PRIVACY BY DESIGN : UN PRINCIPE DE PROTECTION SÉDUISANT MAIS COMPLEXE À METTRE EN ŒUVRE

Matthieu Dary
Avocat associé - Département Droit économique - Membre du groupe pilote national « données personnelles » du cabinet FIDAL

Leila Benaissa
Avocat associé - Département Droit économique - Membre du groupe pilote national « données personnelles » du cabinet FIDAL

Prenant en compte les nouveaux risques induits par les nouvelles technologies exploitant des volumes de plus en plus importants de données à caractère personnel, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après le « Règlement »)[1] prévoit de nouvelles obligations à la charge des responsables de traitement.

Alors que le régime en vigueur repose essentiellement sur la notion de « formalités préalables » auprès des autorités nationales en charge des données personnelles, le Règlement entend responsabiliser les acteurs en leur imposant de mettre en œuvre des mesures de protection des données et être en capacité de démontrer en cas de contrôle leur conformité à la réglementation (principe d'*accountability*).

C'est dans ce cadre que les opérateurs économiques se voient désormais assujettis à une obligation de protéger la vie privée dès la conception, obligation communément désignée par l'expression « *Privacy by Design* ».

Il s'agit pour les responsables de traitement d'anticiper tous les risques liés au traitement de données à caractère personnel *via* l'adoption de mesures proactives destinées à rendre l'individu maître de ses données et, ainsi, de s'inscrire dans une démarche responsable améliorant la confiance des utilisateurs et apportant un avantage compétitif. Si ce mode de régulation apparaît séduisant (I) son implémentation suppose la mise en œuvre de mesures techniques complexes et diverses impliquant l'intervention de toutes les parties prenantes au sein de l'entreprise (II).

I - *PRIVACY BY DESIGN* : UN PRINCIPE *A PRIORI* SÉDUISANT

Alors que jusqu'à présent, le responsable de traitement intervenait *a posteriori*, désormais, celui-ci devra être proactif et agir en amont de chaque projet *via* l'adoption de mesures adéquates afin de protéger les données à caractère personnel et la vie privée des individus.

En effet, aux termes de l'article 25 du Règlement, « [...] le responsable de 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, telles que la pseudonymisation,

1 Règl. (UE) 2016/679 du Parlement européen et du Conseil du 27 avr. 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la dir. 95/46/CE, JOUE n° L 119/1 du 4 mai 2016.

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 ».

Certes, l'article 34 de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés prévoit déjà que « le responsable de traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données, et notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »

Toutefois, l'article 34 semble exiger cette démarche proactive au regard des seules exigences liées à l'obligation de sécurité. L'article 25 du Règlement va au-delà et impose cette démarche proactive dans le but de répondre à toutes les exigences en lien avec la protection des données personnelles, sans la limiter à la seule obligation de sécurité.

La contrainte de la mise en œuvre de ce principe est renforcée par un alourdissement des sanctions prévues par le Règlement dont le plafond est fixé à 10 000 000 € et 2 % du chiffre d'affaires mondial[2], le montant le plus élevé étant retenu.

Le concept de *Privacy by Design* a vu le jour au Canada dans les années 90. Ann Cavoukian, alors commissaire à l'information et à la protection de la vie privée de l'Ontario, est partie du constat selon lequel le cadre légal était insuffisant pour assurer une réelle protection de la vie privée et qu'il fallait intervenir en amont grâce à une démarche qui intègre à toute technologie des mesures techniques et organisationnelles afin que cette technologie ne porte pas atteinte à la vie privée des individus.

À cette fin, l'opérateur économique devra répondre aux exigences suivantes[3] :

- prendre les mesures proactives et non réactives ; des mesures préventives et non correctives. À ce titre, l'opérateur économique doit s'interroger sur les incidents d'atteinte à la vie privée qui peuvent être consécutifs à l'exploitation de la technologie. La difficulté va être liée au fait que l'opérateur économique doit se poser la question à court, moyen et long terme, alors même que l'ensemble des incidents possibles ne peut pas toujours être anticipé ;
- assurer la protection implicite de la vie privée. En application de ce principe, l'opérateur économique doit s'assurer que l'utilisateur bénéficie d'une protection maximale sans avoir aucune intervention à réaliser. Cela signifie que l'opérateur doit définir le niveau de protection maximale et s'assurer que la solution technique la garantit sans qu'aucun réglage par l'utilisateur ne soit nécessaire ;
- intégrer la protection de la vie privée dans la conception des systèmes et des pratiques. Ainsi, la réflexion de la protection de la vie privée doit être prise en compte dès la conception du produit et il appartient au développeur notamment de le considérer lors de la création de la technologie ;
- assurer une fonctionnalité intégrale selon un paradigme à somme positive et non à somme nulle. C'est certainement une des exigences les plus complexes à mettre en œuvre. Elle vise à concilier les intérêts des utilisateurs et ceux de la société, étant rappelé qu'elle ne doit pas non plus conduire à un frein économique pour l'entreprise. Il conviendra en cas de contrôle ou de contestation de démontrer la réalité de la prise en compte de cet équilibre ;
- assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements. Cette obligation n'est pas nouvelle et elle est tout à la fois dans l'intérêt de l'entreprise que des utilisateurs. L'opérateur économique doit être en mesure d'assurer la sécurité de la conservation et de la destruction des données ;
- assurer la visibilité et la transparence. Ce principe de visibilité et de transparence devra être assuré par une docu-

