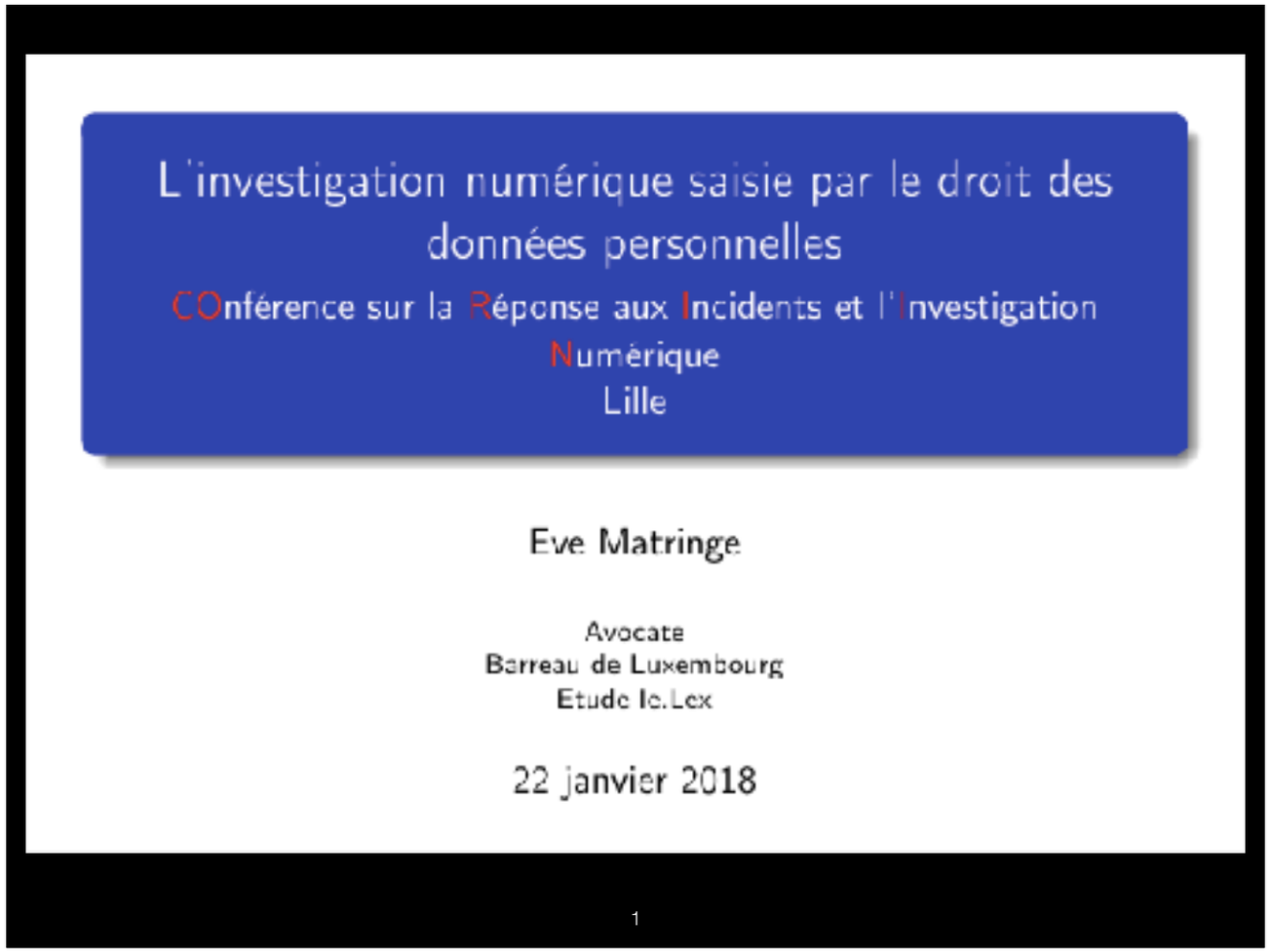

Eve Matringe, je suis avocate au barreau de Luxembourg, mais comme vous l'aurez sans doute remarqué, le droit des données personnelles n'est plus vraiment un droit national. Je vais néanmoins évoquer des décisions françaises pour illustrer certains propos.

