La Newsletter dédiée à la mise en conformité au RGPD

par @DerriennicParis

DERRIENNIC ASSOCIÉS

Conformité RGPD

#NewsDerriennicRGPD 14

Madame, Monsieur,

Nous vous proposons, en ce mois de mai, une lettre RGPD composée des actualités suivantes :

- le bilan 2018 de la CNIL et la communication de sa présidente s'agissant de la fin de la « période de tolérance » liée à l'entrée en application du RGPD ;
- une décision du Conseil d'Etat réduisant la sanction, jugée « disproportionnée », prononcée par la CNIL à l'égard d'Optical Center ;
- l'adoption, par la CNIL, d'un « règlement type » sur les traitements liés à l'authentification biométrique au travail ;
- Une décision de la CJUE concernant un traitement de données à caractère personnel constitué par l'enregistrement et la diffusion d'une vidéo.

Rapport de la Cnil 2018 : bilan et perspective

Le 15 avril dernier, la CNIL a rendu public son bilan de l'année 2018. Elle a également, par l'intermédiaire de sa présidente, affirmé que la « période de tolérance » faisant suite à l'entrée en vigueur du RGPD, touche à sa fin.

Le 15 avril dernier, la CNIL a rendu public son bilan de l'année 2018. Elle a également, par l'intermédiaire de sa présidente, affirmé que la « période de tolérance » faisant suite à l'entrée en vigueur du RGPD, touche à sa fin.

1. La CNIL indique que l'entrée en application du RGPD a marqué une prise de conscience « inédite» des enjeux de protection des données auprès des professionnels et particuliers, ce qui s'est traduit par une augmentation considérable des plaintes (11 077, soit 32,5% de plus qu'en 2017) et demandes d'information (189 877 appels reçus, soit 22% de plus qu'en 2017) adressées à la CNIL.

La CNIL relève que les plaintes reçues pour l'année 2018 se concentraient sur la diffusion de données sur internet (33,7%), le secteur marketing/commerce (21%), les ressources humaines (16,5%), la banque et le crédit (8.9%) et le secteur santé et social (4.2%).

Elle a également observé plusieurs tendances :

- le visionnage à distance des images issues des dispositifs vidéo ;
- l'installation de caméras dans des unités de soin ;
- le souhait des clients de banques ou de services en ligne de contenus d'utiliser leur droit à la portabilité de leurs données ;
- une sensibilité accrue des citoyens concernant la sécurité de leurs données personnelles dans tous les secteurs ;
- des craintes d'utilisateurs de smartphones concernant les données auxquelles les applications mobiles peuvent avoir accès.

La CNIL a réalisé 310 contrôles en 2018, dont 204 sur place, 51 en ligne, 51 sur pièce et 4 auditions. 49 mises en demeure ont été adoptées et 11 sanctions prononcées par la formation restreinte, dont 10 sanctions pécuniaires.

2. La CNIL annonce que ses contrôles se concentreront, s'agissant de l'année 2019, sur les grandes thématiques suivantes :

- l'exercice des droits, notamment suite aux plaintes des personnes concernées;
- la répartition des responsabilités entre les sous-traitants et les donneurs d'ordre;
- les données des mineurs (publication de photos, biométrie et vidéosurveillances dans les écoles, recueil du consentement des parents pour les moins de 15 ans).

Elle a également affirmé que sa stratégie de contrôle serait centrée sur les plaintes reçues, afin de rester en prise avec les attentes des citoyens.

3. Enfin, ce rapport indique également que la CNIL poursuivra ses actions d'accompagnement (initiées en 2018), auxquelles s'ajouteront des actions de contrôle. La CNIL ajoute, par ailleurs, que dans les cas qui le nécessiteront, « des sanctions seront prononcées car la crédibilité du RGPD repose aussi sur une politique de contrôles et de sanctions efficace ».

Cette position laisse entendre que la « période de tolérance » arriverait à son terme, période au cours de laquelle la CNIL s'interdisait de sanctionner des organismes pour des manquements constatés aux nouvelles obligations, telles que prévues dans le RGPD.

