Octobre 2024
Numéro 40


# La Lettre de la S.C.B.

## L'avocat et le risque cyber : exposition, conséquences et prévention

### INTRODUCTION

Quel que soit le secteur d'activité ou la taille de l'organisation, les cyberattaques sont devenues une réelle menace. Cette diversité d'organisations victimes a pu être médiatiquement constatée en 2022 : des centres hospitaliers (Corbeil-Essonnes, Versailles, Cœur Grand Est), des administrations publiques (Conseil départemental de la Seine-Maritime, Région de Guadeloupe, Conseil départemental de Seine-et-Marne) mais également des entreprises du secteur privé (Thalès, Conforama, la coopérative bretonne Eureden).

Selon le rapport annuel de l'Agence nationale de sécurité des systèmes d'information (ANSSI) pour l'année 2022, les TPE, PME et ETI, qui sont des cibles plus faciles pour les pirates, ont été particulièrement visées par les cyberattaques. Elles représentent 40 % des attaques par rançongiciel(1) traitées ou rapportées à l'ANSSI. Les hackers profitent du faible niveau de leurs systèmes d'information beaucoup moins bien protégés que ceux des grandes entreprises. De plus, les méthodes des attaquants sont de moins en moins visibles. Ils ciblent les équipements périphériques tels que les pare-feu ou les routeurs, ce qui permet aux cybercriminels de réussir à obtenir des accès discrets et pérennes aux réseaux de leurs victimes. Et pour arriver à leurs fins, ils recherchent le maillon faible : les prestataires, les fournisseurs, les sous-traitants, et l'écosystème plus large de leur cible. Seul un tiers des TPE et PME est considéré comme correctement paré.(2)

La cybercriminalité et son remède qu'est la cybersécurité sont un véritable sujet d'inquiétude pour la société française et en particulier pour ses acteurs économiques, ainsi qu'en témoigne notamment le rapport d'information sénatorial *« La cybersécurité des entreprises – Prévenir et guérir : quels remèdes contre les cyber-virus ? »* déposé le 10 juin 2021.

C'est également un risque source de préoccupation pour les entreprises d'assurance mais aussi pour l'Autorité de contrôle prudentiel et de résolution des risques(3) (ACPR), leur autorité de contrôle, qui en septembre 2022 les a incitées à examiner l'ensemble des garanties contenues dans leurs contrats par rapport aux risques cyber et, le cas échéant, à clarifier et à rendre plus explicites les formulations des termes et conditions des polices en ce qui concerne la couverture ou l'exclusion de ces risques. L'ACPR a également estimé crucial que les entreprises d'assurance soient en mesure d'identifier et d'évaluer rapidement et de façon exhaustive leur exposition au risque cyber, en particulier implicite, dans les contrats d'assurance(4), pour des raisons notamment de solvabilité.

(1) Le rançongiciel ou ransomware consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement.
(2) Publication du 8 février 2023 sur le site francenum.gouv.fr
(3) Adossée à la Banque de France, l'ACPR est l'autorité administrative qui contrôle les secteurs de la banque et de l'assurance et veille à la stabilité financière. L'ACPR est également chargée de la protection de la clientèle des établissements contrôlés et assure la mission de lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT).
(4) ACPR – Communiqué de presse du 23 septembre 2022 *Garanties implicites contenues dans les contrats en matière de couverture du risque cyber : l'ACPR salue la publication de la position de l'EIOPA.*

Mais qu'en est-il des avocats dans tout cela ? Les cabinets d'avocats ont-ils plus de risques que d'autres secteurs d'activité d'être victimes de la cybercriminalité ? Quelles peuvent-être pour l'avocat les conséquences d'une cyberattaque à l'encontre de son cabinet ? L'avocat dispose-t-il de moyens pour prévenir la réalisation d'un tel sinistre et à tout le moins de le garantir ?

Voici l'ensemble des questions auxquelles va tenter d'apporter des débuts de réponse cette nouvelle Lettre de la SCB, réponses qui mériteront des réflexions plus approfondies au sein de chaque cabinet d'avocats en considération de son activité mais aussi de sa taille.

