RGPD : application territoriale et extra-territoriale

Sylvain Métille/Annelise Ackermann

Table des matières

A. Introduction

Le 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 (RGPD) représente plusieurs nouveautés en matière de protection des donnés. L'une d'elles concerne son champ d'application territorial.

Contrairement à son champ d'application matériel assez traditionnel (B), le RGPD prévoit un champ d'application géographique aux responsables du traitement et sous-traitants présents sur son territoire (C.I), mais surtout il étend la protection des personnes concernées avec une application extraterritoriale à des responsables du traitement (voire des sous-traitants) hors de l'EEE mais qui visent des résidents dans l'EEE ou font du profilage de ceux-ci (C.II).

La question du champ d'application, comme le risque de recevoir une amende, a reçu beaucoup d'interprétations fondamentalement erronées. Nous en discuterons

alors quelques-unes, qui sont progressivement devenues de fausses croyances (D). Nous mentionnerons encore brièvement quelques particularités à prendre en compte lorsque le RGPD s'applique de manière extraterritoriale (E).

B. Champ d'application matériel

D'un point de vue matériel, le RGPD s'applique à tout « traitement de données personnelles, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel[1] qui sont contenues ou pourraient être contenues dans un fichier ».[2]

La forme juridique de l'auteur du traitement n'est pas très importante et le RGPD s'applique tant au traitement mis en œuvre par une personne physique qu'une personne morale de droit public ou privé, lorsqu'elle traite de données personnelles relatives à des personnes physiques. En revanche et contrairement à la Loi fédérale du 19 juin 1992 sur la protection des données (LPD ; RS 235.1), le RGPD ne protège que les personnes physiques : il ne s'applique pas au traitement de données concernant des personnes morales.[3]

L'art. 2 (2) RGPD prévoit quelques exceptions concernant le champ d'application matériel. Les traitements de données personnelles effectués par une personne physique au cours d'activités strictement personnelles ou domestiques, tels qu'un échange de correspondance ou la tenue d'un carnet d'adresses, ne sont pas soumis au RGPD (let. c).[4] Conformément à la let. d, le RGPD ne s'applique pas non plus au traitement effectué par les autorités compétentes 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 des menaces pour la sécurité publique et la prévention de telles menaces. Ce domaine est régi par la Directive (UE) 2016/680 du 27 avril 2016 et concerne principalement la prévention et la détection des infractions pénales. Finalement, le RGPD ne s'applique pas aux données traitées par les États membres de l'EEE dans le cadre de la politique étrangère et la politique de sécurité commune (let. b) ou dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'UE (let. a).

1 Le RGPD parle de données à caractère personnel, ce qui correspond à la notion de données personnelles de l'art. 3 let. a LPD. Les deux notions sont utilisées ici de manière équivalente. Seule la notion de personne diffère, puisque la LPD inclut les personnes morales contrairement au RGPD.

2 Art. 2 (1) RGPD.

3 Consid. 14 RGPD.

4 Consid. 18 RGPD ; art. 2 (2) let. c RGPD. L'art. 2 al. 2 LPD prévoit une exception similaire. Contrairement au RGPD qui inclut dans l'activité strictement domestique l'échange de correspondance et la tenue d'un carnet d'adresses, ou l'utilisation de réseaux sociaux et les activités en ligne qui ont lieu dans le cadre de ces activités (consid. 18), la LPD exige que les données ne soient pas communiquées à des tiers.

C. Champ d'application géographique

I. Application territoriale du RGPD

Comme la plupart des lois, le RGPD impose d'abord des obligations à ceux qui se trouvent sur le territoire où la loi a été adoptée, soit l'Union Européenne (UE)[5] et l'Espace Économique Européen (EEE)[6] à la suite de la décision du Comité mixte du 6 juillet 2018 qui prévoit l'intégration du RGPD dans l'Accord EEE.[7]

Le RGPD s'applique donc aux responsables du traitement et sous-traitants présents sur le territoire de l'EEE.[8] Cette présence est déterminée par la notion d'établissement : l'art. 3 (1) RGPD prévoit une application aux organisations disposant d'un « établissement » dans l'EEE, dès lors que des données personnelles sont traitées « dans le cadre des activités » de tels établissements.

Le critère décisif est celui de l'existence d'un établissement dans l'EEE, ce qui suppose l'exercice effectif et réel d'une activité au moyen d'un dispositif stable. La forme juridique retenue pour un tel dispositif, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante.[9]
La jurisprudence rendue précédemment dans le cadre de la Directive 95/46/CE et du Traité sur le fonctionnement de l'Union européenne (TFUE) permet aussi de mieux définir la notion d'établissement.[10] Il faut retenir « une conception souple de la notion d'établissement, qui écarte toute approche formaliste selon laquelle une entreprise ne serait établie que dans le lieu où elle est enregistrée ».[11] Un rattache-

5 Les États membres de l'UE sont l'Allemagne, l'Autriche, la Belgique, la Bulgarie, Chypre, la Croatie, le Danemark, l'Espagne, l'Estonie, la Finlande, la France, la Grèce, la Hongrie, l'Irlande, l'Italie, la Lettonie, la Lituanie, le Luxembourg, Malte, les Pays-Bas, la Pologne, le Portugal, la République tchèque, la Roumanie, le Royaume-Uni (seulement jusqu'au Brexit), la Suède, la Slovaquie et la Slovénie.

6 Soit le Liechtenstein, la Norvège et l'Islande, en plus des 28 États membres de l'UE.

7 Le contenu de la décision ne manque pas de surprendre sur un aspect en particulier, à savoir la référence aux États membres de l'AELE comme devant être compris dans la notion d'États membres au sens du RGPD. Si cela était pris à la lettre, la Suisse serait incluse (!). Quand bien même cette interprétation serait intéressante dans certaines situations, il faut évidemment comprendre que le texte fait référence uniquement aux États de l'AELE membres de l'EEE, ce qui exclut la Suisse. Le Comité mixte n'aurait de toute façon pas la compétence de prendre des décisions qui engageraient la Suisse.

8 Seul l'EEE sera mentionné dans la suite de la présente contribution, puisque son territoire inclut non seulement les États membres de l'UE mais également les trois États de l'AELE membres de l'EEE.

9 Consid. 22 RGPD ; *Nicolas Passadelis/Simon Roth*, Weisser Rauch über Brüssel. Was Schweizer Unternehmen über die europäische Datenschutz-Grundverordnung wissen müssen, Jusletter, 4 avril 2016, 5.

10 *Philipp Mittelberger*, Der Extraterritoriale Ansatz der Datenschutzgrundverordnung (DS-GVO), 2018, 21 ; *Passadelis/Roth* (note 9), 5.

