M Leboucher
Lycée Malherbe, Caen

Devoir Informatique CPES Mai 2024

I - Expérience

Dans un paragraphe d'une quinzaine de lignes, vous rédigerez une réponse à la question suivante concernant votre projet de site Web :

Comment avez vous obtenu vos données numériques pour étayer vos arguments, comment les avez vous présentés et pourquoi ?

II – Questions de cours

Vous répondrez de la façon la plus précise possible aux 5 questions suivantes :

1) Donnez la définition d'un logiciel WYSIWYG.

2) Donnez au moins 5 formules de tableur utiles pour faire des statistiques.

3) Donnez la définition d'une clef primaire dans une base de donnée.

4) Comment sélectionner un élément d'une base de données en langage SQL ?

5) Donnez la définition de copyleft et de logiciel open source.

III – Rédaction

A l'aide des documents qui suivent et de vos connaissances, vous répondrez en argumentant votre réponse à la question suivante :

La mise en place du RGPD en Europe est-elle une réponse adaptée au problème des fuites de données personnelles dans les entreprises ?

Document 2 : RGPD pour les nuls en 2024, définition, rôle, principes (witik)

Qu'est-ce que le RGPD ?

Le Règlement Général sur la Protection des Données, plus connu sous l'acronyme RGPD, représente le cadre légal instauré par l'Union Européenne pour garantir la protection des données personnelles de ses citoyens. Englobant une multitude d'organisations, tant publiques que privées, le RGPD s'applique dès lors qu'une entité basée sur le sol européen ou ciblant des résidents européens traite des données personnelles, indépendamment de la finalité de ce traitement.

Formellement désigné comme le règlement UE 2016/679 daté du 27 avril 2016, le RGPD se distingue en tant que règlement et non directive. Cela signifie qu'il s'applique de manière directe et uniforme à travers l'ensemble de l'Europe, sans nécessiter une transposition dans les législations

nationales des États membres. Depuis son entrée en vigueur en 2018, il constitue le pilier législatif de la protection des données au sein de l'UE.

À la base de ce règlement, résident quelques concepts clés essentiels à comprendre. En substance, le RGPD encadre le traitement des données personnelles des résidents européens. Ainsi, il est crucial de décortiquer les termes centraux de cette définition. Le "traitement des données" couvre une gamme étendue d'opérations relatives aux données personnelles, englobant la collecte, l'organisation, et l'exploitation de ces données.

Se conformer au RGPD n'est pas une option mais une obligation légale pour toutes les entreprises.

Principaux piliers du RGPD : Quels sont-ils ?

Le RGPD établit plusieurs principes essentiels qui façonnent les normes de protection des données en Europe.

Le consentement

Premièrement, le RGPD amplifie le concept de consentement par rapport aux précédentes régulations. La gestion des consentements est devenue cruciale pour les DPO et les gestionnaires RGPD dans les organisations. Ce consentement doit être manifeste et actif, illustré par une action directe de l'utilisateur, telle qu'un clic sur un bouton d'approbation.

La transparence est intrinsèquement liée au consentement et représente le second pilier du RGPD. Pour que le consentement soit valide, il doit être bien informé, nécessitant ainsi que les organisations fournissent des informations explicites sur les types de données collectées et les intentions derrière cette collecte. C'est dans cette optique que l'approche "Privacy by Design" est recommandée lors de la gestion des données personnelles, assurant ainsi une conformité au RGPD dès le début de tout projet.

Les droits

Le droit des personnes est renforcé par le RGPD. Concrètement, il s'agit d'un ensemble de droits que les entreprises doivent garantir. On peut citer le droit d'accès, qui est défini comme la nécessité pour l'entreprise d'autoriser les utilisateurs à accéder aux informations et aux données les concernant. Le droit à l'oubli doit être respecté : toutes les informations et données personnelles doivent être supprimées sur demande de la personne concernée. Citons également le droit à la portabilité des données : c'est la possibilité pour un utilisateur de récupérer les données le concernant, par exemple pour les transmettre à un nouveau prestataire ou fournisseur de services.

