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

2588/15/FR
WP 232

Avis 02/2015 sur le code de conduite pour l'informatique en nuage du C-SIG

Adopté le 22 septembre 2015

Synthèse

Dans le présent avis, le groupe de travail «Article 29» sur la protection des données (ci-après le «groupe "Article 29"») analyse le code de conduite en matière de protection des données pour les prestataires de services d'informatique en nuage (Data Protection Code of Conduct for Cloud Service Providers – ci-après le «code»), rédigé par le groupe de travail C-SIG (Cloud Select Industry Group), composé de représentants du secteur concerné, et qui a été soumis au groupe «Article 29» le 19 janvier 2015.

Le groupe «Article 29» apprécie l'effort consenti par le secteur pour rédiger ce code de conduite. Le code fournit des orientations importantes aux prestataires de services d'informatique en nuage concernant les règles applicables en matière de protection des données et de respect de la vie privée en Europe. L'adhésion au code de conduite contribuera à garantir une transparence et une sécurité juridique plus grandes pour toutes les parties concernées.

Toutefois, le groupe «Article 29» ne peut approuver formellement le projet de code, qui ne satisfait pas toujours aux exigences juridiques minimales et dont la valeur ajoutée par rapport à la directive 95/46/CE et à la législation nationale n'est pas toujours évidente. Il subsiste donc certaines préoccupations importantes. Le présent avis analyse ces aspects en faisant ressortir les points problématiques, en vue de contribuer à l'adoption d'un code qui apporterait une telle valeur ajoutée.

L'avis examine notamment:

- les conséquences de l'adhésion au code: l'adhésion au code aidera les entreprises à démontrer leur volonté de rendre des comptes, mais elle n'empêche en rien les autorités chargées de la protection des données d'exercer leurs pouvoirs d'exécution;
- la gouvernance du code: le code devrait apporter plus de précisions sur la transition vers le règlement sur la protection des données, sur la différence entre l'auto-évaluation et la certification par des tiers et sur les pouvoirs de l'organe de gouvernance, en particulier en ce qui concerne les mécanismes de dissuasion. De plus, le groupe «Article 29» ne peut pas être membre du comité de pilotage;
- la responsabilité: le code doit empêcher l'adoption de conditions de services qui limitent indûment les obligations et les responsabilités. Le code doit spécifier (dans une annexe) quand le prestataire de services d'informatique en nuage est un responsable du traitement, un responsable conjoint du traitement ou un sous-traitant, et attribuer les responsabilités;
- la transparence à propos du/des lieu(x) du traitement des données;
- le traitement des catégories particulières de données et des données sensibles (comme les données financières ou les données relatives à la santé);
- l'applicabilité de la définition européenne des données à caractère personnel;
- les exigences relatives aux transferts internationaux et aux demandes d'accès des autorités répressives;
- les mesures de sécurité et le niveau de détail des informations relatives à ces mesures;
- le droit de procéder à des audits informatiques;
- la référence à la portabilité des données en tant que droit fondamental des utilisateurs.

Le groupe «Article 29» se félicite des progrès accomplis par le C-SIG dans l'élaboration du code et l'encourage à poursuivre ses efforts pour finaliser le code en tenant compte des observations formulées dans le présent avis. Le C-SIG est dès lors invité à envisager

d'intégrer chacune des observations et recommandations du groupe «Article 29» dans une version finale du Code.

Table des matières

0. Introduction

Le projet de code de conduite en matière de protection des données pour les prestataires de services d'informatique en nuage (Data Protection Code of Conduct for Cloud Service Providers – ci-après le «code»), rédigé par le groupe de travail C-SIG (Cloud Select Industry Group), a été formellement soumis au groupe de travail «Article 29» (ci-après le «groupe "Article 29"») le 27 février 2014. Le groupe «Article 29» a récapitulé une première série d'observations dans une lettre adressée au C-SIG en juin 2014.

Une nouvelle version du code tenant compte d'un certain nombre d'observations émises dans la lettre à propos de la forme et du fond a été soumise au groupe «Article 29» le 21 janvier 2015.

L'article 30, paragraphe 1, de la directive 95/46/CE dispose que «[l]e groupe a pour mission: […] de donner un avis sur les codes de conduite élaborés au niveau communautaire». Dans son document de travail concernant la procédure d'examen des codes de conduite communautaires adopté le 10 septembre 1998 (WP13), le groupe «Article 29» a précisé que, lorsqu'il lui est demandé d'émettre un tel avis, il se prononcera sur le fait de savoir si le projet de code soumis:

- est conforme aux dispositions des directives sur la protection des données et, le cas échéant, aux dispositions nationales prises en application de ces directives;
- présente une qualité et une cohérence interne suffisantes, apporte une valeur ajoutée suffisante par rapport aux directives et à toute autre législation applicable en matière de protection des données, en précisant notamment si le projet de code est suffisamment centré sur les questions et les problèmes particuliers que pose la protection des données au sein de l'organisation ou du secteur auquel il est censé s'appliquer, et apporte de véritables solutions à ces questions et à ces problèmes.

