Il est temps de « désexpertiser » la cybersécurité !

Christiane FERAL-SCHUHL
Avocate

Xavier LEONETTI
Magistrat

Le 16 novembre 2022, le ministre délégué à la transition numérique a annoncé une série de mesures visant à renforcer la sécurité des PME et des collectivités publiques.

Au-delà des trente millions d'euros qui seront alloués à la protection des entreprises et des collectivités, il s'agit de positionner les questions cyber au cœur des stratégies des comités de direction. En effet, dans les entreprises et dans un grand nombre d'administrations, les questions de cybersécurité relèvent encore trop souvent de la technique au lieu de faire partie intégrante de la stratégie. En quelque sorte, les enjeux de cybersécurité et de cyberdéfense au sens large sont perçus comme l'émanation de problématiques liées au service informatique. Or, le numérique comporte à la fois une dimension structurelle, sous la forme de l'architecture technique qui supporte l'activité d'une entreprise ou d'une collectivité, mais également une dimension stratégique en lien avec l'usage qui en est fait : la protection des ressources, la gestion des données internes et des clients, la communication externe… Le cyber est aujourd'hui aussi présent et vital pour les entreprises que l'air que l'on respire. C'est pourquoi il est impératif que ce sujet ne reste pas l'affaire des seuls techniciens.

La sécurité est un sujet qui a toujours existé dans nos sociétés, mais qui a pris une dimension nouvelle avec l'ère du numérique.

La seule évocation du RGPD permet de comprendre que la sécurité des données personnelles est devenue un enjeu au plan national, comme au plan international. Il doit désormais être au cœur des préoccupations des entreprises et des collectivités. De surcroît, les enjeux de cybersécurité nécessitent le suivi et l'anticipation des règles européennes, telles que les récentes publications du Digital Service Agreement (DSA) et du Digital Marketing Agreement (DMA), venus réguler l'offre de produits et de services en ligne.

Pour cela, chacun doit s'approprier les questions cyber.

Aussi, la sécurité des systèmes d'information, la gestion des données ne doivent plus se limiter aux seuls aspects techniques, mais doivent désormais s'intégrer dans un plan global de stratégie de développement positionné au plus près des décideurs, qu'ils soient chefs d'entreprises ou élus locaux. A défaut, lorsque le pilote ne s'interroge pas sur les évolutions de son écosystème, il se condamne à progresser dans « un brouillard décisionnel » au risque de subir des surprises stratégiques et de perdre en termes de compétitivité et d'image.

Le récent crack de la plateforme FTX, l'une des principales plateformes mondiales d'échanges de cryptomonnaies, illustre ce type de surprise survenue faute d'anticipation et de clairvoyance. Cette faillite est le résultat d'un cocktail classique entre aveuglement et négligences. Au cœur du scandale, une partie de l'argent confiée à FTX par ses clients aurait été aspirée par le fonds Alameda Research et détournée au profit du fondateur et des dirigeants de la plateforme. Si le secteur bancaire traditionnel a gardé ses distances avec cette plateforme, d'autres tels que des fonds d'investissement ayant pignon sur rue comme Sequoia, la caisse de retraite des enseignants de l'Ontario, ou le japonais Softbank ont investi massivement dans cette plateforme. Il convient donc de s'interroger sur la légèreté avec laquelle ces établissements ont pu investir dans un placement aussi risqué.

L'appât du gain vers des placements risqués n'est pas sans rappeler la crise de 2008. De même, l'apparente complexité des « subprimes » et de leurs produits financiers dérivés a souvent facilité l'ignorance du plus grand nombre en réservant la connaissance à un cercle de sachants, plus ou moins bien intentionnés.

Ne commettons pas la même erreur en matière numérique en nous désintéressant de ces questions ! Les enjeux cyber ne doivent pas rester concentrés entre les mains des seuls experts !

