Sujet élaboré par une cellule pédagogique nationale

CONCOURS EXTERNE D'ATTACHÉ TERRITORIAL

SESSION 2018

ÉPREUVE DE NOTE

ÉPREUVE D'ADMISSIBILITÉ :

Rédaction d'une note ayant pour objet de vérifier l'aptitude à l'analyse d'un dossier portant sur la conception et la mise en place d'une application automatisée dans une collectivité territoriale.

Durée : 4 heures
Coefficient : 4

SPÉCIALITÉ : ANALYSTE

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni initiales, ni votre numéro de convocation, ni le nom de votre collectivité employeur, de la commune où vous résidez ou du lieu de la salle d'examen où vous composez, ni nom de collectivité fictif non indiqué dans le sujet, ni signature ou paraphe.
- Sauf consignes particulières figurant dans le sujet, vous devez impérativement utiliser une seule et même couleur non effaçable pour écrire et/ou souligner. Seule l'encre noire ou l'encre bleue est autorisée. L'utilisation de plus d'une couleur, d'une couleur non autorisée, d'un surligneur pourra être considérée comme un signe distinctif.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 33 pages.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.
S'il est incomplet, en avertir le surveillant.

Attaché territorial, vous êtes chargé(e) du numérique à la direction générale de la communauté d'agglomération d'Admicom (150 000 habitants) et délégué(e) à la protection des données. La collectivité est engagée dans une démarche de « ville intelligente » (smart city). Vous êtes chargé(e) de coordonner les actions de la collectivité face aux enjeux de la transition numérique et d'assurer la mise en conformité avec la nouvelle réglementation.

À ce titre, le Directeur général des services (DGS) vous demande de rédiger à son attention, exclusivement à l'aide des documents joints, une note sur la sécurité du système d'information et la protection des données au sein de la collectivité.

Liste des documents :

Document 1 : « Cybersécurité : les collectivités territoriales, des cibles potentielles sous surveillance » - Pierre-Alexandre Conte - *laGazette.fr* - 23 février 2017 - 4 pages

Document 2 : « Quelle privacy dans la smart city ? » - extrait de « La plateforme d'une ville - Les données personnelles au cœur de la fabrique de la smart city » - *Cahier IP* n°5 - *CNIL/LINC* - 10 janvier 2017 - 2 pages

Document 3 : « Sécurité du numérique : sensibilisation des dirigeants » - *Secrétariat général de la Défense et de la Sécurité Nationale* - Février 2018 - 2 pages

Document 4 : « Règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données » (extrait) - *Journal officiel de l'Union européenne* - 27 avril 2016 - 3 pages

Document 5 : Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives (extrait) - *Journal officiel de la République française* - 1 page

Document 6 : « Recommandations relatives à l'application du référentiel » - extrait du *Référentiel général de sécurité - version 2.0 - Agence Nationale de la Sécurité du Système d'information (ANSSI)* - 13 juin 2014 - 5 pages

Document 7 : « RGPD : ce qui change pour les collectivités locales » - *Commission Nationale de l'Informatique et des Libertés (CNIL)* - 11 juillet 2017 - 4 pages

Document 8 : « Infographie - Plan d'Impact et d'Analyse (PIA) : vue d'ensemble des obligations et de la méthode » - *Commission Nationale de l'Informatique et des Libertés (CNIL)* - 19 février 2018 - 1 page

Document 9 : « RGPD : protéger les données à caractère personnel dès la conception des traitements » - Élisa Corazza et Yvon Goutal - *laGazette.fr* - 28 février 2018 - 3 pages

Document 10 : « Sensibiliser et tester les attitudes des employés à la sécurité informatique » - Christophe Badot - *Globbsecurity* - 14 février 2018 - 2 pages

Document 11 : « Vie privée et cyber-risques : la sécurité dans la *smart city* » - Nelly Moussu - *Smartcitymag* - Mars 2017 - 2 pages

Document 12 : « Entrée en vigueur de la nouvelle loi Informatique et Libertés » - *CNIL* - 4 juillet 2018 - 1 page

Documents reproduits avec l'autorisation du C.F.C.

Certains documents peuvent comporter des renvois à des notes ou à des documents non fournis car non indispensables à la compréhension du sujet.

SÉCURITÉ INFORMATIQUE

Cybersécurité : les collectivités territoriales, des cibles potentielles sous surveillance

Publié le 23/02/2017 • Par Pierre-Alexandre Conte • dans : Dossiers d'actualité, France

Si elles n'en ont pas toujours conscience, les collectivités territoriales peuvent bel et bien être victimes de cyberattaques. Et ce, pour de multiples raisons. En cas de faute avérée, les sanctions encourues peuvent devenir particulièrement difficiles à assumer.

Chiffres-clés

Date clé

4 mai 2018
C'est la date à laquelle le règlement européen sur la protection des données personnelles entrera en application. Ses objectifs ? Renforcer les droits des personnes, responsabiliser les acteurs traitant des données et crédibiliser la régulation. Les sanctions seront renforcées en cas de manquement à la loi. Les amendes pourront, par exemple, s'élever à 20 millions d'euros pour les collectivités.

Une République numérique. C'est ainsi qu'a été baptisée la loi portée par l'actuelle secrétaire d'État chargée du numérique, Axelle Lemaire, parue le 8 octobre 2016 au « Journal officiel ». Un nom ô combien symbolique et révélateur de la profondeur de la transformation vécue par l'ensemble de la société. Celle-ci touche naturellement les collectivités territoriales, qui bénéficient des multiples avantages qu'elle génère, mais qui doivent, dans le même temps, composer avec de nouvelles obligations. Parmi elles, figure en tête de liste la sécurisation de leur système d'information.

En préambule de son rapport d'activité annuel paru en 2016, l'Agence nationale de la sécurité des systèmes d'information (Anssi) introduisait le sujet comme suit : « Les technologies numériques procurent des gains de productivité et sont donc source de richesse et de compétitivité pour notre pays, mais elles induisent également des vulnérabilités nouvelles. La cybersécurité est devenue, de ce fait, une condition structurante, non seulement de la sauvegarde de notre patrimoine économique et intellectuel, mais aussi de la protection physique de nos concitoyens. » Des propos signés Louis Gautier, secrétaire général de la défense et de la sécurité nationale.

FOCUS

50 %

Dans son rapport d'activité concernant l'année 2015, l'Anssi explique avoir reçu 4 000 signalements, soit 50 % de plus qu'en 2014. L'Agence a aussi dû traiter une vingtaine d'incidents de sécurité majeurs.

Les sites web en première ligne

La première erreur en matière de sécurité informatique consiste à penser qu'une collectivité, quelle que soit sa nature, n'a aucune raison d'être la cible d'une attaque. C'est pourtant un raisonnement fréquemment rencontré au sein des petites et moyennes communes, qui considèrent parfois qu'elles ne détiennent rien qui puisse intéresser d'hypothétiques assaillants. « Comme tout un chacun qui dispose d'une visibilité sur internet, les collectivités territoriales peuvent faire partie des victimes d'une vague d'attaques, précise Guy Flament, référent de l'Anssi au sein de la région Nouvelle Aquitaine.

Leur présence sur internet, notamment par le biais de leurs sites web, offre des surfaces pour les attaquants, qui peuvent leur permettre d'afficher des messages de revendication ou de propagande. Ensuite, les collectivités subissent des attaques par des « rançongiciels » qui prennent en otage leur système d'information et offrent de le libérer contre une rançon. En ce qui concerne les autres menaces informatiques que peuvent être le sabotage ou l'espionnage, elles ne sont pas, pour le moment, particulièrement visées. Mais elles pourraient le devenir, notamment à cause du nombre de données à caractère personnel qu'elles hébergent. »

Les collectivités territoriales brassent en effet de plus en plus de données, dont certaines s'avèrent particulièrement sensibles. Elles sont au cœur de toutes les préoccupations, comme en témoignent les nombreux articles qui leur sont consacrés au sein de la loi pour une République numérique. Il convient donc de les protéger.
« Les collectivités détiennent notamment l'état civil. Il ne faudrait pas qu'un jour ces fichiers puissent être modifiés par des attaquants. Les comptes de la commune intéressent aussi les gens et tout ce qui touche aux dossiers de consultation publique », lance Guy Flament.

Sanctions pénales

La protection des données du citoyen est garantie par la loi « informatique et libertés ». C'est évidemment la Commission nationale de l'informatique et des libertés (Cnil) qui veille au respect de cette dernière. Ses compétences ont été élargies par la loi pour une République numérique.

Sur le plan financier, les collectivités encourent une amende pouvant s'élever jusqu'à 3 millions d'euros ; ce n'est pas rien ! La Cnil peut aussi ordonner que l'organisme sanctionné informe à ses frais les victimes. La loi prévoit par ailleurs la possibilité de sanctionner pénalement les maires, les présidents de conseils régionaux et de conseils généraux en cas de manquement grave, comme le fait de ne pas prendre les mesures nécessaires pour garantir la confidentialité des informations ou l'utilisation de ces dernières à d'autres fins.

À partir du mois de mai 2018, les collectivités devront appliquer le règlement européen sur le sujet. Concernant ce dernier, selon Pierre Deprez, avocat du cabinet DS avocats dans le département « droit de la propriété intellectuelle, technologies numériques et data », on parle d'un « changement de paradigme ». Cela signifie le passage « d'un régime de déclaration et d'autorisation des traitements à un régime d'accountability, d'autoresponsabilité ».

Les communes devront conserver « une trace des moyens techniques et organisationnels qu'elles auront mis en œuvre pour assurer la sécurité des données », dans le but de montrer patte blanche en cas de contrôle.

Mais les données ne sont pas l'unique préoccupation des collectivités. D'autres domaines requièrent leur attention, à l'image des objets connectés. Ce sont de formidables outils, mais ils peuvent aussi se retourner contre ceux qui les utilisent.

« Les objets connectés, comme les smartphones il y a quelques années, représentent une augmentation de la surface d'attaque puisqu'ils sont, par nature, connectés à internet. Si ces objets ne sont pas correctement configurés et sécurisés, ils offrent une porte d'entrée à d'éventuels attaquants », précise Guy Flament.

Des risques divers

« L'émergence des outils connectés implique de prendre ses précautions, déclare de son côté Olivier Fouqueau, directeur général des services d'Infocom94, syndicat intercommunal informatique du Val-de-Marne. Quand une direction générale des services techniques, voire un élu, décide que c'est super d'équiper toutes les places de parking d'un capteur pour permettre de savoir, à distance, par le biais de son téléphone portable, s'il y a une place pour se garer, mais qu'il n'y a pas de sécurité autour, cela peut très vite devenir difficile à gérer. »

Les rapports affirmant que la cybercriminalité est en constante augmentation sont rendus publics de manière quasi quotidienne. Pour autant, il n'est pas si évident de trouver une collectivité territoriale qui accepte de faire part d'une mauvaise expérience. La raison est simple : elle relève de la peur de voir son image se détériorer. C'est là l'un des principaux risques encourus, notamment par les villes.

« Il ne se passe pas une journée sans qu'il y ait un site internet défiguré dans la région », déplore le référent de l'Anssi en Nouvelle Aquitaine. En cas de pertes de données et de responsabilité avérée, le règlement européen demandera également aux collectivités, en 2018, d'informer le public quant à leurs failles de sécurité. Si les communes sont concernées par leur image, elles doivent en plus composer avec l'inaccessibilité de leur site. Ce qui peut altérer de manière plus ou moins grave la mission de service public.

La perte peut aussi être financière, notamment s'il y a demande de rançon, les sommes demandées étant, la plupart du temps, élevées.