Dans le cas présent, bien que le code de conduite soit certainement utile pour les prestataires de services d'informatique en nuage, certaines préoccupations demeurent. Le présent avis examine ces aspects, en vue de contribuer à l'adoption d'un code susceptible d'apporter une valeur ajoutée significative au regard de la directive sur la protection des données et de la législation nationale.

1. Rôle du code de conduite dans la perspective du projet de règlement sur la protection des données

Le code est censé contribuer à l'application correcte des dispositions nationales adoptées en vertu de l'actuelle directive sur la protection des données (article 27) et son évaluation par le groupe «Article 29» reposera donc sur le cadre juridique en vigueur, mais il convient aussi d'envisager cette évaluation à la lumière des dispositions que pourrait contenir le projet de règlement général sur la protection des données concernant les codes de conduite.

Au regard de ce qui précède, le code gagnerait à donner plus d'indications sur les mécanismes qui peuvent garantir une transition sans heurts vers le nouvel environnement réglementaire.

Le futur règlement général sur la protection des données comprend notamment plusieurs dispositions *[sur la responsabilité du traitement, le statut des sous-traitants, les codes de*

conduite (article 38), les certifications (article 39), les pouvoirs et les fonctions des autorités chargées de la protection des données (en particulier le mécanisme de guichet unique)] qui auront des effets considérables, tant pour les responsables du traitement que pour les sous-traitants. Le code établit un comité de pilotage chargé de proposer des modifications du code et de suivre les évolutions dans le domaine concerné (7.1), mais les mécanismes actuellement envisagés à cet effet sont décrits en termes très généraux.

Le code devrait indiquer clairement que l'adhésion à ses principes ne dispense pas les prestataires de services d'informatique en nuage de se conformer aux évolutions du droit de l'Union. En particulier, un prestataire de services d'informatique en nuage qui souscrirait au code avant qu'une modification de la législation ne soit transposée dans le code devrait veiller à respecter la nouvelle législation, même si cela implique des obligations nouvelles ou contradictoires par rapport au code.

2. Code de conduite et mesures d'exécution des autorités chargées de la protection des données

Les prestataires de services d'informatique en nuage qui adhèrent au code entendent certainement atténuer, par ce moyen, le risque de procédures d'exécution formelles (notamment l'application de sanctions) de la part des autorités chargées de la protection des données dans l'Union. Cette préoccupation est légitime au regard des pouvoirs susceptibles d'être conférés aux autorités chargées de la protection des données au titre du futur règlement.

L'adhésion au code ne garantit aucune protection automatique contre d'éventuelles interventions ou actions des autorités compétentes chargées de la protection des données (ou d'autres autorités) dans l'exercice de leurs missions de surveillance et d'exécution.

Tout en insistant sur ce point, le groupe «Article 29» encourage les prestataires de services d'informatique en nuage à souscrire à de tels codes de conduite. Le respect des exigences de ces codes aidera ces prestataires de services d'informatique en nuage à démontrer leur volonté de rendre compte de leurs activités au regard des règles de protection des données, ce qui aura certainement un effet positif dans le contexte de ces missions de surveillance et d'exécution.

3. Gouvernance du code

Une section importante du code est consacrée à la mise en place d'une structure de gouvernance, en vue d'évaluer les conditions d'adhésion et de superviser le respect du code par les acteurs du secteur. Ces aspects peuvent avoir une incidence directe sur le niveau de protection des données garanti aux personnes concernées.

Tout d'abord, **le rôle du groupe «Article 29» doit être clarifié (7.1) dans la mesure où celui-ci ne peut pas participer à la structure de gouvernance du code**. Le groupe «Article 29» a été institué au titre de la directive 95/46/CE, comme organe consultatif de la Commission européenne, avec pour mission (notamment) d'examiner toute question portant sur l'application de la directive, en vue de contribuer à sa mise en œuvre homogène. L'une des principales prérogatives du groupe «Article 29» réside dans son caractère indépendant. De ce point de vue, toute participation du groupe «Article 29» à la structure de gouvernance, comme le propose le code, semble sortir de sa mission ou de son mandat, et peut engendrer, de ce fait, un conflit d'intérêts parmi les entités qui le composent (les autorités nationales chargées de la

protection des données) avec le rôle de surveillance qu'elles exercent au niveau national vis-à-vis des acteurs du secteur de l'informatique en nuage.

