LA PROTECTION DE LA VIE PRIVÉE DANS L'ÈRE DE LA NUMÉRISATION

Mircea CRISTE*

Abstract

La numérisation représente un défi pour le droit constitutionnel, en général, et pour les droits fondamentaux, en particulier, au début du ce siècle. Elle change non seulement notre vie quotidienne, mais aussi notre comportement en tant que citoyens, dans nos relations avec les autorités étatiques et dans l'exercice de nos droits et libertés.

Cette étude analyse l'impact de la digitalisation sur la protection de droits fondamentaux, notamment en ce qui concerne le droit à la vie privée et familiale.

Key Words*: Constitution, fundamental rights, rule of law, private and family life.*
JEL Classification: [K19]

1. Introduction

En traçant le cadre dans lequel il est appliqué l'art. 8 (Droit au respect de la vie privée et familiale) de la Convention européenne des droits de l'homme, la Cour de Strasbourg a précisé que, bien qu'il a pour objet primordial la protection de l'individu face aux ingérences arbitraires des autorités publiques, il ne se limite pas seulement à imposer à l'Etat de s'abstenir de telles ingérences. À cet engagement négatif on peut ajouter des obligations positives, inhérentes au respect effectif de la vie privée ou de famille, qui pourrait nécessiter l'adoption des mesures dans ce sens, y compris les rapports entre les individus. Il n'y a pas une définition donnée pour distinguer entre les obligations positives et négatives de l'Etat, par rapport à l'art. 8, mais les principes applicables sont comparables. Notamment il faut observer le juste équilibre à garder entre l'intérêt général et les intérêts individuels, l'Etat bénéficiant dans toute situation d'une marge d'appréciation[1].

2. La protection de la vie privée – droit constitutionnelle

L'art. 26 de la Constitution, qui oblige les autorités publiques de respecter et de protéger la vie intime, familiale et privée des personnes, constitue la garantie d'un développement plénier de la personnalité humaine. C'est un droit à double

* Professeur de Facultés de droit à l'Université de l'Ouest de Timisoara et l'Université "1 Decembrie 1918" d'Alba Iulia.

[1] Arrêt de la Cour européenne des droits de l'homme no 12.556/03, *Pfeifer c. Autriche*, pt. 37, CEDO 2007-XII.

valence. D'une part, protège l'individu de toute ingérence dans l'intimité de sa vie[2], y compris sous la forme de la surveillance, d'autre part, assure l'identité et l'autonomie de chaque personne, tant au côté individuel, qu'au côté social, qui inclue la famille et le cercle des relations personnelles aussi.

La Constitution ne définit pas la notion de *vie intime, familiale et privée*, mais, pour le faire, la Cour constitutionnelle a appelé à la jurisprudence de la Cour européenne des droits de l'homme, qui a statué dans l'arrêt *Niemetz c. Allemagne* de 1992 que la protection de la vie privée ne couvre seulement la sphère intime des relations personnelles, mais aussi du droit de l'individu de lier et de développer des relations avec ses paires, car il serait trop restrictive la réduction de la notion de vie privée à un cercle intérieur dans lequel l'individu vive sa vie personnelle dans la façon qu'il juge approprié. Pour la C.E.D.O., l'élément définitoire du droit à la vie intime, familiale et privée se réfère à la sphère des relations inter humaines.

La Cour constitutionnelle a décidé qu'alors que le législateur prévoit que toute personne physique a le droit de disposer de soi-même, mais sans violer les droits et les libertés d'autres, l'ordre public ou les bonnes mœurs, ça veut dire que les trois notions de l'art. 26 alin. 1 (vie intime, vie familiale, vie privée) ne peuvent être conçus que dans le respect des droits et des libertés d'autres, de l'ordre public, ainsi que des bonnes mœurs (alin. 2). Ceci signifie que chaque élément de l'alin. 1 doit être rapporté, individuellement, à chacun des trois éléments de l'alin. 2, mais essentiel pour résoudre l'exception d'inconstitutionnalité est d'établir la signification du terme de bonnes mœurs.

Le droit à la vie intime, familiale et privée suppose que toute personne jouait du secret de la vie privée, du respect du droit à la propre image, du droit de ne pas faire publiques, sans son consentement exprès, des données personnelles, exigences

[2] Par la décision no 162 du 26 février 2008, publiée au *Monitorul Oficial* no 263 du 3 avril 2008 et par la décision no 1429 du 2 novembre 2010, publiée au *Monitorul Oficial* no 16 du 7 janvier 2011, la Cour constitutionnelle a retenu que les dispositions qui font référence aux „informations relatives à la santé d'un patient, les résultats des investigations, le diagnostic, le pronostic, le traitement, les données personnelles", étant des informations sur la santé de la personne elles sont incluses dans la notion de vie privée, constituent un mode de réaliser la protection des droits prévus par l'art. 26 de la Constitution, consacrées également par l'art. 8 de la Convention. Dans ce contexte, la Cour a invoqué l'arrêt du 25 février 1997, prononcé par la Cour européenne des droits de l'homme en *Z. c. Finlande*, où on a décidé que „la protection des données personnelles, y compris les données à caractère médical, est d'une importance fondamentale pour qu'une personne pourrait jouir de son droit au respect de la vie privée et de famille, ainsi comme il est garanti par l'art. 8 de la Convention. [...] Dans l'absence d'une telle protection, les personnes qui nécessitent un soin médical ne seraient plus disposés de fournir des informations à caractère personnel et intime, nécessaires à la prescription du traitement approprié pour la maladie de qu'elle il souffre ou de consulter un médecin, ce qui serait de nature à mettre en danger leur vie, et, dans le cas des maladies transmissibles, un tel danger ne peut pas exister pour la collectivité. [...] Pour cette raison, la législation interne des États doit inclure des garanties adéquates pour empêcher toute communication ou divulgation de données avec un caractère personnel relatives à la santé de la personne, conformément aux dispositions de l'art. 8 para 1 de la Convention".

de plus en plus difficiles à respecter dans les conditions d'un développement sans précédent des médias.

