La Directive sur la conservation des données
De la surveillance de masse à son invalidation

Stéphane FOSSE
fosse.fr

15 décembre 2025

Entre 2006 et 2014, une législation européenne a imposé aux fournisseurs de services de télécommunications de l'Union européenne l'obligation de collecter et conserver systématiquement les données de communication de l'ensemble de leurs utilisateurs. Cette Directive 2006/24/CE, dite « Directive sur la conservation des données » (Data Retention Directive), représente l'une des tentatives les plus controversées de l'Union européenne d'encadrer la lutte contre le terrorisme et la criminalité organisée. Son histoire illustre la tension permanente entre impératifs sécuritaires et protection des droits fondamentaux dans les démocraties modernes.

Contexte d'adoption : l'ère post-11 septembre

L'adoption de cette directive s'inscrit dans un contexte marqué par une profonde transformation des politiques sécuritaires occidentales. Après les attentats du 11 septembre 2001, puis ceux de Madrid en 2004 et de Londres en 2005, les gouvernements européens ont cherché à se doter de nouveaux outils pour prévenir et enquêter sur les activités terroristes. Les Conclusions du Conseil Justice et Affaires intérieures du 19 décembre 2002 soulignaient déjà que les données relatives à l'utilisation des communications électroniques constituaient un outil précieux pour la prévention, l'investigation, la détection et la poursuite des infractions pénales, en particulier de la criminalité organisée.

La Déclaration sur la lutte contre le terrorisme adoptée par le Conseil européen le 25 mars 2004 a donné instruction au Conseil d'examiner des mesures visant à établir des règles sur la conservation des données de trafic de communication par les fournisseurs de services. Suite aux attentats de Londres du 13 juillet 2005, le Conseil a réaffirmé, dans sa déclaration condamnant ces attaques, la nécessité d'adopter au plus vite des mesures communes sur la conservation des données de télécommunications.

Cette période marque un tournant où la volonté de sécurité collective semble avoir pris le pas sur la protection de la vie privée individuelle, transformant progressivement la surveillance d'exception en surveillance généralisée.

Une obligation de conservation généralisée

La Directive 2006/24/CE, adoptée le 15 mars 2006 par le Parlement européen et le Conseil, imposait aux États membres d'obliger les fournisseurs de services de communication électroniques accessibles au public et les exploitants de réseaux publics de communications à conserver certaines catégories de données générées ou traitées dans le cadre de la fourniture de leurs services.

L'objectif affiché était d'harmoniser les obligations des fournisseurs de services concernant la conservation de certaines données et de garantir que ces données soient disponibles aux fins d'investigation, de détection et de poursuite d'infractions graves, telles que définies par chaque État membre dans son droit national. La Directive visait à remédier aux divergences entre les législations nationales qui créaient des obstacles au marché intérieur des communications électroniques.

Quelles données devaient être conservées ?

La Directive imposait la conservation de métadonnées concernant toutes les communications électroniques, sans distinction entre citoyens ordinaires et suspects. Ces données comprenaient plusieurs catégories d'informations précises :

Pour la téléphonie fixe et mobile :

— Le numéro de téléphone appelant ;
— Le nom et l'adresse de l'abonné ou de l'utilisateur enregistré ;
— Les numéros composés (les numéros de téléphone appelés), y compris, dans les cas de services supplémentaires tels que le renvoi ou le transfert d'appel, les numéros vers lesquels l'appel est acheminé ;
— Les noms et adresses des abonnés ou utilisateurs enregistrés ;
— La date et l'heure du début et de la fin de la communication ;
— Le service téléphonique utilisé ;
— Les numéros de téléphone appelant et appelé ;
— L'identité internationale d'abonné mobile (IMSI) de la partie appelante ;
— L'identité internationale d'équipement mobile (IMEI) de la partie appelante ;
— L'IMSI de la partie appelée ;
— L'IMEI de la partie appelée ;
— Pour les services prépayés anonymes, la date et l'heure de l'activation initiale du service et l'identification de la cellule (Cell ID) à partir de laquelle le service a été activé ;
— L'identification de la cellule (Cell ID) au début de la communication ;
— Les données permettant d'identifier la localisation géographique des cellules en référence à leur identification (Cell ID) pendant la période de conservation des données de communication.

