FONDATION ROBERT SCHUMAN

POLICY PAPER

**Schuman Paper**
n°846
14 septembre 2026

**Jean MAFART**

# « *Tele 2* », dix ans après : embarras et controverses sur l'accès aux données numériques

Le 21 décembre 2016, la Cour de justice de l'Union européenne (CJUE) rendait un arrêt *Tele 2 Sverige*, dont la portée allait rapidement apparaître comme vertigineuse : il bouleversait les conditions dans lesquelles la justice et les services enquêteurs peuvent exploiter les métadonnées détenues par les opérateurs de communications électroniques. Une juriste perspicace écrivait quelques semaines plus tard,: « *Cet arrêt va changer la donne en matière de surveillance étatique en Europe et, si c'est un cadeau de Noël avant l'heure pour les défenseurs de la vie privée, il devrait susciter des réactions très mitigées de la part des États membres de l'Union*. » C'était peu dire : bien au-delà d'une prétendue « surveillance étatique », la jurisprudence *Tele 2* confronte les États membres à la difficulté de mieux protéger les données personnelles tout en préservant les capacités d'enquête contre le terrorisme, la criminalité organisée, l'espionnage ou la délinquance ordinaire.

Où en sommes-nous dix après ? La question est d'autant moins anodine que le débat ne se cantonne plus aux sphères « justice et affaires intérieures » (JAI) de l'Union européenne : la question de « l'accès aux données » est aussi abordée, désormais, sous l'angle de la résilience européenne, dans le cadre d'une conception globale de la sécurité.

## DE QUOI S'AGIT-IL ?

Les communications électroniques, qu'il s'agisse de la téléphonie ou d'Internet, produisent une masse énorme de métadonnées ; ces données de connexion, de trafic et de localisation sont devenues une « matière première » essentielle aux services de renseignement et de police judiciaire. Il y a vingt-cinq ans déjà, les échanges électroniques de Richard Reid, le Britannique qui avait tenté de faire exploser sa « chaussure piégée » lors d'un vol Paris-Miami en décembre 2001, avaient révélé ses liens avec des réseaux terroristes proches d'Al Qaeda. L'exploitation des métadonnées est d'autant plus cruciale que la diffusion massive des technologies de chiffrement entrave l'accès aux contenus eux-mêmes : tous les enquêteurs savent par exemple que les « écoutes téléphoniques » ne sont plus ce qu'elles étaient.

Pour que les données soient exploitables, la plupart des États membres imposaient aux fournisseurs de communications électroniques de conserver pour une certaine durée les données de leurs clients afin qu'elles puissent, en cas de besoin, être mises à la disposition des services enquêteurs, soit dans le cadre administratif du renseignement, soit dans le cadre d'une enquête judiciaire. Il n'est pas question de « surveillance » puisque les données restent chez les opérateurs, ceux-ci étant simplement tenus de les conserver un certain temps en vue de leur communication éventuelle aux autorités – rien à voir, donc, avec les méthodes dénoncées en son temps par Edward Snowden. C'est cet édifice que la CJUE, néanmoins, remet en cause.

L'arrêt *Tele 2* ne venait pas de nulle part : en 2014, l'arrêt *Digital Rights* avait invalidé la directive du 15 mars 2006 – texte adopté à la suite de l'attentat terroriste de Londres –, qui harmonisait, dans une certaine mesure, les régimes de conservation des données de connexion dans les États membres. La Cour relève en effet que « *ces données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que*

*les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci* ». Une telle immixtion dans la vie privée, estimait la Cour, requérait un encadrement strict que la directive de 2006 ne garantissait pas.

Mais l'arrêt *Tele 2* va plus loin : la Cour énonce que, « *si l'efficacité de la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une réglementation nationale prévoyant la conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation soit considérée comme nécessaire aux fins de ladite lutte* ». Une telle conservation, en effet, s'applique « *même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions pénales graves* ». Aussi l'arrêt suggère-t-il un recueil sélectif des données, sur la base de « critères objectifs », de manière à « délimiter effectivement l'ampleur de la mesure et, par suite, le public concerné ».

