N°85
Mars-Avril
2021

www.village-notaires.com

Le Journal du Village des Notaires

Actualités

Enquête

Management

Associations

Gestion de patrimoine

Immobilier

Communication

Zoom sur

Veille juridique

legiteam Editions

ANNUAIRE DES TRADUCTEURS ASSERMENTÉS DE FRANCE

Liste des traducteurs experts pour 2020 selon les données officielles du Ministère de la justice

+ de 4500 experts de cour d'appel disponibles

Avec plus de 128 langues à disposition, nous sommes capables de répondre aux demandes de traductions assermentées que ce soit pour les documents écrits (procuration, acte notarial, succession, acte de vente ...) ou pour les interprètes avec mise à disposition des coordonnées pour prendre un rendez-vous pour les déplacements à l'étude notarial.

Nous répondons à vos demandes sous 60 minutes.

Pour toute demande de cotation, merci de nous écrire à pro@annuaire-traducteur-assermente.fr ou par téléphone au (0)9.70.44.63.45

LE JOURNAL DU VILLAGE DES NOTAIRES

est édité par LEGI TEAM
198 avenue de Verdun
92130 Issy-les-Moulineaux
RCS B 403 601 750

Directeur de la publication
Pierre MARKHOFF
pmarkhoff@legiteam.pro

Abonnements
smorvand@village-notaires.pro
Tél : 01 70 71 53 80

Imprimeur
JF IMPRESSION
Garo Sud
296 rue Patrice Lumumba
CS97874
34075 Montpellier Cedex 3

Publicité
Régie exclusive : LEGI TEAM
198 avenue de Verdun
92130 Issy-les-Moulineaux
Tél : 01 70 71 53 80
Site : www.legiteam.fr

Responsable
Sandrine MORVAND
smorvand@village-notaires.pro
Tél. : 01 70 71 53 88

N° ISSN 2103-9534

Rédaction
Simon Brenot
simon@village-justice.com

Aude Dorange
a.dorange@legiteam.pro

Alain Baudin

Jordan Belgrave

Maquette
Cyriane VICIANA
pao@legiteam.pro

Diffusion
7 000 exemplaires

Édito

En 2020, dans un contexte de généralisation du télétravail, les signalements d'attaques par des virus informatiques et rançongiciels ont crû de 255 % en France.

Les études notariales ne sont pas épargnées par ces attaques, et il incombe à la profession de fournir outils, conseils et formations pour assurer la protection de tous, garantir l'identification puis la confidentialité des échanges avec nos clients, et sécuriser les flux financiers qui passent par notre comptabilité.

L'infrastructure Intranotaires portée par la Chambre de Paris (messagerie électronique, transfert de fichiers volumineux), Notmail Archives, sont autant de services robustes qui garantissent la sécurité des offices au quotidien. Nous continuerons à les renforcer.

Mais la cybersécurité doit être l'affaire de tous, car la plupart des cyberattaques qui réussissent, et il y en a, y parviennent à cause du « *facteur humain* ». La vigilance doit s'imposer à travers une formation régulière des équipes, la séparation des usages professionnel et personnel, la sécurisation des téléphones, le changement régulier des mots de passe, les mises à jour logicielles, la mise en place de procédures internes, ou bien encore une précaution particulière avant toute ouverture de pièce-jointe. Ces « gestes barrières » constituent notre meilleure protection collective.

Cédric BLANCHET
Président de la Chambre des Notaires de Paris

SAUVEGARDE DE DONNÉES

LE DERNIER REMPART

Firewall, antivirus, antispam...
vos données vous semblent bien protégées

Ransomware, erreur de manipulation, cambriolage, incendie, malveillance, piratage...
Seule une solution efficace de sauvegarde de données vous protège réellement.

Récupérez vos données rapidement et intégralement quoi qu'il arrive

Expert Notaires

Beemo, expert des solutions de sauvegarde de données notariales depuis 2002 s'appuie sur un réseau national de partenaires certifiés. Beemo propose la seule solution de sauvegarde validée par la Chambre des notaires de Paris et équipe déjà plus de 1600 études notariales.

Beemo

Protégez votre activité,
sauvegardez vos données

Solution Française

Audit Gratuit au :
0 800 711 500 Service & appel gratuits

www.beemotechnologie.com

Les offices notariaux sont-ils exposés au **risque cyber** *?*

L'une des particularités du notariat est de s'être très rapidement emparé des outils digitaux et des *process* dématérialisés. Forte d'une transition numérique amorcée depuis au moins une vingtaine d'année, la profession a réussi son virage numérique et continue d'avancer en la matière. Elle veille scrupuleusement à un développement éthique du numérique, en protégeant les droits, les données et, plus largement, les intérêts de ses clients. Le Conseil Supérieur du Notariat a néanmoins récemment attiré l'attention des professionnels en raison d'une recrudescence des tentatives de fraudes, d'usurpation d'identité et de défigurations de sites internet visant spécifiquement les notaires[1]. L'occasion, pour la Rédaction du *Journal du Village des notaires*, de s'interroger sur l'exposition des notaires au risque cyber.

1. La cybersécurité, de quoi parle-t-on ?

Cybersécurité, cyberattaques, cyberrésilience… La « *cyber* » est partout ; impossible d'en faire abstraction. Une stratégie nationale de cybersécurité vient d'ailleurs d'être annoncée[2]. Si le sujet n'est pas très séduisant de prime abord, il est pourtant l'un des enjeux majeurs de la transformation numérique.

La cybersécurité[3] « *n'est pas qu'une question liée à la technologie, mais une question pour laquelle le comportement humain est tout aussi important*[4] ». Elle comporte deux volets. Le premier est sans aucun doute technique. Il repose sur la protection des outils numériques et des réseaux et systèmes d'information. Les besoins en cyberprotection se mesurent en termes de confidentialité[5], de disponibilité[6] et d'intégrité[7] des données et informations[8] ; toutes les informations et données confiées ou créées par le notaire sont concernées, quels qu'en soient les supports.

Le second volet de la cybersécurité est comportemental. Veiller à la sûreté numérique d'une organisation, de quelque nature qu'elle soit, n'est en effet pas qu'une question de sécurité technique des équipements et des logiciels. « *Le sujet est encore trop souvent vu sous un angle technique alors qu'il est essentiellement organisationnel*[9] ». Cet aspect de la cybersécurité

1 - Voir S. Brenot, « Cyberattaques contre les sites des notaires : appel à la vigilance », www.village-notaires.com.
2 - ANSSI, Communiqué de presse, 19 févr. 2021, « Cybersécurité, faire face à la menace : la stratégie française », www.ssi.gouv.fr.
3 - « État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles » (Glossaire de l'ANSSI, www.ssi.gouv.fr).
4 - Cons. 8, Règl. (UE) 2019/881, 17 avr. 2019, JOUE L 151/15, 7 juin 2019.
5- Caractère réservé d'une information ou d'un traitement dont l'accès est limité aux seules personnes admises à la (le) connaître pour les besoins du service, ou aux entités ou processus autorisés (ANSSI, « La cybersécurité des systèmes industriels, Méthode de classification et mesures principales », www.ssi.gouv.fr).
6 - Propriété permettant de rendre le service attendu en temps voulu et dans les conditions d'usage prévues (ANSSI, La cybersécurité des systèmes industriels, précité).
7 - Garantie que le système et l'information traitée ne sont modifiés que par une action volontaire et légitime (ANSSI, Glossaire, www.ssi.gouv.fr).
8 - Ces propriétés répondent aux besoins en cybersécurité. S'y ajoute également un besoin en termes de traçabilité et de preuve, permettant d'identifier l'origine et de reconstituer le parcours d'un « bien essentiel » depuis sa production jusqu'à son utilisation. L'idée est de pouvoir retrouver les circonstances dans lesquelles les données et outils ont évolué : traçabilité des actions menées, authentification des utilisateurs, imputabilité du responsable de l'action effectuée.
9 - Cigref, 2016, « Le cyber risque dans la gouvernance de l'entreprise », www.cigref.fr.

concerne la sensibilisation de l'utilisateur aux risques. Les dangers sont nombreux, mais ils peuvent « *être fortement réduits par un ensemble de bonnes pratiques, peu coûteuses, voire gratuites, et faciles à mettre en œuvre*[10] ». Tel est le but des nombreux guides édités pour prodiguer des conseils en matière de bonnes pratiques numériques[11].

