Consultation publique sur le règlement européen

SYNTHESE DES CONTRIBUTIONS SUR LA NOTIFICATION DE VIOLATIONS, LE CONSENTEMENT, LE PROFILAGE

En mars 2017, la CNIL a lancé une consultation publique sur le règlement européen à destination des professionnels, afin de recueillir les questions concrètes, les difficultés d'interprétation et des exemples de bonnes pratiques.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Table des matières

Les contributions reçues au sujet de la notification des violations de données personnelles 3

Les principales questions posées : 3

1. Qui doit notifier ? 3
2. Dans quel cas la notification de violation de données n'est-elle pas nécessaire ? 3
3. A quel moment doit-on notifier ? 4
4. Quels éléments doivent figurer dans la notification ? 4
5. Dans quels cas et comment informer les personnes concernées ? 5
6. Autres sujets concernant la notification de violations 5

Les propositions (verbatim) 6

A retenir 7

Plan d'action G29 – prochaines étapes et livrables 7

Les contributions reçues au sujet consentement 8

Les principales questions posées : 8

1. Qu'est-ce que le consentement ? 8
2. Le consentement des mineurs et la collecte de données sensibles 8
3. Comment prouver le consentement ? 9
4. Le retrait du consentement 9
5. Autres sujets concernant le consentement 10

Les propositions (verbatim) 10

À retenir 12

Plan d'action G29 – prochaines étapes et livrables 12

Les contributions reçues au sujet du profilage 13

Les principales questions posées : 13

1. Le profilage : pourquoi et comment ? 13
2. Quelles garanties pour les personnes concernées ? 13
3. Le profilage et les réseaux sociaux 14
4. Comment intégrer les principes de "privacy by design and by default" dans le profilage? 15
5. Le profilage appliqué à votre secteur d'activité 15
6. Je fais l'objet d'un profilage : quelles limites ? 15
7. Autres sujets concernant le profilage 16

Les propositions (verbatim) 16

A retenir 17
Plan d'action G29 – prochaines étapes et livrables..... 17

Les contributions reçues au sujet de la notification des violations de données personnelles

La consultation relative à la notification des violations de données personnelles a fait l'objet de 146 contributions auxquelles s'ajoutent celles de la FFA, la FBF, de Syntec Numérique et du collectif ACT.

146 contributions
107 votes

Les principales questions posées :

Il ressort de la consultation 2 types de contributions, s'opposant parfois :

- 1. Des propositions d'interprétation opérationnelles des dispositions du règlement européen sur la protection des données, avec une approche par les risques laissée à l'appréciation des organismes,
- 2. Des questions d'interprétation, sur des notions telles que le risque ou des demandes de guides de conduite basés sur l'exemple, afin de guider finement les organismes.

1. Qui doit notifier ?

39 contributions – 30 votes

Les contributions publiées mettent tout d'abord en avant que la notion de « violation » est majoritairement rattachée à une atteinte à la confidentialité des données. Leur intégrité et leur disponibilité est moins visible ou moins prise en compte dans la réflexion.

- Au sein des grandes et moyennes structures, le délégué à la protection des données devrait être, en collaboration avec le DSI et le RSSI et la hiérarchie, au centre du processus de notification de violations.
- Au sein des structures n'ayant pas désigné de délégué à la protection des données, la notification des violations sera-t-elle sous-traitée à des professionnels ? Est-ce possible ?
- En cas de coresponsabilité du traitement, qui devra être en charge de la notification ? Cela devrait être prévu contractuellement.
- En cas de traitement transfrontalier, qui doit notifier et à quelle(s) autorité(s) ?
- En cas d'intervention dans la chaine du traitement d'un sous-traitant, qui doit notifier quoi ? (cf. Article 33.2.du règlement)
- Lorsque le responsable du traitement est établi en-dehors de l'UE et fait appel à un sous-traitant établi au sein de l'UE, faut-il notifier si le sous-traitant subit une violation ? Le traitement vise-t-il l'UE ou pas ? Est-ce à prendre en compte ?
- Une violation qui serait révélée dans la presse et dont le responsable du traitement n'aurait pas eu écho peut-elle lui être reprochée ? Une activité de veille doit-elle être mise en œuvre ?
- Un responsable du traitement est-il responsable d'une violation si son sous-traitant ne la lui notifie pas tel que prévu par l'article 33-2 du règlement ?

2. Dans quel cas la notification de violation de données n'est-elle pas nécessaire ?

31 contributions – 38 votes

- Toutes les violations devraient être documentées en interne. cf. article 33-5.

