GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

00678/13/FR
WP205

Avis 04/03 sur le modèle d'analyse d'impact relative à la protection des données pour les réseaux intelligents et les systèmes de relevés intelligents (modèle d'AIPD) élaboré par le groupe d'experts 2 de la task-force sur les réseaux intelligents de la Commission

Adopté le 22 avril 2013

LE GROUPE DE PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu les articles 29 et 30 de ladite directive,

vu son règlement intérieur,

A ADOPTÉ LE PRÉSENT AVIS:

1 Contexte

1.1 Introduction

Contexte

Le 9 mars 2012, la Commission européenne a publié une recommandation relative à la préparation de l'introduction des systèmes intelligents de mesure (ci-après la «recommandation de la Commission») afin de fournir des orientations aux États membres concernant le déploiement des systèmes intelligents de mesure sur les marchés de l'électricité et du gaz. Cette recommandation a pour but de donner des orientations concernant les considérations relatives à la protection et à la sécurité des données, une méthodologie pour l'évaluation économique des coûts et des avantages à long terme du déploiement des systèmes intelligents de mesure[1] et les exigences fonctionnelles minimales communes applicables aux systèmes intelligents de mesure de l'électricité.

En ce qui concerne la protection des données et la sécurité des systèmes intelligents de mesure et des réseaux intelligents, la recommandation de la Commission fournit des orientations aux États membres au sujet de la protection des données dès la conception et par défaut, ainsi que de l'application de certains principes de protection des données prévus par la directive 95/46/CE[2]. La recommandation de la Commission prévoit en outre que les États membres devraient adopter et appliquer un modèle d'analyse de l'impact sur la protection des données (ci-après le «modèle d'AIPD»), qui devrait être élaboré par la Commission et soumis pour avis au groupe de protection des personnes à l'égard du traitement des données à caractère personnel

[1] Le déploiement et l'analyse des coûts et des avantages sont exigés par i) la directive 2009/72/CE concernant des règles communes pour le marché intérieur de l'électricité (JO L 211 du 14.8.2009, p. 55) et par ii) la directive 2009/73/CE concernant des règles communes pour le marché intérieur du gaz naturel (JO L 211 du 14.8.2009, p. 94). La directive 2012/27/UE relative à l'efficacité énergétique (JO L 315 du 14.11.2012, p. 1) inclut des dispositions complémentaires sur les compteurs intelligents. Pour le marché de l'électricité, la directive 2009/72/CE prévoit que, si la mise en place de compteurs intelligents donne lieu à une évaluation favorable, au moins 80 % des clients seront équipés de systèmes intelligents de mesure d'ici à 2020. Aucun calendrier précis n'est prévu pour le marché du gaz.

[2] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281 du 23.11.1995, p. 31 à 50.

(ci-après le «groupe de travail "Article 29"») dans un délai de douze mois à compter de la publication de la recommandation de la Commission. Les États membres devraient ensuite garantir que les gestionnaires de réseau et les exploitants de systèmes intelligents de mesure prennent toutes les mesures techniques et organisationnelles appropriées pour assurer la protection des données à caractère personnel conformément au modèle d'AIPD, en tenant compte de l'avis du groupe de travail «Article 29» sur ce modèle[3].

La recommandation de la Commission prévoit par ailleurs que le modèle d'AIPD devrait «*décrire les opérations de traitement envisagées, évaluer les risques pour les droits et libertés des personnes concernées, présenter les mesures envisagées pour faire face aux risques, les garanties, les mesures de sécurité et les mécanismes visant à assurer la protection des données à caractère personnel et à démontrer la conformité avec la directive 95/46/CE, en tenant compte des droits et intérêts légitimes des personnes concernées, entre autres par les données*».

Préparation

En février 2012, la Commission a reconduit le mandat du groupe d'experts 2 de sa task-force sur les réseaux intelligents en vue d'élaborer un modèle d'AIPD pour les réseaux intelligents. Ce groupe d'experts, qui se compose essentiellement de représentants du secteur, a organisé quatre ateliers en 2012. La CNIL[4], le CEPD[5] et l'ICO[6] ont participé à ces ateliers en tant qu'observateurs au nom du groupe de travail «Article 29».

Le 26 octobre 2012, le groupe de travail «Article 29» a envoyé une lettre à la direction générale de l'énergie de la Commission européenne («DG ENER») pour attirer l'attention de la Commission sur plusieurs aspects du projet de modèle d'AIPD qui devaient, selon lui, être considérablement améliorés. Dans sa lettre, il recommandait, entre autres, que le modèle d'AIPD:

i) identifie clairement les acteurs et leurs responsabilités;
ii) se concentre sur les risques sur le plan de la protection des données et de la vie privée pour les personnes concernées;
iii) guide mieux les acteurs afin de les aider à prévoir des contrôles adéquats pour faire face à chaque risque; et
iv) donne des orientations plus spécifiques et pratiques sur la manière de s'attaquer aux risques pour la protection des données et de la vie privée dans le contexte des réseaux intelligents.

Ces commentaires ont été formulés sans préjudice de l'évaluation finale du modèle d'AIPD par le groupe de travail «Article 29».

---

[3] Le groupe d'experts 2 s'est basé sur l'expérience acquise au cours de l'élaboration et de la révision, à la suite des commentaires et avis formulés par le groupe de travail «Article 29», de la proposition du secteur pour un cadre relatif à l'analyse de l'impact sur la protection de la vie privée et des données des applications RFID.

[4] La Commission nationale de l'informatique et des libertés, l'autorité française de contrôle de la protection des données à caractère personnel.

[5] Le Contrôleur européen de la protection des données, l'autorité de contrôle de la protection des données à caractère personnel au niveau des institutions et des organes de l'Union européenne.

