ضوابط التزام مشغلى الإنترنت بتخزين بيانات الاتصال
و الإفصاح عنها لأغراض أمنية
(دراسة مقارنة فى القانون الجنائى)

دكتورة

دعاء محمود سعيد عبد اللطيف

أستاذ القانون الجنائى المساعد

و القائم بعمل رئيس قسم القانون الجنائى

بكلية الحقوق- جامعة الإسكندرية

مـقدمـة

تزامن التطور التكنولوجى غير المسبوق فى وسائل الاتصال بأنواعها، و فى نظم تقنية المعلومات مع ظهور نوعيات جديدة من الجرائم؛ و هى ما عُرفت بجرائم المعلوماتية أو الجرائم الإلكترونية، بالإضافة لاستخدام التكنولوجيا الرقمية فى تيسير ارتكاب الجرائم التقليدية، لا سيما الخطرة منها تلك التى تمس بأمن و استقرار الدول كجرائم أمن الدولة، و الجرائم الإرهابية؛ الأمر الذى حدا بالجهات الأمنية فى مختلف دول العالم إلى إحكام رقابتها على نظم المعلومات، و شبكات التواصل الإلكترونى لضمان حماية مستخدميها من الجرائم التى ترتكب عبرها، و كذا حماية الأمن و النظام العام من خلال استغلال هذه الرقابة فى تسهيل ملاحقة الجناة.

و من ثم صدرت التشريعات المنظمة لتقنيات نظم و شبكات المعلومات مشتملة على نصوص تكرّس هذه الرقابة من خلال وضع التزام قانونى على عاتق مقدمى خدمات تقنية المعلومات (مشغلى الإنترنت) بتخزين البيانات الرقمية للمستخدين لمدة زمنية معينة، و كذا إتاحتها للجهات التى حددها القانون حال طلبها، و ذلك تحت طائلة العقوبات الجنائية.

و قد ورد هذا الالتزام مطلقاً بالنسبة لكافة فئات البيانات بما فى ذلك ما يُعرف ببيانات الاتصال، و بيانات الاتصال بوصفها نوع من البيانات الشخصية بالغة الخصوصية (الحساسية)، فإن تخزينها و إتاحتها للإطلاع يشكلان خطورة بالغة على الحق فى حرمة الحياة الخاصة لمستخدمى شبكات الاتصال الإلكترونى؛ حيث تتضمن بيانات الاتصال علاوة على البيانات المحددة لهوية المستخدم؛ (كرقم الهاتف، و رقم بطاقة (sim)، و عنوان البريد الإلكترونى، و كذا (Ip) الخاص بالجهاز على الشبكة، و بيانات الحسابات البنكية و المدفوعات)، بيانات المرور و الموقع أيضاً، و هى البيانات التى تسمح بتحديد الوسيط الرقمى المتصل، و متلقى الاتصال، و قائمة الاتصالات، و مدة المكالمات، و الأجهزة المستخدمة، و تاريخ الإرسال و الاستقبال، و قائمة عناوين (ip) التى تم الرجوع إليها من عنوان ما، و قائمة الصفحات و المواقع التى تمت زيارتها على الشبكة؛ كما تسمح بتحديد مناطق الإرسال، و الاستقبال للاتصالات و تحديد الجهاز المتصل بواسطة برج الاتصالات التابع له.

و فى ظل ما توافقت عليه المواثيق الدولية و الدساتير الوطنية من حق الإنسان فى حرمة حياته الخاصة، و ما تضمنته-مؤخراً- التشريعات المنظمة لمعالجة البيانات من حق كل شخص فى خصوصية بياناته الشخصية، و الحقوق المتفرعة عن ذلك كحقه فى تأمين بياناته، و تصحيحها، و الاعتراض على معالجتها، بل و حقه فى محوها كليةً كأحد تطبيقات الحق فى النسيان الرقمى؛ أضحى إلزام مشغلى الإنترنت بتخزين، و

إتاحة البيانات الشخصية الرقمية الخاصة بالمستخدمين؛ لاسيما بيانات الاتصال يشكل مساساً واضحاً بحقهم فى الخصوصية و حرمة الحياة الخاصة ما أدى إلى تزايد الأصوات الفقهية الرافضة لفرض هذا الالتزام على إطلاقه، كما وصل السجال إلى المحاكم الأوروبية، التى تدخلت بدورها للنظر فى مدى مساس الالتزام بتخزين البيانات و الإفصاح عنها بحرمة الحياة الخاصة، و بالتالى مدى خروجه عن إطار المشروعية الإجرائية الذى سبق و رسمته المعاهدات الدولية، و التوجيهات الأوروبية و الدساتير و التشريعات الوطنية.

و إذا كانت هذه الإشكالية قد ثارت و بقوة مؤخراً فى القضاء الأوروبى بوجه عام و الفرنسى بوجه خاص، فإنها و لا مناص توشك أن تغدو محل جدل أيضاً فى الواقع القانونى المصرى بعد صدور قانون مكافحة جرائم تقنية المعلومات فى 2018 و الذى حوى بدوره هذا الالتزام، و من بعده قانون حماية البيانات الصادر عام 2020.

لذا ارتأينا أنه من الملائم طرح هذه الإشكالية على طاولة البحث، لتمحيصها على مختلف وجوهها، مقارنين بين القانونين المصرى و الفرنسى فى إطار إلزام مشغلى الإنترنت بتخزين بيانات الاتصال و إتاحتها، فى محاولة لإيجاد إجابات شافية على التساؤلات الآتية:

- من هم مشغلو الإنترنت الذين يقع على عاتقهم الالتزام بتخزين البيانات الشخصية و الإفصاح عنها؟
- ما مضمون و نطاق هذا الالتزام؟
- ما هى بيانات الاتصال، و ما مدى خطورة الكشف عنها؟
- هل يشكل الالتزام بتخزين، و إتاحة بيانات الاتصال انتهاكاً للمبادىء الدولية، و الدستورية فى مجال تكريس الحق فى حرمة الحياة الخاصة، و خصوصية البيانات الشخصية؟
- ما هى الجهات صاحبة الحق فى الاطلاع على بيانات الاتصال، و ما نوع الحالات التى يُصرّح فيها بذلك؟
- إلى أى مدى نجحت الجهود الفقهية، و الاجتهادات القضائية فى رسم إطار أكثر تحديدا لالتزام المشغل بتخزين بيانات الاتصال، و الإفصاح عنها؟
- ما هى الجزاءات الجنائية المترتبة على مخالفة الالتزام بتخزين البيانات الشخصية من ناحية، و الالتزام بإتاحتها للجهات المختصة من ناحية أخرى؟
- و أخيراً هل يحتاج المشرع لإعادة النظر فى صياغة الالتزام بالتخزين، و الإفصاح بصورة تضمن تحقيق التوازن بين الحق فى حرمة الحياة الخاصة، و الضرورات الجنائية و الأمنية لملاحقة الجناة؟

و عليه فقد قسمنا هذه الدراسة إلى مبحثين رئيسين، تناولنا فى أولهما التزام مشغلى الإنترنت بتخزين بيانات الاتصال، و فى الثانى التزام مشغلى الإنترنت بإتاحة بيانات الاتصال للجهات المختصة؛ و قد رأينا ضرورة التعرض للمبادىء العامة فى مجال معالجة البيانات لا سيما الحق فى خصوصية البيانات، و الحق فى النسيان الرقمى بالنظر لكون الالتزام بالتخزين و الإفصاح (الإتاحة) إنما يمثل استثناءً على كليهما، لذا فقد قدمنا لهذين المبحثين بمطلب تمهيدى استعرضنا فيه بكثير من الإيجاز ماهية الحق فى خصوصية البيانات كأحد تطبيقات الحق فى حرمة الحياة الخاصة، و علاقته بالمبادىء الحاكمة لمشروعية معالجة البيانات، بالإضافة للتعريف بالحق فى النسيان الرقمى و أهم أدواته.

مطلب تمهيدى

ماهية الحق فى خصوصية البيانات و النسيان الرقمى

لئِن كانت مبادىء كخصوصية البيانات الشخصية، و الحق فى النسيان الرقمى قد غدت من المبادىء المستقر عليها حالياً كمبادىء حاكمة لمشروعية معالجة البيانات، فإن التزام مشغلى الإنترنت بحفظ بيانات الاتصال، و الإفصاح عنها للسلطات المختصة إنما يُعد استثناءً صارخاً على هذه المبادىء؛ و لمعرفة وجه الاستثناء فى هذا الإلزام التشريعى و تحديد ملامحه، فإنه يلزمنا أولاً أن نعرض بإيجاز لمقتضى هذه المبادىء التى رسختها الاتفاقيات الدولية و التشريعات الداخلية و ذلك فى مبحثٍ تمهيدى نقسمه إلى ثلاثة مطالب، نعرض فى أولها لمفهوم و أساس الحق فى خصوصية البيانات، و فى الثانى لمفهوم معالجة البيانات و المبادىء العامة الحاكمة لمشروعية المعالجة، و أخيراً نعرض لمفهوم الحق فى النسيان الرقمى و مدى تفرده عن غيره من الحقوق المتصلة بالبيانات فى مطلب ثالث.

الفرع الأول

ماهية الحق فى خصوصية البيانات و تكريسه تشريعياً

نتناول فى إطار هذا الفرع ماهية الحق فى خصوصية البيانات و نشأته فى غصنٍ أول، ثم التكريس التشريعى له فى غصنٍ ثانى.

الغصن الأول

مفهوم الحق فى خصوصية البيانات و نشأته

مع التطور الرقمى و اقتحام شبكات الاتصالات للحياة اليومية للناس، لاسيما شبكة الإنترنت بما تحويه حاليا من مختلف منصات التواصل الاجتماعى، و التى يتطلب التواجد عليها و التفاعل اليومى فى فضائها الإدلاء بالعديد من البيانات الشخصية بالتدوين أو بالتدوين و النشر ما أدى إلى تدفق هائل للبيانات، يضاف إلى ذلك ما و فره الاستخدام الدائم لأجهزة الاتصال بأنواعها من إمكانيات لرصد بيانات أخرى كموقع المستخدم، ووقت الدخول على الشبكات، و المواقع التى تم تصفحها و ما إلى ذلك من بيانات، كل هذا أدى إلى ظهور مفهوم جديد للخصوصية يتصل بالبيانات الرقمية.

لاشك إذن أن الحق فى خصوصية البيانات هو حق متفرع عن حق أشمل و أعم هو الحق فى الخصوصية أو الحق فى حرمة الحياة الخاصة، و هو حق من الحقوق اللصيقة بالشخصية.

و يعرّف الحق فى الحياة الخاصة بأنه: " حق الإنسان فى أن يُترك و شأنه بعيداً عن تطفل الآخرين بحيث يكون له القدرة على إبعاد الغير و الحق فى أن يُترك هادئاً"[1] أو "حق الإنسان فى قيادة ذاته فى الكون المحيط به"، أو "الحق فى الحياة الأسرية و الشخصية و الداخلية و الروحية للفرد عندما يعيش وراء بابه المغلق".[2] أو هو" الحق فى أن يخلو الإنسان إلى نفسه و أن يعيش بعيداً عن أعين الرقباء دون تدخل الغير".[3] كما عرفه البعض بصورة أكثر تفصيلاً بكونه: " حق الشخص فى أن يحدد كيفية معيشته كما يروق و يحلو له و ذلك مع أقل قدر ممكن من تدخل الغير فى حياته، فلكل شخص الحق فى المحافظة على سرية خصوصيات حياته، و عدم جعلها عرضة لأن تلوكها ألسنة الناس، أو أن تكون موضوعاً لصفحات الجرائد."[4]

و وفقاً لما ذهب إليه مؤتمر القانونيين لدول الشمال في ستوكهولم المنعقد في مايو 1967فإن الحق فى الخصوصية هو "حق الفرد في أن يعيش حياته بمنأى عن الأفعال الآتية :التدخل في حياته الأسرية أو المنزلية، والتدخل في كيانه البدني أو العقلي، أو حريته الأخلاقية أو العقلية، والاعتداء على شرفه أو سمعته، ووضعه تحت الأضواء الكاشفة، وإذاعة وقائع تتصل بحياته الخاصة، واستعمال اسمه أو صورته، والتجسس والتلصص والملاحظة ، والتدخل في المراسلات سواء تم ذلك عن طريق استخدام وسائل الاتصال الخاصة المكتوبة أو الشفوية، وكذلك إفشاء المعلومات المتحصلة بحكم الثقة والمهنة."[5]

و بعبارات أخرى فإن الحق فى الحياة الخاصة هو التسليم بحق الأفراد فى التمتع بفسحة للتنمية الذاتية أو مجال خاص يحقق لهم حرية التفاعل أو عدم التفاعل مع الآخرين دون الخضوع لتدخل الدولة و لا لتدخل الآخرين.[6]

و تكاد تُجمع كافة التعريفات، و الاجتهادات السابقة على أن الحق فى الحياة الخاصة أو الحق فى الخصوصية إنما يشتمل على عنصرين أساسيين:

---

[1]- تعريف الفقيه الفرنسى كاربونيه، راجع د.إبراهيم داوود، الحماية القانونية للبيانات الشخصية من منظور الحق فى الخصوصية- دراسة تحليلية مقارنة، بحث منشور فى مجلة كلية الحقوق- جامعة الإسكندرية 2017 عدد 1 ص 343

[2]- تعريف الفقيه Martin انظر د.ياسر محمد اللمعى، السياسة الجنائية المعاصرة فى حماية خصوصية البيانات الشخصية الإلكترونية- دراسة تحليلية مقارنة، بحث منشور فى مجلة روح القوانين- مجلة كلية الحقوق، جامعة طنطا، ص19

[3]- د.حسام الدين الأهوانى، حماية الحق فى الخصوصية فى ظل قانون دولة الإمارات العربية المتحدة، بحث منشور فى مجلة الأمن و القانون، 2008، عدد 2، مجلد 16، ص7

4- د.رمضان أبو السعود، النظرية العامة للحق، دار الجامعة الجديدية للنشر، 2005، ص379

5- د.ياسر محمد اللمعى، السياسة الجنائية المعاصرة فى حماية خصوصية البيانات الشخصية الإلكترونية- دراسة تحليلية مقارنة، بحث منشور فى مجلة روح القوانين- مجلة كلية الحقوق، جامعة طنطا، ص 21

[6]- الإنترنت و القانون فى مصر، "الجزء الثالث- الخصوصية الرقمية"، وحدة الأبحاث بمؤسسة الفكر و التعبير، مقال منشور على الانترنت، ص5

1. الحفاظ على سرية الشئون الخاصة للإنسان، و من أهمها كل ما يتعلق بأموره العائلية، و حالته الصحية و معتقداته السياسية و ذمته المالية، و اتصالاته و مراسلاته و صوره.
2. منع الغير من التدخل بالتجسس أو النشر أو بأى صورة كانت فى الشئون الخاصة للإنسان بغير موافقة منه.

و من الحق فى الخصوصية بوجهه العام ينبثق الحق فى خصوصية البيانات كتطبيق مرتبط بالعصر الرقمى بما أسداه للبشرية من زخم فى البيانات من كل نوع، و سهولة جمة فى الوصول إليها و تبادلها و نشرها.

و عليه يمكن القول أن الحق فى خصوصية البيانات هو حق الأفراد فى سرية بياناتهم الشخصية و التحكم أو السيطرة عليها بتقرير من يمكنه الإطلاع عليها، و كيف و متى و إلى أى مدى، و هو ما يقتضى حظر إفشاء هذه البيانات لأية جهة و لو كانت سلطة عامة خارج إطار القيود القانونية.

الغصن الثانى

مراحل التكريس التشريعى للحق فى خصوصية البيانات

يستمد الحق فى خصوصية البيانات مصدره التشريعى من نصوص المواثيق الدولية، و التشريعات الوطنية التى كرست الحق فى الحياة الخاصة ابتداءً، و من ثم تلك التى تعرضت لخصوصية البيانات لاحقاً.

أولاً: التكريس التشريعى للحق فى الحياة الخاصة:

نصت المادة (17) من العهد الدولى للحقوق المدنية و السياسية على أنه: "1. لا يجوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته. 2. من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس."

كما نصت المادة الثامنة من الاتفاقية الأوروبية لحقوق الإنسان، و الحريات الأساسية على أنه:"1- لكل إنسان حق احترام حياته الخاصة، والعائلية، ومسكنه، ومراسلاته. 2-لا يجوز للسلطة العامة أن تتعرض لممارسة هذا الحق إلا وفقاً للقانون وبما تمليه الضرورة في مجتمع ديمقراطي لصالح الأمن القومي وسلامة الجمهور أو الرخاء الاقتصادي للمجتمع، أو حفظ النظام ومنع الجريمة، أو حماية الصحة العامة والآداب، أو حماية حقوق الآخرين وحرياتهم".

و هو نفس ما تبناه الدستور المصرى فى المادة (57) منه حيث جرى على أن: "للحياة الخاصة حرمة، وهى مصونة لا تمس. وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائى مسبب، ولمدة محددة، وفى الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين فى استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفى، وينظم القانون ذلك."

و قد عبّرت المحكمة الدستورية العليا عن الحق فى حرمة الحياة الخاصة فى قضاءٍ سابق لها بقولها أنه: "ثمة مناطق من الحياة الخاصة لكل فرد تمثل أغواراً لايجوز النفاذ إليها، وينبغى دوماً وإعتباره مشروعاً ألا يقتحمها أحد ضماناً لسريتها وصوناً لحرمتها، ودفعاً لمحاولة التلصص عليها أو اختلاس بعض جوانبها، وبوجه خاص من خلال الوسائل العلمية الحديثة التى بلغ تطورها حداً مذهلاً وكان لتنامى قدراتها على الاختراق أثراً بعيداً على الناس جميعهم حتى فى أدق شئونهم ، بل وببيانتهم الشخصية التى غدا الاطلاع عليها وتجميعها نهباً لأعينها ولآذانها، وكثيراً ما ألحق النفاذ إليها الحرج أو الضرر بأصحابها وهذه المناطق من خواص الحياة ودخائلها ، تصون مصلحتين قد تبدوان منفصلتين إلا أنهما تتكاملان ذلك أنهما تتعلقان بوجه عام بنطاق المسائل الشخصية التى ينبغى كتمانها ، وكذلك نطاق استقلال كل فرد ببعض قراراته الهامة التى تكون بالنظر إلى خصائصها وآثارها أكثر اتصالاً بمصيره وتأثيراً فى أوضاع الحياة التى اختار أنماطها، وتبلور هذه المناطق جميعها التى يلوذ الفرد بها مطمئناً لحرمتها يهجع إليها بعيداً عن أشكال الرقابة وأدواتها الحق فى أن تكون للحياة الخاصة تخومها بما يرعى الروابط الحميمية فى نطاقها، ولئن كانت بعض الوثائق الدستورية لا تقرر هذا الحق بنص صريح فيها إلا أن البعض يعتبره من أشمل الحقوق، وأوسعها وهو كذلك أعمقها اتصالاً بالقيم التى تدعو إليها الأمم المتحضرة."[1]

و أكدت نصوص القانون الجنائى توفير الحماية اللازمة للحق فى الحياة الخاصة من خلال تجريم كل تعدى يقع عليه و ذلك بالمواد 309 مكرر و المادة 309 مكرر(أ) حيث جاء فيهما: "يعاقب بالحبس مدة لا تزيد على سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجنى عليه:
(أ) استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه محادثات جرت في مكان خاص أو عن طريق التليفون.

[1]- حكم الدستورية العليا 23 لسنة 16 قضائية- المحكمة الدستورية العليا، مكتبة حقوق الإنسان- جامعة منيسوتا، http://hrlibrary.umn.edu/arabic/Egypt-SCC-SC/Egypt-SCC-23-Y16.html

(ب) التقط أو نقل بجهاز من الأجهزة أياً كان نوعه صورة شخص في مكان خاص.
فإذا صدرت الأفعال المشار إليها في الفقرتين السابقتين أثناء اجتماع على مسمع أو مرأى من الحاضرين في ذلك الاجتماع، فإن رضاء هؤلاء يكون مفترضاً.
ويعاقب بالحبس الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتماداً على سلطة وظيفته.ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة، كما تحكم بمحو التسجيلات المتحصلة عنها أو إعدامها.

و كذا: "يعاقب بالحبس كل من أذاع أو سهل إذاعة أو استعمل ولو في غير علانية تسجيلاً أو مستنداً متحصلاً عليه بإحدى الطرق المبينة بالمادة السابقة أو كان بغير رضاء صاحب الشأن.

ويعاقب بالسجن مدة لا تزيد على خمس سنوات كل من هدد بإفشاء أمر من الأمور التي تم التحصل عليها بإحدى الطرق المشار إليها لحمل شخص على القيام بعمل أو الامتناع عنه.

ويعاقب بالسجن الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتماداً على سلطة وظيفته، ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة أو تحصل عنها، كما يحكم بمحو التسجيلات المتحصلة عن الجريمة أو إعدامها".

المشرع الفرنسى بدوره عاقب على كل الأفعال الماسة بحرمة الحياة الخاصة من خلال المواد 226-1 و226-2 منه.[1]

1 - Art.226-1: “Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :
1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;
2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.
3° En captant, enregistrant ou transmettant, par quelque moyen que ce soit, la localisation en temps réel ou en différé d'une personne sans le consentement de celle-ci.
=Lorsque les actes mentionnés aux 1° et 2° du présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé.
Lorsque les actes mentionnés au présent article ont été accomplis sur la personne d'un mineur, le consentement doit émaner des titulaires de l'autorité parentale.
Lorsque les faits sont commis par le conjoint ou le concubin de la victime ou le partenaire lié à la victime par un pacte civil de solidarité, les peines sont portées à deux ans d'emprisonnement =et à 60 000 euros d'amende. » Art.226-2 : « Est puni des mêmes peines le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou

ثانياً: التكريس التشريعى للحق فى خصوصية البيانات:

ربما كانت الريادة فى مجال تقنين حماية البيانات الشخصية من نصيب المشرع الفرنسى الذى بادر بإصدار القانون رقم 78 -17 لعام 1978 المتعلق بالمعلوماتية و الحريات[1]، و المعدل بالقانون رقم 801 لعام 2004 الخاص بحماية البيانات الشخصية[2] و الذى عُدِل بدوره بالقانون رقم 493 الصادر فى 20 يونيه 2018.[3]

و قد نص قانون 78-17 لعام 1978 فى مادته الرابعة على ضرورة معالجة البيانات الشخصية بطريقة قانونية وعادلة وشفافة، و أن يتم جمعها لأغراض محددة وصريحة ومشروعة، ولا تتم معالجتها لاحقًا بطريقة لا تتوافق مع هذه الأغراض؛ كما أكدت المادة المذكورة على لزوم اتخاذ جميع التدابير المعقولة لضمان مسح أو تصحيح البيانات الشخصية غير الدقيقة، مع مراعاة عدم الاحتفاظ بالبيانات لمدة تُجاوز المدة اللازمة للأغراض التي تتم معالجتها من أجلها.[4]

---

d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes prévus par l'article 226-1.
Lorsque le délit prévu par l'alinéa précédent est commis par la voie de la presse écrite ou audiovisuelle, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables. »

[1] - Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, voir : https://www.cnil.fr/fr/la-loi-informatique-et-libertes#article5

[2] - Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, voir : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000441676

[3] - LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, voir : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952

[4]- Art.4 de La loi Informatique et Libertés dit que : « Les données à caractère personnel doivent
être -Traitées de manière licite, loyale et, pour les traitements relevant du titre II, transparente au regard de la personne concernée ; -Collectées pour des finalités déterminées, explicites et =légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités……Conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées…. »

كما أصدر المشرع الفرنسى قانون الثقة فى الاقتصاد الرقمى رقم 575 لعام 2004 و الذى تضمن عدداً من النصوص التى تكفل تأمين، و سرية البيانات على شبكة الانترنت.[1]

بالإضافة لذلك فقد حوى قانون البريد و الاتصالات الإليكترونية فى القسم الثالث منه (المادة 34 الفقرات من 1 إلى 6) عدداً من الضمانات المتعلقة بسرية البيانات، و بتحديد مدد الاحتفاظ بها و التى ألزم بها مشغلى شبكات الاتصال.[2]

و على المستوى الأوروبى فقد أصدر المجلس الأوروبى الاتفاقية رقم 108 المتعلقة بحماية الأشخاص فى مواجهة المعالجة الآلية للمعطيات ذات الطابع الشخصى الموقعة بتاريخ 28 يناير 1981[3] و من بعدها التوجيه الصادر عن البرلمان الأوروبى CE/46/95 بتاريخ 24 أكتوبر 1995.[4]

و مع التطورات المتسارعة للعالم الرقمى، و ما أسفرت عنه من ظهور العديد من التطبيقات و الخدمات الرقمية على شبكة الانترنت، و ما صحب ذلك من تأثيرات جمة على سهولة نقل و تبادل البيانات، بل و الإدراك المتزايد لما أضحت تمثله البيانات من ثروة حقيقية تتسابق الشركات و الأفراد للحصول عليها أصبح من اللازم تطوير التشريعات الحامية للبيانات بما يلائم هذا التطور الفنى، و هو ما دعا البرلمان الأوروبى مؤخراً لإصدار النظام أو اللائحة رقم 2016/679 المتعلقة بحماية البيانات الشخصية، و المسماه اختصاراً ب"RGPD" و التى دخلت حيز النفاذ فى23 مايو 2018 مُلغية ما تضمنه التوجيه السابق عليها و الصادر فى 1995[5]

و لم يفت المشرع المصرى بدوره أن يكرس نصوصا خاصة لحماية خصوصية البيانات حيث تعرض لتجريم بعض صور انتهاك خصوصية البيانات فى قانون مكافحة جرائم تقنية المعلومات رقم 175 لعام 2018 فى المادة 25 منه، و ذلك بعد أن

---

[1]- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie, (**TITRE III : DE LA SÉCURITÉ DANS L'ÉCONOMIE NUMÉRIQUE (Articles 29 à 46)**

[2]- https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043887545

[3]- محمد حمزة بن عزة، الحق فى النسيان الرقمى، دراسة مقارنة، بحث منشور فى مجلة القانون و الأعمال، جامعة الحسن الأول- كلية العلوم القانونية و الاقتصادية و الاجتماعية- 2021-عدد 68، ص113

[4]- Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, voir : https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A31995L0046%3AFR%3AHTML

[5] - Le règlement général sur la protection des données RGPD,https://www.cnil.fr/fr/reglement-europeen-protection-donnees

أكد فى المادة الثانية منه على ما يقع على عاتق مشغلى خدمات الإنترنت من التزامات بحفظ سرية البيانات، و حظر الإفصاح عنها إلا بأمر مسبب من الجهات القضائية المختصة.

ثم أفرد المشرع المصرى مؤخراً تشريعاً خاصاً ينظم المبادىء و الأطر العامة لمعالجة البيانات، و ذلك بالقانون رقم 151 لعام 2020 المتعلق بحماية البيانات الشخصية.

الفرع الثانى

مفهوم معالجة البيانات و ضوابط مشروعيتها

نعرض فى هذا الفرع لمفهوم المعالجة التقنية للبيانات الشخصية، و من ثم لفئات البيانات الشخصية التى يمكن إخضاعها للمعالجة و ذلك فى غصنٍ أول، و نتلوه بغصنٍ ثانٍ نوجز فيه أهم الضوابط الحاكمة لمشروعية معالجة البيانات بنوعيها الإجرائية و الموضوعية.

الغصن الأول

مفهوم معالجة البيانات

تُعرّف عملية معالجة البيانات و فقاً للمادة الثانية من القانون الفرنسى لحماية البيانات 17-78 المعدل بقانون 801 الصادر فى 6 أغسطس 2004 بكونها: " أي عملية أو مجموعة من العمليات المتعلقة بالبيانات الشخصية مهما كانت العملية المستخدمة، وعلى وجه الخصوص عمليات الجمع أو التسجيل أو التنظيم، أو الحفظ أو التعديل أو الاستخراج أو الفحص أو الاستخدام أو الإفصاح عن طريق النقل أو النشر أو أي شكل آخر للإتاحة أو التوفيق أو الربط البيني، وكذلك الحجب أو المحو أو التدمير."[1]، و بصياغة قريبة من ذلك عرفها الاتحاد الأوروبى فى المادة (2) فى التوجيه 108 الخاص بحماية الأشخاص فى مواجهة معالجة البيانات بكونها: " تشمل أي عملية أو مجموعة عمليات تتم على البيانات الشخصية، مثل جمع أو تسجيل أو تخزين أو تعديل أو استخراج أو نقل أو إتاحة أو محو أو تدمير البيانات الشخصية أو تطبيق العمليات المنطقية أو الحسابية عليها."[2]

[1] -https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000006528061/2004-08-07

[2] - Guide sur la jurisprudence de la Convention européenne des droits de l'homme, Protection des données, Mis à jour le Mis à jour le 31 août 2022, p.9

كما عرفها مؤخراً القانون المصرى لحماية البيانات الشخصية 151 لعام 2020 فى المادة الأولى منه 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 جزئيا أو كليا".

