BTS SIO

2022 - 2023

Cyber Sécurité des services informatiques

LETOUBLON	Thomas
GOUBET	Nicolas

Table des matières

Introduction

Début de la protection des données

Le secret des informations personnelles n'est pas un enjeu récent. On peut trouver dans l'histoire plusieurs traces de celui-ci :

- Secret médical en Inde vers 800 av J.C
- Serment d'Hippocrate vers 400 av J.C
- Secret de l'avocat vers 451 av J.C
- Secret de la confession en 1215

Avec le développement d'internet et du numérique, le partage des données ne connait plus de limite, ce qui génère une grande valeur économique, mais aussi un réel danger pour les personnes dont les données personnelles sont exploitées. Définir un cadre légal pour la protection des données représente donc un défi pour les institution nationales et européennes.

Il faut cependant attendre 1970 en France pour voir apparaitre dans le code civile le principe de « vie privée ».

La France reste cependant précurseur dans la prise de conscience liée aux conséquences potentiellement néfaste du développement de l'informatique. C'est dans cette période qu'on passe de la mécanographie avec les fiches perforées (Cf : IBM et le système nazi) à l'informatique.

Pour surveiller cela, la France créa la CNIL en 1974 qui était surtout là pour surveiller les administrations et les services de police. Désormais c'est la valeur commerciale des données personnelles que la CNIL doit protéger des entreprises.

C'est un fait : les données personnelles en disent long sur notre vie privée. Notre identité circule instantanément et librement dans le monde. Les fichiers et les technologies de traçage ne cessent de se multiplier sans que l'on ne le remarque.

Notre droit à l'intimité est mis en péril. L'internaute est à la fois le danger car il diffuse des informations sur lui-même et les autres mais également la proie, car, consciemment ou non, il devient une cible privilégiée des stratégies de marketing.

Mise en place de la RGPD

Le développement d'internet a vu l'apparition du marketing ciblé. Pour réussir cela, la stratégie de l'entreprise doit placer la connaissance du client au cœur de ses activités.

Si la technologie permet de collecter, réunir, traiter, diffuser des informations presque sans bornes techniques, c'est le droit qui doit définir les limites.

En 2012, la commission européenne a donc présenté une proposition de règlement général sur la protection des données dans l'optique de mettre en place un cadre solide et cohérent de protection permettant à l'économie numérique de se développer au sein du marché intérieur.

Les 3 objectifs du RGPD sont :

- Uniformiser les règles de protection des données au niveau européen
- Accroitre les droits des personnes concernées par les traitements des données
- Renforcer la libre circulation des données en contrepartie d'une responsabilisation des acteurs

Après négociation, le règlement général sur la protection des données est adopté le 27 avril 2016.

En 2017, le mot « données est maintenant sur toutes les lèvres. Les entreprises, les collectivités locales, toutes les organisations, cherchent à se transformer, en exploitant mieux et différemment les données qu'elles produisent, mais également en consommant des données qui viennent d'ailleurs : échangées avec des partenaires, vendues par des grossistes en données ou disponible en Open Data.

Dans ce contexte, la RGPD n'est pas une fatalité mais une réelle opportunité pour les organisations de conserver la confiance de leur client et de mieux les servir. Il est une source d'opportunité pour ceux qui savaient la maitriser ce qui leur donnaient et leur donnent toujours un avantage concurrentiel. La RGPD nous enjoint de respecter les citoyens, de ne plus les réduire à une suite de chiffre. Trop longtemps les entreprises ont considéré leurs clients, non pas comme des êtres humains, mais juste comme des data avec pour ultime data le numéro de carte de crédit.

Le 25 mai 2018, la RGPD rentre en vigueur.

I) Application de la loi

Pour qui et pourquoi

De par son application directe uniforme, le règlement impose aux Etats membres une application complète de tous les principes qu'il contient, sans possibilité de s'y soustraire en se retranchant derrière le droit national.

Le RGPD a pour effet une application harmonisée du cadre légal de protection des données personnelles par les organisations installées sur le territoire de l'UE mais pas seulement. Lorsque le responsable du traitement (ou un sous-traitant) n'est pas basé dans l'Union et entreprend le traitement de données personnelles liées à l'offre de biens ou de services ou à l'observation du comportement de résidents de l'union, le règlement trouvera à s'appliquer (définit par l'article 3).