- Il y a notification à l'autorité de contrôle uniquement lorsque la violation engendre un risque pour les droits et libertés des personnes. Les analyses d'impacts permettront de faire apparaitre la notion de risque ainsi que son niveau.
- Pouvez-vous définir ce qui est entendu par "risque" et par "risque élevé" ? Est-il possible de fournir des exemples ? Une grille de lecture des risques ?
- La CNIL peut-elle fournir un questionnaire préalable permettant d'aider le responsable du traitement à déterminer s'il y a notification à effectuer ou pas ?
- La loi CADA s'appliquera-t-elle à la documentation interne relative aux violations de données pour les organismes publics ?

3. A quel moment doit-on notifier ?

15 contributions – 6 votes

- Le texte du règlement (cf. Article 33-1) indique que la notification doit être réalisée dans les meilleurs délais et si possible 72h au plus tard après avoir pris connaissance de la notification.
- Le responsable du traitement doit-il s'assurer que la violation est avérée et non simplement potentielle avant de notifier une violation ?
- L'objectif étant de protéger les données personnelles, il semble préférable de notifier au plus tôt, de manière incomplète, et de mettre à jour la notification au fil de l'eau.
- Le délai de 72 heures ne devrait pas devenir une obsession (le règlement indique d'ailleurs "*si possible*"). Il ne faudrait pas, dans la précipitation, prendre de mauvaise décision ou créer un "sur-accident".
- Le considérant 87 précise que l'appréciation de la notification dans les meilleurs délais est fonction de la nature de la gravité de la violation des données à caractère personnel et de ses conséquences et effets négatifs pour la personne concernée.
- Les PME et TPE pourront-elles bénéficier d'une assistance pour l'identification de la conduite à tenir en cas de violation ?
- Des interrogations se posent concernant la sécurité et la confidentialité des données transmises aux autorités de contrôle.

4. Quels éléments doivent figurer dans la notification ?

16 contributions – 4 votes

- Le règlement européen sur la protection des données ne requiert pas la fourniture d'éléments techniques dans le registre du responsable de traitement. De tels éléments techniques ne devraient donc logiquement pas figurer dans la notification.
- La notification doit comporter les conséquences probables de la violation (art. 33. 3) c)). Cela ne revient-il pas à lister les impacts sur la vie privée identifiés lors de l'analyse d'impact ?
- La CNIL peut-elle fournir un formulaire type de notification à remplir par le responsable du traitement ou son délégué à la protection des données en cas de violation de données à caractère personnel (avec des cases à cocher sur la nature des données concernées, les pièces à fournir telles que des relevés techniques de la DSI etc.) ?
- La forme de la notification doit être multiple : écrit papier / électronique / langue…) et doit laisser le maximum de souplesse aux entreprises gérant la situation de crise.
- Quelle différence y-a-t-il entre le nombre de personnes concernées et le nombre d'enregistrements concernés ?

- Il est nécessaire que la CNIL prévoie une communication aux entreprises sur le devenir de cette notification, en garantissant la sécurité et la confidentialité des réseaux informatiques des autorités de contrôle pouvant recevoir les notifications.
- Des organismes ou groupements d'organismes sectoriels, soumis à différentes obligations de notification, estiment important d'initier une réflexion visant à répondre aux éléments de complexité engendrés par la mise en œuvre cumulée des obligations.

5. Dans quels cas et comment informer les personnes concernées ?

25 contributions – 16 votes

- La notification aux personnes concernées ne devrait servir qu'un unique objectif : leur donner la possibilité de se protéger, de prendre toute mesure pour réduire - voire annuler- les risques qui pèsent sur eux suite à la violation.
- Les autorités de contrôle pourraient-elles mettre à disposition des responsables du traitement des mentions d'information types ou des exemples d'information « *en des termes clairs et simples* » ?
- Comment rédiger le contenu du message ? Faut-il préconiser des mesures à prendre pour les personnes ? (changer son mot de passe, veiller à son compte en banque…).
- En cas de violation d'une base de données, un message public sur le site internet peut-il suffire pour être considéré comme communication ? Un mail renvoyant à ce message public dans lequel toutes les informations seraient données pourrait-il être suffisant ?
- Quel est le niveau requis de chiffrement pour que le responsable du traitement puisse être exonéré d'une communication aux personnes concernées ?
- Pour une meilleure efficacité de ces notifications à la personne, ne faudrait-il pas cibler les différents cas où le responsable de traitement doit informer les personnes concernées ?
- Comment définir « le risque élevé pour les droits et libertés des personnes physiques » ? Une échelle de gravité en cas de violation de données personnelles sera-t-elle définie et comment le responsable de traitement évaluera-t-il ce risque ? Qui va estimer si les mesures de protection mises en place étaient appropriées ?
- Serait-il possible de fournir quelques lignes directrices sur les exceptions (indices, exemples concrets de situations, mesures de sécurité appliquées sur les données," mesures ultérieures" garantissant que le risque n'est plus susceptible de se matérialiser) ?

