

Concours : les concours de l'Ecole Nationale de la Magistrature

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.



Selon la Commission européenne, plus de 90 % des Européens veulent les mêmes droits en matière de protection des données dans toute l'Union Européenne (document 4).

Les données personnelles de connexion connaissent une évolution rapide à l'ère du numérique (doc 1). Il s'agit de données générées dans le cadre de la fourniture de services de communications électroniques (doc 6). Elles concernent les personnes physiques utilisant une connexion pour effectuer la communication (doc 11). Elles comportent donc les informations transmises lors de cette connexion (doc 11). Ainsi, ces données revêtent-ils un caractère personnel, raison pour laquelle leur protection est un droit fondamental (doc 1). Néanmoins, ce droit ne peut être absolu (doc 1). L'accès et la conservation de ces données peuvent en effet s'avérer très utiles en matière pénale (doc 1). Il doit donc être mis en balance avec d'autres droits fondamentaux (doc 1), dont la protection de l'ordre public. C'est la raison pour laquelle, tout en assurant la protection des données personnelles de connexion, des règles spécifiques sont prévues en matière pénale. Cet équilibre est assuré par le législateur à l'échelle européenne et nationale et contrôlé par les juges. Se pose ainsi la question de l'équilibre entre liberté garantie par la protection des données personnelles de connexion et maintien de l'ordre public assuré par le droit pénal.

Si les législateurs européens et français ont consacré des règles tendant à cet équilibre (I), les juges en ont précisé la mise en œuvre en dégageant des conditions strictes de recours à ces données au nom de leur protection (II).

I] L'équilibre entre la protection des données personnelles de connexion et l'efficacité du droit pénal consacré par le législateur

Par sa volonté d'unifier les législations européennes, le droit de l'Union européenne a consacré un cadre général de protection des données personnelles de connexion (A), amenant le législateur français à faire évoluer les règles en la matière (B).



## A) La protection des données personnelles de connexion : l'unification du droit par le règlement de l'Union européenne

Le règlement général sur la protection des données du Parlement européen et du Conseil du 27 avril 2016 consacre la protection de ces données en tant que droit fondamental (doc 1). L'article 8 de la Charte des droits fondamentaux de l'Union prévoit que toute personne a droit à la protection des données à caractère personnel la concernant (doc 1). Ce règlement entre en vigueur le 24 mai 2016 et s'applique depuis le 25 mai 2018 (doc 4). Il permet d'unifier les droits des citoyens de l'Union européenne, de renforcer leurs droits fondamentaux et de stimuler l'activité économique en clarifiant les règles applicables (doc 4). Le texte rappelle que le niveau de protection des droits et des libertés doit être équivalent dans tous les États membres (doc 1). De plus, le règlement s'applique indépendamment de la nationalité ou du lieu de résidence s'agissant du traitement des données (doc 1).

Cependant, le droit à la protection des données personnelles de connexion n'est pas absolu (doc 1). Il est régi par un acte juridique de l'Union plus spécifique, la directive 2016/680 (doc 4). Cette directive garantit la protection des données à caractère personnel des victimes, témoins, suspects et facilite la coopération transfrontière dans la lutte contre la criminalité (doc 4). Elle est entrée en vigueur le 5 mai 2016 et les États membres devaient la transposer avant le 6 mai 2018 (doc 4). Ainsi, en la matière, les données doivent - elles être collectées pour des finalités légitimes et le traitement doit être nécessaire et proportionné à cette finalité (doc 5). Des délais appropriés doivent être fixés par les États - membres concernant la conservation et l'effacement des données (doc 5). La directive identifie quatre catégories de personnes répondant à un régime distinct et interdit les décisions uniquement fondées sur un traitement automatisé (doc 5). Enfin, le traitement n'est licite que s'il est effectué par une autorité compétente et s'il est rendu nécessaire (doc 5). Le législateur français a donc dû adapter le droit national compte - tenu des dispositions du règlement européen.

## B) La protection des données personnelles de connexion : l'adaptation du droit national

La loi du 20 juin 2018 relative à la protection des données personnelles a été publiée le 21 juin 2018 (doc 2). Auparavant, le droit français protégeait déjà les données personnelles de connexion avec la loi du 6 janvier 1978 (doc 2). Cette dernière a néanmoins dû être adaptée pour se conformer au droit de l'Union européenne. Ainsi, conformément aux exigences du règlement général sur la protection des données, la loi du 20 juin 2018 définit le champ des missions de la Commission nationale de l'informatique et des libertés (CNIL) (doc 2). Quant aux acteurs économiques, le contrôle a priori auquel ils étaient soumis est remplacé par un système de contrôle a posteriori (doc 2). En revanche, concernant les données les plus sensibles, dont les données biométriques



et génétiques, les formalités préalables sont maintenues (doc 2).