11 CJUE, aff. C-230/14, ECLI:EU:C:2015:639, consid. 29 (Weltimmo) ; CJUE, aff. C-191/15, ECLI:EU:C:2016:612, consid. 77 (Verein für Konsumenteninformation).

ment purement technique, comme des serveurs ou des boîtes aux lettres d'entreprises, ne remplit pas à lui seul le critère de l'établissement,[12] mais il faut en revanche que des moyens humains et techniques nécessaires à la fourniture de services particuliers soient disponibles en permanence.[13]

La notion est large et la Cour de justice de l'Union européenne (CJUE) a eu l'occasion de préciser dans l'arrêt *Weltimmo* que la présence d'un seul représentant (en l'espèce une personne physique) peut être suffisante pour constituer un établissement stable, pour autant que ce dernier agisse avec un degré de stabilité suffisant à l'aide de moyens nécessaires à la fourniture des services concrets concernés.[14] Dans cette affaire, la société *Weltimmo*, établie en Slovaquie, organisait l'exploitation d'un site web d'annonces immobilières concernant des biens établis en Hongrie. *Weltimmo* ayant refusé de donner suite aux demandes d'effacement de certains annonceurs, ces derniers ont porté plainte auprès de l'autorité hongroise de contrôle qui a estimé que la collecte de données concernées constituait un traitement sur le territoire hongrois, ce qu'a confirmé la CJUE. Elle a retenu un faisceau d'indices pour considérer que *Weltimmo* disposait d'un établissement en Hongrie, en particulier :

- l'exploitation de sites web d'annonces immobilières concernant des biens situés en Hongrie ;
- des sites web rédigés en langue hongroise ;
- un représentant de la société *Weltimmo* domicilié en Hongrie ;
- un compte bancaire et une boîte aux lettres en Hongrie.

Une organisation peut donc être considérée comme « établie » dès lors qu'elle exerce « toute activité réelle et effective – même minime – » au moyen d'une « installation stable » sur le territoire de l'EEE.[15]

La présence d'un établissement ne déclenche pas l'application du RGPD à toutes les données traitées par un groupe de sociétés, mais seulement aux données personnelles que l'établissement traite dans le cadre de ses activités.[16] Cela suppose de pouvoir déterminer le degré de participation de l'établissement aux activités dans le cadre desquelles des données personnelles sont traitées.[17] Il s'agit ici d'établir quelles activités sont exercées par quel établissement, afin de dissocier les différentes activités exercées par les divers établissements d'une même entreprise situés sur et hors du territoire de l'EEE.[18]

---

12 *Manuel Klar*, in : Jürgen Kühling/Benedikt Buchner (éd.), Kommentar zur DS-GVO, 2017, art. 3 N 46.

13 *Brendan Van Alsenoy,* Reconciling the (extra)territorial reach of the GDPR with public international law, in : Gert Vermeulen/Eva Lievens (éd.), Data Protection and Privacy under Pressure, Transatlantic tensions, EU surveillance, and big data, 2017, 77, 80.

14 CJUE, aff. C-230/14, ECLI:EU:C:2015:639, consid. 30 (Weltimmo).

15 CJUE, aff. C-230/14, ECLI:EU:C:2015:639, consid. 28 (Weltimmo) ; *Mittelberger* (note 10), 8.

16 Cette même condition figurait déjà à l'ancien art. 4 (1) let. a de la Directive 95/46/CE ; *Mittelberger* (note 10), 9.

17 G29, Avis 8/2010 sur le droit applicable du 16 décembre 2010, 16.

18 G29 (note 17), 17.

Le RGPD ne s'applique pas aux données personnelles traitées directement « par » l'établissement concerné, mais à toutes les données personnelles traitées « dans le cadre des activités » de cet établissement.[19]

Dans l'arrêt *Google Spain*, la CJUE a ainsi considéré que « le traitement de données à caractère personnel qui est fait pour les besoins du service d'un moteur de recherche tel que *Google Search*, lequel est exploité par une entreprise ayant son siège dans un État tiers mais disposant d'un établissement dans un État membre, est effectué 'dans le cadre des activités' de cet établissement si celui-ci est destiné à assurer, dans cet État membre, la promotion et la vente des espaces publicitaires proposés par ce moteur de recherche, qui servent à rentabiliser le service offert par ce moteur ».[20] Le Tribunal fédéral avait tenu un raisonnement similaire dans son arrêt concernant *Google Street View* en retenant la légitimation passive non seulement de *Google Inc*. mais également de *Google Suisse Sàrl*.[21]

Le critère de rattachement de l'établissement devient donc de plus en plus lâche. Si la condition de l'établissement est remplie, le RGPD s'appliquera indépendamment du fait que le traitement des données ait effectivement lieu ou non dans l'EEE,[22] de la nationalité ou résidence des personnes concernées. Le RGPD a donc pour vocation de régir tout traitement de données en lien avec l'activité des responsables du traitement présents sur son territoire, même si le traitement effectif n'y a pas lieu ou qu'il concerne exclusivement des personnes qui ne s'y trouvent pas.

Il faut encore ajouter un cas d'application territorial particulier, à savoir les « extensions » du territoire national. Le RGPD s'applique en effet aussi au traitement de données personnelles par un responsable du traitement qui n'est pas établi dans l'EEE mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public.[23] Ce peut être en particulier le cas d'une représentation diplomatique ou consulaire d'un État membre[24] ou alors d'un navire européen se trouvant en haute mer.[25]

II. Application extraterritoriale du RGPD

1. En général

Le RGPD a ensuite pour vocation de protéger ceux qui se trouvent sur son territoire, indépendamment de savoir où se trouve celui qui traite les données. C'est l'application extraterritoriale. Séduisante sous l'angle des larges compétences données

19 CJUE, aff. C-131/12, ECLI:EU:C:2014:317, consid. 52 (Google Spain et Google) ; *Mittelberger* (note 10), 29.

20 CJUE, aff. C-131/12, ECLI:EU:C:2014:317, consid. 55 (Google Spain et Google) ; *Mittelberger* (note 10), 11.

21 ATF 138 II 346, consid. 4 non publié (disponible seulement dans l'arrêt 1C_230/2011 du 31 mai 2012).

22 Consid. 22 RGPD ; *Passadelis/Roth* (note 9), 5.

23 Art. 3 (3) RGPD.

24 Consid. 25 RGPD ; CEPD, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version 2.0 adoptée le 12 novembre 2019, exemple 22, 22.

25 CEPD (note 24), exemple 23, 23.

aux autorités de contrôle et de la protection théoriquement sans faille offerte à ses résidents, elle pose de nombreux problèmes pratiques.

Premièrement, elle ne s'applique pas *urbi et orbi*, mais dans deux cas de figure bien précis, soit dans le cas de l'offre de biens et de services à des résidents de l'EEE[26] et dans le cas du suivi du comportement sur Internet de personnes dans l'EEE.[27] Ces cas peuvent néanmoins s'interpréter largement et couvrir un grand nombre de situations. Deuxièmement, cette application très large n'est pas forcément reconnue par les autres États, en particulier ceux dans lesquels se trouvent des responsables du traitement.[28] Troisièmement, ces responsables du traitement étrangers n'auront pas toujours connaissance des exigences du RGPD lorsqu'ils ne visent pas le marché de l'EEE, qui peut être une législation exotique pour eux.