[6] L'Information Commissioner's Office, l'autorité nationale de contrôle de la protection des données à caractère personnel du Royaume-Uni.

Modèle d'AIPD

Le 8 janvier 2013, la Commission a soumis au groupe de travail «Article 29» la version finale du modèle d'AIPD élaborée par les membres du groupe d'experts 2. Dans la lettre d'accompagnement, la Commission indiquait que, sous réserve des commentaires du groupe de travail «Article 29» et d'une conciliation appropriée, elle pourrait envisager d'adopter le modèle d'AIPD conçu par les membres du groupe d'experts 2 sous la forme d'une recommandation de la Commission[7].
Le présent avis formule des commentaires sur le modèle d'AIPD proposé.

Structure du présent avis

La section 1.2 met en lumière l'importance de la protection de la vie privée et des données pour assurer la bonne mise en œuvre des réseaux intelligents. La section 1.3 décrit les objectifs de la procédure d'AIPD. La section 2 expose l'évaluation du modèle d'AIPD par le groupe de travail «Article 29». La section 3 tire les conclusions finales. L'annexe I complète la section 2 en donnant des commentaires plus détaillés et des suggestions.

1.2 Les réseaux intelligents et la protection des données

Le groupe de travail «Article 29» rappelle son précédent avis WP183 sur les compteurs intelligents[8], ainsi que l'avis du Contrôleur européen de la protection des données (ci-après le «CEPD») du 8 juin 2012 sur la recommandation de la Commission[9].

Ces deux avis mettent en lumière l'importance de la protection des données dans le contexte des réseaux intelligents et des compteurs intelligents et donnent des orientations et des recommandations sur la manière de protéger les droits à la protection des données à caractère personnel dans le cadre de l'introduction des compteurs et des réseaux intelligents en Europe. Cette section ne décrira donc que brièvement le contexte et les principales préoccupations relatives à la protection des données.

Les systèmes de relevés intelligents et les réseaux intelligents visent à permettre une production, une distribution et une utilisation intelligentes et rationalisées de l'énergie.

Les compteurs intelligents de gaz et d'électricité ont pour caractéristique principale

---

[7] Le 17 janvier 2013, le modèle d'AIPD a aussi été soumis au Conseil des régulateurs européens de l'énergie (CEER). Le président du CEER a répondu le 5 mars en saluant les travaux effectués par le groupe d'experts 2 et le projet de modèle d'AIPD qui en résulte. Dans sa lettre, il rappelait l'importance de la sécurité et de la protection des données ainsi que la nécessité pour les consommateurs de pouvoir contrôler leurs données; il renvoyait au précédent avis du CEER publié en 2011 et il demandait que le modèle d'AIPD soit finalisé rapidement.

[8] Avis 12/2011 du groupe de travail «Article 29» sur les compteurs intelligents, adopté le 4 avril 2011 (WP183).

[9] L'avis du CEPD est disponible sur le site internet du CEPD à l'adresse suivante: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-06-08_Smart_metering_FR.pdf.

d'être capables de fournir des données par communication à distance entre le compteur et les fournisseurs d'énergie, les gestionnaires de réseaux et d'autres tiers. Les compteurs intelligents permettent également une communication plus fréquente et rendent possible le relevé et l'enregistrement de la consommation d'énergie à intervalles très rapprochés, par exemple toutes les quinze minutes.

Les systèmes de relevés intelligents constituent un élément important pour les réseaux intelligents, qui sont des réseaux électriques bidirectionnels intelligents combinant des informations provenant des utilisateurs de ces réseaux afin, notamment, de planifier la fourniture d'électricité de façon plus efficace et rationnelle.

Le déploiement à l'échelle européenne de «systèmes intelligents de mesure» rend possible la collecte massive d'informations à caractère personnel provenant des ménages européens, avec un niveau de détails sans précédent et une couverture complète: les compteurs intelligents pourraient permettre de déduire à quelles activités les membres d'un ménage se livrent dans la sphère privée de leur logement, et donc d'établir des profils détaillés de toutes les personnes sur la base des activités auxquelles elles s'adonnent chez elles.

À partir des données détaillées sur la consommation d'énergie collectées par l'intermédiaire des compteurs intelligents, il est possible de déduire beaucoup d'informations sur l'utilisation de produits ou dispositifs spécifiques par les consommateurs, leurs habitudes quotidiennes, leur façon de vivre, leurs activités, leur mode de vie et leur comportement[10].

Par conséquent, l'utilisation de réseaux intelligents et de systèmes de relevés intelligents crée pour les personnes concernées de nouveaux risques susceptibles d'avoir des conséquences dans différents domaines (par exemple, la discrimination en matière de prix, le profilage à des fins de publicité comportementale, la fiscalité, l'accès des services répressifs, la sécurité des ménages). Auparavant, ces risques n'existaient pas dans le secteur de l'énergie, mais se trouvaient déjà typiquement dans d'autres environnements (télécommunications, commerce électronique et web 2.0).

Les compteurs intelligents font aussi partie des premières applications existantes qui préfigurent l'avenir de «l'internet des objets». Les risques posés par la collecte et la disponibilité de données détaillées sur la consommation d'énergie sont susceptibles de grandir, compte tenu de la disponibilité croissante de données provenant d'autres sources, comme les données de géolocalisation, les données disponibles grâce au traçage et au profilage sur l'internet, les systèmes de vidéosurveillance et les systèmes d'identification par radiofréquence (RFID), auxquelles les données des compteurs intelligents peuvent être combinées[11].

1.3 Les objectifs du modèle d'AIPD

[10] À titre d'illustration, avec un intervalle de relevé de deux secondes, il a été démontré qu'il est même possible de déterminer le contenu multimédia consommé dans le ménage: http://www.its.fh-muenster.de/greveler/pubs/preprint_online.pdf.

