Rencontres de la Cybersécurité à Pau (#RCyberPau)

Première édition

21 mars 2018 – Palais Beaumont – Pau

COMPTE RENDU

Avec le soutien de nos partenaires




OPENING SESSION

Nicolas PATRIARCHE, *Maire de Lons - Vice-président en charge du numérique, Agglomération Pau Béarn Pyrénées*
Michel BOURIOU, *Directeur de cabinet de Gilbert PAYET, Préfet des Pyrénées Atlantiques*
Didier LAPORTE, *Président, CCI Pau Béarn*
Guillaume POUPARD, *Directeur général, ANSSI*




Les acteurs, publics et privés, font face à différentes menaces issues du cyberespace, qui peuvent-être regroupées en trois grandes familles selon l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) : les cryptolockers, l'espionnage et la destruction des données ou des systèmes. Face à ces menaces, les 42 règles du *Guide d'hygiène informatique*[1] publié par l'Agence, forment le socle minimum à respecter pour protéger les informations de toute organisation et éviter, pour les professionnels comme pour les particuliers, ces différentes formes d'attaque. L'émergence de nouvelles propositions de type *Crime-as-a-service* dans le Darknet est par ailleurs significatif d'une évolution et d'une professionnalisation du phénomène de la cybercriminalité : les réseaux criminels se structurent. Des personnes mal intentionnées peuvent ainsi acheter certains services à des prix réduits pour des actes de cybermalveillance. Le coût de la cybercriminalité conduit aujourd'hui à une prise en compte de l'importance de développer une véritable culture de cybersécurité.

> « ***La problématique est de toucher et de sensibiliser des acteurs locaux souvent non acculturés à ces thèmes sécuritaires dans les process de transformation numérique*** ».
> **Bénédicte PILLIET**, *Directrice, CyberCercle*

En 2017 en France, 5 300 plaintes liées à la cybercriminalité ont été déposées, un chiffre en augmentation de 32% par rapport à l'année 2016. Pour autant, ce chiffre semble très faible au regard des proportions connues du phénomène qu'est la cybercriminalité : les autorités invitent ainsi toutes les organisations victimes d'actes de cybermalveillance à le signaler et à porter plainte de manière systématique, avec pour objectif d'établir un véritable état de la situation et de mettre en place des indicateurs pertinents de la situation de la cybersécurité en France. La cybercriminalité est une menace pour toutes les structures, et aucune n'est à l'abri. La nécessité de se protéger s'applique à l'ensemble des organisations, privées comme publiques, et doit passer en particulier par la formation de l'ensemble des citoyens aux enjeux de cybersécurité.

> « ***Les collectivités territoriales ont pris la mesure des défis du numérique et des enjeux de la cybersécurité et se déploient dans ce sens*** ».
> **Nicolas PATRIARCHE**, *Maire de Lons - Vice-président en charge du numérique, Agglomération Pau Béarn Pyrénées*

L'un des grands acteurs en la matière sur les territoires est la Gendarmerie nationale. Pour lutter contre la cybercriminalité, elle adopte une approche transversale, suivant 3 axes : anticipation, prévention et répression. Le dispositif national de lutte contre la cybercriminalité repose sur le travail en cohérence de

[1] Disponible sur le site Internet de l'ANSSI : https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

l'ensemble du territoire, afin de protéger les collectivités, les entreprises ainsi que les particuliers.

> « ***La cybersécurité est une nécessité pour la protection des données des citoyens, des infrastructures et le développement des territoires par le numérique*** ».
> **Michel BOURIOU**, *Directeur de cabinet de Gilbert PAYET, Préfet des Pyrénées Atlantiques*

La cybersécurité est une affaire de gouvernance et de sensibilisation. C'est l'une des missions de l'ANSSI, via ses délégués territoriaux, que d'aider et d'accompagner les acteurs locaux dans l'élaboration et la mise en œuvre de bonnes pratiques en matière de sécurité numérique. De l'Etat jusqu'aux collectivités territoriales, la sécurité numérique implique collectivement l'ANSSI, les préfectures, les régions, les départements et l'ensemble des acteurs publics sur les territoires.