Mis à part les cas clairs, notamment ceux où les responsables du traitement visent clairement le marché de l'EEE avec une activité commerciale importante, l'étendue de l'application concrète, et non seulement théorique, du RGPD doit encore être prouvée. Il semble que dans beaucoup de cas les autorités de contrôle veulent se garder une possibilité d'agir, sans pour autant l'utiliser systématiquement. Cela reste néanmoins un risque non négligeable, comme la possibilité qu'un résident européen saisisse une autorité de contrôle ou une autorité judiciaire, voire obtienne des mesures en application du RGPD alors même que le traitement des données concernées ne pourrait en réalité représenter qu'un volume de données tout à fait marginal pour la société étrangère.[29]

2. Offre de biens ou de services

a) Le principe

Le premier cas d'application extraterritoriale est lié au principe du lieu du marché (*Marktort-Prinzip*).[30] Il doit garantir qu'une personne physique ne soit pas exclue de la protection à laquelle elle a droit en vertu du RGPD parce que le responsable du traitement lui fournit des biens ou des services depuis l'étranger. Le traitement de données personnelles de personnes qui se trouvent dans l'EEE par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'EEE est ainsi soumis au RGPD « lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes, qu'un paiement soit exigé ou non ».[31]

---

26 Cf. *infra* C.II.2.

27 Cf. *infra* C.II.3.

28 Elle peut même dans certains cas être incompatible avec le droit local. Cf. *infra* E.IV.

29 Et même dans le cas du profilage d'une seule personne temporairement dans l'UE/EEE !

30 *Lukas Bühlmann/Michael Reinle,* Extraterritoriale Wirkung der DSGVO, digma 2017, 8 ; *Passadelis/Roth* (note 9), 5 ; *Klar* (note 12), art. 3 N 9.

31 Art. 3 (2) RGPD.

b) Des biens et des services

La notion de biens et de services n'est pas définie dans le RGPD, mais on peut s'inspirer de la Directive 2011/83/UE relative aux droits des consommateurs,[32] dont l'art. 2 (3) définit un bien comme « tout objet mobilier corporel, sauf les objets vendus sur saisie ou de quelque autre manière par autorité de justice ». La notion de biens est large et inclut l'eau, le gaz et l'électricité lorsqu'ils sont conditionnés dans un volume délimité ou en quantité déterminée.

Quant aux services, il faut aussi retenir une notion large incluant tous les types de services.[33] La Directive 2006/123/CE relative aux services dans le marché intérieur donne la définition suivante d'un service : « toute activité économique non salariée, exercée normalement contre rémunération ».[34] La Directive fait référence également à la définition des services contenue dans le Traité instituant la communauté européenne (TCE). L'art. 50 TCE précise que les prestations fournies normalement contre rémunération sont considérées comme services dans la mesure où elles ne sont pas régies par les dispositions relatives à la libre circulation des marchandises, des capitaux et des personnes. À titre d'exemples sont citées les activités de caractère industriel, de caractère commercial, artisanales et des professions libérales. À noter qu'il n'est pas nécessaire qu'un paiement soit exigé,[35] qu'il s'agisse de biens ou de services.

c) Des personnes sur le territoire de l'EEE

Il ne suffit pas d'offrir des biens ou des services, encore faut-il une offre à des personnes sur le territoire de l'EEE. Cela ne couvre pas seulement les citoyens de l'EEE, mais toute personne se trouvant sur le territoire de l'EEE, sans qu'il ne soit tenu compte de son domicile, de sa nationalité, ou encore de ses centres d'intérêts vitaux.

Ni l'art. 4 RGPD, ni ses considérants ne précisent ce qu'il faut entendre par « se trouver » sur le territoire de l'EEE. D'un point de vue temporel, il ne semble pas nécessaire que la présence des personnes concernées soit durable. Le terme « se trouver » ne suppose pas un élément de continuité particulière et des travailleurs présents de manière temporaire, des étudiants en échange ou des voyageurs doivent être considérés comme remplissant cette condition. Dans ce contexte, il devrait suffire que les personnes concernées se trouvent dans le territoire de l'EEE au moment des premiers traitements de données personnelles en question.[36] Selon les lignes directrices relatives au champ d'application territorial du RGPD publiées par le Comité Européen de la Protection des Données (CEPD), le critère de la présence

32 Directive 2011/83/UE du Parlement européen et du Conseil du 25 octobre 2011 relative aux droits des consommateurs, modifiant la directive 93/13/CEE du Conseil et la directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la directive 85/577/CEE du Conseil et la directive 97/7/CE du Parlement européen et du Conseil. Texte présentant de l'intérêt pour l'EEE.

33 *Rosemary Jay*, Guide to the General Data Protection Regulation, 2017, n°4-030.

34 Art. 4 (1) Directive 2006/123/CE.

35 Art. 3 (2) let. a RGPD.

36 *Klar* (note 12), art. 3 N 63 ; *Van Alsenoy* (note 13), 85.

des personnes concernées au sein de l'EEE doit simplement être rempli au moment où l'offre de biens ou de services est faite.[37]

d) Une intention de viser le marché

Il faut ensuite établir si le responsable du traitement ou le sous-traitant « envisage » d'offrir des biens ou des services à des personnes concernées dans un ou plusieurs États membres de l'EEE.[38] Le fait qu'un site web soit accessible depuis l'EEE n'est pas suffisant.[39] Il doit au contraire être apparent que la société envisage que ses activités soient dirigées vers les résidents de l'EEE.[40] Le RGPD n'a donc pas pour vocation d'attraper n'importe quel traitement de données concernant une personne présente sur son territoire en application de l'art. 3 (2) let. a RGPD mais seulement les traitements qui ont lieu dans le cadre d'une activité qui vise les résidents de l'EEE.[41] Dans ce sens, on peut attendre de celui qui développe une activité commerciale à destination d'un marché spécifique qu'il en respecte le cadre légal, même s'il agit depuis un pays étranger.

Ce qui est décisif, ce sont les circonstances concrètes et non la manière dont l'entité déclare envisager d'offrir des biens et des services dans l'EEE.[42] Conformément au principe de la bonne foi, une entité suisse qui fournit des biens ou des services à des personnes se trouvant dans l'EEE, de manière ciblée et intentionnelle ne pourra alors pas prétendre ne pas viser spécifiquement le marché européen, ce qui conduira à appliquer le RGPD. La proportion des clients se trouvant dans l'EEE peut être un indice s'agissant du critère de l'intention, mais il ne s'agit pas d'un critère absolu. La situation est différente pour l'entité qui vise prioritairement le marché suisse mais accepte également des clients résidant à l'étranger (y compris dans l'EEE). Dans ce cas, l'application du RGPD ne se justifie pas, faute d'intention de viser les résidents de l'EEE. Il en va de même des clients touchés par inadvertance ou par accident.

