NÉGOCIATION DES CONDITIONS RELATIVES À LA SÉCURITÉ DES DONNÉES ET À LA VIE PRIVÉE NUMÉRIQUE : OBSERVATIONS D'UN AVOCAT SPÉCIALISÉ DANS LES CONTRATS

Je suis le principal avocat d'affaires d'une grande organisation dont les programmes de communication en ligne s'appuient sur des douzaines de fournisseurs de matériel, de logiciels et de services de communications. Cette organisation attache également une grande importance à la vie privée numérique. Je passe donc beaucoup de temps à travailler avec des vendeurs, notamment lors des négociations contractuelles, pour apporter la meilleure protection possible à cette vie privée. Les observations ci-après synthétisent les points clés et défis majeurs auxquels j'essaie de faire attention lors de ces négociations.

Par Me Eric Vieland

1. GARDEZ LES YEUX OUVERTS : LA VIE PRIVÉE NUMÉRIQUE ET LA SÉCURITÉ DES DONNÉES PEUVENT ÊTRE EN JEU DANS UN GRAND NOMBRE DE CONTRATS

Si les questions de vie privée numérique et de sécurité des données ne se posent pas encore dans tous les contrats de vente de biens ou de services, elles se posent assez souvent pour inciter un avocat prudent à les étudier systématiquement. Cela étant dit, certaines catégories de contrats soulèvent forcément ces questions.

- **Services et plateformes de communications.** Tout produit, service ou site connectant des personnes (ou leurs appareils) par voie électronique doit assurer la confidentialité et la sécurité des données transmises et/ou stockées.
- **Sites de commerce électronique.** Tout service facilitant des transactions financières numériques soulève des questions similaires, mais il est probablement soumis à un fardeau réglementaire additionnel.
- **Publicité en ligne.** Lorsque vous diffusez une publicité en ligne visant des audiences sélectionnées selon certains critères de ciblage, vous souhaitez sûrement savoir que le vendeur a obtenu les données de ciblage d'une façon acceptable. De plus, lorsqu'un individu ciblé interagit de quelque façon que ce soit avec cette publicité, vous voulez sûrement savoir ce qui arrivera aux données générées par cette interaction.
- **Acquisition et partage de listes de contacts et d'autres données personnelles.** De la même façon, lorsque vous achetez des données concernant des individus, vous voulez sûrement savoir comment elles ont été obtenues. Par ailleurs, lorsque vous vendez ou échangez des données, vous avez sûrement besoin de savoir comment elles seront traitées.

Source : Guide to Negotiating Digital Privacy and Data Security Terms publié par Stanford PACS Digital Civil Society Lab sur le site Digital Impact Toolkit le 9 novembre 2015 sous licence Creative Commons Attribution 4.0 International.
Traduit en français par Gwendoline Clavé.

- **Tout produit, appareil ou service connecté.** Les systèmes achetés à des fins de transfert ou de stockage de données peuvent être assez faciles à repérer, mais il peut être plus difficile de garder une trace de tous les objets et personnes pouvant être connectés à ces systèmes. L'employé du support informatique qui vient installer un logiciel dans le bureau de votre client, l'application qui permet à votre client de recevoir des rapports sur le trafic internet sur son smartphone, le fournisseur de services tiers qui sera connecté au site Internet de votre client pour fournir une fonctionnalité particulière… Toutes ces situations (et nombre d'autres) exposent vos données à des risques qui peuvent être tout aussi sérieux et difficiles à traiter que les risques encourus dans des contextes plus évidents.

2. LA VIE PRIVÉE NUMÉRIQUE SE DIVISE EN TROIS CATÉGORIES

La vie privée numérique (contrairement à la sécurité des données, que j'aborderai plus tard) se divise en trois catégories correspondant aux différents types de personnes susceptibles de se livrer à des activités d'espionnage : le vendeur (et ses agents et partenaires), les agences gouvernementales (qui peuvent contacter ouvertement le vendeur pour obtenir des informations) et les autres, soit différents types de pirates. Chacune de ces catégories s'assortit d'un ensemble d'analyses spécifique et soulève son propre éventail de défis potentiels lors des négociations.

