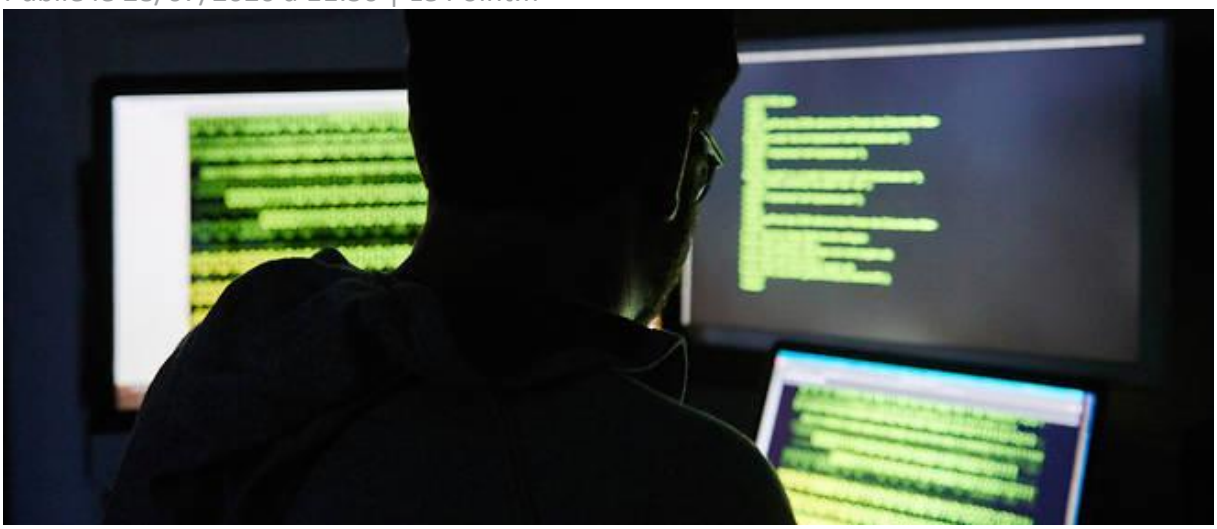
Vol, cybermenace, mauvaises pratiques : que faire face aux fuites de données ?

En partenariat avec les Soldats du droit, un collectif d'avocats, « Le Point » prodigue ses conseils. Aujourd'hui : les atteintes à la sécurité informatique.

*Par Sylvain Dorol**

Publié le 28/07/2020 à 11:30 | Le Point.fr



Quels réflexes adopter face au vol de données ? (Photo d'illustration.) © Annette Riedl / dpa-Zentralbild / dpa Picture-Alliance/AFP

Comment sortir de la crise ? Alors que l'économie française tente d'encaisser les effets du coronavirus, des centaines de questions se posent aux entreprises. Pour vous aider à traverser cette période, Le Point *a noué un partenariat avec les Soldats du droit, un collectif d'avocats créé par M^e^ Céline Astolfe, du cabinet Lombard Baratelli & associés.*

Chaque semaine, des experts, parmi les plus pointus de leur profession, s'appuient sur leur expérience et des cas concrets pour nous prodiguer leurs conseils. Aujourd'hui, Sylvain Dorol, huissier de justice associé au cabinet Vénézia & associés, nous aide à faire face aux fuites de données.

Pourquoi appeler un huissier de justice en cas de fuites de données détectées dans mon entreprise ?

Il est vrai qu'on ne pense que trop rarement à appeler un huissier de justice. Et pourtant, cet officier public et ministériel est un professionnel du droit, exerçant en libéral et chef d'entreprise. À ce titre, il connaît les difficultés que peut rencontrer une entreprise confrontée à une fuite de données. Le cantonner à un simple rôle d'exécutant (saisies, expulsions) est une grave erreur. En effet, son quotidien est d'intervenir dans des situations extrêmement

difficiles et aux très importants enjeux. Qu'on se le dise : dans toute affaire (politique, médiatique, économique), un huissier de justice est appelé à intervenir.
En réalité, pour établir un parallèle avec le monde des soignants, il est possible d'affirmer que l'huissier de justice est en quelque sorte le Samu du droit. À la manière du médecin urgentiste dépêché sur un accident de la route et qui est en charge de stabiliser la victime pour qu'elle soit prise en charge à l'hôpital avec le maximum de chances de survie, l'huissier de justice arrive bien souvent le premier sur le terrain. Son rôle est alors d'évaluer très rapidement le risque juridique qu'encourt le client, d'effectuer les « premiers gestes de secours » afin de stabiliser la situation, puis de laisser le champ libre aux généralistes et spécialistes du droit (avocats, directions juridiques…), qui traiteront et suivront le dossier plus en profondeur.