[11] Recommandation CM/Rec(2010)13 du Comité des ministres du Conseil de l'Europe du 23 novembre 2010 aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage.

Par sa recommandation, la Commission européenne entend encourager les responsables du traitement des données à procéder à une AIPD en vue d'en tirer les avantages suivants:

- une AIPD devrait décrire les opérations de traitement envisagées, évaluer les risques pour les droits et libertés des personnes concernées, présenter les mesures envisagées pour faire face aux risques, les garanties, les mesures de sécurité et les mécanismes visant à assurer la protection des données à caractère personnel et à démontrer la conformité avec la directive 95/46/CE;

- une AIPD devrait aussi aider les autorités nationales compétentes dans le domaine de la protection des données à apprécier dans quelle mesure le traitement est conforme à la directive et, en particulier, à évaluer les risques à l'égard des données à caractère personnel et les garanties correspondantes, lorsque les responsables du traitement les consultent avant toute opération de traitement, comme le prévoit la recommandation de la Commission[12]. Par conséquent, les AIPD devraient aussi aider les responsables du traitement des données à prouver le respect de la directive 95/46/CE[13].

Par ailleurs, les AIPD pourraient aider les consommateurs, les responsables du traitement des données, les autorités responsables de la protection des données, les régulateurs de l'énergie, les organisations de protection des consommateurs et d'autres parties prenantes à se forger une meilleure idée des aspects spécifiques liés à la protection des données des applications de compteurs et de réseaux intelligents. Les informations provenant de l'AIPD pourraient aussi aider les autorités responsables de la protection des données à recenser à la fois les bonnes pratiques et les éventuels domaines à haut risque devant faire l'objet d'audits.

Dans les États membres dans lesquels une notification ou un contrôle préalable est exigé pour les applications de compteurs et de réseaux intelligents, l'AIPD pourrait simplifier la procédure, tant pour les autorités responsables de la protection des données que pour les responsables du traitement. Par conséquent, les AIPD devraient aussi aider les responsables du traitement des données à prouver le respect de la directive 95/46/CE.

Enfin, il convient de souligner que le règlement proposé sur la protection des données[14] renforcerait l'importance de la procédure d'AIPD, qui est considérée comme un outil essentiel pour pouvoir engager la responsabilité des responsables du traitement des données.

---

[12] Cette recommandation s'entend sans préjudice de toute obligation légale de contrôle préalable imposée dans les États membres, en fonction des caractéristiques des opérations de traitement.

[13] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23.11.1995, p. 31).

[14] Le 25 janvier 2012, la Commission a adopté un paquet visant à réformer le cadre européen relatif à la protection des données. Ce paquet comprend i) une «communication» [COM(2012)9 final], ii) une «proposition de règlement sur la protection des données» [COM(2012)11 final] et iii) une «proposition de directive sur la protection des données» [COM(2012)10 final].

1.4 Résumé du modèle d'AIPD proposé

Le groupe d'experts 2 explique qu'il a appuyé ses travaux sur l'expérience acquise au cours de l'élaboration et de la révision, à la suite des commentaires et avis formulés par le groupe de travail «Article 29», de la proposition du secteur pour un cadre relatif à l'analyse de l'impact sur la protection de la vie privée et des données des applications RFID.

Le modèle d'AIPD proposé par le groupe d'experts 2 expose d'abord l'objectif, la portée, les avantages et les parties prenantes de la procédure. Il développe ensuite une approche permettant d'effectuer une AIPD en huit étapes et adresse, pour chaque étape, des orientations au responsable du traitement des données sur la manière de réaliser l'AIPD proprement dite.

2 Analyse du modèle d'AIPD

Le groupe de travail «Article 29» reconnaît le travail considérable accompli par les membres du groupe d'experts 2 et se félicite de ses principaux objectifs, tels que soulignés dans les sections introductives du modèle d'AIPD.

Si l'approche en huit étapes décrite dans le document proposé est d'une manière générale sensée, le groupe de travail «Article 29» a relevé plusieurs points critiques à propos de la méthodologie et du contenu du modèle d'AIPD proprement dit, qui sont détaillés dans les sections suivantes.

2.1 Manque de clarté quant à la nature et aux objectifs de l'AIPD

D'après la définition donnée au paragraphe 3, point c), de la recommandation de la Commission, une analyse de l'impact sur la protection des données est *«un processus systématique à charge du responsable du traitement des données […] ou du sous-traitant agissant pour le compte du responsable, qui vise à évaluer l'impact potentiel des risques spécifiques que les opérations de traitement des données peuvent faire peser, en raison de leur nature, de leur portée ou de leurs finalités, sur les droits et libertés des personnes concernées»*.

Le groupe de travail «Article 29» approuve cette définition, et l'objectif d'une AIPD devrait donc être d'évaluer les incidences des risques sur les personnes concernées.

Cependant, le groupe de travail «Article 29» regrette que le modèle d'AIPD soumis n'aborde pas directement les incidences réelles sur les personnes concernées, comme, par exemple, les pertes financières dues à des factures inexactes, la discrimination en matière de prix ou les actes criminels facilités par un profilage non autorisé. Même si les objectifs de protection des données et de la vie privée indiqués à l'annexe I peuvent se révéler très utiles pour faciliter le respect des dispositions, ils ne suffisent pas dans le contexte d'une approche axée sur les risques. L'évaluation des incidences potentielles sur les personnes concernées est un élément indispensable de cette approche.

Par conséquent, le groupe de travail «Article 29» considère que le modèle d'AIPD, sous sa forme actuelle, ne saurait atteindre son objectif tel que défini dans la

recommandation de la Commission. L'AIPD ne prévoit pas d'outil pratique pour analyser les incidences sur les personnes concernées.