En interne cela reviendrait à laisser les clefs entre les mains d'une seule personne. Au contraire, une vision à 360° doit permettre de positionner les questions numériques et cyber au centre des compétences partagées par la technique informatique, le droit, le marketing, la finance, les ressources humaines… C'est à cette condition qu'une stratégie efficace pourra être développée et déployée. D'autant que les entreprises et les collectivités sont arrivées au milieu du guet, au « turning point », à partir duquel l'ensemble de leur stratégie doit impérativement évoluer, notamment pour faire face à la recrudescence des cyberattaques. On relèvera que, en 2021, 5037 notifications ont été reçues par la CNIL dont 59% résultaient d'un piratage informatique. L'ampleur de ce phénomène doit être prise en compte par chacun, tout particulièrement les RSSI et les Délégués aux données personnelles mais pas seulement. Tous les acteurs doivent se poser les bonnes questions.

En premier lieu, quelles sont les mesures à prendre en cas de cyberattaque ?

Les premiers réflexes à adopter sont ceux du « cyber bon sens » qui mêle technique, juridique et communication. Il convient notamment d'alerter immédiatement le support informatique, d'isoler le système attaqué afin que l'attaque ne se propage pas à d'autres équipements, de constituer une équipe de gestion de crise, de déposer plainte, de conserver les preuves de l'attaque, de procéder à une analyse pour identifier les failles et prévenir les éventuelles répliques… Par ailleurs, une cyberattaque aura bien souvent pour conséquence une violation des données au sens du RGPD. Dans ce cas, une violation de la confidentialité, de l'intégrité ou de la disponibilité des données, fait naître, dans un délai très court, un certain nombre d'obligations à la charge du responsable de traitement. Ce dernier devra par exemple notifier la violation à la CNIL dans un délai de 72 heures. De même, il devra notifier la personne concernée par la violation des données dans le meilleur délai et documenter cette violation en indiquant les faits, les effets et les mesures prises pour y remédier (article 35 du RGPD).

En amont d'une crise, quels sont les points de vigilance sur lesquels se pencher prioritairement ?

Il faut définir le bon niveau de sécurité des données et hiérarchiser les accès. S'agissant plus particulièrement des données à caractère personnel, la désignation d'un Délégué aux données personnelles est souvent une mesure de précaution. Elle peut être obligatoire dans un certain nombre de cas, par exemple pour les collectivités. La CNIL a d'ailleurs récemment mis en demeure 22 collectivités qui n'avaient pas désigné de DPO. Ce dernier joue en effet un rôle essentiel dans la conformité des traitements de données mis en œuvre par les autorités publiques. Il constitue l'interlocuteur privilégié des agents et des administrés sur l'ensemble des sujets relatifs à la protection des données.

Enfin, comment renforcer le dispositif sécuritaire face aux risques cyber ?

Un outil d'auto-diagnostic devrait être prochainement développé permettant notamment aux 750 entreprises issues des secteurs stratégiques (définis par la directive européenne NIS2) de contribuer au bouclier cyber qu'elles devront bientôt mettre en œuvre. Concrètement, à la suite de l'adoption de la directive NIS en 2016, les opérateurs de services essentiels (OSE), tels que dans les secteurs bancaires, de la santé ou de l'énergie, ont dû adopter des mesures spécifiques de cyber protection. La directive NIS2 étendra ces obligations à de nouveaux acteurs.

Pour les collectivités territoriales, le plan annoncé par le secrétaire d'État au numérique leur permettra de renforcer leur cybersécurité au travers de parcours différenciés. Le plan prévoit qu'à la fin de l'année 2023, plus de 1000 collectivités et administrations auront suivi l'un ou l'autre des parcours de cybersécurité. Les plus petites communes disposeront quant à elle d'un accompagnement sous la forme d'outils de cybersécurité « clé en main » mis à leur disposition.

La cybersécurité doit désormais être considérée comme partie intégrante des enjeux stratégiques des entreprises ou des collectivités. Elle doit mettre en réseau la technique et la stratégie, en quelque sorte, à l'image d'un développeur qui devra intégrer une solution technique dans un cadre juridique et stratégique préalablement défini.

Christiane FERAL-SHUHL et Xavier LEONETTI sont les co-auteurs de l'ouvrage :
« Cybersécurité, mode d'emploi » (PUF, 2022)