Les lois vont donc s'appliquer aux grandes entreprises et multinationales ayant leur siège social hors UE. Nous pensons au cloud ou encore aux réseaux sociaux sur lesquels une grande partie de notre vie privée est dévoilée et utilisé à des fins commerciales.

Pourquoi on doit protéger nos données :

- Savoir qui a accès à nos données
- Savoir ce qu'on fait avec nos données
- Savoir à qui nos données peuvent être vendu, donné, échangé
- Savoir si nos données sont supprimées, actualisées… une fois celle-ci dépassé
- Pouvoir déterminer l'origine et le responsable de tout manquement à la loi

Est touché par le RGPD chaque entreprise ou organisation qui collecte des données personnelles mais il y a quelques exceptions (définit par l'article 2.2) :

- Dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union
- Par des Etats membres dans le cadre d'activités qui relèvent du champ d'application du chapitre 2 du titre V du traité sur l'Union européenne
- Par une personne physique dans le cadre d'une activité strictement personnelle ou domestique
- Par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces.

L’ambition de l’UE est bien de réussir à faire appliquer sa loi au plus grand nombre et met également des sanctions pour tout manquement.

Sanctions

En France, c’est la CNIL qui se charge du respect de la réglementation. En tant qu’autorité indépendante, elle ne reçoit aucune instruction des pouvoirs publics.

Ses rôles sont donc de :

- Informer et protéger
- Accompagner et conseiller
- Contrôler et sanctionner
- Anticiper

Que se passe-t-il en cas de manquement aux règles ?

Tout d’abord, en cas de manquement, les retombées en termes d’image peuvent être désastreuses. Or la réputation est un bien très précieux d’une entreprise et à l’ère d’internet ou les informations sont relayées en un temps record, le « bad buzz » peut avoir des répercussions néfastes sur l’activité de l’entreprise.

S’ajoute à ça des sanctions financière (définit par l’article 83 du RGPD).

A l’époque, l’amende maximal prononcé par la CNIL était de 150 000 euros pour Google, bien qu’important, se chiffre est très dérisoire par rapport au 41.6 milliard de dollar de chiffre d’affaires obtenue en 2016. Bien que la nouvelle eût fait parler d’elle, l’entreprise américaine n’avait pas beaucoup changé sa politique en matière de protections des données. C’est pourquoi, il est écrit dans le texte de la RGPD que l’amende doit être « effectives, proportionnées et dissuasives ».

Le plafond de l’amende est ainsi passé de 300 000euros à 3 millions pour les infractions qui ne concerne que la justice française et pas le RGPD

Pour le RGPD, tout manquement peut coûter :

- Un montant de 10 millions d’euros ou correspondant à 2% du chiffre d’affaires annuel mondial total pour une première série de violation. Il s’agit des manquements du responsable à l’analyse de l’impact, au registre des activités de traitement…

- Un montant de 20 millions d'euros u correspondant à 4% du chiffre d'affaires annuel mondial total pour une 2eme série de violation considérées comme grave par l'article 83.5 Ce sont notamment, les manquements aux principes de base d'un traitement.

Il peut également y avoir d'autre sanctions non pécuniaires si les manquements ne sont pas passible d'amende (article 84, dès lors, il pourra y avoir avertissement, rappel à l'ordre, différentes injonctions (prévu par l'article 58).

Pour exemple, Facebook a été condamné en Espagne à une amende de 1.2millions d'euros pour avoir exploités des données personnelles sans consentement.

II) Quoi et qui joue un rôle

Les données personnelles

L'UE donne une définition d'une donnée personnelle dans avec le RGPD n'2016/679, 4 ,1 :

« Constitue une donnée à caractère personnel, toute information se rapportant à une personne physique identifié ou identifiable ; est réputée être une personne physique identifiable une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

On peut tirer quelques observations de cette définition. Les données personnelles ne concernent que des personnes physiques. En conséquence, les personnes morales ne sont pas concernées par le RGPD. Attention, le nom et prénom d'un chef d'entreprise va être concerné par le RGPD.

Le caractère personnel d'une donnée est lié à son pouvoir d'identification. Qu'il soit direct si cette donnée à elle seul peut identifier la personne ou indirect si on peut déduire l'identité d'une personne (numéro de carte d'étudiant).

