La jurisprudence sur la conservation des données des communications électroniques et son impact sur les législations nationales et les procédures pénales

Georges Ravarani, Vice-président honoraire de la Cour européenne des droits de l'homme, Strasbourg

Jurisprudence de la Cour européenne des droits de l'homme

1. Le respect de la vie privée est une valeur fondamentale protégée par l'art. 8 de la Convention européenne des droits de l'homme (la Convention). La Cour européenne des droits de l'homme (la Cour européenne des droits de l'homme ou la Cour) a, dès ses débuts, développé une jurisprudence complète visant à protéger cette valeur fondamentale.

2. Le progrès technologique constitue un défi majeur pour la sauvegarde de la vie privée car, d'une part, les individus bénéficient d'une gamme élargie de moyens pour communiquer en privé mais, d'autre part, il existe des moyens sans précédent permettant l'interception des communications et la conservation des données, ce qui entraîne à son tour des défis majeurs pour la protection des données à caractère personnel. Depuis ses débuts, la Cour européenne des droits de l'homme s'efforce de protéger les individus contre la conservation et le traitement abusifs des données à caractère personnel.

3. Au fil des ans, la Cour a examiné de nombreuses situations dans lesquelles des questions liées à ce problème ont été soulevées. Un large éventail d'opérations impliquant des données à caractère personnel, telles que la collecte, le stockage, l'utilisation et la diffusion de ces données, est désormais couvert par la jurisprudence de la Cour européenne des droits de l'homme. Cette jurisprudence est en constante évolution, parallèlement au développement rapide des technologies de l'information et de la communication.

4. Contrairement à ce que prévoit la Charte des droits fondamentaux de l'UE, le droit à la protection des données à caractère personnel n'est pas un droit autonome parmi les divers droits et libertés prévus par la Convention. La Cour européenne des droits de l'homme a néanmoins reconnu que la protection des données à caractère personnel revêt une importance fondamentale pour la jouissance par une personne de son droit au respect de la vie privée et familiale, du domicile et de la correspondance, tel qu'il est garanti par l'article 8 de la Convention. Cet article est le principal vecteur de protection des données à caractère personnel dans le système de la Convention, même si des considérations liées à cette

protection peuvent également entrer en jeu dans le cadre d'autres dispositions de la Convention et de ses protocoles.

5. L'expression « données à caractère personnel » a une définition large. La Cour européenne des droits de l'homme s'est souvent référée à la Convention n° 108 du Conseil de l'Europe, entrée en vigueur en 1985 et mise à jour en 2018, dont le but est « d'assurer sur le territoire de chaque Partie à toute personne physique [...] le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant » (article 1). La Cour a clairement indiqué qu'en vertu de l'article 2 de la Convention n° 108, la notion de données à caractère personnel est définie comme « toute information se rapportant à une personne physique identifiée ou identifiable ». Ces données couvrent non seulement les informations identifiant directement une personne (la « personne concernée »), telles que le nom et le prénom, mais aussi tout élément identifiant indirectement une personne, tel qu'une adresse IP dynamique. Même si la question de la protection des données à caractère personnel semble concerner principalement les personnes physiques, en ce qui concerne leur droit au respect de la vie privée (article 8), les personnes morales peuvent également invoquer ce droit devant la Cour si elles sont directement affectées par une mesure qui porte atteinte à leur droit au respect de leur « correspondance » ou de leur « domicile ».

Les données à caractère personnel peuvent prendre de nombreuses formes, mais aux fins de la présente intervention, il suffit de souligner que les communications électroniques telles que les données Internet, la messagerie et les communications téléphoniques sont couvertes par le concept de données à caractère personnel.

6. En vertu de l'article 2 de la Convention n° 108, le « traitement des données » comprend : « toute opération ou tout ensemble d'opérations effectuées sur des données à caractère personnel, telles que la collecte, le stockage, la conservation, la modification, l'extraction, la communication, la mise à disposition, l'effacement ou la destruction de ces données, ou l'exécution d'opérations logiques et/ou arithmétiques sur ces données ». Le développement des technologies a entraîné une augmentation des types d'opérations sur les données à caractère personnel pouvant constituer un traitement.

