La cybersécurité et le monde du droit

Entretien avec Frans Imbert-Vier, expert en stratégie de cybersécurité

La donnée serait-elle l'or noir du XXIe siècle ? Alors que le tribunal judiciaire de Paris, le ministère de la Justice et de l'Intérieur et des cabinets d'avocats ont récemment été victimes d'attaques informatiques, la protection des données apparaît aujourd'hui primordiale dans le secteur juridique. Frans Imbert-Vier, spécialiste en cybersécurité, nous apporte son expertise sur la question.

Depuis plusieurs années, nous assistons à une multiplication des cyberattaques. Pourriez-vous nous donner quelques chiffres parlants ?

Les statistiques ne manquent pas, mais peu sont vérifiables. Je ne donnerai qu'un chiffre, celui délivré par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), qui indique une croissance de 200 % des attaques cyber par CryptoLocker par rapport à 2019 ; et l'année n'est pas finie. La courbe des attaques est exponentielle, car l'économie se digitalise de plus en plus, mais aussi la société et ses services associés, et enfin les femmes et les hommes dans leurs échanges qui transposent leurs actions sur les réseaux sociaux et dématérialisent ainsi leurs vies. C'est un constat.

En effet, aujourd'hui, les échanges se font majoritairement par mail. De plus, les données, largement dématérialisées, sont enregistrées sur des Clouds ou dans des coffres-forts. Quels sont les risques ?

Il y a toujours un risque inhérent à chaque action. Dans le cadre des échanges d'informations, il est absolu au sens technique. Il n'existe rien d'invulnérable, mais est-ce nécessaire de s'assurer de tout sécuriser ? Ne vaut-il pas mieux pas apprendre à gérer le caractère sensible d'une information plutôt que de tout fermer ou tout ouvrir ? Ma position veut que l'on apprenne à reconsidérer l'information et que chacun puisse la classifier selon l'intérêt individuel et général. Une information intime relève du secret, une information relevant de l'intérêt général devrait être publique, tel un lanceur d'alerte pourrait le considérer. Ainsi donc, on ne peut pas utiliser le même support pour échanger et stocker une information intime et une information publique. Pourtant, c'est ce que l'on fait. Le système numérique est ainsi construit pour que nous mettions sans tri et sans limite toutes les informations que l'on détient et que l'on produit. Cela nous ramène à votre introduction et conforte l'idée que la donnée est probablement l'or noir du XXIe siècle, tout comme l'eau.

Les cabinets d'avocats sont détenteurs de données confidentielles. Sont-ils, à ce titre, mieux protégés contre les attaques informatiques ?

Non, pas du tout. Si l'on s'attarde sur les indépendants et les petits cabinets (moins de 50 collaborateurs), le niveau de protection est nul. Je n'hésite plus à utiliser ce vocable fort pour le dire, car l'effort pour produire une attaque sur un cabinet est proportionnel à sa résistance, et cette dernière est nulle. Deux facteurs expliquent ce constat. Le premier est la culture de l'avocat et la confiance qu'il accorde au système numérique incontournable à son métier. Cette culture émane de la conscience inculquée lors du cursus académique qui n'enseigne ni la notion du secret, ni l'humilité qu'un acteur de justice se doit d'avoir au principe qu'il est assermenté ou référant d'un métier réglementé qui invoque la confidentialité, la protection du témoin et le secret des affaires. On l'aura compris, il n'est pas suffisant de penser que l'on soit soumis au secret des affaires pour se considérer protégé. Le second facteur provient du marché des technologies qui, jusqu'à il y a six mois, ne savait pas proposer une offre technologique performante à un prix supportable pour une petite organisation. C'est ainsi que depuis l'avènement du numérique, l'avocat se trouve exposé comme jamais à la fuite et au vol d'informations, parce que rien de viable financièrement lui permettait de se couvrir. Juste après le confinement, l'un des leaders mondiaux du firewall, l'Israélien Checkpoint, mettait sur le marché une solution permettant de protéger une petite structure de quelques collaborateurs en permettant non seulement de couvrir le réseau de l'organisation, ses ordinateurs et les téléphones pour quelques dizaines d'euros par mois et par utilisateur. Ce type d'offre va se généraliser et ainsi permettre à chacun de s'équiper à un prix supportable avec une efficacité jusqu'alors réservée aux grandes entreprises. C'est sans omettre qu'à partir de ce moment, l'avocat pourra respecter le RGPD et son article 32 invoquant l'obligation de sécurisation du système d'information. Le gain est universel, car il offre un confort pour l'avocat, un respect de la réglementation, une protection de son cabinet et une amélioration du niveau de confiance pour le client.

Frans Imbert-Vier D.R.

