Image not found or type unknown

Atteinte au RGPD et concurrence déloyale

Conseils pratiques publié le **21/03/2025**, vu **468 fois**, Auteur : Murielle Cahen

La problématique de la protection des données à caractère personnel s'affirme comme un enjeu majeur, suite à l'instauration du Règlement général sur la protection des données (RGPD) par l'Union européenne.

Ce texte législatif, qui a vu le jour le 25 mai 2018, se donne pour mission essentielle de garantir un niveau de protection élevé des droits et libertés fondamentales des individus, en particulier en ce qui concerne le traitement de leurs données personnelles.

Le RGPD représente le couronnement d'une réflexion approfondie sur le délicat nécessité de concilier la sauvegarde des informations personnelles avec les exigences d'une économie numérique en constante évolution et expansion. Dans ce cadre, la question des pratiques commerciales déloyales, et plus particulièrement celles qui touchent à la concurrence entre les acteurs économiques, est devenue un sujet central des débats juridiques au sein de l'Union européenne.

Cette dynamique est d'autant plus pertinente dans un contexte où les entreprises, notamment dans le secteur de la santé, doivent naviguer avec prudence entre l'exploitation commerciale de données et le respect des droits des consommateurs. L'affaire C-21/23, jugée par la Cour de justice de l'Union européenne (CJUE) le 4 octobre 2024, illustre avec éclat les défis contemporains auxquels sont confrontés les acteurs économiques, en l'occurrence les pharmaciens.

Dans ce litige, des divergences sont apparues concernant les pratiques de traitement des données, mettant en lumière non seulement des enjeux de conformité au RGPD, mais aussi des questions de concurrence déloyale. La décision rendue par la CJUE revêt une importance capitale, car elle affirme que le RGPD ne se limite pas à accorder des droits aux seules personnes concernées par le traitement de leurs données, mais qu'il ouvre également la voie à des actions en justice pour les concurrents qui estiment qu'une entreprise enfreint les dispositions de ce règlement. En d'autres termes, la CJUE reconnaît aux acteurs économiques la possibilité d'engager des recours judiciaires au nom de la protection des données personnelles, renforçant ainsi la lutte contre les comportements jugés déloyaux dans le cadre des relations commerciales.

Cette interprétation des droits des concurrents au regard du RGPD souligne l'importance pour les États membres de l'Union européenne d'adopter des dispositions législatives permettant de sanctionner les violations des règles de protection des données. Il est essentiel de comprendre que la protection des données personnelles ne doit pas être envisagée comme un simple ensemble de normes, mais comme un principe fondamental qui conditionne la confiance des consommateurs dans les pratiques commerciales. En effet, la CJUE a précisé que certaines données, notamment celles collectées lors de la vente en ligne de médicaments réservés aux pharmacies, relèvent de la catégorie des données de santé au sens du RGPD.

Cette classification est d'une importance capitale, car elle s'applique même dans les situations où les médicaments concernés ne nécessitent pas de prescription médicale. L'interprétation extensive des données de santé par la CJUE souligne l'impératif d'obtenir un consentement

explicite et éclairé des consommateurs pour le traitement de leurs informations personnelles. Le principe du consentement informé, qui est au cœur du RGPD, a des répercussions significatives sur les pratiques commerciales des pharmaciens opérant en ligne. Ces derniers doivent désormais redoubler de vigilance quant à la manière dont ils collectent, traitent et utilisent les données de leurs clients. Cette obligation de diligence s'inscrit dans une dynamique plus large, où les entreprises doivent s'engager à respecter non seulement les exigences légales, mais aussi les attentes sociétales en matière d'éthique et de transparence.

À la lumière de cette décision, la CJUE éclaire non seulement les contours de la protection des données à caractère personnel, mais elle met également en exergue les implications considérables que cela engendre pour les pratiques commerciales au sein d'un secteur où l'éthique et la conformité légale doivent impérativement converger. Dans un environnement commercial de plus en plus concurrentiel, les entreprises se trouvent dans l'obligation de jongler avec la nécessité de protéger les données personnelles des consommateurs tout en répondant aux exigences du marché. Cette dualité constitue un défi majeur pour les acteurs économiques, qui doivent adopter une approche proactive en matière de conformité légale et d'éthique.