« Le sujet de la sécurité est souvent diabolisé, regrette Frank Mosser, expert dans le domaine de la cybersécurité et président de MGDIS, société éditrice de services logiciels de pilotage et de valorisation de l'action publique, basée à Vannes. Quand ça fait trop peur, on a tendance à mettre la tête dans le sac et à faire l'autruche. Il y a quelques années, ce n'était pas si grave que cela. Là, ça le devient un peu plus. »

FOCUS

Le « rançongiciel », fléau international en pleine expansion

Extorsion – Tout le monde ou presque a entendu parler de Locky. Ce « ransomware » – « rançongiciel » en français – s'est rendu populaire en faisant de nombreuses victimes au cours de l'année passée. Une fois activé sur l'ordinateur de la personne visée, ce dernier chiffre les données et demande une somme d'argent en échange de leur restitution. S'il reste l'exemple le plus connu, Locky n'est pas un cas unique. Loin de là.

290 millions de dollars – Le FBI estime que durant le premier trimestre de l'année 2016, environ 290 millions de dollars ont été extorqués par le biais de « rançongiciels ». Aux Etats-Unis, le Hollywood Presbyterian Medical Center a fait partie des victimes au mois de février 2016. Paralysé pendant plus d'une semaine, il avait fini par débourser la somme de 17 000 dollars pour reprendre une activité normale. Et ce, après avoir dû envoyer de nombreux patients vers d'autres établissements.

Une mésaventure similaire est arrivée trois mois plus tard au Kansas Heart Hospital. Mais cette fois, après avoir payé la rançon, l'hôpital n'a pas pu récupérer ses fichiers. Pire, une seconde somme d'argent lui a été demandée. Fin janvier, c'est la police de Washington qui s'est aperçue que le réseau de vidéosurveillance de la ville ne fonctionnait plus correctement. Avant de prendre connaissance du problème : depuis le 12 janvier, un « ransomware » avait commencé à faire son œuvre, paralysant 123 des 187 caméras utilisées. En cherchant la source du dysfonctionnement, des enquêteurs sont tombés un peu plus tard sur un message les invitant à payer une somme. Ce qui n'a pas été fait. Le réseau a été réinstallé dans l'urgence.

FOCUS

L'expérience traumatisante d'une commune piratée

Chaque jour ou presque, des collectivités découvrent qu'elles ont été victimes d'une attaque informatique. Mais difficile de témoigner à visage découvert. Voici ce qu'une victime raconte, sous couvert d'anonymat : « Nous sommes arrivés un matin et nos postes informatiques étaient bloqués, explique cette directrice générale des services. Impossible de travailler dans ces conditions. Sur les écrans était affiché un message énigmatique et surtout, une demande de rançon. »

Si la police a rapidement été prévenue, la commune a dû se résoudre à trouver une solution au plus vite pour reprendre une activité normale. « Nous ne pouvions pas payer la somme, explique-t-elle. Nous avons appelé notre prestataire informatique qui a fait le déplacement et nous a indiqué qu'une grande partie de nos données, notamment les plus récentes, étaient perdues.

Personne n'avait anticipé le problème. Cela a créé beaucoup de remous au sein de la collectivité, dans la mesure où nous ne savons pas qui est responsable de l'attaque. L'enquête est toujours en cours. Plusieurs pistes ont été évoquées, dont des personnes hostiles à certaines décisions locales. C'est une expérience qui reste encore assez traumatisante pour nous. »

Si le prestataire informatique a fourni une solution d'appoint pour que les données soient plus fréquemment sauvegardées, aucun changement en profondeur, en termes de sécurité, n'a été apporté à ce jour.

RÉFÉRENCES

- Guide d'homologation des systèmes d'information (Anssi)
- Référentiel général de sécurité (RGS)
- Guide d'hygiène informatique

QUELLE PRIVACY DANS LA SMART CITY ?

Données personnelles, les impensées de la smart city

Les publications, études, travaux de recherches et autres *think tanks* sont légions à s'intéresser à la smart city, très bien cotée à l'indice Google : plus de 40000 références dans Google Scholar, 16 millions sur le moteur de recherche, un million sur l'actualité, et une courbe de tendance croissante depuis dix ans. Pourtant, la protection des données personnelles reste le parent pauvre de ces travaux.

L'individu reste aujourd'hui, comme dans la conception première de la smart city 1.0, un problème à régler, ou au mieux, pour certains promoteurs d'une ville participative et contributive, comme un smartphone ambulant dont les données seraient essentielles à la bonne conduite de la ville.

Cependant, les individus forts de leurs droits et libertés sont ceux par qui et pour qui la ville continue à se développer. Alors, le sujet de la protection des droits et de la vie privée devient une sorte de passage obligé : les promoteurs de la smart city en parlent, affirment cette impérieuse nécessité, mais ne savent ou ne veulent l'orchestrer réellement avec les discours traditionnels. Le sujet de la vie privée devient une sorte de « caveat » qu'il faut évoquer pour mieux passer à autre chose, comme dans le dossier « *The rise of the smart city* » du Wall Street journal d'avril 2017[18] : le sujet des inquiétudes concernant la vie privée ouvre le 5ème paragraphe du dossier, avant que le 6ème paragraphe ne referme définitivement ce sujet épineux…

Des enjeux de vie privée intensifiés par la logique de ville intelligente

Dans un article de 2016[19], Rob Kitchin, chercheur à la Maynooth University et spécialiste de la smart city, synthétise les enjeux de la protection de la vie privée et de la sécurité des données dans les villes dites intelligentes. Kitchin expose une série de six enjeux relatifs à la vie privée dans les *smart cities* :

• **Intensification de la datafication :** les technologies mises en œuvre captent des données personnelles dont le volume, la gamme et la granularité sont toujours plus élevés, des données qui approchent l'exhaustivité, qui circulent d'une plateforme à l'autre, d'un service à l'autre, et dont la collecte est potentiellement continue.

• **Risques croissants d'inférences liées aux modèles prédictifs :** les modèles prédictifs peuvent parfois être utilisés pour inférer l'appartenance à des groupes sociaux, des opinions politiques ou religieuses. Des inférences qui, dans certains pays, peuvent mettre les individus en danger, qui peuvent également se révéler fausses, et avoir donc des conséquences pour les individus, par exemple avec les algorithmes prédictifs de crimes, dont une étude de Propublica a démontré qu'ils renforcent les préjugés et stigmatisent certains segments de la population[20].

• **Anonymisation insuffisante permettant la ré-identification :** les données pseudonymisées permettent encore l'identification des personnes. L'auteur souligne à juste titre que le terme « anonymisé » souvent utilisé par les entreprises tient de l'oxymore dès lors que celles-ci ne recourent en réalité qu'à la pseudonymisation. Or après anonymisation, il ne doit plus être possible d'identifier la personne.

• **Opacité et automatisation des systèmes créant de l'obfuscation* et de la perte du contrôle sur les données :** le grand nombre de systèmes, de dispositifs et d'acteurs privés ou publics opérant dans la ville, ainsi que les multiples transferts de données entre chacun d'eux, rend le consentement, le contrôle et la sécurité des données très complexes, dans un système d'autant plus opaque que la collecte des données est le plus souvent automatisée.

• **Données partagées et réutilisées pour des usages et des finalités inattendues et imprévisibles :** ces données peuvent être notamment agrégées, pseudonymisées, puis revendues pour des usages tiers (à l'image des données de Strava Metro[21]). Ces données peuvent également avoir un impact direct ou indirect sur la vie des personnes, notamment dans le cas des données vendues à des *data brokers* (courtiers en données) à des fins de profilage marketing, ou dans leur usage par des algorithmes (i.e : prédiction du crime), menant à une forme de « data déterminisme », ou, selon les termes d'Antoinette Rouvroy, de gouvernementalité algorithmique.

Les termes suivis d'un astérisque sont définis dans le glossaire en fin de cahier.

18 Michael Totty, « The Rise of the smart city », *Wall street journal*, 16 avril 2017. https://www.wsj.com/articles/the-rise-of-the-smart-city-1492395120

19 Pour une analyse plus complète, voir sur linc.cnil.fr : https://linc.cnil.fr/fr/smart-privacy-dans-la-smart-city

20 Julia Angwin, « Machine bias », *ProPublica*, 23 mai 2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

21 Pour en savoir plus, voir sur linc.cnil.fr : https://linc.cnil.fr/fr/les-donnees-cyclistes-redessinent-la-ville

• **Mécanismes d'information et de consentement vides de sens ou absents :** ces deux notions, pierres angulaires de la protection des données personnelles, sont particulièrement affaiblies dans les technologies de la smart city. Le volume et la diversité des données collectées rend très compliqué le contrôle de leurs données par les individus, même pour les plus proactifs : lire et comprendre les conditions générales d'utilisation de chacun des services serait trop compliqué et chronophage.

Sur ce dernier point soulevé par Rob Kitchin, s'ils constituent l'un des enjeux de la numérisation des villes, le respect du droit à l'information des personnes concernées et l'obtention du consentement (sauf s'il existe un autre fondement légal qui justifie le traitement) restent des obligations juridiques dès lors qu'il y a bel et bien des données personnelles.

L'enjeu pour les porteurs de projet réside dans leur capacité à mettre en œuvre des services respectueux des droits des personnes, quelle que soit la complexité des systèmes. D'où l'intérêt pour les porteurs de projets d'effectuer une analyse d'impact (*Privacy Impact Assessment*), dès lors que la mise en œuvre du service engendre un risque élevé pour les droits et les libertés des personnes physiques (article 27 du RGPD*).

Un terrain de jeu idéal pour les menaces « cyber »

Colosse aux pieds d'argile, le rêve de la smart city porte en lui les germes de sa propre faiblesse. Si ces villes permettent de proposer des fonctionnalités plus nombreuses que la simple somme des parties ou des systèmes qui les composent, il en va de même pour les vulnérabilités auxquelles elles sont exposées. En termes de cybersécurité, on parle de très grande « surface d'attaque », les systèmes tout intégrés vont devenir vulnérables à des failles de sécurité qui auront un effet sur l'ensemble de la structure.

Parmi les exemples concrets de risques, on retrouve par exemple le déni de service (DoS) informatique, qui provoquerait l'arrêt des téléservices, et physique (assignation simultanée d'un grand nombre de personnes), le *blackout* (arrêt des services urbains, par exemple éclairage public, système de caméras de vidéoprotection), les fausses alertes (secousse sismique, inondation), la dissémination d'informations, etc. Le mode de fonctionnement intrinsèque de la ville, à savoir 24/7, demande d'assurer la continuité de service (*no shut down*). Ce qui rend les déploiements technologiques inédits, sans phase de test à proprement parler. La maintenance des smart cities présente donc des enjeux cruciaux.

COUP D'ŒIL À LA SCIENCE-FICTION :

l'OS de la smart city

Dans le jeu vidéo Watchdogs (2014), le joueur incarne un hacker qui utilise les failles de ctOS, un OS qui gère l'ensemble de l'infrastructure de la ville de Chicago. Cela lui permet de contrôler les feux de circulation, les informations personnelles des passants et le système de communication de la police. cTOS est présenté comme le produit d'une véritable entreprise sur son site web : http://chicago-ctos.com

En 2015 en France, l'ANSSI a traité vingt attaques majeures de niveau stratégique contre la France. Aux Etats-Unis, le nombre d'attaques sur des infrastructures « critiques » est passé de 200 en 2012 à 300 en 2015, un nombre encore relativement peu élevé, mais un risque réellement présent, tant pour la protection de systèmes qui ont à traiter des données personnelles que pour la protection des infrastructures et des personnes. En 2013, des hackers avaient tenté de prendre le contrôle d'un barrage près de New-York...

Dans une vision prospective, c'est le *hacking* des intelligences artificielles qu'il faudra peut-être craindre, des chercheurs ont démontré que les algorithmes de *machine learning* peuvent être manipulés en exploitant leur propension à cibler des modèles (*patterns*) dans les données : en leur envoyant de fausses informations, les algorithmes construisent des modèles erronés. On peut par exemple tromper un véhicule autonome avec des panneaux d'affichages, ou des assistants à reconnaissance vocale par des signaux inaudibles pour l'oreille humaine. L'algorithme n'est pas encore suffisamment intelligent pour repérer que l'on cherche à le tromper. Pour Patrick McDaniel, professeur à l'université de Pennsylvanie, « le risque est réel [...] les systèmes de *machine learning* opèrent sur tous types de fonctions pour lesquels des personnes pourraient financer des attaques ».