Quelles sont règles à respecter pour les entreprises ?

Même si nous parlons du RGPD de manière simplifiée, il est essentiel de comprendre ses principaux fondements pour assurer une protection optimale des données.

Pour vérifier que les données personnelles recueillies soient traitées selon les règles, les entreprises, comme les PME, les ETI ou encore les grands groupes, doivent mettre en place des mesures permettant d'assurer le respect des grands principes de la protection des données.

À noter que certaines entreprises ont réussi à contourner le RGPD. Nous expliquons dans cet article, comment Lusha a réussi à passer entre les mailles du filet de la CNIL.

Principes de base du traitement des données

Licéité du traitement

Le traitement des données doit avoir un fondement **licite, loyal et transparent**. C'est le principe de licéité du traitement. Les raisons peuvent être multiples :

- Est-ce que l'organisme traite les données parce qu'il y a une obligation légale de le faire (ex : les finances publiques qui traitent vos données pour déterminer vos impots) ?
- Parce qu'il le doit selon un contrat lié avec la personne concernée (ex : la banque qui vous octroie un crédit) ?
- Parce qu'il a obtenu le consentement de la personne pour le faire (ex : pour participer à un jeu concours) ?

Au total, le RGPD propose six bases légales pour le traitement.

Finalité du traitement

Le traitement peut exister légalement mais encore faut-il qu'il ait **un objectif précis et déterminé**. C'est le principe de finalité.

Les données collectées doivent avoir un but spécifique. Par exemple, si vous fournissez votre email pour obtenir un ebook, l'entreprise doit l'utiliser uniquement pour vous envoyer cet ebook.

Minimisation des données

Seules les informations pertinentes pour l'objectif visé doivent être collectées. Si le but est d'envoyer un ebook par email, il n'y a pas besoin de connaître votre date de naissance.

Limitation de la conservation

Les données ne doivent être conservées que le temps nécessaire pour réaliser l'objectif. Après cela, elles doivent être effacées ou anonymisées. Les organismes doivent donc définir des **durées de conservation** pour les traitements qu'ils mettent en place.

Intégrité et confidentialité

Les entreprises doivent garantir la sécurité des données pour éviter tout accès ou traitement non autorisé.

Exactitude :

Les données stockées doivent être à jour et exactes. Tout effort doit être fait pour rectifier ou supprimer des données inexactes.

Preuves de conformité

Pour garantir l'adhésion à ces principes, le RGPD demande aux entreprises de maintenir des documents attestant de leur conformité, comme le registre des traitements et diverses procédures liées à la gestion des données personnelles.

D’autres principes viennent compléter cette liste : **le principe de sécurité** qui vise à assurer l’intégrité et la confidentialité des données ; **le principe d’exactitude des données** qui vise à assurer que les données traitées soient bien à jour.

Pour prouver tout cela le RGPD impose aux organismes des documents prouvant leur bonne conformité : **le fameux registre des traitements, des procédures de gestion des données personnelles diverses et variées**.

Donc mes données personnelles sont bien protégées ?

Le RGPD vient encadrer de manière légale une obligation qui est morale, celle de protéger et de respecter les données personnelles.

Malheureusement, aujourd’hui, de nombreuses entreprises ne respectent pas le RGPD mais le sujet devient de plus en plus brûlant. Tout comme les utilisateurs vont regarder davantage l’éthique en matière d’environnement des entreprises auprès desquelles ils choisissent de passer commande, ils regardent de plus en plus l’éthique en matière de respect des données personnelles.

En France, **l’organisme qui contrôle le respect du RGPD c’est la CNIL** (Commission Nationale de l’Informatique et des Libertés) et en cas de non-respect avéré, l’amende peut être salée – Jusqu’à 4% du chiffre d’affaires ! Un risque que peu d’entreprises peuvent se permettre de prendre.

Document 2 : L’impact économique du RGPD, 5 ans après – CNIL (Commission Nationale de l’informatique et des libertés).

