Facebook Ireland Limited _ le 31 décembre 2021

Facebook Ireland Limited a été sanctionné de 60 millions d'euros pour sa politique sur les cookies. Le CNIL (Commission Nationale de l'Informatique et des Libertés) a reçu plusieurs plaintes en France qui dénonçaient la complexité de refuser les cookies sur le site facebook.com. En effet le CNIL a mené une enquête où elle a réalisé que c'était beaucoup plus simple pour l'utilisateur d'accepter les cookies en un seul click unique plutôt que de les refuser en passant par plusieurs clicks voire même une autre fenêtre intitulée « Accepter les cookies » où le bouton de refus se situe tout en bas de la fenêtre. Le CNIL a jugé ces points déroutant pour l'utilisateur qui pour la plupart du temps aura l'impression **qu'il est impossible de refuser les cookies**. Les cookies sont des empreintes uniques de chaque ordinateur basé sur ses éléments de configuration. Ils sont utilisés afin d'identifier l'ordinateur utilisé sur un site.

Ces actions sont en violation de l'article 82 de la loi Informatique et Libertés qui ont été mis en place pour permettre à l'utilisateur d'exercer pleinement son consentement en ce qui concerne la transmission de ses données quel que soit sa destination.

Facebook Ireland Limited a donc été sanctionné à une amende de 60 millions d'euros. Cette amende a été déterminée en fonction du nombre d'utilisateurs atteints et de la rémunération potentielle par la publicité indirectement obtenue via la confusion des utilisateurs. En plus de l'amende, Facebook Ireland Limited a un délai de 3 mois pour changer la politique de ses cookies en France afin de permettre à l'utilisateur de pleinement choisir d'autoriser ou non les cookies. Au-delà de ce délai, la compagnie aura une amende supplémentaire de 100.000 euros par jour de retard.

La raison pour laquelle ce cas est important est parce que nous avons une présence personnelle sur internet de plus en plus imposante et la rapidité de l'information est de plus en plus rapide. De ce fait, les compagnies se doivent de fournir les moyens nécessaires pour permettre à l'utilisateur d'exercer pleinement son consentement en ce qui concerne la capture de ses informations et le suivi de son activité sur internet. Pour cela, les lois sont nécessaires pour prévoir, punir, et rectifier les éventuels abus.

Stockage des données Facebook US en Europe _ 3 février 2022

Le 3 février dernier, Mark Zuckerberg du groupe Meta avait annoncé qu'il ne pourrait plus proposer les services Facebook et Instagram en Europe. En 2020, la Data Protection Commission impose à Facebook de cesser ses transferts de données de l'Europe vers les Etats Unis. **En effet, les données des utilisateurs européens ne sont pas stockées sur le territoire européen, mais transférés vers des serveurs aux Etats Unis**. Ces informations étant la marchandise cruciale de la plateforme, Mark Zuckerberg avait déjà fait ce genre de menaces par le passé.

La raison pour laquelle l'Europe veut conserver les données de ces utilisateurs sur le sol Européens est non seulement **de l'ordre de la sécurité des données, moins de transfert, moins de risques de piratage, mais aussi de l'ordre législatif**. Les données en Europe sont soumises aux lois européennes alors qu'à l'heure actuelle, elles sont stockées aux Etats Unis donc sujettes aux lois américaines. Facebook s'y oppose parce que naturellement en tant qu'entreprise lucrative, si elle n'a pas le

control total de sa marchandise, cette dernière perd de la valeur. Ce n'est pas la première fois que la Data Protection Commission se prononce sur le sujet comme en 2020, et la compagnie avait déjà faite plusieurs fois cette menace mais elles ont été à chaque fois démenties par la suite par des communiqués officiels.

Cependant la Data Protection Commission a l'intention de réitérer son obligation dans les prochains mois et a moins que Mark Zuckerberg ait l'intention de perdre le 2ème plus gros marché du monde, il va devoir soit se soumettre à la législation et laisser les Européens héberger les données de ses propres utilisateurs, ou trouver un compromis qui satisfera la DPC.

Nouvelle loi « Cyberscore » _ le 1 octobre 2023

Le 3 mars 2022, le Sénat approuve la proposition de la loi « Cyberscore ». Votée le 24 février dernier, la loi impose aux grandes plateformes numériques, aux **services de messageries instantanées**, et aux services de visioconférences de nouvelles obligations envers les utilisateurs vis-à-vis de la **transparence et de la sécurité**. Ils devront par exemple afficher un indice du niveau de sécurité appelée Cyberscore qui sera déterminé en fonction d'un audit de sécurité de leur service. Tout manquement sera sanctionné. Aussi ces services devront indiquer à l'utilisateur la localisation des données stockée par la compagnie ou leurs prestataires tel que cloud. Un décret listera les compagnies concernées en fonction du volume de leur activité et **la loi entrera en vigueur le 1er octobre 2023**.

