Fiche thématique conjointe

La surveillance de masse[1]
Jurisprudence de la CEDH et de la CJUE

(dernière mise à jour : 28/02/2025)

La présente fiche thématique a été préparée par le Greffe de la Cour européenne des droits de l'homme (« CEDH[2] ») et l'Agence des droits fondamentaux de l'Union européenne dans le cadre d'une collaboration visant à présenter la jurisprudence dans des domaines choisis dans lesquels le droit de l'Union européenne et de la Convention européenne des droits de l'homme (« CEDH » ou « Convention EDH ») interagissent.

I. La surveillance de masse

Les évolutions technologiques et sociales récentes dans le domaine des communications électroniques ont amené la CEDH et la CJUE à se pencher sur les risques que les dispositifs de surveillance de masse – des systèmes mettant en œuvre des moyens techniques permettant la collecte en masse d'informations issues de communications électroniques ou associées à de telles communications [3] – représentent pour les droits de l'homme.

À l'époque actuelle, où le numérique est de plus en plus présent, la grande majorité des communications se font sous forme numérique et sont acheminées à travers les réseaux mondiaux de télécommunication de manière à emprunter la combinaison de chemins la plus rapide et la moins chère sans aucun rapport significatif avec les frontières nationales. La surveillance qui ne vise pas directement les individus est par conséquent susceptible d'avoir une portée très large, tant à l'intérieur qu'à l'extérieur du territoire de l'État qui l'opère[4].

Le fonctionnement des régimes de surveillance de masse peut reposer sur la captation et la conservation de grandes quantités de données acheminées par les canaux de transmission des communications Internet (on parle alors d'interception en masse[5]). Ces régimes peuvent aussi imposer aux fournisseurs de services de communication la rétention et le stockage des communications de leurs utilisateurs et des données de communication associées[6], offrir aux autorités

[1] L'expression « surveillance de masse » employée dans cette fiche désigne « la surveillance généralisée des communications ». Les questions de terminologie sont examinées plus en détail dans le rapport intitulé *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update*, publié par l'Agence des droits fondamentaux de l'Union européenne en 2017 (p. 29). Voir aussi le rapport de la FRA intitulé *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU - 2023 update | European Union Agency for Fundamental Rights.*

[2] Le contenu de cette fiche ne lie pas la Cour.

[3] Le terme « information » englobe non seulement les informations recueillies par les services de renseignement, mais aussi les interceptions non ciblées d'informations opérées dans le cadre d'une procédure pénale.

[4] Voir Cour EDH, *Big Brother Watch et autres c. Royaume-Uni* [GC], n^{os} 58170/13 et 2 autres, § 322, 25 mai 2021, et *Centrum för rättvisa c. Suède* [GC], n° 35252/08, § 236, 25 mai 2021.

[5] Voir, par exemple, *Big Brother Watch*, précité, § 15, et, plus généralement, la jurisprudence mentionnée au paragraphe A ci-dessous.

[6] Voir, par exemple, Cour EDH, *Podchasov c. Russie*, n° 33696/19, 13 février 2024 et, plus généralement, la jurisprudence mentionnée au paragraphe B.

nationales un accès direct et illimité à ces données[7] ou leur permettre d'y accéder sur la base de demandes ciblées[8].

La surveillance de masse peut cibler le contenu de communications électroniques et/ou les données de communication associées, notamment les données personnelles des abonnés et utilisateurs enregistrés ainsi que les données relatives au trafic et les données de localisation. La captation de données de communications n'est pas par nature moins intrusive que la collecte de données de contenu, car les données relatives au trafic et les données de localisation, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données sont conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci[9]. S'agissant du contenu des communications électroniques, des questions particulières peuvent se poser lorsque l'interception en masse de communications, leur conservation et la possibilité d'y accéder habilitent les autorités à décrypter des messages électroniques cryptés[10].

II. La surveillance de masse dans la jurisprudence de la CJUE

La CJUE s'est penchée sur les régimes de surveillance de masse principalement sous l'angle de la protection accordée aux données personnelles et au droit à la vie privé par la directive « vie privée et communications électroniques[11] » et par le règlement général sur la protection des données (« RGPD[12] »), lus à la lumière des droits fondamentaux garantis par les articles 7 (droit au respect de la vie privée et familiale), 8 (protection des données personnelles) et 11 (liberté d'expression) de la Charte des droits fondamentaux de l'Union européenne (ci-après « la Charte[13] »).

Dans un certain nombre de cas particuliers, la CJUE a également donné des indications quant à l'interprétation d'autres instruments juridiques de l'UE lus à la lumière des droits fondamentaux susmentionnés, notamment dans les domaines de la coopération judiciaire en matière pénale, des décisions d'enquête européennes[14] et de la lutte contre les abus de marché[15].

---

[7] Voir, par exemple, Cour EDH, *Pietrzak et Bychawska-Siniarska et autres c. Pologne*, n[os] 72038/17 et 25237/18, 28 mai 2024.

[8] Voir, par exemple, Cour EDH, *Ben Faiza c. France*, n° 31446/12, 8 février 2018, et *Škoberne c. Slovénie*, n° 19920/20, 15 février 2024, ainsi que les arrêts respectivement rendus le 2 mars 2021 par la CJUE dans l'affaire *Prokuratuur*, C-746/18, EU:C:2021:152, le 5 avril 2022 dans l'affaire *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, et le 17 novembre 2022 dans l'affaire *Spetsializirana prokuratura*, C-350/21, EU:C:2022:896.

[9] CJUE, arrêt du 8 avril 2014, *Digital Rights Ireland e.a.*, C-293/12 et C 594/12, EU:C:2014:238, § 27, Cour EDH, *Big Brother Watch*, précité, § 342.

[10] CJUE, arrêt du 30 avril 2024, *M.N. (EncroChat)*, C-670/22, EU:C:2024:372, Cour EDH, *Podchasov c. Russie*, précité.

[11] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

[12] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

[13] Veuillez vous reporter à la jurisprudence de la CJUE mentionnée dans les sections C.1 et C.2. ci-dessous.

[14] Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale; voir CJUE, *M.N. (EncroChat)*, précité.

[15] Directive 2003/6/CE du Parlement européen et du Conseil du 28 janvier 2003 sur les opérations d'initiés et les manipulations de marché (abus de marché) et règlement (UE) n ° 596/2014 du Parlement européen et du Conseil

III. La surveillance de masse dans la jurisprudence de la CEDH

La CEDH s'est penchée sur les régimes de surveillance de masse principalement sous l'angle du droit au respect de la vie privée[16] et de la correspondance (article 8 de la CEDH) et de la liberté d'expression (article 10 de la CEDH) dans le domaine de la protection des communications des journalistes.

Sur le terrain de l'article 8 de la CEDH, la CEDH s'est appuyée sur sa jurisprudence relative aux régimes de surveillance secrète autorisant les mesures de surveillance ciblées[17] pour rappeler que dans le contexte particulier des mesures de surveillance secrète, l'exigence de « prévisibilité » veut que le droit interne soit suffisamment clair pour indiquer à tous de manière adéquate en quelles circonstances et sous quelles conditions la puissance publique est habilitée à recourir à pareilles mesures et qu'il définisse l'étendue et les modalités d'exercice du pouvoir d'appréciation accordé aux autorités compétentes avec une clarté suffisante pour fournir à l'individu une protection adéquate contre l'arbitraire[18].

La CEDH a également rappelé que lorsqu'une législation autorisant la surveillance secrète est contestée devant elle, elle doit vérifier en même temps que la mesure litigieuse était « prévue par la loi » et qu'elle était « nécessaire ». Elle a précisé que le droit national doit non seulement être accessible et prévisible dans son application, mais aussi garantir que les mesures de surveillance secrète soient appliquées uniquement lorsqu'elles sont « nécessaires dans une société démocratique », notamment en offrant des garanties et des garde-fous suffisants et effectifs contre les abus[19].

S'agissant des garanties que doit comporter un régime de surveillance de masse pour être compatible avec la Convention, la CEDH a estimé nécessaire de développer les garde-fous énoncés dans sa jurisprudence antérieure relative aux régimes d'interception ciblée et de les adapter pour prendre en compte les caractéristiques particulières de l'interception en masse de communications[20] ainsi que la conservation généralisée des données de communication et l'accès aux données en question[21].

S'agissant de l'article 10 de la CEDH, la CEDH s'est appuyée sur sa jurisprudence relative aux perquisitions au domicile ou sur le lieu de travail des journalistes en adaptant les garanties matérielles et procédurales qui y étaient énoncées au contexte de l'interception en masse[22] et de la conservation généralisée des données[23]. Elle a notamment établi une distinction entre les garanties devant caractériser un régime d'interceptions en masse conforme à la Convention lorsque sont en cause des ingérences intentionnelles dans la liberté d'expression des journalistes et les cas où les

---

du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché); voir CJUE, arrêt du 20 septembre 2022, *VD et SR*, C-339/20 et C-397/20, EU:C:2022:703.

[16] Appelée à statuer sur des ingérences dans le droit au respect de la vie privée résultant de régimes de surveillance de masse, la Cour s'est aussi appuyée sur d'autres instruments juridiques du Conseil de l'Europe, tels que la Convention de 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et le Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données du 8 novembre 2001, la recommandation du Comité des Ministres n° R (95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunication (adoptée le 7 février 1995) et le rapport sur le contrôle démocratique des services de sécurité adopté par la Commission européenne pour la démocratie par le droit.

[17] Voir, par exemple, Cour EDH, *Roman Zakharov c. Russie* ([GC], n° 47143/06, §§ 227-234, CEDH 2015, et la jurisprudence qui s'y trouve citée).

[18] Voir, par exemple, Cour EDH, *Big Brother Watch*, précité, § 333.

[19] *Ibidem*, § 334.

[20] Cour EDH, *Big Brother Watch*, précité, §§ 340-347, et *Centrum för rättvisa*, précité, §§ 254-261.

[21] Cour EDH, *Ekimdzhiev et autres c. Bulgarie*, n° 70078/12, §§ 394-395, 11 janvier 2022.

[22] Cour EDH, *Big Brother Watch*, précité, §§ 447-450.

[23] Cour EDH, *Big Brother Watch*, précité, §§ 524-525 et 528.

communications d'un journaliste ou les données de communication associées n'ont pas été délibérément sélectionnées pour examen et où il apparaît, au stade de l'examen, que les communications ou les données de communication associées contiennent des éléments journalistiques confidentiels[24].

