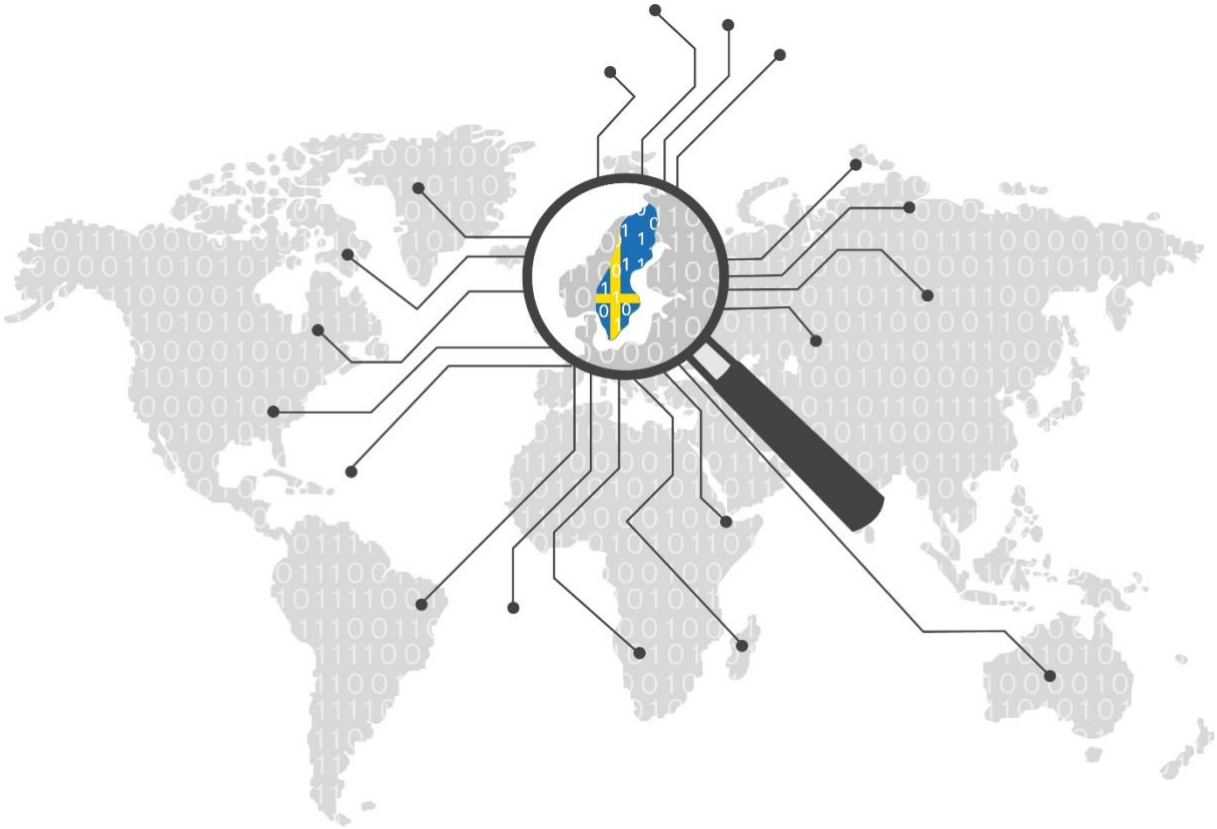

Livre blanc

Service public et informatique en nuage : risques, intérêt et marche à suivre

Försäkringskassan

Service public et informatique en nuage : risques, intérêt et marche à suivre. (Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt) No. de dossier de la Föräkringskassan : 013428-2019

Version: 1.0

Date : 18.11.2019

Table des matières

Sommaire

Tout comme la plupart des administrations suédoise, l'Agence suédoise de la sécurité sociale bénéficie des avantages des services numériques en ligne, aussi appelés services cloud. De tels services ont, dans de nombreux cas, accéléré la mise à disposition des services et sécurisé l'accès aux informations pour un coût raisonnable.

Plusieurs États, dont les États-Unis, la Chine et l'Inde, sont désormais dotés d'une législation qui autorise leurs autorités à prendre connaissance, à certaines conditions, des données et des renseignements stockés chez les fournisseurs de services dépendants de leur juridiction, même si les données en question sont à l'étranger. C'est dans ce contexte qu'est né le débat sur la légalité et la conformité au regard du droit suédois et européen de l'utilisation des services cloud aujourd'hui disponibles. La Försäkringskassan constate qu'il existe des cas, aussi bien dans la législation suédoise que dans le droit européen, qui interdisent aux autorités suédoises d'utiliser certaines solutions cloud du secteur privé à des fins d'administration de données confidentielles ou personnelles si le fournisseur de services est concerné par une législation de ce type.

Nous estimons toutefois que le débat suédois a quasiment ignoré une question tout à fait centrale, à savoir, s'il était pertinent que les administrations suédoises délèguent le contrôle des données des services publics à des acteurs privés voir même à des pays étrangers. Ajoutons à cela les différents aspects liés à la sécurité de la gestion informatique des données. Nous pouvons citer par exemple un accroissement général des vulnérabilités, des risques d'intrusion de personnes non autorisées, la difficulté de contrôler le personnel ainsi que la difficulté de proposer des analyses de risques et de vulnérabilité appropriées.

La Försäkringskassan ne transmettra pas l'administration de ses systèmes numériques stratégiques à des entreprises privées placées sous la juridiction d'un État dont la législation est abordée ci-dessus. Pour ses systèmes informatiques, comme par exemple dans le cas des activités sensibles, l'objectif de l'Agence suédoise de la sécurité sociale est de mettre en place une exploitation informatique proposée par l'État.

Pour parer nos activités de service public aux cyberattaques, préserver l'intégrité privée et réduire notre dépendance vis-à-vis des services disponibles, il est nécessaire que la Suède établisse une stratégie inter-administrative ainsi qu'un plan d'action de souveraineté numérique à long terme.

Pour que les administrations suédoises puissent continuer à bénéficier de toutes les possibilités de la numérisation, nous devons, par une interopérabilité sur le plan national et européenne faire en sorte que les services privés que nous choisissons d'utiliser soient adaptés à nos besoins et aux législations en vigueur : ces services doivent maintenir un niveau de sécurité qui nous permette de conserver la maîtrise de nos activités et de nos informations. Ainsi, nous pourrons bénéficier de la puissance de l'innovation et de l'efficacité des services proposés par les prestataires informatiques privés, tout en sécurisant les intérêts numériques de la Suède.

Contexte

Le calendrier numérique décidé par le gouvernement suédois souligne l'importance d'une action responsable des acteurs privés et publics. Les systèmes numériques doivent être sûrs et l'intégrité des personnes doit être préservée. Le gouvernement souligne aussi une aggravation possible de la vulnérabilité, résultant d'une dépendance technologique accrue, et note que la confiance du public repose sur la sécurité des services d'information.[1]

Les services cloud sont de plus en plus utilisés au sein des administrations suédoises. Dans une enquête effectuée en 2018, une grande partie des autorités suédoises ont répondu qu'elles utilisaient au moins un service cloud appelé public et développé par un prestataire privé.[2]

---

[1] Ministère suédois de l'innovation et de l'industrie : *Med medborgaren i centrum – Regeringens strategi för en digitalt samverkan statsförvaltning* (Le citoyen cœur des administrations : stratégie gouvernementale pour une coopération numérique des administrations publiques) (N1012 :37).

[2] Voir Annexe 2. Définitions et conditions d'utilisation des services cloud. Voir Annexe 2, un regard historique sur l'externalisation des services de l'administration publique et l'ouvrage de Hellberg, Islam, Karlsson, *Säkerhet vid molnlösningar* (La sécurité des solutions cloud), Université d'Örebro *[Suède]* et Autorité nationale suédoise pour la protection civile MSB, page 25.

Objectif

Dans le présent document, nous commencerons par compiler les données factuelles nécessaire à la compréhension de l'utilisation, par la Försäkringskassan, des services cloud publics proposés par des acteurs privés. Ce recueil nous aidera à poser les bases d'une prise de position correctement fondée sur les conditions d'utilisation de ces services cloud. Nous ne prendrons pas position sur les risques liés à d'autres modèles ou technologies de partage de l'information. Bien que ce Livre blanc concerne les activités de la Försäkringskassan, nous espérons fournir un soutien aux différents organismes publics exerçant des activités que nous appelons de portée sociétale. Nous espérons aussi que ce document pourra éclairer ses lecteurs sur la manière dont la Suède perfectionne la maîtrise des technologies de l'information au sein des services publics et que l'utilisation de ces technologies puisse prendre une place plus prépondérante qu'aujourd'hui.

Le concept du Livre blanc est utilisé par différentes organisations, dans de nombreux domaines et notamment au sein de l'Union européenne pour formuler idées et ambitions pour un champ d'application spécifique. Cette notion convient à ce que nous désirons accomplir dans cet ouvrage. Dans ce document, nous prenons position à l'égard de l'utilisation par l'Agence suédoise de la sécurité sociale, des services cloud proposés par différents acteurs privés et souhaitons ainsi que son contenu puisse contribuer à une discussion approfondie et élargie sur un aspect que nous trouvons d'importance cruciale pour toute notre société.

Les conclusions que nous donnerons à la fin de ce document seront, en fonction de leur pertinence, progressivement intégrées dans nos documents internes, tant bien stratégique, qu'administratif.

Nous concentrons cet inventaire et notre analyse sur les activités que nous qualifions d'activités de portée sociétale. Notre analyse révèle un besoin de sécuriser aussi bien les activités importantes pour la société que des fonctions qui ne sont pas directement concernées par cette définition mais dont les activités nous semblent importantes et dont la société est dépendante. Grâce à une définition élargie des activités des services publics, nous pourrons par ailleurs enrichir les discussions et nous baser sur une perspective systémique des fonctions dont la Suède est aujourd'hui dépendante.

Les défis de la mise en place des services cloud se concernent plutôt la manière dont le service est agencé, technologiquement et contractuellement. Le service public suédois est toutefois vivement intéressé par l'utilisation de services cloud publics internationaux proposés par des entreprises privées.[8]

Compte tenu du contexte international et de l'état actuel de la situation globale, nous traiterons principalement dans ce Livre blanc, les problèmes pouvant survenir dans le cas où une administration utiliserait un service cloud public fourni par des prestataires privés. Notre analyse pourra dans certains cas également être appliquées à d'autres solutions de services cloud voir même à d'autres formes d'organisation informatique.

[8] Voir également ci-après, Annexe 2.

Le débat autour du CLOUD Act

Du point de vue de la souveraineté juridique, il est évidemment important que les conditions dans lesquelles les autorités américaines réclament l'accès aux données stockées en dehors des États- Unis soient légalement définies.[21] Les grands fournisseurs de services cloud trouvent aussi que le CLOUD Act apporte un équilibre raisonnable entre les droits des individus et les besoins des autorités de lutte contre la criminalité.[22] Pourtant, les avis divergents ne manquent pas : un bon nombre d'entreprises américaines du secteur des technologies de l'information redoutent que le risque de conflits normatifs potentiels et l'absence d'accord entre les États-Unis et l'Union européenne sur l'accès aux données des autorités anticriminalités constitue un risque pour les intérêts commerciaux américains en Europe.[23]

De sérieuses critiques ont aussi été formulées quant à la protection et le respect des droits de l'homme. Le Conseil des barreaux européens estime que le CLOUD Act ne satisfait pas la norme européenne minimale fixée par la Cour européenne des droits de l'homme et la Cour de justice de l'Union européenne concernant la surveillance électronique des États de leurs citoyens.

Plusieurs organisations indépendantes des droits de l'homme soulignent aussi que la protection des droits humains est bafouée à partir du moment où l'exécutif américain dispose du droit de passer des accords internationaux sans examen préalable du Congrès. Ces organisations affirment aussi que le CLOUD Act accentue le risque d'accords passés avec certains États connus pour leurs infractions aux droits de l'homme. Les conditions d'application de cette législation accroissent aussi le risque d'accès, par ces États, à des informations à des fins anti-démocratiques.[24]

Le Comité Européen de la Protection des Données[25] et le Contrôleur européen de la protection des données[26] ont fait remarquer que le CLOUD Act donne aussi la possibilité aux juridictions concernées d'exiger des métadonnées des prestataires de services. Ces institutions soulignent aussi qu'une demande en vertu du CLOUD Act n'est pas obligatoirement précédée d'une enquête judiciaire ou bien encore d'une véritable présomption de preuve. Tel est le cas, par exemple, lorsqu'il s'agit d'une sommation administrative ou d'une sommation de grand jury.[27] Si les États- Unis passent une convention avec un pays tiers, le pays concerné pourra surveiller en

---

[21] Voir par exemple : Ministère américain de la justice : *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act,* White Paper, avril 2019, Microsoft, *Molntjänster och säkerhet* (Services cloud et sécurité), et Évaluation du Conseil des barreaux européens (CONSEIL DES BARREAUX EUROPÉENS CCBE).

[22] Voir par exemple Punke Michael, *AWS [Amazon Web Services] and the CLOUD Act, AWS Security Blog*, 27.05.2019.

[23] ACT - The App Association et autres, Lettre ouverte au ministre de la justice Barr, 21.06.2019.

[24] Lettre au Congrès américain de 24 organisations, dont Amnesty International États-Unis, Electronic Frontier Foundation et Human Rights Watch, 12.03.2018.

[25] Le Comité Européen de la Protection des Données (EDPB) est un organe de l'Union européenne composé notamment de représentants de l'autorité de protection des données de chaque État membre. La mission de l'EDPB est notamment de promouvoir une application cohérente de la législation de protection des données de toute l'Union. Dans cadre de ce travail, l'EDPB publie notamment des directives pour l'interprétation des notions fondamentales du RGPD.

[26] Le Contrôleur européen de la protection des données (CEPD) surveille le traitement des données à caractère personnel au sein des institutions et organes de l'Union européenne. En émettant notamment des conseils, en traitant les réclamations et en effectuant des enquêtes, le CEPD protège le droit des particuliers à protéger leur vie privée.

[27] *Administrative subpoena* ou *grand jury subpoena*.

Publicité et confidentialité

La confidentialité suppose l'interdiction de divulguer une information, que ce soit oralement, par divulgation de documents publiques ou tout autre manière qui soit. Si une mention de confidentialité concerne un quelconque renseignement, ce document est soumis au secret. [37]

Avant qu'une autorité suédoise n'autorise un prestataire de services à accéder à des données confidentielles, doit notamment pris en en compte la loi suédoise sur la publicité et la confidentialité No. 2009 : 400 et l'autorité doit s'assurer que ces données soient divulguées dans le cadre de ladite loi. Le groupe d'experts juridiques du programme de coopération électronique (dénommé ci-après eSam) a rédigé, en 2018, un avis juridique sur la notion de divulgation lié à l'utilisation de services cloud soumis à une législation étrangère.[38] Cet avis a été complété en septembre 2019. Pour estimer si des informations confidentielles seront considérées comme divulguées à partir du moment où elles seront accessibles à un prestataire de service, eSam estime que la législation suédoise sur la confidentialité nécessite une approche en deux étapes.

Il faut tout d'abord examiner si le prestataire de services, en vertu du contrat passé avec le donneur d'ordre, a le droit ou non de prendre connaissance et/ou de transmettre des données techniquement accessibles au fournisseur. Cela signifie qu'il doit exister, dans le contrat, une condition impérative relative à la confidentialité et assortie de sanctions pour le fournisseur. Le fournisseur ne doit pas non plus être concerné par des réglementations étrangères l'obligeant à fournir des données sans examen préalable de la loi sur la confidentialité ou tout autre législation du droit suédois l'autorisant à transmettre ces données. Si cette première condition est remplie, la deuxième étape consiste en une analyse des circonstances dans lesquelles il serait peu probable que le prestataire de service accède ou transfère les données.

En cas de défaillance de l'une de ces deux conditions, les données concernées sont considérées comme immédiatement divulguées dès qu'elles sont accessibles par le prestataire de services. [39] Si les données sont confidentielles, il est, dans ce cas, nécessaire que l'autorité qui divulgue les données soit autorisée par la loi à produire ces données.

En 2019, l'Agence nationale de services juridiques, financiers et administratifs, Kammarkollegiet, était en accord avec l'estimation d'eSam.[40] Kammarkollegiet affirme aussi qu'il n'est pas compatible avec la loi sur la publicité et la confidentialité qu'un prestataire de services mandaté par une autorité suédoise remette des données confidentielles à une autorité étrangère en vertu du CLOUD Act ou d'une législation semblable. Il n'existe en effet aucune prescription ou ordonnance légale particulière qui autoriserait une telle action. Il n'est pas non plus possible dans un tel cas de s'assurer qu'une donnée ait été remise à une autorité suédoise, ni d'assurer que les

---

[37] Chapitre 3, article 1 de la loi suédoise sur la publicité et la confidentialité.

[38] eSam est un programme pour l'interopérabilité entre 23 autorités administratives subordonnées au gouvernement et aux municipalités et conseils généraux suédois, voir www.esamverka.se.

[39] eSamverkansprogrammet, *Rättsligt uttalande om röjande och molntjänster*, (Avis juridique concernant la divulgation et les services cloud) VER 2018:57, 23.10.2018, ainsi que eSamverkansprogrammet, *Kompletterande information om molntjänster* (Informations complémentaires concernant les services cloud) 20.09.2019.

[40] Agence nationale de services juridiques, financiers et administratifs Kammarkollegiet, *Förstudierapport Webbaserat kontorsstöd*, (Étude préliminaire concernant le soutien bureautique par Internet), page 35.

intérêts suédois aient été préservés.[41] Kammarkollegiet a aussi constaté qu'une autorité suédoise qui laisserait des entreprises soumises à une réglementation semblable au CLOUD Act gérer des données confidentielles donnerait en priorité raison à la réglementation étrangère plutôt qu'à la législation suédoise.[42]

D'autres acteurs du marché avancent cependant qu'un nombre restreint d'affaires relatives à la diffusion de données stockées en dehors des frontières des États-Unis ont été soumises au CLOUD Act et participent ainsi à l'élaboration d'une opinion différente que celle que nous venons d'avancer. Ces acteurs affirment qu'il faut nuancer la notion de divulgation et que notamment le chiffrement et la localisation de halls des serveurs déplace la problématique du débat.[43] L'Association des collectivités territoriales suédoises (SKL) dit, pour donner suite à la position d'eSam, que les services cloud du marché privé, même ceux des sociétés étrangères, sont un élément indispensable à la numérisation.

La SKL estime aussi que cette évolution est maintenant freinée à cause des inquiétudes et incertitudes juridiques relatives à ce débat. La SKL a aussi exprimé des craintes concernant les investissements déjà effectués par une grande partie des municipalités et régions de Suède dans des services cloud privés.[44] En ce qui concerne la notion de divulgation, la SKL a aussi évoqué un jugement de la Cour suédoise du travail Arbetsdomstolen 2019 qui rappelle que les données en elles-mêmes ne sont pas considérées comme divulguées même si elles sont transmises à des personnes étrangères non autorisées.[45]

---

41 Voir chapitre 8, article 3 de la loi suédoise sur la publicité et la confidentialité.

42 Kammarkollegiet, *Förstudierapport Webbaserat kontorsstöd,* (Étude préliminaire concernant l'assistance bureautique en ligne), pages 32 et 33.

43 Voir notamment Microsoft, *Molntjänster och säkerhet* (Services cloud et sécurité), Services cloud et sécurité, Microsoft, Municipalités et conseils généraux de Suède et autres. Séminaire ouvert à Almedalen en 2019, le CLOUD Act – obstacle ou non, ainsi que : Fredrik Blix et Richard Brolin, *Grönt ljus för kommuner, regioner et statliga myndigheter att överväga molntjänster* (Feu vert pour les services cloud pour les municipalités, les régions et les autorités publiques), (Feu vert pour les services cloud pour les municipalités, les régions et les autorités publiques, Cybercom Group, 04.07.2019.

44 Association des collectivités territoriales suédoises (SKL), *Ställningstagande om informationshantering i vissa molntjänster* (Prise de position sur la gestion des informations dans certains services cloud), dossier No. 19/00087, 12.04.2019.

45 Voir Association des collectivités territoriales suédoises (SKL), *Molntjänster och konfidentialitetsbedömning* (Services cloud et appréciation de confidentialité) page 13. L'affaire est AD 2019 No. 15. La question centrale de cette affaire était de savoir s'il existait des motifs légaux lors de la mise à ban l'ancien directeur général de la Direction suédoise des transports Transportstyrelsen. L'une des questions traitées concernait l'État et sa capacité à établir un lien entre la divulgation de données personnelles et confidentielles à deux techniciens de stockage considérés comme non autorisés, les circonstances dans lesquelles ces deux personnes ont eu accès ces données et les accusations de négligences à l'encontre du directeur général conformément au chapitre 19 article 9 du code pénal suédois.

La protection des données

La diffusion vers un pays tiers de données à caractère personnel stockées au sein de l'Union européenne s'applique bien à la nature des données à caractère personnel. Les conditions dans lesquelles un tel procédé est autorisé sont notamment réglementées par le 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), qualifier ci- après RGPD. Avant qu'une autorité suédoise ne donne accès à un prestataire de services à des données à caractère personnel, l'autorité doit examiner si une telle diffusion représenterait un risque d'infraction au RGPD.

Selon les appréciations du Comité Européen de la Protection des Données (EDPB) et du Contrôleur européen de la protection des données (CEPD), le RGPD n'autorise qu'exceptionnellement et ce dans des conditions juridiques particulière les cas où des données à caractère personnel seraient diffusées à un pays étranger et ce en vue d'une quelconque conformité au CLOUD Act. Il ne s'agit là que de certaines situations exceptionnelles dans lesquelles la protection des intérêts des personnes concernés nécessiteraient la diffusion des données. Le Comité Européen de la Protection des Données a aussi affirmé que, dans les cas où il existerait au préalable un contrat international d'entraide judiciaire, les entreprises de l'Union européenne doivent en général rejeter toutes demandes directes et renvoyer l'autorité du pays concernée audit contrat.[46]

Un(e) responsable de la gestion des données à caractère personnel ou tout autre employé(e) préposé(e) aux données à caractère personnel qui, en infraction au RGPD, divulguerait aux autorités d'un pays étranger risquent une condamnation à des pénalités administratives considérables. Il existe cependant aussi un risque de sanctions juridiques aux États-Unis, dans les cas où une exigence du CLOUD Act ne serait pas satisfaite. Cela signifie en pratique, qu'un prestataire de services mandaté par une autorité suédoise peut être confronté à un conflit entre le droit communautaire européen et la législation américaine.[47]

Une autorité suédoise ne sera probablement pas responsable des données à caractère personnel si ces données étaient diffusé par un acteur homologué, par exemple un prestataire de services qui transmettrait ce type de données à un pays étranger et ce, en infraction au contrat.[48] En tant que responsable des données à caractère personnel, l'autorité a cependant l'obligation de recourir à des acteurs dont les garanties sont suffisantes et qui garantissent le respect des droits des personnes concernées à être protégées en conformité au RGPD.[49] Une autorité désireuse d'avoir recours à des services clouds doit donc veiller à ne pas s'engager auprès de prestataires de services susceptible d'enfreindre au RGPD ou au contrat relatif à la protection des données à caractère personnel.

---

[46] Comité Européen de la Protection des Données (EPDB-EDPS), *Joint Response*, Annexe, page 3. Voir aussi Comité Européen de la Protection des Données (EDPB), *Riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679* (Directives 2/2018 pour les exceptions de l'article 49 en vertu du règlement 2016/679), adoptées le 25 mai 2018, page 5.

[47] EPDB-EDPS, *Réponse conjointe*, Annexe, page 2.

[48] Voir aussi Annexe 3.

[49] Voir article 28.1 du RGPD.

Service public et activités de portée sociétale

Comme nous l'avons présenté, le point de départ de ce Livre blanc sont, ce que nous avons décidé d'appeler, les activités de portée sociétale. Selon notre définition, ces activités sont celles traitées par les autorités publiques et fondamentales pour la société dans son ensemble.

Pour définir précisément ces activités cruciales, nous utiliserons les critères de l'Autorité nationale suédoise pour la protection civile - MSB. Une petite partie des activités du service public que nous qualifions aussi de portée sociétale sont les activités dites sensibles relevant de la sécurité de l'information. Cette notion est définie par la loi suédoise sur la sécurité de l'information No.

2018:585 dans laquelle des règles particulières encadre la protection et la manipulation d'informations sensibles. Dans les paragraphes suivants, nous commencerons par définir les services appelés essentiels. À partir de cette définition, nous pourrons parfaire la définition des activités du service public concernées par la notion de portée sociétale. Une troisième partie présentera les risques que peut soulever la numérisation des activités du service public ainsi que les moyens existants pour protéger les données et les informations relatives à ces activités.[50]

[50] La norme ISO/IEC 2382:2015 définit ces données (data) comme un ensemble d'informations qui peut être interprété après correction et dont la forme permet la communication, l'interprétation ou le traitement de cet ensemble. La même norme définit ces informations comme un ensemble des savoirs relatif à un objet, c'est-à-dire l'ensemble des données factuelles à propos d'évènements, de choses, de processus ou d'idées. Ces informations doivent toujours être replacées dans leur contexte. Voir Organisation internationale de normalisation, ISO/IEC 2382:2015(en) *Information technology — Vocabulary.*

Quels sont les services essentiels à la société ?

La défense militaire et la défense civile préparent à la défense de la Nation. La défense civile et ses acteurs permettent à la société de gérer les situations dans lesquelles un état d'alerte est considéré comme élevé. La défense civile se reflète donc dans les activités des administrations publiques, des municipalités, des régions, des entreprises privées et aussi des organisations bénévoles impliqués. En Suède, la défense civile a trois objectifs dont l'un est de sécuriser les activités essentielles nécessaire à l'équilibre de la société.[51]

La MSB étend à ces services essentiels les activités des collectivités, les installations, la construction, les infrastructures et les ressources dont le maintien est décisif au bon fonctionnement des services essentielles des acteurs de la société. Ces activités sont exercées par un grand nombre d'acteurs privés et publics.[52] Pour résumer, font partie des services essentiels, les services dont les perturbations ou la disparition seraient à l'origine d'un danger imminent pour la société. Il peut aussi s'agir des services indispensables à la gestion de crises potentielles ou en cours.[53] La MSB a identifié onze secteurs dont les activités sont indispensables à la société. On y retrouve un large éventail de secteurs, comme l'approvisionnement énergétique, les soins médicaux, la prise en charge des personnes et les transports. Les autres secteurs concernés sont les activités des collectivités territoriales (approvisionnement en eau potable, gestion des eaux usées, entretien des routes) ainsi que ceux en lien avec les régimes des retraites et la protection sociale.[54]

---

[51] Proposition de loi suédoise No. 2014/15:109, *Försvarspolitisk inriktning, Sveriges försvar 2016-2020* (Orientation de la politique de défense – la défense de la Suède de 2016 à 2020), page 12. Rapport de la commission parlementaire suédoise de la défense 2014/15:FöU11 et procès-verbal du Parlement suédois 2014/15:117.

[52] Autorité nationale suédoise pour la protection civile MSB, *Vägledning för identifiering av samhällsviktig verksamhet* (Guide pour l'identification des services fondamentaux de la société), MSB1408, juin 2019, page 7.

[53] Voir les recommandations de la MSB sur les analyses des risques et vulnérabilité des administrations publiques (MSB 2016:7), article 2. Les activités – ou service – fondamentaux y sont définies comme des activités dont au moins l'un de deux conditions suivantes est remplie : 1) La disparition ou d'importantes perturbations des activités des services peuvent, à elle seules, ou associées à d'autres bouleversements similaires mettre à court terme en péril l'équilibre de la société. 2) Ces activités sont nécessaires, voir essentielles, à la résolution rapide et efficace – c'est-à- dire une résolution censée minimiser le plus possible les dégâts – d'une crise sociétale en cours.