6. Autres sujets concernant la notification de violations

20 contributions – 13 votes

- La CNIL envisage-t-elle de publier, sur base de ces notifications et de ses propres constats, une base de sinistralité sur lesquels les délégués à la protection des données pourraient s'appuyer pour consolider leurs recommandations ?
- Ne faudrait-il pas systématiquement, dans les études d'impact sur la vie privée (PIA), intégrer un chapitre relatif aux mesures à prendre en cas de violations ?
- Le règlement prévoit que l'autorité de contrôle « peut » exiger l'information des personnes concernées ou décider que cette information n'est pas nécessaire. Dans quels délais l'autorité se prononcera-t-elle ? Que peut conclure le responsable du traitement en cas de silence de l'autorité ?
- Comment doit-on articuler les dispositions du règlement relatives à la notification de violation de données personnelles avec les dispositions d'autres règlementations spécifiques, telles que la directive e-Privacy, la directive NIS, la LPM ou encore la directive sur les services de paiement (DSP2) ?

- Dans le cas d'une violation de données à caractère personnel ayant des points de rattachement avec plusieurs états membres faut-il utiliser les règles de l'article 56 (autorité chef de file) ? Quel critère appliquer lorsqu'il s'agit de personnes concernées dans plusieurs états membres ?

Les propositions (verbatim)

« […] les autorités doivent se coordonner, préparer des formulaires de notification standards et applicables à tous les pays de l'UE, qui doivent pouvoir être remplis en langue anglaise. »

« Il serait utile que le G29 propose une harmonisation des formules de notification et, afin de garantir une meilleure application des dispositions du règlement relatives à la notification de violation de données personnelles. »

« Il serait utile pour les entreprises que le G29 publie des exemples de cas où la notification aux autorités et/ou aux personnes n'est pas nécessaire en application du principe « de minimus non curat praetor » déjà utilisé dans d'autres domaines du droit et gestion du risque. »

« L'appréciation du préjudice pour la personne physique devrait être relativisée mais dûment motivée, avant de prendre la décision de notification à la personne, voire partagée avec les autorités de contrôle en cas de doute. »

« L'information aux personnes doit être certes complète mais concise. Le contenu doit être simple pour permettre la compréhension du risque. »

« Il est utile de mettre en place une procédure interne de gestion des violations de données personnelles et de disposer, à chaque fois que cela est possible, d'outils permettant la détection automatique des violations de données. »

A retenir

On retiendra principalement deux aspects :

D'une part la forte attente des petites et moyennes entreprises (mais pas uniquement) qui souhaitent des guides pratiques et opérationnels, avec des exemples concrets, afin de savoir comment les notions de risques et de risques élevés doivent être interprétés, dans le but de savoir comment réagir en cas de violation, à quel moment la notification à l'autorité est nécessaires ainsi qu'aux personnes.

D'autre part les organismes plus importants ou plus matures dans la gestion de risque souhaitent quant à eux avoir la possibilité de déterminer leurs niveaux de risque et gérer la crise.

La réponse, quelle qu'elle soit, doit être harmonisée afin que le règlement soit appliqué de façon homogène au sein des pays membres et ce dans l'objectif de ne pas créer de déséquilibres. Les organismes et fédérations professionnelles veulent se préparer dès maintenant et de façon sécurisée à la mise en œuvre concrète de leurs futures obligations.

Des questions se posent quant à l'organisation interne notamment dès lors que le traitement fait appel à des sous-traitants, une coresponsabilité dans la gestion du traitement ou encore dans le cas de traitements transfrontaliers.

Enfin, les contributeurs insistent sur le niveau de confidentialité de ces notifications et sur les mesures de sécurité que les autorités de contrôle devront mettre en œuvre pour les protéger.

Ainsi, au-delà des incontournables actions de communication du G29 et de la CNIL, des supports et outils didactiques semblent particulièrement bienvenus.

Plan d'action G29 – prochaines étapes

Dans le cadre du plan d'actions 2017 du G29, des lignes directrices seront publiées pour accompagner de façon pragmatique les responsables de traitements. Les outils et canaux de déclaration des violations doivent être mis en chantier.

Pour assurer sereinement cette nouvelle obligation, la CNIL réalisera également dans ce contexte des actions de communication auprès des organismes.

