجهود التشريعية والدولية لمكافحة الإعتداء علي الخصوصية في فرعين علي النحو التالي :

الفرع الأول: الجهود التشريعية

تكشف النماذج المعروضة لوضعِ تعريفٍ لهذه الجريمة عن تعدد المصطلحات المُستخدمة للدلالة عليها وتحديدِ مفهومها، فهناك من يُطلق عليها اسم جرائم الحاسبات "Computer crimes" أو إساءة استخدام الحاسب "Computer abuse" أو الجرائم المرتبطة أو المتعلقة بالحاسبات " Computer related crimes " أو جرائم المُعالجة الآلية للبيانات "Automatic processing crimes of data" أو جرائم التكنولوجيا الحديثة أو جرائم تقنية المعلومات " Modern technology crime " أو جرائم المعلوماتية information " crimes" .

والتعريفات السابقة تختلف فيما بينها ضيقاً واتساعاً، ويمكن تصنيفها في ثلاث فئات هي:

- تعريفات مرتبطة بالحاسب.
- تعريفات مرتبطة بموضوع الجريمة.
- تعريفات متنوعة.

أولاً: تعريفات مرتبطة بالحاسب :

الحاسب الآلي هو عبارة عن: "جهاز إلكتروني يقوم بأداء العمليات الحسابية ومنطقة التعليمات المعطاة له بسرعةٍ كبيرة تصل إلى عشرات الملايين من العمليات الحسابية في الثانية الواحدة، كما له القدرة على التعامل مع مجموعة كبيرة من البيانات مع إمكانية تخزين هذه البيانات واسترجاعها عند الحاجة إليها". وانطلاقًا من ذلك أصبح استخدام الحواسيب من قبل

(ISSN: 2356 – 9492)

المؤسسات والدوائر والوكالات الحكومية ومن قِبَل الشركات الخاصة في مجال جمع ومعالجة البيانات الشخصية، وذلك بفضل مقدرة الحوسبة الرخيصة. إلا أن هذا الدور الايجابي للحواسيب خلف آثارًا سلبية تتمثل في:

أولا: إمكانية جعل فرص الوصول إلى هذه البيانات على نحو غير مأذون به بطريق التحايل أكثر من ذي قبل، الأمر الذي يفتح مجالاً أوسع لإساءة استخدامها أو توجيهها توجيها منحرفاً .

ثانيًا: ظهور ما يُعرف ببنوك المعلومات(١)، حيث اتجهت جميع دول العالم بمختلف مؤسساتها إلى انشاءِ قواعد البيانات لتنظيم عملها، وحيث أن المعلومات الشخصية التي كانت منعزلة متفرقة، يصعب التوصل إليها، أصبحت في بنوك المعلومات مجمعة متوافرة، متاحة أكثر من ذي قبل للاستخدام في أغراض الرقابة على الأفراد .

ثالثا: التكامل الحاصل بين المعلوماتية والاتصالات والوسائط المتعددة أتاح وسائل رقابة متطورة سمعية ومرئية ومقروءة، إضافةً إلى برمجيات التتبع وجمع المعلومات آلياً. علاوةً علي هذه المخاطر وما يتفرع عنها من مخاطر أخرى كتلك المتعلقة بالمعالجة المعلوماتية للبيانات الشخصية، كعدم مراعاة الدقة في جمع البيانات وكفالة صحتها وسلامتها، وعدم استخدام المعلومات للغرض التي جمعت من أجله وحتى مدة استخدامها.

فقد عرفها الفقيه الألماني تيدمان Tiedemann بأنها:"كل أشكال السلوك غير المشروع (أو الضار بالمجتمع) الذي يُرتكب باستخدام الحاسب" . في حين عرفها مكتب تقييم التقنية في

(١) لمزيد من التفاصيل حول بنوك المعلومات انظر :شمس الدين ابراهيم أحمد، وسائل مواجهة الاعتداءات على الحياة الشخصية في مواجهة تقنية المعلومات في القانون السوداني والمصري، دراسة مقارنة، دار النهضة العربية، القاهرة، **2005** .

الولايات المتحدة الأمريكية من خلال تعريف جريمة الحاسب " Computer crimes " بأنها: " الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيسياً " .

ويُعرفها البعض على أنها: "كل استخدام للحاسوب ونظامه بغية الاستفادة من الخدمات التي يؤديها دون أن يكون للمستخدم الحق في ذلك".

ثانيًا: تعريفات مرتبطة بموضوع الجريمة:

يرى واضعو هذه التعريفات أن الجريمة المعلوماتية ليست هي التي يكون النظام المعلوماتي أداة ارتكابها، بل هي التي تقع على النظام أو داخل نطاقه، ومن أنصار ذلك التعريف روزن بلاك Rosenblatt وآخرين، والذين يرون أن الجرائم المعلوماتية هي: "نشاط غير مشروع موجّه لنسخ أو تغيير أو حذف أو الوصول للمعلومات المخزنة داخل النظام أو التي تحول عن طريقه ويندرج هذا النوع تحت جرائم المعالجة الآلية للبيانات ".

وفي هذا المعنى أيضاً عرفها البعض على أنها: " السلوك السيئ الُمتعمَّد الذي يستخدم نظم المعلومات لإتلاف المعلومات أو إساءة استخدامها مما يتسبب (أو يحاول التسبُّب)، إما بإلحاق الضرر بالضحية، أو حصول الجاني على فوائد لا يستحقها " .

ثالثًا: تعريفات متنوعة :

هنالك تعريفاتٌ كثيرة تحدّثَ بها القائمون بالبحث في هذا المجال، فيرى ديفيد ثومبسون David Thompson أنها:"جريمة تتطلب لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية النظام المعلوماتي " .

(ISSN: 2356 – 9492)

في حين عرفها Solari. A تحت هذا النمط بأنها: "أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسيةً لارتكابِه". كما عرفتها منظمة التعاون الاقتصادي للتنمية O C D E " بأنها: " كل فعلٍ أو امتناعٍ من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقةٍ مباشرةٍ أو غير مباشرة عن تدخُّل التقنية المعلوماتية"

ومن ثمّ يتضِحُ أنّ الجرائم الإلكترونية "جرائم تقنية المعلومات" تُشير إلى فئتين من الجرائم الجنائية التي قد تطرح مشاكل مماثلة في معاملتها القضائية، وهي:

- الجرائم التي يكون فيها الكمبيوتر هو موضوع الجريمة أو الجريمة ذاتها .
- الجرائم التي يكون فيها الكمبيوتر وسيلة لارتكاب جريمة أو جريمة .

إن الجريمة المعلوماتية– وكما أسلفنا– إما أن تقع على جهاز الحاسب بمكوناته المادية أو المنطقية، بحيث يكون النظام المعلوماتي ذاته محلاً للجريمة، وإما أن تقع بواسطة جهاز الحاسب، بحيث يكون النظام المعلوماتي وسيلة لارتكابها .

الانترنت وعلاقته بالاعتداء على الخصوصية المعلوماتية

يُعرف الانترنت بأنها: " شبكة تتكون من العديد من الحاسبات المرتبطة ببعضها البعض إما عن طريق الاتصالات السلكية أو اللاسلكية وتمتد لتشمل مساحات كبيرة من الكرة الأرضية" فالإنترنت يُقدم خدمات كثيرة في مجالات متعددة للحصول على المعلومات في مختلف مجالات الحياة، ومن ثم فهو خزينة المعرفة وسيل للمعلومات المتدفقة[١] .

(1)Pour plus de détails sur les services Internet, voir: Nahla Abdul Qader Al-Momani, Crimes de l'information, Dar Al-Thaqafa pour l'édition et la distribution, Jordanie, 2008, p. 38 et au-delà .

وإذا كان للإنترنت هذه الأهمية، فإنه يُعدُ أيضًا أداةً رفيعة المستوى لارتكاب الجرائم، حيث يجعل المعلومات المعالجة الكترونيًا محلا للتجسس والسرقة والتلاعب بقصد الحصول على أموال أو خدمات غير مستحقة، حيث أن التصفح والتجول عبر الانترنت يترك لدى الموقع المزار كمية واسعة من المعلومات تتمثل فيما يلي[١] :

١- عنوان بروتوكول الانترنت العائد للعميل IP ومن خلاله يمكن تحديد اسم النطاق ومن ثمّ تحديد اسم الشركة أو الجهة التي قامت بتسجيل الدخول عن طريق نطاق أسماء المنظمات وتحديد موقعها.

٢- المعلومات الأساسية عن المتصفح ونظام التشغيل وتجهيزات النظام المادية المستخدمة من قبل العميل .

٣- وقت وتاريخ زيارة الموقع .

٤- مواقع الانترنت وعنوان الصفحات السابقة التي زارها المستخدم قبل دخوله الصفحة في كل الزيارة .

٥- وقد تتضمن أيضا معلومات محرك البحث الذي استخدمه المستخدم للوصول إلى الصفحة، وتبعا لنوع المتصفح قد يظهر عنوان البريد الالكتروني للمستخدم. وقد يتم التطفل على الحياة الخاصة للغير باستخدام برامج فيروسية، مثل حصان طروادة، الدودة والقنابل المنطقية، أو وسائل تقنية أخرى مثل ملفات الكوكيز وغيرها من البرامج.

(1) Saif Abdullah Al-Jabri, Sécurité de l'information et protection de la vie privée, Conférence internationale sur la sécurité de l'information électronique, Ensemble pour une interaction numérique sécurisée, tenue les 18 et 20 décembre 2005 à Mascate, Oman, p 246 .

(ISSN: 2356 – 9492)

ومن مخاطر الانترنت قيام الهاكرز باختراق أو بالدخول غير المأذون به، أو البقاء غير المشروع في نظام اتصالي خاص، وكذا جمع المعلومات الخاصة عن الآخرين، من خلال برمجيات ذكية يتم إرسالها في البريد الالكتروني، أو من خلال ظهورها كروابط مزيفة بإمكانها التجسس على المستخدم، أو حتى ارتكاب جرائم أخرى كالسرقة المعلوماتية والنصب .

أولاً : الوضع في فرنسا :

مما سبق يتبين أن هناك تحديات جديدة أوجدتها شبكة الانترنت في مواجهة حماية الخصوصية المعلوماتية، فهي زادت من حجم البيانات المجمعة والمعالجة وأتاحت عولمة المعلومات، وبالتالي فقدان المركزية وآليات السيطرة والتحكم .

أ- الجرائم التي يكون فيها الكمبيوتر هو موضوع الجريمة أو الجريمة ذاتها :

١- يهدف "قانون مكافحة جرائم تقنية المعلومات وحماية الحريات "الصادر في ٦ يناير ١٩٧٨ والمتعلق بتكنولوجيا المعلومات وحماية الحريات على وجهِ الخصوص إلى مكافحة إنشاء ملفات سرية ومكافحة العديد من الجرائم التي تنتهك حقوق الشخص والناتجة عن إنشاء تلك الملفات أو المعاملات التقنية.

وفي هذا الصدد:

- يُعاقب بالحبس لمدةٍ تتراوح من عامٍ إلي ثلاثةِ أعوام وبغرامةٍ يصلُ مقدارها إلي ٤٥ ألف يورو من قام، بما في ذلك عن طريق الإهمال، بإجراءِ معالجةٍ تلقائية للمعلومات الشخصية دون الامتثال للإجراءات الرسمية المنصوصِ عليها قبل تنفيذها[١] .

([1]) – Art. 226-16 du Code pénal Français .

- يُعاقب بالحبس لمدةٍ تتراوح من عامٍ إلي خمسةِ أعوام وبغرامةٍ يصلُ مقدارها إلي ٣٠٠٠٠٠ يورو، كل من قامَ أو حاول القيام بعملِ معالجةٍ آلية للمعلومات دونَ اتخاذ كافة الاحتياطات اللازمة للحفاظِ علي أمن تلك المعلومات، لاسيما عدم تشويهها أو تحريفها أو إتلافِها أو إبلاغها للغير الذي لا توجد له أيةُ صفةٍ في تلقي هذه المعلومات أو الاطلاعِ عليها[١] .
- يُعاقب بالحبس لمدةٍ تتراوح من عامٍ إلي خمسةِ أعوام وبغرامةٍ يصلُ مقدارها إلي ٣٠٠٠٠٠ يورو، كل من قام بجمع البيانات بوسائل احتيالية أو غير شريفة أو غير قانونية، أو من قام بمعالجة المعلومات الشخصية المتعلقة بشخصٍ طبيعي يُعارِضُها لأسبابٍ مشروعة[٢] .
- يُعاقب بالحبس لمدةٍ تتراوح من عامٍ إلي خمسةِ أعوام وبغرامةٍ يصلُ مقدارها إلي ٣٠٠٠٠٠ يورو، كل من احتفظ بمعلوماتٍ أو بياناتٍ شخصية دونَ موافقةٍ صريحةٍ من الشخص المعني تُظهِر، بصورةٍ مباشرة أو غير مُباشرة، أصولاً عنصرية أو آراءً سياسية أو فلسفية أو دينية أو توجهاتٍ نقابية أو أخلاقية لبعض الأشخاص[٣] .
- ورُغمَ تعدُّد بنوك المعلومات وكثرة المعلومات أو البيانات المخزنة، إلا أنّ تلك البيانات تحظى بحرمةٍ وقُدسيةٍ كباقي صور الخصوصية، فقد تشمل أسرارهم الشخصية أو توجهاتِهم الذاتية في مختلف الاتجاهات، والحفاظ عليها من العلن مهمةٌ ذاتَ طابعٍ انسانيٍ واخلاقيٍ .

وقد جسد المشرع الفرنسي هذه الحماية للبيانات أيًا كان نوعها [صور، كتابات، أصوات] من الافشاءِ والنقلِ والنشر، كما في المادة (٤٣) من قانون المعالجة المعلوماتية والحريات لسنة ١٩٧٨م ، كما أورد المشرع الفرنسي في المادة (٢٢٦/ ٢٢) من قانون العقوبات الجديد، تجريم

(1) Art. 226-17 du Code pénal Français .
(2) Art. 226-18 du Code pénal Français .
(3) Art. 226-19 du Code pénal Français .

(ISSN: 2356 – 9492)

كل فعل يرتكبه شخصٌ من شانهِ الكشف عن بياناتٍ شخصية، بمناسبة تسجيل أو فهرسة أو نقل أو أي شكلٍ من اشكال معالجة البيانات الشخصية، التي يترتب على كشفها الاعتداء على الشخصية الاعتبارية لصاحب الشأن أو حرمةِ حياته الخاصة في هذه المعلومات دون تصريحٍ بذلك من صاحب الشأن للغير الذي لا توجد له أية صفةٍ في تلقي هذه المعلومات ، وعلى النهج ذاته سار المشرع النمساوي في عقاب كل من افشى عمدًا أو استخدم معلوماتٍ مصرحٌ له وحده، بسبب طبيعة عمله في مجال المعالجة الالكترونية للمعلومات ، باطلاعِ الغيرِ عليها .

ب–يهدف قانون ٥ يناير ١٩٨٨ والمعروف بقانون Godfrain إلي ضمانِ أمن نظم المعلومات.

ووفقًا لقرار مجلس أوروبا المؤرّخِ في ٣١ مارس ١٩٩٢ فإنّ أمن نظم المعلومات مُعترفٌ بهِ كضمانٍ أساسي في كل مجتمعٍ حديث . وتدعو اتفاقية مجلس أوروبا الأخيرة بشأن الجرائم الإلكترونية إلي تجريمِ أي سلوكٍ من شأنه أن يقوّضَ من سرية وسلامة وإتاحة البيانات المعالجة آليًا " المعالجة إلكترونيًا " .

ورغبةً من المشرع الفرنسي في الحد من هذه الظاهرة الاجرامية، فقد قام بتعديل هذا القانون في عام ١٩٩٤ تحقيقًا لهذا الغرض. وكان مُقتضي هذا التعديل، إضافةُ بابٍ ثالثٍ للباب الثاني من القسم الثالث من قانونِ العقوبات بعنوان: " الاعتداءات علي نظم المعالجة الآلية للمعلومات". وقد عالجت المواد من ١/٣٢٣ : ٤/٣٢٣ تلك المسألة علي النحو التالي :

- حيث تُعاقِب المادة ١/٣٢٣ الدخول أو البقاء غير المشروع إلي أحدِ نُظم المعالجة الآلية للمعلومات بعقوبة الحبس لمدةِ عامٍ وبغرامةٍ لا تزيدُ عن ١٥ ألف يورو. مع ملاحظةِ أنه في حالةِ إذا ما ترتب علي واقعة الدخول أو البقاء غير المشروع تعديل أو إلغاء أو إتلاف

البرامج أو نظم المعالجة، فإنّ العقوبة تتضاعفُ إلي الحبس لمدة عامين وبغرامةٍ يصلُ مقدارها إلي ٣٠ ألف يورو[١] .

