

Concours section : 1er concours d'accès

Epreuve matière : Note de synthèse

N° Anonymat : OEAUX866 OP

Nombre de pages : 4

18.5 / 20

Concours : 1^{er} concours

Epreuve : Note de synthèse

CONSIGNES

- Remplir soigneusement, sur CHAQUE feuille officielle, la zone d'identification en MAJUSCULES.
- Ne pas signer la composition et ne pas y apporter de signe distinctif pouvant indiquer sa provenance.
- Numéroté chaque PAGE (cadre en bas à droite de la page) et placer les feuilles dans le bon sens et dans l'ordre.
- Rédiger avec un stylo à encre foncée (bleue ou noire) et ne pas utiliser de stylo plume à encre claire.
- N'effectuer aucun collage ou découpage de la feuille officielle. Ne joindre aucun brouillon.



La protection des données personnelles de connexion

Adopté le 24 mai 2016, le Règlement général de protection des données consacre la protection des données à caractère personnel en tant que droit fondamental (doc. 1), parmi lesquelles figurent les données personnelles de connexion. Celles-ci correspondent aux données de trafic, établissant les contacts de la personne, la date et la durée de ces échanges, et aux données de localisation, permettant notamment d'obtenir la liste des appels (doc. 7). En cela, l'exploitation de ces données est très utile pour prévenir les atteintes à l'ordre public et rechercher les auteurs d'infractions pénales, ces objectifs ayant valeur constitutionnelle. Il s'agit alors de trouver un équilibre entre la protection des données personnelles de connexion et l'accès à ces données pour la sauvegarde de l'ordre public.

La protection des données personnelles de connexion est ainsi assurée tant par le droit européen que par le droit interne (I) et a été récemment renforcée en matière de procédure pénale (II).

I. La protection des données personnelles de connexion assurée par le droit européen et le droit interne

La réglementation posée par l'Union européenne en matière de protection des données personnelles de connexion a conduit à l'adaptation du droit interne (A), adaptation alimentée par la jurisprudence européenne et nationale (B).

A. La protection des données personnelles de connexion garantie par les textes

Le Règlement général de protection des données, adopté le 24 mai 2016 par l'Union européenne, a pour objectif de garantir la

N°

1/1

protection de ces données à l'échelle de l'Union européenne, le niveau de protection devant être équivalent dans tous les États-membres (doc. 1). Le droit à la protection des données personnelles est aussi garanti par la Charte des droits fondamentaux de l'Union européenne (doc. 4). Dans le domaine répressif, le traitement des données personnelles des personnes impliquées dans une procédure pénale, qu'il s'agisse d'un suspect, d'une personne condamnée, d'une victime ou d'un témoin est encadré par la directive 2016/680/UE (doc. 4 et 5), bien qu'une certaine marge de manœuvre soit laissée aux États-membres (doc. 5). Pour garantir la protection des données personnelles, le RGPD a institué le comité européen de la protection des données, organe indépendant. D'autres autorités comme le Contrôleur européen de la protection des données, ont ensuite été créées (doc. 4).

L'entrée en vigueur du RGPD a conduit à l'adoption, à l'échelle nationale, de la loi du 20 juin 2018 relative à la protection des données personnelles, qui adapte la loi du 6 janvier 1978 au cadre juridique européen. Elle redéfinit ainsi les missions de la Commission nationale de l'informatique et des libertés, qui devient l'autorité nationale de contrôle de l'application du RGPD, et opère désormais un contrôle a posteriori. Son pouvoir de sanction est renforcé, les amendes prononcées pouvant aller jusqu'à 4 % du chiffre d'affaires annuel mondial du responsable de traitement (doc. 2).

L'adaptation du droit interne est aussi portée par l'influence de la jurisprudence.

B. La protection des données de connexion fournie par la jurisprudence

La Cour de justice de l'Union européenne, dans un arrêt du 6 octobre 2020 « La Quadrature du Net » a été amenée à interpréter la directive 2002/58/CE du 12 juillet 2002 « ne privée et communications électroniques » (doc. 11). Elle a ainsi jugé que cette directive n'autorisait les États-membres à adopter des mesures législatives limitant la portée des droits et obligations de cette directive, parmi lesquelles l'obligation de confidentialité des communications et données de trafic qu'à des fins de sauvegarde de la sécurité nationale et sous réserve qu'une décision soumise à un contrôle effectif constate l'existence d'une menace grave pour la sécurité nationale, réelle et actuelle, cela pour une durée limitée au strict nécessaire, renouvelable si la menace persiste (doc. 6 et 8).