Cinq ans après l’entrée en application du RGPD, la littérature économique s’est penchée sur son impact économique sur les entreprises. La plupart de ces études se concentrent sur les coûts sans suffisamment mesurer les bénéfices pour les entreprises et les gains de bien-être pour les personnes.

Vouloir faire l’étude de l’impact économique de la mise en œuvre du règlement général sur la protection des données (RGPD) en Europe depuis 2018 peut sembler un exercice superflu : cette réglementation n’a-t-elle pas pour objet la protection des droits fondamentaux des Européens ? Ce texte ne doit-il pas être de toute manière respecté par les entreprises ? Le RGPD n’est-il pas, par ailleurs, devenu un standard mondial, inspirant de nombreux pays ?

Le RGPD, en harmonisant les règles relatives à la protection des données personnelles en Europe, a instauré un espace de libre circulation des données. L’économie numérique, largement fondée sur l’utilisation des données personnelles, ne peut se développer sans la confiance des citoyens, garantie par un haut niveau de protection de ces données. La mise en œuvre du RGPD comporte donc des enjeux économiques forts pour la France et ses entreprises.

Après 5 ans d’application du RGPD, la littérature économique s’est saisie de ce sujet afin d’éclairer son impact, notamment pour les entreprises, essentiellement à partir de

travaux empiriques consacrés au lien entre cette réglementation et la croissance, l'innovation et la concurrence.

Un investissement dans la conformité, un impact nuancé

La littérature économique met souvent l'accent sur les coûts, initiaux et récurrents, de mise en œuvre du RGPD par les entreprises. Ceux-ci sont réels et inévitables : ils correspondent à une préférence collective européenne qu'il convient d'assumer, d'autant plus aisément que toutes les entreprises sont logées à la même enseigne. En réalité, ce coût est un investissement dans la conformité, qui comporte des bénéfices économiques.

À la lecture de ces études, il faut avant tout se garder d'une approche simpliste car la donnée personnelle est un objet économique très particulier : elle fait rarement l'objet d'un échange marchand, n'est pas gratuite à produire, mais se copie quasiment sans coût. En l'absence de réglementation, elle peut donner lieu à des asymétries d'information entre le service et l'usager, ce dernier n'ayant qu'une vision parcellaire de l'utilisation de ses données. Le bien-être des personnes concernées risque d'être affecté par des « externalités négatives » (se produit lorsqu'une activité génère des conséquences négatives non voulues sur d'autres acteurs économiques – par exemple, la revente de données pouvant aboutir à un flux de sollicitations non souhaitées).

De ce fait, l'une des vertus du RGPD peut être, en permettant une meilleure information et plus de rationalité dans les choix, de résorber des « failles de marché » (réduction des nuisances dues aux sollicitations publicitaires ou au profilage par exemple) et de rendre possibles des opérations économiques qui ne le seraient pas en l'absence de protection (comme participer volontairement à une étude en santé).

Par ailleurs, les effets de la mise en œuvre du RGPD sur les entreprises françaises sont nuancés : les études font état d'impacts dans les deux sens, dépendant de l'activité économique et de la nature du modèle d'affaires considéré. Alors que certaines opérations sont plus encadrées (comme le démarchage ou la revente de données client par exemple), d'autres sont facilitées par l'augmentation de la confiance du client.

Les difficultés méthodologiques

Les études d'impact économiques suivent une approche expérimentale, à partir de données mesurées, pour tenter de dégager une approche objective. Cela suppose de pouvoir comparer, par exemple, des entreprises soumises au RGPD et un groupe « témoin » qui n'y est pas soumis, « toutes choses égales par ailleurs ».

Malgré ces approches, il est compliqué, d'un point de vue méthodologique, d'isoler l'effet propre du RGPD par rapport au contexte économique et aux comportements variés des acteurs. C'est avec l'accumulation des études, si elles sont convergentes, que les grandes tendances pourront se dégager.