IV. La jurisprudence de la Cour de justice de l'Union européenne (CJUE) et de la CEDH en matière de surveillance de masse

A. Les régimes d'interception en masse

CJUE, arrêt du 6 octobre 2020, *Privacy International*, C-623/17, EU:C:2020:790

En fait – Au début de l'année 2015, l'existence de pratiques de recueil et d'utilisation de données de communications en masse par les différents services de sécurité et de renseignement du Royaume-Uni fut rendue publique. La législation contestée autorisait le ministre de l'Intérieur à imposer aux fournisseurs de services de communications électroniques, lorsqu'il l'estimait nécessaire dans l'intérêt de la sécurité nationale ou des relations avec un gouvernement étranger, de transmettre aux services de sécurité et de renseignement des données de communications en masse (notamment des données relatives au trafic et des données de localisation ainsi que des informations sur les services utilisés). La transmission de ces données concernait l'ensemble des utilisateurs des moyens de communications électroniques. Une fois transmises, ces données étaient conservées par les services de sécurité et de renseignement et demeuraient à la disposition de ces derniers aux fins de leurs activités, à l'instar des autres bases de données qu'ils détenaient. En particulier, les données ainsi recueillies, qui étaient soumises à des traitements et à des analyses de masse et automatisés, pouvaient être recoupées avec d'autres bases de données comportant différentes catégories de données à caractère personnel en masse ou être divulguées hors de ces services et à des États tiers. Enfin, ces opérations n'étaient pas subordonnées à l'autorisation préalable d'une juridiction ou d'une autorité administrative indépendante et ne donnaient lieu à aucune information des personnes concernées.

Contestant la légalité de ces pratiques, Privacy International – une organisation non gouvernementale – saisit le Tribunal des pouvoirs d'enquête (*Investigatory Powers Tribunal*, « l'IPT »). Celui-ci estima que, puisque leur existence avait été reconnue, les régimes d'acquisition de données litigieux étaient conformes à l'article 8 de la CEDH. Il énonça toutefois quatre exigences, qui découlaient apparemment de l'arrêt rendu par la CJUE dans l'affaire Tele2 Sverige et Watson et autres, et qui semblaient aller au-delà des exigences de l'article 8 de la CEDH : la restriction de l'accès aux données de masse non ciblées, la nécessité d'une autorisation préalable (sauf en cas d'urgence dûment établie) à l'accès aux données, l'existence de mesures prévoyant l'information ultérieure des personnes concernées et la conservation de toutes les données sur le territoire de l'Union européenne.

Le 30 octobre 2017, l'IPT adressa une demande de décision préjudicielle à la CJUE, afin que celle-ci précise la mesure dans laquelle les exigences posées dans l'arrêt Watson seraient applicables dans le cas où l'acquisition de données en masse et le recours à des techniques de traitement automatisé seraient nécessaires pour protéger la sécurité nationale.

En droit – La CJUE a jugé qu'une réglementation nationale permettant à une autorité étatique d'imposer aux fournisseurs de services de communications électroniques de transmettre aux services de sécurité et de renseignement des données relatives au trafic et des données de

[24] Cour EDH, *Big Brother Watch*, précité, § 447.

localisation aux fins de la sauvegarde de la sécurité nationale relevait du champ d'application de la directive « vie privée et communications électroniques ». Elle a déclaré que l'interprétation de cette directive devait tenir compte des droits garantis par les articles 7, 8 et 11 de la Charte. Elle a précisé que les limitations à l'exercice de ces droits devaient être prévues par la loi, qu'elles devaient respecter le contenu essentiel desdits droits et le principe de proportionnalité, et qu'elles devaient être nécessaires et répondre effectivement à des objectifs d'intérêt général reconnus par l'UE ou au besoin de protection des droits et des libertés d'autrui. Elle a ajouté que les limitations à la protection des données à caractère personnel devaient s'opérer dans les limites du strict nécessaire et que, pour satisfaire à l'exigence de proportionnalité, une réglementation devait prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel étaient concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus.

La CJUE a jugé qu'une réglementation nationale imposant aux fournisseurs de services de communications électroniques de procéder à la communication par transmission généralisée et indifférenciée – touchant l'ensemble des utilisateurs de services de communications électroniques – des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement excédait les limites du strict nécessaire, et qu'elle ne pouvait être considérée comme étant justifiée au regard de la directive « vie privée et communications électroniques » lue à la lumière de la Charte.

CEDH, *Big Brother Watch et autres c. Royaume-Uni* [GC], n^{os} 58170/13 et 2 autres, 25 mai 2021

En fait – L'affaire portait sur la question de la compatibilité avec les articles 8 et 10 de la CEDH du régime britannique de surveillance secrète tel qu'applicable au 7 novembre 2017, qui encadrait :

I) l'interception en masse de données de contenu et des données de communication associées ;

II) la réception de renseignements provenant de services de renseignement étrangers ;

III) l'acquisition de données de communication auprès des fournisseurs de services de communication.

En droit – **Sur le point I) et l'article 8 de la CEDH:** les requérantes alléguaient que l'interception massive de communications transfrontalières par les services de renseignement emportait violation de l'article 8.

Sur la question de l'existence d'une ingérence, la CEDH a estimé que l'interception en masse était un processus graduel dans lequel l'intensité de l'ingérence dans l'exercice des droits protégés par l'article 8 augmentait au fur et à mesure de l'avancement du processus, qui comportait quatre étapes :

a) l'interception et la rétention initiale des communications et des données de communication associées;

b) l'application de sélecteurs spécifiques aux communications retenues et aux données de communication associées;

c) l'examen par des analystes des communications sélectionnées et des données de communication associées ; et

d) la rétention subséquente des données et l'utilisation du « produit final », notamment le partage de ces données avec des tiers.

La CEDH a précisé que si l'interception suivie de l'élimination immédiate d'une partie des communications ne constituait pas une ingérence particulièrement importante, l'intensité de l'ingérence dans l'exercice des droits protégés par l'article 8 augmentait au fur et à mesure de la progression du processus d'interception en masse.

S'agissant des principes applicables aux affaires portant sur l'interception en masse, la CEDH a jugé que les États jouissent d'une ample marge d'appréciation pour déterminer de quel type de système d'interception ils ont besoin pour protéger la sécurité nationale ou d'autres intérêts nationaux essentiels contre des menaces extérieures graves, mais elle a estimé que la latitude qui leur est accordée pour la mise en œuvre de ce régime doit être plus restreinte et qu'un certain nombre de garanties doivent être mises en place. Elle a considéré que les garanties applicables aux régimes d'interceptions ciblées doivent être adaptées pour prendre en compte les caractéristiques particulières de l'interception en masse et, en particulier, l'intensité croissante de l'ingérence dans l'exercice par les individus de leurs droits protégés par l'article 8 au fur et à mesure que l'opération passe par les étapes décrites ci-dessus.

Pour déterminer si l'État défendeur avait agi dans les limites de sa marge d'appréciation, la CEDH a examiné conjointement les critères selon lesquels la mesure devait être « prévue par la loi » et « nécessaire », et elle a recherché si le cadre juridique national définissait clairement :

1. Les motifs pour lesquels l'interception en masse pouvait être autorisée ;
2. Les circonstances dans lesquelles les communications d'un individu pouvaient être interceptées ;
3. La procédure d'octroi d'une autorisation ;
4. Les procédures à suivre pour la sélection, l'examen et l'utilisation des éléments interceptés ;
5. Les précautions à prendre pour la communication de ces éléments à d'autres parties ;
6. Les limites posées à la durée de l'interception et de la conservation des éléments interceptés, et les circonstances dans lesquelles ces éléments devaient être effacés ou détruits;
7. Les procédures et modalités de supervision, par une autorité indépendante, du respect des garanties énoncées ci-dessus, et les pouvoirs de cette autorité en cas de manquement ;
8. Les procédures de contrôle indépendant *a posteriori* du respect des garanties et les pouvoirs conférés à l'organe compétent pour traiter les cas de manquement.

S'agissant en particulier des précautions à prendre pour la communication d'éléments interceptés à des tiers, la CEDH a précisé que la transmission de tels éléments à des États étrangers ou à des organisations internationales doit être limitée aux éléments recueillis et conservés d'une manière conforme à la Convention, et qu'elle doit être soumise à certaines garanties supplémentaires relatives au transfert lui-même. Premièrement, les circonstances dans lesquelles pareil transfert peuvent avoir lieu doivent être clairement énoncées dans le droit interne. Deuxièmement, l'État opérant un transfert des informations en question doit s'assurer que l'État destinataire a mis en place, pour la gestion des données, des garanties de nature à prévenir les abus et les ingérences disproportionnées. L'État destinataire doit, en particulier, garantir la conservation sécurisée des données et restreindre leur divulgation à des tiers, étant entendu que cela ne signifie pas nécessairement qu'il doive garantir une protection comparable à celle de l'État qui transfère les informations, ni qu'une assurance doive être donnée avant chaque transfert. Troisièmement, des garanties renforcées sont nécessaires lorsqu'il est clair que les éléments transférés appellent une confidentialité particulière – par exemple s'il s'agit de communications journalistiques confidentielles. Enfin, le transfert d'informations à des partenaires de renseignement étrangers doit également être soumis à un contrôle indépendant.

S'agissant des précautions à prendre pour l'acquisition des données de communication associées dans le cadre d'une interception en masse, la CEDH a relevé que les données en question peuvent faire l'objet d'analyses et de recherches qui permettent de brosser un portrait intime de la personne concernée par le suivi de ses activités sur les réseaux sociaux, de ses déplacements, de ses navigations sur Internet ainsi que de ses habitudes de communication, et par la connaissance de ses contacts. Elle a considéré que l'interception et la conservation des données de communication associées, ainsi que les recherches effectuées sur celles-ci, doivent être analysées au regard des mêmes garanties que celles applicables au contenu des communications, mais qu'il n'est pas nécessaire que les dispositions juridiques régissant le traitement des données de communication associées soient identiques en tous points à celles régissant le traitement du contenu des communications.

Après avoir appliqué les principes susmentionnés au cas d'espèce, la CEDH a considéré que le régime britannique de surveillance secrète ne renfermait pas suffisamment de garanties « de bout en bout » pour offrir une protection adéquate et effective contre l'arbitraire et le risque d'abus, en dépit des garde-fous qu'il comportait. Elle a relevé notamment que ce régime présentait des lacunes fondamentales, à savoir l'absence d'autorisation indépendante, l'absence de mention des catégories de sélecteurs dans les demandes de mandat et le fait que les sélecteurs liés à un individu n'étaient pas soumis à une autorisation interne préalable. Elle a jugé que ces insuffisances affectaient non seulement l'interception du contenu des communications, mais aussi l'interception des données de communication associées. Elle a précisé que si la supervision indépendante et effective exercée sur le régime par le Commissaire à l'interception des communications et le recours juridictionnel solide que l'IPT offrait à toutes les personnes pensant que leurs communications avaient été interceptées par les services de renseignement constituaient des garanties importantes, celles-ci n'étaient pas suffisantes pour contrebalancer les lacunes susmentionnées.