Le groupe «Article 29» a conscience que la phase de transition entre les cadres juridiques dans lesquels s'applique le code s'annonce délicate. Pour cette raison, **il paraît nécessaire de définir une stratégie de gestion de la transition et de mettre en place une véritable structure de gouvernance pour la superviser, de façon à garantir la validité et l'application effective du code durant toute la période de transition et après l'adoption du nouveau règlement.** Dans cette perspective, il convient de remédier à certaines discordances entre la date de mise en application du code et la prise de fonctions de la structure de gouvernance (par exemple, 7.1, p. 35).

Les conditions d'adhésion au code se fondent sur des mécanismes d'auto-évaluation ou de certification par des tiers. Or, ces deux conditions offrent des niveaux d'assurance différents. À cet égard, il y a lieu de clarifier plusieurs points du code:

- **Le code ne prévoit pas d'engagement clair en faveur d'une approche plus rigoureuse de la part des organismes compétents[1] en cas d'auto-évaluation.** La possibilité d'une (ré-)évaluation par des organismes compétents en cas d'adhésion fondée sur l'auto-évaluation devrait être correctement encadrée. En ce sens, il serait approprié de définir un rôle plus actif de la structure de gouvernance.

- En cas d'évaluation à la suite d'une certification, **il convient d'indiquer plus clairement que les certifications admissibles pour l'adhésion fondée sur une certification doivent être spécifiques à l'informatique en nuage** et couvrir non seulement l'aspect sécurité, mais aussi tous les principes de protection des données à caractère personnel définis dans le cadre juridique de l'Union.

- Le groupe «Article 29» se félicite que le code spécifie différentes marques de conformité possibles pour les différents mécanismes d'adhésion (7.4). Néanmoins, il convient de reformuler le passage concerné pour **indiquer sans ambiguïté que les marques de conformité seront différentes selon que les prestataires de services d'informatique en nuage optent pour l'auto-évaluation ou pour la certification.**

Enfin, **le code devrait clarifier les pouvoirs de l'organe de gouvernance, notamment en ce qui concerne la sélection des mécanismes de dissuasion**, ou les conditions et la procédure à observer afin d'évaluer régulièrement la validité des critères imposés et de décider de révoquer éventuellement un statut d'adhésion accordé précédemment (7.2, 7.3, 7.4, 7.5).

4. Scénarios de cas concrets relatifs au traitement de catégories de données sensibles ou au traitement effectué pour des catégories spécifiques de responsables du traitement

Le code ne mentionne actuellement aucun scénario spécifique en matière d'informatique en nuage.

Même s'il ne peut évidemment pas prévoir tous les scénarios possibles, **le code devrait mentionner certains cas particulièrement pertinents de prestataires offrant des services d'informatique en nuage dédiés au traitement des données sensibles,** que ce soit au sens

[1] Les organismes qui examinent et approuvent les déclarations d'adhésion des prestataires de services d'informatique en nuage.

juridique (par exemple, les services d'informatique en nuage pour les données relatives à la santé) ou au sens courant du terme (par exemple, les services d'informatique en nuage liés aux services financiers). Le nombre, la portée et la pénétration de ces services augmentent rapidement, de même que les risques pour la protection des données engendrés par le traitement de données sensibles dans l'environnement en nuage. Ils suscitent donc des préoccupations considérables tant pour les utilisateurs professionnels que pour les particuliers.

Or le code ne contient aucune référence à de telles situations, si ce n'est pour indiquer que, sans préjudice des législations nationales, ce traitement requiert normalement des «précautions supplémentaires».

5. Informations concernant le lieu du traitement

Le problème de la localisation des données a été soulevé dans la lettre adressée au C-SIG en juin 2014 par le groupe «Article 29» concernant la version précédente du code. La lettre mentionnait expressément: *«Il convient surtout de spécifier et de renforcer l'obligation d'information qui incombe aux prestataires de services d'informatique en nuage. En particulier, des informations spécifiques et facilement accessibles devront être fournies concernant la localisation des données, c'est-à-dire des informations plus précises que la simple mention des pays où seront effectués le "traitement", le sous-traitement et/ou le transfert des données ou des personnes qui les réalisent.»*

La version actuelle du code n'indique ni ne garantit que le responsable du traitement peut obtenir des informations concernant les localisations précises où est effectué le traitement[2].