L'utilisation du mot « notamment » indique que la liste énumérée dans l'article n'est pas exhaustive. On peut par exemple, rajouté le format de la donnée (vidéo, photo…)

Le saviez-vous ? La Cour de Justice de l'UE ainsi que la Cour de cassation ont tous les 2 été d'accord sur le fait qu'une adresse IP est bien une donnée à caractère personnel.

Pour contourner le côté identifiant d'une donnée et par conséquent qu'elle ne soit plus soumise au lois RGPD, il est possible de soit les anonymiser ou de les pseudonomyser.

L'anonymisation est un traitement de données à caractère personnel dont le but consiste à empêcher irréversiblement l'identification de la personne concernée. Il n'existe dès lors aucun moyen de remonter jusqu'à la personne concernée. Cette information devenue « neutre » pourra alors être traité comme n'importe qu'elle autre information. Il est cependant difficile en pratique de créer un ensemble de données véritablement anonymes et qu'elles soient toujours exploitables dans une tâche déterminée. C'est la raison pour laquelle de nombreux acteur optent pour la pseudonomysation.

La pseudonomysation est un traitement de données qui consiste à remplacer un identifiant par un pseudonyme. Il est possible d'effectuer une opération de réversibilité. La donnée « pseudonymisée » est toujours donc à caractère personnel. Cependant les risques pour la personne concernée en cas de fuite sont moindres ce qui fait que la pseudonymisation est une mesure de sécurité efficace.

Le RGPD interdisent toutefois le traitement de certaines données considérées comme sensibles ce sont :

- Les origines raciales ou ethnique
- L'orientation sexuelle
- Les convictions religieuses ou philosophiques
- Les opinions politiques
- Les opinions syndicales
- L'état de santé
- Données biométriques
- Données génétiques
- Les condamnations pénales et infractions

Les acteurs

Ces données peuvent faire l'objet de traitement que sous certaines conditions définit par l'article 9.2 du RGPD. Avec l'intérêt grandissant pour la génétique et la biométrie, le règlement laisse aux Etats membres la possibilité de maintenir ou d'introduire des conditions supplémentaires.

Le RGPD définit un traitement dans l'article 4.2, d'une manière générale, un traitement peut concerner toutes interactions faites avec des données à caractère personnel, ayant n'importe qu'elle forme.

La RGPD va mettre à jour 3 acteurs dans le traitement des données : le responsable de traitement qui va déterminer les finalités et les moyens du traitement, les sous-traitant qui va traiter les données pour le compte du responsable de traitement et enfin la personne concernée dont les données personnelles sont traitées.

Le responsable de traitement est défini dans l'article 4.7 du RGPD. Il peut être physique ou morale, par exemple une collectivité territoriale, une banque, une entreprise de vente de vêtement…

La RGPD privilégie « l'autocontrôle », ainsi, c'est le responsable qui devra démontrer qu'il suit la RGPD (définit dans l'article 5.2). Il doit mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément à la réglementation (article 24). Afin d'apporter la preuve, elle peut appliquer un code de conduite (article 40) ou des certifications (article 42). Si dans un traitement, il y a plusieurs responsables de traitement, ils devront se mettre d'accord sur le partage de responsabilité (article 26).

Le RGPD à fait se rapprocher les responsables de traitement et les sous-traitant. Il y a une volonté de responsabiliser le sous-traitant en alignant son régime sur celui du responsable de traitement. Le sous-traitant doit jouer un rôle de conseil voire d'un assistant auprès du responsable. En pratique, le responsable de traitement imposera au sous-traitant le respect d'obligation similaires à celles auxquelles il est lui-même soumis. Si un sous-traitant veut faire sous-traiter des informations dans son domaines, il devra faire la demande écrite au responsable de traitement initiaux (article 28).

Comment traiter les données ?

D'après la RGPD, les données licéité, c'est-à-dire que mes données doivent être traité de manière licite, loyale et transparente au regard des personnes concernée. La licéité des données conditionne à elle seule le déclenchement de tout le processus juridique venant encadrer spécifiquement le traitement. Il y a un chemin logique à suivre, de la conception à la réalisation. On peut distinguer 6 étapes :

- Définir les finalités du traitement
- Contrôler la qualité des données
- Déclarer le traitement
- Informer les personnes et obtenir leur consentement
- Assurer l'exercice des droits de la personne concernée
- Assurer la sécurité et encadrer le transfert hors UE s'il a lieu

a) Les finalités du traitement

L'analyse de la finalité des traitements repose sur le fait que chaque traitement de données à caractère personnel doit avoir une finalité déterminée, explicite et légitime (article 5, b).

