FONDATION ROBERT SCHUMAN

POLICY PAPER

Question d'Europe
n°511
15 avril 2019

"La protection des citoyens européens dans un monde ultra-connecté"

Silvio MASCAGNA
et
Seyda EMEK

Le 3 avril, la Fondation Robert Schuman organisait à Luxembourg avec l'Institut Max Planck une conférence sur le thème : "La protection des citoyens européens dans un monde ultra-connecté". Y assistaient d'éminentes personnalités représentant les institutions européennes et notamment l'avocat général, Henrik Saugmandsgaard Øe, représentant le Président de la Cour de Justice de l'Union européenne. Après la communication de François Molins, Procureur général près la Cour de Cassation de la République française, le 8 avril, nous publions les interventions de deux autres participants. Silvio Mascagna, membre du cabinet de Julian King, Commissaire européen en charge de l'Union pour la sécurité, explique comment la Commission développe l'interoperabilité des bases de données pour lutter contre le terrorisme. Seyda Emek, conseillère du coordonnateur européen pour la lutte contre le terrorisme, Gilles de Kerchove, démontre la nécessité de conserver les données pour faciliter les enquêtes.

1- SILVIO MASCAGNA - MEMBRE DU CABINET DE JULIAN KING, COMMISSAIRE EUROPÉEN EN CHARGE DE L'UNION POUR LA SÉCURITÉ

Dès que l'on interroge les citoyens européens sur leurs sujets de préoccupation les plus importantes, comme le montrent des sondages récents réalisés en vue des élections européennes, la sécurité et la lutte contre le terrorisme restent des sujets prioritaires.

Malgré le défi de Daesh en Irak et en Syrie, la menace terroriste reste élevée en Europe, nous l'avons malheureusement encore constaté en France avec l'attaque du marché de Noël de Strasbourg. Selon le Centre d'Analyse du Terrorisme (CAT) français, 26 incidents terroristes ont visé l'Union européenne en 2018 dont 4 attentats, 1 tentative et 21 projets d'attentats. La menace a toutefois changé de nature, les dernières attaques étant accompli pas des individus agissant seuls, visant les espaces publics, et souvent radicalisés en ligne, ou dans des communautés.

LES TRAVAUX MENÉS POUR RENFORCER L'UNION DE LA SÉCURITÉ

Depuis plus de deux ans maintenant, le Commissaire européen en charge de l'Union de la sécurité, a piloté les travaux menés au niveau européen pour mieux garantir la sécurité de nos concitoyens.
Nous avons adopté une double approche :

- D'une part, en essayent de priver les terroristes des moyens de nuire en limitant leurs accès aux armes à feu, au financement ainsi qu'en limitant leur capacité opérationnelle, cela en renforçant la protection des frontières extérieures.

- D'autre part, nous développons notre résilience, pour éviter et prévenir les attentats ou mieux réagir lorsqu'ils ont lieu. Il s'agit notamment de lutter contre la radicalisation dans les communautés et sur internet, notamment pour retirer les contenus à caractère terroriste en ligne.

Mais garantir et renforcer la sécurité doit nécessairement aller de pair avec le respect des droits fondamentaux.

Dans une Union européenne fondée sur le respect de la dignité humaine, la démocratie, l'état de droit et les droits de l'Homme, la protection et la promotion de la sécurité des citoyens et le respect des droits fondamentaux sont complémentaires et doivent se renforcer mutuellement.

Je reviendrai sur cette question qui est au cœur de notre débat mais permettez-moi de donner

un aperçu rapide des actions menées au niveau européen sous le mandat du Commissaire.

Nous avons renforcé les contrôles aux frontières extérieures : depuis avril 2017 des contrôles systématiques sont effectués sur toutes les personnes entrant et sortant de l'espace Schengen, y compris les ressortissants européens.