L'un des cinq chantiers de la justice concerne la transformation numérique, avec une simplification des procédures en ligne des justiciables et la dématérialisation des données. Y a-t-il lieu de s'inquiéter quant à une éventuelle récupération de ces données ?

J'ai bien peur que oui, car l'État a la fâcheuse habitude de s'appuyer sur les offres des GAFAM (Google, Apple, Facebook, Amazon, Microsoft) pour héberger ses données. On l'a vu avec le scandale du PGE et la BPI qui exploite Amazon pour gérer les prêts Covid, ou le Health Data Care du ministère de la Santé qui s'appuie sur Microsoft. C'est un enjeu de souveraineté qui, en 2020, peut être supporté par les entreprises numériques françaises et européennes, car nous avons la technologie, mais toujours pas le marché. Il est donc probable, compte tenu du comportement de l'État et du gouvernement en place, que rien ne change, malgré des mois d'appels à la réforme des usages numériques pour les services de l'État, qui doit s'imposer de soutenir l'innovation française et européenne pour gérer et héberger ses données. La probabilité que les Américains récupèrent toutes les données, je dis bien toutes, est évidente si l'État ne prend pas les mesures contre. Ceci implique une réforme du Code des marchés publics, une inscription spéciale dans la loi de finances 2021 et, bien sûr, faire ajourner le Plan de Relance de 100 milliards d'un budget de soutien à l'innovation numérique continentale.

La prolifération des legaltechs à laquelle nous assistons nous amène aussi à nous interroger quant à la protection des données déposées sur ces plateformes. Ces start-up sont-elles bien équipées ?

Elles sont censées produire un niveau de sécurité *a minima* conforme aux exigences du Règlement général sur la protection des données (RGPD). Cependant, sur le plan technique, on pourrait douter de la souveraineté produite par leurs architectures, mais avant cela, il est important de connaître la nationalité de l'entreprise, son pays d'exploitation et, bien entendu, la nationalité des détenteurs. Vous savez, la sécurité d'une donnée est conditionnée d'abord par le cadre politique dans lequel elle est produite et par qui elle est détenue. Si je suis en Chine, je suis soumis au droit chinois. Et si je suis Chinois en France, je suis aussi soumis au droit chinois ! Ainsi, la legatech française, hébergée en France avec des actionnaires européens et des capitaux français, est politiquement plus souveraine qu'une legatech américaine qui tombe sous le coup des lois extra – territoriales américaines, à commencer par le *Cloud Act,* le *Cyber Act* et le pire, c'est-à-dire le *Patrioct Act*.

En termes de protections des données, quels conseils donneriez-vous à une start-up fraîchement installée ?

Il ne faut plus considérer la sécurité au sens cyber comme une option des panels d'outils numériques qu'elle utilise. Il y a des solutions françaises peu onéreuses, qui marchent formidablement bien et qui sont souveraines. Cela mettra le client en confiance, distinguera la start up de ses pairs qui n'ont pas encore les bons outils et les bonnes pratiques. Par exemple, utilisez la Suite Office de Microsoft en licence pleine et pas en Office 365 qui utilise le Cloud. Exploitez Seald pour échanger vos pièces jointes avec vos clients. C'est simple, cela coûte 10 euros par mois et cela vous protège complètement, car vous avez la trace d'activité de vos documents. Faites vos visioconférences avec Tixeo et pas sur Zoom. N'utilisez jamais une solution d'échange voix et vidéo américaine ou chinoise. Jamais. Et enfin, mettez un firewall de nouvelle génération pour vous protéger des attaques externes aussi bien sur vos portables que vos téléphones. Avec cela vous avez un sacré coup d'avance à un prix moyen de 50 euros par mois et par collaborateur. Si vous devez utiliser un Cloud, assurez-vous qu'il soit français, cela ne doit pas être discuté. Et n'oubliez pas que la question n'est pas de savoir si vous serez attaqué un jour, mais quand.

Quelles sont les principales cibles des pirates ?

La grande tendance Covid et après Covid, c'est le CryptoLocker, qui chiffre votre disque dur et propose de le déchiffrer contre quelques Bitcoins. Si vous avez une belle sauvegarde, achetez un nouvel ordinateur et le problème et réglé. Cela dit, si vous aviez un *firewall* de nouvelle génération, le problème ne se poserait pas ! Pour les professions assermentées, et les avocats, en particulier, l'enjeu est l'intelligence économique, ou, disons-le clairement, l'espionnage. Dois-je rappeler les écoutes téléphoniques dans l'affaire Sarkozy ? Impensable pour nombre d'avocats, pourtant possible et légale. Si les pénalistes sont par définition les plus sensibles, un avocat du droit social peut, dans une affaire de divorce un peu compliquée, être facilement la cible d'un *dataleaks* (vol de données) en vue de servir les intérêts de la partie adverse. À ce jour, pour quelques milliers d'euros, vous pouvez avoir une bonne information qui peut vous en faire gagner des millions. C'est assez tentant et de plus en plus fréquent. Les organisations cybermafieuses de l'Europe de l'Est sont assez bien dotées et ont des offres étonnantes sur quelques places de marchés hébergées par des sites russes.

