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

2064/13/FR
WP209

Avis 07/2013 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

Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Son secrétariat est assuré par la direction C (Droits fondamentaux et citoyenneté de l'Union) de la direction générale «Justice» de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO-59 02/013.

Site internet: http://ec.europa.eu/justice/data-protection/index_fr.htm

LE GROUPE DE TRAVAIL SUR LA 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 la recommandation 2012/148/UE 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 (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

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.

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 plusieurs ateliers, auxquels des représentants du groupe de travail «Article 29» ont participé en tant qu'observateurs.

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.

Première version du modèle d'AIPD

Le 8 janvier 2013, la Commission a soumis au groupe de travail «Article 29» la première version 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[4].

Le groupe de travail «Article 29» a rendu son avis 04/2013 le 22 avril 2013. Dans cet avis, il reconnaissait, d'une part, le travail considérable accompli par les membres du groupe d'experts 2 et se félicitait de ses principaux objectifs. Par ailleurs, plusieurs points critiques ont été relevés, lesquels peuvent se résumer comme suit:

i. manque de clarté quant à la nature et aux objectifs de l'AIPD;

---

[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] 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.

ii. lacunes dans la méthodologie du modèle d'AIPD;

iii. 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 groupe de travail «Article 29» a conclu que le modèle d'AIPD n'était pas suffisamment abouti et bien développé et a recommandé à la Commission de prendre les mesures nécessaires pour faire en sorte que les travaux sur le modèle d'AIPD se poursuivent et finissent par garantir des orientations pratiques suffisamment spécifiques, utiles et claires aux responsables de la protection des données.

Le groupe de travail «Article 29» a par ailleurs invité la Commission à envisager d'intégrer les meilleures techniques disponibles (MTD, telles que définies au point 3.f de la recommandation) dans le modèle d'AIPD et à soumettre au groupe de travail «Article 29» le document intégré pour avis. Il a également recommandé à la Commission d'envisager de dresser le bilan des travaux passés et en cours dans le domaine des AIPD 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.

Deuxième version du modèle d'AIPD

La Commission a répondu à l'avis du groupe de travail «Article 29» le 27 mai 2013. La lettre faisait état d'une demande adressée par la Commission au groupe d'experts 2 concernant un modèle révisé et remerciait le groupe de travail «Article 29» pour sa disponibilité à apporter son soutien, tout en s'en tenant à son rôle spécifique, aux travaux du groupe d'experts 2. En outre, la Commission avait préféré ne pas intégrer les MTD au modèle en raison, selon elle, de leur portée limitée aux exigences fonctionnelles minimales communes applicables aux systèmes intelligents de mesure et de leur nature évolutive[5]. Quant à la proposition de définir une méthode générale pour les AIPD qui pourrait se révéler bénéfique pour les efforts spécifiques consentis dans un domaine donné, la lettre invoquait un autre département compétent de la Commission, dont aucune réponse n'avait encore été reçue.

Le groupe d'experts 2 a mis en place une équipe éditoriale pour le deuxième projet de modèle, laquelle s'est réunie les 4 juin et 3 juillet 2013. Certains représentants du groupe de travail «Article 29» ont participé à la première réunion en tant qu'observateurs et ont répondu aux questions des représentants du groupe d'experts 2 sur les différents points soulevés dans le modèle.

Le 20 août 2013, la Commission a soumis au groupe de travail «Article 29» la version finale du modèle d'AIPD révisé, préparée par les membres du groupe d'experts 2.

---

[5] «*Je suis d'avis que cela ne serait pas aussi bénéfique que vous le souhaitez, et ce pour les raisons suivantes: i) conformément à la recommandation 2012/148/UE de la Commission, les MTD concernent uniquement les exigences fonctionnelles minimales communes applicables aux systèmes intelligents de mesure, tandis que la portée de l'application du modèle d'AIPD va bien au-delà et couvre tout l'éventail des réseaux intelligents; et ii) si les MTD devaient être intégrées au modèle d'AIPD, leur nature évolutive et illustrative condamnerait ipso facto le modèle d'AIPD à être éphémère et probablement soumis à des révisions trop fréquentes*.»
(lettre ener.b.3 VL/cv(2013)1506536 adressée à M. Kohnstamm, 27 mai 2013)

Structure du présent avis

La section 1 retrace les évènements à l'origine de la révision du modèle d'AIPD et renvoie à différentes sections de l'avis 04/2013 portant sur la question de la protection des données dans les réseaux intelligents et les objectifs de la procédure d'AIPD dans ce contexte.

La section 2 expose l'évaluation du modèle d'AIPD révisé par le groupe de travail «Article 29».

La section 3 tire les conclusions finales.

1.2 La protection des données dans les réseaux intelligents et les objectifs de la procédure d'AIPD dans ce contexte

Les sections 1.2 et 1.3 de l'avis 04/2013 abordaient déjà la question de la protection des données dans les réseaux intelligents et les objectifs de la procédure d'AIPD dans ce contexte. Le groupe de travail «Article 29» n'a pas de nouvel élément à y ajouter.

