Concours ENM
1er, 2ème, 3ème concours

SESSION 2024

Épreuve de note de synthèse

Corrigé du sujet : La protection des données personnelles de connexion.

Présentation du sujet

Enjeux du sujet :

La protection des données personnelles de connexion n'est pas un sujet récent. Le RGPD et sa mise en place datent déjà respectivement de 2016 et 2018. Les éléments de nouveauté du sujet résident dans l'application du RGPD dans le cadre de la lutte contre la criminalité grave et le terrorisme. Ces aspects du sujet ont fait l'objet de vifs débats à propos de la collecte de masse d'informations généralisées et indifférenciées par les autorités publiques et les services de renseignement plus particulièrement.

Toutefois, dans le cadre de l'ENM, ce sujet répond à une préoccupation grandissante qui occupe les magistrats et plus généralement le monde du droit : Le droit confronté au numérique. Ce n'est d'ailleurs pas un hasard que le sujet de la note de synthèse et celui de la composition de culture générale se répondent en 2024.

Principales difficultés du sujet :

Sur le fond, la note n'était pas simple. D'abord, les étudiants ont généralement du mal à traiter de sujets balanciers entre le droit de l'Union européenne et le droit national. Certaines informations de fond pouvaient nécessiter d'avoir du recul sur la notion de règlement et de directive et surtout sur les rapports de système européens et nationaux. De plus le fonctionnement général du RGPD est un point important du dossier mais qui ne doit pas être exagéré. Le dossier se focalise en grande partie sur la conciliation avec les exigences de protection des intérêts nationaux et la défense contre la criminalité. Sur ce dernier point, il fallait distinguer les deux grandes problématiques de la collecte de masses des données et le traitement par des autorité impartiales et indépendantes.

Sur le plan de la méthodologie, il fallait bien différencier les thèmes. Tous n'étaient pas immédiatement visibles. De même, le lien entre les informations et les idées parfois différentes demandait un esprit de synthèse et un recul peu évident sur les informations.

Erreurs à ne pas commettre : Il fallait éviter ici de tomber dans l'écueil d'une simple présentation du RGPD. La problématique de la confrontation avec les intérêts fondamentaux de la Nation devait apparaître clairement.

Corrigé

« Le train de mesures sur la protection des données adopté en mai 2016 vise à adapter l'Europe à l'ère numérique. Plus de 90 % des Européens veulent les mêmes droits en matière de protection des données dans toute l'UE, où que soient traitées ces données ». ***(D4)***

Le RGPD vise à protéger les personnes physiques contre le traitement abusif de leurs données personnelles tout en garantissant la libre circulation de ces données au sein de l'Union européenne ***(D1)****.*

Un régime de protection des données personnelles a été établi dans l'Union européenne ***(I)*** *qui se trouve confronté à la lutte contre la criminalité* ***(II)****.*

I – L'établissement d'un régime de protection des données personnelles de connexion

Le système de lutte résulte d'une coopération européenne ***(A)*** *imposant un régime de protection commun* ***(B)****.*

A – Une collaboration européenne dans la protection

La protection des données personnelles est un droit fondamental, inscrit dans la Charte des droits fondamentaux et le traité sur le fonctionnement de l'UE **(D1 et 4)**. Le RGPD s'applique également dans l'Espace économique européen **(D4).** Le règlement (UE) 2016/679 facilite leur libre circulation au sein de l'UE et réduit les charges administratives inutiles **(D4)**. Les données de connexion peuvent révéler des informations sensibles sur la vie privée des individus, telles que l'orientation sexuelle, les opinions politiques **(D7)**.

Le niveau de protection doit être équivalent dans tous les États membres dans un but d'homogénéité des règles, mais les États membres peuvent adapter les règles à leurs législations nationales **(D1 et 4)**. Ils doivent mettre en place des autorités de contrôle indépendantes chargées de la protection des données **(D1)**. A ce titre, la loi de 2018 adapte la loi du 6 janvier 1978 au RGPD et confie à la CNIL un rôle de publication de référentiels, certification d'organismes et de consultation par le Parlement sur ces questions. Le contrôle a priori est remplacé par un contrôle a posteriori basé sur l'évaluation des risques par les responsables de traitement **(D2)**. La CNIL a un pouvoir de sanction pouvant atteindre 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial consolidé **(D2)**. Au niveau

européen, le Comité européen de la protection des données, organe indépendant composé de représentants des autorités nationales et du Contrôleur européen, doit assurer l'application cohérente des règles **(D4)**.

Lors de l'évaluation de la protection des données dans des pays tiers, la Commission prend en compte les critères de l'État de droit **(D1)**. L'utilisation des données sensibles est autorisée en cas de nécessité absolue avec des garanties appropriées pour protéger des intérêts vitaux ou si les données ont été rendues publiques par la personne concernée **(D5)**.

B – Le régime de protection

L'article 15 de la directive de 2002 définit les données de communication comme toute information transmise via un réseau **(D11)**. Ces données peuvent être collectées et utilisées à diverses fins déterminées **(D5 et 11)**. Les données doivent être explicites et légitimes, limitées à ce qui est nécessaire, exactes et, si nécessaire, mises à jour **(D1 et 5)**. Le traitement des données doit également être transparent, accessible et compréhensible pour les personnes concernées **(D2)**. Le traitement est licite s'il est nécessaire pour une mission d'intérêt public ou fondé sur le droit de l'Union ou d'un État membre, précisant les objectifs et les finalités du traitement. Le changement de finalité est possible si les nouvelles missions sont autorisées par le droit de l'Union ou par celui d'un État membre **(D5)**. Les enfants bénéficient d'une protection spécifique pour leurs données **(D1 et 2)**.