Cette analyse est à rapprocher des propos de la Présidente de la CNIL, tels que rapportés par le site www.numerama.com, qui aurait affirmé qu'il était temps de « faire preuve d'une fermeté accrue », et ajouté : « c'est la fin d'une certaine forme de tolérance liée à la transition».

Le Conseil d'État moins sévère que la Cnil ?

Par arrêt du 17 avril 2019, le Conseil d'Etat a ramené le montant de la sanction prononcée par la CNIL à l'encontre d'OPTICAL CENTER, pour manquement à son obligation de protection des données à caractère personnel, de 250.000 à 200.000 €.

Pour rappel, OPITCAL CENTER avait été condamnée par la CNIL à une amende de 250.000 € (http://derriennic.com/amende-de-250-000-euros-pour-optical-center/), en raison d'un défaut de sécurisation permettant d'accéder aux documents des clients d'OPTICAL CENTER en modifiant le paramètre ID relatif à l'identifiant de la facture, lequel était parfaitement visible au sein de l'URL affichée dans la barre d'adresse du navigateur.

OPTICAL CENTER a demandé au Conseil d'Etat, par une requête et un mémoire en réplique, d'annuler la délibération par laquelle la CNIL l'avait condamnée ou, à défaut, de réduire significativement le montant de la sanction pécuniaire.

Dans cette décision, le Conseil d'Etat a rappelé qu'au titre de l'article 34 de la loi du 6 janvier 1978, il incombe au responsable du traitement de prendre toutes les précautions utiles afin de préserver la sécurité des données.

Le Conseil d'Etat a constaté, à ce titre, que le site internet d'OPTICAL CENTER « n'intégrait pas de fonctionnalité permettant de vérifier qu'un client s'était bien authentifié à son espace personnel avant de lui donner accès à ses factures et bons de commande » et, qu'en conséquence, « c'est à bon droit que la formation restreinte de la CNIL a caractérisé l'existence d'un manquement aux obligations de sécurité prévues par l'article 34 précité ».

En revanche, la haute juridiction a estimé que la CNIL, en raison du comportement d'OPTICAL CENTER et notamment de la célérité avec laquelle cette dernière avait apporté les mesures correctrices de nature à remédier aux manquements, aurait dû lui infliger une sanction plus proportionnée :

« Lorsque la CNIL constate des manquements à l'obligation d'assurer la sécurité et la confidentialité des données, il lui appartient, pour prononcer une sanction sous le contrôle du juge, de tenir compte de la nature, de la gravité et de la durée de ces manquements, mais aussi du comportement du responsable du traitement à la suite de ce constat. En retenant une sanction pécuniaire d'un montant de 250 000 euros sans prendre en compte la célérité avec laquelle la société Optical Center a apporté les mesures correctrices de nature à remédier aux manquements constatés, la formation restreinte de la CNIL a infligé à cette société une sanction disproportionnée. »

En raison de ce qui précède, le Conseil d'Etat a ramené la sanction prononcée par la CNIL à un montant de 200.000 euros.

La CNIL adopte un règlement type sur l'authentification biométrique

Après une consultation publique, la CNIL a, le 28 mars 2019, publié un règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail (délibération n° 2019-001 du 10 janvier 2019).

Pour rappel, les données biométriques sont qualifiées par le RGPD de catégories particulières de données à caractère personnel et sont donc soumises à un régime particulier.

Les nouvelles dispositions de la loi « Informatique et libertés » du 6 janvier 1978 (articles 8, II., 9° et 11, I., 2°, b.) prévoient que des dispositifs de contrôle d'accès biométriques peuvent être mis en place par des employeurs à condition d'être conformes à un règlement type élaboré par la CNIL .

Ce règlement, publié le 28 mars 2019 et qui précise aux organismes comment encadrer leurs traitements de données biométriques, revêt un caractère contraignant. Il constitue le premier acte juridique de ce type élaboré par la CNIL.

En premier lieu, il oblige le responsable du traitement à vérifier que le traitement de données biométriques est nécessaire.

A titre d'exemple, si un système de badge est suffisant, le recours à la biométrie n'est pas nécessaire et le recours à une solution moins intrusive doit être privilégié. Il en est de même si la biométrie ne répond qu'à un besoin de confort, ou si les locaux, applications ou appareils protégés ne sont pas particulièrement sensibles.