2. Être « *cyber friendly*[12] », pour quoi faire ?

La mise en place de mesures de cybersécurité a d'abord pour vocation de limiter le risque de la survenance d'un incident cyber, qui a de nombreuses conséquences. Les effets d'une fuite d'informations relatives à la situation matrimoniale d'un client, particulièrement s'il est connu, sur le contenu d'un testament peuvent être imaginés sans mal. Du côté de l'étude, que dire des conséquences de l'usurpation de l'identité d'un notaire, du détournement d'une remise de fonds ou d'émoluments ou de l'envoi d'un document piégé par mail ? Les impacts sont multiples : sur le fonctionnement (capacité de l'étude à réaliser les prestations attendues) ; impacts humains (menaces ou mise en danger d'une personne, perte de confiance des collaborateurs et salariés, etc.) ; impacts juridiques (engagement de la responsabilité, obligations de notification) et financiers (perte de chiffre d'affaires, dépenses liées au rachat d'équipements, à la restauration des données, aux frais d'expertise et autres « pénalités »), sans oublier, bien sûr, l'impact sur la réputation du praticien. La cybersécurité s'avère, à tous ces égards, être un levier de la pérennité de l'activité des offices.

L'étude et ses membres peuvent être les victimes directes d'un incident cyber. En outre, comme pour d'autres professionnels du droit, il est possible d'accéder, par l'intermédiaire du notaire, à une multitude d'informations qui ne sont généralement pas accessibles (ou sont éparpillées) ailleurs. Par ricochet en quelque sorte, l'auteur de l'acte de cybermalveillance accèdera donc aux données et informations du client. C'est précisément la détention de ces informations, qui doivent rester confidentielles, qui expose les notaires au risque cyber.

Les enjeux d'une gouvernance de l'information soucieuse de la cybersécurité se mesurent dès lors sur le terrain du secret professionnel, que l'activité soit exercée à titre exclusif (successions, donations authentiques, ventes immobilières, etc.) ou en dehors du monopole notarial (gestion immobilière, conseils aux particuliers et aux entreprises , etc.). Le notaire est le « *confident nécessaire de ses clients*[13] ». Le secret professionnel « *général et absolu* », « *couvre tout ce qui a été porté à la connaissance du notaire dans l'exercice de ses fonctions*[14] ». Or, avec la digitalisation, les contours de la confidentialité se modifient. La garantie de confidentialité et l'opposabilité du secret professionnel sont mises à mal dans le cyberespace. La Charte pour un développement éthique du numérique notarial l'envisage clairement : « *les signataires s'engagent à la confidentialité de leurs rapports avec leur clientèle. Ils reconnaissent l'absolue nécessité de garantir le secret professionnel et conviennent que les données des clients finaux qui leur seront confiées ne sauraient être stockées, échangées ou traitées hors d'un cadre sécuritaire adéquat*[15] ».

10 - ANSSI-CPME, « Guide des bonnes pratiques de l'informatique, 12 règles essentielles pour sécuriser vos équipements numériques », www.ssi.gouv.fr.
11 - Voir not. le site de la CNIL, le site www.cybermalveillance.gouv.fr ; ANSSI, 2017, « Guide de l'hygiène informatique. Renforcer la sécurité de son système d'information en 42 mesures », www.ssi.gouv.fr ; ANSSI-CPME, 2018 (MàJ 2020), « Guide des bonnes pratiques de l'informatique : 12 règles essentielles pour sécuriser vos équipements numériques », www.ssi.gouv.fr ; CLUSIF, 2020, « Livre blanc La cybersécurité à l'usage des dirigeants », www.clusif.fr ; ANSSI, févr. 2021, « La cybersécurité pour les TPE/PME en 12 questions », www.ssi.gouv.fr.
12 - Vous nous pardonnerez l'emploi de cet anglicisme ! Il est vrai que les mots français « sympathisant » ou « accueillant » seraient peut-être plus convenables pour désigner cette démarche d'ouverture d'esprit consistant à s'intéresser à la cybersécurité.
13 - Art. 3.4, Règlement national du notariat.
14 - *Ibid.*
15 - Charte précitée.

3. Quelles sont les menaces pesant sur les études ?

Les menaces sont multiples[16] : utilisation illégale d'un mot de passe, vol ou perte d'équipements informatiques, logiciels malveillants et virus informatiques, piratage d'objets connectés, comportements négligents ne sont, malheureusement, qu'une partie des cas auxquels les études notariales peuvent être confrontées. La plupart des *malware*[17] se déploient à partir d'une pièce jointe à un courriel ou d'un autre élément téléchargeable (photos, vidéos, musique, logiciels, appli, etc.). Le « *hameçonnage* »[18] est aussi très répandu, sans parler des *ransomware*[19] , considérés comme la « *menace la plus sérieuse pour les organisations*[20] » : dans ce type d'attaques, ce n'est pas l'accès aux informations elles-mêmes qui compte, comme le dit notamment Mélanie Biberian, *Channel Director* de *Beemo Technologie*[21], « *c'est vraiment une prise d'otage des données et face à ces attaques, la sauvegarde reste le dernier rempart pour redémarrer l'activité sans avoir à payer de rançon* ».

Plus largement, les outils digitaux peuvent tous, peu ou prou, être détournés, espionnés, modifiés ou perdus. D'où l'importance de choisir avec soin les solutions utilisées, particulièrement en temps de travail à distance. À côté des failles[22] de sécurité et des moyens techniques utilisés, il faut prendre la mesure des dangers de l'ingénierie sociale : une personne insuffisamment sensibilisée aux risques, peut être manipulée (corruption, chantage, harcèlement, satisfaction de l'ego, etc.) pour divulguer des données confidentielles ou réaliser d'autres actions (virement bancaire, communication d'un mot de passe, accès physique aux locaux, etc.).

Ceci fait bien sûr l'objet d'une attention particulière du notariat. La note du CSN sur les procurations électroniques et la comparution à distance en est un bon exemple : « *pour faire écho à la charte pour un développement éthique du numérique notarial, le recours à des solutions de signature électronique sous seing privé, veillera à utiliser a minima des solutions de niveau « avancé » au sens du Règlement européen eIDAS*[23]*. En conséquence les signatures de niveau « simple » ne doivent pas être utilisées dans la mesure où le niveau de garantie apporté est bien plus faible* [24] ». Cette préoccupation anime les travaux sur la blockchain notariale, qui, « *par son organisation et l'usage de mécanismes de cryptographie très élaborés (…) permet de certifier qu'une transaction est fiable et certaine*[25]». Les signataires de la Charte pour un développement éthique du numérique notarial « *s'engagent, lorsqu'ils recourent à des services d'informatique en nuage, à s'appuyer sur des prestataires qualifiés par l'ANSSI au niveau essentiel* »[26].