Problématique

Echanges transnationaux, Big data,
Protection de l'individu

<u>Les textes européens:</u>

- **RGPD: règlement européen n°2016/679**
- **Directive n°2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention ou de détection des infractions pénales, d'enquêtes et de poursuites en ma matière ou d'exécution de sanction pénales, et à la libre circulation de ces données**
- **Règlement européen 45/2001**

=> champ d'application défini

Je ne vais pas revenir sur l'historique du GDPR (règlement sur la protection des données). Je vais me limiter à souligner que la question est aujourd'hui particulièrement brûlante en raison d'une part de la production et de la collecte massive de données personnelles, d'autre part de l'explosion des échanges transnationaux. Par ailleurs, l'investigation numérique implique souvent d'examiner le système objet de l'investigation, et donc d'avoir un accès aux données personnelles qu'il comporte. Les récents textes européens en matière de données personnelles traitent explicitement de la question tant en matière de traitement de données nationaux que s'agissant des enquêtes présentant un aspect européen ou transnational. Pour les investigations non concernées par les textes européens, il faut alors appliquer le cadre légal national, en France, la loi informatique et libertés. La maîtrise du cadre légal en la matière est nécessaire pour éviter le reproche d'accès illicite à des données personnelles (et pouvoir signaler les infractions potentielles, obligation pour les fonctionnaire, faculté pour les autres, qui ne sont cependant pas à l'abri de poursuite civile d'une victime).
Il convient par après de savoir ce qu'implique, en terme de réaction et au regard du droit de la protection des données à caractère personnel, la constatation de la compromission d'un traitement de données personnelles, tant du point de vue d'acteurs privés (SI, pentesteurs, CERT) que de celui des autorités judiciaires et policières (la question de la notification par le responsable du traitement a été longuement traité par d'autres, je n'y reviens pas).
Le RGPD s'applique par défaut dès qu'on est dans le champ d'application du droit européen, la directive s'applique spécifiquement aux traitements mentionnés, qui concernent dans certains cas des activités régaliennes de l'Etat. Mais pas la défense ou le renseignement. Le règlement 45/2001 concerne l'union européenne elle-même et les entités qui lui sont rattachées.

Problématique

<u>Angle d'attaque des enquêtes et des fichiers</u>
ex. CJUE

Le risque juridique est d'autant plus grand pour un enquêteur que le résultat de ses investigations va très probablement déboucher sur une procédure judiciaire, où ses travaux seront produits, scrutés, analysés. Par différence avec toutes les entreprises qui collectent et traitent les données personnelles des internautes sans aucune transparence, le travail de l'enquêteur sera rendu public, et donc pourra permettre aux personnes dont les données ont été analysées, de revendiquer l'application du droit des données personnelles.
Un ex. récent : CJUE, 27/9/2017, aff. affaire C-73/16: le fichier élaboré par les autorités fiscales est contesté par l'une des cibles sur base du droit des données personnelles: droit d'accès, droit de rectification, droit d'opposition.

Donnée personnelle

Directive 2016/680, cons. 21

Information concernant une personne physique identifiée ou identifiable par des moyens raisonnables

Non anonymisée

Dir. « *Il y a lieu d'appliquer les principes relatifs à la protection des données à toute information concernant une personne physique identifiée ou identifiable. Pour déterminer si une personne physique 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 pour identifier la personne physique directement ou indirectement, tels que le ciblage*".
La directive reprend les règles posées par le RGPD pour présumer identifiable la personne dont un identifiant (oui je sais) est utilisé (numéro de sécurité sociale, numéro fiscal, numéro de téléphone), des données de localisation (géolocalisation), identifiant en ligne (email), un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale (par ex. identité physique == vidéosurveillance et stockage des données pendant un laps de temps certain == IoT + caméras sur le net).
Moyen raisonnable: « *Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci* ». Donc pas les moyens de la NSA, mais un logiciel de défloutage d'images par exemple.
Tout type de données peut constituer une donnée personnelle, mais certaines catégories sont plus sensibles (génétique, médicale, opinion politique). L'art.9 du RGPD indique que la collecte de certaines données est en principe interdite.
Il n'y a (logiquement) pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable (avec des moyens raisonnables, donc pas ceux de la NSA mais si c'est chiffré avec un chiffrage aisément déchiffrable… bof quoi).

Principes

Directive 2016/680, cons. 26

- **licite, loyal et transparent à l'égard des personnes physiques concernées**
- **être effectué qu'aux fins spécifiques fixées par la loi (intérêt général) : ces finalités devraient être explicites et légitimes, et déterminées au moment de la collecte des données à caractère personnel**
- **qu'elles constituent une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des intérêts légitimes de la personne physique concernée.**
- **Les personnes physiques devraient être informées des risques, règles, garanties et droits en ce qui concerne le traitement de données à caractère personnel les concernant et des modalités d'exercice de leurs droits par rapport au traitement.**
- **Sécurité et de confidentialité**

Ce texte reprend les idées permettant d'évaluer la licité d'un traitement de données personnelles (a contrario, si ces conditions ne sont pas remplies, il faut commencer à se poser des questions, voire à poser des questions par écrit).
Licite: consentement ou contrat ou obligation légale ou intérêts vitaux ou mission de service public ou intérêt légitime du responsable du traitement. (RGPD art.6).
Obligation légale => les Etats membres peuvent préciser par rapport au règlement.
Transparent: la personne doit en être informée en principe.
Ces principes n'interdisent pas en soi aux autorités répressives de mener des activités telles que des enquêtes discrètes ou de la vidéosurveillance. Ces activités peuvent être menées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, pour autant qu'elles soient déterminées par la loi.

