VEILLE JURIDIQUE

Le RGPD

SOMMAIRE

1. Contexte et Enjeux

Aujourd'hui, les données personnelles sont très précieuses sur Internet. Chaque action en ligne laisse des traces que les entreprises récupèrent et analysent.
Cependant, cette collecte massive a posé de gros problèmes pour la vie privée des gens.
Dans le milieu professionnel, et particulièrement pour une entreprise informatique comme Sopra Steria, gérer ces données n'est plus juste une question de stockage. C'est devenu une obligation légale majeure. Protéger les serveurs ne sert plus seulement à éviter les pirates, mais aussi à respecter la loi et protéger la vie privée des clients.

2. Le Cadre Légal : Des origines aux actualités récentes

2.1 Les principes de base

Le 25 mai 2018, l'Europe a mis en place le Règlement Général sur la Protection des Données (RGPD). Il impose des règles très strictes :

- **La sécurité dès le départ :** La protection des données doit être pensée avant même de créer un logiciel.
- **Prouver sa bonne foi :** L'entreprise doit pouvoir montrer à la CNIL qu'elle respecte bien la loi (en gardant des historiques clairs).
- **Le Droit à l'oubli :** Tout client peut demander à ce que ses informations soient totalement effacées.
- **Des sanctions fortes :** Les amendes peuvent être énormes (jusqu'à 4 % du chiffre d'affaires mondial) en cas de fuite de données.

2.2 Actualités récentes

Le monde de l'informatique évolue vite. Voici les sujets du moment concernant la loi et les ordinateurs :

Thème d'actualité	Ce qu'il se passe aujourd'hui
L'Intelligence Artificielle (IA)	Avec des outils comme ChatGPT, les employés copient parfois des informations de l'entreprise par erreur. L'Europe vient de voter une loi (l'AI Act) pour contrôler ces outils et éviter les fuites.
Le Cloud américain	Envoyer des données européennes sur des serveurs aux États-Unis est toujours compliqué. Un nouvel accord a été signé récemment pour faciliter cela, mais il reste très surveillé.
Surveillance des employés	La CNIL donne de grosses amendes aux entreprises qui utilisent l'informatique pour trop surveiller le travail de leurs salariés (comme l'affaire Amazon France).

3. Problématique Opérationnelle : Le cas Chorus Pro

Chez Sopra Steria, je travaille au support technique de Chorus Pro, le site qui gère les factures de l'État.
Mes collègues et moi voyons tous les jours des informations très sensibles : coordonnées bancaires (RIB), noms des patrons, adresses email et historiques de connexion.
La question est donc la suivante :
"Comment une entreprise comme Sopra Steria peut-elle protéger ces données pour respecter la loi, sans bloquer ou ralentir le travail de ses techniciens ?"

4. Impacts et Solutions pour le service informatique

Pour respecter la loi, le service informatique doit mettre en place des règles humaines et des blocages techniques.

Règles de travail (Humain)	Outils de sécurité (Technique)
Le responsable des données (DPO) : Il vérifie que les techniciens ne demandent pas d'informations inutiles aux clients.	**Limiter les accès :** Un technicien du support ne doit avoir accès qu'à ce qu'il lui faut pour dépanner, sans pouvoir fouiller dans les autres dossiers.
Le registre : Un cahier de bord obligatoire qui explique pourquoi on garde chaque donnée (par exemple, garder les logs pendant un an pour la sécurité).	**Suppression automatique :** Des petits programmes qui effacent tout seuls les anciens historiques quand le délai légal est dépassé.
Sensibilisation : Interdire aux collègues de s'envoyer des vrais fichiers clients par email pour résoudre un problème.	**Protection du matériel :** Obligation de chiffrer les disques durs des ordinateurs portables. Si un PC est volé, personne ne peut lire ce qu'il y a dessus.

5. La Synergie : RGPD et Architecture Zero Trust

La loi (le RGPD) donne les règles, et le Zero Trust (mon autre sujet de veille) donne les outils pour les respecter.

- **La sécurité informatique obligatoire :** La loi demande de bien protéger les ordinateurs. Le Zero Trust le fait en bloquant automatiquement un employé si son antivirus n'est pas allumé.
- **Ne voir que l'essentiel :** La loi demande de ne pas accéder à tout. Le Zero Trust découpe le réseau pour que le technicien ne voie que l'application dont il a besoin.
- **Garder des preuves :** La loi exige de pouvoir prouver qui a fait quoi. Le Zero Trust enregistre parfaitement chaque connexion de manière claire.

6. Contraintes et Défis pour les informaticiens

Même si la loi est bonne pour les citoyens, elle donne beaucoup de travail aux informaticiens :

- **Le droit à l'oubli est compliqué à programmer :** Supprimer totalement un client de tous les serveurs et sauvegardes sans casser le fonctionnement de la base de données est très dur techniquement.
- **Les anciens logiciels :** Beaucoup de vieilles applications d'entreprise ne savent pas

supprimer les données automatiquement et coûtent cher à modifier.
- **Beaucoup de papiers à remplir :** Lancer un nouveau serveur prend plus de temps car il faut d'abord faire valider des dossiers de sécurité par des juristes.

7. Conclusion Générale

Il est essentiel de continuer à bien protéger les données. Pour une entreprise, les amendes de la CNIL coûtent trop cher. Surtout, quand on gère les factures de l'État comme avec Chorus Pro, respecter la loi permet de garder la confiance de tout le monde. Si une fuite arrivait, la réputation de l'entreprise serait détruite.
Aujourd'hui, faire de l'informatique, c'est aussi faire du droit. La loi oblige les informaticiens à travailler plus proprement (mieux ranger les serveurs, effacer les vieux fichiers, bloquer les accès inutiles). Au final, ces règles nous aident à rendre nos réseaux beaucoup plus solides contre les attaques des pirates.

8. Annexes

Méthodologie de recherche

- **Suivi de l'actualité :** Utilisation d'outils comme Feedly pour recevoir automatiquement les nouveaux articles sur la loi et l'informatique.
- **Alertes :** Mots-clés surveillés sur Google ("Amendes RGPD", "IA", etc.).
- **Terrain :** Observation de mon travail quotidien au support technique de Sopra Steria.

Glossaire

- **RGPD :** Règlement Général sur la Protection des Données (la loi européenne).
- **CNIL :** Le gendarme français qui vérifie que les entreprises respectent la loi.
- **DPO :** La personne dans l'entreprise chargée de vérifier que les données sont bien protégées.

Sources

1. Site de la CNIL (cnil.fr) - Pour comprendre les règles et voir les sanctions.
2. Site de l'ANSSI - Pour les conseils de sécurité informatique du gouvernement.
3. Sites d'actualité comme ZDNet - Pour suivre l'évolution des lois sur l'Intelligence Artificielle.