- تُعاقِب المادة ٢/٣٢٣ الاعتداءات الإدارية علي سير نظم المعالجة الآلية للبيانات والتي يترتب عليها تعطيل سير النظام أو إعاقتِه بعقوبة السجن لمدة ثلاث سنوات وبغرامةٍ يصل مقدارها إلي ٤٥ ألف يورو[٢] .
- تُعاقِب المادة ٣/٣٢٣ الاعتداءات الحاصِلة بالفعل علي البيانات والمعلومات داخل نظام المعالجة الآلية بذات العقوبة المُقرَّرة في المادة سالفة الذكر[٣] .
- أما المادة ٤/٣٢٣ فإنها تُعاقب علي التجمُّع (المشاركة في ترتيب إجرامي) بقصد إعداد جريمة أو أكثر من الجرائم المنصوصِ عليها في المواد من ١/٣٢٣ : ٣/٣٢٣ من قانون العقوبات[٤] .

٢-الجرائم الجنائية التقليدية المُرتكبة عن طريق الإنترنت:

أ- الجرائم المتعلقة بالمساس بالكرامة الإنسانية:

أولاً: الجرائم المنصوص عليها في قانون العقوبات:

- **الاعتداء علي الأشخاص:** وهي الجَرائم التي يتمّ الوصول فيها إلى الهويّة الإلكترونية للأفراد بطرقٍ غير مشروعة؛ كحسابات البريد الإلكتروني وكلمات السِّر التي تخصُّهم، وقد تصل إلى انتحالِ شخصيّاتهم وأخذ الملفّات والصّور المُهمّة من أجهزتهم، بهدفِ تهديدهم بها ليمتَثلوا لأوامرهم، وتُسمّى أيضاً بجرائم الإنترنت الشّخصية.

(1) – Art. 323-1 du Code pénal Français .
(2) – Art. 323-2 du Code pénal Français .
(3) – Art. 323-3 du Code pénal Français .
(4) – Art. 323-4 du Code pénal Français .

(ISSN: 2356 – 9492)

- حيث يُعاقب علي التهديد بارتكاب جناية او جنحة ضد اشخاص بالشروع في الاعتداء عليهم بالحبس ٦ شهور وغرامة٧٥٠٠ يورو عندما يكون ذلك، متكررًا أو مكتوبًا أو مصورًا او بأي طريقةٍ أخرى. وتُرفع العقوبة الى الحبس لمدةِ ٣ سنوات وبغرامةٍ تصل إلي ٤٥٠٠٠ يورو إذا كان الامر متعلقٌ بتهديد بالقتل(١).
- في حينِ يُعاقبُ علي التهديد، بأي وسيلةٍ كانت، بارتكاب جناية أو جنحة ضد شخص ، بالحبس لمدةِ ٣ سنوات وبغرامةٍ تصل إلي ٤٥٠٠٠ يورو إذا كان مصحوبًا بأمرٍ بتنفيذ شرط . وتُرفع العقوبة إلى الحبس لمدةِ ٣ سنوات وبغرامة تصل إلي٧٥٠٠٠ يورو إذا تعلق الامر بالتهديد بالقتل(٢) .
- يُضافٌ إلي ذلك أيضًا :
- جرائم الابتزاز الإلكتروني: (Cyber extortion crime) : وهي أن يتعرّض نظامٌ حاسوبيّ او موقعٌ إلكترونيّ ما لهجماتِ حرمانٍ أو حظر من خدماتٍ مُعيّنة؛ حيثُ يشنّ هذه الهجمات ويُكرّرها قراصنة محترفون، بهدفِ تحصيلِ مُقابلٍ ماديّ لوقف هذه الهجمات.
- جرائم التّشهير، بهدف تشويه سُمعة الأفراد .
- جرائم السبّ والشتم والقدح

المطاردة الإلكترونية:

هي الجرائم المُتعلّقة بتعقّب أو مطاردة الأفراد عن طريق الوسائل الإلكترونيّة لغاية تعريضهم للمضايقات الشّخصية أو الإحراج العام أو السّرقة المالية، وتهديدهم بذلك؛ حيث يجمع

(1) – Art. 222-17 al 1 du Code pénal Français .
(2) – Art. 222-17 a2. 1 du Code pénal Français – Art. 222-18 al. 2 du Code pénal .

مرتكبو هذه الجرائم معلوماتِ الضّحية الشخصية عبر مواقع الشّبكات الاجتماعي وغرف المحادثة وغيرها.

- في حين تعاقب المادة ١/٢٢٦ من قانون العقوبات الفرنسي الجديد بالحبس لمدة سنة وبغرامة مقدارها ثلاثمائة الف فرنك فرنسي، كل من اعتدى عمدًا بوسيلةٍ أيًا كانت على أُلفة الحياة الخاصة للأخرين:

١- بالتقاطِ صورٍ أو بتسجيل أو بنقل، بدون موافقة صاحب الشأن، كلام صادر له صفة الخصوصية أو السرية[١] .

- كما تُعاقِب المادة ١/١٢/٢٢٥ كل من التمسَ أو قَبِلَ أو حَصُلَ، مُقابلَ أجرٍ، علي علاقة جنسيةٍ مع قاصِرٍ يُمارس البغاء [الدعارة] ولو كانّ ذلك بشكلٍ عرضيٍ:

١- بالحبس لمدة ثلاثِ سنوات وبغرامةٍ مقدارها ٤٥ ألف يورو، عندما تُرتكب الجريمة بصورةٍ اعتيادية أو في مواجهة عددٍ من القاصرين[٢] .

٢- وبالحبس لمدة خمسِ سنوات وبغرامةٍ مقدارها ٧٥ ألف يورو عندما يكون القاصر علي اتصالٍ بالجاني [مُرتكب الجريمة – المروِّج] من خلال استخدام شبكة تواصل لنشر المحتوي إلي جمهورٍ غير محدود[٣] .

- في حين تُعاقب المادة ٢٣/٢٢٧ ، كل من قام ، لغرض النشر ، بتحديد أو تسجيل أو نقل صور القاصر أو تمثيله في الحالات التي تكون فيها تلك الصور أو هذا التمثيل إباحيٌ بطبيعتِه بالحبس لمدة ثلاثِ سنوات وبغرامةٍ مقدارها ٤٥ ألف يورو. كما تُطبّق

(1) – Art. 226-1 du Code pénal Français .
(2) – Art. 225-12-1 du Code pénal Français .
(3) – Art. 225-12-2 du Code pénal Français .

(ISSN: 2356 - 9492)

العقوبات ذاتها علي من يشرُعُ في توزيعِ تلك الصور أو تلك المقاطِع المصوّرة بأي وسيلةٍ كانت[١] وبالحبس لمدة خمسِ سنوات وبغرامةٍ مقدارها ٧٥ ألف يورو في حالة استخدام شبكة اتصالات سلكية ولاسلكية لنشر صورة القاصر أو تمثيله المنطوي علي مقاطِع إباحية لجمهورٍ مجهول الهوية [عن طريق شبكة الإنترانت على سبيل المثال][٢]. وتُعاقب المادة ٢٣/٢٢٧ بالحبس لمدة سنتان وبغرامةٍ مقدارها ٣٠ ألف يورو، كل من حاز أو احتفظ بتلك الصور أ والمقاطِع المُشارِ إليها سلفًا[٣] .

- كما تُعاقب المادة ٢٤/٢٢٧ بالحبس لمدة ثلاثِ سنوات وبغرامةٍ مقدارها ٧٥ ألف يورو، كل من أوجد أو أتاحَ أو نشرَ بأي وسيلةٍ كانت وبصرف النظر عن تلك الوسيلة أو طريقةِ تداولها ، رسالة ذات محتويً عنيفٍ أو إباحيٍ أو كانت تمُسُ بشكلٍ خطيرٍ بالكرامةِ الإنسانية والتي من المُرجّحِ أن ينظر إليها شخصٌ قاصر[٤] .
- كما تُعاقب المادة ٢٥/٢٢٧ بالحبس لمدة خمسِ سنوات وبغرامةٍ مقدارها ٧٥ ألف يورو، كل من أجبر شخص بالغ عُنوةً علي الاعتداءِ الجنسي أو تحت وطئهِ التهديد ، علي شخصٍ قاصر يبلغ من العمر ١٥ سنة[٥].

وتتفاقم الجريمة المحددة في المادة ٢٢٧/٢٥[٦]:

١- عندما تُرتكب من قبل شخص شرعي أو طبيعي أو مُتبنَّي أو من قِبَلِ أي شخصٍ آخر له سلطةٌ على الضحية

(1) – Art. 227-23 du Code pénal Français .
(2) – Art. 227-23 al 2 du Code pénal Français .
(3) – Art. 227-23 al. 4 du Code pénal Français .
(4) – Art. 227-23 al 2 du Code pénal Français .
(5) – Art. 227-25 du Code pénal Français .
(6) – Art. 227-25 du Code pénal Français

٢- عندما يرتكبها شخصٌ يسيئ استعمال السلطة التي يعهد بها إليه بمُقتضي صفته

٣- عندما يرتكبها عدةُ أشخاصٍ يتصرفون كفاعلين أو شركاء

٤- عندما يكون هذا الفعل مصحوبًا بدفع أجر [ممارسة الدعارة أو البغاء]

٥- عندما يكون القاصِر علي اتصالٍ بالجاني عبر شبكة تواصلٍ لنشر المحتوي لجمهورٍ غير محدود. فيُعاقبُ عليها بالحبس لمدة عشرِ سنوات وبغرامةٍ مقدارها ١٥٠ ألف يورو.

- كما تُعاقب المادة ٢٢/٢٢٧ بالحبس لمدة خمسِ سنوات وبغرامةٍ مقدارها ٧٥ ألف يورو كل من يُشجع علي/ أو يُحاوِل إفساد القاصِر. وبالحبس لمدة سبعِ سنوات وبغرامةٍ مقدارها ١٠٠ ألف يورو، عندما يكون القاصِر دونَ سن الخامسة عشر[١]
- في حينِ تعاقب المادة ٢٣/٢٢٢ عن كل عملٍ من أعمال الاعتداء الجنسي، أيًا كان نوعه، يُرتكبُ ضد شخصٍ آخر تحتَ وطئه العنف أو الإكراه [والذي يُعدُ اغتصابًا]، بالسجن مع الأشغال الشاقة لمدةِ ٢٠ عامًا[٢] . وفي حالةِ توافر الظروف المشددة – أي عندما يُرتكب الفعل ضد قاصرٍ، وعندما يكون القاصِر علي اتصالٍ بالجاني عبر شبكة تواصلٍ لنشر المحتوي لجمهورٍ غير محدود – بالحبس لمدة سبعِ سنوات وبغرامةٍ مقدارها ١٠٠ ألف يورو[٣] .

(1) – Art. 227-25 du Code pénal Français
(2) – Art. 222-23 du Code pénal Français .
(3) – Art. 222-28 du Code pénal Français .

(ISSN: 2356 - 9492)

ب- جرائم إلكترونية ضدّ الملكية:

وهي جرائمٌ تستهدف المؤسسات الشخصيّة والحكومية والخاصّة، وتهدف لإتلاف الوثائق الهامة أو البرامج الخاصة، وتتمُّ هذه الجرائم عن طريق نقل برامج ضارّة لأجهزة هذه المؤسسات باستخدام الكثير من الطُّرق كالرسائل مثلاً .

الجرائم السّياسية الإلكترونية: وهي جرائم تستهدفُ المواقع العسكرية للدول بهدف سرقة معلومات تتعلّق بالدّولة وأمنِها .

سرقة المعلومات: وتَشمل المَعلومات المحفوظة إلكترونياً وكذا توزيعها بأساليبٍ غير مشروعة .

ج-الإرهاب الإلكتروني [Cyber terrorism] :

ولأن الإرهاب كما باقي المفاهيم يُطوِّر نفسه ويُسخِّر تطورات العلم في خدمةِ أهدافه ومقاصده، فقد كان للتقنيات الدور الأهم في توسيع آفاق انتشاره واستغلال ما توفره هذه التقنيات لهذا الإرهاب من فُرصٍ متزايدة في انتشاره ، ومن هنا برز نوعٌ آخر يُعدُ الأخطر والأكثر تأثيرًا، ألا وهو الإرهاب الإلكتروني كنوعٍ من أنواع الجرائم الإلكترونية .

ورغم التباين في تعريف الإرهاب الإلكتروني إلا أن الباحثين والمُراقبين اجتمعوا على تعريفه بأنه:

"هو استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين أو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو بيئية"، ويمكن أن نُزيد على ذلك : "بأنه

استخدام التقنية لزعزعة استقرار مجتمعٍ ما أو نظامٍ ما بتخريب بناه التحتية أو بث أفكارٍ هدَّامة وقيمٍ مستحدثة بهدف تحييده أو شله أو إزاحته عن المنافسة " .

وقد عرفت الاتفاقية العربية لمكافحة الإرهاب الصادرة في القاهرة عام ١٩٩٨ بأنه: " كل فعل من أفعال العنف أو التهديد أيًا كانت بواعثه وأغراضه يقع تنفيذًا لمشروعٍ إجرامي فرديٍ أو جماعي ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حريتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو اختلاسها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر".

وعليه يمكننا أن نقترح تعريفا للإرهاب الإلكتروني بأنه: "اختراقاتٌ للأنظمةِ الأمنيّة الحيوية على مواقع الإنترنت، تكونُ جُزءاً من مجهودٍ مُنظّم لمجوعةٍ من الإرهابيين الإلكترونيين أو وكالات مخابراتٍ دوليّة، أو أيّ جماعاتٍ تَسعى للاستفادة من ثغرات هذه المواقع والأنظمة الوصول للمواقع المُشفّرة والمحجوبة " .

د- الانتهاكات ضد قانون حُرية الصحافة [قانون ٢٩ يوليو ١٨٨١][1] :

- حيث يُعاقب بالحبس لمدة ثلاثةِ أشهرٍ وبغرامةٍ مقدارها ٣٧٥٠ يورو في حالةِ ما إذا كان الرفض بعد الحكم، كل من رفض إدخال نسخة مطبوعة أو تصحيحيها[2] .
- يُعاقبُ بالحبس لمدة سنة وبغرامةٍ مقدارها ٤٥ ألف يورو، كل من أنكر الجرائم المرتكبة ضد الإنسانية[1] على النحو المحدد في المادةِ السادسة من النظام الأساسي لمحكمة نورمبرغ العسكرية المُرفق باتفاق لندن المؤرَّخِ في ١٩٤٥/٠٨/٨[2] .

([1]) Cour de cassation, chambre criminelle, 16 octobre 2001 Affaire "Marianne" : T.G contre G.B et R.R. Diffamation - délai de prescription des délits de presse . .

([2]) .Art. 13 de la loi 29/07/1881 relative à la liberté de la presse

(ISSN: 2356 – 9492)

- يُعاقبُ بالحبس لمدة خمسِ سنواتٍ وبغرامةٍ مقدارها ٤٥ ألف يورو، كل من حرَّضَ علي الاعتداء المُتعمّد علي الحياة ، وعلي سلامة الشخص ، وكذا الاعتداءات الجنسية[٣] .
- يُعاقبُ بالحبس لمدة خمسِ سنواتٍ وبغرامةٍ مقدارها ٤٥ ألف يورو، كل من حرّضَ علي السرقة والابتزاز وأعمال العنف والتخريب المُتعمّد والذي يُشكّلُ خطرًا علي الأشخاص[٤].
- يُعاقبُ بالحبس لمدة خمسِ سنواتٍ وبغرامةٍ مقدارها ٤٥ ألف يورو، كل من حرَّضَ علي ارتكابِ جرائم تَضِر بالمصالح الأساسية للأمة[٥] .
- يُعاقبُ بالحبس لمدة خمسِ سنواتٍ وبغرامةٍ مقدارها ٤٥ ألف يورو، كلُ من حاولَ تبرير الجرائم التي تنتهك عمدًا حرية الحياة الخاصة والكرامة الانسانية وكذا الاعتداءات الجنسية[٦]
- يُعاقبُ بالحبس لمدة خمسِ سنواتٍ وبغرامةٍ مقدارها ٤٥ ألف يورو، كلُ من حاولَ تبرير جرائم الحرب أو الجرائم المُرتكبة ضد الإنسانية أو جرائم التعاونِ مع العدو[٧] .
- يُعاقبُ بالحبس لمدة خمسِ سنواتٍ وبغرامةٍ مقدارها ٤٥ ألف يورو، كل من حرَّض علي أو برَّرَ للأعمال (الأفعال) الإرهابية[٨] .
- يُعاقبُ بالحبس لمدة سنة وبغرامةٍ مقدارها ٤٥ ألف يورو، كل من حرَّضَ علي التمييز العنصري أو الكراهية أو العنف علي أساس الأصل أو الانتماء أو عدم الانتماء لجماعةٍ عرقية أو أمة أو علي أساسِ الدين[١] .