Dans le même sens, l'utilisation d'un avertissement indiquant que l'offre de biens ou de services ne s'adresse pas à des personnes concernées se trouvant dans l'EEE ne suffit clairement pas pour échapper à l'application de l'art. 3 (2) RGPD.[43] Par exemple, celui qui, de manière cohérente, indique sur son site web ne pas s'adresser à des résidents européens et ne cherche pas à leur fournir les biens et services proposés à d'autres pays ne devrait pas être soumis au RGPD. En revanche, celui qui se réfugie derrière un avertissement mais a clairement l'intention de diriger son offre à destination des personnes se trouvant dans l'EEE sera soumis au RGPD. Il sera en effet difficile de retenir sa bonne foi. Seul le fait d'envisager

37 CEPD (note 24), 15.
38 Consid. 23 RGPD.
39 *Bühlmann/Reinle* (note 30), 2 ; *Passadelis/Roth* (note 9), 6 ; Consid. 23 RGPD.
40 *Klar* (note 12), art. 3 N 81.
41 Il en va différemment de l'art. 3 (2) let. b RGPD, qui prévoit une application beaucoup plus brutale puisqu'elle est indépendante de la volonté du responsable du traitement. Cf. *infra* C.II.3.
42 *Mittelberger* (note 10), 23.
43 *Klar* (note 12), art. 3 N 81.

d'offrir des biens ou des services est pertinent s'agissant de l'application de l'art. 3 (2) RGPD.[44]

La fréquence de l'offre de biens ou de services n'est pas déterminante non plus pour l'application de l'art. 3 (2) RGPD.[45] Le traitement de données personnelles liées à une offre occasionnelle peut déjà entrer dans le champ d'application du RGPD.[46]

Les éléments suivants sont des indices que le responsable du traitement envisage d'offrir des biens ou des services à des personnes concernées dans l'EEE :[47]

- l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs États membres, avec la possibilité de commander des biens ou des services dans cette autre langue ;[48]
- la mention de clients ou d'utilisateurs qui se trouvent dans l'EEE ;
- le recours à des publicités payantes sur un moteur de recherche pour améliorer le référencement de la société dans les États de l'EEE ;
- la nature internationale de l'activité (hôtellerie, tourisme) ;
- la mention, sur le site web de la société, du numéro de téléphone avec l'indicatif international ;[49]
- l'utilisation d'un nom de domaine autre que celui du pays dans lequel se trouve la société (« .fr » ou « .eu ») ; et
- la description des itinéraires pour parvenir à la société depuis des États membres.

À titre d'exemple,[50] le CEPD mentionne un site web basé et géré en Turquie qui offre des services de création, édition, impression et livraison d'albums de photos de famille personnalisés. Le site est disponible en anglais, français, hollandais et allemand et les paiements peuvent être faits en euros. Le site indique que la livraison peut se faire en France, à destination des pays du Benelux et en Allemagne. La notion de services est clairement remplie. En outre, le fait que le site soit disponible en quatre langues parlées au sein de l'EEE et que la livraison puisse se faire dans plusieurs pays de l'EEE démontre une intention d'offrir ce service à des personnes

44 *Klar* (note 12), art. 3 N 81.

45 *Klar* (note 12), art. 3 N 70.

46 Cela ressort de l'art. 27 (2) let. a RGPD, qui prévoit que le responsable du traitement ou le sous-traitant hors de l'EEE n'a pas l'obligation de désigner un représentant au sein de l'UE/EEE si le traitement est occasionnel et qu'il ne concerne pas des données sensibles ou représente un risque particulier.

47 Consid. 23 RGPD ; CJUE, aff. C-230/14, ECLI:EU:C:2015:639 (Weltimmo) ; CJUE, aff. C-585/08, ECLI:EU:C:2010:740 (Pammer et Hôtel Alpenhof).

48 L'utilisation d'une langue qui est également utilisée en Suisse ne sera pas un indice utile. Dans ce cas, il convient d'apprécier l'intention du responsable du traitement pour le ciblage de son offre de biens et de services. Il faudrait prendre en compte le fait que le prestataire devait s'attendre à ce que son offre de biens ou de services soit accessible à des personnes se situant dans l'UE/EEE, étant donné qu'Internet permet une demande globale.

49 Ce critère ne nous paraît pas très utile, l'affichage d'un indicatif international étant courante en Suisse pour un usage interne ou visant des pays hors de l'EEE exclusivement.

50 CEPD (note 24), exemple 14, 18.

au sein de l'EEE. En revanche, dans un autre exemple,[51] la conclusion inverse s'impose pour une université suisse à Zurich qui lance une procédure de sélection pour un programme de Master en mettant à disposition une plateforme en ligne où les candidats peuvent télécharger leurs coordonnées, CV et lettre de motivation. La procédure de sélection est ouverte à tout étudiant ayant un niveau suffisant d'allemand et d'anglais et au bénéfice d'un Bachelor. Il n'y a pas de publicité spécifique à l'attention des étudiants au sein de l'EEE et le paiement se fait en francs suisses. Ici, une intention de viser le marché européen ne peut pas être démontrée et le traitement des données personnelles correspondant n'est pas soumis au RGPD. En effet, les critères linguistiques s'appliquent indépendamment de la provenance du candidat.

3. Suivi du comportement

Le second cas d'application extraterritoriale vise le suivi du comportement sur Internet. L'idée est aussi de s'assurer d'une application large du RGPD aux personnes présentes sur le territoire de l'EEE. L'application vise ici un cas plus rare, à savoir le suivi du comportement, mais avec des conditions d'application plus larges puisque contrairement au principe du lieu du marché, l'application du RGPD au suivi du comportement de personnes présentes sur le territoire de l'EEE n'exige pas que le responsable du traitement ait en plus l'intention de viser le marché de l'EEE.

Conformément à l'art. 3 (2) let. b RGPD, le RGPD s'applique également au traitement des données personnelles de personnes se trouvant sur le territoire de l'EEE par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'EEE, lorsque les activités de traitement sont liées au « suivi du comportement de ces personnes ».[52]

Il y a un suivi du comportement « si les personnes physiques sont suivies sur Internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage[53] d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit ».[54] Par profilage, il faut entendre tout traitement automatisé effectué sur des données personnelles et qui a pour but d'évaluer des attributs personnels d'individus.[55]

---

51 CEPD (note 24), exemple 16, 19.

52 Art. 3 (2) RGPD.

53 L'art. 4 (4) RGPD définit le profilage comme « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».

54 Consid. 24 RGPD.

55 *Jay* (note 33), n°14-005.

La notion de suivi régulier et systématique des personnes inclut toutes les formes de suivi et de profilage sur Internet,[56] y compris à des fins de publicité comportementale, qui « est une forme de publicité qui repose sur l'observation du comportement des individus au fil du temps. Elle vise à étudier les caractéristiques de ce comportement à travers leurs actions (visites successives de sites, interactions, mots clés, production de contenu en ligne, etc.) pour établir un profil spécifique et proposer aux personnes concernées des publicités adaptées à leurs centres d'intérêts ainsi déduits ».[57]

Le consid. 24 RGPD précise qu'afin de déterminer si une activité de traitement peut être considérée comme un suivi du comportement, il y a lieu d'établir si les personnes physiques sont suivies sur Internet. Les autres types d'opérations de suivi du comportement en dehors d'Internet, comme par exemple l'utilisation d'image satellite (par exemple *Google Earth*) ne devraient à notre avis pas tomber sous le coup du RGPD.[58] Le CEPD semble plutôt vouloir faire une interprétation extensive et les inclure.[59] En revanche, le suivi du comportement par le biais d'objets connectés pourrait tomber sous le coup du RGPD étant donné qu'ils sont reliés à Internet.

