Feedbacks du GTSI sur la recommandation 01/2020 de l'EDPB

Présentation du GTSI

Le GTSI (Groupe de Travail sur la Sécurité de l'Information) regroupe plus de cinquante professionnels de la sécurité de l'information et de la protection des données œuvrant dans les autorités publiques de la Région Wallonne, de la Fédération Wallonie-Bruxelles et de la Communauté germanophone en Belgique. La vocation de ce groupe est de partager les connaissances, les pratiques et d'émettre des conseils en termes de protection des données et sécurité.

Executive Summary

Le GTSI tient sincèrement à saluer le travail important produit par l'EDPB. La recommandation apporte en effet quelques éclaircissements théoriques bienvenus, cependant, elle ne répond pas à de nombreuses problématiques très concrètes que rencontrent les institutions publiques et certainement de très nombreuses entreprises privées. Ces problématiques relèvent essentiellement du recours à des fournisseurs de services ou produits entraînant un transfert des données vers un pays tiers ou vers une organisation internationale.

Suggestions de solutions pragmatiques.

Comme explicité plus en détail par la suite, les responsables de traitements se trouvent parfois dans des situations impraticables. Le contexte actuel et le manque d'outils pragmatiques rendent la charge de la sélection des fournisseurs pouvant satisfaire les exigences du RGPD après l'arrêt Schrems II disproportionnée, surtout pour les responsables de traitements de petite taille.

Il nous semble dès lors indispensable que des solutions pragmatiques prenant en compte la réalité des entreprises tant publiques que privées soient trouvées. En effet, en l'absence de celles-ci, c'est la crédibilité même du RGPD qui pourrait être mise en question, et donc également celle des professionnels de la protection des données. Le risque est aussi très grand que le niveau de protection des personnes concernées (notamment contre la surveillance de masse) ne soit pas assuré dans les faits. Sans compter les effets dévastateurs en termes d'image de réputation et de confiance pour les entreprises et institutions.

Pour se faire, le GTSI suggère :

1) Que l'UE mette en œuvre un système permettant aux responsables de traitement d'identifier rapidement les fournisseurs de services qui répondent aux exigences du RGPD, les dispensant ainsi de devoir procéder eux-mêmes à cette vérification :

   - Soit par la délivrance d'une certification européenne à ces fournisseurs de service (à l'instar ce qui est fait pour les services qualifiés du règlement eIDAS n°910/2014 du 23 juillet 2014 par exemple) apportant la garantie que ces fournisseurs et services offrent un niveau de protection adéquat.
   - Soit par la publication d'une liste de prestataires et des différents services qu'ils offrent, avec une identification claire de chaque service et de ses spécificités, pour lesquels le responsable de traitement peut considérer qu'ils répondent aux exigences du RGPD pour autant que le contrat qui les lie fasse explicitement référence à cette liste et au(x) service(s) concerné(s).

Cela permettrait :

   a. De mettre tous les responsables de traitements, même les plus petites structures (qui sont totalement incapables en termes de ressources et compétences de réaliser une analyse aussi complexe que celle qui est exigée) de choisir un fournisseur offrant toutes les garanties ;

   b. De permettre aux responsables de traitement d'exercer pleinement leur responsabilité même lorsqu'ils sont face à des fournisseurs en position de force ;

   c. De réaliser à l'échelle de l'Europe des économies d'échelle substantielles en évitant que des dizaines de milliers de responsables de traitements opèrent la même analyse ;

   d. De faciliter le travail des fournisseurs de service en ne leur imposant la communication qu'à une seule instance, en leur évitant la demande d'exercice du droit d'audit par tous leurs clients, en leur évitant de devoir négocier les conditions « RGPD » avec tous leurs clients (conditions qui ne seraient de toute façon pas opposables aux autorités du pays tiers).

   e. De relever le niveau de compétitivité des fournisseurs européen et ainsi contribuer à une avancée vers la souveraineté numérique de l'Europe, cette dernière étant probablement la meilleure solution systémique à la problématique des transferts hors UE.

