Que signifie pour une personne concernée de rendre ses données personnelles « manifestement publiques » ?

Valentin Conrad, le 5 novembre 2021

EDWARD S. DOVE et JIAHONG CHANG ont publié récemment un article sur les conséquences juridiques de la publication volontaire de données personnelles à l'aune du RGPD. En voici les éléments clés.

EDWARD S. DOVE et JIAHONG CHANG ont publié récemment un article sur les conséquences juridiques de la publication volontaire de données personnelles à l'aune du RGPD (EDWARD S. DOVE/JIAHONG CHANG, What does it mean for a data subject to make their personal data 'manifestly public' ? An analysis of GDPR Article 9(2)(e), in International Data Privacy Law, Vol. 11, No. 2, pp. 107 ss). Ils dépeignent aussi certains exemples, dans le secteur des données génétiques ou génomiques, mais nous nous bornerons à circonscrire la présente contribution aux réflexions juridiques théoriques de l'article.

En introduction, les auteurs rappellent notamment que le traitement de données sensibles (ou portant sur des catégories particulières de données à caractère personnel selon la terminologie européenne) requiert deux conditions : (i) le traitement doit reposer sur l'une des six bases de légitimité ancrées à l'art. 6 par. 1 RGPD et (ii) le traitement doit se prévaloir de l'une des dix exceptions prévues par l'art. 9 par. 2 RGPD. En effet, le traitement de données personnelles sensibles est en général prohibé.

Parmi ces exceptions, lorsque des données sensibles sont rendues manifestement publiques, l'interdiction général de traitement ne s'applique plus (art. 9 par. 2 let. e RGPD) – pour autant que le traitement repose, en sus, sur une base de légitimité (art. 6 RGPD). Par commodité, nous utilisons le terme de 'données sensibles' pour désigner les catégories particulières de données personnelles dont fait l'objet cet article (qui regroupent notamment les données de santé, les données ethniques, les convictions religieuses ou politiques, etc.). Les auteurs rappellent aussi que les rares guides traitant du sujet se bornent à expliquer que cette exception doit être interprétée restrictivement.

À la suite d'exemples traitant de registres ou plateformes publics permettant l'accès à des données génétiques ou génomiques, les auteurs constatent que le choix de l'exception invoquée entraîne des conséquences juridiques différentes. En effet, le responsable de traitement

qui traitera des données sensibles hésitera entre les exceptions suivantes pour légitimer son traitement de données personnelles : le consentement explicite (art. 9 par. 2 let. a RGPD), la recherche scientifique (art. 9 par. 2 let. j RGPD), ou la publication volontaire (art. 9 par. 2 let. e RGPD).

S'il choisit le consentement explicite, la personne concernée, qui accepte donc de rendre publiquement accessibles des données sensibles, conservera son droit de retirer son consentement en tout temps et obligera généralement le responsable de traitement à non seulement effacer les données concernées (art. 17 par. 1 let. b RGPD), mais aussi à communiquer, si cela n'occasionne pas d'efforts techniques ou financiers disproportionnés, le retrait du consentement aux utilisateurs qui ont téléchargé les données concernées (art. 17 par. 2 RGPD).

Au demeurant, la validité dudit consentement pourrait toutefois être contestée au motif que le but des traitements ultérieurs des données personnelles sensibles n'est pas clairement établi au moment où la personne concernée donne son consentement. Les auteurs mettent en exergue aussi le fait que les États membres peuvent interdire, dans leur législation nationale, aux personnes concernées de consentir à certains traitements de données sensibles et peuvent limiter le traitement de données génétiques, biométriques, ou de santé (art. 9 par. 2 let. a *in fine cum* art. 9 par. 4 RGPD).

Si le responsable de traitement choisit l'exception fondée sur la mise à disposition manifeste du public de données sensibles par les personne concernées, il sera plus difficile pour ces dernières de s'opposer par la suite aux traitements ultérieurs de leurs données sensibles, même si elles peuvent en théorie s'opposer au traitement de leurs données personnelles (art. 21 RGPD).

Premièrement, le droit d'opposition ne garantit pas automatiquement l'effacement des données concernées (art. 17 par. 2 let. c RGPD) puisque le responsable de traitement pourrait lui opposer un motif légitime impérieux.

