Synthèse du Thème D : “ Droit des données à caractère personnel ”

François Pellegrini

Thème D

« Droit des données à caractère personnel »

Les discussions de ce thème ont porté sur les points suivants :

1. Évolution du droit relatif aux données à caractère personnel ;
2. Diversité des pratiques constatées ;
3. Nature des données à caractère personnel.

Évolution du droit relatif aux données à caractère personnel

Le droit des données à caractère personnel, issu en France de la loi « Informatique et Libertés » de 1978, va connaître une profonde transformation avec l'entrée en vigueur en 2018 du Règlement général sur la protection des données (RGPD). Le RGPD propose une harmonisation des règles et des procédures, tout en laissant une marge d'appréciation aux États pour la mise en œuvre de certaines dispositions. Ainsi, des différences entre les pratiques des États pourront perdurer, sans qu'il soit possible actuellement de les énumérer précisément, puisque les États membres ont jusqu'au 25 mai 2018 pour concrétiser le RGPD.

Si les principes généraux ne changent pas, la mise en œuvre opérationnelle des droits subit des modifications substantielles. En France, cela conduira au basculement du régime d'autorisation actuellement mis en œuvre par la CNIL à un régime répressif de « redevabilité » (« *accountability* ») des responsables de traitement. De nouvelles obligations sont créées à la charge des responsables de traitement, exprimées en termes d'objectifs (tels que les obligations de « portabilité des données », de « sécurité », de « recours à des procédés d'anonymisation », etc.) sans que leur mise en œuvre soit précisément décrite. Cela suscite une certaine nervosité chez les responsables de traitement et sous-traitants.

À ce titre, la sécurité des données doit-elle être considérée comme un objet juridique ou seulement technique ? Une section du RGPD est intégralement consacrée à ce sujet. Est-on face à une obligation de moyens ou de résultat ? Il semble qu'il s'agisse d'une « obligation de moyens renforcée », les moyens mis en œuvre étant comparés à l'état de l'art. La mise en place de référentiels (comme ceux devant être rédigés par un GIP dans le cas du partage, de la transmission et de l'hébergement des données de santé, par exemple) doit permettre de définir un niveau de sécurité minimal, et évolutif afin de rester conforme à l'évolution des techniques.

L'obligation de notification à l'autorité de contrôle pose également question. S'il ne s'agit que d'une information factuelle, elle peut conduire au lancement d'une enquête conduisant à l'incrimination du notificateur pour ses manquements. Peut-elle être considérée comme une auto-incrimination ? Comment concilier le droit au respect de la vie privée et le droit au procès équitable ? Ces éléments ont déjà pu être testés en pratique lors de l'affaire « Orange », en 2015.

Le RGPD pose une définition très large des données de santé et de leur origine (indifférence de la source), qui conduit à faire disparaître le flou relatif à la notion de « donnée de bien-être », qui n'a en fait aucune réalité juridique. Étant donné que l'acceptation large de la notion de données de santé se trouve dans le préambule du RGPD, il reviendra à la CJUE d'interpréter la définition des données de santé à la lumière de ces dispositions du préambule du règlement. La distinction entre données de bien être et données de santé devra donc se faire au prétoire, ou éventuellement par les autorités de protection des données. Cette question a déjà été abordée par le G29 dans un document intitulé « *Health data in apps and devices* ».

Sur le plan des droits fondamentaux, la fondamentalisation de la protection des données nécessite d'organiser sa coexistence avec d'autres droits fondamentaux, en s'appuyant sur le principe de proportionnalité. L'un des sujets de friction récemment mis en exergue est celui des activités de renseignement, qui viennent porter atteinte à la protection des données à caractère personnel et à d'autres droits fondamentaux. Ces activités nécessitent un encadrement prenant en compte les questions des finalités, de la proportionnalité et de la création de garde-fous. La technique joue ici un rôle important, les réglementations (nationale et/ou européenne) pouvant être aisément contournées par la mise en œuvre de procédures techniques, comme le routage des données sur l'Internet permettant l'interception « hors sol » dans le cadre d'échanges croisés de données entre services de différents États.

Diversité des pratiques constatées

En parallèle du droit et de son évolution, on constate une très grande diversité de pratiques.