2 Art. 83.4 du Règlement.

3 Privacy by Design – The 7 foundational principles, A. Cavoukian, Information and Privacy Commissioner of Ontario, Canada, mai 2010, https://iapp.org/media/presentations/11Summit/RealitiesHO1.pdf.

mentation réalisée par le responsable de traitement afin de démontrer, notamment en cas de contrôle, que l'utilisation de la technologie est conforme à ses objectifs. Cela permettra également au responsable de traitement d'assurer le droit d'accès à l'utilisateur ;
- respecter la vie privée des utilisateurs. Ce principe donne une place centrale au respect de la vie privée et à la protection des données personnelles de l'utilisateur. Il est une synthèse des autres principes évoqués précédemment.

La mise en œuvre de ces sept principes fondamentaux est censée permettre, et c'est l'objectif de ce nouveau mode d'auto-régulation, la réduction des risques pour les personnes, liés à un mauvais usage de leurs données, qui n'était pas assuré par le régime de « formalités préalables », et la réduction des risques de sanction pour les professionnels, le nouveau régime devant permettre des comportements plus vertueux.

II - *PRIVACY BY DESIGN* : UNE IMPLÉMENTATION COMPLEXE

Si le Règlement est entré en vigueur le 25 mai 2016, les entreprises ont jusqu'au 25 mai 2018 pour se mettre en conformité avec ces nouvelles obligations.

Afin de mettre en œuvre le concept de *Privacy by Design* avant cette date, se posent les questions majeures suivantes :
- quelles sont les entreprises concernées ?
- quels sont les acteurs au sein de l'entreprise qui doivent prendre part au respect de ce principe ?
- quelles sont les technologies touchées ?
- quelles sont les mesures concrètes à mettre en œuvre ?

Le développement de récentes technologies, et tout particulièrement celles liées aux objets connectés, donne des illustrations du champ d'application de ces dispositions (V., C. Zolynski, La *Privacy by Design* appliquée aux Objets connectés : vers une régulation efficiente du risque informationnel ?, Dalloz IP/IT 2016. 404).

Au-delà des seuls objets ou produits collecteurs de données, le respect de la vie privée et la protection des données vont devoir être pris en compte dans le développement et la conception des systèmes informatiques et d'infrastructure des réseaux.

Dès que la technologie va permettre d'être intrusive dans la vie privée des utilisateurs, de collecter massivement des données, et plus particulièrement lorsque ces données ont un caractère sensible ou vont permettre une analyse du comportement de la personne dont les données sont collectées, l'entreprise devra s'interroger sur le respect par sa technologie du principe de *Privacy by Design*.

Les exemples de technologies assujetties au respect de ses obligations sont devenus pléthoriques :
- le scanner à empreintes digitales sur les appareils Apple ;
- les appareils en lien avec l'e-santé (montres, podomètres, etc.) ;
- les différents projets de maisons et voitures connectées (enregistrement des comportements, géolocalisation, etc.) ;
- les réseaux sociaux ;
- la réalité augmentée (avec l'exemple cet été de Pokemon Go) ;
- le développement de l'usage des drones ;
- etc.

Le principe du *Privacy by Design* peut leur imposer de respecter les exigences suivantes :
- minimiser l'utilisation des données personnelles en se limitant aux données strictement nécessaires à l'utilisation de la technologie ;
- limiter le volume des données traitées ;
- limiter la durée de conservation des données ;

- limiter les destinataires des données ;
- privilégier l'anonymisation ou la pseudonymisation des données ;
- intégrer dans les dispositifs technologiques un niveau de sécurité très élevé ;
- éviter toute interconnexion et croisement de données ;
- assurer une formation du personnel de l'entreprise ;
- documenter l'ensemble des mesures prises pour assurer le respect de ces différentes exigences.

Manifestement, le respect de ces contraintes est assez conceptuel et sa mise en œuvre pratique va s'avérer peu aisée.

À la frontière d'obligations juridiques, informatiques, économiques, éthiques et organisationnelles, elle va nécessiter une coopération de l'ensemble des acteurs de l'entreprise.

Elle contraindra les entreprises à insuffler en amont une véritable culture des données personnelles à l'ensemble des intervenants de l'entreprise.

Si cette culture devra être portée en premier lieu par le *Data Privacy Officer*, on comprend aisément que les responsables de développement et de projet vont devoir être les premiers à s'emparer de ce principe de *Privacy by Design* et en tenir compte dès leur réflexion sur le développement de nouvelles technologies.

Les autorités de régulation vont jouer un rôle majeur dans la détermination de méthodologies pour se conformer à ces obligations.