Une fois les données collectées, il n'est plus possible, en principe, de les utiliser pour une raison différente de celle qui a été définis au départ.

Il y a cependant quelques exceptions comme les traitements à des fins de recherche scientifique ou historique ou à des fins statistiques…

Les quatre grands principes sont donc :

- La finalité doit être respecté
- La finalité doit être déterminée, légitime et explicite
- La finalité permet de déterminer la pertinence des données recueillies
- La finalité permet de fixer la durée de conservation des données

b) La qualité des données

La qualité des données à caractère personnel est mesurée par trois grands principes : la minimisation, l'exactitude et la mise à jour des données collectées. Les métiers travaillant avec les datas le savent bien, une base de données n'est économiquement exploitable que si elle est régulièrement mise à jour. Dans ce cas les données conservent voire gagnent en valeur en ayant un outil concurrentiel plus développé.

Le principe de minimisation des données (article 5) est apparu lors de la mise en place de la RGPD même s'il fait écho au principe de nécessité (loi informatique et libertés, 1978, article 6). Pour respecter ce principe, les données collectées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités.

Il conviendra donc au responsable de traitement d'identifier les données strictement nécessaires à la finalité du traitement, d'éviter toute collecte supplémentaire, limiter l'envoi des documents électroniques contenant des données aux seules personnes habilitées et d'utiliser un outil d'effacement sécurisé.

En ce qui concerne la durée de conservation, les données ne peuvent être conservées :

- Pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées
- Pendant des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins statistiques, à des fins archivistes dans l'intérêt public, à des fins de recherche scientifique ou historique (article 5, 1, e)
- Dans le cas d'un archivage définitif des données autorisé par la loi, il est primordial d'anonymiser les données ou tout du moins, les pseudonymiser. Celui-ci doit être sélectif, limité dans le temps et sécurisé.

c) Déclaration

Avec la RGPD, les déclarations ou été simplifié mais certaines subsistent encore comme celle de désigner et de déclarer un PDO (responsable européen), le transfert des données hors UE ou de déclarer certains fichiers comme ceux du secteur de la santé.

Le formulaire à remplir auprès de la CNIL devra détailler le traitement et ses modalités :

- Indentification du responsable
- Finalité
- Données personnelles collectées
- Destinataires des données
- Service interne en charge des droits des personnes dont les données sont collectées
- Transfert des données hors UE
- Niveau de sécurité pour chaque traitement

d) Informer les personnes

L'information délivrée et le recueil du consentement doivent être réalisés de façon claire, intelligible et accessible afin qu'il n'y ait plus aucun doute possible sur le sort des données que la personne concernée confie à l'entreprise. L'information « brute » n'est donc pas suffisante pour la licéité du traitement. Le principe de transparence (article 12) impose que toute information et communication relative au traitement de données à caractère personnel soit aisément accessible, facile à comprendre et formulée en des termes clairs et simples. Il peut être effectuée sous formes écrite, orale ou électronique.

Il faudra soumettre aux personnes dont on collecte les données :

- Nom et coordonnées (Responsable de traitement, sous-traitant, DPO)
- Information sur le traitement (finalité du traitement, durée de conservation…)
- Information sur les droits de la personne
- Information sur le transfert hors UE

En cas de manquement, le responsable du traitement sera sanctionné pénalement (code pénal, article 625-10)

Dans le cas d'une collecte auprès de la personne concernée, ces informations doivent lui être transmises au moment où les données sont obtenues. Lorsqu'elle est faite auprès d'un tiers, la communication doit se faire dans un délai d'un mois maximum après la collecte.

La RGPD introduit également la notion de consentement (article 4, 11), celui-ci doit être libre, spécifique, éclairé et univoque. Ainsi une personne aura manifesté son consentement lorsqu'après avoir été informée du traitement, elle donne son accord par un acte positif clair (cons 32). Un silence ou une inactivité n'est donc pas un consentement

e) Les droits

La loi informatique et libertés avait déjà prévu des droits pour les citoyens sur leur données personnelles. Le RGPD a renforcé et introduit de nouveau droit.

e.1) Les droits déjà existant

Le droit d'information : Les articles 13 et 14 renforcent nettement le droit à l'information en imposant au responsable de traitement la communication de toute une série de mentions.