Pour l'accès à Internet, la messagerie électronique et la téléphonie par Internet :

— Les identifiants utilisateurs (user ID) attribués ;
— L'identifiant utilisateur et le numéro de téléphone attribués à toute communication entrant dans le réseau téléphonique public ;
— Le nom et l'adresse de l'abonné ou de l'utilisateur enregistré auquel une adresse de protocole Internet (IP), un identifiant utilisateur ou un numéro de téléphone a été attribué au moment de la communication ;
— L'identifiant utilisateur ou le numéro de téléphone du destinataire prévu d'un appel téléphonique par Internet ;
— Les noms et adresses de l'abonné ou des abonnés ou de l'utilisateur enregistré ou des utilisateurs enregistrés et l'identifiant utilisateur du destinataire prévu de la communication ;
— La date et l'heure de la connexion et de la déconnexion du service d'accès à Internet, sur la base d'un certain fuseau horaire, ainsi que l'adresse IP, dynamique ou statique, attribuée par le fournisseur de services d'accès à Internet à une communication, et l'identifiant utilisateur de l'abonné ou de l'utilisateur enregistré ;
— La date et l'heure de la connexion et de la déconnexion du service de messagerie électronique Internet ou de téléphonie par Internet, sur la base d'un certain fuseau horaire ;
— Le service Internet utilisé ;
— Le numéro de téléphone appelant pour l'accès commuté ;
— La ligne d'abonné numérique (DSL) ou autre point terminal de l'auteur de la communication.

Il faut souligner que la Directive excluait expressément la conservation du contenu des communications elles-mêmes. Néanmoins, comme l'a relevé la Cour de justice de l'Union européenne dans son arrêt d'invalidation, ces métadonnées, prises dans leur ensemble, permettaient de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de vie quotidienne, les lieux de résidence permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales et les milieux sociaux fréquentés.

Durée de conservation et accès aux données

L'Article 6 de la Directive stipulait que les États membres devaient veiller à ce que les catégories de données soient conservées pendant des périodes d'au moins six mois et d'au plus deux ans à compter de la date de la communication. L'Article 12 permettait même aux États membres, dans des circonstances particulières non spécifiées, de prolonger la période de conservation au-delà de deux ans.

Concernant l'accès à ces données, la Directive laissait une latitude considérable aux États membres. L'Article 4 disposait que les États membres devaient adopter des mesures pour garantir que les données conservées ne soient fournies qu'aux autorités nationales compétentes, dans des cas spécifiques et conformément au droit national. Les procédures à suivre et les conditions à remplir pour accéder aux données conservées conformément

aux exigences de nécessité et de proportionnalité devaient être définies par chaque État membre dans son droit national.

Cette formulation générique posait problème : la Directive ne précisait ni qui étaient exactement ces « autorités compétentes », ni quelles procédures strictes devaient encadrer l'accès aux données. En pratique, 14 États membres sur 28 ont inclus les agences de renseignement dans la définition des « autorités compétentes ». De plus, la notion d'« infraction grave » n'était pas définie au niveau européen, ce qui a conduit à des interprétations nationales très variables. Certains États membres ont adopté des listes spécifiques d'infractions graves, d'autres se sont référés à une durée minimale d'emprisonnement prévue par la loi, tandis que d'autres encore sont allés au-delà du champ d'application de la Directive en prescrivant des obligations de conservation de données et en accordant un accès complet aux autorités de sécurité publique même à des fins préventives.