DOCUMENT 3

VIGIPIRATE

SÉCURITÉ DU NUMÉRIQUE SENSIBILISATION DES DIRIGEANTS

Cette fiche s'adresse aux dirigeants d'entreprises privées ou de collectivités territoriales et vise à les aider à appréhender la question de la sécurité du numérique à travers quelques exemples et recommandations pratiques.

1 Cela pourrait vous arriver...

Les scénarios proposés ci-dessous illustrent quelques exemples (parmi d'autres) de menaces de nature cyber pesant sur les organisations et relevant de la responsabilité de leurs dirigeants.

Usurpation d'identité /hameçonnage

Le hameçonnage consiste à usurper l'identité de l'expéditeur dans le but de duper le destinataire qui est invité à ouvrir une pièce-jointe malveillante ou à suivre un lien vers un site Web malveillant. Une fois cette 1ère machine contaminée, l'attaquant en prend le contrôle pour manœuvrer au sein du système d'information de l'organisation.

Arnaud reçoit une demande d'ajout de contact sur LinkedIn de la part de son supérieur hiérarchique pendant la période des fêtes de fin d'année. Ce dernier est en congés et souhaite lui transmettre des documents car il n'a pas accès à sa boite mail momentanément. Mais ce qu'Arnaud ne sait pas, c'est que la personne qui s'adresse à lui n'est pas son supérieur mais un groupe d'attaquants ayant usurpé son identité. En transmettant à ce collaborateur un simple document contenant une charge malveillante, ils ont pu compromettre les équipements de l'entreprise connectés à Internet et exfiltrer des données sensibles en relation avec une importante négociation commerciale de nature confidentielle. Dès le lendemain, les informations fuitent dans la presse, conduisant ainsi à la rupture de la négociation au profit d'une entreprise concurrente.

Rançongiciel

Le rançongiciel est un programme malveillant chiffrant tout ou partie des données stockées sur un ordinateur ou accessibles par un réseau. L'objectif est de proposer à la victime de récupérer ses données en échange du paiement d'une rançon.

Guillaume est dirigeant d'entreprise. Nous sommes vendredi après-midi avant le début des congés de fin d'année et Guillaume avait déjà autorisé ses employés à partir exceptionnellement à 15h00. Son responsable sécurité lui indique qu'une mise à jour de l'ensemble des postes de travail doit être réalisée mais ne pourra pas être effective avant 15h00. Guillaume décide de fermer l'entreprise comme prévu et de reporter l'opération de mise à jour.

Le 2 janvier, les ordinateurs de tous les employés affichent un écran noir porteur d'un message exigeant d'eux le paiement d'une rançon en échange de la récupération de leurs données. Les employés ne pouvant plus travailler, l'activité de l'ensemble de l'entreprise et de ses sous-traitants est à l'arrêt et mise en péril.

Les conséquences pour votre entreprise peuvent être graves : perte financière importante, atteinte à l'image de l'organisation, etc.

2 S'emparer de la question de la sécurité numérique

5 questions pour faire le point

- Depuis quand n'ai-je pas entendu parler de cybersécurité ?
- Mon entreprise est-elle une cible d'intérêt pour des attaquants ?
- Ai-je pris toutes les précautions pour protéger mes informations et les échanges avec mes partenaires et mes collaborateurs ?
- Quel est la part du budget consacrée à la sécurité informatique ?
- Ai-je déjà parlé de cybersécurité à mes collaborateurs ?

5 questions à poser à mon RSSI

- Quelles sont nos principales vulnérabilités ?
- Quels sont les moyens de protection actuellement en place pour lutter contre les attaques et codes malveillants ?
- A-t-on déjà fait un audit de sécurité des SI ?
  A-t-on déjà fait une analyse de risques ?
  Dispose-t-on d'une cartographie des SI ?
- Sommes-nous préparés si une crise d'origine cyber survenait ?
- Disposons-nous d'une couverture juridique et nos contrats d'assurance intègrent-ils le risque cyber ?

Vous êtes au cœur de la stratégie de gestion des informations clés de l'entreprise. Vos données personnelles sont autant d'informations potentiellement convoitées par des individus aux intentions malveillantes. Soyez notamment vigilant à l'égard de possibles usurpations de votre identité sur les réseaux sociaux et maîtrisez les informations sur votre entreprise qui circulent sur Internet.

Sensibiliser vos employés aux bonnes pratiques

Vos employés doivent être sensibilisés voire formés aux bonnes pratiques de l'informatique et devenir acteur de la sécurité numérique de leur entreprise.

Analyser les risques et protéger les systèmes d'information sensibles

Il est essentiel de savoir quels sont les systèmes d'information les plus cruciaux pour le bon fonctionnement de votre entreprise afin de pouvoir traiter les risques susceptibles de les fragiliser.

Préparer votre entreprise à une attaque informatique

Assurez-vous de disposer d'un plan de réaction aux incidents de sécurité (notamment un processus de sauvegarde régulier des données critiques) et testez-le. En particulier, établissez une chaine de remontée d'incidents connue des employés afin de reconnaitre au plus tôt une tentative d'attaque.

Organiser un exercice simulant une attaque

Un exercice de gestion de crise permet de vérifier la solidité des procédures mises en place dans votre organisme et de les corriger si nécessaire.

3 Vous pensez avoir été victime d'une attaque

Qui prévenir ?

Dirigeant d'une entreprise (TPE, PME) ou d'une collectivité territoriale, il est recommandé de vous rendre sur la plateforme numérique **www.cybermalveillance.gouv.fr** afin d'être mis en relation avec des prestataires de proximité susceptibles de vous assister techniquement. Vous pouvez également déposer plainte auprès d'un service de la Police nationale ou de la Gendarmerie nationale ou adresser un courrier au Procureur de la République auprès du Tribunal de Grande Instance compétent.

4 Documents de référence

Guide des bonnes pratiques de l'informatique
https://www.ssi.gouv.fr/uploads/2017/01/guide_cgpme_bonnes_pratiques.pdf.pdf
Guide d'hygiène informatique (à l'attention des DSI)
https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf
MOOC (Massive Open Online Course) SecNumacadémie de l'ANSSI
https://www.secnumacademie.gouv.fr
En cas d'incident
https://www.ssi.gouv.fr/en-cas-dincident/

SGDSN
SECRÉTARIAT GÉNÉRAL
DE LA DÉFENSE ET DE
LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 11
sgdsn.gouv.fr

Maquette : Pôle graphique, fabrication, déplacements, image – DSAF/DPL – Février 2018.

RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

(...) Section 2
Sécurité des données à caractère personnel

Article 32

Sécurité du traitement

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins:

a) la pseudonymisation et le chiffrement des données à caractère personnel;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article.

4. Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre.

Article 33

Notification à l'autorité de contrôle d'une violation de données à caractère personnel

1. En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

2. Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

3. La notification visée au paragraphe 1 doit, à tout le moins:

a) décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;

b) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

c) décrire les conséquences probables de la violation de données à caractère personnel;

d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

4. Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

5. Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article.

Article 34

Communication à la personne concernée d'une violation de données à caractère personnel

1. Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

2. La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d).

3. La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie:

a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement;

b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser;

c) elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

4. Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe 3 est remplie.

Section 3

Analyse d'impact relative à la protection des donnés et consultation préalable

Article 35

Analyse d'impact relative à la protection des données

1. Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

2. Lorsqu'il effectue une analyse d'impact relative à la protection des données, le responsable du traitement demande conseil au délégué à la protection des données, si un tel délégué a été désigné.

3. L'analyse d'impact relative à la protection des données visée au paragraphe 1 est, en particulier, requise dans les cas suivants:

a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire;

b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10; ou

c) la surveillance systématique à grande échelle d'une zone accessible au public.

4. L'autorité de contrôle établit et publie une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise conformément au paragraphe 1. L'autorité de contrôle communique ces listes au comité visé à l'article 68.

5. L'autorité de contrôle peut aussi établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise. L'autorité de contrôle communique cette liste au comité.

6. Avant d'adopter les listes visées aux paragraphes 4 et 5, l'autorité de contrôle compétente applique le mécanisme de contrôle de la cohérence visé à l'article 63, lorsque ces listes comprennent des activités de traitement liées à l'offre de biens ou de services à des personnes concernées ou au suivi de leur comportement dans plusieurs États membres, ou peuvent affecter sensiblement la libre circulation des données à caractère personnel au sein de l'Union.

7. L'analyse contient au moins:

a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement;

b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités;

c) une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1; et

d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

8. Le respect, par les responsables du traitement ou sous-traitants concernés, de codes de conduite approuvés visés à l'article 40 est dûment pris en compte lors de l'évaluation de l'impact des opérations de traitement effectuées par lesdits responsables du traitement ou sous-traitants, en particulier aux fins d'une analyse d'impact relative à la protection des données.

9. Le cas échéant, le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu, sans préjudice de la protection des intérêts généraux ou commerciaux ou de la sécurité des opérations de traitement.

10. Lorsque le traitement effectué en application de l'article 6, paragraphe 1, point c) ou e), a une base juridique dans le droit de l'Union ou dans le droit de l'État membre auquel le responsable du traitement est soumis, que ce droit règlemente l'opération de traitement spécifique ou l'ensemble des opérations de traitement en question et qu'une analyse d'impact relative à la protection des données a déjà été effectuée dans le cadre d'une analyse d'impact générale réalisée dans le cadre de l'adoption de la base juridique en question, les paragraphes 1 à 7 ne s'appliquent pas, à moins que les États membres n'estiment qu'il est nécessaire d'effectuer une telle analyse avant les activités de traitement.

11. Si nécessaire, le responsable du traitement procède à un examen afin d'évaluer si le traitement est effectué conformément à l'analyse d'impact relative à la protection des données, au moins quand il se produit une modification du risque présenté par les opérations de traitement.

(...)

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

PREMIER MINISTRE

Décret nº 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance nº 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives

(...)

CHAPITRE Ier

Référentiel général de sécurité

Art. 1er. – Le référentiel général de sécurité prévu par l'article 9 de l'ordonnance du 8 décembre 2005 susvisée fixe les règles auxquelles les systèmes d'information mis en place par les autorités administratives doivent se conformer pour assurer la sécurité des informations échangées, et notamment leur confidentialité et leur intégrité, ainsi que la disponibilité et l'intégrité de ces systèmes et l'identification de leurs utilisateurs.

Ces règles sont définies selon des niveaux de sécurité prévus par le référentiel pour des fonctions de sécurité, telles que l'identification, la signature électronique, la confidentialité ou l'horodatage, qui permettent de répondre aux objectifs de sécurité mentionnés à l'alinéa précédent.

La conformité d'un produit de sécurité et d'un service de confiance à un niveau de sécurité prévu par ce référentiel peut être attestée par une qualification, le cas échéant à un degré donné, régie par le présent décret.

Art. 2. – Le référentiel général de sécurité ainsi que ses mises à jour sont approuvés par arrêté du Premier ministre publié au *Journal officiel* de la République française. L'Agence nationale de la sécurité des systèmes d'information concourt à l'élaboration de ce référentiel et à sa mise à jour en liaison avec la direction générale de la modernisation de l'Etat. Ce référentiel est mis à disposition du public par voie électronique.

CHAPITRE II

Fonctions de sécurité des systèmes d'information

Art. 3. – Dans les conditions fixées par le référentiel général de sécurité mentionné à l'article 2 du présent décret, l'autorité administrative doit, afin de protéger un système d'information :

1º Identifier l'ensemble des risques pesant sur la sécurité du système et des informations qu'il traite, eu égard notamment aux conditions d'emploi du système ;

2º Fixer les objectifs de sécurité, notamment en matière de disponibilité et d'intégrité du système, de confidentialité et d'intégrité des informations ainsi que d'identification des utilisateurs du système, pour répondre de manière proportionnée au besoin de protection du système et des informations face aux risques identifiés ;

3º En déduire les fonctions de sécurité et leur niveau qui permettent d'atteindre ces objectifs et respecter les règles correspondantes du référentiel général de sécurité.

