Amendements proposés par **La Quadrature du Net** au projet de loi relatif à la protection des données personnelles, n° 490, déposé le 13 décembre 2017

17 janvier 2018

Article 7 - Données sensibles

Amendement

L'article 7 est ainsi modifié :

1° Avant le 2° est inséré un 1° bis ainsi rédigé : « Le 4° du II est complété par les mots suivants : «, dès lors que ces données révèlent à elles-seules les informations visées au I ».

2° Au 4°, le point ajouté est complété par les mots suivants : «, lorsque ce contrôle est justifié par des risques exceptionnels et qu'un tel accès ne peut être contrôlé en traitant des données non biométriques, et à la condition que, chaque fois que cela est possible, le traitement ne puisse être réalisé qu'à l'aide d'un support ou d'informations mises à la seule disposition de la personne concernée ».

3° Au 5°, la phrase ajoutée est complétée par les mots suivants : « et dont le traitement poursuit l'une des finalités visées aux b), g) et et j) du paragraphe 2 de l'article 9 du règlement (UE) 2016/679 ».

Justifications

L'objectif est de mettre en cohérence ces dispositions avec les recommandations de la CNIL et le RGPD.

1° L'article 9 du RGPD manque de précision en n'interdisant pas explicitement les traitements qui, recoupant des données non-sensibles que la personne concernée a publiées, visent à reconstituer des données sensibles qui, elles, n'ont jamais été publiées par la personne.

2° La CNIL a déjà élaboré une position sur le traitement de données biométriques pour contrôler l'accès au lieu de travail. En effet, en l'état du droit, un tel traitement est soumis à l'autorisation de la CNIL. Elle a ainsi produit deux autorisations uniques détaillant les conditions dans lesquelles ces traitements peuvent être mis en œuvre (https://www.cnil.fr/fr/le-controle-dacces-biometrique-sur-les-lieux-de-travail). Le RGPD faisant disparaître le rôle d'autorisation de la CNIL, celle-ci a annoncé que la licéité de ces traitements (alors automatiquement autorisés) devra être évaluée au regard des mêmes critères que ceux prévus dans ses autorisations uniques. Tel que la CNIL le propose dans son avis (page 14), le projet de loi gagnera en clarté à évoquer directement dans la loi de 1978 ces critères.

3° L'article 9 du RGPD n'autorise le traitement de données sensibles que pour certaines finalités dont il fait la liste exhaustive. Or, l'article 8, III, de la loi de 1978 (tel que modifié par le projet de loi) autoriserait les traitements de données sensibles poursuivant n'importe quelle finalité, pour la simple raison qu'une mesure technique serait appliquée : l'anonymisation à bref délai. Ceci n'est pas autorisé par le RGPD : cette autorisation doit être limitée à des finalités précises. Cette contradiction doit par conséquent être supprimée.

Pour autant, cette mesure d'anonymisation à bref délai n'est pas sans intérêt. En effet, l'article 9 du RGPD prévoit que, s'agissant de certaines finalités, le traitement de données sensibles n'est licite qu'en présence de « mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée ». Pour certaines de ces finalités, la loi de 1978 prévoit effectivement des garanties qui pourraient correspondre à ces « mesures appropriées ». Néanmoins, s'agissant d'autres finalités (celles visées au b), g) et j) du 2 de l'article 9 du règlement), la loi n'en prévoit aucune. Ainsi, dans ce cas précis, la mesure d'anonymisation à bref délai pourrait être une des « mesures appropriées » autorisant la poursuite de ces finalités.

Article 10 bis (nouveau) - Chiffrement

Amendement

Après l'article 10, il est inséré un article 10 bis ainsi rédigé :

Le premier alinéa de l'article 34 de la même loi est complété par la phrase suivante : « Cela implique notamment que, chaque fois que cela est possible, les données soient chiffrées de sorte à n'être accessibles qu'au moyen d'une clef mise à la seule disposition des personnes autorisées à accéder à ces données. »

Justifications

Cet amendement vise à rendre explicite que l'obligation de sécurité prévue dans le règlement se traduit en obligation de chiffrer de bout en bout chaque fois que cela est possible. En effet, le chiffrement de bout en bout où seules les personnes autorisées à accéder aux données (par exemple l'expéditeur et le/les destinataire/s d'un message) ont la clef limite considérablement les risques d'intrusion.

Article 13 bis (nouveau) - Consentement

Amendement

Avant l'article 14, il est inséré un article 13 bis ainsi rédigé :

L'article 7 de la même loi est complété par l'alinéa suivant :

« Pour être valide, le consentement de la personne concernée doit être donné de façon explicite, libre, spécifique et informée. Cela implique notamment que son consentement ne soit pas exigé en contrepartie d'un bien ou d'un service, à moins que le traitement faisant l'objet du consentement ne soit indispensable à la fourniture de ce bien ou service. »

Justifications

Cet amendement vise à intégrer la définition déterminante donnée par la CNIL et le G29 du caractère libre du consentement (voir les dernières propositions de lignes direcrices produites par le G29 à ce sujet : http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849).

