La sécurité des données à caractère personnel : de l'utopie à la réalité.
Approche juridique[1]

Le point de départ de cette contribution réside dans le double constat du renouvellement profond des enjeux relatifs à la protection des données à caractère personnel dans le contexte du développement rapide des nouvelles technologies de l'information et de la communication (TIC) d'une part, et de la nécessité de renforcer en conséquence la sécurité des données comme en atteste l'adoption du nouveau règlement général européen sur la protection des données à caractère personnel en avril 2016[2] d'autre part. La question de la sécurité des données à caractère personnel est, en ce sens, particulièrement épineuse car d'un côté, ces données doivent faire l'objet d'une protection nécessaire pour assurer le droit des personnes concernée au respect de leur vie privée - certaines données telles que les donnée de santé sont de surcroît considérées comme des données sensibles devant faire l'objet d'une sécurité renforcée - et d'un autre côté, le développement prolifique du numérique dans tous les secteurs tend à affaiblir la sécurité de ces mêmes données. Dès lors, notre réflexion principale consiste à s'interroger sur la manière de renforcer la sécurité des données à caractère personnel dans un environnement numérique qui implique à la fois un échange massif de données mais aussi des échanges de données en dehors des strictes relations soumises au secret professionnelle comme par exemple la relation médecin-patient. Le nouveau règlement général européen sur la protection des données à caractère personnel consacre la section 2 de son chapitre IV intitulé « Responsable du traitement et sous-traitant » à la sécurité des données. La section se compose de trois articles dont un portant sur les mesures de sécurité et deux sur les situations de violation de données à caractère personnel entendue comme « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ». A partir de ces trois articles, la réflexion juridique peut être engagée selon deux axes.

Le premier axe s'articule autour de la lecture du premier article de la section, l'article 32, qui préconise la mise en place par le responsable du traitement et le sous-traitant d'une approche par le risque. Une telle approche devrait, en théorie, les conduire à prendre des mesures techniques et opérationnelles pour assurer la sécurité des données. Ces mesures peuvent notamment consister en la pseudonymisation, le chiffrement des données ou encore l'adoption de moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité des données. Or, par exemple, la pseudonymisation n'est pas, selon le groupe de l'article 29, « (…) une méthode d'anonymisation. Elle réduit simplement la corrélation d'un ensemble de données avec l'identité originale d'une personne concernée et constitue par conséquent une mesure de sécurité utile », ce qui signifie que les données ayant fait l'objet d'une pseudonymisation peuvent être ré-identifiées par le responsable du traitement mais parfois aussi par des tiers qui peuvent les combiner avec des informations émanant d'autres sources. Dans cette dernière hypothèse, sommes-nous alors face à une violation des données personnelles ? Quelles mesures doivent alors être combinées par le responsable du traitement et le sous-traitant pour renforcer la sécurité des données ? L'article 32 doit, par ailleurs, nécessairement être lu à la lumière de l'article 25 du Règlement qui consacre la méthodologie du *privacy by design* qui « consiste à intégrer la protection des données personnelles dès la conception des outils de collecte, de traitement et d'exploitation des données en préconisant

[1] Sophie Gambardella, Docteur en droit, Aix-Marseille Université.
[2] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 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 directive 95/46/CE (règlement général sur la protection des données), *JOUE* L119 du 4 mai 2016.

une approche proactive du responsable de traitement afin de prévenir *ex ante* le risque d'atteinte à la vie privée, qui doit se prolonger tout au long de la vie du projet »[3]. Si le règlement tend à renforcer les obligations du responsable du traitement pour une meilleure sécurité des données, au-delà même de l'énonciation de principes ou alors encore de méthodes, la question la plus délicate demeure celle de leur mise en œuvre car de leur mise en œuvre dépend l'effectivité du droit à la vie privée. En effet, à défaut d'être effectifs, les droits de l'Homme ne sont pas des droits mais de simples prétentions. Or, l'effectivité des droits dans ce contexte repose sur des facteurs extérieurs au droit et au juge. C'est la raison pour laquelle, une analyse complète de la sécurité des données à caractère personnel exige d'intégrer dans l'analyse juridique, des réflexions provenant d'autres disciplines et notamment celle de l'informatique : quels sont les obstacles et possibilités au plan informatique de mise en œuvre desdits droits et obligations ?.

Le second axe de réflexion est résolument plus juridique et porte sur les deux autres articles de la section 2 qui, en cas de violation des données à caractère personnel, exige du responsable du traitement et du sous-traitant une notification à l'autorité de contrôle et une communication à la personne concernée de la violation. Une mesure similaire a été introduite, en France, en 2011, par l'article 34 bis de la loi n° 78-17 du 6 janvier 1978. Or, la mise en œuvre de cette disposition a fait l'objet d'un arrêt du Conseil d'Etat en 2015 (Conseil d'État, 18 décembre 2015, n° 385019, *Société Orange*) qui interroge par bien des aspects. En effet, la notification de violation des données faite à l'autorité de contrôle peut conduire le responsable du traitement et le sous-traitant à être sanctionnés pour non-respect des exigences de sécurité. Or, comme le relève Nathalie Metallinos, dans ses observations sur l'arrêt du Conseil d'Etat, « [il] ressort de l'interprétation de la Cour européenne des droits de l'Homme que le droit de garder le silence et de ne pas s'auto-incriminer est une exigence du procès équitable »[4]. Toutefois, le Conseil d'Etat considère que, dès lors que le responsable du traitement n'a pas à notifier ses éventuels manquements à la sécurité, son droit de ne pas s'auto-incriminer est préservé. Il reste que le responsable du traitement et le sous-traitant doivent notifier la violation et donc déclenchent par ce biais une enquête sur un éventuel manquement à leur obligation de sécurité. L'article 33 du règlement européen met ainsi en tension deux droits : d'un côté, le droit au procès équitable du responsable du traitement et d'un autre côté, le droit au respect de la vie privée de la personne concernée. Quelle portée doit-on alors attribuer à l'obligation de sécurité afin de pouvoir concilier ces deux droits ? Quelle est la nature de l'obligation de sécurité qui incombe au responsable du traitement ? Si cet aspect de la problématique a une coloration très juridique, il reste néanmoins fondamental pour aborder entièrement la question de la sécurité des données à l'aune du nouveau règlement européen. De plus, la portée de l'obligation de sécurité nous semble très largement dépendre de ce qui est possible en pratique et donc de considérations extra-juridiques.

---

[3] Célia ZOLYNSKI, « La *Privacy by Design* appliquée aux Objets Connectés : vers une régulation efficiente du risque informationnel ? », *Dalloz IP/IT*, 2016, p. 404. Sur cette question du Privacy by design voir aussi : Matthieu DARRY et Leila BENAISSA, « Privacy by Design : un principe de protection séduisant mais complexe à mettre en œuvre », *Dalloz IP/IT*, 2016, p. 476.

[4] Nathalie METALLINOS, « Notification des violations de données à la CNIL : tendre le bâton pour se faire battre ? Observations sous Conseil d'État, 18 décembre 2015, n° 385019, *Société Orange* », *Dalloz IP/IT*, 2016, p. 144.