Nous avons adopté la directive PNR, et désormais 20 Etats membres ont notifié une transposition complète de la directive.
Nous avons également renforcé les échanges d'informations au plan européen. J'aimerais souligner ainsi le renforcement de l'alimentation et de l'utilisation du Système d'informations Schengen (SIS) depuis 2015. En décembre 2017, il contenait 76.5 millions d'alertes et les Etats membres l'ont consulté plus de 5.2 milliards de fois.

Nous avons organisé la mise en place de deux nouvelles bases de données : entrée-sortie qui permet d'enregistrer les entrées et les sorties des résidents d'Etats tiers. C'est l'ETIAS, l'équivalent de l'ESTA américain. Ces bases feront également partie du nouveau système interopérable.

Nous avons proposé une législation (e-evidence) permettant un accès facilité aux preuves électroniques, souvent situés dans un autre Etat, ou sur le cloud. Cette proposition permettra d'obtenir de manière directe (directement de l'autorité judiciaire à la plateforme internet) l'accès aux preuves électroniques en 10 jours, au lieu de 10 mois en passant par l'entraide judiciaire. Le Conseil a trouvé un accord sur le texte, mais nous ne pourrons malheureusement pas le finaliser avant les élections faute d'accord du Parlement européen. Cet instrument sera très utile alors que nous savons que nombres d'enquêtes ne peuvent pas aboutir faute d'avoir obtenu les preuves électroniques à temps ; c'est notamment plus pertinent encore en matière de terrorisme.

J'ai mentionné l'internet. Ces contenus ont joué un rôle dans chaque attentat perpétré sur le sol européen ces deux dernières années, que ce soit pour inciter à commettre une attaque, pour donner des instructions sur le mode opératoire ou pour en glorifier les effets meurtriers.

Le règlement relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne, que la Commission a adopté en septembre 2018, obligera notamment les plateformes à réagir dans un délai d'une heure lorsque les autorités policières ou judiciaires leur adressent une injonction de suppression.

Nous concentrons maintenant tous les efforts pour obtenir un accord entre le Conseil et le Parlement européen avant les élections européennes. Mais comment garantir que la promotion de la sécurité des citoyens et le respect des droits fondamentaux soient complémentaires l'un à l'autre ?
La Commission a progressivement développé au cours des dix dernières années des mécanismes visant à renforcer l'évaluation systématique de leur impact sur les droits fondamentaux. Le respect des droits fondamentaux a également été évalué ex post dans le cadre général de l'évaluation des politiques de l'Union européenne afin de veiller à justifier leur nécessité et leur proportionnalité aux buts recherchés.

La Cour de justice (CJUE) examine non seulement la compatibilité de la législation de l'Union avec les droits fondamentaux et avec des mesures prises au niveau national par les États membres pour se conformer à la législation européenne ou aux accords internationaux comme le CETA.

Cela inclut par exemple l'invalidation de la directive sur la conservation des données (directive 2006/24/CE). C'est par exemple la décision selon laquelle la législation du Royaume-Uni et de la Suède imposant des exigences « générales et aveugles » aux opérateurs de télécommunication de conserver les données de trafic et de localisation des utilisateurs est incompatible avec la directive sur les communications électroniques (directive 2002/58/CE) par rapport à la Charte des droit fondamentaux (Principe de respect de la vie privée et familiale et protection des données à caractère personnel).

Dans le même temps, la Commission veille à ce que les États membres respectent la Charte dans la mise en œuvre de la législation européenne pertinente.

Pour des initiatives spécifiques, des organismes spécialisés tels que le contrôleur européen de la protection des données (CEPD) sont impliqués. L'expertise spécifique de l'Agence des droits fondamentaux de l'Union, établie en 2007, est également de plus en plus invoquée par les institutions de l'Union européenne afin de mieux répondre aux défis des droits fondamentaux, notamment par des consultations ciblées ou des demandes d'avis sur des sujets ou des propositions spécifiques.

Les garanties relatives aux droits fondamentaux sont souvent une priorité importante dans le processus législatif impliquant le Parlement européen et le Conseil. Les négociations entre les colégislateurs ont conduit à diverses reprises à renforcer davantage les garanties en matière de droits fondamentaux.

