Le risque éthique à travers les atteintes à la sécurité informatique

Les entreprises sont de plus en plus cyberattaquées. Hier, elles subissaient les *hackers* malveillants. Aujourd'hui, les entreprises peuvent aussi être la cible «d'hacktivistes» ou de «cybermilitants» motivés par la défense de causes d'intérêt général. Essentiel, le statut de ces cyberattaquants est bien différent de celui du « lanceur d'alerte » tel que définit dans la loi Sapin II.

Patrice Grenier
Fondateur de Grenier Avocats

L'étude «Risk in focus» menée auprès de 300 professionnels de l'audit interne travaillant dans des entreprises européennes,[1] a montré que la cybersécurité arrive en tête du classement des risques majeurs pour l'année 2019. Espionnage industriel, vol de données, «*ransomware*»… Les entreprises sont toujours plus confrontées à des cyberattaques. Si jusqu'ici elles étaient victimes de *hackers* «malveillants», elles peuvent être aujourd'hui la cible d'«hacktivistes» ou de «cybermilitants» (comme les «*Anonymous*» ou Julian Assange, créateur de Wikileaks).

L'«hacktiviste» a pour objectif de pirater les systèmes informatiques des entreprises, de s'emparer des informations confidentielles et sensibles de celles-ci pour ensuite les divulguer à l'extérieur. Tiers à l'entreprise, contrairement au lanceur d'alerte qui généralement travaille au sein même de l'organisation de laquelle il diffuse des informations compromettantes, l'hacktiviste utilise ses compétences en informatique au profit de l'intérêt général.

> ***«miser sur des mesures efficaces pour identifier, prévenir et traiter les risques éthiques le plus en amont possible»***

Les informations concernées peuvent être liées par exemple à des faits susceptibles de concerner des pratiques de corruption ou de fraude fiscale impliquant une entreprise. Les informations qui pourraient être tout particulièrement la cible de cyberattaques sont celles recueillies dans le cadre du mécanisme de recueil des signalements de comportements non éthiques, obligatoire dans les entreprises de plus de 50 salariés depuis la loi du 9 décembre 2016 dite «loi Sapin II». À l'heure du *Big Data* et de l'hypernumérisation des informations, celles-ci peuvent être plus facilement appréhendées par les *hackers* et révélées au public, sans que l'entreprise ne puisse plus avoir aucun contrôle sur les éléments diffusés.

Si le *hacker* pourra être sanctionné sur le plan pénal pour atteinte au secret des affaires – bien qu'aujourd'hui il existe de nombreuses incertitudes quant à la position du juge face à ces révélations d'ordre éthique, les conséquences pour l'entreprise pourront être très dommageables du fait de la masse d'informations diffusées et l'absence de maitrise possible de ces révélations. Cela pourra notamment entacher l'image de l'entreprise vis-à-vis des consommateurs et de la société civile mais aussi de ses partenaires commerciaux. De plus, ces révélations inopinées pourront entrainer des poursuites à son encontre de la part des autorités.

La question ici n'est pas tant de savoir comment sécuriser davantage ces informations (la première mesure généralement retenue étant d'externaliser le traitement de ces signalements) mais plutôt d'éviter, en cas de cyberattaque, de se retrouver dans une situation de crise ingérable face aux révélations d'informations sensibles et à leurs effets. En d'autres termes, il convient de miser sur des mesures efficaces pour identifier, prévenir et traiter les risques éthiques le plus en amont possible. En cas de cyberattaque, l'entreprise ne sera pas prise au dépourvu et pourra justifier aux yeux du grand public et des autorités concernées des actions mises en œuvre pour faire face aux risques auxquels elle est ou pourrait être confrontée. ■

Hacktiviste, lanceur d'alerte, 2 statuts différents

Il convient de rappeler ici que les «*hacktivistes*» ne peuvent *a priori* pas bénéficier du statut de lanceur d'alerte prévu par la loi Sapin II du 9 décembre 2016. Selon cette loi, pour bénéficier de ce statut protecteur, la personne doit révéler des faits dont elle a eu personnellement connaissance, de manière désintéressée et de bonne foi, relatifs à un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice graves pour l'intérêt général. De plus, elle doit respecter la procédure prévue par la loi :

- signalement auprès du supérieur hiérarchique ;
- en cas d'absence de diligences effectuées par celui-ci dans un délai raisonnable, la personne peut révéler ces faits aux autorités ;
- en dernier ressort, à défaut de traitement par les autorités dans un délai de trois mois, le signalement peut être rendu public (exception : en cas de danger grave et imminent ou en présence d'un risque de dommages irréversibles, le signalement peut être porté directement à la connaissance des autorités ou être rendu public). ■

* Étude publiée par l'Eciia (*European Confederation of Institutes of Internal Auditing*) et l'Ifaci (Institut français de l'audit et du contrôle internes) en sept. 2018, cf. : https://docs.ifaci.com/wp-content/uploads/2018/09/Risk_in_Focus_2019.pdf