Une atteinte disproportionnée aux droits fondamentaux

Dès son adoption, la Directive a suscité de vives contestations de la part d'organisations de défense des droits civiques, de défenseurs de la vie privée et d'une partie de la communauté juridique européenne. Les critiques portaient sur plusieurs aspects fondamentaux :

Une surveillance généralisée et indifférenciée

La Directive imposait la conservation de données relatives à toutes les communications électroniques sur le territoire de l'Union européenne, concernant tout individu utilisant un service de communication électronique accessible au public ou un réseau de communications public, sans qu'il soit nécessaire que ces personnes soient, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Comme l'ont souligné plusieurs juridictions nationales et la Cour de justice elle-même, cette conservation généralisée transformait chaque citoyen en suspect potentiel, inversant la présomption d'innocence.

La Cour constitutionnelle roumaine a ainsi relevé en 2009 que la conservation de données concernant tous les citoyens, indépendamment de toute implication dans des enquêtes criminelles, était susceptible de renverser la présomption d'innocence, transformant tous les utilisateurs de services de communication électronique en suspects potentiels.

Un potentiel de profilage massif

Même si la Directive excluait expressément le contenu des communications, les métadonnées conservées présentaient un potentiel de profilage considérable lorsqu'elles étaient combinées et contextualisées. Ces données, dans leur ensemble, permettaient de déduire des informations détaillées sur la vie privée des personnes : habitudes quotidiennes, lieux de résidence, déplacements, activités, relations sociales et environnements fréquentés.

La collecte et la conservation de tels volumes de données accroissaient également le risque de violations de la vie privée dues à une utilisation abusive ou à un accès non autorisé. La Directive n'imposait pas de prescriptions concernant l'emplacement physique des bases de données, qui pouvaient être librement situées à l'étranger, au-delà de la juridiction nationale et européenne.

L'absence de garanties procédurales suffisantes

La Directive ne prévoyait pas de critères objectifs permettant de délimiter l'accès aux données et leur utilisation ultérieure par les autorités nationales compétentes aux fins de la prévention, de la détection ou de la poursuite pénale d'infractions pouvant être considérées comme suffisamment graves pour justifier une telle ingérence dans les droits fondamentaux. Elle ne subordonnait pas l'accès des autorités nationales compétentes aux données conservées à un contrôle préalable effectué par une juridiction ou une entité administrative indépendante dont la décision vise à limiter l'accès auxdites données et leur utilisation à ce qui est strictement nécessaire.

De plus, la Directive ne comportait aucune obligation pour les États membres d'établir des garanties se rapportant aux normes minimales concernant la sécurité et la protection des données conservées par les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications.

Les contestations nationales

Plusieurs juridictions nationales ont exprimé leurs préoccupations quant à la compatibilité de la Directive et de ses législations nationales de transposition avec les droits fondamentaux. Les Cours suprêmes de Bulgarie et de Chypre, ainsi que les Cours constitutionnelles de Roumanie, d'Allemagne, de République tchèque et, après la décision de la CJUE, d'Autriche, ont examiné cette question.

La Cour constitutionnelle allemande, dans sa décision du 2 mars 2010, a adopté une position particulièrement remarquable. Elle a reconnu que la conservation des données pouvait être conforme aux droits fondamentaux garantis par la Loi fondamentale allemande si elle était intégrée dans une structure législative appropriée à l'ampleur de l'ingérence. Cependant, elle a constaté que les dispositions de transposition allemandes ne garantissaient ni une sécurité adéquate des données, ni une restriction adéquate des finalités d'utilisation des données, ni ne satisfaisaient aux exigences constitutionnelles de transparence et de protection juridique. La Cour a ainsi établi quatre critères qu'une législation proportionnée devrait respecter : des normes de sécurité des données proportionnées, une limitation proportionnée des finalités, la transparence et le contrôle judiciaire avec des recours juridiques effectifs.

La Cour constitutionnelle roumaine, la Cour constitutionnelle tchèque et la Cour suprême de Chypre ont également exprimé des réserves significatives, tout en évitant soigneusement un débat direct sur la légitimité de la Directive elle-même. Plutôt que de rejeter la Directive 2006/24, ces juridictions ont préféré concentrer leurs décisions sur les dispositions nationales de mise en œuvre, appliquant le test de proportionnalité uniquement aux lois nationales. Néanmoins, la Cour roumaine s'est distinguée en articulant un certain malaise à l'égard de la Directive sur la conservation des données, tandis que d'autres tribunaux ont préféré un dialogue « silencieux » et implicite avec les institutions européennes.

