COUR DE JUSTICE

DE

L'UNION EUROPÉENNE

Audience de plaidoiries du 9 septembre 2019

Affaires C-511/18 et C-512/18

sur renvois préjudiciels du Conseil d'État (FRANCE)

OBSERVATIONS ORALES
POUR FRENCH DATA NETWORK

Monsieur le Président,
Mesdames, messieurs les membres de la Cour de justice,
Monsieur l'avocat général,

1. . Comme l'a dit mon confrère de Privacy International, c'est la première fois qu'est soumis à votre office un renvoi préjudiciel portant sur le respect, par le droit français, des règles de l'Union garantissant la confidentialité des communications électroniques.

2. Et ce droit français, en matière de surveillance et de renseignement, a une histoire particulière, une genèse dont le rappel peut utilement éclairer la Cour.

3. En effet, certaines des dispositions dont la Cour est saisie (notamment celles relatives aux analyses automatisées en temps réel) ont été introduite par la loi du 24 juillet 2015, initialement à titre « expérimental et temporaire » jusqu'au 31 décembre 2018, le Gouvernement devant adresser au Parlement français un rapport d'application de cette mesure au plus tard le 30 Juin 2018. C'est d'ailleurs ce que rappelle le Gouvernement français dans ses observations (§ 14) qui, dans une note de bas de page, indique cependant que ces dispositions ont d'ores et déjà été prorogées jusqu'au 31 décembre 2020.

4. Ce faisant, ces dispositions rejoignent la désormais très longue liste de celles qui, toutes en matière de prévention et de lutte contre la criminalité, débutent leur vie juridique sous la forme d'une disposition expérimentale et qui, *in fine*, sont pérennisées voire codifiées en droit français.

5. Cette tendance a débuté en 2001, avec la loi relative à la sécurité quotidienne qui a notamment introduit, à titre « temporaire », l'obligation fait aux opérateurs téléphoniques de conserver les données et de les transmettre aux autorités judiciaires sur demande et qui est directement l'objet des deux premières questions de chaque affaire qui vous est soumise. Là aussi un rapport d'évaluation de l'application de la loi devait être communiqué au Parlement par le Gouvernement. Il n'en fut rien. Et toutes les dispositions dites « temporaires et expérimentales » de la loi du 15 novembre 2001 furent pérennisées par la loi du 18 mars 2003 pour la sécurité intérieure.

6. Sans qu'il soit le lieu ici de les énumérer en détail, près 11 textes législatifs comportant des dispositions initialement expérimentales et temporaires dans le domaine de la sécurité publique sont intervenus en France depuis 2001. Et toutes, sans exception, ont été prorogées, puis définitivement pérennisées, sans que l'évaluation de leur application ne soit d'ailleurs souvent même produite.

7. Cette succession ininterrompue de soi-disant expérimentations qui n'en sont pas, de pérennisation sans réelle évaluation, modifie imperceptiblement, par étapes, l'équilibre global du système juridique français. En effet, toutes ces mesures, qu'il s'agisse de celles ayant donné lieu aux questions dont votre Cour est saisie, ou de celles ayant modifié le code de procédure pénale en matière de perquisition ou de réquisitions pour

ne citer que ces quelques exemples, vont dans le sens de l'accroissement des pouvoirs d'investigation et de collecte de données, y compris de la part de services de police administrative et de renseignement.

8. Ces glissements successifs modifient imperceptiblement, mais durablement, l'équilibre toujours instable entre liberté et sécurité. Et au travers de la question technique et juridique du champ d'application de la Directive 2002/58, c'est donc une plus large et plus grave qui vous est posée : celle de la nécessité de garantir cet équilibre. Et de le garantir en s'assurant que les conditions posées par la Cour, de proportionnalité et de nécessité des mesures de surveillance sont respectées, et que, compte tenu de l'ingérence que comportent les analyses de données en question ici, les critères utilisés pour ces analyses sont effectivement objectifs, *« spécifiques, fiables et non discriminatoires »* comme vous l'avez exprimé avec clarté dans l'avis PNR du 26 Juillet 2017 (§172).

9. Outre cette genèse particulière, le droit français possède une autre singularité qui tient à l'existence et au rôle de la CNCTR (Commission nationale de contrôle des techniques de renseignement). S'agissant des garanties procédurales nécessaires, la Cour a considéré qu'il était « *essentiel que l'accès des autorités nationales compétentes aux données conservées soit, en principe, sauf cas d'urgence dûment justifiés,* ***subordonné à un contrôle préalable effectué*** *soit par une juridiction soit par une entité administrative indépendante, et que la* ***décision*** *de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités présentée »* (arrêt Tele2, point 120, voir aussi : arrêt Digital Rights, point 62).