Les contributions reçues au sujet consentement

La consultation relative au consentement a fait l'objet de 153 contributions auxquelles s'ajoutent celles de l'AACC, de l'UDA, de la FFA, de la FBF, de SFR, du Syntec Numérique, du Collectif ACT – AFAI, CIGREF, TECH IN France.

153 contributions
106 Votes

Les principales questions posées :

Il ressort de la consultation 3 types de contributions:

- 1. Comment interpréter opérationnellement les dispositions du règlement européen sur la protection des données ?
- 2. La CNIL envisage-t-elle la mise en place d'outils spécifiques ?
- 3. Comment évoluera la doctrine de la CNIL ?

1. Qu'est-ce que le consentement ?

34 contributions – 46 votes

- Qu'en est-il de la pratique des « *cookie walls* », sur la liberté du consentement (possibilité de donner accès limité à un service en cas de refus de consentir / ne pas autoriser l'accès si refus de consentir à un traitement strictement nécessaire au fonctionnement du service) ? Doit-on informer des conséquences du refus de consentir ? Quid des clicks accidentels ?
- Quid du consentement dans le cadre de la relation de travail quand il n'y a pas d'autre fondement ?
- Comment doit se matérialiser le recueil du consentement (case pré-cochée, non cochée, taille des boutons « *J'accepte* » supérieure à celles de « *Je n'accepte pas* ») ? Doit-on toujours considérer la poursuite de la navigation comme un acte positif ?
- Peut-on envisager des finalités types nécessitant le consentement (ie surtout celles qui ne le nécessitent pas) ? Peut-on envisager un consentement par groupe de finalités ?
- Il est nécessaire d'adapter les modalités de recueil du consentement au contexte de réalisation du traitement, de la collecte des données et au contexte d'utilisation du service (remplissage d'un formulaire, ou case à cocher, ou poursuite de la navigation). Ainsi, si le contexte ne le justifie pas, le consentement pourrait ne pas être le bon fondement.
- Comment recueillir un consentement dans le contexte des objets connectés ?
- La notion de consentement explicite ne vaut que pour certains traitements (données sensibles, transferts, décisions automatisées). Pour les autres traitements, le consentement peut ne pas être explicite.
- Il devrait être possible de centraliser sur une page dédiée les modalités d'utilisation des données plutôt que d'avoir à recueillir à chaque fois sur tous les formulaires le consentement spécifique de la personne (et éviter les contradictions).

2. Le consentement des mineurs et la collecte de données sensibles

25 contributions – 12 votes

- Que signifie le terme « *explicite* » pour la collecte de ce type de données ? Possibilité de renvoyer à des informations types sur la notion de données sensibles (sur le site des autorités de protection des données par exemple) ?
- Doit-on imposer une information sur les risques inhérents à l'exploitation des données sensibles ?
- Doit-on demander une pièce d'identité pour vérifier l'âge du mineur ? Ne pas se limiter au déclaratif. Doit-on imposer une solution d'identité numérique ? Doit-on encourager des programmes de « confiance en ligne » ?
- Comment gérer les différents âges seuils envisagés par les États membres ?
- Quelles sont les mesures raisonnables que pourrait mettre en place un responsable de traitement pour vérifier l'origine du consentement des parents ? Faut-il dresser une liste de données à collecter en ce sens ? Pour le consentement des parents, une procédure de type case à cocher en ligne avec attestation de la sincérité de la déclaration et rappel des sanctions encourues en cas de faux, est-elle suffisante ?
- Quel est le périmètre de l'article 8 ? S'applique-t-il uniquement aux services de la société d'information uniquement ou spécifiquement adressés aux mineurs ? Ou doit-on systématiquement demander l'âge des personnes ?

3. Comment prouver le consentement ?

40 contributions – 26 votes

- Quelle doit être la durée de conservation de la preuve du consentement ? Doit-on l'aligner sur la durée du traitement lui-même ? À quel moment la durée de conservation de la trace du consentement devient elle excessive ?
- Faut-il envisager différents niveaux de preuve selon l'impact des traitements ?
- L'obligation de la preuve du consentement a-t-elle un effet rétroactif ?
- Comment se ménager la preuve d'un consentement recueilli à l'oral (enregistrement) ?
- Comment concilier le principe de minimisation avec la collecte de données supplémentaires uniquement pour prouver le consentement ?
- Comment matérialiser la preuve du consentement ? Est-il possible de le déduire du comportement de l'utilisateur ? Doit-on, lorsque consentement est exprimé en ligne, conserver des logs ? S'il est possible de démontrer que le traitement est conforme au principe d'*accountability* du règlement (par exemple en démontrant le mode de fonctionnement du traitement) et qu'un service ne peut être utilisé que si la personne a exprimé un consentement, cela permet-il de prouver celui-ci ? La CNIL/G29 devrait proposer des scénarios types permettant de prouver le recueil (ou le retrait) du consentement et ce, pour différents canaux de communication (par téléphone, sur internet, sur un smartphone, à l'écrit, à l'oral…).
- Quelles seraient les conséquences en en cas d'usurpation d'identité (qui est responsable dans ce cas) ?

