L'INTÉRÊT DES SECRETS BIEN GARDÉS

Les forums, conférences et autres évènements commerciaux ayant pour thème la cybersécurité et la protection des informations se sont multipliés ces derniers mois. Et pour cause ! A l'approche du fameux « GDPR » (nouveau règlement n° 2016/679 sur la protection des données à caractère personnel, qui entre en vigueur le 25 mai 2018), les responsables de traitements (à savoir, plus où moins toutes les entreprises) s'affairent, ou devraient s'affairer, à trouver des solutions pour leur mise en conformité.

Grâce à ce règlement (ou sous la menace des sanctions qu'il prévoit), les entreprises semblent (re)découvrir les bonnes pratiques de gestion de données. Certaines restent au stade du « minimum sous la contrainte », mais d'autres réalisent qu'une réflexion approfondie sur la gouvernance de leurs informations peut améliorer leurs performances, renforcer la qualité de leurs services, compléter leurs offres et protéger leurs patrimoines.
Les développements législatifs récents illustrent et renforcent ce phénomène.

Vers une culture de la maîtrise de l'information

A l'ère du tout numérique (qui englobe toutes ces nouvelles tendances telles que le « cloud computing », l' « internet des objets », le « big data » et l' « intelligence artificielle »), tout le monde doit prendre conscience de l'importance, de la valeur et des risques qui sont associés aux données et à leurs traitements. Notre niveau de dépendance aux technologies de l'information et de la communication impose que nous y consacrions les moyens nécessaires, en termes d'attention, de budget et d'organisation : la maîtrise de l'information doit faire partie intégrante de la culture d'entreprise !

Le GDPR : nouvel instrument de protection de la vie privée

Le GDPR devient effectivement le leitmotiv du moment, servant d'argument de vente de solutions de sécurité informatique. Ceci n'est pas négatif en soi, tant la cyber-sécurité doit rester une préoccupation majeure des entreprises à l'ère du digital. Mais celles-ci ne doivent pas tomber dans le piège de la facilité technique : se contenter de « blinder » les systèmes n'assurera pas le respect complet du règlement.
Il ne faut en effet pas oublier que le fondement du GDPR se trouve dans les droits de l'homme, et plus particulièrement le droit au respect de la vie privée. Toute entité qui prend la responsabilité de traiter des données personnelles se voit imposer de nombreuses obligations qui incluent, certes, l'adoption de mesures techniques et opérationnelles afin de sécuriser les données, mais qui impliquent également une réflexion générale sur la légalité des finalités poursuivies, la proportionnalité des traitements et l'adéquation des moyens mis en place (minimisation des risques)... tout ceci afin de limiter l'impact sur la vie privée et les droits et libertés fondamentales des individus.

En d'autres termes, ce n'est pas en sécurisant un traitement intrinsèquement illégal (par exemple, parce qu'il poursuit des finalités illégitimes, qu'il est disproportionné ou qu'il ne respecte pas certaines conditions imposées par le règlement) que ce-dernier deviendra légal ! Encore en d'autres termes, il ne faut pas confondre « privacy » et « security » : un audit juridique doit dès lors accompagner l'audit technique.

Notons encore que le GDPR impose une obligation générale d' « accountability », ce qui signifie que le responsable doit non seulement prendre toutes les mesures nécessaires afin de remplir ses obligations, mais il doit également être en mesure de le démontrer à tout moment (nous renvoyons le lecteur à notre précédente contribution sur le GDPR dans le Classe Export Wallonie n°16). La documentation des mesures adoptées est également un aspect essentiel de mise en conformité.

