TECHNIQUES
DE L'INGÉNIEUR

LES FOCUS
TECHNIQUES DE L'INGÉNIEUR

RGPD
UN AN APRÈS

mai / 2019

SOMMAIRE

INTRODUCTION

Exécutoire depuis un an, le RGPD (Règlement Général sur la Protection des Données) oblige les entreprises à revoir leurs méthodes de traitements des données personnelles et à renforcer leur sécurité informatique. Mais peu d'organisations peuvent affirmer qu'elles sont en conformité. Quand certaines n'ont encore rien fait…

Avec ces 99 articles, le RGPD représente un chemin de croix pour de nombreuses entreprises. Et il faudra là aussi plusieurs années avant que ce règlement ne devienne une « norme ». Complexe à comprendre et nécessitant des adaptations particulières, il exige une profonde évolution des mentalités de tous les services d'une entreprise.

Mais la situation évolue très lentement. Certes, le RGPD a eu le mérite de provoquer une prise de conscience plus ou moins forte, tant de la part des entreprises que des consommateurs, sur les enjeux de la protection des données personnelles. Un récent baromètre CNIL/IFOP indique ainsi que 66% de la population française se dit aujourd'hui plus sensible au sujet qu'avant la mise en vigueur du règlement.

En se focalisant uniquement sur les sanctions, de nombreuses entreprises se sont dit qu'elles ne risquaient rien, la CNIL se concentrant sur les grands groupes et les GAFAM (Google, Amazon, Facebook, Apple et Microsoft) pour montrer l'exemple. Et l'actualité des sanctions leur a donné raison. En janvier dernier, la CNIL a prononcé une sanction de 50 millions d'euros à l'encontre de la société GOOGLE LLC en application du RGPD pour « manque de transparence, information insatisfaisante et absence de consentement valable pour la personnalisation de la publicité ».

IL Y A UN AN...

LOGICIELS ET APPLICATIONS MOBILES : LE CASSE-TÊTE DE LA CONFORMITÉ AVEC LE RGPD

Le 25 mai prochain, le RGPD (Règlement Général sur la Protection des Données) entre en vigueur. En renforçant la protection de tous les citoyens européens, il oblige les éditeurs de logiciels à revoir leurs copies… Pas simple.

Même s'il existe déjà tout un arsenal juridique protégeant les données personnelles des consommateurs et des internautes, le RGPD devient un peu plus contraignant. Tout repose sur la définition d'une donnée à caractère personnel. Il s'agit de toute information permettant d'identifier une personne : nom, prénom, date de naissance, numéro de téléphone privé, mais aussi adresse IP, biométrie…

Une acception suffisamment large pour apparaître comme un casse-tête pour les éditeurs de logiciels et d'applications pour smartphone. Le texte européen prévoit notamment que toute personne peut récupérer l'ensemble de ses données personnelles auprès de n'importe quelle entreprise qui en possède.

L'ensemble de ces données doit impérativement être dans un format standard pour respecter l'interopérabilité.

Or, tout le monde n'est pas prêt à être en conformité avec le RGPD validé en 2016 ! Selon une étude de SafeDK, plus de la moitié des applications sur Play Store ne seraient pas conformes au RGPD. Ce cabinet, spécialisé dans l'utilisation des kits de développement logiciel (SDK) dans les applications mobiles, s'est appuyé sur l'analyse approfondie de centaines de milliers d'applications populaires de Google Play.

La transparence de Microsoft

Bilan ? Plus de la moitié (56 %) des applications ont au moins un SDK qui essaye d'accéder à l'emplacement de l'utilisateur. Deux applications sur cinq ont au moins un SDK qui tente d'obtenir la liste des applications installées sur le dispositif de l'utilisateur, tandis que 29,3 % des applications cherchent à obtenir la liste des contacts de l'utilisateur. Or, les informations personnelles ne sont protégées par aucune option permettant à l'utilisateur d'accorder ou non ce recueil.