L'invalidation par la Cour de justice de l'Union européenne

Le 8 avril 2014, la Cour de justice de l'Union européenne, siégeant en Grande Chambre, a rendu un arrêt historique dans les affaires jointes C-293/12 et C-594/12 (Digital Rights Ireland Ltd contre Minister for Communications et Kärntner Landesregierung). La Cour a déclaré la Directive 2006/24/CE invalide dans son intégralité pour violation des droits fondamentaux garantis par la Charte des droits fondamentaux de l'Union européenne.

Cet arrêt faisait suite à des recours introduits en Irlande par Digital Rights Ireland Ltd, une société à responsabilité limitée qui promeut les libertés civiles et les droits humains en relation avec les technologies de communication, et en Autriche par plusieurs personnes contestant les mesures nationales de transposition de la Directive.

La reconnaissance d'une ingérence grave dans les droits fondamentaux

La Cour a d'abord reconnu que la conservation de données aux fins de permettre aux autorités nationales compétentes d'y avoir éventuellement accès satisfait un objectif d'intérêt général. Toutefois, elle a constaté que la Directive impliquait une ingérence d'une vaste ampleur et d'une gravité particulière dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire.

Même si la législation n'autorise pas la conservation du contenu d'une communication et ne porte donc pas atteinte à l'essence de ces droits, la conservation de données de trafic et de localisation pourrait néanmoins avoir un effet sur l'utilisation des moyens de communication électronique et, en conséquence, sur l'exercice par les utilisateurs de leur liberté d'expression, garantie à l'article 11 de la Charte.

La Cour a particulièrement souligné le caractère intrusif de cette conservation généralisée : « 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 vie quotidienne, les lieux de résidence 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. Le fait que les données soient conservées et exploitées ultérieurement, sans que l'abonné ou la personne enregistrée en soit informé, est de nature à générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante. »

Les manquements au principe de proportionnalité

La Cour a identifié plusieurs manquements graves au principe de proportionnalité :

Premièrement, la Directive couvre de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ou exception soit opérée en fonction de l'objectif de lutte contre les infractions graves. Elle ne prévoit aucune différenciation selon les personnes dont les données sont conservées, ni selon les circonstances ou le nombre de personnes concernées. Elle 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, avec des infractions graves. Elle ne prévoit pas d'exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel.

Deuxièmement, la Directive ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure. L'accès n'est pas subordonné à un contrôle préalable effectué par une juridiction ou une entité administrative indépendante dont la décision vise à limiter l'accès auxdites données et leur utilisation à ce qui est strictement nécessaire. Un tel contrôle préalable constitue une exigence à laquelle il ne peut être dérogé, sauf en cas d'urgence dûment justifiée.

Troisièmement, s'agissant de la durée de conservation, la Directive impose que les données soient conservées pendant une période d'au moins six mois, sans qu'aucune distinction soit opérée entre les catégories de données en fonction des personnes concernées ou de l'utilité éventuelle des données au regard de l'objectif poursuivi. Elle ne comporte pas d'éléments objectifs qui permettraient de s'assurer que la durée de conservation des données est limitée au strict nécessaire.

Quatrièmement, la Directive ne prévoit pas de garanties suffisantes permettant d'assurer une protection efficace des données contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données. Elle n'impose pas l'adoption de règles claires et strictes régissant la protection et la sécurité des données. Elle n'exige pas que les données soient conservées sur le territoire de l'Union, de sorte qu'il ne saurait être assuré que le contrôle, par les autorités de contrôle indépendantes, du respect des exigences de protection et de sécurité, tel qu'expressément requis par la Charte, soit pleinement garanti. Elle ne prévoit pas la destruction irréversible des données au terme de la période de conservation.