([1]) Tribunal de Grande Instance de Paris, ordonnance de référé, 30 octobre 2001 affaire j'Accuse et a. contre l'AFA, Monsieur D et a. contenus illicites - négationnisme-racisme - responsabilité - hébergement étranger – filtrage . . . .

([2]).– Art. 24 bis de la loi de 1881

([3]) – Art. 24 al.1-1° de la loi de 1881

([4]) . – Art. 24 al.1-2° de la loi de 1881

([5]) – Art. 24 al. 2 de la loi de 1881

([6])– Art. 24 al. 3 de la loi de 1881

([7]) .– Art. 24 al. 3 de la loi de 1881

([8]). – Art. 24 al. 4 de la loi de 1881

- يُعاقبُ بغرامةٍ مقدارها ٤٥ ألف يورو، كل من أشاعَ أخبار كاذبة[٢]، مُلفَّقَة، مزورة أو زائفة تُنسَبُ إلى أشخاصٍ آخرين[٣] .
- يُعاقبُ بغرامةٍ مقدارها ٤٥ ألف يورو، كل من قام بالتشهير العلني الذي يستهدِف المحاكم والقوات المسلحة [الجيوش] والهيئات والإدارات العامة[٤] .
- يُعاقبُ بغرامةٍ مقدارها ٤٥ ألف يورو، كل من قام بالتشهير العلني[٥] ضد القضاة والمحلفين والشهود والموظفين العمومين والبرلمان الوطني والمواطن المُكلَّفِ بولايةٍ (وظيفةٍ) عامة، والوزير[٦] .
- يُعاقبُ بغرامةٍ مقدارها ١٢ ألف يورو، كل من قام بالتشهير العلني[٧] للأفراد فيما يتعلق بحياتهم الخاصة [فيما يتعلق بالخصوصية][٨] .
- يُعاقبُ بالحبس لمدة سنة وبغرامةٍ مقدارها ٤٥ ألف يورو، كلُ من قام بالتشهيرِ علي نحوٍ عنصريٍ علي أساس الأصل أو العِرق أو الانتماء أو عدم الانتماء إلي عِرقٍ أو أمةٍ أو دين[٩] .

([1]). – Art. 24 al. 6 de la loi de 1881

([2]) Tribunal de Grande Instance de Paris (17ème chambre) 12 octobre 2000 Alain B-C Associés-Vienne-Informatique-Internet-hébergeur-Responsabilité (non) Forum de discussion -diffusion de messages -site WEB -valeurs juridiques des règles éthiques -Gaz.Pal 14 au 16 octobre 2001 page 56. S.

([3]) – Art. 27 de la loi de 1881.

([4]). – Art. 30 de la loi de 1881

([5]) – Tribunal de Grande Instance de Paris, ordonnance de référé, 6 février 2001 SA Ciriel contre SA Free Contrefaçon de marques- diffamation-responsabilité de l'hébergeur. Cour de cassation, chambre criminelle, 30 janvier 2001 Madame A.R. contre Monsieur A.B. Diffamation - délai de prescription des délits de presse .

([6]) .– Art. 31 de la loi de 1881

([7]) – Tribunal de Grande Instance de Paris, ordonnance de référé, 20 septembre 2000 Sarl One Tel contre SA Multimania Diffamation-responsabilité civile -- loi du 1er août 2000 - identification - responsabilité de l'hébergeur (non) .

([8]). – Art. 32 al. 1er de la loi 1881

([9]) .– Art. 32 al. 2 de la loi 1881

(ISSN: 2356 – 9492)

- يُعاقبُ بغرامةٍ مقدارها ١٢ ألف يورو، كلُ من قامَ بكيل الشتائم والسِّبابِ علنيًا [علي نحوٍ علنيٍ علنيٍ][١]
- يُعاقبُ بالحبس لمدة ستةِ أشهرٍ وبغرامةٍ مقدارها ٢٢ ألف يورو، كلُ من قام بكيلِ الشتائم والسِبابِ بسبب الأصل أو العِرق أو الانتماء أو عدم الانتماء إلي عِرقٍ أو أمةٍ أو دين[٢] .
- يُعاقبُ بغرامةٍ مقدارها ١٥ ألف يورو، كل من قام بنشر صورٍ، دون موافقة الشخص المعني ، لشخصٍ مُقيّدٍ (مُكبَّلٍ) أو مُعاقٍ أو محبوسٍ احتياطيًا[٣] .
- يُعاقبُ بغرامةٍ مقدارها ١٥ ألف يورو، كل من نشر استقصاءً أو أذاع أو علَّقَ علي ذنب شخصٍ مُتهمٍ [مُدعيٍ عليه] أو من المُحتمل الحكم ضده، أو نشر معلوماتٍ تسمح بالتوصُّلِ إلي تلك الاستقصاءات[٤] .
- يُعاقبُ بغرامةٍ مقدارها ١٥ ألف يورو، كل من نشر ، دون موافقة الضحية ، صورًا لمُلابسات ووقائع الجريمة مما يُلحِقُ ضررًا كبيرًا بكرامة هذا الأخير[٥].
- يُعاقبُ بغرامةٍ مقدارها ٣٧٥٠ يورو ، كل من قام بنشر لوائح الاتهام وجميع الإجراءات الجنائية أو الجزائية الأخرى قبل قراءتها في محاكمةٍ علنية – ما لم يُقدم قاضي التحقيق طلبًا مكتوبًا [على سبيل المثال لنشر استطلاع إلكتروني][٦] .

(1) – Art. 33 al. 1er et 2 de la loi de 1881
(2) .– Art. 33 de la loi de 1881
(3) – Art. 35 ter de la loi de 1881
(4)– Art. 35 ter de la loi de 1881.
(5) .– Art. 35 quater de la loi de 1881
(6) .– Art. 38 al. 1er (abrogé) de la loi du 29/07/1881

- يُعاقبُ بغرامةٍ مقدارها ٣٧٥٠ يورو، كلُ من قام بنشر المعلومات المتعلقة بعمل ومداولات المجلس الأعلى للقضاء، باستثناء المعلومات وجلسات الاستماع العامة التي تعقد بشأن المسائل التأديبية المُقدمة ضد القضاة[١] .
- يُعاقبُ بغرامةٍ مقدارها ١٥ ألف يورو، كل من قام بنشر وإتاحة المعلومات المَتعلقة بهوية أو تسمح بتحديدِ هوية:

١- القاصر الذي ترك والديه أو الوصي عليه أو الشخص أو المؤسسة المسئولة عن احتجازه أو التي عُهِد إليه بها.

٢- القاصر الذي تمَّ التخلي عنه أو انتحر .

٣- القاصر ضحية اعتداء أو جريمة . وذلك ما لم يُطلَب من الأشخاص المسئولين عن القاصر أو من السلطات الإدارية أو القضائية[٢] .

- يُعاقبُ بغرامةٍ مقدارها ١٥ ألف يورو ، كل من قام بنشر المعلومات المتعلقة بهوية ضحية الاعتداء الجنسي أو صورته عندما تكون قابلةً للتعرُّفِ عليه ، وبدون موافقته الخطيِّة[٣] .
- يُعاقبُ بغرامةٍ مقدارها ١٨ ألف يورو ، كل من قام بنشر جميع المعلومات المتعلقة بالدساتير الخاصة بالحزب المدني قبل البدء في إجراءات الدعوي العمومية[٤] .
- يُعاقبُ بالحبس لمدة سنتان في حالة العود وبغرامةٍ مقدارها ستة آلاف يورو[٥]:
  - كل من قام بنشر تقرير مداولات محاكم الأحداث،
  - كل من قام بنشرِ نصٍ أو رسمٍ توضيحيٍ يتعلق بهوية وشخصية الأحداث الجانحين.

(1) – Art. 38 al. 2 de la loi du 29/07/1881
(2)Art. 39 bis de la loi de 1881 , art. 227-1 et 227-2 du Code pénal
(3) .– Art. 39 quinquies de la loi de 1881
(4). – Art. 2 loi du 2 juillet 1931
(5) – Art. 14 al. 4 de l'Ordonnance du 2/02/1945

(ISSN: 2356 – 9492)

- يُعاقبُ بغرامةٍ مقدارها ٣٧٥٠ يورو ، كل من قام بنشر حكم محاكم الأحداث الذي يُشير إلي اسم أو هوية القاصر[١] .
- يُعاقبُ بالحبس لمدة ستةِ أشهرٍ وبغرامةٍ مقدارها ٧٥٠٠ يورو ، كلُ من قام بتشويه سمعة قرار المحكمة أو تقويض السلطة القضائية أو استقلالها [باستثناء التعليقات الفنية التي تهدف إلى إصلاح أو مراجعة القرار وتنقيحِه][٢].
- هذا وقد أوضحت محكمة النقض موقفها في حكمين[٣] صادرين في ١٦ أكتوبر ٢٠٠١ و٢٧ نوفمبر ٢٠٠١ تؤكد فيهما من جديد أن فترة التقادم في الإجراءات العامة تمتد، بالنسبة للجرائم الصحفية المُرتكبة على شبكة الإنترنت، اعتبارًا من اليوم الذي أتيحت فيه الرسالة أولاً للمستخدمين .

---

(1). – Art. 14 al. 5 de l'ordonnance du 2 février 1945

(2) – Art. 434-25 du Code pénal Français .

(3)Ces arrêts posent toutefois plusieurs interrogations

• Les notions de réseau et de site : La Cour de cassation ne distingue pas les deux notions. Or d'un point de vue technique, les notions de mise en ligne sur un réseau et mise en ligne sur un site ne se confondent pas . Il est en effet possible de supposer qu'une information diffamatoire mise en ligne pendant plusieurs mois sur un site, sans que les représentants de celui-ci n'aient été inquiétés, soit reprise par un autre site plus de trois mois après la première mise à disposition . Dès lors si l'on retient la date de mise en ligne sur le réseau Internet comme point de départ de la prescription, une poursuite pénale contre les responsables du second site paraît impossible. Il résulte de ces décisions que la prescription peut être acquise sans que l'écrit litigieux soit définitivement retiré du serveur.

• **La notion de réédition :**La chambre criminelle de la Cour de cassation, depuis un arrêt du 16 décembre 1910, rappelé dans un arrêt du 8 janvier 1991, estime que la réédition d'un ouvrage constitue un nouvel acte de publication .

Par ailleurs, la cour d'appel de Paris, dans un arrêt définitif du 15 décembre 1999 a, d'une part considéré que la diffusion sur Internet était un acte de publication continue, et, d'autre part, estimé que la modification de l'adresse du site constituait une nouvelle mise à disposition du public, point de départ d'un nouveau délai de prescription . Ainsi il semblerait possible, dans le cadre de l'exemple ci-dessus proposé, d'envisager des poursuites à l'égard du second site, sans que puisse être opposée l'exception de prescription . Les décisions du 16 octobre 2001 et 27 novembre 2001 considèrent que les infractions commises sur Internet ne dérogent en rien à la législation et à la jurisprudence de la Cour de cassation en matière d'infractions de presse . Par jugement en date du 26 février 2002, le tribunal correctionnel de Paris (17ème chambre) confirme cette analyse, en précisant que "chaque mise à jour du site constitue une infraction nouvelle", "chaque nouvelle mise à disposition d'objets aux internautes, fait courir un nouveau délai de prescription . "

)Décision disponible sur le site http = //www.foruminternet.org). Ainsi, tous faits tels que les provocations à la haine raciale, à la discrimination, la contestation de l'existence des crimes contre l'humanité, l'apologie de ces crimes, et plus généralement l'ensemble des infractions de presse, à partir du moment où ils auront pour support Internet, seront soumis à la prescription trimestrielle.

هـ- جرائم الاحتيال والاعتداء على الأموال[1] :

وتشملُ هذه الجرائم الكثير من الممارسات منها :

- إدخال بيانات غير صحيحة أو تعليماتٍ من غير المشروع التصّريح بها ،
- أو استعمالُ بياناتٍ وعمليّاتٍ غير مسموح الوصول إليها بغيةَ السّرقة من قِبل موظفّين فاسدين في الشّركات والمؤسسات المالية
- حذف أو تعديل المعلومات المحفوظة ،
- أو إساءة استعمال أدوات الأنظمة المُتوافرة وحزم البرامج .

ثانياً: الوضع في مصر:

في البداية يجب التأكيد علي أن القانون الجديد الخاص بحماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ يعد استكمالاً لسياسة التي تسعي مصر لتحقيقها في الفترة القادمة وهي أن تكون(ممر رقمي عالمي)، ومما لاشك فيه أن أي جريمة تتعلق بحماية البيانات أو تقنية المعلومات بشكل عام، يطبق فيه ايضاً قانون مكافحة جرائم تقنية المعلومات المصري الصادر في أغسطس ٢٠١٨، فضلاً عن الرجوع أيضاً لقانون العقوبات المصري.

وحسناً فعل المشرع المصري، لقيامه بإصدار قانون حماية البيانات الشخصية الذي كنا في انتظاره منذ عام ٢٠١٩، وقد تعرض القانون لأهم المسائل التي تعتبر بمثابة جداراً مانعاً

(1) – **Article 313-1** : Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002 L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende.

(ISSN: 2356 – 9492)

للحفاظ علي خصوصية البيانات في ظل العصر الرقمي، ومواكبه للنظام العام لحماية البيانات الشخصية الصادر عن الاتحاد الأوروبي الذي دخل حيز النفاذ عام ٢٠١٨ والذي يقتصر علي حماية كل مواطن داخل الاتحاد الأوروبي من تسريب بيانات.

وقد استعرض القانون في الفصل الخامس إلي إجراءات إتاحة البيانات الشخصية[١]

حيث نصت المادة (١٠) علي " يلتزم كل من المتحكم والمعالج والحائز عند طلب إتاحة البيانات الشخصية بالإجراءات الآتية:

١- أن يكون بناءً علي طلب كتابي يقدم إليه من ذي صفة أو وفقًا لسند قانوني.

٢- التحقق من توافر المستندات اللازمة لتنفيذ الإتاحة والاحتفاظ بها.

٣- البت في الطلب ومستنداته خلال ستة أيام عمل من تاريخ تقديمه إليه ، وعند صدور قرار بالرفض يجب أن يكون الرفض مسببًا ، ويعتبر مضي المدة المشار إليها دون رد في حكم الرفض.

كما نصت في مادة (١١):

يكون للدليل الرقمي المستمد من البيانات الشخصية طبقًا لأحكام هذا القانون ذات الحجية في الإثبات المقررة للأدلة المستمدة من البيانات والمعلومات الخطية متي استوفت المعايير والشروط الفنية الواردة باللائحة التنفيذية لهذا القانون.

كما تطرق القانون في الفصل السادسه إلي البيانات الشخصية الحساسة

[١] الجريدة الرسمية ، العدد٢٧ مكرر (ه)، ١٥ يوليو ٢٠٢٠
https://www.scribd.com/document/469505055/%D8%A7%D9%84%D8%AC%D8%B1%D9%8A%D8%AF%D8%A9-%D8%A7%D9%84%D8%B1%D8%B3%D9%85%D9%8A%D8%A9#fullscreen&from_embed

حيث نصت مادة (١٢): "يحظر علي المتحكم أو المعالج سواء كان شخصًا طبيعيا أو اعتباريًا جمع بيانات شخصية حساسة أو نقلها أو تخزينها أو حفظها أو معالجتها أو إتاحتها إلا بترخيص من المركز. وفيما عدا الأحوال المصرح بها قانونًا، يلزم الحصول علي موافقة كتابية وصريحة من الشخص المعني. وفي حالة إجراء أي عملية مما ذكر تتعلق ببيانات الأطفال، يلزم موافقة ولي الأمر"

يجب ألا تكون مشاركة الطفل في لعبة أو مسابقة أو أي نشاط آخر مشروطة بتقديم بيانات شخصية للطفل تزيد علي ما هو ضروري للمشاركة في ذلك. وذلك كله وفقًا للمعايير والضوابط التي تحددها اللائحة التنفيذية لهذا القانون.