L'INTEROPÉRABILITÉ DES BASES DE DONNÉES

A cet égard, je voudrais mentionner l'initiative législative sur l'interopérabilité des bases de données, sécuritaires et migratoires. Cela concerne le traitement des données à caractère personnel dans les systèmes informatiques à grande échelle.

Nous avons renforcé l'interopérabilité, c'est-à-dire la façon de communiquer entre nos différentes bases de données, sécuritaires et migratoires, afin que nos services de police disposent de toutes les informations en temps utile. Cela permettra également de mieux lutter contre les fausses identités et les identités multiples, car plusieurs des auteurs d'attaques (Marseille, Berlin) étaient enregistrés sous différentes identités dans plusieurs bases européennes. Il permettra ainsi, à travers un moteur de recherche, de consulter toutes les bases sécuritaires et migratoires de manière simultanée, sans toutefois modifier les droits d'accès à ces bases (principe du hit/no hit). Nous espérons que ce système soit opérationnel d'ici 2023 au plus tard. Dans cette proposition, nous avons pris soin de bien maintenir les limites de l'objectif et de protéger les droits fondamentaux.

L'élaboration de nos propositions d'interopérabilité a été un processus inclusif et transparent, en collaboration avec la commission LIBE au Parlement européen et les États membres au sein du Conseil, et impliquant le contrôleur européen de la protection des données et l 'Agence des droits fondamentaux dès le début de notre travail. Notre approche a été d'assurer que la protection des données soit intégrée dans les composants de l'interopérabilité dès sa conception.

Les propositions que nous avons présentées en décembre 2017 sont, selon nous, pleinement conformes à la Charte des droits fondamentaux, au règlement général sur la protection des données (RGPD) et à toutes les législations européennes pertinentes. Toute incidence sur la protection des données serait proportionnée, poursuivant un objectif légitime et équilibré par rapport à d'autres droits.
Nous pensons que les résultats de ce travail de préparation inclusive – y compris les apports du contrôleur européen de la protection des données et de l'Agence des droits fondamentaux – sont clairement reflétés dans le résultat. Leurs avis ont aidé les colégislateurs à clarifier encore davantage les protections et les garanties, par exemple autour du droit à l'information.

L'interopérabilité ne consiste pas à collecter de nouvelles données, ni à fusionner les systèmes individuels. Il s'agit d'utiliser les informations existantes détenues dans nos systèmes de manière plus ciblée et plus efficace, en tenant compte des droits des personnes concernées. À cette fin, les nouvelles fonctionnalités s'appuieront sur les systèmes d'information existants de l'Union européenne, qui garderont leurs règles spécifiques sur la limitation des finalités, l'accès et la rétention des données.
Le traitement des données sera limité à ce qui

est strictement nécessaire et proportionné, conformément aux limitations de finalité existantes. Aucun nouveau type d'information ne sera collecté aux fins de l'interopérabilité.
Au contraire, des garanties pertinentes seront intégrées à chaque composante et attachées à chacun des objectifs d'interopérabilité.

En outre, l'interopérabilité ne concerne pas le profilage. Les propositions d'interopérabilité ne prévoient pas l'utilisation d'outils de profilage. Nous sommes tous d'accord sur l'objectif de la lutte contre la discrimination fondée sur le sexe, la race ou l'origine ethnique, la religion, le handicap, l'âge ou l'orientation sexuelle. Il y a un article dans nos propositions établissant les garanties pertinentes. Les propositions garantissent également que les enfants bénéficient de toute la protection nécessaire au traitement de leurs données à caractère personnel.

Il s'agit sans doute d'un modelé à suivre sur la façon de faire des politiques équilibres et inclusives dans le domaine de la sécurité.