4. Comment gérer sa cyber-vulnérabilité ?

Qu'il s'agisse de prévention ou de réponse à un incident cyber, « *plus les choses auront été préparées en amont, (…) plus la gestion de la crise pourra être efficiente*[27] ». Côté prévention, les solutions sont autant techniques, que liées à la sensibilisation des utilisateurs. Quatre axes peuvent être explorés, sans nécessiter un budget important : les mots de passe, qui doivent être robustes[28] et uniques[29], la sauvegarde régulière des données pour éviter que leur perte soit irréversible, la sécurisation des systèmes d'information (antivirus, pare-feu, connexion wifi sécurisée, chiffrement, etc.) et l'adaptation aux nouvelles façons de travailler (séparation des usages professionnels et personnels, utilisation responsable d'internet, VPN[30] sécurisé, maîtrise des réseaux sociaux, etc.). Spécifiquement en ce qui concerne la sauvegarde des données, pensez à la règle du « *3 2 1* », véritable maxime chez *Beemo Technologie* : « *3 points de stockage de vos données, sur 2 supports différents et 1 copie en dehors des locaux* » ! L'entreprise recommande une solution de sauvegarde automatique, quotidienne, de préférence sur un serveur dédié indétectable au *ransomware*,

16 - Voir not. V. Marchive, « 2020 : l'Anssi et Acyma tirent le bilan d'une année explosive sur le front des cyberattaques », LeMagIT, 13 janv. 2021.
17 - Pour *malicious software*, logiciels malveillants.
18 - Ou *phishing*, qui vise à obtenir du destinataire d'un courriel frauduleux (mais d'apparence légitime), qu'il transmette ses coordonnées bancaires ou ses identifiants de connexion ou bien encore qu'il mette à jour des données personnelles détenues par un tiers de confiance (services financiers, réseaux professionnels, administrations, etc.).
19 - Qui vont empêcher l'accès aux données en les rendant illisibles jusqu'à l'utilisation d'une « clé » pour les déchiffrer fournie par le cybercriminel à la suite du paiement d'une rançon.
20 - Voir not. Guide ANSSI-DACG, sept. 2020, « Attaques par rançongiciels, tous concernés. Comment les anticiper et réagir en cas d'incident ?», www.ssi.gouv.fr.
21 - Beemo Technologie propose des solutions complètes et fiables pour assurer la sauvegarde des données et la reprise d'activité en cas de sinistre ; www.beemotechnologie.com.
22 - Les failles sont des « *vulnérabilité[s] dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal* » (ANSSI, Glossaire, « Faille », www.ssi.gouv.fr).
23 - Règl. (UE) n° 910/2014, 23 juill. 2014, JOUE L 257/73, 28 août.
24 - CSN, Circ. n° 1577, accessible not. sur https://www.cridon-ne.org/wp-content/uploads/2020/04/note_dinformation_du_4_avril_2020.pdf
25 - Notaires du Grand Paris, 7 juill. 2020, « Présentation de la blockchain notariale », Dossier de presse, https://notairesdugrandparis.fr.
26 - CSN, 2018, « Charte pour un développement éthique du numérique notarial », www.notaires.fr.
27 - INHESJ, juill. 2015, « Comment organiser une cellule de crise en cas de cyberattaque ? », Travaux des auditeurs, www.cigref.fr.
28 - 12 caractères (au minimum) et de type différent (majuscules, minuscules, chiffres et caractères spéciaux) et proscrire ceux liés au prénom des enfants, sa date anniversaire, ainsi que les suites logiques simples (123456, azerty, abcdef…).
29 - En utilisant un mot de passe différent pour chaque service afin de cloisonner les comptes.
30 - *Virtual private network* : sorte de tunnel de communication privé et chiffré pour permettre l'accès à distance, par les utilisateurs authentifiés.

avec un historique de vos données de plus de 30 jours et une réplication en dehors de l'étude, si possible dans un centre de stockage sécurisé.

Pour que toutes ces actions puissent être menées, la sécurité doit être l'affaire de tous les membres de l'étude : notaires, clercs, secrétaires, formalistes, comptables, négociateurs immobilier, stagiaires. Au-delà des chartes informatiques, les supports de sensibilisation à la cybersécurité se sont aujourd'hui diversifiés, les acteurs misant notamment sur l'acculturation par le jeu et la mise en situation.

En dépit d'une bonne sécurisation des équipements informatiques et d'une sensibilisation efficace et régulière des utilisateurs, le risque d'une cyberattaque ne peut pas être complètement écarté. Loin de nous l'idée de vouloir véhiculer un discours alarmiste et/ou culpabilisant. Le risque zéro n'existe pas, mais il faut être en mesure de démontrer que tout à été fait pour limiter le risque autant que possible, le système assurantiel intervenant pour couvrir les risques résiduels[31]. C'est adopter une posture non de culpabilité, mais de responsabilité[32]. C'est à la fois se mobiliser pour la promotion des valeurs de la profession et répondre à un enjeu plus global : « *qu'on le veuille ou non, la cybersécurité est devenue un enjeu sociétal* »[33].

A. Dorange
Pour le Journal du Village des Notaires

31 - Voir S. Brenot, « Cyberattaques : assurez vos arrières ! », *Journal du Village des notaires* 85, p. 21.
32 - Au sens du principe d'accountability.
33 - CLUSIF-OSSIR, janv. 2020, « La cybersécurité à l'usage des dirigeants », Livre blanc, https://clusif.fr.

Développer sa résilience face aux **crises cyber** *?*

La résilience prend progressivement le pas sur la sécurité comme concept central de l'informatique, afin d'appréhender les dynamiques de manière multidimensionnelle. Car la probabilité de se faire attaquer et pirater est tellement élevée que la question n'est plus seulement d'organiser la défense, mais également de minimiser l'impact d'un piratage réussi. Pour cela, il faut réagir vite et de la bonne manière.

En 2019, plus de 41% des entreprises de moins de 49 salariés avaient subi une ou plusieurs attaques ou tentatives d'attaques informatiques, qui se répartissaient ainsi pour les principaux types : 24 % de hameçonnage, 20 % *malware*, 16 % de *ransomware* (rançongiciel) et 6 % de fraude au président. En 2020, la tendance est encore plus forte puisque, selon l'éditeur de sécurité *Proofpoint*, 91 % des entreprises auraient été visées, et 65 % l'auraient été à plusieurs reprises. Nul n'est à l'abri, puisque les éditeurs de logiciels et de services numériques sont eux aussi fortement touchés, comme la française *Sopra Steria*, ou l'américaine *Solar Winds*, dont la faille de sécurité a mis en danger un grand nombre de grandes entreprises et de structures gouvernementales aux États-Unis.

Si tout le monde est concerné, le monde notarial a bien sûr ses spécificités. D'une part, il est constitué de TPE-PME, avec, d'une part, une moindre exposition médiatique que les grands groupes, et une plus grande facilité à communiquer en direct avec les autres membres de l'étude dès qu'un problème semble émerger, sans avoir à passer par les réseaux – un avantage que le télétravail pourrait venir entamer.

Les études notariales bénéficient aussi d'un avantage spécifique face au risque cyber qui est que la plupart d'entre elles ont un backup papier et une pratique encore pas totalement numérisée, qui leur permet de pouvoir continuer partiellement leur activité en cas de crise.

En revanche, les notaires traitent des données qui sont non seulement sensibles d'un point de vue financier, mais relèvent pour certaines de l'intime – testaments, contrats de mariage,… ce qui leur donne une responsabilité particulière dans la protection des données personnelles.