كما نصت مادة (١٣) "بالإضافة إلي الالتزامات الواردة بالمادة (٩) من هذا القانون، يلتزم مسئول حماية البيانات الشخصية وتابعوه لدي المتحكم أو المعالج باتباع واستيفاء السياسات والإجراءات التأمينية اللازمة لعدم خرق البيانات الشخصية الحساسة أو انتهاكها"

وأورد في الفصل السابعة إلي البيانات الشخصية عبر الحدود[١]

حيث نصت مادة (١٤): "حظر إجراء عمليات نقل للبيانات الشخصية التي تم جمعها أو تجهيزها للمعالجة إلي دولة أجنبية أو تخزينها أو مشاركتها إلا بتوافر مستوي من الحماية لا يقل عن المستوي المنصوص عليه في هذا القانون، وبترخيص أو تصريح من المركز"

تحدد اللائحة التنفيذية لهذا القانون السياسات والمعايير والضوابط والقواعد اللازمة لنقل أو تخزين أو مشاركة أو معالجة أو إتاحة البيانات الشخصية عبر الحدود وحمايتها.

[١] الجريدة الرسمية ، العدد٢٧ مكرر (ه)، ١٥ يوليو ٢٠٢٠
https://www.scribd.com/document/469505055/%D8%A7%D9%84%D8%AC%D8%B1%D9%8A%D8%AF%D8%A9-%D8%A7%D9%84%D8%B1%D8%B3%D9%85%D9%8A%D8%A9#fullscreen&from_embed

(ISSN: 2356 - 9492)

كما نصت المادة (١٥): "استثناءً من حكم المادة (١٤) من هذا القانون، يجوز في حالة الموافقة الصريحة للشخص المعني بالبيانات أو من ينوب عنه نقل أو مشاركة أو تداول أو معالجة البيانات الشخصية إلي دولة لا يتوافر فيها مستوي الحماية المشار إليها في المادة السابقة ، وذلك في الحالات الآتية:

١- المحافظة علي حياة الشخص المعني بالبيانات، وتوفير الرعاية الطبية أو العلاج أو إدارة الخدمات الصحية له.

٢- تنفيذ التزامات بما يضمن إثبات حق أو ممارسته أمام جهات العدالة أو الدفاع عنه.

٣- إبرام عقد، أو تنفيذ عقد مبرم بالفعل، أو سيتم إبرامه بين المسئول عن المعالجة والغير، وذلك لمصلحة الشخص المعني بالبيانات.

٤- تنفيذ إجراء خاص بتعاون قضائي دولي.

٥- وجود ضرورة أو إلزام قانوني لحماية المصلحة العامة.

٦- إجراء تحويلات نقدية إلي دولة أخري وفقًا لتشريعاتها المحددة والسارية.

٧- إذا كان النقل أو التداول يتم تنفيذًا لاتفاق دولي ثنائي أو متعدد الأطراف تكون جمهورية مصر العربية طرفًا فيه.

كما نصت المادة (١٦): "يجوز للمتحكم أو المعالج، بحسب الأحوال، إتاحة البيانات الشخصية لمتحكم أو معالج آخر خارج جمهورية مصر العربية بترخيص من المركز متي توافرت الشروط الآتية":

١- اتفاق طبيعة عمل كل من المتحكمين أو المعالجين، أو وحدة الغرض الذي يحصلان بموجبه علي البيانات الشخصية.

٢- توافر المصلحة المشروعة لدي كل من المتحكمين أو المعالجين للبيانات الشخصية أو لدي الشخص المعني بالبيانات.

٣- ألا يقل مستوي الحماية القانونية والتقنية للبيانات الشخصية لدي المتحكم أو المعالج الموجودة بالخارج عن المستوي المتوافر في جمهورية مصر العربية

وتحدد اللائحة التنفيذية لهذا القانون الاشتراطات والإجراءات والاحتياطات والمعايير والقواعد اللازمة لذلك.

وفي الفصل الثامن أورد نصوص خاصة بالتسويق الإلكتروني المباشر[١]

حيث نصت مادة (١٧): "يحظر إجراء أي اتصال إلكتروني بغرض التسويق المباشر للشخص المعني بالبيانات ، إلا بتوافر الشروط الآتية" :

١- الحصول علي موافقة من الشخص المعني بالبيانات.

٢- أن يتضمن الاتصال هوية منشئه ومرسله.

٣- أن يكون للمرسل عنوان صحيح وكاف للوصول إليه.

٤- الإشارة إلي أن الاتصال الإلكتروني مرسل لأغراض التسويق المباشر.

٥- وضع آليات واضحة وميسرة لتمكين الشخص المعني بالبيانات من رفض الاتصال الإلكتروني أو العدول عن موافقته علي إرسالها.

كما نصت مادة (١٨): "يلتزم المرسل لأي اتصال إلكتروني بغرض التسويق المباشر بالالتزامات الآتية":

[١] الجريدة الرسمية ، العدد٢٧ مكرر (ه)، ١٥ يوليو ٢٠٢٠
https://www.scribd.com/document/469505055/%D8%A7%D9%84%D8%AC%D8%B1%D9%8A%D8%AF%D8%A9-%D8%A7%D9%84%D8%B1%D8%B3%D9%85%D9%8A%D8%A9#fullscreen&from_embed

(ISSN: 2356 – 9492)

١- الغرض التسويقي المحدد.

٢- عدم الإفصاح عن بيانات الاتصال للشخص المعني بالبيانات.

٣- الاحتفاظ بسجلات إلكترونية مثبت بها موافقة الشخص المعني بالبيانات وتعديلاتها ، أو عدم اعتراضه علي استمراره ، بشأن تلقي الاتصال الإلكتروني التسويقي وذلك لمدة ثلاث سنوات من تاريخ آخر إرسال.

وتحدد اللائحة التنفيذية لهذا القانون القواعد والشروط والضوابط المتعلقة بالتسويق الإلكتروني المباشر .

فضلاً عن قيام هذا القانون بإنشاء مركز حماية البيانات الشخصية[١]

مادة (١٩): "تنشأ هيئة عامة اقتصادية تسمي «مركز حماية البيانات الشخصية»، تتبع الوزير المختص، وتكون لها الشخصية الاعتبارية، ويكون مقرها الرئيس محافظة القاهرة أو إحدى المحافظات المجاورة لها، وتهدف إلي حماية البيانات الشخصية وتنظيم معالجتها وإتاحتها، ولها في سبيل تحقيق أهدافها أن تباشر جميع الاختصاصات المنصوص عليها بهذا القانون، ولها علي الأخص الآتي:

- وضع وتطوير السياسات والخطط الاستراتيجية والبرامج اللازمة لحماية البيانات الشخصية، والقيام علي تنفيذها.
- توحيد سياسات وخطط حماية ومعالجة البيانات الشخصية داخل الجمهورية.

[١] الجريدة الرسمية ، العدد٢٧ مكرر (ه)، ١٥ يوليو ٢٠٢٠
https://www.scribd.com/document/469505055/%D8%A7%D9%84%D8%AC%D8%B1%D9%8A%D8%AF%D8%A9-%D8%A7%D9%84%D8%B1%D8%B3%D9%85%D9%8A%D8%A9#fullscreen&from_embed

- وضع وتطبيق القرارات والضوابط والتدابير والإجراءات والمعايير الخاصة بحماية البيانات الشخصية.
- وضع إطار إرشادي لمدونات السلوك الخاصة بحماية البيانات الشخصية ، واعتماد مدونات السلوك الخاصة بحماية البيانات الشخصية بالجهات المختلفة.
- التنسيق والتعاون مع جميع الجهات والأجهزة الحكومية وغير الحكومية في ضمان إجراءات حماية البيانات الشخصية ، والتواصل مع جميع المبادرات ذات الصلة.
- دعم تطوير كفاءة الكوادر البشرية العاملة في جميع الجهات الحكومية وغير الحكومية القائمة علي حماية البيانات الشخصية
- إصدار التراخيص أو التصاريح والموافقات والتدابير المختلفة المتعلقة بحماية البيانات الشخصية وتطبيق أحكام هذا القانون
- اعتماد الجهات والأفراد ، ومنحهم التصاريح اللازمة التي تتيح لهم تقديم الاستشارات في إجراءات حماية البيانات الشخصية
- تلقي الشكاوي والبلاغات المتعلقة بأحكام هذا القانون ، وإصدار القرارات اللازمة في شأنها
- إبداء الرأي في مشروعات القوانين والاتفاقيات الدولية التي تنظم البيانات الشخصية أو تتعلق أو تنعكس نصوصها بصورة مباشرة أو غير مباشرة عليها
- الرقابة والتفتيش علي المخاطبين بأحكام هذا القانون ، واتخاذ الإجراءات القانونية اللازمة
- التحقق من شروط حركة البيانات عبر الحدود، واتخاذ القرارات المنظمة لها.
- تنظيم المؤتمرات وورش العمل والدورات التدريبية والتثقيفية ، وإصدار المطبوعات لنشر الوعي والتثقيف للأفراد والجهات حول حقوقهم فيما يتعلق بالتعامل علي البيانات الشخصية.

(ISSN: 2356 – 9492)

- قديم جميع أنواع الخبرة والاستشارات المتعلقة بحماية البيانات الشخصية ، وعلي الأخص لجهات التحقيق والجهات القضائية.
- إبرام الاتفاقيات ومذكرات التفاهم والتنسيق والتعاون وتبادل الخبرات مع الجهات الدولية ذات الصلة بعمل المركز وفقًا للقواعد والإجراءات المقررة في هذا الشأن.
- إصدار الدوريات الخاصة بتحديث إجراءات الحماية بما يتوافق مع أنشطة القطاعات المختلفة وتوصيات المركز في شأنها.
- إعداد وإصدار تقرير سنوي عن حالة حماية البيانات الشخصية في جمهورية مصر العربية.

الماده (٢١): "جلس إدارة المركز هو السلطة المهيمنة علي شئونه ومباشرة اختصاصاته ، وله أن يتخذ ما يراه لازمًا من قرارات لتحقيق أغراض المركز والقانون ولائحته التنفيذية وله علي الأخص ما يأتي":

- إقرار السياسات والخطط الاستراتيجية والبرامج اللازمة لحماية البيانات الشخصية.
- اعتماد اللوائح والضوابط والتدابير والمعايير الخاصة بحماية البيانات الشخصية.
- اعتماد خطط التعاون الدولي وتبادل الخبرات مع الجهات والمنظمات الدولية.
- اعتماد الهيكل التنظيمي واللوائح المالية والإدارية والموارد البشرية والموازنة السنوية للمركز
- الموافقة علي إنشاء مكاتب أو فروع للمركز علي مستوي الجمهورية.
- قبول المنح والتبرعات والهبات اللازمة لتحقيق أغراض المركز بعد الحصول علي الموافقات المتطلبة قانونية

مادة (٢٤): "يحظر علي أعضاء مجلس إدارة المركز والعاملين به ، إفشاء أي وثائق أو مستندات أو بيانات تتعلق بالحالات التي يقوم المركز برقابتها أو فحصها أو التي يتم تقديمها

أو تداولها أثناء فحص أو إصدار القرارات الخاصة بها ، ويظل هذا الالتزام قائمًا بعد انتهاء العلاقة بالمركز".

وفي جميع الأحوال، لا يجوز الإفصاح عن المعلومات والوثائق والمستندات والبيانات المشار إليها في هذه المادة إلا لسلطات التحقيق والجهات والهيئات القضائية.

مادة (٢٥): "للمركز بالتنسيق مع السلطات المختصة التعاون مع نظرائه بالبلاد الأجنبية وذلك في إطار اتفاقيات التعاون الدولية والإقليمية والثنائية أو بروتوكولات التعاون المصدق عليها أو تطبيقًا لمبدأ المعاملة بالمثل بما من شأنه حماية البيانات الشخصية والتحقق من مدي الامتثال للقانون من قبل المتحكمين والمعالجين خارج الجمهورية، ويعمل المركز علي تبادل البيانات والمعلومات بما من شأنه أن يكفل حماية البيانات الشخصية وعدم انتهاكها والمساعدة في التحقيق في الانتهاكات والجرائم ذات الصلة وتتبع مرتكبيها.

مادة (٣٤): "يكون للعاملين بالمركز الذين يصدر بتحديدهم قرار من وزير العدل بناءً علي اقتراح الوزير المختص صفة الضبطية القضائية في إثبات الجرائم التي تقع بالمخالفة لأحكام هذا القانون".

كما اختص الفصل الرابع عشر بالجرائم والعقوبات[1]

مادة (٣٥): "مع عدم الإخلال بأي عقوبة أشد منصوص عليها في أي قانون آخر ، ومع عدم الإخلال بحق المضرور في التعويض ، يعاقب علي الجرائم المنصوص عليها في المواد التالية بالعقوبات المقررة لها ".

[1] الجريدة الرسمية ، العدد٢٧ مكرر (ه)، ١٥ يوليو ٢٠٢٠
https://www.scribd.com/document/469505055/%D8%A7%D9%84%D8%AC%D8%B1%D9%8A%D8%AF%D8%A9-%D8%A7%D9%84%D8%B1%D8%B3%D9%85%D9%8A%D8%A9#fullscreen&from_embed

(ISSN: 2356 – 9492)

مادة (٣٦): "يعاقب بغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه كل حائز أو متحكم أو معالج جمع أو عالج أو أفشي أو أتاح أو تداول بيانات شخصية معالجة إلكترونيًا بأي وسيلة من الوسائل في غير الأحوال المصرح بها قانونًا أو بدون موافقة الشخص المعني بالبيانات ".

وتكون العقوبة الحبس مدة لا تقل عن ستة شهور وبغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه، أو بإحدى هاتين العقوبتين، إذا ارتكب ذلك مقابل الحصول علي منفعة مادية أو أدبية، أو بقصد تعريض الشخص المعني بالبيانات للخطر أو الضرر.

مادة (٣٧): "يعاقب بغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه ، كل حائز أو متحكم أو معالج امتنع دون مقتض من القانون عن تمكين الشخص المعني بالبيانات من ممارسة حقوقه المنصوص عليها في المادة (٢) من هذا القانون ويعاقب بغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه كل من جمع بيانات شخصية بدون توافر الشروط المنصوص عليها في المادة (٣) من هذا القانون.

مادة (٣٨): "يعاقب بغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز ثلاثة ملايين جنيه ، كل متحكم أو معالج لم يلتزم بواجباته المنصوص عليها في المواد (٤، ٥، ٧) من هذا القانون.

مادة (٣٩): "يعاقب بالغرامة التي لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه ، كل ممثل قانوني للشخص الاعتباري لم يلتزم بأحد واجباته المنصوص عليها في المادة (٨) من هذا القانون. "

مادة (٤٠): "يعاقب بغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه ، كل مسئول حماية بيانات شخصية لم يلتزم بمقتضيات وظيفته المنصوص عليها في المادة (٩) من هذا

القانون. ويعاقب بغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز خمسمائة ألف جنيه إذا وقعت الجريمة نتيجة لإهمال مسئول حماية البيانات الشخصية.

مادة (٤١): "يعاقب بالحبس مدة لا تقل عن ثلاثة شهور وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز خمسة ملايين جنيه ، أو بإحدى هاتين العقوبتين ، كل حائز أو متحكم أو معالج جمع أو أتاح أو تداول أو عالج أو أفشي أو خزن أو نقل أو حفظ بيانات شخصية حساسة بدون موافقة الشخص المعني بالبيانات أو في غير الأحوال المصرح بها قانونًا ."

مادة (٤٢) :"يعاقب بالحبس مدة لا تقل عن ثلاثة شهور وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز خمسة ملايين جنيه ، أو بإحدي هاتين العقوبتين ، كل من خالف أحكام حركة البيانات الشخصية عبر الحدود المنصوص عليها في المواد (١٤، ١٥، ١٦) من هذا القانون.

مادة (٤٣): "يعاقب بغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه ، كل من خالف أحكام التسويق الإلكتروني المنصوص عليها في المادتين (١٧، ١٨) من هذا القانون.

مادة (٤٤): "يعاقب بغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز ثلاثة ملايين جنيه ، كل عضو مجلس إدارة أو أي من العاملين بالمركز خالف الالتزامات المنصوص عليها في المادة (٢٤) من هذا القانون.

مادة (٤٥): "يعاقب بغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز خمسة ملايين جنيه ، كل من خالف أحكام التراخيص أو التصاريح أو الاعتمادات المنصوص عليها في هذا القانون.

مادة (٤٦): "يعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه ، أو بإحدى هاتين العقوبتين ، كل من منع أحد العاملين بالمركز ممن يتمتعون بصفة الضبطية القضائية من أداء عمله.

(ISSN: 2356 – 9492)

مادة (٤٧): "يعاقب المسئول عن الإدارة الفعلية للشخص الاعتباري المخالف بذات العقوبات المقررة عن الأفعال التي ترتكب بالمخالفة لأحكام هذا القانون ، إذا ثبت علمه بها ، وكان إخلاله بالواجبات التي تفرضها عليه تلك الإدارة قد أسهم في وقوع الجريمة.