## 1/ L'exposition de l'avocat face au risque Cyber

L'ANSSI a publié le 27 juin 2023 un rapport sur l'*état de la menace informatique contre les cabinets d'avocats*, consultable sur le site internet du Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) en cliquant sur le lien suivant : https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-004/

Dans ce rapport, l'ANSSI écrit que *« les avocats et les cabinets d'avocats sont régulièrement la cible d'attaques informatiques conduites par des acteurs aux origines, aux compétences et aux objectifs divers »*.

Cette exposition s'explique par trois principaux facteurs :

- ⇒ l'accès des avocats *« à des données sensibles concernant leurs clients et des procédures judiciaires, que des attaquants pourraient chercher à dérober* ;
- ⇒ *leurs échanges potentiels avec les véritables cibles des attaquants, qui pourraient compromettre un cabinet pour atteindre des personnes ou organisations jugées d'intérêt parmi leurs clients ;*
- ⇒ *leurs recettes financières, que les attaquants pourraient tenter d'extorquer ».*

L'ANSSI relève que la surface d'attaque ou du nombre de points d'entrées dans les systèmes d'information des cabinets d'avocats ne cessent de s'étendre notamment pour les raisons suivantes :

- ⇒ la numérisation croissante des procédures judiciaires ;
- ⇒ les interconnexions entre les réseaux des cabinets et ceux des prestataires extérieurs ;
- ⇒ le manque de cloisonnement entre les équipements utilisés dans le cadre personnel et professionnel ;
- ⇒ le recours croissant au télétravail ;
- ⇒ l'existence de mauvaises pratiques.

L'ANSSI identifie deux catégories d'attaques : les *« attaques à finalité lucrative »* et *« l'espionnage informatique »*.

S'agissant des attaques à finalité lucrative, l'ANSSI souligne que *« les cabinets d'avocats représentent des cibles de choix pour les acteurs malveillants conduisant des attaques à but lucratif. Ils disposent en effet de données sensibles pouvant être revendues en ligne ou permettre, dans le cadre d'attaques par rançongiciel, d'accentuer la pression pour que la victime verse une rançon ».* Il est également observé que depuis 2010, certains attaquants se sont spécialisés dans la compromission de cabinets d'avocats pour dérober des informations permettant de commettre des délits d'initié.

Le nombre d'incidents utilisant le rançongiciel a fortement augmenté depuis 2017. De manière croissante, ils se doublent d'une exfiltration de données que les cybercriminels menacent de rendre publiques en cas de non-paiement de la rançon exigée. L'ANSSI qualifie cette technique de *« double extorsion »*, créant une pression supplémentaire sur la victime et ainsi une chance plus importante d'obtenir le versement de la rançon.

Ces attaques peuvent être aussi dirigées sur les prestataires de services numériques auxquels font appel les avocats, avec la même finalité.

L'ANSSI ajoute que les auteurs de cyberattaques tentent également de monétiser la compromission des cabinets d'avocats *« en détournant directement leurs comptes bancaires ou en exfiltrant les données de leurs systèmes d'information afin de les exploiter ou de les revendre sur des forums spécialisés ».*

Toujours dans la catégorie des attaques à finalité lucrative, l'ANSSI indique avoir observé depuis au moins 2020 l'émergence d'attaques par rançongiciels conduites par des groupes d'attaquants présumés liés à des gouvernements étrangers. Elle précise toutefois qu'il s'agit d'attaques qui demeurent marginales mais qui ne doivent pas être ignorées, même pour des cabinets d'avocats français.

S'agissant de *« l'espionnage informatique »*, il s'agit d'attaques qui ciblent les cabinets d'avocats afin de surveiller leurs activités ou celles de leurs clients. Les auteurs de ces attaques sont généralement étatiques, s'inscrivant dans le cadre de missions d'espionnage économique ou stratégique, avec un intérêt particulier pour les brevets, les dossiers de fusion-acquisition, les procédures judiciaires ou d'arbitrage. L'ANSSI précise que dans le milieu des années 2010, dans le cadre de conflits familiaux ou commerciaux, plusieurs cabinets d'avocats ont été la cible d'attaques perpétrées par des entreprises privées ou des mercenaires privés, engagés par des enquêteurs privés, des entrepreneurs ou des personnalités politiques afin de surveiller la partie adverse.

Il ressort de ce rapport, contenant essentiellement des exemples d'attaques menées contre des cabinets d'avocats étrangers, que les avocats peuvent faire l'objet d'attaques qu'on peut qualifier de masse que tout un chacun, particulier ou professionnel, connaît sans considération de son profil, mais également d'attaques plus ciblées, donc plus « professionnalisées », en raison des données sensibles qu'ils peuvent détenir, ce qui en accentue le risque.

