RGPD, quel rôle pour le CASD ?

Publié par Kamel Gadouche | 10/01/2018 | Tribune |

RGPD ou le principe du « trust and control »

L'entrée en vigueur en mai 2018 du nouveau règlement européen sur la protection des données personnelles (RGPD) destiné à homogénéiser cette protection et à en faciliter le transfert à l'intérieur de l'espace européen, va également opérer un renversement important en matière de responsabilité des différents acteurs pour l'accès et le traitement des données à caractère personnel. Plus contraignant pour l'Etat et les entreprises, ce règlement va dans le sens d'une plus grande responsabilisation des acteurs collecteurs ou producteurs des données selon un principe cher aux Anglo-saxons, le principe du « trust and control » : une plus grande flexibilité, voire agilité, pour les administrations et les entreprises en échange d'une responsabilisation renforcée et de moyens de contrôle du régulateur eux aussi renforcés.

Avec ce règlement on va passer d'une logique de validation a priori par l'autorité de contrôle, la CNIL en France, tel qu'il était inscrit par exemple dans la loi française de 1978 avec les « formalités préalables » (déclaration, autorisation, etc.) à une logique de validation a posteriori du traitement impliquant une responsabilité renforcée des acteurs mais aussi, et c'est un point essentiel, une plus grande flexibilité et réactivité pour les administrations et les entreprises. En effet, demain, une entreprise qui souhaitera effectuer un nouveau traitement aura toutes les cartes en main pour pouvoir le mettre en place dans des conditions et des délais dont elle aura la totale maîtrise. L'entreprise n'aura plus à faire de formalités préalables qui peuvent parfois prendre du temps, voire ne pas aboutir ou tout simplement décourager. En contrepartie, l'entreprise devra avoir fortement pris en considération en amont les enjeux de sécurité des données.

Ce faisant, nombre d'organisations devront investir pour être en mesure de prouver qu'elles ont fait le nécessaire pour garantir la sécurité des données. En cas de contrôle de la CNIL, dont les moyens pour cette mission vont être renforcés, ou en cas d'incident, comme un piratage de données, le responsable de traitement devra apporter la preuve que toutes les mesures de protection des données qui s'imposaient ont été prises. Concrètement en fonction de la sensibilité des données et du traitement envisagé, le responsable de traitement devra avoir effectué une analyse de risque couvrant l'ensemble du périmètre dont il a la responsabilité en mesurant en particulier l'impact sur la vie privée que pourrait produire chaque

risque identifié. L' « actif » données à caractère personnel devra être au centre de cette analyse de risque (PIA : études d'impact sur la vie privée).

Par ailleurs, ce nouveau règlement impose aussi une responsabilité renforcée pour les sous-traitants (data-processor, article 28) pour garantir la sécurité des données. Il donne un pouvoir accru aux responsables de traitement (data-controller) en matière de contrôle sur l'activité du sous-traitant, voire la possibilité de réaliser des audits dans certains cas. Le sous-traitant doit aussi réaliser une analyse de risque sur la partie le concernant qu'il doit transmettre au responsable de traitement. Enfin et surtout, le sous-traitant engage désormais sa responsabilité juridique en cas d'incident, là où auparavant seul le responsable de traitement était responsable.

Le CASD dans le contexte du RGPD

Le CASD est un service permettant aux utilisateurs (chercheurs, entreprises, datascientist…) de travailler à distance, de manière hautement sécurisée, sur des bases de données confidentielles, dans le respect des lois et des exigences de protection de libertés individuelles. Le CASD est une entité du Genes, Groupe des écoles nationales d'économie et statistique, établissement public, qui regroupe l'Ensae, l'Ensai, le Crest et Ensae-Ensai formation continue (le cepe). Le CASD s'adresse principalement à la recherche publique.

Le CASD fournit un accès sécurisé à de nombreuses sources de données confidentielles confiées par différentes administrations et entreprises privées. Ces sources de données sont le plus souvent couvertes par un secret professionnel comme le secret des affaires, le secret statistique, le secret fiscal, le secret médical, le secret industriel et commercial.

Le CASD a mis en place un dispositif ultra sécurisé pour limiter les risques associés à la mise à disposition de ces données qui peuvent être parfois extrêmement sensibles.