[54] Autorité nationale suédoise pour la protection civile MSB, *Vägledning för identifiering av samhällsviktig verksamhet*, (Guide d'identification des activités d'importance sociétale), page 7.

Qu’incluons-nous dans les activités dites de portée sociétale ?

Comme nous l’avons souligné ci-dessus, la notion de service essentiel cerne les activités décisives au maintien de l’équilibre de la société. En pratique, et dans bien des cas, le maintien de ces activités nécessite la continuité de fonctionnement des systèmes informatiques, ce qui en soi n’est pas considéré comme un service essentiel. Citons par exemple la lutte contre l’incendie et les soins médicaux qui, pour fonctionner, dépendent directement d’un service aussi évident que la garde d’enfant. Dans ce Livre blanc, nous avons choisi d’utiliser la notion d’activité de portée sociétale pour décrire les activités fondamentales pour la société, les services essentiels au bon fonctionnement de la société ainsi que les activités dont ces services sont dépendants. Notre définition des activités de portée sociétale se base donc sur la définition donnée par l’Autorité nationale suédoise pour la protection civile MSB. Les limites de cette définition ne sont cependant pas faciles à cerner. La société évolue continuellement et les interdépendances entre les services aussi. Il est donc nécessaire que chaque administration concernée par ces activités essentielles identifie les services dont elle dépendante pour fonctionner correctement. Au-delà des activités du service public et des services essentiels, il existe encore un niveau d’activités, à savoir celui des activités sensibles, c’est-à-dire les activités cruciales pour la sécurité de la Suède en tant que Nation. Nous aborderons ces activités dans *La sécurité de l’information*. Le schéma ci-dessous représente les relations entre les différents services et activités que nous venons d’aborder.

Illustration de la relation entre les notions de portée sociétale, de services essentiels et les activités dites sensibles. Une partie des activités de portée sociétale est constituée des services essentiels, qui comportent à leur tour les activités sensibles (c’est-à-dire relatives à la sécurité de l’information)

Risques identifiés liés à la numérisation ainsi qu'à l'externalisation des activités de portée sociétale

Le développement des technologies, l'évolution des services proposés, la privatisation, l'externalisation et l'automatisation sont à l'origine dépendances de plus en plus complexes entre les différents services de la société. L'Autorité nationale suédoise pour la protection civile MSB a constaté qu'il est indispensable que l'innovation technologique n'affecte pas la capacité de la société à résister et à gérer les troubles auxquels elle peut faire face[55].

La direction générale de la Sécurité suédoise a classé l'innovation technologique comme l'une des sept menaces à laquelle la Suède a dû faire face en 2019[56]. Le gouvernement suédois a aussi constaté que la vulnérabilité des systèmes informatiques mondiaux contemporain est l'un des défis les plus complexes auxquels nous devons faire face et qu'il le restera dans les années à venir. Les activités des milieux cyber ont évolué et sont devenu, au même titre que les forces armées, une menace bien distincte[57]. Des attaques informatiques hostiles, commandités par des États ou soutenues par ces derniers, peuvent avoir pour but d'endommager le fonctionnement de la société et ainsi cibler les services essentiels de plusieurs secteurs[58].

Le forum de préparation à la défense Försvarsberedningen constate que la défense armée du pays est dépendante de la continuité de fonctionnement des activités fondamentales de la société et que ces activités ne sont finalement plus interrompues avant et même pendant une attaque armée et c'est pour cela qu'il est de plus en plus difficile de clairement déterminer où se termine l'infrastructure civile et à quel moment commence l'intervention militaire[59]. Afin de maintenir un niveau de cybersécurité élevé en Suède, le gouvernement suédois estime que les activités essentielles de la société ainsi que leurs systèmes informatiques doivent pouvoir être protégés contre les cyberattaques. L'une des positions stratégiques de défense adoptée par la Suède est que la Suède doit développer et renforcer sa capacité à prévenir, contrer et activement gérer les conséquences des menaces, des évènements et des attaques – qu'elles soient civiles et militaires – dont la cible serait un environnement informatique[60].

Dans ce contexte, il faut également mentionner les activités de renseignement menées par les autorités américaines en vertu de la loi de surveillance des renseignements étrangers FISA (Foreign Intelligence Surveillance Act). Le programme américain de surveillance PRISM épluche les données informatiques

---

55 Autorité nationale suédoise pour la protection civile MSB, *Övergripande inriktning för samhällsskydd och beredskap* (Orientation générale pour la protection de la société et sa préparation), page 7

56 Direction générale de la sécurité suédoise, *Årsbok 2018* (Livre annuel 2018), page 21

57 L'Office suédois des radiocommunications de défense nationale (FRA) estime que les cyberattaques commanditées par des État se produisent continuellement et sont en constante augmentation. On estime que le but de ces attaques est l'accès aux informations confidentielles, tels les informations relatives aux stratégies de politique étrangère de la Suède, aux vulnérabilités du Suède ou encore à propos la défense totale dela Suède. Il peut également s'agir de préparations d'attaques et de perturbations ou encore d'espionnage industriel. Voir le Rapport annuel de l'Office des radiocommunications de la défense nationale de 2018, *Årsrapport 2018*, pages 17 et 19.

58 Voir proposition de loi 2014/15:109, pages 111 à 113.

59 Rapport de ministère Ds 2017:66, *Motståndskraft – Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025* (Puissance de réaction : préparation de la défense totale et élaboration de la défense civile de 2021 à 2025), pages 17 et suivantes et page 113.

60 Voir proposition de loi 2014/15:109, pages 111 à 113.

de ressortissants non américains récupérées chez des prestataires de services du renseignement. [61] En 2013, il a été dévoilé que des millions de comptes utilisateurs, notamment des comptes Google, ont été surveillé dans le cadre de ce programme et que des métadonnées des comptes ont été collectées[62].

La loi FISA est encore en vigueur mais il n'est pas clair de quelle manière elle est appliquée et quelles sont les données recueillies en vertu de cette loi[63].

La direction générale de la sécurité suédoise a identifié l'externalisation des services de l'information, dont font partie les services cloud fournis par des acteurs privés, comme un risque potentiel. Les services de sécurité du pays soulignent que ce risque provient souvent du fait de la centralisation des systèmes et des informations de différents clients du même fournisseur vers un même système informatique physique. Ces procédés sont à l'origine d'aggravations du risque puisqu'une perturbation d'un système d'un client entraînera des perturbations voir même des discontinuations de fonctionnement des systèmes des autres clients du fournisseur. Si une quantité importante d'informations sensibles et secrètes convergent vers un seul et même fournisseur, ce dernier risque de devenir un objectif intéressant, notamment pour les services de renseignements des pays étrangers. La concentration d'un grand nombre d'informations chez un fournisseur peut aussi avoir d'autres conséquences pour la Suède et pour sa propre sécurité, à savoir l'augmentation l'influence de ce fournisseur[64].

Plus spécifiquement, les services cloud représentent, aux yeux du Comité sur l'intégrité, de graves risques pour l'ensemble des administrations et en particulier pour les administrations publiques. La raison avancée est notamment ici, que la majeure partie des données traitées par les autorités sont à caractère personnel et peuvent être considérées comme sensibles, tout particulièrement du point de vue du respect de la vie privée. Le fait que les autorités soient aussi soumises à un grand nombre de règlementations et de règles à suivre comme par exemples les procédures relatives aux documents publics, à la sécurité de l'information et à l'archivage, appuie les propos du Comité. Ce Comité estime que le fait que des autorités décisionnaires souscrive à des services cloud sans vraiment maîtriser les processus des traitements et diffusion des données au sein de leurs services n'est pas un cas isolé. Les petites administrations peuvent aussi ne pas avoir les compétences nécessaires requises pour choisir le service cloud compatible à leurs contraintes juridiques ou de sécurité.

---

[61] Director of National Intelligence, *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 08.06.2013.

[62] Gellman Barton et Soltani Ashkan : *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, The Washington Post, 30.10.2013.

[63] Parlement européen : *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, (PE 583.137), pages 127 et 128.

[64] Voir notamment Direction générale de la sécurité suédoise, *Årsbok 2017* (Livre annuel 2017), page 56.

Toujours selon le Comité sur l'intégrité, les risques liés au traitement des informations demeurent dans les cas où les administrations manipulent, en tant qu'employeurs, des informations personnelles sur un service cloud. En effet, l'acheminement, de plus en plus important, de données vers des prestataires externes peut être à l'origine d'un disséminement difficile à contrôler et de problématiques de stockage lors de la réutilisation des données. Le traitement de ces données suppose en effet des traitements répétitifs, sans que ni l'employeur ni l'employé ne s'en rendent compte[65].

Lorsque l'on parle d'externalisation des données, le traitement des données de télémétrie par les prestataires de services est un facteur supplémentaire de risque. Les données de télémétrie sont des mesures obtenues à distances et traitées par le prestataire qui peuvent contenir aussi bien des contenus factuels que des métadonnées sur l'utilisation d'un service informatique. Ces données peuvent, théoriquement, faire l'objet de transmission en vertu de législations comme le CLOUD Act, mais elles sont cependant principalement traitées par le prestataire de service dans un but perfectionnement et de journalisation de service. Un aspect remarquable dans ce contexte, est qu'un service cloud, en tant que produit commercial, implique souvent un modèle qui lui est propre et qui consiste à utiliser les données des clients pour, par exemple, pour développer de nouveaux services et pour partager des données avec d'autres entreprises qui les utiliseront à d'autres fins commerciales et publicitaires[66]. Même si certains paramètres peuvent limiter la quantité de données télémétriques traitées par le prestataire de services, le client n'a pas la possibilité de complètement maîtriser le processus. Les contrats type des services cloud donnent souvent au prestataire un grand nombre de libertés lui permettant de traiter les données à des fins propres alors que ces contrats types font infraction à la règlementation relative à la protection des données. Lors d'une étude réalisée par les autorités néerlandaises, il est constaté que les fournisseurs, et notamment les fournisseurs de services cloud non encadrés par la loi, collectent données et métadonnées potentiellement sensibles et qu'ils transmettent des données télémétriques à des pays situés en dehors de l'Union européenne[67].

Le Comité sur l'intégrité constate que le risque le plus notable pour l'intégrité des personnes, lors de l'utilisation de services cloud, est lié à la dégradation de la maîtrise et du contrôle qu'implique généralement l'utilisation de ce type de services. En plus des risques déjà évoqués ci-dessus, précisons que cette dégradation est à l'origine de risques liés aux intrusions non autorisées du côté des prestataires et des sous-traitants et au transit des données via des pays dont la législation n'apporte aucune protection suffisante. Les données concernées sont aussi à la portée de sous- traitants inconnus du client ; dans quel cas il est encore plus difficile pour une administration de veiller à ce que les données soient traitées conformément à la règlementation de protection des données[68].

---

[65] Le Comité constate aussi que les particuliers n'ont souvent aucune possibilité d'action légale dans les cas où le traitement par les administrations de ces données à caractère personnel ne soit pas souhaité. Ce traitement, s'il est informatique et en ligne, peut en effet avoir des conséquences graves puisque ces données administratives peuvent être mises à disposition d'acteurs privés. Voir Comité sur l'intégrité, *Hur står det till med den personliga integriteten? – en kartläggning av Integritetskommittén* (Où en est l'intégrité des personnes ? État des lieux dressé par le Comité sur l'intégrité (Rapport des commissions officielles de l'État suédois, SOU 2016:41) pages 53 et 54, 70 et 81.

[66] SOU 2016:41 page 111.

[67] Voir l'Annexe 8 pour plus de détails et d'exemples de données télémétriques traitées par des prestataires. Voir aussi SOU 2016:41 page 112.

[68] Rapport des commissions officielles de l'État suédois, SOU 2016:41 page 111

La direction générale de la Sécurité suédoise constate aussi que de plus en plus d'administrations on recourt à des méthodes dites *offshore* et externalisent de plus en plus leurs services sensibles à des prestataires étrangers[69]. Dans de tels cas, les administrations se doivent d'exiger à ces prestataires des conditions d'utilisation et de fonctionnement des services identiques à celles en application en Suède. L'Autorité nationale suédoise pour la protection civile MSB constate aussi que la délocalisation nécessite des précautions particulières de la part des administrations. Lorsque l'externalisation d'activités se fait au profit d'un prestataire étranger, il est impératif qu'il existe au préalable un accord de protection bilatéral entre la Suède et le pays du siège social du prestataire[70].

En 2017, une enquête sur l'externalisation des systèmes d'information de la Direction suédoise des transports, Transportstyrelsen, constate que confier l'administration et l'entretien de fragments centraux des système techniques capitaux aux bons fonctionnements d'une administration suédoise à des sociétés étrangères est clairement un facteur de risque. Les responsables de l'enquête en concluent que même des systèmes qui doivent rester accessibles et qui ne contiennent pas en soi d'informations sensibles peuvent finalement s'avérer être des services essentiels à la société et qu'il n'est pas souhaitable que le contrôle de ces systèmes soit placé ailleurs qu'en Suède[71].

---

[69] Le fait, de la part d'un le fournisseur de service cloud, de stocker des données ou d'employer des techniciens à l'étranger est une forme de délocalisation.

[70] Direction national de la sécurité suédoise, *Årsbok 2017* (Livre annuel 2017), page 56 et Autorité nationale suédoise pour la protection civile MSB, *Handlingsplan för skydd av samhällsviktig verksamhet,* (Plan d'action pour la protection des activités d'importance sociétale), MBS597, déc. 2013, page 17.

[71] Rapport des commissions officielles de l'État suédois, SOU 2018:6, Examen de l'appel d'offres de services informatiques de la Direction suédoise des transports, page 238.

La protection des activités de portée sociétale

Dans cette partie, nous examinerons les règlementations qui constituent une protection pour les services des autorités et nous nous concentrerons particulièrement sur la protection des services des technologies de l'information. Nous aborderons également le chiffrement, qui, dans certains contextes, a été mis en avant comme solution pour répondre aux enjeux soulevés par les problématiques législatives que nous avons déjà mentionnés.

Les champs d'application cités ne doivent être considérés que comme des exemples. Il est important de rappeler qu'il existe d'autres réglementations relatives à ces problématiques. Citons pour exemple les législations sur la protection des différents types de données, comme la loi relative à la confidentialité des données.

Analyses des risques et des vulnérabilités

Les municipalités, les régions et la grande majorité des administrations publiques doivent mesurer leur vulnérabilité et vérifier si de telles menaces pèsent sur leurs responsabilités et si ces risques pourraient gravement altérer leur capacité à maintenir les activités dans leurs services (analyse de risques et vulnérabilités).

Ce type d'analyse est le premier maillon d'une chaîne visant à identifier et à réduire les vulnérabilités, les menaces et les risques auxquels pourraient être exposé la responsabilité de l'administration et qui pourraient gravement altérer son fonctionnement[72].

Une fois que les risques ont été identifiés, l'analyse en question doit être capable d'évaluer un niveau de risque acceptable et, dans le cas où celui-ci ne le serait pas, d'orienter l'administration vers les mesures à prendre pour contrer ou réduire au minimum les conséquences des risques identifiés[73].

L'Autorité nationale suédoise pour la protection civile MSB souligne que la préparation et la gestion de crise doit aussi être aborder dans le cadre des appels d'offre relatifs aux services essentiels des administrations[74].

Sécurité et classification des informations

Toutes les administrations publiques du gouvernement doivent s'assurer que leurs propres systèmes de gestion de l'information répondent aux exigences fondamentales de sécurité afin de permettre aux services de l'administration d'être assurés de manière satisfaisante[75]. Le travail des autorités sur la sécurité des informations doit viser à préserver la confidentialité, la véracité, la traçabilité et la disponibilité des informations. La classification des informations prépare à cela.

---

[72] Voir loi suédoise No. 2006:544 sur les mesures des communes et des conseils généraux en prévision d'évènements extraordinaires en temps de paix et en cas d'alerte, chapitre 2, article 1, ainsi que l'ordonnance suédoise 2015:1052 sur la préparation aux crises et capacités des autorités de surveillance des états d'alerte, article 8 et article 16.2.

[73] Autorité nationale suédoise pour la protection civile MSB, *Vägledning för risk- och sårbarhetsanalyser*, Guide des analyses de risques et vulnérabilités MSB245, avril 2011, pages 50 et 51.

[74] MSB, *Upphandling till samhällsviktig verksamhet – en vägledning* (Appels d'offres pour le renouvèlement des services essentiels des administrations: un guide). MSB1275, septembre 2018, page 19.

[75] Voir les articles 3 et 19 de l'ordonnance suédoise 2015:1052 sur la préparation aux crises et capacités des autorités de surveillance des états d'alerte.

Cette classification définie le niveau protection nécessaire à une source d'information. Les informations sont classées en différents niveaux ainsi qu'en fonction des conséquences que pourraient avoir un défaut de confidentialité, d'exactitude et de disponibilité.

À partir de cette classification de l'information et de l'analyse des risques, l'autorité sera chargée d'identifier et de prendre les mesures nécessaires afin de répondre aux besoins de protection des données. Chaque administration détermine le modèle le plus adapté à son domaine de compétence[76].

Sécurité de l'information

Comme nous l'avons fait remarquer précédemment, certains services de ce que nous avons appelé activités de portée sociétale sont constitués d'activités sensibles, elles-mêmes essentielles pour la sécurité de la Suède. La loi suédoise relative au renseignement réglemente les activités de prévention contre l'espionnage, le sabotage, les actes de terrorisme et autres menaces[77].

Les activités sensibles sont classées en fonction des préjudices potentiels infligés à la Suède dans les cas où un individu se procurerait ou détruirait des informations relatives à ces activités ou nuirait au bon fonctionnement de ces dernières[78]. Les obligations sur la manipulation des données considérées comme relevant du renseignement sont plus rigoureuses, proportionnellement au niveau de classification spécifié. Ces activités sensibles sont celles des administrations suédoises, parmi lesquelles l'Agence suédoise de la sécurité sociale, Försäkringskassan.

La loi suédoise relative au renseignement prévoit la mise en place de disposition concernant la sécurité des informations et celle du personnel. La sécurité de l'information s'applique à la protection des informations, où qu'elles se trouvent et de manière qu'elles ne puissent être ni partagées, ni modifiées par des personnes non autorisées. Il s'agit aussi de veiller à ce que ces informations ne soient accessibles que lorsque nécessaire[79].

---

[76] Articles 4 et 9, MSB : Instructions pour la sécurité des informations des administrations publiques (MSBFS 2016:1).

[77] Chapitre 1, articles 1 et 2 de la loi suédoise relative au renseignement.

[78] Chapitre 2, article 5 de la loi suédoise relative au renseignement. Les quatre classes de contrôle de sécurité sont : 1) classé secret si le dommage potentiel est particulièrement grave ; 2) secret en cas de dommage grave ; 3) confidentiel en cas de dommage non négligeable ; et 4) secret limité uniquement en cas de dommage mineur.

[79] Chapitre 2, article 2 de la loi suédoise relative au renseignement. Voir également Direction de la sécurité suédoise, *Informationssäkerhet* (Sécurité des informations).

La sécurité du personnel est quant à elle relative aux postes et tâches affectés à des activités sensibles et à laquelle est attribuée une classe de sécurité déterminée en fonction de la nature des données, ainsi qu'à la quantité de ces données auxquelles le personnel pourrait avoir accès[80]. Toute personne chargée de recruter ou de faire appel à une personne affectées à des activités sensibles doit procéder au préalable à un contrôle de sécurité dont la finalité est de prouver que la personne est considérée comme loyale aux intérêts de l'administration[81]. Cette enquête de sécurité implique un examen de base élaborée autour un entretien et d'une collecte d'attestations et de références pertinentes[82].

L'examen de base est suivi d'une habilitation de sécurité dont est chargée la Direction de la sécurité suédoise[83]. Cette habilitation s'appuie sur les données collectées et transcrites dans le registre des infractions et des présomptions en vertu de la loi suédoise 2018:1693 sur le traitement par la police des données à caractère personnel dans le cade de la collecte des données de criminalité[84]. La nationalité suédoise n'est pas exigée auprès des personnes qui, autrement que par leur emploi, participent à des activités sensibles menées par l'État, les municipalités ou les régions[85]. Si un candidat venait à être recruté et que son adresse de domiciliation n'était pas en Suède, les ressources de la Direction de la sécurité seraient alors limitées et compliquerait la validation de l'habilitation. Le Direction général de la sécurité suédoise estime que le service de l'administration chargé de l'habilitation doit, dans de tels cas, se plier à un contrôle approfondi et satisfaire un niveau de contraintes plus élevée lors de la vérification des antécédents de la personne concernée[86]. Un cas concret des difficultés rencontrées lors des contrôles et validation des habilitations des ressortissants étrangers est cité dans l'enquête de 2018 sur l'appel d'offres de la Direction suédoise des transports pour ses services informatiques[87].

Si des activités sensibles d'une administration doivent être confiées à des prestataires choisis sur appel d'offres, l'administration en question doit exiger le même niveau de contrôle et de vérification que celui sollicité pour ses propres activités[88] au moyen d'un contrat de contrôle de sécurité signé par l'émetteur de l'appel d'offres, les fournisseurs et sous- traitants éventuels.

L'administration doit également se charger du suivi et vérifier que les fournisseurs ont bien pris en compte les mesures exigées par l'administration lors de la signature

---

80 Chapitre 3, articles 5 à 10 de la loi suédoise relative au renseignement.

81 Chapitre 4, article 4 et chapitre 3, articles 1 et 2 de la loi suédoise relative au renseignement. Voir aussi Direction de la sécurité suédoise, *Personalsäkerhet* (Sécurité du personnel).

82 Chapitre 3, articles 3 et 4 de la loi suédoise relative au renseignement (2018:585), chapitre 5, article 2 de l'ordonnance sur le renseignement 2018:658 et chapitre 6 article 4 des instructions de la Direction de la sécurité suédoise (PMFS 2019:2) relative au renseignement. Voir aussi Direction de la sécurité suédoise, *Vägledning i säkerhetsskydd* (Guide pour le contrôle de sécurité) pages 11 et 12.

83 Chapitre 43, article 14 de la loi suédoise relative au renseignement 2018:585.

84 Chapitre 3, article 13 de la loi suédoise relative au renseignement.

85 Chapitre 3, article 11 de la loi suédoise relative au renseignement.

86 Direction de la sécurité suédoise, *Vägledning i säkerhetsskydd* (Guide pour le contrôle de sécurité), page 26.

87 Voir Rapport des commissions officielles de l'État suédois, SOU 2018:6, pages 161 à 163.

88 Direction de la sécurité suédoise, Contrôle de sécurité lors de l'émission appels d'offres et de contrats commerciaux.

dudit contrat[89]. Selon la Direction général de la sécurité suédoise, l'un des risques du recourt aux appels d'offres pour les activités sensibles est que les exigences du susdit contrat de contrôle sont parfois trop générales et que le suivi de celui-ci en soit trop complexe[90].

Chiffrement des données

Tous les acteurs, publiques ou privés, amenés à communiquer des données concernées par ces contrôles de sécurité vers un système informatique externe, doivent protéger ces données par le biais de services cryptographiques approuvés par les Forces armées suédoises[91]. Un grand nombre de fournisseurs de services cloud proposent également à leurs clients des services de chiffrement des services non concernés par l'ordonnance sur les habilitations et les contrôles de sécurité. Il a été évoqué que ce type de services pouvait, dans certains cas, être une solution aux problématiques éventuels comme par exemple, celle de l'accès des autorités étrangères à des données stockées en ligne[92].

Le chiffrement interdit aux personnes non autorisées l'accès aux données chiffrées. Si le chiffrement est configuré de manière qu'un utilisateur, comme le prestataire de services, soit autorisé et ait accès à la clé de chiffrement, le chiffrement ne protège, par définition, plus les données auxquelles à accès cet utilisateur. Le chiffrement a généralement un effet négatif sur les performances du service si l'accès aux données n'est pas autorisé au prestataire. Des données cryptées ne peuvent pas non plus être traitées, ce qui réduit significativement les champs d'utilisation du service[93]. L'Agence nationale de services juridiques, financiers et administratifs Kammarkollegiet constate dans son étude préliminaire sur le recourt des services en ligne que le chiffrement n'est pas une mesure de protection réaliste pour les environnements de travail bureautiques[94].

---

89 Chapitre 2, article 6 de la loi suédoise relative au renseignement. Cette disposition vise les appels d'offres et les contrats relatifs aux marchandises, services ou travaux publics dans les cas où l'appel d'offres vise des données classées confidentielles ou d'un niveau de sensibilité plus élevé, ou si lors du traitement de l'appel d'offres, le fournisseur aurait accès à des services sensibles et préjudiciable à la sécurité de la Suède.

90 Direction de la sécurité suédoise, *Årsbok 2017* (Livre annuel 2017), page 56

91 Chapitre 3, article 5 de l'ordonnance 2018:658 des habilitations de sécurité.

92 Au sujet du chiffrement. Voir également Annexe 7.

93 On entend par traitement, toute manipulation autre que le stockage, le chargement ou le téléchargement. Les données seront traitées dans les cas où elles doivent être lues ou modifiées. Des données cryptées sont comparables à une lettre placée à l'intérieur d'une enveloppe cachetée et fermée. L'enveloppe peut être stockée ou transmise mais, contenu ne peut être lisible que si l'enveloppe est ouverte. Voir en outre à l'Annexe 7.

94 Agence nationale de services juridiques, financiers et administratifs Kammarkollegiet, *Förstudierapport Webbaserat kontorsstöd* (Étude préliminaire concernant les outils bureautiques en ligne), page 35. Dans l'analyse de l'utilisation par Microsoft des données télémétriques, les autorités néerlandaises n'ont, en 2017, pas non plus cité le chiffrement comme solution aux problématiques soulevées par l'accès des prestataires de services aux données sensibles de leurs clients. Voir également Annexe 8.

La souveraineté numérique

La politique de sécurité de la Suède vise principalement à garantir l'indépendance et l'autonomie du pays. Il s'agit avant tout de préserver notre souveraineté, nos droits, nos intérêts et nos valeurs ainsi que de protéger la liberté d'action du pays loin de toute pression politique, militaire ou autre contrainte. Le gouvernement suédois a déclaré que l'une des conditions nécessaires à la réalisation des objectifs de sécurité implique l'affirmation de la souveraineté et de l'intégrité territoriale du pays[95].

La souveraineté nationale concerne le contrôle des frontières du territoire, la maîtrise des processus décisionnels de politiques intérieur et la sécurisation de l'approvisionnement de la population en biens de première nécessité. On considère donc que la souveraineté nationale est une des conditions de maintien des valeurs essentiels de la société, comme la vie et la santé des citoyens, l'organisation de la société, ainsi que la démocratie et la sécurité juridique[96].

Dans une époque où les services fondamentaux à la société sont de plus en plus dépendants du numérique, le contrôle des informations des administrations revêt une importance capitale pour l'indépendance de notre pays. Le comité préparatoire à la défense Försvarsberedningen souligne que la maîtrise des évolutions des services de l'information et de cybersécurité améliore la maîtrise de notre souveraineté nationale et contribue activement aux possibilités de réactivité face aux évènements globaux ainsi qu'à la protection nos infrastructures stratégiques[97].

La notion de souveraineté numérique a été évoquée pour la première fois au début des années 2000 et son contenu semble tout d'abord avoir été discutée en France[98]. Les discussions se sont toutefois animées en 2013, lorsqu'il a été annoncé que certains pays avaient massivement surveillé l'identité numérique d'un grand nombre d'individus, notamment de ressortissants européens[99]. Parmi les mesures proposées à l'époque, on comptait un service national de messagerie (Allemagne), un réseau de câbles sous-marins dédiés au trafic Internet (Finlande et Union européenne), des services cloud locaux destinés au stockage en ligne (France, Allemagne, Suisse et Pologne) et des réseaux censés assurer un trafic internet interne à l'Union Européenne (Allemagne)[100].