## 2/ Les conséquences de la réalisation du risque Cyber pour l'avocat

A l'occasion d'une attaque dirigée contre son cabinet, l'avocat peut être à la fois victime, en ce que cette attaque va lui générer des préjudices personnels de différentes natures, mais aussi potentiellement responsable, en ce que cette même attaque pourrait être à l'origine de préjudices subis par ses clients ou des tiers, et enfin potentiellement sanctionnable, cette attaque pouvant justifier que des sanctions administratives soient prononcées à son encontre par la Commission nationale de l'informatique et des libertés (CNIL).

### 2.1 L'avocat victime

Les attaques informatiques dirigées contre un cabinet d'avocats peuvent engendrer des conséquences de trois types.

D'une part, des conséquences opérationnelles : par exemple, l'impossibilité pendant une certaine durée d'accéder au contenu dématérialisé de ses dossiers ou de notifier via le RPVA, empêchant ainsi l'exercice normal de l'activité.

D'autre part, des conséquences financières constituées, selon la nature de la cyber attaque, par notamment le paiement d'honoraires d'une société spécialisée en sécurité informatique, des frais supplémentaires d'exploitation, des pertes d'exploitation, le paiement d'une rançon, les frais de notification…

Enfin, des conséquences réputationnelles, l'incident pouvant révéler une insuffisante sécurisation du système d'information de l'avocat, voire une négligence en la matière, engendrant ainsi une rupture du lien de confiance avec ses clients, ces derniers n'ayant plus l'assurance que le secret professionnel entourant leur dossier est correctement protégé.

Pour garantir certaines de ces conséquences, l'avocat et les cabinets d'avocats peuvent souscrire un contrat d'assurance cyber-risques permettant de couvrir les pertes financières subies ou causées à des tiers (à l'exclusion de celles relevant de la garantie de responsabilité civile professionnelle), provenant d'erreurs de manipulation, de dysfonctionnements et d'actes de criminalité (virus, déni de service, phishing, ransomware, etc.) et portant atteinte au système d'information du cabinet d'avocats en provoquant des situations de blocage et des pertes financières, et/ou aux données informatisées stockées ou en transfert.

La SCB se tient à la disposition des avocats pour envisager la souscription d'un tel contrat.

### 2.2 L'avocat potentiellement responsable

La survenance d'une cyberattaque peut être à l'origine de dommages pour les clients de l'avocat.

Le dommage sera par exemple généré par la circonstance que l'avocat n'aura pas été en mesure de notifier des conclusions d'appels avant l'expiration du délai de l'article 908 du code de procédure civile, étant totalement empêché de travailler, ou n'aura pas exécuté une instruction de son client envoyée par courriel, faute de ne pas avoir eu accès à sa boîte mail. La désorganisation que peut provoquer dans un cabinet d'avocats une cyberattaque peut être source de nombreux autres dommages au préjudice des clients.

Dans de telles hypothèses, le client devra faire la démonstration que son avocat a commis une faute à l'origine du préjudice invoqué. L'avocat pourra alors opposer la force majeure de l'article 1218 du code civil, si celui-ci parvient à démontrer les caractères suivants de l'événement : son imprévisibilité et son irrésistibilité. Et il ne pourra alors lui être reproché la commission d'une faute.

Toutefois, cette affirmation pourrait souffrir d'un important tempérament.

Le 25 mai 2018, est entré en vigueur dans le droit national français le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, qu'on appelle communément RGPD.

L'objectif de ce règlement est de protéger les personnes physiques à l'égard du traitement de leurs données à caractère personnel, dont la définition est donnée par son article 4 : « *toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.* »

Le RGPD place les entités qui traitent ces données à caractère personnel (entreprises, collectivités territoriales…), dénommées *« responsables de traitement »* dans une logique de responsabilité dans le traitement des données personnelles, par le respect de différentes obligations qu'il édicte.

L'article 82 § 1 du règlement prévoit que toute personne ayant subi un dommage matériel ou moral du fait d'une violation du RGPD a le droit d'obtenir du responsable du traitement ou du sous-traitant de ce dernier, réparation du préjudice subi.