2 Analyse du modèle d'AIPD

Le groupe de travail «Article 29» reconnaît le travail accompli par les membres du groupe d'experts 2 dans leur tentative de répondre aux commentaires formulés par le groupe de travail «Article 29» et leur volonté de prendre en considération, en tant que précieux soutien, les conseils du groupe de travail «Article 29».

Cette analyse fait essentiellement suite aux commentaires formulés dans l'avis 04/2013. Elle comprend également des améliorations et optimisations qu'il faudrait considérer pour finaliser le modèle. Les sections ci-dessous tiennent compte des deux aspects.

Pour avoir une compréhension globale et claire, cette analyse doit être lue à la lumière du contenu et de la terminologie de l'avis 04/2013.

2.1 Le modèle d'AIPD et la recommandation 2012/148 de la Commission européenne

Le groupe de travail «Article 29» a saisi l'occasion de réexaminer attentivement cette deuxième version du modèle d'AIPD pour les réseaux intelligents à la lumière de la recommandation de la Commission, qui en définit les objectifs, la portée et l'applicabilité.

2.1.1 Sur la nature discrétionnaire de la réalisation d'une AIPD

Sans toutefois imposer d'obligation juridiquement contraignante, l'existence d'une recommandation de la Commission indique que certaines mesures sont fortement recommandées. La recommandation 2012/148/UE dispose que les opérations de traitement de données à caractère personnel dans les compteurs et réseaux intelligents exigent 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». Le groupe de travail «Article 29» tient à réaffirmer que la nécessité de ce processus, déjà établie dans son avis 12/2011 sur les systèmes de relevés intelligents dans le contexte d'une approche de «prise en compte du respect de la vie privée dès la conception», est largement justifiée par la complexité de l'infrastructure technique et de gestion des réseaux intelligents, par l'ampleur potentielle de leur application et de leur évolution, et par les risques spécifiques qui pèsent sur les libertés et droits fondamentaux des personnes concernées, y compris, notamment, la vie (en cas, par exemple, d'extinction de la fourniture d'énergie si certaines machines électriques assurent des fonctions vitales).

Par ailleurs, le groupe de travail «Article 29» se félicite de ce que la Commission ait proposé un règlement général sur la protection des données qui rendrait les analyses d'impact relatives à la protection des données obligatoires sous certaines conditions. Il convient d'indiquer clairement aux parties prenantes du modèle d'AIPD pour les réseaux intelligents, à savoir les responsables de la protection des données et les sous-traitants, que l'utilisation du modèle doit être considérée comme un moyen de se conformer à une obligation légale à l'avenir. Étant donné les investissements colossaux et le lointain horizon de planification pour les réseaux d'utilité générale, il faut bien comprendre qu'il est dans l'intérêt même des parties prenantes de déjà se forger une expérience avec l'approche des AIPD et de l'appliquer dès le départ dans la conception de leurs systèmes, afin d'éviter les problèmes de conformité au moment de l'entrée en vigueur de la législation actuellement à l'examen. Si les termes utilisés dans le modèle actuel, en particulier à la section 2.1, peuvent être perçus comme laissant une marge considérable à une approche largement discrétionnaire de la part de l'entreprise, la Commission devrait veiller à ce que des précisions soient fournies pour que cette marge soit interprétée au sens strict, afin de garantir l'exécution la plus complète possible d'une véritable AIPD, par exemple en expliquant cette approche dans une recommandation de la Commission qui pourrait accompagner et étayer ce modèle. Le groupe de travail «Article 29» considère le rôle de l'évaluation préalable comme fonctionnel, dans le but de tenir compte de toutes les situations possibles que les futurs responsables de la protection des données et sous-traitants pourraient rencontrer, sur la base des informations traitées, de l'ampleur du (sous-)système analysé, du statut du projet, etc., et non comme une étape dans la méthode servant à affaiblir les objectifs de la recommandation de la Commission.

2.1.2 L'AIPD et les autorités responsables de la protection des données

Le point 8 de la recommandation de la Commission dispose que les États membres devraient garantir que le responsable du traitement des données à caractère personnel consulte l'autorité de contrôle de la protection des données sur l'analyse de l'impact relative à la protection des données, avant toute opération de traitement. Le groupe de travail «Article 29» fait observer que le modèle ne reflète pas pleinement cette approche en de nombreux endroits. Certaines formulations: «en cas de doute» (section 2.1.4), ou simplement consulter le «délégué à la protection des données» (et non l'«autorité de contrôle de la protection des données») «le cas échéant» (section 2.6.2), ou soumettre à l'autorité de contrôle de la protection des données «si elle en fait la demande» une fois le rapport final adopté (section 2.7). Bien qu'il soit préférable que le modèle indique toujours clairement que, à moins que le droit national en matière de protection des données et/ou la politique nationale des autorités responsables de la protection des données ne prévoient une exception explicite, les autorités nationales de contrôle de la protection des données devraient être consultées

avant toute opération de traitement, tel que préconisé dans la recommandation de la Commission, la Commission devrait bien s'assurer qu'il soit clairement indiqué aux parties prenantes que le modèle d'AIPD adopté conformément à sa recommandation ne peut pas modifier les principes adoptés par la recommandation en tant que telle. Les passages susmentionnés ne peuvent être compris que comme suggérant des possibilités supplémentaires d'obtenir des conseils, lesquels sont complémentaires à la consultation des autorités de contrôle de la protection des données, telle que recommandée par la Commission.