4. Le retrait du consentement

24 contributions – 15 votes

- Il paraît nécessaire de disposer d'un schéma de flux des données, indiquant les traitements dans lesquels les données sont impliquées.
- Comment concilier l'obligation de traçabilité du consentement et le respect du droit à l'effacement ?
- Si la possibilité de retirer son consentement est un principe clé posé par l'article 7 3° du règlement européen sur la protection des données, pour sa mise en œuvre pratique, il faudrait effectuer une mise en balance entre le retrait du consentement et ses conséquences sur les actes déjà engagés avant ce retrait et qui peuvent produire des effets après le retrait.

- Il est difficile, pour le responsable de traitement, de prendre immédiatement en compte ce retrait. Il devrait donc être permis un délai raisonnable nécessaire à l'effectivité du retrait du consentement (avec information de la personne sur le délai d'effectivité du retrait).
- Si une personne retire son consentement pour un traitement de données, ce retrait ne devrait pas faire obstacle au maintien des autres traitements qui restent valides sur d'autres fondements juridiques ou lorsque le consentement a été donné pour plusieurs finalités.
- Comment assurer un retrait du consentement dans le cadre de l'utilisation d'applications mobiles ?
- En matière d'assurance, le retrait du consentement (donné pour la collecte de données sensibles nécessaires à la conclusion du contrat) reviendrait à offrir un nouveau droit de résiliation au contrat.

5. Autres sujets concernant le consentement

30 contributions – 7 votes

- Comment s'adapter à des règlementations différentes qui imposeraient, pour certaines, le consentement à certains types de finalités de traitement (problématique groupes internationaux) ?
- Quid de la collecte indirecte de données ? En cas de collecte indirecte, la charge du recueil du consentement ainsi que sa preuve devrait reposer sur la personne qui a directement collecté (via clause contractuelle notamment).
- Comment articuler le règlement européen sur la protection des données avec le prochain règlement E-privacy ?
- Comment, dans certains secteurs très « mouvants » informer sur les destinataires des catégories de données ?

Les propositions (verbatim)

« La preuve du consentement doit en effet pouvoir être conservée durant la période pendant laquelle la responsabilité, pénale ou civile, du responsable de traitement, est susceptible d'être engagée. »

« L'horodatage informatique de la manifestation de la volonté (par un clic ou un acte de navigation) et la mise en place d'une procédure de recueil du consentement, dument documentée, doit pouvoir être considéré comme un moyen valable d'établir la preuve du consentement. »

« Le niveau d'exigence s'agissant de la qualité de la preuve doit être fonction du risque pour les personnes lié au traitement mis en œuvre. »

« La preuve du consentement nécessite trois éléments : ce à quoi la personne a consenti, le moment où elle a consenti, qui a consenti. »

« Dans la pratique, il est recommandable que le retrait de consentement puisse se faire par le même medium que celui utilisé pour donner le consentement : via formulaire papier ou électronique, via courrier, oralement… »

«

« Dans le cas d'un service en ligne, la personne concernée doit facilement avoir accès aux paramètres de confidentialité et doit pouvoir trouver simplement

comment mettre fin à l'exploitation de ses données. Par ailleurs il est indispensable de rappeler que le retrait du consentement doit non seulement entraîner la fin du traitement des données mais également l'effacement de celles-ci, et ce dans toute la chaîne de traitement de données. »

« Les conséquences du refus ainsi que les alternatives à l'absence de consentement devraient être clairement exposées au moment de la demande de consentement. »

« Si la personne ne manifeste pas clairement son consentement ou refuse le traitement dans l'hypothèse où celui-ci ne serait pas nécessaire pour accéder au service (tracker et cookie tiers en ligne par exemple), cela ne doit pas aboutir à un blocage du service. »

« Il doit pouvoir être possible de centraliser sur une page dédiée les modalités d'utilisation des données plutôt que d'avoir à recueillir à chaque fois sur tous les formulaires le consentement spécifique de la personne (et éviter les contradictions). »

