CIFE Note de recherche n°70

Marta-Claudia Cliza et Laura-Cristiana Spataru-Negura**, 27 avril 2018*

Règlement Général de l'Union européenne sur la Protection des Données: tout le monde est-il prêt?

À partir du 25 mai 2018, d'importants changements seront apportés à la législation sur la protection des données personnelles en Europe, quand le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016[1] relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE[2] (Règlement Général sur la Protection des Données - ci-après le « *GDPR* ») adopté le 27 avril 2016, entrera en vigueur.

La présente note de recherche donne un aperçu du GDPR afin de comprendre les nouvelles règles juridiques applicables à la protection des données en relation avec les droits des personnes concernées.

Par le GDPR, le Parlement européen, le Conseil de l'Union européenne et la Commission européenne ont l'intention de renforcer et d'unifier la protection des données pour tous les individus au sein de l'Union européenne.

Afin de mieux standardiser la législation sur la protection des données personnelles, les institutions de l'Union européenne ont décidé d'adopter cette législation par le biais d'un règlement (au lieu d'une directive, comme au présent), car le règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Depuis le debut, nous soulignons que les données sont des *données personnelles* si elles concernent une personne physique *identifiée* ou au moins *identifiable*. Une personne est considérée comme *identifiable* si un élément d'information contient des éléments d'identification par lesquels la personne peut être identifiée, directement ou indirectement. Par exemple, les données personnelles peuvent être contenues dans des fichiers informatiques ou dans des dossiers papier (numéros de téléphone, adresses, informations financières, photographies, images satellites, numéros d'identification, adresses e-mail, dossiers de santé).

Le GDPR se propose d'offrir aux personnes concernées plusieurs droits pouvant être appliqués à l'encontre des entreprises, des autorités publiques ou des organismes privés dans l'intérêt public qui traitent de telles données personnelles. Veuillez noter que toutes les entreprises, les autorités publiques ou les organismes privés à intérêt public agissant en tant que responsables du traitement sont directement concernés par les droits accordés aux personnes concernées, tandis que les entreprises agissant en qualité de sous-traitants sont moins affectées.

Les personnes concernées ont plusieurs droits au titre du GDPR (voir le chapitre 3 du GDPR - *Droits de la personne concernée*), par exemple le droit d'obtenir des informations, le droit d'accès aux données personnelles, le droit de rectification, le droit à l'effacement, le droit à la portabilité des données (un nouveau droit qui n'existait pas dans la legislation européenne, avant le GDRP).

Pour que la personne concernée comprenne les informations fournies par le responsable du traitement, la communication doit être faite, conformément aux dispositions de l'article 12 du GDPR, « *d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant* ». *En outre, les « informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique* » ou oralement (lorsque la personne concernée le demande expressément, à condition que l'identité de la personne concernée soit prouvée par d'autres moyens.)

Il faut considerer que les informations données à la personne concernée ne doivent pas être comprises dans des politiques de confidentialité excessivement longues ou difficiles à comprendre.

Le GDPR préserve la position prise par la directive sur la protection des données (avec seulement des modifications mineures) concernant le droit de ne

pas être évalué sur la base d'un traitement automatisé. Conformément à l'article 22 du GDPR, « *la personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire* ». Cependant, l'article 22, alinéa (2), lettre c) du GDPR précise que le consentement explicite de la personne concernée constitue une base valable pour l'évaluation fondée sur le profilage automatisé.

Ainsi, le GDPR va complètement changer l'interaction des personnes concernées avec les entreprises qui ont accès à leurs données personnelles. Grâce au droit à l'information du GDPR, non seulement elles deviendront plus conscientes de ce que sont les données personnelles, mais aussi de la façon dont les données - lorsqu'elles sont corrélées - peuvent mener à l'analyse des données volumineuses.