2) D'envisager des amendements au RGPD ou d'introduire de nouvelles dispositions dans le règlement ePrivacy afin de limiter la responsabilité des responsables de traitements aux seuls éléments dont ils ont la maîtrise.

Par exemple, lorsqu'il met à disposition un site web sur l'Internet, le responsable de traitement détermine la finalité de ce site web, mais il ne maîtrise aucun composant qui se trouve sur le chemin qui sépare le terminal (PC, smartphone…) de la personne concernée et la connexion internet du responsable de traitement. L'adresse IP du terminal de la personne concernée est divulguée tout au long de ce parcours indéterminé (et donc passant potentiellement via des pays tiers) sans que le responsable de traitement en ait le moindre contrôle.

3) Que l'UE investisse dans le processus permettant de prendre des décisions d'adéquations visées par l'art. 45 du règlement.

Demande de clarifications

Sur le contenu de la recommandation 01/2020, le GTSI souhaite formuler les remarques suivantes :

1) Responsabilité de l'analyse

La recommandation semble faire reposer la responsabilité de l'analyse de l'adéquation de la protection sur l'exportateur des données, qu'il soit responsable de traitements ou non.

Le principe d' « accountability » du responsable de traitement inscrit dans le RGPD n'établit-il pas la responsabilité dans le chef du responsable de traitement ?

Cependant, pour les multiples raisons explicitées plus en détail dans la suite du document, il semblerait plus « juste » de faire reposer la responsabilité sur l'acteur qui est à la cause du transfert vers un pays tiers, qu'il soit exportateur ou importateur, responsable de traitements ou sous-traitant.

2) La dimension contractuelle

La recommandation 01/2020 rappelle qu'en raison de leur nature contractuelle, les clauses de protection ne peuvent lier les autorités publiques des pays tiers, puisqu'elles ne sont pas parties au contrat.

Malgré ce constat, les propositions qui y sont formulées en vue d'adopter des mesures complémentaires ou supplémentaires visent à nouveau, en majeure partie, le recours à des mesures contractuelles, en dépit de leur faiblesse bien connue et le fait qu'elles soient insuffisantes, voire inopérantes. En effet, tant les clauses contractuelles types actuelles de la

Commission européenne que les clauses *ad hoc* ne sont pas opposables *erga omnes*.

L'effort déployé par les différents responsables de traitement en vue de se mettre en conformité au RGPD, après ce processus long et laborieux articulé en 6 étapes, serait vain si le transfert ne repose que sur ces mesures contractuelles. De plus, dans le cas de fournisseurs de services qui sont en position de monopole, il est très peu probable qu'ils acceptent la négociation, que ce soit pour des raisons de pouvoir, ou des raisons simplement pratiques (par ex, pour un géant comme Microsoft ayant des dizaines de milliers de clients, il est inenvisageable de permettre à chacun d'eux d'auditer son système d'information).

3) Territorialité du transfert *vs* nationalité de l'importateur

La recommandation 01/2020 dans son paragraphe 76 cite l'exemple suivant :

« As an example, US data importers that fall under 50 USC § 1881a (FISA 702) are under a direct obligation to grant access to or turn over imported personal data that are in their possession, custody or control. This may extend to any cryptographic keys necessary to render the data intelligible. »

Le GTSI suggère que la recommandation clarifier la position à adopter en ce qui concerne le transfert vers un importateur, qui par sa nationalité, est soumis à un autre régime juridique. Par exemple, préciser quel régime s'applique lorsqu'un responsable de traitements recourt à un fournisseur de nationalité US, mais que les données sont traitées sur le territoire de l'UE ?

Commentaires et suggestions du GTSI

Utilisation de l'internet – Use case 3

Le « use case 3 » de la recommandation prend l'exemple d'un traitement de données transitant par l'Internet. Par la conception même de l'Internet, le chemin que parcourt un paquet de données est indéterminé : l'utilisation du réseau Internet entraîne de facto un risque de transit par un pays qui n'offre pas un niveau de protection en adéquation avec l'Art 45 du RGPD.