Le Conseil d'État, dans un arrêt du 21 avril 2021, a appliqué cette solution en opérant un contrôle de conventionnalité des articles L. 34-1 et R. 10-13 du Code des postes et des communications électroniques notamment (doc. 8). Ces articles ont ainsi été déclarés contraires au droit de l'Union européen-

ne, puisqu'ils ne prévoient pas de réexamen périodique des risques pour la sécurité nationale justifiant la conservation généralisée et indifférenciée des données de trafic et de localisation. Le refus d'abroger l'article R.10-13 du CPCE a donc été annulé par le Conseil d'Etat, qui a enjoint au Gouvernement de modifier l'article R.10-13 pour le rendre conforme au droit de l'UE (doc. 8). Cet article a ainsi été modifié le 21 octobre 2021 (doc. 10).

La protection des données personnelles, incluant celles de connexion, est ainsi assurée par le droit européen et le droit interne, mais a été récemment renforcée en matière de procédure pénale.

II. La protection des données personnelles de connexion récemment renforcée en matière de procédure pénale

Les conditions récemment posées par les juges européens et les juges internes en matière de protection des données de connexion en procédure pénale (A) ont renforcé cette protection tout en laissant subsister diverses interrogations (B).

A. Le récent encadrement des conditions d'accès aux données personnelles de connexion

La Cour de justice de l'Union européenne, dans un arrêt prononcé en grande chambre le 2 mars 2021 « H.K / Prokuratuur », a encadré l'accès des autorités publiques à des données relatives au trafic ou à la localisation de personnes suspectées d'avoir commis une infraction pénale. D'une part, elle précise que l'accès à ces données personnelles de connexion doit être circonscrit à des procédures visant la lutte contre la criminalité grave ou la prévention de menaces graves contre la sécurité publique. Les facteurs tels que la durée d'accès ou la quantité de données disponibles n'ont pas d'incidence. D'autre part, les juges européens encadrent la compétence permettant d'autoriser un tel accès à une autorité publique, et considèrent à cet égard que le ministère public, qui est impliqué dans la conduite de l'enquête pénale et n'est pas neutre vis-à-vis des parties, ne peut être en mesure d'effectuer le contrôle préalable à l'accès aux données que le droit de l'UE impose (doc. 6). Il doit s'agir d'une juridiction ou d'une entité administrative indépendante.

Suivant cette jurisprudence, la chambre criminelle de la Cour de cassation, dans un arrêt du 12 juillet 2022, a été amenée à contrôler la conventionnalité de divers articles du Code de procédure pénale prévoyant un accès aux données de connexion dans le cadre de l'enquête (doc. 3). Des personnes mises

en examen avaient en effet demandé l'annulation des réquisitions portant sur leurs données de trafic et de localisation, délivrées par le juge d'instruction sur commission rogatoire ou par le ministère public lors d'une enquête de flagrance. Les hauts magistrats ont jugé que le juge d'instruction était une juridiction qui pouvait donc, en application du droit de l'Union, contrôler l'accès aux données. Ils ont en revanche considéré, comme la CJUE dans l'arrêt Prokuratuur, que le procureur de la République ne pouvait pas procéder à un tel contrôle, et ont donc déclaré contraires au droit de l'UE les articles retenant sa compétence (doc. 7).

Ces décisions ont eu des conséquences importantes pour la protection des données personnelles de connexion mais laissent subsister des interrogations.

B. Les conséquences de la restriction de l'accès aux données personnelles de connexion

D'une part, même si le contrôle désormais imposé pour l'accès aux données de connexion renforce la protection des droits (doc. 9), l'absence du contrôle requis par la CJUE n'entraînera pas l'annulation systématique des réquisitions de données contestées : en effet, la chambre criminelle, dans l'arrêt du 12 juillet 2022, précise les conditions de la nullité de ces réquisitions : elle ne peut être invoquée que par la personne concernée, c'est-à-dire titulaire ou utilisatrice de la ligne visée, et cette personne devra prouver l'existence d'un grief (doc. 3). Puisque les juges considèrent que ce grief ne peut être caractérisé que lorsqu'il y a une ingérence injustifiée au respect de sa vie privée et à la protection de ses données personnelles, la nullité apparaît possible dans des hypothèses restreintes (doc. 9).

D'autre part, ce changement de pratique imposé par la jurisprudence interroge quant à l'efficacité de la lutte contre l'identification des délinquants, la majorité des affaires comportant des réquisitions téléphoniques, les « fa-dettes » étant qualifiées de pièce maîtresse de la procédure des procureurs et enquêteurs (doc. 12). Ceux-ci attendent ainsi les directives de la direction des affaires criminelles et des grâces pour appliquer concrètement les arrêts de la CJUE et de la Cour de cassation (doc. 12). Il reviendra ensuite au législateur d'adapter la législation en modifiant les articles contraires au droit de l'Union et en confiant le contrôle de l'accès aux données personnelles de connexion au juge des libertés et de la détention par exemple (doc. 9).