Les platesformes en ligne et les applications mobiles (telles que LinkedIn, Facebook, Google) doivent adapter leurs politiques en matière d'utilisation et de partage des données personnelles, afin qu'elles soient conformes au GDPR. Les mécanismes par lesquels les plateformes en ligne informent leurs utilisateurs de la collecte, du stockage, du partage et de l'utilisation de leurs données doivent être modifiés afin que les options d'adhésion aux différents services ne soient plus automatisées ou présélectionnées et qu'elles deviennent, à partir du 25 mai 2018, un consentement conscient, donné de manière pleinement responsable.

Ainsi, nous ne serons plus témoins de l'abonnement automatique au marketing par courriel, du partage automatique des données entre plateformes ou des intégrations multi-plateformes sans notre consentement. Nous soulignons l'importance de la sensibilisation liée à la définition du consentement par le GDPR, car le consentement ne peut plus faire l'objet d'une interprétation - l'utilisateur doit être informé des informations suivantes : le type de données collectées par la plateforme, comment les données seront utilisées, avec qui elles seront partagées, où seront elles transférées, et, surtout, pour combien de temps elles seront retenues. Dans leur quête de conformité au GDPR, les plateformes se précipitent dans la reconstruction de leurs pages afin que l'utilisateur soit correctement informé.

Veuillez noter que l'une des plus grandes plateformes bancaires en ligne - PayPal - vient de dévoiler une liste de partenaires auxquels la plateforme pourrait partager nos données personnelles: une liste de «seulement» 690 partenaires commerciaux (banques, marketeurs, centres d'appels) et autorités (agences internationales, entités fiscales) à qui PayPal pourrait révéler certaines de nos données les plus importantes: par exemple nom complet, compte bancaire, détails de l'entreprise, coordonnées, détails des transactions. Avant le 1er janvier 2018, la page Web ne contenait aucune des informations susmentionnées et aucun de ses utilisateurs ne savait vraiment à qui PayPal avait révélé l'information .[3]

Outre le fait de savoir quelles données seront traitées et de quelle manière, dès la création d'un compte utilisateur sur une plateforme en ligne, à partir du 25 mai 2018, les personnes concernées pourront demander aux contrôleurs de données d'accéder aux données personnelles qu'ils détiennent sur eux. Nous devrions voir dans quelle mesure les grandes plateformes sociales (par exemple Facebook) donneront également accès aux données qu'elles ont historiquement collectées avant le 25 mai 2018. Il serait logique que la personne concernée ait accès à la fois aux données présentes et historiques, aussi longtemps que la plateforme continue d'utiliser des données historiques.

Le plus récent cas de confidentialité lié à Facebook remonte à février 2018, lorsqu'un tribunal belge a menacé d'imposer 250 000 euros EUR par jour au géant social ou jusqu'à 100 000 000 EUR si Facebook continuait à suivre les internautes sur des sites tiers et ne supprimait pas toutes les données sur les citoyens belges titulaires d'un compte sur la plateforme ou non . Juste une brève recherche Google en utilisant les mots-clés suivants « *Facebook amende protection* », conduira à pas moins de 5 millions de résultats.

En 2017, un tribunal espagnol a infligé une amende de 1 200 000 EUR à Facebook après que l'agence nationale de protection des données ait prouvé que Facebook collectait et utilisait des données personnelles utilisées à des fins publicitaires . La plateforme collectait des données sur l'orientation sexuelle et les croyances religieuses des personnes à la fois sur la plateforme Facebook et sur les plateformes tierces, sans consentement.

Ce fut l'une des premières fois où de multiples agences de protection des données dans l'union européenne ont coopéré à une enquête contre un grand acteur sur le marché en ligne. L'agence

espagnole de protection des données a coopéré avec les autres agences de Belgique, de France, d'Allemagne et des Pays-Bas et a réussi à prouver que Facebook n'informait pas ses utilisateurs ou les utilisateurs des sites tiers qu'ils collectaient des données et dans quelle mesure ils les utilisaient.