Les notaires sont-ils pour autant conscients du danger ? « *Malgré une prise de conscience progressive,* explique Arnaud Gressel, expert chez Resco Courtage, *il y a une erreur que j'observe de manière récurrente, qui est de croire que l'on n'est pas concerné parce qu'on n'est pas une cible. Mais c'est sous-estimer le fait qu'il n'y a pas besoin d'être une cible pour être attaqué. Les campagnes d'emailing captent très, très large, et l'on reçoit tous les jours des faux e-mails sur lesquels il suffit que quelqu'un clique une fois. Pour l'instant, je constate que ce sont surtout lorsque des structures ont été touchées ou victimes à un moment donné ou qu'elles ont vu de près une crise qu'elles sont les plus sensibilisées* ».

Comment réagir face à la crise ?

L'élément central d'une crise cyber est la perte de repères. « *Contrairement à des entreprises de grande taille,* indique Emmanuelle Hervé, experte en gestion de crise chez *EH&A, les petites structures se retrouvent seules, sans conseil d'administration derrière, sans comité d'étude des risques qui leur aurait dit, en amont, qu'il faut se préparer à ceci ou cela et comment le faire. Il y a beaucoup d'intuitu personae dans les petites structures, et la personnalité des dirigeants a beaucoup d'influence sur les décisions prises, car ils n'ont pas en interne de système expert d'aide à la décision, qui les aide à déterminer si une situation est suffisamment crisogène pour justifier l'ouverture d'une cellule de crise. Donc, quelle que soit la taille de l'entreprise, la gestion de crise ne s'improvise pas, il y a des processus et des méthodes qu'il convient de travailler en temps de paix* ».

Une situation de crise cyber est donc marquée par la confusion : les ordinateurs ne marchent plus, les mails ne passent plus, l'activité est interrompue. Le dirigeant se retrouve très démuni car il ne sait pas quelle est l'étendue des dégâts : est-ce qu'il y a des *data* volées ? Sont-elles juste cryptées ? Quels types de *data* sont concernées ? Quel volume ? Il est normal d'être déboussolé mais il faut d'abord être clair sur les priorités : redémarrer le plus tôt possible tout en préservant le capital confiance de l'étude. Pour cela, il est indispensable de se faire aider.

« *Le but,* souligne Delphine Mercelat, Directrice des assurances du notariat chez *LSN assurances*, *est que l'étude contacte au plus vite l'assurance afin que le sinistre soit géré en un minimum de temps et que l'activité soit interrompue le moins possible. Plus le notaire réagit vite, plus il nous déclare le sinistre vite, plus ça peut être réglé vite. S'il tarde un peu, le virus peut alors se diffuser et atteindre tout le réseau informatique de l'étude* ».

Un réflexe récurrent mais qui n'est pas pertinent est d'appeler le prestataire informatique habituel, parce que, d'une part, celui-ci n'a peut-être pas forcément le même temps de réactivité ni la même disponibilité que les experts de l'assurance et, d'autre part, le côté cyber peut être quelque chose de nouveau et de compliqué à gérer pour lui. Il n'aura peut-être pas le réflexe de gérer l'incident avec une approche d'expert qui consiste à sauvegarder les preuves pour l'indemnisation et le recours, ou pourrait avoir tendance à débrancher le système informatique alors que certains éléments peuvent encore être sauvés.

Aux côtés de la réponse informatique, les autres pans de la réponse à la crise sont, d'une part juridique, et d'autre part communicationnel. Dans tous ces domaines, la bonne démarche consiste à recourir aux experts mis à disposition par les assurances.

Si le notaire n'a pas la main sur les aspects informatique et juridique, il doit néanmoins concentrer toute son énergie sur la gestion de crise et sur la communication. Une difficulté principale dans une telle situation est qu'il est presque impossible de savoir combien de temps les opérations en cours – déchiffrage, négociation – vont durer : quelques heures, quelques jours ou quelques semaines.

Pour organiser ces aspects, une réunion de crise doit être organisée au plus vite. Elle peut ne prendre que quelques heures, et permet de clarifier les priorités pour cette situation exceptionnelle : « *pour bien analyser tous les scénarios d'évolution,* indique Emmanuelle Hervé, *il faut partir de l'événement et se demander : comment cela peut-il empirer ? Même si*

Que faire en cas de demande de rançon ?

S'ils sont à la recherche de rançons importantes, les hackers ne vont pas viser de notaires, mais des grandes structures. Toutefois, les *ransomwares* génériques circulent, et fonctionnent, puisqu'un certain nombre d'entreprises se font piéger et finissent par payer. S'il faut savoir que la recommandation classique en France, en cas de *ransomware*, est de ne surtout pas payer, une observation essentielle est que « *les entreprises assurées contre le cyber payent beaucoup moins de rançons que les sociétés qui ne sont pas assurées*, précise Arnaud Gressel, expert chez *Resco Courtage*, *du simple fait qu'elles ont une assistance immédiate dès les premières heures. Tout va plus vite, les données vont être mieux préservées, et la pression est moindre. Quand une entreprise est livrée à elle-même, elle va plus facilement se dire qu'il vaut mieux payer pour survivre* ».

l'on a envie de se dire que ça va s'arranger, il faut faire cet effort intellectuel. Si toute l'informatique est bloquée pendant des mois, quelle continuité d'activité est possible ? Si des datas sensibles sont dehors, quels sont les impact côtés clients et employés ? et côté CNIL ? Que faire si nous prenons une amende de 4 % du CA et une procédure au pénal ? il faut balayer toutes les grandes dimensions de la crise par catégorie, business, financier, juridique, humain, réputationnel et dérouler les scénarios d'évolution défavorables jusqu'au bout. C'est ça qui est difficile en général, c'est de le faire jusqu'au bout et, ensuite, de remonter dans l'autre sens en se demandant ce qu'on peut faire pour, soit baisser la probabilité d'occurrence des scénarios qu'on vient de développer, soit diminuer l'impact si jamais ça arrive quand même. Et donc, ça, c'est vraiment un travail à faire en démarrage de gestion de crise ».

Une autre démarche indispensable à réaliser, qu'il aurait même été préférable de réaliser en amont, est la cartographie de toutes les parties prenantes de l'étude. En externe : identifier les clients importants qui vont particulièrement s'inquiéter d'un éventuel vol de données et les appeler directement pour leur assurer que le maximum est fait. En interne : aller parler aux employés qui peuvent craindre pour la perte de leur emploi, ou qui se sont fait voler des photos compromettantes qu'ils gardaient sur l'ordinateur de bureau, et qui peuvent avoir peur qu'elles fuitent. S'il est encore temps, c'est l'occasion de mettre sur papier l'ensemble des contacts pour pouvoir communiquer avec ces personnes même si toutes les données ont été perdues ou bloquées.

Jordan Belgrave

Jean-Marc Couret, notaire à Toulon : « *Je suis très attentif à la protection informatique* »

J'ai mis en place un système automatique de sauvegarde toutes les six heures, que je contrôle régulièrement : trois sauvegardes sur place sur trois serveurs différents plus une sauvegarde en extérieur, donc quatre sauvegardes redondantes. Le backup des bases de données a lieu la nuit et est répercuté sur mes différentes sauvegardes. Je réalise également une copie des images virtuelles de mes serveurs et de mes postes clients une fois par mois. C'est une opération manuelle que j'ai quand même grandement automatisée, mais je dois arrêter moi-même les machines pour éviter que le processus ne démarre alors qu'elles sont en cours de fonctionnement. De la sorte, j'ai une redondance d'informations et je peux réinstaller les postes en partant de zéro et redémarrer l'activité très facilement. À ce niveau-là, on peut difficilement faire plus.