7. La conservation par une autorité publique d'informations relatives à la vie privée d'une personne, quelle que soit la manière dont ces informations ont été obtenues, constitue une ingérence dans le droit au respect de la vie privée de la personne concernée au sens de l'article 8, que les données soient ou non utilisées par la suite. Dans la plupart des cas où le traitement de données à caractère personnel était destiné à permettre aux autorités de mener une enquête sur la personne concernée ou de recueillir des preuves dans le cadre d'une procédure judiciaire devant les juridictions nationales, la Cour a estimé que ce traitement entrait dans le

champ d'application de l'article 8 et avait entraîné une ingérence dans le respect de la vie privée de la personne concernée.

8. L'article 8 est un droit qualifié en ce sens que le paragraphe 2 de cette disposition permet en fait des ingérences dans le droit, à condition qu'elles soient conformes à la loi et nécessaires dans une société démocratique, c'est-à-dire pour la prévention du crime.

9. Les intérêts des personnes concernées et de la communauté dans son ensemble en matière de protection des données à caractère personnel peuvent être contrebalancés par l'intérêt légitime à la prévention du crime. Afin de protéger leur population comme il se doit, les autorités nationales peuvent légitimement mettre en place des bases de données comme moyen efficace de contribuer à la répression et à la prévention de certaines infractions, y compris les formes de criminalité les plus graves, telles que les infractions sexuelles. Si la collecte initiale de ces informations vise à établir un lien entre une personne donnée et le délit dont elle est soupçonnée, leur conservation poursuit l'objectif plus large d'aider à l'identification de futurs délinquants.

La Cour européenne des droits de l'homme a toujours considéré qu'elle ne pouvait remettre en cause la finalité préventive de ces registres. En effet, la lutte contre la criminalité, et en particulier contre la criminalité organisée et le terrorisme, qui est l'un des défis auxquels sont confrontées les sociétés européennes d'aujourd'hui, dépend dans une large mesure de l'utilisation des techniques scientifiques modernes d'enquête et d'identification.

10. En même temps, la protection des données à caractère personnel étant d'une importance fondamentale pour la jouissance par une personne de son droit au respect de la vie privée et familiale, tel que garanti par l'article 8 de la Convention, le droit interne doit prévoir des garanties appropriées pour empêcher toute utilisation des données à caractère personnel qui serait incompatible avec les garanties de cet article.

En vertu de l'article 6 de la Convention n° 108, les données à caractère personnel qui révèlent l'origine raciale, les opinions politiques, les convictions religieuses ou autres, ainsi que les informations relatives à la santé ou à la vie sexuelle d'une personne ou à d'éventuelles condamnations pénales, ne peuvent faire l'objet d'un traitement automatisé que si le droit interne prévoit des garanties appropriées. Les informations relevant de ces catégories, qualifiées de « sensibles » par la Cour, justifient à ses yeux un degré de protection accru.

Le caractère intrinsèquement privé de ces informations impose à la Cour d'examiner attentivement toute mesure étatique autorisant leur conservation et leur utilisation par les autorités sans le consentement de la personne concernée.

Il convient de noter qu'en tout état de cause, pour que l'article 8 entre en jeu, les résultats du traitement des données à caractère personnel doivent atteindre un certain niveau de gravité et porter atteinte à la jouissance personnelle du droit au respect de la vie privée. Or, il est difficile d'imaginer que la conservation des données relatives aux communications électroniques ne soit pas sérieuse.

11. Dans son examen de la justification de l'ingérence par les autorités publiques, la Cour européenne des droits de l'homme a recours à sa procédure traditionnelle en trois étapes pour déterminer si une ingérence dans un droit qualifié est conforme à la Convention, c'est-à-dire si elle est prévue par la loi, poursuit un but légitime et est nécessaire dans une société démocratique.