Les résultats ont été surprenants : les données des utilisateurs étaient collectées à l'aide de cookies tiers placés sur des pages Facebook ou des sites Web de tiers. Les cookies recueillaient des données sur le comportement de l'utilisateur sur les pages Internet sur lesquelles Facebook avait placé ses cookies (*via* le bouton « J'aime »). De plus, il a traité davantage les caractères spéciaux collectés - tels que l'orientation religieuse et sexuelle - et les utilisateurs profilés, afin qu'ils puissent être ciblés par des campagnes de marketing. À aucun moment, les utilisateurs ne pouvaient pas se rendre compte que leurs données étaient collectées, ni ne savaient comment le géant social allait les utiliser - le but et la mesure dans laquelle Facebook ou ses partenaires vont les utiliser. Ce qui semble encore plus tragique, c'est que les personnes qui n'ont jamais eu l'intention d'utiliser une plateforme sociale telle que Facebook avaient leurs données personnelles collectées et utilisées simplement en naviguant sur des sites Web.

De plus, nous avons été temoins aux auditions de Mark Zuckerberg au Congrès americain qui a révélé beaucoup d'informations sur Facebook.

Pendant ce temps, il y a des débats constants sur la façon dont Facebook nous surprend chaque fois que nous naviguons. Imaginez-vous que derrière chaque surprise que vous recevez de Facebook, il y a énormément de données que la plateforme rassemble à votre sujet. Nous devrions débattre de quelques exemples ici : Facebook sait quand vous êtes devenu ami avec quelqu'un et vous en félicite, il sait quand vous êtes né afin qu'il puisse souhaiter bon anniversaire - et il partage cette information avec des amis et même des amis d'amis - peut-être même avec ses amis commerciaux ?!

Cependant, alors que la plupart d'entre nous en sommes conscients et d'accord avec ce qui précède, nous pouvons ne pas être d'accord avec Facebook gardant l'information d'une photo prise avec notre téléphone (les métadonnées de l'image - horodatage ou localisation, type de caméra / téléphone), stockant notre adresse IP et même l'identifiant unique du smartphone. Si vous utilisez Facebook quotidiennement, la plateforme sait même quand vous vous réveillez et vous allez dormir, tout en fonction de votre comportement d'utilisation[6]. Toutes ces informations mélangées à l'intelligence artificielle pourraient conduire à de nombreux cas d'abus.

À partir du 25 mai 2018, avec la mise en conformité au GDPR, les gens ne seront plus soumis à de telles pratiques, car les politiques de cookies ne seront plus tacitement acceptées- le consentement actif devenant obligatoire. De plus, les données spéciales ne peuvent plus être traitées sans un consentement explicite, et certains pays ont même suggéré d'interdire l'utilisation des données spéciales.

Le GDPR fortifie à la fois les personnes concernées et les agences de protection des données. Les agences de protection des données peuvent désormais émettre elles-mêmes des sanctions et des amendes qui, jusqu'à présent, dans certains pays, n'étaient possibles qu'avec l'aide des tribunaux.

L'une des missions les plus importantes du GDPR était de protéger les enfants et leurs données personnelles. À partir de cette année, les données sur les enfants ne peuvent plus être traitées sans le consentement explicite d'un adulte.

En 2016, les plus grandes sociétés de jouets aux États-Unis ont été condamnées à des amendes pour avoir utilisé des technologies de pistage sur des sites Web populaires pour enfants : Viacom devait payer 500 000 USD, Mattel 250 000 USD, JumpStart 85 000 USD[7].

Un cas plus proéminent de 2017 a juste détruit la confiance des parents dans les jouets de nouvelle génération. Les parents en Allemagne ont été invités à détruire une poupée qui pouvait espionner leurs enfants[8]. Le nom de la poupée d'espionnage était Cayla et elle pouvait être consultée *via* Internet à l'aide d'un logiciel de reconnaissance vocale. De plus, la poupée pouvait être contrôlée à l'aide d'une application. La connexion Bluetooth à la poupée s'est révélée si peu sûre que n'importe quel hacker à moins de 15 mètres pouvait écouter ce qui se passait près de la poupée et parler directement à l'enfant qui jouait avec. L'affaire a soulevé un énorme débat sur les jouets intelligents et les dispositifs de suivi liés à l'utilisation des enfants.