En bref, il vaut mieux appeler un huissier de justice pour rien que de ne pas l'appeler alors qu'il aurait fallu… La fuite de données étant une situation d'extrême urgence et générant un très important stress (au moment de la découverte, on ignore les sources et la nature de la fuite, son volume réel, la sensibilité des données concernées, la durée de la fuite, la destination des informations), il est primordial que le chef d'entreprise et ses cadres soient assistés dès sa découverte. C'est pour cette raison qu'il faut, en pareille situation, savoir s'entourer.

Avec le Covid-19, le risque de fuite de données a-t-il augmenté ou diminué ?
Le risque de fuite de données est permanent. Ce n'est pas l'apanage de la période d'état d'urgence sanitaire que nous avons connue. Force est de constater pourtant que bon nombre d'entreprises n'étaient pas préparées à vivre la situation au lendemain du 17 mars 2020. Le télétravail a été adopté à grande échelle par la majeure partie des entreprises, sans la préparation idoine. Il a bien souvent été privilégié la continuité de l'activité par rapport à la nécessité de la sécurisation des données, le tout dans la panique.

En soi, le télétravail n'aggrave pas particulièrement le risque de fuite de données. C'est le télétravail non sécurisé qui l'aggrave, notamment si l'employé utilise son matériel personnel à des fins professionnelles (BYOD), notamment s'il conserve des données professionnelles sur ses supports personnels.

Exemple : la veille du confinement, M. X, collaborateur soucieux de préparer son travail à distance, connecte une clé USB à son ordinateur professionnel pour travailler sur certains dossiers. Outre le risque d'infecter le réseau de l'entreprise par divers virus, cette clé USB personnelle, non cryptée, sera connectée ultérieurement à l'ordinateur familial, et son contenu y sera même peut-être copié. Cet ordinateur étant relié à une box, le contenu de la clé USB s'y trouve également copié. Il suffit qu'un des ports de la box soit ouvert et le contenu de la clé USB est donc librement accessible sur Internet. Si le client dispose d'un système de surveillance, il ne tardera pas à le repérer et à demander des explications à l'employeur de M. X.

En dehors de la période Covid-19, existe-t-il des situations où le risque de fuite de données est plus important que d'ordinaire ?
Si le risque est permanent, il convient de remarquer que certaines périodes sont propices à une fuite de données. L'origine peut alors être un acte de malveillance interne, comme un collaborateur qui se « venge » de son supérieur hiérarchique en effaçant des données, une personne qui « prépare » son départ vers une société concurrente en copiant massivement

des données (transferts de courriels, export sur un support externe de documents confidentiels). Dans certains cas, l'entreprise a affaire non à une fuite de données, mais à une disparition de celles-ci. Cette situation se présente lorsqu'un collaborateur rend son matériel professionnel effacé ou sans les codes personnels.

Exemple de jurisprudence : CA Versailles, 01-07-2020, n° 17/04972

Cet arrêt reconnaît que l'utilisation fautive des outils informatiques mis à la disposition du collaborateur et son refus de communiquer les codes d'accès de son ordinateur constituent un motif de licenciement. En l'espèce, le salarié disposait de 3 ordinateurs professionnels, qu'il avait rendus à son employeur. Le premier était vide de données, le deuxième également, mais disposait d'un disque dur ajouté crypté, et le troisième ordinateur contenait des éléments pornographiques.

Dans cette affaire, l'huissier constatait que « le mot de passe avait été modifié le 3 novembre 2014 à 15 h 58 », pour la dernière fois, soit la veille de l'arrêt de travail définitif le 4 novembre 2014 du collaborateur en question.