SafeDK remarque cependant que l'accès aux données privées des utilisateurs tend à diminuer. Cette évolution positive témoignerait de la volonté d'éditeurs de se préparer à cette nouvelle réglementation. Elle s'explique aussi par la pression de Google qui a jouté de nouvelles règles détaillées sur le Play Store fin 2017.

Elles indiquent que les développeurs doivent « *faire preuve de transparence quant à la façon dont vous gérez les informations sur l'utilisateur [...] y compris en publiant les méthodes de collecte et de partage de ces informations, ainsi que la façon dont vous les utilisez* ». Google insiste : ils doivent « *limiter l'utilisation de ces données au cadre* ». Reste à savoir si ces nouvelles règles s'appliqueront aussi à Google…

De son côté, Apple prône une approche de type "differential privacy" : les données seraient anonymisées lors de leur traitement. Mais il collectera et traitera des données en lien avec photos, email, contacts, calendar, iCloud Drive. La raison ? l'amélioration de ses produits et services en utilisant, de manière confidentielle, les données des comptes iCloud. Bref, pour conserver une vie privée sous iOS, mieux vaut ne pas utiliser iCloud...

Même constat pour Microsoft qui veut mettre en avant son souci de transparence. Le géant entend assurer que les

données qu'il recueille sont utilisées pour améliorer ses produits et non pas pour suivre l'activité de ses utilisateurs...

Début février, l'éditeur a intégré une application permettant de constater les données collectées depuis Windows 10 (via le composant « Connected User Experience and Telemetry »). Cette option existe déjà pour les professionnels. La version « Diagnostic Data Viewer » sera destinée à un usage plus grand public.

Selon ZDNet, la plupart des données de diagnostic appartiennent à l'une des cinq catégories suivantes :

- Les données communes incluent la version du système d'exploitation et un ID terminal unique ;
- Les données de connectivité et de configuration des périphériques ;
- Les données Produit et Performance service comprennent les événements de performances et de fiabilité et des informations sur la santé du poste de travail ;
- Les données d'utilisation du produit et du service, c'est à dire sur Windows et les logiciels ;
- Les données de configuration avec entre autres des détails sur les applications installées et les mises à jour du terminal.

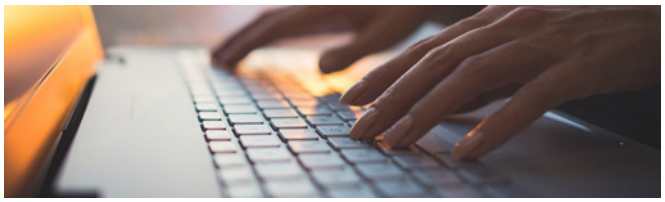
D'autres options permettent de supprimer l'historique de navigation, l'historique de recherche, les données de localisation enregistrées, les données vocales et l'activité de santé .

Philippe Richard

12/02/2018

PROTECTION DES DONNÉES PERSONNELLES : LE RETARD DES ENTREPRISES

Le 25 mai 2018, le Nouveau règlement européen sur la protection des données personnelles entrera en application. Validé en 2016, il renforce la protection des citoyens et accentue les obligations des entreprises. Mais ces dernières sont loin d'être prêtes…



Le GDPR fait trembler les entreprises ! L'acronyme anglais du Règlement Général sur la Protection des Données inquiète les professionnels car il impose la mise en place de nombreuses mesures complexes. Ce nouveau Règlement européen (RGPD) n° 2016/679 du 27 avril 2016 sur la protection des données est applicable à compter du 25 mai 2018.

Pour schématiser, il renforce la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés en vigueur en France. Évolution majeure : la notification des attaques informatiques et des failles de sécurité entrainant des fuites d'informations à caractère personnel.

Avec le GDPR, toutes les entreprises (y compris les sites de e-commerce) auront l'obligation de notifier les violations de données personnelles, contrairement à la Loi de 1978 qui ne concerne que les fournisseurs de services de communications électroniques.