En 2017-2018, certains pays européens ont interdit l'utilisation des montres intelligentes par les enfants (par exemple, l'Allemagne[9]).

L'intelligence artificielle liée aux jouets connectés à Internet pourrait soulever d'énormes problèmes à l'avenir. Imaginez-vous la puissance d'un jouet qui apprend à parler tout en interagissant avec les enfants du monde entier. Le GDPR vient juste à temps pour assurer que les enfants sont protégés contre les abus.

En ce qui concerne la Roumanie, en mai 2016, l'Autorité fiscale roumaine a publié une liste de tous les citoyens ayant des paiements d'impôts en suspens à ce moment-là, également intitulée «la liste de l'humiliation»[10]. Il est très intéressant de constater que certaines dettes ont été contestées devant les tribunaux roumains, donc très susceptibles d'être modifiées ou même annulées. À cet égard, l'autorité roumaine chargée de la protection des données a infligé à l'autorité fiscale une amende fondée sur le plafonnement des amendes en vertu de la loi actuelle sur la protection des données, d'un montant de 16 000 RON (environ 3 500 EUR).

Ayant en vue toutes ces situations, nous considérons que le GDPR apporte plus de clarté et de sécurité juridique en ce qui concerne les allégations qui peuvent être présentées par les personnes concernées que celles qui sont réglementées par la directive sur la protection des données.

Le GDPR modifie fondamentalement les conséquences financières potentielles de la violation de la législation européenne sur la protection des données, le niveau de la sanction potentielle en fonction de la violation et allant des amendes administratives de :

(1) jusqu'au 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'au 2% du chiffre d'affaires annuel total de l'exercice précédent, selon le montant le plus élevé[11] (pour violation de principes tels que « par conception et par défaut », -respect des obligations liées au traitement ou absence de nomination d'un délégué à la protection des données) ou de

(2) jusqu'au 20 000 000 EUR, ou, dans le cas d'une entreprise, jusqu'au 4% du chiffre d'affaires annuel total de l'exercice précédent, le montant le plus élevé étant retenu[12] (pour violation des principes du traitement ou des formalités légales de traitement, et pour violation des droits de la personne concernée).

Nous soulignons que le régime de sanction administrative exigera une évaluation au cas par cas des circonstances de chaque infraction individuelle, par conséquent, il n'impose pas de responsabilité sur une base de responsabilité stricte. Nous considérons que les facteurs à prendre en compte sont la nature, la gravité et la durée de chaque infraction, la forme de la culpabilité (intention ou négligence), les mesures d'atténuation des dommages déjà mises en œuvre, les mesures techniques et organisationnelles déjà mises en manière dont l'autorité de surveillance a pris conscience.

Les États membres sont habilités à fixer les règles selon lesquelles et dans quelle mesure des amendes administratives peuvent être infligées aux autorités publiques et aux organismes privés d'intérêt public établis sur leur téritoire. Par souci de transparence, ils sont tenus de notifier à la Commission européenne les dispositions juridiques qu'ils adoptent au plus tard le 25 mai 2018 et, sans délai, toute loi de modification ultérieure ou toute modification les concernant. En Roumanie, deux sénateurs ont enregistré à l'ordre de jour de la Chambre des Députés un projet de loi visant le GDPR par lequel ils proposent de limiter la somme due par une autorité publique et par un organisme privé dans l'intérêt public a 200 000 lei (environ 43 000 EUR)[13]. Le Conseil Legislatif et le Conseil Economic et Social de Roumanie ont transmis des avis consultatifs, par lequels ils ont apprecié que, compte tenu des objectifs du législateur européen lors de l'adoption du GDPR, ils estiment qu'il ne serait pas approprié d'imposer une responsabilité dérogatoire, moins punitive, aux autorités publiques. Pour cette raison, nous recommandons au législateur roumain (et aux legislateurs d'autres États membres de l'Union européenne) d'adopter une approche équitable pour les entités publiques et privées, en imposant un tel régime de sanction commun à tous les acteurs dans le domaine de la protection des données.