ويكون الشخص الاعتباري مسئولاً بالتضامن عن الوفاء بما يحكم به من تعويضات إذا كانت المخالفة قد ارتكبت من أحد العاملين لديه وباسم الشخص الاعتباري ولصالحه.

مادة (٤٨): "في جميع الأحوال ، وفضلاً عن العقوبات المنصوص عليها في هذا القانون، تقضي المحكمة بنشر حكم الإدانة في جريدتين واسعتي الانتشار، وعلي شبكات المعلومات الإلكترونية المفتوحة علي نفقة المحكوم عليه . وفي حالة العود، تضاعف العقوبات الواردة في هذا الفصل بحديها الأقصى والأدنى.

ويعاقب علي الشروع في ارتكاب الجرائم المنصوص عليها في هذا القانون بنصف العقوبة المقررة لها.

الفرع الثاني

الجهود الدولية

تم انشاء اللائحة العامة لحماية البيانات الشخصية (GDPR) للبرلمان الأوروبي EU/2016/679 والتي تم اعتمادها في ٢٧ ابريل ٢٠١٦ و دخلت حيز النفاذ في ٢٥ مايو ٢٠١٨ وتم إلغاء التوجيه EC/95/46 المؤرخ في ٢٤ أكتوبر ١٩٩٥ ، وهذا التنظيم يسمي

نظاماً فريداً أو مرناً، لأنه علي الرغم من أنه تنظيم من حيث المبدأ يطبق بشكل مباشر إلا أن الدول الأعضاء لديها قدر كبير من الحرية، حيث ينص في عدة محاور علي (شروط مفتوحه)[١].

لذلك قامت الدول الأعضاء بتكييف قوانينها الوطنية لحماية البيانات الشخصية. وبالتالي، عدلت فرنسا القانون رقم 17/78 المؤرخ في ٦ يناير ١٩٧٨ المعروف بأسم (معالجة البيانات والحريات) بموجب القانون رقم 687/2018 المؤرخ في ٢٠ يوينو ٢٠١٨. بإلاضافة ألي ذلك هناك لوائح تنفيذية، مثل المرسوم رقم 687/2018 المؤرخ في أأغسطس ٢٠١٨، الذي يكمل القانون، ولكنه يفوض أيضاً أعمال للمفوضية الأوروبية لتوضيح هذا القانون .

وفي النهاية، هناك عملية تناسل معيارية ليس من السهل دائماً صياغة هذه المعايير، خاصة وأن النظام الأوروبي لحماية البيانات العامة يشجع أصحاب المصلحة علي وضع معايير مرنة، مثل مدونات السلوك أو الشهادات [٢]

وقد ولد النظام الأوروبي لحماية البيانات العامة من صلب أصعب المواقف التي اخترقت خصوصيات الأفراد في أوروبا بكل جرأة، حيث شهد الإتحاد الأوروبي في مطلع عام ٢٠١٨ هزّة في حماية البيانات، حيث دأبت شركة كامبريدج أناليتيكا لتحليل البيانات إلى استقطاب للمعلومات الخاصة بأكثر من ٥٠ مليون مستخدم لموقع فيسبوك، ووجّهت أصابع الإتهام إليها من قِبل الحكومات باعتبار هذه الفضيحة إنتهاكًا صريحًا لخوصيات المستخدمين، مما دفع بدول الاتحاد الأوروبي إلى توجيه الأنظار نحو تشريع قانون صارم وظيفته حماية الخصوصية على الإنترنت والفضاء الإلكتروني تحت عنوان اللائحة العامة لحماية البيانات، وبناءً على ما تقدّم؛

[1] Le nouveau re'glement sur La protection des donees – Celine castets – Renard- 18/10/2018 Http://actu.dalloz.etudiant.fr/focus-sur

[2] Le nouveau re'glement sur La protection des donees – Celine castets – Renard- 18/10/2018 Http://actu.dalloz.etudiant.fr/focus-sur

(ISSN: 2356 – 9492)

فإن القانون قد أكّد على مواجهة كافة الشركات الأوروبية اعتبارًا من ٢٥ من شهر آيار سنة ٢٠١٨ لنظام صارم يُجبرها على حماية البيانات والخصوصية لمستخدمي مواقع التواصل الإجتماعي بمختلف أنواعها.

GDPR ويشار إليه ب General Data Protection Regulation وهو أحد الأنظمة التي سنها قانون الاتحاد الأوروبي لغايات حماية البيانات والخصوصية للأفراد المقيمين فوق أراضي الاتحاد، وبموجب القانون فإن البيانات الشخصية لمرتادي شبكات التواصل الإجتماعي وشبكة الإنترنت بشكل عام تبقى تحت التحكم والسيطرة، ويشار إلى أن المجلس والبرلمان الأوروبي قد سن هذا القانون واعتمده في الرابع عشر من شهر نيسان سنة ٢٠١٦م؛ إلا أنه أُدخل حيز التنفيذ في الخامس والعشرين من شهر آيار سنة ٢٠١٨، وجاء النظام الأوروبي لحماية البيانات العامة ليحل محل حماية البيانات المشرع سنة ١٩٩٥م[١].

أهمية النظام الأوروبي لحماية البيانات العامة

- إلزام الشركات على توفير الحماية الفائقة للبيانات الشخصية والخصوصية للأفراد المقيمين داخل حدود دول الاتحاد الأوروبي.
- فرض القيود على الأنشطة التجارية وطريقة جمعها للبيانات، وتخزينها وتصديرها.
- تقديم أعلى درجات الاحترام للفرد الأوروبي وتبجيل حقوقه.
- ضرورة امتثال الشركات في القطاعين العام والخاص لما يشمله النظام الأوروبي لحماية البيانات العامة.

[١] **النظام الأوروبي لحماية البيانات العامة GDPR**، إيمان الحياري، https://www.mah6at.net/ ٣ يوليو ٢٠١٨

- تنسيق وتنظيم طرق حماية البيانات بكل كفاءة وفاعلية لـ٢٨ دولة عضو في الاتحاد الأوروبي.
- منح الأشخاص حقوقًا موسعة لاستقطاب البيانات التي جاءت بها الشركات حولهم مجانًا بواسطة طلب موضوع البيانات.
- وجوب حذف البيانات للأشخاص في حال سحب موافقتهم
- فرض الغرامة على الشركات المخالفة لبنود القانون، حيث تصل النسبة إلى ٤% من إجمالي القيمة السنوية للتداول.

محتويات النظام الأوروبي لحماية البيانات العامة [١]

- الموافقة والقبول، إذ يمنع استخدام البيانات من قِبل أي جهة دون وجود موافقة صريحة اللهجة من قِبل المستخدم، على أن يتم الحصول عليها بعدم تقديم طلب حصول على معلوماته بلغة يفهمها.
- الحق في المعرفة، يحق للفرد الإطلاع على ما تم تخزينه من معلومات خاصة به، والتعرف على الوجه الذي سيتم استخدام معلوماته به مع ضرورة موافقته على ذلك.
- الخصوصية حسب التصميم الافتراضي، التحقق من حماية المعلومات الشخصية بشكل صحيح، إذ يفرض القانون بناء نظام مصمم لحماية البيانات والقدرة على التحكم في الوصول إلى البيانات، وفرض بنود صارمة على من ينتهك ذلك.

[١] **النظام الأوروبي لحماية البيانات العامة GDPR**، إيمان الحياري، https://www.mah6at.net/ ٣ يوليو ٢٠١٨

(ISSN: 2356 – 9492)

- الإخطار في سرقة البيانات وفقدانها والوصول إليها دون إذن المستخدم، حيث يستلزم الأمر ضرورة إخبار السلطات المختصة بانتهاك الخصوصية في ظرف ٧٢ ساعة كحد أقصى وفقًا للمادة ٣٣.
- الحق في الوصول إلى البيانات والحرية بالتصرف بها ونقلها، حيث يتيح النظام للمستخدم الحرية التامة في تنزيل بياناته الشخصية واستخدامها أو نقلها.
- السماح للسلطات الوطنية بفرض الغرامات على الشركات المنتهكة لبنود اللائحة.
- وجوب الحصول على موافقة الوالدين في معالجة البيانات الشخصية لمستخدمي الإنترنت من فئة الأطفال.

التأثر ببنود النظام الأوروبي لحماية البيانات العامة[١]

اتسعت رقعة الحماية التي يوفرها هذا النظام تدريجيًا؛ لتشمل مرتادي شبكة الإنترنت دون استثناء وليس مواطني الاتحاد الأوروبي فقط، ومن اهم المواقع التي تتأثر بهذه اللائحة:

- موقع مجتمع وورد بريس الذي يعمل على جمع البيانات الشخصية لكل مستخدم.
- متجر قوالب وورد بريس، حيث يشترك به أعداد ضخمة من العملاء بواسطة الحسابات لشراء الإضافات والقوالب الخاصة بهم.
- مدونة ووردبريس، وذلك لاحتوائها على أداة للاشتراك في النشرات الإخبارية.
- حلول التجارة الإلكترونية، كموقع.WooCommerce
- موقع وورد بريس الخاص بتحليل البرمجيات.
- منصات عرض المحتوى.

[١] **النظام الأوروبي لحماية البيانات العامة GDPR**، إيمان الحياري، https://www.mah6at.net/ ٣ يوليو ٢٠١٨

المطلب الثاني: قواعد الاختصاص القضائي في الجريمة المعلوماتية

الاختصاص هو[1]:

السلطة التي يقرها القانون للقضاء في أن ينظر في دعاوى من نوعٍ معين. وبالنظر لطبيعة وخصائص الجريمة المعلوماتية فليس لها مقر ثابت أو دولة معينة بل تنتشر في كل دول العالم، وليست لها أية هيئة أو جهة تشرف عليها ومسؤولة عنها، الأمر الذي يترتب عليه عدم وجود قانون جنائي محدد أو موحد يحكم الجريمة، بل بالعكس، فهناك العديد من القوانين الجنائية التي تتعدّد بتعدُّد الدول والأنظمة القانونية ويرجع ذلكَ أساسًا لارتباط القانون الجنائي بالسيادة الوطنية.

ومن هنا تكمن الإشكالية في أن بعض السلوكيات والأفعال مجرمة في بعض الدول ومباحة في دول أخرى، وفي أغلب الدول لا توجد نصوص تنظم هذه السلوكيات، والسؤال المطروح إلى أي مدى يمكن تطبيق القانون الوطني على جرائم تقنية المعلومات العابرة للحدود؟

أن القاعدة العامة المطبقة في أغلب الدول هي مبدأ الإقليمية، بمعنى أن القانون الجنائي يُطبَّق على كافة الجرائم التي تقع في إقليم الدولة بغض النظر عن جنسية فاعلها أو مرتكبها، ومع هذا فإن تطور الإجرام وتوسُّعه إلى دول العالم تطلب وجود اتفاقياتٍ دولية لتسليم المجرمين، غير أن غالبية الدول لا تسلم رعاياها وفق لمبدأ السيادة من جهة، ومن جهة أخرى للتعارض مع مبدأٍ أساسي في القانون الجنائي وهو "عدم جواز محاكمة شخص عن فعل واحد أكثر من مرة ".

[1] Commission nationale de l'informatique et des libertés CNIL *http://www.cnil.fr* , Forum des droits sur l'Internet *http://www.foruminternet.org*

(ISSN: 2356 – 9492)

وعلى هذا الأساس سنحاول وضع ملامح نظام قانوني يسمح بمتابعة وملاحقة مرتكبي الجرائم المعلوماتية دون المساس بحقوق وحريات الأفراد التي تُقرها المواثيق الدولية، ووجوب احترام مبدأ الشرعية دون إعطاء فرصة للجناة من الإفلات من المتابعة الجنائية وتوقيع العقوبة المناسبة عليهم مما يحقق الأمن والاستقرار للمجتمع، وعليه سنبحث على معيار يتلاءم وطبيعة الجرائم الالكترونية .[١]

١-الاختصاص الإقليمي :

- إنّ البُعد الدولي لشبكة الانترنت يجعل تطبيق قواعد الاختصاص في المسائل الجنائية أمرًا مُعقدًا للغاية[٢]. ورُغمَ ذلك يمكن القول بأنّ المحاكم الفرنسية تختصُ بعددٍ من المنازعات المتعلقة بشبكة الإنترنت [مُنازعات تقنية المعلومات] بموجب القواعد المنصوص عليها في قانون العقوبات. وتستند قواعد الاختصاص إلى معيارين مُشتركين هما: المكان الذي ارتُكبت فيه الجريمة وجنسية مرتكب الجريمة أو الضحية[٣] .
- وقد تناول المشرع الفرنسي "مبدأ الإقليمية" في القانون الجنائي الفرنسي صراحةً ، فوِفقًا للمادة ١١٣-٢ من القانون الجنائي الفرنسي والتي أُدخِلت بموجب القانون رقم ٢٠١٦-٧٣١ المؤرّخِ في ٣ يونيه ٢٠١٦: "فإنّ القانون الجنائي الفرنسي يكون واجبَ التطبيق علي أي جنايةٍ أو جنحة تُرتكب عن طريق شبكة اتصالات إلكترونية، إذا ما ارتُكِبَت أو

[1] Agence pour les technologies de l'information et de la communication dans l'administration – ATICA *http://www.atica.pm.gouv.fr* , Direction centrale de la sécurité des systèmes d'information – Secrétariat général de la défense nationale – SCSSI, *http://www.ssi.gouv.fr*

([2]) (V. ,en ce sens , BÉNICHOU, Cybercriminalité: jouer d'un nouvel espace sans frontière, AJ pénal .2005. P.224) .

– ([3]) (V., en ce sens ,PADOVA, article préc. ,RSC 2002.765,spéc.p.768s).

تمت محاولة ارتكابها ضدَ شخصٍ طبيعيٍ أو اعتباريٍ يُقيمُ في فرنسا، وتُعد الجرائم مُرتكبة داخِلَ فرنسا ، طالما أنّ أحد الأفعال المكوّنة لها تم ارتكابُه داخِلَ فرنسا " .

- وهذا النص يُطبّق بالفعل علي جرائم تقنية المعلومات المُرتكبة داخلَ فرنسا، والمستوجبة لانعقاد الاختصاص للمحاكم الفرنسية، والمُتمثلة في:

– جرائم الاستخدام غير المشروع لأنظمة المعلومات.

– الوصول إلي المحتويات غير المشروعة.

– جرائم الدخول غير المشروع إلي نظامٍ معلوماتي وتعديل المعلومات والبيانات بقصد الحصول علي مبلغٍ من المال بطرُقٍ غير مشروعة.

– جرائم إدخال معلومات مغلوطة، غير صحيحة وغير مشروعة إلي نظامٍ معلوماتي وإتلاف أو تحريف المعلومات والبيانات الموجودة فيه[١] .

– جرائم التشهير العلني التي تُرتكب عن طريق شبكة الإنترنت. ومن ثمّ فإنّ إتاحة معلومات تشهيرية مزعومة للجمهور يستوجب انعقاد الاختصاص للمحاكم الفرنسية[٢] .

– وبالمثل، أشارت محكمة باريس الابتدائية[٣]، والتي أكدت حكمها محكمة الاستئناف في باريس[٤]، إلى أنّ المادة ١١٣-٢ من قانون العقوبات تنطبق على "مسائل جرائم الصحافة المرتكبة بواسطة شبكة الإنترنت أو من خلالها"، ولا سيما عندما يكون الإعلان (العنصر الأساسي المكوّن لجريمة التعدي) مُتاحًا عبر الإنترنت ويمكن الوصول إليه من فرنسا. وهذا العنصر يكفي لإثارة اختصاص المحاكم الفرنسية. وتسعى هذه الأخيرة

(1)– (TGI Paris, 13 nov. 1998, Gaz. Pal. 2000. 1. Doctr. 697, obs. Manseur-Rivet).
(2) – (Limoges, 8 juin 2000, BICC 2001. 210).
(3)– (TGI Paris, 26 févr. 2002, CCE 2002/5. Comm. 77)
(4)– (Paris, 17 mars 2004, CCE 2005/4. Comm. 72, obs. Lepage)

(ISSN: 2356 – 9492)

إلى وضع جميع المعايير التي تُحدد أن الموقع المعني موجهٌ بشكلٍ واضِح نحو مستخدمي الإنترنت الفرنسيين، كاللغة المُستخدمة وتوافر المنتجات المُباعة إلى ذلك الجمهور، لكي ينعقد لها الاختصاص[١] .