10. Or, l'autorisation de mise en œuvre d'un recueil des données en temps réel ne peut être considérée comme satisfaisant les garanties procédurales requises par la Cour, puisque ces dernières ne comprennent qu'un simple *avis* de la CNCTR, sans valeur contraignante. Loin donc d'une « décision » comme l'exige la Cour.

11. Et le fait que les membres de la CNCTR puissent saisir le Conseil d'Etat dans l'hypothèse où le Premier ministre le suivrait pas l'avis de la Commission ne saurait être assimilé à un pouvoir de décision. En effet, cette éventuelle saisine du Conseil d'Etat n'a pas d'effet suspensif sur la mesure d'une part et, d'autre part, si décision il y

a, elle serait prise *a posteriori* et par le juge administratif et non **préalablement** à la mise en œuvre de la mesure comme le demande la Cour.

12. A cette faiblesse procédurale s'ajoute une autre, plus factuelle mais tout aussi importante : l'extrême faiblesse des moyens humains et techniques de la CNCTR. En effet, la CNCTR ne compte que 17 agents pour un budget de 2,9 millions d'euros. Mais surtout, bien qu'il soit difficile d'obtenir des informations précises en la matière, celles publiques indiquent que parmi ces 17 agents ne figurerait qu'un seul ingénieur…. Dans ces conditions, on peut légitiment s'interroger sur la portée du contrôle *a priori* et de l'avis donné par la CNCTR sur des algorithmes, nécessairement complexes, développés par des services de renseignement dotés de puissants moyens humains et techniques… L'effectivité du contrôle n'est pas qu'une question juridique, loin s'en faut.

13. Ceci étant dit, j'en viens maintenant aux observations sur le fond que FDN souhaite produire, en particulier sur trois aspects sur lesquels la Cour a sollicité que les plaidoiries se concentrent.

14. **Le premier point a trait au champ d'application de la Directive 2002/58** et à la question sur l'opportunité de distinguer les mesures **directement** mises en œuvre par l'Etat **sans imposer** d'obligations aux fournisseurs de service d'une part, **des mesures imposant** auxdits fournisseurs des obligations de traiter des données dans le cadre de leur activité même si les mesures en cause dérogent au principe de confidentialité d'autre part.

15. A la réflexion, il nous semble que la question devrait comprendre une troisième possibilité, celle de l'hypothèse où les activités des services de renseignement, de part leur nature, affectent substantiellement l'activité de l'opérateur, voire peuvent le conduire à ne pas être en capacité de respecter ses obligations sans lui imposer de mesures particulières. Et l'actualité très récente atteste qu'il ne s'agit pas d'une hypothèse d'école, loin s'en faut.

16. Prenons les choses dans l'ordre d'évidence : la première évidence est que, comme l'a affirmé la Cour, relève du champ d'application de la Directive une mesure législative qui impose une obligation de traitement de données personnelles à l'opérateur (*Tele2/Watson* §75).

17. A l'inverse, et il s'agit de la deuxième évidence, les opérations menées exclusivement par les agences de renseignement et n'ayant aucune conséquence, aucun impact sur les réseaux de communications électroniques, et n'exigeant aucune participation des opérateurs, nous semblent devoir être exclues du champ d'application de la directive 2002/58. Il en va, par exemple, de la pose d'un traceur GPS dans un véhicule.

18. Mais qu'en est-il des situations intermédiaires ? Celles où les activités des services, de part leur nature même, ont une incidence, des conséquences substantielles sur l'activité des opérateurs voire sur le respect de leurs obligations ? Doit-on considérer que de telles activités se situent en dehors du champ de la Directive ? Nous ne le pensons pas.

19. Cette question est très importante French Data Network que je représente ici, qui est un opérateur associatif, fondé en 1992 et qui est le plus ancien fournisseur d'accès à Internet en France.

20. En effet, que penser des interceptions de communications sur un réseau, réalisées sans le concours d'un opérateur et, donc, à ses dépens, et qui sont susceptibles de faire échec à ses obligations de sécurité, obligations précisément introduites par la Directive 2002/58 et dont l'inobservation est d'ailleurs sanctionnée ?