La France et l'Allemagne ont annoncé en 2015 que les deux pays se chargeaient conjointement de la souveraineté numérique auprès de l'Union européenne. L'objectif était de renforcer la capacité des États membres et de l'Union Européenne

---

95 Proposition de loi 2014/15:109, page 7.

96 Voir notamment Autorité nationale suédoise pour la protection civile MSB, *Övergripande inriktning för samhällsskydd och beredskap*, (Orientation d'ensemble pour la protection de la société et sa préparation), pages 7 et 8.

97 Rapport de ministère Ds 2017:66, page 115.

98 Bellanger Pierre, De la souveraineté en général et de la souveraineté numérique en particulier, Les Échos, 30.08.2011. La notion de souveraineté technologique était aussi utilisée, voir Maurer Tim et autres : *Technological Sovereignty: Missing the Point? An Analysis of European Proposals after June 5, 2013*, New America's Open Technology Institute et the Global Public Policy Institute (GPPi), page 4.

99 Tim Maurer et autres, Souveraineté technologique, page 3. La surveillance était règlementée par le décret d'application Executive order EO12333: Bureau du directeur des renseignements des États-Unis : *United States Intelligence Activities (Federal Register Vol. 40, No. 235 (December 8, 1981), amended by EO 13284 (2003), EO 13355 (2004), and EO 13470 (2008))*.

100 Tim Maurer et autres, *Technological Sovereignty*, page 11.

à protéger les réseaux numériques, développer une industrie numérique autonome, innovante, efficace et diversifiée ainsi que d'accentuer la cybersécurité et d'assurer des services fiables au niveau européen. Cette coopération devait permettre à l'Europe de pouvoir décider seule de la sécurité de ses propres données[101] et la souveraineté de l'Union Européenne a été mentionnée à maintes d'autres occasions. Le Conseil européen estime que l'Europe doit sécuriser sa souveraineté numérique et bénéficier des avantages de la transformation numérique en cours[102].

Le Conseil de l'Union européenne conclue dans ses observations de 2020 sur une Europe très numérisée que la cyber sécurisation de l'Europe doit être renforcée pour notamment protéger sa souveraineté numérique[103]. La question de la souveraineté des États de l'Union Européenne a également été identifiée par la nouvelle présidente de la Commission européenne madame Ursula von der Leyen, comme l'une des mesures à débattre pour préparer l'Europe à l'ère numérique[104]. Des représentants du Contrôleur européen de la protection des données ont également évoqué la question de la souveraineté numérique et ont précisé que l'une des conditions du maintien de la souveraineté était l'implication des autorités dans la protection de toute la chaîne stratégique d'approvisionnement et de veiller à l'élaboration de stratégies de sortie lors de l'utilisation de services cloud[105].

Le contenu de la notion de souveraineté numérique n'a cependant pas été clairement établi. Les recommandations prononcées lors du sommet allemand du numérique Digital Gipfel et relatives à l'institution d'une souveraineté numérique allemande proposent toutefois la définition suivante[106].

La souveraineté numérique d'un état ou d'une organisation relèvent du contrôle total des données stockées ou traitées, ainsi que de la capacité de décider librement des personnes ayant accès à ces données. La souveraineté numérique se consacre aussi à la maîtrise d'un développement indépendant d'outils et de systèmes d'information, leur modification, leur contrôle ainsi que les mises à jour nécessaire à l'ajout de nouvelles fonctionnalités[107].

---

[101] Cette annonce a été publiée lors d'une déclaration conjointe à la sortie d'une réunion ministérielle, en 2016. Voir Ministère de l'Europe et des Affaires étrangères, *Déclaration du conseil franco-allemand de sécurité et de défense,* 2015.

[102] Conseil européen, Nouvel agenda stratégique de 2019 à 2024, juin 2019.

[103] Conseil de l'Union européenne (Conseil "Transports, télécommunications et énergie") , Conclusions sur l'avenir d'une Europe hautement numérisée après 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion". 07.06.2019, page 5, Conclusion 7.

[104] von der Leyen Ursula, Priorités de la prochaine commission européenne, 2019-2024, page 5.

[105] Robert Riemann, au Comité Européen de la Protection des Données (EPDB-EDPS), lors du premier conseil européen des applications informatiques et de services cloud, 29.08.2019. Voir Huizing Lennart, *The Hague Forum for Cloud Contracting*, Privacy Company, 24.10.2019. Une stratégie de sortie est un accord qui décrit les conditions économiques et techniques dans lequel doit s'opérer un changement de d'espace de stockage et de fournisseur.

[106] Le sommet numérique allemand Digital Gipfel est une coopération politique, économique, scientifique et sociétale, présidée par le ministère allemand de l'économie et de l'énergie (Bundesministerium für Wirtschaft und Energi).

Cette coopération est composée de différentes plates-formes, dont la plate-forme « nouvelle numérisation de la vie économique » (Innovative Digitalisierung der Wirtschaft). Au sein de cette plate-forme, les travaux et projets sont abordés lors des réunions des groupes de travail. Le groupe de travail « Souveraineté numérique » a exposé en 2018 ses recommandations sur la souveraineté numérique et s'est concentré sur l'intelligence artificielle. Voir aussi Bundesministerium für Wirstschaft und energie

[107] Voir Digital Gipfel, Digitale Souveränität und Künstliche Intelligenz - Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen, 2018, page 3.

Le ministère fédéral de l'Intérieur allemand a annoncé en septembre 2019 que les années à venir seraient dédiées à renforcer la souveraineté numérique de l'administration publique. La souveraineté numérique allemande passera par la réduction de la dépendance aux fournisseurs de service informatique privés et après un éventuel rapprochement entre États membres de l'Union Européenne, la possibilité d'utiliser des logiciels alternatifs pour remplacer ces des fournisseurs a aussi été évoqué[108]. Ces propositions ont été concrétisées en octobre 2019 et ont pris forme grâce au projet GAIA-X, décrit comme une nouvelle infrastructure informatique fédérée. L'objectif du projet est d'assurer la souveraineté informatique, de réduire le niveau de dépendance de l'Union et de permettre l'innovation et l'utilisation de services cloud qui ne transgresseraient pas le droit européen[109].

Pour ouvrir la voie aux prestataires de services privés, le ministère allemand de l'économie et de l'énergie a aussi publié une liste de critères à respecter pour qu'un service cloud décroche le label qualité "*trusted cloud service*" (service cloud de confiance). Ces critères déterminent le profil du fournisseur et des sous-traitants, les possibilités de révision, les conditions de signature du contrat, la sécurité, l'intégrité, les processus opérationnels, l'interopérabilité ainsi que l'architecture des services en soi[110]. Les fournisseurs qui remplissent les conditions du label font l'objet d'une publication et d'une certification officielle[111].

La Suède a récemment adopté une proposition visant à apporter des modifications de la loi sur les communications électroniques et de la loi l'accès à l'information afin d'assurer la sécurité de la Suède lors de l'utilisation d'émetteurs radio. Dans sa proposition, l'approche du gouvernement est similaire à celle du Digital Gipfel allemand. La notion de souveraineté numérique n'est certes pas expressément mentionnée dans cette proposition, mais le gouvernement suédois estime que les risques auxquels sont exposés la sécurité ainsi que l'accès aux informations lors de la mise en place d'infrastructures d'importance sociétale doivent être pris en compte si les configurations des systèmes et des infrastructures informatiques sont accessibles à des partenaires étrangers. Il est prouvé qu'une attaque étrangère ,ou soutenue par l'étranger, des administrations et des services d'importance sociétale constitue une grave menace au fonctionnement de la société, au maintien de notre souveraineté et de notre intégrité territoriale[112].

---

[108] Ministère fédéral de l'Intérieur, des Travaux publics et de la Patrie *BMI intensiviert Aktivitäten zur Stärkung der digitalen Souveränität in der öffentlichen Verwaltung*, 19.09.2019.

[109] Ministère allemand de l'économie et de l'énergie (BMWi), *Project GAIA-X A Federated Data Infrastructure as the cradle of a vibrant European ecosystem*, pages 6 à 9, 12.

[110] Ministère allemand de l'économie et de l'énergie (BMWi) *Criteria and catalogue for cloud services version 2*, version 2.

[111] Ministère allemand de l'économie et de l'énergie (BMWi), *Trusted Cloud – Cloud providers.*

[112] Proposition de loi 2019/20:15, *Skydd av Sveriges säkerhet vid radioanvändning*, (Services radios et préservation de la sécurité de l'État suédois), page 26.

Conclusions de l’Agence suédoise de la sécurité sociale, Försäkringskassan

- Des conflits surgissent entre les autorités étrangères désireuses d’accéder aux données et la confidentialité des données décidées par l'Union européenne et suédoises.
- Le point de départ de la discussion sur les services informatiques des administrations publiques ne doit cependant pas être ce conflit normatif, mais doit plutôt s’orienter vers les questions de principe relatives à la protection des données lorsqu’elles sont communiquées à des entreprises privées ou aux autorités d'autres pays.
- Les systèmes informatiques stratégiques des activités essentielles de la Försäkringskassan doivent être placés sous le contrôle de l'administration publique suédoise.
- La Försäkringskassan ne transférera pas l'administration de systèmes numériques stratégiques de ses services à des entreprises privées soumises à la juridiction d'un pays dont la loi sur la protection des données serait semblable au CLOUD Act. Pour les systèmes informatiques de certaines activités, comme par exemple les activités sensibles et confidentielles ; l'objectif de la Försäkringskassan est, sur le long terme, de garder l’administration des systèmes informatiques sous la tutelle de l'État suédois.
- Pour pouvoir sécuriser les fonctions de portée sociétale contre les attaques, ainsi que pour réduire l’influence des sociétés privées, la stratégie numérique de la Suède doit être complétée par une prise de position claire sur le contenu et la portée de la notion de souveraineté numérique.
- Dans les cas où des administrations suédoises utilisent des services cloud publics administrés par des acteurs privés, les autorités doivent définir les conditions d’utilisation de ces services. Les administrations publiques suédoises doivent, par le biais d’une coopération national et européenne, faire en sorte que les services que nous désirons utiliser soient proposés à des conditions dans lesquelles soit respectée la législation suédoise et assuré un niveau de protection suffisant.

Avantages des services cloud publics

Les services cloud publics introduisent de nombreux avantages. La transition vers ces services cloud a, dans de nombreux cas, débouché sur de meilleurs services opérationnels, une amélioration de la sécurité et de la disponibilité numérique à des coûts raisonnables[113]. Dans ces conditions, il est souhaitable, et souvent nécessaire, que les autorités puissent tirer parti de cette technologie en tant que telle et profiter

[113] Voir Comité sur l’intégrité, *Hur står det till med den personliga integriteten? – en kartläggning av Integritetskommittén* (Où en est l’intégrité des personnes ? État des lieux dressé par le Comité sur l’intégrité (Rapport des commissions officielles de l'État suédois, SOU 2016:41), page 110. Le Comité constate cependant que les services cloud ne sont pas sans risque pour les autorités.

simultanément de la capacité d'innovation du secteur privé. Les effets positifs de ces services ne doivent cependant pas inciter les autorités suédoises à utiliser des services cloud publics sans avoir au préalable analysé la pertinence d'une telle évolution ainsi que l'impact d'une telle transition sur l'intégrité des individus. Nous nous pencherons dans les paragraphes suivants sur une telle possibilité pour la Försäkringskassan.

Conflits normatifs constatés dans le cadre de l'utilisation de services cloud privés

Le CLOUD Act et les autres législations similaires ont suscité en Suède un débat dans lequel ont surtout été évoquées les problématiques du droit des autorités étrangères d'exiger l'accès à des données stockées chez des prestataires de services de leur juridiction d'une part, et la législation communautaire et suédoise sur la protection et la confidentialité des données, d'autre part.

Sur la protection des données, nous pouvons simplement constater que le Comité Européen de la Protection des Données a déclaré qu'une restitution de données à caractère personnel en vertu du CLOUD Act ou autres législations similaires n'est compatible au règlement RGPD que dans des cas exceptionnels. Compte tenu de la nature des missions et de la direction du Comité, le poids de ces déclarations n'est pas négligeable dans la mesure ou la Cour de justice de l'Union européenne ne s'est pas encore prononcée sur la question[114].

Dans le panorama que nous entendons dresser dans ce Livre blanc, nous ne faisons aucune autre appréciation sur la loi suédoise sur la confidentialité que celle du programme eSam et celui de l'Agence nationale de services juridiques, financiers et administratifs Kammarkollegiet. Le fait d'employer des prestataires de services susceptibles de divulguer des données aux autorités d'un pays étranger ne peut pas non plus être considéré comme compatible avec les principes fondamentaux de la loi suédoise sur la confidentialité des données qui suppose que *l'autorité suédoise* (et non le prestataire de services ou une autorité étrangère) doit se pencher *sur chaque cas particulier* pour décider de la restitution de données[115].

Le fait que des données confidentielles soient mises à la disposition d'un prestataire de services répondant du CLOUD Act ou à des législations semblables soient considérées comme divulguées, rappelle qu'il n'est pas possible de résoudre ces conflits via des analyses de risque. Une analyse de risque des données confidentielles n'aboutirait qu'à une appréciation de la nature des données que l'autorité serait prête à divulguer afin de pouvoir profiter des avantages du service cloud. Nous estimons que cette position n'est pas acceptable . Toutes les données confidentielles doivent être protégées d'une divulgation illégale et toute restitution doit, comme nous l'avons dit, être traité au cas par cas et non pas dans le cadre d'une analyse générale.

Le chiffrement n'est pas non plus une solution aux conflits normatifs même s'il offre une protection générale aux accès non autorisés. Il est tout d'abord impossible

---

[114] Notons qu'un accord entre l'Union Européenne et les États-Unis pourrait repositionner le Comité Européen de la Protection des Données.

[115] Cette procédure sera très certainement maintenue. Les conditions de l'étude sur la transition informatique sécurisée et rentable des administrations publiques renvoient notamment aux amendements éventuels de la loi suédoise sur la confidentialité des données et sur le fait que ces changements ne doivent pas se faire au détriment de la procédure et de la méthodologie employée, ni engendrer d'amendement ou d'ajouts aux dispositions légales existantes. Voir directive 2019:64.

d'exclure le fait qu'une autorité étrangère, qui s'estime autorisée à accéder à des données, puisse aussi avoir le droit d'accéder aux clés de chiffrement. En l'état actuel des choses, il n'est pas possible d'apprécier l'issue d'un tel litige. Deuxièmement, les méthodes de chiffrement élaborées et capables d'accroître la protection d'accès aux données auraient pour conséquence de détériorer les fonctionnalités des services cloud.

Les conflits normatifs ne traitent pas pleinement ces problématiques

La restitution des données en ligne des administrations suédoises à un pays étranger en vertu du CLOUD Act ou d'une législation similaire a occupé une grande partie du débat en Suède. Nous avons remarqué que, depuis un an, les discussions autour de l'utilisation des services cloud publics proposés par des entreprises privées se sont malheureusement concentrées sur une question déjà élucidée, à savoir les attributs et limites de la règlementation sur la protection des données et la confidentialité des données. Des problématiques plus urgents ont, quant à elle, totalement été occultées.

Nous estimons qu'il est désormais grand temps d'orienter le débat vers des problématiques plus essentielles. En tant qu'administration publique, nous nous devons de questionner puis de répondre aux problématiques liées aux *risques* d'accès étrangers à nos données dans le cas où ces pays étrangers ajusteraient unilatéralement leurs législations dans un tel but. Ce risque n'est pas aujourd'hui considéré comme essentiel. Nous devons aussi nous écarter des conflits normatifs existants afin de comprendre ces risques et si les réponses apportées sont convenables. Plusieurs questions rendent compte de cette problématique et nous en avons aujourd'hui identifié quatre :

Est-il pertinent et envisageable que les autorités suédoises confient des activités de portée sociétale à un prestataire de services répondant d'une juridiction d'un autre État et autorise *de facto* cet État à récupérer les données de ces services sans l'autorisation de la Suède ?

Est-il pertinent et envisageable que les autorités suédoises confient à un partenaire commercial la procédure de contestation dans le cas où des données confidentielles seraient sollicités par une autorité étrangère ?

Est-il pertinent et envisageable que les autorités suédoises n'aient ni la maîtrise, ni le droit de déterminer quels pays pourraient récupérer des données essentielles en accord avec les lois du pays dont est originaire le prestataire de services ?

Est-il convenable que la Suède cède ses compétences législatives sur le traitement de ses données à un autre pays après que ces informations aient été transférées vers un service cloud ?

Nous estimons que ces questions doivent être abordées avec beaucoup de précaution lors des décisions relatives au choix d'un prestataire de services cloud par une administration publique. Ces questions nous conduisent vers une problématique plus urgente, c'est-à-dire notre responsabilité commune envers la société suédoise et la protection des services essentiels à son fonctionnement.

L’utilisation des services cloud publics proposés par les entreprises privées accroît la vulnérabilité des données et les risques de violation de la vie privée

Ce Livre blanc se concentre sur l’utilisation des services cloud publics proposés par des entreprises privées. Il existe un grand nombre de problèmes liés à la protection du fonctionnement de la société suédoise et de la vie privée lors d’une éventuelle externalisation des services informatiques en ligne. Les problématiques suivantes sont celles que nous considérons comme essentielles.

Augmentation de la vulnérabilité générale

Comme nous l’avons déjà précisé, l’utilisation de services cloud proposés par des entreprises privées - exactement comme tout autre type d’externalisation – est un facteur de risque de cyberattaques plus complexes lancées ou soutenus par un État étranger. Il est également important de considérer qu’une quantité importante de données des administrations suédoises sont stockées chez un seul et même prestataire de services puisque le marché est dominé par un nombre restreint de prestataires. Cette situation et la possibilité de perturbations informatiques accroît la vulnérabilité pour un grand nombre d’administrations simultanément. Les risques d’attaques des systèmes d’information augmentent rapidement à partir du moment où de grandes quantités d’informations sont stockées à un même endroit[116] et les administrations n’ont pas accès aux informations de connexion aux données suédoises des prestataires de services. Si le secteur public suédois n’a pas de vue d’ensemble sur cette situation, il n’existe aucun tableau général des relations des administrations avec les prestataires de services ; ce qui accroît encore un peu plus les risques auxquels est confrontée la société.

Ces risques surgissent que les services soient en ligne ou non. Puisque plusieurs services cloud peuvent être proposés à un grand nombre de clients aussi d’une même administration, les risques sont cependant plus importants lors de la mise en place de services cloud plutôt que lors de l’utilisation d’autres processus bureautiques[117].

Hausse du risque d’intrusions non autorisées

Le CLOUD Act et les législations similaires ont contribué à lancer le débat sur le contrôle des administrations suédoises de leurs propres données. Ce genre de législation n’est cependant pas la seule problématique de sécurité liée à l’utilisation de services cloud proposés par des entreprises privées. Cette problématique n’en est pas moins illustrée par les révélations de 2013 sur la surveillance américaine des citoyens européens. Tout aussi important, n’oublions pas de rappeler les activités de surveillance systématique de la Russie, de la Chine et de l’Iran, qui exigent des autorités suédoises une coopération systématique en matière de cybersécurité[118]. Dans le contexte de sécurité actuel ainsi que du développement des innovations des technologies de l’information, le risque d’accès d’autorités étrangères aux données de portée sociétale confidentielles – ou protégées par la RGPD – suédoises est désormais pris beaucoup plus au sérieux qu’il ne l’a jamais été.

---

[116] Il faut bien évidemment tenir compte des risques liés à la concentration de données lors de l’élaboration de solutions informatiques internes destinées à une ou plusieurs administrations.

[117] Il faut aussi noter que les risques liés à la concentration des données et de fonctionnalités existent que le prestataire de services soit public ou privé.

[118] Voir notamment Kristiansson Stefan, *Om underrättelsehotet mot Sverige, Frivärld* (La menace des services de renseignements en Suède, Le monde libre), Rapport No. 7 2019.

Il faut ajouter à cela que les prestataires de services, au nom de l'entretien et de la mise des jours de leurs services, accèdent aussi aux données télémétriques des clients. Dans les cas de souscription à un service cloud via lequel le fournisseur a, par définition, un accès direct au données, cette collecte de données télémétriques doit être sérieusement prise en compte. Une enquête remise aux autorités néerlandaises indique que les prestataires de services ont collecté des données sans autorisation explicite de la part de l'utilisateur et fait infraction au RGPD sans que cela soit ne précisé dans les conditions des contrats de prestation de service[119]. Ces infractions inquiètent et altèrent la relation de confiance nécessaire aux administrations et aux prestataires de services afin de satisfaire un niveau protection des données satisfaisant. Même si ces données de télémétrie ne sont utilisées par le prestataire de services que dans le but d'améliorer la fonctionnalité du service, il est alarmant que les clients n'aient ni droit de regard sur le processus, ni possibilité de contrôler la valeur des données collectées et ainsi faire objection ou limiter la collecte de ce type de données. Il est aussi extrêmement grave que des données relatives aux activités de portée sociétale de la Suède, des données à caractère personnel, confidentielles ou non, puissent être accessibles de cette manière à des personnes non autorisées. L'exemple de Cambridge Analytica nous rappelle à quel point l'accès à de grandes quantités de données peut avoir un effet néfaste sur les valeurs les plus fondamentales d'un État démocratique[120] lorsque des fournisseurs manipulent des données personnelles sans en informer qui que soit dans leurs conditions d'utilisation, et que ces données sont rendues accessibles à des tiers.

Une Habilitation et un suivi difficile voire impossible du personnel

Les contrôles et habilitations sont d'autant plus compliqués si les données confidentielles d'une administration suédoise sont traitées par des prestataires dont les services informatiques sont administrés par du personnel basée l'étranger. Afin de pouvoir assurer un taux de disponibilité élevée, les fournisseurs de services cloud publics internationaux ont, dans un grand nombre de cas, du personnel technique dans plusieurs pays différent. Ce personnel est rarement en charge d'un seul client spécifique alors que l'habilitation n'est valable que pour une personne. Même si le prestataire de services met à disposition du client une équipe dont le personnel est clairement identifié, la vérification de registres, qui constitue une partie importante du processus d'habilitation, ne sera pas pertinente pour ces personnes non domiciliées en Suède.

Ce manquement doit être compenser par un développement des autres étapes de l'habilitation. Il est également important de réfléchir sur les possibilités des autorités de suivre concrètement les contrats de sécurité des prestataires de service cloud publics mondiaux dans les cas où le personnel en contact avec les données est basé à l'étranger.

---

[119] Ministry of Justice and Security Strategic Vendor Management Microsoft, *DPIA Office 365 ProPlus version 190*5 *(June 2019) Data protection impact assessment on the processing of diagnostic data*, voir aussi Annexe 8.

[120] Cambridge Analytica était une entreprise de conseils en stratégie de communication politique dotée d'outils d'analyses de données. Cette entreprise a fait faillite après qu'ait été révélée l'utilisation, en infraction aux conditions générales, de Facebook à des fins d'identification et manipulation d'électeurs potentiels. On estime que les activités de cette entreprise ont influencé le résultat des élections, notamment aux États- Unis, en Grande-Bretagne et aux Philippines. Pour en savoir plus : Auchard Eric, *Cambridge Analytica stage-managed Kenyan president's campaigns: UK TV, Reuters,* 20.03.2018, Cadwalladr, Carole, *The Great British Brexit robbery how our democracy was hijacked*, The Guardian, 07.05.2017 et Gutierrez Natashya, *Did Cambridge Analytica use Filipinos' Facebook data to help Duterte win?* Rappler, 05.04.2018.

Des évaluations de risque de plus en plus difficiles

On recense enfin d'autres incertitudes au sujet du CLOUD Act et notamment la manière dont la loi serait applicable aux autorités suédoises et les conditions dans lesquelles ces autorités seraient contrainte de restituer les données les concernant. Ajoutons à cela la variabilité des arbitrages des tribunaux américains confrontés au refus des prestataires de restituer des données lors d'un conflit opposant intérêts suédois et américains. Il est aussi incertain et difficile de prédire les conditions et les pays avec lesquels les autorités américaines passeront des accords de restitution de données en vertu du CLOUD Act[121].

Dans ces circonstances, l'Agence suédoise de la sécurité sociale, Försäkringskassan, constate qu'il est aujourd'hui impossible d'avoir une idée claire des conséquences qu'aurait pour les administration suédoises l'utilisation de services cloud de fournisseur soumis à la législation américaine - ce qui est le cas de nombreux acteurs du marché. Il sera aussi difficile, en vue des appels d'offres de services cloud, d'élaborer des analyses d'impact RGPD ainsi que des analyses objectives de risque et de vulnérabilité liées à la transmission d'une des parties des activités des administration à un prestataire de services privé. Le CLOUD Act sert d'exemple, mais ces problèmes subsistent pour tous les services cloud fournis par les prestataires de services étrangers des pays dont les lois donnent aux autorités accès aux données des prestataires concernés. Les risques deviennent d'autant plus difficiles à estimer que ces services peuvent aussi consister en un certain nombre de services externes proposés par d'autres prestataires, dont les subordinations juridiques sont amenées à changer. Une problématique d'autant plus complexe dans le cas où le pays de domiciliation du prestataire reverrait ses lois. Il est aussi possible que le pays de domiciliation du prestataire passe une convention avec un pays tiers soumis à une législation semblable à celle du CLOUD Act.

Risques liés à la protection de la vie privée

Une vulnérabilité des autorités accrue implique *de facto* un risque pour la protection de la vie privée. Prenons par exemple les risques liés aux accès de personnes non autorisées aux données, dans les cas où il ne serait pas possible d'avoir une vue d'ensemble sur tous les sous-traitants du service et que les données soient utilisées à d'autres fins que celles prévues selon le contrat.

Comme l'a constaté le Comité sur l'intégrité, les administrations traitent souvent une grande quantité de données à caractère personnel et ces données sont souvent des renseignements personnels confidentiel en rapport à la vie privée des personnes concernées. Perdre le contrôle de ces données et ne pas maîtriser les caractéristiques du traitement de ces données sur le nuage informatique constitue, selon nous, un risque particulièrement élevé pour l'intégrité des administrations.

---

[121] On peut cependant noter qu'une première convention, passée avec la Grande-Bretagne en octobre 2019, sera présentée au Congrès des Etats-Unis. Voir Department of Justice, Office of Public Affairs, U.S : And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online 03.10.2019.

Prise de position de la Försäkringskassan au sujet de l'utilisation future de services cloud proposés par des entreprises privées

Comme nous l'avons exposé ci-dessus, il existe aujourd'hui une quantité non négligeable de problématiques liées à la sécurité lors de l'utilisation de nombreux services cloud proposés par les grandes entreprises privées du marché. Un grand nombre des services cloud améliore la sécurité technique et l'accessibilité aux données mais ces évolutions ne compensent cependant pas les risques de perte de contrôle des données ; risques auxquels s'exposent les autorités suédoises. Le point de départ de toute dématérialisation des services des administration doit être, selon nous, un refus clair de tout niveau de sécurité des services cloud inférieur à celui des équipements actuels des administrations.

Selon les observations de la Försäkringskassan sur les questions liées à la sécurité des données ainsi qu'à la pertinence des nouvelles technologies de l'information et sans tenir compte des conflits normatifs, que les services numériques stratégique nécessaire au fonctionnement de nos activités de portée sociétale doivent dépendre du contrôle de l'administration publique. Dans les faits, cette prise de position rappelle notamment que la Försäkringskassan ne transfèrera pas l'administration de ses systèmes à des entreprises privées placées sous la juridiction d'un pays dont la législation est semblable au CLOUD Act. Ce point de vue sera naturellement corrigé dans le cas où le groupe d'étude, récemment mandaté par l'État suédois et chargé d'examiner les services informatiques publique sécurisée ainsi que leur rentabilité, réévaluera nos conclusions et notre point de vue.