La protection particulière assurée à la propre image résulte du fait que celle-ci représente un attribut important de la personnalité humaine, exprimant son originalité et la différenciant des autres personnes. Celle-ci est la raison pour laquelle, en invoquant ce droit fondamental, on peut demander l'interdiction de la publication des certaines photos, prises sans consentement de la personne photographiée. Le droit à la vie intime, familiale et privée est protégé, spécialement par des moyens de droit pénal, l'art. 226 du code pénal prévoyant que la violation de la vie privée, sans droit, par photographie, capture ou enregistrement des images, les écoutes avec des moyens techniques ou l'enregistrement audio d'une personne qui se trouve dans une chambre ou d'une conversation privée est sanctionnée par la peine de prison de un à six mois ou avec une amende.

Alors que les juges décident dans quelle mesure ils donnent priorité au droit à l'information, ils ont à observer si l'image publiée présent ou non un interêt rapporté à son contenu, en se limitant à la question de savoir si celle-ci peut contribuer au processus de la formation de l'opinion publique. Par conséquent, on peut affirmer que la publication d'une image n'est pas justifiée que dans la mesure dans laquelle le public aurait privé de la possibilité de former une opinion dans le cas où celle-ci n'était pas faite publique. D'autre part, le droit de photographier sans restriction des personnalités publiques dans le but de publier les images dans les médias, alors que celle-ci ne se trouvent pas dans des espaces privés, n'est pas garanti du point de vue constitutionnel[3].

Il faut faire une distinction entre la situation des personnes et celle de ceux ne sont pas publiquement connues, la sphère d'intimité étant plus restreinte dans le cas de la première catégorie. Et on peut affirmer que, dans une certaine mesure, ce fait est compréhensible, en prenant en considération que le qualificatif même des „personnes publiques" mette en évidence le fait qu'elles s'exposent à l'intérêt de la société, et parfois elles encouragent cet intérêt. La jurisprudence développée dans les États-Unis où la presse a une large liberté d'expression, dans l'arrêt *New York Times Co. v. Sullivan* de 1964[4], a décidé que ceux qui occupent une fonction publique ont à prouver, dans un procès de calomnie, la mauvaise foi des journalistes, respectivement le fait que ceux-ci connaissaient que les affirmations publiées étaient fondées sur des fausses informations relatives à la personne publique.

Toutefois, cette réalité ne permet pas de conclure que les personnes publiques ne bénéficient plus d'intimité. Ils ne sont pas publics, indiffèrent de personne, les

[3] Décision du premier Sénat du Tribunal constitutionnel allemand du 26 février 2008, http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080226_1bvr160207.html.

[4] https://supreme.justia.com/cases/federal/us/376/254. La jurisprudence de l'instance suprême américaine était confirmée ensuite dans le cas *Gertz v. Robert Welch* de 1974 (https://supreme.justia.com/cases/federal/us/418/323).

informations ou les images qui ne relèvent pas sa vie professionnelle ou ses activités officielles, chacun pouvant fixer les limites de ce qu'on peut publier ou non sur sa vie privée, ainsi que les circonstances et les conditions dans lesquelles celles-ci peuvent intervenir. La jurisprudence française considère que le droit à l'information du public est limité, d'une part, aux éléments pertinents par rapport aux personnes publiques appartenant à la vie officielle, et d'autre part, aux informations et aux images délivrées par ceux intéressés ou qui justifient une actualité ou un débat d'intérêt général. Ainsi, les photos représentant certaines personnes publiques sur la terrasse d'une propriété privée, dans des moments d'intimité, de relaxation et légèrement habillées, ne regardent pas leurs activités publiques ou officielles et ne peuvent pas être, par conséquent, considérées un sujet d'intérêt général qui justifierait l'information du public[5].

La limitation de l'exercice des droits individuels, dans la considération des certains droits collectifs et des intérêts publics, qui viseraient la sécurité nationale, l'ordre public ou la prévention pénale, a constitué en permanence une question sensible sous l'aspect de la réglementation, étant nécessaire de maintenir un équilibre juste entre les intérêts et les droits individuels, d'un part, et ceux de la société, d'autre part[6]. Il s'agit de la soit-dite surveillance du *Big Brother*[7].

La Cour européenne des droits de l'homme a souligné le fait qu'alors qu'il s'agit de l'interception d'une communication, la condition de prévisibilité impose que le droit interne précise surtout la définition des catégories des personnes susceptibles d'être mises sous écoute judiciaire, la nature des infractions, l'établissement d'une limite de la durée de la mesure, les conditions pour rédiger un procès-verbal qui consigne les conversations interceptées et l'utilisation et l'effacement des enregistrements réalisés[8].