Sur le point I) et l'article 10: les requérantes alléguaient que le régime d'interception de communications en masse était contraire à l'article 10 en ce qu'il avait selon elles un effet dissuasif sur la liberté de communication des journalistes.

La CEDH a opéré une distinction entre l'hypothèse d'un accès intentionnel des services de renseignement à des éléments journalistiques confidentiels au moyen de l'utilisation délibérée de sélecteurs ou de termes de recherche liés à un journaliste ou à un organe de presse et celle d'un accès fortuit découlant de la prise accidentelle de tels éléments dans les « filets » d'une interception en masse. Elle a considéré que l'ingérence qui se manifestait dans la première hypothèse était comparable à celle qui aurait résulté d'une perquisition au domicile ou sur le lieu de travail d'un journaliste, et elle a déclaré que ces sélecteurs ou termes de recherche devaient avoir été autorisés par un juge ou un autre organe décisionnel indépendant et impartial habilité à déterminer si cette mesure était « justifiée par un impératif prépondérant d'intérêt public » et, en particulier, si une mesure moins intrusive aurait suffi à satisfaire un tel impératif. S'agissant de la seconde hypothèse, la CEDH a déclaré qu'il était impossible de prévoir d'emblée l'importance de l'atteinte portée à ces communications et/ou sources journalistiques, et qu'un juge ou un autre organe indépendant n'était donc pas en mesure de déterminer, au stade de l'autorisation, si une telle atteinte était ou non justifiée. Elle a toutefois précisé que la surveillance qui ne visait pas directement les individus était susceptible d'avoir une portée très large compte tenu des progrès technologiques. L'examen de communications journalistiques ou de données de communication associées par un analyste pouvant conduire à l'identification d'une source, la CEDH a estimé que le droit interne devait impérativement comporter des garanties solides en ce qui concerne la conservation, l'examen, l'utilisation, la transmission à des tiers et la destruction de ces éléments confidentiels.

La CEDH a également considéré que lorsqu'il apparaît que des communications journalistiques ou des données de communication associées contiennent des éléments journalistiques confidentiels, la prolongation de leur conservation et la poursuite de leur examen par un analyste ne doivent être

possibles qu'à la condition d'être autorisées par un juge ou un autre organe décisionnel indépendant et impartial habilité à déterminer si ces mesures sont « justifiées par un impératif prépondérant d'intérêt public ».

Après avoir appliqué les principes susmentionnés au cas d'espèce, la CEDH a jugé que les garanties prévues par le régime juridique britannique encadrant la conservation, la transmission à des tiers et la destruction des éléments journalistiques confidentiels étaient adéquates, mais qu'elles ne remédiaient pas aux lacunes mises en évidence par elle dans son analyse du régime litigieux sous l'angle de l'article 8 et ne satisfaisaient pas non plus à l'exigence selon laquelle l'utilisation de sélecteurs ou de termes de recherche dont on savait qu'ils étaient liés à un journaliste devait être autorisée par un juge ou un autre organe décisionnel indépendant et impartial habilité à déterminer si cette mesure était « justifiée par un impératif prépondérant d'intérêt public » et si une mesure moins intrusive aurait suffi à satisfaire un tel impératif. En outre, la CEDH a estimé que le régime litigieux ne comportait pas de garde-fous suffisants garantissant que lorsqu'il apparaissait que des communications n'ayant pas été sélectionnées pour examen par l'utilisation délibérée d'un sélecteur ou d'un terme de recherche dont on savait qu'il était lié à un journaliste contenaient malgré tout des éléments journalistiques confidentiels, la prolongation de leur conservation et la poursuite de leur examen par un analyste ne seraient possibles qu'à la condition d'être autorisées par un juge ou un autre organe décisionnel indépendant et impartial habilité à déterminer si ces mesures étaient « justifiées par un impératif prépondérant d'intérêt public ».

Sur le point II) et l'article 8: les requérantes se plaignaient essentiellement de la réception, par les autorités internes, d'éléments interceptés demandés à des services de renseignement étrangers.

La CEDH a estimé que les demandes d'éléments interceptés adressées aux États non contractants devaient avoir une base en droit interne, être accessibles à la personne concernée et prévisibles quant à leurs effets, et que l'échange de renseignements devait être encadré par des normes claires et précises indiquant à tous de manière suffisante en quelles circonstances et sous quelles conditions les autorités étaient habilitées à formuler de telles demandes et offrant des garanties effectives contre l'utilisation de ce pouvoir à des fins de contournement du droit interne et/ou des obligations imposées aux États par la CEDH.

La CEDH a déclaré que dès la réception des éléments interceptés, l'État destinataire devait avoir mis en place des garanties suffisantes pour leur examen, leur utilisation, leur conservation, leur transmission à des tiers, leur effacement et leur destruction, et que tout régime autorisant des services de renseignements à demander à des États non contractants de procéder à une interception ou de leur transmettre des éléments interceptés devait être soumis à une supervision indépendante et devait également prévoir la possibilité d'un contrôle *a posteriori* indépendant.

Après avoir appliqué les principes susmentionnés au cas d'espèce, la CEDH a observé que le cadre juridique mis en place au Royaume-Uni comportait des normes claires et précises indiquant à tous de manière suffisante en quelles circonstances et sous quelles conditions les autorités étaient habilitées à demander des éléments interceptés à un service de renseignement étranger, que le droit interne offrait des garanties effectives contre l'utilisation de pareilles demandes à des fins de contournement de ses dispositions et/ou des obligations imposées au Royaume-Uni par la CEDH, que les garanties instaurées par le Royaume-Uni pour l'examen, l'utilisation, la conservation, la transmission à des tiers, l'effacement et la destruction des éléments en question étaient adéquates, que le régime en cause était soumis à la supervision indépendante du Commissaire à l'interception des communications et qu'il pouvait faire l'objet d'un contrôle *a posteriori* exercé par l'IPT.

Sur le point II) et l'article 10: les requérantes alléguaient que le régime d'échange de renseignements emportait violation de leurs droits tels que garantis par l'article 10. La CEDH a jugé

que ce grief ne soulevait aucune question distincte ou supplémentaire par rapport à celui fondé sur l'article 8.

Sur le point III): veuillez vous reporter au paragraphe C ci-dessous.

Conclusion – Violation des articles 8 et 10 de la CEDH concernant l'interception en masse. Non-violation des articles 8 et 10 de la CEDH concernant la réception de renseignements provenant de services de renseignement étrangers.

CEDH, *Centrum för rättvisa c. Suède* [GC], n° 35252/08, 25 mai 2021

En fait – L'affaire portait sur la compatibilité du régime suédois encadrant le renseignement d'origine électromagnétique tel qu'applicable en mai 2018, et plus précisément l'interception en masse du contenu des communications avec l'étranger et des données de communication associées.

La requérante alléguait principalement que la législation et la pratique internes relatives à l'interception en masse de communications emportaient violation de l'article 8 de la CEDH.

En droit – Après avoir appliqué les principes posés dans l'arrêt *Big Brother Watch* (précité), la CEDH a estimé que les caractéristiques principales du régime suédois d'interception en masse répondaient aux exigences de la CEDH relatives à la qualité de la loi, et elle a jugé que le fonctionnement dudit régime demeurait dans la plupart de ses aspects dans les limites de ce qui était « nécessaire dans une société démocratique ». Toutefois, elle a constaté que ce régime présentait trois carences, à savoir l'absence de règle claire concernant la destruction des éléments interceptés ne contenant pas de données à caractère personnel, le fait que la loi pertinente ne prévoyait pas l'obligation de prendre en compte les intérêts liés à la vie privée lors de l'adoption d'une décision de transfert de renseignements au profit de partenaires étrangers et l'absence d'un contrôle *a posteriori* effectif.

Conclusion – Violation de l'article 8 de la CEDH.

CEDH, *Wieder et Guarnieri c. Royaume-Uni*, n^{os} 64371/16 et 64407/16, 12 septembre 2023

En fait – Les requérants, qui résidaient hors de l'État défendeur, se plaignaient principalement du régime britannique d'interception en masse, qu'ils estimaient incompatible avec l'article 8 de la CEDH.

En droit – La principale question juridique qui se posait dans cette affaire consistait à savoir si des personnes résidant hors d'un État contractant désireuses de faire valoir un grief tiré de l'article 8 relevaient de la juridiction de celui-ci à partir du moment où leurs communications électroniques étaient (ou risquaient d'être) interceptées, analysées et examinées par les services de renseignement de cet État opérant à l'intérieur de ses frontières.

Estimant que l'interception, l'analyse, l'examen et l'utilisation de ces communications portaient clairement atteinte à leur confidentialité et qu'il en résultait aussi une atteinte au droit au respect de la vie privée, la CEDH a jugé que l'ingérence dans l'exercice, par les requérants, de leurs droits tels que garantis par l'article 8 relevait de la juridiction territoriale de l'État défendeur.

S'agissant du fond du grief dont elle était saisie, la CEDH a renvoyé aux conclusions auxquelles elle était parvenue dans l'arrêt *Big Brother Watch* (précité).

Conclusion – Violation de l'article 8 de la CEDH.

CJUE, arrêt du 30 avril 2024, *M.N. (EncroChat)*, C-670/22, EU:C:2024:372

En fait – Dans le cadre d'une enquête menée par les autorités françaises, il apparut que des personnes poursuivies utilisaient des téléphones portables cryptés qui fonctionnaient sous une licence dénommée « EncroChat » pour commettre des infractions principalement liées au trafic de stupéfiants. Ces téléphones portables permettaient, grâce à un logiciel spécial et à un matériel modifié, d'établir une communication chiffrée de bout en bout qui n'était pas susceptible d'être interceptée par des méthodes d'enquête traditionnelles (le « service EncroChat »). Avec l'autorisation d'un juge, un logiciel de type « cheval de Troie » fut installé sur un serveur au printemps de l'année 2020 et, de là, sur lesdits téléphones portables au moyen d'une mise à jour simulée. 32477 utilisateurs, sur un total de 66134 utilisateurs inscrits, répartis dans 122 pays, auraient été concernés par ledit logiciel, dont environ 4600 en Allemagne. Les représentants des autorités françaises et néerlandaises informèrent les représentants des autorités des autres États membres de l'enquête qu'ils menaient. Les représentants des autorités allemandes manifestèrent leur intérêt pour les données des utilisateurs allemands. La police allemande annonça ouvrir une enquête contre un ensemble inconnu d'utilisateurs du service EncroChat pour trafic organisé présumé de stupéfiants en quantité non négligeable et association de malfaiteurs. Le 2 juin 2020, le parquet général de Francfort demanda aux autorités françaises, au moyen d'une première décision d'enquête européenne, l'autorisation d'utiliser les données issues du service EncroChat dans des procédures pénales.