Au passage, la Cour confirme exercer une vigilance particulière lorsque les données sont exploitées par les services de police : l'argument, récurrent dans la jurisprudence de la CJUE comme de la CEDH, tient en l'espèce à ce que « *la conservation des données relatives au trafic et des données de localisation à des fins policières est susceptible, à elle seule, de porter atteinte au droit au respect des communications, consacré à l'article 7 de la Charte, et d'entraîner des effets dissuasifs sur l'exercice par les utilisateurs des moyens de communications électroniques de leur liberté d'expression, garantie à l'article 11 de celle-ci* ».

Or la conservation sélective des données de connexion est une chimère, comme l'expliquait le Conseil d'Etat français en termes à peine plus diplomatiques : « *Une conservation ciblée […] présenterait un intérêt opérationnel particulièrement incertain, dès lors qu'elle ne permettrait pas […] d'accéder aux données de connexion d'une personne suspectée d'une infraction qui n'aurait pas été préalablement identifiée comme étant susceptible de commettre un tel acte. Ainsi, notamment pour les cas de primo-délinquants, mais également lorsque les auteurs d'infractions pénales ont recours à des téléphones dotés de cartes prépayées qu'ils n'utilisent que pour une durée limitée […], les services d'enquête judiciaire ne pourraient pas accéder aux données de connexion indispensables à l'élucidation des affaires dont ils sont saisis. Par ailleurs, il est impossible de définir par avance des zones géographiques où, par nature, aucun acte de criminalité grave susceptible de justifier la conservation des données de connexion ne pourrait survenir. Une obligation de conservation des données de connexion limitée à certaines zones géographiques, à supposer même qu'elle soit techniquement envisageable, ferait ainsi obstacle à l'action des services d'enquête dans les autres parties du territoire national lorsque de telles infractions y seraient commises. Enfin, aucune présomption de dangerosité ne saurait être légalement retenue à l'encontre de personnes en fonction de leur lieu de résidence ou d'activité professionnelle pour justifier la conservation de leurs données de trafic et de localisation.* »

Enfin, la jurisprudence Tele 2 n'affectait pas que la police judiciaire : elle portait aussi atteinte à l'exploitation des données de connexion dans le cadre administratif du renseignement – donc le plus souvent dans un domaine, la sécurité nationale, que les traités européens réservent à « *la seule responsabilité de chaque État membre* » (TUE, art. 4, § 2). A une question opérationnelle s'ajoutait donc une question de principe, celle des compétences respectives de l'Union et de ses Etats membres. La communauté européenne du renseignement, dont les activités s'organisent pour l'essentiel en dehors du cadre juridique et institutionnel de l'Union, vivait comme une entrave injustifiée le nouvel état du droit[1].

## L'URGENCE D'UNE PARADE ET L'ÉVOLUTION DE LA CJUE

Peu d'arrêts de la CJUE auront suscité une telle émotion dans les enceintes européennes, à la mesure de la satisfaction exprimée par certaines ONG. Dès 2017, la question de la « rétention des données » devint un « marronnier » des discussions dans les enceintes JAI

***[1]*** *J. Mafart, la Politique européenne de sécurité intérieure, Bruylant, 2015, ch. II.*

de l'Union, des groupes d'experts jusqu'aux réunions des ministres de l'Intérieur ou de la Justice. Dans ses conclusions du 23 juin 2017, le Conseil européen souligna la nécessité d'un « *accès effectif aux preuves électroniques* » et d'assurer la « *disponibilité des données* ». Cependant, les discussions au Conseil demeurèrent longtemps sans conclusion probante, d'autant plus que la proposition de règlement « vie privée et communications électroniques » (e privacy), qui aurait pu résoudre une partie du problème, ne put aboutir sous la législature achevée en 2024 (la Commission l'a finalement retirée l'année dernière).

En attendant une solution européenne très incertaine, les États membres connurent l'angoisse. Une affaire sordide eut un retentissement particulier : alors qu'en 2015 la justice irlandaise avait condamné à la réclusion à perpétuité le meurtrier d'une jeune femme vulnérable, sur fond de pratiques sadomasochistes, l'individu fit valoir qu'il n'aurait pu être confondu sans la pratique, désormais interdite, de la conservation généralisée et indifférenciée. La CJUE allait-elle prononcer la nullité de l'enquête et provoquer l'élargissement d'un assassin sadique ? Combien d'autres affaires criminelles risquaient-elles de « tomber » à travers l'Europe, du seul fait que les services d'enquête s'étaient appuyés sur des données obtenues sur le fondement d'un régime de conservation générale ? La Cour s'en tira, en 2022, en confirmant l'interdiction d'un tel régime tout en rappelant le principe d'autonomie procédurale des États membres : il n'appartenait qu'à ces derniers de définir le régime d'admissibilité de la preuve pénale. Autrement dit, l'accusé ne pouvait utilement faire valoir que la loi irlandaise était contraire au droit de l'Union[2] et il resta fort heureusement en prison. L'Irlande n'en dut pas moins réviser sa législation en toute hâte.