Si les risques et leurs conséquences sur les personnes concernées ne sont pas considérés dans leur intégralité, il n'est pas possible de déterminer et d'appliquer correctement les contrôles et les garanties nécessaires.

2.2 Défauts dans la méthodologie du modèle d'AIPD

Le groupe de travail «Article 29» pense qu'en plus des principales lacunes indiquées ci-dessus, et parfois en lien avec celles-ci, le modèle d'AIPD souffre de plusieurs défauts méthodologiques qui compromettent son application.

Premièrement, le modèle d'AIPD proposé confond souvent risques et menaces[15].

Deuxièmement, aucun lien n'est établi entre les risques à limiter et la liste de contrôles possibles figurant à l'annexe II. Même si chaque scénario de risque est spécifique et devrait être évalué de manière particulière, il est souvent possible de déterminer que certaines catégories de contrôles sont efficaces pour limiter certaines catégories de risques. Un exemple typique de cette idée est donné dans la norme ISO/IEC 27002:2005 sur la sécurité de l'information, dans laquelle les contrôles sont présentés comme des bonnes pratiques pour limiter les risques dans certains domaines. Les mesures de réduction proposées, si elles ne remplacent pas l'indispensable procédure axée sur le risque, peuvent servir de référence pour une approche efficace et cohérente. Par exemple, le risque que les données sur la consommation d'énergie des consommateurs soient interceptées lorsqu'elles transitent par un canal non protégé peut généralement être réduit par des techniques de chiffrement. L'évaluation du risque spécifique pourrait ensuite amener à choisir certains algorithmes de chiffrement et certaines longueurs de clé ou des mesures d'atténuation complémentaires ou différentes, voire à accepter ou à transférer le risque (et donc à ne pas prendre de mesures d'atténuation).

En outre, le modèle d'AIPD proposé ne donne pas non plus d'orientations suffisamment détaillées et spécifiques sur la notion de vulnérabilité ni sur la manière de calculer des risques et de les classer par ordre de priorité, de choisir les contrôles appropriés et d'évaluer les risques résiduels qui subsistent après que les contrôles ont été mis en place. Même s'il est fait référence à un document externe, le groupe de travail «Article 29» aurait souhaité que le modèle d'AIPD même contienne plus d'orientations et d'explications, afin de donner au lecteur un document unique. Il n'est

---

[15] Voir la définition ISO/IEC 27005:2008 du risque dans le domaine de la sécurité de l'information: «potentiel qu'une menace donnée exploite les vulnérabilités d'un actif ou d'un groupe d'actifs et cause ainsi un préjudice à l'organisation». Il n'existe pas de définition directe des menaces, mais on peut en tirer une définition opérationnelle de la norme ISO/IEC 27001:2005. En conséquence, les menaces sont la capacité d'exploiter les vulnérabilités des actifs à protéger, ce qui aura des conséquences sur ces actifs en termes de perte de propriétés de sécurité. Des exemples de menaces typiques liées à la sécurité sont énumérés dans l'annexe C de la norme ISO/IEC 27005:2008.
(Voir aussi la méthodologie de la CNIL: http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_Securite_avance_Methode.pdf et le rapport sur l'état de la menace de l'ENISA: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape/at_download/fullReport)

pas non plus indiqué clairement comment il convient de compléter les formulaires proposés.

Enfin, le modèle d'AIPD ne donne pas suffisamment de conseils concernant la manière de déterminer les rôles et les responsabilités en matière de protection des données des différentes parties prenantes. Il est seulement fait référence à un autre document du groupe d'experts 2. Les futures applications de réseaux intelligents seront diverses et proposées par de multiples parties prenantes. Il semble dès lors essentiel de fournir au secteur des orientations permettant l'identification des responsables du traitement des données et des sous-traitants. Par exemple, le modèle d'AIPD pourrait inclure, dans la troisième étape, une quatrième section visant à déterminer les différentes responsabilités de chacune des entités participant au traitement des données.

Des informations plus détaillées sur ces lacunes et d'autres lacunes méthodologiques sont disponibles à l'annexe I.

2.3 Le contenu du modèle d'AIPD n'est pas suffisamment spécifique au secteur: les risques spécifiques du secteur et les contrôles pertinents pour y faire face devraient être répertoriés et mis en correspondance

Le contenu du modèle d'AIPD n'est pas suffisamment spécifique au secteur. Les risques et les contrôles énumérés dans le modèle sont d'ordre général et ne contiennent que peu d'orientations ou de bonnes pratiques spécifiques au secteur qui pourraient se révéler véritablement utiles. Bref, les risques et les contrôles ne reflètent pas l'expérience du secteur en ce qui concerne les principales préoccupations et les bonnes pratiques.

Le groupe de travail «Article 29» a cru comprendre que le groupe d'experts 2 prépare un recueil des «meilleures techniques disponibles» (ci-après les «MTD») qui permettrait à toute organisation qui effectue une AIPD de choisir les mesures adéquates le cas échéant, et donc de remédier à certaines des critiques formulées dans la section précédente. Le groupe de travail «Article 29» insiste sur l'importance de ce document, complémentaire au modèle d'AIPD.

Cependant, le document sur les MTD ne saurait se substituer à la détermination, dans le modèle d'AIPD lui-même, des risques les plus souvent rencontrés dans le secteur et des éventuels contrôles correspondant à ces risques. C'est d'autant plus vrai que, contrairement au modèle d'AIPD, le document sur les MTD ne sera pas soumis au groupe de travail «Article 29» pour qu'il puisse l'évaluer et donner des orientations, et ne devra pas être adopté par la Commission. Compte tenu des lacunes relevées dans le modèle d'AIPD, la Commission devrait envisager d'y intégrer les MTD et de soumettre le document intégré au groupe de travail «Article 29» pour avis.

