

NIS2 élargit fortement le nombre d'organisations soumises à des obligations de cybersécurité. En France, environ 15 000 entités pourraient être concernées. Mais son apport majeur réside peut-être ailleurs : jusqu'à présent, une cyberattaque conduisait à l'indemnisation de l'entreprise victime pourvu qu'elle ait souscrit une police cyber. Désormais, va se poser la question de savoir si les dirigeants, de par les obligations mises à leurs charges, encourent une responsabilité accrue.

L'article 20 de NIS2 impose aux organes de direction d'approuver les mesures de gestion des risques en matière de cybersécurité et d'en superviser la mise en œuvre. Leurs membres doivent également suivre une formation dédiée. La directive ne transforme pas le dirigeant en expert informatique. Elle lui impose pourtant de contrôler que le risque cyber est identifié, pris en compte et effectivement supervisé.

Certes, NIS2 n'instaure pas un régime autonome de responsabilité civile. À ce titre, rappelons qu'en droit français, la mise en cause du dirigeant est fondée sur un mécanisme qui lui est propre, dont les fondements diffèrent selon la forme juridique de la société et l'identité du réclamant. La directive vient toutefois préciser les standards de diligence attendus du dirigeant en matière de cybersécurité, lesquels pourront désormais être pris en compte dans l'appréciation de l'éventuelle commission d'une faute de gestion.

LA CYBERATTAQUE, RÉVÉLATEUR D'UNE DÉFAILLANCE DE GOUVERNANCE ?

Une attaque informatique ne saurait, à elle seule, caractériser la faute. Encore faut-il, selon le régime de responsabilité invoqué, démontrer l'existence d'une faute imputable au dirigeant répondant aux conditions du régime de responsabilité applicable, d'un préjudice et d'un lien de causalité.

À ce titre, la responsabilité du dirigeant pourrait être recherchée lorsque la survenance ou les conséquences du sinistre révèlent des défaillances dans l'anticipation ou la gestion du risque cyber. Tel pourrait notamment être le cas en présence d'un défaut de prise en compte des alertes préalables, d'une insuffisance des mesures de prévention, d'une réaction tardive face à l'incident ou encore de l'absence de procédures internes adaptées à la gestion de crise. La cyberattaque ne caractérise pas la faute, mais peut constituer le révélateur d'une éventuelle défaillance de gouvernance.

Avec la directive NIS2, le législateur européen place les organes de direction au cœur de la gestion du risque cyber. Cette réglementation, qui doit encore être transposée, dessine un nouveau cadre auquel dirigeants et assureurs doivent se préparer. Ce risque est désormais un enjeu de gouvernance.

À SAVOIR

L'assurance responsabilité civile des mandataires sociaux (RCMS)

protège le patrimoine personnel des dirigeants d'entreprise contre les conséquences financières des fautes commises dans l'exercice de leurs fonctions : erreurs de gestion, omissions, les violations des statuts ou manquements réglementaires.

PEOPLEIMAGES

CYBERATTAQUE DIRIGEANTS ET LE

LA RESPONSABILITÉ DES DIRIGEANTS DE PLUS EN PLUS MISE EN CAUSE ?

La question intéresse directement la gestion de ce nouveau risque. L'assurance cyber est une assurance de dommages destinée, selon les garanties souscrites, à couvrir certaines conséquences de l'incident pour l'entreprise. L'assurance RCMS⁽¹⁾ consiste, quant à elle, à garantir la responsabilité du dirigeant lorsqu'une réclamation le met personnellement en cause. Les conditions de cette mise en cause diffèrent selon l'auteur de l'action. La société peut rechercher la responsabilité de son dirigeant en démontrant notamment la commission d'une faute de gestion ou la violation des dispositions légales ou réglementaires qui lui sont applicables. En revanche, l'action d'un tiers contre le dirigeant suppose la caractérisation d'une faute séparable de ses fonctions.

Une telle action n'est pas seulement théorique en matière cyber. La tierce victime, par exemple,



ARIANE DELION
AVOCATE
COLLABORATRICE
CABINET STREAM

PAGES
COORDONNÉES
PAR MARINE
CALVO



La responsabilité du dirigeant

pourrait être recherchée lorsque la survenance ou les conséquences du sinistre révèlent des défaillances dans l'anticipation ou la gestion du risque cyber.

INFORMATIQUE

UE: UN RISQUE ÉMERGENT POUR LES ASSUREURS DE RESPONSABILITÉ

d'un vol de données, pourra rechercher la responsabilité personnelle du dirigeant en démontrant avoir subi un préjudice qui lui est propre. Mais il lui faudra alors démontrer, selon la définition consacrée, que le dirigeant a commis « *une faute intentionnelle d'une particulière gravité, incompatible avec l'exercice normal des fonctions sociales* ». ⁽²⁾

Ainsi, un même événement est susceptible de soulever des problématiques assurantielles distinctes puisque la cyberattaque relèvera de la garantie dommages du contrat cyber de l'entreprise tandis que le dirigeant, en cas de recours à son encontre, mobilisera la garantie du contrat RCMS souscrit pour son compte. Il n'est d'ailleurs pas exclu que l'assureur cyber ayant indemnisé l'entreprise, et donc subrogé dans ses droits, exerce son recours contre le dirigeant et son assureur RCMS.

À l'instar de l'assureur couvrant le risque cyber, l'assureur RCMS, sauf à exclure de sa garantie ce

type de risque, sera conduit à contrôler la maturité cyber de l'entreprise souscriptrice tant au stade de la souscription, durant la vie du contrat, jusqu'à la survenance du sinistre.

L'ARTICULATION DES GARANTIES: UN NOUVEL ENJEU ASSURANTIEL

La question se pose ainsi de savoir quelle va être la position des intervenants proposant des garanties RCMS à l'avenir: accepteront-ils de couvrir le risque encouru par ces nouvelles contraintes pesant sur le dirigeant ou chercheront-ils, au contraire, à l'exclure du périmètre de la garantie? Pour les assureurs, l'enjeu sera donc d'articuler les garanties afférentes aux risques cyber et RCMS, qui ont vocation à devenir complémentaires. À n'en pas douter, une adaptation des garanties est à prévoir s'agissant de la délimitation du risque et des plafonds de garantie. ■

1. Responsabilité civile des mandataires sociaux.
2. Cour de Cassation, chambre commerciale, du 20 mai 2003, 99-17.092, Publié au bulletin.