إذن كل تعامل مع البيانات الشخصية للغير سواء بصورة يدوية أو إلكترونية هو معالجة للبيانات، مما يعنى أن مفهوم المعالجة هو مفهوم شامل لكل ما يمكن أن يجرى على البيانات الشخصية من عمليات.

و هو ما يقودنا إلى ضرورة تحديد نطاق ما يسمى بالبيانات الشخصية التى هى دون غيرها محل حماية القانون. و بالرجوع للقانون الفرنسى لحماية البيانات نجد أنه عرفها بكونها:" كل معلومة تتعلق بشخص طبيعى محدد الهوية أو يمكن تحديد هويته بشكل مباشر أو غير مباشر سواء تم ذلك من خلال رقم بطاقة هويته أو أى عنصر آخر خاص به؛ أما إذا كان الشخص قابلا للتحديد، فيجب النظر في جميع الوسائل التي من خلالها يمكن التوصل لتحديد هويته سواء كان ذلك من قبل مسئول المعالجة أو أي شخص آخر."[1]

و عليه فإن المشرع الفرنسى قد تبنى نطاقاً واسعاً لمفهوم البيانات الشخصية، بحث اعتبر أن أى معلومة تتعلق بشخص طبيعى هى بيان شخصى ما دام هذا الشخص الطبيعى محدد الهوية أو يمكن تحديد هويته بطريق مباشر أو غير مباشر.[2]

و بصيغة مقاربة جاء فى التوجيه الأوروبى رقم CE/46/95 فى مادته الثانية أن البيانات الشخصية هى:" كل معلومة تتعلق بشخص طبيعى محدد الهوية أو يمكن تحديد هويته بشكل مباشر أو غير مباشر لا سيما بالرجوع إلى رقمه الشخصى أو واحد أو

[1] - Art:2 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés qui dit : « …Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne… »

[2]- و قد كان مفهوم البيانات الشخصية أضيق من ذلك قبل التعديل الذى جرى على التعريف بقانون 801-2004، حيث لم يكن يتضمن الشخص القابل للتحديد، راجع فى ماهية البيانات الشخصية: د.ياسر اللمعى، المرجع السابق، ص 26؛ د.طارق راشد، الحماية القانونية لخصوصية البيانات الشخصية فى القانون القطرى و المقارن، المجلة القانونية و القضائية، 2017، العدد2، ص 87 (13)

أكثر من العناصر الخاصة بتحديد هويته المادية أو الفسيولوجية أو النفسية أو الاقتصادية أو الاجتماعية."[1]

و على ضوء ذلك يمكن تقسيم البيانات الشخصية إلى أربعة أصناف على نحو ما يلى:

1- بيانات التعريف المباشر:

و هى البيانات التى تعرف عن هوية الشخص بسهولة و تتضمن البيانات الاسمية للشخص (اسمه و لقبه و اسم العائلة، و اسم الشهرة)، و كذلك صورته (ثابته أو متحركة) و صوته.

2- بيانات التعريف غير المباشر:

و هى البيانات التى قد تسمح بصعوبة -تزيد أو تقل- بتحديد هوية الشخص، و فى الغالب هى لا تسمح بذاتها بالكشف عن هويته، و إنما من خلال ارتباطها بغيرها من البيانات فى سياق معين[2]

و تتضمن هذه الفئة مختلف الأرقام و العناوين المتصلة بالشخص، كرقم الهوية، و رقم الهاتف، و أرقام رخصة القيادة أو لوحة السيارة، و كذا أرقام الحسابات البنكية. بالإضافة إلى العنوان الجغرافى للشخص أو محل إقامته، و عنوان بريده الإلكترونى، و أخيراً عنوان برتوكول الانترنت أو (IP) رقم التعريف المخصص لجهاز الحاسب الآلى أثناء التصفح على شبكة الانترنت، و الذى يسمح بتحديد موقع الجهاز الذى يتم الاتصال بالشبكة من خلاله.

3- البيانات الحساسة:

هى فئة من البيانات غير المتفق على تحديدها بصورة حاسمة، و لذا قد تتباين مشتملاتها من تشريع لآخر، ووفقاً للقانون المصرى فالبيانات الحساسة هى: " البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية، أو بيانات القياسات الحيوية (البيومترية) أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الحالة الأمنية، وفي جميع الأحوال تعد بيانات الأطفال من البيانات الشخصية الحساسة."

و عليه فإن هذه الفئة تتضمن أولاً: البيانات البيومترية للانسان كمواصفاته الشكلية، و بصماته (بصمة الإصبع- الكف- العين -الصوت- الحمض النووى- بصمة التوقيع)

---

[1]- د.سليم محمد سليم، الحماية الجنائية للبيانات الشخصية المعالجة آلياً دراسة مقارنة، مجلة العلوم القانونية و الاقتصادية، كلية الحقوق، جامعة عين شمس، 2020-عدد 62، ص 10.

[2]- راجع بتوسع: د.سليم محمد سليم، الحماية الجنائية للبيانات الشخصية المعالجة آلياً، المرجع السابق، ص 18

بالإضافة إلى البيانات المتصلة بأصوله العرقية و الإثنية، و حالته الصحية، و كذا بياناته المالية، و معتقداته الدينية و آراءه السياسية، و أخيراً سجله الجنائى. كما أن البيانات الشخصية للأطفال جميعها تعد من البيانات الحساسة.

و يلاحظ هنا أنه وفقاً للاتحاد الأوروبى تضاف فئة البيانات المتعلقة بالانتماء النقابى، و بالحياة الجنسية كصنف من أصناف البيانات الحساسة.

4- البيانات الوصفية (بيانات الاتصال و بيانات المحتوى):

و هى البيانات التى تصف سلوك المستخدم على الشبكة الإلكترونية، و تضم هذه الفئة كافة ما يجريه المستخدم على شبكة المعلومات الدولية من تصرفات منذ ولوجه و حتى خروجه منها.[1]

من ذلك بيانات موقع المستخدم، و بيانات التصفح، و تاريخ التصفح و بيانات استخدام الوسائط كمقاطع الفيديو، و استجابات النقر على الاعلانات، إضافةً إلى بيانات محتوى الاتصال كمحتوى رسائل البريد الالكترونى أو المنشورات و التعليقات على مواقع التواصل ..الخ

الغصن الثانى

ضوابط مشروعية معالجة البيانات

كائنةً ما كانت عملية المعالجة التى تجرى على أية فئة من فئات البيانات الشخصية سابقة الذكر، فإنه لا بد من أن تتقيد عملية المعالجة بمجموعة من الضوابط الإجرائية و الموضوعية التى نص عليها القانون كى يسبغ عليها وصف المشروعية، و بالتالى تكون بمنأى عن الجزاءات الجنائية المرصودة لكل ما من شأنه المساس بخصوصية البيانات.

و يقع الالتزام بضوابط مشروعية معالجة البيانات- بصفة أساسية- على شخص المسئول عن عملية المعالجة، و قد أطلق عليه القانون المصرى اسم (المتحكم) و عرّفه بكونه:" أي شخص طبيعي أو اعتباري، يكون له - بحكم أو طبيعة عمله- الحق في الحصول على البيانات الشخصية وتحديد طريقة وأسلوب ومعايير الاحتفاظ بها، أو معالجتها والتحكم فيها طبقا للغرض المحدد أو نشاطه"؛ بينما المعالج هو "أي شخص طبيعي أو اعتباري مختص، بطبيعة عمله، بمعالجة البيانات الشخصية لصالحه، أو لصالح المتحكم بالاتفاق معه ووفقا لتعليماته."[2]؛ و كان المشرع الفرنسى قد عرّف

[1]- مصطفى ابراهيم العربى، مظاهر الحماية الجنائية للحق فى النسيان الرقمى، المجلة العربية لعلوم الأدلة الجنائية و الطب الشرعى، جامعة نايف العربية للعلوم الأمنية،سبتمبر2020، المجلة 2- العدد2، ص 208، 209

[2]- المادة (1) من القانون المصرى لحماية البيانات الشخصية رقم 151 لعام 2020.

المسئول عن معالجة البيانات بأنه: الشخص الطبيعى أو السلطة العامة أو أى وكالة أو مؤسسة يمكنها تحديد وسائل و أهداف المعالجة."[1]

يستفاد من ذلك ببساطة أن المعالج هو من يقوم بعملية أو عمليات المعالجة، أما المتحكم أو المراقب أو المسئول عن معالجة البيانات هو من تتم المعالجة لحسابه، و هو من يضع السياسات العامة لعملية المعالجة. و عليه فإن المتحكم أو القائم بمعالجة البيانات هو الملتزم بحسب الأصل بضوابط مشروعية المعالجة، و يعد إخلاله بها مناطاً للمساءلة الجنائية، و لا يمنع ذلك من مساءلة المعالج عن الإخلال بضوابط المشروعية إن ثبتت مسئوليته عن الإخلال.

و فيما يلى نورد بإيجاز أهم ضوابط مشروعية معالجة البيانات، و نرى تقسيم هذه الضوابط لقسمين تبعاً لطبيعتها، فنتناول أولاً الضوابط المحققة للمشروعية الإجرائية لنظام معالجة البيانات؛ و من ثم تلك التى تعزز مشروعيتها الموضوعية.

أولاً: ضوابط المشروعية الإجرائية لنظم معالجة البيانات:

أ) الحصول على ترخيص من الجهة المختصة:

يتقيد المسئول عن معالجة البيانات-وفقاً للقانون المصرى- بالحصول على ترخيص أو تصريح من الجهة المختصة و هى مركز حماية البيانات الشخصية من أجل الحصول على البيانات الشخصية أو إجراء أى عملية عليها.[2]

و يفرق القانون بين الترخيص بمعالجة البيانات، و التصريح بالمعالجة حيث إن الترخيص يكون للشخص الاعتبارى فقط و يكون موقوت بمدة ثلاث سنوات قابلة للتجديد لمدد أخرى؛ بينما التصريح فيصدر للشخص الطبيعى أو الاعتبارى و لا تجاوز مدته سنة واحدة قابلة للتجديد لمدد أخرى.[3]

بينما يشترط المشرع الفرنسى للقيام بإنشاء نظام معالجة للبيانات و لو لحساب الدولة صدور مرسوم وزارى من الوزير المختص يسمح بالمعالجة، أو مرسوم من مجلس

[1]- "Le responsable de traitement est la personne morale (entreprise, commune, etc.) ou physique qui détermine les finalités et les moyens d'un traitement, c'est à dire l'objectif et la façon de le réaliser. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal »,voir : https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp169_fr.pdf

[2]- بند رقم 10 من المادة الرابعة لقانون حماية البيانات المصرى 151 لعام 2020.

[3]- راجع التعريفات فى المادة (1) من قانون حماية البيانات الشخصية سالف الذكر.

الدولة و ذلك بعد أخذ رأى اللجنة الوطنية للمعلوماتية و الحريات على أن يصدر هذا الرأى مسبباً و يتم نشره.[1]

و تحدد التراخيص الصادرة بمراسيم وزارية أو بمرسوم من مجلس الدولة الإطار التفصيلى لنظام المعالجة المصرح به فتتضمن معلومات من أهمها:

- الغرض من المعالجة و اسمها عند الاقتضاء.
- الخدمات التى يمارس بها حق الولوج إلى البيانات.
- فئات البيانات الشخصية المسجلة.
- المستلمون أو فئات المستلمين المخولين بتلقي هذه البيانات.[2]

و يلاحظ أن عدم الالتزام بالقيوم الشكلية فى إنشاء نظام معالجة البيانات يعاقب عليه القانون الفرنسى بالسجن خمس سنوات و غرامة 300 ألف يورو.[3] و يعاقب عليه القانون المصرى بغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه ؛ 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 تمت مخالفة القانون مقابل الحصول على منفعة مادية أو أدبية، أو بقصد تعريض الشخص المعني بالبيانات للخطر أو الضرر.[4]

ب) الشفافية و الرضائية:

يلتزم المسئول عن المعالجة أو المتحكم بالحصول على الموافقة المستنيرة للشخص المعنى فى حالة جمع البيانات أو أى عملية أخرى من عمليات المعالجة، مالم تكن عملية المعالجة ضمن الحالات المصرح بها قانوناً كما فى حالة الحصول على البيانات من أجل الإحصاءات الرسمية، أو للأغراض الإعلامية أو لأغراض الضبطية

[1]-Art 31 à 36 de la **Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.**

[2]- Art 35 de la **Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.**

[3] - Art.**226-16 du droit penal, Modifié par Ordonnance n°2018-1125 du 12 décembre 2018 - art. 13**

[4]- مادة (36) من قانون حماية البيانات الشخصية 151 لعام 2020.

القضـائية، أو لأغـراض حمايـة الأمـن القـومى، بالإضـافة إلـى البيانـات لـدى البنـك المركزى المصرى، و الجهات الخاضعة لرقابته و إشرافه.[1]

ووفقاً للمشرع الفرنسى فموافقة صاحب البيانات مشترطة لمشروعية المعالجة أيضاً إلا فى الحالات التالية:

1- إذا كانت المعالجة ضرورية لتنفيذ العقد الذي يكون موضوع البيانات طرفًا فيه، أو لتنفيذ تدابير ما قبل العقد المتخذة بناءً على طلب موضوع البيانات؛
2- إذا كانـت المعالجـة ضـرورية للامتثـال لالتـزام قـانوني يخضـع لـه مراقـب البيانات؛
3- إذا كانت المعالجة ضرورية لحماية المصـالح الحيويـة لصـاحب البيانـات أو أي شخص طبيعي آخر؛
4- إذا كانت المعالجة ضرورية لتنفيذ مهمة ذات مصلحة عامة أو تتعلق بممارسة السلطة العامة المخولة للمراقب.
5- بخـلاف المعالجـات التـى تقـوم بهـا السـلطات العامـة، فـإن المعالجـة تعتبـر ضرورية لأغراض المصالح المشروعة التى يسعى إليها المراقب (المسئول عن المعالجـة) أو الغير متـى كانـت لا تتعـارض مـع حقـوق و حريـات أساسـية للشخص المعنى لا سيما إذا كان طفلاً.[2]

و يلاحظ أن القانون الفرنسى لم يشترط صراحةً أن تكون موافقة الشخص المعنى بالبيانات موافقة كتابية، و كذا القانون المصرى لم يشترط الموافقة الكتابية إلا فى حالة معالجـة البيانـات الشخصـية الحساسـة، و فـى حالـة كـون المعالجـة تنصـب علـى بيانـات لأطفال فلابد من موافقة كتابية من ولى الأمر بالنظر إلى كون بيانات الأطفال هى دوماً من البيانات المعتبرة بيانات حساسة.[3]

كمـا أن القـانون يعطـى الشـخص المعنـى بالبيانـات حـق سـحب موافقتـه علـى معالجـة البيانات إذا كانت المعالجة قد تمت على أساسها، و كذا حقوق التصـحيح أو التعديل أو المحـو أو الإضـافة أو التحديث للبيانـات الشخصـية، و كـذا الاعتـراض علـى معالجـة

33 - مادة 2 من قانون 151 لعام 2020

[2] - Art.5 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Créé par LOI n°2018-493 du 20 juin 2018 - art. 10

[3]- مادة 12 من قانون 151 لسنة 2020.

البيانات الشخصية أو نتائجها متى تعارضت مع الحقوق والحريات الأساسية للشخص المعني بالبيانات.[1]

و فى غير الحالات التى تشترط فيها موافقة صاحب الشأن فإنه يلتزم المسئول عن المعالجة بإعلام صاحب الشأن بالبيانات الموجودة لدى المتحكم (المسئول عن المعالجة) و تمكينه من الإطلاع عليها [2]، و قد استثنى المشرع الفرنسى من هذا الالتزام بعض الحالات التى يتعذر فيها إعلام صاحب الشأن كما فى حالة جمع البيانات لأغراض البحث العلمى، أو التاريخى، أو لأغراض البحث فى مجال الصحة، و كذا جمع البيانات لأغراض الأمن الوطنى و لأغراض الوقاية من الجريمة أو الملاحقة القضائية لمرتكبى الجرائم.[3]

ثانياً: ضوابط المشروعية الموضوعية لنظم معالجة البيانات:

أ) دقة البيانات و ضرورة تأمينها:

يلتزم المسئول عن معالجة البيانات بالتحقق من صحة البيانات التى تجرى عليها عملية المعالجة، و أن تكون البيانات دقيقة و كاملة و محدثة طوال فترة المعالجة، و ذلك من خلال تعديل البيانات بما يتوائم مع أى تغير فى أوضاع الأشخاص المعنيين بالبيانات.

و عليه فإنه يقع على عاتق المتحكم اتخاذ كافة التدابير الفنية التى تمكنه من تصحيح البيانات الخاطئة أو إكمال ما ينقص منها، أو محو البيانات فى حالة عدم مطابقتها للحقيقة.

و يستوجب ذلك وضع نظم داخلية لتلقى شكاوى الأشخاص المعنيين بالبيانات، و طلبات الوصول للبيانات و التصحيح و التعديل و الحذف.[4]

و عطفاً على ما سبق فإن مشروعية المعالجة ترتهن بضرورة تأمين البيانات محل المعالجة و المحافظة على سريتها [5]، و يستلزم ذلك بطبيعة الحال استخدام التقنيات

---

[1]- المادة 2 من قانون 151 لعام 2020

[2]- يلاحظ أن المشرع المصرى قد استثنى الحالات المصرح بها قانوناً (حالة الحصول على البيانات من أجل الإحصاءات الرسمية، أو للأغراض الإعلامية أو لأغراض الضبطية القضائية، أو لأغراض حماية الأمن القومى، بالإضافة إلى البيانات لدى البنك المركزى المصرى و الجهات الخاضعة لرقابته و إشرافه.) من سريان كافة أحكام قانون حماية البيانات الشخصية و بالتالى فهى مستثناه من تطلب الموافقة المستنيرة لصاحب الشأن و كذا مستثناه من الحق فى إعلامه و إطلاعه على البيانات. و عليه فلا يكاد القانون المصرى يفرق بين الحق فى الموافقة المستنيرة و الحق فى الاعلام الذى يفترض عدم تطلب موافقة صاحب الشأن و إنما فقط إعلامه بالمعالجة التى تجرى على بياناته.
كما يعتبر من اللافت فى هذا الإطار أن الاستثناءات التى استبعدها المشرع المصرى من إطار تطبيق قانون حماية البيانات قد صيغت فى عبارات فضفاضة دون تحديد ضوابطها و قيودها.

[3]- Art.30 et 67 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

4- سليم محمد سليم ، الحماية الجنائية للبيانات المعالجة آلياً- دراسة مقارنة، المرجع السابق، ص 71

[5]- البند 2 من المادة 3 من قانون حماية البيانات الشخصية 151 لعام 2020

المتطورة لحماية البيانات، و تأمينها من الاعتداء عليها سواء بالاطلاع و الولوج غير المشروع أو التدمير، أو التشويه. من ذلك تقنيات التشفير و اخفاء هوية أصحاب البيانات.[1]

و يتطلب تنفيذ هذه التقنيات و غيرها وجود فريق مدرب على أعلى مستوى بالإضافة إلى وضع نظم داخلية للإدارة الفعالة للبيانات الشخصية يؤمن إجراء عمليات مراجعة، و تدقيق دورية و شاملة لنظم حماية البيانات، و الإبلاغ عن أى تجاوز للإجراءات التى تهدف لحمايتها.[2]

و قد نصت اللائحة التنفيذية لقانون تقنية المعلومات رقم 175 لعام 2018 على إجراءات ملزمة لمشغلى خدمات الانترنت تهدف لتأمين البيانات، و المحافظة على سريتها فى المادة (2) من اللائحة، من هذه الإجراءات:

- الإلزام بتشفير البيانات و المعلومات باستخدام نظام تشفير قياسى متماثل أو غير متماثل بمفتاح شفرة لا يقل عن 128 بت مع الحفاظ على سرية مفتاح التشفير.
- و كذا تنصيب و استخدام نظم و برامج مكافحة البرمجيات و الهجمات الخبيثة، و التأكد من صلاحيتها و تحديثها.
- استخدام بروتوكولات آمنة لنقل البيانات، استخدام نظم و برمجيات الجدران النارية لحماية الشبكات و النظم.
- إجراء اختبار سنوى للكشف عن المخاطر الأمنية، و الاختراقات.

و تعرض مخالفة الالتزام بسرية البيانات، و تأمينها المخالف لعقوبة الغرامة التى لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز ثلاثة ملايين جنيه فى القانون المصرى، و لعقوبة السجن خمس سنوات وغرامة ثلاثمائة ألف يورو وفقاً للقانون الفرنسى.[3]

---

[1]- Art.4 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Modifié par Ordonnance n°2018-1125 du 12 décembre 2018 - art. 1

[2]- د.طارق جمعة راشد، الحماية القانونية لخصوصية البيانات الشخصية فى القانون القطرى و المقارن، المرجع السابق، ص131 (57).

[3] - **Article 226-17, Modifié par Ordonnance n°2018-1125 du 12 décembre 2018 - art. 13**

ب) الغائية و التناسب (الضرورة):

تفترض مشروعية عملية معالجة البيانات، أن تستهدف المعالجة غاية أو غايات محددة، و هو ما عبر عنه القانون المصرى لحماية البيانات فى مادته الثالثة بقوله: " يجب لجمع البيانات الشخصية ومعالجتها والاحتفاظ بها، توافر الشروط الآتية: 1- أن تجمع البيانات الشخصية لأغراض مشروعة ومحددة ومعلنة..."

و يستفاد من ذلك أنه لابد من أن تؤطر عملية المعالجة سواء كانت جمعاً للبيانات، أو تخزيناً أو نقلاً أو غير ذلك بأهداف محددة، و معلنة للشخص المعنى، و للهيئة التى تصدر الترخيص بالمعالجة؛ و بالتالى لكى لا تفقد المعالجة مشروعيتها لا مناص من التزامها لأهدافها المحددة و المعلنة مسبقاً. و ينبنى على ذلك أنه لا يجوز إعادة استخدام بيانات تم تجميعها لغاية محددة من أجل غاية أخرى.

فمثلاً إذا تم جمع البيانات الشخصية لمجموعة من الموظفين بهدف إلحاقهم بنظام تأمينى معين لا يجوز من بعد ذلك تسريب هذه البيانات لجهات تقوم باستخدامها لأغراض التسويق، أو لأغراض تجارية، و كذا إذا تم جمع بيانات شخصية من أجل إجراء بحث علمى أو تاريخى فلا يجوز إعادة استخدامها فى الدعاية السياسية. إذن فالإعلان عن أهداف المعالجة ضرورة لضمان التزام المسئول عن المعالجة (المتحكم) بأهداف، و غايات المعالجة إذ يعرضه الخروج عنها لخطر المساءلة القانونية.

و مبدأ الغائية كان قد كرسه القانون الفرنسى لحماية البيانات فى المادة (4) منه، و التى جرت على أنه: "يتم جمع البيانات لأغراض محددة وصريحة ومشروعة، ولا تتم معالجتها لاحقًا بطريقة لا تتوافق مع هذه الأغراض .ومع ذلك، فإن المعالجة الإضافية للبيانات لأغراض الأرشفة من أجل المصلحة العامة، أو لأغراض البحث العلمي أو التاريخي، أو للأغراض الإحصائية تعتبر متوافقة مع الأغراض الأصلية لجمع البيانات، إذا تم تنفيذها وفقًا لأحكام اللائحة (الاتحاد الأوروبي) 679/2016 بتاريخ 27 أبريل 2016 .."[1]

و يرتبط مبدأ الغائية بمبدأ آخر لا يقل عنه أهمية هو مبدأ التناسب أو الضرورة و الذى مفاده أن تكون البيانات الشخصية محل المعالجة متوافقة، و متناسبة مع الغاية التى من أجلها تم جمع هذه البيانات و معالجتها بحيث يقتصر الجمع على البيانات الضرورية فقط من أجل تحقيق الغاية من المعالجة.[2]

[1]- Art.4 de la loi **Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460**

[2]- بند 3 من المادة الثالثة من قانون حماية البيانات 151 لعام 2020.

فإن تم جمع بيانات أكثر مما تتطلبه الغاية من المعالجة، أو تم جمع بيانات لا تربطها صلة مباشرة بالغاية بحيث تتجاوزها، فإن المعالجة تفقد مشروعيتها. و عليه فقد قضى مثلاً بأن إنشاء قاعدة بيانات بيومترية قائمة على قراءة التقنيات الحيوية لموظفى المدينة الجامعية و المتمثلة فى بصمات الأصابع بغرض تأمين النفاذ الآمن و السريع للمبنى إنما يعدّ مجاوزاً للغاية و ليس له ما يبرره . بينما على النقيض من ذلك اعتُبِر مُبرَراً و ضرورياً لتحقيق الغاية إنشاء نظام للمراقبة البيومترية بهدف تأمين نظام طباعة الامتحانات، و الدخول لغرف الأرشيف فى إطار الحاجة للمحافظة على سرية الامتحانات.[1]

و يمثل الانحراف عن الغاية الأصلية االتى جمعت من أجلها البيانات جريمة يعاقب عليها القانون الفرنسى بذات العقوبة المقررة لمخالفة ضوابط المشروعية سالفة البيان[2]، كما يعاقب القانون المصرى على هذه الجريمة بالغرامة التى لا تقل عن ثلاثمائة ألف جنيه و لا تجاوز ثلاثة ملايين جنيه.[3]

ج) الزمنية (الحفظ المحدود للبيانات):

لا يكفى أن تتوافر الضوابط السابقة كى تتحقق مشروعية المعالجة، و بالأخص لا يكفى أن تكون المعالجة محددة الهدف و ألا يجاوز جمع المعلومات أهداف المعالجة، بل إنه لابد -بالاضافة إلى ذلك- أن تتحدد مدة حفظ البيانات بشكل مؤقت يرتبط بالغاية من المعالجة، ذلك أنه لا يفترض أن يكون للمسئول عن معالجة البيانات الاحتفاظ بصورة مطلقة و مؤبدة بالبيانات محل المعالجة إذ أن ذلك إنما يمس بحق الأشخاص المعنيين بالبيانات فى النسيان.

و بوجه عام تتحدد مدة الاحتفاظ بالبيانات بالفترة الضرورية لتحقيق الغاية أو الهدف من المعالجة و هو ما صاغه المشرع المصرى فى المادة (3) من قانون حماية البيانات الشخصية باشتراطه لمشروعية المعالجة: " ألا يتم الاحتفاظ بها (البيانات) لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها."

و تضمنته المادة (4) من القانون الفرنسى فى البند الخامس منها بقولها: "يتم الاحتفاظ بها في نموذج يسمح بتحديد هوية الأشخاص المعنيين لمدة لا تتجاوز الفترة اللازمة للأغراض التي تتم معالجتها من أجلها. ومع ذلك، قد يتم الاحتفاظ بالبيانات الشخصية

[1]- سليم محمد سليم ، الحماية الجنائية للبيانات المعالجة آلياً- دراسة مقارنة، المرجع السابق، ص 90

[2] - **Article 226-21 de code penal.**

[3]- مادة 38 من قانون حماية البيانات الشخصية.

بعد هذه الفترة فى إطار معالجة حصرية لها لأغراض الأرشفة للمصلحة العامة، أو لأغراض البحث العلمي أو التاريخي، أو لأغراض إحصائية..."[1]

و هو ما مفاده أن المسئول عن معالجة البيانات يلتزم بعدم الاحتفاظ بأية بيانات تسمح بتحديد هوية أصحابها أكثر من المدة الضرورية لتحقيق الغرض من المعالجة. و مخالفة هذا الالتزام إنما يعرّض المخالف لعقوبة السجن ثلاث سنوات و غرامة قدرها 45 ألف يورو وفقاً للقانون الفرنسى[2]، و لعقوبة الغرامة التى حدها الأدنى مائتى ألف جنيه و حدها الأقصى مليونى جنيه بمقتضى القانون المصرى.[3]

[1] - Art.4 de la loi **Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460**

[2] -Art.226-20 du code pénal, Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 () JORF 7 août 2004.

[3]- المادة 37 من قانون حماية البيانات الشخصية رقم 151 لعام 2020.

الفرع الثالث

الحق فى النسيان الرقمى

للتعرف على ماهية الحق فى النسيان الرقمى فلابد أولاً من تحديد مفهومه، و مدى ارتباط هذا الحق أو استقلاله عن الحق فى الخصوصية، إضافةً إلى التعرض لموقف التشريعات و أحكام القضاء من الاعتراف بوجوده. لذا نقسّم هذا المطلب إلى فرعين على نحو ما يلى:

الغصن الأول

مفهوم الحق فى النسيان الرقمى و علاقته بالحق فى الخصوصية

الحق فى النسيان الرقمى هو حق من الحقوق المستحدثة الذى جرت محاولات فقهية كثيرة لتعريفه و تحديد طبيعته، و مدى ارتباطه أو استقلاله عن الحق فى الخصوصية أو حرمة الحياة الخاصة.

