Chronique de droit des militaires 2021/1

Sous la direction de D. Mainguy, Professeur à la faculté de droit et science politique de Montpellier (CDCM UMR-CNRS 5815 « Dynamiques du droit ») avec l'équipe « droit des militaires » de la Clinique juridique de Montpellier[1]

I. Généralités

(…)

5. Les limites de la collecte de métadonnées par les agences de renseignement : CJUE 6 oct. 2020 (2 arrêts, aff. Jointes C-511/18, C-512/18, C-520/18 et Aff/ C-623/17). Les besoins du renseignement, qu'il soit militaire, contre-terroriste, policier ou économique, facilités par les progrès immenses de la technologie, sont susceptibles de heurter des principes de liberté et, plus récemment, de protection des données personnelles, notamment lorsque les outils technologiques et juridiques permettent aux Etats d'imposer aux fournisseurs d'accès une obligation générale de collecte et de conservation des données, de traitement en temps réel de ces données, y compris les données de localisation ou des services fournis. L'idée selon laquelle les citoyens qui n'ont rien à se reprocher n'ont, par conséquent, rien à craindre de cette pratique, ne résiste pas à l'évolution des règles européennes de protection des données personnelles, tandis que l'irénisme généralisé facilite, évidemment toutes sortes d'actes illicites. Entre un système type *precrime* ou de surveillance généralisée approchant la fiction orwellienne ou des injonctions en temps réel chinoises, et un rempart absolu autour des données personnelles, les règles européennes ont vocation à poser un curseur qui ne peut ignorer d'une part, les exigences d'un Etat de droit, autour des logiques de protection des libertés fondamentales et de recours contre les abus, et d'autre part, l'accélération des menaces dont certaines passent, très évidemment, par l'utilisation des fournisseurs d'accès ou de services en ligne. La réponse, en termes policiers ou militaires, suppose une forme d'égalité des armes, notamment pour la lutte contre les menaces les plus importantes, par exemple terroristes, mais également toutes les expériences, diverses, de cybercriminalité. L'amoncellement des menaces ne doit être ni surestimé ni sous-estimé, ne serait-ce que parce que les auteurs et complices de ces menaces dans la mesure où, à défaut de la possibilité de l'utilisation des outils appropriés, notamment via des obligations faites aux opérateurs, privés le plus souvent, de permettre l'accès aux données qu'ils collectent, y compris la conservation de métadonnées de manière indifférenciée, c'est-à-dire la possibilité d'aspirer des flux de données. Il est évident qu'une telle mesure, parce qu'indifférenciée, est, sans limites, une atteinte aux droits fondamentaux tels qu'ils sont posés dans un Etat démocratique et posés en droit de l'Union européenne. Tout l'intérêt de l'analyse des dispositions nationales, à l'aune des référents et des compétences particulières, par exemple le référent européen face aux mesures législatives prises par les Etats, dont la France, repose précisément sur la question de la place de ce curseur. Loin de l'image donc, d'une surveillance généralisée ou au contraire de la limitation absolue des moyens, l'ensemble de la législation et de la jurisprudence européenne ou nationale cherche à placer le curseur au bon endroit, par exemple entre le contrôle « à la française » limité par les dispositions du Code de la sécurité intérieure (cf. infra) ou « à l'anglaise », générale et indifférenciée, a priori contraire au droit européen ce qui, s'agissant de l'Angleterre et sous la réserve d'une position de la CEDH ou des juges internes, leur est désormais indifférent.

[1] Ont contribué à cette chronique les membres de l'équipe « droit des militaires » de la Clinique juridique de Montpellier : Alexandra Bruno, étudiante Master 1 Droit privé de l'économie, Alice Caldumbide, Doctorante, Faculté de droit et science politique de Montpellier, Eloi Clément, Maître de conférences à la faculté de droit de science politique de Montpellier, Thiphaine Collot, Etudiante, Master 2 Droit privé de l'économie, Charlotte Houlard, faculté de droit de science politique de Montpellier, Charlotte Houlard, Etudiant, Master 2 Droit privé de l'économie, Maxime Khalaf, Etudiant, Master 2 Droit privé de l'économie, Léa Larrieu, Etudiante, Master 2 Droit privé de l'économie, Daniel Mainguy, Professeur à la faculté de droit de science politique de Montpellier, Delphine Maniller, Etudiante, Master 2 Droit privé de l'économie, Bruno Siau, Maître de conférences à la faculté de droit de science politique de Montpellier, Alain Terral, Pharmacien, Docteur en droit, avocat au barreau de Béziers.