12. L'évolution constante des progrès technologiques a permis d'aller au-delà des interceptions individuelles ciblées et de recourir à des interceptions de masse qui représentent un défi encore plus grand pour la vie privée. La Cour européenne des droits de l'homme a donc été obligée d'adapter sa jurisprudence aux nouveaux développements techniques. Quelques considérations supplémentaires concernant les spécificités des interceptions de masse seront ajoutées à la fin.

13. Légalité : La Cour a examiné dans un certain nombre d'affaires la question de savoir si l'exigence, énoncée à l'article 5 de la Convention n° 108, selon laquelle les données à caractère personnel faisant l'objet d'un traitement automatisé doivent avoir été collectées et traitées loyalement et licitement, a été ou non respectée. Dans certains cas, la Cour a constaté une violation de l'article 8 uniquement en raison de l'absence de base juridique au niveau national pour autoriser des mesures susceptibles d'interférer avec les droits concernés. Dans d'autres cas, la Cour a constaté une violation de l'article 8 au motif que le droit interne, censé protéger les données à caractère personnel, était inaccessible ou confidentiel ou n'était pas suffisamment clair et prévisible.

14. Dans le contexte spécifique des mesures de surveillance secrète, telles que l'interception des communications, la Cour a estimé que le terme « prévisibilité » ne peut être compris de la même manière que dans de nombreux autres domaines. Selon elle, cela ne peut signifier qu'un individu devrait être en mesure de prévoir quand les autorités sont susceptibles d'avoir recours à de telles mesures afin qu'il puisse adapter son comportement. Toutefois, les risques d'arbitraire sont évidents, surtout lorsqu'un pouvoir exécutif est exercé en secret. Il est donc

essentiel de disposer de règles claires et détaillées sur les mesures de surveillance secrète, d'autant plus que les technologies disponibles sont de plus en plus sophistiquées. Le droit interne doit être suffisamment clair pour donner aux citoyens une indication adéquate sur les circonstances et les conditions dans lesquelles les autorités publiques sont habilitées à recourir à de telles mesures. En outre, la loi doit indiquer l'étendue du pouvoir discrétionnaire conféré aux autorités compétentes et les modalités de son exercice avec suffisamment de clarté pour assurer à l'individu une protection adéquate contre les ingérences arbitraires.

15. Dans sa jurisprudence relative à l'interception de communications dans le cadre d'enquêtes pénales, la Cour a établi que, pour prévenir les abus de pouvoir, la loi doit au moins énoncer les six éléments suivants (« garanties Weber ») : la nature des infractions pouvant donner lieu à une ordonnance d'interception ; la définition des catégories de personnes dont les communications peuvent être interceptées ; le délai d'exécution de la mesure ; la procédure à suivre pour l'examen, l'utilisation et la conservation des données collectées ; les précautions à prendre pour la transmission des données à d'autres parties ; et les circonstances dans lesquelles les données d'interception peuvent ou doivent être effacées ou détruites.

16. Le contrôle et la surveillance des mesures de surveillance secrète peuvent intervenir à trois stades : au moment où la surveillance est ordonnée pour la première fois, pendant qu'elle est exécutée ou après qu'elle a pris fin. En ce qui concerne les deux premières étapes, la nature et la logique même de la surveillance secrète exigent que non seulement la surveillance elle-même mais aussi le contrôle qui l'accompagne soient effectués à l'insu de l'individu. Par conséquent, étant donné que l'individu sera nécessairement empêché d'exercer un recours effectif de son propre chef ou de participer directement à toute procédure de réexamen, il est essentiel que les procédures mises en place fournissent elles-mêmes des garanties adéquates et équivalentes pour la sauvegarde de ses droits. Dans un domaine où les abus dans les cas individuels sont potentiellement si faciles et peuvent avoir des conséquences si néfastes pour la société démocratique dans son ensemble, la Cour a estimé qu'il est en principe souhaitable de confier le contrôle de surveillance à un juge, le contrôle juridictionnel offrant les meilleures garanties d'indépendance, d'impartialité et de régularité de la procédure.