Or, même si toutes les conditions citées dans ce « use case » sont rencontrées, les données de connexion, dont l'adresse IP et les informations temporelles ne sont pas chiffrées et sont directement disponibles sur toutes les infrastructures par où les paquets de données transitent.

Ainsi donc, le simple fait de mettre à disposition un site web sur l'Internet, même si celui-ci utilise le protocole HTTPS, impose à l'utilisateur du site de révéler son adresse IP à des dizaines,

voire centaines d'opérateurs impliqués dans le « routage » de l'information sur l'Internet. Le responsable de traitements ne peut pas mettre en œuvre des moyens empêchant cela, seul l'utilisateur peut décider d'utiliser des outils permettant la dissimulation de son adresse IP (utilisation de TOR et/ou de VPN).

Il en est de même lorsque le responsable de traitements permet à l'utilisateur de le contacter par email, lui offre de visionner une vidéo en ligne, etc.

Pour une surveillance de masse, les données de connexions peuvent être plus révélatrices que le contenu de la communication elles-mêmes.

Il en découle que les traitements de données utilisant l'internet sont incompatibles avec le RGPD, puisque le responsable de traitements est incapable de maîtriser le secret de toutes les données personnelles de bout en bout. Dès lors, étant donné qu'il serait totalement irréaliste dans le monde actuel d'interdire le recours à des sites internet ou l'échange d'emails, les responsables de traitement se trouvent face à une règle impraticable. Ce faisant, c'est la crédibilité même du RGPD qui se voit mise en doute. Sans compter les effets dévastateurs en termes d'image de réputation et de confiance pour les entreprises et institutions.

Nous pensons donc qu'il est indispensable d'amender le RGPD ou d'introduire de nouvelles dispositions dans le futur règlement ePrivacy afin de réduire le champ et le degré de responsabilité du responsable de traitements.

Responsabilité de l'exportateur ?

Le texte laisse penser que la charge de la vérification d'un niveau de protection essentiellement équivalent repose sur les épaules de l'exportateur des données uniquement, l'importateur n'ayant qu'un devoir de collaboration.

Il nous semble que la responsabilité devrait reposer sur celui qui décide ou impose de recourir à un transfert de données vers un pays tiers, peu importe qu'il soit exportateur ou importateur.

En outre, l'exportateur des données est parfois dans une position intenable (suite à la situation de monopole de fait de certains fournisseurs de services)

Complexité de l'analyse du niveau de protection équivalent

La présente recommandation qui vise à aider dans «the complex task of assessing third countries and identifying appropriate supplementary measures where needed » témoigne de l'extrême complexité que revêt une analyse destinée à déterminer si le transfert de données vers un pays tiers offre une protection de « niveau équivalent » à celui de l'UE.

Si nous nous réjouissons de cette initiative, nous ne pouvons pas nous empêcher de penser que la majorité des responsables de traitements sont, en pratique, dans l'incapacité de réaliser une telle analyse. Il faut en effet une armée de juristes spécialisés dans les droits internationaux et dans le domaine très spécifique de la surveillance, ainsi que des spécialistes techniques dont

très peu d'organisations disposent (et cela est d'autant plus vrai en Région wallonne (Belgique) où le tissu économique est essentiellement constitué de petites entreprises). Étant donné que chaque pays tiers est susceptible de modifier sa législation sans préavis, le responsable de traitement devrait non seulement mettre en place un monitoring permanent de la législation applicable notamment à ses sous-traitants, mais aussi, disposer d'une procédure de rapatriement des données qui devrait être activée avant que la nouvelle législation n'entre en vigueur. Aussi performante qu'elle soit, cette procédure de rapatriement des données ne pourra jamais être mise en œuvre avant l'entrée en vigueur de dispositions légales nouvelles avec effet immédiat.