Finalités

Directive 2016/680, cons. 26

- **Le traitement (collecte, analyse, usage) doit être effectué qu'aux fins spécifiques fixées par la loi (intérêt général, dir.)**
- **(RGPD): ces finalités devraient être explicites et légitimes, et déterminées au moment de la collecte des données à caractère personnel**

Les finalités doivent être légales ou sur base d'un contrat établi avec les personnes dont les données sont collectées (et toujours dans les limites ce qui est légalement possible).
Ex. Aspiration d'annuaires, case à cocher pour accord pour transfert des données aux partenaires commerciales du prestataire.
≠ urgence : l'investigation se déroule parfois dans le feu de l'action, au moins dans un premier temps. quid?
cons. 49: RGPD Le traitement de données à caractère personnel dans la mesure strictement nécessaire et proportionnée aux fins de garantir la **sécurité** du réseau et des informations, c'est-à-dire la capacité d'un réseau ou d'un système d'information de résister, à un niveau de confiance donné, à des événements accidentels ou à des actions illégales ou malveillantes qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité de données à caractère personnel conservées ou transmises, ainsi que la sécurité des services connexes offerts ou rendus accessibles via ces réseaux et systèmes, par des autorités publiques, des équipes d'intervention en cas d'urgence informatique (CERT), des équipes d'intervention en cas d'incidents de sécurité informatique (CSIRT), des fournisseurs de réseaux et de services de communications électroniques et des fournisseurs de technologies et services de sécurité, **constitue un intérêt légitime du responsable du traitement concerné**. Il pourrait s'agir, par exemple, d'empêcher l'accès non autorisé à des réseaux de communications électroniques et la distribution de codes malveillants, et de faire cesser des attaques par «déni de service» et des dommages touchant les systèmes de communications informatiques et électroniques.
Encore faut-il que l'urgence ne s'éternise pas. Donc l'excuse de réponse à incident ne couvre pas la totalité de l'investigation, et une fois passé l'urgence, il convient de revenir aux principes de base évoqués plus haut.

Finalités

2017 netzpolitik.org: **Privatfirmen forschten für RWE und Porsche politische Aktivisten in Großbritannien aus**

British Airways, die Royal Bank of Scotland, RWE, Caterpillar und Porsche haben private Sicherheitsfirmen beauftragt, um politische Gruppen in Großbritannien zu überwachen. Diese Erkenntnisse beruhen auf hunderten Seiten geleakter Unterlagen solcher Firmen aus den Jahren 2003-2011, welche der Guardian und das Bureau for Investigative Journalism ausgewertet haben.

Die Überwachung beruhte nicht nur auf der Auswertung öffentlich verfügbarer Informationen, sondern schloss auch den Einsatz falscher Aktivisten mit ein, welche die Gruppen infiltrierten. Dabei halfen die privaten Spitzel bei Kampagnen, gingen zu Demonstrationen und beschafften sich interne Dokumente und Kommunikation. Bei den privaten Geheimdiensten handelte es sich um die Firmen Inkerman und C2i. Letztere warb gegenüber potenziellen Kunden damit, sie verfüge über Echtzeit-Quellen bei Greenpeace, Friends of the Earth, bei lokalen Umweltgruppen in Oxford sowie bei Fluggegnern. C2i versuchte seine Dienste auch an Donald Trump zu verkaufen als dieser seinen Golfplatz in Schottland baute.

Cet article indique que des entreprises privées britanniques ont exercé ont mandaté des entreprises de sécurité (Inkerman et C2i) pour réaliser la surveillance d'activistes. Cette surveillance ne s'exerçait pas seulement par de la collecte d'informations publiquement accessibles mais aussi par le recours à des infiltrés dans les groupes cibles.
(la technique d'infiltration est légalement possible pour la police, la législation pose les conditions de régularité de ces mesures d'enquête. A l'évidence, des investigateurs privés ne sont pas dotés de ces pouvoirs, de sorte que ce simple fait est une violation de principe de collecte loyale et transparente des données). Ceci est donc un exemple du type d'investigation qui pourrait vous être demandée (à vous d'expliquer en quoi c'est problématique) ou que vous pourriez découvrir dans le cadre d'une prestation de service informatique.