Le droit d'accès : La personne concernée a le droit d'obtenir que ses données à caractère personnelles ne soient pas ou sont traitées (article 15) et si elles le sont, de se voir communiquer toutes les informations précitées (finalité, catégorie des données…). Mais se droit n'est pas absolue et le responsable peut s'y opposer.

Le droit d'opposition : la personne concernée peut s'opposer à tout moment à un traitement de données à caractère personnel la concernant. Cependant un motif légitime devra être avancé pour qui souhaite prévaloir ce droit. Le responsable de traitement ne pourra plus traiter à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux (article 21).

Le droit de rectification : La personne concernée a le droit d'obtenir la rectification des données personnelles la concernant qui sont inexactes. Elle a également le droit d'obtenir que les données incomplètes soient complétées y compris en fournissant une déclaration complémentaire (article 16).

Le droit à la mort numérique : Bien qu'il ne soit pas repris par le RGPD, ce droit reste inscrit dans la législation française et devra être respecté (Loi informatique et libertés, article 40.II). Ce droit permet à toute personne de laisser des directives générales ou particulièrement sur le sort de ses données après son décès.

e.2) Les nouveaux droit

Le droit à la limitation : La personne concernée a le droit d'obtenir du responsable du traitement qu'il « limite » celui-ci (article 18). Cette limitation est définie comme étant le marquage de données personnelles conservées mais dont le traitement futur sera interdit (article 4.3). Seule

la conservation des données est alors possible sans qu'aucun autre traitement ne puisse être effectué (cons 67).

Le droit au non-profilage : La RGPD définit le profilage comme toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique (article 4.4). Le règlement n'interdit pas le profilage mais l'encadre en prévoyant des garanties pour les personnes concernées par ce type de traitement. Ainsi, la personne doit être informé d'un profilage, sur l'importance et les conséquences de ce traitement (article 13). Cela permet à ce qu'on ne traite pas les données d'une personne sans que l'intéressé présente ses observations. Il existe qu'elle exception prévue par l'article 22.

Le droit à la portabilité des données : Ce droit permet à une personne de récupérer les données qu'elle a fournis sous une forme aisément réutilisable ou que le responsable de traitement transfert directement ses données à un tier choisi lorsque cela est techniquement faisable (article 20). A noter que le droit de la portabilité était déjà appliqué dans le cas du BtoC (Code de la consommation article L224-42-1).

Le droit à l'effacement (article 17) : Il comprend le droit au déréférencement des données personnelles indexées par un moteur de recherche. Un droit à l'effacement des données après X années (cons 87). Ce droit n'est pas absolu mais sa mise en œuvre reposera sur le responsable de traitement qui devra faire attention aux exceptions.

f) Les flux hors UE

Une entreprise ne peut pas transférer des données à caractère personnel vers un Etat tiers situé hors UE. Des dérogations existent lorsque l'Etat tiers assure un niveau de protection suffisant en matière de protection des données.

Deux types de transferts sont donc possibles :

- Des transferts fondés sur une décision d'adéquation de la Commission européenne (article 45) qui reconnait que le pays destinataire dispose d'un niveau de protection adapté.
- Des transferts fondés sur des garanties appropriées (article 46)

Le but est d'assurer aux citoyens, un niveau de protection a minima équivalent à celui du RGPD lorsque leurs données sont traitées dans des pays autres.

En pratique

Au cours des dernières années, le nombre de cyber attaques est en perpétuelle augmentation avec comme objectif principale de voler les données des entreprises ciblées ainsi que les données de leurs clients. En effet ces entreprises récoltent de plus en plus de données sur leurs clients afin d'améliorer leur compétitivité, leurs performances et donc leurs revenus. Bien que cette pratique ne soit pas néfaste en soit, car celle-ci permet de proposer un service toujours plus adapté et personnalisé pour leurs clients, ces entreprises peuvent mettre en dangers les données personnelles de leur clientèle.

En 2022, dans son rapport annuel du 11 Mai 2022, la CNIL annonce une augmentation du nombre de notifications de violations de données personnelles de plus de 79 % par rapport à 2020. Ce chiffre peut s'expliquer par la crise sanitaire qui a poussé des entreprises, non préparés à cette éventualité ou pas assez, à recourir au télétravail pour maintenir leur activité.