La CJUE a, le 6 octobre 2020[2], rendu un arrêt réitérant cette position en réponse à plusieurs questions préjudicielles posées par le Royaume Unis, la France et la Belgique (par le Conseil d'Etat s'agissant de la France), validant, pour l'essentiel, les dispositions françaises. Cette décision fait d'ailleurs suite à l'arrêt *Tele2 Sverige »* du 21 décembre 2016. Elle se distingue de la question du transfert de données à une personne privée dans un Etat en dehors de l'Union européenne, assurant un niveau de protection différent comme dans les arrêts « *Schrems »* du 16 juillet 2020 (*Privacy shield*) et du 6 octobre 2015 (*Safe harbor*)[3]. L'arrêt *« Tele2 Sverige »* avait, reprenant la solution de l'arrêt *Schrems* dans le champ de la surveillance étatique des données personnelles, condamné à nouveau le stockage de données à caractère personnel sur la base d'une « obligation façon générale et indifférenciée »[4].

L'ensemble repose en outre sur la série de normes de source européenne, dont la directive n°2002/58 « vie privée et communication électronique » ou « *ePrivacy* » (art 15 §1) et la directive n°2000/31 « société de l'information » (art. 12 à 15), mais également le règlement n°2016/679 « RGPD », dont la réserve de son article 23 relatif à la protection de la sécurité national ou publique et la défense nationale dans des conditions nécessaires et proportionnées, et la compatibilité de mesures nationales prises, dans les pays visés, dans une logique de prévention de délits ou crimes ou d'enquêtes, notamment dans un contexte de tension terroriste, visant à recueillir des données personnelles, dans les conditions posées, notamment, aux articles L. 811-3 et 4, 821-1 et 851-1[5] et suivants du Code de sécurité intérieure, R. 10-13 du Code des postes et des communications électroniques[6], notamment en ce qu'elles auraient pour objet d'imposer aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement, une obligation de conservation des données.

L'arrêt est important dans la mesure où il assure la pesée des logiques de protection des données personnelles, telles que diffusées dans divers outils électroniques susceptibles d'être interceptés par des services de renseignement ou de police, et les moyens permis, dont la liste est proposée par l'arrêt s'agissant de la France (aff. 511/18 et 512/18). Une première lecture de l'arrêt pourrait permettre d'insister sur le fait que la CJUE, dans cet arrêt, réitère le principe de la condamnation d'une surveillance de masse, généralisée et indifférenciée, y compris dans un contexte de lutte contre le terrorisme. Une lecture plus approfondie permet d'observer que l'appréciation de la CJUE est plus nuancée. L'apport principal de l'arrêt repose sans doute sur la considération que, dans la mesure où ce traitement serait imposé aux fournisseurs d'accès ou d'hébergement, l'appréciation de ces mesures relève du droit européen, principalement la directive *ePrivacy* et le Règlement RGPD, de telle manière que la Cour devait alors répondre à plusieurs questions précises. Savoir si une obligation de conservation généralisée et indifférenciée imposée aux fournisseurs est ou non, dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, une ingérence justifiée. Savoir si des mesures de recueil en temps réel des données relatives au trafic et à la localisation d'individus déterminés sans imposer une obligation spécifique de conservation des données est ou non possible. Savoir si, dans des cas de procédure de recueil des données, les personnes visées doivent, ou non être informées.

Sur la première question, la question de l'obligation de conservation généralisée et indifférenciée, la question de posait de la compatibilité en premier des dispositions françaises avec l'article 15 §1 de la directive *ePrivacy* autorisant des limitations aux obligations des articles 5 (confidentialité), 6 (consentement au traitement des données) et 9 (données de localisation) pour des objectifs de sureté nationale si elle sont nécessaires, appropriées et proportionnées. Si elle rappelle (point 112) que les objectifs justifiant une exception ne doit pas devenir la règle, de sorte que la conservation des données doit tenir compte de l'importance du droit au respect de la vie privée, du droit à la protection des données à caractère personnel, ainsi que du droit à la liberté d'expression (point 114) et qu'une obligation de conservation des données à caractère personnel doit être justifiée par des critères objectifs établissant un rapport entre les données à conserver et l'objectif poursuivi (point 133).