و قد عُرّف الحق فى النسيان الرقمى بكونه: "حق يخول الشخص الطبيعى أو الاعتبارى مكنة محو معلومة تخصه، أو طلب التوقف عن نشرها بعد مرور فترة زمنية معينة." أو هو "الحق الذى يخول صاحبه مكنة السيطرة من حيث الزمان على بياناته الشخصية بغية الحصول على حذفها أو محوها عندما يرغب فى ذلك".[1]

كما عُرّف أيضاً بأنه "حق الشخص فى ألا يتم الاحتفاظ ببياناته لمدة زمنية تجاوز الغرض أو الغاية الأصلية التى جمعت لأجلها البيانات."[2]

و من أدق و أوضح التعريفات التى سيقت للدلالة على مضمون هذا الحق هو التعريف الذى تبنته اللجنة الوطنية للمعلوماتية و الحريات فى فرنسا حيث عرفته بكونه: "الحق الذى يخول صاحبه مكنة السيطرة على آثاره الرقمية، و حياته على الإنترنت سواء الخاصة أو العامة."[3]

و عليه فلا ينحصر محل هذا الحق فى البيانات الشخصية للفرد تلك التى يحرص على سريتها و من بينها البيانات الوصفية المتعلقة بنشاطه على الشبكة، و إنما ينصب أيضاً على البيانات العلنية التى سبق له نشرها على شبكة الانترنت حين تنصرف إرادته

---

[1]- بو خلوط الزين، الحق فى النسيان الرقمى، مجلة الفكر، جامعة محمد خيضر بسكرة- كلية الحقوق و العلوم السياسية،2017-العدد 14،ص 581

[2]- أمين الخنتورى، معالم تنظيم الحق فى النسيان الرقمى فى التشريع المغربى، مجلة المنارة للدراسات القانونية و الإدارية،2021، العدد 36- ص 170

[3] - « la possibilité offerte à chacun de maîtriser ses traces numériques et sa vie en ligne, qu'elle soit privée ou publique » voir : Maryline Boizard, le temps, le droit àl' loublie et le droit à l'effacement, dalloz (les cahiers de la justice),2016/n 4 ,p.4

لاحقاً إلى ضرورة محوها أو زوالها من الفضاء الرقمى لتغير الظروف، أو لما قد تسببه هذه المنشورات من حرج أو اساءة لسمعته.

إذن فالحق فى النسيان الرقمى يهدف أساساً إلى حماية البيانات الشخصية من البقاء الأبدى على مواقع الشبكة، و كذا حمايتها من الفهرسة الآلية من قبل محركات البحث التى تقوم بتوفير روابط تحيل إلى هذه البيانات أو المعلومات بمجرد القيام بأى عملية بحث على الشبكة.

يستوى فى ذلك بيانات المستخدم الشخصية التى يحرص على سريتها و التى أدلى بها أثناء قيامه بتدشين حساب إلكترونى أو موقع، أو بيانات نشاطه على الشبكة (الصفحات التى زارها، توقيت دخوله أو خروجه، موقعه، عنوان IP الخاص بجهازه ..الخ) أو بياناته المعلنة تلك التى سبق أن شاركها أو نشرها عبر حسابه. (منشور مكتوب- صورة- تسجيل صوتى أو فيديو).

و الحق فى النسيان الرقمى يختلف عن الحق فى الخصوصية الرقمية برغم التداخل الشديد بين الحقين؛ إذ أنه يهدف أساساً إلى توفير سياج حمائى زمنى للبيانات، و لو كانت بيانات علنية أتاحها الشخص لاطلاع العامة بموافقته، فيما يشبه الحق فى التقادم. حيث يكون الفرد بحاجة لإسدال ستار النسيان على وقائع أو أحداث فى حياته مرّ عليها زمن بحيث لم يعد يريد إذاعتها من جديد، أو حتى التمكين من الوصول إليها. و بالتالى فالحق فى النسيان يتيح للمستخدم مراقبة و التحكم فى بياناته و لو كان قد سبق له أن قام بالإفصاح عنها.

و هو ما يستفاد من الألفاظ التى استخدمتها اللجنة الوطنية للمعلوماتية و الحريات CNIL فى تعريفها للحق فى النسيان، حيث تبنت تعبير "الآثار الرقمية أو traces numériques "بدلاً من "البيانات الشخصية Données personnelles" للدلالة على شمول هذا الحق لكل ما قد يكون صدر عن الشخص قى الفضاء الرقمى، و هو ما أكدته حين أردفت: "و حياته على الانترنت سواء الخاصة أو العامة."

بينما الحق فى خصوصية البيانات كما أسلفنا موضوعه التحكم و السيطرة على البيانات الشخصية فى المطلق، بفرض سياج من السرية عليها، و تحديد من يمكنه الاطلاع عليها حصراً، و يهدف هذا الحق أساساً إلى حماية البيانات ذات الطابع السرى أو الخاص و التى لم يسبق إفشائها بصورة علنية من قبل.

و إزاء هذا التشابه و التقاطع بين الحق فى النسيان و الحق فى خصوصية البيانات، فقد ذهب بعض الفقه إلى اعتبار أن الحق فى النسيان يشكّل عنصراً من عناصر الحق فى الخصوصية بوصف الأخير أوسع منه نطاقاً، و علتهم فى ذلك أن نطاق الحياة الخاصة

إنما يشمل الماضى الذى عاشه الإنسان و الذى يحوله مرور الزمن إلى سر يستوجب الكتمان و إن كان قد تم إفشاؤه قبلاً.[1]

بينما يذهب البعض الآخر إلى كون الحق فى النسيان الرقمى هو حق مستقل يتمتع بذاتية خاصة فى مواجهة الحق فى الخصوصية نظراً لاختلاف النطاق و اختلاف الهدف.[2]

بل إن أصحاب هذا المذهب يؤكدون أن الحق فى النسيان الرقمى أوسع نطاقاً من الحق فى الخصوصية، حيث إن محل الحق فى النسيان لا يتوقف عند البيانات الشخصية (السرية بطبيعتها) و إنما يضم أيضاً كل ما قد يكون الشخص قد أفشاه فى الماضى من أمور أو أخبار أو آراء تتصل بحياته أو تعبر عنه.

كما أن الهدف الأساسى من الحق فى النسيان ليس حماية السرية و الخصوصية، و إنما حماية ما يسمى بالسمعة الرقمية أو الهوية الرقمية و التى تمثّل الصورة الافتراضية التى ترسمها للشخص كافة البيانات و المنشورات المتعلقة به على الشبكة سواء كان شخصاً طبيعياً أو اعتبارياً.[3]

و من ناحيتنا فإننا نرى أن لكل من الرأيين وجاهته غير المنكورة، و إن كنا نميل إلى الرأى القائل بذاتية الحق فى النسيان الرقمى، و استقلاله عن الحق فى الخصوصية و إن تقاطعا فى العديد من القواسم المشتركة.

---

[1] - Voir plus en détail cette référence : Marie Ranquet, **Le droit à l'oubli : vers un nouveau droit fondamental de l'individu ?, Dans Communications 2019/1 (n° 104), Éditions Le SeuilLe, CAIRN.INFO,P. 149 à 159**

[2]- بو خلوط الزين، الحق فى النسيان الرقمى، مجلة الفكر، جامعة محمد خيضر بسكرة- كلية الحقوق و العلوم السياسية،2017-العدد 14،ص 586

[3]-" on définit l'e-réputation comme la réputation, c'est-à-dire l'image ou encore l'identité, dont dispose une personne à partir des données la concernant répertoriées sur internet. L'e-réputation est donc liée à la fois à la problématique de l'identité numérique que du marketing. Chaque individu peut être affublé d'une e-réputation, ainsi que toute personne morale =(entreprise, association, etc). », Droit à l'oubli : Définition juridique et spécificité : https://www.litige.fr/definitions/droit-a-l-oubli

الغصن الثانى

التكريس التشريعى و القضائى للحق فى النسيان الرقمى

كان لأحكام القضاء لاسيما فى فرنسا، و بلجيكا فضل السبق فى ترسيخ مفهوم الحق فى النسيان الرقمى كأحد عناصر أو تطبيقات الحق فى الخصوصية فى بداية الأمر، و ذلك من خلال بعض أحكام منفردة لمحاكم بلجيكية كمحكمة بروكسل (1997) و لمحاكم فرنسية منها محكمة مونبلييه (ديسمبر 2011)[1]، و محكمة باريس الإبتدائية (فبراير 2012)[2] و ذلك قبل أن تظهر البداية الحقيقية للإعتراف على نطاق واسع بالحق فى النسيان الرقمى كحق له ذاتية خاصة؛ و ذلك من خلال الحكم الشهير لمحكمة العدل الأوروبية فى قضية "Google Spain" الصادر فى 2014[3]

و من أجل تفعيل الحق فى النسيان فقد خولت التشريعات الحامية للبيانات على مستوى أوروبا لأصحاب البيانات الشخصية و المعنيين بها آليات يمكنهم اللجوء إليها متى أرادوا السيطرة على بياناتهم و منشوراتهم فى الفضاء الرقمى؛ و من أهم هذه الآليات الحق فى المحو، و الحق فى الإلغاء من محركات البحث.

---

[1]- بو خلوط الزين، الحق فى النسيان الرقمى، المرجع السابق، ص587.

[2] - TGI PARIS, 15 fevrier 2012, https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-ordonnance-de-refere-15-fevrier-2012/

و قد صدر هذا الحكم بشأن نزاع تتلخص وقائعه فى أن شابة تعمل سكرتيرة قانونية كانت قى ماضى حياتها قد عملت فى تمثيل الأفلام الإباحية، وإزاء انتشار هذه الأفلام و رقمنتها على الشبكة العنكبوتية و ما سببه الربط بين هذه المقاطع و بين اسم عائلتها على الفضاء الرقمى، فقد طلبت من منتج هذه الأفلام سحبها من التداول، إلا أنه رفض ذلك؛ فلجأت إلى القضاء مطالبة المحكمة بإلزام محرك البحث جوجل بمحو و إزالة الروابط التى تبث هذه الأفلام و قد أجابتها المحكمة إلى طلبها على اعتبار أن من حق المدعية أن يدخل ماضيها فى طى النسيان فى العالم الرقمى إذ أن الأفلام محل النزاع و إن كانت لا تدخل فى ذاتها فى الحياة الخاصة للمدعية فإنها تشهد على فترة معينة من حياتها تريد أن تستفيد بشأنها من الحق فى النسيان.

[3] - CJUE,14 mai 2014, ***Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González ,***
https://en.wikipedia.org/wiki/Google_Spain_v_AEPD_and_Mario_Costeja_Gonz%C3%A1lez

و تتعلق وقائع هذه القضية بمواطن اسبانى يدعى جونزاليس كان قد سبق أن نشر اسمه فى الصحف عام 1998 بصفته مالك عقار معروض للبيع فى المزاد العلنى لتسديد ديونه، و لسنوات طويلة بعد زوال أزمته المالية ظل اسمه مرتبطاً بهذا الخبر على الفضاء الرقمى، مما أثر عليه نفسياً و تجارياً، فلجأ إلى الجهة المختصة بحماية البيانات و التى أمرت جوجل بمسح الروابط المتعلقة بالخبر المذكور من محركات البحث إلا أن جوجل لم تستجب و تم اللجوء إلى القضاء الاسبانى الذى أحال بدوره الأمر إلى محكمة العدل الأوروبية و التى جاء قضاءها فى صالح جونزاليس حيث ألزمت المحكمة محرك البحث بإزالة النتائج التى تظهر عقب كتابة اسمه، و أيضاً روابط الإحالة التى تحيل إلى صفحات ويب تم نشرها من الغير و تتضمن معلومات تخص هذا الشخص، و حتى و لو كان النشر فى حد ذاته قد تم بصورة مشروعة.

أ) الحق فى المحو:

يعرّف الحق فى المحو بأنه: "هو حق الشخص فى أن يطلب محو بياناته الشخصية من البيئة الرقمية مالم يكن هناك سبب قانونى لاستمرار وجودها أو معالجتها."[1]

و قد جاء النص الصريح على الحق فى المحو (Droit à l'effacement) كأحد آليات الحق فى النسيان الرقمى للمرة الأولى فى نص المادة 17 من التوجيه الأوروبى المسمى بالقواعد العامة لحماية البيانات أو RGPD لعام 2016 و التى نصت على أنه:" يحق لصاحب البيانات أن يطلب من مسئول معالجة البيانات محو البيانات الشخصية المتعلقة به، ويلتزم المسئول بمحو هذه البيانات الشخصية دون تأخير لا مبرر له، عندما ينطبق أحد الأسباب التالية:

1- لم تعد البيانات الشخصية ضرورية فيما يتعلق بالأغراض التي تم جمعها أو معالجتها من أجلها؛

2-إذا سحب صاحب البيانات الموافقة التي تستند إليها المعالجة.

3-إذا كانت عملية المعالجة من الأساس غير مشروعة؛

4-اعترض صاحب البيانات على المعالجة وفقاً للمادة 21 من التوجيه.

5- إذا كان هناك التزام قانونى يفرض على مسئول المعالجة إزالة البيانات وفقاً للقانون الاتحادى أو أحد قوانين الدول الأعضاء الخاضع لها المسئول.

6- إذا كانت المعالجة على أساس الفقرة الأولى من المادة 8 و المتعلقة بمعالجة البيانات الخاصة بالأطفال."[2]

---

[1]- محمد حمزة بن عزة، الحق فى النسيان الرقمى، دراسة مقارنة، بحث منشور فى مجلة القانون و الأعمال، جامعة الحسن الأول- كلية العلوم القانونية و الاقتصادية و الاجتماعية- 2021-عدد 68، ص 127

[2] -Art.17 du RGPD : "1. La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique:
=> Article: 12, 15, 19

a) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière;

b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), et il n'existe pas d'autre fondement juridique au traitement;

c) la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2;

d) les données à caractère personnel ont fait l'objet d'un traitement illicite;

و تطبيقاً لذلك قام المشرع الفرنسى بإصدار قانون 493-2018 الذى تضمن فى المادة 24 منه تعديل المادة 40 من قانون 17-78 المتعلق بالمعلوماتية و الحريات لكى تنص صراحةً على حق المستخدم فى الحذف أو المحو فجرى نصها على أنه: "يجوز لأي شخص طبيعي يثبت هويته أن يطلب من المسئول عن معالجة البيانات، حسب الحالة، تصحيح أو إكمال أو تحديث أو قفل أو حذف البيانات الشخصية المتعلقة به والتي تكون غير دقيقة أو غير كاملة أو ملتبسة أو قديمة. أو فى حال كان جمع البيانات أو التوصل إليها أو حفظها قد تم بصورة غير مشروعة.....و في حالة عدم تنفيذ محو البيانات الشخصية أو في حالة عدم استجابة مراقب البيانات خلال شهر واحد من الطلب، يجوز للشخص المعني الاتصال باللجنة الوطنية لحماية تكنولوجيا المعلومات والحريات، التي تفصل فى هذا الطلب خلال ثلاثة أسابيع من تاريخ استلام الشكوى..."[1]

كما اشتمل القانون 493 سالف الذكر فى نفس المادة النص على تعديل المادة 34 من قانون البريد و الاتصالات الإلكترونية فى فقرتها الثانية بحيث تُلزم مشغلى الانترنت بمحو أنواع معينة من البيانات، حيث جاء فيها:" يقوم مشغلو الاتصالات الإلكترونية، ولا سيما الأشخاص الذين يتمثل نشاطهم في توفير الوصول إلى خدمات الاتصالات للجمهور عبر الإنترنت، بمسح أو إخفاء هوية أي بيانات تتعلق بحركة المرور، مع مراعاة أحكام الثالث والرابع والخامس والسادس .ويجب على الأشخاص الذين يقدمون خدمات الاتصالات الإلكترونية للجمهور، مع مراعاة أحكام الفقرة السابقة، وضع إجراءات داخلية تمكنهم من الاستجابة لطلبات الجهات المختصة".[2]

=> Article: 18

e) les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis;

f) les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1 »

1 - Art.40 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés Modifié par LOI n°2018-493 du 20 juin 2018 - art. 24.

2 - Art.34-1 du Code des postes et des communications électroniques. Modifié par LOI n° 2013-1168 du 18 décembre 2013 - art. 24- Modifié par Décision n°2021-976/977 QPC du 25 février 2022, v. init.

ب) الحق فى الإلغاء من محركات البحث:

الحق فى الإلغاء من محركات البحث أو (le droit au déréférencement) هو الحق الذى يسمح لمستخدم شبكة الانترنت بمطالبة محركات البحث (جوجل أو ياهو مثلا) بحذف نتائج البحث التي تظهر مرتبطة باسمه أو لقبه، دون أن يؤدى ذلك إلى محوها من موقعها الأصلي الذي نشرت فيه.

إذن فهذا الحق يكفل للمستخدم أن يطالب محركات البحث حين فهرسة النتائج بإلغاء نتائج البحث المتحصل عليها عقب كتابة اسمه، وأيضا روابط الإحالة التي تحيل نحو صفحات ويب تم نشرها من الغير وتتضمن معلومات تخصه، حتى ولو كان النشر في حدّ ذاته مشروعا. [1]

و يختلف هذا الحق عن الحق فى المحو فى كونه لا يتعلق إلا بمحركات البحث، كما أنه لا يتطلب محو البيانات، أو المنشورات من الموقع أو صفحة الويب التى نُشرت فيها، و إنما فقط منع ظهور الروابط الخاصة بالموقع، أو الصفحة محل النشر على محركات البحث عقب إجراء أى عملية بحث باستخدام اسم الشخص المتعلقة به البيانات أو لقبه؛ و بالتالى فهذه المكنة أضيق نطاقاً من الحق فى المحو الذى يفترض إزالة البيانات كليةً من الفضاء الرقمى بحيث لن يكون من العسير الوصول إليها، بل إن ذلك سيكون مستحيلاً.

و يمارَس هذا الحق-وفقاً للقانون الفرنسى- عن طريق طلب يوجه إلى محرك البحث المعنى عبر الصفحات المخصّصة لذلك من طرف المحرك، يحدد الطالب من خلاله عنوان URL محل طلب الإلغاء وأيضاً أسباب الطلب، يكون بعد ذلك لمحرك البحث أجل أقصاه ثلاثة أشهر للرد على الطلب، وفي حالة عدم الرد أو الرفض يكون للطالب الحق في التوجه نحو اللجنة الوطنية للمعلوماتية والحريات، فإن لم تستجب لا يكون للطالب إلا اللجوء إلى القضاء الإدارى ممثلاً فى محاكم مجلس الدولة.[2]

و يلاحظ أن مكنات طلب محو المحتوى الإلكترونى أو إلغاءه ليست مكنات مطلقة للمستخدم (صاحب البيانات أو المحتوى) و إنما تحدها بعض القيود التى تضمنها نص المادة 40 من قانون 17-78 و هى ضرورة ألا يؤدى المحو أو الإلغاء إلى:

- مساس بممارسة الحق في حرية التعبير و إتاحة المعلومات؛[3]
- مساس بالتزام قانوني يتطلب معالجة هذه البيانات.

---

[1] - Benjamin A. du Chaffaut, Droit au déréférencement : mise en œuvre et zones d'ombre, Dans Légipresse 2019/HS1 (N° 61), dalloz, CAIRN, pages 15 à 20

[2]- https://www.cnil.fr/fr/le-dereferencement-dun-contenu-dans-un-moteur-de-recherche.

[3] -https://incyber.org/le-droit-a-loubli-nest-pas-un-droit-absolu/

- عرقلة لمصلحة عامة (لاسيما المصالح الصحية العامة) يقتضى تحقيقها معالجة هذه البيانات؛ أو كانت معالجة البيانات قد تمت لأغراض البحث العلمي، أو التاريخي، أو لأغراض إحصائية فى حال كان المحو يجعل تحقيق هذه الأغراض مستحيلاً؛
- مساس بإنشاء حقوق قانونية أو ممارستها أو الدفاع عنها.[1]

و هذه القيود كما هو واضح تحمل معانٍ فضفاضة، و لذا فإنها تخضع لتقدير اللجنة الوطنية للحريات تحت رقابة القضاء بطبيعة الحال، حيث تتم الموازنة فى كل حالة على حدة بين حق الشخص فى النسيان الرقمى و بين المصالح الأخرى التى قد تقتضي معالجة بياناته و بقاءها فى الفضاء الرقمى.

و عليه فقد اعتمد قضاء مجلس الدولة الفرنسى عدة معايير يتم على أساسها تقدير طلبات إلغاء روابط الإحالة من محركات البحث و ذلك فى حكمه الصادر فى 6 ديسمبر 2019 حيث يمكن بلورة هذه المعايير فيما يلى:

1- يتخذ القاضي قراره فى كل طلب من طلبات الإلغاء فى ظل مراعاة الظروف والقانون المعمول به في التاريخ الذي ينظر فيه المسألة.

2- إن إلغاء الإشارة إلى الرابط الذي يربط اسم شخص بصفحة ويب تحتوي على بيانات شخصية تتعلق به هو حق من حقوقه.
3- أن الحق في النسيان ليس مطلقاً، ويجب تحقيق التوازن بين حق مقدم الطلب في الخصوصية وحق الجمهور في الحصول على المعلومات، و تعتمد المفاضلة بين هاتين الحريتين الأساسيتين على ثلاثة عناصر هى:

أ) طبيعة البيانات الشخصية؛ و فى هذا السياق فإن هنالك ثلاث فئات من البيانات الشخصية تعد محل اعتبار و هى:

- **البيانات الحساسة** (البيانات الأكثر تدخلاً في حياة الشخص مثل تلك المتعلقة بصحته، وحياته الجنسية، وآرائه السياسية، ومعتقداته الدينية، وما إلى ذلك)،
- **البيانات الجنائية** (المتعلقة بالإجراءات القانونية أو الإدانة الجنائية)،

و البيانات فى هاتين الفئتين هى الأكثر تقديراً بحيث لا يمكن رفض طلب إلغاء الإشارة قانونًا إليها إلا إذا كان الوصول إلى البيانات الحساسة أو الجنائية من خلال البحث عن اسم مقدم الطلب ضروريًا للغاية للمعلومات العامة.

[1]- أمين الخنتورى، معالم تنظيم الحق فى النسيان الرقمى فى التشريع المغربى، مجلة المنارة للدراسات القانونية و الإدارية، 2021- عدد36، ص168.

- **البيانات التي تؤثر على الحياة الخاصة دون أن تكون حساسة.** و بالنسبة لهذه الفئة يكفي أن تكون هناك مصلحة عامة غالبة في الوصول إلى المعلومات المعنية لكى يتم رفض إلغاء الروابط الخاصة بها من محركات البحث.

ب) <u>الوضع الاجتماعى لمقدم الطلب:</u>

و يتعلق هذا العنصر بسمعة مقدم الطلب، ووظيفته فى المجتمع و دوره فى الحياة العامة.

ج) <u>الظروف التى تم فيها جمع البيانات و نشرها؛</u> على سبيل المثال، إذا كان صاحب البيانات قد أتاحها لاطلاع العامة بنفسه، فإن ذلك قد يجعل من الاستجابة لطلب الإلغاء أكثر صعوبة.[1]

أما فى إطار القانون المصرى لحماية البيانات فقد تضمن القانون النص على حق الشخص المعنى بالبيانات فى تصحيح البيانات أو تعديلها أو محوها، بالإضافة إلى حقه فى العدول عن الموافقة المسبقة بالاحتفاظ بالبيانات أو معالجتها، و كذا حقه فى الاعتراض على معالجة البيانات أو نتائجها متى ما تعارضت معالجة البيانات مع الحقوق و الحريات الأساسية للشخص المعنى.[2]

كما ألزم المتحكم فى البيانات بمحو البيانات الشخصية لديه فور انتهاء الغرض المحدد لها و تصحيح أى خطأ فيها فور علمه أو إبلاغه بذلك.[3]

[1] - Arrêts du 6 décembre 2019, le Conseil d'État, les décisions n°391000, 393769, 395335, 397755, 399999, 401258, 403868, 405464, 405910, 407776, 409212, 423326 et 429154- Voir : https://www.conseil-etat.fr/actualites/droit-a-l-oubli-le-conseil-d-etat-donne-le-mode-d-emploi

[2]- مادة (2) من قانون حماية البيانات الشخصية 151 لعام 2020

[3]- مادة (4) من قانون حماية البيانات الشخصية 151 لعام 2020، و لكن لم يتعرض القانون المصرى للحق فى الإلغاء من محركات البحث كآلية أخرى للحق فى النسيان.

المبحث الأول

التزام مشغلى الإنترنت بتخزين بيانات الاتصال

تطلبت الضرورات الأمنية منذ بدايات صدور القوانين المنظمة لتقنية المعلومات على مستوى العالم إلزام مشغلى الانترنت لا سيما متعهدى الوصول أو الشركات المزودة لخدمات الانترنت بحفظ أو تخزين بيانات الاتصال الخاصة بكافة عمليات الاتصال التى تتم عبر الشبكة بصورة مؤقتة؛ و بمرور الوقت تبينت المخاطر الجمة لهذا الالتزام على حرمة الحياة الخاصة للأفراد، و بالتالى أخذ الفقه و القضاء الأوروبى على عاتقه وضع قيود جديدة على هذا الالتزام لا تتعلق فقط بمدة التخزين، و إنما بفئات بيانات الاتصال المسموح بتخزينها، و كذا بموجبات هذا التخزين.

و لنفصل الحديث حول هذه النقاط يلزمنا أن نعرض أولاً لمضمون الالتزام بالتخزين، و محله فى مطلب أول، و من ثم نتناول الاتجاه الحديث لتقييد الالتزام بتخزين بيانات الاتصال فى مطلب ثانٍ.

المطلب الأول

مضمون الالتزام بتخزين بيانات الاتصال و المسئول عن تنفيذه

نتناول فحوى هذا المطلب فى فرعين نعرض فى أولهما للتعريف بمشغلى الإنترنت الذين يقع على عاتقهم تنفيذ الالتزام بتخزين البيانات، ثم نعالج فى الثانى المصادر التشريعية التى كرست هذا الالتزام فى القانون الأوروبى و الفرنسى و كذا فى القانون المصرى، بالإضافة إلى مضمون الالتزام و نطاقه.

الفرع الأول

المسئول عن تنفيذ الالتزام بتخزين البيانات

(مشغلى الإنترنت)

يقع الالتزام بحفظ "تخزين" البيانات وفقاً للتوجيهات الأوروبية، و التشريعات الوطنية على مشغلى الانترنت "مقدمى خدمات الانترنت"، حيث عبرت التوجيهات الأوروبية و التشريعات الفرنسية عنهم بمصطلح Les opérateurs de communications électroniques"، بينما عبر عنهم القانون المصرى لتقنية المعلومات ب "مقدمى خدمات تقنية المعلومات".

و يُقصد بمشغلى الانترنت أو مقدمى الخدمة: متعهدى الوصول و متعهدى الإيواء دون غيرهم من المتدخلين فى الفضاء الإلكترونى كمزودى المحتوى، أو مقدمى خدمات البحث الآلى أو غيرهم.

أولاً: متعهد الوصول:

و متعهد الوصول "مزود خدمة الانترنت" أو fournisseur d'accès à Internet" هو "كل مشروع يتيح للعميل الوصول إلى الانترنت أو إلى أى شبكة اتصال بوجه عام، و ذلك عن طريق تقديم الوسائل الفنية اللازمة للحصول على هذه الخدمة، فيقوم بتأمين الاتصال بين مقدمى الخدمات (متعهدى الإيواء و موردى المضمون الإلكترونى) من ناحية و بين المستخدم من ناحية أخرى."[1]

إذن فدور متعهد الوصول -و الذى قد يكون شخص من أشخاص القانون العام أو شركة تجارية- هو ربط المستخدم بالموقع الذي يريده فهو مجرد دور فني خالص يقتصر على إتاحة وصول العميل للمعلومات على الشبكة؛ أى أنه مجرد بوابة للمرور إلى الإنترنت. و يتم تقديم خدمات الدخول أو الوصول إلى الإنترنت عن طريق قيام متعهد الوصول بتزويد المشتركين معه بموجب عقد" تقديم خدمات الدخول "بالوسائل و الأجهزة الفنية اللازمة لدخولهم إلى شبكة الإنترنت، والتي تمكنهم من الوصول للمواقع الإلكترونية المختلفة بغرض الاطلاع و التصفح أو حتى النشر.

و عليه فمتعهد الوصول و إن كان يعلم البروتوكول المستخدم من قبل مستخدمى الانترنت للوصول إلى صفحات الويب (بروتوكول HTTP) إلا أنه لا يعلم بمضمون ما يتم تداوله بينهم أى أنه لا يعلم بمضمون المحتوى الذى يمر من خلاله، و مع ذلك

[1]- أشرف جابر سيد، مسئولية مقدمى خدمات الإنترنت عن المضمون الإلكترونى غير المشروع، مجلة حقوق حلوان للدراسات القانونية و الاقتصادية، 2010، عدد 22، ص20

يمكنه -بطبيعة الحال- تتبع مصدر المضمون الإلكتروني، كمصدر الاتصال، و نظام المعلومات المستخدم، و نوع، و طبيعة ووقت اجراء الاتصال، و نوع البروتوكول المستخدم أو الشبكة المستخدمة، و ليس هذا فحسب إنما يمكنه تتبع أى تعديل أو حذف أو إضافة تجرى على المحتوى الإلكتروني.[1]

و فيما يتعلق بالبيانات الشخصية لمستخدمى الانترنت (المشتركين) كالاسم، و محل الإقامة، و العنوان البريدى و عنوان البريد الإلكتروني، و رقم الهاتف، و كلمة المرور؛ فيُفترض علمه بها لدى قيامه بالتعاقد معهم، كما أنه يُفترض علمه أو قدرته على العلم بهوية موردى المحتوى (أصحاب المواقع مثلا) حيث يقدم مورد المحتوى معلوماته الشخصية إلى متعهد الإيواء عند إبرام عقد الإيواء.

