Données personnelles
Règlement 2016/679

Céline Castets-Renard

Professeur, Université Toulouse Capitole

Membre de l'Institut Universitaire de France

1. Nouvelles définitions du règlement 2016/679 (art. 4)

- «profilage» :
  - toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique;

Décision individuelle automatisée (profilage)

- Art. 22 : mesures fondées sur le profilage et décisions individuelles
- 1. 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.
- 2. Exceptions :
- a) décision nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement;
- b) décision est autorisée par le droit de l'Union ou le droit de l'État membre
- c) décision est fondée sur le consentement explicite de la personne concernée.

- 3. le responsable du traitement respecte le droit de la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision.
- Gouvernance des algorithmes / politique des algorithmes

2. Le champ d’application territorial

- Art. 3 règlement 2016/679 :
  - 1. Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.
- 2. Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées:
  - a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; ou
  - b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

Régime des données personnelles
3. Changement de logique

- La suppression des contraintes *a priori* pesant sur le responsable du traitement / le renforcement *a posterori* de sa responsabilité = d'un contrôle *a priori* (formalités préalables) à un contrôle *a posteriori*.
- D'une logique « bureaucratique » de contrôle à une logique de « responsabilisation »
- Suppression des obligations de notification préalable (déclaration/autorisation)
- En contrepartie : responsabilité renforcée = responsabilité globale
- Obligation de prévoir la protection des données dès la conception du traitement *privacy by design / privacy by default*
- Etudes d'impacts, registre des activités de traitement = mise en place de procédures internes d'*accountability* = rendre compte

Les principes, droits et obligations

LES OBLIGATIONS

- Obligation de collecte et traitement loyal et licite
- Finalités déterminées, licites et légitimes
- Les obligations d'exactitude et mise à jour
- Les obligations de confidentialité et sécurité
- Suppression déclaration/autorisation : nouvelles procédures internes = « accountability »

LES DROITS

- Principe du consentement préalable
- Le droit à l'information
- Le droit d'accès et rectification
- Le droit d'opposition
- Le droit à l'oubli/effacement
- Le droit à la portabilité

Obligations des responsables de traitement

- Art. 24 et suivants : responsabilité du responsable de traitement

adoption de règles internes

- Art. 24§1 :

  Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, **le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées** pour s'assurer et être en mesure de **démontrer** que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire.
- §2. Mise en œuvre d'une politique appropriée de protection des DP.
- §3. Peut se traduire par l'application d'un code de conduite (art. 40) ou des mécanismes de certification approuvés (art. 42)

- «pseudonymisation» :
  - le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable;

Privacy by design

- Art. 25§1 : protection des données dès la conception
  - Compte tenu de l'état des connaissances, des **coûts** de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des **risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques**, le responsable du traitement met en œuvre, tant au moment de la **détermination des moyens du traitement** qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la **pseudonymisation**, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la **minimisation des données, de façon effective** et à assortir le traitement des **garanties nécessaires** afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.
- Mécanisme de **certification** (art. 42) peut être utilisé pour prouver le respect de cette obligation

Sécurité des données

- Art. 32§1 obligation de sécurité des données
  - Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins:
  - a) la pseudonymisation et le chiffrement des données à caractère personnel
  - b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
  - c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;
- d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.
- §2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques
- §3. code de conduite approuvé (art. 40) ou certification approuvée (art. 42)

Notification des failles de sécurité

- Art. 33 : obligation de notifier les failles de sécurité à l'autorité de contrôle sauf si pas de risques pour les droits et libertés des personnes physiques. Indique notamment :
  - - nature de la violation
  - - conséquences probables de la violation
  - - mesures prises
- Art. 34 : notification à la personne concernée si risques élevés d'atteinte à sa vie privée et droits fondamentaux
- Mêmes informations

- Mêmes obligations à la charge du sous-traitant

Privacy by default

- Art. 25§2 :
  - Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, **par défaut**, seules les données à caractère personnel qui sont **nécessaires au regard de chaque finalité spécifique du traitement sont traitées**. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, **par défaut**, les données à caractère personnel **ne sont pas rendues accessibles à un nombre indéterminé** de personnes physiques sans l'intervention de la personne physique concernée.
- Mécanisme de **certification** (art. 42) peut être utilisé pour prouver le respect de cette obligation

Registre des activités de traitement

- Art. 30§1.
  - Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité :
    - - nom et coordonnées du responsable de traitement
    - - finalités du traitement
    - - description de catégories de personnes concernées et DP
    - - catégorie de destinataires
    - - flux transfrontaliers
    - Description générale des mesures de sécurité

- Mêmes obligations pour le sous-traitant

- Obligation de coopération avec l'autorité nationale de contrôle (art. 31)

Analyse d’impact

- Art. 35§1 :
  - analyse préalable d’impact pour les traitements présentant un risque élevé pour les droits et libertés des personnes physiques (nature, contexte, finalités du traitement)
- Art. 31§3 : analyse obligatoire
  - a) l'évaluation systématique et approfondie d'aspects personnels et sur la base de laquelle sont prises des décisions produisant des effets juridiques ou l'affectant de manière significative
  - b) le traitement à grande échelle de données sensibles ou de données relatives à des condamnations pénales et à des infractions
  - c) la surveillance systématique à grande échelle d'une zone accessible au public.