Dans la majorité des cas donc, il nous semble totalement irréaliste de faire reposer cette tâche sur les responsables de traitement. De plus, nous pensons que cette complexité, qui laisse une grande part de flou, ne bénéficiera pas aux personnes concernées, car malheureusement ce sont les interprétations les moins restrictives qui seront généralement les plus adoptées par les responsables de traitement. Ces derniers, en effet, souhaiteront limiter un maximum les coûts de la conformité.

Nous pensons donc que la tâche d'analyse doit être rendue plus simple par l'introduction des normes :

- d'adéquation des cadres juridiques;
- des standards techniques permettant de compléter les clauses contractuelles types.

Nous pensons que c'est la seule solution réellement pragmatique qui permet à la fois d'apporter des garanties aux personnes concernées (car les normes définissent un niveau concret plus facilement appréhendable) et d'alléger le travail des responsables de traitements. Cela représente également, à l'échelle de l'UE, une économie d'échelle substantielle puisque les coûts de ces analyses en deviennent largement réduits pour tous les responsables de traitements.

Nous suggérons également qu'un organe européen répertorie et publie ces normes et leur compatibilité avec chaque pays tiers.

Par ailleurs, pour que le respect du RGPD et la conformité aux normes techniques puissent être transparents vis-à-vis des utilisateurs d'un service, et pour qu'il y ait une saine concurrence dans le secteur des prestataires de services, il nous paraît nécessaire que les services des prestataires soient certifiés, idéalement sous accréditation, par rapport aux normes pour lesquelles une conformité est annoncée. De cette façon, le recours à un prestataire certifié offrira un niveau de garantie raisonnable et suffisant au responsable de traitements. De même, cette certification évitera aux prestataires de devoir démontrer, sans arrêt et à grands frais, leur conformité à leurs clients, mais aussi à leurs prospects.

Position dominante de certains fournisseurs

La réalité de la position dominante de certains fournisseurs est une problématique qu'il est indispensable de prendre en compte si le souhait est de vraiment arriver à une meilleure protection et non à une protection de façade.

Impossibilité de changer rapidement de solutions, ou inexistence de solutions alternatives crédibles.

La première problématique est que les acteurs dominants du marché technologique, souvent de nationalité US, mènent des politiques commerciales créant une dépendance des clients (le phénomène est connu sous le terme anglais de *lock-in*). Il est des situations dans lesquelles le responsable de traitement est inextricablement engagé dans des solutions technologiques et dont il lui est impossible de sortir dans des délais courts. Nous citons par exemple le système d'exploitation Microsoft Windows. La politique de Microsoft est de transformer ces produits (vendus sous forme de licences perpétuelles) en services (vendus sous forme d'abonnement). Ainsi donc, Windows s'est au fil du temps transformé afin de dépendre de plus en plus de service en ligne. Par exemple, l'assistant Cortana fait appel à l'IA de Microsoft et donc nécessite de transmettre des données à Microsoft, dont au moins l'adresse IP et un identifiant permettant de vérifier l'état de la licence. Autre exemple, Windows doit être mis à jour régulièrement pour ajouter des fonctionnalités (et donc créer la dépendance), mais aussi pour corriger des failles de sécurité. Il est donc possible que ce qui était conforme avant la mise à jour ne le soit plus après celle-ci. Vu la fréquence des mises à jour et le nombre de services à surveiller, même en y attribuant des moyens d'analyse importants, le responsable de traitement ne pourra réagir qu'*a posteriori*. Il est même possible que le travail d'analyse ne puisse être effectivement réalisé avant que la mise à jour suivante ne soit introduite. Citons encore l'antivirus intégré qui est susceptible d'envoyer des fichiers suspects à Microsoft pour analyse. Windows envoie donc des données personnelles à Microsoft, et ce n'est pas initialement le choix de son utilisateur, c'est une stratégie commerciale de Microsoft qui profite de sa position de monopole pour imposer ce mode de fonctionnement. Windows est utilisé par la toute grande majorité des entreprises européennes, il en est de même de Microsoft Office qui est devenu un standard *de facto* pour la production de documents bureautiques.