Silvio MASCAGNA

2- SEYDA EMEK - CONSEILLÈRE DE GILLES DE KERCHOVE, COORDONNATEUR EUROPÉEN POUR LA LUTTE CONTRE LE TERRORISME

Europol a recueilli auprès de ses membres des exemples concrets d'affaires affectées par le régime actuel de conservation des données dans l'Union européenne. La contribution a été partagée en 2017 par le groupe « Échange d'informations et protection des données" (DAPIX) du Conseil chargé des travaux concernant la mise en œuvre de la législation et des politiques en matière d'échange d'informations et de protection des données à caractère personnel dans le domaine de l'application de la loi. Il coopère également étroitement avec Europol, surtout en ce qui concerne la stratégie de gestion de l'information relative à la rationalisation des échanges transnationaux d'informations.

La liste n'est pas exhaustive, mais se concentre sur des scénarios d'application de la loi qui peut affecter le travail quotidien des enquêteurs et les conséquences qui s'ensuivent pour ces enquêtes en raison de problèmes de conservation des données.

En substance, l'attribution d'une activité criminelle est soit considérablement retardée, soit rendue impossible en raison de la manière dont les informations et les données sont stockées, traitées et partagées par les fournisseurs de communication et de contenu en ligne.

I - POURQUOI LA CONSERVATION DES DONNÉES EST-ELLE NÉCESSAIRE ?

Quelques exemples tirés de l'expérience du coordonnateur européen de la lutte contre le terrorisme.

1er exemple :

Dans le cadre d'une enquête menée par le bureau du Procureur général allemand sur un réseau de personnes soupçonnées de soutenir l'État islamique, le juge d'instruction de la Cour fédérale de justice a demandé des fichiers d'un forum de discussion utilisé par le groupe pour communiquer. Le juge a reçu une série d'adresses IP différentes sans numéro de port source (non enregistrées par l'hébergeur du forum de discussion). Une demande d'identification des abonnés utilisant ces adresses IP a été envoyée au fournisseur de services Internet allemand concerné. Le fournisseur d'accès à Internet n'a pas été en mesure d'identifier les abonnés uniques par adresse IP en raison de l'utilisation de réseaux de qualité porteuse (Carrier-Grade Network Address Translation - CGN) et de l'absence de numéros de port source. Le procureur général n'a pas été en mesure de poursuivre cette enquête.

L'absence d'obligation harmonisée de conservation des données dans toute l'Europe affecte également la capacité des fournisseurs de communication et des fournisseurs d'accès à Internet à se conformer à leurs obligations légales de permettre l'identification de leurs abonnés sur la base d'une adresse IP et lorsqu'une décision judiciaire ou une demande de police leur est signifiée. Cela crée une grave lacune dans les capacités en ligne de la magistrature et des organismes d'application de la loi en matière d'enquêtes et d'attribution des crimes.

Cela est dû à une combinaison de différents facteurs :
- avant tout à l'absence d'obligation légale pour les fournisseurs de services électroniques (ESP), tels que les plateformes de médias sociaux, les services de messagerie Web et les services d'hébergement, d'enregistrer une information appelée « numéro de port source".

- deuxièmement, à l'adoption massive par les fournisseurs d'accès à Internet d'une technologie appelée Carrier-Grade Network Address Translation (CGN), qui permet aux fournisseurs d'accès à Internet de partager une adresse IP avec jusqu'à 65.000 abonnés. En l'absence du numéro de port source, les fournisseurs d'accès à Internet ne peuvent pas différencier les abonnés connectés au même fournisseur de services électroniques avec la même adresse IPv4 partagée à un moment donné.