Le consid. 24 RGPD précise qu'est déterminante la question de savoir si le comportement des personnes suivies a lieu au sein de l'EEE. Cette notion est au moins aussi large que celle applicable s'agissant du principe du lieu du marché. En revanche, il suffit que les personnes soient sur le territoire, même si le responsable du traitement ne les vise pas sur ce territoire. Il suffit qu'un suivi du comportement ait lieu. Le CEPD confirme cette application très large et rappelle que contrairement à l'art. 3 (2) let. a, ni l'art. 3 (2) let. b, ni le consid. 24 n'introduisent expressément une exigence liée à l'intention de viser.[60]

Le CEPD illustre le cas du suivi du comportement à l'aide de l'exemple suivant : une entreprise de conseil en commerce de détail établie aux États-Unis fournit des conseils sur la disposition des marchandises à un centre commercial en France en se basant sur l'analyse des mouvements des clients dans le centre commercial collectés à travers le wifi. L'entreprise de conseil procède à du suivi de comportement de personnes se trouvant au sein de l'EEE et doit donc respecter le RGPD.[61]

L'application suivante du RGPD est en revanche assez choquante. Imaginons un responsable du traitement qui met à disposition de résidents suisses une application mobile, dans le cadre de services fournis exclusivement sur le territoire suisse et qui nécessitent un suivi régulier du comportement. Si un seul des clients qui ont consenti au suivi de leur comportement devait se rendre un week-end en vacances dans un pays voisin, le RGPD s'appliquerait (à l'insu même du responsable du traitement). L'art. 3 (2) let. b ne requiert en effet pas l'intention de viser le marché, contrairement à l'art. 3 (2) let. a RGPD. L'exemple donné par le CEPD laisse tou-

56 *Klar* (note 12), art. 3 N 92.
57 G29, Avis 2/2010 sur la publicité comportementale en ligne du 22 juin 2010, 5.
58 *Klar* (note 12), art. 3 N 92. Avis contraire: *Mittelberger* (note 10), 25.
59 CEPD (note 24), 19-20.
60 CEPD (note 24), 20.
61 CEPD (note 24), exemple 17, 20.

tefois planer le doute sur une interprétation plus raisonnable du RGPD : un responsable du traitement australien qui offre un service d'information et de contenu vidéo, basé sur les préférences et intérêts des utilisateurs, exclusivement à des personnes situées en Australie, même lorsqu'un des utilisateurs se rend en vacances en Allemagne et continue à utiliser le service, n'est pas soumis au RGPD.[62] Il n'est toutefois pas certain que le CEPD envisageait le service basé sur les préférences et intérêts des utilisateurs comme un suivi du comportement.

D. Mythes et fausses croyances

I. Leur origine

Le RGPD a été adopté le 27 avril 2016 et est entièrement applicable depuis le 25 mai 2018. Alors que les juristes ont mis passablement de temps avant de se rendre compte de son impact, en particulier hors de l'EEE, de nombreux consultants y ont vu rapidement un marché et se sont auto-proclamés experts en conformité RGPD. Malheureusement leur expertise juridique était parfois limitée, voire teintée de mauvaise foi, ce qui aboutissait *grosso modo* chaque fois à un discours faisant croire que toutes les entreprises suisses étaient systématiquement soumises au RGPD lorsqu'un citoyen européen risquait de figurer dans un de leurs fichiers[63] et qu'une amende d'au moins 4% du chiffre d'affaires était probable.[64]

L'application hors de l'EEE a aussi été un sujet d'importance secondaire pour beaucoup de juristes au sein de l'EEE, comme pour les autorités de contrôle. On en veut pour preuve que les lignes directrices n'ont été adoptées pour consultation qu'en novembre 2018 et qu'un consensus pour adopter la version finale n'a été trouvé qu'en novembre 2019.[65]

Parmi les erreurs les plus fréquentes,[66] on peut citer l'application systématique aux résidents européens (sans être dans un cas de l'art. 3 (2) RGPD), l'application aux travailleurs frontaliers et aux citoyens européens, et la non-application aux administrations publiques suisses.

II. Les données de travailleurs frontaliers

Le RGPD ne s'applique pas à un responsable du traitement établi en Suisse uniquement parce qu'il emploie des salariés frontaliers (qu'ils soient de nationalité suisse ou européenne). Les lignes directrices du CEPD donne l'exemple d'une entreprise basée à Monaco qui traite des données personnelles de ses employés, dont un grand nombre réside en France et en Italie. Ce n'est pas parce qu'elle a des

62 CEPD (note 24), exemple 8, 15.
63 Ce qui est évidemment faux.
64 Ce qui est tout aussi faux, l'amende n'étant qu'une des mesures à disposition des autorités de contrôle et le chiffre de 4% est un maximum pour la catégorie des violations les plus graves.
65 Et pourtant plusieurs questions n'y trouvent toujours pas de réponses claires.
66 Mise à part évidemment la mauvaise application des règles présentées précédemment.

travailleurs frontaliers que le RGPD est applicable à cette entreprise.[67] En effet, proposer un emploi à un ressortissant européen n'équivaut pas à fournir un service sur le territoire de l'EEE au sens de l'art. 3 (2) let. a RGPD. Tout au plus, s'il fallait y voir une notion de service, c'est bien plus l'employé frontalier qui offrirait un service à son employeur suisse. Les employeurs suisses qui occupent des salariés frontaliers ne peuvent pas non plus être considérés comme effectuant un suivi de comportement de ces personnes. Une exception, certes assez rare, concerne le cas où l'employeur suisse fournit des biens ou des services à ses employés sur le territoire de l'EEE et que ces biens ou services ne sont pas une composante du salaire, par exemple parce que le salarié est aussi client de l'entreprise et qu'il y achète des biens et des services. Le RGPD ne s'appliquera cependant qu'aux données liées à cette relation de client (par exemple la liste des achats) et non pas l'ensemble des données du salarié.

Le RGPD s'applique en revanche aux données de travailleurs frontaliers employés par un établissement dans l'EEE en application de l'art. 3 (1) RGPD, même s'ils résident en Suisse.

III. Les voyages d'affaires au sein de l'EEE

Lorsque des employés d'une entreprise établie hors de l'EEE, en Suisse par exemple, se trouvent de manière temporaire au sein de l'EEE pour un voyage d'affaires et que leurs données sont traitées par leur employeur, la question de l'applicabilité du RGPD semblait se poser pour certaines personnes.

Les données traitées le sont pourtant en lien avec les rapports de travail, par exemple en vue du remboursement du logement ou d'autres dépenses.

Certes, il y a un traitement de données de personnes se trouvant sur le territoire de l'EEE. En revanche, ce traitement n'est pas en lien avec une offre de biens ou de services. Le RGPD ne s'applique donc pas, sauf si un suivi du comportement des employés est effectué.[68]

IV. Les citoyens européens

Un responsable du traitement qui traite des données de nationaux européens résidant en Suisse ou qui emploie des salariés de nationalité européenne (qu'ils résident en Suisse ou dans l'EEE) n'est pas soumis au RGPD. Ce n'est pas la nationalité de la personne concernée qui compte, mais sa présence dans l'EEE au moment du traitement de ses données.[69] Cela peut s'illustrer de la manière suivante : l'autorité d'immigration canadienne qui traite des données personnelles des citoyens européens qui entrent sur son territoire n'est pas soumise au RGPD.[70]

67 CEPD (note 24), exemple 15, 18-19.
68 CEPD (note 24), exemple 13, 16-17.
69 *Jay* (note 33), n°4-029.
70 CEPD (note 24), exemple 12, 16.