Les principes qui ont conduit à la conception de l'équipement CASD peuvent être illustrés par une analogie avec un équipement couramment utilisé par les chercheurs dans le domaine de la chimie. Lorsqu'un chimiste doit travailler sur un produit dangereux qui nécessite une atmosphère particulière, il utilise ce qu'on appelle une boîte à gants (« glovebox » en anglais) : il s'agit d'une enceinte étanche dans laquelle sont placés les produits et les outils nécessaires à la manipulation de ceux-ci. De longs gants étanches sont intégrés à une paroi transparente de l'enceinte afin que le chercheur puisse glisser ses mains à l'intérieur de ces gants et puisse ainsi interagir avec les éléments qui sont présents dans l'enceinte afin d'en préserver

le confinement. L'utilisateur est bien identifié, il peut voir les produits, il dispose des outils pour manipuler les produits, il peut travailler dans un environnement qui lui est familier. Il ne peut cependant pas introduire, ni extraire de produit sans une procédure particulière. Enfin, il est aussi lui-même protégé du risque de dissémination des produits chimiques.

Cette analogie est très illustrative de ce qu'est un centre d'accès sécurisé aux données. L'objectif est de maintenir la confidentialité des données en les confinant et en garantissant l'identité de l'utilisateur même lorsqu'il s'agit d'une utilisation à distance. Pour son travail, l'utilisateur peut voir les données, dispose des outils logiciels pour les manipuler dans de bonnes conditions dans un environnement qui lui est familier. Pour garantir le confinement, le dispositif empêche techniquement l'utilisateur d'introduire ou de récupérer de lui-même des fichiers de données (par téléchargement, copier/coller, impression, clés usb…). Des procédures spécifiques sont prévues pour insérer des scripts, des données ou des nomenclatures, et pour sortir des fichiers de résultats qui ne contiennent plus de données confidentielles. Le confinement, ainsi qu'une authentification forte, sont nécessaires pour garantir un haut niveau de sécurité et préserver la confidentialité des données.

L'équipement CASD est constitué de boîtiers d'accès spécifiquement conçus à cet effet : les SD-Box, qu'on pourrait comparer aux gants ci-dessus, et une infrastructure centrale sécurisée (l'enceinte de confinement ou « bulle sécurisée »), hébergée dans les locaux du Genes, et accessible uniquement à partir de boîtiers SD-Box. Ce boîtier et cette infrastructure centrale forment un ensemble fermé et étanche dans lequel les utilisateurs authentifiés de manière biométrique peuvent travailler sur les données sans qu'à aucun moment ils ne puissent les récupérer par eux-mêmes sous forme de fichiers.
Le CASD poursuit aussi une stratégie de certification pour formaliser et garantir son niveau de sécurité (hébergeur de données de santé, ISO27001, GDPR…). Maintenir un niveau de sécurité élevé sur tous les composants du service demande une implication forte des équipes que ce soit pour la veille technologique, la recherche et le développement (R&D) ou pour l'exploitation courante. Cela exige donc une garantie de moyen qui se traduit dans les contrats que signe le CASD avec les détenteurs de données par une obligation de résultats.

Ces exigences deviennent de fait des obligations dans le cadre du nouveau règlement européen (RGPD). Le CASD a réalisé et continue de réaliser des analyses de risque exhaustives sur l'ensemble des traitements dont il a la responsabilité. Un des principes fondamentaux du CASD est de limiter au strict nécessaire la surface d'exposition de ses services afin, bien entendu, de limiter les risques pour les données. C'est ainsi que l'infrastructure du CASD, appelée « bulle sécurisée », est totalement indépendante de tout autre système d'information : elle fonctionne en circuit fermé avec des boitiers totalement dédiés (appelés SD-Box) qui ne communiquent que via des tunnels chiffrés. Cette restriction de la surface d'exposition permet aussi de concentrer ses efforts sur un périmètre de sécurité plus restreint et de le maîtriser de bout en bout.

Pour les entreprises, le nouveau règlement européen entraînera certainement des mutations profondes de leurs systèmes d'information pour limiter davantage, à l'instar de que fait le CASD, les risques qui pourraient peser sur les données à caractère personnel qu'elles détiennent. Nous devrions assister dans les prochaines années à l'émergence de « bulles sécurisées » dans les entreprises pour les traitements sur des données particulièrement sensibles. C'est même une préconisation des services de la CNIL.

Déjà, le CASD commence à répondre à de nombreuses sollicitations d'organismes de recherche afin de leur fournir un service de bulle sécurisée. Une telle technologie permet notamment de concentrer l'investissement nécessaire en sécurité sur l'institution détentrice des données sans avoir besoin d'en réaliser davantage dans les institutions utilisatrices souvent nombreuses et dispersées comme cela est particulièrement le cas dans le domaine de la recherche en santé.

Cette technologie pourrait également trouver des développements dans la création dans le contexte de la recherche scientifique de réseaux de centres sécurisés à l'intérieur des espaces nationaux ou de l'espace européen (pour ce dernier facilité par l'homogénéisation induite par le RGDP) permettant l'utilisation conjointe de données personnelles et sensibles détenues dans des centres différents.