Dans le cadre de la procédure pénale engagée contre M.N., la juridiction de renvoi a posa une question préjudicielle portant sur un certain nombre d'aspects procéduraux et matériels de la compatibilité des décisions d'enquête européenne avec le droit de l'UE, demandant si, et le cas échéant dans quelles conditions l'article 6 § 1 directive concernant la décision d'enquête européenne s'opposait à ce que le parquet adopte une décision d'enquête européenne visant la transmission de preuves déjà en la possession des autorités compétentes de l'État d'exécution, lorsque ces preuves avaient été acquises à la suite de l'interception, par ces autorités, sur le territoire de l'État d'émission, de télécommunications de l'ensemble des utilisateurs de téléphones portables qui permettaient, grâce à un logiciel spécial et à un matériel modifié, une communication chiffrée de bout en bout.

En droit – La CJUE a jugé que la légalité des décisions d'enquête européenne est soumise aux mêmes conditions que celles applicables, le cas échéant, à la transmission de telles données dans une situation purement interne à l'État d'émission. Par conséquent, si le droit de l'État d'émission subordonne cette transmission à l'existence d'indices concrets de commission d'infractions graves par la personne poursuivie ou à l'admissibilité des preuves que constituent les données en cause, l'adoption d'une décision d'enquête européenne est soumise à l'ensemble de ces mêmes conditions. En revanche, l'article 6 § 1 b) de la directive concernant la décision d'enquête européenne n'exige pas, y compris dans une situation telle que celle en cause au principal, où les données en question avaient été collectées par les autorités compétentes de l'État d'exécution sur le territoire de l'État d'émission et dans l'intérêt de celui-ci, que l'émission d'une décision d'enquête européenne visant à la transmission de preuves déjà en la possession des autorités compétentes de l'État d'exécution soit soumise aux mêmes conditions de fond que celles appliquées, dans l'État d'émission, en matière de collecte de ces preuves.

À cet égard, la CJUE a rappelé que la décision d'enquête européenne est un instrument relevant de la coopération judiciaire en matière pénale, laquelle est fondée sur le principe de reconnaissance mutuelle des jugements et des décisions judiciaires ainsi que sur la présomption réfragable que les autres États membres respectent le droit de l'Union et, en particulier, les droits fondamentaux. Il

s'ensuit que l'autorité qui émet une décision d'enquête européenne n'est pas autorisée à contrôler la régularité de la procédure distincte par laquelle l'État membre d'exécution a collecté les preuves dont elle demande la transmission.

La CJUE a également rappelé que l'article 14 § 1 de la directive 2014/41 impose aux États membres de veiller à ce que des voies de recours équivalentes à celles ouvertes dans le cadre d'une procédure nationale similaire soient applicables à la mesure d'enquête faisant l'objet d'une décision d'enquête européenne et que, dans ce cadre, il appartient à la juridiction compétente de contrôler le respect des conditions d'émission d'une telle décision en s'assurant qu'elle est nécessaire et proportionnée aux finalités de la procédure ouverte dans l'État d'émission et que les mesures d'enquête indiquées dans la décision d'enquête européenne auraient pu être ordonnées dans les mêmes conditions dans le cadre d'une procédure nationale similaire.

Enfin, la CJUE a jugé que dans le cadre d'une procédure pénale ouverte contre une personne soupçonnée d'actes de criminalité, les juridictions pénales nationales doivent écarter des informations et des éléments de preuve obtenus au moyen d'une décision d'enquête européenne si cette personne n'est pas en mesure de commenter efficacement ces informations ainsi que ces éléments de preuve et que ceux-ci sont susceptibles d'influencer de manière prépondérante l'appréciation des faits.

CEDH, *A.L. et E.J. c. France (déc.)*, n^{os} 44715/20 et 47930/21, 24 septembre 2024

En fait – Les requêtes portaient sur la captation, par les autorités françaises, de données relatives à des utilisateurs de téléphones mobiles équipés d'Encrochat et sur le transfert de ces données aux forces de l'ordre britanniques. Les requérants firent l'objet de poursuites pénales au Royaume-Uni dans deux affaires distinctes, dans le cadre desquelles l'usage d'EncroChat leur fut reproché. Devant la CEDH, ils invoquaient l'article 8, pris isolément et combiné avec les articles 13 et 6 de la Convention.

En droit – S'appuyant sur les principes posés dans l'arrêt *Wieder et Guarnieri*, (précité), la CEDH a constaté que la captation, la conservation et la transmission des données litigieuses aux autorités britanniques avaient été menées depuis le territoire français. Elle en a déduit que l'État défendeur était territorialement compétent pour connaître de l'atteinte portée aux droits des requérants tels que garantis par l'article 8. Elle a souligné que cette conclusion se conciliait avec la jurisprudence de la CJUE (*M.N. (EncroChat)*, précité) selon laquelle le principe de reconnaissance mutuelle des jugements et des décisions judiciaires interdit aux autorités ayant émis une décision d'enquête européenne de contrôler la régularité de la procédure distincte par laquelle les preuves dont la transmission est demandée ont été collectées dans l'État d'exécution.

S'agissant de l'épuisement des voies de recours internes, la CEDH a jugé que ni la circonstance que les requérants résidaient hors du territoire français ni la circonstance qu'ils n'aient pas choisi de leur plein gré de se placer sous la juridiction de l'État défendeur n'étaient de nature à les exempter de leur obligation d'épuiser les voies de recours internes ouvertes dans cet État. Elle a constaté que l'ordre juridique interne contenait des dispositions transposant l'article 14 de la directive 2014/41, qui prévoit que les États membres doivent veiller à ce que des voies de recours équivalentes à celles ouvertes dans le cadre d'une procédure nationale similaire soient applicables aux mesures d'enquête indiquées dans une décision d'enquête européenne, et elle a observé que ces dispositions paraissaient se concilier de façon cohérente avec la jurisprudence de la CJUE selon laquelle les États membres sont tenus d'assurer le respect du droit à un recours effectif consacré à l'article 47 de la Charte dans le cadre de la procédure d'émission et d'exécution d'une décision d'enquête européenne. Notant que, selon le droit interne, le versement au dossier d'une procédure pénale d'éléments de preuves obtenus dans le cadre d'une procédure distincte était un acte

susceptible d'être contesté par la personne mise en examen, qui pouvait notamment invoquer la violation des droits garantis par la Convention, elle a constaté que pareil recours était ouvert aux requérants, qui auraient pu demander l'annulation de la mesure d'exécution de la décision d'enquête européenne litigieuse dans les mêmes conditions et selon les mêmes modalités qu'aurait pu le faire une personne mise en examen en France, notamment en invoquant l'article 8 de la Convention.

La CEDH a jugé que les requérants avaient disposé d'un recours effectif. Pour se prononcer ainsi, elle a également observé que l'article 14 § 7 de la directive 2014/41 impose à l'État d'émission de tenir compte du fait qu'une décision d'enquête européenne a été contestée avec succès et que, dès lors que les poursuites diligentées à l'encontre des requérants étaient toujours pendantes, les juridictions répressives britanniques étaient contraintes de tenir compte du succès éventuel d'un tel recours devant les juridictions françaises.

Conclusion – Irrecevabilité des griefs fondés sur l'article 8 de la Convention pour non-épuisement des voies de recours internes; irrecevabilité des griefs fondés sur les articles 6 et 13 de la Convention pour défaut manifeste de fondement.

B. Les obligations des fournisseurs de services de communication relatives à la conservation des données et l'accès ciblé par les autorités nationales

B. 1. Données d'abonnés

CJUE, arrêt du 2 octobre 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788

En fait – Dans le cadre d'une enquête sur le vol d'un portefeuille et d'un téléphone mobile, la police espagnole demanda à un juge d'instruction l'autorisation d'accéder aux données visant à l'identification des titulaires de numéros de téléphone activés avec le téléphone mobile volé pendant une période de douze jours à compter de la date du vol. Le juge d'instruction rejeta cette demande, au motif notamment que les actes à l'origine de l'enquête ne constituaient pas des infractions « graves ».

Par la suite, la juridiction de renvoi sollicita l'avis de la CJUE sur la fixation du seuil de gravité des infractions susceptibles de justifier une ingérence dans les droits fondamentaux.

En droit – La CJUE a jugé que l'article 15 § 1 de la directive « vie privée et communications électroniques », lu à la lumière des articles 7 et 8 de la Charte, doit être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, s'analyse en une ingérence dans les droits fondamentaux de ces derniers qui ne présente pas une gravité telle que cet accès doit être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave. Elle a notamment observé que, conformément au principe de proportionnalité, une ingérence grave ne peut être justifiée, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, que par un objectif de lutte contre la criminalité devant également être qualifiée de « grave ». En revanche, lorsque l'ingérence que comporte un tel accès n'est pas grave, ledit accès est susceptible d'être justifié par un objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général. La CJUE a estimé que l'accès aux données visées par la demande ne constituait pas une ingérence particulièrement grave, car les données en question permettaient uniquement de mettre en relation, pendant une période déterminée, les cartes SIM activées avec le téléphone mobile volé avec l'identité des titulaires de ces cartes SIM.

Elle a observé que sans un recoupement avec les données afférentes aux communications effectuées avec lesdites cartes SIM et les données de localisation, ces données ne permettaient de connaître ni la date, l'heure, la durée et les destinataires des communications effectuées avec les cartes SIM en cause, ni les endroits où ces communications avaient eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée. Lesdites données ne permettaient donc pas de tirer de conclusions précises concernant la vie privée des personnes dont les données étaient concernées.

CEDH, *Breyer c. Allemagne*, n° 50001/12, 30 janvier 2020

En fait – Invoquant principalement l'article 8 de la Convention (droit au respect de la vie privée), les requérants se plaignaient de ce que, en tant qu'utilisateurs de cartes SIM prépayées pour téléphone mobile, certaines données à caractère personnel les concernant (leur numéro de téléphone, leur nom et adresse ainsi que leur date de naissance et la date de conclusion de leur contrat) avaient été stockées par leurs fournisseurs de services de télécommunication respectifs en application d'une obligation légale entrée en vigueur le 1er janvier 2008.