Dans les conditions fixées par le référentiel susmentionné, l'autorité administrative réexamine régulièrement la sécurité du système et des informations en fonction de l'évolution des risques.

Art. 4. – Pour mettre en œuvre dans un système d'information les fonctions de sécurité ainsi déterminées, l'autorité administrative recourt à des produits de sécurité et à des prestataires de services de confiance ayant fait l'objet d'une qualification dans les conditions prévues au présent décret ou à tout autre produit ou prestataire pour lesquels elle s'est assurée de la conformité de leurs fonctions de sécurité au référentiel général de sécurité.

Art. 5. – L'autorité administrative atteste formellement auprès des utilisateurs de son système d'information que celui-ci est protégé conformément aux objectifs de sécurité fixés en application de l'article 3.

Dans le cas d'un téléservice, cette attestation est rendue accessible aux usagers selon les mêmes modalités que celles prévues à l'article 4 de l'ordonnance du 8 décembre 2005 susvisée pour la décision de création du téléservice.

(...)

Chapitre 7. Recommandations relatives à l'application du référentiel

Au-delà de l'analyse de risques et de l'homologation, l'ANSSI recommande l'adoption de bonnes pratiques relatives à la méthodologie, aux procédures et à l'organisation.

7.1 Organiser la sécurité des systèmes d'information

a Organiser les responsabilités liées à la sécurité des systèmes d'information

Les autorités administratives doivent mettre en œuvre une organisation qui endosse les responsabilités liées à la sécurité des systèmes d'information. Elle peut être mutualisée avec celle requise pour la protection des informations classifiées de défense, telle que définie dans l'*instruction générale interministérielle sur la protection du secret de la défense nationale* n° 1300/SGDSN/PSE/PSD.

De préférence dirigée par un représentant de l'autorité administrative, cette organisation doit disposer des moyens matériels nécessaires à la réalisation de ses missions et de la capacité à gérer les risques, les crises ou les incidents qui pourraient en résulter. Le cas échant, elle s'appuie sur une chaîne fonctionnelle SSI chargée de l'assister dans le pilotage, la gestion et le suivi des moyens SSI : le responsable de la sécurité des systèmes d'information (RSSI), l'officier de la sécurité des systèmes d'information (OSSI), le correspondants SSI, etc.

Éventuellement à l'aide de la chaîne fonctionnelle SSI, l'organisation mise en place par l'autorité administrative peut assurer les missions suivantes :

- coordination des actions permettant l'intégration des clauses liées à la SSI dans les contrats ou les conventions impliquant un accès par des tiers à des informations ou à des ressources informatiques ;
- formalisation de la répartition des responsabilités liées à la SSI (définition des périmètres de responsabilité, des délégations de compétences, etc.) ;
- établissement des relations nécessaires avec les autorités externes de défense des systèmes d'information, notamment pour la gestion des intrusions et des attaques sur les systèmes.

b Mettre en place un système de management de la sécurité des systèmes d'information

Il est recommandé de mettre en œuvre des processus permettant de rechercher une amélioration constante de la SSI. Par exemple, la mise en place d'un système de management de la sécurité de l'information, tel que défini dans la norme ISO 27001, permet non seulement de planifier et de mettre en œuvre les mesures de protection du système d'information, mais également d'en vérifier la pertinence et la conformité par rapport aux objectifs établis.

c Élaborer une politique de sécurité des systèmes d'information

Il est recommandé d'élaborer et de formaliser une politique de sécurité des systèmes d'information (PSSI). Elle peut être générale ou déclinée en fonction des besoins spécifiques de chaque domaine de chaque système d'information. Le guide « *Politique SSI* » de l'ANSSI fournit une aide pour son élaboration.

7.2 Impliquer les instances décisionnelles

Les instances décisionnelles des autorités administratives doivent être impliquées dans la sécurisation des systèmes d'information dont elles ont *in fine* la responsabilité, afin de donner les orientations adéquates, notamment en termes d'investissement humain et financier, et de valider les objectifs de sécurité et les orientations stratégiques. La norme ISO 27001 fournit, à titre indicatif, une liste de sujets susceptibles d'être traités au niveau de la direction d'une autorité administrative.

7.3 Adapter l'effort de protection des systèmes d'information aux enjeux de sécurité et prendre en compte la SSI dans les projets

La sécurité d'un système d'information doit être adaptée aux enjeux du système lui-même et aux besoins de sécurité de l'autorité administrative, afin d'y consacrer les moyens financiers et humains nécessaires et suffisants. Dans ce but, il est recommandé d'utiliser les guides de l'ANSSI « *Maturité SSI* » et « *Gestion et intégration de la SSI dans les projets* » (GISSIP). Ils permettent, dans le cadre du développement d'un projet de système d'information, de déterminer les enjeux relatifs à la sécurité et d'identifier l'ensemble des livrables relatifs à la SSI.

7.4 Adopter une démarche globale

L'ensemble de la démarche de sécurisation des systèmes d'information doit procéder d'une volonté cohérente et globale, afin d'éviter la dispersion des efforts des équipes en charge de la SSI ou la mise en œuvre de mesures de sécurité parcellaires. Chaque décision doit être prise au juste niveau hiérarchique. Il est ainsi recommandé :

- de prendre en considération tous les aspects qui peuvent affecter la SSI, qu'ils soient techniques (matériels, logiciels, réseaux) ou non (organisations, infrastructure, personnel) ;
- d'envisager tous les risques et menaces, quelle que soit leur origine ;
- de prendre en compte la SSI à tous les niveaux hiérarchiques. La SSI repose sur une vision stratégique et nécessite des choix d'autorité (enjeux, moyens humains et financiers, risques résiduels acceptés) ainsi qu'un contrôle des actions et de leur légitimité ;
- de responsabiliser tous les acteurs (décideurs, maîtrise d'ouvrage et d'œuvre, utilisateurs) ;
- d'intégrer la SSI tout au long du cycle de vie des systèmes d'information (depuis l'étude d'opportunité jusqu'à la fin de vie du système).

D'une manière similaire, la sécurité doit être prise en compte dès la phase de définition des objectifs fonctionnels des systèmes d'information, afin de :

- limiter les surcoûts inhérents à l'application tardive de mesures de sécurité ;
- garantir l'efficacité des mesures mises en œuvre ;
- favoriser l'appropriation de la sécurité par les équipes en charge du SI.

7.5 Informer et sensibiliser le personnel

L'ensemble des agents d'une autorité administrative, et le cas échant les contractants et les utilisateurs tiers, doivent suivre une formation adaptée sur la sensibilisation et recevoir régulièrement les mises à jour des politiques et des procédures qui concernent leurs missions. Cette formation doit permettre de réduire les risques liés à la méconnaissance des principes de base et des règles élémentaires de bonne utilisation de l'outil informatique.

La sensibilisation du personnel doit être régulière. À cet effet, l'ANSSI publie des bonnes pratiques pour l'application de principes de base en matière de sécurité des systèmes d'information : www.ssi.gouv.fr/fr/bonnes-pratiques/principes-generaux.

7.6 Prendre en compte la sécurité dans les contrats et les achats

Les exigences de sécurité relatives aux produits ou aux prestations acquis doivent faire l'objet d'une étude et doivent être clairement formalisées et intégrées dans les dossiers d'appels d'offres, au même titre que les exigences fonctionnelles, réglementaires, de performance ou de qualité.

Ces exigences peuvent concerner le système qui fait l'objet de la consultation, mais aussi la gestion du projet lui-même (formation ou habilitation des personnels), en incluant les phases opérationnelles et de maintenance. Il convient notamment de :

- veiller à intégrer aux règlements de consultation ou aux cahiers des charges les référentiels de l'ANSSI applicables (produits certifiés, qualifiés, agréés…);
- demander à ce que les produits de sécurité soient fournis avec l'ensemble des éléments permettant d'en apprécier le niveau de sécurité ;
- préciser les clauses relatives à la maintenance des produits acquis ;
- préciser les clauses concernant les conditions de l'intervention et de l'accès physique et logique des sous-traitants :
- préciser les clauses garantissant la qualité et la sécurité des prestations et produits fournis ;
- préciser les conditions de propriété des codes sources ;
- prévoir, le cas échéant, la réversibilité des prestations et la portabilité des données générées pendant celles-ci en s'assurant en particulier que les bases de données sont extractibles, que celle-ci peut être distinguée du système lui-même et que les formats utilisés sont ouverts ;
- préciser la nature et les modalités de réalisation des tableaux de bord et mécanismes de suivi des prestations de sécurité ;
- prévoir les modalités de réaction aux crises et aux incidents susceptibles d'affecter le système ;
- prévoir des points de contact compétents à même de répondre aux besoins des autorités administratives ;
- vérifier, dans les réponses à appel d'offres, la couverture des exigences sécurité inscrites dans la consultation.

Une attention particulière devra être portée aux mécanismes de validation et de recette des composants mettant en œuvre les exigences de sécurité.

7.7 Prendre en compte la sécurité dans les projets d'externalisation et d'informatique en nuage

Le recours à l'externalisation ou à « l'informatique en nuage » présente des risques spécifiques qu'il convient d'évaluer avant d'aborder une telle démarche. Ces risques peuvent être liés au contexte même de l'opération d'externalisation ou à des spécifications contractuelles déficientes ou incomplètes. Dans cette hypothèse, il est recommandé d'appliquer les prescriptions décrites dans le guide de l'ANSSI « *Maîtriser les risques de l'infogérance – Externalisation des systèmes d'information* ». Ce guide fournit :

- une démarche cohérente de prise en compte des aspects SSI lors de la rédaction du cahier des charges d'une opération d'externalisation ;
- un ensemble de clauses types ainsi qu'une base d'exigences de sécurité, à adapter et à personnaliser en fonction du contexte particulier de chaque projet d'externalisation.

7.8 Mettre en place des mécanismes de défense des systèmes d'information

En complément des mécanismes de protection des systèmes d'information, et en fonction de leurs enjeux de sécurité, les autorités administratives doivent adopter des mesures complémentaires relatives à la défense des systèmes d'information. Ces mesures consistent, en particulier, à assurer :

- la connaissance des systèmes exploités par l'autorité administrative, ou en relation avec elle (cartographie des SI, répertoire des interconnexions, etc.) ;

- la détection des malveillances, des erreurs et des imprudences, en périphérie ou à l'intérieur des systèmes d'informations des autorités administratives ;
- la traçabilité des actions et des accès réalisés sur les systèmes d'information (journalisation, notamment) ;
- la pérennisation des savoir-faire et des compétences, notamment en termes d'exploitation des SI ;
- la conservation de la preuve des infractions découvertes.

7.9 Utiliser les produits et prestataires labellisés pour leur sécurité

La qualification est un label, créé par l'ordonnance du 8 décembre 2005, qui permet d'attester de la confiance que l'on peut accorder à des produits de sécurité et à des prestataires de services de confiance (PSCO), ainsi que de leur conformité aux règles du RGS qui leurs sont applicables. D'autres labels existent pour attester de la compétence des professionnels, notamment en matière de SSI.

La nécessité de recourir à des produits de sécurité ou à des prestataires de services de confiance a été régulièrement rappelée par le Premier ministre [6], ainsi il est recommandé :

- d'utiliser chaque fois que possible des produits de sécurité qualifiés (cf. § 5.1) par l'ANSSI ;
- de recourir chaque fois que possible à des PSCO qualifiés (cf. § 5.2) ;
- de prendre en considération, pour le choix des prestataires, en plus de leur qualification, leur éventuelle certification selon la norme ISO 27001 ou d'autres normes équivalentes ;
- de prendre en considération, pour le choix de prestataires, la certification de leurs personnels lorsque des compétences particulières sont requises pour une fonction.