Selon le baromètre de la CESIN (Club des Experts de la Sécurité de l'Information et du Numérique), en 2022, plus d'une entreprise sur deux à été victime de cybercriminalité. La plupart de ces attaques ayant pour but de mettre en place un rançongiciel : Un rançongiciel ou logiciel d'extorsion est un logiciel malveillant qui prend en otages toutes les données auquel il a pu avoir accès. On peut noter également que ces attaques se concentrent généralement sur les entreprises de petites tailles car généralement moins bien préparés et moins sécurisés. Ces petites entreprises représentent un point d'accès idéal pour attaquer de plus grosses entreprises partenaires de celles-ci.

En plus de mettre en danger nos informations personnelles, une entreprise qui subit une cyber-attaque peut perdre beaucoup. En effet les pertes moyennes d'une attaque provoquant l'interruption de l'activité de l'entreprise, s'estime à 27% de leur chiffre d'affaires mensuel. De plus, 60% des PME attaquées déposent le bilan dans les 18 mois suivant l'attaque. Une attaque peut également provoquer une détérioration du matériel informatique impliquant des coûts pour remettre le système d'information en Etat, elle impacte également sur l'image publique de la société qui entraînera inévitablement une forte perte de clientèle et cette attaque pourra également entrainés des fuites de données. C'est pour cela que de plus en plus d'entreprises ont commencé à payer les rançons exigées par les cybercriminelles, estimant que l'interruption d'activité est plus nocive pour leur entreprise même si le rapport du spécialiste en sécurité Sophos prévient que peu de ses entreprises récupèrent intégralement leur donnée après paiement de cette rançon (8%)

La gravité des chiffres relatifs aux cyberattaques en France rend impensable pour les entreprises de ne pas investir dans leur système d'information afin de garantir l'intégrité, la disponibilité et la confidentialité de leur organisation face à des attaques. Elles doivent également rester à jour dans leur procédures et code de conduites afin de satisfaire les exigences légales Françaises et Européennes.

I / Facteur Humain

Afin de maintenir l'intégrité d'un système d'Information, une entreprise doit passer en premier temps dans l'étape la plus importante de la sécurisation d'un SI même si le risque zéro n'existe pas en informatique, des mesures nécessaires limitent les risques. Mettre en plan un en matière de cybersécurité et cela commence par sensibiliser les employés travaillant pour cette entreprise quel que soit leur poste. En effet, la principale menace, devant l'exploitation de failles de sécurité, est le phishing ou hameçonnage en français : est la technique la plus utilisé par les cybercriminelles pour obtenir des renseignements permettant l'usurpation d'identité ou permettant d'amorcer une attaque visant à voler des données. Le phishing s'exprime le plus souvent sous le format de courriers électroniques ou de faux sites.

Il faut donc former ses employés aux bonnes pratiques en matière de cybersécurité mais une erreur humaine n'est jamais à l'abri d'arriver. C'est pour cela que la société doit mettre en place une politique sur l'utilisation d'Internet et des réseaux sociaux dans l'entreprise. Elle doit également mettre en place des directives claires avec des restrictions sur les types de sites web disponible aux employés, les logiciels qu'ils ont la possibilité de télécharger et les obliger d'utiliser des mots de passes robuste. Toutes ces directives peuvent aisément s'appliquer dans le cadre de postes professionnels cependant dans le cadre du télétravail, là où le personnel et le professionnel se mélange, celle-ci sont plus difficiles à faire respecter. En effet près de la moitié (47%) des télétravailleurs se sont déjà fait piéger par des tentatives de phishing lorsque ceux-ci travailler depuis leur domicile.

Ces tentatives réussissent malgré la mise en place de plus en plus fréquente de solutions applicatives utilisés par les SI pour protéger leurs employés en mettant en place des filtres et des analyses sur les mails reçus extérieurs à l'entreprise. En effet le social Engineering (une pratique de manipulation psychologique à des fins d'escroqueries) de ces attaques est toujours de plus en plus sophistiqué et l'utilisation d'informations volés à des partenaires peut rendre ce type d'attaque très dur à totalement éradiqué.