En droit – La CEDH a rappelé sa jurisprudence bien établie relative aux ingérences dans le droit au respect de la vie privée garanti par l'article 8 résultant de la conservation, du traitement et de l'utilisation de données à caractère personnel (citant notamment l'arrêt *Ben Faiza c. France*, n° 31446/12, 8 février 2018).

S'agissant de la justification de l'ingérence, la CEDH a jugé que la conservation litigieuse des données à caractère personnel avait en droit interne une base suffisamment claire et prévisible et que la durée et les aspects techniques de la conservation étaient clairement définis. Sur la question de la nécessité de l'ingérence dans une société démocratique, la CEDH a constaté que l'enregistrement préalable des abonnés à la téléphonie mobile simplifiait et accélérait nettement les enquêtes menées par les organes chargés de l'application de la loi, et qu'il pouvait donc contribuer à l'effectivité de l'application des lois, de la défense de l'ordre et de la prévention des infractions pénales. Elle a également rappelé qu'en matière de sécurité nationale, les autorités internes bénéficient d'une certaine marge d'appréciation dans le choix des moyens propres à atteindre le but légitime que constitue la protection de la sécurité nationale, et elle a constaté qu'il n'existait pas de consensus entre les États membres quant à la conservation des données relatives aux abonnés ayant fait l'acquisition de cartes SIM prépayées. S'agissant de la marge d'appréciation, elle a estimé que l'obligation de conserver des informations relatives aux abonnés constituait, de manière générale, une réponse adaptée à l'évolution à la fois des comportements en matière de communication et des moyens de télécommunication. Dans son appréciation de la proportionnalité de l'obligation légale litigieuse, elle a distingué la présente affaire de celles mettant en jeu la conservation d'informations hautement personnelles (telles que l'affaire *Ben Faiza*, précitée), et elle s'est aussi appuyée sur l'arrêt rendu par la CJUE dans l'affaire *Ministerio fiscal* (précitée) pour conclure que l'ingérence litigieuse était limitée.

La CEDH a également observé que même si les requérants ne se plaignaient que de la conservation des données à caractère personnel les concernant, elle ne pouvait apprécier la proportionnalité de l'ingérence litigieuse sans évaluer de près les possibilités de consultation et d'utilisation ultérieures des données en question. Elle a constaté que l'accès à ces données était limité à un certain nombre d'autorités qui étaient spécifiquement énumérées, auquel cas l'accès leur était accordé au moyen d'une procédure centralisée et automatisée, ou identifiées par référence aux tâches qu'elles accomplissaient, auquel cas l'accès devait faire l'objet d'une demande écrite. En outre, elle a relevé qu'un certain nombre de garanties encadraient l'accès aux données, notant que seuls l'Agence

fédérale des réseaux ou l'opérateur concerné pouvaient transmettre des données, que l'accès était limité aux données nécessaires, que cette exigence de nécessité était garantie par l'obligation générale, pour les autorités ayant obtenu des informations, d'effacer sans retard indu toutes les données qui ne leur étaient pas utiles et que, dans le contexte de la poursuite des infractions, il devait y avoir au moins un soupçon initial. S'agissant des possibilités d'examen et de surveillance des demandes d'informations, la CEDH a établi une distinction entre la présente affaire et de précédentes affaires où étaient en cause diverses ingérences dans les droits garantis par l'article 8, estimant que, compte tenu du caractère limité des données en jeu, ces garanties devaient être considérées comme un élément important, mais non décisif, aux fins de l'appréciation de la proportionnalité. À cet égard, elle a considéré que le cadre juridique pertinent offrait des garanties suffisantes puisque chaque récupération de données et les informations pertinentes concernant la récupération étaient enregistrées à des fins de contrôle de la protection des données, mission assurée par des autorités indépendantes chargées de la protection des données, et que toute personne estimant que ses droits avaient été violés pouvait former un recours.

Conclusion – Non-violation de l'article 8 de la CEDH.

B. 2. Données de trafic et de localisation

CJUE, arrêt du 8 avril 2014, *Digital Rights Ireland e.a.*, C-293/12 et C 594/12, UE:C:2014:238

En fait – L'affaire avait pour origine deux demandes de décision préjudicielle qui portaient sur la validité de la directive sur la conservation des données et avaient été formulées dans le cadre de procédures nationales où la légalité de mesures législatives et administratives nationales en matière de conservation des données de communications électroniques était contestée au regard des droits constitutionnels et européens à la protection des données.

En droit – La CJUE a estimé que l'obligation faite aux FSC de conserver des données relatives à la vie privée et aux communications et l'accès ultérieur des autorités nationales à ces données portaient atteinte aux droits garantis par les articles 7 et 8 de la Charte. L'ingérence a été jugée particulièrement grave et susceptible de générer chez les personnes concernées le sentiment que leur vie privée faisait l'objet d'une surveillance constante.

La CJUE a jugé que l'analyse de proportionnalité incluait une appréciation : i) du caractère approprié et ii) de la nécessité des mesures contestées au regard de leurs objectifs. S'appuyant également sur les principes énoncés dans la jurisprudence de la CEDH en matière de marge d'appréciation, la CJUE a dit que l'étendue du pouvoir d'appréciation du législateur de l'Union pouvait s'avérer limitée en fonction d'un certain nombre d'éléments, notamment le domaine concerné, la nature du droit en cause, la nature et la gravité de l'ingérence ainsi que la finalité de celle-ci, et que, dans le cas d'espèce, ce pouvoir d'appréciation était réduit du fait de l'importance de la protection des données à caractère personnel et de la gravité de l'ingérence.

La CJUE a admis que les mesures contestées pouvaient être considérées comme appropriées mais elle a jugé, eu égard à l'importance croissante des moyens de communication électronique et de leur utilité en tant qu'instrument utile pour les enquêtes pénales, que la directive sur la conservations des données ne se limitait pas à ce qui était strictement nécessaire pour atteindre ses objectifs, ce pour les raisons exposées ci-dessous.

Premièrement, la directive visait de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données de trafic sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif de lutte contre les infractions graves. Elle ne se limitait pas à une conservation portant sur des données afférentes à

une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave.

Deuxièmement, la directive ne posait aucune condition matérielle et procédurale à l'accès des autorités nationales compétentes aux données et à leur utilisation ultérieure. En se contentant de renvoyer, de manière générale, aux infractions graves telles qu'elles étaient définies par chaque État membre dans son droit interne, la directive ne prévoyait aucun critère objectif permettant de délimiter quelles infractions pouvaient, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence. De plus, l'accès par les autorités nationales compétentes aux données conservées n'était pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire.

Troisièmement, la directive imposait la conservation de toutes les données pendant une période d'au moins six mois sans que soit opérée une quelconque distinction entre les catégories de données en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées. La CJUE a conclu que la directive comportait une ingérence d'une vaste ampleur et d'une gravité particulière dans les droits fondamentaux consacrés par les articles 7 et 8 de la Charte sans que cette ingérence ne soit précisément encadrée par des dispositions permettant de garantir qu'elle était effectivement limitée au strict nécessaire. Elle a également noté que la directive ne prévoyait pas de garanties suffisantes, au moyen de mesures techniques et organisationnelles, permettant d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données. La directive ne garantissait pas non plus la destruction irrémédiable des données au terme de leur durée de conservation, ni n'exigeait qu'elles soient conservées sur le territoire de l'Union.

CJUE, arrêt du 21 décembre 2016, *Tele2 Sverige et Watson et autres*, C-203/15 et C-698/15, UE:C:2016:970

En fait – L'affaire avait pour origine deux demandes de décisions préjudicielles sur la compatibilité avec le droit de l'UE d'une législation nationale prévoyant la conservation généralisée de toutes les données de trafic et de localisation à des fins de lutte contre la criminalité.

En droit – La CJUE a estimé que l'article 15 § 1 de la directive « vie privée et communications électroniques », lu à la lumière des articles 7, 8 et 11 et de l'article 52 § 1, de la Charte, devait être interprété en ce sens qu'il s'opposait à une réglementation nationale :

1) qui, aux fins de la lutte contre la criminalité, prévoyait la conservation généralisée et indifférenciée de l'ensemble des données de trafic et des données de localisation de tous les utilisateurs concernant tous les moyens de communication électronique.

En particulier, la CJUE s'est appuyée sur l'arrêt *Digital Rights Ireland e.a.*, précité, et a précisé que la conservation des données devait être limitée au strict nécessaire en ce qui concerne les catégories de données, les moyens de communication concernés, les personnes visées et la durée de conservation retenue. Pour satisfaire à ces exigences, la législation nationale devait, en premier lieu, prévoir des règles claires et précises régissant la portée et l'application d'une telle mesure de conservation des données et imposant un minimum d'exigences. En second lieu, elle devait prévoir des conditions matérielles de conservation des données afin d'établir un rapport entre les données à conserver et l'objectif poursuivi.

2) et qui régissait la protection et la sécurité des données de trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, i) sans limiter,

dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, ii) sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et iii) sans exiger que les données en cause soient conservées sur le territoire de l'UE.

CEDH, *Ben Faiza c. France*, n° 31446/12, 8 février 2018

En fait – L'affaire portait principalement sur la compatibilité avec l'article 8 de la CEDH de l'accès par la police judiciaire, avec l'autorisation d'un magistrat du parquet, aux données de trafic et de localisation conservées par les FSC.

En droit – La CEDH a jugé que l'accès des autorités nationales aux données de trafic et de localisation s'analysait en une ingérence dans les droits du requérant découlant de l'article 8.

Sur la justification de l'ingérence, la CEDH a estimé que l'accès était prévu par le droit interne et qu'il était prévisible. Quant aux garanties contre l'arbitraire, elle a observé que la police judiciaire pouvait avoir accès aux données de communication avec l'autorisation d'un magistrat du parquet. De plus, l'accès était soumis à un contrôle juridictionnel *a posteriori* dans le cadre d'une procédure pénale contre la personne concernée, qui permettait aux juges d'apprécier la légalité l'accès et, s'ils devaient le juger illégal, d'exclure de la procédure les preuves recueillies par ce moyen. La CEDH a également noté que les garanties entourant l'accès aux données de communication étaient moins strictes que celles concernant la localisation en temps réel, mais elle a estimé que cette différence était justifiée parce que l'ingérence était moins grave.

Quant à la nécessité de l'ingérence dans une société démocratique, la CEDH a considéré qu'elle était nécessaire en vue de démanteler un trafic de stupéfiants de grande ampleur. De plus, les informations obtenues avaient été utilisées dans le cadre d'un procès pénal au cours duquel le requérant avait bénéficié d'un contrôle effectif tel que voulu par la prééminence du droit et apte à limiter l'ingérence litigieuse à ce qui était nécessaire dans une société démocratique.

Conclusion : non-violation de l'article 8 de la CEDH.