Article 16 - Action de groupe

Amendement

L'article 16 est ainsi modifié :

Le dernier alinéa est complété par la phrase suivante : « Lorsqu'elle constate un manquement, la Commission peut ordonner au responsable de traitement de rembourser à l'association ou à l'organisation qui en fait la demande les frais engagés par celle-ci pour exercer les droits des personnes concernées ».

Justifications

L'action de groupe instituée par le RGPD ne saurait revêtir un caractère effectif si elle ne reposait sur aucune source de financement dédiée. À moins que les personnes concernées ne puissent être indemnisées du préjudice qu'elles ont subi, il y a peu de chance qu'elles financent elles-mêmes une association pour les représenter. Or, mener efficacement une action de groupe a un coût important, qui peut s'avérer dissuasif sans mesures d'accompagnement appropriées. Mettre directement ce coût à la charge des responsables de traitements sanctionnés permettra d'atteindre l'équilibre financier le plus pertinent.

Article 21 - Liberté d'expression

Amendement

L'article 21 est ainsi modifié :

1° Après le 6° est inséré un 6° bis ainsi rédigé : « Le titre du chapitre XI est remplacé par le titre suivant : « Publication de données à caractère personnel. » ».

2° Le 7°, a), est remplacé par le point suivant : « Le premier alinéa est remplacé par l'alinéa suivant : « Les traitements qui consistent à mettre des données personnelles à disposition du public ne sont licites qu'avec le consentement de la personne concernée ou si ces données contribuent à un débat d'intérêt général. Le 5° de l'article 6, les articles 8, 9, 32, et 39 et les articles 68 à 70 ne s'appliquent pas à de tels traitements, de même que le e) du 1 de l'article 4, les articles 10, 13 et 14 et le chapitre V du règlement (UE) 2016/679. » ».

Justifications

L'article 85 du RGPD exige que « les États membres concilient, par la loi, le droit à la protection des données à caractère personnel au titre du présent règlement et le droit à la liberté d'expression et d'information ».

Or, la loi de 1978 se contente de prévoir une série de dérogations (à l'interdiction de traiter des données sensibles ou à l'obligation de déclaration, par exemple) en faveur des seuls traitements mis en œuvre aux fins d'expression littéraire et artistique ou d'exercice de la profession de journaliste. Ce faisant, la loi ne concilie qu'une partie particulièrement réduite de la liberté d'expression avec le droit à la protection des données, omettant entièrement de concilier toutes les autres façons dont la liberté d'expression et d'information peut être mise en œuvre (débats politiques publics entre particuliers, investigations réalisées par d'autres personnes que des journalistes professionnels, etc.). La loi est trop restreinte et se conformer au règlement exige donc de viser le champ complet des activités mettant en œuvre la liberté d'expression et d'information : la publication de données personnelles, par n'importe quelle personne.

Ensuite, la loi de 1978 est floue sur la base légale qui autorise la publication de données personnelles (par des journalistes ou autres). Dans la plus part des cas, cette base est l'intérêt légitime du public à avoir accès à l'information publiée (le 5° de l'article 7 de la loi de 1978 autorisant les traitements poursuivant la réalisation de l'intérêt légitime du destinataire des données). Ce flou rend la loi trop imprévisibile pour concilier efficacement la liberté d'expression et le droit à la protection des données. L'amendement proposé vise à corriger ce défaut en intégrant explicitement la jurisprudence très claire de la Cour européenne des droits de l'Homme, qui réalise cette conciliation en autorisant uniquement les atteintes à la vie privée qui sont une « *contribution à un débat d'intérêt général* », en considérant « *qu'ont trait à [cet] intérêt général les questions qui touchent le public dans une mesure telle qu'il peut légitimement s'y intéresser, qui éveillent son attention ou le préoccupent sensiblement notamment parce qu'elles concernent le bien-être des citoyens ou la vie de la collectivité* » (CEDH, Grande chambre, 10 novembre 2015, Couderc et Hachette Filipacchi associés c. France, req. n°40454/07, § 103).

Enfin, la loi de 1978 (dans son état actuel et telle que modifiée par l'actuel projet de loi) prévoit une dérogation injustifiable à l'article 40, I : dès lors qu'un traitement de données à caractère personnel bénéficie d'une dérogation pour liberté d'expression, les personnes concernées ne peuvent pas exiger du responsable de traitement que des informations les concernant soient corrigées ou effacées lorsqu'elles sont inexactes ou que leur publication est illicite. Cette dérogation doit être supprimée.