2.2 Clarté quant à la nature et aux objectifs de l'AIPD

2.2.1 Prise en considération de l'impact final sur les droits et libertés des personnes concernées

Le groupe de travail «Article 29» se félicite que l'étape relative à l'évaluation des risques de la méthode exposée dans le modèle (section 2.5) vise à considérer les incidences réelles sur les libertés et droits fondamentaux et sur les libertés civiles des personnes concernées (comme, par exemple, les pertes financières, la discrimination en matière de prix ou les actes criminels facilités par un profilage non autorisé) comme des effets des «évènements redoutés» dus à un traitement déloyal et illicite, et non plus comme étant l'impact des objectifs en matière de respect de la vie privée.

Une certaine confusion semble toutefois subsister dans le texte expliquant la méthode d'évaluation des risques (voir la section y consacrée dans le présent avis), et en particulier à la section 2.5.1.1 du modèle, qui décrit comment évaluer l'incidence des évènements redoutés. En particulier, la phrase visant à recenser les éléments afin d'évaluer «*l'incidence et la gravité d'une certaine menace détectée*» n'apporte aucune clarté. Elle cite les objectifs de respect de la vie privée en tant qu'éléments de cette évaluation (voir la section 2.2.2 du présent avis) sans plus de détails et sans expliquer comment ils y trouvent leur place, épingle les «*risques liés à la criminalité*» sans raison évidente et distingue des éléments tels que «*la libre circulation, la perte d'indépendance, la perte d'égalité*» en les désignant par l'expression «*autres principes du respect de la vie privée*»[6].

Le groupe de travail «Article 29» tient à souligner que l'AIPD évalue toujours et invariablement l'incidence sur les «*libertés et droits fondamentaux de la personne concernée*», tel que rappelé à la section 2.1 de l'avis 04/2013 et correctement indiqué en plusieurs endroits du modèle. Lorsque le modèle utilise une terminologie différente, par exemple en ne citant que le droit à la vie privée, il faut y voir une référence au concept plus global. Cela devrait être corrigé lors des révisions futures du modèle.

[6] Une suggestion serait de prolonger la dernière phrase du premier paragraphe du point «2.5.1.1 Incidence des évènements redoutés» par d'autres éléments, en la libellant comme suit: «Cette incidence potentielle est définie par les conséquences que chaque évènement redouté peut avoir sur la vie privée et les autres libertés et droits fondamentaux des personnes concernées, tels que, par exemple, les risques liés à la criminalité, comme le vol d'identité et la fraude, ou la libre circulation, l'indépendance, l'égalité de traitement, les relations sociales, les intérêts financiers, etc. dues, par exemple, au profilage, au marketing non sollicité, à la discrimination ou à des décisions personnelles fondées sur des informations erronées…»

En outre, s'il est vrai que le même évènement redouté peut avoir de nombreuses incidences sur les personnes concernées, il pourrait s'avérer utile, dans un souci de sensibilisation et afin de mesurer l'incidence, de dresser la liste des incidences les plus importantes sur les personnes concernées en rapport avec les évènements redoutés dans les exemples donnés à la section 3.4.1. Ce lien entre l'évènement redouté et l'incidence sur les libertés et droits fondamentaux de la personne caractérise cet effort dans le contexte de la protection des personnes en ce qui concerne le traitement des données à caractère personnel, par opposition, par exemple, à une simple évaluation des risques pour la sécurité de l'information.

2.2.2 La gestion des objectifs en matière de respect de la vie privée

La façon de traiter les objectifs en matière de respect de la vie privée est l'un des points les plus importants dans une analyse d'impact sur la protection de la vie privée. En effet, elle a pour finalité de garantir que les objectifs en matière de respect de la vie privée soient correctement pris en considération.

Pour l'instant, les objectifs en matière de respect de la vie privée sont:

- mentionnés à la section «2.5.1.1 Incidence des évènements redoutés» en tant qu'éléments à prendre en considération lors de l'évaluation de l'incidence et de la gravité d'une certaine menace détectée,
- mentionnés à la section «2.6.3 Risques résiduels et acceptation des risques» en tant qu'objectifs à atteindre,
- énumérés et décrits à l'«Annexe 1. Objectifs en matière de respect de la vie privée et de protection des données».