Dans les années qui suivirent l'arrêt *Tele 2*, la plupart des États membres préférèrent ne pas se précipiter pour adapter leur droit interne ; parmi eux se forma même un camp des « intransigeants », mené par la France. Cette attitude de fermeté offensive et le choix de la simple inertie reposent toutes deux sur une sorte de pari : « tenir » jusqu'à ce que la position de la CJUE s'assouplisse, quitte à assortir – le plus tard possible – le régime de conservation ou d'exploitation des données de restrictions raisonnables pour préserver le principe de la conservation générale. Outre la France, on comptait dans cette école l'Italie, l'Espagne, le Danemark ou certains États d'Europe centrale et orientale en dépit des craintes d'origine historique (comme en Allemagne ou en Autriche) à l'égard de tout ce qui peut évoquer la surveillance des citoyens. En tout état de cause, l'espoir de préserver le *statu quo* autant que possible ne s'accommodait pas de la simple inertie. En 2018, un chef de gouvernement effectua une démarche officieuse auprès du président Juncker pour dissuader la Commission de publier des « lignes directrices » sur l'application de la jurisprudence *Tele 2* : un tel document n'aurait pu que rappeler aux Etats membres les exigences de la CJUE et fragiliser ceux qui, plus ou moins ouvertement, avaient choisi la voie du *statu quo*.

De manière beaucoup plus officielle, la Fondation Robert Schuman et l'Institut Max Planck organisèrent en avril 2019 à Luxembourg – là où, par un heureux hasard, siège la CJUE – un intéressant colloque sur « la protection des citoyens européens dans un monde ultra-connecté ». La communication d'un haut magistrat français mérite d'être citée: « *Il est à craindre*, observait le procureur Molins, *que la Cour de Luxembourg n'ait en effet pas maîtrisé comment les services qui sont chargés des investigations parviennent à identifier des auteurs de crimes ou des membres de réseau criminel, dont la parfaite maîtrise des techniques policières les conduit à "professionnaliser" l'effacement des traces et indices traditionnels.* » Quant à la conservation sélective des données, elle était qualifiée de « *vue de l'esprit* ».

Décidées à obtenir un infléchissement de la position de la CJUE, plusieurs juridictions nationales cherchèrent à lui en fournir l'occasion. A cet égard, l'arrêt *Quadrature du Net*, en réponse à des questions préjudicielles venues de plusieurs États membres, représente une étape essentielle. La Cour explicite d'abord le mécanisme par lequel le droit européen intervient dans le champ de la sécurité nationale : pour l'essentiel, il tient à ce que les obligations imposées par les opérateurs en matière de protection de la vie privée de leurs clients (directive « e privacy » de 2002) forment un bloc et ne peuvent dépendre de la finalité pour lesquelles les données sont conservées. C'est

***[2]*** *CJUE, 5 avril 2022, G.D. c. Commissioner of An Garda Síochána.*

donc seulement dans l'hypothèse où « *les États membres mettent directement en œuvre des mesures dérogeant à la confidentialité des communications électroniques, sans imposer des obligations de traitement aux fournisseurs de services de telles communications* », que le droit national prévaut.

Comme pour compenser cette immixtion du droit européen dans le champ de la sécurité nationale, la CJUE apporte ensuite un assouplissement à la jurisprudence *Tele 2* : elle admet qu'un État membre puisse imposer aux opérateurs une conservation générale et indifférenciée des données de connexion « *pendant une période limitée, dès lors qu'il existe des circonstances suffisamment concrètes permettant de considérer que l'État membre concerné fait face à une menace grave […] pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible* ».