Le simple traitement en Suisse de données personnelles relatives à des résidents européens (qu'ils soient ou non de nationalité européenne) ne déclenche pas l'application du RGPD. Encore faut-il que les données traitées le soient dans le cadre d'une offre de biens ou de services dans l'EEE ou dans le cadre du suivi du comportement en ligne.[71]

V. Le sous-traitant dans l'EEE d'un responsable du traitement suisse

Le responsable du traitement est la personne physique ou morale, l'autorité publique, le service ou un autre organisme « qui détermine les finalités et les moyens d'un traitement ».[72] Être responsable du traitement résulte essentiellement du fait qu'une entité a choisi de traiter des données à caractère personnel pour des finalités qui lui sont propres.[73] Le sous-traitant est celui qui « traite des données à caractère personnel pour le compte du responsable du traitement ».[74] L'aspect le plus important est l'exigence que le sous-traitant agisse pour le compte du responsable du traitement. « Agir pour le compte de » signifie servir les intérêts d'un tiers.[75] Une très grande variété de prestataires de services, qui peuvent être des entreprises, des organismes publics, ou des associations, peuvent être qualifiés de sous-traitants au sens du RGPD.[76]

Lorsqu'un responsable du traitement en Suisse recourt à un sous-traitant sur le territoire l'EEE, il n'est pas soumis par ricochet au RGPD.[77] L'interprétation littérale et systématique du RGPD le confirme. En effet, l'art. 3 (2) RGPD ne mentionne que deux exceptions au principe d'établissement dans l'UE, à savoir l'offre de biens ou de services dans l'EEE ou le suivi du comportement. Le recours à un sous-traitant n'est pas prévu et il n'est pas possible d'étendre le champ d'application extraterritorial à d'autres cas de figures que ceux mentionnés expressément à l'art. 3 (2) RGPD. En revanche, le sous-traitant sera soumis au RGPD.

---

71 *David Vasella*, EDÖB zur DSVO und ihren Auswirkungen auf die Schweiz, daten:recht, 23 décembre 2017, 9.

72 Art. 4 (7) RGPD ; Voir également *David Rosenthal*, Controller oder Processor : Die datenschutzrechtliche Gretchenfrage, Jusletter, 17 juin 2019; *European Data Protection Supervisor,* Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 7 novembre 2019 ; *Bayerisches Landesamt für Datenschutzaufsicht*, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO, 17 décembre 2018.

73 G29, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant » du 16 février 2010, 9.

74 Art. 4 (8) RGPD.

75 G29 (note 73), 27.

76 CNIL, Guide du sous-traitant de septembre 2017, 3. On peut citer par exemple les prestataires de services informatiques (hébergement, maintenance), les intégrateurs de logiciels, les sociétés de sécurité informatique, les entreprises de service du numérique qui ont accès aux données, ou encore tout organisme offrant un service ou une prestation impliquant un traitement de données à caractère personnel pour le compte d'un autre organisme.

77 PFPDT, Le RGPD et ses conséquences sur la Suisse, juillet 2018, 6 ; CEPD (note 24), 12.

VI. Le sous-traitant suisse d'un responsable du traitement soumis au RGPD

De manière générale, on peut distinguer quatre cas de sous-traitants établis hors de l'EEE.

Premièrement, le sous-traitant établi hors de l'EEE qui a l'intention d'offrir des biens ou des services à des résidents de l'EEE sera soumis directement au RGPD de manière extraterritoriale, comme le prévoit l'art. 3 (2) let. a RGPD. On peut néanmoins se demander si un sous-traitant qui décide seul de viser un marché ne devrait pas être qualifié de responsable du traitement.

Deuxièmement, le sous-traitant établi hors de l'EEE d'un responsable du traitement établi dans l'EEE n'est pas soumis au RGPD. Il doit néanmoins respecter des obligations contractuelles qui le lient au responsable du traitement et qui sont imposées à ce dernier par l'art. 28 RGPD. L'art. 28 RGPD ne prévoit pas l'application du RGPD directement au sous-traitant et il s'agit donc bien d'une application contractuelle de certaines obligations figurant dans le RGPD, mais pas d'une application en tant que telle du RGPD (dans son ensemble).[78]

Troisièmement, il y a le cas où le sous-traitant et le responsable du traitement sont tous les deux établis hors de l'EEE et aucun ne vise le marché de l'EEE ou ne fait du suivi de comportement. Le RGPD ne s'applique donc pas.

Quatrièmement, il y a le cas particulier où le sous-traitant et le responsable du traitement sont tous les deux établis hors de l'EEE, mais le responsable du traitement est soumis au RGPD de manière extraterritoriale, soit parce qu'il vise les résidents de l'EEE pour leur fournir des biens et des services, soit parce qu'il suit leur comportent dans l'EEE. C'est le cas par exemple d'un fournisseur d'hébergement suisse engagé par une entreprise américaine qui fournit des services en ligne de manière globale (y compris en visant l'EEE). Comme dans le cas deux (responsable du traitement établi dans l'EEE), le sous-traitant ne devrait pas être soumis au RGPD mais seulement à des obligations contractuelles. Le CEPD considère pourtant depuis la version définitive des lignes directrices publiées en novembre 2019 que le RGPD s'applique directement au sous-traitant hors de l'EEE.[79]

Cette interprétation très expansionniste est autant discutable que difficile à respecter en pratique, le sous-traitant ne décidant pas de cibler un marché, voire n'étant même pas au courant des intentions du responsable du traitement.[80] Elle n'est pas non plus justifiée puisque lorsque le RGPD s'applique déjà au responsable du traitement, le besoin de protection des personnes se trouvant dans l'EEE ne nécessiterait pas que le sous-traitant suisse soit également soumis au RGPD.[81]

---

78 Cela est d'ailleurs expressément admis par le CEPD : CEPD (note 24), 9-10.

79 CEPD (note 24), 20-22.

80 Un fournisseur d'hébergement ou de services d'envois de messages ne saura pas dans quel cadre le responsable du traitement traite les données.

81 *David Vasella*, Zum Anwendungsbereich der DSGVO, digma 2017, 220.

VII. L'administration publique

Le RGPD peut s'appliquer aux administrations communales, cantonales et fédérales, en particulier lorsqu'elles disposent d'un établissement dans l'EEE,[82] lorsqu'elles traitent des données personnelles en lien avec l'offre de biens ou de services à des résidents européens,[83] ou dans le cas d'un suivi du comportement en ligne,[84] ou encore si elles interviennent comme sous-traitants d'un responsable du traitement hors de l'EEE soumis au RGPD.