Par ailleurs, la notion de «modèle d'AIPD» est différente de celle de «cadre pour l'AIPD». Un cadre doit fixer les objectifs, donner les grandes lignes d'une méthodologie et définir la portée de l'évaluation, et donc les limites de la procédure ou du système analysé. Un modèle doit aller plus loin et constituer un instrument opérationnel permettant de gérer les risques du système ou de la procédure en question et ses cas d'utilisation; il doit aussi suggérer des contrôles possibles et des

meilleures techniques disponibles pour limiter ces risques, et enfin donner des orientations spécifiques. C'est en particulier nécessaire lorsqu'aucune compétence spécifique n'est disponible (par exemple, dans les PME ou, comme dans le cas des réseaux intelligents, dans un secteur qui a auparavant été confronté à relativement peu de problèmes liés à la protection de la vie privée et des données).

Le modèle d'AIPD devrait avoir pour objet d'élaborer des orientations plus spécifiques au secteur et plus faciles à utiliser. En particulier, il convient de mieux définir les incidences potentielles sur les personnes concernées dans le contexte des réseaux intelligents et de donner des orientations plus précises concernant le type de contrôles pouvant être effectués.

La Commission aurait pu fournir au groupe d'experts 2 une méthodologie générale d'évaluation des risques pour la protection de la vie privée et des données[16]. Le groupe d'experts 2 aurait alors pu appliquer cette méthode et, sur la base de celle-ci, il aurait pu rendre le modèle d'AIPD plus spécifique au secteur. Cette approche lui aurait permis de se concentrer sur les questions pertinentes, comme les risques et les contrôles spécifiques aux réseaux intelligents, tout en s'appuyant sur le cadre de référence pour les aspects méthodologiques fondamentaux. Le groupe de travail «Article 29» suggère que le groupe d'experts 2 et la Commission adoptent cette approche pour le développement futur de ce modèle d'AIPD ainsi que pour tout autre modèle d'AIPD sectoriel.

3 Conclusion et recommandations

Le groupe de travail «Article 29» reconnaît les progrès accomplis par rapport aux versions précédentes et les éléments utiles que le modèle d'AIPD contient déjà. Néanmoins, il estime que le modèle d'AIPD sous sa forme actuelle n'est pas suffisamment abouti et bien développé.

Par conséquent, le groupe de travail «Article 29» recommande à la Commission de prendre les mesures nécessaires pour faire en sorte que les travaux sur le modèle d'AIPD se poursuivent et que sa version finale donne des orientations pratiques suffisamment spécifiques, utiles et claires aux responsables de la protection des données.

Afin de faciliter la poursuite des travaux, le groupe de travail «Article 29» formule des recommandations plus spécifiques à l'annexe I du présent avis. Toutefois, compte tenu des défauts méthodologiques du document et de son manque de spécificité par rapport au contexte des réseaux intelligents, il n'est pas en mesure d'apporter une contribution plus détaillée et concluante à ce stade.

À la lumière des lacunes relevées dans le modèle d'AIPD, le groupe de travail «Article 29» recommande par ailleurs que la Commission envisage d'intégrer les MTD dans le modèle d'AIPD et de lui soumettre le document intégré pour avis[17].

---

[16] Voir, par exemple, la méthodologie de la CNIL susmentionnée.

[17] Cela n'empêche pas que le document sur les MTD puisse être actualisé périodiquement à l'avenir afin de refléter les évolutions technologiques et l'état de la technique.

De plus, et de manière plus générale, le groupe de travail «Article 29» recommande à la Commission d'envisager de dresser le bilan des travaux passés et en cours dans le domaine des AIPD[18] et d'envisager l'opportunité de définir une méthode générale pour les AIPD, qui pourrait se révéler bénéfique pour les efforts spécifiques consentis dans un domaine donné.

Enfin, pour ce qui est de la nécessité d'une analyse d'impact obligatoire, le groupe de travail «Article 29» rappelle l'expérience acquise avec le projet PIAF RFID et souligne que les statistiques disponibles dans les États membres montrent que le recours aux analyses d'impact pour le RFID a été extrêmement faible. Si ces chiffres peuvent s'expliquer par plusieurs raisons, l'un des principaux facteurs semble assurément être l'absence actuelle d'obligation de mener une telle analyse d'impact.

Fait à Bruxelles, le 22 avril 2013

Pour le groupe de travail
Le président
Jacob KOHNSTAMM

[18] Voir, par exemple, le projet PIAF: http://www.piafproject.eu/Index.html, ainsi que les méthodologies existantes précitées.

Annexe I: Commentaires spécifiques sur le modèle d'AIPD

La présente annexe complète la section 2 de l'avis. La structure des commentaires suit celle du modèle d'AIPD.

→ Portée de l'AIPD

- Le modèle ne donne pas de définition ni de description précise des types d'opérations de traitement des données qui sont soumises à une AIPD. En outre, la portée de l'AIPD n'est pas définie précisément dans la section 1.2 du modèle d'AIPD. Dans sa recommandation, la Commission définit clairement l'AIPD comme un «processus systématique […] qui vise à évaluer l'impact potentiel des risques spécifiques que les opérations de traitement des données peuvent faire peser, en raison de leur nature, de leur portée ou de leurs finalités, sur les droits et libertés des personnes concernées». Cette définition inclut les droits fondamentaux visés aux articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne (ci-après la «charte»), à savoir, respectivement, le droit du respect de la vie privée et le droit à la protection des données à caractère personnel. Il faudrait tenir compte du fait que le modèle est lié à la protection des données à caractère personnel telle que définie dans la directive 95/46/CE[19].
- Comme souligné dans les commentaires généraux, le modèle d'AIPD devrait se concentrer sur les incidences sur la personne concernée. S'il faut impérativement atteindre les objectifs en matière de protection de la vie privée et des données définis à l'annexe I et respecter la législation sur la protection des données, le respect de cette dernière n'est pas un objectif en soi. L'objectif ultime de la procédure d'AIPD est donc de déterminer les contrôles qui réduisent au minimum les conséquences négatives sur les droits et les libertés des personnes concernées.
- Les exemples suivants permettront peut-être d'illustrer la différence entre une approche réduite à un simple contrôle de conformité et une approche fondée sur l'évaluation des risques réels et de leurs conséquences réelles sur les personnes concernées:
    - les risques liés à la criminalité: si les mesures techniques et organisationnelles adoptées pour assurer la sécurité des données sur la consommation d'énergie sont insuffisantes, il est possible d'accéder illégalement aux données sur la consommation d'énergie d'un ménage. Cela peut augmenter le risque que le consommateur concerné soit victime de criminalité. Par exemple, le fait de connaître les habitudes comportementales pouvant être déduites des données sur la consommation d'énergie, et en particulier de savoir qu'une maison est vide à un moment donné, peut entraîner un risque accru de cambriolages et de vols;