La justification du recours au traitement de données biométriques doit être documentée, en indiquant le contexte spécifique rendant nécessaire un niveau de protection élevé, ainsi que la justification du recours à la biométrie plutôt qu'à une autre technologie et la justification du choix du type de biométrie (iris, empreinte digitale, réseau veineux de la main, etc.), notamment la raison d'utilisation d'une caractéristique biométrique plutôt qu'une autre.

Les données concernées par ce traitement sont:

- les données renseignées par l'employeur (données d'identifications, données relatives à la vie professionnelle, zones et plages horaires autorisées pour l'accès au locaux, matériels ou applicatifs concernés le cas échéant) ;
- les données générées par le dispositif (accès utilisés, horodatage des tentatives d'accès, matériel ou applicatif concerné, etc.)
- les données biométriques, à savoir les caractéristiques morphologiques ;
- les données d'enregistrement brut de la caractéristique biométrique ;
- les gabarits, qui sont les mesures mémorisées lors de l'enregistrement des caractéristiques morphologiques.

Ce règlement type indique également :

- les personnes habilitées à traiter les données ;
- les conditions de détention des gabarits ;
- les durées de conservation applicable à chaque donnée :

- le temps du calcul du gabarit s'agissant des enregistrements bruts ;
- la durée d'habilitation de la personne concernée s'agissant des gabarits ;
- 6 mois en base active s'agissant des données de journalisation ;
- 6 mois à l'issue de la durée d'habilitation s'agissant des données d'identification.

- les mesures de sécurité.

Ce règlement précise enfin que l'employeur doit effectuer une analyse d'impact relative à la protection des données et informer ou consulter les instances représentatives du personnel.

L'application du RGPD à une vidéo « amateur »

La transformation numérique de ces trente dernières années a profondément modifié la société et les comportements de chacun. Les outils technologiques font effectivement partie de notre quotidien - au point, souvent, de ne plus pouvoir s'en passer - et sont surtout d'importants vecteurs de captation et de diffusion d'informations en temps réel et à grande échelle.

Ce faisant, les traitements de données à caractère personnel prolifèrent sans qu'ils ne soient toujours identifiés comme tels par les personnes qui en sont responsables, ni contrôlés voire contrôlables aussi bien par les personnes concernées que par les autorités. L'entrée en vigueur du règlement général à la protection des données à caractère personnel, dans le prolongement de la directive 95/46 et la loi n°78-17 du 6 janvier 1978 modifiée, a permis une prise de conscience plus importante des droits et obligations attachés à tout traitement de données personnelles. Il n'en reste pas moins que les cas d'usage des données personnelles, multiples et variés, soulèvent constamment des interrogations quant à leur soumission à ce corpus législatif et règlementaire et dans quelles limites.

C'était le cas de cette affaire soumise à la Cour de justice de l'Union européenne. Un particulier de nationalité lettone, M. Buivuids, qui se trouvait dans les locaux du commissariat de police nationale, a filmé la prise de sa déposition dans le cadre d'une procédure d'infraction administrative. La vidéo réalisée, qui montrait ainsi des membres de la police et leur activité dans le commissariat, a été publiée par M. Buivuids sur le célèbre site de vidéos en ligne YouTube. L'Autorité nationale de protection des données locale a considéré que, par-là, Monsieur Buivuids avait violé certaines dispositions de la loi lettone relative à la protection des données transposant la directive 95/46 - applicable aux faits concernés - notamment parce qu'il n'avait pas respecté le droit à l'information des membres de la police, en leur qualité de personnes concernées, en particulier sur la finalité du traitement de leurs données. M. Buivuids estimait, quant à lui, que, par la publication de cette vidéo, il avait tenté d'attirer l'attention de la société sur une action de la police qu'il considérait comme illégale. Il a également fait valoir que la vidéo montrait des fonctionnaires de la police nationale, c'est-à-dire des personnes publiques dans un lieu accessible au public, qui ne relèveraient pas à ce titre du champ d'application personnel de la loi relative à la protection des données à caractère personnel.