La directive 95/46/CE[7] définit dans la plupart de ses dispositions des conditions spécifiques pour le traitement des données à caractère personnel et une série d'obligations que les responsables de la protection des données et les sous-traitants doivent respecter. La directive ne prévoit pas de marge de discrétion ni de niveaux acceptables de non-conformité à ces dispositions. Tout en garantissant que la sécurité du traitement compte au nombre de ces obligations, pour sa mise en œuvre, la directive prévoit, à l'article 17, une approche de gestion des risques en indiquant que «ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger». Dans le contexte d'un modèle d'analyse d'impact, il importe de savoir que des stratégies de gestion des risques telles que celles élaborées dans le domaine de la sécurité peuvent être appliquées à la protection des données, mais uniquement en ce qui concerne les questions de sécurité, et que, pour la majeure partie des obligations, une conformité totale s'impose. Le modèle utilise l'expression «objectifs en matière de respect de la vie privée» pour désigner les obligations de conformité et il précise à sa section 2.6.3 que les concepts de risques résiduels et d'acceptation des risques ne s'appliquent pas à ces objectifs en matière de respect de la vie privée, qui «doivent être atteints» (p. 33).

[7] 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.

Le groupe de travail «Article 29» se félicite de ce que cette distinction entre la gestion des risques et la conformité soit reconnue dans le modèle, mais aurait souhaité une présentation plus claire et plus visible.

Par conséquent, il devrait toujours y avoir deux actions distinctes et complémentaires face aux conclusions d'une AIPD. La première action est liée aux risques pour les données à caractère personnel. Ils doivent être soumis à une évaluation des risques (évalués, traités, etc.). La deuxième action a trait à la réalisation des objectifs en matière de respect de la vie privée eux-mêmes, en tant qu'obligations juridiques. Il faut y voir des questions de conformité (mesures mises en œuvre ou envisagées pour atteindre les objectifs de respect de la vie privée, justification en l'absence de mesure, risques juridiques du non-respect, contrôles prévus pour vérifier si ces obligations sont respectées ou pas et comment...).

En ce qui concerne l'analyse des risques, il convient de souligner que les évènements redoutés décrits à la section «2.4.1 Introduction» devraient être systématiquement examinés. Leurs incidences potentielles sur les personnes concernées doivent être recensées et l'estimation des effets préjudiciables doit se fonder sur ces incidences potentielles. Néanmoins, la Commission peut vouloir vérifier ce qui différencie le dernier évènement redouté (le transfert de données à caractère personnel … à des personnes qui n'en ont pas besoin) du troisième (l'accès illégal à des données à caractère personnel … par des personnes non autorisées).

Le groupe de travail «Article 29» tient à suggérer certains outils pour compléter la méthode proposée dans le modèle, de façon à en faciliter l'applicabilité. Il invite la Commission à transmettre ces suggestions aux utilisateurs potentiels du modèle, par exemple en transmettant le présent avis avec le modèle ou en y faisant référence dans un instrument d'accompagnement. Ces outils complémentaires sont décrits à l'annexe du présent avis.

2.3 La méthode utilisée dans le modèle d'AIPD

Dans l'ensemble, la méthode définie dans le modèle a été précisée et est plus facile à suivre. Il subsiste toutefois de nombreux éléments obscurs et complexes, y compris dans la liste des menaces générales fournie à la section 3.4.1, dans les formulaires du modèle et dans le questionnaire fourni.

Certains de ces éléments ont été soulignés à la section 2.1 dans le cadre de la clarté quant à la nature et aux objectifs de la procédure d'AIPD. Les autres seront abordés ci-après.

2.3.1 La méthode d'évaluation (gestion) des risques

La plupart des éléments de la méthode de gestion des risques seraient essentiellement basés sur l'ISO 31 000, sur la méthode EBIOS et sur la synthèse élaborée par la CNIL[8].

Recensement des actifs

[8] http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf

Il existe une définition des actifs primaires et de soutien en tant qu'objectifs de l'évaluation globale des risques.

Détermination et évaluation des menaces et vulnérabilités

La distinction entre les menaces et les risques est désormais définie. Il existe davantage d'orientations sur le concept de vulnérabilité.

Le groupe de travail «Article 29» est toutefois préoccupé par le fait que la présentation des objectifs manqués en matière de respect de la vie privée en tant que menaces générales énumérées à la section 3.4.1, en particulier à la section 3.4.1.4, pourrait, à tort, laisser penser que le modèle «définit un objectif manqué de respect de la vie privée comme une menace» afin de cadrer avec l'évaluation des objectifs en matière de respect de la vie privée dans le contexte de la méthode d'évaluation des risques. Cette question a déjà été abordée à la section 2.2.2 du présent avis.