Pour respecter l'arrêt Schrems II, les responsables de traitements devraient arrêter d'utiliser MS Windows et MS Office. Basculer sur un système d'exploitation Linux et la suite LibreOffice par exemple demanderait des efforts énormes et engendrerait de nombreux problèmes d'interopérabilité dans les échanges de fichiers bureautiques. Pour de nombreux responsables de traitement, le changement pourrait nécessiter plus de 5 ans. La réalité est que l'Europe est très loin d'avoir une souveraineté numérique et que les responsables de traitements sont pris en otage si c'est sur eux que l'on fait reposer la responsabilité des transferts.

Domination du marché technologique par les USA et la Chine

Le paragraphe 76 de la recommandation cite l'exemple suivant :

> *« As an example, US data importers that fall under 50 USC § 1881a (FISA 702) are under a direct obligation to grant access to or turn over imported personal data that are in their possession, custody or control. This may extend to any cryptographic keys necessary to render the data intelligible. »*

Il rappelle ainsi que faire appel à un sous-traitant de nationalité US peut se révéler problématique. Cela soulève la deuxième problématique : le monde technologique est aujourd'hui dominé par les USA (les GAFAM), la toute grande majorité des solutions de pointes proviennent d'entreprises US… concurrencées par les BATX chinois. En l'absence d'une offre européenne compétitive, les entreprises tant privées que publiques qui souhaitent répondre à la demande du monde actuel n'ont dans les faits pas d'autres choix de se tourner vers ces fournisseurs, car ne pas y recourir signifierait, pour la plupart d'entre elles, mourir. Et entre choisir de ne pas respecter le RGPD ou de mourir, leur choix sera vite fait…

Difficultés d'analyse

La troisième problématique est qu'en l'absence de transparence sur le respect des standards, il est extrêmement difficile d'identifier les services permettant d'offrir un niveau de conformité adéquat.

En effet, si l'on peut comprendre qu'un responsable de traitements ne peut se dédouaner du choix qu'il opère en utilisant un fournisseur de service, il n'en reste pas moins que de nombreux responsables de traitement sont réellement, dans l'état actuel du monde, dans l'incapacité d'opérer un choix en toute connaissance de cause, que ce soit en termes de ressources ou de compétences nécessaires (voir section précédente).

Dans de nombreux cas, les coûts et le temps d'une analyse approfondie seraient totalement disproportionnés par rapport aux projets envisagés : par exemple, si un responsable de traitement souhaite réaliser ponctuellement une campagne d'information massive en recourant à des ressources dont il ne dispose pas en interne, le responsable de traitement devra procéder à une analyse détaillée pour chaque candidat potentiel. Il serait naïf de penser que les entreprises n'utiliseront pas ces services même si elles ne sont pas capables de procéder à l'analyse, car les impératifs économiques auront vite fait de faire pencher la balance risques de sanction et bénéfices en faveur de ces derniers.

Dès lors, pour les trois raisons citées ci-dessus, nous en appelons à du pragmatisme et pensons que la seule solution réaliste, lorsque le transfert de données vers un pays tiers est le fruit d'une condition imposée par un fournisseur à son client pour la fourniture de ses services, est de faire reposer la responsabilité du transfert sur ce seul fournisseur.

En outre, nous pensons qu'à l'instar du RGPD qui exige une information claire et adaptée envers les personnes concernées, l'information de ces fournisseurs envers leurs clients, même

professionnels devraient être tout aussi simple et claire. C'est la raison pour laquelle nous suggérons d'imposer aux fournisseurs de communiquer une information répondant à un standard ou une norme, par exemple, en les obligeant de procéder à une déclaration à un organe centralisateur européen. Ces fournisseurs devraient déclarer :

1. le(s) pays où les données sont susceptibles d'être *traitées* : (et non le lieu de stockages des « données au repos », comme c'est trop souvent le cas, induisant ainsi volontairement une confusion auprès des clients) ;
2. les garanties fournies : cadres juridiques et mesures de protection permettant d'assurer un niveau de protection équivalent à celui de l'UE.
3. Le cas échéant, les restrictions concernant le type de données ou de traitement de données autorisées à être traitées au vu des protections mises en œuvre (par exemple, les protections mises en œuvre ne peuvent protéger les traitements de données visées par l'article 9 du RGPD, ou encore les traitements de données concernant des personnes fragilisées).