ثانياً: متعهد الإيواء:

أما متعهد الإيواء "المستضيف" أو "Fournisseur d'hébergement" فالمقصود به : " كل شخص طبيعى أو معنوى يضع و لو بدون مقابل تحت تصرف الجمهور عبر الإنترنت خدمة تخزين النصوص و الصور و الصوت و الرسائل أيا كانت طبيعتها، و التى تزود بواسطة المستفيد من هذه الخدمات."[2] أو هو "هو شخص طبيعي أو معنوي يتولى تخزين وحفظ البيانات والمعلومات لعملائه، ويوفر الوسائل الفنية والمعلوماتية التي تسمح لهم بالحصول على هذه البيانات والمعلومات طوال ساعات اليوم وذلك عبر الانترنت." [3]

إذن فدور متعهد الإيواء هو إيواء صفحات ال"ويب" على حواسيبه الخادمة مقابل أجر فهو بمثابة مؤجر لمكان على الشبكة للمستأجر "الناشر" الذى ينشر عليه ما يريد من نصوص أو صور أو ينظم مؤتمرات أو ينشيء روابط معلوماتية من المواقع الأخرى.[4]

إن الإيواء أو التخزين المباشر والدائم للمواقع الإلكترونية ولصفحات الويب على الحواسيب لمتعهد الإيواء، والمرتبطة على الدوام بشبكة الإنترنت، هو الذي يميز هذا الأخير عن الناقل الفني البسيط أو (cashing) الذي يتولى، في سبيل تسريع عملية

---

[1]- أشرف جابر سيد، المرجع السابق، ص 102

[2]- Art.6-2 de la **LOI n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (1)**

[3]- د.عبد الفتاح محمود الكيلانى، مدى المسئولية القانونية لمقدمى خدمة الانترنت، بحث منشور عبر منصة المنظومة الإلكترونية، ص495

[4]- د.حسن البنا عبد الله عياد، المسئولية المدنية و الجنائية لمقدمى بعض خدمات الانترنت، رسالة دكتوراة، جامعة عين شمس، ص 118

اتصال الجمهور بالشبكة، الاحتفاظ آليا بنسخة مؤقتة عن كل صفحة ويب ينقلها إلى طالبيها من المستخدمين.

إذن لا سبيل أمام كل من يرغب فى بث مضمون إلكترونى بصورة دائمة، و مباشرة إلا الاستعانة بخدمات متعهد الإيواء.

و للإيواء أربعة أنواع و هى: الإيواء التعاونى" بالمشاركة" و هو الأكثرها شيوعاً لقلة تكلفته؛ و فيه يشترك على ذات الجهاز الخادم العديد من المواقع، و الإيواء المميز أو" الاستئثارى" حيث يكون لكل عميل جهاز خادم خاص به يؤوى موقعه وحده دون أن تشاركه فى جهازه مواقع أخرى و يكون للعميل هنا حرية تامة فى إدارة الخادم.

هناك أيضاً الإيواء بنظام تسليم المفتاح و الذى يشبه الإيواء المميز مع فارق أساسى هو تدخل متعهد الإيواء مع العميل فى إدارة الجهاز الخادم، و أخيرا الإيواء بطريق التصنيف حيث يقوم متعهد الإيواء بتخصيص مساحة للتخزين فى الجهاز الخادم الخاص به.

و يُفهم مما سبق أن متعهد الإيواء يختلف عن مورد المضمون حيث إن مورد المضمون هو المؤلف أو الناشر أو مدير موقع الويب الذى يضع محتوى معين على الانترنت سواء كان صوراً أو نصوصاً أو محتوى سمعى أو بصرى؛أى قد يكون مورد المضمون مستخدما عاديا للانترنت أو مديرا لموقع يقوم على تصميم الموقع ووضع المضمون الإلكترونى فى قالب فنى إحترافى.[1]

نخلص مما سبق إلى أن ما عناه المشرع (المصرى و الفرنسى) بمشغلى الانترنت الذين يقع على عاتقهم الالتزام بتخزين بيانات الاتصال هم-بصفة أصلية- متعهدى الوصول و متعهدى الايواء.

[1]- سيد أشرف جابر، المرجع السابق، ص 23

الفرع الثانى

مضمون الالتزام بتخزين بيانات الاتصال و نطاقه

يتفاوت مضمون الالتزام بتخزين البيانات و نطاقه الموضوعى و الزمنى باختلاف التشريعات المنظمة له، و عليه فإننا نتناول أولاً مضمون هذا الالتزام فى إطار التوجيهات الأوروبية و القانون الفرنسى فى غصنٍ أول، و من ثم نعرض له وفقاً لما جاءت به نصوص القانون المصرى لتقنية المعلومات فى غصنٍ ثانى.

الغصن الأول

مضمون الالتزام بتخزين البيانات فى التوجيهات الأوروبية و القانون الفرنسى (قبل 2020)

وُضِع الإطار العام لالتزام مشغلى الانترنت بتخزين بيانات الاتصال لأول مرة على مستوى أوروبا بواسطة التوجيه الأوروبى رقم 58 لعام 2002 الذى جاء كصدى للتوصيات الصادرة عن البرلمان، و المجلس الأوروبى عام 1995 بالتوجيه رقم 95/46/EC حيث تضمن فى مادته رقم 15 ضرورة اعتماد الدول الأعضاء لتدابير تشريعية تقيد نطاق الحقوق، و الالتزامات الواردة فى هذا التوجيه (التى تضمن حماية خصوصية البيانات و التقليل من نطاق معالجة البيانات الشخصية أو معالجتها بصورة مجهلة كلما أمكن ذلك) عندما يشكل التقييد إجراءً ضروريًا ومناسبًا ومتناسبًا داخل مجتمع ديمقراطي لحماية الأمن القومي ، والدفاع، والأمن العام، ومنع الجرائم الجنائية أو الاستخدام غير المصرح به لنظام الاتصالات الإلكترونية؛ بالإضافة إلى ما جاء صراحةً فى المادة المذكورة من ضرورة اعتماد تدابير تشريعية تنص على الاحتفاظ بالبيانات لفترة محدودة إذا كان لذلك ما يبرره بشرط أن تتوافق هذه التدابير مع المبادىء العامة للقانون الأوروبى.[1]

و فى ظل هذا الإطار العام الذى يمنح التشريعات الوطنية سلطة تقييد حقوق ذوى الشأن فيما يتعلق بخصوصية بياناتهم، تبنى التشريع الفرنسى نصوصاً تقيد من التزام مشغلى الاتصالات بمحو بيانات الاتصال مباشرةً أو تجهيلها فى حالات معينة.

[1]- Directive 2002/58/EC of the European Parliament and of the Council-of 12 July 2002, https:// eur lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058

من ذلك ما نصت عليه المادة L.34-1 و المادة R10-13 من قانون البريد و الاتصالات الإلكترونية من إجازة احتفاظ مشغلى خدمات الاتصالات و بالأخص مزودى خدمات الاتصالات الإلكترونية (متعهدى الوصول) ببيانات الاتصال (إرجاء محوها أو تجهيلها) لمدة مؤقتة فى حالات معينة؛ و من جماع هاتين المادتين يمكن القول أن هناك حالتين يسمح فيهما بالاحتفاظ ببيانات الاتصال، و هما:

أولاً: التخزين لأغراض البحث و الكشف عن الجرائم الجنائية و ملاحقتها:

يُرجأ محو بيانات الإتصال لمدة أقصاها عام واحد، و تشمل بيانات الاتصال المذكورة ما يلى:

أ) البيانات التى تمكن من التعرف على هوية المستخدم.
ب) بيانات المعدات الطرفية المستخدمة فى الاتصال.
ت) المواصفات التقنية، و تاريخ و موعد و المدة التى استغرقها كل اتصال.
ث) البيانات المتعلقة بالخدمات الإضافية المطلوبة بواسطة المستخدم.
ج) البيانات التى تمكن من التعرف على وجهة الاتصال أو متلقى الاتصال.
ح) البيانات التى تحدد مصدر الاتصال و موقعه.

و الحفظ لأغراض البحث، و الكشف عن الجرائم يكون لمدة أقصاها عام واحد من تاريخ الاتصال، و تتحمل السلطات القضائية تحديد تكلفة هذه الخدمة (الحفظ) و تعويض المشغلين عنها وفقا للمادة R. 213-1 من قانون الإجراءات الجنائية. [1]

مع ملاحظة أنه لا يجوز بأى حال من الأحوال تخزين أية بيانات تتعلق بفحوى الاتصالات أو المراسلات المتبادلة، أو أية معلومات وردت فى سياقها.

ثانياً: التخزين لأغراض تسويق الخدمات و غيره:

يجوز معالجة بيانات المرور (الحركة)، و كذا بيانات مواقع المعدات الطرفية، و الاحتفاظ بها بموافقة المستخدم لأغراض تسويق الخدمات لفترة محددة ترتبط بالغرض من التخزين، على أن تكون موافقة المستخدم موافقة مستنيرة تقوم على إعلام المستخدم بكل ما يتعلق بعملية المعالجة، و فئات البيانات محل المعالجة، و مدة الحفظ و الغرض منه. و للمستخدم فى هذه الحالة سحب موافقته فى أى وقت، و بدون أى رسوم.

[1]- Article L34-1 de code de la poste-Modifié par Loi n°2006-64 du 23 janvier 2006 - art. 5- JORF 24 janvier 2006m et Article R10-13- Création Décret n°2006-358 du 24 mars 2006 - art. 1 - JORF 26 mars 2006.

و لا تتيح هذه الحالة أيضاً تخزين أية بيانات تتعلق بفحوى الاتصالات أو المراسلات المتبادلة تحت أى ظرف من الظروف.

الغصن الثانى

مضمون الالتزام بتخزين البيانات فى القانون المصرى

نص قانون تقنية المعلومات فى المادة رقم (2) منه على إلزام مقدم الخدمة ب " حفظ وتخزين سجل النظام المعلوماتى أو أى وسيلة لتقنية المعلومات لمدة 180 يوما متصلة وتتمثل البيانات الواجب حفظها وتخزينها فيما يلى :

أ) البيانات التى تمكن من التعرف على مستخدم الخدمة.
ب) البيانات المتعلقة بمحتوى ومضمون النظام المعلوماتى المتعامل فيه متى كانت تحت سيطرة مقدم الخدمة.

ج) البيانات المتعلقة بحركة الاتصال.

د) البيانات المتعلقة بالأجهزة الطرفية للاتصال.

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

كما كان قانون تنظيم الاتصالات رقم 10 لعام 2003 قد نص فى المادة 64 منه على ما يلى:

"يلتزم مشغلو ومقدمو خدمات الاتصالات والتابعون لهم وكذلك مستخدمو هذه الخدمات بعدم استخدام أية أجهزة لتشفير خدمات الاتصالات إلا بعد الحصول على موافقة من كل من الجهاز والقوات المسلحة وأجهزة الأمن القومي ، ولا يسرى ذلك على أجهزة التشفير الخاصة بالبث الإذاعي والتليفزيوني.
ومع مراعاة حرمة الحياة الخاصة للمواطنين التي يحميها القانون يلتزم كل مشغل أو مقدم خدمة أن يوفر على نفقته داخل شبكة الاتصالات المرخص له بها كافة الإمكانيات الفنية من معدات ونظم وبرامج واتصالات داخل شبكة الاتصالات والتي تتيح للقوات المسلحة وأجهزة الأمن القومي ممارسة اختصاصها في حدود القانون، على أن يتزامن تقديم الخدمة مع توفير الإمكانيات الفنية المطلوبة ، كما يلتزم مقدمو ومشغلو خدمات الاتصالات ووكلائهم المنوط بهم تسويق تلك الخدمات بالحصول على معلومات وبيانات دقيقة عن مستخدميها من المواطنين ومن الجهات المختلفة بالدولة. "

و مما يسترعى الانتباه هنا وجود فارقين هامين بين القانونين المصرى و الفرنسى فى إطار تنظيمهما للإلزام بتخزين بيانات الاتصال، و هما:

1- النطاق الزمنى للالتزام بالتخزين:

فنجد أنه فى القانون المصرى أضيق منه فى القانون الفرنسى، حيث أن مداه الزمنى ستة أشهر فى القانون المصرى بينما هو سنة فى القانون الفرنسى.

2- النطاق الموضوعى للالتزام بالتخزين:

يبدو أن القانون المصرى- و لو ظاهرياً- يوسّع من نطاق الإلزام بالتخزين حيث يضيف لفئات بيانات الاتصال الواجب تخزينها "أى بيانات أخرى يصدر بتحديدها قرار من مجلس إدارة الجهاز" و المقصود بالجهاز فى هذا السياق الجهاز القومى لتنظيم الاتصالات.[1]

أى أن لهذا الجهاز سلطة تحديد فئات بيانات إضافية يلتزم مشغلو الخدمة بحفظها مدة الستة أشهر المذكورة، و هنا يثور التساؤل هل يتصور أن يكون من بين هذه الفئات بيانات تتعلق بمحتوى الاتصال؟ لا سيما و أن المشرع لم ينص صراحةً على استبعاد هذه البيانات من نطاق الإلزام بالتخزين.

و على النقيض من ذلك نجد أن المشرع الفرنسى قد حدد حصراً البيانات التى يجوز حفظها لأغراض مكافحة الجريمة، و إن كانت تشمل كافة بيانات الاتصال بما فيها بيانات تحديد الموقع، و هوية متلقى الاتصال، و بيانات حركة الاتصال بما لها جميعاً من خطورة على الحق فى خصوصية البيانات. كما أنه استبعد صراحةً و فى أكثر من موضع إمكانية حفظ أو تخزين البيانات التى تتعلق بفحوى الاتصال أو المراسلات الإلكترونية.

[1]- مادة (2) من قانون تقنية المعلومات 175 لعام 2018

المطلب الثانى

الاتجاه لتقييد الالتزام بتخزين بيانات الاتصال

(رفض التخزين المعمم للبيانات)

- **تمهيد و تقسيم:**

إزاء تعارض إلزام مشغلى الانترنت بتخزين بيانات الاتصال مع حق مستخدمى الإنترنت فى خصوصية البيانات، فقد تعرّض القضاء الأوروبى ممثلاً فى محكمة العدل الأوروبية، و القضاء الداخلى الفرنسى لإعادة النظر فى مدى مشروعية هذا الإلزام، و مدى توافقه مع التوجيهات الأوروبية المتعلقة بحرمة الحياة الخاصة و خصوصية البيانات؛ ما أدى إلى تعديلات تشريعية تتعلق بمضمون الإلزام بالتخزين، و بقاء بعض النقاط محل خلاف و جدل لم يُحسم بعد.

و لطرح مجريات الاتجاه الحديث لتقييد الالتزام بتخزين البيانات، فإنه يحسن تقسيم الدراسة فى هذه الجزئية إلى فرعين يتناول أولهما تصنيف بيانات الاتصال من حيث مدى خطورتها على الحق فى حرمة الحياة الخاصة، و يعرض الثانى لإشكالية تخزين بيانات المرور و الموقع بوصفها أكثر بيانات الاتصال حساسية.

الفرع الأول

تصنيف بيانات الاتصال بحسب الخطورة

لاشك أن حفظ بيانات الاتصال الإلكترونى، و الإفصاح عنها إنما يمثل انتهاكاً خطيراً لحق الإنسان فى الخصوصية؛ فبيانات الاتصال و إن لم تكن تشتمل على بيانات فحوى الاتصال أو المراسلة، يمكنها أن تعطى معلومات أكثر مما ينبغى عن الحياة الخاصة للفرد، ففرط اعتماد البشر فى العصر الحديث على شبكة الانترنت فى الاتصالات عبر الشبكة أو فى مجال استخدام شبكات التواصل الاجتماعى يتيح لمشغلى الخدمة جمع العديد من البيانات حول المستخدم كبيانات الهوية المدنية، و الحسابات المصرفية، و هوية الجهاز الذى يستخدمه للاتصال عبر الشبكة، و بيانات الموقع الذى يتصل منه، و مواقع الإرسال و الاستقبال و هوية متلقى الاتصال، و قائمة الأسماء التى يتصل بها عادةً (قائمة المكالمات)، ووقت الاتصالات و مدتها، و التقنيات المستخدمة فى كل اتصال. كل هذا القدر الهائل من البيانات و بربطها معاً تعطى صورة دقيقة عن حياة المستخدم، و عاداته، و أماكن تواجده، و علاقاته الاجتماعية. و بالتالى فبيانات الاتصال هى بيانات حساسة للغاية لابد من أن يتم التعامل معها بحذر حفاظاً على حق

الإنسان فى خصوصية بياناته، الحق الذى كفلته المواثيق الدولية و الدساتير و التشريعات الوطنية كما سبق و أشرنا فى مبحثنا التمهيدى.

بيانات الاتصال إذن أو البيانات الوصفية (métadonnées) كما يطلق عليها البعض، هى البيانات التى تسمح بتوفير معلومات حول الوسيط الرقمى المتصل بالشبكة، دون التعرض لبيانات المحتوى التى تتضمن فحوى المحادثات و المراسلات الرقمية و المعلومات المتبادلة فيها. و لتقريب الأمر فإنه قياساً على الرسائل البريدية، فإن بيانات الاتصال تمثل البيانات المكتوبة على المظروف، بينما بيانات المحتوى هى البيانات التى تمثل مضمون الرسالة.[1]

و مع ذلك فبيانات الاتصال ليست كلها على ذات القدر من الخطورة على الحق فى الخصوصية، و لذا فقد تناولت محكمة العدل الأوروبية هذا الموضوع فى حكمها الصادر مؤخراً فى 6 أكتوبر 2020 و الذى صدر كرد على الاستفسارات المطروحة من مجلس الدولة الفرنسى فيما يتعلق بتفسير القانون الأوروبى ضمن هذا الإطار.

و قد انتهت محكمة العدل الأوروبية فى حكمها سالف الذكر إلى تصنيف بيانات الاتصال إلى ثلاث فئات من البيانات على النحو التالى:

أولاً: بيانات تحديد الهوية:

و تشمل البيانات التى تسمح بتحديد هوية المستخدم؛ كرقم الهاتف، أو رقم بطاقة (sim)، أو عنوان البريد الإلكترونى، و كذا (Ip) الخاص بالجهاز أو بروتوكول تعريف الجهاز على الشبكة، و يضاف إليها بيانات الحسابات و المدفوعات التى تتم عبر الشبكة. و هى الفئة الأقل خطورة ضمن بيانات الاتصال.[2]

ثانياً: بيانات الحركة (المرور):

و هى تلك المتعلقة بالوسيط الرقمى المتصل، و متلقى الاتصال، و بيانات مفصلة حول قائمة الاتصالات و مدة المكالمات و الأجهزة المستخدمة، و تاريخ الارسال و الاستقبال، و قائمة عناوين (ip) التى تم الرجوع إليها من عنوان ما، و قائمة الصفحات و المواقع التى تمت زيارتها على الشبكة.

---

[1]- Matthieu Audibert, L'enjeu de la conservation des données de connexion, Revue de la gendarmerie
Nationale , 2022,- numéro spécial Forum International de la cybersécurité 2022, 272, pp. 37-43. hal-03689580, p.2

[2]- Matthieu Audibert, L'enjeu de la conservation des données de connexion, Revue de la gendarmerie
Nationale , 2022,- numéro spécial Forum International de la cybersécurité 2022, 272, pp. 37-43. hal-03689580, p.2

ثالثاً: بيانات الموقع:

و هى تلك التى تشمل تحديد بيانات مناطق الارسال، و الاستقبال للاتصالات و تحديد الجهاز المتصل بواسطة برج الاتصالات التابع له.

و قد فرّقت المحكمة بين الفئة الأولى من البيانات من ناحية، و بين الفئتين الثانية و الثالثة من ناحية أخرى، حيث سمحت بالحفظ المعمم، و غير المتمايز لبيانات الفئة الأولى التى تشمل بيانات الحالة المدنية، و بروتوكول تعريف الجهاز على الشبكة، و كذا بيانات الحسابات البنكية و المدفوعات على الشبكة إذ أن هذه الفئة تشكل السبيل الوحيد للاستدلال، و التعرف على مرتكبى الجرائم على الانترنت و تتبعهم و ضبطهم، ما يعطى ضمانة هامة لحماية مستخدمى الشبكة من خطر استغلالهم عبرها، بالإضافة إلى أهمية التعرف على هوية كل مستخدم على الشبكة لتوقى ما قد يتهدد الأمن القومى من مخاطر محتملة.[1]

و قد انحاز مجلس الدولة الفرنسى لذات الموقف الذى تبنته محكمة العدل الأوروبية بالنسبة لبيانات تحديد الهوية فى حكمه الصادر بتاريخ 21 أبريل 2021 حيث جرى حكمه على أنه: " لا يجوز للحكومة أن تفرض على مشغلى خدمة الانترنت أو مزودى الخدمة، أو متعهدى الإيواء التخزين "الحفظ" المعمم و غير المتمايز للبيانات بخلاف بيانات الهوية المدنية، و عناوين IP بالإضافة إلى البيانات المتعلقة بالحسابات، و المدفوعات و ذلك بغرض مكافحة الجرائم و توقى الأخطار التى قد تهدد النظام العام، و دون إغفال لقانون الاتحاد الاوروبى فى هذا الشأن."[2]

أما فيما يتعلق بتخزين بيانات الحركة (المرور)، و بيانات الموقع فقد انتهجت محكمة العدل الأوروبية نهجاً آخر، فأوصت بضرورة إحاطة هذا التخزين بالعديد من القيود، و الضمانات؛ و هو ما نعرض له فى الفرع اللاحق.

---

[1] - CONSEIL d etat-COMMUNIQUÉ DE PRESSE, Données de connexion : le Conseil d'État concilie le respect du droit de l'Union européenne et l'efficacité de la lutte contre le terrorisme et la criminalité, Paris, le 21 avril 2021,p.1-2

[2] - *Commentaire Décision n° 2021-976/977 QPC du 25 février 2022 « M. Habib A. et autr », Question prioritaire de constitutionnalité portant sur les paragraphes II et III de l'article L. 34-1 du code des postes et des communications électroniques, Le Conseil constitutionnel, p.15*

الفرع الثانى

إشكالية تخزين بيانات المرور و الموقع

نتناول بداءةً موقف محكمة العدل الأوروبية من تقييد تخزين بيانات المرور و الموقع، و من ثم نعرض لموقف القضاء الفرنسى، و مدى تجاوبه مع توجيهات المحكمة.

الغصن الأول

الاتجاه الأوروبى لتقييد تخزين بيانات المرور و الموقع

تبنت محكمة العدل الأوروبية- كما أسلفنا- اتجاهاً جديداً ينحو إلى التقييد من إطار إلزام مشغلى الانترنت بتخزين بيانات الاتصال، لاسيما بيانات المرور، و الموقع بالنظر لما تتسم به من حساسية و خطورة كبيرة على حق الأفراد فى الخصوصية.

و تبدى ذلك من خلال سلسلة من الأحكام التى بدأت تصدر عن المحكمة منذ عام 2014، و تُوِّجَت مؤخراً بحكمين هامين للمحكمة أولهما كان حكمها الصادر فى 6 أكتوبر 2020[1]، و الذى جاء كرد على تساؤلات أولية طرحها مجلس الدولة الفرنسى على المحكمة، و ثانيهما كان حكمها الصادر فى 2 مارس 2021[2] و الذى جاء رداً على تساؤلات المحكمة العليا الإستوانية بشأن واقعة أُدين فيها المتهم بجرائم سرقات، و احتيال، و أعمال عنف على أساس تقارير مستمدة من بيانات الاتصال الإلكترونية الخاصة به، و التى حصل عليها المحققون بناء على إذن من المدعى العام، و كانت قد أخذت بها محكمة أول درجة، و أيدتها فى مسلكها محكمة الاستئناف، فطعن المحكوم عليه على الحكم الصادر ضده أمام المحكمة العليا مؤسساً طعنه على عدم مشروعية التقارير الحاوية لبيانات اتصال خاصة به، و عليه فقد أوقفت المحكمة العليا نظر الدعوى، موجهة ثلاثة تساؤلات أولية لمحكمة العدل الأوروبية مفادها:

1- هل من الملائم تفسير المادة 1/15 من التوجيه الأوروبى 2002/58 بصورة متوافقة مع المواد 7،8،11، 52 بحيث يمكن القول أن السماح للسلطات الوطنية فى إطار الإجراءات الجنائية (إجراءات مكافحة الجريمة) بالوصول لبيانات الاتصال لاسيما البيانات التى تحدد مصدر الاتصال، و اتجاهه، و تاريخه، و ساعته، و مدته، بالاضافة إلى تحديد موقع الجهاز المتصل إنما

[1] -CJUE, grande ch., Digital Rights Ireland, 8 avril 2014, C-293/12 et C-594/12 ; CJUE, grande ch., Tele2 Sverige et
a., 21 décembre 2016, C-203/15 et C-698/15 ; CJUE, grande ch. La Quadrature du Net et a., 6 octobre 2020, C-
511/18, C-512/18 et C-520/18

[2]- CJUE- affaire C-746/18-Arret du 2 mars 2021-H.K/PROKURATUUR.

يمثل انتهاكاً خطراً للضمانات الأساسية المكفولة للأفراد بموجب مواد التوجيه سالف الذكر؛ حيث يُفترض أن يكون الوصول لهذه البيانات الخاصة في إطار إجراءات ملاحقة الجرائم، و الكشف عن الجناة محدداً من حيث المدة التي يمكن للسلطات أن تصل فيها للبيانات المخزنة، و كذلك محدداً بدرجة خطورة معينة للجرائم محل الملاحقة؟

2- هل من الملائم تفسير المادة 15 فقرة (1) من التوجيه المذكور في ظل مبدأ التناسب المنصوص عليه بالبنود من 55 إلى57 من حكم 2 أكتوبر 2018، بمعنى أنه لابد أن يُنظر إلى كم البيانات و مدى أهميتها للكشف عن الجريمة للقول بمدى توافر الضرورة لانتهاك الحقوق الأساسية للشخص؟

3- هل ينبغي- طبقا للالتزام المنصوص عليه في البند الثاني من حكم 21 ديسمبر 2016 -أن يكون وصول السلطات للبيانات خاضعاً لرقابة مسبقة من سلطة قضائية أو إدارية مستقلة طبقاً للمادة 15-فقرة (1) من التوجيه؟[1]

ورداً على تلك التساؤلات فقد أصدرت المحكمة الأوروبية حكمها الذي قررت فيه **عدم مشروعية إلزام مشغلي الانترنت بالتخزين المعمم، و غير المتمايز للبيانات كقاعدة عامة، و ضرورة إخضاع جمع و تخزين البيانات لمبدأ التناسب و الضرورة كأحد المبادىء العامة الحاكمة لمشروعية معالجة البيانات**، و عليه فإن التشريعات الأوروبية الوطنية تعد مخالفة لقانون الاتحاد الأوروبي، و لذا وضعت المحكمة قيوداً على جمع و تخزين البيانات يمكن أن نبلورها فيما يلي:

1- أن يكون تخزين البيانات تبرره ضرورة قصوى:

و لا يكفي في القول بتوافر الضرورة أن يهدف التخزين للكشف عن الجرائم، و ملاحقة الجناة في أي نوع من الجرائم، ذلك أن الجرائم الخطرة وحدها هي التي تبيح هذا الانتهاك الصارخ لحق الإنسان في الخصوصية، لاسيما فيما يتعلق ببيانات الحركة (المرور)، و بيانات الموقع.

يُضاف إلى ذلك أن حالات الخطر الذي يهدد الأمن القومي للبلاد، و سواء كان حقيقياً أو محتملاً إنما يمثل ضرورة قصوى تسمح-استثناءً- بحفظ بيانات المرور و الموقع. و بالتالي فنصوص القوانين الوطنية التي تسمح بالتخزين المفتوح لبيانات الاتصال لا تتفق مع قانون الاتحاد الأوروبي لما يمثله ذلك من انتهاك

[1] - le capitaine Matthieu Audibert, la conservation et l'accès aux données techniques de connexion. Vers un nouveau paradigme pour les enquêtes judiciaires ?, Centre de recherche de l'ecole des officiers de la Gendarmerie nationale- Veille juridique n 94,p.18-19

لخصوصية المشتبه فيهم؛ و عليه فلا حجية للأدلة المتحصلة عن تخزين معمم للبيانات أمام القاضى الجنائى الوطنى.[1]

2- أن يكون التخزين متناسباً من حيث الكم، و النوع مع الهدف منه:

و يعنى ذلك أنه لابد أن تكون البيانات التى يتم جمعها، و حفظها من المرجح أن تسهم فعلاً فى إيضاح ملابسات جريمة خطرة، أو كشف غموض ما يمثل تهديداً للأمن القومى.