C'est dans ce cadre que la CJUE a été saisie par la Cour suprême lettone, statuant sur le litige, de deux questions préjudicielles :

1. « Les actions telles que celles en cause dans la présente affaire (filmer des membres de la police dans un commissariat de police pendant l'exécution d'actes de nature procédurale et publier la vidéo ainsi enregistrée sur le site Internet www.youtube.com) relèvent-elles du champ d'application de la directive 95/46 ?

2. Convient-il d'interpréter la directive 95/46 en ce sens que les actions susmentionnées peuvent être considérées comme un traitement de données à caractère personnel aux fins de journalisme, au sens de l'article 9 de la directive [95/46] ? ».

A noter que si cet arrêt a été rendu au visa de la Directive 95/46, il intéresse des règles qui ont été reprises de façon identique ou similaire

dans le RGPD et la loi n°78-17 du 6 janvier 1978 telle que modifiée, ce qui le rend d'autant plus intéressant.

L'enregistrement en cause et sa diffusion sur YouTube constituent bien des traitements de données à caractère personnel

Comme le rappelle CJUE, la directive 95/46 s'applique au traitement de données à caractère personnel automatisé en tout ou partie (la règle est la même pour le RGPD). Concernant l'enregistrement vidéo, la CJUE se réfère à sa jurisprudence passée, selon laquelle, d'une part, l'image d'une personne enregistrée par une caméra constitue une donnée à caractère personnel au sens de la directive 95/46, et d'autre part, un enregistrement vidéo de personnes stocké dans un dispositif d'enregistrement continu - à savoir le disque dur de ce système - est un traitement de données à caractère personnel automatisé conformément à ladite directive.

En l'espèce, parce « qu'il est possible de voir et d'entendre les membres de la police sur la vidéo en cause, de telle sorte qu'il y a lieu de considérer que les images des personnes ainsi enregistrées constituent autant de données à caractère personnel, au sens de l'article 2, sous a), de la directive 95/46 » et qu'il « s'agit d'un enregistrement vidéo des personnes stocké dans un dispositif d'enregistrement continu, à savoir la mémoire de ladite caméra [une caméra photo numérique] », il s'agit bien, pour la Cour, d'un traitement de données à caractère personnel au sens de la directive 95/46. S'agissant de la diffusion de la vidéo sur internet, la CJUE, s'appuyant sur deux précédents arrêts, a considéré que « le fait de publier sur un site Internet de vidéos, sur lequel les utilisateurs peuvent envoyer, regarder et partager celles-ci, un enregistrement vidéo, telle que la vidéo en cause » constitue bien un tel traitement. Si, sur le plan des principes, une telle position n'est pas surprenante, il en va autrement sur le terrain des exceptions dont ces traitements de données pourraient bénéficier…

Ces traitements n'entrent pas dans l'« exception domestique »

Après avoir caractérisé l'enregistrement vidéo et la diffusion en cause de traitement de données à caractère personnel, la CJUE s'est interrogée sur le point de savoir si ces traitements ne relèveraient pas de l'une des exceptions au champ d'application de la directive 95/46. Ce texte ne s'applique effectivement pas à deux types de traitements : ceux mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, et, en tout état de cause, ayant pour objet la sécurité publique, la défense, la sûreté de l'État et les activités de l'État relatives à des domaines du droit pénal ; ceux effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques. Ces deux exceptions ont été reprises de façon similaire dans le RGPD. Après avoir précisé que ces exceptions doivent faire l'objet d'une interprétation stricte, la CJUE a écarté fort logiquement l'application de la première exception aux traitements concernés. En effet, il a déjà été jugé que les activités visées par cette exception sont, dans tous les cas, des activités propres aux Etats et aux autorités étatiques, et donc étrangères à celles mises en œuvre par des particuliers, telle que celle de M. Buivuids.