- **Espionnage par l'autre partie**

    - Faire promettre à l'autre partie de préserver la « confidentialité » des données ne suffit sûrement pas. Vous devriez préciser, au minimum, que cette promesse implique : (i) de n'utiliser les données qu'aux seules fins énoncées dans le contrat, (ii) de ne pas divulguer les données à quelque autre partie que ce soit, (iii) de mettre en œuvre des mesures de sécurité appropriées afin de protéger les données de toute divulgation accidentelle, et (iv) de restituer ou détruire l'ensemble des copies et des versions dérivées après la fin du contrat.

    - Certains contrats et certains professionnels emploient le langage de la « propriété » pour remplacer toutes ces notions ou certaines d'entre elles. Il peut être important de préciser que votre client possède certaines données, pour d'autres raisons, mais cela ne vous dispense pas d'exiger les promesses spécifiques susmentionnées.

    - Les détails opérationnels relatifs à la façon dont le vendeur fait son travail peuvent compliquer les promesses susmentionnées. Il a peut-être besoin d'utiliser des cookies, des relais ou d'autres appareils similaires pour gérer du trafic. Le fonctionnement du produit nécessite peut-être la préparation et le stockage de données dérivées, ou même le partage de données anonymisées à travers les comptes clients. Il existe différentes manières de s'adapter à ces contraintes, mais vous ne pouvez vous y adapter correctement que si vous comprenez les détails opérationnels.

    - Les biens et services liés aux données sont rarement autonomes ; de nombreux vendeurs ont des relations avec d'autres entreprises qui leur fournissent tout ce dont ils sont besoin, du personnel aux modules logiciels en passant par la capacité de stockage des données. Vous devez savoir qui sont toutes ces parties, vous assurer qu'elles ont toutes la volonté et la capacité de respecter les promesses du vendeur principal en matière de confidentialité et, si possible, amener le vendeur principal à garantir qu'elles s'y conformeront. Cette garantie devrait certes être implicite dans l'entente de sous-traitance, mais dans le contexte de fournisseurs technologiques « imbriqués », vous pouvez avoir de nombreuses raisons de vouloir la rendre explicite.

- **Espionnage par le(s) gouvernement(s)**

Source : Guide to Negotiating Digital Privacy and Data Security Terms publié par Stanford PACS Digital Civil Society Lab sur le site Digital Impact Toolkit le 9 novembre 2015 sous licence Creative Commons Attribution 4.0 International.
Traduit en français par Gwendoline Clavé.

- Les agences gouvernementales peuvent adresser aux vendeurs différents types de demandes visant à obtenir des informations concernant votre client ou les utilisateurs finaux de la plateforme de communication de votre client. Certaines demandes sont facultatives, d'autres obligatoires, et le vendeur peut avoir ou non le droit de parler de ces demandes à votre client, en fonction des moyens légaux spécifiques choisis par le gouvernement dans chaque situation.

- L'objectif des négociations est, par conséquent, de limiter la coopération discrétionnaire du vendeur avec le gouvernement, tout en reconnaissant les limites de cette discrétion. Typiquement, un vendeur devrait promettre : (i) de notifier toute demande de ce type à votre client lorsque la loi l'y autorise ; (ii) en cas de notification, de participer aux efforts de votre client afin d'empêcher ou de limiter toute divulgation ; et (iii) dans tous les cas, de ne divulguer quoi que ce soit que s'il y est contraint par la loi et, même dans ce cas, de ne le faire que dans la mesure requise.

- Bien que le droit fédéral américain tende à être le cadre dominant de ce type de négociation, lorsque des clients américains construisent des systèmes américains, les juridictions étrangères peuvent être importantes, non seulement si le système que vous construisez doit avoir des composants internationaux, mais aussi lorsque les utilisateurs sont tous américains si vous utilisez un fournisseur avec des centres de données ou d'autres opérations à l'étranger. Certains vendeurs donnent à votre client la possibilité de conserver l'ensemble des données aux États-Unis, ce qui peut être avantageux.

- **Espionnage par des pirates**

  - On ne peut pas normalement attendre du vendeur qu'il fournisse une garantie absolue contre le piratage, mais votre client devrait obtenir des garanties raisonnables concernant les mesures de sécurité du vendeur et sa vigilance continue. La nature exacte de ces garanties dépendra en grande partie des forces et faiblesses inhérentes aux technologies employées ; ce domaine illustre donc la nécessité d'une bonne rédaction précédée d'une bonne analyse technologique.