Or, dans certains États membres, la transposition de la directive 95/46/CE dans le droit national comprend des dispositions qui imposent au responsable du traitement d'assurer activement la supervision, le suivi et au besoin le contrôle des opérations et des mesures de sécurité en place, lorsque le traitement est confié à des sous-traitants. Le responsable du traitement ne peut remplir ces obligations qu'à condition de disposer d'informations précises sur les adresses de tous les lieux où le traitement est effectué par le prestataire de services d'informatique en nuage et ses sous-traitants, le cas échéant. Il devrait en outre être averti de toute modification de ces adresses.

Afin de contribuer à la bonne application des dispositions nationales prises par certains États membres, le code doit donner des orientations plus précises concernant les informations à fournir sur les adresses des lieux où le traitement est effectué. Pour des raisons de sécurité, il ne peut être fourni qu'une localisation générale avant la conclusion du contrat. Cette description générale devrait, au moins, permettre au responsable du traitement de déterminer le droit applicable et, lorsque des données sont envoyées en dehors de l'Union, d'en informer la personne concernée. Dès qu'un contrat est signé entre le responsable du traitement et le prestataire de services d'informatique en nuage agissant comme sous-traitant, le responsable du traitement et l'autorité chargée de la protection des données devraient pouvoir accéder aisément aux adresses précises, à tout moment.

[2] Conformément à l'article 27, paragraphe 1, de la directive 95/46/CE, les codes de conduite sont destinés à contribuer à la bonne application des dispositions nationales prises par les États membres en application de la directive.

6. La notion de données à caractère personnel

Si le code fait référence aux notions de responsables du traitement des données et de sous-traitants, il ne contient pas actuellement de définition de la notion de données à caractère personnel. Ce choix semble découler du fait que, comme l'indique le code, *«en règle générale, un prestataire de services d'informatique en nuage agissant comme sous-traitant chargé du traitement des données n'identifie pas les données à caractère personnel qui lui sont confiées, notamment quand il n'est pas autorisé par le contrat de services à identifier ces données à caractère personnel, ou quand le client a mis en place des outils comme le chiffrement des données, qui l'empêchent d'identifier les données à caractère personnel dont il a la charge»*.

Tout d'abord, si cette phrase peut être pertinente dans le cas des modèles de services PaaS/IaaS, la possibilité d'identification est fréquente dans le modèle SaaS. Il convient donc de reformuler la phrase de façon à ne pas exclure la possibilité d'identification par les prestataires de services d'informatique en nuage dans la pratique.

En outre, **le groupe «Article 29» souhaiterait voir confirmer le fait que la définition des données à caractère personnel qui s'applique au code est celle de l'Union. Cette référence pourrait être combinée avec un renvoi à la notion d'anonymisation qui est actuellement absente du code.** Le niveau d'exigence élevé recommandé par le groupe «Article 29» dans son avis sur l'anonymisation pourrait être mentionné, ainsi que le fait que **la pseudonymisation, s'il devait en être question, ne peut être considérée que comme une mesure de sécurité et non comme un moyen d'exonérer les prestataires de services d'informatique en nuage ou leurs clients de leurs responsabilités au regard du droit en matière de protection des données.**

7. Transferts internationaux et demandes d'accès des autorités répressives

Le projet actuel du code n'aborde que superficiellement la question des demandes d'accès des autorités répressives ou des pouvoirs publics. Or, comme indiqué dans l'avis 05/2012 du groupe «Article 29» sur l'informatique en nuage, il s'agit là d'une question majeure en rapport avec la protection des données et l'informatique en nuage.

Le groupe «Article 29» insiste expressément sur ses exigences spécifiques en matière de transfert ou de divulgation de données aux autorités de pays tiers, sur la base de son interprétation de la proposition d'article 43 *bis* du règlement général sur la protection des données. L'inclusion de ces exigences dans le projet de code répondrait aussi aux attentes du groupe «Article 29» qui considère qu'un code de conduite doit aller au-delà du simple respect du droit[3].

Comme indiqué dans des avis précédents[4], le code devrait aussi préciser:

- qu'un sous-traitant doit aviser le responsable du traitement de toute demande juridiquement contraignante de divulgation de données à caractère personnel émanant d'une autorité répressive, sauf disposition contraire,

[3] Voir le document WP 13.
[4] Voir le document WP 204 rev.01 – Explanatory Document on the Processor Binding Corporate Rules.