Une autre menace, d'ordre humaine, non négligeable se trouve dans l'introduction de matériels informatiques extérieurs à l'entreprise sur son réseau interne. En effet, l'insertion d'un périphérique vérolé comme une clé USB ou un autre appareil sur le réseau peut servir de porte d'accès direct au serveur de l'entreprise sans passer par les sécurités mises en place contre les attaques externes. Le service informatique doit donc être capable de restreindre l'utilisation de périphériques externes et de contrôler l'accès des nouveaux appareils sur le réseau en toute sécurité. Il est également recommandé de mettre à disposition un réseau externe pour les personnes extérieurs à l'entreprise venant temporairement en son sein.

Assurer la pérennité de l'entreprise passe également à travers la sauvegarde de ses données sur des éléments extérieurs au réseau et la segmentation du réseau pour limiter les potentiels dégâts causés par une attaque.

II/ L'application du RGPD

a) Mise en place

Après cette première phase importante dans la sécurisation de l'entreprise et donc par extension des données qu'elle pourrait stocker. Pour être conforme avec les règles établies dans la RGPD ou la loi française, une entreprise doit respecter de nombreuses conditions et bonnes pratiques afin de pouvoir démontrer la bonne application de ses règles. Pour cela il faut appliquer 6 étapes comme défini par la CNIL :

> *Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.*
>
> **Article 121 de la loi Informatique et Libertés**

- **Désigner un pilote :** Une personne faisant le rôle de référent sur les questions relatives à la protection des données relatives. Celui-ci a pour rôle de conseiller et contrôler le respect du règlement. Il a également le devoir de rester à jour sur les nouvelles obligations. Il a pour rôle de sensibiliser l'entreprise sur l'effet de ces nouvelles obligations.

- **Cartographier :** Le pilote doit établir un registre précis sur les traitements sur les données effectués dans l'entreprise afin de les catégoriser en fonctions de leurs finalités, les acteurs qui les manipulent, l'origine et destination des flux ainsi que leur stockage et la durée de conservation. Ce registre est prévu par l'article 30 du RGPD, il participe à la documentation de la conformité de l'entreprise au règle RGPD.

  Dans la pratique, la CNIL recommande de tenir 2 registres : un pour les traitements de données dont l'entreprise est responsable et un autre pour les traitements que vous opérez en tant que sous-traitant pour le compte de vos clients.
  Il faut également vérifier que dans les pays dans lesquels l'entreprise transfère ces données, que ceux-ci soient reconnus adéquat par la Commission Européenne. Le pilote doit être capable de mesurer l'impact du règlement sur ces données.

- **Prioriser les actions à mener :** Au regard du registre préalablement établi, prioritiser des actions afin d'anticiper les futures obligations pour rester en avance sur le règlement européen notamment en révisant les mentions d'information ou en identifiant la base juridique sur laquelle se fonde les traitements.
  Il est également important de s'assurer que sont seulement les données strictement nécessaires qui sont collectés et que le droit des personnes comme le droit d'accès ou de rectification peut s'appliquer sur la gestion de vos données.

- **Gérer les risques :** Si lors de ces contrôles, le pilote a identifié des traitements de données personnelles susceptibles d'engendrer des risques, celui-ci doit effectuer pour chaque traitement une analyse d'impact relative à la protection des données (AIPD). Cette analyse est un outil d'évaluation d'impact sur la vie privée, elle est obligatoire selon l'article 35 du RGPD et doit être réalisé s'il rencontre au moins 2 des 9 critères établis par le G29 :

  1. Evaluation ou notation;
  2. Décision automatisée avec effet juridique ou effet similaire significatif;
  3. Surveillance systématique ;
  4. Données sensibles ou données à caractère hautement personnel ;
  5. Données personnelles traitées à grande échelle ;
  6. Croisement d'ensembles de données ;
  7. Données concernant des personnes vulnérables ;
  8. Usage innovant ou application de nouvelles solutions technologiques ou organisationnelles ;
  9. Exclusion du bénéfice d'un droit, d'un service ou contrat.