Mais qu'en est-il en matière de criminalité ? La Cour estime d'abord que « *l'importance de l'objectif de sauvegarde de la sécurité nationale […] dépasse celle des autres objectifs* ». Il en résulte une hiérarchie des finalités (sécurité nationale, puis « lutte contre la criminalité grave » et « prévention des menaces graves contre la sécurité publique », puis « lutte contre la criminalité » et « sauvegarde de la sécurité publique »)[3]. A cette hiérarchie correspond une autre hiérarchie, celle des mesures d'investigation en fonction du degré d'atteinte à la vie privée. Autrement dit, l'objectif de « lutte contre la criminalité en général, même grave » ne saurait comme la sécurité nationale justifier une conservation générale des données. Il faudra se contenter d'une injonction de « conservation rapide », c'est-à-dire demander aux opérateurs, pour les besoins d'une enquête, de protéger l'intégrité des données de connexion déjà en leur possession.

Par un autre arrêt important, l'arrêt *Prokuratuur*, la CJUE précise les conditions d'accès aux données (et non de leur conservation) dans un cadre judiciaire : d'une part, cet accès doit être cantonné à la « criminalité grave » (notion que le droit européen ne définit d'ailleurs pas) et à la « prévention de menaces graves contre la sécurité publique » ; d'autre part, l'accès doit être autorisé par une juridiction ou une autorité indépendante, à l'exclusion d'un « ministère public qui dirige la procédure d'enquête et exerce, le cas échéant, l'action publique ».

## LA DISPARITÉ DES RÉPONSES DES ÉTATS MEMBRES

L'arrêt *Quadrature du Net* rebattait un peu les cartes : d'une part, la Cour entrouvrait la porte à une conservation généralisée et indifférenciée des données en matière de sécurité nationale ; d'autre part, elle ouvrait une brèche en matière de criminalité puisque, outre la « conservation rapide », elle n'interdisait pas explicitement d'utiliser dans un cadre judiciaire des données conservées à des fins administratives de sécurité nationale. L'arrêt *Prokuratuur* permettait en outre, en dépit de nouvelles restrictions, de ne pas faire porter tout l'effort de protection de la vie privée sur la conservation des données : les conditions d'accès pouvaient aussi être révisées[4]. Une voie s'ouvrait donc à une adaptation des cadres juridiques nationaux sur une base plus réaliste et plus claire. On ne peut qu'être frappé, pourtant, par la disparité de ces adaptations nationales.

D'après un bilan publié en novembre 2024 par Eurojust, douze États membres ont révisé leur régime de conservation des données par suite de la jurisprudence de la CJUE. Mais cette catégorie recouvre des situations très différentes puisqu'on y trouve à la fois la France et la Belgique.

En France, le Conseil d'Etat a choisi de réaffirmer la primauté de la Constitution et se réserve la possibilité d'écarter l'application d'une directive ou d'un règlement européen lorsque, tel qu'interprété par la CJUE, il « *aurait pour effet de priver de garanties effectives* » un principe constitutionnel (en l'espèce, la sécurité) « *qui ne bénéficierait pas, en droit de l'Union, d'une protection équivalente* »[5]. S'abstenant toutefois d'appliquer cette solution au cas d'espèce, il s'est appuyé sur l'assouplissement de la jurisprudence de la CJUE pour juger la législation française compatible avec le droit européen, sous réserve de quelques évolutions qui sont effectivement intervenues peu après. La réaction de la Quadrature du Net ne s'est pas fait attendre, le Conseil d'Etat étant accusé de « valider durablement la surveillance de

*[3] Sur la sécurité nationale, v. J. Mafart, « Sécurité nationale », in H. Moutouh et J. Poirot (dir.), Dictionnaire du renseignement, Perrin, 2018*

*[4] Dès 2014, le Conseil d'Etat français avait proposé une approche portant sur les conditions d'accès plutôt que sur la conservation : prenant acte que le recueil général et préalable des données de connexion était la condition même de leur exploitation, il préconisait de moduler les conditions d'accès en fonction de la finalité (terrorisme, criminalité organisée, etc.) ; le Numérique et les droits fondamentaux, étude annuelle, Paris, Conseil d'Etat, 2014.*

*[5] Dans ses observations écrites, le gouvernement avait demandé au Conseil d'Etat de statuer ultra vires, c'est-à-dire de passer outre l'arrêt de la CJUE en constatant que celle-ci ne respectait pas la répartition des compétences entre l'Union et ses Etats membres. C'était la première fois depuis le traité de Rome qu'une telle option était envisagée en France (alors qu'elle a déjà été utilisée en Allemagne) ; c'est dire l'importance que les autorités accordaient au sujet.*

masse » et même – tant qu'à faire – de « libérer les renseignements français des principes de l'État de droit ».

