

**COUR EUROPEENNE DES DROITS DE L'HOMME – ARRET DE LA COUR (CINQUIEME SECTION), 30 JANVIER 2020, BREYER C. ALLEMAGNE, REQUETE N°50001/12**

**MOTS CLES : carte SIM prépayées – collecte de données – données personnelles – identification – ingérence proportionnée – opérateurs de téléphonie mobile – respect de la vie privée – sécurité nationale – stockage de données – télécommunications – utilisateurs**

*Par son arrêt du 30 janvier 2020 la Cour européenne des droits de l'Homme est venue se prononcer sur la conservation des données personnelles des utilisateurs de cartes SIM prépayées par les opérateurs de téléphonie mobile et le fait de savoir si cet acte pouvait porter atteinte au droit à la vie privée des intéressés. En retenant que cette mesure était nécessaire à la protection de la sécurité nationale, les juges européens ont convenu que l'obligation tenant à collecter ces données pour permettre l'identification des utilisateurs desdites cartes n'emporte pas violation de l'article 8 de la Convention européenne des droits de l'Homme relatif au droit à la vie privée.*

**FAITS :** En 2004, la loi allemande sur les télécommunications connaît des modifications et implique désormais l'obligation pour les opérateurs de téléphonie mobile de recueillir et conserver les données personnelles des utilisateurs de cartes SIM prépayées comme le numéro de téléphone, le nom ou encore la date de naissance. En 2005, face à cette disposition, deux ressortissants allemands opposés aux surveillances étatiques et bénéficiaires de ce type de cartes, décident alors d'introduire une action devant la Cour constitutionnelle allemande contre les articles de cette loi qui obligent les fournisseurs de services à collecter et stocker ces informations personnelles et qui en permet l'accès aux autorités. En effet, les requérants estiment que les dispositions en question sont incompatibles avec la loi fondamentale allemande.

**PROCEDURE :** Entre temps, une loi du 21 décembre 2007 est venue à nouveau modifier la loi sur les télécommunications, invitant ainsi les requérants à étendre leur recours et à considérer la loi dans sa version en vigueur au 1<sup>er</sup> janvier 2008. Dans une décision du 24 janvier 2012, la Cour constitutionnelle fédérale d'Allemagne a finalement retenu que les dispositions litigieuses étaient justifiées et proportionnées de sorte qu'elles étaient ainsi compatibles avec la loi fondamentale allemande. Les requérants décident alors de saisir la Cour européenne des droits de l'Homme estimant que la conservation de leurs données personnelles procédant de l'utilisation de cartes SIM prépayées porte atteinte à l'article 8 de la Convention tenant au droit au respect de la vie privée. La Cour a introduit la requête le 27 juillet 2012.

**PROBLEME DE DROIT :** La conservation des données personnelles des utilisateurs de cartes SIM prépayées porte-t-elle atteinte au droit à la vie privée tel que protégé par l'article 8 de la Convention européenne des droits de l'Homme ?

**SOLUTION :** La Cour européenne des droits de l'Homme répond par la négative à la question posée estimant que l'obligation de collecte des données des utilisateurs de cartes SIM prépayées, par les opérateurs de téléphonie mobile, à des fins d'identification, n'emporte pas violation du droit à la vie privée et n'est ainsi pas contraire à l'article 8 de la Convention. En effet, si la Cour assure que la conservation des données à caractère personnel des usagers de cartes SIM prépayées constitue une ingérence dans l'exercice du droit à la vie privée, celle-ci est toutefois proportionnée en ce qu'elle est nécessaire dans une société démocratique.



**NOTE :**

La Cour rappelle dans sa décision que la protection des données personnelles relatives aux abonnés joue un rôle fondamental dans l'exercice du droit au respect de la vie privée de sorte que toute utilisation de ces données ne doit pas être contraire aux garanties de l'article 8 de la Convention européenne des droits de l'Homme relatif au droit à la vie privée.

Cependant, il existe des restrictions à cet article 8. En effet, toute atteinte aux droits de l'Homme doit être proportionnée au but légitime poursuivi et l'article 8 en son second paragraphe énumère les buts légitimes qui peuvent justifier une ingérence dans l'exercice du droit à la vie privée, comme la nécessaire protection de la sécurité nationale, retenue en l'espèce.

***La légitime protection de la sécurité nationale nécessaire dans une société démocratique***

Chaque État membre du Conseil de l'Europe bénéficie d'une marge d'appréciation dans le respect des droits de l'Homme et notamment dans l'application de leurs exceptions prévues par la Convention. Ainsi, les autorités nationales jouissent d'une certaine marge de manœuvre dans le choix des moyens permettant d'atteindre l'objectif légitime de protection de la sécurité nationale.

En l'espèce, la Cour a estimé que l'Allemagne n'avait pas enfreint sa marge de manœuvre en choisissant les buts de sécurité nationale et de lutte contre les infractions pénales. En effet, si le gouvernement fédéral allemand a admis que la loi en cause portait bien atteinte au droit à la vie privée des utilisateurs de cartes prépayées, il a néanmoins rajouté que cette ingérence était limitée en ce qu'elle poursuivait des buts légitimes.