« Le consentement aux traitements de données sensibles doit satisfaire les mêmes conditions que le consentement au traitement de n'importe quel type de donnée personnelle. Mais il est indispensable de rappeler l'importance du caractère spécifique du consentement lors du traitement de telles données, qui se matérialiserait par une case à cocher bien distincte. »

« Définir l'âge d'un utilisateur pour déterminer l'applicabilité du consentement revient à requérir une solution d'identité numérique qui permette de garantir avec un certain niveau de certitude que l'âge de l'utilisateur est soit supérieur à 18 ans, soit entre 16 ans et 18 ans, soit inférieur à 16 ans… »

À retenir

On retiendra les fortes attentes de réponses pragmatiques en lien avec les impératifs opérationnels et économiques des entreprises.

Pour la société civile, une application stricte des principes du règlement européen sur la protection des données est essentielle : la preuve du consentement doit être écrite, le refus de consentir ne doit pas interdire l'accès au service, le retrait du consentement doit entraîner l'effacement des données.

Pour les entreprises en revanche, une application souple est indispensable, leur permettant d'adapter le recueil du consentement en fonction du contexte du traitement, de l'expérience de l'utilisateur, du type des données traitées (consentement explicite notamment), etc. Elles rappellent en outre à de nombreuses reprises que le consentement constitue un des fondements, au même titre que l'intérêt légitime qui leur parait, dans les communications électroniques, plus approprié. Globalement, les remarques les plus récurrentes portent sur : les communications électroniques et tout particulièrement les témoins de connexion (recueil du consentement, preuve du consentement, intérêt légitime, retrait du consentement, acte positif, consentement explicite), les conséquences du refus à consentir, la particularité de consentement dans le cadre des relations de travail, les réelles difficultés à vérifier l'âge du mineur et, partant, à obtenir le consentement des parents.

Ainsi, des supports seraient particulièrement bienvenus, et notamment : une section dédiée aux données sensibles sur le site de la CNIL, la production de scénario type sur le recueil de la preuve du consentement, la liste des finalités nécessitant le consentement.

Plan d'action G29 – prochaines étapes

Publication de l'avis relatif au consentement envisagé pour le second semestre 2017.

La problématique relative aux cookies étant très présente à l'aune des différents retour, un avis du G29 sur le projet de règlement E-privacy est également prévu pour le mois de mai.

Les contributions reçues au sujet du profilage

La consultation relative au profilage a fait l'objet de 97 contributions auxquelles s'ajoutent celles de la Fédération Française de l'Assurance (FFA), de l'Association Agrée des Agents Commerciaux (AAAc), de SFR, de l'UDA (Union des Annonceurs en Mouvement), de la Fédération Bancaire Française (FBF), du Syntec Numérique, et du Collectif ACT – AFAI, CIGREF, TECH IN France.

97 contributions
61 Votes

Les principales questions posées :

Il ressort de la consultation 3 types de contributions:

- Une demande de définitions plus précises de certaines notions abordées dans les articles du règlement européen sur la protection des données relatifs au profilage :
- Une interrogation sur l'étendue des droits des personnes, notamment vis-à-vis du degré de précision de l'information à fournir à la personne concernée ainsi que de son consentement ;
- Une argumentation visant à prouver la nécessité du profilage dans certains secteurs d'activité, notamment en matière de marketing (publicité ciblée), du secteur public et dans le domaine des ressources humaines.

1. Le profilage : pourquoi et comment ?

28 contributions – 17 votes

- **Interrogations sur la définition:**
  - La notion d'impact significatif sur la vie privée : est-ce priver une personne d'un droit ? Ou proposer des conditions tarifaires moins favorables aux conditions normales ?
  - La personne concernée n'est-elle pas privée d'un droit s'il y a une intervention humaine ?
  - Il conviendrait de se séparer de l'idée selon laquelle l'impact est nécessairement financier : il peut s'agir d'un impact sur un droit ou une liberté, par exemple la liberté de penser ou d'avoir sa propre opinion politique car l'objectif du profilage est de devancer les désirs des personnes concernées
  - Pour qu'il y ait du profilage, doit-il y avoir une décision individuelle automatisée ? Qu'en est-il des souscriptions de contrats d'assurance qui se font entièrement en ligne : cela constitue-t-il du profilage ?
  - Le profilage devrait seulement être encadré s'il concerne des services essentiels : hypothèques, assurance et emplois ou s'il est attentatoire à la dignité et aux libertés.
- **Interrogations sur les formalités :**
  - Un DPIA est-il nécessaire en présence d'un profilage ?
  - Le profilage repose-t-il sur un système d'opt-in ou d'opt-out ?