Principe de proportionnalité

CJUE, 27/9/2017, aff. affaire C-73/16: principe de proportionnalité. (…) la protection du droit fondamental au respect de la vie privée au niveau de l'Union exige que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire (voir, en ce sens, arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 96 ainsi que jurisprudence citée).

Dans cette affaire, un citoyen slovaque, M. Peter Puškár, était en litige avec la direction des finances de la République slovaque et le bureau de lutte contre la criminalité financière de Slovaquie, dont il exigeait qu'il supprime son nom d'une liste de personnes considérées par les autorités comme des prête-noms, établie par celle-ci dans le cadre de la perception de l'impôt et la lutte contre la fraude fiscale. La Cour estime la constitution de tel fichier licite dès lors que les conditions notamment de légalité et de proportionnalité sont remplies.

Droit à la sécurité des données

Cons. 96 de la directive (délai d'implémentation):

« le responsable du traitement ou le sous-traitant devra s'être doté des moyens effectifs de démontrer la licité du traitement des données, de pratiquer l'autocontrôle et de garantir l'intégrité et la sécurité des données, tels que des journaux ou d'autres formes de registres »

Le texte parle de lui-même, le RGPD comme le droit français des données personnelles connaissent le même principe.
Un exemple extrême de violation du droit des données personnelles nous est donné par un arrêt de la chambre criminelle du 5 février 2013, n°12-80.573, approuvant la condamnation d'un gardien de la paix qui épluchait les fichiers de police pour donner des informations à sa femme, gérante de sociétés dans le domaine de l'immobilier. La justice a sanctionné le détournement de finalité du traitement de données personnelles s'agissant de l'agent, et le recel, dans le chef de la femme. Cet exemple est caricatural car en l'espèce, il est évident que les auteurs avaient conscience du caractère illicite de leurs agissements. Il permet cependant de comprendre la nécessité pour les professionnels de l'investigation numérique de maîtriser le cadre légal.
=> mise en place de contrôle
=> sensibilisation du personnel (ne pas collecter trop de données, ne pas les détourner, confidentialité)
=> signalement des abus constatés (et il faudrait aussi relever le défaut de dispositif de traçage des accès lorsque vous procédez à un audit d'une base de données)

Sanctions

Autorités de contrôle

Réparations civiles

Sanctions c/ l'auteur de l'infraction

Complicité, recel

La directive comme le GDPR rappelle que la protection des données est confiée à des autorités indépendantes, dotées de moyens et de pouvoir d'investigation. La CNIL est l'autorité française, mais tous les pays européens ont un équivalent. A cela s'ajoute le chargé de la protection des données au niveau de l'Union européenne.
L'apport du GDPR est de tenir compte du caractère transfrontière des fuites de données, et définir des règles de compétence entre les différentes autorités nationales ainsi que les moyens pour les individus de les saisir et d'en recevoir réponse, même lorsqu'il s'agit d'une autorité d'un autre Etat membre.
Réparations civiles: problème de l'évaluation du préjudice subi par la victime d'une compromission de la sécurité d'une base de données.
Sanction(s) pénale(s) de l'auteur de l'infraction de collecte / usage illicite de données personnelles
Les infractions annexes:
- complicité = fourniture de moyens? la non dénonciation de crime n'est pas assimilable à un acte de complicité. C'est une infraction autonome. La non dénonciation de délit n'est pas une infraction. (Art.40 du code pénal fr: Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs. Obligation sanctionnée seulement disciplinairement pour les fonctionnaires.)

- recel = tirer profit du produit d'une infraction
- (Complément par rapport à ce qui a été dit lors de la conférence) GROS RISQUE: le Luxembourg assimile le vol de données à un vol pur et simple, et a admis sur la base de la **législation anti-blanchiment** la sanction celui qui réutilise le produit de ce vol. Donc, en bonne logique, toute personne qui réutilise les données personnelles « volées » tombe sous le coup de cette incrimination. A voir si le droit français va s'aligner sur cette position, étant précisé que la réglementation anti-blanchiment est commune à tous les pays européens dans ses principes. Vous risquez donc de retrouver le même type de solution dans d'autres pays de l'Union.

Responsable du traitement

met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire.