CJUE, arrêt du 16 juillet 2020, *Facebook Ireland et Schrems*, C-311/18, UE:C:2020:559

En fait – À la suite de l'arrêt rendu par la CJUE le 6 octobre 2015 dans l'affaire *V. Schrems*, C-362/14, UE:C:2015: 650, qui avait statué sur la validité de la décision sur la «sphère de sécurité », selon laquelle la Commission européenne avait estimé que les États-Unis assuraient un niveau de protection adéquat des données personnelles transférées, M. Schrems contesta de nouveau le transfert de ses données par Facebook Ireland vers les États-Unis et la conservation de ses données sur des serveurs installés dans ce pays. Il se plaignait de ce que la législation des États-Unis obligeait Facebook Inc. à mettre les données à caractère personnel qui lui étaient transférées à la disposition de certaines autorités américaines, telles que la National Security Agency et le Federal Bureau of Investigation. M. Schrems soutenait que, puisque ces données étaient utilisées dans le cadre de divers programmes de surveillance d'une manière incompatible avec les articles 7, 8 et 47 de la Charte, la décision 2010/87/UE ne pouvait justifier le transfert de ces données aux États-Unis.

Le juge national avait saisi la CJUE de plusieurs questions préjudicielles, demandant entre autres si le droit de l'UE s'appliquait au transfert de données d'une société privée de l'UE vers une société privée d'un pays tiers et, dans l'affirmative, comment apprécier le niveau de protection dans le pays tiers ; et si le niveau de protection offert par les États-Unis respectait l'essence des droits garantis par l'article 47 de la Charte.

En droit – La CJUE a jugé que le règlement général sur la protection des données (« RGPD ») s'appliquait au transfert de données à caractère personnel à des fins commerciales par un opérateur économique établi dans un État membre à un autre opérateur économique établi dans un pays tiers, indépendamment de ce que, au cours ou à la suite de ce transfert, ces données étaient susceptibles d'être traitées par les autorités de ce pays tiers à des fins de sécurité publique, de défense et de sûreté de l'État. En outre, les garanties appropriées, les droits opposables et les voies de droit effectives requis par le RGPD devaient assurer que les droits des personnes dont les données à caractère personnel étaient transférées vers un pays tiers sur le fondement de clauses types de protection des données bénéficient d'un niveau de protection substantiellement équivalent à celui garanti au sein de l'UE. À cet effet, l'évaluation du niveau de protection assuré dans le contexte d'un tel transfert devait, notamment, prendre en considération tant les stipulations contractuelles convenues entre le responsable du traitement ou son sous-traitant établis dans l'Union et le destinataire du transfert établi dans le pays tiers concerné que, en ce qui concerne un éventuel accès des autorités publiques de ce pays tiers aux données à caractère personnel ainsi transférées, les éléments pertinents du système juridique de ce pays.

Par ailleurs, sauf s'il existait une décision d'adéquation valablement adoptée par la Commission, l'autorité de contrôle compétente était tenue de suspendre ou d'interdire un transfert de données vers un pays tiers lorsque cette autorité de contrôle considérait, à la lumière de l'ensemble des circonstances propres à ce transfert, que les clauses types de protection des données n'étaient pas ou ne pouvaient pas être respectées dans ce pays tiers et que la protection des données transférées requise par le droit de l'Union ne pouvait pas être assurée par d'autres moyens.

L'adoption par la Commission d'une décision d'adéquation exigeait la constatation que le pays tiers concerné assure effectivement, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection des droits fondamentaux substantiellement équivalent à celui garanti dans l'ordre juridique de l'UE. La CJUE a invalidé la décision relative à la sphère de sécurité. La disposition pertinente ne faisait ressortir d'aucune manière l'existence de limitations à l'habilitation qu'elle comportait pour la mise en œuvre des programmes de surveillance aux fins du renseignement extérieur, pas plus que l'existence de garanties pour des personnes non-américaines potentiellement visées par ces programmes. Dans ces conditions, elle n'était pas susceptible d'assurer un niveau de protection substantiellement équivalent à celui garanti par la Charte. En outre, en ce qui concerne les programmes de surveillance, il était clair que ce texte ne conférait aucun droit opposable aux autorités des États-Unis devant les tribunaux de ce pays.

CJUE, arrêt du 6 octobre 2020, *La Quadrature du Net et autres*, C-511/18, C-512/18 et C-520/18, UE:C:2020:791

En fait – L'affaire avait pour origine trois demandes de décision préjudicielle portant sur l'application de la directive « vie privée et communications électroniques » à une législation nationale qui imposait aux fournisseurs de services de communications électroniques l'obligation :

i) de conserver de façon généralisée et indifférenciée les données de trafic et des données de localisation à des fins de sauvegarde de la sécurité nationale et de lutte contre le terrorisme ;

ii) de mettre en œuvre sur leurs réseaux des mesures permettant l'analyse automatisée ainsi que le recueil en temps réel des données de trafic et des données de localisation ainsi que le recueil en temps réel des données techniques relatives à la localisation des équipements terminaux utilisés.

En droit – La CJUE a souligné que l'objectif de sauvegarde de la sécurité nationale n'avait pas encore été spécifiquement examiné par elle dans ses arrêts interprétant la directive « vie privée et communications électroniques ». Elle a confirmé que si cette directive, lue à la lumière de la Charte, s'opposait à des mesures législatives prévoyant la conservation généralisée et indifférenciée des

données de trafic et des données de localisation, il n'y avait aucun obstacle à ce qu'un État membre se trouvant face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, adopte des mesures législatives imposant aux FSC de conserver, de manière généralisée et indifférenciée, les données de trafic et les données de localisation pendant une durée limitée au strict nécessaire, mais pouvant être prolongée si la menace persistait. En pareil cas, la décision imposant une telle injonction devait faire l'objet d'un contrôle effectif soit par une juridiction, soit par une entité administrative indépendante, dont la décision était dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues. Aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, un État membre pouvait également prévoir, dans une mesure limitée au strict nécessaire dans le temps, une conservation ciblée des données de trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique ou d'adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire. Les États membres pouvaient aussi procéder à une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communication électronique, sans que cette conservation soit limitée dans le temps.

En outre, la directive « vie privée et communications électroniques », lue à la lumière de la Charte, ne s'opposait pas à l'adoption de règles nationales imposant aux FSC de recourir, d'une part, à l'analyse automatisée et au recueil en temps réel des données de trafic et des données de localisation et, d'autre part, au recueil en temps réel des données techniques relatives à la localisation des équipements terminaux utilisés, lorsque cela se limitait aux situations dans lesquelles un État membre était confronté à une menace grave pour la sécurité nationale, réelle et actuelle ou prévisible, et où le recours à une telle analyse pouvait faire l'objet d'un contrôle effectif par une juridiction ou une entité administrative indépendante dont la décision était dotée d'un effet contraignant; et où le recours au recueil en temps réel de données de trafic et de données de localisation était limité aux personnes à l'égard desquelles il existait une raison valable de soupçonner qu'elles étaient impliquées d'une manière ou d'une autre dans des activités de terrorisme et était soumis à un contrôle préalable, effectué, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant.

CJUE, arrêt du 2 mars 2021, *Prokuratuur*, C-746/18, UE:C:2021:152

En fait – L'affaire avait pour origine une demande de décision préjudicielle sur l'application de la directive « vie privée et communications électroniques » à une législation nationale qui autorisait l'accès aux données conservées par les fournisseurs de services de communications électroniques dans le cadre de procédures pénales.

En droit – La CJUE a rappelé que l'article 15(1) de la directive « vie privée et communications électroniques » n'autorisait l'accès aux données de trafic ou de localisation conservées aux fins de la lutte contre la criminalité que lorsqu'il s'agissait de criminalité grave ou de menaces graves contre la sécurité publique, indépendamment de la durée de la période pour laquelle l'accès est sollicité et de la quantité ou de la nature des données disponibles pour une telle période.

La CJUE a ensuite estimé que le pouvoir d'examiner les demandes d'accès ne pouvait être conféré au ministère public, étant donné que ses missions de direction de l'instruction préalable et d'exercice de l'action publique pouvaient nuire à son indépendance vis-à-vis des parties au procès pénal.

CEDH, *Big Brother Watch et autres c. Royaume-Uni* [GC], précité

En fait – Veuillez vous reporter à l'encadré au paragraphe B ci-dessus.

En droit – Les requérants soutenaient que le régime d'acquisition de données de communication auprès des FSC était incompatible avec leurs droits découlant des articles 8 et 10 de la CEDH. S'agissant de ces deux griefs, la Grande Chambre a confirmé les conclusions de la chambre :

Sur le terrain de l'article 8, à la date de l'examen de l'affaire par la chambre, une procédure interne était en cours concernant une nouvelle législation qui régissait la conservation par les FSC des données de communication. Au cours de cette procédure, le gouvernement britannique avait admis que le régime juridique en question était incompatible avec le droit de l'UE, si bien que les juges nationaux l'avaient jugé incompatible avec les droits fondamentaux garantis par le droit de l'UE.

Compte tenu à la fois de la primauté du droit de l'UE sur le droit britannique à l'époque et de ce qu'avait admis le gouvernement au cours de la procédure interne, la CEDH a jugé qu'il était clair que le droit interne commandait que tout régime permettant aux autorités d'accéder aux données conservées par un FSC limitait cet accès à la lutte contre les « infractions graves » et le soumettait au contrôle préalable d'un tribunal ou d'une instance administrative indépendante. Le régime antérieur présentant les mêmes « défauts » que son successeur, la CEDH a conclu qu'il ne pouvait être considéré comme prévu par la loi au sens de l'article 8 de la Convention.

Sur le terrain de l'article 10, la CEDH a reconnu que le régime litigieux offrait une protection renforcée lorsque les données étaient recherchées dans le but d'identifier la source d'un journaliste. Néanmoins, ces dispositions ne s'appliquaient pas à chacune des demandes visant les données de communication d'un journaliste ou susceptibles de conduire à une intrusion collatérale dans ces données de communication. De plus, il n'y avait pas de dispositions spéciales restreignant l'accès aux données de communication d'un journaliste au but de lutter contre les « infractions graves ». En conséquence, la CEDH a estimé que ce régime n'était pas prévu par la loi, au sens de l'article 10 de la CEDH.

Conclusion – Violation des articles 8 et 10 de la CEDH à raison du régime d'acquisition des données de communication auprès des FSC.

CEDH, *Ekimdzhiev et autres c. Bulgarie*, n° 70078/12, 11 janvier 2022

En fait – L'affaire portait sur la compatibilité avec l'article 8 des lois et pratiques bulgares en matière de conservation des données de communication et d'accès à celles-ci. Les requérants, deux avocats et deux organisations non gouvernementales, soutenaient que la nature de leurs activités les exposait au risque que les autorités accèdent à leurs données de communication.