> « ***Opportunité ou contrainte, le RGPD est un atout pour les organisations et pour les territoires*** ».
> **Didier LAPORTE**, *Président, CCI Pau Béarn*

Les collectivités territoriales n'échappent pas en effet à ce phénomène de la cybercriminalité. Elles ont pris la mesure des défis du numérique et des enjeux de la cybersécurité. Dans cette dynamique, un syndicat mixte va être créé dans le département des Pyrénées-Atlantiques, avec pour mission de s'occuper de la sécurité des infrastructures ainsi que des données des usagers. La nécessité de protéger les données des citoyens, les infrastructures et le développement des territoires par le numérique entraîne les collectivités sur la voie de l'instauration d'une plus grande sécurité numérique.

> « ***La cybersécurité n'est pas une affaire strictement parisienne, mais est l'affaire de tous*** ».
> **Guillaume POUPARD**, *Directeur Général, Agence Nationale de Sécurité des Systèmes d'Information - ANSSI*

L'Union européenne s'est également saisie de ce sujet, et a renforcé le cadre réglementaire de la sécurité numérique en adoptant en 2016 la directive NIS et le RGPD. Les exigences imposées par ce cadre réglementaire peuvent rebuter au regard des coûts et des ressources nécessaires, mais des solutions existent pour les collectivités territoriales les plus modestes, à travers notamment la mutualisation des ressources. Opportunité ou contrainte, le RGPD est un atout pour les organisations et pour les territoires et nécessite de sensibiliser et former l'ensemble des échelons de la hiérarchie, et en premier lieu les dirigeants et les décideurs.

TABLE RONDE

RGPD, NIS : LES ENJEUX DE LA REGLEMENTATION EUROPEENNE POUR LES ACTEURS PUBLICS ET PRIVES DES TERRITOIRES

Guy FLAMENT, *Délégué territorial Nouvelle-Aquitaine, ANSSI*
François COUPEZ, *Avocat associé, Cofondateur, ATIPIC Avocat*

> « ***Le RGPD permet de se poser en amont de toute opération les questions essentielles que la collecte et le traitement de données à caractère personnel soulèvent, de déterminer quelles sont les données devant nécessairement être collectées, la manière de cibler ces données ou encore la durée de leur conservation*** ».
> ***Guy FLAMENT***, *Délégué territorial Nouvelle-Aquitaine, ANSSI*

Le RGPD comporte deux révolutions majeures.
L'extraterritorialité, qui rend les obligations réglementaires applicables à toute entreprise traitant des données personnelles de citoyens européens, que cette entreprise soit européenne ou non ;
La coresponsabilité, astreignant les sous-traitants aux mêmes règles et devoirs auxquels le responsable du traitement est astreint, la chaîne des acteurs impliqués au cours du processus de collecte jusqu'au traitement étant conjointement responsables en cas de manquement aux obligations réglementaires.
Le RGPD est une véritable révolution copernicienne en matière de traitement des données, en remettant notamment le pouvoir entre les mains des citoyens et des consommateurs : c'est par exemple le cas avec le droit à la portabilité de ses données. La conformité au RGPD n'est pas un handicap mais une nécessité et un élément de compétitivité, qui est un prérequis pour une ouverture à l'international dans certains pays. C'est par exemple le cas de l'Allemagne.

Cette nouvelle réglementation européenne met en place un certain nombre d'obligations, dans le but de responsabiliser les acteurs, à travers notamment des obligations de moyens, parmi lesquelles la mise en place d'une politique de sécurité interne ainsi que la nomination d'un Délégué à la protection des données (DPD, ou *Data Protection Officer – DPO*). La politique de sécurité et de confidentialité deviendra un élément supplémentaire pour montrer sa conformité au RGPD et un véritable atout face aux utilisateurs/clients. Le DPO, quant à lui, est un poste à part, créé par le RGPD et remplaçant le Correspondant Informatique et Libertés (CIL), et ne pourra pas être cumulé avec un autre poste dans la structure. Le DPO ne peut par exemple pas être Responsable de la Sécurité des Systèmes d'Information (RSSI), du fait du risque important de conflit d'intérêt que cela entrainerait.