Si ces accusations manquent un peu de mesure, il est intéressant de constater que, du même arrêt *Quadrature du Net* de la CJUE, la Cour constitutionnelle de Belgique tire des conclusions bien différentes de celles du Conseil d'Etat : dans une décision rendue le lendemain, elle a invalidé la législation belge sur la conservation des données, estimant que l'arrêt de la CJUE impose un « changement de perspective » et que « l'obligation de conservation des données relatives aux communication électroniques doit être l'exception, et non la règle ». Elle ne conteste à aucun moment, comme le faisait explicitement le Conseil d'Etat, la possibilité d'opérer une conservation sélective des données. C'est ainsi que la Belgique a fini par réviser sa législation beaucoup plus profondément que la France : une loi du 20 juillet 2022 a institué en particulier des obligations de conservation des données circonscrites à certaines zones géographiques.

On est tenté de se demander comment deux États voisins, de traditions juridiques similaires, peuvent tirer des conclusions aussi divergentes de la même jurisprudence. À en juger par les propos tenus en 2021 par le président de la CJUE, le Belge Koen Lenaerts, il semble bien cependant que les deux solutions répondent aux exigences de la Cour[6] : « *Le Conseil d'État français a rendu un arrêt entièrement conforme à celui de la Cour de justice, même s'il a émis quelques critiques ici et là […]. Nous avons bien reçu le message. La Cour constitutionnelle de Belgique a annulé toute la loi contestée, sans émettre la moindre critique.* » Plusieurs autres États membres, comme l'Autriche ou le Danemark, ont adopté une conservation sélective reposant sur des catégories d'individus ou des zones géographiques. Outre les problèmes de principe et d'efficacité déjà évoqués, cette voie pose cependant de réels problèmes de faisabilité technique et de coût pour les opérateurs. D'autres États membres modulent les règles de conservation selon la nature des données : la Suède, par exemple (pays de l'opérateur Tele 2), applique des règles beaucoup plus restrictives à la géolocalisation qu'aux données de trafic ou aux simples adresses IP.

L'étude d'Eurojust fait aussi apparaître que trois États membres ont conservé de larges obligations de conservation fondées sur la directive de 2006 (celle invalidée par l'arrêt *Digital Rights*). L'Espagne et la Grèce, en particulier, avaient assorti bien avant 2016 leur régime de conservation générale d'un contrôle très strict au stade de l'accès aux données : le juge judiciaire intervient dans tous les cas, même lorsque la consultation répond à une finalité administrative de renseignement. L'Italie, sous la pression de la CJUE, s'est ralliée à ce modèle de conservation relativement large assortie d'une autorisation par le juge judiciaire (et non plus le parquet). Quant à la Pologne, elle subit la pression des deux cours européennes : en 2024, la Cour européenne des droits de l'Homme (CEDH) a jugé que la législation polonaise portait une atteinte disproportionnée au droit à la vie privée.

A l'inverse, quelques États membres ne disposent d'aucun régime de conservation obligatoire des données, même restreint : en Allemagne, aux Pays-Bas, en Slovénie et en Roumanie, les services enquêteurs – auxquels il ne reste que la « conservation rapide » – sont entièrement tributaires des données conservées par les opérateurs pour leurs propres besoins techniques ou commerciaux. La Cour constitutionnelle de Roumanie n'avait pas attendu *Tele 2* : sur le fondement de la Constitution, et non du droit de l'Union, elle avait censuré en 2009 puis en 2014, pour défaut de proportionnalité – et dans les modalités de conservation et dans les modalités d'accès –, la législation nationale transposant la directive européenne de 2006. L'absence de toute obligation de conservation des données occasionne de réelles vulnérabilités, comme le relevait en 2024 un groupe d'experts : « *De ce fait, les enquêtes s'apparentent souvent à une course contre la montre car les enquêteurs doivent identifier le fournisseur des données et transmettre leur demande […] avant que celles-ci ne soient supprimées, ce qui ne prend parfois que quelques jours, voire quelques heures. Dans certains cas, les entreprises ne fournissent pas d'informations sur les données spécifiques qu'elles traitent et détiennent, ce qui complique la tâche des autorités compétentes […].* »