Sur la base de ces constats, la Cour a conclu que le législateur de l'Union avait excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7, 8 et 52, paragraphe 1, de la Charte.

Les conséquences de l'invalidation

L'invalidation de la Directive par la CJUE a eu des effets rétroactifs (c'est-à-dire depuis l'entrée en vigueur de la Directive) et s'impose à toutes les juridictions nationales de l'Union européenne. La décision constitue de facto une annulation et doit être considérée comme *erga omnes*, c'est-à-dire opposable à tous.

Lorsqu'une décision préjudicielle déclare une directive invalide, elle lie non seulement les institutions européennes, mais aussi les juridictions nationales. Conformément aux principes fondamentaux de la certitude juridique et de l'application uniforme du droit européen, ainsi qu'à l'article 51 de la Charte qui définit le champ d'application de celle-ci, la décision s'applique dans tous les États membres de l'Union européenne.

Toutefois, les conséquences pratiques de cette invalidation se sont avérées incertaines et variables selon les États membres. Alors que certains pays ont engagé une révision de leur réglementation nationale en matière de conservation des données ou ont même déclaré leurs lois nationales invalides, d'autres ont cherché des mesures alternatives pour continuer à conserver les données, ou n'ont pris aucune mesure concrète.

La Slovénie a ainsi déclaré sa loi nationale de conservation des données inconstitutionnelle en juillet 2014. En Allemagne et en Suède, la situation s'est révélée paradoxale : suite à l'arrêt de la Cour constitutionnelle allemande déclarant l'illégitimité des dispositions de transposition, la Commission européenne a lancé une procédure d'infraction contre l'Allemagne pour avoir refusé d'adopter une nouvelle transposition. De même, la Suède, l'un des derniers pays à avoir transposé la Directive, a été sanctionnée deux fois par la Commission européenne pour exécution incomplète de la Directive. Ces situations illustrent les contradictions dans lesquelles se sont trouvés certains États membres, pris entre leurs obligations européennes (à l'époque encore en vigueur), leurs juridictions nationales et les exigences de protection des droits fondamentaux.

Cette disparité de réactions a laissé les fournisseurs de services Internet dans un vide juridique, certains cessant la collecte de données d'abonnés malgré le maintien en vigueur des lois nationales de conservation des données. En Suède, quatre opérateurs de télécommunications ont ainsi cessé de stocker les données de leurs clients dès avril 2014.

La persistance des législations nationales et les clarifications ultérieures

L'invalidation de la Directive n'a pas automatiquement entraîné la disparition des législations nationales de transposition. La question était de savoir si ces lois nationales restaient applicables et, surtout, si elles étaient conformes au droit de l'Union européenne après l'invalidation de leur fondement juridique européen.

La réponse à cette question dépend en partie de l'application de la Directive 95/46/CE relative à la protection des données personnelles et de la Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. L'article 3, paragraphe 2, de la Directive 95/46/CE stipule qu'elle ne s'applique pas au traitement de données à caractère personnel effectué dans le cadre de mesures nationales concernant la sécurité publique. L'objectif des lois nationales de conservation des données étant la sécurité publique, on pourrait considérer qu'elles échappent au champ d'application de cette directive.

Cependant, une interprétation restrictive de cette exception pourrait être retenue : il ne suffit pas de déclarer qu'une mesure nationale poursuit l'objectif de la sécurité publique pour qu'elle échappe au champ d'application de la directive. Cette approche serait conforme à la jurisprudence de la CJUE dans des cas similaires où le droit primaire de l'Union vise à réaliser les objectifs des traités. Une telle approche pourrait également s'appliquer au niveau du droit dérivé de l'Union et donc au niveau de la directive relative à la protection des données, dans l'idée de réaliser l'objectif de la directive : l'harmonisation des lois nationales de protection des données en lien avec la promotion du marché intérieur.