Concernant les 2e et 3e points, nous pensons que des normes[1] définissant les mesures de protection devraient être imposées (voir section précédente). Afin d'assurer une crédibilité, la mise en œuvre de ces mesures devrait être l'objet d'une certification.

A noter que cette solution permet également une économie d'échelle substantielle, puisque les clients sont bien plus nombreux que les fournisseurs.

La dimension contractuelle

La recommandation 01/2020 rappelle qu'en raison de leur nature contractuelle, les clauses de protection ne peuvent lier les autorités publiques des pays tiers, puisqu'elles ne sont pas parties au contrat.

Malgré ce constat, les propositions qui y sont formulées en vue d'adopter des mesures complémentaires ou supplémentaires visent à nouveau, en majeure partie, le recours à des mesures contractuelles, en dépit de leur faiblesse bien connue et le fait qu'elles soient insuffisantes, voire inopérantes. En effet, tant les clauses contractuelles types actuelles de la Commission européenne que les clauses *ad hoc* ne sont pas opposables *erga omnes*.

L'effort déployé par les différents responsables de traitements en vue de se mettre en conformité au RGPD, après ce processus long et laborieux articulé en 6 étapes (dont les clauses à négocier avec les opérateurs en position dominante pour peu que ces derniers acceptent), serait vain si le transfert ne repose que sur ces mesures contractuelles.

Pour preuve, prenons l'exemple d'un transfert UE-US pour lequel le responsable de traitement décide de s'appuyer uniquement sur les clauses contractuelles types pour le transfert de données avec l'opérateur, peu importe la qualification des responsabilités des parties

[1] La norme ISO 27701 pourrait constituer une base.

(responsable de traitement ou sous-traitant, sans compter le cas de la responsabilité conjointe non abordé par les clauses contractuelles types en vigueur), le responsable de traitement doit analyser et évaluer si le pays tiers (US) présente un niveau de protection des données équivalent à celui offert par le RGPD.

Or, le responsable s'expose à une non-conformité ; à titre d'exemple, l'article 4 alinéa1.a) de la décision de la Commission européenne n° 2010/87/A précise que l'autorité nationale de protection des données peut suspendre ou interdire le flux lorsqu' *« il est établi que le droit auquel l'importateur de données ou un sous-traitant ultérieur est soumis oblige ce dernier à déroger au droit applicable à la protection des données au-delà des limitations nécessaires dans une société démocratique pour l'une des raisons énoncées à l'article 13 de la directive 95/46/CE lorsque cette obligation risque d'avoir des conséquences négatives importantes pour les garanties offertes par le droit applicable à la protection des données et les clauses contractuelles types ».*

Ainsi, pour les nombreux transferts US, il ressort, de l'analyse concrète des dispositions internes US (ex : FISA, Cloud Act,...), que les autorités publiques américaines imposent une obligation de communication/divulgation de données (ex : surveillance de masse) allant au-delà des limites nécessaires dans une société démocratique et, donc, contraire au RGPD.

D'ailleurs, la Cour de Justice, dans son arrêt du 16 juillet 2020, a justement soulevé que le droit applicable était disproportionné et que les obligations qui en découlent risquent d'avoir des conséquences négatives sur les garanties offertes pour atteindre un niveau équivalent de protection de données.

Il en résulte que le mécanisme de décision d'adéquation prévu par l'article 45 du RGPD est la meilleure solution pour le responsable de traitements, car elle lui offre des garanties pour la conformité de ses transferts vers un pays tiers ou une organisation internationale. Le GTSI espère que les négociations notamment en cours pour le cas US iront en ce sens dans un avenir proche, afin d'éviter de continuer à travailler dans ce vide juridique.