Pour comprendre, dans une évolution chronologique, le rapport entre le droit à la vie privée et la liberté d'expression, d'une part, et la protection de l'ordre publique et de la sécurité dans une société démocratique, d'autre part, on part de la décision no. 1258 du 8 octobre 2009 de la Cour constitutionnelle, qui est même antérieure à l'intervention de la Cour de justice de l'Union européenne, qui a confirmé d'ailleurs la décision de l'instance constitutionnelle roumaine. Par ladite décision fut contrôlée la constitutionnalité des dispositions de la Loi no. 298/2008 relative à la rétention des données générées ou traitées par les fournisseurs des services des communications électroniques destinées au public ou des réseaux publics de communication, ainsi que pour la modification de la Loi no. 506/2004

[5] Le Tribunal de grande instance de Nanterre, l'arrêt du 18 septembre 2012, citée par Bogdan IONESCU, *Dreptul la propria imagine. O perspectiva practica*, Bucarest, Universul Juridic, 2013.

[6] DCC no. 1258 du 8 octobre 2009, publiée au *Monitorul Oficial* no. 798/2009.

[7] Le terme de *Big Brother* est definit par les dictionnaires par référence à un Gouvernement, un *leader* ou une personne avec autorité qui détient le pouvoir absolu et qui tente à contrôler le comportement et les pensées des hommes et de limiter la liberté de ceux-ci.

[8] *Valenzuela Contreras c. Espagne*, 30 juillet 1998, § 59, Collection des arrêts et décisions 1998; *R.E. c. Royaume Uni*, no 62498/11, § 123, 27 octobre 2015.

relative au traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. Critiquées furent notamment les dispositions de l'art. 1 et de l'art. 15 de la Loi no. 298/2008, qui stipulaient l'obligation de ces fournisseurs de retenir les données de trafic et de localisation des personnes physiques et morales, ainsi que les données connexes nécessaires pour l'identification de l'utilisateur et de les mettre à la disposition des autorités compétentes dans le but de leur utilisation dans le cadre des activités de recherche, découvert et poursuit des infractions graves.

Par ladite décision, la Cour constitutionnelle a retenu que les dispositions de la Loi no. 298/2008 sont dans leurs totalités inconstitutionnelles. Ainsi, elles ne définissent pas, sans équivoque, ce que signifie l'expression „données connexes". Or, l'absence d'une réglementation légale claire, qui déterminerait d'une façon précise la sphère des données nécessaires à l'identification des personnes physiques ou juridiques utilisatrices, permette les abus dans l'activité de rétention, traitement et utilisation des données stockées par les fournisseurs des services de communications électroniques destinées au public ou des réseaux publics de communication. La limitation de l'exercice du droit à la vie privée et au secret de la correspondance, ainsi qu'à la liberté d'expression, doit être faite d'une façon claire, prévisible et sans équivoque, pour qu'elle soit éliminée, le plus possible, l'apparition de l'arbitraire ou de l'abus de la part des autorités dans ce domaine.

La même manière ambiguë de rédaction, qui n'est pas conforme aux normes de technique législative, fut retrouvée dans la rédaction de l'article 20 de la Loi no. 298/2008, selon lequel, dans le but de la prévention et de l'élimination des menaces à la sécurité nationale, les autorités avec des attributions dans ce domaine peuvent avoir accès aux données retenus par les fournisseurs des services et des réseaux publics de communications électroniques. Parce qu'on n'a pas défini clairement qu'est-ce qu'il signifie „menaces à la sécurité nationale", les juges constitutionnels avait considéré qu'il est possible que différents actions, informations ou activités journalières, de routine, des personnes physiques et morales soit appréciées, d'une façon arbitraire et abusive, comme ayant la nature des telles menaces. En plus, ces personnes peuvent êtres inclues dans la catégorie des personnes suspectes sans qu'elles le sachent et sans pouvoir prévenir, par leur comportement, les conséquences. La personne appelée est ainsi exposée sous l'aspect de la rétention des données que tient à sa vie privée, indépendant d'un acte ou d'une manifestation propre de volonté, mais seulement en fonction du comportement de l'appelant, sans qu'il puisse contrôler les actions de celui-ci. Bien qu'il soit un sujet passif dans cette communication, la personne appelée peut devenir, sans volonté, suspecte. Or, considérait la Cour constitutionnelle, de ce point de vue l'ingérence dans la vie privée de la personne devient excessive.

D'autre part, la Cour a souligné que l'utilisation de l'expression „peuvent avoir" induit l'idée que les données visées par la Loi no. 298/2008 ne sont pas retenues dans le but exclusif de leur utilisation par les seules autorités de l'État avec des attributions spécifiques dans la protection de la sécurité nationale et de l'ordre

public, mais aussi par d'autres personnes ou entités, une fois que ceux-ci *peuvent*, et pas *ont*, accès à ces données, dans les conditions prescrites par la loi.