Dans cette perspective, la Cour pourrait également appliquer le principe de proportionnalité et conclure que la clause d'exception de l'article 3, paragraphe 2, de la directive relative à la protection des données ne pourrait pas « justifier » les mesures nationales de conservation des données qui sont identiques à celles exigées par la Directive désormais invalide. Seules les mesures absolument nécessaires pour garantir la sécurité publique échapperaient au champ d'application de la directive. Dans le cas contraire, les lois nationales de transposition correspondantes de la directive relative à la protection des données et la directive elle-même exigeraient que tout traitement de données soit proportionné pour être conforme au droit de l'Union. Comme la CJUE l'a jugé le 8 avril 2014, ce n'est pas le cas en ce qui concerne la conservation des données de la manière concrète dont elle était exigée par la Directive sur la conservation des données.

Par conséquent, si les lois nationales de conservation des données n'avaient fait que transposer les règles de la Directive sans les critères supplémentaires établis par la CJUE, elles pourraient être conformes au droit constitutionnel national, mais violer simultanément le droit de l'Union européenne.

L'article 15, paragraphe 1, de la Directive 2002/58/CE, qui répète la formulation de l'article 13, paragraphe 1, de la Directive 95/46/CE, pourrait également conduire à une exception dans le cas de la conservation des données. Dans tous les cas, les mesures de conservation des données devraient probablement présenter un lien assez fort avec une menace concrète pour la sécurité publique afin de répondre aux critères de ces dispositions.

L'arrêt Tele2 Sverige et Watson de 2016

Le 21 décembre 2016, la Cour de justice de l'Union européenne a rendu un arrêt important dans les affaires jointes C-203/15 et C-698/15 (Tele2 Sverige AB contre Post- och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a.). Cet arrêt a clarifié et renforcé les principes établis dans l'arrêt Digital Rights Ireland.

La Cour a jugé que les États membres ne peuvent pas imposer aux fournisseurs de services une obligation de conservation généralisée et indifférenciée des données, même lorsqu'ils mettent en œuvre cette obligation pour des questions liées à la sécurité ou à la lutte contre la criminalité. La conservation des données doit être l'exception et non la règle, et ne peut être utilisée qu'avec de fortes garanties en raison de la violation très grave que constitue une telle conservation pour la vie privée.

Selon la CJUE, 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 quotidiennes, les lieux de résidence permanents ou temporaires, les déplacements quotidiens ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par elles.

La Cour a réaffirmé que la conservation des métadonnées constitue en soi une forme de surveillance, indépendamment de toute exploitation ultérieure de ces données : « Le fait que les données soient conservées sans que l'abonné ou la personne enregistrée en soit informé est susceptible de faire en sorte que les personnes concernées aient le sentiment que leur vie privée fait l'objet d'une surveillance constante. »

L'arrêt a également précisé que la Cour exige un contrôle préalable par une autorité indépendante. Il conviendrait de veiller à ce que ni la Commission nationale de contrôle des techniques de renseignement (CNCTR) — pour les questions de renseignement —, ni le Conseil d'État ne puissent être utilisés en France comme autorités de surveillance pseudo-indépendantes. Ces deux organisations, quelles que soient leurs bonnes intentions, ne présentent pas les garanties d'indépendance nécessaires.

La situation en France et en Europe en 2025

Plus de dix ans après l'invalidation de la Directive, la situation demeure complexe et fragmentée en Europe. Plusieurs États membres maintiennent des législations nationales de conservation des données, souvent en contradiction avec les principes établis par la CJUE.

En France, le groupe de travail politique « Les Exégètes Amateurs », qui englobe FDN, la fédération FFDN et La Quadrature du Net, a porté un recours devant le Conseil d'État contre la législation française, mais celui-ci a considéré que la France n'était pas concernée par la décision Digital Rights Ireland et a refusé de saisir officiellement la CJUE sur la question, malgré une demande explicite des Exégètes. La décision du 21 décembre 2016 a mis le Conseil d'État français face à ses contradictions et constitue une étape importante pour les affaires opposant les Exégètes et la France, ainsi que dans la lutte contre la surveillance de masse.