جرائم التزوير :

وفي هذا الصدد " في حالة التزوير"، ينعقد الاختصاص إما للمحكمة التي ارتُكب الانتهاك (التزوير) في نطاق اختصاصها المكاني أو للمحكمة التي نُشِر في نطاق اختصاصها المكاني الوثائق المزورة المُعالجة إلكترونيًا. وفي حالة التزييف على الإنترنت، يجوز للضحية أن يتخذ إجراءً قِبَل الدولة التي بيع فيها المنتج المُزيف. وتجدر ملاحظة، أنه وإن كانت اللغة المُستخدمة علي الموقع الأجنبي للترويج للمنتج غير الفرنسية، فإنّ ذلك لا يؤثر على تحديد الجمهور المقصود [الفرنسيين][٢]. ومنذ عدة سنواتٍ، ما فتئت محكمة النقض تُعالج مسألة اختصاص المحاكم الفرنسية في "مسألة التزييف على شبكة الإنترنت". وفي هذا الصدد، أقرت المحكمة الفرنسية – في حكمٍ أصدرته في ٩ ديسمبر ٢٠٠٣، استنادًا إلى قواعد القانون الدولي

(1) – (Crim. 9 sept. 2008, n° 07-87.281– Le président du tribunal de grande instance de Paris a, également, par une ordonnance de référé (TGI Paris, 24 janv. 2012, www.legalis.net), ordonné à Twitter la communication des données de nature à permettre l'identification des auteurs des messages à caractère antisémite, en se fondant sur le fait que les utilisateurs de Twitter sont soumis à l'application de la loi pénale française dès lors que l'un des éléments constitutifs de l'infraction a lieu dans le pays. De même encore, dans une ordonnance du 11 octobre 2012, le président du tribunal de grande instance de Nanterre, a conclu que « les juridictions françaises étaient compétentes pour connaître de l'entier préjudice occasionné par les atteintes alléguées à son droit à l'image » par des sites étrangers (TGI Nanterre, ord. ME, 11 oct. 2012, www.legalis.net , À cette fin, le juge a rappelé la jurisprudence de la Cour de justice de l'Union européenne selon laquelle « la personne qui s'estime lésée peut saisir soit les juridictions de l'État membre du lieu d'établissement de l'émetteur de ces contenus, soit les juridictions de l'État membre dans lequel se trouve le centre de ses intérêts ». En l'espèce, le juge a constaté que le centre des intérêts de la victime se situait en France, car elle y était née, elle y résidait avec sa famille et y exerçait son activité professionnelle).

(2)– La Cour de cassation, dans un arrêt du 12 février 2013 (n° 11-25.914) répond par la négative et souligne que « la commande unique de couteau passée par le titulaire de la marque française ne saurait suffire à caractériser la compétence de la juridiction française car les sites sur lesquels se trouvaient les produits incriminés ne visaient pas le public de France ».

الخاص– باختصاص المحكمة الفرنسية في معالجة الأضرار الناجمة عن انتهاك العلامات التجارية على موقعٍ باللغة الإسبانية على الإنترنت يمكن الوصول إليها في فرنسا. ويتضح في هذه القضية أن: " محكمة الاستئناف وجدت أن هذا الموقع حتى وإن كان متداولاً، كان متاحًا على الأراضي الفرنسية بحيث أن الضرر المزعوم لم يكن ظاهريًا ولا ممكنًا، إلا أنها قدمت لقرارها ما يُبرّرهُ قانونًا" ومن ناحيةٍ أخرى، فقد أعلنت محكمة الاستئناف في باريس[١] أن محكمة باريس العليا " محكمة النقض " لا تملك أي اختصاصٍ للنظر في دعوى انتهاك العلامة التجارية من قبل موقع لشركة لبنانية، في حين أن الموقع كان متاحًا الوصول إليه من فرنسا، خاصةً وأن الموقع مكتوبٌ باللغة الانجليزية[٢] وبالتالي لم يكن يُخاطب، بشكلٍ مباشر أو غير مباشر، مُستخدم الإنترنت الفرنسي .

وهذا الرفض لتنظيم اختصاص المحاكم الفرنسية على أساس "معيار الوصول إلى الموقع" يفيد شركة Google، نظرًا لأنّ محكمة الاستئناف في باريس تضع معيارًا جديدًا للولاية القضائية الإقليمية، وهو تحديد "وجود صلة (علاقة) كافية أو جوهرية أو هامة بين تلك الأفعال أو الحقائق ، والضرر المزعوم". وفي ضوءِ ذلك، ألغت الدائرة التجارية حكم الاستئناف الصادر في ٢٩ مارس ٢٠١١، على أساس أنها احتفظت باختصاص المحكمة الفرنسية، وترى أن:

(1) .– (Paris, 26 avr. 2006, legalis.net, art. 1653)

(2) – Elle souligne que la compétence de la juridiction française aurait pu être retenue si la cour d'appel avait recherché « si les annonces litigieuses étaient destinées au public de France », tel n'était pas le cas de ces annonces rédigées en anglais et diffusées sur le site **EBay .com**. La chambre criminelle va dans le même sens et casse un arrêt en matière de contrefaçon en soulignant « qu'il ne résulte pas que le site exploité par la société Universal Entertainment GMBH était orientée vers le public français, alors que la perpétration de la contrefaçon sur le territoire de la République est un élément constitutif de l'infraction » (Crim. 14 déc. 2010, n° 10-80.088). . En présence de faits commis à l'étranger, la loi pénale française est applicable « à tout crime ainsi qu'à tout délit punit d'emprisonnement commis par un Français ou par un étranger hors du territoire de la République lorsque la victime est de nationalité française au moment de l'infraction »(C. pén., art. 113-7) .

(ISSN: 2356 – 9492)

"مجرد إمكانية الوصول إلى موقعٍ على شبكة الإنترنت على الأراضي الفرنسية لا يكفي للإبقاءِ على ولاية المحاكم الفرنسية، باعتبارها ولاية مكان الضرر المزعوم"[١].

غير أنه فيما يتعلق بحماية المُصنفات الأدبية والفنية، تنص اتفاقية برن " convention de Berne " المؤرّخة في ٩ سبتمبر ١٩٨٦ في الفقرة الثانية من المادة ٥ على : " أن التمتع بهذه الحقوق وممارستها لا يخضع لأي إجراءٍ شكليٍ؛ وهذه الممارسة وكذلك التمتع بها مُستقلانِ عن وجود حمايةٍ في بلد المنشأ . وبناءً على ذلك، وباستثناء أحكام هذه الاتفاقية، فإن نطاق الحماية ووسائل الانتصاف المكفولة لصاحب البلاغ لضمان حقوقه يحكمها حصرًا قانون البلد الذي يُطلبُ فيهِ الحماية". وقد اعتمدت الدائرة الجنائية على هذا الحكم لاستبعاد تطبيق القانون الجنائي الفرنسي على أساس أن البلد الذي تُلتمس فيه الحماية هو"البلد الذي حدث فيه الاحتيال، وليس البلد الذي وقع فيه الضرر"[٢] .

ثم تنص المادة ١١٣–٥ من القانون الجنائي على: " أنّ قانون العقوبات الفرنسي يُطبّقُ على كل متهمٍ على أراضي الجمهورية ، كشريكٍ في الجناية او الجنحة المُرتكبة في الخارج إذا كانت الجناية أو الجنحة مُعاقبًا عليها على حدِ السواء في القانون الفرنسى والقانون الأجنبي ، وإذا كانت تلك الجريمة مُثبتة بقرارٍ نهائيٍ من القضاء الأجنبي". ويتعلق هذا الحكم بجرائم الإنترنت الُمرتكبة في الأراضي الفرنسية وفي الخارجِ على حدٍ سواء.

وأخيرًا، فيما يتعلق بالجرائم المرتكبة خارج أراضي الجمهورية الفرنسية، فسيكون منَ المناسب التمييز وِفقًا للتوصيف الجنائي للوقائع أو علي أساس المسئولية التقصيرية. ففي المسائل الجنائية، ينطبق القانون الجنائي الفرنسي على أي جريمةٍ يرتكبها فرنسيٌ خارج أراضي

(1) – (Com. 29 mars 2011, n° 10-12.272).
(2)– (Crim. 29 nov. 2011, n° 09-88.250 , AJ pénal 2012. 164, note Lasserre Capdeville).

الجمهورية. ولا ينطبق القانون الجنائي الفرنسي، في حالة الضرر المستوجِب للمسئولية التقصيرية، إلا على الجرائم التي يرتكبها الفرنسيون خارج أراضي الجمهورية إذا كانت تلكَ الوقائع يُعاقب عليها تشريع البلد الذي ارتُكِبَت فيه[١]. وإذا لم نعد نشير إلى طبيعةِ الجريمة، بل إلى المجني عليه، فإن المادة ١١٣-٧ من قانون العقوبات تنص على أن: يُطبّق القانون الفرنسي على كلِ جنايةٍ أو جنحة مُعاقبٌ عليها بالسجن، يرتكبها فرنسيٌ أو أجنبيٌ خارج أراضي الجمهورية اذا كانت الضحية تحمل الجنسية الفرنسية وقت ارتكاب الجريمة ". ويمكن أن ينطبق هذا الحكم، على وجه الخصوص، على ضحايا الاستغلال الجنسي من الأطفال الذين ستنشر صورهم على شبكة الانترنت.

وقد تعززت ولاية المحاكم الفرنسية هذه بالمادة ٦٨٩ من قانون الإجراءات الجنائية، التي تسمح للمحاكم الفرنسية أيضًا بمحاكمة مرتكبي الجرائم المرتكبة خارج أراضي الجمهورية عندما تمنح اتفاقية دولية المحاكم الفرنسية الاختصاص للبت في الجرائم المُرتكبة. وفي الحالات التي وُجِهت فيها تهديداتٌ بالقتل من الخارج إلى أشخاصٍ في فرنسا وتم الإبلاغ عنها رقميًا، ترى الدائرة الجنائية أنّ: "مكان ارتكاب الانتهاك هو المكان الذي صدرت فيه التهديدات وليس البُلدان التي أبلغ عنها فيما بعد بواسطة التلفاز أو الصحافة المكتوبة أو الإلكترونية، والتي تُمكِّن الشخص المعني من الاطلاع عليها"[٢] . وفي الحالاتِ المنصوصِ عليها في المادتين ١١٣-٦ و ١١٣-٧ من قانون العقوبات، لا يجوز مُلاحقة مرتكبي الجرائم إلا بناءً على طلب المدعي العام [النيابة العامة] . ويجب ان يسبق الدعوى شكوى من المجني عليه أو أصحاب الحق أو

(1) – (C. pén., art. 113-6, al. 2).
(2) – (Crim. 8 déc. 2009, nos 09-82.135 et 09-82.120 , Bull. crim. no 206).

(ISSN: 2356 - 9492)

بناءً علي اخطارٍ رسميٍ من سلطات الدولة التي ارتكبت بها الواقعة[1]. وعلى الرغم من أحكام الفقرة الثانية من المادة ١١٣-٦ من القانون الجنائي، فإن الجرائم المنصوص عليها في المواد ٢٢٧-٢٢ و٢٢٧-٢٣ و٢٢٧-٢٥ إلى ٢٢٧-٢٧ من نفس القانون التي يرتكبها في الخارج، فرنسيٌ أو شخصٌ يُقيم عادةً في الأراضي الفرنسية، تقع في نطاق القانون الفرنسي دون حاجةٍ إلي إصدارِ لائحةِ اتهامٍ مزدوج ودون قصرِها علي طلب المدُعي العام. وتهدف المادة ٢٢٧-٢٧-١ من قانون العقوبات، على وجه الخصوص، إلى المُعاقبة علي الجرائم التي تنطوي على نشر محتوى غير مشروع "غير قانوني" [كإفساد قاصرٍ أو تسجيل أو نقل صورة إباحية لشخصٍ قاصر أو الاعتداء الجنسي على قاصر] على شبكة الإنترنت ومُكافحتِها.

تأخذ أغلب التشريعات الوضعية بهذا المبدأ، حيث تنص على تطبيق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الدولة صاحبة التشريع. كما أخذ بهذا المبدأ المشرع الفرنسي في المادة ١١٣/٢ من قانون العقوبات الجديد، والتي تنص علي أن: "يُطبّق القانون الفرنسي على الجرائم المرتكبة على إقليم الجمهورية و تُعتبر كذلك إذا كان أحد عناصر الجريمة قد وقع على هذا الإقليم ".

ويعني هذا المبدأ أن قانون العقوبات يُطبّق على أي جريمةٍ تقع داخل القطر الوطني بغض النظر عن جنسية مرتكبيها أو المجني عليه، وينعقد الاختصاص وفقا لهذا المبدأ بتحقق أحد العناصر المكونة للجريمة سلوكًا أو نتيجةً. وعلاوةً علي ذلك، فإنّ هذا المبدأ يسمح بمتابعة كل من ارتكب أحد العناصر المكونة للجريمة ولو كان الفعل غير معاقبًا عليه في بلد المنشأ الأصلي (أي بداية السلوك الإجرامي)، ومن ثم تنقل البيانات والمعلومات بين العديد من الدول

(1) –(C. pr. pén., art. 113-8).

وبمجرد اقتراف احدى سلوكيات الجريمة في القطر الوطني ينعقد الاختصاص للقاضي الوطني، ومن ثم يجب تطبيق قانون العقوبات الوطني. كما يمكن بناءً على هذا المبدأ متابعة الجاني خارج القطر متى كان مُساهمًا أو شريكًا في الجريمة التي وقعت داخل القطر لأن العِبرة بمكان وقوع الجريمة.

غير إن هذا المبدأ يجد صعوبةً كبيرة في تطبيقه بالنسبة للجريمة المعلوماتية وهذا بالنظر لطبيعتها و الخصائص التي تميزها عن الجريمة التقليدية وخصوصًا صعوبة تحديد مكان وقوعها وارتكباها بدقة وكذا زمان حدوثها .[١]

كما أن هذا المبدأ يجد صعوبةً في تطبيقه في قانون العقوبات الفرنسي حيث تنص المادة ٥/١١٣ علي أن:" يُطبّق القانون الفرنسي على كل من ارتكب فعلاً في إقليم الجمهورية يجعله شريكًا في جنايةٍ أو جنحة وقعت بالخارج، إذا كانت الجناية أو الجنحة معاقبًا عليها في القانون الفرنسي والقانون الأجنبي وكانت ثابتة بمقتضى حكم نهائيٍ من القضاء الأجنبي ".

وعليه وبناء على نص المادة أعلاه فإنه لكي يُسأل الشريك يجب توافر ما يلي:[٢]

- أن يكون الفعل مُجرّمًا في البلد المنشأ – الفعل الأصلي –
- أن يصدر حكم الإدانة عن الفاعل الأصلي في البلد المنشأ.

وعليه، فإن تطبيق هذا النص يصطدم بعقبةٍ مادية تتمثل في "صعوبة تحديد مكان وقوع الفعل الأصلي"، لأنه شرطٌ أوليٌ لعقد الاختصاص للقاضي الوطني، لأن ذلك يترتب عليه معرفة ما إذا كان الفعل مُباحًا أو مُجرمًا في ذلك البلد .

[1] Mission interministérielle pour l'accès public à la micro-informatique, à l'internet et au multimédia, *http://www.accespublics.premier-ministre.gouv.fr*
[2] Juriscom.net,http*://www.juriscom.net*

(ISSN: 2356 – 9492)

وأخيرا، يُمكننا القول: أن مبدأ الإقليمية يقوم على أساس مكان وقوع الجريمة أو أحد عناصرها المادية وهذا المبدأ يبدوا أنه غير ملائمٍ للجريمة المعلوماتية، وهذا بالنظر لطبيعتها غير المادية من جهة ومن جهة أخرى لصعوبة اكتشافها وتحديد مكان وزمان وقوعها بدقة.[1]

٢-مبدأ الاختصاص الشخصي:

ولهذا المبدأ وجهان، وجهٌ إيجابي وآخرٌ سلبي ..... وسنحاول توضيح ذلك كما يلي:

• **الوجه الإيجابي:** ويعني تطبيق القانون الجنائي على كل من يحمل جنسية الدولة ولو ارتكب الجريمة خارج إقليمها.* **أما الوجه السلبي:** فيعني تطبيق القانون الجنائي على كل جريمة يكون فيها المجني عليه مُنتميًا لجنسية الدولة ، ولو كان الجاني أجنبيًا ، وارتكب الفعل خارج إقليم الدولة .

غير أن هذا المبدأ وردت عليه قيود بصفةٍ عامة و بالتالي فإن الاختصاص لا ينعقد في المحاكم الوطنية بشكلٍ تلقائي بالنسبة للجرائم التي تقع في الخارج بل يجب علم النيابة العامة بها، كما أنه لا يجوز محاكمة الشخص على نفس الفعل الواحد مرتين وهذه الإجراءات طويلة ومُكلّفَة وتُقيِّد تطبيق مبدأ الاختصاص الشخصي.