Le groupe de travail «Article 29» reconnaît néanmoins que les exemples pertinents et les orientations fournies (pour les données des tableaux à la section 3.4.1 qui décrit les objectifs manqués en matière de respect de la vie privée) dans les autres colonnes restent utiles, à condition qu'ils soient améliorés, pour respecter les objectifs mêmes de respect de la vie privée. Le groupe de travail «Article 29» propose d'utiliser ces informations dans le contexte d'une approche plus large et plus détaillée des objectifs de respect de la vie privée (voir aussi les considérations à la fin de la section 2.2.2 du présent avis) afin de fournir des orientations sur la façon de les atteindre. Ces informations pourraient être présentées dans des tableaux ou, mieux encore, dans une section y consacrée où des conseils pourraient être donnés aussi dans le contexte d'opérations de traitement risquées (comme le profilage ou les décisions prises sur des personnes sur la base d'opérations de traitement automatisé).

Calcul/hiérarchisation des risques

Des orientations plus claires sont fournies sur la manière de calculer et de hiérarchiser les risques. Une meilleure formulation et plus de clarté dans la section consacrée au calcul des risques (2.5.1.3) sont nécessaires.

Traitement des risques

La section «2.6.1 Modification des risques: contrôles mis en œuvre et prévus» devrait être intégrée à la section «2.5 Étape 5 – Évaluation des risques pour la protection des données», et prise en considération dans la première estimation des risques. Le titre ne devrait toutefois pas indiquer «modification des risques», qui est l'une des options de traitement des risques. Cette partie pourrait simplement s'intituler «Contrôles mis en œuvre et prévus». Ensuite, à la section 2.6 « Étape 6 – Détermination et recommandation de contrôles et risques résiduels», et en particulier à la section « 2.6.2 Traitement des risques», des contrôles supplémentaires sont déterminés et des risques sont à nouveau estimés comme étant des risques résiduels.

Dans son avis 04/2013, le groupe de travail «Article 29» a fait remarquer qu'il n'existait aucun lien dans la première version du modèle entre les risques à limiter et la liste de contrôles possibles figurant à l'annexe II. Le groupe de travail «Article 29» se félicite de ce que, dans la nouvelle version du modèle, la description de l'objectif

des contrôles possibles inclut souvent le type de risques qu'il est en règle générale supposé limiter. En outre, la liste non exhaustive des menaces générales à la section 3.4.1 relie ces menaces aux contrôles possibles figurant à l'annexe II.

Risques résiduels

Afin de mesurer de façon équilibrée les risques résiduels à la fin du processus de gestion des risques, il est tout aussi important de déterminer tous les intérêts en présence à un stade précoce. Ceux-ci peuvent être déduits du processus global de gestion des risques de l'entreprise, s'il existe. Peuvent être représentés non seulement les intérêts économiques ou légitimes, mais aussi d'autres enjeux, tels que, par exemple, la responsabilité sociale ou la conformité à d'autres exigences juridiques.

Le groupe de travail «Article 29» suggère qu'une nouvelle section soit ajoutée afin de recenser les enjeux du traitement. Cette section pourrait s'intercaler entre les sections 2.3.1 et 2.3.2 et s'intituler «2.3.2 Enjeux du traitement». Elle pourrait décrire les opportunités de la création d'un traitement du réseau intelligent (marketing/économique, sociétal, conformité juridique, etc.).

Une évaluation des risques résiduels compte tenu des enjeux pourrait être ajoutée, après le premier paragraphe de la section «2.6.4 Résolution». Ce paragraphe pourrait expliquer que la résolution consiste à décider d'accepter ou non les risques résiduels compte tenu des enjeux recensés à la section 2.3.

2.3.2 Rôles et responsabilités

Le groupe de travail «Article 29» salue l'intégration (section 1.4.2) d'une liste des différents types de gestionnaires de réseaux intelligents, laquelle comprend une description générale des fins auxquelles ils peuvent traiter des données à caractère personnel.

L'existence d'une sous-section spécifique, la sous-section 2.1.2, souligne désormais plus distinctement la nécessité d'une répartition claire des responsabilités entre le responsable du traitement et le sous-traitant. L'exemple fourni dans le texte sur les responsables du traitement et les responsabilités de l'éventuel sous-traitant dans le cas d'un compteur intelligent devrait être intégré à d'autres exemples abordant des situations plus complexes. Un autre exemple est mentionné dans le texte (gestionnaire de microréseau et compagnie d'assurances impliquée), où le problème est relevé sans qu'aucune orientation ne soit toutefois fournie.

En outre, comme le groupe de travail «Article 29» l'a déjà suggéré dans son avis 04/2013, 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 (lorsqu'un formulaire correspondant existe déjà à la section 3).

2.3.3 Les formulaires du modèle

En plus des autres considérations formulées dans d'autres sections du présent avis, le groupe de travail «Article 29» tient à souligner d'autres manquements dans les sections décrivant certains formulaires à utiliser pour mettre en œuvre l'AIPD.

Par exemple, à la section 3.3, la relation entre les différents modèles utilisés pour l'identification, la caractérisation et la description des systèmes de réseaux intelligents, la séquence de l'utilisation et leur mode exact d'utilisation ne sont pas clairs. Le texte fait référence à un document externe, sans aucun commentaire sur la raison de cette référence. Aussi, la méthode ne semble indiquer nulle part quand le formulaire figurant à la section 3.3.5 doit être utilisé.