- et **qu'en tout état de cause, les transferts de données à caractère personnel par un sous-traitant à une quelconque autorité publique ne peuvent être effectués d'une manière massive, disproportionnée et indifférenciée qui irait au-delà de ce qui est nécessaire dans une société démocratique.**

Enfin, il faut rappeler aux prestataires de services d'informatique en nuage que, pour les transferts internationaux de données aussi, il leur incombe d'agir strictement dans les limites des instructions reçues du client. Le prestataire de services d'informatique en nuage peut cesser d'être considéré comme un sous-traitant, avec toutes les conséquences que cela comporte, notamment en termes de responsabilité, dans les cas où ses actions dépassent de loin les capacités normales d'un sous-traitant, qui est supposé n'avoir aucune liberté par rapport aux instructions du responsable du traitement. Cela peut être le cas, par exemple, lorsque les prestataires de services d'informatique en nuage organisent de manière autonome des transferts internationaux de données en réponse aux demandes d'une autorité répressive ou de la sûreté de l'État, sans essayer d'y associer les responsables du traitement concernés[5].

8. Responsabilité

Le code n'apporte pas suffisamment de précisions sur le régime de responsabilité applicable aux parties en cas de violation des leurs obligations de protection des données.

L'avis 05/2012 du groupe «Article 29» sur l'informatique en nuage a souligné l'importance de clarifier le rôle de chacune des parties afin de déterminer leurs obligations particulières au regard de la législation sur la protection des données et d'attribuer les responsabilités attachées aux violations éventuelles de ces règles. Cela contribuerait à éviter de possibles vides où aucune des parties ne garantit le respect des obligations ou des droits nés de la législation en matière de protection des données[6]. La proposition d'article 26, paragraphe 4, du futur règlement général sur la protection des données[7] devrait inciter les prestataires de services d'informatique en nuage à assurer davantage de clarté sur leurs obligations et leur responsabilité dans de tels cas. À cet égard, **le code doit empêcher l'adoption de conditions de services défavorables aux clients, qui limiteraient indûment les obligations et responsabilités des prestataires de services d'informatique en nuage et restreindraient les droits des clients**[8].

L'attribution des responsabilités entre parties commerciales est une source d'inquiétude pour les personnes physiques quand elle peut avoir pour elles des conséquences négatives. Il faut donc que le code spécifie que, quelle que soit cette répartition des responsabilités, elle ne devrait jamais priver les personnes de leurs droits ou de la possibilité d'obtenir une réparation pour un préjudice éventuel. En particulier, en cas de responsabilité conjointe du traitement, les différents rôles et responsabilités concernant le traitement des données devraient être clairement répartis entre les prestataires de services d'informatique en nuage et le client, de façon à faciliter l'exercice de leurs droits par les personnes concernées. Il serait aussi

[5] Voir la p. 13 de l'avis 10/2006 sur le traitement des données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT).
[6] C'est d'autant plus important qu'il peut exister différents niveaux de responsabilité du traitement et que, dans certaines situations, un prestataire de services d'informatique en nuage peut, selon les circonstances concrètes, être considéré comme responsable conjoint ou comme responsable à part entière du traitement.
[7] Qui prévoit que le sous-traitant qui traite des données à caractère personnel d'une manière autre que celle définie dans les instructions du responsable du traitement est lui-même considéré comme responsable du traitement.
[8] Voir l'avis du CEPD relatif à la communication de la Commission intitulée «Exploiter le potentiel de l'informatique en nuage en Europe», 16 novembre 2012, p. 6.

nécessaire de définir plus clairement le régime de responsabilité applicable aux clients et aux prestataires de services d'informatique en nuage, respectivement, ainsi qu'aux sous-traitants éventuels, en plus du contrat de services (comme indiqué à la section 5.1, par exemple). Cela concerne notamment le traitement des réclamations/demandes des personnes concernées (5.8). **Par conséquent, l'annexe C devrait préciser quels aspects du traitement sont gérés par le prestataire de services d'informatique en nuage, en tant que responsable du traitement, responsable conjoint du traitement ou sous-traitant, et donner des informations sur la répartition des responsabilités entre le prestataire de services d'informatique en nuage et son client.**

En outre, l'article 77 du futur règlement général sur la protection des données envisage une présomption de responsabilité conjointe du traitement et plusieurs régimes de responsabilité, au titre desquels le responsable du traitement ou le sous-traitant peut être exonéré de cette responsabilité s'il prouve que le dommage ne lui est pas imputable. Cette présomption de responsabilité peut donc être réfutée par tout acteur impliqué dans le traitement des données, sans préjudice des recours du responsable du traitement vis-à-vis du sous-traitant au cas où ce dernier n'est pas en mesure de démontrer que le dommage spécifique ne lui est pas imputable. Ce projet de cadre juridique s'accorde, en fait, avec la position adoptée par le groupe «Article 29», en particulier dans son avis sur l'informatique en nuage et le sous-traitement (document WP196, p. 11 et 12). Dans cet avis, l'accent était mis sur la nécessité de répartir clairement les responsabilités entre les différents acteurs et aussi de prévoir des garanties spécifiques à l'égard des personnes concernées. De telles garanties pourraient notamment consister dans des droits de tiers bénéficiaires sur le modèle de ceux prévus par les clauses contractuelles types appliquées aux relations entre responsable du traitement et sous-traitant.