On rappellera encore que certaines activités typiques de l'administration publique sont exclues du champ d'application matériel, en particulier le traitement de données à des fins de prévention et de détection des infractions pénales.[85]

E. Particularités en cas d'application extraterritoriale

I. Pas toutes les données

Lorsque le RGPD s'applique de manière extraterritoriale, ce ne sont pas tous les traitements de données personnelles effectués par un responsable du traitement ou un sous-traitant qui y sont soumis. Seules les données personnelles liées à une offre de biens ou de services ou à un suivi de comportement devront être traitées en respectant le RGPD.[86]

II. Représentant dans l'EEE

Lorsque le RGPD s'applique de manière extraterritoriale, le RGPD impose au responsable du traitement ou au sous-traitant de désigner un représentant[87] dans un des États membres[88] dans lesquels se trouvent les personnes physiques dont les données personnelles font l'objet d'un traitement lié à l'offre de biens ou de services, ou dont le comportement fait l'objet d'un suivi.[89] Lorsque les personnes concernées se trouvent dans différents États membres, le CEPD recommande à titre de bonne pratique de désigner le représentant dans l'État membre où se trouve la majorité

82 Par exemple, un bureau de promotion économique ou touristique.
83 Par exemple, une école publique qui démarche activement des étudiants européens.
84 Par exemple, si un tel site est accessible dans l'EEE.
85 Ce traitement sera soumis à la loi fédérale du 28 septembre 2018 sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal (LPDS ; RS 235.3).
86 CEPD (note 24), 14.
87 Le représentant est défini à l'art. 4 (17) RGPD.
88 Non seulement de l'UE, mais de l'EEE également, pour autant qu'un lien suffisant existe avec ledit État.
89 Art. 27 (1) et (3) RGPD.

des personnes concernées.[90] Par exemple,[91] une entreprise pharmaceutique indienne, sans établissement au sein de l'EEE, qui sponsorise des essais cliniques dans des hôpitaux en Belgique, au Luxembourg et aux Pays-Bas. La majorité des patients participants aux essais cliniques se trouvant en Belgique, il est recommandé de nommer un représentant en Belgique.

Cette obligation ne s'applique pas aux autorités et organismes publics, ni aux responsables du traitement privés qui ne traitent qu'occasionnellement des données personnelles et pour autant qu'il ne s'agisse pas de données sensibles ou représentant un risque important.[92] La notion de traitement occasionnel reste vague et conduira à des interprétations diverses dans la pratique. *A contrario*, le caractère régulier du suivi des personnes concernées dans le cadre de l'art. 37 (1) let. b RGPD est développé par les lignes directrices concernant les délégués à la protection des données du Groupe de travail « Article 29 ».[93] Le terme « régulier » recouvre les significations suivantes : continu ou se produisant à intervalles réguliers au cours d'une période donnée ; récurrent ou se répétant à des moments fixes ; ayant lieu de manière constante ou périodique. La notion de traitement occasionnel peut donc se définir comme l'inverse de ce qui précède. Dans tous les cas, les exceptions doivent être interprétées de manière stricte.[94]

En principe, il n'y a pas non plus d'obligation de nommer un représentant lorsqu'il y a un établissement au sein de l'EEE. En effet, cet établissement et les activités qui y sont liées sont soumis au RGPD de manière territoriale et la désignation d'un représentant n'est donc pas requise. En revanche, si l'on prend l'exemple d'un groupe d'entreprises, il faudra se poser la question de quelle entreprise a le statut d'établissement principal. L'établissement principal est celui du lieu de l'administration centrale au sein de l'EEE (ou l'établissement principal du groupe d'entreprises le cas échéant). Différents facteurs peuvent être utilisés pour déterminer le lieu de l'établissement principal, notamment : où les décisions finales quant aux finalités et aux moyens du traitement sont-elles prises ; où les décisions relatives aux activités commerciales nécessitant un traitement de données sont-elles prises ; où le pouvoir de faire appliquer les décisions se concentre-t-il effectivement ; où le directeur assumant la responsabilité générale de la gestion du traitement transfrontalier est-il établi ; où le responsable du traitement ou le sous-traitant est-il inscrit au registre des sociétés, s'il est implanté dans un seul territoire ?[95] Si les décisions relatives aux finalités et aux moyens du traitement des données à caractère personnel sont prises dans un autre établissement que celui de l'administration centrale, alors cet autre établissement sera le principal.[96] Si l'établissement principal est en Suisse, quand bien même le groupe posséderait des établissements

90 CEPD (note 24), 26.
91 CEPD (note 24), exemple 25, 26-27.
92 Art. 27 (2) RGPD ; consid. 80 RGPD.
93 G29*,* Lignes directrices concernant les délégués à la protection des données, version révisée et adoptée le 5 avril 2017, 10.
94 *Mittelberger* (note 10), 29.
95 G29*,* Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant, révisées et adoptées le 5 avril 2017, 7-8.
96 Consid. 36 RGPD.

dans l'EEE, un représentant devrait y être désigné, dans la mesure où lesdits établissements n'effectueraient pas les mêmes activités. Il pourrait donc y avoir une obligation de nommer un représentant dans l'EEE pour certains traitements même en cas de présence d'un établissement.

La désignation du représentant doit se faire par un mandat écrit du responsable du traitement ou du sous-traitant pour agir en son nom en ce qui concerne les obligations qui lui incombent en vertu du RGPD.[97] Il n'est en revanche pas obligatoire d'annoncer son représentant aux autorités de contrôle,[98] mais son identité et ses coordonnées font partie des informations à fournir à la personne concernée.[99]

Les tâches du représentant, sont notamment de tenir un registre des activités de traitement[100] et de coopérer avec l'autorité de contrôle en lui communiquant sur demande toute information dont elle a besoin pour l'accomplissement de ses missions.[101] Enfin, le représentant pourrait faire l'objet de mesures coercitives en cas de non-respect du RGPD par le responsable du traitement ou le sous-traitant.[102] Il n'est pas très clair si cela inclut la possibilité de tenir le représentant responsable en cas d'imposition d'amendes. Toutefois, la désignation d'un représentant n'affecte pas la responsabilité du responsable du traitement ou du sous-traitant qui l'a désigné.[103]

III. Pas de *one stop shop*

Le RGPD a pour but (théorique ?) de simplifier les contacts entre le responsable du traitement et les autorités, et d'assurer un traitement uniforme par les autorités de contrôle. C'est ce que prévoit notamment le système de l'autorité de contrôle chef de file.[104]

L'autorité de contrôle chef de file est l'autorité qui assume la responsabilité principale de la gestion d'une activité de traitement transfrontalière,[105] par exemple lorsqu'une personne concernée introduit une réclamation concernant le traitement de ses données à caractère personnel. On parle parfois de mécanisme *one stop shop.* L'autorité de contrôle chef de file coordonnera toute enquête éventuelle, en y associant les autres autorités de contrôle concernées. La désignation de l'autorité de