Les ordinateurs de notre étude font tourner des machines virtuelles Windows sous Linux, car je trouve que Linux a une plateforme stable et sécurisée, notamment pour les serveurs (ne pas oublier que plus de 60 % des serveurs servant d'infrastructure d'internet sont des machines Unix (Linux ou BSD)... C'était encore plus vrai avant Windows 10. Sous Linux, les machines sont, par défaut, en mode utilisateur et, quand vous avez de l'administration à faire, vous entrez seulement à ce moment-là en mode administrateur. La base de la sécurité informatique est que seuls l'informaticien ou le dirigeant aient le statut administrateur. Sans quoi, tout le monde peut s'installer des logiciels sur sa machine et risquer d'infecter des postes. Dans le même esprit, les ports USB sont désactivés par défaut.

Il est certain que la virtualisation ralentit un petit peu les machines par rapport à une machine exécutant en direct Windows, mais on est sur un niveau de sécurité supplémentaire parce que, si la machine Windows est piratée, les machines sous Linux, et notamment les serveurs, sont mieux protégées. La sécurité informatique absolue n'existe pas, mais mon système permet au moins de limiter les risques et de traquer d'où a pu partir la fuite.

J'ai déjà eu une attaque au crypto-virus sur un serveur Windows. J'ai interrompu toutes les machines de l'office, étant sensibilisé aux principes de sécurité informatique et d'isolation des postes. Une fois que tous les ordinateurs étaient éteints, j'ai pu les vérifier chacun indépendamment sans connexion avec le réseau, puis réinstaller une image virtuelle de sauvegarde sur les postes contaminés, déterminer le serveur et restaurer les données corrompues. Tout cela m'a pris quatre heures et, le lendemain, toute l'informatique était opérationnelle sur l'étude. Pour le même problème, un confrère a eu 15 jours d'immobilisation de son étude.

*Les nouveautés de l'*archivage notarial *?*

L'archivage fait partie de l'ADN des notaires : préserver le passé pour assurer leur mission aujourd'hui et préparer la transmission en bon ordre à ceux qui viendront après. Pour autant, les choix sont nombreux et variés, et font jouer tout autant des aspects financiers, organisationnels, que culturels, entre partisans du zéro papier et sceptiques du numérique, ainsi que dans l'appréhension des diverses technologies disponibles.

L'archivage est d'abord une question d'organisation : « *Je me suis rendu compte,* souligne Françoise Cohen-Cassuto, dirigeante d'*Un dossier Une place*, *que la plupart des gens ne savent pas contextualiser, titrer ou simplement classer comme les normes professionnelles d'archivistique le recommandent. C'est bien normal : bien classer, bien nommer, ce n'est pas le cœur de l'activité des professionnels ! Pour cette raison, une fois que le paramétrage des délais d'archivage est déterminé et que l'arborescence est en place, il est beaucoup plus pertinent de confier ces tâches à un logiciel* ». Un tel logiciel intègre donc le cycle de vie des dossiers et documents dans leur intégralité, pour les dossiers papier comme numériques, depuis leur création, leur nommage, en passant par la gestion des emprunts et des retours. Un tel suivi logiciel permet de déterminer, par exemple, qui est la dernière personne qui a recherché ce dossier que l'on ne retrouve plus, « *parce qu'il est très probable que ce soit chez cette personne que se trouve le dossier* ». Quel que soit le niveau d'ordre et de désordre d'où l'on parte, aucune situation n'est désespérée ! Un *process* de réorganisation bien rôdé peut rapidement venir à bout de tous les chaos, qu'ils soient physiques ou numériques.

Pour mettre en place un stockage papier, différentes options sont envisageables, qui ont toutes un coût. Stocker au sein de l'étude est onéreux quand le foncier est cher, faire stocker par un prestataire représente une dépense récurrente, mais stocker loin de l'étude où le foncier est plus accessible montre vite ses limites : « *nous avons travaillé,* indique Laurent Biet, directeur commercial du pôle Notaires chez *Xelians*, *avec des notaires dont les archives étaient à quelques kilomètres de chez eux. Puisqu'il y a presque autant d'actes recherchés que d'actes créés, ils doivent y envoyer des collaborateurs ou faire ce déplacement eux-mêmes, ce qui représente autant de temps perdu et donc un coût caché* ».

Le choix porte aussi sur la forme que prend la conservation. Elle peut se faire en conteneurs ou en linéaires, le premier étant moins cher à stocker mais plus coûteux pour chaque consultation, « *parce que,* explique Erwan Vilain, responsable commercial chez *Novarchive*, *il y a sept conteneurs les uns sur les autres avec chacun l'équivalent de 50 cm d'archives, donc l'archiviste, pour consulter un seul document, peut avoir à manutentionner un certain nombre de conteneurs avant de trouver ce qu'il cherche, ça n'est pas fait pour être consulté*

tous les jours ». Le linéaire est donc intéressant dès lors qu'il y a des insertions ou consultations récurrentes à faire dans un dossier.

Une autre option plutôt raffinée consiste à relier ses archives pour en faire des livres, avec évidemment un coût supérieur aux autres solutions, mais beaucoup d'avantages : « *d'une part,* précise Laurent Biet, *on n'a jamais mieux fait que des livres pour conserver du papier en bon état et de manière pérenne, d'autre part, il y a un souci d'élégance parce que les études choisissent la toile, la couleur et personnalisent ainsi des livres avec tous leurs actes originaux dedans, qu'ils n'auront d'ailleurs pas à utiliser, puisque, par ailleurs, tout est numérisé* ». Donc, pour les nombreux notaires qui n'aiment pas se dessaisir de leurs archives papier, il est possible d'aller gagner de la place dans l'étude tout en conservant ses minutes.

Gérer les archives numériques

La numérisation des pratiques du notariat est un acquis depuis de nombreuses années, mais l'archivage numérique reste un enjeu qui soulève de nombreuses questions. Si le choix est fait de numériser les archives papier, comment opérer ?

Préférez-vous qu'une équipe vienne numériser sur place, ou envoyer vos archives être numérisées chez le prestataire ?

Souhaitez-vous une numérisation dite « *fidèle* » conforme à la norme NF Z42-026 qui permettra de se débarrasser de l'original papier d'un grand nombre de documents justificatifs, notamment pour les dossiers d'annexes ?

Souhaitez-vous récupérer vos archives papier ou les laisser en dépôt ?

Souhaitez-vous une numérisation immédiate ou une option « *scan on demand* » ? « *Lorsque l'on est pas certain,* souligne Erwan Vilain, *que l'ensemble du fonds va être consulté dans les 10 ans ou 20 ans à venir, la solution scan on demand peut avoir beaucoup de sens* ». Dans ce cas, les documents sont stockés chez votre prestataire qui numérise les documents en fonction de vos besoins, et chaque demande de numérisation que réalise l'étude est ainsi l'occasion d'enrichir progressivement les archives numériques. C'est notamment utile lorsque les autres études font des demandes de documents, et la facturation de cette demande permet de couvrir les frais de numérisation sans faire l'avance des fonds. « *Les notaires reçoivent le document numérisé et n'ont alors plus qu'à transférer le mail à l'étude qui en a fait la demande* ».