Cette loi permet plus de transparence et plus de sécurité pour les utilisateurs. Ce sont des aspects importants étant donné qu'il est très courant de nos jours que des informations importantes soient échangées en message direct ou en visioconférence par pure convenance et dans une certaine intimité perçue. La loi « Cyberscore » assurera donc que l'utilisateur soit pleinement conscient du niveau de sécurité du site ou du service avant de décider d'envoyer par exemple des informations bancaires à son interlocuteur. Il sera capable de faire un choix plus informé en ce qui concerne son partage de données sur internet. Quant à la localisation des données, il est important de savoir où elle se trouve exactement. Les lois et les processus à propos du stockage des données et leur traitement varient d'un pays à un autre. L'utilisateur aura donc connaissance si ses données sont susceptibles d'être vendues à des entreprises de marketing ou observées et stockées par le gouvernement local.

La transparence est un élément crucial pour l'utilisateur afin de pouvoir exercer pleinement son consentement en ce qui concerne le choix de confier ou non des informations importantes ou/et privées sur un site ou un service. Dans notre société, seules les lois peuvent garantir cette sécurité aux utilisateurs.

À partir d'octobre 2023, les sites internet générant le plus de trafic en France pourraient être dans **l'obligation d'afficher un score lié à leur niveau de sécurisation**. En cas de manquement, les contrevenants seraient sanctionnés d'une amende.

L’état veut allouer 7.5 milliards d’euros sur 5 ans pour la Cybersécurité _ le 12 janvier 2022

Le ministre de l’intérieur Gerald Darmanin a pour projet de **numériser tous les documents officiels** tels que les cartes d’identité, carte grises... **ainsi que toutes les procédures pénales afin de centraliser la base de données et faciliter le transfert des informations**. Pour cela il faudrait une sécurité sans faille ou les données risqueraient d’être piratées. Pour prévoir une telle éventualité, le gouvernement a décidé d’éventuellement allouer 7.5 milliards d’euros pour la cybersécurité.

Cependant la protection ne s’applique pas que pour les données gouvernementales. Il y a de plus en plus de gens capables de pirater des serveurs à distance, donc il est naturel qu’il faille investir davantage dans la sécurité. Le nombre de cyberattaques a été multiplié par 4 l’an dernier et depuis le début de l‘année, il y a eu des attaques régulièrement toutes les semaines contre les hôpitaux. Lors des jeux olympiques de Tokyo, les autorités ont dû empêcher plus de 3500 attaques cyber par jour. Il est donc normal que le gouvernement soit concerné étant donné que les jeux olympiques de Paris approchent en 2024 et on n’y prévoit pas moins de 400000 attaques cyber. C’est face à ces attaques incessantes que le gouvernement a décidé d’investir davantage dans la cybersécurité.

Ce budget comprend aussi **une portion de 500 millions pour la recherche contre les cyberattaques**. La France n’a jamais eu les moyens adéquats pour maintenir la sécurité et dépend généralement des organisations externes ou des pays comme les Etats Unis ou Israël. Le gouvernement planifie donc de se garantir d’une indépendance dans les prochaines années en développant sa propre cybersécurité. La fin de la dépendance dans le domaine assurera l’autonomie de la France, surtout avec les enjeux internationaux en constante évolution.

Amende de 10000 euros à la SNBC pour publicité non sollicitée

Le 5 mai dernier - 2022, l'Autorité de Protection des Données (APD) a infligé **une amende de 10000 euros à la Société Nationale des Chemins de fer Belge (SNCB)** pour avoir envoyé un courriel publicitaire a tous les ménages ayant demandé le Hello Belgium Railpass. La particularité de ce courriel est le fait que c'est **une newsletter récurrente qui n'a pas d'option pour se désabonner** et donc en infraction directe à l'article 7 alinéa 3 du Règlement Général sur la Protection des Données (RGPD). Cette dernière stipule que "**La personne concernée a le droit de retirer son consentement à tout moment. (...) Il est aussi simple de retirer que de donner son consentement**."
La SNCB a tenté une défense où elle a proclamé que le courrier était nécessaire dû à la situation précaire laissée par la deuxième vague de la pandémie du COVID, mais l'APD en a juste vu une tactique de marketing direct et non sollicitée.
Plus de 3 millions de ménages sont concernés, la SNCB a donc 30 jours pour faire appel si elle souhaitait se défendre davantage.

Comment supprimer vos informations personnelles de Google

Il est courant que les informations personnelles (numéro de téléphone, adresse mail, des données médicales personnelles, des images de signature manuscrite ou de pièce d’identité…) de quelqu'un soit disponible sur internet. En effet le nombre croissant de comptes de toutes sortes ainsi que le marché de vente des données signifie que vos données personnelles circulent librement avec ou sans votre consentement**. Google a donc mis au point une fonction simple et accessible pour retirer vos infos**

personnelles. **Selon la loi du 20 Juin 2018 relative à la protection des données, les internautes peuvent demander à ce que leurs informations soient supprimée ou au moins rendues invisible aux yeux des moteurs de recherche**. Cependant Google va plus loin, ils ont rajouté une fonctionnalité permettant à l'utilisateur de masquer leurs informations sur des sites. Les masquer ne veut pas dire supprimer, en effet le site possède toujours vos informations. Mais pour y accéder, il faudra l'URL complet. Aussi ça ne cachera pas vos infos des autres moteurs, vos informations seront tout simplement déférencées.