3- محدودية نطاق التخزين من الناحية الشخصية أو الجغرافية:

إذا كان التخزين-كما أسلفنا- يخضع لمبدأ الضرورة و التناسب، فإن ذلك ينبنى عليه بطبيعة الحال محدودية إطار التخزين من حيث الأشخاص، لذا اشترطت المحكمة إما أن يستهدف تخزين بيانات المرور و الموقع أشخاصاً بعينهم يكونون محل شبهة جنائية، أو يمثلون خطراً على الأمن القومى للبلاد، و ذلك فى الدول التى تواجه أخطار أو تهديدات لأمنها القومى سواء كانت أخطاراً فعلية أو محتملة.

أو أن يستهدف التخزين محيط منطقة جغرافية معينة، أو مناطق معينة من المحتمل أن تكون هدفاً إجرامياً، و ذلك وفقاً لاتفاقية بودابست 2001 حيث يكون للسلطات أن تطلب من مشغلى الانترنت حفظ بيانات الحركة و الموقع بصورة محدودة و لفترة قصيرة عن طريق التخزين السريع للبيانات أو conservation rapide des données"[2]"

4- محدودية نطاق التخزين من الناحية الزمنية:

يضاف إلى الشروط السابقة ضرورة أن يكون تخزين بيانات المرور و الموقع محدد بمدة زمنية قصيرة تتماشى مع الهدف منه، و مع مقتضيات الضرورة.

5- الرقابة السابقة على عمليات الجمع و التخزين من قبل سلطة مستقلة:

و مفاد هذا الشرط كما أوضحت المحكمة ضرورة الحصول على إذن مسبق من سلطة قضائية أو إدارية تتمتع بالاستقلال للقيام بأى عملية لجمع أو حفظ بيانات

[1] - le capitaine Matthieu Audibert, la conservation et l'accès aux données techniques de connexion. Vers un nouveau paradigme pour les enquêtes judiciaires ?, Centre de recherche de l'ecole des officiers de la Gendarmerie nationale- Veille juridique n 94,p.22,23

[2] - Conseil d'état -COMMUNIQUÉ DE PRESSE, Données de connexion : le Conseil d'État concilie le respect du droit de l'Union européenne et l'efficacité de la lutte contre le terrorisme et la criminalité, Paris, le 21 avril 2021,p.2

المرور، و الموقع. و قد اعتبرت المحكمة أن المدعى العام قد لا يمثل سلطة قضائية مستقلة بوصفه من يدير التحقيق الجنائى، و يحرك الدعوى الجنائية، و عليه فقد انتهت المحكمة إلى عدم مشروعية ما تضمنته التشريعات الوطنية للدول من تخويل السلطة فى طلب الافصاح عن بيانات الاتصال للمدعى العام.[1]

6- الفحص الدورى لمدى استمرار توافر الشروط السابقة فى عمليات الجمع، و التخزين لاسيما شرطى الضرورة و المحدودية.

أكدت المحكمة أيضاً على ضرورة أن تنص التشريعات الوطنية على إلزام السلطات العامة بإعادة تقييم دورية فى تواريخ منتظمة لمدى استمرار وجود خطر فعلى أو محتمل يهدد الأمن القومى بما يتطلب ضرورة تخزين بيانات المرور، و الموقع لأشخاص بعينهم أو فى مناطق جغرافية معينة.

و بوجه عام حتى فى حالات ضرورات الملاحقة الجنائية، فإنه لابد من الفحص الدورى لمدى ضرورة الإبقاء على إلزام مشغلى الانترنت بتخزين بيانات الاتصال الخاصة بمشتبه فيهم معينين.[2]

[1] - le capitaine Matthieu Audibert, la conservation et l'accès aux données techniques de connexion. Vers un nouveau paradigme pour les enquêtes judiciaires ?, Centre de recherche de l'ecole des officiers de la Gendarmerie nationale- Veille juridique n 94, p. 19

[2] - Dans quelles hypothèses des données de connexion peuvent elle faire l'objet d'une conservation? Le conseil d'état répond à cette question ; dans une décision du 21 avril 2021 ; Recherche publiée en ligne: https://www.village-justice.com/articles/donnees-connexion-quelles-sont-les-limites-leur-conservation,40314.html

الغصن الثانى

موقف القضاء الفرنسى من تقييد تخزين بيانات المرور و الموقع

أولاً: موقف مجلس الدولة الفرنسى:

بمناسبة فحص مدى توافق اللوائح الفرنسية مع متطلبات قانون الاتحاد الأوروبى فيما يتعلق بالتزام مشغلى الانترنت بالتخزين المعمم لبيانات الاتصال، أصدر مجلس الدولة الفرنسى حكمه بتاريخ 21 أبريل 2021 و الذى أكد فيه عدم تعارض التشريعات الفرنسية من حيث المبدأ مع قانون الاتحاد الأوروبى، و فى تفصيل ذلك جرى حكم المحكمة على أن: " قانون الاتحاد الأوروبى كما فسرته محكمة العدل الأوروبية لا يكفل حماية متوازنة للضمانات المتباينة؛ لاسيما فيما يتعلق بضمانة حماية الحقوق، و الحريات الأساسية للإنسان فى مواجهة ضمانة حماية الأمن العام، و مكافحة الجريمة، بينما دستور الدولة يفعل. و فى هذا الصدد فإن المتطلبات الدستورية المرتبطة بحماية المصالح الأساسية للدولة، و منع الاعتداء على النظام العام، و تأمين الأشخاص و الممتلكات، و مكافحة الإرهاب، و ملاحقة مرتكبى الجرائم لا تحظى بحماية كافية وفقا لقانون الاتحاد الأوروبى، مما يعنى ضرورة التحقق مما إذا كان تطبيق القانون الأوروبى كما تفسره محكمة العدل لا يضر بهذه المتطلبات الدستورية.

و عليه فإن للقاضى الإدارى إعفاء نفسه من بعض المتطلبات الناشئة عن قانون الاتحاد الأوروبى فى بعض الحالات، و إعطاء الأولوية للمتطلبات المنصوص عليها فى الدستور."[1]

و قد ذهبت المحكمة إلى التفرقة بصدد الإلزام بالتخزين المعمم، و غير المتمايز لبيانات المرور و الموقع بين التخزين لأغراض الأمن القومى، و التخزين لأغراض الملاحقة الجنائية لمرتكبى الجرائم؛ فاعتبرت أن التخزين المعمم لهذه البيانات لمدة عام واحد لأغراض حماية الأمن القومى لا يتعارض مع المعايير الأوروبية؛ نظراً لما تواجهه فرنسا من تهديدات جدية و حقيقية لأمنها القومى فى الوقت الراهن. شريطة أن تضاف ضمانة جديدة لهذا النوع من التخزين و هى ضرورة المراجعة، و التقييم الدورى للأخطار التى تتهدد الأمن القومى، و مدى تطلبها لبقاء هذا الإلزام.

بينما فيما يتعلق بالتخزين المعمم و غير المتمايز لبيانات الاتصال لأغراض مكافحة الجريمة و الملاحقة الجنائية للجناة فقد ارتأت المحكمة أنه لا يتماشى مع قانون الاتحاد الأوروبى وفقا لتفسير محكمة العدل الأوروبية، و مع ذلك فباعتبار كون هذا النوع من

[1]-Laure lands-Gronowski-Marie Miliotis, la conservation des données de connexion : un équilibre entre sécurité et vie privé délicat à trouver ; 16 june 2021, p.9

التخزين هو شرط حاسم أحياناً لنجاح التحقيقات التى يتم إجرائها، و هو الطريقة الوحيدة للعثور على مرتكبى الجرائم؛ فلا مانع من السماح بالتخزين الهادف و المحدود (غير المعمم) لهذه البيانات على أساس عناصر موضوعية، وفقاً لفئات الأشخاص المعنيين، أو عن طريق معيار جغرافى لفترة زمنية محددة، و فى إطار الضرورة القصوى التى تتمثل فى حالات الجرائم الخطرة.[1]

و مع ذلك فقد أشارت المحكمة إلى وجود صعوبات عملية، و تقنية قد تعيق الأخذ بالضمانات التى كرستها محكمة العدل الأوروبية فى مجال تقييد تخزين بيانات المرور و الموقع، يمكن بلورتها فى أربع صعوبات:

أ) غموض مفهوم الجريمة الخطرة:

قيدت محكمة العدل الأوروبية مشروعية تخزين بيانات المرور و الموقع بوصفها من بيانات الاتصال الحساسة بتوافر الضرورة، و ترجمت فكرة الضرورة فى إطار أغراض مكافحة الجريمة و ملاحقة الجناة، بلزوم كون الجريمة التى يجرى التحرى بشأنها عن طريق جمع و تخزين بيانات المرور الحساسة هى جريمة من الجرائم الخطرة، التى تبرر خطورتها هذا القدر من التعرض لحرمة الحياة الخاصة، و مع ذلك لم تحدد محكمة العدل بدقة مفهوم الجريمة الخطرة، و فى هذا الإطار عبّر مجلس الدولة فى حكمه عن ما مفاده أنه لو تبنينا معيار جسامة العقوبة فى تحديد مفهوم الجريمة الخطرة فإن ذلك سيعنى استبعاد العديد من الجنح المعاقب عليها بعقوبات غير جسيمة كالحبس الذى لا يجاوز عام أو عامين برغم خطورتها الفعلية، و ثمة قائمة طويلة جداً من الجنح التى ينطبق عليها هذا الوصف برغم بساطة عقوباتها- مقارنةً بالجنايات- من ذلك الجرائم الإلكترونية، و جرائم الاعتداء على حرمة الحياة الخاصة، و جرائم التحريض على العنف و الكراهية... فهل ينطبق وصف الخطورة على هذه الجرائم و مثيلاتها وفقاً لمحكمة العدل الأوروبية أم لا؟!

إن استبعاد هذا النوع من الجرائم من وصف الجريمة الخطرة إنما يعنى عدم إمكانية استخدام آليات جمع و تخزين بيانات المرور و الموقع فى مجال الاستدلال و التحقيق بشأنها، برغم الأهمية الجوهرية لهذه الوسائل فى إثبات هذه الجرائم مما سيؤثر مستقبلاً على فعالية وسائل التحقيق، و مدى إمكانية الكشف عن الجرائم و ملاحقة الجناه فيها.[2]

---

[1]- *Commentaire Décision n° 2021-976/977 QPC du 25 février 2022 « M. Habib A. et autr », Question prioritaire de constitutionnalité portant sur les paragraphes II et III de l'article L. 34-1 du code des postes et des communications électroniques, Le Conseil constitutionnel, p.12-13*

[2]- Matthieu Audibert, la conservation et l'accès aux données techniques de connexion. Vers un nouveau paradigme pour les enquêtes judiciaires ?, op.cit, p.27-28

ب) الاستحالة العملية المتعلقة بالتحديد المسبق لنطاق تخزين البيانات من حيث المناطق الجغرافية أو الأشخاص.

نوّه مجلس الدولة أيضاً إلى أنه من غير الممكن من الناحية العملية تحديد أو توقع المتورطين فى الجرائم أو المشتبه فيهم بصورة مسبقة بحيث يمكن قصر جمع و تخزين بيانات الاتصال عليهم، ناهيك عن أنه من المستحيل على جهات التحقيق أصلاً أن تعرف مقدماً البيانات التى هى بحاجة إليها لكشف الحقيقة بشأن جريمة معينة أو خطر محتمل، و نفس الشىء بالنسبة للتكهن بالمناطق الجغرافية التى يُحتمل أن ترتكب جريمة فى نطاقها،

و عليه فقد اقترح مجلس الدولة أن يتم الإبقاء على الجمع أو التخزين السريع (الآلى) للبيانات بصورة معممة و غير متمايزة (وفقاً لاتفاقية بودابست 2001)، بينما يتم تقييد وصول السلطات القضائية لهذه البيانات بضرورة توافر الشروط، و المعايير الأخرى التى حددتها محكمة العدل الأوروبية.[1]

ج) الالتزام بالرقابة المسبقة على عمليات التخزين من قبل سلطة مستقلة:

قررت المحكمة أن ربط مشروعية تخزين بيانات الاتصال الحساسة بصدور إذن مسبق من سلطة قضائية أو إدارية مستقلة إنما يقود إلى فوات الغرض من التخزين، بسبب الوقت الذى سيتطلبه الحصول على الإذن، و الذى قد يجرد عملية التخزين من قيمتها حيث سيستحيل حينئذٍ استعادة معلومات الاتصال بأثر رجعى (و التى لم يتم تخزينها)، و الحل الواقعى فى هذه الحالة هو السماح بالتخزين دون اشتراط الإذن المسبق، و جعل الرقابة المسبقة ضمانة قاصرة على الوصول للبيانات دون تخزينها، أو بعبارة أخرى ربط الحصول على البيانات و الوصول إليها بالإذن المسبق من سلطة قضائية أو إدارية مستقلة، بحيث يمكن الرجوع إلى البيانات التى تم حفظها بالفعل وفقاً لآلية الحفظ السريع للبيانات.[2]

و فيما يتعلق باستغلال البيانات المخزنة لحاجات أجهزة الاستخبارات لأغراض حماية الأمن القومى، فقد قررت المحكمة أنه لا يتوافق مع قانون الاتحاد الأوروبى لعدم توافر رقابة مسبقة على هذا النوع من المعالجة بواسطة هيئة مستقلة، لاسيما و أن الرقابة التى تباشرها اللجنة الوطنية لمراقبة تقنيات الاستخبارات ليست مما يحقق

[1]- Matthieu Audibert, L'enjeu de la conservation des données de connexion, Revue de la gendarmerie nationale, op.cit, p.3 -
[2]- Communique de presse, op.cit, p.2

معيار الرقابة الذى حددته محكمة العدل الأوروبية، إذ أن قرارات هذه الهيئة -خارج إطار حالات الطوارىء- لا تجاوز كونها توصيات غير ملزمة.[1]

د) المخاوف المتعلقة باستقرار الأوضاع:

تأكيداً على الدور الجوهرى الذى غدت تلعبه الأدلة الرقمية القائمة على حفظ بيانات الاتصال لاسيما البيانات المتعلقة بالأجهزة الطرفية المستخدمة فى المحادثات، و تواريخ الاتصالات و مواعيدها، و مددها، بيّنت المحكمة أنه فى عام 2020 فقط قام أكثر من 85 فى المائة من التحقيقات الجنائية على هذا النوع من الأدلة، أى حوالى اثنين و نصف مليون تحقيق قضائى تم اللجوء خلاله إلى مشغلى الاتصالات من أجل الكشف عن بيانات الاتصال الخاصة بالمشتبه فيهم، أو المتهمين و ذلك فى جرائم كالتحرش السيبرانى، و الانتقام الاباحى، و جرائم القتل، إضافة إلى نشر المحتويات غير المشروعة من محتوى إباحى أو محرض على الإرهاب.

مما يعنى أن التسليم اللاحق بعدم مشروعية هذه الأدلة إنما يهدد بهدم كافة التحقيقات السابقة، و ما ترتب عليها من أحكام إدانة، لذا قرر المجلس صراحةً أن ما تم من إجراءات لا مجال للطعن اللاحق عليه بعدم الدستورية.[2]

و إجمالاً فقد انتهى مجلس الدولة إلى عدم تعارض نصوص القانون الفرنسى المتعلقة بالإلزام بتخزين البيانات مع تفسير محكمة العدل لقانون الاتحاد الأوروبى من حيث المبدأ؛ و مع ذلك وجّه بضرورة تعديل النصوص التشريعية محل النزاع بإضافة ما كرّسه قضاء المحكمة الأوروبية من ضمانات لم تشتمل عليها؛ و حدد مهلة أقصاها ستة أشهر من تاريخ اعلام رئيس مجلس الوزراء بهذا الحكم الصادر فى 21 أبريل 2021 من أجل القيام بهذا التعديل.[3]

<u>ثانياً: موقف المجلس الدستورى الفرنسى:</u>

- **الإطار العام لرقابة المجلس الدستورى على مشروعية معالجة البيانات:**

منذ حكمه رقم 2012/652 الصادر فى 22 مارس 2012 و الذى انتهى فيه إلى مشروعية إنشاء ملف للبيانات البيومترية و الحالة المدنية للمواطنين [4]؛ دأب المجلس الدستورى الفرنسى على ربط مشروعية معالجة البيانات الشخصية، و تسجيلها، و

---

[1] - Laure lands-Gronowski-Marie Miliotis, op.cit, p.11

[2]- Matthieu Audibert, L'enjeu de la conservation des données de connexion, Revue de la gendarmerie nationale, op.cit, p.2 et suiv.

[3] - Laure lands-Gronowski-Marie Miliotis, op.cit, p.12

[4] - https://www.conseil-constitutionnel.fr/decision/2012/2012652DC.htm

حفظها، و فحصها، و نقلها بمدى خدمة ذلك للمصلحة العامة، و تنفيذه بما يتلاءم و يتناسب مع الهدف منه.

كما حرص المجلس فى إطار رقابة الملاءمة (الرقابة التناسبية) التى يباشرها على مشروعية عمليات معالجة البيانات أن يضع دائماً بعين الإعتبار العناصر الآتية:

- الأغراض المنشودة من حفظ البيانات
- طبيعة البيانات التى يتم جمعها
- حجم الملف
- خصائصه الفنية
- طرق حفظه
- المعلومات التى يتضمنها
- شروط فحص الملف و الاطلاع عليه

و عليه فقد سبق و قضى بعدم دستورية النصوص القانونية التى أنشأت سجلاً وطنياً لاعتمادات الأفراد يهدف إلى إدراج القروض الاستهلاكية التى حصل عليها الأِشخاص الطبيعيون لتلبية حاجات غير مهنية، و الذى يتضمن فضلاً عن ذلك المعلومات المتعلقة بحالات المديونية المفرطة و التصفيات القضائية. و علل المجلس موقفه هذا بقوله: " أن هذا السجل يهدف لجمع و تخزين بيانات دقيقة، و مفصلة لعدة سنوات تتعلق بعدد كبير من الأشخاص المدنيين الطبيعيين، و أنه يمكن الرجوع إليه فى مناسبات عديدة، و فى ظروف شديدة التنوع، و أن المؤسسات و المنظمات المالية مخولة باستخدام المعلومات التى تم جمعها، و لم يحدد المشرع بصورة حصرية عدد العاملين فى هذه المؤسسات الذين من المحتمل أن يسمح لهم بالرجوع إلى هذا السجل."[1]

كما سبق و أن قضى بعدم دستورية بعض ما تضمنته المادة230-8 من قانون الإجراءات الجنائية المتعلقة بإنشاء ملف "TAJ" الذى أُنشِىء لمعالجة البيانات الشخصية لمن تعرضوا لإدانات جنائية، و توقيع عقوبات أو تدابير أمنية، على أساس كون هذا الملف لا تقتصر معلوماته فقط على من خضعوا للعقوبات الجنائية، و إنما أيضاً من صدرت فى حقهم أحكام بالبراءة، أو قرارات بحفظ الواقعة، أو قرارات بألا وجه لإقامة الدعوى دون أية إمكانية فعالة لمحو بيانات هؤلاء الأشخاص. كما أكد المجلس على ضرورة تحديد مدة قصيرة فيما يتعلق بحفظ البيانات الجنائية للقُصّر بما

[1]- Décision n°2014-690 DC du 13 mars 2014-loi relative ala cosommation, cons. 53-57, voir : ***Commentaire Décision n° 2021-976/977 QPC du 25 février 2022 « M. Habib A. et autr », op.cit, p.19***

يحقق المواءمة بين ضرورة التعرف على القُصّر الجانحين من ناحية، و ضرورات السعي للتعافي المعنوي، و التربوي لهؤلاء القصّر.[1]

و كذا بعدم دستورية بعض أحكام المادة 154 من القانون المالي لعام 2020 و التي تسمح-على أساس تجريبي- و لمدة ثلاث سنوات لإدارتي الضرائب و الجمارك بجمع و معالجة البيانات الشخصية آلياً بطريقة تمكّن الجمهور من الوصول لهذه البيانات عبر المواقع الإلكترونية لبعض مشغلي الاتصالات لأغراض التحقيق في المخالفات الضريبية.[2]

و على النقيض من ذلك فقد قضى بدستورية إنشاء ملف للمواطنين الأجانب القاصرين غير المصحوبين بذويهم لتحقيق عدة أغراض[3]، كما قضى المجلس مؤخراً بدستورية الأحكام القانونية التي تنظم نقل البيانات الطبية المجمعة ضمن النظام الوطني للبيانات الصحية "SNDS" الذي نصت عليه المادة 11 من قانون546-2020 بهدف مكافحة وباء كوفيد-19

و الذي يتضمن بيانات الأشخاص المعرضين لخطر الإصابة و حالتهم الصحية، و على سبيل الاستثناء من مبدأ السرية الطبية يسمح بمعالجة البيانات، و مشاركتها عند الضرورة دون موافقة الأشخاص المعنيين، و يمّكن عدد كبير من المختصين في الرعاية الصحية من الوصول لهذه البيانات حال توافر الضرورة، مع العلم أن فترة الاحتفاظ بهذه البيانات قد تصل إلى عشرين عاماً. و قد تبنى المجلس هذا الموقف سعياً لتحقيق القيمة الدستورية المتعلقة بحماية الصحة العامة من خلال تحسين المعرفة بفيروس كوفيد-19 و آثاره طويلة المدى بهدف تعزيز وسائل مكافحته، كما أكد المجلس أن البيانات المنقولة داخل نظام "SNDS" تم وضعها بأسماء مستعارة لا تسمح بتحديد هوية أصحابها، و بذلك لم يغفل المشرع الحق في حماية الحياة الخاصة للمعنيين بالبيانات؛ حيث تمت معالجة البيانات لتأخذ شكل إحصائية مجمعة أو بيانات فردية على نحو يجعلها متاحة للجمهور مع استحالة تحديد هوية أصحابها لا بشكل مباشر، و لا غير مباشر. علاوة على كون الوصول للبيانات الكاملة يخضع

[1]- Décision n°2017-670 QPC du 27 octobre 2017, voir: https://www.sba-avocats.com/avocat-penaliste-effacement-fichier-taj-decision-du-conseil-constitutionnel-du-27-octobre-2017.html

[2]- Décision n°2019-796 DC du 27 decembre 2019; loi de finances pour 2020 ; voir : https://www.conseil-constitutionnel.fr/decision/2019/2019796DC.htm

[3] - ***Commentaire Décision n° 2021-976/977 QPC du 25 février 2022 « M. Habib A. et autr », op.cit, p.20***

لبروتوكلات السرية المهنية و سلامة البيانات المنصوص عليها فى قانون الصحة العامة.[1]

- **رقابة المجلس الدستورى على مشروعية تخزين بيانات الاتصال:**

و أخيراً فى إطار تعرضه لفحص دستورية المادة 1-34 من قانون البريد و الاتصالات الإلكترونية قضى المجلس فى حكمه الصادر بتاريخ 25 فبراير 2022 بأن بيانات الاتصال بشمولها لما يسمح بتحديد هوية الأشخاص و مواقعهم الجغرافية، و سجلات مكالماتهم،.. الخ، و نظراً لطبيعة المعالجة التى تخضع لها فإنها توفر قدراً كبيراً من المعلومات التى تمس الحياة الخاصة للأشخاص. لذلك فإنه بالرغم من كون حفظ هذه البيانات إنما يتم لأغراض مكافحة الجرائم، و حماية النظام العام و هى أغراض يكرسها الدستور؛ فإنه لابد من التحقق فى كل حالة من توافر التناسب بين الهدف المنشود، و بين احترام الحياة الخاصة. و هو ما لم يؤمّنه نص المادة المذكورة؛ حيث لم يكفل الضمانات الكافية للتحقق من هذا التناسب فى كل حالة، لاسيما و أن حفظ بيانات الاتصال يشمل كافة المستخدمين، كما أنه ينصب دون تمييز على كافة بيانات الاتصال مهما كانت طبيعتها أو خطورتها، و بغض النظر عن درجة خطورة الجرائم محل التحقيق.

إذن انتهى المجلس الدستورى إلى أن السماح بالاحتفاظ المعمم، و غير المتمايز ببيانات الاتصال إنما ينتهك حرمة الحياة الخاصة، و عليه فإن النص المطعون فيه يعدّ غير دستورى فيما لم يشتمل عليه من ضمانات. [2]

[1]- Décision n°2021-819 DC du 31 mai 2021 ; loi relative à la gestion de la sortie de crise sanitaire, voir : https://www.vie-publique.fr/loi/279666-loi-gestion-de-la-sortie-de-crise-sanitaire-etat-durgence-sanitaire

[2]- ***Commentaire Décision n° 2021-976/977 QPC du 25 février 2022 « M. Habib A. et autr », op.cit, p.30 et suiv.***

المطلب الثالث

جزاء مخالفة مشغلى الإنترنت الالتزام بتخزين بيانات الاتصال

عاقب المشرع الفرنسى على القيام بمعالجة البيانات الشخصية دون التقيد بالالتزامات الشكلية التى فرضها القانون للقيام بأيٍ من عمليات المعالجة بعقوبة السجن خمس سنوات و غرامة قدرها 300 ألف يورو، و ذلك سواء كان الاخلال بالالتزامات القانونية متعمداً أو عن طريق الإهمال.[1]

كما عاقب الأشخاص المعنوية المرتكبة لأى من الجرائم المنصوص عليها فى القانون بعقوبة الغرامة التى تساوى خمسة أضعاف الغرامة المعاقب بها الشخص الطبيعى عن نفس الجريمة، و إذا تعلق الأمر بجريمة لا يعاقب فيها الشخص الطبيعى بغرامة فإن الشخص المعنوى يتكبد غرامة تقدر بمليون يورو.[2]

و كذا تُوقع العقوبات التكميلية الوجوبية الآتية:

1- المنع بشكل دائم أو لمدة خمس سنوات على الأكثر من ممارسة النشاط.
2- الاستبعاد من العقود العامة بشكل دائم أو لمدة خمس سنوات على الأكثر.
3- المنع، لمدة خمس سنوات على الأكثر، من إصدار شيكات غير تلك التي تسمح للساحب بسحب الأموال من المسحوب عليه أو تلك المعتمدة أو من استخدام بطاقات الدفع.
4- عرض القرار الصادر أو نشره إما عن طريق الصحافة المكتوبة، أو بأية وسيلة تواصل أو نشر إلكترونية.[3]

أما فى القانون المصرى فيعاقب المشرع على الاخلال بالالتزام الخاص بحفظ البيانات بغرامة تتراوح بين خمسة و عشرة ملايين جنيه مصرى، و تُضاعف الغرامة فى حالة العود، و فى حالة العود للمحكمة أن تقضى أيضاً بإلغاء الترخيص الصادر للشخص (الطبيعى أو الاعتبارى) بمزاولة النشاط كعقوبة تكميلية جوازية.[4]

---

[1]- Art.226-16 de code pénal.

[2]- **Article 131-38 de code pénal.**

[3]- art.226-24 et art.131-39 de **code pénal.**

[4]- مادة 33 من قانون تقنية المعلومات – الفقرة الاولى منها؛ و نحيل فى تفصيلات العقوبات التبعية و التكميلية فى القانون المصرى إلى المطلب الثالث من المبحث الثانى.

المبحث الثانى

التزام مشغلى الإنترنت بإتاحة بيانات الاتصال للسلطات المختصة

فى إطار دراستنا لالتزام مشغلى الإنترنت بإتاحة بيانات الاتصال للسلطات المختصة، يلزمنا أن نتعرض أولاً لمضمون الالتزام بالإتاحة (الإفصاح) فى صورته التقليدية فى القانون الفرنسى، ثم للتعديلات التى طرأت عليه مؤخراً كنتيجة لصدور حكم المجلس الدستورى الفرنسى بعدم دستورية بعض العبارات التى وردت فى المواد القانونية المنظمة لهذا الالتزام؛ و ذلك فى سياق المقارنه بينه و بين مضمون الالتزام بالإتاحة فى القانون المصرى.

و عليه نقسّم هذا المبحث إلى مطلبين نعالج فى أولهما الالتزام بالإتاحة فى صورته التقليدية فى القانون الفرنسى مقارناً بالقانون المصرى، و فى الثانى نتناول الاتجاه المستحدث لتقييد الالتزام بإتاحة بيانات الاتصال.