[19] Toute référence à la notion de «confidentialité des données» ou toute tentative de donner une définition ad hoc de la «protection de la vie privée» dans la section 1.2 ou dans le glossaire ne sont pas nécessaires et pourraient induire en erreur. Il faudrait utiliser chaque fois que possible la terminologie de la directive 95/46/CE. Le modèle peut citer les articles 7 et 8 de la charte et y renvoyer pour de plus amples informations.

- les personnes peuvent recevoir une facture erronée si les données sur la consommation d'énergie sont falsifiées[20];
- le profilage, l'exclusion, la discrimination, la publicité non désirée: la disponibilité accrue de données sur les utilisateurs de réseaux intelligents peut entraîner une intensification du profilage, laquelle pourrait, à son tour, conduire à une discrimination en matière de prix et à l'exclusion (par exemple, la mise sur liste noire ou l'application de tarifs plus élevés), à des publicités comportementales ciblées non désirées, ainsi qu'à un déséquilibre global dans la situation économique du consommateur vis-à-vis des prestataires de service et des responsables du traitement des données qui peut ensuite être utilisé de manière abusive;
- les risques d'utilisation incompatible et illégale par les services répressifs ou d'autres tiers, et le risque de surveillance accrue du gouvernement (qui pourrait être limité, par exemple, en réduisant au minimum les données à caractère personnel traitées).

- Les exemples susmentionnés ainsi que d'autres exemples de risques et de conséquences possibles sur les personnes concernées devraient être pris en considération et inclus dans l'analyse d'impact.

→ Parties prenantes

- Le modèle d'AIPD ne tient pas compte des rôles et fonctions des différents acteurs de l'écosystème de réseaux intelligents et, par conséquent, n'opère pas de distinction entre leurs responsabilités. Or, les réseaux intelligents ne peuvent atteindre leurs objectifs que grâce à une coopération organisée et à un échange de données entre les différentes organisations participantes. Pour produire une AIPD significative, les participants devront collaborer. Le modèle d'AIPD proposé ne donne pas suffisamment d'orientations sur la manière de mener une AIPD lorsque plusieurs intervenants sont concernés et réalisent des activités connexes de traitement des données.
- Dans la section 1.3.3., «gestionnaire de réseaux intelligents» est un terme très général et ne tient pas compte du fait que divers acteurs peuvent remplir des fonctions différentes dans le secteur des réseaux intelligents, ce qui influence fortement les limites et la portée de l'AIPD menée[21]. Ces fonctions devraient être décrites en mettant un accent tout particulier sur leurs rôles dans l'échange des informations personnelles nécessaire aux procédures opérationnelles liées aux réseaux intelligents. Une définition concise et actualisée des rôles des parties participant à la procédure d'AIPD devrait être incluse dans le modèle d'AIPD (voir, par exemple, le rapport du groupe d'experts 2 du 16 février 2011[22]).
- Il faudrait rappeler la nécessité de respecter la législation applicable.

---

[20] Les propriétaires de panneaux solaires ou de micro-installations de cogénération peuvent aussi être confrontés à des risques similaires en ce qui concerne leur facturation.

[21] Voir, par exemple, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGConceptualModel#Smart_Grid_Conceptual_Model_Doma.

[22] Voir http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf.

- Le modèle d'AIPD devrait aussi mentionner parmi les parties prenantes i) les destinataires des données et ii) les délégués à la protection des données (le cas échéant) de l'organisation.

→ 1re étape

- Les critères d'évaluation préalable doivent être réexaminés. En conséquence, le questionnaire de la section 3.1. doit aussi être révisé. C'est également nécessaire afin d'assurer la cohérence avec la section 2.1.
- L'ordre des critères doit être modifié afin de suivre l'ordre logique dans lequel ils devraient être examinés:
    1. des données à caractère personnel sont-elles traitées?
    2. l'organisation est-elle responsable du traitement des données?
    3. le traitement des données a-t-il des conséquences sur les droits et les libertés?
    4. quand sera-ce le bon moment et quelle sera la motivation?
- Parmi les types de données énumérées dans le modèle d'AIPD en tant que données pouvant être considérées comme des données à caractère personnel, certaines ne sont manifestement pas des données à caractère personnel (estimation de la demande du bâtiment, du campus et de l'organisation). En revanche, certaines données pouvant être des données à caractère personnel ne figurent pas dans la liste ou figurent dans la mauvaise liste (la température intérieure d'une maison peut être une donnée à caractère personnel étant donné qu'elle peut indiquer si la maison est occupée ou non; les endroits successifs où une voiture électrique a été rechargée sont des données à caractère personnel dans la mesure où ils montrent où l'utilisateur se trouve, etc.). Il faudrait fournir davantage d'orientations pour aider l'organisation à déterminer les données à caractère personnel qui seront traitées.
- En outre, toujours concernant le premier critère, une AIPD devrait aussi être effectuée pour les systèmes existants qui n'ont pas été créés en tenant compte de la «protection des données dès la conception» et pour lesquels aucune AIPD n'a été menée auparavant. Cet aspect devrait être souligné dans le texte, par exemple en ajoutant un point supplémentaire à la liste des éléments déclencheurs déjà dressée sous la rubrique «Moment adéquat», ou en ajoutant un nouveau paragraphe après cette liste.