Le groupe «Article 29» recommande de développer cette section du code, en prêtant une attention particulière au traitement des réclamations/demandes des personnes concernées (5.8) et à la coopération nécessaire entre le prestataire de services d'informatique en nuage et ses clients à cet effet.

Les dispositions du code qui prévoient des avantages spécifiques pour les personnes physiques pourraient aussi être expressément mentionnées comme étant des mesures que ces personnes peuvent faire appliquer directement, et il convient de préciser que le régime de responsabilité applicable aux parties devrait être exclusivement l'un de ceux mis en place par les États membres de l'Union.

9. Sécurité

La protection des données à caractère personnel comprend la sécurité informatique. Le groupe «Article 29» recommande de prendre cet élément en compte dans la structure et le contenu du code, où les aspects liés à la sécurité ne doivent pas être considérés comme s'ajoutant à la protection des données à caractère personnel, mais plutôt comme des composantes essentielles de cette protection.

Un sous-traitant «n'agit que sur la seule instruction du responsable du traitement» (article17, paragraphe 3) et devrait donc se cantonner dans le rôle d'un simple exécutant pour le compte du responsable du traitement, sans aucune implication dans la sémantique du traitement ni aucune marge de manœuvre pour quelque traitement ultérieur que ce soit[9]. Ce principe devrait

[9] Selon l'avis 1/2010 du groupe «Article 29» sur les notions de «responsable du traitement» et de «sous-traitant», cependant, «la délégation peut impliquer une certaine liberté d'appréciation sur la façon de servir au mieux les

se refléter dans les interfaces techniques au moyen desquelles interagissent les responsables du traitement et le prestataire de services d'informatique en nuage opérant seulement comme sous-traitant. Les rôles et les responsabilités devraient donc être clairement définis dans le code.

En outre, des mesures de sécurité et des capacités d'audit devraient être mises en place de façon à prendre en compte les particularités et les risques inhérents aux divers modèles émergents pour les services d'informatique en nuage, à savoir les modèles IaaS (Infrastructure as a service), PaaS (Platform as a service) et SaaS (Software as a service), dans lesquels un niveau de risque croissant en matière de respect de la vie privée est envisagé du fait de leurs spécificités.

Le code indique qu'*«un objectif clé de l'aspect sécurité consiste, pour le prestataire de services d'informatique en nuage, à permettre au client de procéder à une évaluation des risques en matière de sécurité et à une analyse d'impacts sur la protection des données»*. Cette condition est en effet nécessaire pour que le responsable du traitement (le client) puisse mettre en place des mesures permettant d'assurer un niveau de sécurité qui, conformément à l'article 17 de la directive, doit être *«approprié au regard des risques présentés par le traitement et de la nature des données à protéger»*.

À cet effet, il est fondamental que le prestataire de services d'informatique en nuage communique au client *«un niveau de détail suffisant concernant les mesures de sécurité déployées par le prestataire de services d'informatique en nuage»*. Cela devrait cependant être complété par un **niveau d'information suffisant sur les menaces auxquelles sont exposés le service et l'infrastructure du prestataire, sur leurs vulnérabilités et sur les décisions de gestion des risques prises par le prestataire.** Si ce n'est pas le cas, le client ne sera pas en mesure d'assurer sa propre gestion des risques en matière de protection des données dans un contexte adéquat. Néanmoins, la communication de ces informations devrait s'effectuer en tenant compte des impératifs de confidentialité du prestataire de services d'informatique en nuage pour des raisons de sécurité et de secret des affaires.

Le code lui impose aussi une obligation de procéder à une évaluation des risques *«afin de garantir à la personne concernée le droit à la protection de ses données à caractère personnel»*. **Le prestataire de services d'informatique en nuage devrait envisager d'établir différents niveaux de protection selon *«le traitement et [...] la nature des données à protéger»* et de les annoncer publiquement en proposant ses services.** Cela réduirait le caractère parfois insuffisant des informations fournies par le prestataire de services d'informatique en nuage à ses clients potentiels sur les menaces, les vulnérabilités et la gestion des risques en général.