  - L’autorité nationale de contrôle peut établir une liste d’opérations de traitement pour lesquelles une analyse d’impact est requise

Quelle analyse d’impact ?

- Art. 35§7. L'analyse contient au moins:
- a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement;
- b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités;
- c) une évaluation des risques pour les droits et libertés des personnes concernées
- d) les mesures envisagées pour faire face aux risques, y compris les mesures de sécurité visant à assurer la protection des données

Consultation préalable

- *Article 36*
  - 1. Le responsable du traitement consulte l'autorité de contrôle préalablement au traitement lorsqu'une analyse d'impact indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque.
  - 2. Lorsque l'autorité de contrôle est d'avis que le traitement envisagé constituerait une violation du présent règlement, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque, l'autorité de contrôle fournit par écrit, dans un délai maximum de huit semaines à compter de la réception de la demande de consultation, un avis écrit au responsable du traitement

Codes de conduite

- Art. 40 :
  - 1. Les États membres, les autorités de contrôle, le comité et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer à la bonne application du présent règlement, compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises.
  - 2. Les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent élaborer des codes de conduite, les modifier ou les proroger, aux fins de préciser les modalités d'application du règlement
    - Traitement loyal et transparent
    - ex. intérêts légitimes du responsable de traitement
    - Pseudonymisation

Certifications

- Art. 42 :
  - Les États membres, les autorités de contrôle, le comité et la Commission encouragent, en particulier au niveau de l'Union, la mise en place de mécanismes de certification en matière de protection des données ainsi que de labels et de marques en la matière, aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le présent règlement. Les besoins spécifiques des micro, petites et moyennes entreprises sont pris en considération.

  - Organismes de certification : notamment les autorités nationales de contrôle

Procédures internes de conformité / Politique de protection des DP

- - registre de traitement des données
- - code de conduite ou certifications (labels reconnus par la CNIL)
- - études d'impact
- - *privacy by design / by default*
- - règles d'entreprise contraignantes en cas de flux transfrontaliers de données (BCR)

- - délégué à la protection des DP (obligatoire/facultatif)

4. Qui ?
Responsabilité du sous-traitant

- Art. 28 :
- §1. Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées (…)
- §2. Le sous-traitant ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement (…)
- §3. Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique (...), qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement.
- §5. Recours possible à un code de conduite approuvé (art. 40) ou à un mécanisme de certification approuvé (art. 42)
- §7. La Commission européenne peut établir des clauses contractuelles type (CCT)
- §8. Les autorités nationales de contrôle peuvent établir des CCT
- §10. Si le sous-traitant détermine les finalités et moyens du traitement, il est considéré comme responsable de traitement

Le délégué à la protection des données

- Art. 37 : désignation obligatoire lorsque :
  - a) le traitement est effectué par une autorité publique ou un organisme public
  - b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou
  - c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

Fonctions du délégué

- Art. 38§1 : est associé à toutes les questions relatives à la protection des DP
- §2 : est aidé dans ses missions (ressources nécessaires, connaissances spécifiques)
- §3 : ne reçoit aucune instruction. Ne peut être relevé de ses fonctions ou pénalisé. Fait rapport au niveau le plus élevé de la direction du responsable de traitement
- §4. personnes concernées peuvent prendre contact avec le délégué
- §5. Est soumis au secret professionnel

Missions du délégué

- Art. 39§1:
- - Informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent
- - contrôler le respect de la réglementation sur la protection des DP et règles internes du responsable de traitement
- - dispenser des conseils sur demande, en ce qui concerne l'analyse d'impact
- - coopérer avec l'autorité de contrôle
- - point de contact pour l'autorité de contrôle

- Art. 39§2 : tient compte du risque associé aux opérations de traitement

5. Recours et réparations dans le règlement

- Art. 77 et art. 78 : droit à un recours juridictionnel contre les autorités de contrôle : compétence des juridictions de l'Etat membre sur le territoire duquel l'autorité de contrôle est établie
- Art. 78 : recours juridictionnel contre les responsables des traitements : compétence des juridictions du lieu d'établissement du responsable ou lieu de résidence habituelle de la personne concernée = option de compétence
- Asymétrie des recours
- Droit à réparation : art. 82
- Sanctions pénales (art. 82) et sanctions administratives (art. 83) : montant élevé (jusqu'à 10 millions d'euros ou 2% du CA annuel mondial). Le double si récidive

Loi « pour une république numérique » adoptée le 7 octobre 2016

- Sanctions de la CNIL : De 150 000 euros à trois millions d'euros
- Phase de transition avant l'entrée en vigueur du règlement européen sur les données personnelles.
- À partir du 25 mai 2018, la CNIL pourra aller jusqu'à 20 millions d'euros (ou, pour les entreprises, 4 % de leur chiffre d'affaires annuel mondial) si récidive.

Conclusion

- Des avancées dans la protection des personnes physiques

  mais :

  - Un règlement qui risque de mal s'appliquer aux activités de l'économie numérique pour les opérateurs hors UE (problème de l'effectivité / efficacité du contrôle)
  - Un règlement difficile et lourd à mettre en place pour les entreprises et administrations en dehors de l'économie numérique
  - Un règlement qui repose sur les capacités de contrôle effectif pour donner sens à « l'accountability »