  - Si l'on s'attend à ce que le vendeur fournisse des services pendant une longue période, ou si le vendeur doit stocker des données critiques de son côté, il peut être approprié que votre client (probablement par l'intermédiaire d'un fournisseur de services de sécurité distinct) participe activement et continuellement à la vigilance en matière de sécurité. À nouveau, les détails doivent découler de l'analyse technologique, mais ici, l'avocat peut jouer un rôle plus actif, en demandant à l'expert en technologie s'il serait utile (et raisonnable compte tenu des circonstances) de demander des mesures telles que des audits de sécurité indépendants réguliers des installations du vendeur dédiées aux données, ou de demander à être tenu au courant des changements concernant l'architecture des données du vendeur.

  - Le vendeur devrait être tenu de notifier rapidement à votre client toute atteinte à la sécurité (voire de prendre des mesures précises pour y remédier). Le problème est qu'une « atteinte à la sécurité » peut en fait désigner plusieurs risques différents, et il peut être très difficile pour le vendeur d'identifier certains de ces risques dans certaines situations. Le vendeur saura-t-il s'il y a eu un accès à des données ? Qu'en est-il d'une tentative ratée d'accéder à des données ? Et si une mesure de sécurité venait à échouer, de sorte à ce que les données soient relativement exposées, même s'il n'y avait aucune tentative d'exploiter cette vulnérabilité ? Le vendeur devrait accepter de partager tout ce qu'il sait à ces égards, et votre client devrait tenir compte des problèmes pouvant survenir lorsque ce type d'information n'est pas disponible.

Source : Guide to Negotiating Digital Privacy and Data Security Terms publié par Stanford PACS Digital Civil Society Lab sur le site Digital Impact Toolkit le 9 novembre 2015 sous licence Creative Commons Attribution 4.0 International.
Traduit en français par Gwendoline Clavé.

- Si vous avez négocié des garanties ou normes précises en matière de sécurité à l'encontre de l'espionnage par des tiers, assurez-vous qu'aucune autre section du contrat, comme la clause de force majeure, n'interfère avec les devoirs du vendeur relatifs aux actions des tiers.

3. LA VIE PRIVÉE PEUT S'ENTREMÊLER AVEC D'AUTRES ASPECTS IMPORTANTS DE LA SÉCURITÉ DES DONNÉES

En plus de la confidentialité des données des utilisateurs, la vie privée numérique et la sécurité des données peuvent impliquer d'autres sujets connexes qui devraient faire l'objet de négociations en parallèle. Ces autres sujets peuvent être moins susceptibles de revêtir une importance critique dans toute entente commerciale, mais lorsque cela se produit, ils peuvent également nécessiter leurs propres séries d'analyses et discussions.

- Si la disparition de données peut nuire à quelqu'un, le vendeur devrait montrer, et garantir, des fonctionnalités solides de protection contre la perte de données. La partie potentiellement lésée pourrait être un utilisateur final qui comptait sur la transmission ou le stockage de certaines données ou, plus communément, votre client, qui doit savoir que la base de données entière sera disponible pour assurer la continuité de son activité actuelle ou pour servir de base à une activité subséquente.

- Dans certains cas, il peut être crucial de se prémunir contre toute corruption de données, par exemple dans certaines situations où les fichiers de données font l'objet de fusions ou de superpositions. Le vendeur devrait être en mesure de faire des déclarations appropriées concernant l'intégrité des données.

- Avoir de très bons moyens d'authentifier la source d'un message est parfois crucial. Quant à savoir si vous avez besoin de promesses précises concernant la technologie d'authentification, ce sera le cas si vous permettez à vos utilisateurs d'effectuer des transactions monétaires, mais également dans d'autres situations dans lesquelles une erreur d'identité (qu'elle soit ou non frauduleuse) pourrait avoir des conséquences néfastes.

- Enfin, si les utilisateurs s'attendent à être anonymes, une autre série de discussions est nécessaire, puisque la protection de l'anonymat peut nécessiter un nouvel ensemble d'outils, de normes ou de stratégies en matière de gestion des données.