Quels sont les bons et mauvais comportements en pareille circonstance ?

Il existe plusieurs mauvais réflexes. Le premier mauvais comportement est de croire qu'il est possible de faire face à une pareille situation seul, alors même que son entreprise n'y est pas préparée et n'a jamais eu affaire à ce type de cybermenace. En pareil cas, le risque est d'altérer les preuves informatiques, les rendant presque inutilisables pour les exploiter juridiquement.

Même si la société dispose d'un service informatique performant, il est primordial de recourir aux services d'experts dans ce type d'affaires. En effet, un regard extérieur est toujours utile, sans oublier qu'ils savent comment manipuler l'outil informatique sans l'altérer (le simple fait d'allumer un ordinateur ou un smartphone peut altérer son contenu dans certaines circonstances), disposent d'une grande expérience en la matière et sauront adapter leurs investigations en fonction du contexte.

La deuxième erreur est la conséquence de la première : le retard dans la prise en charge de la cybermenace. En effet, le fait de vouloir régler le problème en interne, en plus de présenter le risque d'altération de la preuve, est chronophage. Tout ce temps perdu avant de confier le dossier à son avocat et son huissier de justice peut compromettre les chances de succès si une suite judiciaire est donnée à l'affaire.

***Exemple** : Il est possible de trouver une illustration dans le cadre d'un contentieux prud'homal (CA Paris, 1er déc. 2015, nº 15/01089, inédit). Un employé avait restitué son ordinateur le 28 juin à son employeur. Ce dernier s'était aperçu de la suppression de fichiers sur ce matériel le 29 juin mais n'avait requis un huissier de justice pour constater la situation que le 16 juillet suivant. Les juges estimèrent que le constat était trop tardif et était insuffisant pour prouver que la suppression des fichiers litigieux était antérieure au 28 juin. Plus généralement, il en est de même si plusieurs mois séparent le fait du procès-verbal de constat (CA Paris, 5 oct. 2016, no 14/20421, inédit. – CA Riom, 15 mars 2017, no 15/03229, inédit. CA Nîmes, 1er févr. 2018, no 16/04730, inédit), ou plusieurs jours si le requérant avait la détention du matériel juridique depuis cette même période (CA Rennes, 20 mai 2016, no 14/03682, inédit). L'appréciation de l'urgence d'une situation n'est donc pas subjective. Ce n'est pas uniquement le risque de disparition de la preuve qui la dicte, mais également son altération par le simple écoulement du temps (CA Paris, 7 mai 2018, no 16/10697, inédit).*

Le bon comportement est évident : faire appel à des professionnels habitués à gérer ce type de situation, sachant qu'au final, il n'y a toujours qu'un seul décideur : le client.

Existe-t-il des règles de base à connaître pour se prémunir de la fuite de données ?
Ces règles de base sont celles de la sécurité informatique élémentaire : renouveler ses mots de passe et que ceux-ci soient fiables, tenir à jour son matériel informatique, sensibiliser les collaborateurs, chiffrer les supports sensibles, limiter les accès… Certaines entreprises recourent même à des sociétés spécialisées pour effectuer des tests d'intrusion informatiques.

En pratique, en cas de départ d'un collaborateur ou d'un associé suspecté de concurrence déloyale ou de vol de données, la précaution de base veut qu'il remette son matériel informatique (smartphone et ordinateur si le smartphone est remis allumé, penser à activer le mode avion, qui empêche un effacement à distance) à un huissier de justice pour qu'il en soit effectué une copie conservatoire préventive. Cette précaution, rapide et très facile à mettre en œuvre, permet ensuite aux services informatiques de la société requérante d'effectuer leurs investigations puisque la copie de l'original aura été faite et sécurisée par l'huissier de justice.

Pour résumer : la fuite de données est une crise que traverse l'entreprise. Si celle-ci est massive, elle peut compromettre gravement son activité. Parce que cette situation est souvent inédite pour l'entreprise concernée, le chef d'entreprise ne doit surtout pas improviser son traitement et savoir s'entourer d'un huissier et d'un avocat pour en ressortir le plus vite possible.