21. Cette hypothèse est expressément prévue en droit français puisque l'article 323-8 du code pénal (créé par loi du 24 Juillet 2015) a introduit une exemption de responsabilité pénale au profit des services spécialisés du renseignement qui peuvent, pour assurer hors du territoire national (donc en Europe) la protection des intérêts fondamentaux de la Nation : (i) accéder ou se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données ; (ii) entraver ou de fausser le fonctionnement d'un système de traitement automatisé, (iii) importer, détenir, offrir, céder ou mettre à disposition un équipement, un instrument, un programme

informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs de ces infractions.

22. En Belgique, dans l'affaire du piratage de l'opérateur Belgacom et selon la presse Belge, l'enquête menée par le parquet fédéral aurait établi que l'opération d'infiltration aurait été menée par les services secrets d'un pays membre de l'Union.

23. Nous ne pensons pas que ces mesures devraient être exclues du champ de l'UE du seul fait qu'elles poursuivent des finalités tenant à la sécurité nationale et qu'elles sont réalisées par l'Etat sans le concours des opérateurs. Nous pensons, au contraire, que **dès lors que ces mesures affectent (qu'elles possèdent une incidence) sur l'activité d'un opérateur et qu'elles remettent en cause sa capacité de respecter son obligation de garantir la confidentialité des communications elles doivent relever du champ du droit de l'Union**.

24. Le fait de considérer que le droit de l'Union s'applique dans cette hypothèse a pour unique objectif et pour seul effet de s'assurer que ces mesures, lorsqu'elles doivent être mises en œuvre, respectent les critères de proportionnalité, qu'elles sont adaptées et limitées au strict nécessaire dans une société démocratique au sens droit de l'UE et de la Charte.

25. Car n'oublions pas que la confidentialité des réseaux des opérateurs est la condition première et *sine qua non* de la confiance des utilisateurs dans ces réseaux, personnes physiques et personnes morales confondues. Et que, sans confiance, économiquement il ne peut y avoir de croissance dans les services numériques, et que, sans confiance, politiquement, s'installe la défiance qui ronge nos démocraties.

26. La deuxième question de la Cour sur laquelle FDN souhaite tout particulièrement insister est la suivante : c**omment le caractère intrusif des mesures visant l'accès aux données des opérateurs peut-il être apprécié en comparaison de celles tendant à l'accès au contenu ?**

27. Ce faisant la Cour se fonde sur la distinction traditionnelle entre données techniques de trafic et de localisation, d'une part, et le contenu des communications, d'autre part,

l'accès aux premières n'étant pas de nature, selon la Cour, à porter atteinte au *« contenu essentiel »* des droits fondamentaux consacrés aux articles 7 et 8 de la Charte (Tele2 Sverige § 101). Cette *summa divisio* nous semble devoir être réinterrogée, en particulier dans le cadre du droit français, mais surtout au vu du progrès technique, de la capacité d'analyse algorithmique actuelle et des rapides développements de l'IA.

28. Comme l'a déjà indiqué la Cour, prises dans leur ensemble, ces données techniques permettent de tirer des conclusions très précises concernant la vie privée des personnes, telles que leurs habitudes de la vie quotidienne, les lieux de séjour, les déplacements ou autre activités, les relations sociales, les milieux sociaux fréquentés. Les profils des personnes ainsi établis sont une *« information tout aussi sensible au regard du droit au respect de la vie privée que le contenu même des communications »* a considéré la Cour dans son arrêt du 21 décembre 2016 (Telesverige2 § 99). Dès lors pourquoi maintenir cette distinction ?

29. En effet, parmi les données techniques dont il est question dans le droit français, figure également l'URL, c'est-à-dire l'adresse du site et de la page internet consultée. La frontière entre données technique et données de contenu devient particulièrement ténue ici, et il suffit pour s'en convaincre de lire l'exemple fourni par le Gouvernement dans sa réponse au § 29.

30. S'agissant précisément de l'URL, il est intéressant de relever que la CNIL (autorité de protection des données en France), saisie pour avis du décret d'application relatif aux techniques de renseignement (avis du 17 décembre 2015) a considéré que l'URL est *« porteuse **par nature** des informations consultées »* : donc d'informations relatives au contenu. C'est la raison pour laquelle, la CNIL était défavorable à la transmission de l'URL au titre des informations recueillies par l'autorité administrative auprès des opérateurs de communications électroniques. La CNIL n'a malheureusement pas été suivie par le Gouvernement sur ce point, ce qui est souvent le lot des avis des autorités administratives en France.