والُملاحظ أن هذا المبدأ يعتمد بصفة أساسية على الجاني من حيث الكشف عن هويته ومن ثم التعرف علي جنسيته، وهذه المعلومات تُعد صعبةً وعسيرةً في جرائم الانترنت حيثُ تُستعمل أساليب التشفير، والأسماء المستعارة بالإضافة إلى اللغة الصعبة والمعقدة في كشفها

[1] Forum des droits sur l'Internet *http://www.foruminternet.org*
[1] Agence pour les technologies de l'information et de la communication dans l'administration

والتعامل معها . كما أن محاكمة المجرم الذي يقيم في دولةٍ أجنبية تحتاج إلى إجراءاتٍ طويلة وشاقة ومُعقدة ومُكلفة، وهذا ما يصدق كذلك بالنسبة لتنفيذ الأحكام الصادرة في الخارج.

ويُضاف إلي ذلك أن من مخاطر تطبيق القانون الوطني على الجرائم التي تقع في الخارج والتي يختص بها القانون الأجنبي في ذات الوقت أنه قد يؤدي إلى المساس بمبدأ عدم جواز محاكمة الشخص عن الفعل الواحد أكثر من مرة وهو إحدى المبادئ الأساسية للقانون الجنائي. علاوةً علي ذلك، فاذا لم يكن القانون الوطني مُختصٌ بنظر الواقعة، تثار الإشكالية بالنسبة للمضرور من الجريمة الذي يجب عليه أن ينتقل إلي الدولة التي وقع بها الفعل ليرفع دعواه المدنية. والأخطر من ذلك أن يكون الفعل غير معاقبًا عليه في هذه الدولة. ولذلك نري بأنه يجب أن يكون هناك قانونٌ جنائيٌ دوليٌ على غرار القانون الدولي الخاص ليطبق على جرائم المعلوماتية.

٣-مبدأ الاختصاص العيني:

طبقا لهذا المبدأ يطبق القانون الجنائي الوطني على الجرائم التي ترتكب بالخارج بصرف النظر عن جنسية مرتكبها، ويرجع هذا المبدأ إلى المساس بسيادة الدولة وحقها في الدفاع عن جميع صور الاعتداء على مصالحها الحيوية والأساسية ولو وقعت تلك الجرائم خارج إقليمها.

وعلى هذا الأساس يمكن أن يطبق هذا المبدأ على جرائم المعلوماتية إذا كانت تمس بالسيادة الوطنية ووحدة الدولة أو تعمل على المساس بالمصالح الحيوية ولو ارتكبت من قبل أجانب وخارج إقليم الدولة.

(ISSN: 2356 - 9492)

غير أن هذا المبدأ في الواقع يصادف العديد من الصعوبات ترجع بالأساس إلى طبيعة وخصائص الجريمة المعلوماتية حيث لا تظهر مادياتها بوضوح، كما أن الفاعل يبقى مجهولا بالإضافة إلى تعدد وتنوع الأنظمة القانونية في العالم واختلافها مما يترتب عليه البطء والتعقيد وطول مدة الإجراءات.

٤- مبدأ الاختصاص العالمي:[1]

وفقًا لهذا المبدأ، يُطبّق القانون الجنائي على كل جريمةٍ يُقبضُ على مرتكبها في إقليم الدولة أيًا كان مكان ارتكابها وجنسية الفاعل أو الجاني.

وهذا المبدأ يُعطي لقانون العقوبات مجالاً مُتسِعًا يشمل العالم كله، فلا يتقيد بمكان ارتكاب الجريمة أو أحد سلوكياتها ولا بجنسية مرتكبها ولا بطبيعة الجريمة ومساسها بالسيادة والمصالح الوطنية. وإنما يتطلب فقط القبض على الجاني في إقليم الدولة ليعطي للقانون الجنائي الوطني الاختصاص، وهذا المبدأ يتلاءم كثيرًا وطبيعة الجريمة المعلوماتية رغم ما يطرحه من تنازعٍ حادٍ بين التشريعات الجنائية في مُختلف الدول.

وعليه يمكننا القول، بأهمية هذا المبدأ ومدى ملائمته للجريمة المعلوماتية من ناحية خطورتها من جهة، ومن ناحية طبيعتها من جهةٍ أخرى، كونها سهلة الوقوع من أشخاص يحملون جنسيات مختلفة وتمتد عناصرها المادية وسلوكياتها الإجرامية بين أكثرِ من دولة ، وفي فتراتٍ زمنيةٍ قصيرةٍ جداً، ورُغم ذلك، فإنّ هذا المبدأ– أي العالمية– يبقى عاجزًا عن معالجة جميع القضايا في هذا الشأن ما لم يكن هناك تعاونٌ دوليٌ جادٌ وسريعٌ ،وكذا وجوب إعدادِ

[1] Direction du développement des médias site portail de l'action gouvernemental pour la société de l'information *http://www.internet.gouv.fr*

تشريعاتٍ وطنيةٍ لتجريم الظاهرة ، والتي علي إثرها تُتاح إمكانية معاقبة كل من يتم القبض عليه على إقليم الدولة دون مراعاةٍ لجنسيته أو مكان وقوع الفعل الإجرامي.

– والمُلاحظ أن اغلب التشريعات الوضعية لم تنص على هذا المبدأ بالرغم من أهميته خصوصًا في مجال الجريمة المعلوماتية، ولذلك نرى وجوب النص عليه عند إعداد قانون خاص بمعالجة الجريمة المعلوماتية وجرائم الكمبيوتر والانترنت، هذا بالرغم من أن الاتفاقيات الدولية تُركِّزُ بل وتعول عليه بشكلٍ دائم في هذا المجال ، وبشكلٍ خاص" اتفاقية بودابست الصادرة في عام ٢٠٠١ لمكافحة الجريمة المعلوماتية"، وكذا" القانون العربي النموذجي لمكافحة جرائم تقنية أنظمة المعلوماتية ٢٠٠٣ في مادته السادسة والعشرين".[١]

[1] Conseil de l'Europe *http://www.coe.int*
Ce guide a été réalisé par la Direction des Affaires criminelles et des Grâces
• Sous-Direction de la justice Pénale générale
- Bureau des politiques pénales et de la protection des libertés individuelles :
Madame Myriam Quemener, chef du bureau,
Monsieur Matthieu Bourrette, MACJ,
• Sous-Direction de la justice Pénale spécialisée
Monsieur Gilles Sorba, lieutenant-colonel de gendarmerie, cadre spécialisé (D.A.C.G.) ;
et le service de l'Information et de la Communication du ministère de la Justice (SICOM)
avec la collaboration :
• des Officiers de liaison Intérieur et défense : Madame Lilianne Leymarie, Commissaire divisionnaire et Monsieur le Colonel de gendarmerie Richard Alexandre ;
• du Service des Affaires Européennes et Internationales (SAEI) : Madame Sonya Djemni -Wagner, magistrat en
charge des questions liées aux nouvelles technologies de l'information et de la communication ;
• de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la Communication :
Madame Catherine Chambon, chef de service. Monsieur Daniel Bertinet adjoint au chef de service ;
Monsieur Joël Ferry, Lieutenant-colonel, chargé de mission à (L'OCLCLTIC),
• Institut de Recherches Criminelles de la Gendarmerie Nationale : Capitaine Eric Freyssinet
• du Service Technique de Recherches Judiciaire et de Documentation de la Direction Générale de la Gendarmerie
Nationale : adjudant Toussaint ;
• Monsieur Bruno Nedellec, magistrat détaché au Ministère des Affaires Etrangères ;
• de Madame Nicole Tricart, commissaire Divisionnaire, responsable de la brigade des Mineurs de Paris ;
• de Monsieur Fabrice Gauthier, capitaine de police, Brigade des Mineurs de Paris ;
• de la Direction de la Protection Judiciaire de la Jeunesse.(Bureau K2) ;
• de Monsieur Christian Boucard, Directeur adjoint des Douanes, cadre spécialisé ;
• de Monsieur Rodolphe Uguen, rédacteur au Bureau de la criminalité (D.A.C.G.).

(ISSN: 2356 – 9492)

كما يري الفقه بوجوب الأخذ به على غرار جريمة القرصنة في القانون الدولي الجنائي. ونعتقد أن الجريمة المعلوماتية لا تقل أهميةً عن جريمة القرصنة كونها تُهدِّد امن وسلامة المجتمع الدولي من خلال اهتزاز الثقة في التعامل بالبيانات والمعطيات على الشبكة العنكبوتية مما يهدد الاقتصاد العالمي الذي يشهد وتيرةً متصاعدة وبشكلٍ خاص في المجال المالي والمصرفي، وعليه أصبح من الضروري الاخذ بهذا المبدأ ومعاقبة الجاني في أي إقليمٍ يتم فيه القبض عليه دون مراعاةٍ لجنسيته أو مكان ارتكاب جريمته وذلكَ لارتكابه جريمةً عالمية.

و قد نصت المادة (الخامسة) من قانون المصري الخاص بحماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ علي : " تختص المحاكم الاقتصادية بنظر الجرائم التي ترتكب بالمخالفة لأحكام القانون المرافق" .

كما نصت المادة (١٤)من ذات القانون علي : يحظر إجراء عمليات نقل للبيانات الشخصية التي تم جمعها أو تجهيزها للمعالجة إلي دولة أجنبية أو تخزينها أو مشاركتها إلا بتوافر مستوي من الحماية لا يقل عن المستوي المنصوص عليه في هذا القانون ، وبترخيص أو تصريح من المركز . وتحدد اللائحة التنفيذية لهذا القانون السياسات والمعايير والضوابط والقواعد اللازمة لنقل أو تخزين أو مشاركة أو معالجة أو إتاحة البيانات الشخصية عبر الحدود وحمايتها .

كما نصت مادة (٢٥) من ذات القانون علي : للمركز بالتنسيق مع السلطات المختصة التعاون مع نظرائه بالبلاد الأجنبية وذلك في إطار اتفاقيات التعاون الدولية والإقليمية والثنائية أو بروتوكولات التعاون المصدق عليها أو تطبيقًا لمبدأ المعاملة بالمثل بما من شأنه حماية البيانات الشخصية والتحقق من مدي الامتثال للقانون من قبل المتحكمين والمعالجين خارج الجمهورية ، ويعمل المركز

علي تبادل البيانات والمعلومات بما من شأنه أن يكفل حماية البيانات الشخصية وعدم انتهاكها والمساعدة في التحقيق في الانتهاكات والجرائم ذات الصلة وتتبع مرتكبيها.

(ISSN: 2356 – 9492)

الخاتمة

حماية البيانات هي القوة الكامنة وراء حقنا في الخصوصية ،على الرغم من التطورات الحديثة في تشريعات وممارسات خصوصية البيانات ، فإن خصوصية المستهلك تتعرض بانتظام للغزو أو المساومة من قبل الشركات والحكومات. وقد أدى ذلك بالبعض إلى المجادلة بأن المستهلكين فقدوا بالفعل حرب الخصوصية.

وبعد إستعراض محاور بحثنا ، مؤكدين علي أن خصوصية البيانات الشخصية و حمايتها لا يكفي الحديث عنه في بحث واحد ، لان طرق معالجة البيانات و أساليب جمعها و حمايتها متشعبه و متسعه ، نظراُ لأن كل تفصيله في تلك الممارسات لها أثرها القانوني .

يهدف القانون العام لحماية البيانات في الاتحاد الأوروبي ، الصادر في مايو ٢٠١٨ ، إلى حماية البيانات الشخصية لمواطني الاتحاد الأوروبي ، وله بالفعل تأثيرات كبيرة على الشركات في أوروبا. هناك العديد من جوانب القانون العام لحماية البيانات (GDPR) ، والعديد من المهام التي يتعين على الشركات القيام بها لتحقيق الامتثال للائحة العامة لحماية البيانات والمحافظة عليه. وتشمل على سبيل المثال لا الحصر: موافقة صريحة على الاشتراك من المستخدمين، الحق في طلب البيانات من الشركات، الحق في حذف بياناتك.

يمنح القانون العام لحماية البيانات (GDPR) المستهلكين حقوقًا معينة على بياناتهم بينما يفرض أيضًا التزامات أمنية على الشركات التي تحتفظ ببياناتها. بالنسبة للشركات ، يتمثل أحد جوانب التحدي في التشريع في شرط الاستجابة لطلبات الوصول الموضوعية .الحقيقة هي أن معظم المؤسسات لا يمكنها بسهولة تحديد موقع البيانات الشخصية للفرد أو توفيرها أو حذفها عند الطلب.

يعتمد العديد من مديري المعلومات ومسؤولي خصوصية البيانات على برنامج الامتثال للقانون العام لحماية البيانات (GDPR) الذي يكتشف البيانات الشخصية تلقائيًا ويصنفها من أجل الحفاظ عليها محمية وللمساعدة في تسريع طلبات الوصول إلى موضوع البيانات.

ومنذ صدور قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ و الذي كنا جميعا في انتظار صدوره ، لما نتعرض له جميعا من انتهاكات لخصوصيتنا المعلوماتيه ، واستغلالها ومعالجتها وتحليلها دون رقابة . ويرجع صدور هذا القانون لتحقيق أمرين في غاية الأهمية أولهما : حماية خصوصية الموطن ، و ثانيهما: بعرض الاستثمار في تطور تكنولوجيا المعلومات و مواكبه النظام العام لحماية البيانات الشخصية الصادر من الاتحاد الأوروبي، فمسؤولية أمن بيانات مواطني الاتحاد الاوروبي الذين لديهم الرغبه في الاستثمار داخل جمهورية مصر العربيه أو لمجرد السياحه تقع علي عاتق قانون الدولة المصرية . و من هنا نقول حسناً فعل المشرع المصري لإصدار القانون و لكننا في حاجه ماسه لصدور اللائحة الخاصه به ، حتي يتسني تطبيقه بشكل دقيق و فعال.

التوصيات

أدى الانتشار الكبير للإنترنت في الحياة العملية إلى البحث عن الحلول العملية للمشاكل الناتجة عن استخدام القضاء الإلكتروني في ضوء القواعد العامة للقانون وتوجيه نظر المشرع إلي وضع قواعد خاصة لتنظيم استخدام القضاء الإلكتروني في بعض المجالات الحيوية واستخلاص القواعد الرئيسية في هذا المجال والتي يمكن للمشرع أن يستهدي بها إذا أراد أن ينظم مجال أو اكثر من مجالات استخدام الأنترنت خاصة بالنسبة لتسرب البيانات حيث أن كثير من

(ISSN: 2356 – 9492)

البيانات مكشوفة ولا يتطلب الاستيلاء عليها أساليب معقدة ومجرمو الشبكة العالمية لها بالمرصاد.

فانتشار استخدام كلمات السر في مواقع التعامل الإلكتروني جعل قليلاً من التخمين كافياً لفتح آليات المغلق أمام أجهزة وتخزين البيانات غير المحمية كأصابع USB فهي تفتح المجال أمام نقل المعلومات بسهولة وأيضاً أدي تقارب التقنيات المختلفة إلي مضاعفة التهديدات وجعل أنظمة الحماية لا تقوم بمهمتها علي الوجه المطلوب وعلى ذلك فإن التدخل التشريعي دائماً مطلوباً بقوة في هذه المرحلة بشكل أكبر من أي وقت مضى في ظل سرعة إخلاق دليل إثبات الجريمة ذاتها والتدخل السريع لضبط متعلقات الجريمة وأطرافها وارتباط الجريمة بأنظمة أخرى أو لحقوقه وحرياته الكثيرين أو التفريط بضمانات المتهم وما توجبته قرينة البراءة المقررة له وهذا التناقض لا يمكن فضه إلا بإقامة معيار تعكسه القواعد التشريعية وعدم إلزام أى جهة بتقديم أى بيانات بشأن الخدمات المعقدة للزبائن لأن هذه البيانات سرية ولا يجوز إنشائها إلا وفق القانون والحاجة ماسة إلى التدخل التشريعي لإتاحة آلية للضبط السريع مع الأمر بكف يد المشتبه به عن الاستخدام فوراً بمجرد البدء بإجراءات التفتيش بالإضافة إلى الحق في ضبط الأجهزة لإجراء التفتيش عليها في مقار التحقيق باستخدام التقنيات ، لذا فإننا نوصي :

١- ضرورة إصدار اللائحة الخاصة بقانون حماية البيانات الشخصية في أسرع وقت توطئة لمعالجة إشكاليات التعدي علي الخصوصية وتنفيذ القانون بشكل دقيق وفعال.