Les experts s'accordent finalement sur deux constats : d'une part, moins de données sont disponibles dans les États membres, soit parce que le cadre juridique national est faible soit parce que les

***[6]*** *K. Lenaerts, audition devant la commission des affaires européennes, Paris, Assemblée nationale, compte rendu no 191, 18 mai 2021. Le président Lenaerts ajoute que le Conseil d'État « a parfaitement mis en œuvre notre arrêt ».*

juridictions ou les opérateurs eux-mêmes s'appuient sur la jurisprudence européenne pour retenir une approche très restrictive en matière de conservation ou d'accès ; d'autre part, la moindre disponibilité des données à l'échelle européenne et la disparité même des régimes nationaux affectent la coopération en matière de sécurité, notamment dans le cadre des décisions d'enquête européennes.

## PERSPECTIVES

A l'approche du dixième anniversaire de *Tele 2*, l'idée d'une harmonisation européenne continue de circuler avec insistance. Elle a pour elle la logique : l'extrême faiblesse de certains dispositifs nationaux représente une vulnérabilité évidente pour l'ensemble de l'espace de liberté, de sécurité et de justice dès lors que le terrorisme ou la criminalité organisée se jouent des frontières intérieures. Plusieurs exemples, comme celui de l'Irlande, de la Belgique ou du Danemark, montrent par ailleurs ce que peut avoir de précaire un régime national de conservation des données « à l'ancienne ». Mais il est aussi évident que, par rapport à la directive invalidée par l'arrêt *Digital Rights*, un nouveau texte devra être plus précis et plus directif quant à la protection de la vie privée, sans pour autant compromettre les capacités opérationnelles des États membres. C'est là que le bât blesse : certains, comme la France ou l'Italie, peuvent légitimement craindre qu'un texte européen strictement aligné sur la jurisprudence *Tele 2* ne vienne affaiblir le cadre juridique qu'ils ont réussi à préserver. Plongée dans des travaux préparatoires qu'on devine délicats, la Commission européenne n'a pas encore fixé d'orientations nettes. Dans sa stratégie de sécurité intérieure d'avril 2025, elle s'en était tenue à un langage très prudent, annonçant « *préparer une analyse d'impact en 2025, en vue d'actualiser, en tant que de besoin, les règles de l'UE relatives à la conservation des données* »[7]. La discussion d'une future directive promet en tout cas d'énormes difficultés.

Plusieurs évolutions récentes – sans même évoquer de nouvelles évolutions toujours possibles de la CJUE – tendent néanmoins à favoriser une approche plus opérationnelle de la question des données. L'« accès aux données », en premier lieu, est devenu un sujet à part entière des débats européens. En juin 2023 a ainsi été constitué un groupe de haut niveau (GHN) « sur l'accès aux données pour une police efficace », avec des représentants des États membres, de la Commission, des agences européennes et du coordonnateur européen pour le contre-terrorisme. L'Union européenne n'est pas isolée dans cette réflexion : au sein du G7, un groupe de travail a été institué sur le même thème. Les travaux européens font apparaître que, si le développement des technologies numériques engendre quantité de données potentiellement exploitables, il a un autre effet, moins attendu: « *Paradoxalement, alors que la transformation numérique a entraîné la création, la transmission et la conservation d'un volume de données toujours plus important, la disponibilité des preuves électroniques et l'accès à celles-ci […] sont devenus le principal défi à relever pour protéger les citoyens de l'Union contre la menace que représentent le terrorisme, la grande criminalité et la criminalité organisée. – Si ce défi n'est pas nouveau, il continue de prendre de l'ampleur chaque jour. Les services de police sont littéralement "plongés dans le noir" [going dark]*. »

Le rapport final de ce groupe de haut niveau aborde aussi la question du chiffrement : « *Les données enregistrées sur certains types d'appareils modernes protégés par des puces cryptographiques ou par des algorithmes de chiffrement puissants et des mots de passe complexes ne sont pas accessibles aux services enquêteurs, même en utilisant les plates-formes de déchiffrement les plus puissantes. Le chiffrement et d'autres mesures de cybersécurité et de protection de la vie privée sont nécessaires pour protéger les systèmes d'information et les données de communication et personnelles, mais ces mesures […] réduisent la capacité des forces de l'ordre de recueillir des preuves.* » Aussi le GHN invite-t-il la Commission à « *élaborer et mettre en œuvre une feuille de route technologique axée sur les défis du chiffrement, en abordant tous les aspects pertinents, y compris les aspects liés à la technologie, au marché, à la cybersécurité, aux droits fondamentaux, à la normalisation, à la police judiciaire et à la recherche* ». Il s'agit plus largement de définir un cadre juridique et technologique des « interceptions légales », en coopération avec l'industrie.