Comme prévu par le règlement de l'Union européenne, le droit national prévoit des règles spécifiques en matière pénale. La loi du 20 juin 2018 renforce notamment les droits des personnes en créant un droit à l'information de la personne concernée par les données personnelles traitées en matière pénale (doc 2). Le respect du droit de l'Union européenne par les États membres est contrôlé par le Comité européen de la protection des données et le contrôleur européen de la protection des données (doc 4). Ainsi, des règles spécifiques au droit pénal en matière de protection des données personnelles de connexion sont-elles prévues aux articles L.34-1 et R.10-13 du code des postes et communications électroniques (doc 10). L'article 34-1 prévoit que les opérateurs de communications électroniques peuvent conserver certaines données personnelles de connexion pour les besoins de la procédure pénale. La durée de conservation varie selon qu'il est question de menaces contre la sécurité publique, de sauvegarde de la sécurité nationale, ou encore de lutte contre la criminalité et la délinquance grave (doc 10). Cette durée varie alors entre un an et cinq ans.

Les législateurs ont donc encadré le droit à la protection des données personnelles de connexion tout en prévoyant des règles spécifiques en matière pénale. Par la suite, les juges ont précisé ces règles en dégageant des conditions strictes de recours à ces données en procédure pénale.

## II) La protection des données personnelles de connexion : le recours aux données en matière pénale strictement encadré par la jurisprudence

Les juges ont dégagé de strictes conditions en matière d'accès et de conservation des données en procédure pénale (A), ce qui a suscité des réactions partagées de la part des acteurs du droit pénal (B).

### A) La protection des données personnelles de connexion : l'accès et la conservation en procédure pénale strictement encadrés par la jurisprudence

Concernant l'accès, la Cour de justice de l'Union européenne dans un arrêt du 2 mars 2021, affaire *Prokuratura*, s'autorise en procédure pénale à la condition qu'il permette la lutte contre la criminalité grave ou qu'il permette de prévenir des menaces graves contre la sécurité publique (doc 6). En revanche, elle s'oppose à ce que cet accès soit autorisé par le ministère public en ce qu'il n'est pas une autorité indépendante (doc 6). Pour un autre motif, le Conseil constitutionnel a restreint l'accès général et indifférencié aux données pendant l'enquête préliminaire dans une décision du 3 décembre 2021 (doc 9). La loi du 2 mars 2021 a d'ailleurs encore renforcé les conditions d'accès aux données pendant l'enquête, qui est conduite par le procureur de la République (doc 9). Finalement, dans un arrêt du 12 juillet 2022, la chambre criminelle affirme que la possibilité pour le procureur de la République d'autoriser l'accès aux données de connexion est contraire au droit de l'Union européenne en ce qu'il est partie au procès, contrairement au



juge d'instruction (doc 3).

Concernant la conservation, le Conseil d'Etat dans une décision du 21 avril 2021 annule le refus d'abroger l'article R. 10-13 du CPCE et l'article 1<sup>er</sup> du décret du 25 février 2021 en ce qu'ils ne prévoient pas un réexamen périodique de la nécessité de conserver les données de connexion au regard du risque pour la sécurité nationale (doc 8). L'article R. 10-13 a donc été réécrit et prend en compte cette exigence depuis le 21 octobre 2021 (doc 10). Dans son arrêt du 12 juillet 2022, la chambre criminelle affirme que la sauvegarde de la sécurité nationale permet une conservation générale et indifférenciée dans son régime antérieur à la loi du 30 juillet 2021 (doc 7). Elle estime qu'afin d'assurer le droit de l'Union européenne, le juge doit vérifier que les faits en cause relèvent de la criminalité grave et que la conservation rapide des données respecte les limites du strict nécessaire (doc 7). Les conditions strictes dégagées par la jurisprudence suscitent des réactions de la part des acteurs du droit pénal.

### B) La protection des données personnelles de connexion : les réactions partagées des acteurs du droit pénal.

D'une part, certains soulignent que les catégories de personnes identifiées à l'article 6 de la directive sont définies trop imprécisément (doc 5). En effet, elles doivent être distinguées "dans la mesure du possible" et des précisions ont été sollicitées afin que la distinction soit plus ferme (doc 5). Par ailleurs, le procureur Nicolas Septe affirme avoir demandé à réduire le recours aux réquisitions de données de connexion (doc 12). En effet, les parquetiers sollicitent une définition des "infractions les plus graves" (doc 12) alors que le droit européen n'en fournit pas. En outre Frédéric Lagache du syndicat de police Alliance estime que l'arrêt de la chambre criminelle du 13 juillet 2022 limitant le recours aux données de connexion par les enquêteurs rend plus difficile l'efficacité des enquêtes (doc 12). Le recours doit en effet être autorisé par une autorité indépendante, ce qui risque de multiplier de façon conséquente le nombre de réquisitions auprès du juge de la liberté et de la détention (doc 12).

D'autre part, d'autres acteurs estiment que la limitation des pouvoirs du procureur de la République en matière de réquisitions de données de connexion ne constitue pas tant un obstacle qu'un changement de pratique (doc 9). Il ne s'agit pas de rendre impossible les réquisitions mais de les soumettre à un contrôle de nécessité (doc 9). Cet encadrement permet donc toujours d'effectuer des enquêtes efficaces tout en respectant les droits et libertés ainsi qu'en se conformant au droit de l'Union européenne (doc 9). De la même façon, le critère de criminalité grave ne serait pas davantage un obstacle en ce qu'il est assez souple pour justifier l'accès aux données (doc 9). Ainsi les enquêteurs devront-ils adapter leurs modes d'investigation (doc 9). Se pose aussi la question de confier au juge de la liberté et de la détention la compétence en la matière (doc 9).