Il convient également de rappeler des exemples jurisprudentiels antérieurs, tels que l'affaire Google Spain SL, où la CJUE a établi un droit à l'oubli pour les individus. Cette décision a eu pour effet de renforcer la protection des données personnelles face aux exigences d'indexation et de recherche en ligne, illustrant ainsi la capacité de la jurisprudence à adapter les règles de protection des données aux réalités changeantes du numérique.

I- Les fondements juridiques de la protection des données à caractère personnel et leur impact sur les pratiques commerciales

A- Le RGPD : un cadre juridique protecteur et contraignant

1. Présentation des objectifs et des principes fondamentaux du RGPD

Le Règlement général sur la protection des données (RGPD) constitue une avancée majeure en matière de protection des données personnelles. Son adoption a été motivée par la nécessité d'harmoniser les législations des États membres de l'Union européenne, tout en répondant aux préoccupations croissantes des citoyens en matière de confidentialité et de sécurité des informations personnelles.

Le RGPD est articulé autour de plusieurs principes fondamentaux, dont la légalité, la transparence et la limitation des finalités. Ce dernier impose que les données personnelles soient collectées pour des finalités déterminées, explicites et légitimes, et qu'elles ne soient pas traitées de manière incompatible avec ces finalités. Le principe de minimisation des données impose également que seules les informations strictement nécessaires soient collectées, tandis que le principe de précision exige que les données soient tenues à jour.

Enfin, le RGPD établit des obligations de responsabilité, stipulant que les responsables de traitement doivent démontrer leur conformité aux exigences du règlement. Ces principes visent à garantir non seulement la protection des données individuelles, mais aussi à instaurer un climat de confiance entre les citoyens et les entités qui traitent leurs données.

2. Les droits des personnes concernées et les obligations des responsables de traitement

Le RGPD confère un ensemble de droits puissants aux personnes concernées. Parmi ceux-ci, on trouve le droit d'accès, qui permet aux individus de connaître les données les concernant détenues par une entreprise, ainsi que le droit de rectification, qui leur donne la possibilité de corriger des informations inexactes.

Le droit à l'effacement, souvent désigné comme le "droit à l'oubli", permet aux individus de demander la suppression de leurs données dans certaines circonstances. Par ailleurs, le droit à la portabilité des données permet aux personnes de transférer facilement leurs données d'un responsable de traitement à un autre. Les responsables de traitement, quant à eux, sont soumis à des obligations strictes. Ils doivent mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté aux risques. De plus, ils sont tenus de réaliser des analyses d'impact sur la protection des données lorsque le traitement présente un risque élevé pour les droits et libertés des personnes physiques. Ces obligations visent à renforcer la responsabilité des entreprises en matière de traitement des données personnelles et à garantir un respect rigoureux des droits des individus.

B- La concurrence et les pratiques commerciales déloyales : une interaction nécessaire avec le RGPD

1. La capacité des concurrents à agir en justice au titre des pratiques commerciales déloyales

Dans le cadre du RGPD, les États membres ont la latitude d'établir des dispositions législatives permettant à des concurrents d'agir en justice contre des entreprises soupçonnées de pratiques contraires aux principes de protection des données. Cette faculté d'action est particulièrement pertinente dans les secteurs où les violations des données peuvent avoir des répercussions non seulement sur les consommateurs, mais également sur la concurrence. En permettant à des concurrents de contester des pratiques commerciales jugées déloyales, le législateur vise à promouvoir une concurrence équitable et à dissuader les comportements fautifs.

Les actions en justice des concurrents peuvent aussi contribuer à la protection des droits des personnes concernées, en renforçant la vigilance autour des pratiques de traitement des données. Cette dynamique incite les entreprises à adopter des comportements conformes au RGPD, sachant qu'elles peuvent être tenues responsables non seulement vis-à-vis des régulateurs, mais également vis-à-vis de leurs pairs. Ainsi, la possibilité d'une action en justice par un concurrent apparaît comme un outil efficace dans la lutte contre les violations des données.

2. La contribution de cette démarche à la protection des données et à la concurrence loyale

En intégrant la possibilité pour les concurrents d'agir en justice, la législation renforce indéniablement la protection des données. Cela crée un écosystème dans lequel les entreprises sont davantage incitées à respecter les normes de conformité. En effet, lorsque les entreprises savent qu'elles peuvent être tenues responsables par leurs concurrents pour des violations potentielles, cela les pousse à investir dans des pratiques de gestion des données conformes et éthiques. Cette approche favorise également une concurrence loyale sur le marché.