Selon l'article 33 du RGPD, cette notification doit intervenir dans les 72 heures à compter de sa connaissance auprès de l'autorité de contrôle (en l'occurrence, la CNIL) et lorsque la violation est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne. L'entreprise, victime de cette fuite de données, doit également avertir par lettre recommandée avec AR tous ses clients et salariés.

En cas de non-application du RGPD, l'entreprise encourt des sanctions financières allant jusqu'à 4 % du chiffre d'affaires mondial annuel, limité à 20 M€. (Article 83.6 du Règlement).

Par ailleurs, ce règlement renforce la protection des citoyens. Les entreprises doivent obtenir un consentement explicite de la part de l'utilisateur final quant à l'utilisation ou au stockage de ses données privées. Elles doivent permettre la portabilité des données personnelles aux utilisateurs qui en feraient la demande. Ces derniers bénéficient d'un droit à la suppression de ses données personnelles par l'entreprise qui les traite.

Devant de telles contraintes, les entreprises doivent adopter des mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données nécessaires au regard de leurs besoins soient traitées (autrement appelé le « Privacy by Design »). Ces mesures techniques peuvent prendre plusieurs formes :

- la pseudonymisation et le chiffrement des données ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et des services de traitement...

Elles doivent obligatoirement nommer un délégué à la protection des données (Data Privacy Officer-DPO). Celui-ci sera le référent et s'assurera de la bonne mise en œuvre et du contrôle des traitements par mandat des utilisateurs et de l'administration.

Pour des nombreuses entreprises, quelles que soient leur taille et activité, ce GDPR est très contraignant et complexe. Résultat, de nombreuses études indiquent qu'elles ne sont pas encore prêtes.

Cette situation, anxiogène pour de nombreux chefs d'entreprise de PME, devrait profiter aux sociétés spécialisées dans la sécurité informatique. D'après le cabinet d'études Canalys, les ventes de licences et d'équipements en protection des systèmes d'information devraient progresser de 16 % (à 11,5 Md$ l'an prochain sur le vieux continent.) l'année prochaine.

Cette même étude signale que de nombreuses PME se tourneront vers leur prestataire de services IT pour ne pas avoir à payer les amendes prévues.

Par **Philippe Richard**

09/06/2017

LES ATTAQUES INFORMATIQUES CONCERNENT TOUTES LES ENTREPRISES

À l'occasion de la 17e édition des Assises de la Sécurité qui se tiennent à Monaco du 11 au 14 octobre, le patron de l'ANSSI a rappelé que personne n'est à l'abri. Un constat confirmé par l'Observatoire de la Cybersécurité réalisé par IDC.

La protection des données sensibles est la principale priorité pour 76 % des entreprises en matière de sécurité IT. C'est la principale conclusion de l'Observatoire de la Cybersécurité réalisé par IDC en partenariat avec Malwarebytes.

Cette conclusion n'est finalement pas très étonnante étant donné le contexte. Les résultats de l'étude montrent que les entreprises sont très nombreuses à avoir subi les conséquences négatives de ces attaques sur leur activité au cours des 12 derniers mois. Elles sont près de 70 % à mettre en avant les conséquences directes de ces cyber-attaques sur leur activité : indisponibilité du site Internet de l'entreprise pendant plusieurs heures (39 %), retard de livraison auprès des clients (27 %) ou encore arrêt de la production pendant quelques heures.

Cycle de vie des données

Pour les entreprises, la problématique est complexe. D'un côté, les attaques informatiques se multiplient et de l'autre côté, les entreprises se lancent dans leur transformation numérique en multipliant les connexions et les appareils échangeant des données entre eux. Le but ? Être le plus réactives possible pour répondre aux exigences de leurs clients et des consommateurs.

Mais cet objectif ne peut plus être atteint sans respecter un parcours très balisé par le Réglement européen pour la protection des données (RGPD). Un des élément-clés de ce texte, qui entre en application en mai prochain, a été de renforcer les droits de personnes au regard de leurs données, et notamment de s'assurer qu'elles donnent leur consentement à leur traitement. Dorénavant, les entreprises doivent mettre en place différentes techniques renforçant leur sécurité, mais également gérer leur cycle de vie pour rester en conformité (de la création d'une data à sa suppression) comme les droits à la portabilité (transmission

des données à des tiers) et à l'oubli.