En ce qui concerne la troisième étape, après la fin de la surveillance, la question de la notification ultérieure des mesures de surveillance est un facteur pertinent pour évaluer l'efficacité des recours devant les tribunaux et, partant, l'existence de garanties effectives contre l'abus des pouvoirs de surveillance. En principe, les possibilités de recours au juge par l'individu concerné sont limitées si celui-ci n'est pas informé des mesures prises à son insu et ne peut donc pas en contester la légalité a posteriori ou, à titre subsidiaire, si toute personne qui soupçonne qu'elle a fait l'objet d'une surveillance peut saisir les tribunaux, dont la

compétence ne dépend pas de la notification des mesures prises à la personne faisant l'objet d'une surveillance.

17. Légitimité : Dans un certain nombre d'affaires, la Cour a examiné si l'exigence, énoncée à l'article 5 de la Convention n° 108, selon laquelle les données à caractère personnel faisant l'objet d'un traitement automatisé doivent avoir été collectées pour des finalités explicites, déterminées et légitimes, avait été ou non respectée. Dans ces cas, l'examen des finalités légitimes qui peuvent justifier une ingérence dans l'exercice des droits de l'article 8, tels qu'énumérés au paragraphe 2, est assez succinct. Ces buts sont la protection de la sécurité nationale, de la sûreté publique et du bien-être économique du pays, la défense de l'ordre et la prévention des infractions pénales, la protection de la santé ou de la morale, ou la protection des droits et libertés d'autrui. La Cour constate généralement l'existence d'un ou plusieurs de ces buts légitimes invoqués par le gouvernement.

18. Nécessité : Pour être nécessaire dans une société démocratique, toute mesure portant atteinte à la protection des données à caractère personnel au titre de l'article 8 doit répondre à un « besoin social impérieux » et ne doit pas être disproportionnée par rapport aux buts légitimes poursuivis. Bien que les États jouissent d'une large marge d'appréciation pour choisir la meilleure façon d'atteindre le but légitime, la Cour européenne des droits de l'homme examine, dans le cadre de son contrôle européen, les raisons invoquées par le gouvernement, qui doivent être pertinentes et suffisantes. S'il appartient aux autorités nationales de procéder à l'appréciation initiale à tous ces égards, l'évaluation finale de la nécessité de l'ingérence reste soumise au contrôle de la Cour quant à sa conformité avec les exigences de la Convention.

19. Les facteurs suivants ont été considérés comme pertinents pour l'évaluation de la nécessité :

20. Champ d'application : nature des données stockées. Dans plusieurs affaires, la Cour a mis en cause le large champ d'application du système de stockage des données mis en place par les autorités, qui n'établissait pas de distinction selon la nature ou le degré de gravité de l'infraction ayant donné lieu à la condamnation, ou selon que la personne concernée avait été condamnée, acquittée, relaxée ou simplement mise en garde, après avoir été soupçonnée d'avoir commis une infraction. La Cour estime que les dispositifs mis en place par les autorités pour aider à la répression et à la prévention de certaines infractions ne peuvent pas être mis en œuvre dans le cadre d'une volonté abusive de maximiser les informations qui y sont stockées. En effet, sans le respect de la proportionnalité requise par rapport aux buts légitimes assignés à de tels mécanismes, leurs avantages seraient sans commune mesure avec les atteintes graves qu'ils porteraient aux droits et libertés que les Etats doivent garantir en vertu de la Convention aux personnes relevant de leur juridiction.

21. Il existe un risque de stigmatisation lorsque des personnes qui n'ont été condamnées pour aucune infraction et qui bénéficient de la présomption d'innocence sont traitées de la même manière que les personnes condamnées. Même si la conservation de données privées concernant des personnes soupçonnées d'une infraction mais acquittées ou relaxées ne peut être assimilée à l'expression de soupçons, leur sentiment de ne pas être traitées comme des innocents est renforcé par le fait que leurs données sont conservées indéfiniment au même titre que les données des personnes condamnées, alors que les données des personnes qui n'ont jamais été soupçonnées d'une infraction sont tenues d'être détruites. Par conséquent, le fait qu'une personne ait bénéficié d'une décharge après avoir été soupçonnée d'une infraction justifie qu'elle soit traitée différemment d'une personne condamnée.