7.10 Élaborer des plans de traitement d'incidents ainsi que de continuité et de reprise d'activité

Les autorités doivent se préparer à faire face à des incidents de sécurité pour lesquels toutes les mesures préventives auraient échoué. A ce titre, elles doivent mettre en œuvre un *plan de continuité d'activité* et *un plan de reprise d'activité* qui identifient les moyens et les procédures nécessaires pour revenir à une situation nominale le plus rapidement possible, en cas d'incident grave. Ces documents doivent être régulièrement mis à jour. Les plans et les procédures qui en découlent doivent faire l'objet de test réguliers.

7.11 Procéder à des audits réguliers de la sécurité du système d'information

Les autorités administratives doivent réaliser ou faire réaliser des audits réguliers de leurs SI. À cet effet, le *référentiel d'exigences relatif aux prestataires d'audit de la sécurité des systèmes d'information* (annexe C du RGS) fixe les règles que doivent respecter les prestataires tiers qui réalisent des audits de la sécurité des systèmes d'information des autorités administratives. Cette annexe décrit également des recommandations à l'intention des commanditaires d'audits, dans le cadre de la passation de marchés publics ou d'un accord contractuel, ainsi qu'aux prestataires d'audit dans le cadre de leur devoir de conseil.

Afin de s'assurer qu'elles recourent à des prestataires qui respectent ces exigences, les autorités administratives doivent, autant que possible, faire appel à des prestataires ayant obtenu une qualification, selon le schéma décrit au chapitre 5.

---

[6] Cf. communication relative à la protection des systèmes d'information lors du conseil des ministres du 25 mai 2011 et allocution sur la politique de cybersécurité de la France du 20 février 2014.

7.12 Réaliser une veille sur les menaces et les vulnérabilités

Se tenir informé sur l'évolution des menaces et des vulnérabilités, en identifiant les incidents qu'elles favorisent ainsi que leurs impacts potentiels, constitue une mesure fondamentale de défense. Les sites institutionnels, comme celui du CERT-FR (www.cert.ssi.gouv.fr), ou ceux des éditeurs de logiciels et de matériels constituent des sources d'information essentielles sur les vulnérabilités identifiées, ainsi que sur les contre-mesures et les correctifs éventuels. Les mises à jour des logiciels et d'autres équipements, les correctifs des systèmes d'exploitation et des applications font l'objet d'alertes et d'avis qu'il est indispensable de suivre.

7.13 Favoriser l'interopérabilité

L'administration électronique ne saurait évoluer sans une prise en compte des règles relatives à l'interopérabilité et à la mise en cohérence des différents systèmes d'information des autorités administratives et de leurs partenaires (usagers, acteurs industriels, etc.). L'interopérabilité est en particulier traitée à travers le *Référentiel général d'interopérabilité*. Le processus de référencement est, quant à lui, décrit dans l'arrêté du 18 janvier 2012 relatif au référencement de produits de sécurité ou d'offres de prestataires de services de confiance.

(...)

CNIL.

DOCUMENT 7

RGPD : CE QUI CHANGE POUR LES COLLECTIVITÉS LOCALES

11 juillet 2017

En quoi les collectivités territoriales sont-elles impactées par le règlement européen sur la protection des données ?

Les collectivités territoriales traitent chaque jour de nombreuses données personnelles, que ce soit pour assurer la gestion administrative de leur structure (fichiers de ressources humaines), la sécurisation de leurs locaux (contrôle d'accès par badge, vidéosurveillance) ou la gestion des différents services publics et activités dont elles ont la charge.

Certains de ces traitements présentent une sensibilité particulière, comme les fichiers d'aide sociale et ceux de la police municipale.

Quels sont les enjeux des collectivités en matière de protection des données ?

Le développement de **l'e-administration** constitue un levier majeur de la modernisation de l'action publique. De ce fait, les collectivités recourent de plus en plus aux technologies et usages numériques : téléservices, open data, systèmes d'information géographique, *cloud computing*, compteurs intelligents, réseaux sociaux, lecture automatique de plaques d'immatriculation, etc.

Par ailleurs, le nombre de **cyberattaques** ne cesse d'augmenter, et ce, quel que soit la taille des organisations visées.

De plus, **les citoyens sont de plus en plus soucieux** de la manière dont leurs données sont utilisées. À ce titre, la loi pour une République numérique est venue consacrer en octobre 2016 un droit à l'auto-détermination informationnelle que l'on retrouve posé à l'article 1er de la loi Informatique et Libertés : « *toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant* ».

Les nouveaux services numériques, pour qu'ils créent de la confiance auprès des administrés, doivent donc répondre aux exigences de protection des données dont **la sécurité** est une des composantes essentielles.

Enfin, la nécessité pour les collectivités de prendre en compte ces exigences est aujourd'hui d'autant plus importante que le règlement européen sur la protection des données, applicable à compter du 25 mai 2018, renforce encore les obligations en matière de transparence des traitements et de respect des droits des personnes, s'axe sur une logique globale de responsabilisation de l'ensemble des acteurs et crédibilise la régulation des « CNIL » en musclant considérablement leur pouvoir de sanction. Ainsi, outre des avertissements publics, elles pourront prononcer des amendes administratives allant jusqu'à 20 millions d'euros ou, pour une entreprise, 4% du chiffre d'affaires mondial.

En quoi le règlement européen sur la protection des données impacte-t-il les collectivités territoriales ?

- **Une logique de responsabilisation**

Si les grands principes déjà présents dans la loi Informatique et Libertés ne changent pas, **un véritable changement de culture s'opère**. On passe en effet d'une logique de contrôle a priori basé sur des formalités administratives à une **logique de responsabilisation** des acteurs privés et publics. Ce changement de posture devra se traduire par **une mise en conformité permanente et dynamique de la part des collectivités. Elles devront ainsi adopter et actualiser des mesures techniques et organisationnelles leur permettant de s'assurer et de démontrer à tout instant qu'elles offrent un niveau optimal de protection aux données traitées.**

Les organismes publics et privés auxquels les collectivités sous-traitent la mise en œuvre de tout ou partie de leurs traitements (ex. : prestataires de service hébergeant des données)

devront obligatoirement participer à la démarche de mise en conformité, en aidant celles-ci à satisfaire leurs diverses obligations, sous peine de sanctions.

- **La protection des données dès la conception et par défaut**

Les collectivités devront intégrer un nouveau principe de protection des données dès la conception (Privacy by design) du traitement et par défaut (Privacy by default).

Elles devront ainsi tenir compte le plus en amont possible, dès la phase de conception du produit, du service ou du traitement, de définition des outils qui seront utilisés et des paramétrages par défaut, des règles d'or de la protection des données. Il s'agira en particulier de minimiser à tout point de vue le traitement effectué.

Par exemple :

- *favoriser par principe les menus déroulants ou les cases à cocher plutôt que les zones de commentaires libres sur les formulaires de collecte et dans les bases de données internes, pour limiter dès le départ le nombre et la nature des données enregistrée*s ;
- *restreindre au maximum les droits d'accès informatiques aux données et les opérations susceptibles d'être réalisées ;*
- *pseudonymiser les données toutes les fois où leur exploitation sous une forme identifiante n'apparaît pas nécessaire à la satisfaction du besoin ;*
- *appliquer un mécanisme automatique de purge des données à l'issue de la durée de conservation nécessaire à la réalisation de la finalité.*

- **La gouvernance des données**

Avec le règlement, on assiste à un allègement considérable des obligations en matière de formalités préalables, puisque le régime déclaratif est totalement supprimé, pour rentrer dans l'ère de la gouvernance des données personnelles. Une bonne gouvernance nécessite toutefois une documentation continue des actions menées pour être en capacité de piloter et de démontrer la conformité. Les collectivités seront ainsi appelées à tenir un registre de leurs activités de traitement, à encadrer les opérations sous-traitées dans les contrats de prestation de services, à formaliser des politiques de confidentialité des données, des procédures relatives à la gestion des demandes d'exercice des droits, à adhérer à des codes de conduite ou encore à certifier des traitements.

Dans certains cas, pour les traitements à risques, elles devront effectuer des analyses d'impact sur la vie privée et notifier à la CNIL, voire aux personnes concernées, les violations de données personnelles.

La désignation d'un délégué à la protection des données est-elle obligatoire pour les collectivités ?

À compter du 25 mai 2018, la désignation d'un délégué à la protection des données (*Data protection Officer*), successeur du correspondant informatique et libertés (CIL) dont la désignation est aujourd'hui facultative, sera obligatoire pour les organismes et autorités publics, et donc pour les collectivités.

- **Missions**

Le délégué aura **pour principales missions** :

- d'informer et de conseiller le responsable de traitement de la collectivité ou le sous-traitant, ainsi que les agents ;
- de diffuser une culture Informatique & Libertés au sein de la collectivité ;
- de contrôler le respect du règlement et du droit national en matière de protection des données, via la réalisation d'audits en particulier ;
- de conseiller la collectivité sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ;
- de coopérer avec la CNIL et d'être le point de contact de celle-ci.

Dans l'exercice de ces missions, le délégué devra être à l'abri des conflits d'intérêts, rendre compte directement au niveau le plus élevé de la hiérarchie et bénéficier d'une liberté certaine dans les actions qu'il décidera d'entreprendre.

- **Expertise et moyens**

De plus, la collectivité devra s'assurer qu'il dispose **d'un niveau d'expertise et de moyens suffisants pour exercer son rôle de façon efficace**. Ainsi, le délégué devra :

- être désigné sur la base de ses connaissances spécialisées du droit et des pratiques en matière de protection des données ;
- être associé en temps utile et de manière appropriée à l'ensemble des questions Informatique & Libertés ;
- bénéficier des ressources et formations nécessaires pour mener à bien ses missions.

Dans ce contexte, la mutualisation de la fonction de DPO apparaît un enjeu essentiel pour les collectivités territoriales, notamment pour celles de petite taille.

À quel niveau envisager la mutualisation du délégué à la protection des données ?

Aujourd'hui, si les grandes collectivités ont déjà engagé cette démarche (2/3 des régions, la moitié des départements, 2/3 des métropoles, 1/3 des communautés urbaines, 1/10 des communautés d'agglomération), seulement 2% des communes ont désigné un correspondant. Pour ces collectivités, qui ont des préoccupations identiques, la mutualisation de la fonction semble tout à fait adaptée. Elle permet de limiter les coûts et de bénéficier de professionnels disposant des compétences et de la disponibilité nécessaires à un bon pilotage de la conformité.

- **Les structures de mutualisation informatique (SMI) et les centres de gestion**

Les structures de mutualisation informatique, spécialisées dans le développement de l'e-administration sur leur territoire, constituent une bonne solution de mutualisation de la fonction de délégué pour les collectivités. Ces structures portent très souvent le développement numérique des territoires, que ce soit à travers le réseau des infrastructures ou des services proposés (ex. : plateformes de téléservices), et proposent aux collectivités un accompagnement dans leur transition numérique.

Elles regroupent maîtrise d'ouvrage et maîtrise d'œuvre et c'est à leur niveau que les besoins des collectivités sont identifiés, que des progiciels sont développés, que les mesures de sécurité et paramétrages par défaut sont définis, et qu'éventuellement les données sont hébergées. Ayant vocation à se multiplier, elles couvrent déjà 50% des départements et permettent aux collectivités adhérentes de rationaliser les dépenses tout en optimisant les conditions juridiques, organisationnelles et fonctionnelles du déploiement d'outils numériques de gestion de leurs missions de service public.

Certaines de ces structures, telles que l'ALPI (Agence landaise pour l'informatique) propose déjà un service de CIL mutualisé aux communes, établissements publics et groupements de collectivités de leur ressort territorial. D'autres, telles que l'ADICO dans l'Oise (association pour le développement et l'innovation numérique des collectivités) ont commencé à travailler sur une offre de délégué mutualisé.