Nous ne voulons pas dire que la seule solution aux problématiques numériques est une gestion publique des infrastructures. Pour certains services des administrations publiques, des services cloud proposée par des entreprises privées pourraient dans les circonstances actuelles, convenir aux appels d'offres proposés aux d'entreprises privées de Suède ou, dans certains cas, aux entreprises européennes à condition que les appels d'offres autorisent ces modalités. Chaque solution devra être étudiée au cas par cas et devra être considéré en fonction des spécificités du prestataire étranger, et se baser sur le type d'administration concernée ainsi que le degré de sensibilité des données traitées. Il est aussi nécessaire de s'assurer que les conditions d'application des contrats reflètent un niveau de sécurité convenable et que l'administration des données ne soient pas transmises à un pays tiers. Dans le cas où des services privés seraient utilisés, les exigences légales doivent naturellement être prises en compte.

Certaines activités de portée sociétale exigent, selon nous, un contrôle et une gestion plus stricte de la part de l'État. Dans le cas de la Försäkringskassan, citons par exemple nos activités stratégiques et liées à la sécurité de l'État. Pour les systèmes informatiques de ces services, notre objectif est de nous assurer que l'administration informatique de ces services soit réglementée et gérée par l'État.

Pour atteindre un niveau de sécurité satisfaisant des informations numérisées des décisions des administrations, la Försäkringskassan estime que la Suède doit aussi participer au débat d'ensemble sur la portée de la protection numérique.

La souveraineté numérique : vers une minimisation de la vulnérabilité de l'État

Introduction

Une part croissante des activités de portée sociétale de la Suède dépend de la continuité de fonctionnement de nombreux systèmes informatiques. Dans de tels circonstances, il est important de prendre très au sérieux les risques identifiés par la Direction général de la sécurité suédoise liés à l'évolution des technologies et à l'externalisation des technologies de l'information. La protection des systèmes informatiques des autorités a aussi trait à la politique de défense de la Suède dans un société de plus en plus dépendante des évolutions technologiques et où la différenciation entre les infrastructures civiles et militaires est de plus en plus incertaine.

La stratégie numérique de la Suède met en avant la nécessité pour les administrations suédoises de pouvoir répondre de la sécurité de leurs systèmes informatiques et de l'intégrité des personnes.

Nous constatons que cette problématique ne peut être traitée sans comprendre notre dépendance des systèmes informatiques, aux interdépendances entre les différentes fonctions sociétales de nos services – qu'elles soient considérées comme fondamentales ou non – et la vulnérabilité dont ces dépendances sont à l'origine. Pour que cette problématique soit traitée correctement, nous estimons que la notion de souveraineté numérique et de contrôle des environnements informatiques doit désormais être mise en avant de manière plus significative.

La souveraineté numérique de la Suède doit être à l'ordre du jour

Comme l'a constaté l'Autorité nationale suédoise pour la protection civile MSB, la notion de souveraineté nationale relève de la capacité de l'État à sécuriser le contrôle du territoire, les processus décisionnels politiques et l'approvisionnement en biens de première nécessité. Dans les cas où la Suède ne pourrait pas assurer sa souveraineté, nous ne pourrions pas non plus assurer les services essentiels à la société ainsi que la défense de la démocratie et la sécurité juridique du pays.

Des échanges toujours plus dématérialisés nécessitent un contrôle des données des activités de portée sociétale et revêtent une importance toujours croissante pour l'indépendance de notre pays. Dans de telles circonstances, nous estimons qu'il est impératif pour la Suède de revoir la définition de souveraineté numérique. Tout en maintenant sa souveraineté au sens traditionnel du terme, la Suède doit établir les conditions dans lesquelles sa souveraineté numérique sera assurée.

La décision du gouvernement suédois de missionner l'Office de radiocommunications de la défense nationale, les Forces armées, l'Autorité nationale suédoise pour la protection civile MSB et la Direction générale de la sécurité de se préparer à créer un centre national de cybersécurité constitue un premier pas en ce sens[122]. Comme l'a constaté le comité préparatoire de la défense Försvarsberedningen, le développement des technologies de l'information et les progrès en matière de cybersécurité apporteront de meilleures possibilités pour assurer notre souveraineté.

---

[122] Ministère suédois de la défense, *Uppdrag inför inrättandet av ett nationellt cybersäkerhetscenter* (Commission pour la création d'un centre national de cybersécurité), Fö2019/01000/SUND, 26.09.2019.

Pour maintenir cette souveraineté numérique, il est cependant nécessaire que la Suède adopte une définition générale et détermine le contenu de la notion. Les discussions de l'Union Européenne et de ses États membres abordées par le gouvernement suédois lors de l'élaboration de la proposition de loi sur la protection de la sécurité de la Suède et des radio-transmissions ont notamment concerné l'autonomie et le contrôle total des systèmes informatiques, de leur utilisation et de leur élaboration. Elles se sont aussi penchées sur le contrôle des données stockées informatiquement et sur les personnes autorisées à y accéder. Nous considérons que ces discussions peuvent servir de point de départ à la définition de la notion de souveraineté, à laquelle, nous Suédois, adhérerons. Définir clairement la notion de souveraineté est primordial pour pouvoir sécuriser nos services et activités de portée sociétale contre les attaques étrangères et réduire notre dépendance aux services privés du marché. L'objectif est de protéger notre société ainsi que les droits des citoyens.

Tout comme pour les autres aspects relatifs à la notion de souveraineté, il existera toujours différents niveaux de dépendance, tant bien vis-à-vis d'autres États que vis-à-vis des acteurs privés. Il n'est pas avéré que la souveraineté numérique suppose une indépendance totale vis-à- vis d'entreprises privées et étrangères mais l'environnement changeant dans lequel nous vivons et la vulnérabilité que peut entraîner notre dépendance vis-à-vis des systèmes informatiques est, pour nous en tant que nation, à l'origine des questions nous allons poser ci-dessous.

Quel est le niveau de contrôle des services informatiques à maintenir pour assurer le fonctionnement des services essentielles des administrations suédoises ?

Pour répondre à cette question, nous devons tout d'abord tenir compte du fait que le risque d'attaque dépend du contrôle et des services que nous ne maîtrisons plus. Un autre aspect important de cette problématique est la prise en compte, au cas par cas, de la dépendance cumulée des administrations du pays envers un prestataire de services ou un service en particulier et des effets d'un enfermement que pourraient entraîner une telle dépendance. Dans le cadre de nos observations, nous devons aussi peser le poids de certains facteurs que nous considérons aujourd'hui comme ambigu. Compte tenu de la situation sécuritaire et politique actuelle, nous ne pouvons pas exclure le risque pour la Suède, d'être impliquée dans des conflits étrangers et que ces changements politiques n'affectent la vulnérabilité numérique du pays. Nous devons aussi tenir compte de la confiance du public envers les administrations. Si les autorités suédoises privilégient les rendements financiers et les solutions à court terme à la protection des services des administrations et à la vie privée des citoyens, nous risquerions de perdre la confiance de la société envers les administrations de l'État.

La souveraineté numérique de la Suède a besoin d'une gestion des services claire et un plan d'action sur le long terme

Quel que soit la définition et le contenu de la notion de souveraineté numérique, il est décisif de mener ce débat à un niveau global et que toutes les administrations publiques suédoises soit considérées de même nature. La stratégie globale de la Suède pour protéger nos fonctions de portée sociétale et ses environnements informatiques est aujourd'hui pratiquement constituée de toutes les décisions – réfléchies et imprudentes – prise par chaque administration. La Försäkringskassan estime que cette attitude est trop passive, aussi bien lors des décisions administrations publiques face aux opportunités de dématérialisation que pour les choix indispensables à la protection des activités de portée sociétale. Nous avons aujourd'hui la possibilité de soutenir les initiatives de l'Allemagne et des Pays-Bas pour renforcer le contrôle des administrations publiques sur les données et aussi

réduire notre dépendance face aux fournisseurs informatiques privés. Nous renverserons ainsi la tendance actuelle qui consiste en un délaissement du contrôle des services des administrations publiques au profit d'entreprises et d'États étrangers.

Nous sommes clairement convaincus que l'administration public peut continuer à bénéficier de tous les avantages de la dématérialisation et de la numérisation tout en conservant son indépendance. Sur le court terme, nous avons aussi confiance dans les innovations des acteurs privés et publics, à condition que les ressources nécessaires soient suffisantes et que les caractéristiques des collaborations soient clairement définies. Aucun résultat ne pourra être validé sans une analyse minutieuse des faits et des décisions des hiérarchies centrales.

Le temps est désormais aux décisions et à la définition des moyens nécessaires à mettre en œuvre afin de protéger la souveraineté numérique de la Suède. Une conduite claire de l'État ainsi qu'un plan de protection des systèmes informatiques de nos fonctions de portée sociétale sont désormais indispensables. Pour cette raison, nous estimons que la stratégie numérique de la Suède doit être complétée par une prise de position plus claire sur la souveraineté nationale. Ce n'est que lorsque cette perspective sera en place que les administrations suédoises pourront pleinement prendre part à la sécurisation de leurs activités.

Amélioration rapide des accès aux infrastructures physiques

Pour assurer la sécurisation des services informatiques des administrations suédoises, il est impératif de réunir tous les conditions pratiques nécessaires. Nous n'avons pas aujourd'hui la capacité d'assurer au secteur civil de l'administration publique un accès à des espaces informatiques et à des communications sécurisées. L'Administration suédoise des fortifications Fortifikationsverket a analysé les conditions de mise en place des grappes informatiques – *data cluster* – régionales et l'Administration suédoise des postes et télécommunications, Post- och Telestyrelsen PTS, a présenté au gouvernement, une proposition de modèle d'administration et de coordination des espaces informatiques sécurisés. Aucune de ces propositions n'a cependant été réalisée à ce jour.

Le fait que gouvernement suédois ait récemment créé un groupe d'enquête sur une gestion informatique sécurisée et rentable de l'administration publique est bien entendu une bonne chose [123].

Nous estimons cependant que ce type de propositions nécessite un accès à une infrastructure physique dont nous ne disposons pas aujourd'hui et dont la réalisation prendra plusieurs années à partir du moment où les décisions seront prises. Pour cette raison, nous considérons qu'il est très raisonnable que le gouvernement, parallèlement à l'enquête en cours, valide les propositions de l'Administration suédoise des fortifications et de la PTS. Dans le cas contraire, la mise en place d'une politique informatique d'État globale sera retardée et entraînerait une augmentation des vulnérabilités des services informatiques des administrations. Nous vous aussi souligner dans ce contexte, qu'une infrastructure informatique physique sécurisée - espaces informatiques et de communications sécurisés – ne doit pas se limiter aux administrations d'État. Il n'est pas envisageable que les autorités municipales et certaines entités privées chargées des services informatiques de portée sociétale n'aient pas accès à un niveau de sécurité adéquat.

[123] Voir directive 2019:64.

Les acteurs publics suédois doivent s’unir pour s’assurer que les services cloud soient proposés à des conditions de sécurité adéquates

Nous sommes conscients que la gestion des services cloud publics que nous réclamons implique des autorités suédoises une réévaluation des investissements et des décisions liés à leurs activités d'ores et déjà déterminés. Ces réajustements concernent aussi la Försäkringskassan, qui doit revoir des projets en cours, prévus ou déjà réalisés. Nous estimons cependant que la sécurité de la Suède et le fonctionnement des administrations sont essentiels et ne peuvent être soumis aux considérations d’investissements passés. Quels seraient ces coûts, si la société suédoise était attaquée et que nous échouions à maintenir la protection de nos activités de portée sociétale ainsi que celles liées à la vie privée de nos citoyens ? Compte tenu de la dépendance des services d’une part, et des décisions - défavorables voire même illégales – que les administrations suédoises ont prise ou sont en passe de prendre d’autre part, il sera délicat de maintenir le fonctionnement des services aux conditions que nous réclamons. Des solutions à ces problématiques existent mais l’ensemble du secteur public doit y adhérer. Grâce à une telle coordination, les fournisseurs privés auront aussi une image plus claire des exigences du secteur public et pourront plus facilement, via des investissements cohérents, ajuster les services sollicités.

Les administrations suédoises sont amenées à travailler conjointement

Les services cloud accélèrent les échanges et répondent largement aux attentes du public d’une administration publique simple et accessible. Correctement paramétrés, ces services contribuent aux efforts du service public à l’égard des exigences de mise à disposition des évolutions de la dématérialisation du gouvernement.

Le maître-mot est bien ici « correctement paramétrés ». Les services utilisés par les autorités suédoises doivent être adaptés aux besoins et aux exigences de sécurité et non pas s’appuyer sur les solutions déjà existantes proposées par les entreprises privées. L’évolution rapide des technologies de l’information ne doit pas non plus faire accepter des clauses contractuelles standard qui ne répondent pas aux exigences des législations en vigueur et qui ne garantissent pas la sécurité et l’intégrité des utilisateurs.

Comment aller en ce sens ? La Försäkringskassan souhaite rappeler que le secteur public suédois est dans son ensemble un donneur d’ordre important et qu’il dispose de leviers suffisants pour clairement formuler ses exigences lors les appels d’offre des services concernés. Une administration publique unie pourvu d’un message clair ne peut pas être ignorée. Grâce à cahier des charges concis et élaboré communément, nous ne nous contentons pas seulement d’influencer les acteurs du marché mais donnons aussi la possibilité à de nouveaux acteurs d’élaborer des solutions innovantes répondant à nos exigences.

Les exemples qui vont dans ce sens ne manquent pas. Pour répondre aux exigences du RGPD, le gouvernement néerlandais a obtenu un avenant au contrat type Microsoft Office de Microsoft.

L’ambition des Pays-Bas est de faire en sorte que tout le secteur public de l’Union Européenne puisse bénéficier de cet avenant. Les administrations suédoises arriveront à bénéficier des efforts néerlandais si elles travaillent ensemble dans le cadre de l’élaboration des cahiers des charges.

L'initiative néerlandaise ne résout certes que les problématiques légales de la protection des données et la Suède doit aussi, sur le plan national et international, se joindre aux initiatives de coopération entre les pays membres de l'Union Européenne pour obtenir de meilleures conditions contractuelles de la part des grands prestataires de services[124]. Cette initiative nous permettra d'accroître notre capacité d'incitation et ainsi influencer le marché à proposer des services répondant à la préservation de la gestion des données plutôt que de la transférer à des acteurs privés ou à des pays étrangers[125]. Pareillement, nous devons nous assurer que les services privés s'adaptent à la législation suédoise ainsi qu'aux modalités que la Suède se doit d'exiger pour conserver le contrôle de ses activités. Aux Pays-Bas, l'avenant susmentionné a été négocié par une autorité désignée à laquelle a été donnée la responsabilité de représenter les intérêts des Pays-Bas. Face à la tâche à laquelle la Suède doit faire face, le pays à tout intérêt à coordonner ses prises de décision de manière similaire.

Compendium

L'Agence suédoise de la sécurité sociale, Försäkringskassan, estime est que les débats sur les conditions d'utilisations des administrations des services cloud publics proposés par des acteurs privés n'a pas été correctement orientée. La Försäkringskassan estime qu'il existe des conflits normatifs entre les législations étrangères et européenne en rapport à la vulnérabilité des données stockées chez les prestataires de services. Ces discussions ne doivent cependant pas uniquement se concentrer ni sur ces conflits normatifs, ni sur le fait que les autorités des pays étrangers profitent de ces moyens d'accès aux données des administrations suédoises. Le débat doit au contraire se développer autour de l'engagement conjoint des administrations et de la pertinence des services cloud en vue d'assurer la protection des services essentielles à la société.

Nous estimons que les services cloud proposés par les entreprises privées et utilisés par les administrations publiques augmentent la vulnérabilité générale des services ainsi que les risques d'accès de personnes non autorisées aux données. L'utilisation de ces services cloud pose aussi des problématiques considérables – et parfois inéluctables – liées à l'habilitation des personnes chargées des activités stratégiques et au suivi des contrats de sécurité. Pareillement, le CLOUD Act et les lois du même type ne permettent pas de procéder avec exactitude à des analyses de retombés ou de vulnérabilité. Ajoutons à cela la problématique selon laquelle les administrations suédoises se débarrasseraient de la gestion des données de leurs services au profit d'entreprises privées ou d'autorités étrangères.

[124] Citons The Hague forum for Cloud contracting, (Forum de La Haye des marchés des services cloud), organisé par le ministère de la justice des Pays-Bas et le Strategic Vendor Management, dont la prochaine édition aura lieu au printemps 2020.

[125] Un service de ce type pourrait être élaboré à partir d'un service cloud on-site pour permettre à l'administration concernée de souscrire à une solution cloud paramétrée sur ses propres serveurs.

Compte tenu des conclusions de ce Livre Blanc, la Försäkringskassan ne délèguera pas l'administration de ses systèmes informatiques à des entreprises privées dépendantes de législations étrangères similaires à celles du CLOUD Act. Les conditions d'émission des appels d'offres des services informatiques peuvent cependant être déterminées par des acteurs suédois ou européens et seront examinées au cas par cas en fonction de leurs pertinences ainsi que du type d'activités, du degré de sensibilité des données et des conditions contractuelles applicables. Pour la Försäkringskassan, Les services stratégiques doivent en revanche rester sous la tutelle de l'État.

Pour que les administrations suédoises soient en mesure de maintenir un niveau de protection adéquat des données numériques, la Försäkringskassan estime que l'État suédois doit amorcer un débat sur le contenu et la définition de la notion de souveraineté numérique. Nous sommes d'avis que l'un des points de départ de ces discussions doit être la protection des services essentiels à la société et son exposition à d'éventuelles attaques ainsi que la nécessité de réduire la dépendance vis-à-vis des services privés. Nous pourrons ainsi évaluer la confiance que nous accorderons les citoyens dans le cadre de la gestion des leurs données personnelles. Il est désormais temps que la Suède renonce à son attitude passive face aux problématiques de souveraineté numérique et définisse clairement cette notion pour la gestion des activités quotidiennes des administrations. Ces changements stratégiques nécessitent une orientation claire et un plan d'action sur le long terme qui couvre la totalité du secteur public. Ce plan d'action doit également assurer la mise en place d'une infrastructure sécurisée, d'espaces informatiques et de communications sûres, ainsi que d'un modèle de gestion durable de cette infrastructure.

Cette stratégie ne doit pas ralentir la numérisation du secteur public. Nous sommes convaincus que la force d'un secteur public doté de ressources suffisantes et de conditions claires peut contribuer à l'adoption par les autorités suédoises des avancés de la numérisation sans mettre en jeu la sécurité des services des administrations publiques. Grâce à une coopération national et européenne, les administrations suédoises pourront veiller à ce que les services privés choisis soient adaptés à nos choix, nos législations et à un niveau de sécurité adéquat au contrôle de nos activités. Tout initiative doit toujours être celle des autorités et non celle des entreprises privées susceptibles de déterminer les conditions d'application et les paramètres des services adoptés.

Les références

Abelson Harold et autres : *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*, (MIT-CSAIL-TR-2015-026), novembre 2015

Access Now, European Digital Rights (EDRi), Electronic Frontier Foundation, Panoptykon Foundation, *Letter to US Congress*, 19.03.2018 https://edri.org/files/cross-borderaccesstodata/lettertocongress_CLOUDAct_20180319.pdf

Amnesty International États-Unis, Electronic Frontier Foundation et Human Rights Watch et autres, Lettre au Congrès des État-Unis, 12.03.2018. https://www.eff.org/document/coalition-letter-opposing-cloud-act (Collectée le 02.09.2019).

Auchard Eric Reuters, *Cambridge Analytica stage-managed Kenyan president's campaigns*: UK TV, 20.03.2018 https://www.reuters.com/article/us-facebook-cambridge-analytica- kenya/cambridge-analytica- stage-managed-kenyan-presidents-campaigns-uk-tv- idUSKBN1GV300 (Collectée le 10.11.2019)

Autoriteit Persoonsgegevens (Département néerlandais des affaires politiques), *Summary of Investigation Report Public Version Microsoft Windows 10 Home and Pro*, Août 2017

AWS, AWS Service nuagique du gouvernement pour l'État américain https://aws.amazon.com/govcloud-us/ (Collectée le 10.09.2019)

AWS, *Global Infrastructures Regions and AZs* https://aws.amazon.com/about-aws/global- infrastructure/regions_az/?p=ngi&loc=2 (Collectée le 10.09.2019)

AWS, *Information Request Report* https://d1.awsstatic.com/certifications/Information_Request_Report_June_2019.pdf (Collectée le 10.09.2019)

AWS Protection Data using encryption https://docs.aws.amazon.com/ AmazonS3/latest/dev/UsingEncryption.html (Collectée le 10.11.2019)

Bellanger Pierre, *De la souveraineté en général et de la souveraineté numérique en particulier*, Les Échos, 30.08.2011

Fredrik Blix et Richard Brolin, *Grönt ljus för kommuner, regioner et statliga myndigheter att överväga molntjänster* (Feu vert pour les municipalités, les régions et les autorités publiques pour envisager les services cloud), Cybercom Group, 04.07.2019. https://www.cybercom.com/sv/Om- Cybercom/Bloggar/digital-sakerhet/gront-ljus- for-kommuner- regioner-och-statliga-myndigheter- att-overvaga-molntjanster/ (Collectée le 04.09.2019)

Bondcap, *Internet Trends 2019* https://www.bondcap.com/report/itr19 (Collectée le 20.09.2019)

Bundesministerium des Innern, für Bau und Heimat, *BMI intensiviert Aktivitäten zur Stärkung der digitalen Souveränität in der öffentlichen Verwaltung*, 19.09.2019 https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2019/09/digitale-souveraenitaet-oeff-verwltg.html (Collectée le 20.09.2019)

Bundesministerium für Wirstschaft und energie, Digital Gipfel https://www.de.digital/DIGITAL/Navigation/DE/Service/Digital-Gipfel/Digital-Gipfel.html (Collectée le 20.09.2019)

Butler Brandon, *What is hybrid cloud computing? The benefits of mixing private and public cloud services, Networkworld*, 2017-10-17 https://www.networkworld.com/article/3233132/what-is-hybrid-cloud-computing.html (Collectée le 09.11.2019)

Cadwalladr Carole, *The Great British Brexit robbery how our democracy was hijacked* (La grande escroquerie du Brexit, comment notre démocratie a été détournée), The Guardian, 2017-05-07 https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked- democracy (Collectée le 10.11.2019)

Corey Varma, *Encryption vs. Fifth Amendment* http://www.coreyvarma.com/2015/07/encryption-vs-fifth-amendment/ (Collectée le 17.09.2019)

Conseil des barreaux européens (CCBE) *Assessment of the US CLOUD Act,* Avis sur le CLOUD Act, 28.02.2019

Daskal Jennifer, Unpacking the CLOUD Act, EUCRIM, 31.01.2019 https://eucrim.eu/articles/unpacking-cloud-act/ (Collectée le 02.09.2019)

Department of Justice, Office of Public Affairs, *U.S.. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online*, 2019-10-03 https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists (Collectée le 09.10.2019)

Digital Gipfel, Plattform Innovative Digitalisierung der Wirtschaft: Fokusgruppe Digitale Souveränität in einer vernetzten Gesellschaft, *Digitale Souveränität und Künstliche Intelligenz - Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen*, 2018 https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2018/p2-digitale- souveraenitaet-und-kuenstliche-intelligenz.pdf? blob=publicationFile&v=5 (Collectée le 15.10.2019)

Director of National Intelligence, *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 08.06.2013 https://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf (Collectée le 03.09.2019)

Rapport de ministère suédois Ds 2017:66, *Motståndskraft - Inriktningen av totalförsvaret et utformningen av det civila försvaret 2021-2025* (Force de résistance : orientation de la défense totale et structure de la défense civile de 2021 à 2025)

Rapport de ministère Ds 2018:6, *Granskning av Transportstyrelsens upphandling av it-drift (*Examen de l'appel d'offre de services informatiques de la Direction suédoise des transports)

Délégation à l'informatique, *Strategi för myndigheternas arbete med e-förvaltning* (Rapport des commissions officielles de l'État suédois, SOU 2009:86)

Délégation suédoise à l'informatique, *Så enkelt som möjligt för så många som möjligt* (Aussi simple que possible pour le plus de gens possible)(Rapport des commissions officielles de l'État suédois, SOU 2011:67)

Comité Européen de la Protection des Données (EPDB-EDPS), *Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection* , 10.07.2019,

Autorité nationale de la gestion financière Ekonomistyrningsverket, *It-kostnadsmodell* (Modèle de coûts informatiques)(2014:50), 01.10.2014

Electronic Frontier Foundation, *EFF and 23 Groups Tell Congress to Oppose the CLOUD Act*, 11.03.2018 https://www.eff.org/deeplinks/2018/03/eff-and-x-groups-tell-congress-oppose- cloud-act (Collectée le 08.08.2019).

Electronic frontier Foundation, *EFF in the United States Court of Appeals for the Eleventh Circuit Case:* 11-12268

Electronic frontier Foundation, *The U.S. CLOUD Act and the EU: A Privacy Protection Race to the Bottom*, 09.04.2018 https://www.eff.org/de/deeplinks/2018/04/us-cloud-act-and-eu-privacy- protection-race-bottom#_ftn1 (Collectée le 07.08.2019)

eSamverkansprogrammet, *Kompletterande information om molntjänster* (Complément d'informations sur les services cloud), 20.09.2019

eSamverkansprogrammet, *Rättsligt uttalande om röjande et molntjänster* (Avis juridique sur la divulgation et services cloud), VER 2018:57, 23.10.2018

eSamverkansprogrammet, *Röjandebegreppet enligt offentlighets- och sekretesslagen*, (La notion de divulgation selon la loi sur la publicité et le secret), VER 2015-190, 17.12.2015

Parlement européen, Résolution du Parlement européen du 5 juillet 2018 sur l'adéquacité de la protection de la vie privée dans l'Union Européenne et aux États-Unis (2018/2645(RSP))

Parlement européen, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices* (PE 583.137)

Comité Européen de la Protection des Données, *Riktlinjer 2/2018 för undantagen i Artikel 49 enligt förordning 2016/679, antagna den 25 maj 2018* (Directives 2/2018 pour les exceptions de l'Article 49 en vertu du règlement 2016/679, adoptées le 25 mai 2018)

Commission européenne, *Brief of the European Commission on behalf of the European Union as amicus curiae in support of neither Party in the case United States v. Microsoft Corp*

Conseil européen, *En ny strategisk agenda för 2019-2024, juni 2019* (Un nouvel agenda stratégique pour 2019-2024, juin 2019) https://www.consilium.europa.eu/media/39936/a-new-strategic-agenda-2019-2024- sv.pdf (Collectée le 01.10.2019)

Conseil de l'Union européenne (Transport, Telecommunications et Énergie), *Conclusions on the Future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion*", 07.06.2019 https://consilium.europa.eu/media/39667/st10102-en19.pdf

Ministère allemand de l'économie et de l'énergie (BMWi), *Criteria and catalogue for cloud services version 2*

Ministère allemand de l'économie et de l'énergie (BMWi), *Project GAIA-X A Federated Data Infrastructure as the cradle of a vibrant European ecosystem*

Ministère allemand de l'économie et de l'énergie (BMWi), *Trusted Cloud - Cloud providers* https://www.trusted-cloud.de/en/cloud-services (Collectée le 10.11.2019)

Fedramp, *Third Party Assessment Organization (3PAO)* https://www.fedramp.gov/assessors/ (Collectée le 20.09.2019)

Ministère suédois des finances, *Regleringsbrev för Ekonomistyrningsverket 2014* (Lettre de cadrage pour l'Autorité nationale de la gestion financière 2014)

Ministère suédois des finances, *Uppdrag att föreslå en förvaltningsmodell för skyddade it- utrymmen*, (Mission de proposer un modèle de gestion pour des espaces informatiques protégés) (DNR Fi2017/03084/DF).