De même, si beaucoup d'études concernent des secteurs traditionnellement peu régulés, où l'impact du RGPD est le plus fort (e-commerce, publicité en ligne, marketing), les résultats pour ces secteurs ne sont pas généralisables à l'ensemble de l'économie. Toutefois, une approche plus générale, macroéconomique, n'a pas été réalisée à ce stade en raison des difficultés inhérentes à la modélisation des questions de données personnelles.

Prendre en compte les bénéfices pour les entreprises et les personnes

Intéressantes dans leurs résultats, les études sont incomplètes pour ce qui est de leur champ : elles ne traitent que marginalement des bénéfices de la conformité pour les entreprises, car moins aisément observables. Or, on constate d'un point de vue qualitatif un retour sur investissement de la conformité RGPD, en termes de réputation aux yeux des clients et des partenaires, de sécurité informatique, de connaissance de la « donnée » disponible au sein d'une entreprise ou d'économies opérationnelles, par exemple. Il serait utile que les économistes tentent d'objectiver ces gains pour réaliser une véritable analyse coûts/bénéfices.

De même, la mise en œuvre du RGPD permet d'importants gains de bien-être pour les consommateurs, qui maîtrisent ainsi mieux leurs données et sont mieux à même de mesurer les risques de leur dissémination. Plus vigilants, ils sont moins sujets à l'exploitation frauduleuse de leurs données ou à des irritants comme le démarchage abusif, qui occasionnent des préjudices économiques.

Ces gains ne sont toutefois pas directement observables sur un marché et sont donc difficiles à mesurer. Seule une comparaison quantifiée entre l'effet sur les entreprises et l'effet sur les individus permettra de confirmer (ou d'infirmer) si cette réglementation a apporté un bénéfice net pour la société dans son ensemble.

Les leçons à tirer pour le régulateur

Les études économiques réalisées jusqu'ici, bien que surtout focalisées sur les coûts induits par la mise en œuvre du RGPD et dans l'attente d'une nouvelle étape en analysant finement les bénéfices, comportent néanmoins quelques leçons à tirer pour la CNIL. D'abord, elles valident la pertinence de l'approche d'accompagnement du régulateur consistant à fournir aux entreprises des outils adaptés à leurs besoins, réduisant ainsi le coût de la conformité, tout comme la fourniture de sécurité juridique à travers des référentiels, conseils ou guides de bonnes pratiques.

Ensuite, ces études montrent que la vie privée est à considérer comme un bien public. Sa protection ne naît pas spontanément du fonctionnement des marchés ni même des comportements individuels des personnes mais comporte une dimension de « paternalisme libertarien » (c'est-à-dire, organiser des conditions dans lesquelles les personnes sont incitées à un comportement qui les protège). L'action du régulateur

permet de faciliter les choix individuels qui concourent à instaurer un haut niveau de protection des données. Celui-ci, en retour, bénéficie à l'ensemble des acteurs des marchés numériques, en créant un cadre de confiance indispensable au développement de ces derniers (développement de la French Tech depuis 2017 par exemple).

Enfin, ces études montrent que le RGPD est proportionnellement plus favorable aux gros acteurs économiques, qui ont plus de moyens à consacrer à la conformité, mais qui sont néanmoins plus régulièrement contrôlés. Le régulateur doit compenser activement cette tendance par une politique exigeante envers les grands acteurs, et plus encore avec les très grands acteurs, à proportion des risques qu'il suscitent et des moyens dont ils disposent. Ainsi, comme le précise d'ailleurs la déclaration conjointe CNIL-Autorité de la concurrence de décembre 2023, la CNIL assume déjà, et va assumer encore plus à l'avenir, une dimension asymétrique de son action de régulation sur les marchés numériques, associée à une pleine compréhension des modèles d'affaires, au bénéfice des personnes et de la protection de leurs droits fondamentaux.

