Conformité et sécurité : un cran au-dessus ?

François COUPEZ
Avocat à la Cour
Senior Advisor du CyberCercle
Fondateur de Level Up Legal

Sécurité des systèmes d'information et conformité, notamment en matière de protection des données, sont deux concepts qui sont fortement liés à l'heure actuelle, que ce soit par la réglementation ou les régulateurs.

Il fut toutefois un temps où la situation était différente. L'auteur de ces lignes se rappelle encore l'émoi qu'a causé, il y a quelques années, la volonté d'envoyer des documents hautement confidentiels sous forme chiffrée à un régulateur européen, celui-ci ayant plutôt insisté pour recevoir plutôt un bon vieux fichier Excel par message électronique…

Mais tel n'est définitivement plus le cas aujourd'hui. La sécurité des systèmes d'information faisant régulièrement la une des journaux, la « culture sécurité » infusant dans tous les secteurs économiques, les régulateurs ont changé de vision et intègrent cet élément de façon cruciale dans leurs audits des entreprises dont ils ont la supervision. Pour la CNIL par exemple, la sécurité est un angle d'audit d'autant plus important que plusieurs facteurs se coagulent : l'afflux d'anciens de l'ANSSI dans ses rangs a accru sa compétence, le RGPD s'inscrit dans la droite ligne de la loi du 6 janvier 1978 et se fonde peu ou prou sur la sécurisation des systèmes d'information, la protection des données ne peut être assurée que si la sécurité des systèmes d'information et des infrastructures est elle-même renforcée, etc.

PDCA et protection des données

Si l'on étudie justement le sujet de la protection des données personnelles sous cet angle, on se rend compte que la situation a nettement évolué avec l'avènement du RGPD d'une part, et depuis son entrée en vigueur en 2016 puis en application en 2018 de l'autre. En cela, le cycle PDA, central les normes ISO en matière de qualité, puis de management de la sécurité de SI, semble produire tous ses effets.

Rappelons que PDCA signifie Plan Do Check Act et qu'il désigne une méthode de conception et de gestion itérative utilisée dans les entreprises pour le contrôle et l'amélioration continue des processus et des produits[1]. Cette méthode est composée des phases de notions de planification, d'exécution/de développement, de vérification/contrôle, **mais surtout de réaction/ajustement pour optimiser et améliorer les process concernés.**

En clair : on peut (et il faut) toujours mieux faire !

Or cette notion est centrale dans les normes ISO qui peuvent exister en matière de qualité (9001) et de

[1] Transposée graphiquement sous la forme d'une « roue de Deming », du nom du statisticien l'ayant fait connaître dans les années 1950.

systèmes de management (14 001 en matière d'environnement… et 27 001 et suivants en matière de sécurité de système d'information).

Si le RGPD ne mentionne la notion que dans son article 32d comme un exemple des « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque », la notion irrigue en réalité la règlementation en la matière, surtout telle qu'elle est interprétée par les régulateurs (CEPD, CNIL, etc.).

Si l'on s'intéresse par exemple à la notion de violation de données à caractère personnel, l'ancêtre du CEPD indiquait, par exemple, dans ses « Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679 » dès leur première version d'octobre 2017, que l'obligation de notification ne s'arrêtait pas au fait de constater une violation et allait bien plus loin. L'organe rassemblant les régulateurs européens en matière de protection des données indiquait ainsi que « Le responsable du traitement **se voit ainsi tenu de prendre les mesures nécessaires pour s'assurer de prendre "connaissance" de toute violation dans les meilleurs délais** afin de pouvoir réagir de façon appropriée ». Pour le G29/CEPD, l'obligation prévue devait donc largement être mise en perspective par rapport aux objectifs de protection des personnes concernées…. Et l'obligation initiale devait nécessairement s'assortir d'une vision à 360° plus globale.

De la même façon, les positions de régulateurs n'ont été que crescendo concernant les scénarios de risque à établir préalablement aux traitements qui le nécessitent. Si l'on s'intéresse au résultat final de ces scénarios, soit les notifications à mettre en œuvre quand les hypothèses se réalisent, la différence est ici frappante entre les lignes directrices précitées, ne donnant que quelques exemples utilisables en pratique (annexe B p. 35 à 38), et les « Lignes directrices du 14 janvier 2021 » dont la trentaine de pages est dédiée à ce seul et unique sujet.

Vers un autre niveau d'exigence de conformité

Sur tous les sujets, le niveau de maturité augmente et les exigences en termes de conformité ne font que croître, en France comme à l'étranger.

Si l'on reprend l'exemple de la protection des données personnelles :

- Avant 2016, le fait pour une entreprise privée d'avoir un CIL, voire mieux, un réseau de correspondants locaux au niveau d'un Groupe, était le signe de meilleures pratiques.

- En 2018, avoir un DPO/DPD est devenu obligatoire dans nombre de cas, c'est alors devenu la norme.