- **Organiser les processus internes :** Mise en place de procédures internes afin d'assurer la protection des données à tout moment et face à tous types d'évènements au cours de la vie d'un traitement comme une faille de sécurité, modification des données, changement de prestataire etc… Anticiper les violations de données en prévoyant la notification à l'autorité de protection des données

- **Documenter :** La documentation doit être regrouper, tenu à jour et réalisé à chaque étape pour prouver la conformité de l'entreprise. Cette documentation se compose de :

    - Registre des traitements
    - Analyses AIPD
    - Encadrement des transferts de données
    - Les mentions d'informations
    - Les modèles de recueil du consentement des personnes concernées ainsi que la preuve de leur consentement.
    - Les procédures mises en place pour l'exercice des droits ainsi que les procédures internes.
    - Les contrats avec les sous-traitants

Pour assurer la sécurité du service d'information de l'entreprise, il est également primordial de tenir rigoureusement à jour les procédures pour chaque activité et chaque utilisation des applications dans l'entreprise. Cette documentation permet de trouver rapidement d'éventuels failles de sécurité ou d'éviter de perdre du temps lorsqu'un problème apparaît dans la chaîne d'instructions. Cette documentation permet également de faciliter les audits en sécurité que pourrait faire l'entreprise.

b) Sous-Traitance

Comme évoqué précédemment, de nombreux cybercriminels préfèrent attaquer des TPE / PME en premier lieu dû à leur lacune en sécurité qui pourrait être des sous-traitants et ainsi faire une attaque par rebond (constitue une famille d'attaques de système d'information qui consistent à utiliser un ou des systèmes intermédiaires, participant à leur insu, et permettant à un assaillant de rester cacher) sur l'entreprise qui sous-traite. C'est pour cela qu'il est également important d'établir des clauses dans la relation traitement / sous-traitement.

En effet, les sous-traitants doivent également respecter le RGPD et être encadrés par un contrat avec le responsable de traitement. Dans le cadre de cette relation, l'article 28 du RGPD prévoit une série de dispositions relatives à la mise en place d'un contrat spécifique entre les parties afin de définir exactement l'utilisation que le sous-traitant peut faire des données fournies, pendant combien de temps, dans quel contexte et leur responsabilité. Ce contrat a pour but de garantir la sécurité des données collectées, d'assurer la réponse aux demandes d'exercices des droits des personnes et en cas de violation de donnée, le sous-traitant doit également aider le responsable de traitement à remplir ses obligations de notification à la CNIL.

c) Conservation des données personnelles

Les données personnelles ne peuvent être conservées indéfiniment : une durée de conservation doit être déterminée par le responsable de traitement en fonction de la finalité ayant la collecte de ces données. Il est important de définir la durée au préalable selon des référentiels lors de la collecte de la donnée et d'en informer clairement l'individu. C'est ainsi que le RGPD parle de cycle de vie de la donnée personnelle. Ce cycle contient 3 phases :

1) Conservation en base active : durée nécessaire à la réalisation de la finalité du traitement, ces données sont accessibles dans l'environnement de travail immédiat pour les services opérationnels qui ont la charge de ce traitement.
2) Archivage Intermédiaire : Le données personnelles ne sont plus utilisés pour la réalisation de la finalité du traitement mais présentent encore un intérêt administratif pour l'entreprise ou pour répondre à une obligation légale de traitement. Ces données peuvent être consultées de manière ponctuelle et motivée par des personnes spécifiquement habilitées.
3) Archivage Définitif : En raison de leur valeur et intérêt, certaines informations sont archivées de manière définitive et pérenne

d) Consentement

RGPD :

« *Toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* »

Comme indiqué précédemment, pour être conforme aux réglementations du RGPD, l'entreprise doit pouvoir fournir les preuves du consentement des individus concernées. Pour cela, le consentement doit tout d'abord être :

- Libre de toute contrainte ou influence,
- Spécifique à un traitement dont la finalité a été déterminé,
- Éclairé d'un certains nombres d'informations concernant :
    - L'identité du responsable du traitement ;
    - Les finalités poursuivies ;
    - Les catégories de données collectées ;
    - L'existence d'un droit de retrait du consentement ;
    - Objet d'un transfert hors UE.
- Univoque : aucune ambigüité

Bibliographie

- Livre (Le RGPD expliqué à mon boss, Gérard Haas, Editions Kawa – 2017)
- Livre (Cybersécurité et Cyberdéfense : Enjeux Stratégiques, Yann Salamon, ELLIPSES – 2020)
- Site ANNSI
- Site CNIL
- Site CESIN
- Podcast (Le hacking au XXIe siècle ? Zax et Doomer – Thinkeriew – 2021)