Document 3 : Article publié sur Le Monde, le 21 Avril 2022

Fuite de données médicales de 500 000 Français : l'entreprise Dedalus condamnée à 1,5 million d'euros d'amende

La CNIL reproche à la société, éditrice d'un logiciel vendu à plusieurs laboratoires, d'importants manquements de sécurité qui ont conduit à la fuite de données.

La Commission nationale de l'informatique et des libertés (CNIL), le « gendarme » français des données personnelles, a annoncé jeudi 21 avril avoir condamné l'entreprise Dedalus à une lourde amende de 1,5 million d'euros à la suite d'une vaste fuite de données de santé.

A la mi-février 2021, un internaute mettait en libre accès, sur un forum de discussion, une base de données contenant des informations médicales sensibles concernant un demi-million de Français. On pouvait notamment y trouver leur nom, prénom et adresse postale, mais aussi leur numéro de téléphone et adresse e-mail ainsi que leur groupe sanguin ou leur numéro de Sécurité sociale. Des informations médicales ultrasensibles figuraient aussi dans les données publiées, notamment relatives *« au VIH, cancers, maladies génétiques, grossesses, traitements médicamenteux suivis par le patient, ou encore des données génétiques »*, précise la CNIL.

La source de la fuite avait été rapidement identifiée comme provenant d'un logiciel commercialisé auprès de laboratoires par la société Dedalus Biologie. A l'époque, la CNIL avait ouvert une enquête et procédé à des contrôles auprès de l'entreprise. Les résultats de ces contrôles, accablants, ont conduit l'autorité administrative à infliger une amende élevée, mais aussi à rendre publique cette sanction.

« Nombreux manquements »

La CNIL estime la société responsable d'importantes infractions vis-à-vis du Règlement général sur la protection des données (RGPD), le cadre européen en matière de données personnelles. Elle reproche en particulier à l'entreprise de *« nombreux manquements techniques et organisationnels en matière de sécurité »*, en particulier *« l'absence de chiffrement »* de certaines données, *« l'absence d'authentification »* pour accéder à une partie de l'infrastructure informatique, ou encore *« l'absence d'effacement automatique des données après* [leur] *migration »*.

Pour la CNIL, *« cette absence de mesures de sécurité satisfaisantes est l'une des causes de la violation de données qui a compromis les données médico-administratives de près de 500 000 personnes »*. La CNIL accuse également la société d'avoir outrepassé les demandes de ses clients, en l'occurrence des laboratoires médicaux, lors *« de la migration d'un logiciel vers un autre outil »*, extrayant *« un volume de données plus important que celui requis »*.

Sollicitée après l'annonce de l'amende infligée par la CNIL, Dedalus assure avoir, *« dès la révélation de la cyberattaque en 2021 »*, *« déployé toutes les mesures possibles »* pour *« identifier d'éventuelles vulnérabilités »* et avoir travaillé à *« remédier aux manquements relevés par la CNIL »*. L'entreprise affirme avoir procédé au *« renforcement de certaines infrastructures IT »*, à *« l'amélioration de plusieurs procédures internes et externes »*, lancé *« un volet important de formation interne »* et réalisé des *« embauches additionnelles »* dans les services responsables de la cybersécurité de l'entreprise.

Une enquête judiciaire ouverte

Quelques jours après la révélation de la fuite de données, le tribunal judiciaire – saisi en référé par la CNIL – avait ordonné aux fournisseurs d'accès à Internet français de bloquer l'accès des internautes au site sur lequel étaient publiées les données.

Si l'amende infligée par la CNIL vient sanctionner des manquements en matière de sécurité, le ou les responsables du piratage et de la mise en ligne des données n'ont pas été identifiés. Ces données pourraient d'abord avoir été proposées à la vente, plusieurs mois avant la découverte publique de la fuite, sur des forums en ligne spécialisés. Le vendeur initial aurait ensuite publié ces données en libre accès à la suite d'un conflit avec un acheteur.

Le parquet de Paris a ouvert une enquête pour piratage informatique et l'a confiée à l'unité de police spécialisée dans la lutte contre la cybercriminalité.

Document 4 : Graphiques à propos du RGPD en Europe