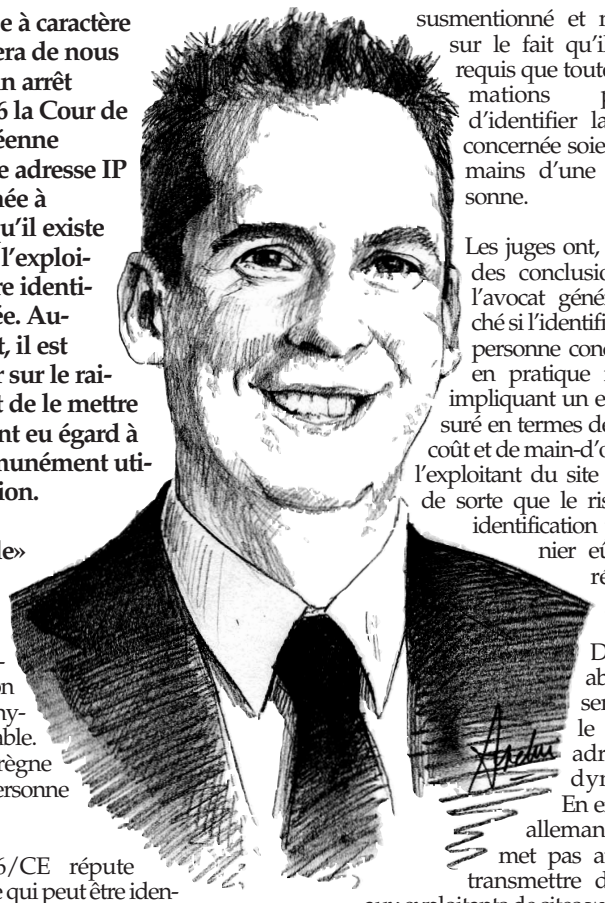
Affaire *Breyer* - la CJUE et la notion de «donnée à caractère personnel» :

Quel statut pour les données anonymisées, pseudonymisées et/ou encryptées dans des contrats informatiques ?

La notion de «donnée à caractère personnel» ne cessera de nous surprendre. Dans un arrêt Breyer du 19 octobre 2016 la Cour de justice de l'Union européenne («CJUE») a estimé qu'une adresse IP dynamique est une donnée à caractère personnel lorsqu'il existe des moyens légaux pour l'exploitant d'un site web de faire identifier la personne concernée. Au-delà de cet enseignement, il est intéressant de se pencher sur le raisonnement de la CJUE et de le mettre en perspective notamment eu égard à certaines pratiques communément utilisées de pseudonymisation.



Une donnée «identifiable» au sens de la directive 95/46/CE

Une donnée à caractère personnel est toute information concernant une personne physique identifiée ou identifiable. Une certaine incertitude règne autour de la notion de personne «identifiable».

L'actuelle directive 95/46/CE répute «identifiable» toute personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.

Le considérant 26 de la directive 95/46/CE précise en outre que pour déterminer si une personne est «identifiable», il convient de considérer l'ensemble des moyens susceptibles d'être *raisonnablement* mis en œuvre soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne. Lorsque la personne n'est pas identifiable conformément à ces principes, notamment lorsque les données ont été rendues anonymes, les principes de la protection des données ne s'appliquent pas.

Interprétation prétorienne extensive

Les adresses IP «dynamiques», à la différence des adresses IP «statiques», changent à l'occasion de chaque connexion internet. *A priori*, ces adresses IP dynamiques ne permettent pas de faire le lien – au moyen de fichiers accessibles au public – entre un ordinateur donné et le branchement physique au réseau utilisé du fournisseur d'accès à Internet («FIA»). Pour déterminer si une telle adresse constitue néanmoins une information permettant l'identification d'une personne physique, la CJUE s'est fondée sur le considérant 26 susmentionné et notamment sur le fait qu'il n'est pas requis que toutes les informations permettant d'identifier la personne concernée soient entre les mains d'une seule personne.

Les juges ont, sur la base des conclusions de M. l'avocat général, recherché si l'identification de la personne concernée était en pratique irréalisable, impliquant un effort démesuré en termes de temps, de coût et de main-d'œuvre pour l'exploitant du site web visité, de sorte que le risque d'une identification par ce dernier eût paru en réalité insignifiant.

De prime abord, tel semblait être le cas des adresses IP dynamiques. En effet, le droit allemand ne permet pas aux FIA de transmettre directement aux exploitants de sites web les informations nécessaires à l'identification de la personne concernée «cachée» derrière l'adresse IP «dynamique».