22. Même en cas de condamnation, la conservation des données n'est pas automatiquement justifiée. La Cour a examiné une série d'affaires relatives à l'enregistrement dans des bases de données destinées à la répression et à la prévention de la criminalité des données à caractère personnel de personnes condamnées pour des infractions mineures ou même pour une série d'infractions qui n'étaient ni mineures ni particulièrement graves.

23. Durée de conservation et effacement des données. La durée pendant laquelle les autorités décident de conserver les données à caractère personnel d'une personne est un aspect important, bien que non décisif, à prendre en compte pour évaluer si la conservation de données à caractère personnel dans un fichier ou une base de données à des fins policières est ou non proportionnée au but légitime poursuivi.

24. Si l'absence de durée maximale de conservation des données à caractère personnel n'est pas nécessairement incompatible avec l'article 8, des garanties procédurales sont nécessaires lorsque la conservation des données dépend entièrement de la diligence avec laquelle les autorités s'assurent de la proportionnalité de la période de conservation des données. Si aucun délai effectif n'est prévu, il doit exister une procédure judiciaire permettant à la personne intéressée de demander l'effacement des données dont la conservation n'est plus nécessaire. Dans de tels cas, lorsqu'il n'y a pas de délai automatique pour la conservation des données, l'existence ou l'absence d'un contrôle indépendant de la justification de la conservation des informations selon des critères définis tels que la gravité de l'infraction, la force des soupçons pesant sur la personne, les condamnations antérieures et toute autre circonstance particulière, constitue une garantie majeure pour assurer la proportionnalité des périodes de conservation des données. La Cour s'est montrée satisfaite d'un système qui ne prévoyait pas de durée maximale de conservation des données s'il existait un examen périodique indépendant de la nécessité de continuer à les conserver. L'existence, au niveau national, d'une procédure judiciaire de suppression des données prévoyant un contrôle indépendant de la justification de la conservation des informations selon des critères définis

et offrant des garanties adéquates et effectives du droit au respect de la vie privée de la personne concernée est un facteur important dans la mise en balance des différents intérêts en présence. La Cour n'a pas constaté de violation de l'article 8 dans des affaires où, même si les données avaient été conservées pendant de « longues » périodes allant jusqu'à trente ans, voire indéfiniment, la personne concernée avait bénéficié d'une procédure judiciaire garantissant un contrôle indépendant de la justification de la conservation de ses données selon des critères définis, lui permettant d'obtenir l'effacement des données avant l'expiration de la période maximale prévue par la loi ou, en cas de conservation indéfinie des données, dès que cette conservation n'avait plus de raison d'être.

25. Il va de soi que la durée maximale de conservation doit être effective. Une durée maximale de conservation des données à caractère personnel prévue par le droit interne peut s'apparenter, en pratique, davantage à une norme qu'à un véritable maximum si les chances d'acceptation d'une demande d'effacement des données avant l'expiration de la durée prévue par la loi sont purement hypothétiques.

26. Limitation de l'utilisation des données à la finalité pour laquelle elles ont été enregistrées. La Cour a estimé qu'il est important de limiter l'utilisation des données à la finalité pour laquelle elles ont été enregistrées. Ainsi, par exemple, l'utilisation dans le cadre d'une enquête disciplinaire de données provenant d'écoutes téléphoniques effectuées dans le cadre d'une enquête pénale, et par conséquent pour une finalité différente de celle qui avait justifié leur collecte, a été jugée contraire à l'article 8.