Dans la matière des droits individuels, tels que le droit à la vie privée et la liberté d'expression, la règle largement reconnue alors qu'il s'agit du traitement des données à caractère personnel est celle de la garantie et du respect de ces droits, respectivement de la confidentialité. Dans ce sens, l'État a des obligations habituellement négatives, d'abstention, de la manière qu'il soit évité, le plus possible, son ingérence dans l'exercice dudit droit ou liberté. Cette exigence ne se retrouvée pas dans les dispositions de la Loi no. 298/2008, qui instituaient la règle de la rétention continue des données à caractère individuel, pour une période de 6 mois comptée du moment de leur interception. Cette disposition met en contradiction la Loi no. 298/2009 avec les dispositions de la Loi no. 677/2001 sur la protection des personnes relative au traitement des données à caractère personnel et la libre circulation de ces données et de la Loi no. 506/2004 sur le traitement des données à caractère personnel et la protection de la vie privée dans le domaine des communications électroniques, vidant de contenu le principe de la protection des données à caractère personnel et de leur confidentialité.

En invoquant la jurisprudence de la CEDO aussi[9], les juges constitutionnels mettent en évidence le fait que l'obligation légale qu'impose la rétention continue des données à caractère personnel ne peut pas se transformer d'une exception au principe de la protection effective du droit à la vie privée et à la libre expression, dans une règle absolue. Ainsi, le droit apparaît comme réglementé d'une manière négative, sa part positive ne gardant plus le caractère prédominant.

La décision no 1258 de 2009 de la Cour constitutionnelle a examiné aussi s'elle était respectée une autre exigence requise pour les cas de limitation de l'exercice de certains droits ou libertés fondamentales, à savoir le principe de la proportionnalité. Selon celui-ci, la mesure de restriction doit être en accord avec la situation qui a déterminé son application et, pareillement, de cesser une fois que la cause déterminante n'existe plus. Or, la Loi no 298 de 2008 imposait l'obligation de la rétention des données d'une façon continue, du moment de son entrée en vigueur, sans considération de la nécessité de mettre fin à cette mesure une fois que la cause déterminante n'existait plus. L'ingérence dans le libre exercice du droit était permanente et d'une façon indépendante de l'intervention d'un fait justifiant, d'une cause déterminante.

Même s'il n'existerait pas une obligation de retenir et de transmettre le contenu de la communication, nous sommes dans la présence d'une violation de la liberté d'expression par la rétention des autres données qui servent à l'identification de l'appelant et de l'appelé, de la source, destination, date, heure et durée de la communication, du type de communication, de l'équipement de communication ou des dispositifs utilisées et de leur location, ainsi que des autres *données connexes*.

[9] L'arrêt du 12 juillet 2001, prononcé dans le cas *Prince Hans-Adam II de Lichtenstein c. Allemagne*.

Bien que la restriction de certains droits fondamentaux pourrait être justifiée par rapport à des droits collectifs et des intérêts publics qui viseraient la sécurité nationale, l'ordre public ou la prévention pénale[10], la prise de certaines mesures de surveillance, sans garanties adéquates et suffisantes, peut „détruire la démocratie sous le prétexte de sa protection"[11].

Suite à la décision 1258/2009 a été adoptée la Loi no 82/2012 qui, à son tour, a fait l'objet d'une saisine à la Cour constitutionnelle. Pour solutionner cette exception[12], l'instance constitutionnelle avait comparé les dispositions de l'ancienne réglementation avec celles de la nouvelle loi, en constatant que dans toutes les deux, les cas dans lesquels les autorités judiciaires ou les organes avec des attributions dans le domaine de la sécurité nationale ont accès aux données générées ou traitées par les fournisseurs des réseaux publics de communications électroniques et des fournisseurs des services de communications électroniques destinées au public sont ceux qui ont pour but les activités de prévention, recherche, découverte et poursuit pénal des *infractions graves*. En plus, la Cour observe que la Loi no 82/2012 augmente d'une façon importante la sphère des infractions circonscrites à cette notion par rapport à la Loi no 298/2008, en permettant l'accès aux données retenues des organes judiciaires et des organes d'Etat avec des attributions dans le domaine de la sécurité nationale pour résoudre les cas des personnes disparues ou pour exécuter un mandat d'arrêt d'exécution d'une peine aussi.

Ni le fait que le législateur a renoncé par la nouvelle réglementation à l'expression „données connexes", en la replaçant avec celle de „données nécessaires", n'était pas satisfaisant pour les juges de la Cour, autant qu'on garde le caractère imprécis de la rédaction et on ne définit ni dans la nouvelle loi le sens de cette expression.

Quant à la possibilité des autorités d'État avec des attributions dans le domaine de la prévention et de la lutte contre les menaces visant la sécurité nationale d'avoir accès aux données retenues par les fournisseurs des services et des réseaux publiques de communications électroniques, prévue par l'art. 20 de la Loi no 298/2008, la Cour constitutionnelle constate que le droit de ces autorités d'État d'avoir accès aux données retenues se retrouve aussi dans la Loi no 82/2012 (art. 16 alinéa 1er), en maintenant une situation pareille à celle prévue par l'ancienne loi.

Le caractère continu de la rétention des données générées ou traitées dans le cadre de l'activité des fournisseurs des réseaux publics de communication électroniques et des fournisseurs des services de communications électroniques

[10] Le droit au respect de la vie privée, le secret de la correspondance et la liberté d'expression, „bien qu'ils soient indissolublement liés à l'existence humaine, toute personne ayant le droit de l'exercer sans restriction, ils ne sont toutefois des droits absolus, mais ils sont conditionnés" (DCC no 1258/2009).

[11] CEDO arrêt du 6 septembre 1978, *Klass et alia c. Allemagne*, paragraphe 49.