Néanmoins, la CJUE a constaté qu'il existe des voies légales permettant aux exploitants de sites web de s'adresser, notamment en cas d'attaques cybernétiques, à l'autorité compétente afin que celle-ci entreprenne les démarches nécessaires pour obtenir ces informations auprès du FIA et pour déclencher des poursuites pénales.

Le raisonnement de la CJUE semble aller relativement loin puisque la mise en œuvre de voies de droit pour obtenir des informations nécessaires à l'identification d'une personne pouvait sembler engendrer un effort démesuré en termes de temps et de ressources notamment. De plus, l'aléa lié à toute procédure judiciaire laisse la porte ouverte à un refus des juridictions de faire droit à une telle demande, ce qui est susceptible d'empêcher toute identification.

Cette solution rendue à la lumière du droit allemand aurait probablement été similaire dans un contentieux soumis au droit luxembourgeois. En effet, en cas de cyberattaque, des voies de droit existent au Luxembourg pour en identifier l'auteur (notamment par son adresse IP dynamique le cas échéant). Une telle identification est strictement encadrée et est limitée dans le temps (l'obligation de conservation à la charge des FIA étant limitée à 6 mois) mais semble permettre une interprétation analogue aux développements de l'arrêt *Breyer*.

Données non «personnelles», qu'en reste-t-il ?

Pour pouvoir être exempté des règles de protection des données à caractère personnel, il appartient donc de prouver que la personne concernée n'est pas ou plus identifiable. Il est important de distinguer *anonymisation* et *pseudonymisation*. Tandis que la première méthode empêche de façon irréversible toute identification, la seconde réduit simplement la corrélation d'un ensemble de données avec l'identité originale d'une personne concernée en évitant que les données puissent être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires qui sont conservées séparément.

Lorsque les données sont seulement pseudonymisées (notamment par le biais de techniques telles que la cryptographie à clé secrète, le hachage par clé avec clé enregistrée ou la tokenization), les règles relatives à la protection des données sont donc en principe applicables aux personnes qui ont à la fois accès aux données pseudonymisées et aux données supplémentaires permettant l'identification des personnes concernées.

Pour les autres personnes, le risque de mise en corrélation avec l'identité originale d'une personne concernée est réduit mais ne peut pas être exclu dans l'absolu. A la lecture de l'arrêt *Breyer*, il semble falloir rechercher si ces personnes en possession de données pseudonymisées (dont le niveau de sécurité est suffisamment élevé pour empêcher toute lecture par un tiers sans clé) disposent de moyens pour obtenir d'un tiers les informations nécessaires à l'identification de la personne concernée. Dans le cas *Breyer*, la CJUE a considéré que tel était le cas puisqu'il existait des voies de droit permettant l'obtention de ces informations.

Quel impact pour les contrats informatiques ?

Appliqué aux prestataires de services informatiques qui ne traitent que des données encryptées sans y avoir accès à défaut de posséder la clé permettant le déchiffrement des données, le raisonnement de la CJUE semble plaider en faveur d'un défaut d'application des règles relatives à la protection des données dans leur chef. Tel sera le cas lorsqu'ils ne disposent d'aucun moyen susceptible, et notamment d'aucun recours juridique, d'être *raisonnablement* mis en œuvre pour déchiffrer les données et d'identifier les personnes concernées y figurant.

Toutefois, les prestataires de services informatiques sont souvent au service d'un client disposant d'une clé de déchiffrement et qui est, en principe, responsable des données personnelles contenues dans le contenu chiffré. Une question hautement débattue à cet égard (et qui donne lieu à des positions divergentes entre autorités compétentes au sein de l'UE) est celle de savoir si un prestataire de services qui traite des données qui sont à caractère personnel dans le chef de son client mais pas dans le chef du prestataire-même (par exemple, faute d'accès en cas de cryptage des données), est à considérer comme un «sous-traitant» au sens de la réglementation relative à la protection des données.

Nous aurions tendance à répondre à cette question par la négative. En effet, un «sous-traitant» au sens de cette réglementation «traite des données à caractère personnel» même s'il le fait au nom et pour le compte d'une personne. Faute de données qui sont «à caractère personnel» dans son chef, il n'en traite pas et ne sera pas à considérer comme le «sous-traitant» d'un traitement de données à caractère personnel.

Qu'en sera-t-il avec le RGPD ?

Le Règlement général sur la protection des données («RGPD»), adopté en avril dernier et dont l'entrée en application est prévue le 25 mai 2018, ne modifie pas substantiellement la définition de «données à caractère personnel». Le considérant 26 du RGPD précise, tout comme la directive 95/46/CE interprétée par la CJUE dans l'arrêt *Breyer*, que pour déterminer si une donnée est identifiable, il convient de prendre en considération l'ensemble des «moyens raisonnablement susceptibles d'être utilisés» par le responsable du traitement ou par toute autre personne.