De façon plus inattendue, la Cour a refusé de reconnaître que ces traitements ont été effectués pour des activités exclusivement personnelles ou domestiques, et ce pour la raison suivante : « dans la mesure où M. Buivuids a publié, sans restriction d'accès, la vidéo en cause sur un site Internet de vidéos sur lequel les utilisateurs peuvent envoyer, regarder et partager celles-ci, rendant ainsi

accessibles des données à caractère personnel à un nombre indéfini de personnes, le traitement de données à caractère personnel en cause au principal ne s'inscrit pas dans le cadre de l'exercice d'activités exclusivement personnelles ou domestiques ». La CJUE a adopté cette position « par analogie » avec des solutions dégagées dans d'autres affaires, lesquelles ne concernaient toutefois pas le cas de l'enregistrement d'une vidéo par un particulier ni sa publication sur la toile.

Une telle motivation, de par sa généralité, n'est pas sans conséquence sur la pratique courante de particuliers qui filment des évènements (manifestations…), des personnes dans des lieux publics ou privés et les partagent sur internet, via YouTube ou toute autre plateforme accessible, de façon générale, à tout internaute, tels que les réseaux sociaux (pour autant que les paramètres de confidentialité actionnés permettent une lecture et un partage de la vidéo par « un nombre indéfini de personnes »). En effet, sur ces vidéos, certaines personnes physiques peuvent apparaître et être identifiées ou identifiables. A suivre la CJUE, l'enregistrement et la diffusion de telles vidéos constituent des traitements de données à caractère personnel soumis à la législation et règlementation relative à la protection des données à caractère personnel impliquant ainsi, le respect, par celui qui les publie, d'un certain nombre d'obligations telles que le respect des droits des personnes concernées (droit à l'information, recueil du consentement, droit d'accès et de rectification…). Mais comment un vidéaste amateur pourrait, en pareil cas, obtenir le consentement des personnes concernées, leur fournir les informations requises notamment sur les finalités du traitement ou encore leur permettre de s'opposer à l'enregistrement et à la diffusion de la vidéo les faisant apparaître ?

Dans certains cas, ces traitements pourraient relever de l'exception journalistique

Pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression, la directive 95/46 laissaient le soin aux Etats membres de prévoir des exemptions au respect de certaines de ses règles, telles que le recueil du consentement et les droits des personnes concernées, notamment pour les traitements « effectués aux seules fins de journalisme ». Le RGPD donne aux Etats membres la même faculté. Si le législateur français a repris cette exception, il a, en revanche, précisé qu'elle ne concerne que les traitements qui ont pour seule fin « l'exercice, à titre professionnel, de l'activité de journaliste dans le respect des règles déontologiques de cette profession ». Dans son arrêt, la CJUE précise qu'il convient d'interpréter de manière large la notion de journalisme, et ce « afin de tenir compte de l'importance que détient la liberté d'expression dans toute société démocratique ». Pour la Cour, cette notion s'applique ainsi « non seulement aux entreprises de médias, mais également à toute personne exerçant des activités de journalisme » « qui ont pour finalité la divulgation au public, d'informations, d'opinions ou d'idées, sous quelque moyen de transmission que ce soit » y compris sur internet. La Cour en conclut que l'enregistrement et la diffusion en cause peuvent constituer un traitement de données à caractère personnel aux seules fins de journalisme, pour autant qu'il ressorte de la vidéo que ledit enregistrement et ladite diffusion ont pour seule finalité la divulgation au public d'informations, d'opinions ou d'idées, ce qu'il appartient à la juridiction de renvoi de vérifier. Toutefois, la CJUE livre d'ores et déjà des éléments d'interprétation importants : le fait que M. Buivuids ne soit pas un journaliste de profession et que la mise en ligne de la vidéo ait été effectuée sur un site Internet tel que YouTube ne sauraient exclure cette exception.

Ce faisant, les juges européens prennent une position bien plus souple que celle du législateur français, lequel, rappelons-le, limite

le bénéfice de l'exception journalistique aux seuls journalistes professionnels et « dans le respect de leurs règles déontologiques ». Cela signifie donc qu'en application de la législation française, un particulier, qui ne serait pas titulaire d'une carte de presse, ne pourrait pas se prévaloir de l'exception susvisée, de sorte que la publication de sa vidéo serait subordonnée au respect des obligations visées dans le RGPD, exposant ainsi ledit particulier à d'éventuelles sanctions. « Filmer, poster » : la prudence doit donc être de mise.

DOCTRINE

Alexandre FIEVEE

Alice ROBERT