Ministère suédois des finances, *Uppdrag att föreslå en förvaltningsmodell för skyddade it- utrymmen*, (Mission de proposer un modèle de gestion pour des espaces informatiques protégés) (DNR Fi2017/03084/DF).

Office de radiocommunications de la défense nationale , *Årsrapport 2018* (Rapport annuel 2018)

Ministère suédois de la défense, *Uppdrag inför inrättandet av ett nationellt cybersäkerhetscenter* (Mission pour l'instauration d'un centre national de cybersécurité), Fö2019/01000/SUND, 26.09.2019.

Forces armées suédoises, *Godkända kryptoapparater*, (Appareils de chiffrement approuvés par les Forces armées suédoises) septembre 2019 https://www.forsvarsmakten.se/sv/organisation/holegkvarteret/militara-underrattelse- och- sakerhetstjansten/kryptografiska-funktioner/ (Collectée le 01.10.2019)

Rapport de la commission parlementaire de la défense 2014/15:FöU11

Agence suédoise de la sécurité sociale Försäkringskassan, *Delredovisning samordnad et säker statlig it-drift* (Rapport financier partiel et informatique d'État sécurisée et coordonnée) (046278- 2017), 24.11.2017

Agence suédoise de la sécurité sociale Försäkringskassan, *Delredovisning samordnad et säker statlig it-drift* (Rapport financier partiel et informatique d'État sécurisée et coordonnée) (046278- 2017), 29.10.2018

Gartner, Market Insight: *Finding Cloud Opportunities in the government*, 27.06.2017 ID: G00327356

Gellman Barton and Soltani Ashkan, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say, The Washington Post,* 30.10.2013-10-30 https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to- yahoo-google- data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74- d89d714ca4dd_story.html (Collectée le 24.09.2019)

Google, *Begäran om användarinformation* https://transparencyreport.google.com/user-data/overview (Collectée 2019-09-05)

Gutierrez, Natashya, *Did Cambridge Analytica use Filipinos' Facebook data to help Duterte win?, Rappler*, 05.04.2018 https://www.rappler.com/nation/199599-facebook-data-scandal-cambridge- analytica-help-duterte-win-philippine-elections (Collectée le 10.11.2019)

Hellberg, Islam, Karlsson, *Säkerhet vid molnlösningar* (La sécurité dans les solutions nuagiques). Université d'Örebro *[Suède]* et Autorité nationale suédoise pour la protection civile MSB

Hern Alex, *Facebook agrees to pay fine over Cambridge Analytica scandal, The Guardian,*30.10. 2019 https://www.theguardian.com/technology/2019/oct/30/facebook-agrees-to-pay-fine-over- cambridge-analytica-scandal (Collectée le 10.11.2019)

Huizing Lennart, *The Hague Forum for Cloud Contracting,* Privacy Company, 24.10.2019 https://www.privacycompany.eu/en/the-hague-forum-for-cloud-contracting/ (Collectée le 24.10.2019)

Ministère suédois de l'infrastructure, *Ändring av uppdrag att erbjuda samordnad et säker statlig it- drift* (Modification de la mission de proposer des opérations informatiques coordonnées et sécurisées) (I2019/02515/DF).

Infrastrukturdepartementet, *Ändring av uppdrag att erbjuda samordnad och säker statlig it-drift* (I2019/02515/DF)

Comité sur l'intégrité, *Hur står det till med den personliga integriteten? – en kartläggning av Integritetskommittén* (Où en est l'intégrité des personnes ? État des lieux dressé par le Comité sur l'intégrité (Rapport des commissions officielles de l'État suédois, SOU 2016:41)

International Organization for Standardization, ISO/IEC 2382:2015(en) Information technology - Vocabulary

Justitiedepartementet, Lagrådsremiss *Hemlig dataavlyssning,* 2019-10-24

Ministère suédois de la justice, Saisine du Conseil législatif, *Hemlig dataavläsning* (Lecture secrète de données), 24.10.2019

Ministère suédois de la justice, *Uppdrag till MSB att genomföra riktade utbildningsinsatser på informationssäkerhetsområdet till offentlig sektor (*Mission pour l'Autorité nationale suédoise pour la protection civile MSB d'effectuer des efforts de formations dans le domaine de la sécurité informatique du secteur public) (Ju2019/03057/SSK)

Agence nationale de services juridiques, financiers et administratifs Kammarkollegiet, *Förstudierapport Webbaserat kontorsstöd*, (Étude préliminaire concernant le soutien bureautique par Internet), DNR 23.2-6283-18, 22.02.2019

Kristiansson Stefan, La menace des renseignements contre la Suède, Frivärld, Rapport No. 7 2019.

Le ministère de l'Europe et des Affaires étrangères, *Déclaration du conseil franco-allemand de sécurité et de défense, 2015* https://www.diplomatie.gouv.fr/IMG/pdf/_16-04-07_declaration_cfads__cle8eaec8.pdf

Ministère de l'Europe et des Affaires étrangères, *Déclaration du conseil franco-allemand de sécurité et de défense*, 2015 https://www.diplomatie.gouv.fr/IMG/pdf/_16-04-07_declaration_cfads cle8eaec8.pdf

Maurer Tim et autres, *Technological Sovereignty: Missing the Point? An Analysis of European Proposals after June 5, 2013*, New America's Open Technology Institute et the Global Public Policy Institute (GPPi) https://www.gppi.net/media/Maurer- et-al_2014_Tech-Sovereignty- Europe.pdf

Microsoft, Association des collectivités territoriales suédoises (SKL) et autres, Séminaire ouvert à Almedalen 2019,*CLOUD Act - hinder eller ej* (Le CLOUD Act, entrave ou non). https://www.youtube.com/watch?v=tqCRZt81bZk (Collectée le 04.09.2019)

Microsoft, *Configure ADRMS restrictions* https://docs.microsoft.com/sv-se/azure/information- protection/configure-adrms-restrictions (Collectée le 23.09.2019)

Microsoft, *Konfigurera diagnostikdata för Windows i din organisation*, (Configurez des données diagnostiques pour Windows dans votre organisation) 2019 https://docs.microsoft.com/sv- se/windows/privacy/configure-windows-diagnostic- ata-in-your-organization (Collectée le 24.09.2019)

Microsoft, *Law Enforcement Requests Report* https://www.microsoft.com/en-us/corporate- responsibility/lerr (Collectée le 10.09.2019)

Microsoft, *Molntjänster och säkerhet* (Services cloud et sécurité) 13.12.2018 https://news.microsoft.com/sv-se/2018/12/13/molntjanster-och-sakerhet/ (Collectée le 04.09.2019)

Microsoft, *Office 365 Government cloud för amerikanska staten* https://docs.microsoft.com/en- us/office365/servicedescriptions/office-365-platform-service-description/office-365-us- government/office-365-us-government (Collectée le 23.09.2019)

Microsoft, *Service encryption with Customer Key for Office 365 FAQ*, 2018-07-31 https://docs.microsoft.com/en-us/office365/securitycompliance/service-encryption-with-customer- key-faq (Collectée le 24.09.2019)

Microsoft, *Bring your own key* (BYOK) informations sur Azure Information Protection, 22.09.2019 https://docs.microsoft.com/sv-se/azure/information-protection/byok-price-restrictions (Collectée le 25.09.2019)

Ministerie van Justitie en Veiligheid, *Verificatie op de uitvoering van het overeengekomen verbeterplan met Microsoft* (Ons kenmerk 2635551), 01.07.2019

Ministry of Justice and Security Strategic Vendor Management Microsoft, DPIA Office 365 ProPlus version 1905 (June 2019) Data protection impact assessment on the processing of diagnostic data

Autorité nationale suédoise pour la protection civile MSB, *Handlingsplan för skydd av samhällsviktig verksamhet,* (Plan d'action pour la protection des activités d'importance sociétale), MSB597, décembre 2013

Autorité nationale suédoise pour la protection civile MSB *Upphandling till samhällsviktig verksamhet – en vägledning* (Appels d'offres pour des activités d'importance sociétal : un guide). MSB1275, septembre 2018

Autorité nationale suédoise pour la protection civile MSB, *Vägledning för identifiering av samhällsviktig verksamhet* (Guide pour l'identification des activités d'importance sociétale), MSB1408, juin 2019

Autorité nationale suédoise pour la protection civile MSB, *Vägledning för risk- och sårbarhetsanalyser* (Guide pour les analyses de risque et de vulnérabilité) MSB245, avril 2011

Autorité nationale suédoise pour la protection civile MSB, *Övergripande inriktning för samhällsskydd och beredskap* (Orientation d'ensemble pour la protection de la société et sa préparation), MSB708, juin 2014

Ministère suédois de l'entreprise et de l'innovation, *Med medborgaren i centrum - Regeringens strategi för en digitalt samverkande statsförvaltning* (Avec le citoyen au centre : stratégie du gouvernement pour l'interopérabilité de la gestion publique) (N2012:37)

Office of the Director of National Intelligence United States Intelligence Activities (Federal Register Vol. 40, No. 235 (December 8, 1981), amended by EO 13284 (2003), EO 13355 (2004), and EO 13470 (2008))

Office suédois des pensions Pensionsmyndigheten, *Molntjänster i staten - en ny generation av outsourcing* (Les services cloud dans la gestion publique : une nouvelle génération d'externalisation) (avec l'Annexe Analyse juridique du traitement des informations par les administrations dans le nuage), 2016

Administration suédoise des postes et télécommunications Post- och Telestyrelsen *Förslag till en förvaltningsmodell för skyddade it-utrymmen* (Proposition d'un modèle de gestion pour des espaces informatiques protégés) (Dnr: 17-8280)

Proposition de loi suédoise No. 2014/15:109, *Försvarspolitisk inriktning, Sveriges försvar 2016- 2020* (Orientation de la politique de défense – la défense de la Suède de 2016 à 2020)

Proposition de loi 2019/20:15, *Skydd av Sveriges säkerhet vid radioanvändning*, (Protection de la sécurité de la Suède lors de l'utilisation de la radio),

Punke Michael, AWS and the CLOUD Act, *AWS Security Blog*, 27.05.27 https://aws.amazon.com/blogs/security/aws-and-the-cloud-act/ (Collectée le 02.09.2019)

Gouvernement suédois, *Säker och kostnadseffektiv it-drift för den offentliga förvaltningen* (Des opérations informatiques sécurisées et économiques pour la gestion publique) (Dir. 2019:64).

Communication du gouvernement 2010/11:138, *Riksrevisionens granskning av it inom statsförvaltningen et statliga it-projekt* (Examen par la Riksrevisionen, *IT inom statsförvaltningen - har myndigheterna på ett rimligt sätt prövat frågan om outsourcing bidrar till ökad effektivitet*? (L'informatique dans la gestion publique : les administrations ont-elles raisonnablement examiné la question de savoir si l'externalisation contribue à une meilleure efficacité ?) (RiR 2011:4), page 63 et suivantes. de l'informatique dans la gestion publique et des projets informatique de l'État).

Procès-verbal du Parlement suédois 2014/15:117

Riksrevisionen, *Granskning om IT-förvaltning delvis missförstådd* (L'examen de la gestion informatique a été partiellement mal compris), 26.09.2017. https://www.riksrevisionen.se/om-riksrevisionen/kommunikation-och-media/nyhetsarkiv/2017-09- 26-granskning-om-it-forvaltning-delvis-missforstadd.html (Collectée le 30.09.2019)

Riksrevisionen, *IT inom statsförvaltningen - har myndigheterna på ett rimligt sätt prövat frågan om outsourcing bidrar till ökad effektivitet*? (L'informatique dans la gestion publique : les administrations ont-elles raisonnablement examiné la question de savoir si l'externalisation contribue à une meilleure efficacité ?) (RiR 2011:4)

Centre national de services aux administrations publiques Statens servicecenter, *En gemensam statlig molntjänst, Delrapport i regeringsuppdrag om samordning et omlokalisering av myndighetsfunktioner* (Un service nuagique commun à l'État, Rapport partiel de la mission du gouvernement concernant la coordination et le relocalisation des fonctions administratives) 07.02.2017 (DNR 10052-2016/1121)

Strategic Vendor Management Microsoft for the Dutch Government and Ministerie van Veiligheid en Justitie, Union EuropéenneSoftware and Cloud Supplier Customer Council https://www.youtube.com/watch?v=96EVKaosVps&feature=youtu.be (Collectée le 25.09.2019)

Association des collectivités territoriales suédoises (SKL), *Molntjänster och konfidentialitetsbedömning* (Services cloud et appréciation de confidentialité) https://skl.se/download/18.3414859716e267c4fe2ad9d8/1572961426896/Molntja%CC%88nster%20och%20konfidentialitetsbedo%CC%88mning_191105.pdf (Collectée le 09.11.2019)

Association des collectivités territoriales suédoises (SKL), *Ställningstagande om informationshantering i vissa molntjänster* (Prise de position concernant la gestion des informations dans certains services cloud), dossier No. 19/00087, 12.04.2019

Service de la sûreté suédoise, *Informationssäkerhet* (Sécurité des informations) https://www.sakerhetspolisen.se/sakerhetsskydd/informationssakerhet.html (Collectée le 05.09.2019)

Service de la sûreté suédoise, Service de la sûreté suédoise, *Personalsäkerhet* (Sécurité du personnel) https://www.sakerhetspolisen.se/sakerhetsskydd/personalsakerhet.html (Collectée le 05.06.2019)

Service de la sûreté suédoise, *Säkerhetsskydd vid upphandlingar och affärsavtal* (Contrôle de sécurité lors d'appels d'offres et de contrats commerciaux) https://www.sakerhetspolisen.se/sakerhetsskydd/sakerhetsskydd-vid-upphandlingar-och- affarsavtal.html (Collectée le 06.09.2019)

Service de la sûreté suédoise *Vägledning i säkerhetsskydd - Introduktion till säkerhetsskydd* (Guidage en protection de sécurité : Initiation au contrôle de sécurité) https://www.sakerhetspolisen.se/download/18.7acd465e16b4e0e54c64d/15607773 15837/Vagledning-Introduktion-till-sakerhetsskydd.pdf (Collectée le 05.09.2019)

Service de la sûreté suédoise, *Vägledning i säkerhetsskydd – personalsäkerhet* (Guidage en protection de sécurité : Sécurité du personnel), juni 2019

Service de la sûreté suédoise, *Årsbok 2017* (Livre annuel 2017)

Service de la sûreté suédoise, *Årsbok 2018* (Livre annuel 2018)

The App Association et autres, Lettre ouverte à l'Attorney General Barr, 21.09.2019 https://www.bsa.org/files/policy-filings/06212019bsaletteruseulea.pdf (Collectée le 22.09.2019)

Agence de la recherche de la défense nationale suédoise et Administration suédoise des fortifications, *Strategisk utblick 8 - Totalförsvarets tillväxt - utmaningar et möjligheter, Så kan vi skydda Sveriges säkerhetskänsliga it-tjänster*, (Regard stratégique 8 : croissance de la défense nationale : défis et possibilités, Voici comment nous pouvons protéger les services informatiques suédois sensibles du point de vue de la sécurité) (FOI 4773), mai 2019.

Direction suédoise des transports, *Kartläggning av hanteringen av vissa uppgifter* (Inventaire du traitement de certaines données) (TSG 2017- 2515), 23.01.2018

United States Department of commerce, *Security and Privacy Controls for Federal Information Systems and Organizations* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800- 53r4.pdf (Collectée le 15.10.2019)

United States Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, White Paper, avril 2019

United States District Court for the District of Vermont., No. 2:06-mj-91, 2009 WL 424718 Feb. 19, 2009. MEMORANDUM of DECISION In re Grand Jury Subpoena to Sebastien Boucher

Enquête sur la lecture secrète des données, *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet* (Lecture secrète de données : un outil important dans la lutte contre la criminalité grave) (Rapport des commissions officielles de l'État suédois, SOU 2017:89

Enquête sur la convention sur la délinquance informatique, *Europarådets konvention om it-relaterad brottslighet,* (Convention du Conseil de l'Europe sur la délinquance informatique) (Rapport des commissions officielles de l'État suédois, SOU 2013:39)

von der Leyen Ursula, *Politiska riktlinjer för nästa europeiska kommission* (Priorités de la prochaine commission européenne), 2019-2024

Annexe 1 L'externalisation des opérations informatiques de l'État suédois : éclairage historique

Dès le premier rapport de la délégation de l'informatique, en 2009, une proposition était mise en avant pour que le gouvernement pose des exigences envers les administrations pour qu'elles élaborent une stratégie pour leur approvisionnement en services informatiques, une stratégie dite de sourcing. Cette stratégie devait tenir compte de la situation spécifique des autorités. Les paramètres qui devaient renforcer le choix de sourcing étaient surtout le coût, la qualité et la flexibilité[126].

En 2011, la Direction nationale suédoise du contrôle de la gestion publique Riksrevisionen a effectué une analyse pour savoir si les administrations publiques envisageaient l'externalisation dans une étendue suffisante pour répondre aux besoins d'informatique[127]. La conclusion de la Riksrevisionen a été que l'externalisation n'était pas suffisamment considérée. La raison indiquée était que les administrations ne peuvent pas comptabiliser leurs coûts d'informatique, que la direction interne est lacunaire, que les exigences d'efficacité n'existent pas dans les divisions informatiques des administrations, que les compétences d'achat sont faibles, qu'il y a des incertitudes en ce qui concerne la classification des informations en « informations sensibles », que la diffusion des connaissances entre administrations est déficiente et que le gouvernement n'a pas facilité l'externalisation. C'est pourquoi la Riksrevisionen a recommandé au gouvernement d'instaurer des directives et d'augmenter les échanges d'expériences entre les administrations[128].

Le gouvernement a notamment répondu au rapport que la question de l'externalisation des services informatiques par les administrations serait étudiée plus avant. Le gouvernement estimait aussi qu'il était souhaitable qu'une grande partie des besoins en informatique des administrations soient satisfaits par l'externalisation[129].

Par la suite, la Riksrevisionen a fait le commentaire, lors des discussions qui ont suivi l'externalisation par la Direction suédoise des transports de ses opérations informatiques, que la conclusion de son rapport avait été mal comprise[130].

Dans sa stratégie de numérisation de 2012, le gouvernement souligne qu'une étude préliminaire approfondie sera effectuée en 2012-2013 par la Délégation à

---

[126] Délégation à l'informatique, *Strategi för myndigheternas arbete med e-förvaltning* (Stratégie pour le travail des administrations en gestion informatisée), (Rapport des commissions officielles de l'État suédois, SOU 2009:86), page 15 et suivantes.

[127] Nous utilisons dans ce document l'expression externalisation. L'expression anglaise fréquente est outsourcing. Offshoring (en français délocalisation) est utilisé lorsque l'externalisation se déroule vers un autre pays.

[128] Riksrevisionen, *IT inom statsförvaltningen - har myndigheterna på ett rimligt sätt prövat frågan om outsourcing bidrar till ökad effektivitet*? (L'informatique dans la gestion publique : les administrations ont-elles raisonnablement examiné la question de savoir si l'externalisation contribue à une meilleure efficacité ?) (RiR 2011:4), page 63 et suivantes.

[129] Communication du gouvernement 2010/11:138, *Riksrevisionens granskning av it inom statsförvaltningen et statliga it-projekt* (Examen par la Riksrevisionen de l'informatique dans la gestion publique et des projets informatique de l'État).

[130] Riksrevisionen, *Granskning om IT-förvaltning delvis missförstådd* (L'examen de la gestion informatique a été partiellement mal compris), 26.09.2017.

l'informatique E-delegationen[131]. La Délégation à l'informatique a décrit que l'objectif de son étude préliminaire était d'identifier et de décrire les possibilités d'améliorer l'efficacité des opérations informatiques des administrations au- delà des limites des ministères et des administrations, y compris de proposer des manières de structurer ces solutions. Cette étude préliminaire devait éclairer la manière dont l'État, dans l'avenir, devait exploiter, échanger ou acheter et vendre des services informatiques au sein du secteur public, y compris une évaluation de différents modèles de sourcing. Elle devait également éclairer les exigences de sécurité des informations et comporter une analyse des obstacles et des propositions de stratégie d'instauration[132]. Cependant, le rapport de cette étude préliminaire n'a jamais été publié.

En 2014, le gouvernement a confié à l'Autorité nationale de la gestion financière Ekonomistyrningsverket la mission de développer le travail des administrations concernant les coûts et les investissements informatiques et l'externalisation, et le gouvernement, dans son rapport annuel, a déclaré que la question de la stratégie de sourcing devait, par ce fait, être déclarée comme préparée définitivement au sein des Services du gouvernement[133]. La mission confiée à Ekonomistyrningsverket était de préparer un modèle de coûts informatiques. Cette autorité devait aussi considérer de quelle manière ce modèle comporterait le suivi des choix stratégiques, tel que la stratégie d'approvisionnement informatique[134]. Le rapport d'Ekonomistyrnings-verket a décrit, en 2014, les coûts informatiques de l'État[135].

Parallèlement à la mission d'Ekonomistyrningsverket, l'Office suédois des pensions Pensionsmyndigheten a reçu mission, au printemps de 2015, d'analyser et d'évaluer le potentiel d'utilisation de services cloud au sein de l'État, ainsi que de rendre compte des risques et des obstacles éventuellement liés à l'utilisation de services cloud dans la gestion publique. Cette analyse devait également montrer comment l'utilisation de services cloud peut contribuer à atteindre l'objectif d'une gestion plus simple, plus ouverte et plus efficace. Pensionsmyndigheten souligne dans son rapport que les services cloud ont certaines limites pour les activités publiques et que plus les informations sont sensibles et plus il y a d'intégrations, d'autant plus difficile sera l'externalisation. Il a été recommandé à chaque administration d'effectuer un contrôle de légalité et d'assurer le maintien d'une sécurité suffisante des informations[136]. Les aspects juridiques étaient élucidés dans une annexe dédiée. Dans cette annexe, Pensionsmyndigheten mettait en avant la question de la sécurité nationale et soulignait qu'elle nécessitait une plus grande focalisation.

---

[131] Ministère suédois de l'entreprise et de l'innovation, *Med medborgaren i centrum - Regeringens strategi för en digitalt samverkande statsförvaltning* (Avec le citoyen au centre : stratégie du gouvernement pour l'interopérabilité de la gestion publique) (N2012:37), page 22.

[132] Délégation à l'informatique, *Så enkelt för så många som möjligt* (Le plus simple possible pour autant de gens possible) (Rapport des commissions officielles de l'État suédois, SOU 2011:67), page 30.

[133] Ministère suédois des finances, *Årsredovisning för staten 2012*, Rapport financier de l'État suédois 2012, page 115, *Årsredovisning för staten 2013*, Rapport financier de l'État suédois 2013, page 116 et *Årsredovisning för staten 2014*, Rapport financier de l'État suédois 2014, page 124.

[134] Ministère suédois des finances, *Regleringsbrev för Ekonomistyrningsverket 2014* (Lettre de cadrage pour l'Autorité nationale de la gestion financière 2014), page 5.

[135] Autorité nationale de la gestion financière Ekonomistyrningsverket, *It-kostnadsmodell* (Modèle de coûts informatiques) (2014:50).

[136] Office suédois des pensions Pensionsmyndigheten, *Molntjänster i staten - en ny generation av outsourcing,* (Les services cloud dans la gestion publique : une nouvelle génération d'externalisation) 2016, page 73 et suivantes.

Pensionsmyndigheten recommandait donc aussi la poursuite de l'étude de services cloud d'État[137].

Le Centre national de services aux administrations publiques Statens servicecenter a reçu du gouvernement mission, en 2016, d'analyser les possibilités de services cloud d'État, justement. Son rapport a été remis en février 2017. La conclusion du Centre était que la plus grande partie des opérations informatiques des administrations publiques doivent être coordonnées dans un service nuagique d'État, qui proposera aux administrations deux services : la puissance informatique et le stockage[138].

En 2017, le gouvernement a confié à l'Administration suédoise des postes et télécommunications Post och telestyrelsen PTS la mission de préparer des propositions de modèles de gestion d'espaces informatiques protégés[139]. Le rapport final de la PTS, présenté en février 2018, proposait une analyse approfondie suivie d'une mise en œuvre d'un modèle de gestion qui permettrait une coordination d'espaces informatiques protégés[140].

La mission de la PTS a été complétée en août 2017 par une mission destinée à l'Agence suédoise de la sécurité sociale Försäkringskassan de proposer une opération informatique d'État coordonnée et sécurisée aux fonctions et administrations adéquates entre 2017 et 2020[141]. La Försäkringskassan devait en outre préparer des propositions de formes pertinentes d'opérations informatiques d'État coordonnées après 2020. Dans ses rapports partiels de 2017 et 2018, la Försäkringskassan insiste sur le fait que le besoin de soutien pour les opérations informatiques est important au sein des administrations publiques et que ce sont surtout les petites administrations qui ont besoin d'une prise en charge totale[142]. Dans son rapport en retour de 2018, la Försäkringskassan soulignait l'importance de réaliser le modèle d'espaces informatiques protégés proposé par la PTS en 2018[143].

L'Administration suédoise des fortifications a effectué, de 2016 à 2019, un certain nombre d'études préliminaires concernant l'accès à des espaces informatiques

---

[137] Pensionsmyndigheten, *Molntjänster i staten - en ny generation av outsourcing,* (Les services cloud dans la gestion publique : une nouvelle génération d'externalisation) 2016, page 58 et suivantes.

[138] Centre national de services aux administrations publiques Statens servicecenter, *En gemensam statlig molntjänst, Delrapport i regeringsuppdrag om samordning et omlokalisering av myndighetsfunktioner* (Un service nuagique commun à l'État, Rapport partiel de la mission du gouvernement concernant la coordination et la relocalisation des fonctions administratives) (DNR 10052-2016/1121).

[139] Ministère suédois des finances, *Uppdrag att föreslå en förvaltningsmodell för skyddade it-utrymmen,* (Mission de proposer un modèle de gestion pour des espaces informatiques protégés) (DNR Fi2017/03084/DF).

[140] Administration suédoise des postes et télécommunications Post- och Telestyrelsen PTS, *Förslag till en förvaltningsmodell för skyddade it-utrymmen* (Proposition d'un modèle de gestion pour des espaces informatiques protégés) (Dnr: 17- 8280).

[141] Ministère suédois des finances, *Uppdrag att föreslå en förvaltningsmodell för skyddade it-utrymmen,* (Mission de proposer un modèle de gestion pour des espaces informatiques protégés) (DNR Fi2017/03084/DF).

[142] Nous entendons par engagement total l'accès à une division informatique externe qui gère le développement, la gestion et l'opération comme le ferait une division informatique interne. Voir Agence suédoise de la sécurité sociale Försäkringskassan, *Delredovisning samordnad et säker statlig it-drift,* (Rapport partiel concernant des opérations informatiques d'État coordonnées et sécurisées) (046278-2017), 24.11.2017 et Försäkringskassan, *Delredovisning samordnad et säker statlig it-drift*, (Rapport partiel concernant des opérations informatiques d'État coordonnées et sécurisées) (046278-2017), 29.10.2018.

[143] Administration suédoise des postes et télécommunications PTS F*örslag till en förvaltningsmodell för skyddade it- utrymmen* (Proposition d'un modèle de gestion pour des espaces informatiques protégés), Dnr: 17-8280.

protégés. Une étude préliminaire financée par l'Autorité nationale suédoise pour la protection civile MSB analysait un besoin élargi de l'administration publique pour pouvoir réaliser une coordination des services informatiques.

Après avoir terminé cette étude préliminaire, l'Administration suédoise des fortifications constatait qu'une part essentielle de la constitution de la capacité de défense totale de la Suède est constituée par la protection des activités d'importance sociétale, et surtout en ce qui concerne les systèmes informatiques d'importance sociétale[144].