3 milliards de comptes piratés !

À juste titre, on peut se demander si les entreprises, même internationales, protègent sérieusement les données qu'ils leur confient ! Début octobre, Yahoo ! a annoncé que la cyberattaque massive dont il a été victime en 2013 a affecté l'ensemble des 3 milliards de comptes d'utilisateurs et non pas seulement 1 milliard comme initialement annoncé.

Pour renforcer la sécurité des données qu'elles stockent et échangent, de plus en plus d'entreprises (75 %, selon cette étude d'IDC réalisée auprès de 200 structures basées en France et regroupant chacune plus de 500 salariés) misent sur le Cloud.

Mais une politiquer de sécurité ne peut être efficace que si elle est globale. C'est un processus qui peut être long, mais qu'il est indispensable d'entamer le plus tôt possible. C'est le message qu'a martelé hier le directeur général de l'ANSSI (Agence nationale de la sécurité des systèmes d'information), Guillaume Poupard, aux Assises de la sécurité à Monaco : « Il n'y aura pas de transformation numérique sans sécurité numérique. (...) Nos PME sont sans doute les premières ciblées, probablement. Je suis incapable de mesurer malheureusement, ce n'est pas glorieux, car on n'a pas de statistiques fiables sur les attaques, mais les PME sont directement ciblées. Et il y en a qui meurent en silence, qui mettent la clé sous la porte à cause d'attaques informatique »

Philippe Richard

13/10/2017

AUJOURD'HUI

RGPD : UNE MISE EN CONFORMITÉ LOIN D'ÊTRE GÉNÉRALISÉE

Exécutoire depuis un an, le RGPD oblige les entreprises à revoir leurs méthodes de traitements des données personnelles et à renforcer leur sécurité informatique. Mais peu d'organisations peuvent affirmer qu'elles sont en conformité. Quand certaines n'ont encore rien fait…

Rome ne s'est pas faite en un jour. Avec ces 99 articles, le RGPD représente un chemin de croix pour de nombreuses entreprises. Et il faudra là aussi plusieurs années avant que ce règlement ne devienne une « norme ». Complexe à comprendre et nécessitant des adaptations particulières, il exige une profonde évolution des mentalités de tous les services d'une entreprise.

Mais la situation évolue très lentement. Certes, le RGPD a eu le mérite de provoquer une prise de conscience plus ou moins forte, tant de la part des entreprises que des consommateurs, sur les enjeux de la protection des données personnelles. Un récent baromètre CNIL/IFOP indique ainsi que 66% de la population française se dit aujourd'hui plus sensible au sujet qu'avant la mise en vigueur du règlement.

La CNIL plus sévère

Excepté des entreprises appartenant à des secteurs très réglementés, « *la majorité des PME et des TPE que je côtoie ou pour lesquelles j'interviens sont très loin de la conformité* », avoue un DPO (Data Protection Officer ou délégué à la protection des données).

Or, cette politique de l'autruche ou ce « *retard à l'allumage* » n'est certainement pas la bonne méthode. Pour deux raisons principales. Premièrement, les plaintes déposées auprès de la CNIL ont fortement augmenté (plus de 11 000 l'année dernière). Deuxièmement, la CNIL va se montrer plus sévère. Dans un entretien accordé à La Tribune, la nouvelle présidente de la Commission nationale de l'informatique et des libertés (CNIL), Marie-Laure Denis, a déclaré qu'il faut « *désormais, faire preuve de davantage de fermeté. Notre action de régulation ne sera efficace que si nous actionnons à parts égales les deux leviers à notre disposition, c'est-à-dire la pédagogie d'un côté, et le contrôle avec éventuellement des sanctions de l'autre* ».