À noter aussi que des collectivités bénéficient dès à présent de CIL mutualisés au niveau de centres de gestion de la fonction publique territoriale (CDG11, CDG54, CDG60 et le CDG59).

- **Les établissements publics de coopération intercommunale (EPCI)**

Les communautés de communes, d'agglomération, les communautés urbaines et les métropoles, peuvent également proposer aux collectivités qui en sont membres les services d'un délégué mutualisé.

Enfin, sans aller jusqu'à mutualiser la fonction de délégué, les collectivités ayant les mêmes préoccupations peuvent opportunément travailler ensemble pour se préparer au mieux aux nouvelles obligations posées par le règlement européen. Les 12 départements de la région Nouvelle Aquitaine se sont ainsi engagés dans une telle démarche : identification des besoins des uns et des autres, définition d'un plan d'action comprenant différentes étapes, développement d'un outil commun d'information et de partage de connaissances, etc.

COMMENT LES COLLECTIVITÉS PEUVENT-ELLES SE PRÉPARER DÈS MAINTENANT ?

Sans attendre 2018, les collectivités peuvent d'ores et déjà désigner un correspondant informatique libertés ayant vocation à occuper ensuite la fonction de délégué à la protection des données. Le correspondant désigné pourra ainsi profité des nombreux ateliers d'information généralistes et thématiques proposés gratuitement aux CIL par la CNIL, ainsi que de son service dédié à l'accompagnement de ces professionnels dans leurs démarches de mise en conformité.

La liste des organismes ayant désigné un CIL est disponible sur data.gouv.fr elle référence notamment les collectivités territoriales ayant d'ores et déjà désigné un CIL, et permet d'identifier qui pourrait éventuellement mutualiser cette fonction.

La CNIL propose une méthodologie en 6 étapes pour se préparer et anticiper les changements liés à l'entrée en application du règlement européen le 25 mai 2018. La démarche permet d'accompagner les professionnels et de leur apporter une sécurité juridique maximale.

Quelles sont les différentes obligations qui incombent aujourd'hui aux collectivités territoriales en matière de sécurité et de protection des données ?

De nombreuses informations sont disponibles dans la rubrique « collectivités » du site, qui comprend notamment :

- **Les principes clés de la loi informatique et libertés avec des exemples dédiés aux collectivités ;**
- **Des informations sur l'encadrement des principaux traitements** (gestion de l'état civil, de la liste électorale, exploitation de systèmes d'information géographique, développement de téléservices, etc.)
- une méthodologie pour réaliser des analyses d'impact sur la vie privée et un catalogue de mesures à adopter pour les contrer ou limiter leurs effets est également disponible

Le respect de ces règles par les décideurs publics constitue un gage de sécurité juridique, en les protégeant notamment contre un risque pénal particulièrement important, un gage de sécurité informatique profitable à l'ensemble du patrimoine informationnel de la collectivité, ainsi qu'un vecteur de confiance et de valorisation de l'image de cette dernière auprès de toutes les personnes concernées par ses traitements (employés et administrés en particulier). Ainsi, si la conformité a un coût, elle doit surtout être perçue comme un investissement.

PIA

Vue d'ensemble des obligations et de la méthode

0.
Lancer un nouveau traitement

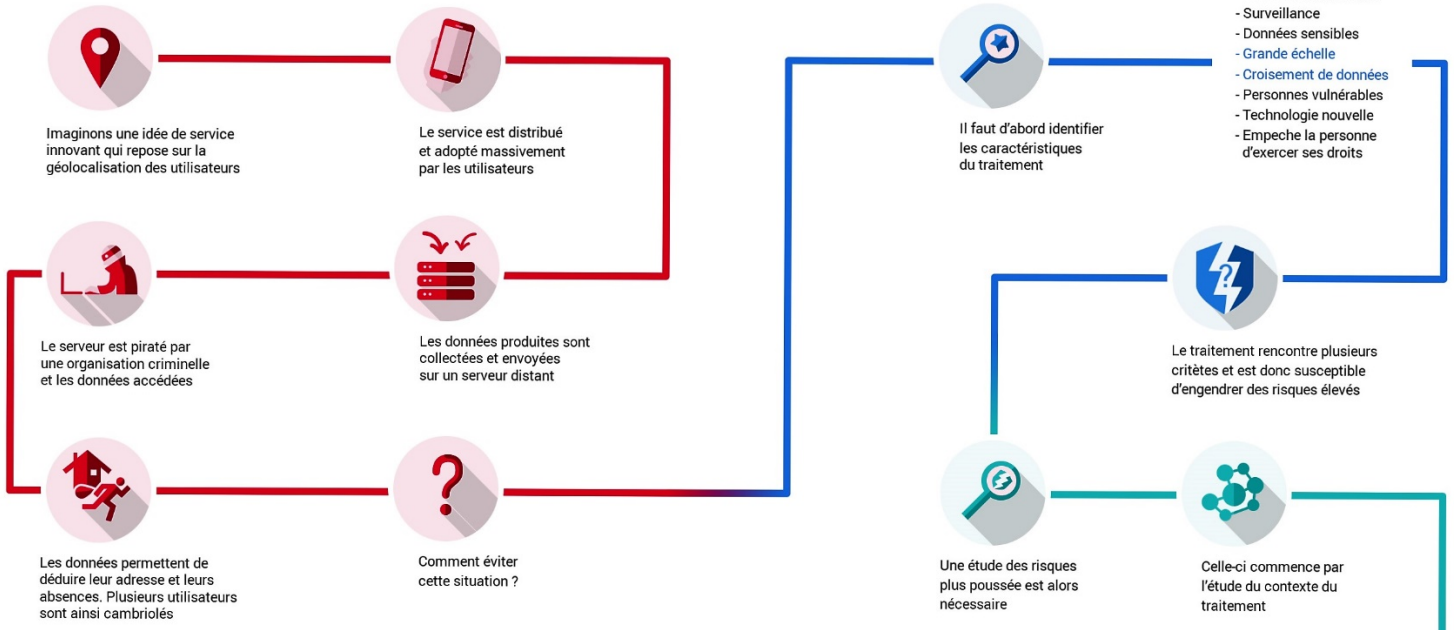
De nombreux services sont créés tous les jours dans le monde du numérique.

Qu'ils répondent aux besoins internes d'organismes ou à ceux de leurs clients, ces services reposent pour la grande majorité sur des traitements de données à caractère personnel.

Adressés à des groupes d'utilisateurs définis, ils collectent ces données à la volée lors de leur usage.

Stockées sur des serveurs, les données collectées sont vulnérables à différents risques : l'accès illégitime, la modification non désirée et la disparition.

Ces risques sont susceptibles d'avoir un impact important sur la vie privée des utilisateurs concernés.



1.
Qualifier le traitement

Ces risques sont indésirables, aussi bien pour le responsable de traitement que pour les utilisateurs du service.

Ainsi, avant de lancer un traitement, il est important d'en faire une première analyse afin d'en déterminer les risques qu'il est susceptible d'engendrer.

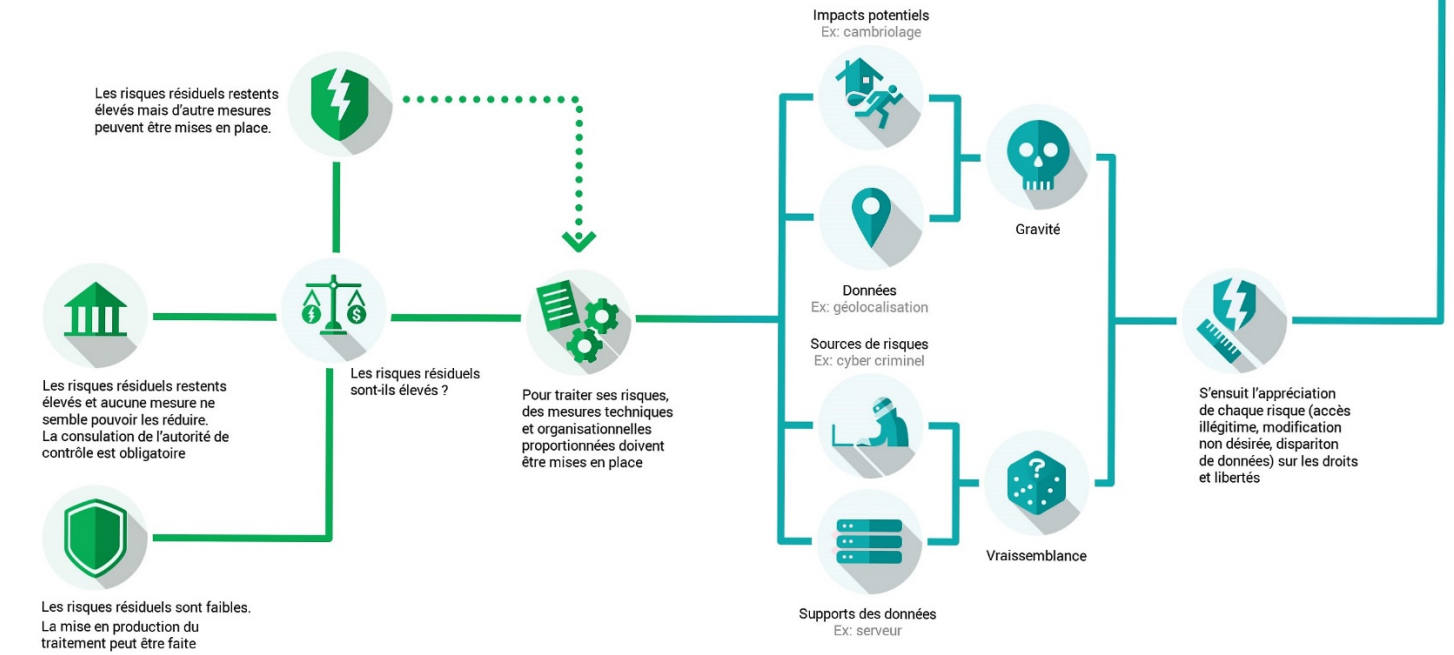
Plusieurs facteurs influencent la dangerosité d'un traitement comme par exemple le type de données traité.

En général, si deux des critères listés sont rencontrés, le traitement comporte probablement des risques importants sur la vie privée. Dans ce cas de figure, il est approprié de mener une *« analyse d'impact relative à la protection des données »*.

2.
Apprécier les risques vie privée

L'analyse établit tout d'abord le contexte dans lequel évolue le traitement, en posant, entre autre, les bases de son rôle et de son fonctionnement.

En complément de l'étude juridique consistant à évaluer la nécessité et la proportionnalité du traitement, il est nécessaire d'analyser chaque risque et d'estimer sa vraisemblance et sa gravité selon les impacts potentiels sur les droits et libertés, les données traitées, les sources de risques, et les vulnérabilités des supports de données.



3.
Traiter les risques

Une fois les risques identifiés, des mesures techniques et organisationnelles doivent être déterminées jusqu'à ce que les risques soient réduits à un niveau acceptable.

Si ça ne semble pas possible avec les moyens envisagés, l'autorité de contrôle doit être consultée.

Dans tous les cas, les mesures devront être appliquées avant la mise en œuvre du traitement.

RGPD : protéger les données à caractère personnel dès la conception des traitements

Publié le 28/02/2018 – Élisa Corazza et Yvon Goutal, Avocats, cabinet Goutal, Alibert et associés

LaGazette.fr - M. Gobert

Les collectivités territoriales constituent des responsables de traitements de données personnelles au sens du règlement général sur la protection des données (RGPD). Les dispositions du RGPD, qui imposent une protection accrue des données personnelles, entreront en vigueur le 25 mai 2018. Les collectivités devront notamment avoir intégré le principe de protection des données dès la conception ou « privacy by design ».