Par un arrêt du 4 mai 2023, saisie d'un renvoi préjudiciel d'une juridiction autrichienne, la Cour de justice de l'Union européenne (CJUE) a donné son interprétation de cet article[5] et ainsi décidé que la simple violation des dispositions du RGPD ne suffisait pas pour conférer un droit à réparation. La Cour a précisé qu'il doit exister un dommage en lien avec cette violation et que les juges nationaux doivent appliquer les règles internes de chaque Etat membre relatives à l'étendue de la réparation pécuniaire.

Au regard des règles posées ci-dessus par le RGPD et de leur interprétation par la CJUE, la question se pose de savoir si, bien que victime d'un acte malveillant qu'est la cyberattaque, l'avocat ne pourrait-il pas pour autant être reconnu comme étant fautif et devoir réparation ?

En effet, comme évoqué plus avant, une cyberattaque peut être révélatrice d'une sécurisation insuffisante du système d'information de l'avocat ou du cabinet d'avocats.

Or, l'article 32 du RGPD qui consacre le principe de la sécurité du traitement des données à caractère personnel, prévoit que *« compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins:*

*a) la pseudonymisation et le chiffrement des données à caractère personnel ;*

*b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;*

*c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;*

*d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement. »*

Aussi, une protection considérée comme insuffisante pourrait-elle être constitutive d'une violation du RGPD susceptible de générer un dommage pour le client de l'avocat. Bien sûr, il appartiendra à l'auteur d'une telle demande de rapporter la preuve d'une violation du RGPD dans le traitement de ses données à caractère personnel, ainsi que de la réalité et de la certitude de son préjudice.

S'agissant d'une potentielle responsabilité civile professionnelle au préjudice de son client, l'avocat est garanti en cas de sinistre par le contrat souscrit collectivement par son barreau en exécution de l'article 27 de la loi n°71-1130 du 31 décembre 1971.

### 2.3 L'avocat potentiellement sanctionnable

Lorsqu'une attaque informatique engendre la violation de données à caractère personnel, l'article 33 du RGPD impose au responsable de traitement qu'est l'avocat de notifier à la CNIL ladite violation dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

Rappelons que la violation de données à caractère personnel est selon l'article 4.12 du RGPD *« une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données »*

(5) CJUE, 4 mai 2023, aff. C-300/21, Österreischiche Post.

Il doit ainsi porter à la connaissance de la CNIL l'incident dont il a été victime et indirectement permettre à cette autorité de détecter une potentielle violation de ses obligations découlant du RGPD.

Cette violation peut également susciter une plainte auprès de la CNIL par toute personne titulaire des données à caractère personnel objets de la violation ainsi que le prévoit l'article 77 du RGPD.

Dans son rapport annuel 2022, la CNIL indique qu'elle a procédé à 345 contrôles et que 43 % des missions effectuées faisaient suite à une plainte ou un signalement.

La CNIL a le pouvoir de sanctionner les responsables de traitement et les sous-traitants pour méconnaissance des dispositions du RGPD.

Le montant des sanctions pécuniaires prononcées peut s'élever jusqu'à 20 millions d'euros ou dans le cas d'une entreprise jusqu'à 4 % du chiffre d'affaires annuel mondial. La CNIL a la possibilité de rendre ses sanctions publiques.

Cela a bien évidemment des conséquences économiques mais également réputationnelles pour le responsable de traitement ou le sous-traitant sanctionné.

Et information importante : aucun contrat d'assurance ne prend en charge de telles sanctions, ne s'agissant pas d'indemnisations versées en réparation d'un quelconque dommage, mais de sanctions administratives.

Telles sont les potentielles conséquences d'une cyberattaque pour un avocat ou un cabinet d'avocats, et la liste n'est pas exhaustive.

Comme tout risque, il existe des moyens d'en prévenir la réalisation, étant précisé que le risque zéro en la matière n'existe pas.

## 3/ Les moyens de prévention du risque Cyber

Ces moyens sont de deux ordres : les moyens de prévenir le risque cyber et les moyens de prévenir les éventuelles actions en indemnisation ou les éventuelles sanctions dont pourrait être l'objet l'avocat.