Le RGPD précise qu'il convient de prendre en compte des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, ainsi que les technologies disponibles au moment du traitement et de l'évolution de celles-ci. L'entrée en application du RGPD ne devrait donc pas avoir de conséquences substantielles sur l'interprétation dégagée par la CJUE dans l'arrêt *Breyer*.

Une guidance sur ce point serait toutefois la bienvenue, notamment eu égard à la question de savoir si un prestataire de services informatiques est «sous-traitant» lorsqu'il traite des données qui, dans son chef, ne sont pas identifiables. Une réponse claire à cette question est d'autant plus pressante que le RGPD a une incidence importante sur les contrats existants et futurs entre les responsables de traitement et les sous-traitants qui interviennent dans le cadre d'un tel traitement et sur lesquels nous reviendrons dans notre prochaine contribution.

Vincent WELLENS (picture)
Avocat à la Cour
Partner NautaDutilh Avocats Luxembourg S.à r.l.
vincent.wellens@nautadutilh.com

Anne-Sophie MORVAN
Avocat au Barreau de Paris (Liste IV)
Associate NautaDutilh Avocats Luxembourg S.à r.l.
annesophie.morvan@nautadutilh.com

ADA | Midi de la microfinance et de l'inclusion financière

Les services bancaires mobiles et la microfinance : quid des clients ?

Lors du 36e Midi de la microfinance organisé par ADA et le réseau InFiNe.lu, les invités internationaux du secteur des payements mobiles dans les pays du sud ont présenté les avantages et les risques du développement de ces services pour le secteur de la microfinance.

«Une institution financière qui n'irait pas vers le digital aurait un avenir très limité», explique James Onyutta, directeur de l'institution de microfinance (IMF) kényane Musoni. Le digital en général et le mobile banking en particulier deviennent aujourd'hui des éléments essentiels dans la stratégie des IMF.

«Il faut dire que les services de paiement mobile permettent de gagner du temps pour les consommateurs, réduisent les déplacements, renforcent la sécurité et facilitent même l'anonymat», explique Devyani Parameshwar, chef de produit à M-Pesa, la filiale du géant Vodafone, qui compte 25 millions d'utilisateurs dans le monde. «C'est d'abord une question d'efficacité», rajoute Laurent de la Vaissière, directeur en Information & Technology Risk chez Deloitte, et modérateur de cette rencontre.

Une transaction toutes les 30 secondes

Selon James Onyutta, les agences doivent utiliser les nouvelles technologies pour réduire leurs coûts et accroître la rapidité de traitement d'informations.

(de gauche à droite) : Devyani Parameshwar (M-Pesa/ Vodafone), Laurent de la Vaissière (Deloitte) et James Onyutta (Musoni)

De fait, le passage aux services mobiles, permet aux agents d'IMF de traiter plus de dossiers sans pour autant négliger la proximité et le suivi du client, en leur offrant des formations pour améliorer la gestion clients, cœur du métier de la microfinance. Par ailleurs, les clients peuvent utiliser le service à tout moment de la journée. Au Kenya, une transaction est effectuée toutes les 30 secondes. Autre facteur important du succès de l'IMF dans l'utilisation du mobile banking, Musoni est très à l'écoute du client, en adaptant ses services en fonction des besoins ressortant des enquêtes qu'ils effectuent régulièrement. Mais pourquoi le digital fonctionne aussi bien au Kenya ?

Selon Devyani Parameshwar, pour que le digital banking fonctionne et se développe dans un pays, 3 facteurs sont essentiels : le bon management de l'institution, un bon réseau de distribution, ainsi que le cadre réglementaire de partenariat entre réseaux de télécoms et institutions financières.

Et les risques ?

Vu l'importance de données de clients traitées, la question de la sécurité de ces derniers a été abordée. La représentante de M-Pesa, réseau qui compte plus de 25 millions de clients actifs dans le monde, nous rassure qu'aucun échange de données n'est autorisé sans l'accord du client. Il est également peu probable qu'un jour les IMF soient remplacées par les réseaux de télécoms, étant donné que la régulation ne leur permet pas d'offrir de crédits.

En revanche, la possibilité que les gouvernements s'intéressent aux revenus générés par les transferts via mobile et mettent en place des systèmes de taxation a été clairement évoquée.

Lancement de la digital financial inclusion initiative par ADA

En conclusion, Laura Foschi, directrice adjointe de ADA, a annoncé le lancement du nouveau projet de digital financial inclusion initiative par l'ONG luxembourgeoise. 12 pays ont été sélectionnés pour ce projet qui sera mis en place en deux phases à partir de 2017.