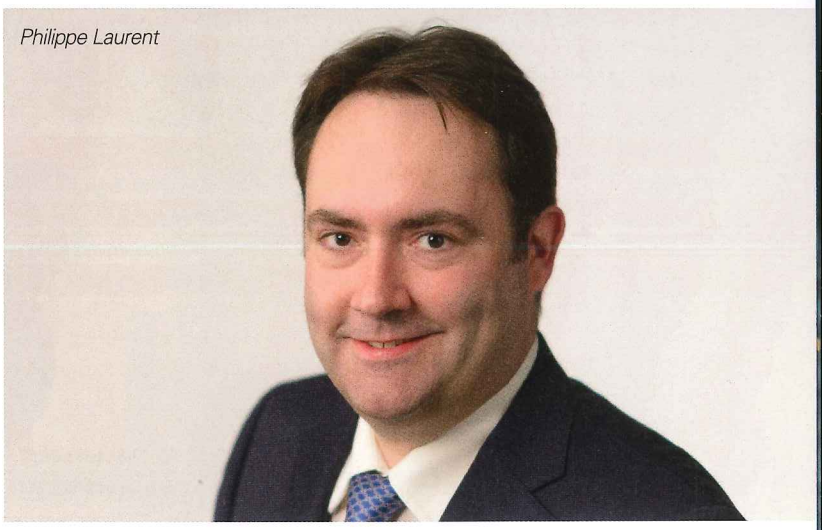
Obligations de sécurité des opérateurs de services essentiels et des fournisseurs de services numériques.

Mais il n'y a pas que le droit de la vie privée qui impose la sécurisation des données...

La dépendance aux technologies informatiques ne cesse de croître, en ce compris dans les secteurs indispensables à l'organisation de notre société et de nos modes de vie actuels. Une nouvelle directive (n°2016/1148, dite « NIS ») a été adoptée afin d'assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union Européenne. Cette dernière, qui doit être transposée en droit belge pour le 10 mai 2018 au plus tard, va bien au-delà de la protection des données personnelles : elle impose aux acteurs des secteurs concernés l'adoption de mesures de sécurisation des réseaux et systèmes, ainsi que de toutes les informations qui y transitent.

Ces règles s'appliqueront aux opérateurs de services essentiels (énergie, transports, banques, santé, distribution d'eau, infrastructures numériques,...) mais également aux fournisseurs de services numériques, ce qui comprend les « marketplaces », les moteurs de recherche et les services « cloud ». Elles imposeront entre autres des niveaux de sécurité élevés et des procédures en cas d'incidents.

On peut trouver dans cette directive d'importantes similarités avec le GDPR, mais les objectifs poursuivis sont d'une autre nature : ce sont les fonctions économiques et sociétales des systèmes d'information que l'on veut préserver, afin de protéger la société dans son ensemble. Les enjeux sont dès lors davantage la qualité, la fiabilité et la continuité des services.


Philippe Laurent

Bien gérer ses informations, c'est également protéger le patrimoine de l'entreprise !

Une autre directive, adoptée spécifiquement pour protéger les intérêts des entreprises elles-mêmes, implique également une sérieuse prise en main de la gestion de l'information : il s'agit de la nouvelle directive 2016/943 sur la protection des secrets d'affaires.

Cette directive (qui devrait être transposée en droit belge le 6 juin 2018 au plus tard) vise à harmoniser au niveau européen la protection juridique des informations commerciales non divulguées. Les « secrets d'affaires » y sont définis comme étant des informations qui répondent à trois conditions cumulatives :

1) elles sont secrètes (en ce sens qu'elles ne sont pas généralement connues ou accessibles par les personnes du secteur d'activité) ;

2) elles ont une valeur commerciale parce qu'elles sont secrètes

3) elles ont fait l'objet de dispositions raisonnables destinées à les garder secrètes.

Ainsi, pour pouvoir bénéficier des mesures de protection établies par cette directive, les entreprises doivent prendre des mesures pour protéger les secrets et en contrôler l'accès. Comme pour le GDPR ou la directive NIS, ces mesures devraient être à la fois des mesures techniques (protection des accès) et organisationnelles (on pense immédiatement, par exemple, à l'adoption de clauses de confidentialité et la signature de « non disclosure agreements »).

Les mesures prévues par cette directive comprennent entre autres la possibilité de s'adresser au juge en cas de divulgation ou d'accès illégaux, afin de faire cesser les fuites informationnelles, réparer les dégâts et sanctionner les responsables. Dans ce cadre, les détenteurs des informations protégées devront d'abord démontrer au juge qu'il s'agit bien de secrets d'affaires et, donc, que des mesures ont été prises pour en assurer le contrôle. A nouveau, tout comme dans le cadre du GDPR, la documentation des mesures adoptées sera déterminante.

Philippe Laurent