La numérisation des archives papier est la première brique, car elle permet l'indexation de tous les documents par titulature mais aussi par contenu au moyen de processus OCR, quelle que soit la diversité des supports, puisque les classeurs d'actes papier des années 70 peuvent côtoyer le cartulaire des années 60 et les boîtes d'archives plus contemporaines réalisées dans les années récentes. Tout ceci est numérisé, indexé et intégré à la base documentaire de l'office. « *C'est le passé papier,* indique Laurent Biet, *puis viennent les actes électroniques réalisés par les notaires depuis la mise en place des logiciels métier. Ils vont être extraits, indexés et versés dans la base documentaire. Puis vient ce que j'appelle 'le fil de l'eau', à savoir les AAE produits au fur et à mesure par l'étude, et ceux-ci vont, soit être versés directement par l'étude dans la base documentaire, soit être gérés par un opérateur qui vient à l'étude de manière régulière pour les extraire et les indexer* ».

L'accès à cette base de données est bien sûr sécurisé et requiert identifiant et mot de passe, et la possibilité existe, surtout avec le développement du télétravail, de relever la sécurisation de l'accès en requérant un code unique envoyé par SMS. Le plan de classement mis en place lors de la numérisation est également très important puisqu'il va déterminer un accès sécurisé aux archives. En effet, la personne désignée comme administrateur du système d'archivage donne des droits d'accès afin que chacun n'ait accès qu'aux archives qui le concernent : quelqu'un qui gère, par exemple, la comptabilité fournisseur, n'aura pas accès aux minutes, et ne pourra ni verser un nouveau document ni détruire des archives.

Où se trouvent vos données une fois numérisées ? Dans une base de données installée à l'étude pour y accéder via votre interface. Et si vous souhaitez des archivages extérieurs ? Ils sont installés, avec une double écriture, et pas une simple réplication, sur des serveurs situés en France, et non sur un *cloud* à la localisation ambiguë. Quand un document de type Word, Excel, Jpeg est versé sur l'archivage électronique, si la durée utile de conservation est de moins de dix ans, l'image est transformée au moment du versement pour créer un PDF. Au-delà des dix ans, il est préconisé de créer ce qu'on appelle un PDF/A. Pour assurer une sécurité maximale, des tests de lecture récurrents sont effectués pour vérifier l'état des archives : « *nous contrôlons les archives électroniques chaque année,* souligne Erwan Vilain*, pour vérifier, au travers des scellés, que les documents n'ont pas été altérés, et pour vérifier l'intégrité de la lecture* ».

Jordan Belgrave

xelians NOTARIAT

Bénéficiez de solutions globales pour la gestion complète de vos fonds documentaires physiques et numériques.

Votre office souhaite améliorer l'expérience client et gagner du temps au quotidien dans son activité.

- → Numérisation probante des actes notariaux (NF Z42-026)
- → Indexation, gestion et stockage des AAE (minutier électronique)
- → Reliure des actes notariaux
- → Archivage physique et électronique (SIAF, NF Z42-013)
- → Gestion et dématérialisation des flux de courriers entrants
- → Solutions sur-mesure (portail, data room...)

xelians NOTARIAT

20 années d'expertise au service des Offices et de leur transition digitale

606 rue Fourny - 78536 Buc Cedex
01.30.97.03.30 / notariat@xelians.fr
www.xelians.fr

Les associations en armes de guerre contre la **cybercriminalité** *?*

Le cybercrime prospère dans la sphère virtuelle où des braqueurs en bandes organisées, avides de gains rapides et conséquents, rançonnent particuliers, entreprises et collectivités qui contre-attaquent en renforçant leur sécurité pour protéger leurs données. Engagées dans la lutte, les associations sont leurs solides et précieux alliés.

Une pandémie d'attaques informatiques de plus en plus sophistiquées se propage en douce dans l'ombre du coronavirus. Depuis un an, les alertes redoublent sur les assauts de *ransomwares* (rançongiciels) qui, introduits dans un système d'information, en prennent le contrôle à distance. Les données en otage ne seront libérées qu'en échange d'une rançon, le plus souvent en Bitcoins (BTC), une cryptomonnaie dont la valeur à l'unité atteint les 57 515 $ (47 440 €) le 22 février 2021.

Des numéros de cartes bancaires volées aux comptes piratés de médias sociaux, la moindre donnée sensible attise les convoitises. Sur le marché noir du darknet, les prix varient de 3 à plusieurs dizaines de milliers de dollars, selon l'étude Dark Web Price Index 2020 publiée en octobre sur le site PrivacyAffairs[1]. Une carte American Express clonée avec code PIN est ainsi bradée à 35 $ (29 €).

Parmi les protagonistes les plus recherchés des « *PME du crime* », se profilent Ryuk (1/3 des attaques ransomware, 180 M$ de bénéfices estimés), Egregor (ex-Maze, entre 200 et 250 attaques en 2020), REvil/ Sodinokibi (230), Netwalker (143) ou DoppelPaymer (125). Si certains « *montent en puissance* » (Conti, Pysa/ Mespinosa, Ragnar, SunCrypt, Thanos…), d'autres (Gothmog, Nemty, XINOF, Zeoticus...) font figure de groupes « *émergents* »[2].
« *Il y a une véritable explosion* », met en garde Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), dont la tâche est « *de faciliter une prise en compte coordonnée, ambitieuse et volontariste des questions de cybersécurité en France* ». Au service du Premier ministre et sous l'égide du Secrétaire général de la défense et de la sécurité nationale (SGDSN), l'autorité protège « *l'État, les administrations, 230 acteurs d'importance vitale, publics et privés* » et « *à terme, de l'ordre d'un millier d'entreprises considérées comme opérateurs de services essentiels* », conformément à une directive européenne datant du début d'année.

L'ANSSI (580 jeunes experts) veille, détecte, alerte sur les menaces informatiques (espionnage, grande criminalité, risques « *quasiment* » militaires...) et elle « *apporte des solutions à un problème en explosion totale.* » « *Dans les victimes qui font appel à nous (…), un chiffre à la louche : 50 opérations en 2019, 200 en 2020 ; donc c'est fois quatre* », constate Guillaune Poupard, interrogé le 11 janvier dernier sur BFMTV[3]. L'ANSSI précise qu'elle a traité 104 attaques par rançongiciels entre janvier et août

1 - www.privacyaffairs.com/dark-web-price-index-2020/
2 - « Écosystème du cybercrime », Panorama de la cybercriminalité, 21e édition, CLUSIF, Gérôme Billois & Marine Martin, 26 janvier 2021.

2020, pointant la « *menace extrêmement forte* » et « *l'augmentation en fréquence* » d'une cybercriminalité aux « *conséquences de plus en plus dévastatrices sur la continuité d'activité voire la survie de l'organisation victime* » (ssi.gouv.fr).

Crime organisé

Parmi les associations de référence, le Club de la sécurité de l'information français (CLUSIF, réunissant utilisateurs et offreurs des différents secteurs de l'économie) confirme l'augmentation croissante du nombre des victimes sur le fond d'une cybercriminalité en forte hausse, à coups de *ransomwares* qui sont la principale menace.

C'est d'ailleurs ce que révèle fin janvier dernier la rétrospective Panocrim[4], où la cartographie des victimes que dresse Pierre-Antoine Bonifacio signale un pic d'attaques particulièrement élevé entre septembre et novembre 2020. De leur côté, Gérôme Billois et Marine Martin observent que les assaillants opèrent désormais en groupes « *de mieux en mieux structurés et organisés* », citant REvil qui revendique « *une équipe d'une dizaine de développeurs* ».

Panocrim fait encore état des situations critiques des 30 % de collectivités locales et territoriales ciblées en 2020[5] et d'autant plus touchées qu'elles sont alors, à l'inverse des grandes entreprises, souvent démunies des moyens nécessaires pour s'abriter de cyberagressions en plein essor.