Comprendre les concepts de « privacy by design » et « privacy by default »

Le responsable du traitement est celui qui définit les finalités et moyens du traitement des données à caractère personnel [(1)]. Il lui incombe à ce titre, durant la phase de détermination des moyens, de concevoir des outils et règles d'organisation garantissant la protection des données personnelles. C'est le principe de « privacy by design » ou protection des données personnelles dès la conception des traitements, consacré à l'article 25 du règlement général sur la protection des données (RGPD) [(2)].

Par ailleurs, les moyens mis en œuvre devront assurer que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de la finalité spécifique de l'opération seront traitées. Autrement posé, l'utilisateur ne doit pas être obligé d'engager des démarches pour activer sa protection. C'est le principe de « privacy by default ».

Le RGPD n'édicte cependant pas de prescriptions techniques standard permettant de respecter ces deux concepts : le responsable doit être capable de démontrer qu'il a pris les mesures techniques et organisationnelles appropriées à sa situation. Celles-ci dépendent, pour chaque collectivité, de l'importance de ses moyens, et, pour chaque opération, de la sensibilité des données traitées, des finalités poursuivies et des risques que présente le traitement pour les droits et libertés des personnes physiques.

Le RGPD prévoit, du reste, la possibilité d'instaurer un mécanisme de certification du respect des principes de privacy by design et by default. En France, les labels octroyés par la Commission nationale de l'informatique et des libertés (Cnil), notamment de gouvernance, pourraient remplir cet office.

Anticiper la publication et la réutilisation

Lorsque les collectivités territoriales mettront en place de nouveaux traitements, elles devront tenir compte, le plus en amont possible, des principes clés de la protection des données [(3)]. Ce qui implique de concevoir des outils, non seulement en fonction des besoins des services utilisateurs, mais également des droits des usagers à l'accès aux documents administratifs et à la réutilisation des informations publiques.

En effet, avant d'être communiqués, les documents administratifs doivent être expurgés de tout secret protégé au titre des articles L.311-5 et L.311-6 du code des relations entre le public et l'administration (secret de la vie privée, secret industriel et commercial, etc.) [(4)]. Pour être publiés en ligne, mais aussi réutilisés, ils doivent en outre ne comporter aucune donnée à caractère personnel, c'est-à-dire permettant l'identification directe ou indirecte de personnes physiques [(5)].

Cependant, les administrations ne sont tenues de les communiquer et de les publier que s'il est possible d'occulter ou de disjoindre les mentions non communicables et non publiables [(6)] : la

Commission d'accès aux documents administratifs (Cada) considère qu'un document comportant un très grand nombre de mentions couvertes par un secret et dont l'occultation s'avérerait difficile pour l'administration peut être regardé comme non communicable [(7)].

Ainsi, afin de permettre l'exercice le plus effectif possible des droits de l'open data, les collectivités devront veiller à ce que leurs outils de traitement permettent de rendre facilement communicables, publiables et réutilisables les documents administratifs et les informations publiques qu'ils contiennent. Elles devront, par exemple, concevoir leurs bases de données de sorte que leur partie communicable puisse être aisément extraite par un traitement automatisé d'usage courant.

Attention, les outils préexistants sont également concernés : la Cada exige des responsables de traitements qu'ils engagent, avant l'entrée en vigueur du RGPD, des démarches de transformation progressive des outils déjà en place, telle la base de données Nausicaa.

Appliquer le principe de minimisation

Protéger les données personnelles, c'est d'abord en manipuler le moins possible. Cette règle de minimisation figure à l'article 5 1 c) du RGPD : seules celles à caractère personnel qui sont strictement indispensables au regard de chaque finalité spécifique du traitement doivent être traitées. Il ne s'agit donc plus pour les collectivités d'accumuler et de thésauriser à toutes fins utiles le plus d'informations possibles sur leurs administrés.

Le changement de paradigme est important : la collectivité n'est pas propriétaire des données à caractère personnel qu'elle collecte, elle n'en est que la gardienne, pour un temps limité et à une fin déterminée. La minimisation s'applique à tous les niveaux : quantité de données à caractère personnel récupérées, étendue de leur traitement, durée de conservation et accessibilité.

Concrètement, il convient de s'interroger au moment de la mise en place du traitement sur les données véritablement utiles pour l'objectif poursuivi, et lui seul, et d'exclure toute collecte superflue. Il est de plus interdit, par principe, de recueillir des données sensibles (origines raciales, religion, option politique, santé…) [(8)]. Ainsi, l'adresse et le numéro de téléphone des parents sont importants pour l'inscription d'un enfant dans un établissement scolaire, au contraire des numéros de Sécurité sociale et, a fortiori, de la confession religieuse.

Afin d'éviter toute collecte de données inutile, on réduira au maximum les zones de texte libre dans les logiciels de traitement, de type « commentaire » ou « bloc-notes », et on favorisera les menus déroulants ou les cases à cocher. La minimisation impose aussi de déterminer, en amont, la durée de conservation adéquate à la réalisation de l'objectif poursuivi. Il n'est pas utile, par exemple, de garder le curriculum vitae d'un candidat pour un stage pendant plusieurs années.

Il convient, enfin, de faire en sorte que, par défaut, les données à caractère personnel ne soient pas rendues accessibles à un nombre de personnes physiques supérieur à celui strictement nécessaire, tels que les dossiers « RH » des agents de la collectivité.

Pseudonymiser

Au nombre des mesures techniques et organisationnelles appropriées, destinées à mettre en œuvre les principes relatifs à la protection des données, figure la pseudonymisation [(9)]. Ce processus consiste à remplacer des informations (identifiants ou données à caractère personnel) par un pseudonyme, de telle façon qu'elles ne puissent plus être attribuées à la personne concernée sans avoir recours à des informations supplémentaires, conservées séparément. Le terme d'anonymisation est réservé aux opérations irréversibles.

On utilise celui de pseudonymisation si l'opération est réversible. Il faut garder à l'esprit que la seule pseudonymisation ne permet pas de sortir du champ d'application du RGPD, contrairement à l'anonymisation. Le RGPD recommande de mettre en œuvre cette mesure dès que possible, soit dès lors que l'exploitation des données sous une forme identifiante n'apparaît pas nécessaire à la réalisation de la finalité poursuivie.

Un exemple de la Cnil : « Une pseudonymisation limitant efficacement le risque de réidentification directe peut, ainsi, être effectuée en générant une clé secrète longue et difficile à mémoriser (une combinaison de caractères aléatoires), puis en appliquant une fonction dite à sens unique sur

les données (un algorithme de hachage à clé secrète, comme le HMAC) » [(10)].

Être exigeant avec ses sous-traitants

Dans l'idéal, les collectivités créeraient seules les outils de traitement adaptés à leurs besoins et conformes au RGPD, et les utiliseraient en autonomie. Ce qui éviterait de confier des données à caractère personnel à des tiers [(11)]. Dans la réalité cependant, rares sont les collectivités territoriales qui créent ce type d'outils. Elles sont même nombreuses à confier des traitements à des prestataires extérieurs : intégrateurs ou éditeurs de logiciels (utilisation d'Outlook comme progiciel de gestion des emails), entreprises de SSI (sécurité des systèmes informatiques) et autres prestataires de services informatiques (hébergement, maintenance, etc.).

Dans ce cas, en tant que responsables du traitement, elles ont l'obligation de s'assurer que leurs sous-traitants offrent les garanties suffisantes pour mettre en œuvre un traitement conformément aux exigences du règlement européen. Le RGPD recommande à cet égard de prendre en considération les principes de protection des données dès la conception et de protection des données par défaut dans le cadre des marchés publics [(12)].

Qu'une procédure de marché soit ou non nécessaire, il convient dans tous les cas de choisir avec soin ses prestataires et, pour ce faire, d'être notamment attentifs à leur méthodologie et leurs systèmes de sécurité. Un label de la Cnil, de type gouvernance des données, peut déjà constituer un indice sérieux : il garantit que le sous-traitant respecte le RGPD dans le cadre des traitements qu'il met en œuvre pour son propre compte. Il est ensuite indispensable d'introduire dans les contrats de sous-traitance des clauses garantissant le respect du RGPD.

Dans l'hypothèse, fréquente, où la collectivité emploie un progiciel (à bas coût, voire gratuit) et ne peut négocier son contrat, il lui est recommandé, pour limiter les risques, d'écrire à l'éditeur pour le mettre en demeure de se mettre en conformité avec le RGPD et de conserver cette preuve.

RÉFÉRENCES

- Règlement (UE) 2016/679 du Parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD).
- Livre III du code des relations entre le public et l'administration.

Notes

Note 01 Article 4, 7) du RGPD.
Note 02 Mise en œuvre du RGPD : comment documenter sa conformité
Note 03 Réaliser une analyse d'impact pour protéger les données en cinq étapes
Note 04 Article L.311-7 du code des relations entre le public et l'administration.
Note 05 Article L.312-1-2, ibid.
Note 06 Articles L.311-7 et L.312-1-2, ibid.
Note 07 avis Cada n° 20163729 du 15 décembre 2016.
Note 08 Article 8 de la loi n° 78-17 du 6 janvier 1978.
Note 09 Article 25 du RGPD.
Note 10 Fiche n° 10, « Sécurité des données », Cnil, juillet 2014
Note 11 Désigner un délégué à la protection des données au sein de sa collectivité en 6 étapes
Note 12 Considérant (78) du RGPD.

DOCUMENT 10

Sensibiliser et tester les attitudes des employés à la sécurité informatique

By Christophe Badot on février 14, 2018 Cybersécurité, Experts invités

Lors de la dernière étition du Mois Européen de la Cybersécurité en octobre dernier, l'une des actions phares de l'évènement a été le test effectué par le Ministère de l'Economie qui n'a pas hésité à procéder à une **fausse campagne de phishing** afin de sensibiliser ses propres employés à la sécurité. Résultat ? Sur 145 000 agents, plus de 30 000 ont cliqué sur le lien entre 10h et midi, soit un taux de clic de 20 %. De quoi rendre envieux la plupart des professionnels de l'emailing marketing.

Comme la majeure partie des professionnels de la sécurité le savent, **les pirates utilisent souvent des techniques assez peu sophistiquées pour pénétrer dans le système d'information des entreprises**. Les mots de passe faibles, vulnérables aux essais de force brute, ou les failles de logiciels qui n'ont jamais été supprimées constituent des vecteurs d'attaques simples. Et comme le démontre l'opération du Ministère de l'Economie, **le phishing offre une porte d'entrée des plus efficaces**.

En général, l'e-mail de phishing est conçu pour paraître officiel. Il semble souvent provenir d'une adresse légitime ou d'un nom de domaine qui se rapproche de l'original (varomis.com au lieu de varonis.com par exemple). L'objectif est de prendre les victimes par surprise alors qu'elles naviguent dans leur boîte de réception, puis de les pousser à cliquer sur un lien qui les dirigera vers un site web compromis (téléchargement d'un programme malveillant, d'un ransomware, récupération d'identifiants/mots de passe, etc.). Plus les pirates disposent de données sur leur « cible », plus un email de phishing à de chances de réussir.

Les pirates se concentrent souvent sur des cibles à forte valeur comme les cadres dirigeants. Ce genre d'escroquerie a déjà permis de duper des personnes situées au sommet de la hiérarchie, l'objectif le plus courant étant d'obtenir un accès privilégié à des informations confidentielles ou de propriété intellectuelle, et éventuellement des renseignements embarrassants.

Sensibilisation et pratique : clé de la sécurité

La sensibilisation est un moyen d'atténuer les attaques ciblant les dirigeants et les employés. Quelques entreprises à l'exemple du Ministère de l'Économie effectuent des tests plus ou moins réguliers visant à sensibiliser leurs employés et leur inculquer les bons réflexes. L'exercice est loin d'être inutile car au même titre que **sensibiliser les employés aux bons gestes en cas d'alerte** incendie, une telle procédure pourrait être répliquée sur

le plan numérique et faire partie d'un programme global de protection de la propriété intellectuelle.