2ème exemple :

Dans le cadre d'une enquête liée au terrorisme islamiste, une équipe commune d'enquête a recherché les personnes de contact, c'est-à-dire les donneurs d'ordre et leurs complices éventuels, d'une des personnes accusées. La recherche sur les réseaux sociaux a permis d'identifier des profils de réseaux sociaux pertinents de personnes de contact possibles. L'entreprise de réseau social a pu fournir les adresses IP utilisées pour se connecter à la plateforme mais pas le numéro de port source. Selon elle, le stockage des ports est techniquement possible, mais pour des raisons de protection des données (directive « vie privée et communications électroniques"), l'entreprise ne peut collecter et stocker que les données qui sont nécessaires au fonctionnement du réseau et à la facturation. Ce n'est pas le cas pour les détails du port source. L'analyse des adresses IP transmises par l'entreprise indique qu'elles appartiennent à un fournisseur d'accès Internet mobile allemand. Toutefois, le fournisseur d'accès n'a pas été en mesure d'attribuer les adresses IP aux abonnés parce que l'entreprise attribue la même adresse IP à plusieurs milliers de clients en même temps (CGN). Par voie de conséquence, il n'a pas été possible d'identifier d'autres cibles potentielles au moyen des adresses IP.

3ème exemple :

En ce qui concerne la menace d'une attaque à Paris, les autorités policières compétentes enquêtaient sur un individu derrière un compte de média social. Les journaux ont montré que l'individu se connectait avec des adresses IP mobiles fournies par un fournisseur d'accès d'Internet mobile français. En raison de l'utilisation du CGN, la personne n'a pas pu être identifiée ou localisée par des moyens techniques.

II - POURQUOI AVONS-NOUS BESOIN D'UN INSTRUMENT EUROPÉEN ?

Quelques réflexions :

1. La situation actuelle n'est pas viable. Les entreprises ne sont plus légalement tenues de conserver les données relatives au trafic des communications dans des États membres comme l'Allemagne, la Suède et les Pays-Bas après les arrêts de la Cour européenne de justice.

2. 28 systèmes différents de conservation des données dans l'Union doivent être évités. Cela serait très difficile à gérer pour les entreprises. L'absence d'une approche harmonisée au sein de l'Union peut entraîner des difficultés dans l'application de la loi et la coopération judiciaire.

3. La rétention ciblée n'est pas une solution.

Cela est impossible du point de vue de la sécurité, car il n'est pas possible de savoir à l'avance qui commettra des infractions graves.
Il serait également discriminatoire du point de vue des droits de l'Homme si, par exemple, les quartiers où vivent de nombreux immigrés ou des quartiers défavorisés étaient désignés pour la conservation des données, alors que les zones les plus riches étaient exemptées. Les criminels pourraient contourner la rétention si cela était connu.
Il ne suffit pas non plus de le conserver pendant quelques semaines avant ou après les événements.

4. Les données conservées à des fins commerciales sont inégales d'une entreprise à l'autre et ne sont pas suffisantes.

5. Compte tenu de l'utilisation accrue par les criminels et les terroristes du cryptage, qui rend l'accès au contenu difficile, voire impossible, la conservation des données relatives au trafic est encore plus cruciale pour éviter que les autorités compétentes ne soient « aveugles ».

6. L'instrument communautaire de conservation des données est nécessaire pour répondre aux besoins des services répressifs et des autres autorités compétentes, ainsi qu'aux exigences de la CJUE. Le coordonnateur européen a fait des suggestions en vue d'un éventuel acte législatif de l'Union au cours de récentes discussions au sein du Conseil.

III - EXIGENCES DE JURISPRUDENCE DE LA CJUE DANS L'ARRÊT TELE2

La mesure doit être limitée au strict nécessaire, être fondée sur des éléments de preuve tangibles et objectifs et doit établir des règles claires et précises. La CJUE déclare que la rétention doit être limitée en ce qui concerne les noms de domaine :

a) les données relatives à une période et/ou une zone géographique particulière et/ou à un groupe de personnes susceptibles d'être impliquées, d'une manière ou d'une autre, dans un crime grave,
b) soit des personnes qui pourraient, pour d'autres raisons, contribuer, par la conservation de leurs données, à la lutte contre la criminalité.