Par ailleurs, un tableau reprenant les actifs primaires et les actifs de soutien correspondants est essentiel pour orienter l'évaluation des risques.

De façon générale, il convient de fournir davantage d'orientations sur l'utilisation des formulaires. Il serait très utile de donner l'un ou l'autre exemple dans une annexe.

2.4 Le contenu spécifique au secteur dans le modèle d'AIPD

L'une des principales questions soulevées dans l'avis 04/2013 concernait le fait que les risques et les contrôles énumérés dans la première version du modèle ne reflétaient pas l'expérience du secteur en ce qui concerne les principales préoccupations et les bonnes pratiques.

Le groupe de travail «Article 29» constate et salue le fait qu'un contenu spécifique a été ajouté à la liste non exhaustive des menaces générales reprise à la section 3.4.1.1, en particulier dans la colonne intitulée «Exemples spécifiques au secteur de l'énergie de vulnérabilités d'actifs secondaires». Le groupe de travail «Article 29» continue toutefois de penser que certaines améliorations et davantage d'orientations restent nécessaires, tant dans le texte que dans le modèle, et notamment pour respecter les objectifs en matière de respect de la vie privée (voir aussi la section 2.2.2).

Comme indiqué à la section 1.1, la Commission a rejeté la proposition formulée par le groupe de travail «Article 29» d'intégrer au modèle le recueil des meilleures techniques disponibles (MTD) que le groupe d'experts 2 est en train de préparer, en raison, selon elle, de leur portée limitée aux compteurs intelligents et de leur nature évolutive.

Le groupe de travail «Article 29» confirme son point de vue selon lequel considérer les MTD comme un recueil lié de façon inhérente au modèle permettrait à une organisation procédant à une AIPD de choisir les mesures adéquates, au besoin. La nature évolutive des MTD n'empêche pas leur rôle complémentaire au modèle d'AIPD. Qui plus est, le modèle lui-même aura besoin d'un cycle de révision afin de maintenir et peaufiner la méthode après une première phase d'application et, quoi qu'il en soit, de manière périodique. Le fait que la portée des MTD soit limitée aux compteurs intelligents et ne soit dès lors pas exhaustive n'est pas non plus une raison d'exclure son utilisation dans le cadre de l'exercice d'une AIPD. Les compteurs intelligents constituent des sous-systèmes ou des données à caractère personnel sont essentiellement collectées et traitées et, en tout état de cause, il est préférable d'avoir quelques orientations plutôt que de ne pas en avoir du tout. En outre, le groupe de travail «Article 29» saisit cette occasion de suggérer à la Commission et à l'industrie d'explorer la possibilité d'étendre le travail précieux relatif aux MTD à tout l'éventail des réseaux intelligents.

Dans son avis 04/2013, et notamment à l'annexe II, le groupe de travail «Article 29» recommandait 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, puis davantage détaillées dans le document complémentaire sur les MTD. Cela n'a pas été fait. Le groupe de travail «Article 29» reste d'avis qu'il serait très utile au secteur de disposer d'un portefeuille de mesures à mettre en œuvre et d'être plus conscient de l'existence des technologies renforçant la vie privée afin de concevoir des contrôles plus adéquats.

2.5 Nécessité de tester/valider le modèle d'AIPD

Le groupe de travail «Article 29» suggère qu'il serait nécessaire de tester/valider le modèle d'AIPD sur le terrain, sur la base de la version existante, et de tenir compte autant que possible des commentaires ci-dessus. Le groupe de travail «Article 29» propose qu'à l'issue de ce test, le modèle et sa méthode soient réexaminés et renforcés à la lumière de ces expériences et en tenant compte des commentaires formulés ci-dessus. Ces tests, sur lesquels le groupe de travail «Article 29» devrait être informé et auxquels différentes autorités de contrôle de la protection des données pourraient contribuer, peuvent aussi s'avérer utiles pour fournir des exemples précieux à inclure dans les annexes du modèle afin de mieux comprendre la méthode proposée.

2.6 Autres considérations

2.6.1 Le concept de données à caractère personnel

La section 2.1 décrit comment déterminer si des données à caractère personnel sont traitées dans le sous-système de réseaux intelligents considéré. Le groupe de travail «Article 29» fait observer que le classement en tant que données à caractère personnel dans les exemples repris semble correct, même si la justification donnée pour qualifier une information de donnée à caractère personnel n'applique pas toujours la terminologie légale.

Par exemple, ce que l'on appelle les «données sur l'utilisation» sont considérées comme des données à caractère personnel parce qu'«elles fournissent des indications sur la vie quotidienne de la personne», alors qu'il s'agit de données à caractère personnel uniquement parce qu'elles se rapportent à la personne qui est titulaire du contrat et à sa famille, le cas échéant. Le fait qu'elles fournissent des indications sur la vie quotidienne constitue une incidence sur la vie privée. Cette considération vaut aussi pour d'autres éléments repris sur la liste. Si la liste des exemples est assurément utile pour les utilisateurs potentiels du modèle, l'impression est que cette incidence considérable sur la vie privée est nécessaire pour que les données soient considérées comme étant des données à caractère personnel. Il convient par ailleurs d'indiquer clairement que la liste des exemples n'est pas exhaustive.

