EXPERTISES
DES SYSTÈMES D'INFORMATION

Cybersécurité
Le risque, le nouveau concept clef du RGPD et de NIS

La notion de risque est citée à 78 reprises dans le RGPD et à 39 reprises dans la directive NIS prenant ainsi en compte le fait qu'il n'existe pas de risque zéro et que la sécurité des systèmes d'information doit être organisée. Les deux textes nous éclairent aussi sur les méthodes susceptibles de limiter la survenance des risques et de les minimiser.

Les cyberattaques sont aujourd'hui devenues monnaie courante. Dès lors, nous pouvons nous demander si cela n'est pas la preuve éclatante de ce que les sociétés considèrent désormais qu'une bonne politique de cybersécurité est celle qui accepte le potentiel échec face à la cyberattaque.

A l'ère d'internet et du big data, le risque est omniprésent

En droit civil, le risque désigne généralement un « *événement éventuel, incertain, dont la réalisation ne dépend pas exclusivement de la volonté des parties et pouvant causer un dommage* »[1]. Toutefois, cette notion n'est pas un terme intrinsèquement juridique, les enjeux sont aussi économiques, techniques, individuels et collectifs.

À l'ère du big data, de l'intelligence artificielle et des objets connectés, les données s'amassent et circulent, le risque est bel et bien devenu omniprésent : fuite de données, piratage, ransonware, faille informatique, etc.

On le trouve cité à 78 reprises dans le Règlement général sur la protection des données - RGPD (Règlement UE n° 2016/679 du 27 avril 2016), et à 39 reprises dans la Directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union - NIS (Directive UE n° 2016/1148 du 6 juillet 2016), deux textes qui seront applicables en mai 2018.

Cette directive NIS définit le risque comme étant « *toute circonstance ou tout événement raisonnablement identifiable ayant un impact négatif potentiel sur la sécurité des réseaux et des systèmes d'information* ». Le risque, une fois réalisé, devient un incident qui a un impact négatif réel sur la sécurité des réseaux et des systèmes d'information.

Aujourd'hui, le constat est double : (i) le risque zéro n'existe pas et les entreprises doivent apprendre à faire avec, (ii) assurer la sécurité des systèmes d'information consiste à optimiser leur capacité à résister aux actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données et des services associés.

La Cnil (Commission nationale de l'informatique et des libertés) a récemment mis en demeure une société commercialisant deux jouets connectés, car il a été constaté que tout dispositif bluetooth pouvait détecter les jouets allumés, écouter à distances les conversations captées par le microphone des jouets, les enregistrer, et communiquer avec les enfants via les jouets, sans aucune authentification. Cette absence de sécurisation porte atteinte à la vie privée des personnes, cela d'autant plus qu'elle touche un public vulnérable. La Cnil liste alors les différentes mesures de remédiation à prendre pour éviter ces risques : sécurisation du dispositif de communication bluetooth, chiffrement du canal de communication lors du transfert des données, information complète sur le traitement de données (mise en demeure Cnil n° 2017-073 du 20 novembre 2017[2]).

Accepter les risques, les anticiper, les minimiser et les gérer

La lecture des deux règlementations européennes précitées nous éclaire sur les méthodes susceptibles de limiter au maximum la survenance des risques potentiels, et de minimiser les conséquences dommageables des incidents survenus.

Les risques sont multiples, évolutifs, et les hackers ont bien souvent un temps d'avance. C'est pourquoi, appréhender les risques pour l'entreprise comme pour les personnes physiques, nécessite tout d'abord de les cartographier, selon leur degré de probabilité et de gravité.

Par exemple, cette évaluation peut dépendre de la quantité de données traitées, de leur provenance, du nombre de personnes habilitées à y accéder, du caractère particulier / sensible des données. En effet, le traitement des données sensibles[3] est par principe interdit, sauf exceptions limitatives, telles que le consentement explicite ou la sauvegarde des intérêts vitaux (article 9 du RGPD).