Article 19 bis (nouveau) - Activités de renseignement

Amendement

Après l'article 19, il est inséré un article 19 bis ainsi rédigé :

1° Après l'article L. 822-4 du code de la sécurité intérieure, est créé un article L. 822-5 ainsi rédigé : « Lorsque la mise en œuvre d'une technique de recueil de renseignement prend fin, le service qui l'a réalisée informe promptement la personne concernée de la nature et de la durée de la technique, du type et du volume de renseignements recueillis, de la finalité du recueil et de l'identité du service, ainsi que de ses droits prévus à l'article L. 841-1 du présent code. La transmission de ces informations ne peut être retardée qu'en présence d'un risque manifeste et effectif de compromettre l'objectif qui a initialement justifié la mise en œuvre de la technique, et à la condition que la Commission nationale de contrôle des techniques de renseignement soit dûment informée de ce retard ».

2° Au 4° de l'article L. 833-2 du code de la sécurité intérieure, les mots suivants sont supprimés : « communiqués par des services étrangers ou par des organismes internationaux ou ».

3° À l'article L. 854-9 du code de la sécurité intérieure, avant le dernier alinéa, est ajouté l'alinéa suivant : « Le Conseil d'État, statuant dans les conditions prévues au chapitre III bis du titre VII du livre VII du code de justice administrative, peut aussi être saisi par toute personne souhaitant vérifier qu'aucune technique de renseignement prévue au présent chapitre n'est irrégulièrement mise en œuvre à son égard et justifiant de la mise en œuvre préalable de la procédure prévue au quatrième alinéa du présent article ».

4° À l'article L. 863-2, à la fin du premier alinéa, est ajoutée la phrase suivante : « Ces services ne peuvent transmettre ou obtenir des renseignements à d'autres services, français ou étrangers, que dans les conditions prévues au chapitre Ier du titre II du présent livre ainsi que, s'agissant des autorités d'un État n'appartenant pas à l'Union européenne, dans les conditions prévues à l'article 70-25 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ».

Justifications

1° Le premier paragraphe de l'article 13 de la directive (UE) 2016/680 exige que le responsable de traitement mette à la disposition des personnes concernées les informations concernant l'identité du responsable, les finalités du traitement et les droits de la personne concernée et ne prévoit aucune dérogation à cette mesure. Les seules dérogations de l'article concernent le deuxième paragraphe sur la communication d'autres types d'informations, telle que la nature des données traitées lorsque la finalité poursuivie les permet. Or, le code de la sécurité intérieure autorise des traitements de données personnelles sans prévoir que les personnes concernées ne reçoivent la moindre information, en aucune circonstance. Cette absence d'information est donc contraire à la directive et doit être corrigée.

2° L'article 46, 1, a), de la directive (UE) 2016/680 exige que, dans chaque État membre, une autorité « *contrôle l'application des dispositions adoptées en application de [cette] directive et de ses mesures d'exécution et veille au respect de celles-ci* ». En France, en matière de renseignement, cette autorité de contrôle est définie par l'article L. 833-1 du code de la sécurité intérieure comme étant la Commission nationale de contrôle des techniques de renseignement (CNCTR). L'article 47, 1, de la directive (UE) 2016/680 exige que « chaque État membre prévoit, par la loi, que chaque autorité de contrôle dispose de pouvoirs d'enquête effectifs. Ces pouvoirs comprennent au moins celui d'obtenir du responsable du traitement ou du sous-traitant l'accès à toutes les données à caractère personnel qui sont traitées ». Or, l'article L. 833-2, 4°, du code de la sécurité intérieure prévoit que la CNCTR ne peut pas avoir accès aux renseignements collectés, exploités, échangés ou conservés par les services français dès lors que ces renseignement ont

initialement été « *communiqués par des services étrangers ou par des organismes internationaux* ». Cela empêche frontalement la CNCTR de vérifier que les données personnelles collectées et exploitées par les services le sont de façon licite, ce qui est en totale contradiction avec les exigences de la directive.

3° L'article 54 de la directive (UE) 2016/680 exige, sans aucune exception possible, que les États membres ouvrent aux particuliers une voie de recours juridictionnel pour contester la licéité d'un traitement portant sur leur données personnelles (et ce indépendamment des voies administratives qui leur seraient ouvertes par ailleurs). Or, l'article L. 854-9 du code de la sécurité intérieure prévoit que, en matière de surveillance internationale (et contrairement au droit commun du renseignement), les particuliers ne peuvent pas agir en justice pour contester la licéité d'une mesure mise en œuvre à leur égard - seule la CNCTR a ce pouvoir, étant entièrement libre d'agir ou non. Cette absence de voie de recours juridictionnel est parfaitement contraire aux exigences de la directive et doit être corrigée.

4° Le code de la sécurité intérieure n'impose aucune condition ni contrôle s'agissant des échanges de renseignement par les autorités françaises avec d'autres autorités, françaises ou étrangères. Le code doit ainsi être modifié, non seulement pour imposer aux autorités françaises de respecter le cadre des transferts hors-UE posé par la directive (UE) 2016/680, mais aussi pour exiger que ces échanges, avec des autorités françaises, européennes ou hors-UE, poursuivent un des intérêts fondamentaux de la Nation prévus à l'article L. 811-3 du code (tel que doit le faire n'importe quelle autre collecte de renseignement) et que la CNCTR soit en mesure d'en assurer le contrôle.