Les opérations d'enquêtes et d'infiltrations des autorités françaises et étrangères aboutissent cependant l'an passé aux démantèlements de réseaux mondiaux, dont Encrochat (communications cryptées, utilisé par 90 % des groupes criminels), Trickbot (diffusé par *spams* et *phishing*) ou Safe-Inet, un important opérateur de VPN (*virtual private network*, réseau virtuel privé, ndlr) prisé des cybercriminels. Fin janvier 2021, Europol et le FBI éliminent aussi le *botnet* Emotet, « *le malware le plus dangereux au monde* » (liens et fichiers piégés par e-mails), d'après un communiqué d'Europol[6].

En France, l'action judiciaire débouche sur la condamnation du Russe Alexander Vinnik à 5 ans de prison et 100 000 € d'amende pour blanchiment d'argent. Il « *était soupçonné d'être le cerveau de BTC-e, la plateforme mondiale d'échange de bitcoins, et d'avoir blanchi plus de 4 Md$ ces dernières années* », précise le Clusif, indiquant qu'il était aussi « *soupçonné d'être à l'origine du ransomware Locky* » (135 M€ de préjudice aux entreprises françaises entre 2016 et 2018, près de 200 victimes).

Proies faciles

Sournoise et galopante, la cybercriminalité n'épargne plus personne. Si on note une recrudescence d'attaques visant les collectivités publiques, les entreprises, voire les secteurs de la santé, les menaces (atteinte à l'image, usurpation d'identité, espionnage, hameçonnage, sabotage…) pèsent autant sur les particuliers, laissant entrevoir de graves impacts.
« *Depuis le début de l'année 2020, plus de 1 100 victimes, dont 26 % de particuliers, ont demandé de l'assistance sur notre plateforme pour faire face à une attaque par rançongiciel* », témoigne Jérôme Notin, directeur général de cybermalveillance.gouv.fr (assistance et prévention en sécurité numérique, ANSSI – ministère de l'Intérieur), un dispositif qui dispense conseils et bonnes pratiques pour protéger des risques.

Parmi les facteurs favorables au cybercrime, la travail à domicile imposé par la crise sanitaire et le confinement qui, d'après les spécialistes, ont amplement ouvert la voie aux attaques. « *Le télétravail a multiplié les liaisons entre les agents à distance et leur réseau interne. C'est autant de vecteurs possibles d'attaques* », démontre Rémy Février, maître de conférences au Conservatoire national des arts et métiers (CNAM) et expert en Sécurité des systèmes d'information. « *Pour un pirate, c'est royal !* », affirme l'ancien officier de Gendarmerie (20minutes.fr, 22 janvier 2021).

Un agent au travail chez lui « *utilise soit un équipement personnel qui n'est pas forcément sécurisé, soit son ordinateur qui sort du réseau sécurisé* », observe Emmanuel Vivé, directeur général de l'association Adico (développement et innovation numérique des collectivités, Oise). « *En ouvrant toutes ces petites fenêtres, il y a forcément beaucoup plus d'entrées dans la bâtisse* », précise-t-il le 18 janvier sur France 3 Hauts-de-France.

La récente divulgation sur le *dark web* de plus de trois milliards d'identifiants de connexion à des messageries Hotmail et Gmail et des comptes LinkedIn ou Netflix illustre de façon effrayante l'ampleur prise par les violations de données. Baptisée « *Comb* » (Compilation of many breaches), l'hémorragie a été révélée le 12 février 2021 par cybernews.com[7], un nouveau média web, radio et TV entièrement dédié à la cybersécurité, qui a aussitôt créé un moteur de recherches ouvert aux internautes susceptibles d'en être les victimes.

3 - « Guillaume Poupard : Le nombre de cyberattaques explose en 2020», BFM Business, Le Grand Journal de l'Éco, Hedwige Chevrillon, 11 janvier 2021.
4 - « Rançongiciels, tendance 2020 », Panorama de la cybercriminalité, 21e édition, CLUSIF, Sylvain Correia-Prazeres & Xavier Aghina, 26 janvier 2021.
5 - Selon l'étude « Menaces informatiques et pratiques de sécurité en France », CLUSIF, 2020.
6 - « World's most dangerous maleware Emotet disrupted through global action », Europol (europol.europa.eu/newsroom/news), 27 janvier 2021.
7 - « COMB: largest breach of all time leaked online with 3.2 billion records », cybernews.com, 12 février 2021, Bernard Meyer.

ASSOCIATIONS

Vade-mecum

Si l'explosion démesurée du *phishing* (hameçonnage) convainc aujourd'hui de l'importance à recourir aux connexions chiffrées et sécurisées en télétravail, l'efficacité technique ne doit pas exclure la vigilance individuelle. Pour endiguer les menaces accrues d'agressions, l'ANSSI relaie sur Tweeter un arsenal de précautions, simples et efficaces, à mettre en œuvre (#CyberVigilant). L'Agence diffuse encore sur son site une large gamme de plaquettes et de flyers qui dispensent de bonnes pratiques tout en vulgarisant une approche pédagogique des risques pour mieux s'en prémunir.

Afin de renforcer la sécurisation des systèmes d'information et des équipements personnels (ordinateurs, tablettes, smartphones…), l'ANSSI propose de surcroît un catalogue de guides fortement recommandés. D'abord destinés aux professionnels de la sécurité informatique et maintenant tout public, le *Guide des bonnes pratiques de l'informatique* (douze règles essentielles pour la sécurité des systèmes d'information des PME) et le *Guide d'hygiène informatique* (42 mesures) « *constituent une base méthodologique riche* » et ils « *traitent d'une large diversité de sujets*[8] ».

En juin 2019, l'ANSSI et le CERT-EU[9] ont par ailleurs annoncé la création conjointe d'OpenCTI (Cyber threat intelligence), une puissante plateforme communautaire ouverte, destinée à « *structurer, stocker, organiser, visualiser et partager le renseignement sur les menaces à plusieurs niveaux* », selon l'ANSSI qui vise à en « *aider et faciliter l'échange (...) pour construire une vision collective et de plus en plus précise de ces menaces*[10]».

Depuis sa naissance en mars 2020, l'association Luatix (recherches et développement en cybersécurité et gestion de crise) administre et déploie OpenCTI qui, réactualisée à la mi-décembre dernier, totalise à ce jour plus de 300 000 téléchargements libres et gratuits[11].

Riposte associative

Très investies elles aussi, les associations jouent un rôle majeur dans la lutte contre la cybercriminalité et la plupart a inscrit l'échange d'informations, le partage d'expériences et la mutualisation des ressources et des compétences parmi ses objectifs. Crypt-On, née en 2016 (+ 50 % d'adhérents en 2019), entend garantir une sécurité informatique optimale auprès du plus grand nombre par « *l'organisation et l'animation d'ateliers, de conférences, de réunions, de rédactions et diffusion de publications à destination de tout public, basé sur l'entraide et sur le partage des connaissances tous niveaux* » (crypt-On.fr).

En mai 2017, l'université américaine Carnegie Mellon (Pittsburgh, Massachussets) a référencé le CERT-Crypt-On (CERT-CO) afin de partager en interne des informations sur les menaces, de maintenir une veille constante « *indispensable* » et, si besoin, d'accompagner les adhérents. Ces diverses missions incombent aux membres bénévoles, tous spécialisés en cybersécurité.
Depuis février 2006, l'Association internationale de lutte contre la cybercriminalité (AILCC, cybercrime-fr.org) intervient pour sa part dans les domaines du droit pénal de l'informatique et de la sécurisation des cyberespaces et des échanges électroniques. Attachée à l'information, la formation et la recherche interdisciplinaire, elle s'appuie sur la vigilance de spécialistes, de professionnels et de partenaires rompus aux usages abusifs des nouvelles technologies d'information et de communication (NTIC) .
À la mi-novembre 2020, le CIGREF, une association d'accompagnement des grandes entreprises et des administrations publiques dans la maîtrise du numérique, a de son côté alerté Matignon sur « *le risque économique lié à la cybercriminalité* », réclamant « *des mesures réelles* ». Aucun secteur autre que le numérique « *n'accepterait de se développer dans un tel contexte de faiblesse du droit applicable et de quasi impunité des criminels* », a fait valoir le CIGREF dans sa lettre ouverte au Premier ministre[12].