La Commission nationale de l'informatique et des libertés (CNIL) n'a pas attendu l'adoption du Règlement pour intégrer ce concept dans ses recommandations. Elle y faisait ainsi déjà référence dès 2014 lorsqu'elle a établi un pack de conformité pour les compteurs communicants à accompagner l'innovation des industriels du secteur en intégrant la protection des données personnelles le plus en amont possible dans la définition des nouveaux services [4].

Il sera particulièrement intéressant d'étudier les recommandations de la CNIL qui résulteront du groupe de travail en charge d'établir un pack de conformité consacré aux véhicules connectés. L'objectif étant en effet de « constituer une "boîte à outils" de la conformité spécifique du véhicule connecté et de mettre en avant une nouvelle vision de la régulation visant à privilégier une démarche positive de "*Privacy by Design*" » [5].

Il convient également de citer l'initiative de la Commission nationale pour la protection des données du Grand-Duché de Luxembourg qui propose une étude de cas pour illustrer le principe du *Privacy by Design* [6].

Devant les contraintes imposées par cette nouvelle réglementation, il est légitime pour les opérateurs économiques de se poser la question de l'opportunité de mettre en œuvre ces dispositions.

Le changement de paradigme qui passe désormais par une anticipation des risques constitue une opportunité pour faire de la protection des données un élément de valorisation de leurs actifs.

En anticipant les usages et les risques de l'utilisation des données personnelles, les entreprises vont regagner la confiance de leurs clients, de plus en plus sensibles à ces questions. Moins méfiants, les clients adhéreront plus facilement à ces nouvelles technologies.

CE QU'IL FAUT RETENIR

Face à la numérisation croissante des activités de l'entreprise, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 a consacré de nouveaux principes dont celui de *Privacy by Design*, qui met à la charge des responsables de traitement une obligation d'anticipation de tous les risques liés au traitement de données à caractère personnel *via* l'adoption de mesures techniques et organisationnelles en amont de tout projet.

Une implémentation efficace du principe de *Privacy by Design* est destinée à réduire les risques liés à un mauvais usage de leurs données pour les personnes physiques, de même que les risques de sanction pour les professionnels.

Il n'en demeure pas moins que cette implémentation n'est pas aisée en raison de la généralité et le flou qui entourent les principes fondamentaux de la *Privacy by Design*, qui doivent pourtant être traduits en des actions techniques et organisationnelles concrètes avant le 25 mai 2018, date à laquelle le règlement européen sera applicable.

4 https://www.cnil.fr/fr/innovation-dans-le-pilotage-energetique-du-logement-un-pack-de-conformite-pour-les-compteurs.

5 https://www.cnil.fr/fr/en-route-vers-un-pack-de-conformite-consacre-aux-vehicules-connectes.

6 http://www.cnpd.public.lu/fr/dossiers-thematiques/nouvelles-tech-communication/privacy-by-design/Le-_Privacy-by-Design_-en-action_-etude-de-cas/index.html.

En outre, elles se prémunissent bien entendu :

- des poursuites judiciaires qui pourraient être intentées par les personnes dont les données sont collectées, les autorités de contrôle ou par les concurrents, qui eux respecteraient leurs obligations ;
- de vols de données qui pourraient être utilisées pour les concurrencer, c'est donc un moyen de préserver son activité commerciale ;
- des risques inhérents à des pertes ou des vols qui pourraient avoir des conséquences irrémédiables sur l'image de la société.

Si ce mode de régulation imposant une protection dès la conception semble séduisant *a priori*, la mise en œuvre pratique des sept principes fondamentaux évoqués précédemment apparaît bien complexe en pratique. Nombreux sont ceux qui s'accordent sur le flou qui entoure les termes très généraux de ces principes. Comment dès lors, traduire ces principes en concepts techniques ? Comment un responsable de tion par exemple, il a été démontré que la plupart des techniques d'anonymisation n'étaient pas infaillibles et qu'il était possible de ré-identifier des personnes physiques *via* un croisement de plusieurs données anonymisées[7] ?

Les principes fondamentaux de la *Privacy by Design* semblent par ailleurs contraires au principe même de fonctionnement de certaines technologies : comment minimiser les données à l'accomplissement d'un objectif alors que, par exemple, le *Big Data* trouve sa raison d'être dans le traitement de volumes gigantesques de données dans un dessein qu'il est censé découvrir lui-même ?

Par ailleurs, il est extrêmement difficile d'anticiper tous les usages qui peuvent être liés tant à l'évolution des comportements que de la technologie initiale. Une intervention *a posteriori* en application d'un principe, que certains nomment *Privacy by Redesign*, qui aurait pour objectif d'appliquer les principes fondamentaux de *Privacy by Design* aux systèmes existants, pourrait être une réponse[8].

7 C. Zolinski, P. Pucheral, A. Rallet et F. Rochelandet, La *Privacy by Design* : une fausse bonne solution aux problèmes de protection des données personnelles ?, Légipresse, nº 340, juill.-août 2016.

8 J. Verdure, Le concept de « Privacy by Design » : un remède à l'insuffisance des moyens actuels de protection de la vie privée, févr. 2012, http://www.e-juristes.org/le-concept-de-privacy-by-design-un-remede-a-linsuffisance-des-moyens-actuels-de-protection-de-la-vie-privee/.