

Concours : Deuxième concours ENM

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.



Le monde intérieur et l'évolution des technologies et de la mondialisation ont engendré une intensification des échanges de données à caractère personnel (doc 1).

Ces données à caractère personnel peuvent concerner des données relativement sensibles comme l'origine ethnique, les opinions politiques ou encore les convictions religieuses (doc 2). Il est dès lors apparu nécessaire d'assurer leur protection, cette dernière étant d'ailleurs un droit fondamental. Ces données posent surtout de nombreuses questions en matière pénale notamment en ce qui concerne les requêtes de données de trafic et de localisation plus communément appelées "fadoles" (doc 3, 12).

Le cadre juridique de la protection des données au niveau européen et son interprétation (I) ont nécessité une importante construction jurisprudentielle française (II).

I Le cadre juridique de la protection des données en Europe et son interprétation

L'Union européenne a instauré un cadre juridique par l'adoption de la protection des données (A). Son application fait l'objet d'une interprétation de la CJUE (B).

A) Le cadre juridique de la protection des données de connexion

L'article 15 de la directive 2002/58/CE du Parlement européen et du Conseil vise à garantir la protection de la vie privée dans le secteur des communications électroniques et encadre les données relatives au trafic (doc 11). L'arsenal juridique a été grandement complété par le règlement général

Sur la protection des données du 24 mai 2016. Il rappelle que la protection des données des personnes physiques est un droit fondamental. A ce titre il vient préciser la réglementation unique des Etats de l'Union européenne tout en leur laissant une marge d'interprétation (doc 1, 9).

La directive UE 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en lien avec des infractions pénales vient compléter le dispositif. Quatre catégories de personnes sont protégées par cette dernière en cas de réquisition de données. Il s'agit de personnes capables d'infraction, des suspects, des victimes et des témoins (doc 5). Des instances européennes comme le Comité européen de la protection des données veille à l'application cohérente de cette législation dans l'ensemble des Etats qui ont également mis en place des instances nationales chargées de la protection des données (doc 9). En France, il s'agit de la Commission nationale de l'informatique et des libertés (CNIL) dont les missions sont définies par la loi du 20 juin 2018 (doc 2). L'application de cette directive a nécessité des précisions.

B) La nécessaire interprétation de la CSUE à propos des réquisitions de données en matière pénale.

La Cour de justice de l'Union européenne dans l'affaire H.K./Prokuratur du 2 mars 2021 est venue préciser l'application de la directive européenne. En effet cette dernière est venue préciser dans un premier temps l'accès à des fins pénales aux données de trafic et de localisation notamment au regard de l'article 15 de la directive "vie privée" du 12 juillet 2002. Ainsi, l'accès à ces données de trafic et de localisation n'est autorisé qu'en vue de lutter contre le crime grave ou de réprimer des menaces graves contre la sécurité publique. En dehors de ces cas, le principe de proportionnalité de l'atteinte ne peut pas justifier. (doc 6).

Surtout la CSUE est venue préciser la compétence de l'autorité pouvant solliciter ces données auprès des organismes publics ou privés. Elle en conclut que l'autorité chargée d'exercer le contrôle doit être indépendante, quelle doit être un tiers par rapport à celle qui est à l'origine

des requêtes. Cela implique que l'autanté en question ne soit pas chargée de conduire l'enquête pénale et qu'elle soit recourue vis-à-vis des parties à la procédure pénale. En l'espèce, tel n'était pas le cas du ministère public étranger qui exerce l'action publique. C'est également le cas du ministère public français d'où la construction jurisprudentielle qui a suivi.

II) La construction jurisprudentielle française et ses conséquences

La construction jurisprudentielle française est venue clarifier les règles en la matière (A) et emporter plusieurs conséquences (B).

A) La construction jurisprudentielle française en matière de requêtes de données

Le Conseil d'Etat est venu rappeler le 21 avril 2021 que l'article C34-1 du code de postes et des communications électroniques (doc 10) était conforme au droit de l'UE en permettant la conservation rapide de données dans un objectif de sécurité nationale (doc 8).

La Cour de cassation est venue par la suite se prononcer dans 4 arrêts de 2022 sur les conditions d'accès à ces données de trafic et de localisation (doc 7). Elle rappelle que cela ne peut concerner que des faits relevant de la criminalité grave et qu'elles doivent être strictement nécessaires. Elle rappelle également que la "conservation rapide" des données est autorisée par le CSUE (doc 9). Surtout se basant sur la jurisprudence de cette dernière elle en déduit que le juge d'instruction est bien autorisé à procéder à de telles requêtes car il est un juge d'instruction ce qui n'est pas le cas du ministère public. Elle précise également que l'ingérence doit être strictement nécessaire et proportionnée et qu'en cas d'infractions entrant dans le champ de la criminalité organisée comme le trafic de stupéfiants cette exigence était bien respectée (doc 3). La Cour de cassation met ainsi fin à son appréhension comprehensive en la matière.

B) Les conséquences des arrêts de la Cour de cassation en matière de protection de données de connexion.

Dans ses arrêts, la Cour de cassation est venue préciser les conditions de validité des requêtes d'accès aux données de connexion (doc 7). Elle précise que la validité ne peut être invoquée que par la personne titulaire de la ligne en question qui doit faire preuve d'un grief en établissant qu'il a été victime d'une ingérence injustifiée au regard du respect à sa vie privée. Le rôle en la matière est ainsi particulièrement restrictif. En l'espèce les demandes formées par le mis en cause ont été rejetées car les catégories de données visées et le degré d'accès étaient limités et strictement nécessaires au bon déroulement de l'enquête. Comme même elles ont été à l'initiative du parquet (doc 7).

Les arrêts ont suscité des critiques de la part de nombreux magistrats tant les requêtes sont essentielles pour mener des enquêtes. C'est surtout leur nombre qui inquiète car il est très complexe de saisir à chaque fois le juge de libertés et de la détention et le effectif des tribunaux risquant de ne pas pouvoir suivre (doc 12). Les magistrats attendent de ce fait une circulaire de la direction des affaires criminelles et des grâces pour l'application concrète de ces arrêts. En attendant qu'une loi vienne préciser le cadre juridique à venir et notamment en conformité au TCD la charge de cet accès de données de trafic et de localisation essentielles aux enquêtes et par conséquent aux enquêtes les plus graves (doc 9).