4. COMPRENDRE LES LIMITES DE CE QUE VOUS POUVEZ FOURNIR À VOTRE CLIENT AU MOYEN D'UN RECOURS CONTRACTUEL

Si difficile soit-il de déterminer de quelles mesures de sécurité et de confidentialité votre client a besoin, et quelles mesures le vendeur veut et peut fournir, il peut être encore plus difficile de relier ces promesses à des recours contractuels sérieux. Les facteurs suivants, ensemble ou séparément, peuvent contribuer à ce problème lors de toute négociation.

- Il peut être très difficile d'associer des valeurs monétaires aux préjudices tels que l'atteinte à la vie privée ou la perte de données. Il y a cependant une exception : si le préjudice implique une atteinte à la sécurité sujette à des règles fédérales ou étatiques relatives à la notification

Source : Guide to Negotiating Digital Privacy and Data Security Terms publié par Stanford PACS Digital Civil Society Lab sur le site Digital Impact Toolkit le 9 novembre 2015 sous licence Creative Commons Attribution 4.0 International.
Traduit en français par Gwendoline Clavé.

obligatoire des consommateurs ou à d'autres recours connexes, il peut être relativement aisé de calculer les coûts associés à cette notification ou à ces recours. Cependant, même dans ce cas, le calcul peut constituer une piètre mesure des dégâts subis par les utilisateurs finaux ou par l'entreprise de votre client.

- Les vendeurs chercheront systématiquement à exclure leur responsabilité en cas de dégâts indirects et consécutifs. Mais dans ce domaine, presque tous les dégâts sont indirects ou consécutifs, en supposant que ces conditions s'appliquent dans le contexte du traitement des données. Assurez-vous de faire préciser dans le contrat les formes de dégâts qui importent.

- Les vendeurs chercheront systématiquement à plafonner leur responsabilité à bas niveau, souvent par rapport au volume des frais payés par votre client. Même si vous avez raison de dire que ce plafonnement est inapproprié et que les risques pertinents ne peuvent être contrôlés que par le vendeur, cela ne changera rien : attendez-vous à faire face à des visages choqués et consternés lorsque vous laisserez entendre que le vendeur devrait défendre son service. Préparez-vous à être vous-même choqué et consterné en découvrant que le vendeur ne semble jamais avoir entendu parler d'assurance de responsabilité commerciale.

- Dans certains cas, une violation peut être difficile à prouver. Par exemple, si vous pouvez montrer que des données ont fuité, mais pas exactement quand ni comment, il est possible que vous soyez incapable de démontrer que la fuite constitue une violation d'une promesse spécifique faite par le vendeur.

- Nombre des dispositions que vous négocierez seront au profit d'utilisateurs (autres que votre client) exposant leurs données personnelles au vendeur. Vous devrez donc choisir une stratégie pour (i) fournir à ces utilisateurs des recours directs contre le vendeur, (ii) poursuivre le vendeur pour leur compte, ou (iii) faire en sorte que votre client dédommage les utilisateurs et se tourne ensuite vers le vendeur pour être indemnisé. Vous devrez ensuite faire en sorte que le contrat appuie cette stratégie.

- Si le vendeur met un contrat type sur la table, toute disposition relative au transfert de responsabilité est susceptible d'aller dans l'autre sens, en faisant (par exemple) assumer à votre client toute responsabilité en cas de réclamations des utilisateurs finaux à l'encontre du vendeur. Bien que cela puisse être approprié à certains égards, notamment en ce qui concerne la responsabilité du vendeur vis-à-vis des contenus fournis par votre client, cette responsabilité ne doit pas être étendue pour inclure la responsabilité en cas de mauvaise gestion des données des utilisateurs par le vendeur ou ses agents.

- Vous pouvez également voir des clauses d'arbitration ou de médiation obligatoires. Celles-ci ne sont pas appropriés dans ce type de contrat pour plusieurs raisons, mais au minimum, notez que votre client devra peut-être demander une injonction contre certaines pratiques de gestion des données et devrait préserver l'accès aux tribunaux au moins pour ce type de situation.

5. VOUS DEVREZ SOUVENT CRÉER UN CONTRAT UNIQUE RÉUNISSANT PLUSIEURS « COUCHES » POUR LES SYSTÈMES MULTIVENDEURS

Les plateformes et systèmes de communication se composent habituellement de myriades de produits et services, fournis par des vendeurs différents. Cet arrangement crée certains problèmes pour l'avocat spécialisé dans les contrats.