Le groupe «Article 29» prend acte et se félicite de l'existence d'un ensemble d'objectifs de sécurité minimaux. Cependant, ceux-ci sont formulés en termes généraux et, en cas d'auto-évaluation, ils risquent donc de ne pas offrir de garanties suffisantes d'une gestion fiable de la sécurité. Ces objectifs et leur formulation pourraient être mieux alignés sur ceux énumérés dans les normes et les meilleures pratiques existantes en matière de sécurité. Par exemple, même si le code prévoit une approche de gestion des risques, il n'existe pas d'objectif de sécurité clair qui s'y rapporte. Le groupe «Article 29» recommande en outre d'inscrire ces objectifs de sécurité dans le contexte d'un ensemble plus vaste d'objectifs de protection des données.

---

intérêts du responsable du traitement, permettant au sous-traitant de choisir les moyens techniques et d'organisation les plus appropriés».

Des «clés de démonstration» sont considérées comme une alternative possible, qui n'est cependant pas équivalente et dont le niveau d'assurance est différent. Par exemple, la section 6.1 indique que le *«prestataire de services d'informatique en nuage précisera les mesures techniques, matérielles et organisationnelles en place pour protéger les données à caractère personnel contre toute destruction accidentelle ou illicite, perte accidentelle, altération, utilisation non autorisée, modification, divulgation ou accès et contre toute autre forme de traitement illicite»*. Ces informations ne figurent pas nécessairement dans *«une copie du certificat ou une attestation démontrant qu'un audit a été effectué par un tiers indépendant avec des résultats satisfaisants»*.

Enfin, le groupe «Article 29» tient à insister sur le fait que la norme ISO/IEC 27018 constitue un catalogue des meilleures pratiques pour les prestataires de services d'informatique en nuage agissant comme sous-traitants. Elle contient une liste de contrôles susceptibles d'améliorer le respect de la vie privée. Cette norme présente seulement un bon ensemble de contrôles non obligatoires, non exhaustifs et non maximalistes qui peuvent être mis en place. Par conséquent, la norme ISO/IEC 27018 n'est pas censée servir à des fins de certification en tant que document autonome. Elle peut être utilisée conjointement avec la norme ISO/IEC 27001, qui permet une certification. La norme ISO/IEC 27001 ne tient pas compte des spécificités de la protection de la vie privée, comme les incidences pour les personnes physiques, mais elle garantit un niveau élevé de protection des informations dans l'intérêt des organisations. L'ajout de bonnes pratiques fondées sur la norme ISO/IEC 27018 peut donc contribuer à faire en sorte que le respect de la vie privée soit mieux pris en considération, mais cela ne prouve pas qu'il ait été tenu compte des risques pour le respect de la vie privée. Idéalement, la norme ISO/IEC 27018 ne devrait être utilisée qu'après une évaluation des risques pour la vie privée des personnes concernées, afin d'y répondre de manière proportionnée. Aucune norme publiée à ce jour ne décrit la façon de procéder. Les travaux en cours à l'ISO pourront contribuer à combler cette lacune dans les prochaines années.

10. Droit d'audit

En principe, ce droit d'audit devrait être généralement garanti et non strictement limité au cas où le prestataire de services d'informatique en nuage n'a pas été certifié par un organisme indépendant. En effet, la directive 95/46/CE dispose que:

- le responsable du traitement doit veiller au respect de toutes exigences de qualité des données énoncées à l'article 6, paragraphe 1 (article 6, paragraphe 2),

- le sous-traitant n'agit que sur la seule instruction du responsable du traitement (article 16 et article 17, paragraphe 3).

Le devoir de supervision qui incombe au responsable du traitement sous-tend le droit qui lui est accordé d'exercer correctement son contrôle sur les activités mises en place par le sous-traitant. Ce droit devrait être exercé par tout responsable du traitement, quels que soient son pouvoir économique, ses compétences ou ses capacités techniques.

Il s'ensuit que la condition préalable d'une surveillance effective de la façon dont les données sont traitées par le prestataire de services d'informatique en nuage réside dans le respect, par le secteur concerné, d'un certain nombre d'indicateurs de performance clés relatifs à son activité. Un responsable du traitement est effectivement en mesure de rendre des comptes s'il peut démontrer de manière mesurable qu'il a satisfait à ses obligations de protection des données au regard du droit de l'Union. L'obligation de rendre des comptes qui incombe au

responsable du traitement ne peut être correctement remplie si elle n'est pas liée à la possibilité d'évaluer selon des critères mesurables le traitement mis en place par le prestataire de services d'informatique en nuage sur la base des instructions reçues du responsable du traitement (surtout s'il existe un déséquilibre important entre les deux).