2.6.2 Autres remarques sur la terminologie relative à la protection des données

Dans certaines sections, le modèle utilise des termes tels que «propriétaire du système», ce qui fait sens dans le domaine de l'application, mais ne précise pas toujours la relation à la terminologie de la protection des données qui peut s'appliquer (comme responsable du traitement des données,…) (p. 14, 18, 32,…), ou «la

personne», «le consommateur», le «client», sans lien clair avec la personne concernée (p. 10, 15,…).

En outre, certaines expressions utilisées, telles que «convenu avec le consommateur» (p. 10) ou «les consommateurs doivent avoir le choix» (p. 11), peuvent être rapprochées de la nécessité d'obtenir le «consentement» tel que défini à l'article 2, point h), de la directive.

Le groupe de travail «Article 29» invite à envisager le recours à la terminologie appropriée en matière de protection des données, ainsi que d'expliquer le niveau d'interopérabilité des termes, le cas échéant.

2.7 Conclusions et recommandations

Le groupe de travail «Article 29» reconnaît le travail accompli par les membres du groupe d'experts 2 et constate que la deuxième version du modèle représente une amélioration considérable par rapport à la version précédente, en ce sens que la méthode est mieux définie et plus facile à suivre. Il subsiste toutefois une série d'éléments confus et un besoin de clarté par endroits, des lacunes qui, si elles sont comblées comme indiqué, contribueront de façon déterminante au bon déploiement et à l'utilisation réussie du modèle.

Le groupe de travail «Article 29» comprend que la version qu'il a examinée peut encore faire l'objet de corrections linguistiques et juridiques.

Le groupe de travail «Article 29» est conscient de la nécessité pressante d'une AIPD dans le secteur et se réjouit de l'adoption rapide d'une version finale du modèle, dont l'efficacité, après une certaine période d'utilisation, devra assurément être vérifiée et améliorée. Il recommande par conséquent d'organiser une phase de tests, avec des cas réels, sur lesquels le groupe de travail «Article 29» devrait être informé et auxquels différentes autorités de contrôle de la protection des données pourraient contribuer, et qui devraient aussi contribuer à garantir que le modèle offre une meilleure protection des données aux personnes concernées dans le contexte du déploiement des réseaux intelligents. Lors de la phase de test et comme prévu dans le modèle, le secteur est encouragé à faire attention aux concepts clés de la réforme de la protection des données, comme la protection des données dès la conception et par défaut, la minimisation des données, le droit à l'oubli numérique et la portabilité des données.

En outre, le groupe de travail «Article 29» continue de recommander à la Commission 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.

Fait à Bruxelles, le 4 décembre 2013

Pour le groupe de travail
Le président
Jacob KOHNSTAMM

Annexe: outils méthodologiques supplémentaires

À la section «3.5. Étape 5 – Évaluation des risques pour la protection des données», le tableau suivant pourrait être utilisé pour évaluer les évènements redoutés:

Traitement et données à caractère personnel	Niveau de détermination (ND)	Évènements redoutés	Incidences potentielles	Effets préjudiciables (EP)	Gravité (ND+EP)
[liste des données à caractère personnel impliquées]	[le niveau le plus approprié sur l'échelle des ND, sur la base des données à caractère personnel]	[évènement redouté]	[liste des conséquences potentielles sur les personnes concernées si l'évènement redouté se produit]	[le niveau le plus approprié sur l'échelle des EP, sur la base des incidences potentielles]	[addition]

Lorsque les données à caractère personnel ne sont pas évaluées de manière globale, ces lignes doivent être répétées (par exemple, pour chaque traitement).

Le même tableau pourrait accueillir d'autres colonnes correspondant aux menaces, afin de présenter la totalité des risques:

Traitement et données à caractère personne	Niveau de détermination (ND)	Évènements redoutés	Incidences potentielle	Effets préjudiciables (EP)	Gravité (ND+EP)	Principales menaces	Vulnérabilités (VUL)	Source de risque	Capacités (CAP)	Probabilité (VUL+ CAP)

Il convient d'ajouter une nouvelle section afin de démontrer la réalisation des objectifs en matière de respect de la vie privée. Cette section pourrait s'intercaler entre les sections 2.6.2 et 2.6.3 et s'intituler «2.6.3 Conformité aux objectifs en matière de respect de la vie privée». Dès lors que ces objectifs sont obligatoires et non négociables, il y a lieu d'indiquer, pour chaque objectif de respect de la vie privée, que la façon dont il est réalisé doit être décrite, ou qu'une justification de non-réalisation doit être fournie[9].

Le tableau suivant pourrait être utilisé à cet effet:

[9] Comparable à la notion de «déclaration d'applicabilité» dans l'ISO/IEC 27001.