### 3.1 Les moyens de prévenir le risque cyber

Dans son rapport du 27 juin 2023, l'ANSSI fournit des recommandations qui visent à répondre aux menaces qu'elle a identifiées. Elle précise que ces recommandations *« doivent être contextualisées, adaptées et priorisées en fonction de chaque cabinet d'avocats (taille de l'entité, moyens humains et financiers, sensibilité des dossiers, etc.) ».*

Les recommandations sont de trois types :

- ⇒ la maîtrise des risques (mener une analyse des risques intégrant l'ensemble des prestataires informatiques, dresser un inventaire des données métier, faire régulièrement une sauvegarde en ligne…) ;
- ⇒ la protection du poste de travail (proscrire l'usage d'équipements personnels, interdire l'installation de logiciels *via* un compte utilisateur, définir une politique de mots de passe robuste, limiter la connexion des clés USB à des clés dédiées à l'usage professionnel…) ;
- ⇒ la protection de la confidentialité de données (chiffrer entièrement les disques durs du poste de travail, ne pas utiliser votre messagerie personnelle dans un but professionnel, configurer un verrouillage automatique de la session du poste…).

L'ANSSI fournit ainsi 30 recommandations dont certaines sont très simples d'application. D'autres nécessitent le recours à des prestataires informatiques ou des entreprises spécialisées dans la sécurité des systèmes d'information.

[(6)]Rapport annuel 2020 Commission nationale de l'informatique et des libertés, page 77.


**3.2 Les moyens de prévenir les actions en indemnisation ou les sanctions administratives**

Le moyen de prévention pour se protéger contre de telles actions ou sanctions est de veiller à sa conformité aux dispositions du RGPD.

Pour cela, les avocats et les cabinets d'avocats ont à leur disposition différents outils :

- ⇒ Le Guide pratique intitulé *La sécurité numérique du cabinet d'avocat* établi par le Conseil national des barreaux (CNB) édition octobre 2023, téléchargeable sur le site du CNB ;
- ⇒ le Guide pratique de sensibilisation au RGPD pour les petites et moyennes entreprises de la CNIL (téléchargeable en ligne) ;
- ⇒ le MOOC de la CNIL qui est une formation en ligne gratuite, illimitée et ouverte à tous, qui permet de sensibiliser les professionnels à la protection des données et d'accompagner leur mise en conformité (site de la CNIL).

En fonction de la taille de leur cabinet mais aussi de la nature de leur activité, les avocats peuvent avoir recours à des prestataires externes afin de les accompagner dans leur mise en conformité au RGPD.

**CONCLUSION**

Au même titre que tout citoyen et acteur économique, l'avocat est une potentielle victime d'une cyberattaque avec toutefois une particularité qu'il partage avec d'autres organisations telles que les établissements de santé par exemple : il peut être une cible privilégiée en raison de la sensibilité des informations qu'il détient dont la connaissance ou la divulgation peut permettre de porter atteinte aux clients qui lui ont confié la défense de leurs intérêts.

En effet, le secret professionnel auquel est soumis l'avocat, qui permet à ses clients de lui remettre en toute sécurité des informations de toute nature sans redouter leur divulgation, font de ce professionnel une cible de choix pour des cyberattaquants, la suppression ou la diffusion de ces informations étant susceptibles d'impacter significativement ses clients.

Ainsi qu'il l'a été exposé, les dommages générés par ces événements sont garantis ou peuvent être garantis par des contrats d'assurance, dans leur grande majorité.

Il convient toutefois d'être vigilant puisque si le risque cyber venait à devenir d'ampleur en termes de fréquence et/ou d'indemnisation, il est à redouter que les entreprises d'assurance formulent des exigences pouvant rendre plus difficile la souscription de contrats couvrant ce risque et plus compliquée la mobilisation des garanties en cas de sinistre.

L'un des moyens pour éviter que le cyber risque emprunte ce chemin, est que chaque avocat et cabinet d'avocats, en fonction de la nature de ses activités et de sa taille, prenne les mesures organisationnelles et techniques pour se prémunir contre les cyberattaques.

SOCIÉTÉ DE COURTAGE DES BARREAUX

Contactez nos équipes :

Par téléphone : **04.13.41.98.30**
Par mail : **contact@scb-assurances.com**

♦

Retrouvez toute l'information nécessaire sur notre site:
**www.scb-assurances.com**

*Directeur de publication : Larry PELLEGRINO, Président de la SCB*
*Rédacteur : Nicolas LHOMMEAU, Directeur Juridique et Compliance*