> « ***Le cumul de poste avec la fonction de DPO n'est pas une bonne idée. Le profil parfait serait un ancien directeur Marketing, ayant ainsi une expérience opérationnelle pour savoir « quelles données sont collectées et nécessaires », ce qui facilitera sa mission de DPO qui est de savoir « qui gère quelles données au nom de qui »*** ».
> **François COUPEZ**, *Avocat associé, Cofondateur, ATIPIC Avocat*

Après la loi votée le 26 février 2018 transposant en droit interne la directive européenne NIS relative à la Sécurité des Réseaux et de l'Information, la France doit maintenant arrêter la liste des OSE avant le mois de Novembre 2018. Cette liste sera suivie d'un décret puis d'arrêtés sectoriels qui seront promulgués. Trois obligations s'appliqueront en vertu de la réglementation européenne aux Opérateurs de Services Essentiels (OSE) : une obligation de moyens, une obligation de détection ainsi qu'une obligation de signalement des incidents à l'ANSSI. Comme pour tous les projets de sécurité numérique, la réussite passe d'abord par la gouvernance et la prise de conscience

par chacun des responsabilités qui en découlent et lui incombent.

> « ***La mise en conformité au cadre réglementaire (directive NIS et RGPD) entraînera des coûts certains, mais les sanctions prévues en cas de non-conformité seront plus élevées que ces coûts cumulés*** ».
> **Guy FLAMENT**, *Délégué territorial Nouvelle-Aquitaine, ANSSI*

La date du 25 mai 2018 marque véritablement un tournant pour le traitement des données. Les sanctions prévues par le RGPD ne sont pas illusoires, la jurisprudence existant déjà : la CNIL a condamné en janvier 2018 Darty pour avoir « *manqué à son obligation de sécurité des données personnelles* » à une amende de 100 000 euros.

Le nouveau cadre réglementaire imposé par l'Union européenne, à travers la directive NIS et le RGPD, aura un impact sur l'ensemble des acteurs des territoires. Se pose aujourd'hui la question de l'accompagnement des acteurs dans leur démarche de mise en conformité réglementaire, et de la création de structures à même de mener à bien ces missions, notamment pour les PME-PMI ou les petites communes.

CLOSING SESSION

Angelina GROS TCHORBADJISKA, *Responsable de politiques, Secrétariat de la Task-Force pour l'Union de la Sécurité, DG Home, Commission européenne*

La lutte contre les cyberattaques et la lutte contre les Fake News se retrouvent dans plusieurs textes de loi au niveau français et européen : ils constituent les priorités de l'action de la Commission européenne en 2018 en matière de sécurité numérique, accompagnés d'un renforcement des investissements de R&D en matière de cybersécurité de la part de la Commission européenne en 2018.

Si le mois de novembre est la date limite pour désigner les OSE, une autre échéance toute aussi importante doit être prise en considération : la nécessité dans les mois et les années à venir de renforcer l'ENISA, dans ses missions et ses ressources, pour qu'elle devienne une véritable agence européenne de la cybersécurité à même de soutenir les Etats membres de l'UE de manière plus efficace et effective. C'est notamment l'objectif du *Cybersecurity Act* européen et de ses différents volets, qui vise à accroître la confiance des citoyens et des usagers dans le numérique et les institutions.

> « ***En matière de sécurité collective et plus particulièrement de sécurité numérique, la coopération internationale doit être une priorité pour les Etats membres de l'Union européenne*** ».
> **Angelina GROS TCHORBADJISKA**, *Responsable de politiques, Secrétariat de la Task-Force pour l'Union de la Sécurité, DG Home, Commission européenne*

QUATRE MESSAGES PRINCIPAUX A RETENIR

- Les 42 règles du *Guide d'hygiène informatique* publié par l'ANSSI, forment **le socle minimum à respecter pour protéger les informations de toute organisation**.
- Le RGPD comporte deux révolutions majeures : l'**extraterritorialité** et la **coresponsabilité.**
- **La conformité au RGPD et à la directive NIS n'est pas un handicap mais une nécessité et un élément de compétitivité**.
- **La mutualisation des moyens et des ressources** est un axe à travailler pour les structures de taille modeste

cybercercle.com

@CyberCercle

CyberCercle

CyberCercle

contact@cybercercle.com