La France a adopté plusieurs lois de surveillance au cours des dernières années et a constamment refusé de se sentir concernée par les nombreux signaux envoyés par la plus haute juridiction européenne, même si ces signaux devenaient de plus en plus clairs. Au-delà de la question de la surveillance des citoyens par la conservation des données de connexion, il sera nécessaire d'examiner les pratiques du système judiciaire, qui recourt massivement à l'utilisation de ces données de connexion et de localisation, y compris dans des enquêtes qui ne sont pas liées à la criminalité grave ni au terrorisme.

En 2025, la Commission européenne a relancé le débat sur la conservation des données. Entre avril et juin 2025, elle a reçu plus de 5 000 réponses à son appel à contributions pour une évaluation d'impact concernant le rôle des règles de conservation des données au niveau de l'Union européenne. Nombre de ces réponses se sont fermement opposées à l'initiative de la Commission visant à relancer les obligations de conservation des données.

Selon la Commission, certaines métadonnées traitées par les fournisseurs de services sont nécessaires pour lutter efficacement contre la criminalité. En l'absence d'un cadre juridique européen obligeant les fournisseurs à conserver les métadonnées pendant une période raisonnable et limitée aux fins des procédures pénales, les données peuvent ne plus exister au moment où les autorités les demandent. L'absence de règles harmonisées de conservation des données pour les catégories clés de données a été identifiée par la police, les services de poursuite et les autorités judiciaires comme un défi substantiel pour les procédures pénales nationales dans les crimes se produisant en ligne et hors ligne, et entrave la coopération transfrontalière dans l'ensemble de l'Union.

La Commission envisage différentes options, notamment des mesures de droit souple (*soft law*) pour améliorer la coopération entre les autorités publiques et les fournisseurs de services de communication électroniques, telles que des normes communes au niveau européen pour la catégorisation des données, des formulaires pour demander et fournir des données, des lignes directrices sur les périodes minimales de conservation des données des abonnés et des adresses IP avec horodatage, et la coopération volontaire. Elle envisage également des mesures législatives établissant des exigences obligatoires pour tous les fournisseurs de services couverts par le Code européen des communications électroniques (EECC) concernant la conservation et l'accès aux données non-contenu, en conformité avec la jurisprudence existante de la Cour de justice de l'Union européenne.

La Commission devra néanmoins tenir dûment compte de la décision de la CJUE du 8 avril 2014 concernant la conservation des données vis-à-vis de la Charte des droits fondamentaux de l'Union européenne, en particulier le droit à la vie privée. Dans ce contexte, la Commission plaide pour que « conserver les métadonnées avec un objectif et une retenue peut devenir une pierre angulaire de la cybersécurité proactive. Cela peut contribuer à protéger non seulement les institutions mais aussi le citoyen ordinaire. »

Toutefois, de nombreux citoyens de l'Union ont exprimé avec force leurs préoccupations en matière de protection de la vie privée. L'évaluation d'impact est annoncée pour le premier trimestre 2026.

Conclusion : un équilibre précaire entre sécurité et liberté

L'histoire de la Directive sur la conservation des données illustre la tension fondamentale entre les impératifs de sécurité collective et la protection des droits fondamentaux dans les démocraties modernes. Adoptée dans le contexte anxiogène de l'après-11 septembre et des attentats terroristes en Europe, cette législation représentait une tentative de réponse sécuritaire face à des menaces perçues comme existentielles. Cependant, en imposant une surveillance généralisée et indifférenciée de l'ensemble de la population européenne, elle a franchi la limite de ce qui peut être considéré comme proportionné dans une société démocratique respectueuse des droits fondamentaux.

L'invalidation de la Directive par la Cour de justice de l'Union européenne en 2014 constitue un moment charnière dans la défense des droits numériques en Europe. En affirmant avec force que la collecte systématique de métadonnées de communication représente en soi une forme de surveillance, indépendamment de l'exploitation ultérieure de ces données, la CJUE a posé un principe fondamental : dans une démocratie, la surveillance doit être l'exception, ciblée et proportionnée, et non la règle généralisée.