Source : Guide to Negotiating Digital Privacy and Data Security Terms publié par Stanford PACS Digital Civil Society Lab sur le site Digital Impact Toolkit le 9 novembre 2015 sous licence Creative Commons Attribution 4.0 International.
Traduit en français par Gwendoline Clavé.

- Dans le contexte des systèmes multivendeurs, les contrats ne peuvent aider à créer des normes sérieuses en matière de gestion des données que si vous atteignez deux objectifs : (i) mettre tous les vendeurs d'accord sur le même ensemble de normes ou presque, et (ii) définir les responsabilités respectives des vendeurs afin de vous donner des chances d'identifier précisément le responsable de tout incident prévisible lié aux données.

- Des produits et services spécifiques sont susceptibles d'avoir été inclus dans le projet en raison des capacités uniques qu'ils offrent. Mais ces capacités peuvent être solidement ancrées dans des normes ou techniques de gestion des données qui ne correspondent pas aux normes que vous essayez d'instaurer dans l'ensemble du projet. Si vous vous en rendez compte assez tôt, il peut être possible d'échanger un produit ou une stratégie contre un(e) autre ; sinon, vous risquez d'être coincé avec pour seule solution d'essayer de limiter les dégâts potentiels.

- Il arrive que certains vendeurs ne réalisent pas que leurs propres produits sont eux-mêmes de nature composite. Par exemple, un vendeur peut vous dire de bonne foi qu'il ne fait appel à aucun sous-traitant, mais si vous lui demandez précisément à quel endroit il stocke de grands volumes de données client, il peut révéler qu'il utilise un service externe de stockage dématérialisé à ces fins. Le vendeur peut considérer cela comme un simple outil, mais de votre point de vue, si ce prestataire de stockage dématérialisé ne participe pas au programme de sécurité des données du projet de votre client, vous n'avez pas atteint votre objectif. Et n'oubliez pas de demander comment le vendeur transfère et récupère les données auprès de ce prestataire de stockage dématérialisé.

6. UN PAQUET D'AUTRES PROBLÈMES

- Les prestataires spécialisés dans la technologie ou les données, et notamment les prestataires de services de stockage dématérialisé, adorent généralement les contrats à parcourir en cliquant qui n'existent que sous la forme de combinaisons de pages en ligne liées à un bouton « J'accepte ». De plus en plus souvent, les vendeurs pensent que ce format est également approprié aux contrats d'entreprises, et (étonnamment) aux contrats dont les conditions ont fait l'objet de négociations significatives. D'importants volumes de documents justificatifs, y compris de conditions générales cruciales, peuvent être incorporés par le biais de liens. De nombreux documents liés peuvent indiquer que le vendeur est libre de les modifier de temps à autres. Certains vendeurs aideront à trouver une solution de rechange s'ils sont poussés à le faire, mais vous pouvez parfois avoir du mal à démontrer avec exactitude ce qui a été convenu. Votre dernier recours peut être d'imprimer une « preuve du contrat » comprenant des captures d'écran datées de l'ensemble des documents en ligne pertinents et, avec un peu de chance, une déclaration du vendeur indiquant qu'un contrat a été établi à cette date.

- Les clients qui accordent une grande importance à la vie privée peuvent également accorder une grande importance à la liberté d'expression. De la même façon, les vendeurs désinvoltes à l'égard de la vie privée peuvent également être désinvoltes à l'égard de la liberté d'expression. Par conséquent, si vos négociations portent sur l'un de ces sujets, elles peuvent très bien porter également sur l'autre. Une attitude désinvolte à l'égard de la liberté d'expression est susceptible de se refléter dans la « politique d'utilisation acceptable » du vendeur, dans laquelle le vendeur peut se réserver le droit de surveiller les communications et d'exclure les utilisateurs sur la base de contenus « offensants », « inappropriés » ou de nombreux autres critères. De nombreux vendeurs interdisent les communications qui « soutiennent le terrorisme », sans la moindre précision quant à la signification de ce critère. À tous ces égards, le vendeur a un intérêt légitime à faire promettre à votre client de ne pas commettre ou permettre sciemment toutes communications illégales, mais aucun intérêt légitime à aller plus loin. La décision de se battre à ce sujet relève principalement d'un jugement personnel et ne fait pas partie des aspects traités

Source : Guide to Negotiating Digital Privacy and Data Security Terms publié par Stanford PACS Digital Civil Society Lab sur le site Digital Impact Toolkit le 9 novembre 2015 sous licence Creative Commons Attribution 4.0 International.
Traduit en français par Gwendoline Clavé.

dans ce guide. Cependant, notez que le droit d'un vendeur de surveiller ou de s'immiscer dans les communications, caché dans une disposition sur l'utilisation acceptable, peut amoindrir les promesses faites ailleurs par le vendeur concernant le respect de la vie privée des utilisateurs.