→ 2e étape

- Il importe de veiller à ce que, lorsque les ressources de l'organisation le permettent, l'équipe qui réalise l'AIPD soit indépendante par rapport à l'équipe qui travaille sur l'application de réseaux intelligents elle-même, ce qui contribuera à une AIPD équitable et objective. Cette exigence n'est pas incluse dans le document.

→ 3e étape

- La description du système ne comprend pas de description claire des actifs sur lesquels le traitement des données à caractère personnel repose (par exemple,

une base de données faisant office de répertoire des données collectées dans un domaine particulier). Ce serait important, car certaines menaces cibleront aussi ces actifs. Les différents types de données à caractère personnel traitées doivent aussi être recensés de manière exhaustive, de même que les finalités du traitement et la manière dont elles sont traitées. Les délais de conservation proposés doivent aussi être indiqués.

→ 4e étape

- Cette étape repose essentiellement sur la liste de menaces figurant dans les questionnaires du modèle d'AIPD. Il semble y avoir une confusion entre menaces et risques (voir la section 2.2 du présent avis). De plus, certains des éléments de la liste concernent «l'absence de mesures» (par exemple, un mécanisme de journalisation insuffisant, un manque d'unification du mécanisme de demandes d'accès des personnes concernées) plutôt que des menaces.

→ 5e étape

- Les conséquences des menaces pour la protection des données sont mesurées en termes d'incidences sur les objectifs de protection de la vie privée et des données définis à l'annexe I, et non en termes d'incidences sur les personnes concernées. De plus, le modèle d'AIPD à proprement parler ne contient pas d'orientations suffisantes sur le type de conséquences et sur la méthodologie.
- La probabilité de matérialisation du risque est décrite comme étant la combinaison du niveau de vulnérabilité et de la facilité d'exploitation de la vulnérabilité. Or, comme les actifs sur lesquels repose le traitement des données à caractère personnel n'ont pas été définis à la troisième étape, rien n'indique ce qu'est la vulnérabilité.

→ 6e étape

- Il est également essentiel que le modèle d'AIPD lie clairement chaque risque à un ou plusieurs contrôle(s) adéquat(s) en vue de limiter le risque (tout en établissement clairement que, le cas échéant et si c'est dûment justifié, certains risques peuvent aussi être transférés ou acceptés). Ce lien devrait devenir un élément central du document. La structure actuelle du modèle ne défend pas une telle approche intégrée, comme le groupe de travail «Article 29» l'a déjà signalé dans sa lettre d'octobre 2012.
- Pour ce qui est des risques résiduels (section 6), ainsi que le groupe de travail «Article 29» l'a déjà mentionné dans ses commentaires d'octobre 2012, le droit à la protection des données à caractère personnel est un droit fondamental, et son respect est une prescription légale claire et prioritaire. Ce fait devrait être davantage mis en lumière lorsqu'il est question de la possibilité d'accepter un certain degré de risques résiduels: on pourrait expliquer que, quel que soit le résultat de toute éventuelle évaluation des risques, les objectifs en matière de protection des données et de la vie privée doivent être atteints. Par exemple, les personnes concernées doivent dans tous les cas être informées de manière appropriée et le traitement doit aussi s'appuyer sur un motif légal (par exemple, une obligation légale ou le

consentement de la personne concernée). Il est essentiel d'établir très clairement que la législation sur la protection des données doit toujours être respectée. L'évaluation des risques peut contribuer à déterminer la meilleure manière de respecter cette législation. Par exemple, le type de chiffrement à utiliser pour assurer le niveau approprié de sécurité des données, le délai de conservation qui peut être considéré comme approprié ou la meilleure manière de réduire au minimum la quantité de données collectées et traitées ultérieurement. Néanmoins, l'évaluation des risques ne devrait pas servir d'excuse pour justifier le non-respect des prescriptions légales lorsque les risques sont perçus comme étant comparativement inférieurs. Enfin, de manière plus générale, aucun conseil n'est donné concernant la façon de déterminer le niveau de risque résiduel acceptable.

Annexe II: Liste des contrôles possibles

Les contrôles énumérés à l'annexe II ne sont pas suffisamment spécifiques pour donner des orientations utiles aux responsables du traitement. Par ailleurs, la plupart d'entre eux n'abordent pas les spécificités du contexte des réseaux intelligents et ne reflètent pas l'expérience du secteur en ce qui concerne les principales préoccupations et les bonnes pratiques.

Pour illustrer le niveau de détail et les exemples pratiques que nous attendons du modèle, nous tenons à souligner certaines des questions les plus importantes que le modèle devrait, selon nous, aborder en profondeur.

Base juridique et choix

Le groupe de travail «Article 29» voudrait que le modèle contienne davantage d'orientations sur la base juridique à choisir pour le traitement des données et sur les choix qui devraient être offerts aux personnes concernées. En particulier, il devrait y avoir des orientations claires sur ce qui peut être fait sans le consentement de l'utilisateur et sur les opérations pour lesquelles le consentement de l'utilisateur est nécessaire. Il convient d'attacher une attention particulière à la mise en œuvre de la désactivation à distance et des relevés détaillés[23].