En septembre 2019, le gouvernement suédois a présenté des mesures pour renforcer la sécurité des informations et la cybersécurité. Il a pris notamment la décision de constituer un centre national de cybersécurité dans le but de renforcer la capacité totale de la Suède de prévenir, à découvrir et à gérer les cybermenaces. L'Autorité nationale suédoise pour la protection civile MSB a reçu mission d'effectuer des efforts de formation dédiés dans ce domaine et d'élaborer une structure de suivi du travail systématique sur la sécurité informatique dans l'administration publique[145].

Ces missions ont été complétées par l'initiative du gouvernement de créer un groupe d'enquête sur la sécurité et l'économie des opérations informatiques au sein des administrations publiques.

L'objectif de cette étude était, selon sa directive, de créer de meilleures conditions pour que l'administration publique ait accès à des opérations informatiques sûres et économiques, soit au moyen d'opérations informatiques d'État, soit des conditions juridiques plus claires permettant d'engager des fournisseurs d'informatique privés. Dans sa directive, le gouvernement souligne l'incertitude concernant les conditions juridiques de l'externalisation, surtout en ce qui concerne l'interprétation du fait qu'une donnée doit être considérée comme divulguée selon les termes de la législation concernant le secret. Le gouvernement confirme que cette inquiétude s'est intensifiée à cause de la loi CLOUD Act. Le gouvernement constate que si la transmission de données comporte des données à caractère personnel, l'autorité qui externalise doit aussi s'assurer que le traitement des données à caractère personnel à effectuer est conforme à la règlementation sur la protection des données. Le gouvernement identifie aussi qu'un défi particulier pour une administration qui externalise peut être d'apprécier si le fournisseur est en mesure de donner des garanties suffisantes qu'il effectuera les mesures techniques et organisationnelles adéquates de manière que le traitement des données soit conforme à l'ordonnance de protection des données, que les droits des personnes enregistrées soient protégées et

---

[144] Agence de la recherche de la défense nationale suédoise Totalförsvarets forskningsinstitut et Administration suédoise des fortifications, *Strategisk utblick 8 - Totalförsvarets tillväxt - utmaningar et möjligheter, Så kan vi skydda Sveriges säkerhetskänsliga it-tjänster,* (Regard stratégique 8 : croissance de la défense nationale : défis et possibilités, Voici comment nous pouvons protéger les services informatiques suédois sensibles du point de vue de la sécurité) (FOI 4773), mai 2019.

[145] Ministère suédois de la justice, *Uppdrag till Myndigheten för samhällskydd och beredskap MSB att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen* (Mission pour l'Autorité nationale suédoise pour la protection civile MSB d'effectuer des efforts de formation dans le domaine de la sécurité informatique du secteur public) (Ju2019/03057/SSK), Ministère suédois de la justice, *Uppdrag till Myndigheten för samhällsskydd och beredskap att ta fram en struktur för uppföljning av det systematiska informationssäkerhets-arbetet i den offentliga förvaltningen* (Mission pour la MSB d'élaborer une strusture de suivi du travail systématique pour la sécurité des informations dans l'administration publique) (Ju2019/03058/SSK, Ju2019/02421/SSK) et Ministère suédois de la défense, *Uppdrag inför inrättandet av ett nationellt cybersäkerhetscenter,(*Mission en prévision de la création d'un centre national de cybersécurité) (Fö2019/01000/SUND).

que les données ne soient pas transférées sans autorisation vers des pays tiers, c'est-à-dire hors de l'Union Européenne et de l'Espace économique européen (EEE)[146].

Lors de l'instauration des directives de comités, le gouvernement a également décidé de prolonger la mission de la Försäkringskassan de proposer des opérations informatiques d'État coordonnées et sécurisées. Le gouvernement a déclaré que, de cette manière, le délai accordé à la Försäkringskassan pour sa mission correspondait mieux à la durée de l'enquête pour le nouveau groupe d'enquête et le délai nécessaire pour le traitement ultérieur de la proposition du groupe d'enquête[147].

[146] Ministère suédois de l'infrastructure, *Säker et kostnadseffektiv it-drift för den offentliga förvaltningen* (Des opérations informatiques sécurisées et économiques pour la gestion publique) (Dir. 2019:64).

[147] Ministère suédois de l'infrastructure, *Ändring av uppdrag att erbjuda samordnad et säker statlig it-drift* (Modification de la mission de proposer des opérations informatiques coordonnées et sécurisées) (I2019/02515/DF).

Annexe 2 Notion de service cloud et estimation de l'utilisation de services cloud publics au sein du secteur public suédois

On peut définir les services cloud de plusieurs manières différentes. Ce rapport utilise la définition présentée par la norme ISO/IEC 17788:2014 (ISO, 2014) qui définit le service nuagique comme :

"une ou plusieurs fonctions comprises dans des services informatiques basées sur un nuage […] et auxquelles il est fait appel au moyen d'une interface définie", le service informatique basé sur un nuage étant « un concept qui permet l'accession par un réseau à un pool modulable et élastique de ressources physiques ou virtuelles partagées qui, en libre-service, sont fournies et administrées à la demande. Dans cette définition, les ressources comprennent notamment les serveurs, les systèmes d'exploitation, les réseaux, les logiciels, les applications et l'équipement de stockage"[148].

Les propriétés (caractéristiques) principales définies par l'ISO et l'Institut suédois de normalisation SIS et qui encadrent, en outre, la notion sont énumérées ci-dessous :

- Les utilisateurs peuvent atteindre des ressources physiques et virtuelles à partir de différents lieux à l'aide de différents clients et unités, tant qu'il existe des réseaux accessibles.
- Les clients ne paient que pour les ressources qu'ils utilisent.
- Les ressources physiques ou virtuelles sont réparties de manière que plusieurs utilisateurs partagent un environnement, mais leurs calculs et leurs données sont isolées et inaccessibles les uns pour les autres.
- Les services permettent aux utilisateurs de faire ce qu'ils ont à faire quand ils ont besoin de le faire, sans nécessiter d'autres interactions humaines d'utilisateurs ou d'autres frais d'administration. Les services cloud peuvent, dans certains cas, être commandés, paramétrés et commencés à être utilisés sans interaction humaine.
- Les ressources physiques ou virtuelles peuvent être fournies rapidement et élastiquement, automatiquement dans certains cas, ce qui fait que les ressources peuvent rapidement être augmentées ou réduites, et l'avantage opérationnel ressenti par le client est de ne pas avoir besoin de s'inquiéter pour des ressources limitées ou pour la planification de capacité.
- Les fournisseurs de services cloud peuvent soutenir l'utilisation multiple, tout en utilisant l'abstraction comme une manière de dissimuler au client la complexité du processus.

---

[148] La norme ISO/IEC 17788:2014 est la norme internationale qui, d'une part, fournit une vue d'ensemble de ce que signifient les services cloud et, d'autre part, une recommandation de termes et de définitions à utiliser dans ce contexte. Voir Hellberg et autres, *Säkerhet vid molnlösningar* (La sécurité dans les solutions nuagiques).

Les services cloud peuvent être offerts à différents groupes de clients. Dans les cas où le service nuagique ne peut être accédé que par un seul client (qui peut être sa propre organisation) le service nuagique est appelé privé (private cloud). Dans ce contexte, le mot privé n'est pas utilisé comme une description du statut juridique du prestataire de service. Un service nuagique proposé à un groupe limité de clients est appelé un service nuagique communautaire (partner cloud/community cloud), alors qu'un service nuagique proposé à un groupe plus large ou au public est appelé un service nuagique public (public cloud). Il est cependant important de souligner que, dans ce contexte, le mot « public » ne signifie pas que le public a accès à toutes les données du service, car chaque client n'a accès qu'à « ses » données seulement. Au sein de la gestion publique suédoise, il existe des exemples des trois types de services cloud. L'Agence suédoise de la sécurité sociale Försäkringskassan utilise, par exemple, des services cloud pour proposer certaines fonctions à ses propres employés. Dans le cadre de la mission d'État du gouvernement

« Coordination d'opérations informatiques d'État sécurisées » certains services sont offerts conjointement avec les administrations avec lesquelles la Försäkringskassan a lancé l'interopérabilité de certains services au moyen de services cloud communautaires. Un bon nombre d'administrations utilisent aussi des services cloud publics comme Office 365 pour la fourniture de soutien bureautique. Mentionnons, dans ce contexte aussi, que la notion d'Hybrid Cloud signifie que plusieurs modèles sont utilisés de manière complémentaire pour fournir des services à un client[149].

Il existe trois types de services cloud établis sur le plan international qui décrivent trois domaines fonctionnels différents. Puisque leur définition est mondialisée, nous utilisons les termes anglais et leurs abréviations

Infrastructure as a Service (IaaS) (l'infrastructure en tant que Service) signifie qu'il existe des services infrastructurels dans le réseau. Le client peut créer et utiliser les ressources d'un ou plusieurs fournisseurs de services cloud sous forme de matériel physique comme des serveurs, des réseaux, des espaces de stockage, une structure architecturée, l'équilibre des charges, le calcul, etc. Le client se procure lui-même les plates-formes et les applications qui fonctionnent dans l'infrastructure. Le client n'a pas le contrôle de l'infrastructure sous-jacente mais il a donc le contrôle, par exemple, du système d'exploitation, du stockage et des applications développées et déroulées dans l'infrastructure.

Platform as a Service (PaaS) (une plateforme en tant que Service) signifie que le fournisseur procure des plates-formes d'applications par Internet ou par un autre réseau, pour que les utilisateurs installent leurs propres applications. Un exemple de service PaaS est un service d'environnements de développement en tant que service.

Software as a Service (SaaS) (Logiciel en tant que service) signifie que le fournisseur procure des logiciels comme service, c'est-à-dire des applications terminées ou paramétrables sur Internet ou un autre réseau. Ce type de service est parfois appelé *Applications as a service* (AaaS) (Applications en tant que service). Ce type de service peut être fourni de différentes manières et être accessible, par exemple, par un navigateur web. C'est le fournisseur qui se charge de la maintenance[150].

---

[149] Butler, *What is hybrid cloud computing? The benefits of mixing private and public cloud services.*

[150] Office suédois des pensions Pensionsmyndigheten, *Molntjänster i staten* (Les services cloud dans la gestion publique), Pensionsmyndigheten, page 13 et suivantes.

Selon l'enquête effectuée par l'Office suédois des pensions Pensionsmyndigheten en 2016, les solutions SaaS étaient, de loin, le modèle le plus fréquent[151], et rien n'indique de changements intervenus sur ce point.

Puisque les avantages opérationnels sont ressentis aussi bien par le client que par le fournisseur, les services cloud sont devenus un modèle de prestation de plus en plus fréquent. Sur le plan mondial, des services cloud sont utilisés maintenant pour gérer approximativement 22 % de toutes les données organisationnelles. L'évolution a été très rapide et, dans quelques années, les services cloud seront utilisés sur le plan mondial pour de plus grandes quantités de données que les données stockées localement ou pour des serveurs propres au client[152].

Trois entreprises américaines ont une position très forte sur le marché des services cloud. Amazon Web Services (AWS), Microsoft et Google proposent des services cloud publics. Ces entreprises ont une offre large de services cloud publics destinés aussi bien aux particuliers qu'aux grosses organisations. Le rythme de croissance est rapide et le bénéfice d'ensemble de ces trois services s'élevait au premier trimestre de 2019 à un peu moins de 47 milliards de dollars[153].

Un certain nombre de fournisseurs importants, y compris AWS et Microsoft, ont construit des services cloud privés particuliers pour les administrations américaines[154]. Cela pour répondre aux exigences qu'imposent le administrations américaines à leurs fournisseurs[155]. Des stratégies correspondantes se retrouvent dans plusieurs pays, avec pour motivation d'assurer la souveraineté[156].

Les administrations suédoises font, elles aussi, une utilisation croissante des services cloud. Dans une étude financée par l'Autorité nationale suédoise pour la protection civile MSB en 2018, 75 % des municipalités et administrations interrogées répondent qu'elles utilisent au moins un service nuagique négocié. Parmi les autorités municipales, plus de 80 % utilisent au moins un service nuagique public[157].

La raison la plus souvent invoquée pour le choix des services cloud est leur haut degré de flexibilité, mais aussi des avantages de coûts considérés comme importants pour plus de la moitié des répondants[158].

En ce qui concerne les municipalités, l'administration des formations est citée comme le service le plus fréquent, alors que les administrations publiques déclarent avoir une plus grande diversité des types de services.

---

[151] Pensionsmyndigheten, *Molntjänster i staten* (Les services cloud dans la gestion publique), page 56 et suivantes.

[152] Bondcap, *Internet Trends 2019*, page 153.

[153] Bondcap, *Internet Trends 2019*, page 116.

[154] Microsoft, *Microsoft Office 365 Government cloud för amerikanska staten* (Nuage gouvernemental de Microsoft Office 365 pour l'État américain) et AWS, *AWS Government cloud för amerikanska staten*. (Nuage gouvernemental d'AWS pour l'État américain).Toutes les administrations américaines n'utilisent pas ces services cloud et plusieurs administrations américaines utilisent les services cloud publics proposés par ces entreprises.

[155] Fedramp, *Third Party Assessment Organization (3PAO) et United States Department of commerce, Security and Privacy Controls for Federal Information Systems and Organizations.*

[156] Gartner, *Market Insight: Finding Cloud Opportunities in Government*, ID: G00327356, 27.06.2017.

[157] Hellberg et autres, *Säkerhet vid molnlösningar* (La sécurité dans les solutions nuagiques), page 25.

[158] Hellberg et autres, *Säkerhet vid molnlösningar* (La sécurité dans les solutions nuagiques), page 28.

Les répondants avaient également la possibilité d'indiquer la raison pour laquelle ils étaient empêchés d'utiliser des services cloud. La raison principale était le manque de contrôle et la législation. Plus de 20 % ont répondu qu'ils étaient en passe de commencer à utiliser ces services[159].

Un grand nombre des services cloud publics se basent sur le fait que les clients et les utilisateurs se trouvent dans le monde entier et doivent avoir accès 24 heures sur 24 et sept jours sur sept. Pour répondre à ces exigences, il existe des installations et des personnels généralement dispersés dans le monde entier. La localisation exacte des différentes installations et des différents personnels est généralement un secret d'entreprise, mais certaines informations sont ouvertes au public. Par exemple, AWS dit qu'ils sont localisés aux États-Unis, au Brésil, en Suède, en France, en Allemagne, au Danemark, en Finlande, en Grande-Bretagne, en Norvège, en Italie, en République tchèque, en Autriche, en Pologne et en Suisse, en Afrique du Sud, dans les Émirats Arabes unis, en Israël, en Inde, à Hongkong, en Chine, en Malaisie, aux Philippines, au Japon, en Corée, à Singapour et à Taiwan ainsi qu'en Australie[160].

C'est un défi de savoir quelle est la législation applicable lorsque les détenteurs d'informations, les données stockées et, respectivement, le personnel technique qui peut avoir accès aux données se trouvent dans des pays différents. Cela est illustré notamment par le débat qui a lieu au sujet des possibilités des autorités de lutte contre la criminalité d'avoir accès à des données se trouvant dans des services cloud publics.

[159] Hellberg et autres, *Säkerhet vid molnlösningar* (La sécurité dans les solutions nuagiques), page 33.

[160] AWS, *Global Infrastructures Regions and AZs.*

Annexe 3 Conflits entre la législation des pays tiers, le droit de l'Union Européenne et le droit national

Pour une grande part, le débat suédois autour de la loi CLOUD Act et des législations similaires a concerné les conflits de normes apparus entre ce type de législation, d'une part, et, d'autre part, le droit de l'Union Européenne et le droit suédois d'autre part. Dans la présente Annexe, nous relatons les discussions qui ont été menées dans les domaines de la publicité et du secret et de la protection des données.

La publicité et le secret

La loi suédoise sur la publicité et le secret – vue d'ensemble

Le droit, institué par l'une des lois organiques de la Suède, de prendre connaissance de documents publics, est limité par la loi suédoise sur la publicité et le secret (2009:400)[161]. Si un renseignement est soumis au secret, il est interdit de le divulguer, que ce soit oralement, par remise d'un document public ou d'autre manière[162]. L'interdiction de divulgation s'applique aux administrations, mais aussi aux personnes qui ont eu connaissance de données parce que cette personne participe pour le compte du public aux activités d'une administration, par exemple pour cause d'emploi ou de mission dans cette administration[163]. En règle générale, le secret ne s'applique pas seulement par rapport à une personne particulière, mais aussi entre administrations, ainsi qu'envers des autorités étrangères et des organisations internationales[164].

Ce qui est particulièrement intéressant en ce qui concerne la loi CLOUD Act et les autres législations similaires, c'est la possibilité de transmettre des données soumises au secret à des administrations étrangères. Un tel transfert ne peut avoir lieu qu'en vertu de prescriptions légales ou règlementaires, ou si le renseignement aurait pu, dans des cas correspondants, être transmis à une administration suédoise. Dans ce dernier cas, il est en outre nécessaire que l'administration transmetteuse effectue un contrôle pour savoir s'il est conforme aux intérêts de la Suède que le renseignement soit transmis à l'autorité étrangère[165].

Il existe, toutefois, des dispositions particulières qui lèvent le secret. Ces dispositions peuvent permettre la transmission de renseignements qui seraient, en d'autres circonstances, soumis au secret, si cela est nécessaire pour que l'administration en question puisse exécuter ses tâches ou pour répondre aux besoins légitimes de particuliers[166].

---

[161] Chapitre 2, articles 1 et 2 du Règlement suédois sur la liberté de la presse.

[162] Chapitre 3, article 1 de la loi suédoise sur la publicité et lesecret.

[163] Chapitre 2, article 1 de la loi suédoise sur la publicité et lesecret.

[164] Chapitre 8, articles 1 à 3 de la loi suédoise sur la publicité et le secret.

[165] Chapitre 8, article de la loi suédoise sur la publicité et le secret.

[166] Des dispositions annulant le secret, annulant tout secret ou tout secret visé par de très nombreuses dispositions de secret se trouvent au chapitre 10 de la loi suédoise sur la publicité et le secret. Des dispositions qui lèvent le secret à la suite de la ou des dispositions concernées figurent dans les sections IV et V de la loi suédoise sur la publicité et le secret.

Avant qu'une autorité suédoise n'accorde l'accès d'un prestataire de services à des renseignements soumis au secret, cette autorité doit notamment analyser si cela équivaut à la divulgation de renseignements, dans le sens compris par la loi suédoise sur la publicité et le secret. Les autorités doivent, en outre, assurer continuellement que les règles de secret soient respectées. Il doit donc exister une préparation à ce que les nouvelles règlementations, par exemple dans d'autres pays, soient susceptibles d'influencer les solutions informatiques que les administrations suédoises ont choisi d'utiliser[167].

Le conflit entre la législation similaire à la loi CLOUD Act et la loi suédoise sur la publicité et le secret

En 2015, le groupe d'experts juridiques du programme eSam a déclaré que des renseignements ne doivent normalement pas être considérés comme divulgués dans le sens où l'entend la loi suédoise sur la publicité et le secret, bien que ces renseignements aient été techniquement mis à la disposition d'un prestataire de services, dans les cas suivants :

- Si le prestataire de services n'est contractuellement pas autorisé à prendre connaissance de ces renseignements ni à les transmettre ; et
- Si, par ailleurs, il est improbable, vu les circonstances, que cela se produise quand même[168].

Pour donner suite à la loi CLOUD Act et aux autres législations similaires, eSam a produit, en 2018, un nouvel avis juridique. Cet avis vise spécifiquement la notion de divulgation lors de l'utilisation de services cloud soumis à une législation étrangère. eSam était d'avis que les renseignements soumis au secret doivent être considérés comme divulgués s'ils sont mis techniquement à disposition d'un prestataire de services qui, suite, par exemple, à des conditions d'actionnariat, est tenu par les règlements d'un autre pays, en vertu desquels le prestataire de services peut se retrouver dans l'obligation de transmettre des informations sans que l'entraide juridique internationale soit intervenue ni qu'un autre motif juridique du droit suédois soit présent. eSam estime que, dans de telles situations, on ne peut pas considérer qu'il est improbable que les renseignements puissent être transmis à des tiers. De même pour les situations dans lesquelles les conditions d'actionnariat ou la localisation géographique des aides techniques d'un prestataire de services font craindre que les droits de l'homme (par exemple la protection de la vie privée) ou l'intérêt public (par exemple la sécurité de l'État) ne seraient pas assurés si les données des administrations suédoises avaient été mises à la disposition du prestataire de services[169].

En septembre 2019, eSam émet un commentaire sur son avis juridique et déclare notamment ce qui suit, un peu simplifié. Dans une première étape, la règlementation juridique des relations entre les parties doit avoir été structurée de manière soutenable. Il doit exister un secret contractuel juridiquement impératif et sanctionné et le fournisseur ne doit pas être tenu par des règles de droit étranger l'autorisant à transmettre des renseignements sans un contrôle préalable du secret ou un autre motif

---

[167] Voir aussi Agence nationale de services juridiques, financiers et administratifs Kammarkollegiet, *Förstudierapport Webbaserat kontorsstöd*,(Étude préliminaire concernant le soutien bureautique par Internet), Dnr 23.2-6283-18, 22.02.2019, page 35.

[168] eSam, *Röjandebegreppet enligt offentlighets- och sekretesslagen*, (La notion de divulgation selon la loi suédoise sur la publicité et le secret), VER 2015- 190, 27.12.2015.

[169] eSam, *Rättsligt uttalande om röjande et molntjänster*, (Avis juridique sur la divulgation et les services cloud) VER 2018:57, 23.10.2018.

légal du droit suédois en faveur de la remise. En cas de lacunes sur ce point, une mise à la disposition du fournisseur entraîne que les renseignements sont considérés comme divulgués dans le sens entendu par la loi suédoise sur la publicité et le secret. Il n'est alors pas question d'une estimation de probabilité. Si, par contre, une administration estime qu'une externalisation prévue aurait une base juridique stable, il faut effectuer une estimation pour savoir s'il est improbable que le prestataire de services ou son personnel, qui n'ont pas le droit de prendre connaissance des renseignements ni de les transmettre, utiliseront quand même les renseignements de manière non autorisée.

En 2019, l'Agence nationale de services juridiques, financiers et administratifs Kammarkollegiet est d'accord avec l'estimation d'eSam[170]. Kammarkollegiet dit encore qu'il n'est pas compatible avec la loi suédoise sur la publicité et le secret qu'un prestataire de services engagé par une administration suédoise transmette des renseignements soumis au secret à une autorité étrangère en vertu de la loi CLOUD Act ou d'une législation similaire. Cela, un peu simplifié, puisqu'il n'existe aucune disposition de loi ou de règlement qui autorise cette transmission. Il n'est pas non plus possible d'assurer qu'un renseignement aurait été transmis dans un cas correspondant à une autorité suédoise, ni d'assurer que les intérêts suédois sont préservés[171]. Kammarkollegiet constatait aussi que si une autorité suédoise laisse une entreprise soumise à une règlementation du type CLOUD Act gérer des renseignements soumis au secret, il semble que cette entreprise donne la priorité à la règlementation étrangère au détriment de la législation suédoise[172].

Microsoft, entre autres, est d'un autre avis. Cette société estime que le CLOUD Act apporte des arguments encore plus explicites pour qu'il soit considéré comme improbable qu'un prestataire de services engagé par les administrations suédoises prenne connaissance de renseignements soumis au secret ou les transmette. Microsoft estime donc qu'une « divulgation automatique » ne se produit pas dans ces situations et il affirme que l'on ne doit pas seulement regarder l'actionnariat étranger mais faire une appréciation plus nuancée, à partir, notamment, des engagements contractuels, de l'historique et de l'architecture technique. Microsoft invoque, en outre, que le nombre d'affaires lors desquelles elle a reçu une demande de transmission de données stockées en dehors des frontières des États-Unis est très faible[173]. Cette circonstance est également soulignée par le Cybercom Group, sous-traitant d'AWS. Cybercom dit que la réalité est maintenant différente de lorsque eSam a émis son avis juridique, en 2018. Cybercom souligne que certains des services cloud sont proposés à partir de halls informatiques suédois et qu'il existe des procédures de sécurité, par exemple le chiffrement, que l'administration contrôle totalement par elle-même vis-à- vis du fournisseur de service nuagique. Cette société estime aussi qu'une connaissance détaillée est nécessaire au sujet de la solution technique de sécurité proposée par les fournisseurs de services cloud pour pouvoir déterminer s'il est improbable que des informations soient divulguées de manière non autorisée. La conclusion de Cybercom est qu'il n'existe actuellement aucun obstacle contre le fait que des municipalités, des régions et des autorités d'État

---

[170] Kammarkollegiet, *Förstudierapport Webbaserat kontorsstöd,* (Étude préliminaire concernant le soutien bureautique par Internet), Dnr 23.2-6283-18, 22.02.2019, page 35. Il faut remarquer que la prise de position de Kammarkollegiet ne concernait que les avis de l'eSam en 2015 et 2018.

[171] Comparer au chapitre 8, article 3 de la loi suédoise sur la publicité et le secret.

[172] Kammarkollegiet, *Förstudierapport Webbaserat kontorsstöd,* (Étude préliminaire concernant le soutien bureautique par Internet), pages 32 et 33

[173] Voir notamment Microsoft, *Molntjänster och säkerhet,* (Services cloud et sécurité) 13.12.2018, SKL et autres, Séminaire ouvert à Almedalen 2019, *CLOUD Act - hinder eller ej* (Le CLOUD Act, entrave ou non).

envisagent l'utilisation de services cloud, même si leurs propriétaires sont étrangers[174]. Cette société affirme que la même opinion s'est faite jour lors d'une table ronde fermée à Almedalen, en 2019, à laquelle participaient des représentants d'administrations centrales suédoises dans le domaine de la protection des informations et de la cybersécurité, des directeurs généraux d'administrations d'État ainsi que des représentants de l'Association des collectivités territoriales suédoises (SKL)[175].

La SKL a déclaré, notamment à cause de la prise de position d'eSam en 2018, que les services cloud du marché, mêmes ceux qui sont détenus à l'étranger, sont un aspect inévitable de la dématérialisation. La SKL affirme aussi qu'une grande partie des municipalités et des régions de Suède utilisent déjà des services cloud, qui, dans certains cas, ont été négociés par des autorités publiques. L'incertitude concernant les questions juridiques est déjà considérée comme ayant entraîné un ralentissement de la numérisation et eu pour effet que des ressources considérables ont été utilisées pour l'interprétation et l'adaptation au lieu de la réalisation d'opérations. Puisqu'il s'agit de très gros investissements, à venir et déjà effectués, la SKL estime qu'il est nécessaire de fixer une orientation nationale et cohérente dans la question pour les organisations publiques. La SKL estime, en outre, que l'absence de vues conjointes sur la situation juridique des services cloud détenus de l'étranger peut entraîner de grands problèmes pour la coopération numérique entre des acteurs publics et, dans le prolongement, moins de possibilités de livrer les services qu'attend le public. Dans la mesure où il y a de telles limites à la gestion, au stockage ou à la communication de données soumises au secret, décrites dans l'avis de l'eSam, la SKL estime que cela doit être tiré au clair par une législation complétée ou modifiée[176].

Le règlement de protection des données de l'Union Européenne

Lorsque des informations contenant des données à caractère personnel sont transmises vers un pays tiers (un pays en dehors de l'Union Européenne) après une demande en vertu du CLOUD Act ou d'une autre législation similaire, cela constitue un traitement de données à caractère personnel.

Les conditions dans lesquelles un traitement de ce type est autorisé sont règlementées par le 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), dénommé ci-après le RGPD.

---

[174] Cybercom se réfère aussi aux rapports de deux cabinets d'avocats différents qui ont analysé la situation juridique et seraient parvenus à la conclusion que la règlementation actuelle permet d'envisager l'utilisation de services cloud de propriété étrangère, mais qu'une analyse doit être effectuée dans chaque cas particulier. Cette société dit aussi que des auteurs de l'avis d'eSam en 2018 auraient exprimé une interprétation moins sévère de cet avis.