Le problème est que la jurisprudence de la CJUE ne donne pas d'indications sur ce que les juges de la CJUE considéreraient comme des moyens nécessaires en matière de conservation des données (aucune explication positive par exemple de ce que le tribunal jugerait « nécessaire »). Le tribunal ne fait qu'encadrer la conservation éventuelle en termes négatifs.

IV - LA SUGGESTION DU COORDONNATEUR EUROPÉEN DE « RESTREINDRE L'ACCÈS AUX DONNÉES CONSERVÉES".

1. Une approche législative différente est possible : Il faudrait réserver l'accès aux données conservées aux luttes contre les crimes graves et le terrorisme.

Des garanties plus élevées en ce qui concerne le stockage, l'accès et l'utilisation des données permettraient d'assurer globalement la « proportionnalité ».

Le Conseil Justice-Affaires intérieures du 7 décembre 2017 a reconnu que le concept pourrait à terme servir de base à l'élaboration d'un cadre de conservation des données au niveau européen et a encouragé à faciliter les travaux préparatoires d'une matrice de données connexes en étroite collaboration avec les experts techniques des États membres en vue de la poursuite des discussions au sein du groupe Échange d'informations et protection des données (DAPIX) qui s'est réuni à cette fin.

Europol a organisé deux ateliers réunissant des enquêteurs spécialisés et des experts légistes des États membres. Eurojust y a participé.

Le groupe « Échange d'informations et protection des données » se réunit régulièrement depuis 2 ans pour examiner les arrêts de la CJUE, la jurisprudence et le cadre juridique des États membres afin de trouver des solutions de conservation des données.

Le Coordonnateur européen a fait des suggestions au Conseil en vue d'une éventuelle législation communautaire fondée sur l'idée d'une conservation limitée des données.

L'ancienne législation communautaire reposait sur les règles du marché intérieur. De nouvelles dispositions tendraient à garantir la protection des droits fondamentaux.

L'instrument européen inclurait toutes les conditions d'accès strictes fixées par la CJUE dans l'arrêt Tele2 :

- Restreindre l'accès au seul objectif de la lutte contre le terrorisme et la grande criminalité.

- L'instrument pourrait en outre envisager de combiner la conservation des données à des fins de prévention, d'enquête et de poursuite des infractions graves avec un système parallèle visant à garantir l'accès des fournisseurs aux données conservées à des fins professionnelles (non soumis à des obligations de stockage ou conservés à des fins professionnelles bien qu'il existe également des obligations stockées, modèle hybride).

- Un tel modèle hybride pourrait contribuer à garantir la disponibilité des données dans les situations d'urgence ou les situations mettant la vie en danger et qui ne sont pas nécessairement liées à des activités criminelles, par exemple les personnes disparues.

- Prescrire des règles claires et précises indiquant dans quelles circonstances et sous quelles conditions les fournisseurs de services de communications électroniques doivent accorder

aux autorités nationales compétentes l'accès aux données.

- Accès sous réserve d'un contrôle préalable par un tribunal ou une autorité administrative indépendante (exception : cas d'urgence)

- Adoption de la structure de la réglementation relative à la protection de la vie privée dans le secteur des communications électroniques à la lumière de la décision Tele2

L'instrument européen pourrait évaluer la menace terroriste qui pèse actuellement sur l'Union européenne ainsi que l'utilisation accrue des technologies de l'espace cybernétique et des communications pour les crimes graves, mettant en cause la sécurité publique. Il pourrait inclure une clause de révision après plusieurs années et exiger de chaque État membre qu'il procède à l'évaluation régulière sur son territoire de la menace et des risques pour la sécurité publique, qui nécessiteraient la poursuite de la conservation des données.

Dans un premier temps, pour répondre à l'une des préoccupations de la CJUE, il pourrait y avoir une possibilité d'opt-out pour les personnes dont les communications sont soumises, selon les règles du droit national, à l'obligation du secret professionnel. Cela signifie que ces utilisateurs pourraient demander que leurs données ne soient pas consultées et donc consentir au traitement de leurs données personnelles pertinentes pour l'application de cette exception. Il conviendrait de préciser les règles applicables à une telle renonciation.