[12] DCC no 440 du 8 juillet 2014, publiée au *Monitorul Oficial* no 653/2014.

destinées au public constituent pour l'instance de contentieux constitutionnel un motif d'inconstitutionnalité. Et cette obligation continue de retenir les dites données se retrouve dans la loi no 82 de 2012 aussi, raison pour laquelle elle est inconstitutionnelle à son tour. Ces ingérences sont d'une grande ampleur et d'une gravité particulière, d'autant plus que leur stockage et leur utilisation ultérieure, faites sans que l'abonné ou l'utilisateur enregistré soit informé, est susceptible de générer dans la croyance des personnes visées le sentiment que leur vie privée fait l'objet d'une surveillance constante. Le traitement des données prises en considération par la Loi no 82/2012 conduit à des conclusions très précises relatives à la vie privée des personnes dont les données furent gardées, regardant les coutumes de la vie quotidienne, les résidences permanentes ou temporaires, les déplacements fréquents ou autres déplacements, les activités déroulées, les relations sociales de ces personnes et les milieux sociaux fréquentés par eux. Or, une limitation de l'exercice du droit à la vie privée et au secret de la correspondance, ainsi qu'à la liberté d'expression, doit être faite d'une façon claire, prévisible et sans équivoque, pour qu'elle soit éliminée, le plus possible, l'apparition de l'arbitraire ou de l'abus de la part des autorités dans ce domaine.

La Cour a constaté aussi le manquement des critères objectifs qui limiteraient au strict nécessaire le nombre des personnes qui ont accès et peuvent utiliser ultérieurement les données stockées et que l'accès des autorités nationales aux données stockées n'est pas conditionné, dans tous les cas, par le contrôle préalable d'une instance ou d'une entité administrative indépendante, qui limiterait cet accès et l'utilisation des données à ce qui est strict nécessaire pour que l'objectif soit atteint. Les garanties légales concernant l'utilisation concrète des données stockées ne sont pas suffisantes et adéquates pour écarter la suspicion que les droits individuels, à nature intime, ne sont pas violés.

Enfin, dans l'appréciation de la constitutionnalité de la soit-dite législation *Big Brother*, la décision no 440 de 2014 ne fait pas abstraction de la réalité normative et de la jurisprudence existante dans d'autres États membres de l'Union européenne. Il est cité l'arrêt du 2 mars 2010 de la Cour constitutionnelle allemande, qui souligne la nécessité de certaines réglementations suffisamment précises et claires relatives à la sécurité des données et la restriction de leur utilisation, dans le but d'assurer la transparence et la protection légale. La Cour de Karlsruhe a considéré que le stockage des données représente une ingérence grave, bien que le contenu des communications ne fait pas l'objet du stockage, car les données ainsi obtenues font possible la connaissance détaillée de la sphère intime de la personne, en particulier en ce qui concerne l'appartenance sociale ou politique, les préférences, les inclinations et les faiblesses des personnes, en permettant de dresser des profils pertinents et en créant le risque d'exposer certains citoyennes, qui ne donnent aucune raison d'être soumis à une investigation, à des telles actions. Dans l'espèce, la Cour constitutionnelle allemande a retenu une violation du principe de la proportionnalité, alors que les dispositions critiquées renvoient seulement à la diligence nécessaire, généralement, dans le domaine des télécommunications, mais

laissent les exigences de sécurité au bon gré des opérateurs de télécommunications, auxquels ils ne sont pas imposés des hauts standards de sécurité, mais qui peuvent subir des sanctions plus élevées pour le non-respect de l'obligation de stockage, que pour la violation de la sécurité des données.

Elle est rappelée aussi, la décision du 22 mars 2011 de la Cour constitutionnelle tchèque, qui constate l'inconstitutionnalité de certaines dispositions législatives pour manquement des garanties suffisantes offertes aux citoyens en ce qui concerne le risque des abus et d'arbitraire dans l'utilisation des données archivées. Dans cette dernière décision elle est mise en évidence la nécessité de définir d'une manière suffisante les règles concernant l'accomplissement des conditions sur la sécurité du stockage des données et la restriction de l'accès des tiers à ces données.

Les juges constitutionnels roumains se réfèrent aussi à la jurisprudence de la Cour Suprême Administrative de Bulgarie, qui a annulé par la décision no 13627 du 11 décembre 2008, une disposition qui permettait au Ministère de l'intérieur de retenir des données dans les terminales des ordinateurs et aussi, d'offrir aux services de sécurité et à des autres autorités l'accès à ces données, sans autorisation d'un organe judiciaire. Dans ce cas également, le motif de l'annulation fut celui qu'il n'était pas prévu aucune garantie pour la protection du droit à la vie privée et aucun mécanisme qui garantirait cette protection contre les interférences illégales, de la manière qu'on ne touche pas à l'honneur, à la dignité ou à la réputation d'une personne.

La législation roumaine en matière de la rétention des données générées ou traitées par les fournisseurs des réseaux publics de communications électroniques et par les fournisseurs des services de communications électroniques représente la transposition de la Directive 24 du 15 mars 2006 du Parlement européen et du Conseil. Celle-ci, en modifiant la Directive no. 58/2002, a été adoptée en réponse aux attaques terroristes du 7 juillet 2005 de Londres[13], et a visé, principalement, l'harmonisation de la législation des États membre relative aux obligations des fournisseurs des services de communications électroniques accessibles au public ou des réseaux de communications publiques de garder certaines données générées ou traitées, en vue d'assurer la disponibilité de ces données pour la prévention, la recherche, le découvert et la poursuite pénale des crimes graves, telles que la criminalité organisée et le terrorisme.