المطلب الأول

مضمون التزام مشغلى الإنترنت بإتاحة بيانات الاتصال للجهات المختصة

يجد التزام مشغلى الانترنت بإتاحة بيانات الاتصال للجهات القضائية فى القانون الفرنسى مصدره فى المواد 60-1، 60-2، 77-1-1، 77-1-2، 99-3، 99-4 من قانون الإجراءات الجنائية الفرنسى، حيث يُلزم المشرع-فى إطار هذه المواد- أى شخص، أو مؤسسة، أو إدارة عامة أو خاصة بتسليم ما لديها من معلومات ذات أهمية للتحقيق القضائى، و ذلك بناءً على طلب من إحدى الجهات التالية:

1- المدعى العام (النائب العام)،
2- قاضى التحقيق.
3- مأمور الضبط القضائى بناء على تصريح من المدعى العام ، أو ندب من قاضى التحقيق.[1]
4- و كيل مأمور الضبط القضائى بناء على تصريح من المدعى العام و تحت اشراف مأمور الضبط القضائى.
5- مساعد التحقيق (و ذلك بإذن مسبق من المدعى العام، أو قاضى الحريات و الحبس عندما يتعلق الأمر بالتسجيلات فى أنظمة حماية الفيديو)

[1]- يُلاحظ أن صياغة المادة 1/60 تسمح بصدور طلب الاتاحة من مأمور الضبط القضائى دون إذن مسبق من المدعى العام على خلاف ما جرت عليه المادة 77-1-1 إجراءات.

و يشمل هذا الالتزام البيانات الرقمية أو الناتجة عن معالجة البيانات الشخصية، حيث يلتزم مشغلوا الانترنت بتقديم ما يتم طلبه من بيانات أياً كانت طبيعتها دون أن يكون لهم رفض إتاحة البيانات بدعوى إلتزام السرية المهنية إلا بالنسبة للأشخاص الذين شملتهم المادة 56 فى فقراتها من 1الى 5، و التى تتضمن الصحفيين، و المحامين، الأطباء، و كتاب العدل، و المحضرين، و العاملين فى القضاء، و عناصر الدفاع الوطنى؛ حيث لا يمكن تقديم أية بيانات تخصهم إلا بعد الحصول على موافقتهم على ذلك.[1]

و يجوز أن تصدر تصريحات المدعى العام فيما يتعلق بطلب إتاحة البيانات فى صورة تعليمات عامة تمتد فى الزمن بما لا يجاوز ستة أشهر، و ينطبق ذلك على الطلبات المتعلقة بأنواع معينة من البيانات التى تفيد فى كشف الحقيقة فى جناية أو جنحة معاقب عليها بالسجن، من ذلك طلبات الإتاحة المتعلقة ب:

أ- التسجيلات من نظام حماية الفيديو فيما يتعلق بالأماكن التي ارتكبت فيها الجريمة أو الأماكن التي يحتمل أن يتم العثور فيها على واحد أو أكثر من المشتبه فيهم بناءً على أسباب معقولة.
ب- الحسابات المصرفية التي يملكها شخص يوجد ضده سبب معقول أو أكثر للاشتباه في أنه ارتكب أو حاول ارتكاب جريمة، و كذلك بيانات رصيده.
ج- البيانات المتعلقة بالحالة المدنية ووثائق الهوية وتصاريح الإقامة المتعلقة بالشخص الذي يوجد ضده سبب معقول أو أكثر للاشتباه في أنه ارتكب أو حاول ارتكاب الجريمة.
د- البيانات المتعلقة بالقراءة الآلية للوحات الأرقام، عندما يتم ارتكاب الجريمة باستخدام مركبة ومن المرجح أن تتيح هذه البيانات تحديد مكان الشخص الذي يوجد ضده سبب معقول أو أكثر للاشتباه في أنه قام بارتكاب أو حاول ارتكاب الجريمة.[2]

نخلص مما سبق إلى أن الالتزام بالإتاحة وفقاً للقانون الفرنسى قبل عام 2022 كان التزاماً مطلقاً من حيث طبيعة، و نوع البيانات التى يلتزم مشغلو الانترنت بإتاحتها للسطات القضائية، حيث جاءت النصوص عامة فى الإلزام بتسليم كل ما يتوافر لدى مشغلى الإنترنت من معلومات ذات أهمية للتحقيق القضائى، و ذلك بناءً على طلب جهات التحقيق (قاضى التحقيق أو المدعى العام) أو مأمورى الضبط القضائى بتصريح من جهات التحقيق.

[1] - Art.77-1-1 et art.60-1 du code de procédure pénale (avant modification).
[2]- art.77-1-1 du code de procédure pénale (avant modification).

دون تقييد ذلك بأى شروط لا من حيث نوع البيانات أو درجة خطورتها، و لا من حيث نوع أو جسامة الجرائم المتطلب كشف الحقيقة فيها.

بينما فى القانون المصرى فقد جاء النص على التزام مشغلى الإنترنت بإتاحة بيانات الاتصال للجهات القضائية من خلال نص المادة (6) من قانون تقنية المعلومات، و الذى جرى على أنه: " لجهة التحقيق المختصة -بحسب الأحوال- أن تُصدر أمراً مسبباً لمأمورى الضبط القضائى المختصين، لمدة لا تزيد على ثلاثين يوماً قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة فى ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون، بواحد أو أكثر مما يلى:
1- ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات، وتتبعها فى أى مكان أو نظام أو برنامج أو دعامة إليكترونية أو حاسب تكون موجودة فيه، ويتم تسليم أدلتها الرقمية للجهة مصدرة الأمر على ألا يؤثر ذلك على استمرارية النظم وتقديم الخدمة أن كان لها مقتضى.

2- البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقا لغرض الضبط.
3- **أن تأمر مقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتى أو جهاز تقنى، موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمى خدمته وحركة الاتصالات التى تمت على ذلك النظام أو الجهاز التقنى**، وفى كل الأحوال يحب أن يكون أمر جهة التحقيق المختصة مسبباً. ويكون استئناف الأوامر المتقدمة أمام المحكمة الجنائية المختصة منعقدة فى غرفة المشورة فى المواعيد، ووفقا للإجراءات الجنائية."

و الملاحظ هنا أن الأصل فى صدور طلب الإتاحة أن يصدر فى صورة أمر قضائى مسبب لمدة ثلاثين يوماً، تصدره جهة التحقيق، و جهة التحقيق فى القانون المصرى هى النيابة العامة أو قاضى التحقيق، و لم يتطلب المشرع لصدور هذا الأمر أن تقوم جهة التحقيق باستصدار إذن أو تصريح من جهة أعلى لا من النائب العام و لا من القاضى الجزئى.

و كان المفترض فيما نرى- و قياساً على ما للنيابة العامة من سلطات بشأن ضبط الخطابات و المراسلات، و مراقبة المحادثات أو تسجيلها [1]- إلزام النيابة باستصدار إذن مسبب من القاضى الجزئى كإجراء سابق على إصدارها للأمر بتسليم البيانات، و ذلك من باب أولى حيث إن ما تسببه إتاحة البيانات الشخصية من مساس بحرمة الحياة

[1]- راجع المادة 206 (1) من قانون الإجراءات الجنائية 150 لسنة 1950.

الخاصة يساوى إن لم يكن يجاوز فى خطورته إفشاء سرية الرسائل و تسجيل المحادثات الخاصة.

لا سيما و أن البيانات التى يلتزم مقدمو الخدمة بإتاحتها لم يقيدها نص القانون بنوع أو بطبيعة معينة-كما هو الحال فى القانون الفرنسى قبل عام 2022- و بالتالى فهذا الالتزام يشمل كافة أنواع البيانات الشخصية بما فى ذلك بيانات حركة الاتصال (بيانات المرور) كما هو موضح صراحةً فى البند الثالث من المادة (6).

علاوة على ذلك فإن المشرع فى ذات القانون فى المادة (2) منه قد ألزم مقدمى الخدمة بأن يوفروا لأية جهة حكومية مختصة أى معلومات يُقدّر جهاز حماية المستهلك أهميتها لحماية مستخدمى الخدمة و يصدر بتحديدها قرار من الوزير المختص.

و كذا ألزمهم بأن يوفروا حال طلب جهات الأمن القومى، ووفقاً لاحتياجاتها كافة الإمكانيات الفنية التى تتيح لتلك الجهات ممارسة اختصاصاتها وفقاً للقانون.

و يُعد ذلك ترديداً لما نص عليه من قبل قانون تنظيم الاتصالات رقم 10 لسنة 2003 فى المادة (64) منه، و التى نصت على أنه: "يلتزم مشغلو ومقدمو خدمات الاتصالات والتابعون لهم وكذلك مستخدمو هذه الخدمات بعدم استخدام أية أجهزة لتشفير خدمات الاتصالات إلا بعد الحصول على موافقة من كل من الجهاز والقوات المسلحة وأجهزة الأمن القومي، ولا يسري ذلك على أجهزة التشفير الخاصة بالبث الإذاعي والتليفزيوني .ومع مراعاة حرمة الحياة الخاصة للمواطنين التي يحميها القانون يلتزم كل مشغل أو مقدم خدمة أن يوفر على نفقته داخل شبكة الاتصالات المرخص له بها كافة الإمكانيات الفنية من معدات ونظم وبرامج واتصالات داخل شبكة الاتصالات والتي تتيح للقوات المسلحة وأجهزة الأمن القومي ممارسة اختصاصها في حدود القانون، على أن يتزامن تقديم الخدمة مع توفير الإمكانيات الفنية المطلوبة..."

و الحق أن ورود صياغة هذه المواد بتلك الصورة الفضفاضة المعممة يفرغ الضمانة التى اشتملت عليها المادة (6) من قانون تقنية المعلومات من معناها، حيث يكون لأية جهة حكومية أن تطلب من مقدمى الخدمة إتاحة أى نوع من البيانات طالما أن ذلك مصرح به من قبل جهاز حماية المستهلك و البيانات محددة بقرار من الوزير المختص، أى أن لهذه الجهات التنفيذية ما للسلطة القضائية من حق فى الاطلاع على البيانات بموجب قيام هذه الأخيرة بواجبها فى استجلاء الحقائق حول الجرائم المرتكبة!!

و ينطبق نفس الشيء على جهات الأمن القومى التى جاء النص بشأن حقها فى الاطلاع على البيانات مطلقاً من أى قيد، فهل يكفى استهلال المشرع نصه الملزم فى كل مرة

بقوله "و مع مراعاة حرمة الحياة الخاصة للمواطنين التى يحميها القانون.." لكى يكون قد كرّس حقيقةً ضمانات حرمة الحياة الخاصة، و خصوصية البيانات؟! [1]

المطلب الثانى

الاتجاه لتقييد التزام مشغلى الانترنت بإتاحة بيانات الاتصال

تغيا الاتجاه لتقييد الالتزام بإتاحة بيانات الاتصال تحقيق أمرين؛ أولهما تقييد الإتاحة بحسب نوع البيانات، و قصر إتاحة الحسّاسة منها على حالات الضرورة الإجرائية، و الثانى: التقييد من ناحية السلطات المخولة بطلب الاطلاع على البيانات من خلال اشتراط رقابة مسبقة على طلب الإتاحة على أن تمارس هذه الرقابة سلطة خارجية لا علاقة لها بعملية التحقيق الجنائى؛

و فيا يلى نعرض لوجهى التقييد، كلٌ فى فرعٍ مستقل.

الفرع الأول

الاتجاه للتقييد الموضوعى للبيانات محل الإتاحة

كنتيجة للصياغة الفضفاضة، و المعممة للنصوص الإجرائية الملزمة لمشغلى الإنترنت بإتاحة بيانات الاتصال للجهات المختصة، تم الطعن على هذه النصوص لاسيما نص المادة 77-1-1، و 77-1-2 من قانون الإجراءات الفرنسى بعدم الدستورية أمام المجلس الدستورى الفرنسى الذى أصدر حكمه رقم 952-2021 فى الثالث من ديسمبر لعام 2021 بعدم دستورية هذه المواد فيما تضمنته من تعميم نصت عليه العبارة :"بما فى ذلك من البيانات الناتجة عن نظام معلوماتى أو معالجة بيانات شخصية." من المادة 77-1-1، و العبارة: " يكون للمدعى العام أو مأمور الضبط القضائى أو وكيله، بإذن من المدعى العام، أن ينفذ الطلبات المنصوص عليها بالفقرة الأولى من المادة 60-2 "..

و قرر المجلس ما مفاده أن عموم هذه العبارات إنما يعنى سلطة الجهات المذكورة فى طلب بيانات الاتصال بخصوص أية جريمة مهما كانت بسيطة، و دون مراعاة للضرورة التى تتلاءم مع خطورة إتاحة هذا النوع من البيانات على حق الأفراد فى حرمة الحياة الخاصة.

و اشتراط تلك المواد لضرورة صدور الطلب من المدعى العام أو قاضى التحقيق أو بناء على إذن من المدعى العام أو إنابة قضائية من قاضى التحقيق -و إن كان يشكل ضمانة هامة حيث يناط بهذه الجهات طبقاً للقانون تقدير مدى شرعية و تناسب

[1]- راجع المادة (2) من قانون تقنية المعلومات، و كذا المادة 64 من قانون تنظيم الاتصالات.

الإجراءات- إلا أنه بحد ذاته لا يعتبر ضمانة كافية؛ و عليه فقد قام المشرع الإجرائى بتعديل المواد المقضى بعدم دستوريتها من خلال قانون 299-2022، فأضاف بالمادة 12 منه مادة جديدة هى المادة 60-1-2 إجراءات و التى وضعت شروطاً صارمة لإتاحة البيانات الرقمية الحساسة للجهات القضائية؛ فاشترطت لطلب البيانات التقنية المتعلقة بحركة الاتصال، أو مصدر الاتصال، أو المعدات الطرفية المستخدمة أن تكون الجريمة التى يجرى التحقيق أو الاستدلال بشأنها إما:

1- جناية أو جنحة معاقب عليها بالسجن ثلاث سنوات على الأقل؛
2- أو جنحة من الجنح المرتكبة باستخدام شبكة اتصالات إلكترونية إذا كان معاقباً عليها بالسجن لمدة سنة واحدة على الأقل على أن يكون الغرض الوحيد من الطلب فى هذه الحالة هو تحديد هوية مرتكب الجريمة ليس إلا.
3- البحث عن شخص مفقود (فى إطار الإجراءات المنظمة لهذه المسألة).
4- إذا كان الطلب متعلقاً ببيانات المعدات الطرفية للمجنى عليه فلابد أن تتم الإتاحة بناءً على طلب من المجنى عليه نفسه، و فى حالة ارتكاب جريمة معاقب عليها بالسجن.[1]

و قيد المشرع كافة المواد المتعلقة بإلزام مشغلى الانترنت بإتاحة البيانات الرقمية للجهات القضائية كالمواد 77-1-1، 77-1-2 ، 60-1، 60-2 بضرورة مراعاة أحكام المادة الجديدة (60-1-2) من قانون الإجراءات الجنائية.[2]

و على ضوء ما سبق فإنه يمكن القول أن المشرع من خلال هذا التعديل قد حصّن بيانات الحركة، و الموقع من المساس بها فى صورة إتاحة الاطلاع عليها إلا إذا توافرت إحدى حالات الضرورة الأربع التى جاءت بها المادة المذكورة، و جدير بالإشارة هنا أن القيد ورد على طلب البيانات، و التمكين من الوصول إليها فى إطار إجراءات الاستدلال و التحقيق، و لم يرد على تخزين هذه البيانات و جمعها.

---

[1]- **Article 60-1-2 du code de procédure pénale, Création LOI n°2022-299 du 2 mars 2022 - art. 12, voir :**
https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000045289397

[2]- Sofian Goudjil, Juriste assistant, parquet général de la cour d'appel d'Angers, **Réquisition de données informatiques dans le cadre d'une information judiciaire : le régime est constitutionnel 8 juillet 2022 ,DALLOZ, Édition du 11 janvier 2024,P.4,5**

الفرع الثانى

الاتجاه للتقييد من حيث الجهات صاحبة السلطة فى طلب الإتاحة

(تفعيل الرقابة المسبقة)

أولاً: موقف محكمة العدل الأوروبية:

قررت محكمة العدل الأوروبية بدايةً من حكمها الصادر فى 21 ديسمبر 2016 مروراً بالأحكام اللاحقة عليه أنه: " وفقاً للمادة 15 فى فقرتها الأولى من توجيه 58 لعام 2002 و الذى تم تعديله بتوجيه 136 لعام 2009، مقروءاً فى ضوء المواد 11،8،7 بالإضافة للمادة 52 فقرة (1) من وثيقة الحقوق الأساسية، فإنه لابد لمشروعية طلب إتاحة بيانات الاتصال لاسيما بيانات المرور و الموقع من أن يخضع الطلب لرقابة مسبقة من قبل سلطة قضائية أو إدارية مستقلة."

و فى حكمها الصادر فى 2 مارس 2021 قدمت المحكمة توضيحات هامة فيما يتعلق بتفسير مفهوم استقلال السلطة القضائية أو الإدارية، و فى هذا السياق قررت أنه لكى نقول عن سلطة ما أنها مستقلة فلابد أن:

- تتمتع هذه السلطة بوضع الطرف الثالث بالنسبة للطرف الذى يطلب الوصول للبيانات، و الطرف المعنى بالبيانات كى تتمكن من ممارسة رقابتها بصورة محايدة، و موضوعية و غير متحيزة، و دون أية تأثيرات خارجية.[1]
- و مقتضى ذلك ألا تكون هذه السلطة مشاركة بأية صورة فى إجراءات التحقيق لكى يمكن القول أنها تتسم بالحياد تجاه أطراف الدعوى.[2]

و عليه فقد ارتأت المحكمة أن هذه الشروط لا تنطبق على "المدعى العام" حال قيامه بطلب إتاحة البيانات كونه طرفاً فى الدعوى الجنائية، و بالتالى لا يتوافر له الحياد و الاستقلال.

---

[1] -Cécile Crichton, **Précisions sur l'accès aux métadonnées lors du procès pénal, DALLOZ, Édition du 26 mars 2024**

[2]- Sofian Goudjil, Juriste assistant, parquet général de la cour d'appel d'Angers, **Réquisition de données informatiques dans le cadre d'une information judiciaire : le régime est constitutionnel 8 juillet 2022 , DALLOZ, Édition du 11 janvier 2024,P.5**

و إذا كان ذلك هو موقف محكمة العدل فيما يتعلق بالمدعى العام، فهل ينطبق ذات الموقف بالنسبة لقاضى التحقيق الذى يناط به تقدير مدى ملاءمة توجيه الاتهام و الإحالة إلى قضاء الحكم، و التى تعد من أعمال الملاحقة القضائية ؟

ثانياً: موقف المجلس الدستورى الفرنسى:

لم يتبن القضاة الدستوريون موقف محكمة العدل الأوروبية فى هذا الخصوص، فبالرجوع لحكم المجلس الدستورى رقم 952 لعام 2021 نجد أنه اعتبر أن صدور طلب الاتاحة من المدعى العام أو بناءً على تصريح من قبله يعد ضمانة هامة لهذا الإجراء لاسيما أن المدعى العام هو "رئيس الشرطة القضائية " magistrate de l'order judiciaire " و ذلك تطبيقاً للمادة 39-3 من قانون الإجراءات الجنائية، و التى يجرى نصها على أنه: "يجوز للمدعي العام، في إطار مسؤولياته كمدير للشرطة القضائية، أن يصدر تعليمات عامة أو خاصة للمحققين تحكم شرعية الوسائل التي تستخدمها هذه الأخيرة، وفقاً لمدى ملاءمة (تناسب) أعمال التحقيق لطبيعة الوقائع وخطورتها، والتوجيه المعطى للتحقيق فضلا عن جودته، ويتأكد من أن التحقيقات تهدف إلى كشف الحقيقة، وأن تتم بهدف الملاحقة والتبرئة، فى ظل احترام حقوق الضحية والشاكي والمشتبه به." [1]

يستفاد من ذلك أن المدعى العام وفقاً لاختصاصه الأصيل فى قانون الإجراءات الفرنسى هو المنوط به تقدير مشروعية الوسائل، و الإجراءات المستخدمة فى الاستدلال، و بالتالى فشرط الرقابة المسبقة من سلطة قضائية مستقلة على مشروعية طلب إتاحة البيانات يعد متحققاً فى حال كون الطلب مقدم من المدعى العام أو بناءً على إذن منه.[2]

و من باب أولى تعتبر ضمانة الرقابة المسبقة من سلطة مستقلة متحققة فيما إذا كان طلب إتاحة البيانات مقدم من قاضى التحقيق أو بناءً على تفويض منه، و هو ما قرره المجلس الدستورى مؤخراً فى حكمه الصادر 17يونيو 2022 [3] رداً على الطعن فى دستورية المادتين 99-3، 99-4 من قانون الإجراءات، و اللتان تنصان على سلطة قاضى التحقيق فى طلب المعلومات من مختلف الجهات لاسيما البيانات الإلكترونية من مشغلى الانترنت بالقيود المنصوص عليها فى المادة 60-1-2 السالف ذكرها.

---

[1] - https://incyber.org/article/decision-n-2021-952-qpc-du-3-decembre-2021-m-omar-y/

[2]- Sofian Goudjil, Juriste assistant, parquet général de la cour d'appel d'Angers, **Réquisition de données informatiques dans le cadre d'une information judiciaire : le régime est constitutionnel 8 juillet 2022 ,DALLOZ, Édition du 11 janvier 2024,P.4,5.**

[3]- **Décision n° 2022-1000 QPC du 17 juin 2022 , https://www.conseil constitutionnel.fr/decision/2022/20221000QPC.htm**

و قد أكد المجلس الدستورى أن قاضى التحقيق يتمتع بوضع يضمن له الاستقلال الكامل، و أن الضمانات التى تتيحها المواد المطعون فيها تكفى لتوفير الرقابة القضائية الصارمة على طلب إتاحة البيانات، و أنها على نحو ما سبق لا تتعارض مع الدستور، و لا مع التوجيهات الأوروبية التى تشترط الرقابة المسبقة من سلطة مستقلة.[1]

و الحاصل إذن أن المجلس الدستورى رفض الانصياع لنظرة محكمة العدل الأوروبية لا فيما يتعلق بشرط الرقابة المسبقة على طلب إتاحة البيانات، و إنما فيما يتعلق بتفسير المحكمة لهذا الشرط.

المطلب الثالث

مخالفة مشغلى الإنترنت للالتزام بإتاحة بيانات الاتصال

- **تمهيد و تقسيم:**

قد تتخذ مخالفة الالتزام بإتاحة بيانات الاتصال للسلطات المختصة إحدى صورتين؛ إما صورة سلبية تتمثل فى الامتناع عن إتاحة بيانات الاتصال للجهات المختصة بالاطلاع عليها وفقاً للقانون، أو صورة إيجابية تتحقق بإتاحة البيانات للجهات المختصة فى غير الأحوال، و بغير القيود التى حددها القانون للاطلاع. و عليه نعرض لكلا الصورتين فى فرعين متعاقبين.

[1] - Baptiste Nicaud, **Restrictions à la conservation des données de connexions et à leur accès : la Cour de cassation tire les conséquences de la jurisprudence de la CJUE , DALLOZ, 26 Mars 2024, https://www.dalloz-actualite.fr/flash/restrictions-conservation-des-donnees-de-connexions-et-leur-acces-cour-de-cassation-tire-conse**

الفرع الأول

الامتناع عن إتاحة البيانات و التستر على مخالفة القانون

(الصورة السلبية)

يشكل رفض الاستجابة للالتزام الذى وضعه القانون على مشغلى الانترنت، أو مقدمى الخدمة جريمة جنائية لا تتحقق إلا بتوفر ركنيها المادى و المعنوى كما حددهما النموذج القانونى لها، و بتوافرهما تتحقق المسئولية الجنائية لمقدم الخدمة أو المشغل. و يمكن تفصيل الحديث حول هذه النقاط فى غصون ثلاثة على نحو ما يلى:

الغصن الأول

الركن المادى لجريمة الامتناع عن إتاحة البيانات للجهات المختصة

تقوم جريمة الامتناع عن إتاحة البيانات على السلوك السلبى المتمثل فى الامتناع ؛ و لكى يتحقق الركن المادى لجريمة الامتناع عن إتاحة البيانات فلابد أن يصدر الامتناع عن أحد الأشخاص المكلفين بالالتزام أو مقدمى الخدمة؛ و الذين هم مزودى خدمات الاتصال أو متعهدى الوصول بصفة أساسية و متعهدى الإيواء بصفة ثانوية، و هم جميعا من الأشخاص المعنوية فى غالب الأحوال؛ كما أنه لابد أن تتوافر مواصفات معينة فى طلب إتاحة البيانات يمكن بلورتها فى عنصرين:

<u>أولاً: من حيث الجهة المتقدمة بطلب الإتاحة:</u>

لابد لكى يتحقق الامتناع المجرم جنائياً من قبل المشغل أو مقدم الخدمة أن يكون طلب إتاحة بيانات الاتصال مقدماً من جهة من الجهات المختصة بالاطلاع على البيانات وفقاً للقانون؛ و التى تقتصر فى القانون الفرنسى على المدعى العام، و قاضى التحقيق، و مأمور الضبط القضائى بناءً على إذن المدعى العام أو تفويض قضائى من قاضى التحقيق؛ و كذا وكيل مأمور الضبط القضائى تحت إشراف مأمور الضبط و بإذن من المدعى العام، أو مساعد التحقيق فى الحالات الخاصة المنصوص عليها بالمادة 77-1-1 سالفة الذكر.

أما فى القانون المصرى فتتعدد الجهات التى يمكنها طلب إتاحة بيانات الاتصال، و ذلك على نحو ما يلى:

1- جهة التحقيق المختصة: و الأصل أن جهة التحقيق فى القانون المصرى هى النيابة العامة، و فى بعض الحالات قد يقوم بالتحقيق قاضى التحقيق أو مستشار التحقيق [1]، و

[1]- راجع المواد 64، 65 من قانون الإجراءات الجنائية.

لجهة التحقيق-بصفة أصلية- أن تطلب البيانات من مشغلى خدمات الإنترنت، كما أن لمأمور الضبط القضائى بناءً على أمر مسبب من جهة التحقيق أن يتقدم بطلب الإتاحة، و يصدر الأمر لمدة لا تزيد عن ثلاثين يوماً، قابلة للتجديد مرة واحدة فقط من قبل سلطة التحقيق.[1]

مع ملاحظة أنه لكى يصدر الأمر المسبب صحيحاً لمأمور الضبط القضائى، فإنه يتعين أن يكون لهذا الإجراء فائدة فى كشف الحقيقة بخصوص الجريمة محل التحقيق، و مفاد ذلك ضرورة توافر قرائن ترجح تمخض الإجراء (الكشف عن البيانات) عن أدلة تفيد فى كشف الحقيقة فيما يخص الجريمة محل التحقيق و إلا كان الأمر باطلاً، و كذا الأدلة التى سيسفر عنها الاطلاع على بيانات الاتصال.

2- الجهات الحكومية:

توسعت المادة (2) من قانون تقنية المعلومات فى منح سلطة طلب إتاحة البيانات الإلكترونية الشخصية، فأوجبت على مقدم الخدمة أن يوفر لأية جهة حكومية مختصة، و كذا لمستخدمى خدماته مجموعة من البيانات المسماة هى؛ اسم مقدم الخدمة، و عنوانه، و معلومات الاتصال المتعلقة بمقدم الخدمة، بما فى ذلك عنوان الاتصال الإلكترونى، و بيانات الترخيص، و الجهة المختصة التى يخضع لاشرافها.

و لكن بالإضافة إلى ذلك ألزمت مقدم الخدمة بتقديم أى معلومات يقدّر جهاز حماية المستهلك أهميتها لحماية مستخدمى الخدمة، على أن يصدر بتحديدها قرار من الوزير المختص.

و الأرجح أن القانون هنا لم يقصد إلزام مقدم الخدمة بتقديم بيانات الاتصال الخاصة بمستخدمى خدماته، و غاية ما هنالك أنه قصد إلزامه بتقديم بياناته المفصلة للجهات الحكومية المختصة، و مع ذلك فالطريقة الفضفاضة التى صيغت بها الفقرة ثانياً من المادة (2) من القانون قد تفتح الباب أمام التعدى على خصوصية البيانات باسم حماية مستخدمى الإنترنت.

3- جهات الأمن القومى:

يوجب المشرع فى الفقرة ثالثاً من المادة (2) سالفة الذكر على مقدمى الخدمة توفير كافة الإمكانيات الفنية التى تتيح لجهات الأمن القومى ممارسة اختصاصاتها، و يفهم من ذلك بالضرورة أن لهذه الجهات طلب ما تشاء من البيانات دون الرجوع للجهات القضائية، و جهات الأمن القومى كما تم تعريفها فى المادة (1) من القانون هى:

[1]- مادة (6) من قانون تقنية المعلومات لعام 2018

- رئاسة الجمهورية
- وزارة الدفاع
- وزارة الداخلية
- المخابرات العامة
- هيئة الرقابة الإدارية

و ما قيل بالنسبة للفقرة ثانياً يُقال أيضاً بالنسبة للفقرة ثالثاً من المادة (2) حيث تُطالعنا ذات الصياغة الفضفاضة التى لا تضع قيوداً موضوعية، أو إجرائية كافية ما يعرّض حرمة الحياة الخاصة لخطر الانتهاك، و لا يغض من ذلك ما استُهلت به الفقرة ثالثاً بقولها: " مع مراعاة حرمة الحياة الخاصة التى يكفلها الدستور"؛ حيث إن مراعاة حرمة الحياة الخاصة ليست التزاماً مرسلاً على عاتق جهات الأمن القومى، و إنما هى التزام يقع على عاتق المشرع بتفعيل الضمانات الدستورية بواسطة نصوص القانون، و إلا وُصمت هذه النصوص بالعوار الدستورى، و هو ما نعتقد بتوافره فى حالة الفقرة ثانياً و ثالثاً من المادة (2) من قانون تقنية المعلومات كونها تتيح لغير الجهات القضائية، و فى غير ظروف التحقيق القضائى إتاحة البيانات الخاصة بجمهور مستخدمى الانترنت لاسيما بيانات الاتصال لمجموعة كبيرة من الجهات الإدارية و الأمنية دون ضوابط أو قيود محددة ما يمثل انتهاكاً للدستور الذى يقرر فى المادة 57 منه أن: "للحياة الخاصة حرمة، وهى مصونة لا تمس. وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائى مسبب، ولمدة محددة، وفى الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين فى استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفى، وينظم القانون ذلك."