97 Consid. 80 RGPD.
98 Contrairement à ce qui prévaut pour le délégué à la protection des données.
99 Art. 13 (1) let. a et 14 (1) let. a RGPD.
100 Art. 30 (1) RGPD.
101 Art. 58 (1) RGPD ; consid. 82 RGPD ; art. 30 (4) RGPD.
102 Consid. 80 *in fine* RGPD. La question de la responsabilité subsidiaire du représentant est débattue en doctrine, étant donné la formulation ambiguë de l'art. 27 (5) RGPD et le fait que ni les art. 57 et 58 RGPD traitant du pouvoir des autorités de contrôle, ni l'art. 83 RGPD traitant des amendes administratives ne mentionnent la question de sa responsabilité. *Jay* relève que cette insécurité juridique est problématique, étant donné que selon l'interprétation retenue, d'autres entités que les sous-traitants ou responsables du traitement pourraient être tenues à des obligations primaires (*Jay* (note 33), n°4-039).
103 Art. 27 (5) RGPD ; CEPD (note 24), 27.
104 Art. 56 RGPD.
105 Consid. 124 ; art. 56 RGPD.

contrôle chef de file dépend du lieu de l'établissement principal ou de l'établissement unique dans l'EEE du responsable du traitement.[106] Toutefois, chaque autorité de contrôle reste compétente pour traiter d'une violation du règlement qui concerne uniquement l'établissement dans l'État membre dont elle relève.[107]

Au sens du RGPD, un traitement transfrontalier est un traitement de données qui a lieu dans plusieurs États de l'EEE ou dans un État de l'EEE mais qui affecte sensiblement des personnes dans plusieurs États de l'EEE.[108] Un traitement dans le cadre d'une application extraterritoriale du RGPD n'est pas un traitement transfrontalier et ne bénéficie pas du mécanisme de l'autorité de contrôle chef de file.

Cela signifie qu'un responsable du traitement en Suisse, sans établissement au sein de l'EEE, doit s'adresser aux autorités de contrôle locales dans chaque État membre dans lequel il exerce des activités et ne bénéficie pas du concept de guichet unique.

À la suite de plaintes déposées à l'encontre de *Google*, la Commission nationale (française) de l'informatique et des libertés (CNIL) a rendu une décision le 21 janvier 2019.[109] Elle a notamment examiné sa compétence, en application du concept du guichet unique. L'autorité de contrôle chef de file doit dans tous les cas se coordonner avec les autres autorités nationales de contrôle. En l'espèce, les échanges avec les autres autorités, notamment l'autorité de protection des données irlandaise où se situe le siège européen de *Google*, n'ont pas permis de considérer que *Google* disposait d'un établissement principal dans l'EEE. En effet, à la date à laquelle la CNIL a entrepris ses poursuites, l'établissement irlandais ne disposait pas d'un pouvoir de décision sur les traitements mis en œuvre dans le cadre du système d'exploitation Android et des services fournis par *Google LLC* en lien avec la création d'un compte utilisateur lors de la configuration d'un téléphone mobile. Le système dit du guichet unique n'étant pas applicable, la CNIL, au même titre que toutes les autres autorités de contrôle de l'EEE, était dès lors compétente pour prendre des décisions concernant les traitements mis en œuvre par *Google LLC*. On peut néanmoins sérieusement se demander si cet arrêt ne viole pas le concept du guichet unique.

IV. Reconnaissance en Suisse

Comme nous l'avons exposé, le RGPD peut s'appliquer à des responsables du traitement suisses. Du point de vue européen, cette application est incontestable si les conditions posées par le RGPD sont remplies. En revanche, du point de vue suisse,[110] cela peut conduire à des situations compliquées puisque le RGPD n'est pas un texte de droit national ou de droit international applicable en Suisse.

106 G29 (note 95), 5.
107 Consid. 127 et 131 RGPD.
108 Art. 4 RGPD.
109 Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société *Google LLC*.
110 Et des autres pays hors EEE.

Il pourrait même être contraire à certaines dispositions, comme l'art. 271 du Code pénal suisse (CP ; RS 311) qui réprime les actes exécutés sans droit pour un État étranger.[111] Un responsable du traitement respectant notamment son obligation de notifier une faille de sécurité à l'autorité de contrôle compétente au sein de l'EEE serait donc potentiellement en infraction du Code pénal suisse. Le Département fédéral de justice et police (DFJP) s'est prononcé sur la question dans une note explicative.[112] En substance, une notification d'une faille de sécurité contenant les informations prévues dans le RGPD[113] ne constitue pas une atteinte à la souveraineté de la Suisse, car une notification n'est pas un acte relevant des pouvoirs publics au sens de l'art. 271 CP.

En outre, il est certain que le Préposé fédéral à la protection des données et à la transparence (PFPDT) ne peut pas être considéré comme une autorité de contrôle du RGPD et que le responsable du traitement doit remplir ses obligations vis-à-vis d'une autorité de contrôle d'un État de l'EEE.[114]

Une autorité de contrôle d'un État de l'EEE qui souhaite obtenir des informations, dans le cadre d'une procédure par exemple, devra recourir aux voies habituelles de l'entraide administrative.

Finalement, on peut encore se demander si les autorités suisses reconnaîtront une décision européenne prise en application du RGPD et comment les autorités de contrôle européennes procéderont à l'encaissement d'une amende imposée à une entreprise suisse, pour laquelle une procédure de poursuites n'est pas possible. La reconnaissance et l'exécution des décisions prises par les autorités européennes n'est pas permise en l'état en droit suisse, que ce soit sous l'angle de l'entraide administrative ou pénale internationale, ou encore conformément à la Convention de Lugano.[115]

Toutes ces questions liées à l'exécution du RGPD en Suisse dépassent largement le cadre de cette contribution et sont encore peu claires. Elles feront peut-être l'objet d'une étude ultérieure.

F. Conclusions

Le champ d'application large du RGPD offre, en théorie, une protection presque sans faille aux résidents de l'EEE et il garantit aux autorités de contrôle de pouvoir

111 *Philippe Vladimir Boss,* L'autorisation d'exécuter un acte pour un État étranger dans la pratique récente, La Revue de l'Avocat, 2017, 77.

112 DFJP, Note explicative relative à l'obligation de notifier une violation des données à caractère personnel en vertu de l'art. 33 du Règlement (UE) 2016/679 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 (RGPD), 4 septembre 2018.

113 Art. 33 RGPD.

114 Voir notamment la Motion 16.3752 (Doris Fiala) du 28 septembre 2016 « Contre les doublons en matière de protection des données » qui invite le Conseil fédéral à négocier un accord avec l'UE sur la compétence et la collaboration des autorités de contrôle.

115 (CL ; RS 0.275.12) ; *Yaniv Benhamou/Emilie Jacot-Guillarmod,* RGPD sur sol suisse : mise en œuvre, digma 2018, 142.

intervenir dans presque toutes les situations, en s'en prenant au besoin au représentant (pour autant qu'il ait été désigné). Cette application large, en particulier l'application extraterritoriale et l'application aux données traitées par des responsables du traitement sur le territoire de l'EEE mais concernant des personnes hors de ce territoire contribue aussi fortement à relever le niveau de protection des personnes dans le monde entier.

L'application extraterritoriale, dans le cas de l'offre de biens et services mais encore plus s'agissant du suivi du comportement, peut conduire à des situations où l'application du RGPD est excessive et parfois inenvisageable pour les responsables du traitement et les sous-traitants étrangers. La protection de la bonne foi de ces derniers devrait commander une application plus limitée. La version finale des lignes directrices sur l'application territoriale ne va malheureusement pas dans ce sens.