Dès lors, s'agissant de mesures prévoyant la conservation préventive des données relatives au trafic et des données de localisation aux fins de la sauvegarde de la sécurité nationale (points 134 s.), celles-ci sont possibles « dès lors qu'il existe des circonstances suffisamment concrètes permettant de considérer que l'État membre concerné fait face à une menace grave (…) pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible » et « être temporellement limitée au strict

[2] CJUE 6 oct. 2020 (2 arrêts, aff. jtes C-511/18, C-512/18, C-520/18 et Aff/ C-623/17.

[3] CJUE, 16 juill. 2020, aff. C-311/18, *Data Protection Commissioner c/ Facebook Ireland Ltd, Maximillian Schrems,* AJ Contrat, 2020, p. 436, note Th. Douville, D. actu. 22 juill. 2020, obs. C. Crichton, CCE 2020. Comm. 35, obs. N. Metallinos ; RLDI 2020, n° 169, p. 35, obs. R. Perray nvalidant, la décision de la commission 2016/1250 du 12 juillet 2016 relative à l'adéquation de la protection assurée par le bouclier de protection des données (dit *Privacy Shield*) UE-États-Unis ; CJUE, 6 oct. 2015, *Schrems c/ Data Protection Commissioner*, C-362/14, D. 2016. 111, note B. Haftel, p. 2025, obs. L. d'Avout et S. Bollée, AJ pénal 2015. 601, obs. E. Daoud, Dalloz IP/IT 2016. 26, étude C. Théard-Jallu, J.-M. Job et S. Mintz, RTD eur. 2015. 786, obs. M. Benlolo-Carabot, p. 2017. 361, et p. 365, obs. F. Benoît-Rohmer, CCE 2015. étude 21, note R. Perray et J. Uzan-Naulin. Un autrichien, Schrems, utilisait le réseau social Facebook depuis 2008 et ses données personnelles avaient été transférées de Facebook Ireland vers la société mère se trouvant aux Etats Unis (CJUE, Communiqué de presse n°91/20, 16 juillet 2020). Schrems s'en été plaint auprès de l'autorité de contrôle irlandaise afin que ce transfert soit interdit car les Etats Unis ne proposent pas une protection suffisante des données, plainte rejetée car la Commission (Déc. Comm. n° 2000/520 du 26 juillet 2000 (JOUE, 25 août 2020, L. 215/1), conformément à la directive 95/46/CE du 24 oct. 1995 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* modifiée par le règlement (CE) no 1882/2003 du Parlement européen et du Conseil, du 29 septembre 2003) dans l'une de ses décisions avait constaté que les Etats Unis assuraient un niveau adéquat de protection (thèse du *« Safe Harbor »*). Sur question préjudicielle ensuite posée par la Haute Cour Irlandaise, la CJUE y explicitait l'idée selon laquelle les pays tiers vers lesquels sont transférées des informations doivent bénéficier d'une protection équivalente à celle garantie par l'Union Européenne. Elle en profitait donc pour interdire le stockage de masse de façon généralisée et indifférenciée de données à caractère personnel. La Hight Court a, dans la décision de renvoi, formulé plusieurs questions préjudicielles, alors que, entretemps, la Commission a rendu une nouvelle décision sur la question dite du « *Privacy shield »* et constatant l'adéquation de la protection des données sur ce fondement (Décis. d'exécution de la Commission du 12 juill. 2016 conformément à la directive 95/46/CE relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis ; C. Castets-Renard, « Adoption du *Privacy Shield* : des raisons de douter de la solidité de cet accord », Dalloz IP/IT 2016. 444). Or les questions préjudicielles portaient sur l'application du droit de l'Union au cas de transfert de données personnelles vers un pays tiers et leur traitement, là, à des fins de sécurité publique : en clair, le droit de l'UE peut-il s'opposer à ce que des agences américaines utilisent les données collectées de ressortissants de l'UE ? Or, La Cour répond, sur le terrain du RGPD en considérant qu'il s'applique aux transferts de données, quel que soit le traitement ensuite opéré que la protection assurée par le *Privicy Shield* est insuffisante, invalidant la décision de 2016

[4] CJUE, 21 déc. 2016, *Tele2,* aff. jtes, C-203/15 et C-698-15.