Les entreprises qui respectent le RGPD et qui adoptent des pratiques transparentes de traitement des données peuvent ainsi se différencier positivement de celles qui choisissent des voies moins scrupuleuses. Une telle dynamique contribue à créer un environnement commercial plus équitable, où les consommateurs peuvent avoir confiance dans les pratiques des entreprises qui traitent leurs données.

En effet, lorsque les entreprises savent qu'elles doivent se conformer aux normes du RGPD pour éviter d'éventuelles poursuites de la part de concurrents, cela limite la tentation de contourner les règles pour obtenir un avantage compétitif. Cela renforce l'idée que la conformité à la législation sur la protection des données n'est pas seulement une obligation légale, mais aussi un atout commercial. De plus, cette approche favorise l'innovation en matière de protection des données. Les entreprises sont incitées à développer des solutions technologiques et des pratiques commerciales qui respectent les droits des consommateurs.

Cela peut inclure le développement d'outils de gestion des consentements, des plateformes de transparence sur l'utilisation des données, et des systèmes de sécurité avancés pour protéger les informations sensibles. En conséquence, les entreprises qui investissent dans des pratiques conformes au RGPD peuvent non seulement éviter des sanctions, mais aussi se positionner comme des leaders dans un marché de plus en plus conscient des enjeux de la protection des données.

II- L'interprétation des données de santé et le consentement explicite dans le cadre de la vente en ligne de médicaments

A- La qualification des données de santé au sens du RGPD

1. Analyse des informations relatives à la santé dans le cadre des commandes en ligne

Dans le cadre de la vente en ligne de médicaments, la collecte et le traitement des données personnelles relatives à la santé soulèvent des questions essentielles. Selon le RGPD, les données de santé sont considérées comme des données sensibles qui nécessitent une protection renforcée. La Santé inclut toutes les informations concernant la santé physique ou mentale d'une personne, y compris les informations sur des traitements médicaux, des diagnostics, et des prescriptions.

Lorsqu'un consommateur commande un médicament en ligne, des données telles que son historique médical ou ses allergies peuvent être collectées, ce qui augmente les obligations en matière de consentement et de sécurité. La reconnaissance des données de santé comme sensibles oblige les pharmacies en ligne à mettre en place des mesures strictes de protection des données, notamment en matière de cryptage et de contrôle d'accès. De plus, les entreprises doivent être conscientes que toute violation de ces données peut avoir des conséquences graves, tant sur le plan juridique que sur la réputation. En ce sens, l'affaire C-21/23 a mis en lumière la nécessité pour les pharmaciens de comprendre et de respecter les exigences du RGPD lorsqu'ils traitent des données de santé, même dans des cas où des médicaments ne nécessitent pas de prescription.

2. Implications de la reconnaissance de ces données comme sensibles pour les pharmaciens

La qualification des données de santé comme sensibles a des implications significatives pour les pharmaciens, surtout dans un contexte de vente en ligne.

Tout d'abord, cela implique que les pharmaciens doivent obtenir un consentement explicite et éclairé de la part des consommateurs avant de traiter leurs données. Ce consentement doit être donné librement, spécifique, informé et univoque, ce qui signifie que les consommateurs doivent être clairement informés des finalités pour lesquelles leurs données seront utilisées.

En outre, les pharmaciens doivent s'assurer que les consommateurs comprennent les risques associés à la fourniture de leurs données personnelles. Cela nécessite de mettre en place des dispositifs de communication clairs et accessibles, expliquant comment les données seront protégées et utilisées. Les pharmacies doivent également être prêtes à répondre aux demandes de retrait de consentement, ce qui pourrait nécessiter des ajustements dans leurs systèmes de gestion des données.

B- L'importance du consentement explicite et de l'information des consommateurs

1. Les exigences en matière de consentement pour le traitement des données de santé

Le RGPD impose des exigences strictes en matière de consentement pour le traitement des données de santé. Les pharmaciens doivent s'assurer que le consentement est recueilli de manière proactive et que les consommateurs sont pleinement conscients des implications de leur accord. Cela inclut la nécessité d'expliquer clairement quelles données seront collectées, pourquoi elles le seront, et comment elles seront utilisées. De plus, le consentement doit être documenté, et les entreprises doivent être en mesure de prouver qu'elles ont obtenu ce consentement en cas de litige. Il est également essentiel que les pharmaciens mettent en place des mécanismes permettant aux consommateurs de retirer leur consentement à tout moment. Cela renforce le contrôle des consommateurs sur leurs propres données et est conforme aux principes de transparence et de responsabilité prévus par le RGPD. De plus, les pharmacies doivent être prêtes à répondre aux demandes des consommateurs concernant l'accès à leurs données, ainsi qu'à la rectification ou à l'effacement de celles-ci.