- Depuis, les exigences augmentent encore et l'on s'intéresse maintenant aux compétences et au rôle pratique du DPO dans l'entité.
En l'occurrence :

- à la réelle indépendance du DPO/DPD. Est-il en situation de conflit d'intérêts du fait de ses multiples fonctions ? Rappelons que l'Autorité de protection belge (APD) a infligé une amende de 50 000 euros à un responsable de traitement pour non-respect de l'obligation d'éviter tout conflit d'intérêts, le DPD étant également directeur de la compliance, du risk management et directeur de l'audit interne ;

- ou même s'il n'a pas outrepassé en réalité ses fonctions de DPO pour agir comme un responsable de traitement. À ce titre, une autre décision de la même APD du 28 mai 2019 est très intéressante : elle sanctionne un responsable du traitement parce que son DPD avait pris de lui-même la décision d'effacer des données à caractère personnel en réponse à un droit d'accès… se comportant de facto comme un mandataire du responsable de traitement[2].

[2] Une question centrale commence enfin à être posée en pratique, même si CNIL et CEPD avaient pour le moment jeté un voile pudique sur cette problématique : à quel titre le DPO aurait-il la possibilité de remplir un registre de traitement ? Donc en lieu et place du responsable de traitement ? En tant

- Difficile de ne pas mentionner ici le niveau des sanctions, qui lui également ne cesse de croître :

- Plus de 3 M EUR pour les filiales du Groupe Carrefour au total en novembre 2020, 100 M EUR pour les filiales de Google et 35 M pour Amazon en décembre 2020, 500 000 EUR pour Brico Privé en juin 2021, 1,75 M pour AG2R La Mondiale, 50 000 EUR pour les cookies du Figaro et surtout 746 M EUR pour Amazon en juillet 2021 ;

- Et la pression européenne sur l'autorité irlandaise de protection des données qui finit par payer, avec une sanction historique de 255 M EUR concernant WhatsApp qui vient d'être annoncée.

Des exigences de sécurité comme base de la conformité… et du business !

Les effets de cette maturité croissante en la matière ne s'arrêtent pas là. Face aux cyberattaques par ransomware par exemple [3]:

- Il devient à l'heure actuelle de plus en plus difficile de souscrire une « assurance cyber », certains assureurs se retirant peu à peu du marché (nous parlons bien ici des assurances globales, hors option spécifique du paiement des rançons) ;
- Et surtout les assureurs imposent de façon préalable la mise à niveau de la sécurisation des SI de l'entité, avec des questionnaires s'inspirant plus que fortement des normes ISO 2700x.

En réalité, ces éléments ne sont que le signe d'exigences croissantes en matière de sécurité des systèmes d'information de la part des principaux acteurs économiques. Ayant pris conscience de ces fortes exigences, ils ont été conduits à identifier leurs partenaires économiques et prestataires comme des vecteurs d'attaque malgré eux et leur imposent depuis quelques années un niveau de sécurisation minimum avant d'entrer en relation contractuelle.

La nouveauté est, là aussi, que :

- Ces exigences se renforcent très fortement [4]et surtout se systématisent, quelle que soit la taille de l'interlocuteur économique ;
- Et se diffusent elles-mêmes auprès d'opérateurs économiques de taille plus toujours plus restreinte. En réaction, les prestataires de grands groupes challengent leurs propres prestataires pour répondre aux impératifs, comprenant que ce n'est ni une lubie passagère, ni un domaine qui ne donnera jamais lieu à vérification, audit… ou défaut de conformité susceptible d'être publiquement connu !

Plus encore qu'hier, la conformité et la sécurité des systèmes d'information doivent marcher de concert pour permettre le développement du business et non conduire à ce que les portes des marchés se ferment.

Pour conclure, il est intéressant à ce titre de faire un parallèle avec les expériences de deux start-ups ayant connu un contrôle de la CNIL. L'une, Fidzup, considérait que la régulation devait s'adapter au business. Ayant notamment perdu clients et investisseurs à la suite d'une mise en demeure de la CNIL pour non-conformité, la start-up n'a tout simplement pas survécu à l'expérience et a publiquement accusé la CNIL d'avoir causé sa perte[5]. L'autre, Alan, avait anticipé un certain nombre de problématiques, a profité de l'expérience pour renforcer la sécurité de ses process… et a renforcé son image sur le plan médiatique pour avoir bien fait savoir qu'ils avaient passé le contrôle sans encombre[6].

Et vous, quel camp choisirez-vous ?

---

que son mandataire ? Mais quid alors des situations de conflits d'intérêts quand il agit ainsi ?

[3] Nous ne traiterons pas ici de l'intéressante question du paiement des cyber-rançons et renvoyons le lecteur intéressé vers un débat récent sur le sujet : https://www.youtube.com/watch?v=Bqy3jOi3Yms.

[4] Les questionnaires sécurité représentant très souvent des annexes de taille conséquente lors des négociations avec les directions des achats, avec des engagements souvent imposés.

[5] https://business.lesechos.fr/entrepreneurs/actu/0602712976681-fidzup-tire-le-rideau-et-accuse-la-cnil-de-l-avoir-tue-334901.php.

[6] https://blog.alan.com/tech-et-produit/controles-par-la-cnil.