Au-delà du phishing, **on pourrait également envisager une expérience similaire dans le cadre de scénarii de sécurité de fichiers sensibles**. Un responsable de la sécurité pourrait ainsi amorcer un dossier fréquenté du serveur de l'entreprise, par exemple avec un fichier au nom tentant du genre « *Hautement confidentiel : projet de fusion* » [ou tout autre appât au choix], lui donner des permissions d'accès très larges, et voir ce qu'il se produit. Il faudra bien entendu être en mesure de pouvoir tracer l'ensemble des accès au dossier.

47 % des entreprises laissent au moins 1 000 fichiers sensibles ouverts à tous les employés

Pourquoi élargir à ce type de tests ? Les résultats du dernier *« Varonis Data Risk Report »,* mettait en avant le fait que **47 % des entreprises laissent au moins 1 000 fichiers sensibles ouverts à tous les employés** et une récente étude du Ponemon Institute, soulignait de son côté que 62 % des utilisateurs finaux affirment avoir accès à des données de l'entreprise qu'ils ne devraient probablement pas pouvoir consulter. On imagine facilement les risques encourus en cas de piratage, d'infection par un ransomware ou si un employé à de mauvaises intentions.

Mais **les risques pourront également aller bien au-delà de la simple atteinte aux données puisqu'à compter de mai 2018**, le nouveau Règlement Général sur la Protection des Données (RGPD) constituera une loi uniforme dans l'ensemble de l'UE et comprendra une obligation de notification des violations de 72 heures.

La nouvelle législation clarifie la notion de violation de données. Il s'agit de « *la destruction, la perte ou l'altération accidentelle ou illicite, la divulgation ou l'accès non autorisés aux données à caractère personnel transmises, stockées ou autrement traitées* ». Cela signifie que **le simple accès est considéré comme une violation** et que les ransomware qui chiffrent les données personnelles nécessiteront une notification aux individus et organisme concernés. Et les sanctions en cas d'infraction à cette obligation de déclaration font courir à l'entreprise le risque de se voir infliger d'importantes amendes administratives pouvant aller jusqu'à 20 millions d'euros, ou, dans le cas d'une entreprise, de 2 à 4 % du chiffre d'affaires annuel mondial.

Sous cet angle il semble évident, qu'au-delà de toutes les mesures de sécurité que pourront prendre les entreprises, il devient essentiel pour ces dernières de sensibiliser leurs employés et de s'assurer que les principes inculqués seront « *bien intégrés* ». **Pouvoir tester les acquis des employés régulièrement au travers de scenarii différents va donc devenir un élément primordial de la sécurité.**

DOCUMENT 11

Vie privée et cyber-risques : la sécurité dans la *smart city*

Sécurité
Nelly MOUSSU

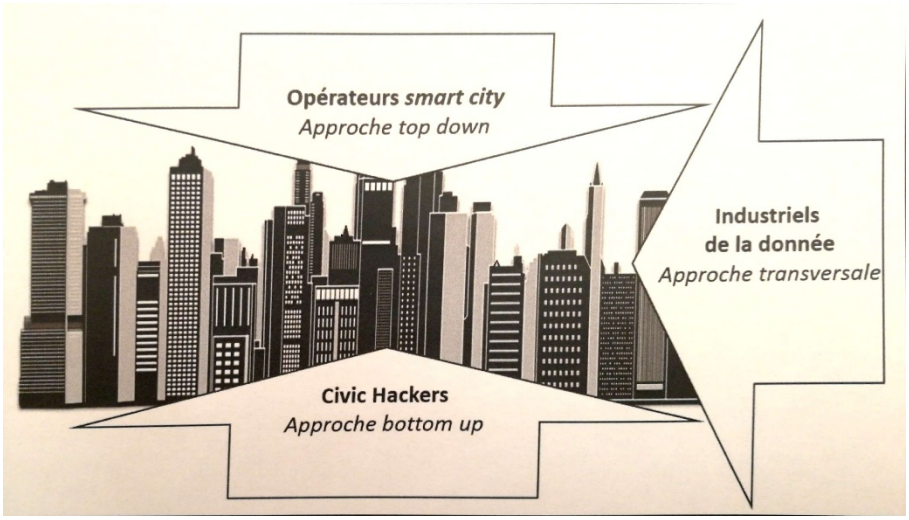
Dans le cadre de son cycle d'ateliers dédié aux smart cities, France Stratégie a convié Régis Chatellier de la CNIL et Yves Verhoeven de l'ANSSI pour aborder les enjeux de la vie privée et les impacts des cyber-risques dans la ville intelligente. Et leur constat n'est pas des plus rassurant : les collectivités ne maîtriseraient pas suffisamment ces sujets.

France Stratégie organise un cycle d'ateliers dédié aux smart cities. Au fond à droit Régis Chatellier de la CNIL et à sa gauche Yves Verhoeven de l'ANSSI.

Équipées de capteurs collectant des données, s'appuyant sur des systèmes d'information pour optimiser leurs services, favorisant un usage croissant du digital, les *smart cities* sont de plus en plus connectées. Le revers de la médaille ? L'augmentation des risques de sécurité liés au numérique. Afin de préserver le fonctionnement de la ville et de ses services, mais aussi de protéger les données personnelles de leurs administrés, les collectivités se doivent d'agir. Or, ces sujets restent aujourd'hui à la marge de leurs préoccupations.

L'enjeu des données personnelles

Du côté des données, Régis Chatellier, chargé des études innovation et prospective à la CNIL (Commission nationale de l'informatique et des libertés), note une évolution de l'approche *smart city.* Elle a commencé par la sollicitation d'un seul opérateur technique pour superviser une ville. Ensuite est venue la *Civic Hackers*, une ville dans laquelle les citoyens produisent eux-mêmes les données pour développer des services. Enfin une approche plus transversale, portée par les grands industriels, est en train d'émerger. *« L'entreprise Waze demande actuellement aux villes leurs données, notamment celles concernant les travaux de voirie,* cite en exemple Régis Chatellier. *Ces informations, complémentaires à celle que la société collecte auprès des citoyens, permettent d'améliorer son offre de service. »*



Un service qui se substitue à celui que pourrait proposer une commune pour répondre aux attentes de ses administrés. *« Les villes moyennes n'ayant pas les moyens de développer leur propre plate-forme, elles sont tentées d'accepter cette proposition de partage des données »* indique le représentant de la CNIL. Dans ce contexte se posent les questions du consentement citoyen, de l'anonymisation des informations, de l'éthique des algorithmes ou encore de la souveraineté des données... « *On doit pouvoir faire valoir ses droits sur ses données, peu importe qui les collecte ou le lieu où elles sont stockées »* plaide Régis Chatellier.

Le risque cyber

L'autre volet sécuritaire de la *smart city*, lié aux nouvelles technologies, est le risque cyber. *« Il se définit par la rencontre entre les vulnérabilités d'un système d'information, les menaces générées par un ou des agents malveillants et les impacts potentiels »* indique Yves Verhoeven, sous-directeur des relations extérieures et coordination à l'ANSSI (Agence nationale de la sécurité des systèmes d'information). Il concerne aussi bien les opérateurs d'importance vitale du pays, que les futurs opérateurs d'importance essentielle (définis par la directive européenne de juillet 2016 sur la sécurité des réseaux et de l'information, et dont les dysfonctionnements sont susceptibles d'impacter fortement l'économie française) ou que les collectivités.

Dans une *smart city*, le risque cyber est accru par la présence d'objets connectés, piliers des services innovants proposés par la ville. *« Ils font potentiellement peser un risque sur la sûreté des personnes, accru par l'interconnexion des services,* souligne Yves Verhoeven. *Les services sont en effet portés par des systèmes d'information distincts mais interconnectés pour mettre en relation les feux de signalisation, l'éclairage, la distribution d'énergie, etc. »* Rassemblées, les données collectées permettent par exemple de définir des itinéraires alternatifs afin de fluidifier le trafic routier et, par conséquent, de réduire les émissions de CO^2. Un enjeu, parmi d'autres, dans la ville intelligente.

Or, si le risque cyber peut se maîtriser, *« il est particulièrement complexe à appréhender pour la smart city et il est nécessaire qu'une gouvernance soit mise en place pour traiter ce sujet, y compris par les collectivités* » insiste Yves Verhoeven. Mais les villes n'ont pas toujours les compétences ou les moyens financiers pour faire avancer ce sujet. L'ANSSI n'a d'ailleurs pas connaissance aujourd'hui qu'un projet *smart city « ait entamé une prise en compte du risque cyber à son juste niveau »*. Loin d'être fataliste face à cette situation, l'institution a commencé à déployer des agents sur le terrain pour sensibiliser les collectivités à ces questions. La CNIL œuvre en parallèle pour accompagner les communes de plus de 3 500 habitants sur l'anonymisation des données, une initiative inscrite dans le cadre des démarches *Open Data* qui leur seront obligatoires en 2018.

DOCUMENT 12

CNIL. *Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles*

Entrée en vigueur de la nouvelle loi Informatique et Libertés

04 juillet 2018

La loi n° 2018-493 du 20 juin 2018, promulguée le 21 juin 2018, a modifié la loi Informatique et Libertés afin de mettre en conformité le droit national avec le cadre juridique européen. Elle permet la mise en œuvre concrète du Règlement général sur la protection des données (RGPD) et de la Directive « police-justice », applicable aux fichiers de la sphère pénale. La lisibilité du cadre juridique national sera améliorée par une ordonnance qui sera prise dans un délai de six mois.

La nouvelle loi Informatique et Libertés permet l'application effective des textes européens, qui représentent un progrès majeur pour la protection des données personnelles des citoyens et la sécurité juridique des acteurs économiques.

Elle dote notamment la CNIL des pouvoirs nécessaires à l'exercice de ses missions, dans un contexte marqué par la reconnaissance de nouveaux droits aux citoyens et le renforcement de la responsabilité des opérateurs.

Elle organise l'articulation nécessaire des procédures internes de la CNIL aux nouveaux mécanismes de coopération européenne.

Elle exerce certaines des « marges de manœuvre nationales » autorisées par le RGPD, transpose en droit français la Directive « police-justice » et modifie certaines de ses dispositions pour les rapprocher de la lettre du RGPD.

La bonne compréhension du cadre juridique suppose de combiner désormais les deux niveaux, européen et national. Le RGPD s'applique directement en droit français : il remplace sur de nombreux points (droits des personnes, bases légales des traitements, mesures de sécurité à mettre en œuvre, transferts, etc.) la loi nationale. Sur d'autres points (les « marges de manœuvre nationales »), la loi Informatique et libertés reste en vigueur et vient compléter le RGPD : il s'agit par exemple du traitement des données de santé ou des données d'infraction, de la fixation à 15 ans du seuil d'âge du consentement des mineurs aux services en ligne, des dispositions relatives à la mort numérique, etc. Enfin, la loi nationale reste pleinement applicable pour tous les fichiers « répressifs », qu'il s'agisse de la sphère pénale ou du domaine du renseignement et de la sûreté de l'État. De nombreuses dispositions spéciales sont prévues en ces matières.

Une ordonnance de réécriture complète de la loi Informatique et Libertés est prévue, dans un délai de six mois, notamment afin de résoudre ces difficultés de lisibilité de ce cadre juridique composite. Dans l'attente, il convient de prêter une attention particulière au cadre juridique applicable à chaque traitement.

Le droit national doit également être complété par un nouveau décret d'application de la loi Informatique et Libertés pour achever la mise en conformité du droit national au cadre juridique européen. Ce décret, sur lequel la CNIL a été saisie pour avis, devrait être publié dans les prochaines semaines. Il permettra de fixer plus précisément les procédures de traitement par la CNIL des différents dossiers dont elle a la charge et de préciser certaines dispositions de la loi.

La CNIL rappelle enfin la nécessité d'adopter ce décret et cette ordonnance dans les plus brefs délais, afin de rendre le nouveau cadre juridique plus lisible pour les professionnels et les citoyens.