[175] Blix Fredrik et Brolin Richard, *Grönt ljus för kommuner, regioner et statliga myndigheter att överväga molntjänster* (Feu vert pour les municipalités, les régions et les autorités publiques pour envisager les services cloud), 04.07.2019.

[176] Association des collectivités territoriales suédoises (SKL) *Ställningstagande om informationshantering i vissa molntjänster* (Prise de position concernant la gestion des informations dans certains services cloud), dossier No. 19/00087, 12.04.2019.

Responsable des données à caractère personnel et préposé aux données à caractère personnel

Le responsable des données à caractère personnel est responsable du fait que le traitement des données à caractère personnel est effectué en vertu du RGPD. Le responsable des données à caractère personnel est la personne qui, seule ou avec d'autres, décide des fins et des moyens utilisés lors du traitement des données à caractère personnel. Le responsable des données à caractère personnel peut engager un préposé aux données à caractère personnel qui traite les données à caractère personnel pour le compte du responsable des données à caractère personnel. Un tel préposé se trouve toujours en dehors de l'organisation du responsable des données à caractère personnel et il doit traiter les données à caractère personnel uniquement selon les instructions du responsable des données à caractère personnel. Le responsable des données à caractère personnel n'a à son tour le droit que d'engager des préposés aux données à caractère personnel et qui donnent des garanties suffisantes pour que le traitement soit effectué en vertu du RGPD et pour que les droits de la personne concernée soient protégés[177].

Lorsque une administration achète les services cloud d'un prestataire de services, cette administration est responsable des données à caractère personnel. Par l'intermédiaire du préposé aux données à caractère personnel, le prestataire de services reçoit des instructions sur le but du traitement et la manière dont il doit se dérouler. Le fournisseur est préposé aux données à caractère personnel tant qu'il traite les données à caractère personnel pour le compte de l'administration et conformément au contrat. Si le prestataire de services traite les données à caractère personnel dans un autre but que ceux qui ont été fixés par le contrat, le fournisseur doit être considéré comme le responsable des données à caractère personnel[178]. Avant qu'une administration suédoise n'engage un prestataire de services comme préposé aux données à caractère personnel, cette autorité doit cependant analyser si cela implique un risque que les données à caractère personnel soient traitées en infraction au RGPD.

La relation entre le CLOUD Act et le règlement de protection des données de l'Union Européenne

Aussi bien le Comité Européen de la Protection des Données que le Contrôleur européen de la protection des données que la Commission de l'Union Européenne se sont exprimés sur la question de savoir s'il est conforme au RGPD qu'un prestataire de services transmette des données à caractère personnel stockées au sein de l'Union Européenne à une administration étrangère, par exemple dans un but de lutte contre la criminalité. Le Comité Européen de la Protection des Données et le Contrôleur européen de la protection des données préconisent un test en deux étapes pour s'assurer que la transmission des données à caractère personnel à un pays tiers répond aux exigences du RGPD. Premièrement, il doit y avoir un motif juridique pour le traitement des données à caractère personnel et toutes les autres exigences du Règlement doivent être satisfaites, par exemple en ce qui concerne les principes généraux de proportionnalité, de véracité, de minimalisation du stockage[179]. Deuxièmement, la transmission doit correspondre aux dispositions du chapitre V du

---

[177] Articles 4.7, 4.8, 5.2, 26.1, 28.1 et 28.3 du RGPD.

[178] Voir article 28.10 du RGPD et Agence nationale de services juridiques, financiers et administratifs Kammarkollegiet, *Förstudierapport Webbaserat kontorsstöd*, (Étude préliminaire concernant le soutien bureautique par Internet), page 14.

[179] Voir Article 5 du RGPD.

RGPD, qui règlemente de manière exhaustive les conditions auxquelles les données à caractère personnel ont le droit d'être transmises à un pays tiers[180].

Motifs juridiques

L'une des conditions fondamentales pour qu'une administration ou une entreprise ait le droit de traiter des données à caractère personnel est qu'il existe un motif juridique pour ce traitement. Le RGPD règlemente de manière exhaustive quels sont les motifs juridiques acceptables pour ce traitement. Lorsque des données à caractère personnel sont transmises vers les autorités d'un autre pays après une demande, en vertu de la législation de ce pays, c'est surtout quatre motifs juridiques qui pourraient entrer en jeu.

Premièrement, le traitement peut être nécessaire pour accomplir une obligation juridique qui repose sur le responsable des données à caractère personnel (Article 6.1c), pour effectuer une tâche d'intérêt général ou comme une partie de l'exercice d'autorité concernant les données à caractère personnel (Article 6.1e). Une obligation juridique, une tâche d'intérêt général ou l'exercice de l'autorité doit être fixé en vertu du droit communautaire ou du droit national pour constituer un motif juridique légal[181]. Le Comité Européen de la Protection des Données et autres estiment que, tant que la procédure en vertu du CLOUD Act n'a pas été reconnue par une convention internationale entre l'Union Européenne et les États-Unis, les motifs juridiques d'obligation juridique, de tâche d'intérêt général ou d'exercice de l'autorité ne peuvent s'appliquer lorsque le prestataire de services transmet des données à caractère personnel conformément à une demande de ce type[182].

Deuxièmement, le traitement peut être nécessaire dans des buts qui concernent le responsable des données à caractère personnel ou les intérêts légitimes d'un tiers, si les intérêts de la personne concernée ou ses droits et libertés fondamentaux pèsent plus lourd et exigent une protection des données à caractère personnel (Article 6.1f). On doit donc trouver un équilibre entre les intérêts du responsable des données à caractère personnel et les intérêts de la personne concernée. Le Comité Européen de la Protection des Données et autres estiment que l'intérêt du responsable des données à caractère personnel pourrait consister, ici, à ne pas s'exposer à des sanctions juridiques des autorités américaines pour ne pas avoir entendu une demande de remise de données. En l'absence d'une convention internationale qui soutient la remise de données prévue par le CLOUD Act, le Comité Européen de la Protection des Données et autres estiment cependant que la remise des données pourrait s'effectuer sous la protection qu'une convention de ce type apporte, notamment pour le droit de la personne concernée à des moyens juridiques efficaces (comparer avec l'article 47 de la charte). Le Comité Européen de la Protection des Données et autres soulignent aussi qu'une demande en vertu du CLOUD Act par sa nature est telle qu'il est en pratique impossible, pour le responsable des données à caractère

---

[180] Voir Article 44 du RGPD. Voir aussi Comité Européen de la Protection des Données (EPDB-EDPS), Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection (Réponse conjointe à la Commission des libertés civiles, de la justice et des affaires intérieures (LIBE) concernant l'impact de la loi américaine CLOUD Act sur le cadre juridique européen de protection des données à caractère personnel) , 10.07.2019, Annexe, pages 3 et 4.

[181] Voir Article 6.3 du RGPD. Le chapitre 2, articles 1 et 2 de la loi suédoise No. 2018:218 comportant des dispositions complémentaires au règlement de protection des données de l'Union Européenne comporte des dispositions qui explicitent que cette exigence implique, pour la part de la Suède, que l'obligation juridique ou la tâche d'intérêt général doit être instaurée par la loi ou un autre texte législatif pour pouvoir constituer un motif juridique acceptable.

[182] EPDB-EDPS *Joint Response to the LIBE Committee*, Annexe, pages 5 et 6.

personnel, de faire une appréciation correcte de toutes les circonstances et de l'impact pour la personne concernée que pourrait entraîner une remise des données. Dans ces circonstances, le Comité Européen de la Protection des Données et autres estiment que l'intérêt de la personne concernée, à savoir que les données à caractère personnel ne soient pas transmises, doit peser plus lourd que l'intérêt du responsable des données à caractère personnel de fournir les données dans les cas où une demande de remise de renseignements est adressée au prestataire de services en vertu du CLOUD Act.

Pour conclure, le traitement peut être nécessaire pour protéger des intérêts d'importance fondamentale pour la personne concernée ou pour une autre personne physique (Article 6.1d). Il ressort des motifs du RGPD que le traitement des données à caractère personnel ne peut s'appuyer que sur ce motif juridique si le traitement ne peut pas avoir un autre motif manifeste[183]. Puisque le traitement des données à caractère personnel qui est effectué lors de la remise de données à caractère personnel en vertu du CLOUD Act pourrait être effectué, à la place, en vertu de la procédure fixée dans des conventions passées sur l'entraide juridique internationale (MLAT), le Comité Européen de la Protection des Données et autres estime qu'une remise de ce type ne peut pas être considérée comme nécessaire pour protéger les intérêts d'une personne physique autre que la personne concernée. Le Comité Européen de la Protection des Données et autres n'exclut cependant pas que, dans des circonstances exceptionnelles, il peut arriver qu'une remise de données en vertu du CLOUD Act peut s'avérer nécessaire pour protéger les intérêts de la personne concernée. Citons comme exemple que les données à caractère personnel sont nécessaires dans une enquête concernant des enlèvements d'enfants. Notons cependant qu'un tel traitement doit, dans le même temps, répondre aux exigences pour le transfert à un pays tiers qui sont formulées à l'Article 49.1f (voir ci-dessous)[184].

Transmission de données à caractère personnel vers un pays tiers

La règle principale du RGPD est que la transmission ou la fourniture de données à caractère personnel qui se basent sur une décision de justice ou des autorités d'un pays tiers ne doit être effectuée que si la décision se base sur une convention internationale applicable entre le pays tiers demandeur et l'Union ou un État tiers, par exemple un MLAT (Article 48). Comme l'a constaté la Commission de l'Union Européenne, il ressort clairement de cette disposition qu'une décision de justice d'un pays tiers n'implique pas, en elle-même, qu'une transmission de données à caractère personnel est légale en vertu du RGPD[185]. Dans ses directives, le Comité Européen de la Protection des Données a en outre déclaré que, dans les situations où il existe un MLAT ou similaires, une entreprise se trouvant dans l'Union Européenne devrait en général refuser les demandes directes de remise et renvoyer l'administration du pays tiers au contrat en cours[186].

La transmission de données à caractère personnel doit en outre s'effectuer si la Commission a pris la décision que le pays tiers assure un niveau de sécurité adéquat. Si une telle décision n'est pas prise, les données à caractère personnel peuvent être

---

[183] Voir les motifs 46 du RGPD.

[184] EPDB-EDPS, *Joint Response to the LIBE Committee*, Annexe, pages 7 et 8.

[185] Commission européenne, *Brief of the European Commission on behalf of the European Union as amicus curiae in support of neither Party in the case United States v. Microsoft Corp*. Voir aussi Comité Européen de la Protection des Données, *Directives 2/2018 pour des exceptions dans l'article 49 en vertu du Règlement 2016/679*, adoptées le 25 mai 2018, page 5.

[186] Comité Européen de la Protection des Données, *Directives 2/2018*, page 5.

transmises à un pays tiers après que certaines mesures adéquates données aient été prises et à la condition que les droits légitimes et des moyens juridiques efficaces soient accessibles pour les personnes concernées (Articles 45, 46 et 47). La Commission a adopté la position qu'aucune de ces conditions n'est probablement remplie dans une situation dans laquelle les autorités d'un pays tiers demandent l'accès à des données stockées au sein de l'Union Européenne[187].

A partir des appréciations du Comité Européen de la Protection des Données et de la Commission concernant les Articles 45 à 48 du RGPD il faut donc l'une des situations d'exception présentées à l'Article 49.1 pour qu'une transmission des données à caractère personnel en vertu de la législation d'un pays tiers soit légale en vertu du RGPD[188]. Dans une telle situation, c'est surtout quatre de ces exceptions qui peuvent entrer en jeu.

La première exception vise les transmissions nécessaires pour des raisons importantes qui concernent l'intérêt public (Article 49.1 d). Cet intérêt général doit être reconnu dans le droit de l'Union ou dans le droit national qui concerne le responsable des données à caractère personnel[189]. Le Comité Européen de la Protection des Données et autres estime qu'il ne faut pas tenir compte des intérêts d'un pays tiers dans le cas présent. Il n'est pas non plus suffisant que les intérêts du pays tiers, par exemple pour entreprendre une enquête donnée, coïncident aussi avec les intérêts de l'Union Européenne ou ceux d'un État membre[190].

La seconde exception qui pourrait s'appliquer est l'exception aux transmissions nécessaires pour pouvoir établir, faire valoir ou défendre des prétentions juridiques (Article 49.1e). Le Comité Européen de la Protection des Données et autres soulignent que cette exception exige un lien proche entre la transmission de données et une procédure spécifique et que l'exception ne peut pas être utilisée pour motiver la transmission de données à caractère personnel sur la seule base qu'un procès ou une procédure formelle peuvent avoir lieu dans l'avenir[191].

La troisième exception qui peut entrer en jeu est que la transmission est nécessaire pour protéger les intérêts fondamentaux de la personne concernée ou les intérêts fondamentaux d'autres personnes, lorsque la personne concernée est empêchée physiquement ou juridiquement de donner son accord (Article 49.1f). Le Comité Européen de la Protection des Données et autres estiment que, exactement comme pour le motif juridique de l'Article 6.1d, la protection des intérêts de la personne concernée pourrait entraîner que les conditions de cette exception sont remplies. Le Comité Européen de la Protection des Données et autres ont aussi déclaré que l'exigence que la personne concernée doit être empêchée de donner son acceptation peut couvrir des situations où c'est la personne concernée qui doit être empêchée de donner son accord peut comprendre des situations dans lesquelles c'est la personne concernée qui constitue une menace immédiate contre la vie d'autres personnes ou leur intégrité physique. Une condition est cependant citée comme étant qu'il existe suffisamment d'informations pour établir la légitimité. Le Comité Européen de la Protection des Données souligne cependant que les intérêts d'autres personnes ne

---

[187] Commission européenne, *Brief of the European Commission*

[188] Si la Commission n'a pris aucune décision concernant le niveau de protection adéquat et qu'aucune mesure de précaution n'a été prise, la transmission à un pays tiers ne peut avoir lieu que si l'une des situations d'exception énoncées à l'Article 49.1 du RGPD est présente.

[189] Voir Article 49.4 du RGPD.

[190] EPDB-EDPS, *Joint Response to the LIBE Committee*, Annexe page 6

[191] EPDB-EDPS, Joint Response to the LIBE Committee, Annexe pages 6 et 7 et Comité Européen de la Protection des Données, Directives 2/2018, pages 11 et 12.

peuvent pas être utilisés comme motif juridique pour une transmission vers un pays tiers s'il existe d'autres motifs juridiques qui peuvent être utilisés à la place, par exemple lorsqu'il existe une procédure MLAT convenue[192].

Si aucune des exceptions mentionnées précédemment n'est applicable, il existe une dernière exception applicable dans l'Article 49.1, alinéa second du RGPD. En vertu de cette exception, une transmission vers un pays tiers ne peut avoir lieu que s'il est nécessaire, pour des objectifs qui concernent les intérêts légitimes impératifs du responsable des données à caractère personnel et les intérêts de la personne concernée, ou des droits et des libertés qui ne pèsent pas plus lourd. Il faut donc mûrement peser ces deux intérêts l'un par rapport à l'autre. Le domaine d'application de cette exception est particulièrement étroit et l'exception contient un certain nombre de critères qui doivent être satisfaits pour qu'elle soit applicable. Le responsable des données à caractère personnel doit, par exemple, avoir estimé toutes les circonstances autour de la transmission et, à partir de cette appréciation, pris les mesures de protection adéquates pour les données à caractère personnel. Le responsable des données à caractère personnel est aussi dans l'obligation d'informer aussi bien l'autorité de tutelle que la personne concernée.

La Commission de l'Union Européenne estime que l'intérêt du responsable des renseignements de ne pas faire l'objet de sanctions juridiques dans un pays tiers pourrait constituer un intérêt légitime visé par cette dernière exception[193]. Le Comité Européen de la Protection des Données et autres constatent cependant que les exigences à satisfaire concernant cette exception sont beaucoup plus sévères que celles qui concernent l'utilisation du motif juridique de comparaison des

intérêts, Article 6.1f du RGPD. Le Comité Européen de la Protection des Données et autres soulignent aussi plusieurs difficultés pour se servir de cette exception lors d'une demande en vertu du CLOUD Act. Premièrement, c'est exactement comme lorsqu'il s'agit du motif juridique de comparaison des intérêts, difficile d'effectuer une estimation correcte de toutes les circonstances et conséquences possibles pour la personne concernée. Deuxièmement, une demande de transmission en vertu du CLOUD Act est souvent assortie d'une interdiction de divulgation pour ne pas compromettre une enquête criminelle. Cela entraîne des difficultés pour le responsable des données à caractère personnel lorsqu'il s'agit, pour lui, d'informer l'autorité de tutelle et la personne concernée. Troisièmement, il ne sera pas possible, en pratique, pour le responsable des données à caractère personnel de prendre les mesures de protection adéquates pour la transmission. Dans ces circonstances, le Comité Européen de la Protection des Données et autres estiment que l'exception de l'Article 49.1, alinéa second, ne peut être appliquée pour transmettre légalement des données à caractère personnel aux autorités américaines sur une demande présentée en vertu du CLOUD Act[194].

---

[192] EPDB-EDPS, Joint Response to the LIBE Committee, Annexe page 7.

[193] Commission européenne, *Brief of the European Commission.*

[194] Comité Européen de la Protection des Données (EPDB-EDPS), *Joint Response to the LIBE Committee*, Annexe, page 7.

La conséquence du conflit entre le CLOUD Act et le RGPD pour les administrations suédoises

Selon l'appréciation faite par le Comité Européen de la Protection des Données et autres, il n'existe donc, pour le moment, de motif juridique pour la transmission de données à un pays tiers en vertu du CLOUD Act que dans des cas exceptionnels, dans le but de protéger les intérêts de la personne concernée. De même pour les conditions d'une transmission légitime vers un pays tiers en vertu des dispositions du chapitre V du RGPD.

Un responsable des données à caractère personnel ou un préposé aux données à caractère personnel qui transmet des données à caractère personnel aux autorités d'un pays tiers sans qu'il y ait un motif juridique à cela prévu par le RGPD risque, dans le pire des cas, d'être condamné à des pénalités administratives considérables[195]. Les conditions sont les mêmes lorsque des données à caractère personnel sont transmises à un pays tiers sans qu'aucune des conditions de la section V du RGPD ne soit remplie. Toute personne qui se conforme à une demande en vertu du CLOUD Act risque donc des sanctions prévues par le droit de l'Union Européenne. Si une telle demande n'est pas suivie d'effet, il existe un risque de sanctions juridiques aux États-Unis. Cela signifie en pratique que les prestataires de services risquent d'être exposés à un conflit entre le droit de l'Union Européenne et la loi américaine[196196].

Une administration suédoise n'est probablement pas le responsable des données à caractère personnel quand il s'agit du traitement des données à caractère personnel qui est effectué lorsqu'un employé préposé aux données à caractère personnel, par exemple le prestataire de services, fournit des données à un pays tiers en infraction au contrat. En tant que responsable des données à caractère personnel, l'administration n'a toutefois le droit d'engager uniquement des préposés offrant des garanties suffisantes pour que les droits des personnes concernées soient protégés et pour que le traitement soit effectué selon les termes du RGPD. Tout défaut dans ce traitement peut résulter en des pénalités[197]. Une administration qui désire utiliser des services cloud doit donc faire en sorte qu'il ne soit pas engagé de prestataire de services susceptible d'enfreindre le RGPD ou le contrat du préposé aux données à caractère personnel.

---

[195] Voir les Articles 44 et 48 comparés à l'Article 83.5c du RGPD. Les montants des sanctions peuvent aller jusqu'à un maximum de 20 millions d'euros ou 4% du chiffre d'affaires global annuel d'une entreprise.

[196] EPDB-EDPS, *Joint Response to the LIBE Committee,* Annexe, page 2.

[197] Voir articles 28.1 et 83.4 du RGPD. Pour une administration, ces pénalités peuvent atteindre au maximum 10 millions d'euro.

Annexe 4 Exemples de restitution par des prestataires de services de données de clients à des autorités de lutte contre la criminalité

Plusieurs fournisseurs publient régulièrement des rapports sur les demandes de données provenant d'autorités de lutte contre la criminalité. Nous ignorons à quel point ces rapports sont complets, et, puisque différents acteurs publient différentes informations de différentes manières, ils ne sont pas comparables. L'objectif de la présente section est d'obtenir, à partir d'informations divulguées au public, une vue d'ensemble des données éventuellement transmises par des fournisseurs et des informations qui sont accessibles pour leur transmission par les gros fournisseurs.

Microsoft publie un rapport tous les six mois. Une bonne partie des demandes concerne les comptes des personnes privées, mais Microsoft décrit aussi des demandes de comptes autres que consommateurs. Microsoft indique que, pendant les six derniers mois de 2018, 61 demandes lui sont parvenues sur le plan mondial concernant des comptes associés à des clients nuagiques, avec plus de 50 comptes utilisateurs. Dans 22 affaires, Microsoft a fourni les données, après examen.

Parmi ces 22 affaires, du contenu a été livré dans 15 affaires et des métadonnées ont été fournies dans sept affaires. Parmi les 15 affaires pour lesquelles des contenus ont été transmis, huit étaient associées aux autorités américaines d'application de la loi. Dans la même période, les autorités américaines d'application de la loi ont transmis des données dans 36 affaires qui concernant des clients comportant plus de 50 utilisateurs. Parmi ces demandes, une concernait des données stockées en dehors des États-Unis[198].

AWS ne publie pas de données distinctes concernant les comptes des particuliers ou les services des organisations. AWS publie notamment des demandes concernant spécifiquement leur service nuagique, AWS. Si l'on exclut les demandes ayant trait à la sécurité de l'État, qui sont totalement soumis au secret, 271 demandes avaient été reçues en 2018. Dans ces affaires, des données avaient été remises dans 200 cas[199].

Google publie continuellement des rapports sur les demandes et les remises de données aux autorités. Ils décrivent aussi qu'ils désirent être ouverts sur ces informations, car ils désirent orienter l'attention sur la grande quantité de demandes, ainsi que sur les lois et procédures juridiques qui affectent l'accès aux informations en ligne.

Google rapporte aussi la proportion d'affaires dans lesquelles la demande aboutit à la transmission de données. Au total, Google déclare que, entre 2011 et 2018, des données ont été transmises aux autorités anticriminalité dans i 375.604 cas. Le nombre de demandes augmente et les données sont fournies dans environ 75 % des affaires[200].

---

[198] Microsoft, *Law Enforcement Requests Report.*

[199] AWS, *Information Request Report.*

[200] Google, *Begäran om användarinformation* (Demandes d'informations utilisateurs).

Annexe 5 Protection & sécurité

Les dispositions concernant la protection de sécurité constituent une part importante de la protection des fonctions de portée sociétale. Cette Annexe expose brièvement la protection des activités sensibles du point de vue de la sécurité instituée par la loi suédoise No. 2018:585 sur le contrôle de sécurité.

Activités sensibles du point de vue de la sécurité et protection des informations et des personnels

La loi suédoise sur le contrôle de sécurité s'applique aux personnes qui exercent des activités sensibles du point de vue de la sécurité, ce qui comprend notamment les activités importantes pour la sécurité de l'État suédois[201]. Toute personne exerçant des activités sensibles du point de vue de la sécurité est dans l'obligation de les protéger par un travail de prévention contre l'espionnage, le terrorisme et certaines autres menaces[202]. Les activités sensibles du point de vue de la sécurité sont identifiées à partir du préjudice causé à la sécurité de la Suède si un attaquant se procure des informations sur les activités, détruit des informations ou empêche d'autre manière les activités de se dérouler[203]. Le travail de protection de sécurité doit se baser sur une analyse de la protection de sécurité visant à identifier les activités et les accès aux informations qui sont soumis à la loi suédoise sur le contrôle de sécurité et si la protection de ces informations est suffisante[204]. Les exigences concernant le traitement des données classifiées comme relevant de la protection de sécurité augmentent avec le niveau de classification.

Les activités sensibles du point de vue de la sécurité sont notamment le fait des administrations suédoises, par exemple l'Agence de la sécurité sociale Försäkringskassan. La loi suédoise sur le contrôle de sécurité comporte des dispositions sur les mesures de contrôle de sécurité qui doivent être prises pour les activités sensibles du point de vue de la sécurité. Ces mesures concernent notamment la sécurité des informations et des personnels[205].

La sécurité des informations consiste à protéger des informations, où qu'elles soient, d'une manière telle qu'elles ne puissent être partagées ni modifiées par des personnes non autorisées. Il s'agit aussi de faire en sorte que les informations soient à portée lorsque nécessaire. Tout cela dans le but d'éviter les graves conséquences négatives pour des activités que de telles situations peuvent entraîner[206].

Un emploi ou une autre participation à des activités sensibles du point de vue de la sécurité est habituellement placé dans une classe de sécurité, à partir du type de données dont la personne prendra connaissance et dans quelle mesure cela se

---

[201] Chapitre 1, article 1 de la loi suédoise sur le contrôle desécurité.

[202] Chapitre 1, article 2 de la loi suédoise sur le contrôle desécurité.

[203] Chapitre 2, article 5 de la loi suédoise sur le contrôle de sécurité. Les quatre classes de sécurité sont : 1) classé secret si le dommage qui peut se produire est particulièrement grave ; 2) secret lors d'un dommage grave ; 3) confidentiel lors d'un dommage non négligeable ; et 4) partiellement secret lors d'un dommage seulement peu important.

[204] Chapitre 2, article 1 de la loi suédoise sur le contrôle de sécurité.

[205] La loi couvre également la sécurité physique. Se chapitre 2, articles 2 à 4 de la loi suédoise sur le contrôle de sécurité.

[206] Chapitre 2, article 2 de la loi suédoise sur le contrôle de sécurité. Voir aussi Service de la sûreté suédoise, Sécurité des informations.

produira[207]. Lors d'un emploi dans un État, une municipalité ou une région placés dans la classe de sécurité 1 ou 2, il est exigé que la personne soit de nationalité suédoise. Cette exigence ne s'applique cependant pas pour d'autres participations à des activités sensibles du point de vue de la sécurité qui sont exercées par un État, une municipalité ou une région[208].

L'objectif de la sécurité du personnel est d'empêcher que les personnes non fiables participent à des activités leur donnant l'accès à des données classifiées du point de vue de la sécurité ou à des activités qui, pour une autre raison, sont sensibles du point de vue de la sécurité. La sécurité des personnels doit aussi assurer que les personnes qui participent à des activités sensibles du point de vue de la sécurité détiennent des connaissances suffisantes sur la protection de sécurité. Ceux qui doivent engager ou confier une mission à une personne dans des activités sensibles du point de vue de la sécurité doivent effectuer un contrôle de sécurité avant que la personne ne participe aux activités. Cela s'applique que la participation soit le fait d'un emploi ou d'autre manière. L'objectif du contrôle de sécurité est d'établir si la personne peut être supposée loyale envers les intérêts à protéger et, par ailleurs, loyale sur le plan de la sécurité. Un autre but est de rechercher les éventuelles vulnérabilités qui pourraient faire que la personne ne se retrouve dans une situation exposée et ne devienne vulnérable à des pressions externes[209].