Pour admettre cela, dans un premier temps, les juges estiment que cette ingérence est nécessaire car de nos jours, pour prévenir efficacement les infractions, les méthodes d'enquête doivent s'adapter aux moyens de communication modernes

des individus. Ainsi, la Cour considère que cette obligation tenant à conserver les données permet de répondre à l'évolution des modes de communications.

Par cet arrêt, la Cour rappelle à quel point l'objectif légitime de protection de la sécurité nationale peut primer sur les droits des individus. En effet, cette situation est considérée comme un besoin social impérieux par les juges, et même si les requérants estimaient en l'espèce que les opérateurs n'ont pas à collecter les données de leurs clients qui n'ont jamais commis d'infraction, la Cour estime que l'ingérence en question permet d'assurer sécurité et prévention à la société.

La Cour ne s'abstient pas de porter atteinte au droit à la vie privée lorsque le but poursuivi est relatif à la sécurité nationale et à la prévention du crime : tel était le cas par exemple dans son arrêt Ben Faiza contre France du 8 février 2018 où les juges ont toléré l'utilisation de surveillance par GPS dans les enquêtes criminelles, cela au détriment de l'article 8.

***Une atteinte à la vie privée justifiée et proportionnée***

L'ingérence est-elle proportionnée de sorte qu'un juste équilibre soit assuré entre les intérêts publics de l'État et les intérêts privés des individus ? Si l'intérêt de l'État est de protéger sa sécurité nationale par des mesures strictes de surveillance, cela doit se faire en respectant au maximum la vie privée des individus.

Sur ce point, les juges européens soulignent que les données recueillies étaient limitées, de sorte à ne pas être trop personnelles et ne suffire que pour identifier l'utilisateur et cela sur une période définie et limitée avec des moyens de recours et des garanties effectives en cas d'abus comme par exemple en énumérant dans la loi les autorités habilitées à demander accès aux données collectées.

Ainsi, la Cour reconnaît certes qu'il y a eu une ingérence dans l'exercice des droits



des utilisateurs par les requérants mais que celle-ci était conforme aux exigences de la Convention en ce qu'elle est prévue par la loi, poursuit un but légitime et qu'elle est nécessaire dans une société démocratique. De cette façon, si cette ingérence faite au droit à la vie privée semble incontestable en l'espèce, celle-ci est toutefois justifiée et proportionnée au buts légitimes poursuivis de sorte à ce qu'elle ne viole pas l'article 8 de la Convention.

**Candice GUERPILLON**

Master 2 Droit des Médias Électroniques  
AIX-MARSEILLE UNIVERSITÉ, LID2MS-IREDIC 2020



**ARRET :**

COUR EUROPÉENNE DES DROITS DE L'HOMME – ARRÊT DE LA COUR (cinquième section), 30 janvier 2020, requête n°50001/12, *Breyer c. Allemagne*.

[...]

**73.** The Court reiterates that private life is a broad term not susceptible to exhaustive definition.

[...] **79.** The Court has acknowledged that, when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his private life, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security.

[...] **81.** [...] the Court reiterates that the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 of the Convention (*Leander v. Sweden*, 26 March 1987, § 48, Series A no. 116).

[...] **86.** Having regard to the context of the data storage at issue and in particular to the purposes of information requests and the authorities entitled to them under sections 112 and 113 of the Telecommunications Act, the Court accepts the Government's argument that the interference pursued the legitimate aims of public safety, prevention of disorder or crime and the protection of the rights and freedoms of others.

[...] **88.** An interference will be considered "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and if it is proportionate to the legitimate aim pursued. The Court finds that the fight against crime, and in particular against organised crime and terrorism [...], upholding public safety and the protection of citizens constitute "pressing social needs" [...]. It also recognises that modern means of telecommunications and changes in

communication behaviour require that investigative tools for law enforcement and national security agencies are adapted.

[...] **91.** The question, however, remains whether the interference was proportionate and struck a fair balance between the competing public and private interests.

**92.** [...] that only a limited data set was stored. This data did not include any highly personal information or allow the creation of personality profiles or the tracking of the movements of mobile-telephone subscribers. Moreover, no data concerning individual communication events was stored. [...] Moreover, the case has to be distinguished from cases in which the registration in a particular database led to frequent checks or further collection of private information.

[...] **95.** In sum, the Court concludes that the interference was, while not trivial, of a rather limited nature.

[...] **108.** [...] as there is no consensus among the member States concerning collection and storage of limited subscriber information [...] member States had a certain margin of appreciation in choosing the means for achieving the legitimate aims of protecting national security and fighting crime, which Germany did not overstep in the present case.

**109.** Having regard to the above, the Court concludes that the storage of the applicants' personal data by their respective service providers pursuant to section 111 of the Telecommunications Act [...] was proportionate and therefore "necessary in a democratic society".

**110.** There has accordingly been no violation of Article 8 of the Convention.

**FOR THESE REASONS, THE COURT**

**1.** Declares, unanimously, the application admissible;

[...]