Cette phase de cartographie permettra ensuite d'adapter les mesures de sécurité à mettre en Suvre et à documenter, en fonction des risques identifiés. Ainsi, anonymiser les données implique de rendre impossible une ré-identification des personnes physiques concernées, les données ne sont donc plus personnelles. En outre, pseudonymiser ou chiffrer les données personnelles permet de rendre plus difficilement identifiables les personnes concernées ; et assurer la suppression de données personnelles, dès que possible, réduit la quantité de données compromises en cas d'incident. Enfin, en présence d'un risque élevé pour les droits et libertés des personnes physiques, en dépit des précautions prises, les responsables de traitements de données personnelles devront mener une analyse d'impact préalable (article 35 du RGPD). Dans ses guidelines, le groupe de travail G29 a établi une liste de neuf critères à prendre en compte pour déterminer si une analyse d'impact s'avère nécessaire, en particulier : en cas de profilage, de surveillance systématique, de traitement de données sensibles ou à grande échelle, de croisement de données, ou encore, dans l'hypothèse d'une utilisation innovante ou impliquant une solution technologique nouvelle, telle que l'internet des objets[4].

Il faut donc aujourd'hui repenser les cycles de vie des données dans un souci perpétuel et continu de proportionnalité, afin que seules les données nécessaires à la finalité du traitement envisagé soient traitées.

Pour être efficace, la gestion des risques requiert, d'une part, une réelle collaboration entre le service juridique, le responsable de la sécurité des systèmes d'information et le délégué à la protection des données éventuellement désigné, et d'autre part, une formation continue des employés ainsi qu'une sensibilisation des personnes physiques, car en réalité, tout le monde est concerné.

Une obligation de transparence, pour pouvoir tirer les leçons des incidents notifiés

En matière de droit de la propriété industrielle, les demandes de brevet sont toutes publiées au Bulletin officiel de la propriété industrielle par l'Inpi. Dès lors, si le brevet permet à son titulaire de bénéficier d'un monopole d'exploitation sur l'invention brevetée, la publication du brevet permet de rendre publique l'évolution de l'état de la technique. Cela évite d'effectuer des recherches, alors que la solution technique à un problème spécifique a déjà été trouvée via l'invention brevetée.

Cette logique d'équilibre entre la protection des intérêts propres à l'inventeur et ceux de l'intérêt général, se retrouve également en matière de sécurité et de protection des données à caractère personnel.

En effet, en cas de violation de données à caractère personnel, le responsable du traitement doit notifier cette violation à la Cnil dans les 72 heures de sa connaissance (article 33 du RGPD). Cela implique d'être réactif et de pouvoir, très rapidement, décrire la nature de la violation, les conséquences probables, et les mesures de remédiation prises. Dans certaines circonstances, la violation doit par ailleurs être communiquée aux personnes physiques concernées (article 34 du RGPD).

Les opérateurs de services essentiels (énergie, transport, banque, service DNS&) comme les les fournisseurs de services numériques (places de marché en ligne, moteurs de recherches, services d'informatique en nuage) doivent également notifier tout incident ayant un impact significatif sur les services fournis, et en évaluer l'ampleur (articles 14 et 16 de la Directive NIS).

La Cnil et l'Anssi (Agence nationale de la sécurité des systèmes d'informations) ont notamment pour mission de formuler des recommandations et bonnes pratiques. Le fait qu'elles reçoivent les notifications d'incidents leur permet d'avoir une approche plus concrète des marchés, des évolutions technologiques, des enjeux et risques en présence.

Cette mise en balance est présente à différents niveaux, et explique par exemple qu'un traitement de données puisse être fondé sur les intérêts légitimes du responsable de traitement ou d'un tiers, tels que la prévention de la fraude, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux des personnes concernées.

On n'arrête pas le progrès, les avancées technologiques sont en marche et reflètent l'évolution de notre société qui est de plus en plus connectée. Il n'est pas question de les stopper, mais plutôt d'adopter le réflexe sécurité et protection des données personnelles, tant pour les entreprises proposant des produits et services innovants, que pour les personnes les utilisant.

Comme disait Jean de la Fontaine, « *Deux sûretés valent mieux qu'une, Et le trop en cela ne fut jamais perdu* » (Fable : Le Loup, la Chèvre et le Chevreau).

Clara PETIT
Avocate ITEANU Avocats
Membre du Clusif et de son groupe de travail sur la synergie entre RSSI et DPO

Notes

(1) *Lexique des termes juridiques 2017-2018 DALLOZ, page 1010*

(2) *https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000036142140&fastReqId=606052286&fastPos=2*

(3) *Les catégories particulières de données sont celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique*

(4) *Les guidelines du G29 : http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083*