Objectifs en matière de respect de la vie privée	Explications	Description / justification
Sauvegarder la qualité des données à caractère personnel	L'évitement du recours aux données et leur limitation, la spécification et la limitation de la finalité, la qualité des données et la transparence sont les objectifs clés qu'il convient de garantir.	[description de la façon dont l'objectif de respect de la vie privée a été atteint OU justification de sa non-réalisation]
Légitimité du traitement des données à caractère personnel	La légitimité du traitement des données à caractère personnel doit être garantie en fondant le traitement des données sur le consentement explicite, sur un contrat, sur une obligation légale, etc.	[description de la façon dont l'objectif de respect de la vie privée a été atteint OU justification de sa non-réalisation]
Légitimité du traitement des données à caractère personnel sensibles	La légitimité du traitement des données à caractère personnel sensibles doit être garantie en fondant le traitement des données sur le consentement explicite, sur une base juridique spéciale, etc.	[description de la façon dont l'objectif de respect de la vie privée a été atteint OU justification de sa non-réalisation]
Respect du droit de la personne concernée à être informée	Il faut garantir que la personne concernée est informée en temps utile de la collecte de ses données.	[description de la façon dont l'objectif de respect de la vie privée a été atteint OU justification de sa non-réalisation]
Respect du droit de la personne concernée à accéder à ses données et à les corriger et les effacer	Il faut garantir que le souhait de la personne concernée d'accéder à ses données, de les corriger, de les effacer et de les bloquer est respecté en temps utile. Le respect du droit à l'oubli numérique et du droit à la portabilité des données doit être encouragé.	[description de la façon dont l'objectif de respect de la vie privée a été atteint OU justification de sa non-réalisation]
Respect du droit d'objection de la personne concernée	Il faut garantir que les données de la personne concernée ne soient plus traitées si elle s'y oppose. La transparence des décisions automatiques par rapport aux personnes doit être garantie, notamment en cas de profilage.	[description de la façon dont l'objectif de respect de la vie privée a été atteint OU justification de sa non-réalisation]
Sauvegarde de la confidentialité et du traitement	Empêcher l'accès non autorisé, consigner le traitement des données, la sécurité du réseau et du transport et empêcher les pertes accidentelles de données sont les objectifs clés qu'il convient de garantir. Une procédure de notification des violations doit être promue.	[description de la façon dont l'objectif de respect de la vie privée a été atteint OU justification de sa non-réalisation]
Respect des exigences de notification	La notification du traitement des données, le contrôle préalable du respect et la documentation sont les objectifs clés qu'il convient de garantir. L'AIPD doit être considérée comme un outil essentiel à cette fin.	[description de la façon dont l'objectif de respect de la vie privée a été atteint OU justification de sa non-réalisation]
Respect des exigences de rétention des données	La rétention des données doit se faire durant une période de temps la plus courte possible, conformément à la finalité de la rétention ou à d'autres exigences légales.	[description de la façon dont l'objectif de respect de la vie privée a été atteint OU justification de sa non-réalisation]

Objectifs en matière de respect de la vie privée	Explications	Description / justification
Respect de la vie privée dès la conception	Compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, des mesures et procédures techniques et organisationnelles doivent être prévues à la fois au moment où sont choisis les procédés de traitement et lors du traitement lui-même, de façon à respecter pleinement le droit à la vie privée et le droit à la protection des données de la personne concernée.	[description de la façon dont l'objectif de respect de la vie privée a été atteint OU justification de sa non-réalisation]
Respect de la vie privée par défaut	Il convient de mettre en œuvre des mécanismes garantissant que, par défaut, seules sont traitées les données à caractère personnel nécessaires pour chaque finalité spécifique du traitement, et qu'en particulier, les données ne sont ni recueillies ni conservées au-delà du minimum nécessaire pour remplir lesdites finalités, à la fois en termes de quantité de données et de durée de stockage.	[description de la façon dont l'objectif de respect de la vie privée a été atteint OU justification de sa non-réalisation]

Bien entendu, chacune des entrées ci-dessus peut être multipliée afin de ventiler davantage encore les objectifs de respect de la vie privée, au besoin. Par exemple, la «qualité des données» recouvre de nombreux autres principes, comme la limitation des données et l'évitement du recours à ces données, la nécessité et la proportionnalité par rapport aux objectifs, etc. En outre, différents contrôles utilisés pour respecter le même objectif en matière de respect de la vie privée appellent différentes entrées pour se différencier.

En conclusion, les risques pour la protection des données sont ainsi gérés (évalués et traités) et les mesures prises pour atteindre les objectifs de respect de la vie privée sont décrits (et peuvent être contrôlés).

Une approche combinée reste possible, en étudiant aussi les risques de la non-réalisation de certains objectifs de respect de la vie privée (pas seulement la sécurité, mais aussi, par exemple, la limitation de la finalité, la nécessité et la proportionnalité, la rétention des données, la garantie des droits de la personne concernée, etc.).