2. La nécessité d'informer les consommateurs de manière claire et accessible

Pour que le consentement soit valide, il est crucial que les informations fournies aux consommateurs soient claires, compréhensibles et facilement accessibles. Les pharmacies en ligne doivent donc veiller à rédiger des politiques de confidentialité qui expliquent de manière détaillée les pratiques de traitement des données, en évitant le jargon juridique complexe. Cela peut inclure des éléments tels que :

Personnelles de données collectées (par exemple, informations sur la santé, coordonnées personnelles).

- Les finalités du traitement (par exemple, la délivrance de médicaments, le suivi des commandes).

- Les droits des consommateurs concernant leurs données (accès, rectification, effacement). - Les mesures de sécurité mises en place pour protéger les données.

- Les coordonnées du responsable du traitement ou du délégué à la protection des données. En adoptant une approche proactive en matière d'information, les pharmacies peuvent non seulement

se conformer aux exigences légales, mais aussi établir une relation de confiance avec leurs clients. Cela peut contribuer à renforcer la fidélité des consommateurs et à améliorer l'image de marque des entreprises dans un secteur de plus en plus concurrentiel.

III- Les enjeux de la conformité et des sanctions en matière de protection des données dans le secteur pharmaceutique

A- Les conséquences juridiques de la non-conformité au RGPD

1. Les types de sanctions encourues par les entreprises

La non-conformité au RGPD peut entraîner des sanctions lourdes pour les entreprises, notamment des amendes financières qui peuvent atteindre jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial, selon le montant le plus élevé. De plus, les entreprises peuvent faire face à des actions en justice de la part des consommateurs ou d'organismes de régulation, ce qui peut entraîner des coûts juridiques significatifs et nuire à la réputation de l'entreprise. Outre les sanctions financières, une non-conformité peut également entraîner des mesures correctives imposées par les autorités de protection des données, telles que l'obligation de cesser certaines pratiques de traitement ou d'implémenter des audits réguliers. Cela peut perturber les opérations commerciales et entraîner des pertes de revenus.

2. L'impact sur la réputation et la confiance des consommateurs

Les conséquences de la non-conformité ne se limitent pas aux sanctions financières. En effet, la perception du public envers une entreprise peut être gravement affectée par une violation de données ou une non-conformité au RGPD. Les consommateurs sont de plus en plus sensibles aux questions de protection des données et peuvent choisir de ne pas faire affaire avec des entreprises qui ne respectent pas leurs droits. La réputation d'une entreprise peut être difficile à rétablir après une violation, et les consommateurs peuvent partager leurs expériences négatives sur les réseaux sociaux, amplifiant ainsi l'impact sur la réputation de la marque. En revanche, les entreprises qui démontrent un engagement fort en matière de protection des données peuvent bénéficier d'une amélioration de leur image de marque et d'une fidélisation accrue de leur clientèle.

B- Les bonnes pratiques pour garantir la conformité au RGPD

1. Mise en place d'une culture de la protection des données au sein de l'entreprise

Pour garantir la conformité au RGPD, il est essentiel d'instaurer une culture de la protection des données au sein de l'entreprise. Cela inclut la sensibilisation et la formation des employés sur les enjeux de la protection des données, ainsi que sur les obligations légales qui en découlent. Les entreprises doivent veiller à ce que tous les employés comprennent leurs responsabilités en matière de traitement des données et soient conscients des conséquences potentielles de la non-conformité.

2. Élaboration de politiques et de procédures claires de protection des données

Les entreprises doivent établir des politiques et des procédures claires concernant le traitement des données personnelles, y compris des protocoles pour la collecte, le stockage, le partage et la destruction des données. Cela inclut la mise en place de mesures de sécurité techniques et organisationnelles appropriées pour protéger les données, ainsi que des procédures pour gérer les violations de données.

Sources :

CJUE : atteinte au RGPD contestée en justice par un concurrent comme pratique commerciale déloyale - LE MONDE DU DROIT : le magazine des professions juridiques

CURIA - Documents

Guide de la sécurité des données personnelles 2024

RGPD : Qu'est-ce qu'une donnée sensible ? - Définition