*[7] On attend toujours ladite « analyse d'impact ».*

Les quarante-deux propositions, présentées aux ministres en décembre 2024, promettent plusieurs années de riches discussions. Dans sa stratégie de sécurité intérieure, la Commission indique qu'elle proposera une « feuille de route » pour « garantir un accès légal et effectif aux données » – bien au-delà, donc, des difficultés nées de la jurisprudence *Tele 2*. Rappelons aussi que le règlement et la directive du 12 juillet 2023 sur l'accès transfrontalier à la preuve électronique représentent un immense progrès dans l'accès aux données numériques indispensables aux enquêtes, surtout lorsqu'il s'agit de données détenues par les multinationales d'Internet[8].

Relevons une deuxième tendance notable : dans le cadre d'une approche globale de la sécurité que la Commission promeut avec beaucoup de ténacité – non sans ambitions d'ordre institutionnel face aux États membres, dans un contexte géopolitique propice aux avancées sur la « souveraineté européenne » –, la question de l'accès aux données apparaît comme un enjeu de résilience européenne face aux crises. En octobre 2024 est paru le rapport de l'ancien président finlandais Sauli Niinistö sur la préparation (*preparedness* et *readiness*) aux crises. La question de l'accès aux données numériques pour les services enquêteurs y est abordée : rejoignant les conclusions du groupe de haut niveau, il recommande de « *veiller à la création d'un cadre solide pour l'accès légal aux données chiffrées afin de soutenir la lutte des autorités des États membres contre l'espionnage, le sabotage et le terrorisme, ainsi que la criminalité organisée* ». Si la « stratégie de préparation » de mars 2025 ne mentionne pas ces aspects, la stratégie de sécurité intérieure d'avril 2025 les abordait directement.

Enfin, la présidente von der Leyen a annoncé en janvier 2026 une stratégie européenne de sécurité. L'initiative ne convainc pas tous les observateurs : certains relèvent l'accumulation des documents stratégiques et appellent de leur vœux un document véritablement utile[9]. Un grand mystère entoure encore ce document mais il ne ressemblera pas totalement aux précédents documents de ce type, notamment la *Boussole stratégique* de 2022. Traitant de la sécurité européenne sous l'angle le plus large, il vise à présenter un cadre global permettant de mettre en cohérence les différentes politiques européennes et nationales, internes et externes. Un document utile traiterait donc des questions de sécurité intérieure : par exemple les menaces hybrides, phénomène d'origine géopolitique, sont devenues un aspect majeur des politiques de sécurité intérieure. Dix ans après *Tele 2*, et dans le prolongement du rapport Niinistö, il faut donc souhaiter que la question des données trouve toute sa place dans la réflexion stratégique européenne.

**Jean Mafart**

Préfet, ancien directeur des affaires européennes et internationales du ministère de l'Intérieur, auteur de la Politique européenne de sécurité intérieure (Bruylant, 2025), membre du comité scientifique de la Fondation Robert Schuman.

***[8]*** *Au lieu de recourir aux mécanismes très contraignants de la coopération pénale internationale pour obtenir des données détenues par des sociétés d'Internet aux Etats-Unis ou ailleurs, les magistrats peuvent désormais adresser des injonctions directement à ces sociétés, qui ont l'obligation de désigner au sein de l'Union européenne un « représentant légal » pour recevoir et traiter rapidement ces injonctions.*

***[9]*** *V. F. Koesterke, « The EU is talking strategy: make it worthwhile », Institut Egmont, 24 mars 2026 ; P. Veron, « A new European security strategy: what for ? », ECDPN, 3 juin 2026 ; P. Vimont, « European Security Strategy : in search of a new ambition », Carnegie Europe, 11 juin 2026.*

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

Directeur de la publication : Pascale JOANNIN
ISSN 2402-614X