Dir. = autorité publique ou privée, mais investie de prérogatives de puissance publique (art.3 point 7)
Responsable du traitement: Dir. (art.3 point 8): « *l'autorité compétente qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel*. » => si vous copiez et analysez un disque dur avec des données bancaires dans le cadre d'une investigation privée ou publique, vous êtes celui qui détermine les finalités (ici, chercher des informations) et les moyens (les outils d'analyse) du traitement. VOUS ENTREZ DONC DANS LE CHAMP d'application du droit des données personnelles.
RGPD = tous les autres.
Sous traitant = art.28 RGPD « Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée. » = blinder les contrats et tout faire valider par écrit en principe. §§3 et 4 de l'article 28: UE ou l'Etat peuvent proposer des clauses types.
Ex. Le sous-traitant « veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité » => s'assurer (dans la mesure du possible) que personne ne quitte l'entreprise avec un disque dur comprenant les dernières investigations. Envisager de déclarer les données que vous utilisez dans le cadre de vos recherches, de façon à ne pas encourir les foudres de la CNIL.

Responsable du traitement

Art. 11 de la directive: « 1. Lorsque les données n'ont pas été collectées auprès de la personne concernée, les États membres prévoient que le responsable du traitement ou son représentant doit, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard lors de la première communication de données, fournir à la personne concernée au moins les informations énumérées ci-dessous, sauf si la personne en est déjà informée :

a) l'identité du responsable du traitement et, le cas échéant, de son représentant ;

b) les finalités du traitement ;

c) toute information supplémentaire telle que :

– les catégories de données concernées,

– les destinataires ou les catégories de destinataires des données,

– l'existence d'un droit d'accès aux données la concernant et de rectification de ces données,

dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données. »

=> information de la personne concernée (ex. Linkedin, faille, aucune information)
=> notification de la violation de la confidentialité des données / d'une collecte illicite de données.

Signalement

-> données illicites (collecte illicite)

-> fuite de données

-> accès illicite

Dans le cas d’audit privé, ces faits devraient faire l’objet de signalement, d’abord au DPO (chargé de la protection des données), puis à la CNIL/Procureur de la République. Il vaut quand même mieux commencer par le DPO, qui aura peut-être une bonne explication à vous fournir par écrit. Et s’il n’y en a pas dans l’entreprise, c’est le moment de lui suggérer d’étendre la mission à l’aspect données personnelles.

Questions

- Sebastien Larinier: NDA quid? Quelle responsabilité du prestataire dans ce cas?
- Comment obtenir la suppression d'information d'entreprise sur Shodan?
- (questions par après) RGPD et Action de groupe?

R. Aucun contrat ne peut dispenser un individu de respecter les dispositions pénales (art. 6 du Code civil français (texte qui existe depuis 1804): On ne peut déroger, par des conventions particulières, aux lois qui intéressent l'ordre public et les bonnes moeurs »). Donc, sans revenir sur ce qui précède, disons qu'un accord de confidentialité (NDA= non disclosure agrement) ne vous protège pas d'une sanction de votre inaction vis-à-vis par exemple d'une collecte de données illégale. Par contre, comme vous n'êtes a priori pas le responsable de la collecte, vous n'êtes pas concernés au premier chef, et le contrat peut vous permettre de démontrer, en cas d'investigation, que votre client connaissait le caractère illicite de son comportement (ce serait plutôt un élément qui jouerait contre lui). Le RGPD traite expressément de la question de la responsabilité des sous-traitants à l'article 82 point 2, qui sont exonérés de toute responsabilité quand ils ont agi dans le cadre d' « instructions LICITES » du responsable du traitement et dans le respect des obligations édictés par le RGPD.
R2. Les données personnelles protègent les personnes physiques, non les sociétés. En plus, on va dire que casser le thermomètre parce qu'il fait froid, ça n'aide pas vraiment à se réchauffer. A mon sens, ce n'est pas Shodan le problème, étant précisé, qui si un moteur de recherche public peut exposer les failles d'un SI, cela signifie que certains attaquants, notamment étatiques ou de groupes mafieux organisés, ont la même possibilité. Mais eux le feront silencieusement, ce qui me semble être un bien plus gros problème.
R3. Le RGPD n'emploie pas le terme d'action de groupe, mais ça y ressemble (article 80). Il semblerait que notre législateur national ait décidé lors des débats à l'AN de ne pas inclure de disposition relative à l'action de groupe dans la loi. Mais le RGPD étant un règlement européen, il sera applicable, même en l'absence de transposition. Personnellement, je pense que la Quadrature du Net par exemple, pourra se prévaloir du texte européen. De plus, même si nos associations nationales n'avaient pas cette possibilité, il ne faut pas négliger le fait que d'autres droits nationaux européens vont sans doute être moins timides et que les fuites de données ne sont que rarement franco-française.