Les formalités préalables sont maintenues pour les données biométriques, génétiques, de santé et les numéros d'inscription au répertoire national **(D2)**. Les données sensibles comprennent les informations sur l'état de santé physique ou mentale, passées, présentes ou futures d'une personne **(D1 et 2)**. Les décisions basées exclusivement sur un traitement automatisé, y compris le profilage, sont interdites sauf si autorisées et comportant des garanties appropriées **(D5)**. Les données doivent être traitées de manière à garantir leur sécurité et leur confidentialité **(D2, 5 et 11)**. Le règlement crée un droit à l'information et exercice direct des droits d'accès, de rectification et d'effacement des données **(D2)**.

L'article R10-13 du CCPE précise les informations que les opérateurs de communications électroniques doivent conserver et les informations qui doivent être effacées ou anonymisées **(D10)**. Les États doivent instaurer des procédures pour garantir le respect des délais d'effacement **(D5)**.

II – Les limites de la protection des données personnelles de connexion à l'aune de la lutte contre la criminalité

*La lutte contre la criminalité se heurte aux exigences de protection des données qui interdit la collecte de masse **(A)** et exige une utilisation par des organes indépendants **(B)**.*

A – L'utilisation excessive de la collecte des données en matière pénale

Le RGPD ne s'applique pas aux activités relevant de la sécurité nationale. La directive UE/2016/680 régit la protection des données utilisées à des fins de prévention et de répression des infractions pénales **(D1)**. Doivent être distingués les suspects, coupables, victimes, et témoins **(D5)**. La directive facilite la coopération transfrontalière **(D4)**. Le Premier ministre peut ordonner la conservation d'autres catégories de données de trafic et de localisation pour un an, renouvelable si la menace persiste **(D10)**. Les autorités peuvent ordonner la conservation rapide des données pour prévenir et réprimer la criminalité grave ou pour la défense de la sécurité nationale **(D9 et 10)**. L'article L. 34-1 du CCPE, prévoyant une conservation généralisée des données pour la sécurité nationale, est conforme au droit de l'Union européenne **(D9)**. La Cour de Justice, en 2021, s'oppose à l'accès des autorités publiques aux données de trafic et de localisation sans que cet accès soit limité à la lutte contre la criminalité grave ou la prévention de menaces graves **(D6)**.

Le Conseil d'Etat en 2021 admet que la conservation généralisée des données de connexion sans réexamen périodique est contraire au droit de l'UE. Le gouvernement doit modifier ces dispositions dans un délai de 6 mois pour inclure un réexamen périodique de la nécessité de conserver les données **(D8)**. Toutefois, le Conseil rappelle que la France fait face à des menaces graves pour la sécurité nationale justifiant une telle conservation généralisée **(D8)**. La Cour de cassation, le 12 juillet 2022, affirme que les États membres ne peuvent imposer une conservation généralisée et indifférenciée des données de trafic et de localisation aux opérateurs de communications électroniques sauf en cas de menace grave pour la sécurité nationale **(D3 et 7)**. Concernant la criminalité grave, les États peuvent imposer une conservation « rapide » avec certaines garanties **(D7)**.

B – L'accès aux données par un organe indépendant

Selon la CJUE, l'accès aux données doit être autorisé par une autorité indépendante excluant le ministère public et les tiers **(D6 et 7)**. Cette autorité agit de manière objective et impartiale et respecte la vie privée par un contrôle indépendant et proportionné **(D6)**. Seul le

juge d'instruction est habilité à contrôler l'accès aux données **(D9)**. La violation de l'exigence de contrôle indépendant peut être invoquée uniquement si elle porte atteinte à la vie privée de l'accusé **(D7).** La conservation doit être autorisée par une autorité indépendante et concerner un certain type de données comme les contacts téléphoniques et SMS, dates, heures, durée des échanges **(D7)**. Le Conseil d'Etat rappelle en 2021 que le CSI ne respecte pas le droit de l'UE, faute d'un contrôle préalable par une autorité indépendante dotée d'un pouvoir d'avis conforme **(D8)**. Ainsi, le Premier ministre ne peut autoriser les techniques de renseignement mentionnées en cas d'avis défavorable de la CNCTR avant une décision du Conseil d'État **(D8)**.

De surcroît, la Cour de cassation dans un arrêt de 2022 a décidé de limiter l'utilisation des "fadettes", permettant de consulter les SMS et les données de géolocalisation par les enquêteurs, afin de protéger les libertés publiques **(D12)**. Désormais, les procureurs ne pourront plus ordonner leur consultation sans l'autorisation d'une autorité indépendante et dans les cas de terrorisme, de criminalité organisée et d'infractions graves **(D12)**. Selon certains, cette décision risque d'entraver la lutte contre la délinquance du quotidien **(D12)**. La Cour de cassation a reconnu que l'accès aux données de trafic et de localisation par les enquêteurs doit être contrôlé par une autorité indépendante comme le juge d'instruction **(D3)**.

Depuis la loi du 2 mars 2022, les procureurs peuvent accéder aux données de connexion pour des crimes et délits punis d'au moins trois ans d'emprisonnement ou d'autres cas spécifiques. Ils doivent justifier l'accès aux données par la criminalité grave et la stricte nécessité **(D9)**. La Conférence nationale des procureurs de la République considère ces arrêts comme un obstacle majeur à l'identification des délinquants et criminels **(D9)**.