Deuxièmement, le champ d'application du droit d'opposition inscrit à l'art. 21 RGPD est fortement limité. Le droit d'opposition par la personne concernée n'existe que si la base de légitimité ressort notamment d'une mission d'intérêt public ou d'un intérêt légitime poursuivi par le responsable de traitement (art. 21 par. 1 RGPD). Selon les auteurs, il en résulterait que les responsables de traitement seraient plus enclins à soulever le consentement explicite comme exception à l'interdiction de traiter des données personnelles sensibles, car cela sauvegarde mieux les intérêts des personnes concernées. Par ailleurs, ils soulèvent les

contradictions d'interprétation des termes « manifestement rendues publiques » par les autorités de protection des données.

Pour mieux appréhender la teneur de l'art. 9 par. 1 let. e RGPD, Edward S. Dove et Jiahong Chang proposent une analyse en trois temps :

1. il sied de vérifier que l'activité de traitement est directement liée aux données rendues publiques ;
2. il existe des indices que la personne concernée a, par un acte délibéré et affirmatif, rendu les données publiques et que ces données peuvent raisonnablement être accessible par un membre intéressé du public ;
3. la personne concernée a rendu elle-même ses données personnelles accessibles ou a donné une indication claire à un intermédiaire de le faire à sa place.

Pour conclure, les auteurs jugent l'exception de la mise à disposition manifeste du public de données sensibles comme n'étant ni éthiquement ni juridiquement appropriée. En outre, l'invocation de cette exception nécessite de remplir des standards élevés. Nous sommes plutôt d'accord avec ce constat.

Bien que ce ne soit pas le propos de l'article, il est cependant dommage que les auteurs effleurent seulement l'exception liée à la recherche scientifique. Ils soulèvent quand même que l'exception liée à la recherche (art. 9 par. 2 let. j RGPD) oblige les chercheurs à un devoir accru en matière de sécurité des données, mais pourrait les exempter de redemander le consentement des personnes concernées comme base de légitimité, car le RGPD présume la compatibilité d'un but de recherche scientifique avec le but initial du traitement de données personnelles (art. 5 par. 1 let. b RGPD). Nous ajouterions que les allègements liés à la recherche dépendent essentiellement du droit des États membres de l'Union européenne (art. 89 par. 2 RGPD), ce qui complique passablement la tâche des chercheurs.

Commentaire

Il était intéressant de mettre en exergue cet article, car de nombreux chercheurs, dans nos universités ou centres de recherche, utilisent des données publiques, issues de registres publics ou des réseaux sociaux, pour réaliser leurs projets de recherche, pour entraîner leurs algorithmes, ou pour enrichir leurs bases de données.

Or, le fait qu'une donnée personnelle soit accessible au public n'ôte pas aux données concernées leur protection issue du droit de la personnalité ou de la protection des données, les

données personnelles étant un prolongement de notre personnalité juridique, fussent-elles publiques. D'aucuns confondent fréquemment la possibilité d'utiliser une œuvre publique, car fondée sur le droit d'auteur (à travers la publication sous licence libre), et la possibilité d'utiliser des données personnelles.

En Suisse aussi, nous avons une disposition similaire, mais dont le champ d'application s'applique tant aux données sensibles qu'aux données personnelles ordinaires. Il faut rappeler ici que le droit suisse n'exige pas de base de légitimité pour traiter des données personnelles – sauf pour les organes fédéraux, lesquels sont soumis au principe de la légalité – mais protège contre les traitements de données qui porteraient atteintes à la personnalité des personnes concernées. L'art. 30 al. 3 nLPD prévoit que « En règle générale, il n'y a pas atteinte à la personnalité lorsque la personne concernée a rendu les données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement ». Différentes décisions judiciaires ont pu préciser son libellé.

À l'instar de ce que proposent Edward S. Dove et Jiahong Chang à l'aune du RGPD, le Tribunal administratif fédéral a par exemple exigé que les données personnelles soient divulguées publiquement par la personne elle-même et de façon volontaire. De plus, il ne suffit pas de tolérer l'action d'un tiers sans contribuer à rendre accessible les données. Un comportement passif de la personne concernée ne suffit pas à admettre son intention (TAF, arrêt A-4232/2015 du 18 avril 2017, consid. 5.4.1 ; TAF, arrêt A-4086/2007 du 26 février 2008, consid. 5).

Enfin, comme précisé dans le message du Conseil fédéral (FF 2017 6565), il s'agit d'une présomption légale et non d'une fiction, ce qui signifie que la personne concernée aura toujours la possibilité de démontrer qu'elle a subi une atteinte à sa personnalité.

Proposition de citation : Valentin Conrad, Que signifie pour une personne concernée de rendre ses données personnelles « manifestement publiques » ?, 5 novembre 2021 *in* www.swissprivacy.law/100