La Directive 24 est arrivée sous la loupe des juges de Luxembourg, après que ceux-ci furent appelés à répondre à deux questions préliminaires, formulées en 2012

[13] Le 13 juillet 2005, le Conseil a réaffirmé dans sa déclaration qui condamnait les attaques terroristes de Londres, la nécessité d'adopter, plus vite que possible, certaines mesures communes sur le stockage des données de télécommunications. La Directive 24 de 2006 prévoit l'obligation des fournisseurs des services de communications électroniques accessibles au public ou des réseaux de communications publiques de garder certaines des données générées ou traitées par ces fournisseurs.

par la Haute Cour d'Irlande et, respectivement par la Cour constitutionnelle d'Autriche.

La question soulevée par la Haute Cour irlandaise (C-293/12) visait la requête de Digital Rights Ireland Ltd. contre le Ministère de communications, Marine et Ressources naturelles, le Ministère de Justice, Égalité et Réforme législative, le Commissaire de la Police nationale, l'Irlande et le Procureur général, requête qui contestait la légalité des mesures législatives et administratives nationales relatives au stockage des données sur les communications électroniques.

Dans son question (C-594/12), la Cour constitutionnelle de Vienne faisait référence à des actions en contentieux constitutionnel introduites par le gouvernement du land de Carinthie, MM. Seitlinger, Tschohl et autres, ayant pour objet la compatibilité de la loi autrichienne de transposition de la Directive 24 de 2006 avec la constitution fédérale.

La Cour de justice de l'Union européenne, dans l'arrêt du 8 avril 2014, en contrôlant la Directive attaquée par rapport aux dispositions de la Charte des droits fondamentaux de l'Union européenne, a constaté que le stockage des respectives données répond à un intérêt général, qui contribuerait à combattre la criminalité qui menace la sécurité publique, et que cela ne porte pas atteinte à la substance des droits fondamentaux protégés dans la Charte. Toutefois, les mesures disposées par la Directive représentent une ingérence sur l'exercice des droits garantis par l'art. 7 et l'art. 8 de la Charte, violant le principe de la proportionnalité entre les mesures prises et l'intérêt public protégé.

La Cour a retenu dans ce sens, que les données qui font l'objet de la règlementation de la Directive no. 24/2006 conduisent aux conclusions très précises relativement à la vie privée des personnes dont données furent archivées, qui peuvent viser les coutumes de la vie quotidienne, les lieux de résidence permanente ou temporaire, les courses journalières ou autres déplacements, les activités déroulées, les relations sociaux de ces personnes et les cercles sociaux fréquentés par elles. Dans ces conditions, même si, selon l'art. 1er alin. 2 et l'art. 5 alin. 2 de la Directive 2006/24/CE, il est interdit de garder le contenu des communications et des informations, car ce simple fait peut porter atteinte à l'utilisation des moyens de communications prévus par cette Directive et, par conséquent, la liberté d'expression des utilisateurs, garantie par l'art. 11 de la Charte des Droits fondamentaux de l'Union européenne.

On a constaté aussi, que le fait de garder les données dans le but d'assurer éventuellement l'accès des autorisations nationales compétentes, touche directement et spécifiquement la vie privée et, par cela, les droits garantis par l'art. 7 de la Charte. Un tel stockage des données violent aussi les dispositions de l'art. 8 de la Charte, car il représente un traitement de certaines données à caractère personnel et il doit remplir les exigences de protection des données, prévues dans ledit article. En conséquence, la Cour de justice est arrivée à la conclusion que l'obligation imposée par l'art. 3 et par l'art. 6 de la Directive 24/2006 aux fournisseurs des services de communications électroniques de garder pour une

période les données relatives à la vie privée d'une personne et à ses communications, constitue une ingérence dans les droits garantis par l'art. 7 de la Charte, ainsi qu'une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti par l'art. 8 de la Charte, parce qu'elle prévoit un traitement des données à caractère personnel. Ces ingérences sont d'une grande ampleur et d'une gravité particulière, d'autant plus que leur stockage et leur utilisation ultérieure, faites sans que l'abonné ou l'utilisateur enregistré soit informé, est susceptible de générer dans la croyance des personnes visées le sentiment que leur vie privée fait l'objet d'une surveillance constante.

La Cour de Luxembourg s'était préoccupée aussi du respect du principe de la proportionnalité, arrivant à la conclusion que l'objectif d'intérêt général de la Directive, bien qu'il est fondamental, ne peut pas justifier la nécessité des telles mesures comme celles prévues par cette norme européenne, dans le but de combattre les infractions indiquées par elle.

Pour donner efficacité aux dispositions de l'art. 7 et de l'art. 8 alin. 1er de la Charte des droits fondamentaux de l'Union européenne, la Directive européenne devrait inclure des normes claires et précises sur la contenue et sur l'application de la mesure de la rétention des données et de prévoir toute une série de restrictions, pour que les personnes desquelles données ont été archivées bénéficient des garanties suffisantes qui assurent une protection efficiente contre les abus et tout accès ou utilisation illicite.