Mais en se focalisant uniquement sur les sanctions, de nombreuses entreprises se sont dit qu'elles ne risquaient rien, la CNIL se concentrant sur les grands groupes et les GAFAM (Google, Amazon, Facebook, Apple et Microsoft) pour montrer l'exemple. Et l'actualité des sanctions leur a donné raison. En janvier dernier, la CNIL a prononcé une sanction de 50 millions d'euros à l'encontre de la société GOOGLE LLC en application du RGPD pour « *manque de transparence, information insatisfaisante et absence de consentement valable pour la personnalisation de la publicité* ».

Attention aux CNIL européennes

Un an après, « *nous restons en France dans une logique de « pas vu, pas pris » et on attend de voir comment la CNIL va réagir* », constate Maître Anne-Sophie POGGI, Avocate à la Cour spécialisée en droit de la donnée.

Mais les entreprises ont tort de croire que les sanctions ne peuvent venir que de la CNIL. Premièrement, une CNIL italienne ou allemande par exemple peut demander des comptes à une entreprise française si elle a reçu des plaintes de citoyens italiens ou allemands. Le RGPD est en effet un règlement européen qui protège tous les citoyens de l'UE ! Deuxièmement, le donneur d'ordre français (ou, là aussi, européen) d'un sous-traitant français peut aussi exiger que celui-ci prouve sa conformité sous peine de perdre ce contrat…

Le RGPD instaure en effet une coresponsabilité entre les

entreprises et leurs sous-traitants. Une entreprise peut donc mandater un cabinet spécialisé pour réaliser des audits RGPD et de sécurité (les deux étant liés, contrairement à ce que pensent à tort de nombreux professionnels) afin de vérifier que les données personnelles qu'elle leur confie sont bien protégées...

Les entreprises sont loin d'en avoir fini avec le RGPD. Ce n'est que le début !

24/05/2019

LE RGPD : BIENTÔT UN « STANDARD » MONDIAL ?

La Commission européenne a adopté une décision d'adéquation concernant la protection des données personnelles circulant sur internet au Japon. Cette décision garantit aux internautes européens, particuliers et entreprises, de bénéficier des normes de protections élevées lorsque leurs informations sont transférées vers ce pays.

Les principes du Règlement général sur la protection des données (RGPD) sont repris par de nombreux pays. « *Aux États-Unis, tous les regards seront tournés vers la Californie avec son "California Consumer Privacy Act", la loi la plus sévère (aux USA, Ndlr) en matière de protection de la vie privée. Cette loi amènera probablement d'autres États à adopter leurs propres lois dans ce domaine. Par ailleurs, le NIST (National Institute of Standards and Technology) prépare un cadre de protection de la vie privée* », explique Michael Magrath, directeur de la réglementation et des normes mondiales chez OneSpan (une entreprise spécialisée dans la signature électronique).

Le RGPD s'exporte aussi à l'Est avec la décision d'adéquation récemment adoptée par la Commission Européenne. Il s'agit d''un des outils prévus par le règlement général sur la protection des données pour transférer des données à caractère personnel de l'UE vers des pays tiers.

Une meilleure définition des données sensibles

L'adéquation n'exige pas que le système de protection des données du pays tiers soit identique à celui de l'UE. Elle est basée sur le standard de l'équivalence essentielle. Pour que cet accord puisse être mis en œuvre, le Japon s'est engagé à introduire des garanties additionnelles dans ses règles de protection des données. Les données personnelles des Européens au Japon ne pourront être utilisées que dans des mesures « nécessaires et proportionnelles ».

Des garanties ont été définies afin de combler certaines différences entre les deux systèmes de protection des données. Par exemple, la définition japonaise des données sensibles a été élargie. L'exercice des droits individuels sera facilité et le transfert ultérieur des données des Européens du Japon vers un autre pays tiers sera soumis à un niveau de protection supérieur.