2. Quelles garanties pour les personnes concernées ?

31 contributions – 12 votes

- **Information de la personne concernée :**

- Quel est le degré d'information à fournir à la personne concernée au sujet de la « logique sous-jacente » ? Faut-il informer les personnes de la segmentation réalisée ?
- Quid du *machine learning* dans la mesure où les données utilisées évoluent et sont « jetées » au fur et à mesure de l'amélioration de l'algorithme => comment informer la personne de la logique si les données sont jetées ?
- Est-il nécessaire de donner une information séparée des autres informations au sujet de l'existence d'une décision automatisée ou d'un profilage ? Si oui, sous quelle forme ?

- **Consentement des personnes :**
  - La formulation de l'article 22 peut induire que la règle par défaut est l'autorisation de ces pratiques et que la personne concernée doit spécifiquement demander à ne pas être profilée.
  - Si les conditions du profilage changent, comment le responsable du traitement peut-il s'assurer que la personne consent aux nouveaux aspects du traitement ? Doit-on lui envoyer un email ?
  - Le consentement de la personne doit avoir lieu au moment où elle envoie ses données personnelles qui vont servir au profilage
  - Les garanties de l'article 22 ne doivent être apportées que si le profilage entraine une privation des droits
  - Le responsable de traitement peut-il refuser de faire droit à la personne de contester la décision ? Le droit d'exprimer des remarques et des contestations est inadapté en cas de profilage lié à la prospection commerciale
- **Droit d'opposition :**
  - Ce droit s'applique-t-il lorsque la personne concernée a déjà consenti au profilage ? Ce droit est-il limité aux situations dans lesquelles le profilage conduit à une décision produisant « des effets juridiques ou affectant la personne de manière significative de façon similaire », sur un modèle similaire à celui prévu par l'article 22 ?
  - L'utilisateur ne voulant pas être profilé peut-il, tout simplement, ne pas poursuivre la navigation du site en cause mis gratuitement à sa disposition ?
- **Intervention humaine :**
  - Qui doit prouver que l'intervention humaine qui est mise en place est effective ? La personne concernée est-elle en mesure d'apporter la preuve qu'il y a bien eu une intervention humaine ?
  - Si dans 99% des cas, l'intervention humaine revient à confirmer la décision automatique, il faut remettre en question la validité de l'intervention humaine.
  - Dans le secteur des assurances, le droit à une intervention humaine est déjà mis en œuvre par les sociétés qui ont mis en place un service de réclamation.

3. Le profilage et les réseaux sociaux

1 contribution – 0 vote

- L'utilisation des données générées sur les réseaux sociaux pour mesurer la solvabilité pourrait encourager les utilisateurs à mentir et manipuler leur profil, ou même à faire appel à des entreprises s'occupant de la gestion de réputation en ligne
- Le profilage est utile pour aider les utilisateurs à des fins d'introspection : les utilisateurs peuvent en apprendre plus sur leurs habitudes alimentaires, sur leur manière de conduire.

4. Comment intégrer les principes de “privacy by design and by default” dans le profilage?

11 contributions – 3 votes

- La finalité du profilage doit être précise et concise et la collecte ne doit pas dépasser ce qui est nécessaire pour atteindre la finalité.
- Pour atteindre le privacy by design, le responsable de traitement doit faire preuve de transparence et divulguer les fondements de sa réponse automatique.
- La personne physique doit pouvoir s’authentifier avec une identité qu’elle a choisi librement (identité virtuelle, pseudonyme…)
- L’utilisation d’une blockchain pour le profilage permettrait d’atteindre le « privacy by design », car les données sont sécurisées, cryptographiées et consultables uniquement à travers des clés privées générés par les utilisateurs
- La transparence et la pédagogie à l’égard des clients sont importantes, ainsi que les études d’impact.