Mais que se passe-t-il dans les systèmes juridiques qui ne prévoient pas d'amendes administratives (le Danemark, l'Estonie) ? Le GDPR réglemente expressément que, dans ces États membres, l'amende sera « *déterminée par l'autorité de contrôle compétente et imposée par les juridictions nationales compétentes, tout en veillant à ce que ces voies de droit soient effectives et aient un effet équivalent aux amendes administratives imposées par les autorités de contrôle.* »[14].

Pour toutes les raisons mentionnées ci-dessus, la conformité au GDPR devient ainsi une aubaine pour les personnes concernées, alors que pour les autorités publiques, pour les organismes privés

d'intérêt public, pour les entreprises, y compris les plateformes en ligne, les marketeurs, les banques, les institutions d'assurance, cela devient un véritable défi.

En tout cas, pour tous les acteurs impliqués dans la protection des données, le compte à rebours final a commencé pour le GDPR !

*__Marta-Claudia Cliza__, *Avocate, docteur en sciences juridiques, Maître de conférences à la Faculté de Droit, Université « Nicolae Titulescu » de Bucarest, Roumanie (http://www.univnt.ro/en/), où elle enseigne depuis 2002. À la fois, elle est Fondatrice et Associée gérante du Bureau d'avocats Cliza - http://www.cliza.ro/team (courriel : cliza_claudia@yahoo.com).*

**__Laura-Cristiana Spataru-Negura__, *Avocate, docteur en sciences juridiques, Maître de conférences à la Faculté de Droit, Université « Nicolae Titulescu » de Bucarest, Roumanie, où elle enseigne depuis 2009. Elle est également Managing Associate du Bureau d'avocats Cliza - http://www.cliza.ro/team (courriel : negura_laura@yahoo.com) et intervient dans les programmes d'été du CIFE depuis 2009.*

1. Note inspirée de Laura-Cristiana Spataru-Negura, Cornelia Lazar, « Lifting the Veil of the GDPR to Data Subjects », CKS eBook 2018, Bucarest, 2018, voir http://cks.univnt.ro/cks_2018.html.

Notes:

1. Disponible en ligne https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679.

2. Disponible en ligne https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:31995L0046.

3. Liste disponible en ligne https://www.paypal.com/ie/webapps/mpp/ua/third-parties-list.

4. Disponible en ligne https://www.reuters.com/article/us-facebook-belgium/facebook-loses-belgian-privacy-case-faces-fine-of-up-to-125-million-idUSKCN1G01LG.

5. Disponible en ligne http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_09_11-iden-idphp.php.

6. Voir https://9to5mac.com/2018/03/12/how-to-download-your-facebook-data/amp/.

7. Voir http://www.dailymail.co.uk/sciencetech/article-3787859/NY-settles-4-companies -stop-tracking-children-online.html.

8. Voir http://www.bbc.com/news/world-europe-39002142.

9. Voir http://www.rfi.fr/europe/20171123-allemagne-interdiction-smartwatch -montre-connectee-enfants-gps.

10. Voir https://economie.hotnews.ro/stiri-finante-21000512-fiscul-publicat-lista-persoanelor -fizice-datorii-peste-1-500-lei-peste-187-230-romani-restante-fiscale-care-insumeaza-3-4-miliarde-lei.htm.

11. Voir l'article 83 alinéa (4) du GDPR.

12. Voir l'article 83 alinéas (5) et (6) du GDPR.

13. Voir http://www.cdep.ro/pls/proiecte/upl_pck2015.proiect?cam=2&idp=16976.

14. Voir l'article 83 alinéa (9) du GDPR.

Administration: Aline Palige et Jean-Claude Vérez
Policy Paper / Note de recherche est publiée
par le Centre international de formation européenne,
association dont le siège est 81, rue de France, F-06000-Nice.

www.cife.eu

Ce projet a été financé avec le soutien de la Commission européenne. Cette publication (communication) n'engage que son auteur et la Commission n'est pas responsable de l'usage qui pourrait être fait des informations qui y sont contenues.

Avec le soutien du programme Erasmus+