« *Cette décision d'adéquation va créer le plus grand espace de flux de données sécurisées au monde* », affirme Vera Jourova, la commissaire européenne à la Justice et aux Consommateurs. « *Il permettra aux entreprises européennes d'avoir un accès privilégié à un marché de 127 millions de consommateurs. Cet accord servira de modèle pour les futurs partenariats et aidera à fixer des normes mondiales* ».

Dans deux ans, les autorités des deux zones procéderont à une évaluation du système.

La Commission a adopté des décisions appropriées pour les pays et territoires suivants : Andorre, Argentine, Canada, États-Unis, îles Féroé, Guernesey, Israël, île de Man, Jersey, Nouvelle-Zélande, Suisse, Uruguay et États-Unis (bouclier de protection de la vie privée UE-USA).

Mais la décision d'adéquation du Japon est la première adoptée depuis l'entrée en vigueur du règlement général sur la protection des données le 25 mai 2018.

Avec les États-Unis, il s'agit d'une décision d'adéquation « partielle ». En l'absence d'une loi générale sur la protection des données privées outre-Atlantique, seules les entreprises qui s'engagent à respecter les principes contraignants de protection de la vie privée bénéficient des transferts gratuits de données.

15/02/2019

CCPA : LA CALIFORNIE AURA BIENTÔT SON RGPD VERSION LIGHT

Dans moins d'un an, cet État adoptera le California Consumer Privacy Act (CCPA). Cette loi renforcera les droits des consommateurs. Comme le règlement européen (RGPD), elle donnera aux particuliers un droit de regard sur l'usage qui en est fait de leurs informations professionnelles. Mais le CCPA n'est pas aussi strict que le RGPD.

Alors que le RGPD est exécutoire depuis le 25 mai 2018 en Europe, les États-Unis se préparent – doucement – à renforcer les droits des citoyens. En janvier 2020, le California Consumer Privacy Act (CCPA) entrera en application en Californie.

C'est une version light de notre règlement européen puisque le CCPA ne s'applique qu'aux entreprises californiennes dont le chiffre d'affaires est supérieur à… 25 millions de dollars et aux data brokers (spécialisés dans la revente de données personnelles). Rappelons que sur le vieux continent, toutes les entreprises européennes doivent se mettre en conformité.

Autre différence, le texte européen prévoit une gradation des sanctions en cas de non-conformité et/ou d'atteinte à la protection des données. Elles peuvent atteindre jusqu'à 4 % du chiffre d'affaires annuel global de l'entreprise ou 20 millions d'euros (le montant le plus élevé étant retenu).

Mauvais élèves

En Californie, les amendes seront appliquées par infraction (jusqu'à un maximum de 7 500 $ par infraction). La différence fondamentale concerne la conformité. En Europe, une entreprise peut être condamnée même si elle n'a pas été victime d'une fuite de données. Le CCPA ne sanctionnera qu'à partir du moment où une violation aura été constatée. Autre différence, les consommateurs américains peuvent poursuivre l'entreprise pour violation.

Néanmoins, le CCPA représente une première étape vers une meilleure protection des citoyens. D'autres États pourraient instaurer une réglementation plus ou moins similaire.

Mais comme en Europe, les entreprises californiennes traînent des pieds. Selon une étude de Trustar, une minorité d'entreprises sont d'ores et déjà en conformité.

Cependant, certaines entreprises américaines n'attendent pas d'être victimes d'une fuite de données pour entamer leur mise en conformité. Ces « bons élèves » californiens sont ceux qui sont déjà sensibilisés à ces problématiques.

21 % des entreprises qui ont travaillé sur la conformité avec le RGPD sont conformes avec le CCPA, comparativement à seulement 6 % pour les entreprises qui n'ont pas travaillé sur la conformité avec le texte européen.

Dans la majorité des cas, l'objectif principal des Californiens est de répondre aux exigences des partenaires et/ou des clients. Selon l'enquête de Trustar, un tiers mentionne le risque d'amendes ou les recours collectifs comme principal facteur de risque. Enfin, 18 % estiment qu'elle pourrait avoir un impact négatif sur leur réputation.

28/05/2019