27. Quelques mots pour conclure sur l'interception de masse. Comme souligné dans les affaires Weber et Saravia et Liberty e.a. et répété dans l'affaire Big Brother Watch, les principes applicables aux interceptions ciblées sont fondamentalement les mêmes : l'article 8 est applicable et la décision d'opérer des interceptions ciblées doit être prise dans le respect de l'article 8 de la Constitution. 8 est applicable et la décision d'appliquer un régime d'interception de masse afin d'identifier des menaces pour la sécurité nationale ou contre des intérêts nationaux essentiels continue de relever de la marge d'appréciation des États. Toutefois, en raison des progrès techniques réalisés depuis que la Cour européenne des droits de l'homme s'est prononcée pour la première fois sur les interceptions de masse, qui permettent de dresser un portrait intime d'une personne grâce à la cartographie des réseaux sociaux, au suivi de la localisation, au suivi de la navigation sur Internet, à la cartographie des modes de communication et à la connaissance des personnes avec lesquelles une personne a interagi, et en raison de l'augmentation des abus potentiels, la Cour a ressenti le besoin de développer davantage son approche des interceptions de masse. Elle a constaté que pour déterminer si l'État défendeur a agi dans le cadre de sa marge d'appréciation, la Cour devrait tenir compte d'un éventail de critères plus large que les six garanties de Weber (voir ci-dessus, n° 15).

Dans le contexte de la marge d'appréciation, il ne faut pas perdre de vue qu'il serait difficile pour une cour internationale d'être trop prescriptive quant à l'évaluation de l'imminence des menaces terroristes et quant aux moyens à déployer pour prévenir de telles attaques. La science joue dans les deux sens, les terroristes utilisent aussi des outils de plus en plus sophistiqués. Il ne faut pas non plus oublier que les États ont également une obligation positive au titre de la Convention, à savoir protéger la vie de leurs citoyens, comme le prévoit l'article 2 de la Convention. 2 de la Convention.

28. Plus précisément, en examinant conjointement les notions de « conformément à la loi » et de « nécessité », comme le veut l'approche établie dans ce domaine, la Cour examinera si le cadre juridique interne a clairement défini

1. les motifs pour lesquels l'interception de masse peut être autorisée ;

2. les circonstances dans lesquelles les communications d'un individu peuvent être interceptées ;

3. la procédure à suivre pour l'octroi de l'autorisation ;

4. les procédures à suivre pour la sélection, l'examen et l'utilisation du matériel d'interception ;

5. les précautions à prendre lors de la communication du matériel à d'autres parties ;

6. les limites de la durée de l'interception, le stockage du matériel d'interception et les circonstances dans lesquelles ce matériel doit être effacé et détruit ;

7. les procédures et les modalités de contrôle par une autorité indépendante du respect des garanties susmentionnées et les pouvoirs dont elle dispose pour remédier au non-respect de ces garanties

8. les procédures de contrôle indépendant a posteriori du respect de ces garanties et les pouvoirs conférés à l'organe compétent pour traiter les cas de non-respect.

29. Afin de réduire au minimum le risque d'abus du pouvoir d'interception de masse, la Cour estime que le processus doit être soumis à des « garanties de bout en bout », ce qui signifie que, au niveau national, il convient d'évaluer à chaque étape du processus la nécessité et la proportionnalité des mesures prises, que l'interception de masse doit faire l'objet d'une autorisation indépendante dès le départ, lorsque l'objet et la portée de l'opération sont définis, et que l'opération doit être soumise à une supervision et à un contrôle indépendant a posteriori. De l'avis de la Cour, il s'agit là de garanties fondamentales qui constitueront la pierre angulaire de tout régime d'interception de masse conforme à l'article 8.

30. La conservation des données semble être une histoire sans fin. Et comme toujours avec le progrès scientifique, le droit est désespérément à la traîne, essayant d'encadrer l'utilisation des développements technologiques et d'empêcher les abus les plus flagrants. Mais qu'est-ce qu'un abus ? La lutte contre la criminalité n'en est certainement pas un. L'exercice est donc extrêmement délicat et comme dans tant d'autres domaines, la Cour européenne des droits de l'homme a tenté et tente encore, l'avenir nous dira dans quelle mesure, de trouver un juste

équilibre entre l'utilisation légitime de la conservation des données et les abus qui risquent de porter atteinte à l'État de droit et aux libertés fondamentales des citoyens.