Que savons-nous de ces pirates du net ?

Le rapport d'Interpol de 2017 évoquait un budget de R&D, pour une organisation cyber mafieuse, supérieur à 2 milliards d'euros, quand l'Europe débloque 6 millions pour se protéger des *bots* russes lancés en amont de la campagne européenne ! Les organisations criminelles ont des niveaux d'expertises et techniques équivalents à ceux d'une grande puissance numérique (France, Allemagne, UK, USA, Chine, Russie). Les petits *hackers* s'améliorent de plus en plus et surtout, ils sont de plus en plus nombreux, car c'est une vraie économie parallèle. Dès lors, la technologie d'attaque est plus accessible, moins chère et intéresse donc plus de monde, à commencer par le trafic de drogue qui dépérit en raison de la légalisation douce de plus en plus évidente en Europe et un marché saturé. Le numérique implique un investissement faible, le risque est presque nul et peut être tout aussi profitable pour ceux qui sont un peu malins et qui travaillent bien !

Que se passe-t-il après une attaque ? Que deviennent les données ainsi récupérées ?

Un vol de données, c'est un *dataleaks*. Soit on l'exploite contre vous et on applique un chantage contre une rançon, sans quoi l'information sera mise en ligne publiquement. Soit on n'en fait rien et elle bénéficie à l'intelligence économie, autrement dit vos adversaires qui sauront mieux se défendre contre vous, ou bien elle sert à nuire, comme l'affaire Grivaux par exemple. Si vous avez un *firewall* et un disque dur chiffré, le problème du *dataleaks* est réduit à néant, enfin presque. Il reste encore la torture comme moyen de coercition.

Dans le prolongement, quels conseils donneriez-vous à une entreprise ou un cabinet qui viendrait de se faire attaquer ?

Cette question est très importante. Si vous voyez un comportement anormal sur un ordinateur, éteignez-le et courez débrancher la connexion Internet de l'entreprise pour stopper la circulation des informations. Appelez votre avocat ou votre confrère spécialiste qui mettra en place les acteurs spécialistes comme un expert cyber, votre assurance et la gestion de la communication. Cela produira une cellule de crise qui évaluera pour vous l'ampleur du risque, des dégâts et la meilleure stratégie pour protéger l'image et les clients, mais aussi la remise en état. N'appelez surtout pas votre partenaire informatique. Il voudra bien faire et risque fort d'aggraver sans le vouloir la situation. Porter plainte est absolument nécessaire ne serait-ce que pour votre assureur. Enfin, apprenez qu'une attaque contre son entreprise, est une action très violente, tout autant pour les collaborateurs. Le déni est vite le meilleur sentiment, mais le pire allié. Garder son sang-froid, gérer son émotion et s'appuyer sur l'expertise de crise comme celle du groupement d'avocats WeLawCare qui accompagne, avec l'expertise qui se doit, ce type d'événement qui, au final, reste très marquant.

Enfin, comment la France se situe-t-elle en termes de protection des données ?

Le RGPD est très difficilement applicable, surtout pour les petites structures. Plus de 80 % des entreprises n'a pas de *firewall* et moins de 2 sur 5 ont une sauvegarde viable. Autant dire que ce n'est pas terrible, mais nos voisins ne sont pas mieux. Au niveau étatique, c'est en revanche dramatique, car l'État va au plus simple et concède tout aux sociétés américaines. De la gestion du renseignement avec Palentir à la fourniture des solutions académique avec Mircosoft pour l'Éducation nationale, je me sais dur et sec en invoquant l'absence de souveraineté pour l'ensemble de nos données civiles, c'est-à-dire la *data* citoyenne. Il y a eu des progrès grâce à quelques acteurs privés, mais la France reste très en retard. En revanche, l'ANSSI est une agence qui est très performante, mais mériterait plus de moyens pour accompagner les entreprises. On regrette toujours que le MEDEF, mais aussi les CCI, les chambres des métiers et la BPI ne considèrent pas comme prioritaire la mise en œuvre d'une politique de protection de nos données dans un cadre souverain. On est en 2020 et les efforts produits restent encore très insuffisants.

Propos recueillis par Constance Périn

2020-6243