Le contrôle de sécurité des personnes qui doivent participer à des activités sensibles du point de vue de la sécurité doit être effectué par la personne responsable de l'embauche ou d'autres participations aux activités sensibles du point de vue de la sécurité. Si une administration a le pouvoir de décider si une personne convient pour participer à des activités sensibles du point de vue de la sécurité auprès d'un acteur particulier, c'est alors cette administration qui effectuera l'appréciation finale[210]. Le contrôle de sécurité se compose normalement d'une enquête de base, du contrôle de registres et de la formation en protection de sécurité. Lors de l'enquête de base, la situation personnelle de la personne est établie sous l'aspect pertinent pour le contrôle de sécurité. Cette étape est réalisée notamment sous la forme d'un entretien de protection de sécurité qui est l'un des outils essentiels pour collecter les bases de cette appréciation. En outre, on peut collecter des certificats, des attestations et des références pertinentes et les apprécier. D'autres données, telles que, par exemple, des informations de sources ouvertes comme les médias sociaux et Internet, peuvent contribuer à créer une image plus complète de la personne[211]. Après une enquête de base ayant donné des résultats satisfaisants en ce qui concerne la loyauté, la fiabilité et la vulnérabilité, le contrôle de sécurité doit normalement être complété par une demande de contrôle de registres auprès du Service de la sûreté suédoise, si le service est placé dans une classe de sécurité[212]. Le contrôle de registres comprend des données collectées dans le registre des infractions, le registre des présomptions et

---

[207] Chapitre 3, articles 5 à 10 de la loi suédoise sur le contrôle de sécurité.

[208] Chapitre 3, article 11 la loi suédoise sur le contrôle de sécurité.

[209] Chapitre 2, article 4 et chapitre 3, articles 1 et 2 de la loi suédoise sur le contrôle de sécurité. Voir aussi Service de la sûreté suédoise, *Personalsäkerhet* (Sécurité du personnel).

[210] Chapitre 3, article 4, alinéa 2 de la loi suédoise sur le contrôle de sécurité et chapitre 5, article 4 de l'ordonnance concernant le contrôle de sécurité. Voir aussi Service de la sûreté suédoise, *Vägledning i säkerhetsskydd - personalsäkerhet* (Guidage en protection de sécurité : sécurité du personnel), juin 2019, page 18.

[211] Chapitre 3, articles 3 et 4 de la loi suédoise sur le contrôle de sécurité (2018:585), chapitre 5, article 2 de l'ordonnance 2018:658 concernant le contrôle de sécurité et chapitre 6 , article 4 des Prescriptions du Service dela sûreté suédoise (PMFS 2019:2) concernant la protection de sécurité. Voir aussi Service de la sûreté suédoise, *Vägledning i säkerhetsskydd* (Guidage en protection de sécurité), pages 11 et 12.

[212] Chapitre 3, article 14 de la loi suédoise sur le contrôle de sécurité (2018:585).

des données traitées en vertu de la loi suédoise No. 2018:1693 sur le traitement par la police des données à caractère personnel dans le domaine de la loi sur les données de criminalité[213].

En ce qui concerne des personnes ayant été domiciliées dans un autre pays, le Service de la sûreté suédoise n'a cependant que des possibilités limitées d'effectuer des contrôles de registres qualitatifs. Le Service de la sûreté suédoise estime que, dans ces cas-là, le responsable des activités doit tenir compte de ce fait dans son contrôle de sécurité, par exemple en approfondissant le contrôle des antécédents. Le Service de la sûreté suédoise recommande de poser des exigences plus sévères lors de la collecte de références du contrôle de sécurité, en ce qui concerne les personnes non domiciliées en Suède, car les possibilités d'utiliser des outils de contrôle suédois sont limitées à l'étranger[214].

Appels d'offres sous protection

Les activités sensibles doivent avoir la même protection, quel que soit l'acteur qui les exerce. Une autorité doit donc exiger le même niveau de protection chez les fournisseurs qu'elle place dans ses propres activités[215]. Les appels d'offres sous protection sont le processus par lequel l'autorité adjudicatrice analyse quelles sont les valeurs sécuritaires qui résident dans l'appel d'offres. Les autorités d'État, les municipalités et les conseils généraux qui procèdent à certains types d'appels d'offres liés à des activités sensibles du point de vue de la sécurité doivent passer un contrat de sécurité avec le soumissionnaire ou le fournisseur qui établit de quelle manière ce fournisseur doit satisfaire les exigences de protection de sécurité. Un tel contrat doit aussi être signé avec d'autres éventuels sous-traitants. L'autorité doit également contrôler et effectuer le suivi du fait que les fournisseurs ont réellement pris les mesures que l'autorité a exigées[216]. Le Service de la sûreté suédoise désigne comme l'un des risques lors des appels d'offres d'activités sensibles du point de vue de la sécurité le fait que les exigences formulées dans le contrat de protection de sécurité sont parfois si générales qu'il est difficile d'en effectuer le suivi[217].

Le contrat de protection de sécurité constitue aussi une base de décision pour l'embauche et autres participations des fournisseurs qui doivent être placés en classe de sécurité. Lorsqu'une autorité signe un contrat de protection de sécurité avec un fournisseur, ce fait doit être signalé au Service de la sûreté suédoise. L'objectif est que le Service de la sûreté suédoise puisse effectuer un contrôle de registres sur les personnes qui, en relation avec le contrat, occuperont des postes classés sécurité[218].

---

[213] Chapitre 3, article 13 de la loi suédoise sur le contrôle de sécurité.

[214] Service de la sûreté suédoise, *Vägledning i säkerhetsskydd* (Guidage en protection de sécurité), page 26.

[215] Service de la sûreté suédoise, *Säkerhetsskydd vid upphandlingar och affärsavtal* (Contrôle de sécurité lors d'appels d'offres et de contrats commerciaux).

[216] Chapitre 2, article 6 de la loi suédoise sur le contrôle de sécurité. Cette disposition vise les appels d'offres et les contrats concernant des marchandises, des services ou des marchés de travaux si l'appel d'offres contient des données classées sécurité de classe confidentielle ou plus élevée, ou si l'appel d'offre vise par ailleurs ou ouvre au fournisseur l'accès à des activités sensibles du point de vue de la sécurité d'importance équivalente pour la sécurité de la Suède.

[217] Service de la sûreté suédoise, *Årsbok 2017* (Livre annuel 2017), page 56.

[218] Service de la sûreté suédoise, *Säkerhetsskydd vid upphandlingar och affärsavtal* (Contrôle de sécurité lors d'appels d'offres et de contrats commerciaux).

Annexe 6 La classification des activités d'importance sociétale, l'exemple de la Direction suédoise des transports Transportstyrelsen

La Direction suédoise des transports a pour objet d'atteindre une bonne accessibilité, une qualité élevée, des transports sûrs et dépollués dans le domaine des chemins de fers, des transports aériens, maritimes et routiers. La Direction suédoise des transports élabore des règles, accorde des permis et effectue le suivi de leur respect. A l'aide d'un registre, cette autorité traite des tarifs, des permis et des changements de propriétaire.

En 2017 la Direction suédoise des transports a effectué une analyse de sécurité pour identifier les activités à protéger, les antagonistes potentiels, les conséquences lors de l'effacement ou la destruction ainsi que les mesures à prendre pour éliminer les vulnérabilités. Cette analyse de sécurité n'est pas accessible au public, mais certaines conclusions générales ont été publiées dans une enquête demandée par le gouvernement suédois[219].

Selon cette analyse de sécurité, la Direction suédoise des transports gère de très grandes quantités d'informations et de données. Une très petite partie des informations est secrète et une petite partie des informations est soumise au secret professionnel. La plus grande part des informations doit toutefois être considérée comme officielle et peut être demandée par le public.

Une autre problématique est que la quantité totale d'informations est en elle-même un actif à protéger. Cela puisque des données de base à haute résolution, vu leur richesse en détails, apportent une image trop complète du contenu informatif, considéré sous différents aspects de sécurité. Une personne qui a accès à la totalité peut, en analysant différents renseignements, découvrir des divergences et, de cette manière, par déduction, parvenir à des informations secrètes. Un accès sans restriction à de grandes quantités d'informations entraîne généralement des risques de mesures et d'analyses qui ne doivent pas exister pour des raisons de sécurité. L'absence même d'informations qui auraient dû exister peut constituer un risque[220].

[219] Direction suédoise des transports, *Kartläggning av hanteringen av vissa uppgifter* (Inventaire du traitement de certaines données).

[220] La Police de Suède, effectue au besoin, par exemple, des recherches dans le registre de la Direction suédoise des transports.

Dans l'enquête de 2017 concernant l'externalisation de la Direction suédoise des transports, on constate que, pour des raisons de sécurité, la Direction suédoise des transports avait pour stratégie que le plus petit nombre de personnes possible devait avoir connaissance des types de renseignements traités par cette Direction. C'est pourquoi la totalité de la masse d'informations doit être considérée comme sensible du point de vue de la sécurité. Puisque les renseignements couverts par le secret et la classification sont divulgués dans le reste des informations, il devient problématique d'élaborer un soutien informatique lorsque certaines parties doivent être traitées comme non importantes pour la société alors que d'autres parties ne le sont pas[221].

[221] Rapport des commissions officielles de l'État suédois, SOU 2018:6, *Granskning av Transportstyrelsens upphandling av it-drift* (Examen de l'appel d'offres d'opérations informatiques de la Direction suédoise des transports), pages 76 et 77, 84, 100, 220 et 223.

Annexe 7 Chiffrement, la protection & divulgation des renseignements

Le chiffrement consiste à rendre des informations difficiles à lire pour toutes les personnes qui ne doivent pas pouvoir les lire. Pour rendre les informations lisibles à nouveau, il faut les décrypter. Cela signifie que celui qui crypte les informations et celui qui doit lire les informations doivent avoir accès à la clé nécessaire pour décrypter les informations. Ce sont surtout les organisations militaires et politiques qui ont une longue expérience du chiffrement. Le chiffrement est effectué pour que les personnes non autorisées n'aient pas accès aux informations.

Cependant, aussi longtemps que le chiffrement a existé, des personnes non autorisées se sont efforcées de trouver la clé de chiffrement pour accéder aux informations.

Dès l'apparition des ordinateurs, le chiffrement et le déchiffrement ont été automatisés et les codes doivent être de plus en plus complexes pour que les personnes non autorisées ne puissent pas les casser.

Le chiffrement peut, en principe, s'appliquer lors de deux situations de principe : lorsque les informations sont stockées et lorsque les informations sont transportées. Puisque les défis sont différents pour le stockage et pour le transport, il est important de pouvoir sécuriser la forme de chiffrement visée.

Il est également important de considérer que, en pratique, les données ne peuvent pas être traitées lorsqu'elles sont cryptées. Pour pouvoir traiter des données, il faut tout d'abord les décrypter. Cela signifie que si le traitement est effectué dans une fonction qui se trouve chez le fournisseur, le fournisseur doit avoir la possibilité de décrypter.

En vertu du chapitre 3, article 5 de l'ordonnance suédoise 2018:658 concernant le contrôle de sécurité, toutes les activités, publiques et privées, qui traitent des données classifiées pour la protection de sécurité et qui doivent être communiquées à un système d'informations hors du contrôle du détenteur des activités, doivent protéger les données à l'aide de fonctions cryptographiques approuvées par les Forces armées suédoises[222]. Les fonctions cryptographiques des Forces armées suédoises ne sont pas prévues ni adéquates pour tous les types d'informations et activités.

Les fournisseurs peuvent proposer à leurs clients le chiffrement comme une partie de leur offre de services. Les services offerts ainsi que la protection proposée varient et cela ne peut être considéré que comme un exemple. Il vaut cependant la peine de noter qu'un bon nombre des services proposés par les grandes prestataires de services cloud ne sont pas approuvés par les Forces armées suédoises.

Microsoft propose trois services de base pour le chiffrement de ses services cloud : Customer key, Bring your own key et Hold your own key. AWS propose aussi des services de chiffrement dans lesquels aussi bien le client qu'AWS détiennent la clé et l'exemple ci-dessous n'est qu'un exemple d'utilisation[223].

---

[222] Forces armées suédoises, *Försvarsmaktens föreskrifter om signalskyddstjänsten och Försvarsmakten, Godkända kryptoapparater,* (Prescriptions des Forces armées suédoises sur le service de protection du chiffre et Appareils de chiffrement approuvés par les Forces armées suédoises) septembre 2019

[223] AWS, *Protection Data using encryption.*

Customer key/service encryption

Microsoft propose ce service pour Sharepoint Online, Onedrive Business et Exchange Online. Ce service implique une protection contre l'accès physique aux données, si, par exemple, une personne non autorisée accède à un disque dur.

Cette méthode de chiffrement ne protège pas contre l'accès aux données d'une personne autorisée. Les données cryptées selon cette méthode peuvent être accédées par un technicien autorisé chez le fournisseur et peuvent être remises à une administration étrangère en vertu de la législation en vigueur[224].

Bring your own key

Microsoft propose ce service pour le chiffrement de documents particuliers, c'est pourquoi il peut convenir à des messages courriels ou documents particuliers.

Le propriétaire peut choisir de crypter les documents. Cependant, Microsoft a accès à la clé pour pouvoir lire et indexer les données, et protège les documents contre l'accès non autorisé.

Les données cryptées selon cette méthode peuvent être rendues accessibles par un technicien autorisé chez le fournisseur et peuvent être remises à une administration étrangère en vertu de la législation en vigueur[225].

Hold your own key

Ce service est proposé par Microsoft pour le chiffrement de documents particuliers, c'est pourquoi il peut convenir à des messages courriels ou documents particuliers. Le propriétaire peut choisir de crypter les documents. Le client détient cependant toute la chaîne de codes, ce qui signifie que le fournisseur n'a pas accès à la clé de déchiffrement.

Cette absence d'accès entraîne cependant que les possibilités d'utilisation du service informatique sont très limitées. Un exemple est que l'utilisateur ne peut pas utiliser les fonctions de recherche et que l'interopérabilité avec d'autres entités extérieures en est très limitée.

Tant qu'une autorité étrangère n'exige pas d'avoir l'accès au code de chiffrement, cette méthode pourrait empêcher l'accès d'un technicien autorisé chez le fournisseur et les données ne peuvent pas être remises décryptées à une administration étrangère en vertu de la législation en vigueur.

Cette solution impliquerait cependant une moins bonne fonctionnalité pour les utilisateurs dans leur utilisation quotidienne, par exemple, de logiciels bureautiques. D'une part, puisque certaines fonctions ne seraient pas accessibles du tout, d'autre part, puisque les performances seraient affectées négativement[226].

---

[224] Microsoft, *Service encryption with Customer Key for Office 365 FAQ.*

[225] Microsoft, *Prisnivåer och begränsningar för BYOK* (Niveaux de prix et limitations de *Bring your own key).*

[226] Microsoft, *Håll din egen nyckel skydd* (Hold your own key) pour Azure Information Protection

Accès d'autorités étrangères aux codes de chiffrement

Des lois de transmission de codes de chiffrement existent dans un certain nombre de pays. Le Conseil de l'Europe a proposé en 2013 que cette possibilité soit instaurée au sein de l'Union Européenne[227]. La Suède n'a actuellement pas ce type de législation. Le 24 octobre 2019, le gouvernement a toutefois effectué une saisine du Conseil de législation sur la lecture secrète de données. Il y est proposé que les autorités anticriminalité aient la possibilité de se servir, notamment, du déchiffrement comme moyen secret de coercition lors de présomptions de crimes graves[228].

Dans les Pays nordiques, le Danemark a été le premier pays à instaurer, en 2002, une législation permettant la lecture secrète de données. Une législation correspondante a ensuite été adoptée en Finlande et en Norvège et ces législations comprennent la possibilité de déchiffrement[229].

Une étude de 2017, sur mission du Parlement de l'Union Européenne, démontre que des méthodes de lecture secrète de données sont utilisées dans les États membres de l'Union Européenne soumis à la comparaison, dans certains cas conformément à des dispositions légales explicites, et non dans d'autres cas. Dans les États qui n'ont pas de législation explicite, un travail législatif est en cours actuellement[230].

L'enquête du Parlement européen analyse aussi trois pays non européens. Elle constate que l'Australie n'a pas de législation explicite, mais que l'enquête a pu exclure que des moyens de coercition secrets sont utilisés en vertu d'une autre législation plus ancienne[231]. Elle constate qu'Israël a une législation plus claire et ménage notamment la possibilité du déchiffrement[232].

Puisque l'exemple utilisé ici décrit la législation américaine, nous utilisons aussi la situation légale actuelle des États-Unis pour donner aussi des exemples plus détaillés des possibilités des autorités étrangères d'accéder à des codes de chiffrement. L'enquête effectuée en 2017 sur mission du Parlement européen illustre aussi comment des moyens de coercition secrets sont utilisés par les autorités anticorruption américaines[233].

Le cinquième article de la constitution américaine déclare qu'une personne ne doit pas être obligée de présenter des preuves qui parlent contre son propre intérêt et que cela peut être considéré comme un obstacle pour exiger l'accès à des codes de chiffrement[234]. Il existe cependant des cas juridiques lors desquels les codes de chiffrement et les mots de passe ont été remis. Le premier cas était *In re Boucher*

---

[227] Enquête sur la convention sur la délinquance informatique, *Europarådets konvention om it-relaterad brottslighet,* (Convention du Conseil de l'Europe sur la délinquance informatique) (Rapport des commissions officielles de l'État suédois, SOU 2013:39), pages 280 et suivantes.

[228] Ministère suédois de la justice, Saisine du Conseil législatif, Lecture secrète de données, 24.10.2019, pages 1 et 57.

[229] Enquête sur la lecture secrète des données, *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet* (Lecture secrète de données : un outil important dans la lutte contre la criminalité grave) (Rapport des commissions officielles de l'État suédois, SOU 2017:89), pages 121 à 147.

[230] Parlement européen, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices,* (PE 583.137), pages 72 à 110.

[231] PE 583.137 pages 111 à 116.

[232] PE 583.137 pages 117 à 120.

[233] PE 583.137 pages 121 à 128.

[234] Corey Varma, *Encryption vs. Fifth Amendment.*

dans laquelle l'accusé avait initialement promis l'accès à son propre disque dur, mais dans lequel des parties du disque dur étaient cryptées toutes les informations ne pouvaient pas être accédées. Le ministère public a déclaré qu'ils n'avaient pas demandé au prévenu son mot de passe, mais que le contenu devait être mis à disposition du jury et que pour cette raison cela ne ferait pas infraction à l'article 5 de la constitution et le juge a approuvé cette demande puisque le prévenu avait déjà offert de donner l'accès au disque dur[235].

Dans une autre affaire, l'article 5 est jugé applicable et les codes de chiffrement ne sont pas transmises. Dans ce cas, le FBI américain a saisi un certain nombre d'ordinateurs et de disques durs, mais n'est pas parvenu à décrypter les disques durs. L'organisation Electronic Frontier Foundation (EFF) a représenté l'homme en justice et le tribunal 11e US Circuit court a approuvé la demande de EFF et a affirmé que les codes de chiffrement de l'homme étaient protégés par l'Article 5[236].

La demande de codes de chiffrement par l'intermédiaire d'un fournisseur a notamment été traitée dans un rapport du Massachusetts institute of technology (MIT). Le rapport décrit que, dès 1997, il existait une proposition, Clipper Chip, qui exigeait que tous les systèmes forts de chiffrement se trouvent chez une entité de confiance et, après un procès juridique, pourraient être remis à des autorités anticorruption. Les coûts et les risques ont été, finalement jugés devenir trop élevés et le projet a été abandonné[237].

Le rapport analyse les propositions existantes en 2015 que les administrations anticriminalité se voient accorder la possibilité, après avoir décidé d'un procès juridique, d'avoir accès à des codes de chiffrement. Le rapport affirme que cela aurait pour conséquence que les fonctions introduites maintenant pour rendre Internet plus sûr auraient probablement une diffusion plus limitée, puisque la confiance dans la protection serait altérée. Le rapport souligne aussi que les fournisseurs doivent avoir l'obligation de pouvoir mettre à disposition des codes de chiffrement, cela entraînerait en pratique des systèmes plus complexes qui, en eux-mêmes, entraînent généralement de nouveaux risques. Enfin, les fonctions sont estimées pouvoir décrypter comme un but en soi pour les antagonistes, ce qui peut mener à des vulnérabilités supplémentaires[238].

Pour résumer, la situation juridique n'est pas claire en ce qui concerne les possibilités des administrations américaines d'accéder aux codes de chiffrement après un procès juridique elle dépend de l'estimation du cas individuel.

La situation juridique pour un fournisseur dont le siège est dans un pays mais qui stocke les données dans un autre pays semble incertaine, en particulier puisque les règles peuvent varier selon les éventuels contrats entre les pays et qu'un service peut être composé de services de différents fournisseurs de différents pays. Si un fournisseur ou un service est acheté, la situation juridique est encore plus difficile à apprécier.

---

[235] United States District Court for the District of Vermont. No. 2:06-mj-91, 2009 WL 424718 Feb. 19, 2009. *Memorandum Of Decision In re Grand Jury Subpoena to Sebastien Boucher.*

[236] EFF in the United States Court of Appeals for the Eleventh Circuit Case: *11-12268*

[237] Abelson Harold et autres, *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications 2015* (MIT-CSAIL-TR-2015-026) page 6.

[238] Abelson Harold et autres, *Keys Under Doormat,* page 24 et suivantes.

Annexe 8 Gestion de données télémétriques par les fournisseurs

Les données de télémétrie sont des données de mesures. De nombreux fournisseurs collectent des données télémétriques et les exemples ci-dessus n'en sont qu'une illustration[239].

Selon ses dires, Microsoft utilise des données télémétriques dans les buts suivants :

- pour maintenir une application à jour ;
- assurer qu'une application est sûre, fiable, et fonctionne bien ;
- améliorer une application par le fait que Microsoft peut analyser des données d'utilisateur agrégées ;
- personnaliser le ressenti de l'utilisateur ; et
- créer la compréhension pour la manière dont les utilisateurs utilisent ou non des fonctions[240].

Microsoft a indiqué qu'ils collectent notamment les données télémétriques suivantes en ce qui concerne Windows :

- Type de matériel,
- Quelles applications sont installées sur l'unité et comment elles sont utilisées.
- Comment fonctionnent les pilotes et
- Les paramètres de l'utilisateur

En 2017 la Dutch Data Protection Authority a analysé les données télémétriques dans Windows 10[241].

L'enquête a démontré que si l'utilisateur choisissait le paramètre le plus limitatif, des données sensibles étaient envoyées à Microsoft. Même lors de l'utilisation du paramètre le plus permissif, des données très sensibles étaient envoyées, telles que les sites visités et le contenu des documents. Cette étude a démontré que les données collectées à partir de l'utilisation d'applications comprenait des données à caractère personnel sensibles, par exemple à partir d'une application pour les horaires de prières musulmanes et une application pour les femmes enceintes. Les données

---

[239] Les données télémétriques ne sont pas seulement collectées à partir des utilisateurs de services cloud et, comme le montre l'exemple, les données télémétriques peuvent aussi être collectées à partir de services installés chez le client. Cependant, les services cloud publics ouvrent de plus grandes possibilités pour la collecte de données télémétriques.

[240] Microsoft, *Konfigurera diagnostikdata för Windows i din organisation*, (Configurez les données de diagnostic de Windows dans votre organisation) 2019.

[241] Autoriteit Persoonsgegevens (Dutch DPA), *Summary of Investigation Report Public Version Microsoft Windows 10 Home and Pro*, Août 2017. Notons que Windows 10 n'est pas un service nuagique public.

collectées étaient notamment utilisées pour présenter à l'utilisateur des publicités adaptées[242].

En 2018, le gouvernement néerlandais a fait effectuer une analyse d'impact en vertu du RGPD qui traitait notamment les données télémétriques dans Microsoft Office Pro Plus, y compris Office 2016 et Office 365 qui sont non connectés. L'objet était d'aider les organismes d'État à inventorier et apprécier les risques envers les personnes enregistrées lors de ces utilisations, ainsi que de prévoir des mesures adéquates pour les gérer[243].

Selon l'analyse d'impact, Microsoft collecte, par exemple, approximativement 25.000 différents types d'évènements sur Office 365. Les données télémétriques sont envoyées cryptées aux serveurs de Microsoft. Microsoft collecte aussi les données télémétriques concernant le système d'exploitation Windows 10, mais cela se limite à 1.000 évènements. D'après les réponses fournies par Microsoft lors de l'enquête, un certain nombre d'équipes de développement ont un accès total aux données.

L'enquête concernant Office Pro Plus identifie les risques suivants liés à l'accès de Microsoft à ces données.

- Il n'y a pas de transparence pour le public sur les informations dont Microsoft prend connaissance puisqu'il manque des informations accessibles au public. Cela empêche une organisation d'effectuer une estimation de risque.

- I n'existe pas de possibilités de déterminer quelles données télémétriques sont envoyées.

- Microsoft collecte et stocke des données potentiellement sensibles, aussi bien sous la forme de métadonnées[244] que de contenus[245], et pour cela il n'y a pas de support légal.

- Microsoft agit comme préposé aux données à caractère personnel au lieu de responsable commun des données à caractère personnel, ce que Microsoft devrait faire en vertu de l'Article 26 du RGPD.

- Il n'existe pas de contrôle des sous-procédés et de la gestion réelle.

- Il n'existe aucune limitation pour les objectifs dans lesquels sont collectées des données et des évènements nouveaux, par exemple lors de mises à jour.

- La transmission est effectuée vers des pays en dehors de l'Union Européenne.

---

[242] Ce rapport ne décrit pas explicitement comment les données ont été traitées et quels sont les tiers qui y ont eu accès, mais on ne peut pas exclure que des données ont été mises à la disposition de tiers pour permettre des publicités personnalisées.

[243] Ministry of Justice and Security Strategic Vendor Management Microsoft, DPIA Office 365 *ProPlus version 1905 (June 2019) Data protection impact assessment on the processing of diagnostic data.*

[244] Par exemple si l'utilisateur appuie plusieurs fois de suite sur la touche de recul puis un numéro IP.

[245] On va récupérer, par exemple, le titre du message.

- Il n'est pas dit combien de temps les données sont sauvegardées et le client n'a pas la possibilité d'effacer des données[246].

- Au cours de 2019, le gouvernement des Pays-Bas a négocié un avenant avec Microsoft qui ajuste les conditions de Microsoft Office Pro Plus pour qu'elles correspondent au règlement RGPD[247].

Cet avenant a notamment réglementé dans quelles situations spécifiques Microsoft a le droit de collecter des données télémétriques et de quelle manière ces données doivent être anonymisées. Il entraîne aussi une interdiction pour Microsoft d'utiliser les données des clients pour le profilage, par exemple, et la publicité, et une possibilité pour le client de supprimer la possibilité de collecte de données. Le contrat contient en outre des dispositions sur la possibilité du client de faire exécuter un audit chez un acteur extérieur pour assurer que Microsoft gère les données conformément au contrat. Le gouvernement des Pays-Bas a pour ambition de mettre cet avenant à la disposition de la totalité du secteur public de l'Union Européenne[248].

---

[246] Ministry of Justice and Security Strategic Vendor Management Microsoft, *DPIA Office 365 ProPlus version 1905 (June 2019) Data protection impact assessment on the processing of diagnostic data*, pages 76 et autres.

[247] Ce contrat a été négocié par une administration gouvernementale. Microsoft Strategic Vendor Management Office (SLM Rijk). Ce contrat concerne Microsoft Office Pro Plus en plus des applications mobiles et ne comprend pas Microsoft Office 365.

[248] Voir Strategic Vendor Management Microsoft for the Dutch Government and Ministerie van Veiligheid en Justitie *EU software and Cloud Supplier Customer Council*, et Ministerie van Justitie en Veiligheid Verificatie op de uitvoering van het overeengekomen verbeterplan met Microsoft (Ons kenmerk 2635551) 01.07.2019.

Sa dépendance toujours croissante de services numériques faciles à utiliser et robustes incite l'Agence suédoise de la sécurité sociale Försäkringskassan à faire le point pour son propre compte sur l'adéquacité et la possibilité d'utiliser les services cloud publics proposés par des fournisseurs privés.

Dans l'analyse présentée dans ce Livre blanc, la Försäkringskassan se base sur ses propres activités. Nous espérons, toutefois, qu'il pourra servir de soutien à d'autres administrations qui désirent élaborer une stratégie numérique pour leurs activités de portée sociétale.