Au-delà de ces exceptions, il est suggéré de limiter la conservation au minimum en concentrant les efforts de test de nécessité sur les catégories de données et les fournisseurs et ne conserver que les catégories de données qui sont absolument nécessaires pour sauvegarder la sécurité publique.

Le critère de nécessité ne s'appliquerait pas à des groupes de personnes ou à des zones géographiques spécifiques sur le territoire d'un État membre. Cela permettrait de limiter la rétention tout en répondant pleinement aux besoins des services répressifs.

Il y aurait une approche générale à l'échelle européenne, dont les paramètres et les critères stricts seraient définis dans l'instrument, sur la base de tests de stricte nécessité quant au type de données qu'il est absolument nécessaire de conserver. L'instrument juridique ou les mesures d'exécution pourraient contenir des éléments de preuve objectifs quant à la nécessité de ces types de données.

Ces mesures devraient être régulièrement renouvelées après de nouvelles évaluations de la nécessité. Un test de stricte nécessité pourrait et devrait être effectué pour les catégories de données qui sont indispensables pour rétention. Effectuer ces évaluations de nécessité, en fonction des besoins des services répressifs et d'autres autorités compétentes, requiert des efforts et une analyse, mais permet de réduire la portée des données et être limité au minimum nécessaire à des fins répressives, conformément aux exigences de la CJUE. S'il existait des filtres de stricte nécessité, la conservation des données ne serait pas généralisée (seule une partie des catégories de données de communication sera conservée, même si elle peut couvrir un pourcentage important de l'ensemble des données de la population).

D'autre part, la conservation ne serait pas ciblée sur des périodes, des lieux ou des groupes de personnes spécifiques qui ne répondraient pas aux besoins des services répressifs. Les dérogations supplémentaires pour les personnes liées au secret professionnel signifient également que l'ensemble de la population n'est pas concerné. La population couverte par les mesures relèverait de la catégorie des personnes qui « ils pourraient, pour d'autres raisons, contribuer, par la conservation de leurs données, à la lutte contre la criminalité ».

L'instrument communautaire de conservation des données devrait montrer pourquoi la conservation de

certains types de données est absolument nécessaire, tout en montrant qu'il existe une méthodologie approfondie pour déterminer les données et les obligations de conservation.

Pour satisfaire aux exigences de la CJUE, la possibilité pour les autorités compétentes d'accéder aux données stockées pourrait être limitée aux seules fins de la lutte contre le terrorisme et la criminalité organisée et grave, y compris les cyberattaques. La période de conservation de six mois serait la limite inférieure de l'ancienne législation communautaire sur la conservation des données. Pour se conformer au paragraphe 122 de l'arrêt Tele2, il semble que l'instrument communautaire devrait exiger la destruction irréversible des données à la fin de la période de conservation des données. Toutefois, il faudrait clarifier le lien avec les données qui sont conservées à des fins commerciales de toute façon (lorsque les mêmes données sont couvertes par l'obligation de conservation). Cela signifierait probablement la destruction des données qui, autrement, n'auraient pas été conservées.

Stockage en Europe et de manière codée / pseudonymisation

La CJUE exige « d'imposer des garanties minimales, afin que les personnes dont les données ont été conservées aient des garanties suffisantes de protection efficace de leurs données personnelles contre le risque d'une mauvaise utilisation".

Par conséquent, le fait d'imposer des exigences en matière de sécurité des données, de stockage des données dans l'Union (comme l'exige la CJUE au paragraphe 122 de l'arrêt Tele2) et de manière cryptée, protégerait contre un accès non autorisé. Il faudrait préciser si le stockage crypté est possible en ce qui concerne les modèles d'affaires et quelles autres mesures de protection de la vie privée pourraient être incorporées.

Seyda EMEK

Retrouvez l'ensemble de nos publications sur notre site :
www.robert-schuman.eu

Directeur de la publication : Pascale JOANNIN