31. Pour se convaincre définitivement de la fragilité de la distinction entre données techniques été données de contenu, j'invite la Cour à lire l'étude publiée en 2016 par

trois professeurs de l'Université de Stanford aux Etats-Unis (et dont je tiens les références à sa disposition : Evaluating the privacy properties of telephone metadata, dans la revue PNAS proceeding of the national academy of sciences of the United states of America https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4878528/).

32. Cette étude, réalisée à partir des seules métadonnées des téléphones portables de personnes volontaires, donc avec moins de données que celles collectées par les services de renseignement français, a permis de déduire, par inférence, que le participant volontaire C possédait des armes à feu, que le participant B était atteint d'arythmie cardiaque et que le participant A souffrait de sclérose en plaque (données éminemment « sensibles » pour les personnes concernées, également au sens juridique du terme en application de l'article 9 du RGPD).

33. Il est évident que le progrès technique et celui de l'intelligence artificielle en particulier ne vont faire que faciliter la possibilités de réaliser de telles inférences à partir des métadonnées et d'en déduire des conclusions particulièrement intrusives sur les personnes, sur leur profil, leur vie privée, leurs opinions politiques, leur santé.

34. Dans ces conditions, nous appelons la Cour a faire preuve, non pas d'audace, mais de pragmatisme : d'un pragmatisme qui prenne en compte l'état de l'art technologique d'aujourd'hui. Car la distinction entre données techniques et contenu s'estompant, le caractère intrusif des mesures visant à y accéder aux premières doit être désormais considéré comme équivalent à celui permettant l'accès au contenu des communication. Aujourd'hui, et encore davantage demain, les deux mesures sont désormais susceptibles de porter atteinte, à nos yeux, au contenu essentiel des droits fondamentaux consacrés aux articles 7 et 8.

35. **Le dernier point** sur lequel FDN souhaite concentrer sa plaidoirie a trait à l'interrogation de la Cour sur les conditions permettant à un accès général aux données d'être considéré comme *« respectant le contenu essentiel du droit au respect de la vie privée et le caractère strictement nécessaire dans une société démocratique »* ? (Question 3).

36. L'une de ces conditions, qui n'est pas la seule mais qui est la première d'entre elle, est l'information des personnes. Car sans information, aucun droit ni recours ne peut être exercé par les personnes. C'est ce qu'a rappelé avec force la Cour dans ses arrêts Tele2 Sverige 2 (§ 121) et dans son avis PNR (26 Juillet 2017 § 220) : cette information est ***« nécessaire »*** pour permettre aux personnes d'exercer leurs droits.

37. Que cette information puisse, au cas d'espèce, être différée dans le temps afin de ne pas compromettre les enquêtes, c'est incontestable. Que cette information puisse intervenir même quelques années après la mesure, c'est probablement nécessaire dans certains cas. Mais que le principe de l'information des personnes soit garanti l'est tout autant.

38. A cet égard, le droit français applicable aux affaires dont la Cour est saisie est d'un silence assourdissant en la matière : aucune information des personnes n'est prévue, à aucun moment, de toute éternité.

39. Cette situation, particulièrement grave, est d'autant plus surprenante en droit français que la Cour de cassation a établi de longue date que ce qui caractérise la collecte déloyale de données, délit puni d'une peine de 5 ans d'emprisonnement et de 300 000 euros d'amende (article 226-18 du code pénal), est le fait de collecter les données à *« l'insu des personnes »*. En effet, la Cour de cassation a affirmé, en matière pénale, qu'est « *déloyal le fait de recueillir, à leur insu »* des adresses électroniques de personnes physiques sur l'espace public d'Internet, car ce procédé fait **obstacle** à l'exercice de leurs droits [1]. (Arrêt du 14 mars 2006).

40. Il nous semble donc difficilement envisageable de considérer qu'un régime de collecte de données, fut-il fondé sur la légitime finalité de lutte et de prévention du terrorisme, ne prévoit aucune modalité d'information des personnes dans le temps, organisant de ce seul fait un système pérenne de collecte déloyale qui, dans le droit commun, constitue un délit. Car l'existence de l'information des personnes, même différée dans le temps, est ce qui sépare une société démocratique d'une société de surveillance.

Sous toutes réserves, seul le prononcé faisant foi.

YANN PADOVA

AVOCAT AU BARREAU DE PARIS

1 Cour de cassation, Ch. Crim., 14 mars 2006