- Si votre client construit une plateforme de communication de quelque type que ce soit, ou même s'il se contente d'apposer sa marque sur une version d'une plateforme construite par d'autres, le client voudra probablement rédiger et publier une politique de confidentialité, et peut-être d'autres conditions d'utilisation de la plateforme affectant la gestion des données. L'une de vos missions consiste à vous assurer que l'ensemble des vendeurs fournissant des éléments de cette plateforme ont la volonté et la capacité de respecter la politique publiée. Une autre de vos missions consiste à vous assurer que votre client comprend que les listes de contacts accumulées en vertu d'une politique publiée peuvent effectivement être associées de façon permanente à cette politique. En d'autres termes, une fois que vous avez recueilli le nom et l'adresse e-mail d'une personne en vertu d'une politique de confidentialité très protectrice, vous pouvez rencontrer des difficultés à utiliser ces données de contact dans des contextes nouveaux et en évolution, du moins sans violer ce qui constitue un ensemble permanent de promesses envers cette personne.

- Des générations de contrats liés aux données ont déjà été rédigées en employant le terme « Informations personnelles identifiantes » (IPI) pour décrire des données comme les noms, numéros de cartes bancaires et de sécurité sociale, et dessiner une clôture protectrice autour de ce type de données spécifique. Avec cette approche, d'autres informations que l'on ne peut pas identifier intuitivement comme appartenant à un individu peuvent être librement exploitées (par exemple, la piste anonymisée d'un utilisateur passant par une série de pages web d'une façon spécifique, ou un enregistrement indiquant qu'une personne a regardé une publicité pour un certain produit dans une certaine gare). Si cette approche IPI / pas IPI a pu être appropriée à une époque, elle ne l'est plus aujourd'hui. Les analyses de données modernes peuvent rétroconcevoir l'identification personnelle, ou au moins les adresses d'appareils spécifiques, à partir de points de données qui étaient autrefois considérés avec certitude comme inoffensifs. Pour protéger les utilisateurs, il faut désormais regarder l'ensemble des données générées par leurs interactions avec la plateforme ou le service de votre client ou recueillies en lien avec ceux-ci.

7. SOYEZ PRÊT À AJUSTER VOS ATTENTES CONCERNANT VOTRE RÔLE D'AVOCAT

- Dans d'autres contextes commerciaux, les avocats peuvent souvent effectuer un travail convenable lors des négociations contractuelles en travaillant seuls, même sans une maîtrise technique complète de l'activité de leur client et des produits du vendeur ; ils peuvent passer outre le manque de connaissances grâce à des promesses contractuelles privilégiant les résultats ou suffisamment vagues pour passer sur les divers détails opérationnels. Les recours consistant tout simplement à indemniser le client si quelque chose ne fonctionne pas sont des outils très prisés. Cependant, dans le contexte des systèmes d'information, cette stratégie n'est habituellement pas viable, pour de multiples raisons. Puisque ces contrats concernent principalement l'assemblage de produits et de protocoles visant à créer un environnement sécurisé, et puisque les recours qu'ils fournissent en cas de manquement ne constituent qu'une deuxième ligne de défense distante et poreuse, un avocat peut faire plus de mal que de bien s'il s'appuie sur des stratégies de négociation basées sur les résultats, en particulier s'il ne fait pas part des limites de son expertise. Travaillez avec un expert en technologie qui peut vous dire précisément : (i) où se trouvent les vulnérabilités, (ii) à quels niveaux le vendeur doit accepter de prendre des mesures spécifiques et non standard concernant la gestion des

Source : Guide to Negotiating Digital Privacy and Data Security Terms publié par Stanford PACS Digital Civil Society Lab sur le site Digital Impact Toolkit le 9 novembre 2015 sous licence Creative Commons Attribution 4.0 International.
Traduit en français par Gwendoline Clavé.

données et (iii) dans quels cas les systèmes conçus peuvent être considérés avec certitude comme sûrs. Idéalement, cet expert en technologie est le concepteur du système de votre client.