ثانياً: محل طلب الإتاحة:

لكى تعتبر جريمة الامتناع عن الاستجابة لطلب إتاحة البيانات متحققة فلابد أن تكون البيانات محل الطلب مما يحق للجهة الطالبة أن تحصل عليه، و بالرجوع للنصوص الفرنسية نجد أنه لسلطات التحقيق السابق ذكرها طلب كافة أنواع البيانات فيما عدا:

أ) البيانات الخاصة بإحدى الفئات المستثناه بموجب المادة 56 (من فقرة 1 الى فقرة 5) السالف الإشارة إليها، حيث لا يجوز تقديم بيانات هذه الفئات إلا بموافقة أصحابها.[1]

[1]- الفئات المقصودة تتضمن الصحفيين، و المحامين، الأطباء، و كتاب العدل، و المحضرين، و العاملين فى القضاء، و عناصر الدفاع الوطنى؛ حيث لا يمكن تقديم أية بيانات تخصهم إلا بعد الحصول على موافقتهم على ذلك.

ب) بيانات حركة الاتصال، و الموقع الخاص بأى انسان إلا إذا توافرت الضوابط التى حددتها المادة 60-1-2 و التى تتطلب جسامة خاصة للجريمة محل التحقيق أو حالات خاصة.[1]

ج) البيانات الكاشفة عن المصدر الصحفى، حيث إنه لا يجوز أن تمثل الاستجابة لطلب إتاحة البيانات كشفاً عن أحد المصادر الصحفية إلا فى حالات الضرورة القصوى، و ذلك وفقاً لما تضمنته المادة (2) من قانون الصحافة الفرنسى، و التى جاء فيها: "... لا يجوز تقويض سرية المصادر لا بشكل مباشر و لا غير مباشر إلا إذا كانت الضرورة القصوى للمصلحة العامة تبرر ذلك، وإذا كانت التدابير المتوخاة ضرورية للغاية ومتناسبة مع الهدف المشروع المنشود. ولا يمكن بأي حال من الأحوال إلزام الصحفي بالكشف عن مصادره. و يعد انتهاكاً غير مباشر لسرية مصادر الصحفى عملية السعي لاكتشاف مصادر الصحفي عن طريق التحقيقات المتعلقة بأي شخص قد يكون لديه بحكم علاقاته المعتادة مع الصحفي معلومات لتحديد هذه المصادر. و فى إطار الإجراءات الجنائية لابد أن يؤخذ بعين الاعتبار تقييم جسامة أو خطورة الجريمة محل الإجراء، و أهمية المعلومات المطلوبة لقمع هذه الجريمة أو منعها، و مدى أهمية تدابير التحقيق المتوخاة فى الكشف عن الحقيقة."[2]

أما فى إطار القانون المصرى فلم يضع المشرع أى قيد على حق الجهات المختصة فى طلب إتاحة البيانات الشخصية، حيث نجد النصوص قد جاءت عامة شاملة لكافة أنواع البيانات، فمن ناحية ألزم المشرع مقدمى الخدمة بتقديم كافة الإمكانات الفنية لجهات الأمن القومى لممارسة اختصاصاتها [3]، و من ناحية أخرى تضمنت المادة (6) تحديداً لفئات البيانات التى يلتزم مقدمو الخدمة بتقديمها لجهات التحقيق فقررت أنه لجهة التحقيق: " أن تأمر مقدم الخدمة بتقديم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتى، أو جهاز تقنى موجودة تحت سيطرته أو مخزنة

---

[1]- و قد اشترطت المادة 60-1-2 إجراءات –كما سبق الذكر-لطلب البيانات التقنية المتعلقة بحركة الاتصال، أو مصدر الاتصال، أو المعدات الطرفية المستخدمة أن تكون الجريمة التى يجرى التحقيق أو الاستدلال بشأنها إما:

1- جناية أو جنحة معاقب عليها بالسجن ثلاث سنوات على الأقل؛
2- أو جنحة من الجنح المرتكبة باستخدام شبكة اتصالات إلكترونية إذا كان معاقباً عليها بالسجن لمدة سنة واحدة على الأقل على أن يكون الغرض الوحيد من الطلب فى هذه الحالة هو تحديد هوية مرتكب الجريمة ليس إلا.
3- البحث عن شخص مفقود (فى إطار الإجراءات المنظمة لهذه المسألة).
4- إذا كان الطلب متعلقاً ببيانات المعدات الطرفية للمجنى عليه فلابد أن تتم الإتاحة بناءً على طلب من المجنى عليه نفسه، و فى حالة ارتكاب جريمة معاقب عليها بالسجن.

[2]- art.2 de la Loi du 29 juillet 1881 sur la liberté de la presse, Modifié par LOI n°2010-1 du 4 janvier 2010 - art. 1 (V)

[3]- المادة (2) البند ثالثاً من قانون تقنية المعلومات المصرى.

لديه، و كذا بيانات مستخدمى خدمته، و حركة الاتصالات التى تمت على ذلك النظام أو النظام التقنى."

مما يعنى أنه لا توجد أية بيانات مستثناه من الالتزام بالإتاحة لجهات التحقيق، أو جهات الأمن القومى، فالمشغل يلتزم بتقديم ما لديه من معلومات أو بيانات للجهات المختصة دون قيود اللهم إلا القيود الإجرائية للأمر؛ و التى تتصل بضرورة صدوره مسبباً، و يتعلق ببيانات تفيد فى كشف الحقيقة عن الجريمة محل التحقيق، و هو ما لا يناط تقييمه بالمشغل أو مقدم الخدمة، بل بجهات التحقيق ذاتها تحت رقابة قاضى الموضوع بطبيعة الحال.

و يلاحظ أن المشرع لم يحدد لا فى القانون الفرنسى، و لا فى نظيره المصرى مدة معينة للوفاء بالالتزام بتقديم البيانات المطلوبة حتى يعتبر الامتناع بفوات هذه المدة محققاً للركن المادى للجريمة؛ و بالتالى مرتباً للمسئولية الجنائية لمقدم الخدمة. و هو ما يعتبر قصوراً فى النص يستوجب التدخل التشريعى لتلافيه.

و إلحاقاً بهذا التجريم فقد جرم المشرع فعل الامتناع عن الإبلاغ عن أى جريمة مما نُص عليه فى قانون تقنية المعلومات إذا صدر هذا الامتناع عن شخص مسئول عن الإدارة الفعلية للشخص الاعتبارى.[1]

[1]- مادة 35 من قانون تقنية المعلومات.

الغصن الثانى

الركن المعنوى لجريمة الامتناع عن إتاحة البيانات للجهات المختصة

لم يتناول نص التجريم صراحةً صورة الركن المعنوى المتطلب لقيام هذه الجريمة، و المرجح لدينا أن المشرع يسوّى فى قيام الجريمة بين القصد الجنائى و الخطأ، بحيث إنه إذا لم يثبت ارتكاب الامتناع عمداً فإن الفعل المرتكب يكون خطئياً، و فى هذه الحالة يعتبر الخطأ مفترضاً فى حق المخالف للالتزام كتطبيق لصورة الخطأ الخاص الذى يكفى لتوافره مجرد مخالفة التزام قانونى، و افتراض الخطأ قرينة قانونية بسيطة قابلة لإثبات العكس.[1]

و مفاد افتراض الخطأ نقل عبء إثبات الخطأ من جهة الادعاء إلى المتهم، فعلى المتهم إثبات انعدام الخطأ فى حقه، و ذلك لتوافر ظرف معين خارج عن إرادته أدى إلى استحالة وفاءه بالالتزام بإتاحة البيانات؛ كحدوث قوة قاهرة حالت دون قدرته على حفظ البيانات بسبب أعطال تقنية غير متوقعة، أو حالت دون قدرته على استعادة البيانات المحفوظة و تقديمها فى مدى زمنى ملائم للجهات المختصة.

و تمتنع المسئولية الجنائية للمخالف -بطبيعة الحال- إذا توافر سبب مشروع لرفض تقديم البيانات، و لا يكاد يُتصور هذا الفرض إلا فى إطار القانون الفرنسى حيث نطاق البيانات المسموح بتقديمها للجهات المختصة أكثر تحديدا بمقتضى النصوص التشريعية؛ من ذلك حالة طلب بيانات الاتصال الخاصة بطبيب أو محامى أو صحفى، حيث لا يجوز تقديم هذه البيانات لجهات التحقيق إلا بموافقة أصحابها؛ أو حالة طلب بيانات تكشف عن مصدر صحفى.

[1]- قد يرى البعض أن هذه الجريمة تمثل إحدى نماذج الجريمة المادية، التى لا يتطلب القانون لقيامها ركناً معنوى و إنما يكفى فيها توافر الركن المادى، و لا نذهب من ناحيتنا إلى ترجيح هذه النظرة إذ لا نؤمن بإمكان توافر مسئولية جنائية لا تقوم على الخطأ (فى صورته العامة-الإثم الجنائى).

الغصن الثالث

الجزاء الجنائى لمخالفة الالتزام بإتاحة البيانات

يعاقَب على مخالفة الالتزام بالإتاحة فى القانون الفرنسى بعقوبة أصلية واحدة هى الغرامة التى تقدر ب 3750 يورو، و ذلك أيا كانت الجهة الطالبة للبيانات؛ فالعقوبة واحدة فى حالة رفض طلب مقدَّم من المدعى العام أو من ينوب عنه، أو من قاضى التحقيق أو من يفوضه.

بينما يعاقب القانون المصرى على مخالفة الالتزام بإتاحة البيانات بمجموعة متنوعة من العقوبات يمكن تقسيمها على نحو ما يلى:

أولاً: العقوبات الأصلية:

- **عقوبات توقع على الشخص الطبيعى:**

تتباين عقوبات الامتناع عن إتاحة البيانات بحسب الجهة التى تم رفض طلبها أو امتُنِع عن الاستجابة له؛ فإذا كان الامتناع قد انصب على طلب صادر من جهة تحقيق فإن العقوبة المقررة تكون هى الحبس الذى حده الأدنى ستة أشهر و حده الأقصى ثلاث سنوات، بالإضافة إلى الغرامة التى لا تقل عن عشرين ألف جنيه و لا تجاوز مائة ألف جنيه.أو يُكتفى بإحدى هاتين العقوبتين، أى الحبس أو الغرامة.

أما إذا انصب الامتناع على طلب مقدم من إحدى الجهات الحكومية المختصة (بصدد البيانات الخاصة بمقدم الخدمة نفسه) تكون العقوبة هى الغرامة التى حدها الأدنى عشرين ألف جنيه و الأقصى مائتى ألف جنيه.

و أخيراً إذا تمثلت المخالفة المرتكبة فى عدم تمكين جهات الأمن القومى من آداء واجباتها سواء بعدم توفير الإمكانات الفنية أو البيانات المطلوبة فإن العقوبة هى الحبس الذى حده الأدنى ثلاثة أشهر و الأقصى ثلاث سنوات، بالإضافة إلى الغرامة التى لا تقل عن مائتى ألف جنيه و لا تجاوز مليون جنيه.

و يلاحظ أن العقوبة فى هذه الحالة أشد من العقوبات فى الحالتين السابقتين حيث لا مجال للاختيار بين الحبس و الغرامة و إنما يحكم بهما معاً، كما أن الحد الأقصى للغرامة يصل إلى أعلى حد له و هو مليون جنيه توقع على مقدم الخدمة المخالف.

و يُعاقب على الشروع فى هذه الجرائم بما لا يجاوز نصف الحد الأقصى للعقوبات المقررة.

و قد وضع المشرع ظرفاً مشدداً عاماً لكل الجرائم الواردة فى قانون تقنية المعلومات يقضى بتشديد العقوبات المقررة فى القانون المذكور لتصل إلى السجن المشدد فى حالة توافر قصد خاص لدى الجانى يتمثل فى الإخلال بالنظام العام، أو تعريض سلامة المجتمع و أمنه للخطر، أو الاضرار بالأمن القومى للبلاد أو بمركزها الاقتصادى، أو منع أو عرقلة ممارسة السلطات العامة لأعمالها أو تعطيل أحكام الدستور أو القوانين أو اللوائح أو الإضرار بالوحدة الوطنية و السلام الاجتماعى.

و يجدر بالملاحظة أن القصد الخاص كظرف مشدد لجرائم قانون تقنية المعلومات يتصف بالإبهام و الغموض لاسيما فى شقه الخاص بغرض " تعطيل أحكام الدستور أو القوانين أو اللوائح"؛ فإذا كان تحقق هذا القصد الخاص كافياً لتحويل العقوبات الأصلية للجرائم من عقوبات الجنح (الحبس و الغرامة) إلى عقوبة مقررة أصلاً للجنايات (السجن المشدد) فإن الأمر -فيما نرى- يستدعى إعادة النظر فى طريقة صياغة هذا الظرف المشدد ليكون أكثر وضوحاً و تحديداً.[1]

- **عقوبات توقع على الشخص المعنوى:**

قرر قانون تقنية المعلومات صراحةً مسئولية الشخص المعنوى عن كافة الجرائم المتضمنة فيه؛ فعاقب المسئول عن الإدارة الفعلية للشخص المعنوى بذات عقوبات الفاعل الأصلى إذا ارتكب المسئول أى من الجرائم السابق الإشارة إليها باسم و لحساب الشخص المعنوى، أو حتى سهّل ارتكابها للغير.

بل إن عدم اشتراك المسئول عن الإدارة الفعلية للشخص المعنوى فى ارتكاب الجريمة المرتكبة لحساب الشخص المعنوى يعرّضه للمسئولية الجنائية إذا توافر علمه بأن الجريمة تُرتكب، و لم يقم بإبلاغ الجهات الرسمية المختصة حال علمه بذلك، و يعاقب بذات عقوبة الفاعل الأصلى.[2]

فإذا كانت الجريمة التى تستر على حدوثها مُرتكبة لا لحساب الشخص المعنوى الذى يديره و إنما ضد النظام المعلوماتى المخصص للكيان الذى يديره؛ فتكون العقوبة هى الحبس مدة لا تقل عن ثلاثة أشهر، و الغرامة لا تقل عن ثلاثين ألف جنيه، و لا تجاوز مائة ألف جنيه أو إحدى هاتين العقوبتين.[3]

و على ضوء ما سبق يتبين لنا أن القانون يقرر مسئولية المسئول عن الإدارة الفعلية للشخص المعنوى عن الجرائم المرتكبة لحسابه دون أن يرتب ذلك استبعاد المسئولية

---

[1]- المادة 34 من قانون تقنية المعلومات 175 لسنة 2018

[2]- مادة 36 من قانون تقنية المعلومات 175 لسنة 2018

[3]- مادة 35 من قانون تقنية المعلومات 175 لسنة 2018

الجنائية للأشخاص الطبيعيين مرتكبى الجرائم سواء كانوا فاعلين أو شركاء.[1] و لا يفترض ذلك-بطبيعة الحال- عقاب شخص واحد عن ذات الفعل مرتين إذا كان الفاعل هو نفسه المسئول عن الإدارة الفعلية للشخص المعنوى تطبيقا للمبادىء الدستورية فى هذا الشأن.[2]

ثانياً: العقوبات التكميلية:

1- العقوبات التكميلية الوجوبية:

أ) المصادرة:

تُعد عقوبة المصادرة عقوبة تكميلية وجوبية على المحكمة أن تقضى بها متى قضت بالإدانة، و ذلك فى أية جريمة من الجرائم المنصوص عليها فى قانون تقنية المعلومات، و محل المصادرة هو الأدوات أو المعدات، أو الأجهزة التى لا يجيز القانون حيازتها، أو تلك التى تكون قد استخدمت فى ارتكاب الجريمة، أو سهّلت ارتكابها[3]، و كون المصادرة عقوبة تكميلية وجوبية يعنى أن خلو حكم الإدانة منها يجعل الحكم معيباً مستوجباً للطعن عليه بالطرق المقررة فى القانون، و فى كل الأحوال لا يجوز تنفيذ المصادرة إلا إذا تضمنها الحكم القضائى تطبيقاً لما قررته المادة 40 من الدستور.[4]

ب) الغلق:

توقع عقوبة الغلق على الشخص الاعتبارى الذى وقعت منه إحدى جرائم تقنية المعلومات، إذا لم يكن قد حصل على ترخيص بمزاولة نشاطه فى الحالات التى يوجب فيها القانون الحصول على ترخيص لمزاولة النشاط ، و يعد الغلق فى هذه الحالة عقوبة وجوبية أيضاً.[5]

ج) نشر الحكم:

نص القانون على نشر حكم الإدانة كعقوبة تكميلية وجوبية، و يكون النشر على نفقة الشخص الاعتبارى المدان فى جريدتين يوميتين واسعتى الانتشار.[6]

---

[1]- و هو ما ينعته البعض –خروجاً على مقتضيات الدقة- بازدواج المسئولية الجنائية.

[2]- حكم المحكمة الدستورية العليا رقم 3 لسنة 10 دستورية، https://egyls.com/

[3]- مادة 38 من قانون تقنية المعلومات 175 لعام 2018.

[4]- جاء فى المادة 40 من الدستور أن: "المصادرة العامة للأموال محظورة، و لا تجوز المصادرة الخاصة إلا بحكم قضائى."

[5]- مادة 36 من قانون 175 لعام 2018.

[6]- مادة 38 من قانون تقنية المعلومات 175 لعام 2018.

2- العقوبات التكميلية الجوازية:

أ) العزل:

يُعتبر العزل عقوبة تكميلية جوازية يكون للمحكمة توقيعها على الجانى إذا توافرت فيه صفة الموظف العام، و لم يوضح القانون مفهوم الموظف العام فى إطار تطبيقه و هل المقصود بالموظف العام هنا الموظف العام بمفهوم القانون الإدارى، أم الموظف العام بمعناه الواسع فى القانون الجنائى كما فى جرائم الوظيفة العامة و جرائم المال العام؟ (1)

و يُشترط لتوقيع عقوبة العزل أن تكون الجريمة قد ارتكبت من الموظف العام أثناء تأدية وظيفته أو بسببها. و العزل فى هذه الحالة مؤقت، و لم يحدد المشرع مدته و إنما ترك تحديدها لسلطة القاضى التقديرية.

و يتحول العزل لعقوبة تكميلية وجوبية إذا ارتكبت الجريمة لغرض من الأغراض المنصوص عليها فى المادة 34 من قانون تقنية المعلومات أى فى حالة توافر ظرف التشديد سابق الذكر. و العزل فى حالة توافر ظرف التشديد و إن كان وجوبياً إلا أن المشرع لم يجعله عزلاً دائماً فى هذه الحالة!

ب) ايقاف الترخيص:

للمحكمة أن تقضى بإيقاف ترخيص مزاولة الشخص الاعتبارى لنشاطه مدة لا تجاوز سنة كعقوبة تكميلية جوازية فى حالة ارتكابه لإحدى جرائم تقنية المعلومات، و فى حالة العود لها أن تحكم بإلغاء الترخيص أو حل الشخص الاعتبارى.

رابعاً: الإعفاء من العقاب:

قررت المادة 41 اعفاءً وجوبياً للفاعل أو الشريك الذى يبلغ عن الجريمة قبل علم السلطات بها. و قررت اعفاءً جوازياً من العقاب إذا أبلغ الفاعل أو الشريك عن الجريمة بعد كشف السلطات للجريمة و ذلك إذا توافرت شروط محددة هى:

أ) أن يتم الإبلاغ قبل التصرف فى التحقيق، (و المقصود قبل الإحالة للمحاكمة)
ب) أن يمكن هذا الابلاغ السلطات من القبض على مرتكبى الجريمة الآخرين، أو أن يمكن هذا الابلاغ من ضبط الأموال موضوع الجريمة، أو أن يفيد فى كشف الحقيقة فى الجريمة محل التحقيق أو فى القبض على مرتكبى جريمة أخرى مماثلة لها فى النوع و الخطورة.

[1]- راجع المواد 111، 119 من قانون العقوبات المصرى.

و فى كل الأحوال لابد من القضاء برد أية أموال متحصلة عن جريمة من جرائم تقنية المعلومات. و قد أجاز القانون الصلح فى جرائم تقنية المعلومات فى أى حالة كانت عليها الدعوى قبل صيرورة الحكم باتاً بالشروط التى تضمنتها المادة 42 من القانون المذكور.[1]

الفرع الثانى

إتاحة بيانات الاتصال بالمخالفة للقانون

إذا كان إعراض مشغلى الانترنت عن تنفيذ الالتزام بإتاحة البيانات الشخصية -لاسيما بيانات الاتصال- للجهات التى نص عليها القانون يجعلهم مسئولين جنائياً، فإن قيام مشغلى الانترنت بإتاحة هذه البيانات لغير الجهات المختصة إنما يشكل جريمة إفشاء للبيانات، كما أن إتاحتها البيانات للجهات المختصة خروجاً على الشروط التى حددها القانون، أو فى غير الأحوال المصرح بها قانوناً يجعل الدليل المستمد من هذه البيانات دليلاً باطلاً.

أولاً: إتاحة البيانات لغير الجهات المختصة:

يعاقب قانون العقوبات الفرنسى على فعل إتاحة البيانات الشخصية لغير الجهات التى حددها القانون، و دون رضاء الشخص المعنى بالبيانات بالسجن لمدة خمس سنوات، و غرامة قدرها 300 ألف يورو و ذلك إذا كان الإفشاء متعمداً، أما فى حال ما إذا تم إفشاء البيانات للغير بصورة غير عمدية، كما لو حدث نتيجة إهمال من معالج البيانات فإن العقوبة فى هذه الحالة تكون هى السجن ثلاث سنوات، و غرامة قدرها 100 ألف يورو.[2]

---

[1]-" يجوز للمتهم فى أية حالة كانت عليها الدعوى الجنائية، وقبل صيرورة الحكم باتا،إثبات الصلح مع المجنى عليه أو وكيله الخاص أو خلفه العام، أمام النيابة العامة أو المحكمة المختصة بحسب الأحوال، وذلك فى الجنح المنصوص عليها فى المواد (14، 15، 16،17، 18، 19، 23، 26، 28، 30، 31) من هذا القانون. ولا يُنتج إقرار المجنى عليه بالصلح المنصوص عليه بالفقرة السابقة أثره إلا باعتماده من الجهاز بالنسبة للجنح
المنصوص عليها بالمواد (14، 17، 18، 23) من هذا القانون. كما لا يُقبل التصالح إلا من خلال الجهاز بخصوص الجنح المنصوص عليها بالمادتين (29، 35) من هذا القانون ولا يسقط حق المتهم فى التصالح برفع الدعوى الجنائية إلى المحكمة المختصة إذا دفع ثلثى الحد الأقصى للغرامة المقررة للجريمة أو قيمة الحد الأدنى أيهما أكثر، وذلك قبل صدور حكم نهائى فى الموضوع. وفى جميع الأحوال، يجب على المتهم الذى يرغب فى التصالح أن يسدد قبل رفع الدعوى الجنائية مبلغًا يعادل = =ضعف الحد الأقصى للغرامة المقررة للجريمة. ويكون السداد إلى خزانة المحكمة المختصة أو النيابة العامة بحسب الأحوال. ويترتب على الصلح انقضاء الدعوى الجنائية، ولا أثر للصلح على حقوق المضرور من الجريمة أو على الدعوى المدنية."

[2] -Article 226-22,de code penal « Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 () JORF 7 août 2004"

كما يعاقب القانون المصرى لحماية البيانات على فعل إفشاء البيانات الشخصية فى المادة (36) منه بالغرامة التى لا تقل عن مائة ألف جنيه، ولا تجاوز مليون جنيه حيث يجرى نص المادة على تقرير هذه العقوبة ل" كل حائز أو متحكم أو معالج جمع أو عالج أو أفشى أو أتاح أو تداول بيانات شخصية معالجة الكترونيا بأية وسيلة من الوسائل في غير الأحوال المصرح بها قانونا أو بدون موافقة الشخص المعني بالبيانات.."

و تتعاظم جسامة العقوبة فى حالة توافر العمد المقترن بقصد خاص يتمثل فى ارتكاب جريمة الإفشاء بغرض الحصول على منفعة مادية أو أدبية، أو بغرض تعريض الشخص المعنى بالبيانات للخطر[1]؛ فى هذه الأحوال تكون العقوبة هى الحبس الذى حده الأدنى ستة أشهر، و تتضاعف الغرامة لتتراوح بين مائتي ألف و مليوني جنيه، و يكون للقاضى إما الحكم بالحبس و الغرامة معاً أو اختيار إحدى العقوبتين.

و جدير بالبيان هنا أنه يكفى لتحقق القصد الخاص أن تتجه إرادة الفاعل إلى الحصول على المنفعة أو تعريض المجنى عليه للخطر دون أن تتحقق هذه النتائج فعلياً.

ثانياً: إتاحة البيانات للجهات المختصة دون التقيد بالشروط القانونية للإتاحة: (البطلان الإجرائى)

و تفترض هذه الصورة أن مشغل الانترنت أو مقدم الخدمة يستجيب لطلب إتاحة البيانات المقدم من إحدى الجهات المصرح لها قانوناً بالحصول على البيانات، و لكن فى غير الحالات أو بغير الشروط التى قيد بها القانون مشروعية هذا الطلب.[2]

و ليس من المُتصور من الناحية الواقعية أن مشغل الإنترنت سيمارس أى نوع من الرقابة على مشروعية طلب الإتاحة من حيث استيفائه للشروط القانونية طالما أنه قد تم تقديمه من جهة مصرح لها بطلب البيانات.[3]؛ و عليه لا يُتصور قيام المسئولية الجنائية لمشغل الإنترنت لعدم تحققه من توافر الشروط القانونية فى طلب الإتاحة، إذ أن القانون يخاطب بهذه الشروط-بصفة أصلية- الجهات المصرح لها بطلب البيانات و

---

[1]- يلاحظ أن الخطر المقصود هنا ليس بالضرورة الخطر المتعلق بالحياة أو السلامة البدنية، فقد يكون الخطر متمثلاً فى المساس بالسمعة أو غير ذلك من الأخطار المعنوية التى قد تهدد بضرر يصيب الشخص نتيجة إفشاء بياناته الشخصية.

[2]- كما فى حالة اتاحة بيانات المرور فى القانون الفرنسى فى غير الجرائم و الحالات التى وضعتها المادة 60-1-2 سالفة الذكر.

[3]- بعض الشركات الكبرى قد تمارس هذا النوع من الرقابة بل و بصورة متعنتة؛ من ذلك حالة رفض شركة (أبل) طلبا من المباحث الفيدرالية (FBI) باختراق جهاز أحد منفذي هجوم سان بيرناردينو بدعوى كون هذه الخطوة تهدد أمن المستخدمين:

https://arabic.cnn.com/world/2016/02/17/apple-fbi-request

الاطلاع عليها، و بالتالى فإن عدم تقيد هذه الأخيرة بتلك الشروط لا جزاء له إلا بطلان الأدلة المبنية على إتاحة غير مشروعة للبيانات الشخصية لاسيما بيانات الاتصال.

و قد قررت محكمة النقض الفرنسية فى هذا الإطار أنه:

" يناط بمحكمة الموضوع متى أتيحت لها وسيلة التحقق أن تتأكد من توافر العناصر الواقعية التى تبرر الحاجة لمثل هذا الإجراء (طلب إتاحة البيانات)؛ من ذلك استيفاء معيار خطورة الجريمة محل التحقيق، و كون التخزين التلقائى (السريع) لبيانات المرور و الموقع و إتاحة هذه البيانات إنما يحترم حدود ما هو ضرورى للغاية."[1]

كما قررت أن: "الأصل أن تقدير مشروعية الإجراء منوط أولاً: بغرفة التحقيق التى عليها أن تستوثق من كون الإجراء لا يمثل انتهاكاً غير مبرر لحرمة الحياة الخاصة، و أنه روعيت فى اتخاذه الشروط التى حددها القانون. و مفاد ذلك أنه على غرفة التحقيق التأكد من توافر الآتى:

1- أن الوصول تم بالنسبة لبيانات تُخزن تلقائيا و بانتظام.
2- أن البيانات المطلوبة من فئة البيانات المسموح بإتاحتها وفقاً للقانون.
3- أن الوصول للبيانات قد تم بمناسبة، و فى التوقيت الذى كان يجرى فيه التحقيق فى الواقعة، و فى الإطار الذى تبيحه ضرورات التحقيق.