L'arrêt du 8 avril 2014 a retenu aussi que la Directive 24/2006 concernait l'ensemble des personnes qui utilisent les services de communications électroniques, sans que celles-ci se retrouvent, même indirectement, dans une situation susceptible à donner lieu à une poursuite pénale. Ainsi, les dispositions de la Directive s'appliquent aussi à ceux pour qui existeraient des indices qu'ils auraient liés, même d'une façon indirecte ou éloignée, avec la commission des infractions graves. Il fut souligné aussi le fait que la Directive ne prévoyait aucune exception en ce qui concerne les personnes dont communications ont été soumises, en conformité avec le droit national, au secret professionnel.

Une autre violation des articles 7 et 8 de la Charte de droits fondamentaux de l'Union européenne a été identifiée dans le fait que la Directive ne prévoit pas aucun critère objectif qui permettrait la délimitation de l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure dans le but de la prévention ou de la poursuite pénale par rapport aux infractions qui ne peuvent pas être considérées suffisamment graves pour justifier une telle ingérence.

Par cet arrêt on a retenu aussi que la Directive 24 ne prévoit pas des critères objectifs qui limiteraient au strict nécessaire le nombre des personnes qui ont accès et peuvent utiliser ultérieurement les données stockées. Il n'était pas réglementé un contrôle préalable effectué par une instance ou par une entité administrative indépendante, qui limiterait l'accès des autorités nationales aux données stockées et leur utilisation strictement à ce qui est nécessaire pour la réalisation de l'objectif

poursuivi, comme il n'était réglementé ni l'obligation des États membres d'établir de telles limitations.

Quant à la durée du stockage des données, on a retenu que la Directive imposait de les garder pour une période de 6 à 24 mois, sans prévoir toutefois des critères objectifs pour limiter le stockage des données au strict nécessaire et sans distinguer entre les catégories des données en fonction de leur utilité pour la réalisation de l'objectif poursuivi ou en fonction des personnes visées.

Enfin, on a constaté que la Directive n'imposait pas que les données stockées soient gardées sur le territoire de l'Union européenne, ainsi que le contrôle du respect des exigences de protection et de sécurité, prévues par l'alinéa 3 de l'art. 8 de la Charte et qui constituent un élément essentiel de la protection des personnes en ce qui concerne le traitement des données à caractère personnel, n'était pas garanti en totalité.

Ainsi, par l'arrêt du 8 avril 2014, la Cour de justice de l'Union européenne décida que la Directive no 24 de 2006 est contraire aux dispositions des articles 7, 8 et 52 alin. 1 de la Charte des droits fondamentaux de l'Union européenne.

Un autre cas significatif pour la problématique de la protection des données personnelles, cette fois stockées dans les portables, c'était celui qui a opposé en 2016 le Bureau fédéral d'enquêtes américain (FBI) et la compagnie Apple, mais il est à observer qu'une jurisprudence sur ce sujet c'était développé en Amérique de nord avant même ce moment-là. Ainsi, la Cour suprême des États-Unis a donné un répons négatif à la question à savoir si on peut rechercher des informations digitales sur le portable d'une personne arrêtée, dans l'absence d'un mandat dans ce sens, avec la motivation que, vu la capacité de stockage des générations actuelles de portables, la plupart des personnes stockent sur ceux-ci des différentes informations (en format photo, vidéo et texte), qui couvrent des longs périodes, de plusieurs ans même[14]. Au Canada, la Cour suprême a décidé avec une majorité de 4 juges sur 7, que la police peut rechercher les données dans un portable de la personne arrêtée, même sans mandat, si la raison de la recherche est en liaison directe avec la cause pour laquelle on a pris la mesure d'arrêt et sous condition de garder un enregistrement en détail de la procédure déroulée[15].

L'état des faits dans le cas *F.B.I. v. Apple,* était le suivant:

Le 2 décembre 2015, apparemment sans aucune motivation, deux employés d'un centre régional pour des personnes avec déshabilités de San Bernardino, Syed Rizwan Farook et son épouse Tashfeen Malik, avaient tué 14 personnes et blessé autres 22 personnes, participantes à une réunion semestrielle des employés. Avant d'être eux-mêmes tués dans l'échange de coups de feu avec les forces de police, ils ont essayé de détruire le téléphone portable qu'ils avaient utilisé. Après plusieurs tentatives, le 9 février 2016, le FBI avait annoncé qu'il ne peut pas décoder l'iPhone

[14] Décision *Riley v. California*du 25 juin 2014 de la Cour suprême des États-Unis, https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf.

[15] https://globalnews.ca/news/1721144/police-can-search-cellphones-without-warrant-during-arrest-court.

5c à cause du niveau de sécurité impénétrable du système d'exploitation iOS, raison pour laquelle il a sollicité à la compagnie Apple de créer un nouveau système d'exploitation qui soit installé dans le portable et qui désactiverait les mesures de sécurité.

Parce qu'Apple, en invoquant sa politique de a ne pas diminuer le degré de sécurité de ses produits, a refusé de créer un soit-dit *backdoor*, FBI a sollicité et a reçu de la part d'un juge fédéral une décision judiciaire qui obligeait Apple à coopérer avec FBI dans l'enquête.