- Si vous pouvez avoir besoin de faire appel à un expert en technologie pour vous aider à comprendre les limites des produits du vendeur en matière de conception et de performance, vous pouvez tout de même comprendre le modèle commercial du vendeur. Comme dans toute négociation, comprendre le modèle commercial de l'autre partie est crucial pour comprendre sur quels points il y a matière à faire des compromis. Les vendeurs de systèmes d'information, du plus petit au plus grand, ont souvent des stratégies commerciales particulièrement étroites et arrêtées ; ils n'ont ciblé qu'une seule manière de placer un produit dans une seule niche, et c'est comme ça. Donnez-vous comme priorité de savoir si vous vous trouvez dans cette situation et, le cas échéant, ce que cela implique pour les négociations.

- Si vous additionnez toutes les bizarreries évoquées ci-dessus, vous verrez qu'un avocat doit être prêt à renoncer à la plupart de ses missions habituelles lors des négociations commerciales. Nous essayons habituellement d'identifier les risques, de les éliminer lorsque cela est possible, et de reporter la responsabilité pour ceux-ci sur l'autre partie dans le cas contraire. Mais quand votre client achète des produits présentant des risques intrinsèques (et, en général, les groupe ensemble), en particulier quand il n'existe aucun recours contractuel garantissant que tout le monde sera indemnisé dans le pire des cas, l'avocat peut devoir accepter que le document sur la table au terme du processus de négociation puisse ne pas apporter les types de protection dont il aime normalement faire profiter ses clients.

- D'un autre côté, si l'avocat rejoint la table des négociations assez tôt, alors que le client (ou le concepteur du système du client) réfléchit encore aux produits et stratégies, l'avocat peut jouer un rôle crucial dans l'identification et le rassemblement de prestataires dont les produits et services sont adaptés aux objectifs du client.

- L'avocat joue également un rôle crucial en conseillant le client quant aux limites des contrats dans le contexte des systèmes d'information. Ce rôle consiste souvent à faire en sorte que le client revoie ses attentes à la baisse en ce qui concerne l'utilité du contrat en cas de violation de données et à la hausse vis-à-vis d'une sécurité sérieuse, en concentrant ses efforts sur les mesures pratiques spécifiques que peut fournir l'expert en technologie. Ces mesures peuvent par exemple inclure : (i) des environnements de chiffrement contrôlés par le client, (ii) des analyses des systèmes d'exploitation des vendeurs et (iii) la séparation des flux de données visant à ne faire circuler des données sensibles que lorsque cela est nécessaire. Le processus de négociation contractuelle peut être une occasion d'aider à déterminer quand et pourquoi ces types de mesures peuvent être importants.

- Enfin, l'avocat peut jouer un rôle crucial en fournissant des versions préliminaires claires et précises des documents contractuels ainsi que des notifications et politiques destinées aux utilisateurs finaux. S'agissant des risques en matière de sécurité des données et de vie privée numérique, le consentement éclairé est un concept essentiel, aussi bien pour votre client, qui conclut des accords concernant des systèmes d'information, que pour les utilisateurs finaux, qui divulguent des informations à ces systèmes. Lorsque vous ne pouvez pas réduire les risques ou les reporter sur quelqu'un d'autre, vous pouvez au moins vous assurer que ceux qui assument ces risques ont la meilleure chance possible de comprendre ce qu'ils font.

Eric Vieland est Avocat-conseil en entreprise et Responsable de la gestion des risques de l'Union américaine pour les libertés civiles (ACLU). Cependant, les observations ci-dessus ne reflètent que ses pensées personnelles, et non une quelconque politique ou activité de l'ACLU. Bien entendu, les observations ci-dessus peuvent être incomplètes ou erronées dans le cadre de négociations particulières. Elles ne constituent pas des conseils juridiques et ne doivent pas être prises comme tels.

Source : Guide to Negotiating Digital Privacy and Data Security Terms publié par Stanford PACS Digital Civil Society Lab sur le site Digital Impact Toolkit le 9 novembre 2015 sous licence Creative Commons Attribution 4.0 International.
Traduit en français par Gwendoline Clavé.