En droit – Les requérants estimaient que le système de conservation et d'accès ultérieur aux données de communication (abonnés, trafic et géolocalisation) ne répondait pas aux exigences de l'article 8 de la CEDH.

S'appuyant sur sa jurisprudence antérieure (arrêts *Breyer*, *Centrum för rättvisa* et *Big Brother Watch*, tous précités), la CEDH a dit ceci :

a) la seule conservation de ces données s'analysait en une ingérence dans le droit des requérants au respect de leur vie privée et de leur correspondance et dans le droit des personnes morales requérantes au respect de leur correspondance ;

b) l'accès des autorités aux données de communication conservées s'analysait en une ingérence distincte sur le terrain de l'article 8.

Sur la justification de l'ingérence, s'appuyant sur les arrêts *Centrum för rättvisa* et *Big Brother Watch*, tous deux précités, la CEDH a jugé que l'acquisition de ces données par une interception en masse pouvait être aussi intrusive que l'acquisition en masse du contenu des communications et que les mêmes garanties que celles applicables au contenu devaient donc s'appliquer. De même, elle a ajouté que la conservation générale des données de communication par les FSC et l'accès à celles-ci par les autorités dans des cas individuels devaient s'accompagner, *mutatis mutandis*, des mêmes garanties que celles entourant la surveillance secrète (elle s'est appuyée en particulier sur l'arrêt *Roman Zakharov*, précité).

Appliquant ces principes au cas d'espèce et analysant un certain nombre d'éléments (l'accessibilité de la loi ; le niveau de protection des données conservées garanti par les FSC ; l'analyse des motifs pour lesquels les données conservées pouvaient être consultées par les autorités ; les procédures d'accès ; la durée de conservation et d'usage des données consultées non utilisées ultérieurement dans le cadre d'un procès pénal ; les procédures de conservation, d'accès, d'examen, d'utilisation, de communication et de destruction des données consultées par les autorités ; les modalités de contrôle ; la notification aux personnes concernées ; les recours), la CEDH a conclu que le régime juridique litigieux ne respectait pas les garanties minimales contre l'arbitraire et les abus requises par l'article 8 de la CEDH, ce pour les raisons suivantes :

a) la procédure d'autorisation n'apparaissait pas à même de garantir que les autorités n'auraient accès aux données de communication conservées que lorsque cela serait « nécessaire dans une société démocratique » ;

b) aucun délai précis n'avait été fixé pour la destruction des données auxquelles les autorités avaient eu accès dans le cadre de procès pénaux ;

c) il n'existait aucune règle accessible au public concernant la conservation, l'accès, l'examen, l'utilisation, la communication et la destruction des données de communication recueillies par les autorités ;

d) le système de contrôle n'apparaissait pas à même de vérifier efficacement les abus ;

e) les modalités de notification étaient trop restrictives ; et

f) il n'y avait pas de recours effectif.

Conclusion : violation de l'article 8 de la CEDH à raison du régime de la conservation des données de communication et de l'accès à celles-ci.

CJUE, arrêt du 5 avril 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, UE:C:2022:258

En fait – L'affaire avait pour origine une demande de décision préjudicielle sur l'application de la directive « vie privée et communications électroniques » à une législation nationale qui autorisait l'accès aux données conservées par les fournisseurs de services de communications électroniques dans le cadre de procédures pénales.

En droit – La CJUE a confirmé sa jurisprudence constante selon laquelle le droit de l'UE s'oppose à des mesures législatives prévoyant, à titre préventif, aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des données de trafic et des données de localisation. Elle a toutefois estimé que le droit de l'UE ne s'opposait pas :

– à une conservation ciblée, pendant une durée limitée, des données de trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires ;

– à une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pendant une durée limitée ;

– à une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, et

– au recours à une injonction faite aux FSC, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données de trafic et des données de localisation détenues par les FSC ;

dès lors que ces mesures assuraient, par des règles claires et précises, que la conservation des données en cause était subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposaient de garanties effectives contre les risques d'abus.

En outre, la CJUE a estimé que le droit de l'UE s'opposait à une législation nationale en vertu de laquelle le traitement centralisé des demandes d'accès à des données conservées par les FSC, émanant de la police dans le cadre de la recherche et de la poursuite d'infractions pénales graves, incombait à un fonctionnaire de police, assisté par une unité instituée au sein de la police jouissant d'un certain degré d'autonomie dans l'exercice de sa mission et dont les décisions pouvaient faire ultérieurement l'objet d'un contrôle juridictionnel.

CJUE, arrêt du 20 septembre 2022, *SpaceNet et Telekom Deutschland*, C-793/19 et C-794/19, UE:C:2022:702

En fait – L'affaire avait pour son origine deux demandes de décision préjudicielle sur l'application de la directive « vie privée et communications électroniques » à une législation nationale imposant aux fournisseurs de services de communications électroniques de conserver, de manière généralisée et indifférenciée, la plupart des données de trafic et des données de localisation des utilisateurs finaux de ces services (y compris les données relatives aux sites Internet visités et les données tirées des services de messagerie électronique), en fixant une durée de conservation de plusieurs semaines et des règles destinées à assurer la protection effective des données conservées contre les risques d'abus et contre tout accès illicite à celles-ci.

En droit – La CJUE a confirmé sa jurisprudence constante en matière de conservation généralisée et indifférenciée des données de trafic et des données de localisation à des fins de lutte contre la criminalité grave ou de prévention des menaces graves contre la sécurité publique (arrêts *La Quadrature du Net* et *Commissioner of An Garda Síochána*, tous deux précitées). Elle a dit que la législation nationale en question n'était pas conforme au droit de l'UE, malgré l'existence de garanties et une période de conservation plus courte que dans les affaires précédentes. Elle a également jugé que la conservation de ces données et l'accès à celles-ci constituaient des ingérences distinctes dans les droits fondamentaux des personnes concernées, nécessitant une justification distincte, et que, dès lors, une législation nationale assurant le respect intégral des conditions tirées de la jurisprudence en matière d'accès aux données conservées ne pouvait, par nature, être à même de limiter, voire de remédier, à l'ingérence grave dans les droits des personnes concernées qui résulterait de la conservation généralisée de ces données.

CJUE, arrêt du 20 septembre 2022, *VD et SR*, C-339/20 et C-397/20, UE:C:2022:703

En fait – L'affaire avait pour origine deux demandes de décision préjudicielle concernant l'interprétation de dispositions de l'UE relatives aux abus de marché, lues conjointement avec l'article 15(1) de la directive « vie privée et communications électroniques ». Les demandes avaient

été formulées dans le cadre de procédures pénales engagées contre VD et SR pour délits d'initié, recel de délits d'initié, complicité, corruption et blanchiment.

En droit – La CJUE a jugé que la directive sur les abus de marché et le règlement sur les abus de marché, lus conjointement avec la directive « vie privée et communications électroniques » et à la lumière des articles 7, 8 et 11 de la Charte, n'autorisaient pas la conservation généralisée et indifférenciée des données de trafic par les FSC pendant une durée d'un an à compter du jour d'enregistrement, aux fins de la lutte contre les infractions d'abus de marché.

La CJUE a également jugé que le droit de l'Union s'opposait à ce qu'une législation nationale limite dans le temps les effets d'une déclaration d'invalidité qui lui incombait, en vertu du droit national, à l'égard de dispositions nationales qui, d'une part, imposaient aux FSC une conservation généralisée et indifférenciée des données relatives au trafic et, d'autre part, permettaient la communication de telles données à l'autorité compétente en matière financière, sans autorisation préalable d'une juridiction ou d'une autorité administrative indépendante, en raison de l'incompatibilité de ces dispositions avec l'article 15 § 1, de la directive « vie privée et communications électroniques », lu à la lumière de la Charte. L'admissibilité des éléments de preuve obtenus en application des dispositions législatives nationales incompatibles avec le droit de l'UE relevait, conformément au principe d'autonomie procédurale des États membres, du droit national, sous réserve du respect, notamment, des principes d'équivalence et d'effectivité.

CJUE, arrêt du 17 novembre 2022, *Spetsializirana prokuratura*, C-350/21, UE:C:2022:896

En fait – L'affaire avait pour origine une demande de décision préjudicielle sur l'application de la directive « vie privée et communications électroniques » à la lumière des articles 7, 8, 11 et 52 de la Charte à une législation nationale :

i) qui imposait aux FSC de conserver, de manière générale et indifférenciée, toutes les données de trafic et les données de localisation des utilisateurs finaux de ces services aux fins de la lutte contre la criminalité grave, en fixant une durée de conservation de six mois et des règles destinées à garantir certaines garanties ; et

ii) qui ne limitait pas l'accès à ces données au strict nécessaire, ni ne prévoyait le droit d'être informé lorsque ces informations n'entravaient pas les procédures pénales et le droit de recours contre l'accès illicite.

En droit - La CJUE a confirmé sa jurisprudence constante en matière de conservation généralisée et indifférenciée des données de trafic et des données de localisation aux fins de la lutte contre la criminalité grave (arrêts *La Quadrature du Net* et *Commissioner of An Garda Síochána*, tous deux précités). Elle a estimé que la législation nationale en question n'était pas conforme au droit de l'UE, malgré l'existence de garanties et d'une période de conservation de six mois. En ce qui concerne les garanties procédurales contre l'accès illicite, elle a dit qu'une autorisation délivrée par un tribunal national ne suffisait pas, en tant que telle, à assurer la protection effective des personnes concernées contre les risques d'abus et d'accès illicite aux données qui les concernaient lorsque, comme en l'occurrence, la réglementation nationale en cause prévoyait que cette autorisation était octroyée sur le seul fondement d'une demande formée par les autorités nationales compétentes en matière d'enquêtes pénales, sans que les personnes concernées eussent été entendues et, partant, sans que la juridiction compétente pour délivrer une telle autorisation eût été en mesure de prendre en compte les possibles objections de ces personnes.

CEDH, *Škoberne c. Slovénie*, n° 19920/20, 15 février 2024

En fait – Les données de trafic et de localisation du requérant – qui avaient été conservées par les FSC pendant quatorze mois dans le cadre d'une mesure systémique – furent obtenues par les autorités répressives en application d'ordonnances judiciaires fondées sur des soupçons de participation du requérant à des faits de corruption. L'affaire concernait la compatibilité avec l'article 8 de la CEDH d'une législation qui autorisait la conservation des données de télécommunication du requérant et leur utilisation par les autorités dans le cadre du procès engagé contre lui.