Dans la plupart des cas, un consentement donné librement, informé et explicite serait requis pour tout traitement allant au-delà du traitement nécessaire à i) la fourniture d'énergie, ii) la facturation de cette fourniture, iii) la détection d'une fraude consistant en la consommation non payée de l'énergie fournie[24] et iv) la préparation des données agrégées nécessaires au maintien de l'efficacité énergétique du réseau (prévision et transaction)[25]. Parmi les exemples de cas dans lesquels le consentement serait requis, on peut citer le traçage et le profilage aux fins de la publicité ciblée.

Pour que le consentement soit valable, il faut que les consommateurs comprennent ce qu'il advient des données les concernant. Il est important, dans le cas du profilage, qu'ils aient le droit de connaître leur profil personnel et la logique de tout algorithme utilisé pour l'exploration des données. Les informations sur la fonctionnalité d'activation/de désactivation à distance sont tout aussi importantes: les consommateurs doivent savoir quels événements peuvent entraîner une désactivation.

Limitation des données et technologies renforçant la protection de la vie privée

Le modèle d'AIPD devrait également encourager les entreprises concernées à faire en sorte que seules les données à caractère personnel absolument nécessaires soient

[23] Voir, par exemple, le point 48 de l'avis du CEPD du 8 juin 2012, précité dans la note de bas de page 3 ci-dessus.

[24] De toute évidence, le traitement des données aux fins de la détection de la fraude doit néanmoins respecter toutes les autres garanties pertinentes pour la protection des données, y compris l'exigence de proportionnalité et le principe de limitation des données.

[25] Le cas échéant, les finalités pour lesquelles aucun consentement n'est requis correspondent généralement aux tâches réglementaires des responsables du traitement des données.

collectées et traitées. À cette fin, plusieurs méthodes peuvent être envisagées et nous recommandons qu'au moins les technologies renforçant la protection de la vie privée les plus courantes et d'autres «meilleures techniques disponibles» pour la limitation des données soient chacune décrites brièvement et de manière technologiquement neutre dans le modèle d'AIPD. Cela pourra être ensuite davantage détaillé dans le document complémentaire sur les MTD que le groupe d'experts 2 élaborera afin de contribuer à promouvoir le déploiement des compteurs intelligents et des technologies de réseaux intelligents dans le respect de la protection des données.

En particulier, il existe des technologies renforçant la protection de la vie privée novatrices, actuellement à différents stades de recherche et de développement, et qui pourraient permettre d'atteindre les objectifs élémentaires du système de relevés intelligents [facturation, maintien de l'efficacité énergétique du réseau (prévision et transaction) et garantie de sécurité (y compris la prévention de la fraude)], de sorte que l'on pourrait complètement éviter, du moins pour ces objectifs élémentaires, que les relevés de compteurs détaillés doivent sortir du compteur intelligent ou du ménage où le compteur intelligent est installé. En outre, les points suivants pourraient être abordés:

- la fréquence des relevés des compteurs: l'intrusion dans la vie privée augmente fortement à mesure que les relevés de compteurs deviennent plus fréquents. Le groupe de travail «Article 29» souhaite que le modèle d'AIPD contienne davantage d'orientations sur cette question, y compris quelques références[26] et exemples;
- l'échantillonnage: le recours à l'échantillonnage (c'est-à-dire la collecte de données uniquement auprès d'un pourcentage représentatif de tous les ménages) pourrait contribuer à éliminer la collecte et le traitement de données provenant de l'ensemble des ménages pour certaines finalités (comme la prévision). Ici aussi, des exemples devraient être inclus dans le modèle d'AIPD;
- l'agrégation combinée à l'effacement: pour certaines finalités, notamment la prévision, il devrait être suffisant de ne conserver les relevés de compteurs détaillés que jusqu'au calcul de l'agrégation. Dans ces cas-là, les données pourraient être effacées définitivement dès que ce calcul a été effectué. Une fois de plus, il conviendrait de donner des exemples;
- la collecte de données agrégées d'emblée (au lieu de la collecte de données individuelles, suivie de l'agrégation de ces données): pour certaines finalités (y compris certaines finalités liées à la prévision, au maintien de l'efficacité énergétique du réseau et à la détection de la fraude), il devrait être suffisant pour le gestionnaire de réseau de distribution d'électricité ou de gaz de collecter des données à partir de compteurs qui ne mesurent pas la consommation de ménages individuels, mais qui sont placés à des endroits du réseau où ils ne peuvent mesurer que la consommation agrégée d'un certain nombre de ménages (par exemple, d'un grand immeuble d'habitation, d'une rue ou d'un quartier). Dans ces cas, et pour ces finalités, la collecte de données

[26] Voir le point EG2.P.1 du document «Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection» (http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2_deliverable.pdf).

détaillées auprès de ménages individuels peut être totalement évitée. À nouveau, il serait utile d'inclure des exemples concrets et parlants dans le modèle d'AIPD pour inciter au respect de la législation sur la protection des données et des bonnes pratiques;

- afin de contribuer à réduire au minimum non seulement la quantité de données collectées, mais aussi la période durant laquelle les données seront conservées, le modèle d'AIPD devrait aussi donner davantage d'orientations sur les délais de conservation. Selon nous, en principe, le stockage de données détaillées sur la consommation des différents ménages collectées à des fins de facturation ne devrait être autorisé que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement. (Cela s'entend bien sûr sans préjudice du droit du consommateur de bénéficier d'une durée de conservation plus longue s'il y consent, par exemple, pour obtenir des conseils ciblés en matière d'énergie ou pour d'autres éventuelles fins légitimes).

Glossaire

Le groupe de travail «Article 29» recommande que le glossaire soit révisé attentivement pour veiller à ce que la terminologie soit conforme à celle actuellement employée dans la directive 95/46/CE et compatible avec le nouveau cadre relatif à la protection des données proposé.