[5] CSI, art. L. 851-1 : « Dans les conditions prévues au chapitre Ier du titre II du présent livre, peut être autorisé le recueil, auprès des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications ».

[6] CPCE, art. 10-13 : « En application du III de l'article L. 34-1 les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales (…) ».

nécessaire », en « un laps de temps prévisible » éventuellement renouvelable.

S'agissant des mesures prévoyant la conservation préventive des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité et de la sauvegarde de la sécurité publique (points 140 s.), la Cour ne les admet que s'il existe, eu égard à la gravité de l'atteinte aux droits des personnes, des moyens limités au strict nécessaire, en ce qui concerne les catégories de données à conserver, les moyens de communication visés ou les personnes concernées (point 147, visant l'arrêt *Tele2* de 2016) ou encore leur durée.

S'agissant des mesures prévoyant la conservation préventive des adresses IP et des données relatives à l'identité civile aux fins de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, la Cour impose le même type de réserves (points 152 s.), comme s'agissant des mesures prévoyant la conservation rapide des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité grave (points 160 s.).

La réponse conclusive à la question est alors (point 168) que : « l'article 15, paragraphe 1, de la directive 2002/58, s'il s'oppose à des mesures législatives prévoyant une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, il ne s'oppose pas à des mesures législatives, 1) permettant, aux fins de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, la décision prévoyant cette injonction pouvant faire l'objet d'un contrôle effectif soit par une juridiction, soit par une entité administrative indépendante, cette injonction ne pouvant être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace ; 2) prévoyant une conservation ciblée des données relatives au 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, pour une période temporellement limitée au strict nécessaire, mais renouvelable ; 3) prévoyant une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ; 4) prévoyant une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, 5) permettant une injonction faite aux fournisseurs de services de communications électroniques, 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 relatives au trafic et des données de localisation, le tout dès lors que ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus ».

Sur la deuxième question, celle concernant l'obligation faite aux fournisseurs d'adopter des mesures de traitement automatisé assurant le recueil en temps réel des données, et le recueil en temps réel des données de localisation, la Cour observe que les articles L. 851-1 et suivants du CSI n'imposent une exigence spécifique de conservation de ces données, mais des mesures permettant de détecter, en fonction de critères définis, des connexions susceptibles d'identifier une menace terroriste. La réponse de la Cour, analysant le contenu réel des textes français conclut alors (point 192) que : « l'article 15, paragraphe 1, de la directive 2002/58 ne s'oppose pas à une réglementation imposant aux fournisseurs de services de communications électroniques de recourir, d'une part, à l'analyse automatisée ainsi qu'au recueil en temps réel, notamment, des données relatives au 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 1) le recours à l'analyse automatisée est limité à des situations dans lesquelles un État membre se trouve confronté à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, l'ensemble pouvant faire l'objet d'un contrôle effectif ; 2) le recours à un recueil en temps réel des données relatives au trafic et des données de localisation limité aux personnes à l'égard desquelles il existe une raison valable de soupçonner qu'elles sont impliquées d'une manière ou d'une autre dans des activités de terrorisme, soumis à un contrôle préalable, par une juridiction ou une entité administrative indépendante ».

Sur la question de l'obligation faite aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement de la conservation généralisée et indifférenciée, notamment, des données à caractère personnel afférentes à ces services, au regard de l'article 6 de la LCEN, la Cour considère que l'ingérence est trop importante de sorte que (point 212) l'article 23, paragraphe 1, du règlement 2016/679, s'oppose à une réglementation nationale imposant aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement la conservation généralisée et indifférenciée, notamment, des données à caractère personnel afférentes à ces services, ce dont on peut déduire qu'il ne s'opposerait sans doute à des mesures limitées dans les conditions identifiées dans les réponses aux précédentes questions.

Au final, il en résulte que les dispositions françaises, notamment celles du Code de la sécurité intérieure sont validées, y compris le traitement en temps réel tel que l'envisagent les articles L. 851-1 du CSI mais précisément, incluant le traitement préventif, parce que (ou à condition que) ce traitement s'effectue dans les conditions prévues par la Cour, à savoir un traitement finalisé, temporellement limité et soumis à autorisation, même s'il renvient désormais au Conseil d'Etat, en retour, d'apprécier concrètement ces règles à l'aune de l'arrêt de la Cour.

Tiphaine Colot et Daniel Mainguy