La publicité ciblée est un très grand moteur d'innovations techniques et de pratiques, du fait des montants en jeu au niveau mondial. Elle conduit de nombreux fournisseurs de solutions techniques à mettre en œuvre des mécanismes de collecte, parfois sans laisser le choix à leurs usagers.

Tel est le cas de la géolocalisation, que la plupart des usagers ne savent pas désactiver. Tel est aussi le cas de la collecte des conversations d'ambiance, effectuée de façon passive par certains équipements de salon sans que l'usager en ait conscience (du fait de Conditions générales d'utilisation peu claires, de façon délibérée ou non) et sans que ces fonctionnalités puissent être facilement désactivées, si tant est qu'elles puissent l'être. Le fait de ne plus pouvoir retirer la batterie de son ordiphone est une modalité technique qui a une influence sur le niveau de confidentialité que l'on peut atteindre. De nombreux équipements peuvent être détournés de leur usage pour collecter des données à caractère personnel : courbe de consommation électrique instantanée renseignant sur le film que l'on visionne, accéléromètre des ordiphones pour identifier la démarche des personnes ou les vibrations de l'air dues aux conversations ambiantes, etc. Afin de limiter ces risques, il est essentiel d'appliquer les principes du « *privacy by design* » lors de la conception des dispositifs.

Les notions de loyauté et de finalités de la collecte sont essentielles sur le plan juridique pour éviter les abus. Elles conditionnent également la mise en œuvre effective du consentement de l'usager à la collecte de ses données. Or, les formes de consentement sont profondément renouvelées par le numérique. Dans l'environnement en ligne, qu'est-ce qu'un consentement explicite, ou encore spécifique ? Les usagers sont face à un « *privacy paradox* », à savoir l'écart entre l'affirmation de la préoccupation personnelle et les usages constatés.

Ceci conduit à une privatisation du droit, par la recherche de la responsabilisation d'acteurs privés ayant des objectifs qui ne paraissent pas toujours conciliables avec ceux de la protection des données. Cette asymétrie conduit à une surestimation du caractère protecteur du RGPD, dont il faudrait pouvoir mesurer pratiquement l'effectivité. Selon quels critères cette mesure de l'effectivité peut-elle être étudiée ? Quels outils pourraient-ils permettre aux individus d'assurer la protection de leurs données personnelles, de pouvoir choisir le niveau de protection qu'ils souhaitent, ou de prendre conscience des enjeux autour de la protection des données personnelles ? Cela pourrait être l'objet d'études empiriques portant sur l''effectivité de la protection des données du RGPD, sur la base d'un échantillon de personnes et d'entreprises.

Nature des données à caractère personnel

On constate une prolifération de données et d'informations, constituées tant de données brutes que de données induites, résultant d'un traitement appliqué à un unique ensemble de données brutes ou bien par croisement de plusieurs ensembles.

La question de la définition même des catégories de données semble parfois faire débat. Qu'est ce qu'une donnée ? À partir de quel moment sommes nous face à une donnée à caractère personnel ? Par capillarité, il semble que toute donnée dont la variation est conditionnée par l'action d'une personne puisse en théorie être considérée comme une donnée à caractère personnel.

Une distinction supplémentaire est effectuée avec le statut de donnée sensible. Tout comme le rythme des pas d'une personne, sa voix renseigne sur l'état émotionnel et de santé de cette personne. La voix doit-elle donc toujours être considérée comme une donnée sensible ? Il semble plus pertinent que cette catégorisation soit conditionnée par l'usage qui est fait de la donnée, et donc de la nature des traitements qui lui sont appliqués.

Le RGPD définit de manière exhaustive ce qui peut être une donnée sensible mais il semble qu'en pratique les utilisateurs, de manière subjective, considèrent bien plus de leurs données comme étant sensibles. Or, elles ne bénéficient pas du régime juridique de protection renforcée imposant le principe d'interdiction de traitement des données. En la matière, la marge de manœuvre des États-membres est importante, le consentement de la personne et les exceptions possibles sont nombreuses. Malgré tout, l'existence du principe d'interdiction oblige les États à se justifier de la licéité des traitements réalisés contrairement aux traitements opérés sur des données à caractère personnel non sensibles. Ici encore, il semble que responsables de traitement et utilisateurs ont une approche subjective des notions parfois en décalage avec les catégories créées par le droit.

Synthèse réalisée par François Pellegrini à partir des éléments débattus collectivement lors de la table ronde