و فى كل الأحوال فإن القانون الفرنسى-كما تقرر النقض- يوفر الضمانات الكافية للطعن فى الأدلة الناتجة عن اساءة استعمال البيانات الشخصية."[2]

و على ضوء ذلك، يمكن القول أن رقابة قاضى الموضوع على الأدلة الناجمة عن تخزين أو إتاحة غير مشروعة للبيانات هى رقابة استبعاد؛ حيث إن القاضى الجنائى ملزم باستبعاد كافة المعلومات، و الأدلة التى تم الحصول عليها بطريق من طرق التخزين المعمم، و غير المتمايز لبيانات المرور، و الموقع كفئة حساسة من فئات بيانات الاتصال، كونها أدلة غير مشروعة وفقاً للقانون؛ لاسيما حين لا يكون من

[1]- Cour de cassation - Chambre criminelle — 12 juillet 2022 - n° 21-83.710, n° 21-83.820, n° 21-84.096, et n° 20-86.652.

[2]- Baptiste Nicaud, **Restrictions à la conservation des données de connexions et à leur accès : la Cour de cassation tire les conséquences de la jurisprudence de la CJUE , DALLOZ, 26 Mars 2024, https://www.dalloz-actualite.fr/flash/restrictions-conservation-des-donnees-de-connexions-et-leur-acces-cour-de-cassation-tire-conse**

الممكن للشخص المعنى بالبيانات (المشتبه فيه) الدفاع بفاعلية ضد هذه المعلومات، و الأدلة مما يُرجح أن يكون لهذه الأدلة تأثير طاغى على تقييم وقائع الدعوى.[1]

نخلص مما سبق إلى أنه من الصعوبة بمكان مساءلة مشغل الانترنت عن إفشاء البيانات الشخصية فى حالة إتاحتها لجهة مختصة خروجاً على الشروط التى يقررها القانون للإتاحة لأنه لا رقابة للمشغل على مبررات الجهة طالبة البيانات، و إنما الجزاء الوحيد المتصور فى هذه الحالة هو بطلان الأدلة الناجمة عن الإجراء غير المشروع؛ حيث يفقد الدليل قيمته الثبوتيه، و هو الأمر الذى يخضع لتقدير غرفة التحقيق تحت رقابة محكمة الموضوع.

و قد أحسن المشرع المصرى إذ صاغ صراحةً شروط حجية الأدلة الرقمية فى المادة (9) من اللائحة التنفيذية لقانون مكافحة جرائم تقنية المعلومات الصادرة بقرار رئيس مجلس الوزراء رقم 1699 لعام 2020، و إن كان الأوفق ورود هذه الشروط فى صلب القانون نفسه؛ و قد جرى نص المادة المذكورة على أنه: " تحوز الأدلة الرقمية ذات القيمة والحجية للأدلة الجنائية المادية في الإثبات الجنائى إذا توافرت فيها الشروط والضوابط الآتية:

أ) أن تتم عملية جمع أو الحصول أو استخراج أو استنباط الأدلة الرقمية محل الواقعة باستخدام التقنيات التى تضمن عدم تغيير أو تحديث أو محو أو تحريف للكتابة أو البيانات والمعلومات ، أو أى تغيير أو تحديث أو إتلاف للأجهزة أو المعدات أو البيانات والمعلومات ، أو أنظمة المعلومات أو البرامج أو الدعامات الالكترونية وغيرها. ومنها على الأخص تقنية Digital Images Hash، Write Blocker، وغيرها من التقنيات المماثلة.

ب) أن تكون الأدلة الرقمية ذات صلة بالواقعة وفي إطار الموضوع المطلوب إثباته أو نفيه ، وفقًا لنطاق قرار جهة التحقيق أو المحكمة المختصة.

ج) أن يتم جمع الدليل الرقمى واستخراجه وحفظه وتحريزه بمعرفة مأمورى الضبط القضائى المخول لهم التعامل في هذه النوعية من الأدلة ، أو الخبراء أو المتخصصين المنتدبين من جهات التحقيق أو المحاكمة ، على أن يبين في محاضر الضبط ، أو التقارير الفنية على نوع ومواصفات البرامج والأدوات والأجهزة والمعدات التى تم استخدامها ، مع توثيق كود وخوارزم Hash الناتج عن استخراج نسخ مماثلة ومطابقة للأصل من الدليل الرقمى بمحضر

[1]- **Cour de cassation, Chambre criminelle, 25 octobre 2022, 21-87.397, Publié au bulletin, https://justice.pappers.fr/decision/df9e7d732700544777291de761e14723**

الضبط أو تقرير الفحص الفنى ، مع ضمان استمرار الحفاظ على الأصل دون عبث به.

خ) في حالة تعذر فحص نسخة الدليل الرقمى وعدم إمكانية التحفظ على الأجهزة محل الفحص لأى سبب يتم فحص الأصل ويثبت ذلك كله في محضر الضبط أو تقرير الفحص والتحليل.

د) أن يتم توثيق الأدلة الرقمية بمحضر إجراءات من قبل المختص قبل عمليات الفحص والتحليل له وكذا توثيق مكان ضبطه ومكان حفظه ومكان التعامل معه ومواصفاته. "

كما تضمنت المادة (10) تحديداً مفصلاً لكيفية توصيف، و توثيق الدليل الرقمى، ما يعطى قاضى الموضوع سلطة الرقابة على توافر هذه الضوابط و الاشتراطات فى الدليل الرقمى المقدم فى الدعوى، فإذا جاء الدليل مخالفاً لهذه الضوابط كان مهدراً و فاقداً لكل حجية أمام القضاء.[1]

[1]- نصت المادة 10 من اللائحة التنفيذية لقانون تقنية المعلومات على أنه: **"يتم توصيف وتوثيق الدليل الرقمى من خلال طباعة نسخ من الملفات المخزن عليها أو تصويرها بأى وسيلة مرئية أو رقمية ، واعتمادها من الأشخاص القائمين على جمع أو استخراج أو الحصول أو التحليل للأدلة الرقمية ، مع تدوين البيانات التالية على كل منها:**

-تاريخ ووقت الطباعة و التصوير.

-اسم وتوقيع الشخص الذى قام بالطباعة و التصوير.

-اسم أو نوع نظام التشغيل ورقم الإصدار الخاص به.

-اسم البرنامج ونوع الإصدار أو الأوامر المستعملة لإعداد النسخ.

-البيانات والمعلومات الخاصة بمحتوى الدليل المضبوط.

-بيانات الأجهزة والمعدات والبرامج والأدوات المستخدمة. "

خاتمة

سيظل تحديد أُطر الحقوق و الحريات الإنسانية محلاً للجدل المحتدم، و اختلاف الرؤى ما بقيت القوانين الوضعية قائمة، و ذلك سعياً لتحقيق غايةٍ صعبة المنال هى خلق التوازن الأمثل بين الحقوق و الحريات بأنواعها من ناحية، و بينها جميعاً و بين المصالح الاجتماعية الأخرى من ناحية ثانية.

و فى إطار بحثنا هذا حاولنا بدورنا دراسة مدى إمكانية تحقيق التوازن بين حق الأفراد فى خصوصية البيانات كمظهر من مظاهر حرمة الحياة الخاصة، و بين مصلحة الدولة و المجتمع فى الأمن و الاستقرار من خلال استغلال البيانات الرقمية الشخصية لاسيما بيانات الاتصال فى الملاحقة الجنائية لمرتكبى الجرائم. و قد انتهينا من خلال دراستنا للقوانين الحاكمة للبيانات و نظم تقنية المعلومات على مستوى الاتحاد الأوروبى، و كذا القوانين الوطنية فى مصر و فرنسا إلى ما يلى:

- **النتائج:**

1- وضع المشرع المصرى مؤخرا قانون رقم 151 لعام 2020 لحماية البيانات الشخصية، و لكن مما يؤسف له أن هذا القانون و إن دخل حيز النفاذ فإنه لم يتم تفعيله على أرض الواقع لعدم صدور لائحته التنفيذية حتى الآن، و بالتالى عدم انشاء مركز حماية البيانات الذى ناط به القانون العديد من الالتزامات التى يتوقف عليها تنفيذه، مثل إصدار تراخيص و تصريحات معالجة البيانات، و الرقابة على مشروعية عمليات المعالجة.

2- اشتمل القانون على بعض جوانب القصور فى حماية البيانات الشخصية من بينها تعدد الاستثناءات التى تخرج عن نطاق تطبيق أحكام هذا القانون، من ذلك البيانات التى يتم جمعها لأغراض احصائية أو اعلامية، و البيانات الشخصية المتعلقة بمحاضر الضبط و الدعاوى القضائية، و كذا البيانات الشخصية لدى جهات الأمن القومى، و لدى البنك المركزى و الجهات الخاضعة لرقابته و اشرافه.

3- لم ينظم قانون حماية البيانات المصرى الحق فى الإلغاء من محركات البحث كأحد آليات الحق فى النسيان الرقمى.

4- يقع الالتزام بالتخزين، و الإفصاح عن البيانات الشخصية فى التشريعين المصرى و الفرنسى على عاتق مقدمى خدمات تقنية المعلومات (مشغلى الانترنت)؛ و الذين هم متعهدى الوصول- بصفة أصلية- و متعهدى الإيواء دون غيرهم من المتدخلين فى عمليات بث و نقل المحتوى الإلكترونى.

5- مرّ الالتزام بتخزين البيانات الشخصية فى القانون الفرنسى بمرحلتين؛ ما قبل عام 2022، و ما بعده؛ حيث كانت إجازة تخزين البيانات الشخصية قبل 2022 تتضمن احتفاظ مشغلى خدمات الاتصالات، و بالأخص مزودى خدمات الاتصالات الإلكترونية (متعهدى الوصول) بكافة بيانات الاتصال عدا بيانات فحوى الاتصال أو المراسلات الإلكترونية، و ذلك لمدة أقصاها عام واحد من تاريخ الاتصال لأغراض الكشف عن الجرائم الجنائية و ملاحقتها. و ذلك قبل أن يصدر حكم المجلس الدستورى فى فبراير 2022 بتقييد مضمون الالتزام بالتخزين. أما القانون المصرى لمكافحة جرائم تقنية المعلومات فقد صدر متضمناً نفس الالتزام، و إن اختلفت مدة التخزين فكان حدها الأقصى مائة و ثمانين يوماً، كما لم تستبعد نصوصه صراحةً بيانات فحوى الاتصال من نطاق الالتزام بالتخزين.

6- أصدرت محكمة العدل الأوروبية سلسلة من الأحكام التى تناولت مشروعية تخزين البيانات الشخصية، و التى كان من أهمها الحكم الصادر فى أكتوبر 2020 و الذى صنفت فى إطاره بيانات الاتصال من حيث الخطورة، و اعتبرت أن التخزين المعمم لبيانات الاتصال غير جائز إلا بالنسبة لبيانات الهوية، بينما لا يجوز تخزين الفئات الأخرى من بيانات الاتصال كبيانات المرور و الموقع إلا فى حالات الضرورة؛ و عليه فقد قررت عدم مشروعية إلزام مشغلى الانترنت بالتخزين المعمم، و غير المتمايز لبيانات الاتصال كقاعدة عامة، و ضرورة إخضاع عمليات جمع و تخزين البيانات الشخصية لمبدأ التناسب و الضرورة كأحد المبادىء العامة الحاكمة لمشروعية معالجة البيانات.

7- تعرض مجلس الدولة الفرنسى لنظر الموضوع بمناسبة فحص مدى توافق اللوائح الفرنسية مع متطلبات قانون الاتحاد الأوروبى، و قرر فى الحكم الصادر منه ما مفاده أن القانون الفرنسى لا يتعارض مع قانون الاتحاد الأوروبى فى هذا الشأن، و لكن تفسير محكمة العدل الأوروبية للقانون لا يكفل حماية متوازنة للضمانات المتباينة التى يشتمل عليها قانون الاتحاد الأوروبى؛ و بالتالى فالمحكمة (مجلس الدولة) غير ملزمة بهذا التفسير الذى يخل بضمانة حماية الأمن العام، و ملاحقة الجناة لصالح ضمانات أخرى كالحق فى حرمة الحياة الخاصة؛ و عليه فقد ذهبت المحكمة إلى التفرقة بصدد الإلزام بالتخزين المعمم، و غير المتمايز لبيانات المرور و الموقع بين التخزين لأغراض الأمن القومى، و التخزين لأغراض الملاحقة الجنائية لمرتكبى الجرائم؛ فاعتبرت أن التخزين المعمم لهذه البيانات لمدة عام واحد لأغراض حماية الأمن القومى لا يتعارض مع المعايير الأوروبية؛ نظراً لما تواجهه فرنسا من تهديدات جدية، و حقيقية لأمنها القومى فى الوقت الراهن،

شريطة أن تضاف ضمانة جديدة لهذا النوع من التخزين و هى ضرورة المراجعة، و التقييم الدورى للأخطار التى تتهدد الأمن القومى، و مدى تطلبها لبقاء هذا الإلزام.

بينما فيما يتعلق بالتخزين المعمم و غير المتمايز لبيانات الاتصال لأغراض مكافحة الجريمة و الملاحقة الجنائية للجناة فقد ارتأت المحكمة أنه لا يتماشى مع قانون الاتحاد الأوروبى وفقا لتفسير محكمة العدل الأوروبية، و مع ذلك فباعتبار كون هذا النوع من التخزين هو شرط حاسم أحياناً لنجاح التحقيقات التى يتم إجرائها، و هو الطريق الأنجع للعثور على مرتكبى الجرائم؛ فلا مانع من السماح بالتخزين الهادف و المحدود (غير المعمم) لهذه البيانات على أساس عناصر موضوعية، وفقاً لفئات الأشخاص المعنيين، أو عن طريق معيار جغرافى و لفترة زمنية محددة، و فى إطار الضرورة القصوى التى تتمثل فى حالات الجرائم الخطرة. (إذن استثنى مجلس الدولة الفرنسى تخزين بيانات الاتصال الحساسة لأغراض الأمن القومى من أى التزام بالتقييد)

8- وصل الأمر فى النهاية إلى المجلس الدستورى الفرنسى بعد توجه محكمة النقض إليه بالسؤال الأوّلى حول دستورية المادة 34-1 من قانون البريد و الاتصالات، فى 25 فبراير 2022 و قد انتهى المجلس الدستورى فى حكمه إلى أن السماح بالاحتفاظ المعمم، و غير المتمايز ببيانات الاتصال إنما ينتهك حرمة الحياة الخاصة، و عليه فإن النص المطعون فيه يعدّ غير دستورى فيما لم يشتمل عليه من ضمانات توفر التحقق من وجود التناسب بين الهدف المنشود من التخزين، و بين احترام الحق فى حرمة الحياة الخاصة.

9- عاقب المشرع الفرنسى على القيام بمعالجة البيانات الشخصية دون التقيد بالالتزامات الشكلية التى فرضها القانون للقيام بأيٍ من عمليات المعالجة بعقوبة السجن خمس سنوات، و غرامة قدرها 300 ألف يورو، و ذلك سواء كان الاخلال بالالتزامات القانونية متعمداً أو عن طريق الإهمال. كما عاقب الأشخاص المعنوية المرتكبة لأى من الجرائم المنصوص عليها فى القانون بعقوبة الغرامة التى تساوى خمسة أضعاف الغرامة المعاقب بها الشخص الطبيعى عن نفس الجريمة، و إذا تعلق الأمر بجريمة لا يعاقب فيها الشخص الطبيعى بغرامة فإن الشخص المعنوى يتكبد غرامة تقدر بمليون يورو. بالاضافة إلى العقوبات التكميلية. أما فى القانون المصرى فقد عاقب المشرع على الاخلال بالالتزام الخاص بحفظ البيانات بغرامة تتراوح بين خمسة و عشرة ملايين جنيه مصرى، و تُضاعف الغرامة فى حالة العود، و فى حالة العود للمحكمة أن تقضى أيضاً بإلغاء الترخيص الصادر للشخص بمزاولة النشاط (الطبيعى أو الاعتبارى) كعقوبة تكميلية جوازية.

10- نص قانون الإجراءات الجنائية الفرنسى على إلزام مشغلى الإنترنت بإتاحة بيانات الاتصال لجهات التحقيق التى حددها حصراً دون غيرها، بينما وسّع المشرع المصرى من نطاق الجهات المصرح لها بطلب بيانات الاتصال بحيث تضمنت بالإضافة لسلطات التحقيق، جهات الأمن القومى (رئاسة الجمهورية، ووزارة الدفاع، و وزارة الداخلية، و المخابرات العامة، و هيئة الرقابة الإدارية.)

11- بناء على الحكم الصادر من المجلس الدستورى الفرنسى بعدم دستورية الإتاحة غير المقيدة لبيانات الاتصال لجهات التحقيق؛ قام المشرع الإجرائى بتعديل المواد 60-2، 77-1-1 من قانون الإجراءات الجنائية بإضافة المادة رقم 60-1-2 ، و التى وضعت شروطاً صارمة لإتاحة البيانات الرقمية الحساسة للجهات القضائية؛ فاشترطت لطلب البيانات التقنية المتعلقة بحركة الاتصال، أو مصدر الاتصال، أو المعدات الطرفية المستخدمة أن تكون الجريمة الجارى التحقيق بشأنها من الجرائم ذات الخطورة الخاصة، و من ثم عدّدت حصراً الجرائم التى يجوز حال التحقيق فيها طلب إتاحة بيانات المرور و الموقع الخاصة بالمتهم.

12- رفض المجلس الدستورى ما قررته محكمة العدل الأوروبية فى حكمها من عدم انطباق شرط الرقابة المسبقة من سلطة مستقلة على طلب إتاحة البيانات فى حالة تقديم الطلب من المدعى العام، و اعتبر أن صدور طلب الإتاحة من المدعى العام، أو بناءً على تصريح منه يعد ضمانة هامة لهذا الإجراء بوصف المدعى العام هو "رئيس الشرطة القضائية "، و بالتالى القائم على تقدير مشروعية الإجراءات و الوسائل التى تستخدمها هذه الأخيرة من أجل كشف الحقيقة فى الجريمة محل الدعوى.

13- تتحقق مخالفة الالتزام بإتاحة بيانات الاتصال فى صورتين: صورة سلبية، و تتمثل فى الامتناع عن إتاحة البيانات للجهات التى صرح لها القانون بالاطلاع عليها، و قد عاقب القانون الفرنسى على هذه الجريمة بعقوبة أصلية واحدة هى الغرامة التى تقدر ب 3750 يورو، و ذلك أيا كانت الجهة الطالبة للبيانات؛ بينما عاقب القانون المصرى على الامتناع عن الإتاحة عقوبات تتفاوت شدتها بحسب نوع الجهة الطالبة للبيانات، و تصل فى أشد صورها إلى الحبس الذى يتراوح بين ثلاثة أشهر و ثلاث سنوات، بالإضافة إلى الغرامة التى لا تقل عن مائتى ألف جنيه، و لا تجاوز مليون جنيه؛ هذا إلى جانب ما قرره قانون تقنية المعلومات من مسئولية الشخص المعنوى عن الجرائم المرتكبة لحسابه؛ كما تتحقق مخالفة الالتزام بالإتاحة فى صورة إيجابية تتوافر إما بإفشاء البيانات لغير الجهات المصرح لها- و هنا تنطبق عقوبات إفشاء البيانات- أو بالإتاحة للجهات المختصة، و لكن بالخروج عن القيود التى حددها القانون، و فى هذه الصورة فالجزاء الوحيد

المتصور هو البطلان الإجرائى للدليل المستمد من الإجراء غير المشروع. و ذلك وفقاً لما انتهت إليه محكمة النقض الفرنسية فى أحكامها الصادرة فى يولية 2022.

- **التوصيات:**

1- تفعيل قانون حماية البيانات رقم 151 لعام 2020 من خلال إصدار لائحته التنفيذية، و تقليص فئات البيانات المستثناه من تطبيق أحكام هذا القانون.

2- تضمين قانون حماية البيانات الشخصية حق الشخص المعنى بالبيانات فى إلغاء روابط الإحالة إلى بياناته من محركات البحث الآلى و إجراءات استقضاء هذا الحق.

3- تعديل نص المادة (2) من قانون 175 لعام 2018 لمكافحة جرائم تقنية المعلومات بحيث ينص صراحةً على قصر الحق فى إتاحة بيانات الاتصال - لاسيما الحساسة منها- على سلطة التحقيق على أن يكون ذلك بناءً على أمر مسبب من سلطة قضائية، و بحيث يصبح حصول الجهات الأمنية على بيانات الاتصال الحساسة (بيانات المرور و الموقع) غير وارد إلا بالرجوع للجهات القضائية، و بمناسبة التحقيق فى جريمة من الجرائم ذات الخطورة الخاصة تطبيقاً لنص المادة 57 من الدستور.

4- تقييد الالتزام بالتخزين الواقع على عاتق مقدمى خدمات الانترنت بحيث تُستثنى منه صراحةً بيانات محتوى الاتصال أو المراسلات الإلكترونية لما يتضمنه هذا النوع من التخزين و بخاصة لمدة زمنية طويلة تمتد لستة أشهر من انتهاك خطر لحرمة الحياة الخاصة متمثلاً فى التعدى على خصوصية البيانات، و المحادثات الخاصة.

5- تضمين المواد المتعلقة بإلزام مقدمى الخدمة بإتاحة بيانات الاتصال للسلطات المختصة فى التشريعين المصرى و الفرنسى مدة محددة للوفاء بهذا الالتزام حتى يعتبر الامتناع بفوات هذه المدة محققاً للركن المادى لجريمة الامتناع عن إتاحة البيانات؛ و بالتالى مُرَتباً للمسئولية الجنائية لمقدم الخدمة.

مراجع البحث

أولاً: المراجع العربية:

- د.إبراهيم داوود، الحماية القانونية للبيانات الشخصية من منظور الحق فى الخصوصية- دراسة تحليلية مقارنة، بحث منشور فى مجلة كلية الحقوق- جامعة الإسكندرية 2017 العدد الأول.
- د.أشرف جابر سيد، مسئولية مقدمى خدمات الإنترنت عن المضمون الإلكترونى غير المشروع، مجلة حقوق حلوان للدراسات القانونية و الاقتصادية، 2010، العدد 22.
- الإنترنت و القانون فى مصر، "الجزء الثالث- الخصوصية الرقمية"، وحدة الأبحاث بمؤسسة الفكر و التعبير، مقال منشور على الإنترنت.
- د.أمين الخنتورى، معالم تنظيم الحق فى النسيان الرقمى فى التشريع المغربى، مجلة المنارة للدراسات القانونية و الإدارية،2021، العدد 36.
- د.بو خلوط الزين، الحق فى النسيان الرقمى، مجلة الفكر، جامعة محمد خيضر بسكرة- كلية الحقوق و العلوم السياسية،2017-العدد 14.
- د.حسام الدين الأهوانى، حماية الحق فى الخصوصية فى ظل قانون دولة الإمارات العربية المتحدة، بحث منشور فى مجلة الأمن و القانون، 2008، عدد 2، مجلد 16.
- د.حسن البنا عبد الله عياد، المسئولية المدنية و الجنائية لمقدمى بعض خدمات الإنترنت، رسالة دكتوراة، جامعة عين شمس،2015
- د.رمضان أبو السعود، النظرية العامة للحق، الإسكندرية، دار الجامعة الجديدة للنشر، 2005
- د.سليم محمد سليم، الحماية الجنائية للبيانات الشخصية المعالجة آلياً دراسة مقارنة، مجلة العلوم القانونية و الاقتصادية، كلية الحقوق، جامعة عين شمس، 2020-عدد 62.
- د.طارق راشد، الحماية القانونية لخصوصية البيانات الشخصية فى القانون القطرى و المقارن، المجلة القانونية و القضائية، 2017، العدد2.
- د.عبد الفتاح محمود الكيلانى، مدى المسئولية القانونية لمقدمى خدمة الانترنت، بحث منشور عبر منصة المنظومة الإلكترونية.
- د.محمد حمزة بن عزة، الحق فى النسيان الرقمى، دراسة مقارنة، بحث منشور فى مجلة القانون و الأعمال، جامعة الحسن الأول- كلية العلوم القانونية و الاقتصادية و الاجتماعية- 2021-عدد 68.

- د.مصطفى ابراهيم العربى، مظاهر الحماية الجنائية للحق فى النسيان الرقمى، المجلة العربية لعلوم الأدلة الجنائية و الطب الشرعى، جامعة نايف العربية للعلوم الأمنية،سبتمبر2020، المجلة 2- العدد2.
- د.ياسر محمد اللمعى، السياسة الجنائية المعاصرة فى حماية خصوصية البيانات الشخصية الإلكترونية- دراسة تحليلية مقارنة، بحث منشور فى مجلة روح القوانين- مجلة كلية الحقوق، جامعة طنطا، يناير 2022، المجلد 34- العدد97.

ثانياً: المراجع الأجنبية:

- Baptiste Nicaud, Restrictions à la conservation des données de connexions et à leur accès : la Cour de cassation tire les conséquences de la jurisprudence de la CJUE , DALLOZ, 26 Mars 2024.
- Benjamin A. du Chaffaut, Droit au déréférencement : mise en œuvre et zones d'ombre, Dans Légipresse 2019/HS1 (N° 61), Dalloz, CAIRN.
- Cécile Crichton, Précisions sur l'accès aux métadonnées lors du procès pénal, DALLOZ, Édition du 26 mars 2024.
- CONSEIL d etat-COMMUNIQUÉ DE PRESSE, Données de connexion : le Conseil d'État concilie le respect du droit de l'Union européenne et l'efficacité de la lutte contre le terrorisme et la criminalité, Paris, le 21 avril 2021.
- *Commentaire Décision n° 2021-976/977 QPC du 25 février 2022 « M. Habib A. et autr », Question prioritaire de constitutionnalité portant sur les paragraphes II et III de l'article L. 34-1 du code des postes et des communications électroniques, Le Conseil constitutionnel.*
- Dans quelles hypothèses des données de connexion peuvent elle faire l'objet d'une conservation? Le conseil d'état répond à cette question ; dans une décision du 21 avril 2021 ; Recherche publiée en ligne: https://www.village-justice.com/articles/donnees-connexion-quelles-sont-les-limites-leur-conservation,40314.html

- Guide sur la jurisprudence de la Convention européenne des droits de l'homme, Protection des données, Mis à jour le Mis à jour le 31 août 2022.
- Laure lands-Gronowski-Marie Miliotis, la conservation des données de connexion : un équilibre entre sécurité et vie privé délicat à trouver ; 16 june 2021.
- le capitaine Matthieu Audibert, la conservation et l'accès aux données techniques de connexion. Vers un nouveau paradigme pour les enquêtes judiciaires ?, Centre de recherche de l'ecole des officiers de la Gendarmerie nationale- Veille juridique n 94.
- Marie Ranquet, Le droit à l'oubli : vers un nouveau droit fondamental de l'individu ?, Dans Communications 2019/1 (n° 104), Éditions Le SeuilLe, CAIRN.INFO.
- Maryline Boizard, le temps, le droit àl' loublie et le droit à l'effacement, dalloz (les cahiers de la justice),2016/n 4.
- Matthieu Audibert, L'enjeu de la conservation des données de connexion, Revue de la gendarmerie Nationale , 2022,- numéro spécial Forum International de la cybersécurité 2022, 272, pp. 37-43. hal-03689580.
- Sofian Goudjil, Juriste assistant, parquet général de la cour d'appel d'Angers, Réquisition de données informatiques dans le cadre d'une information judiciaire : le régime est constitutionnel 8 juillet 2022 ,DALLOZ, Édition du 11 janvier 2024.

ثالثاً: روابط ذات صلة:

- https://www.cnil.fr/fr/la-loi-informatique-et-libertes#article5
- https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000441676
- https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952

- https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043887545
- https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A31995L0046%3AFR%3A HTML
- https://www.cnil.fr/fr/reglement-europeen-protection-donnees
- https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000006528061/2004-08-07
- https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp169_fr.pdf
- https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460
- https://www.litige.fr/definitions/droit-a-l-oubli
- https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-ordonnance-de-refere-15-fevrier-2012/
- https://en.wikipedia.org/wiki/Google_Spain_v_AEPD_and_Mario_Costeja_Gonz%C3%A1lez
- https://www.cnil.fr/fr/le-dereferencement-dun-contenu-dans-un-moteur-de-recherche.
- https://incyber.org/le-droit-a-loubli-nest-pas-un-droit-absolu/
- https://www.sba-avocats.com/avocat-penaliste-effacement-fichier-taj-decision-du-conseil-constitutionnel-du-27-octobre-2017.html
- https://www.conseilconstitutionnel.fr/decision/2019/2019796DC.htm
- https://www.vie-publique.fr/loi/279666-loi-gestion-de-la-sortie-de-crise-sanitaire-etat-durgence-sanitaire
- https://incyber.org/article/decision-n-2021-952-qpc-du-3-decembre-2021-m-omar-y/
- https://www.conseilconstitutionnel.fr/decision/2022/20221000QPC.htm

- https://arabic.cnn.com/world/2016/02/17/apple-fbi-request
- https://justice.pappers.fr/decision/df9e7d732700544777291de761e14723