5. Le profilage appliqué à votre secteur d’activité

17 contributions – 15 votes

- Le profilage est nécessaire dans le secteur de services à la personne (handicap, dépendance, aide éducative), par exemple pour les algorithmes servant à anticiper les accidents des personnes âgées) => Serait-il opportun d’intégrer une notion d’opposition pour « motif légitime » ?
- Dans la santé : le profilage des clients d’une pharmacie pourrait permettre d’identifier les personnes qui seraient intéressées à participer dans des essais cliniques (puisque les données relatives à leur état de santé et les médicaments qu’elles prennent par exemple, seraient collectées).
- Secteur des assurances : le profilage est au cœur du secteur. Il n’est qu’un moyen et non une finalité (comme la géolocalisation). Il faut à ce titre faire une distinction entre la souscription d’un contrat pour une assurance de prêt (dans le cadre duquel l’évaluation porte directement sur la personne) et un contrat multirisques habitation (où c’est le bien qui est évalué, comme par exemple sa situation géographique, sa superficie…). Le fait d'examiner si des critères de souscription sont remplis ou non par une personne relève-t-il systématiquement du profilage ?
- Profilage des salariés et gestion du personnel/entretien annuel d’évaluation : le profilage permet de compléter les entretiens et d’envisager une meilleure allocation des ressources humaines. Le profilage est-il soumis au consentement du salarié ou rentre-t-il dans le cadre de l’exécution d’un contrat ?
- Profilage et marketing : Le fait d’offrir des offres ciblées a-t-il des effets juridiques ou affecte-t-il la personne concernée de manière significative ? Avantage des offres ciblées : la publicité est moins importune car elle est adaptée aux centres d’intérêts du consommateur. L’opposition doit prendre la forme d’une simple suppression de compte par la personne concernée ou la renonciation à utiliser le service. Le fait de déposer des cookies est-il constitutif de profilage ?
- Profilage et service public : le profilage permet l’optimisation des infrastructures techniques ainsi que son adaptabilité et contribue à garantir ainsi sa continuité. N’est-il pas nécessaire de distinguer profilage commercial et profilage public ?

6. Je fais l’objet d’un profilage : quelles limites ?

10 contributions –5 votes

- Il est nécessaire de pouvoir contester rapidement auprès d’une autorité compétente une décision automatisée prise sur la base de profilage (exemple : magistrats)
- Il est nécessaire d’être informé sur les conséquences de profilage, et aucun profilage ne devrait avoir lieu sans l’accord préalable de l’intéressé

- Est-il possible de réfléchir à des règles distinctes concernant le profilage dans le milieu professionnel et celui dans la sphère privée ?
- Est-il possible d'associer un logo au profilage pour l'identifier et le rattacher aux informations pertinentes, ex : « P » stylisé et cliquable afin de consulter les conditions générales attachées à ce profilage
- Interdiction de baser le profilage sur le consentement dans le cas des mineurs

7. Autres sujets concernant le profilage

17 contributions –9 votes

- Le profilage et les algorithmes partent du présupposé du libre arbitre parfait et absolu, alors qu'il est de plus en plus clair que nos actes sont influencés par notre environnement.

Les propositions (verbatim)

« En tout état de cause, à mon sens, le data marketing ou prospection ciblée ne doit pas être considéré comme produisant des effets juridiques ou affectant l'utilisateur de manière significative. »

« Intérêt de disposer d'une définition précise du profilage (finalité commerciale et par exemple, finalité de gestion d'un service public) avec des obligations différentiées. »

« Chaque personne concernée par un profilage (encore faut-il qu'elle le sache) doit pouvoir exprimer un droit à la singularité. »

« « Cela devrait-être à la charge du responsable de traitement de prouver que l'intervention humaine qu'il met en place est effective. »

« Pour auditer ce consentement explicite, cela signifie que la personne physique ait pu s'authentifier avec une identité qu'elle a choisie librement »

« Il pourrait néanmoins être intéressant d'encadrer le profilage, de définir le degré de profilage à ne pas dépasser pour éviter de porter atteinte à la vie privée des personnes concernées. »

« Ne serait-il pas plus adéquat d'intégrer une notion d'opposition pour "motif légitime" comme c'est déjà le cas pour l'opposition au traitement de données ? »

« Il me semble qu'il y a 2 aspects: le profilage dans le milieu professionnel et un profilage dans la sphère privée. »

« A partir du moment où le concept de profilage entre dans le règlement Européen et qu'il est structurant, il faut lui associer un logo simple et utilisable par tout le monde, pour s'y référer y trouver les conditions générales attachées à chaque profilage. »

« Le recours au profilage dans la publicité ciblée a donc de graves conséquences sur la liberté d'expression et sur la pluralité des opinions dans nos sociétés. »

A retenir

On retiendra les fortes attentes de la part des entreprises pratiquant la publicité ciblée, des organismes et fédérations professionnelles qui veulent se préparer dès maintenant et de façon sécurisée à la mise en œuvre concrète de leurs futures obligations.
Il existe également une attente forte quant à la définition de « l'impact significatif » et de la « décision automatisée ».
Enfin, les personnes concernées s'inquiètent de l'atteinte que peut porter le profilage à leur libre arbitre et à la possibilité de contester la décision prise sur le fondement d'un profilage.

Plan d'action G29 – prochaines étapes

Publication de l'avis relatif au profilage envisagé pour le second semestre 2017.