Cette décision est fondée sur une loi qui date de l'aube de la naissance des États Unis, *All Writs Act* de 1789, qui autorise les instances fédérales à émettre tout ordre nécessaire ou bénéfique pour lesdites juridictions, conformément aux usages et aux principes du droit[16]. Apple conteste l'application de cette loi dans l'espèce, et finalement l'État renonce au procès, parce que FBI a trouvé un moyen, un peu controversé (un hacker), pour débloquer le portable[17].

La protection du droit à la vie privée dans l'ère de l'informatique et de l'internet a fait naître un droit nouveau, le soi dite *droit à l'oubli*, qui est partie de la problématique de la protection des données à caractère personnel. Emblématique dans cette question est l'arrêt de 13 mai 2014 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja*[18], de la Cour de justice de l'Union européen, qu'avait reconnue le droit des individus de demander aux moteurs de recherche, dans certaines conditions, d'éloigner les renvois contenant des informations personnelles sur eux, dans le cas qu'elles ne sont pas claires, sont inadéquates, non relevantes ou excessives pour le but du traitement des données. Toutefois, le droit à l'oubli n'est pas un absolu, mais il doit être équilibré par rapport à des autres droits fondamentaux, tel que la liberté d'expression, raison pour laquelle la décision va être prise cas par cas, en fonction du type d'information, le degré de sensibilité pour la vie privée et l'intérêt du public d'avoir accès à celle information, comme le rôle que la personne joue dans la vie publique peut être aussi relevant. Il est vrai aussi qu'il est assez difficile d'assurer le droit à l'oubli dans un milieu tellement dynamique et instable comme celui de l'internet[19]; on a constaté que certaines publications avaient procédé à la republication des informations après que celles-ci furent effacées de la liste.

Conclusions

[16] Le recours à cette loi a occasionné des autres cas célèbres aussi, qui avaient écrit l'histoire de la justice de l'Amérique du Nord, tel le bien connu *Marbury v. Madison*.

[17] https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html.

[18] http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065.

[19] Le degré dans lequel la vie privée d'une personne peut être envahie est exemplifié aussi par le cas *Cambridge Analytica/Facebook*, où les données personnelles des millions des utilisateurs Facebook étaient utilisés non seulement sans l'accord, mais aussi sans la connaissance des ceux-ci (https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html).

L'impact d'une nouvelle société, digitalisée, sur la sphère de la vie privée, réanime un vieux dilemme: faut-il donner priorité à la sécurité générale, communautaire, chaque fois qu'il existe le simple soupçon d'une menace, en renonçant aux éléments essentiels de la liberté individuelle conquise avec des efforts et des sacrifices pendant des siècles ou cette liberté doit être gardée en tant que valeur suprême, même avec le risque des sacrifices humains de masse. En plus, représente-elle la liberté individuelle une valeur plus importante que la sécurité personnelle et la sécurité collective? C'est une question qui se pose dans des termes particuliers dans cette période de confrontation avec la pandémie de Covid-19.

Telle qu'il résulte du cas *Apple*, ce dilemme semble nous partager dans deux camps et de nous radicaliser. Les défenseurs, de bonne foi, de la liberté devient les complices des terroristes qui menacent le monde démocratique et libre. D'autre part, ceux qui généralisent la sûreté sociale sont soupçonnés qu'ils poursuivent, conscients ou non, d'enrégimenter toute la société et de transformer la liberté individuelle d'un droit naturel, dans un privilège qui peut ou pas être accordé à l'une ou à l'autre par ceux qui contrôlent le Pouvoir.

La liberté et la sécurité individuelle étant des attributs de chacun d'entre nous, il devient de plus en plus évident qu'on se trouve dans la situation de l'animal de Buridan, ayant à choisir entre deux choses également nécessaires et inaliénables, avec la perspective de perdre toutes les deux finalement.

Références

Arrêts de la Cour européenne des droits de l'homme
Klass et alia c. Allemagne, 6 septembre 1978
Pfeifer c. Autriche, no 12.556/03
Prince Hans-Adam II de Lichtenstein c. Allemagne, 12 juillet 2001
R.E. c. Royaume Uni, no 62498/11, § 123, 27 octobre 2015
Valenzuela Contreras c. Espagne, 30 juillet 1998

Arrêts de la Cour suprême des États-Unis
Gertz v. Robert Welch de 1974 - https://supreme.justia.com/cases/federal/us/418/323
New York Times Co. v. Sullivan de 1964 - https://supreme.justia.com/cases/federal/us/376/254
Riley v. California du 25 juin 2014, https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf

Arrêt de Le Tribunal de grande instance de Nanterre
L'arrêt du 18 septembre 2012, citée par Bogdan IONESCU, *Dreptul la propria imagine. O perspectiva practica*, Bucarest, Universul Juridic, 2013

Décisions de Cour constitutionnelle de Roumanie
DCC no 162 du 26 février 2008, publiée au *Monitorul Oficial* no 263 du 3 avril 2008
DCC no. 1258 du 8 octobre 2009, publiée au *Monitorul Oficial* no. 798/2009
DCC no 1429 du 2 novembre 2010, publiée au *Monitorul Oficial* no 16 du 7 janvier 2011
DCC no 440 du 8 juillet 2014, publiée au *Monitorul Oficial* no 653/2014

Décision du premier Sénat du Tribunal constitutionnel allemand du 26 février 2008, http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080226_ 1bvr160207.html

Sources électroniques

https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html

http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065

https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

https://globalnews.ca/news/1721144/police-can-search-cellphones-without-warrant-during-arrest-court