٢-الضرورة الملحة لإنشاء مؤسسات رقمية تعليميه وتوجيهيه للمواطنين لتوعيهم بثقافة الأمن المعلوماتي و الخصوصية المعلوماتيه.

٣- عقد دورات لموظفي الحكومه و الشركات لتوعيتهم بشأن إشكاليات تسريب البيانات والمعلومات الموكله لهم بالحفاظ عليها (خاصة البيانات الشخصية الحساسه).

٤- ضرورة ضبط جودة الخدمات المعلومات في العصر لإكتروني : قياس الاجراءات الفنية والخدمات الموجهة للمستفيدين .

٥- ضرورة عقد إتفاقيات في الوطن العربي ، لإنشاء منظمات تعمل علي حث المؤسسات العليمية علي مواكبة تطور الثورة التكنولوجية و المعلوماتيه.

٦- ضرورة إصدار قوانين وتشريعات خاصة بممارسة الإتجار في العملات الرقمية الغير معلومه المصدر و أماكن تعدينها و تحويلها داخل القطر المصري دون رقابه.

- بعض التوصيات الخاصة بالمواطن العادي لحماية بياناته الشخصية

١- لا تفتح رسائل البريد الإلكتروني المشبوهة. إذا تلقيت رسالة بريد إلكتروني يفترض أنها من مؤسسة مالية بها سطر موضوع ينذر بالخطر- مثل "الحساب معلق!" أو "الأموال المعلقة" -احذفها. إذا كنت قلقًا من وجود مشكلة، فقم بتسجيل الدخول إلى حسابك أو اتصل بالبنك مباشرة. إذا كانت هناك مشكلة بالفعل في حسابك المصرفي أو بطاقتك الائتمانية، فستجد المعلومات بمجرد تسجيل الدخول.

٢- لا تنقر على الروابط المشبوهة في رسائل البريد الإلكتروني. إذا فتحت بريدًا إلكترونيًا من شخص لا تعرفه وتم توجيهك للنقر فوق ارتباط، فلا تفعل ذلك. غالبًا ما تنقلك هذه الروابط إلى مواقع ويب مزيفة ستشجعك بعد ذلك إما على تقديم معلومات شخصية أو النقر فوق الروابط التي قد تقوم بتثبيت برامج ضارة على جهاز الكمبيوتر الخاص بك.

(ISSN: 2356 - 9492)

٣- لا ترسل معلومات مالية عبر البريد الإلكتروني. لن يطلب منك البنك أو مزود بطاقتك الائتمانية أبدًا تقديم أرقام الحسابات المصرفية أو رقم الضمان الاجتماعي أو كلمات المرور عبر البريد الإلكتروني.

٤- لا تنقر فوق الإعلانات المنبثقة. يمكن للقراصنة إضافة رسائل احتيالية تنبثق عند زيارة مواقع الويب الشرعية. في كثير من الأحيان، ستحذرك النوافذ المنبثقة من إصابة جهاز الكمبيوتر الخاص بك وتطلب منك الاتصال برقم هاتف أو تثبيت الحماية من الفيروسات. تجنب هذا الإغراء. يستخدم المحتالون هذه الإعلانات إما لتثبيت برامج ضارة على جهاز الكمبيوتر الخاص بك أو خداعك للحصول على دفعة مقابل تنظيف جهاز كمبيوتر لست بحاجة إليه.

٥- اشترك في الحماية من الفيروسات. تأكد من أن جهاز الكمبيوتر الخاص بك محمي ببرنامج أمان قوي متعدد الطبقات.

٦- بالنسبة لمخاطر ال Cookies : لتجنب الاحتيال، من الأهمية أن تحافظ على تحديث متصفحك، حيث تم تصميم العديد من عمليات الاحتيال في ملفات تعريف الارتباط للاستفادة من الثغرات الأمنية في المتصفحات القديمة. من المهم أيضًا أن تتجنب المواقع المشكوك فيها وأن تنتبه إذا حذرك متصفحك من احتمال أن يكون أحد المواقع ضارًا. إذا كانت لديك مخاوف بشأن الخصوصية بشأن ملفات تعريف الارتباط، فاضبط الإعدادات في متصفحك لتصبح أكثر صرامة. من الجيد أيضًا استخدام وضع التصفح الخاص أو التصفح المتخفي، حيث سيسمح لك ذلك بتصفح الإنترنت بدون ملفات تعريف الارتباط المخزنة.

٧- لا تعطي لأي شخص صورة الرقم القومي الخاص بك دون سبب ، وعدم ارسال الرقم القومي عن طريق الرسائل الالكترونية علي أي تطبيق علي الهاتف دون التأكد من هوية المؤسسه أو الشخص المرسل إليه هذا البيانات.

- حفظ الله مصر و مواطنيها .....

(ISSN: 2356 – 9492)

قائمة المراجع

المراجع العربية :

رشاد عبد الله الإنترنت في مصر و العالم العربي ، طذ ، أفاق للنشر و التوزيع ، ٢٠٠٥.

عبد الله علي الشنبري التحولات المعرفيه الكبري منذ العصر الحجري وحتي جوجل ، مدارك للنشر، ٢٠١١.

شمس الدين ابراهيم أحمد وسائل مواجهة الاعتداءات على الحياة الشخصية في مواجهة تقنية المعلومات في القانون السوداني والمصري، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٥

المراجع باللغة الإنجليزية و الفرنسية :

1- ***La vie privée à l'ère de l'information***:Centre de traduction et d'édition Al-Ahram, Le Caire, 1999,

2- ***Lucas, Jean Devese et Jean Freyssinet****:* droit de l'informatique et de l'internet, Presses Universitaires de France, Economies, paris

3-***Fabien Marchadier***: réseaux sociaux sur internet et vie privée, « technique et droit humains », Montchrestien Lex, 2010

4-***Younis Arab***: Le rôle de la protection de la vie privée dans la promotion de l'intégration dans la société numérique, document présenté lors du Symposium du club arabe pour l'éthique de l'information, 17 18 octobre 2002, Amman, Jordanie.

5-***Shade***, L.R. Reconsidering the right to privacy in Canada .Bulletinof science , techonolgy and Society . (2008).

6- ***Larose, R.,& Rifon, N. J. promoting i-Safety***: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior. Journal Of Consumer Affairs

7- ***Martin Hilbert and Priscila Lopez***. The world's Technological Capacity to Store, Communicate, and Computer Information. Especially Supporting online material, Science (Journal)

8- ***Muench,David***, " Wisconsin Community Slogans: Their Use and local Impacts", December 1993 .April 10,2007

9- ***Hunton& Williams LLP***, New Requirements for online Privacy Policie, Basic Books, 2004

10- ***Krishnamurthy B***, Wills CE. On the Leakage of Personally Identifiable Information Via Online Social Networks,, US Press, (2009)

11- ***Shraddha, Peter J.Lyons &Co.***:LEO Computers (2002)

12- ***Roger Clarker's Privacy and Social Media***: An Analytical Framwork, " Data Surveillance and Information Privacy" (2013)

13- ***Jerry Berman & Deirdre Mulligan*** , Privacy in the Dighital age: work in progress, Nova Law Review, volume 23, Number 2, the Internetand Law , (winter 1999)

14- ***Eneken Tikk***, IP,address subject to personal data regulation , out Law, 2013

15-***Lori Andrews***, Social Networks and the Death of Privacy, Free Press, 2011

16-***Anne Blise***, PHD, Technology and Privacy in the new Milliennium, Ethica Publishing , 2004

17- ***Jason Angiulo and Graut Kleinwachter*** Privacy in a Transparent world , Ethica Publishing , 2010

(ISSN: 2356 – 9492)

18- ***Narayanan, A.;Shmatikov ,V. "*** Myths and fallacies of " personally identifiable information", communications (2010)

19- ***Sigmund Freud***, “Three Essays on the Theory of Sexuality” (1905), trans. and ed. James Strachey, *The Standard Edition of the Complete Psychological Works of Sigmund Freud*, vii, 24 vols. (London: Hogarth Press, 1974)

20- ***Blanchette,J.f.& Johnson***, D.G.Data retention and the panoptic society: the social benefits of forgetfulness.

21- ***Deighton, J.A*** The Presentatio of self in the Information age Harvard Business SchoolWorking Knowledge. (2006)

22- ***Roger Clarke***, The suprevisor's Dilemma: Reconcilition possible between , the Candidate's Nedds and the supervisor's Integrity, Sloenia (June2013)

23- ***Saul Hansell***, "Big Web Sites to Track Steps of Their Users" , N.Y. TIMES ABSTRACT , Aug.16,1998, at 1, available in 1998 WL5422846

24- ***Karen Kaplan***, In Giveawayof 10.000 Pcs, the price is Users' Privacy Marketing : Recipients Must agree to Let Pasadena Firm Monitors Where They Go on Internet and What They Buy , L.A. TiMES, (Feb,8,2009), at A1.

25- ***Peng,Weihnong***: Cisna, Jennifer HTTp cookies-" A Prromissing technology" , (2000)

26**-** ***Peneberg,Adam***;CookiesMonsters,Slate , (November 7, 2005)

27- ***Nahla Abdul Qader Al-Momani***, Crimes de l'information, Dar Al-Thaqafa pour l'édition et la distribution, Jordanie, 2008 .

28- ***Saif Abdullah Al-Jabri,*** Sécurité de l'information et protection de la vie privée, Conférence internationale sur la sécurité de l'information électronique, Ensemble pour une interaction numérique sécurisée, tenue les 18 et 20 décembre 2005 à Mascate, Oman.

29- ***V. ,en ce sens , BÉNICHOU***, Cybercriminalité: jouer d'un nouvel espace sans frontière, AJ pénal .2005)

30- ***Did LuzlzSec***, Trick police Into Arresting the wrong Guy? – technology. The Atlantic Wire.2011

See also " protection of Personal data- Justice". Ec.europa.eu.2011-01-18.23/10/2012

31- ***James W.H. McCord and Sandra L. McCord*** , Criminal Law and procedure for the paralegal : a system approach ,supra,2000

32- ***Bygrave L.Data Protection Law***: " Approaching its Rationale, Logic and Limits" coma press (2002)

33- The Data Protection Act 1998 (DPA) is a United Kingdom Act of Parliament which defines UK law on the processing of data on identifiable living people.

Websites:

- http://icsa.cs.up.ac.za/issa/2004/proceedings/full/078.pdf.

Accessed 15 Aug 2019 P.23

- Vincent D. Blondel : Unique in the Crowd: the privacy bounds of human mobility . Nature srep 2013, p 78.

(ISSN: 2356 – 9492)

http://ww.whitehouse.gov/sites/default/files/omb/assets/legislative_reports/fy14_preview_and_joint_committee_reductions_reports_04102013.Pdf

* Le nouveau re'glement sur La protection des donees – Celine castets – Renard- 18/10/2018 Http://actu.dalloz.etudiant.fr/focus-sur

*Https://eur.lex.europa.eu/legal-content/EN/TXT/?uri=CELEx, See also , GUIDE DE SENSIBILISATION AU RGPD, https://www.cnil.fr/professionnel

*https://www.gdprsummary.com/gdpr-definitions/prossing/

*https://www.gdprsummary.com/gdpr-definitions/prossing/

*http://ww.localenterprise.ie/Dublincity/sart-or-Grow-your-Business/Knowlegde-centre/eBusiness/Data

*Report available at https://www.Privacyrigts.org/speeches.testimeny

*http://www.gartner.com/technologhy/supply-chain-professionals.JSP

*Pierre Truche, Jean-Paul Faugère, Patrice Flichy, *Administration électronique et protection des données personnelles – Livre Blanc*, http://www.ladocumentationfrancaise.fr/var/storage/rapportspublics/024000100/0000.pdf,

*The “Do Not Track” standard, developed for browsers by W3C (http://www.w3.org/TR/tracking-dnt/)”, *Numérama*, 11 June 2012, http://www.numerama.com/magazine/22853-donot-track-pourquoi-microsoft-vous-veut-du-bien.html

*John Battelle’s searchblog http://battellemedia.com.

*For example, see http://www.laviedapres.com

*The Commission nationale de l'informatique et des libertés (CNIL) website provides information on case law dating from 2011: http://www.cnil.fr/la-cnil/actu-cnil/article/article/maitriser-les-informations-publiees-sur-les-reseaux-sociaux/, accessed 30 October 2012; Christelle Dardant's article, "Incertitudes autour de la jurisprudence 'Licenciements Facebook'", *Institut de recherche et d'études en droit de l'information et de la communication* (IREDIC), 31 January 2012, http://junon.univ-cezanne.fr/u3iredic/?p=8378, .

*Maslow's hierarchy of needs", *Wikipedia*, http://en.wikipedia.org/wiki/Maslow's_hierarchy_of_needs.

* See the debates on the Loppsi and Hadopi laws, the Edwige file, etc

* See Janna Quitney Anderson, Lee Rainie, "The Future of The Internet", *Pew Internet*, http://www.pewinternet.org/2014/03/11/digital-life-in-2025/,

* Clay Shirky", *Wikipedia*, https://en.wikipedia.org/?title=Clay_Shirky.

*David Price New Study: The Size and Scope of Global Internet Piracy is on the rise (VIDEO) of NetNamws retriveted , http://cretivefuture.org/new-study-the-size-and-scope-of-global-internet-priracy-is-on-the-rise-video/16/6/2014

*What is phishing? How to recognize and avoid phishing scams https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html *https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html

(ISSN: 2356 – 9492)

*The Center For Democracy and Technonlogy 's noop Demonstration att://snoop.cdt.org/ for example of information that can be easily captured by sites on the World Wide Web

*What is phishing? How to recognize and avoid phishing scams, https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html

*What are cookies ?, https://us.norton.com/internetsecurity-privacy-what-are-cookies.html

* Le nouveau re'glement sur La protection des donees – Celine castets – Renard- 18/10/2018

Http://actu.dalloz.etudiant.fr/focus-sur

* Commission nationale de l'informatique et des libertés CNIL *http://www.cnil.fr* , Forum des droits sur l'Internet *http://www.foruminternet.org*

*Agence pour les technologies de l'information et de la communication dans l'administration – ATICA *http://www.atica.pm.gouv.fr* , Direction centrale de la sécurité des systèmes d'information – Secrétariat général de la défense nationale – SCSSI, *http://www.ssi.gouv.fr*

* Mission interministérielle pour l'accès public à la micro-informatique, à l'internet et au multimédia, *http://www.accespublics.premier-ministre.gouv.fr*

Juriscom.net,http://www.juriscom.net*

* Forum des droits sur l'Internet *http://www.foruminternet.org*

*Direction du développement des médias site portail de l'action gouvernemental pour la société de l'information *http://www.internet.gouv.fr*

[*]Conseil de l'Europe *http://www.coe.int*

*مراحل عملية معالجة البيانات في الحاسوب، إيمان الحياري، https://www.mah6at.net/ ١٠ أغسطس ٢٠١٨

* [١] النظام الأوروبي لحماية البيانات العامة GDPR، إيمان الحياري، https://www.mah6at.net/ ٣ يوليو ٢٠١٨

Judgements

*Cour de cassation, chambre criminelle, 16 octobre 2001 Affaire "Marianne" : T.G contre G.B et R.R. Diffamation - délai de prescription des délits de presse . .

*Tribunal de Grande Instance de Paris, ordonnance de référé, 30 octobre 2001 affaire j'Accuse et a. contre l'AFA, Monsieur D et a. contenus illicites - négationnisme-racisme - responsabilité - hébergement étranger – filtrage . . . .

*Tribunal de Grande Instance de Paris (17ème chambre) 12 octobre 2000 Alain B-C Associés-Vienne-Informatique-Internet-hébergeur-Responsabilité (non) Forum de discussion -diffusion de messages -site WEB -valeurs juridiques des règles éthiques - Gaz.Pal 14 au 16 octobre 2001 page 56. S.

*Tribunal de Grande Instance de Paris, ordonnance de référé, 6 février 2001 SA Ciriel contre SA Free Contrefaçon de marques-diffamation-responsabilité de l'hébergeur. Cour de cassation, chambre criminelle, 30 janvier 2001 Madame A.R. contre Monsieur A.B. Diffamation - délai de prescription des délits de presse .

*Tribunal de Grande Instance de Paris, ordonnance de référé, 20 septembre 2000 Sarl One Tel contre SA Multimania Diffamation-

(ISSN: 2356 – 9492)

responsabilité civile -- loi du 1er août 2000 - identification - responsabilité de l’hébergeur (non) .

* Court of justice of the European Union , Press release No.70/14, Luxembourg, 13 May 2014 , judgment in case c-131/12, Google Spain SL, Google Inc. v Agenecia Espanola de Proteccion de Datos , Mario Costeja Gonzalez.