Pourtant, plus d'une décennie après cette décision historique, le débat demeure vivace et les pratiques nationales continuent de diverger. Certains États membres maintiennent des législations de conservation des données qui semblent en contradiction avec les principes établis par la jurisprudence européenne. La France, en particulier, a multiplié les lois de surveillance ces dernières années et a souvent semblé ignorer les signaux répétés de la plus haute juridiction européenne.

Le défi qui se pose aujourd'hui aux législateurs, aux juridictions et aux citoyens européens est celui de la reconstruction : comment bâtir un système où l'équilibre des droits est respecté ? Comment protéger efficacement la sécurité publique sans transformer chaque citoyen en suspect potentiel ? Comment combattre le terrorisme et la criminalité grave tout en préservant les libertés fondamentales qui définissent nos sociétés démocratiques ?

Ces questions exigent l'invention de nouvelles méthodes, la recherche d'un nouvel équilibre, et surtout des choix politiques fondés sur la nécessité absolue de respecter les droits civils, y compris et surtout dans les périodes troublées où les décideurs politiques sacrifient volontiers ces droits fondamentaux au profit de politiques sécuritaires dont l'efficacité accrue grâce à la surveillance n'a jamais été démontrée.

Comme l'a souligné Philippe Aigrain, cofondateur de La Quadrature du Net, après l'arrêt de décembre 2016 : « Alors que nous avons vécu 15 années pendant lesquelles invoquer — souvent de manière trompeuse — la sécurité suffisait à justifier une atteinte permanente à l'État de droit, jusqu'à permettre que tout un chacun soit placé sous surveillance constante et omniprésente, la CJUE rappelle aux États membres le Droit. Nous nous efforcerons dans toutes nos actions — judiciaires avec les Exégètes Amateurs, et aussi politiques — de faire en sorte que personne ne l'oublie. »

L'initiative de la Commission européenne en 2025 de relancer le débat sur la conservation des données montre que cette question n'est pas close. Elle rappelle également la vigilance constante nécessaire pour protéger les droits fondamentaux face à la tentation permanente de la surveillance de masse, même lorsqu'elle est justifiée par des objectifs légitimes de lutte contre la criminalité et le terrorisme.

La véritable leçon de l'histoire de la Directive sur la conservation des données est peut-être celle-ci : dans une démocratie, la fin ne justifie pas tous les moyens. La sécurité collective ne peut être achetée au prix de la liberté individuelle, et toute ingérence dans les droits fondamentaux doit être strictement nécessaire, proportionnée et encadrée par des garanties procédurales robustes. C'est ce que la plus haute juridiction européenne a réaffirmé avec force, et c'est ce principe que les citoyens, les organisations de défense des droits civiques et les juridictions nationales doivent continuer à défendre avec détermination.

Références

[1] Arrêt de la Cour (Grande Chambre) du 8 avril 2014, Affaires jointes C-293/12 et C-594/12, Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources et autres, et Kärntner Landesregierung et autres. Arrêt. 8 avr. 2014.

[2] Bird & Bird. Time to revisit data retention. Insights. 27 juin 2025.

[3] Communications électroniques – Directive 2006/24/CE – Réseaux publics de communications – Conservation de données – Droit au respect de la vie privée. Arrêt. 8 avr. 2014.

[4] Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE. Directive. 15 mars 2006. 13.4.2006.

[5] La Quadrature du Net. Generalised data retention: a blow to mass surveillance! Anglais. Communiqué de presse. 22 déc. 2016.

[6] Sebastian Leuschner. Data retention: the directive is out. Are national laws next? 9 avr. 2014.

[7] NATO Cooperative Cyber Defence Centre of Excellence. EU Data Retention Directive Invalid. 2014.

[8] Arianna Vedaschi et Valerio Lubello. Data Retention and its Implications for the Fundamental Right to Privacy: A European Perspective. In : *Tilburg Law Review* 20 (2015), p. 14-34.