En droit – La CEDH a recherché si le régime de conservation des données était nécessaire dans une société démocratique, en examinant i) la gravité de l'ingérence ; ii) l'étendue de la marge d'appréciation et iii) l'existence d'un « juste équilibre ».

Sur le point i), la CEDH a distingué cette affaire de l'affaire *Breyer*, précitée, en constatant que l'ingérence était plus grave en l'espèce car elle touchait les données de communication.

Sur le point ii), la CEDH, s'appuyant sur sa jurisprudence antérieure, a rappelé que la lutte contre la criminalité, le maintien de la sûreté publique et la protection des citoyens constituaient des « besoins sociaux impérieux » et que les autorités nationales disposaient d'une certaine marge d'appréciation dans le choix des moyens pour atteindre de tels buts légitimes. Elle a toutefois ajouté que cette marge tendait à être plus étroite lorsque, comme en l'espèce, le droit en jeu était essentiel à la jouissance effective par le justiciable de droits d'ordre intime ou fondamentaux ou lorsque l'ingérence était de grande ampleur.

Sur le point iii), la CEDH a estimé que les garanties entourant la conservation générale des données de communication par les FSC et à l'accès à celles-ci par les autorités dans des cas individuels devaient être les mêmes, *mutatis mutandis*, que celles entourant la surveillance secrète.

La CEDH a constaté que le régime juridique contesté ne prévoyait aucune disposition limitant la portée et l'application de la mesure à ce qui était nécessaire pour atteindre les buts poursuivis par la conservation des données de télécommunication. S'appuyant en outre sur l'arrêt rendu par la CJUE en l'affaire *Digital Rights Ireland*, précité, elle a dit que le droit interne devait définir le champ d'application de la mesure en question et encadrer par des procédures appropriées l'adoption et/ou le contrôle de celle-ci en vue de la maintenir dans les limites du nécessaire. La simple limitation de la durée de conservation à quatorze mois ne pouvait remettre en cause cette conclusion. La CEDH a également jugé qu'il ne pouvait être conclu de l'invalidation du régime de conservation par la CJUE et la Cour constitutionnelle postérieurement à la consultation des données en question que ce régime était conforme à l'article 8 au moment des faits.

La CEDH a relevé en outre que, bien que le requérant eût clairement fait valoir que ses données de communication avaient été conservées en violation de son droit au respect de sa vie privée, les juridictions nationales avaient limité leur examen presque exclusivement aux motifs pour lesquels les ordonnances judiciaires avaient autorisé l'accès à ces données, alors même que le requérant n'avait pas contesté ces motifs. La CEDH a souligné que, quand bien même l'accès à ses données eût été entouré de certaines garanties (telles qu'un contrôle juridictionnel), celles-ci, quoiqu'elles fussent parmi les critères à respecter, n'étaient pas en elles-mêmes suffisantes pour rendre le régime de conservation conforme à l'article 8 de la CEDH. La CEDH s'est également appuyée sur l'arrêt *SpaceNet et Telekom Deutschland* de la CJUE, précité.

Quant à l'acquisition et à l'utilisation des données du requérant dans le cadre de la procédure interne, la CEDH, s'appuyant sur l'arrêt de la CJUE *Commissioner of An Garda Síochána e.a.*, précité, a estimé que lorsque la conservation des données de communication était jugée contraire à l'article 8 au motif qu'elle ne respectait pas l'exigence de « qualité de la loi » et/ou le principe de

proportionnalité, l'accès à ces données – et leur traitement et stockage ultérieurs par les autorités – ne pouvait, pour le même motif, être conforme à l'article 8.

Conclusion – Violation de l'article 8 de la CEDH.

CEDH, *Pietrzak et Bychawska-Siniarska et autres c. Pologne*, n^os^ 72038/17 et 25237/18, 28 mai 2024

En fait – L'affaire portait sur la compatibilité avec l'article 8 du régime polonais de surveillance secrète régissant le stockage et le traitement des données de communication[25]. Les requérants se plaignaient non pas d'avoir été effectivement placés sous surveillance, mais d'un risque d'être soumis à de telles mesures.

Les requérants soutenaient que le système de conservation et d'accès ultérieur aux données de communication (données de trafic et de localisation et données relatives aux recherches en ligne) ne répondait pas aux exigences de l'article 8 de la CEDH.

En droit – S'appuyant sur l'arrêt *Ekimdzhiev*, précité, la CEDH a estimé que la conservation et l'accès ultérieur aux données de communication s'analysaient en des ingérences distinctes sur le terrain de l'article 8 et que la conservation générale des données de communication par les FSC et l'accès à ces données par les autorités dans des cas individuels devaient s'accompagner, *mutatis mutandis*, des mêmes garanties qu'en matière de surveillance secrète.

La CEDH a distingué la présente affaire de l'affaire *Ekimdzhiev* précitée en relevant que le régime contesté permettait aux autorités nationales d'avoir un accès permanent, direct et illimité aux données de communication, sans même que les FSC en eussent connaissance et sans aucune intervention de leur part. Elle a jugé très graves les ingérences en cause. Elle a ajouté que si l'arrêt *Ekimdzhiev* précité concernait un régime de conservation des données de communication similaire à celui ici en cause, elle ne s'était pas prononcée sur la conformité du régime en cause lui-même aux exigences de l'article 8, mais s'était plutôt focalisée sur les garanties entourant l'accès et la conservation des données collectées.

S'appuyant également sur la jurisprudence de la CJUE (arrêts *Digital Rights Ireland e.a.*, *Privacy International*, *Commissioner of An Garda Síochána e.a.*, tous précités, et *La Quadrature du Net e.a.*[26]), la CEDH a estimé que le régime contesté imposait une conservation généralisée et indifférenciée des données de communication de tous les utilisateurs de services de communication, touchant des personnes qui ne se trouvaient pas, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. En outre, ce régime donnait aux services de police et de renseignement un accès à ces données à n'importe quelle fin relevant de l'exercice de leurs fonctions légales respectives. Dans ces conditions, les garanties contre d'éventuels abus, y compris le contrôle juridictionnel *a posteriori*, étaient insuffisantes pour rendre le régime en question conforme aux exigences de l'article 8.

Conclusion – Violation de l'article 8 de la CEDH à raison du régime de conservation des données de communication et d'accès à celles-ci.

[25] Les requérants se plaignaient également, sous l'angle de la même disposition, du contrôle opérationnel opéré dans le cadre des activités de police et des mesures de surveillance secrète exécutées dans le cadre de la lutte contre le terrorisme, au moyen de techniques telles que la mise sur écoute, l'enregistrement du contenu des conversations téléphoniques ou de la correspondance échangée par le biais des réseaux de télécommunications et de communication numérique. Ce volet de l'arrêt ne sera pas analysé car le système contesté qui permettait les mesures de surveillance ciblées n'est pas l'objet de la présente fiche.

[26] Arrêt du 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, UE:C:2020:791.

B.3 Le contenu des communications

CEDH, *Podchasov c. Russie*, n° 33696/19, 13 février 2024

En fait – Le requérant, utilisateur de Telegram, contestait la compatibilité avec l'article 8 de la CEDH de l'obligation légale faite aux « organisateurs de communication sur l'Internet » (« OCI ») de conserver toutes les données de communication pendant un an et le contenu de toutes les communications pendant six mois, et de soumettre ces données aux autorités répressives ou aux services de sécurité dans les circonstances prévues par la loi, ainsi que les informations nécessaires pour déchiffrer les messages électroniques s'ils étaient cryptés.

En droit – La CEDH s'est appuyée sur sa jurisprudence antérieure (arrêts *Breyer, Ekimdzhiev et Roman Zakharov*, tous précités) pour conclure que le stockage continu des communications en ligne du requérant et des données de communication connexes par Telegram ainsi que l'accès potentiel des autorités à ces données s'analysaient en une ingérence dans les droits du requérant découlant de l'article 8. Quant à l'obligation faite à Telegram de fournir aux autorités des clés de cryptage leur permettant de déchiffrer de bout en bout les communications cryptées, la CEDH a retenu l'argument du requérant selon lequel il était techniquement impossible de fournir aux autorités des clés de cryptage associées à des utilisateurs spécifiques de Telegram sans affecter tous les utilisateurs de leurs services. Elle a donc reconnu que le requérant était touché par cette disposition légale aussi.

La CEDH a estimé que, si l'affaire devait certes être principalement examinée sous l'angle de la question du stockage des données personnelles du requérant (comme dans les affaires *Breyer et Ekimdzhiev*, précitées), elle devait également l'être, le cas échéant, à la lumière de sa jurisprudence sur la surveillance secrète (arrêts *Roman Zakharov*, *Big Brother Watch*, précités).

Sur le stockage des communications en ligne et des données de communication, la CEDH a souligné la portée considérable des obligations de conservation des données faites par la législation contestée, notant que celle-ci englobait le contenu de toutes les communications en ligne et des communications connexes touchant tous les utilisateurs de communications en ligne, même en l'absence de soupçon raisonnable de participation à des activités criminelles ou d'activités mettant en danger la sécurité nationale, ou de toute autre raison de croire que la conservation des données pouvait contribuer à lutter contre les infractions graves ou à protéger la sécurité nationale, et sans aucune limitation quant à l'ampleur de la mesure pour ce qui est de son champ d'application territorial ou temporel ou des catégories de personnes susceptibles de voir leurs données personnelles conservées. Elle a jugé que l'ingérence était d'une ampleur et d'une gravité exceptionnelles.

Sur l'accès potentiel aux données conservées à des fins de surveillance secrète ciblée, la CEDH a constaté que le droit interne n'imposait pas aux autorités répressives de présenter l'autorisation judiciaire aux FSC avant d'obtenir l'accès aux communications d'une personne. En outre, les OCI étaient tenus d'installer des équipements offrant aux services de sécurité un accès direct aux données conservées, de sorte qu'ils disposaient des moyens techniques pour contourner la procédure d'autorisation et pour accéder aux communications en ligne et aux données de communication conservées sans autorisation judiciaire préalable. La CEDH a également repris ses conclusions sur l'absence de garanties adéquates et suffisantes contre les abus exposées dans l'arrêt *Roman Zakharov*, précité, où le même régime juridique avait été examiné dans le contexte des interceptions de communications par téléphonie mobile.

Enfin, quant à l'obligation légale de déchiffrer les communications, la CEDH l'a jugée disproportionnée aux objectifs légitimes poursuivis au motif que, si les criminels pouvaient certes

se servir eux aussi du cryptage, la disposition contestée risquait d'affaiblir le mécanisme de cryptage pour tous les utilisateurs.

Conclusion – Violation de l'article 8 de la CEDH.