Le droit d'audit peut dès lors être institué de façon à couvrir diverses phases du traitement et à tenir compte des spécificités des risques associés au traitement ou à la nature des données. Il peut englober le droit d'inspecter les locaux où sont situés les serveurs sur lesquels les données sont traitées et stockées, le droit de vérifier le code (les algorithmes) utilisé au cours des diverses étapes envisagées pour l'ensemble du traitement et le droit de contrôler les mesures de sécurité mises en place par le sous-traitant.

Le groupe «Article 29» accueille favorablement l'application de normes à l'informatique en nuage, en particulier en ce qui concerne l'interopérabilité, la portabilité et la sécurité des données, et il encourage le secteur à adopter, comme condition préalable à l'adhésion au code, des solutions acceptées à l'échelle internationale dans ces domaines. Tous les efforts possibles devraient aussi être consentis pour mettre en place des interfaces entre les systèmes des sous-traitants et l'application du responsable du traitement, de façon à faciliter la bonne utilisation des capacités d'audit prévues par les prestataires de services d'informatique en nuage.

Ces possibilités devraient transparaître clairement dans le code, à travers des cas d'utilisation où sont définis les rôles et les responsabilités, ainsi que les capacités d'audit que les prestataires mettront à disposition.

11. Droits de l'utilisateur

Actuellement, la plupart des prestataires de services d'informatique en nuage n'utilisent pas de formats de données ni d'interfaces de service standardisés facilitant l'interopérabilité et la portabilité entre différents prestataires. Si un client décide de migrer d'un prestataire à un autre, ce manque d'interopérabilité peut rendre impossible, ou pour le moins difficile, le transfert des données (à caractère personnel) du client au nouveau prestataire de services d'informatique en nuage[10]. Il en va de même des services que le client a développés sur une plateforme offerte par le premier prestataire (PaaS).

Bien que la section 5.8 du code prévoie une coopération de bonne foi du prestataire de services d'informatique en nuage afin de protéger les droits de la personne concernée, ces droits sont simplement énumérés comme étant: le droit d'accéder à ses données à caractère personnel, celui de les faire corriger et celui de les faire supprimer de manière diligente et efficace. L'unique mention relative à la portabilité des données figure actuellement dans le formulaire de transparence en annexe A. Dès lors que le code vise à contribuer à «anticiper la réforme de la protection des données», **une référence à la portabilité contribuerait à assurer la durabilité du code.**

Enfin, en ce qui concerne la relation avec la personne concernée, le groupe «Article 29» attire l'attention du C-SIG sur l'article 10 de la directive 95/46/CE[11].

---

[10] C'est ce qu'on appelle aussi la dépendance vis-à-vis du fournisseur.

[11] *«Les États membres prévoient que le responsable du traitement ou son représentant doit fournir à la personne auprès de laquelle il collecte des données la concernant au moins les informations énumérées ci-dessous, sauf si la personne en est déjà informée:*
a) l'identité du responsable du traitement et, le cas échéant, de son représentant;

Par conséquent, **il serait souhaitable d'ajouter au code une clause qui rappellerait clairement aux prestataires de services d'informatique en nuage qu'il leur appartient, selon le contexte, de fournir des informations adéquates à la personne concernée ou de coopérer de bonne foi avec leur client pour lui permettre d'informer correctement les personnes concernées.**

12. Conclusion

Le groupe «Article 29» se félicite des progrès accomplis par le C-SIG dans l'élaboration du code et l'encourage à poursuivre ses efforts pour finaliser le code en tenant compte des observations formulées dans le présent avis et dans les échanges de correspondance préalables.

Le groupe «Article 29» reconnaît qu'un tel code peut apporter une valeur ajoutée au secteur de l'informatique en nuage et qu'il aide le responsable du traitement des données à évaluer un prestataire, un produit ou un service d'informatique en nuage en particulier. Toutefois, dans sa forme actuelle, il présente encore certaines lacunes importantes auxquelles il convient de remédier pour finaliser le code.

Le groupe «Article 29» recommande donc au C-SIG d'envisager d'intégrer chacune de ses observations et recommandations dans une version finale du code.

---

b) les finalités du traitement auquel les données sont destinées;
c) toute information supplémentaire telle que:
- les destinataires ou les catégories de destinataires des données,
- le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse,
- l'existence d'un droit d'accès aux données la concernant et de rectification de ces données,
dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.»