Agir davantage

« *N'importe qui peut acheter sur le darkweb un cryptovirus et une base de données d'e-mails pour quelques milliers d'euros* », avertit Vincent Trély[13], président et fondateur voilà 10 ans de l'Association pour la sécurité de systèmes d'information de santé (APSSIS, apssis.com). Face aux risques élevés d'assauts contre des laboratoires de recherche et des centres hospitaliers, l'APSSIS « *fédère et anime l'écosystème pluriprofessionnel de la SSI santé* », fondant ses actions sur l'éthique, la sécurité et la réglementation de la transformation numérique. Forte de 120 adhérents, l'association propose ses publications (+ de 300 à ce jour) et ses formations SSI (+ de 3 000 professionnels sensibilisés).

8 - ssi.gouv.fr/particulier/precautions-elementaires/
9 - Le CERT (Computer Emergency Response Team) a pour objectifs de centraliser les demandes d'assistance en cas d'attaques, traiter les alertes, établir une base de données des vulnérabilités, sensibiliser sur les précautions à prendre pour limiter les risques et les conséquences d'incidents et veiller à une coordination entre les centres de compétence réseaux, les fournisseurs d'accès à internet les CERT nationaux et internationaux.
10 - opencti.io/fr
11 - « OpenCTI – The open source solution for processing and sharing threat intelligence knowledge », ANSSI, 28 juin 2019 .
12 - cigref.fr/leconomie-au-risque-de-la-cybersecurite
13 - « N'importe qui peut acheter sur le darknet un cryptovirus », Lequotidiendumedecin.fr, 17 février 2021, Martin Dumas-Primbault.

Vous êtes à la recherche de réponses sur le management de votre étude

Abonnez-vous gratuitement au Journal du Village des Notaires

Journal dédié au Management d'une étude notariale

vous y trouverez des dossiers pratiques, l'actualité des partenaires, veille et actualités juridiques...

Étude : .....
Madame / Monsieur : .....
Prénom : .....
Nom : .....
Adresse : .....
Code Postal : .....
Ville : .....
Mail : .....
Téléphone : .....

Abonnement gratuit au Journal du Village des Notaires

« *Alors que pendant longtemps la cybercriminalité était réservée à une élite informatique, on arrive aujourd'hui à des outillages qui sont à la portée du premier délinquant pas trop idiot* », se préoccupe Vincent Trély, qui préconise de nouvelles pistes pour accroître la sécurité après les récentes frappes contre les hôpitaux de Dax (Landes) et Villefranche-sur-Saône (Rhône).

Une lutte efficace passe cependant en amont par l'intégration de notions de cybersécurité aux formations au numérique dispensées en France afin de favoriser une coopération avec les experts, d'accentuer la vigilance, d'anticiper d'éventuelles carences et de provoquer une réaction immédiate en cas d'incident. C'est notamment l'objectif de l'association CyberEdu (cyberedu.fr) qui, initiée en mai 2016 par l'ANSSI, a tout d'abord élaboré les outils pédagogiques nécessaires à ces formations avant d'en promouvoir une labellisation conforme aux requêtes du Livre blanc sur la défense et la sécurité nationale, daté d'avril 2013[14].

Les labels décernés, qui référencent et accréditent aujourd'hui la cybersécurité dans un parcours d'enseignement supérieur, attestent également que les diplômés ont toute compétence pour veiller - *a minima* – sur les infrastructures informatiques des entreprises. Selon CyberEdu, près de 80 formations étaient déjà homologuées à la mi-septembre 2019.

Renforts de l'État

Peu après les attaques des hôpitaux de Dax et de Villefranche-sur-Saône, Emmanuel Macron a, le 18 février dernier, présenté une stratégie nationale de lutte contre une cybercriminalité 2.0 dont les propensions à nuire redoublent actuellement dans un contexte sanitaire qui lui est favorable. Le Président de la République a notamment annoncé une enveloppe de 1 Md€ (dont 700 M€ de fonds publics) pour « *renforcer la filière* », en doubler à terme les effectifs à 40 000 et « *tripler son chiffre d'affaires à 25 Mds€ en 2025* », selon l'Élysée.

Le chef de l'État entend en outre instaurer un « *écosystème de la cybersécurité* » en resserrant les liens de coopération entre les chercheurs du public et du privé. Un « *Campus Cyber* », où seront regroupés une soixantaine de ces acteurs clé, va donc être aménagé dans un espace de 20 000 m² du quartier de la Défense à Paris. L'ANSSI verra également ses effectifs atteindre les 600 d'ici la fin de l'année, contre 400 en 2017.

Dans l'immédiat, les premiers principes de vigilance et de précaution face à l'actuelle épidémie de piratages reposent surtout sur une distanciation et des gestes-barrières appliqués aux e-mails suspects. Ce sont autant de mesures simples, fiables et efficaces pour se protéger d'un virus sans doute à l'affût, tapi quelque part dans un lien ou une pièce jointe.

Alain Baudin

Fondation des Monastères
14 rue Brunel
75017 Paris
Tél. : 01 45 31 02 02
Mail : fdm@fondationdesmonasteres.org
Site Web :
www.fondationdesmonasteres.org

Un conseil expert aux côtés des notaires et de leurs collaborateurs

Depuis plus de 50 ans, au sein d'une œuvre civile atypique, religieux et laïcs sont au service des communautés monastiques chrétiennes et de leur patrimoine religieux, culturel et artistique. La Fondation des Monastères leur apporte un **soutien financier** sous la forme de subventions pour la conservation du patrimoine, l'aménagement des hôtelleries et lieux d'accueil, les aides sociales, ou de prêts pour l'amélioration de leur outil économique, ainsi qu'un **conseil administratif, juridique et fiscal.** Reconnue d'utilité publique, elle recueille, dans ce but, tous dons, conformément à la législation fiscale sur les réductions d'impôts et les déductions de charges, ainsi que les donations, legs et assurances vie en franchise des droits de succession.
L'**Espace Notaires** de son site permet aux notaires et à leurs collaborateurs d'accéder à une documentation adaptée aux libéralités et donne de précieux conseils sur la rédaction des testaments en leur faveur : *Moines et moniales, testateurs et héritiers, Libéralités à la Fondation des Monastères et aux communautés religieuses…*
Au lendemain de son cinquantenaire, la Fondation des Monastères reste pleinement engagée avec ses partenaires pour soutenir les communautés religieuses chrétiennes et relever jour après jour ce défi plein d'avenir !

14 - *Livre blanc, Défense et sécurité nationale* (2013), issu des travaux de la commission désignée par François Hollande, Président de la République, et présidée par Jean-Marie Guéhenno, conseiller maître à la Cour des comptes.

Menace cyber *: assurez vos arrières !*

La cyberattaque, un mot qui fait frémir, et pourtant une réalité qui se fait de plus en plus menaçante à mesure que la connexion entre nos outils de travail se renforce. Un sinistre est malheureusement vite arrivé, d'autant plus si les systèmes informatiques ne sont pas suffisamment protégés. Pour couvrir les professionnels désireux de continuer à travailler après un incident cyber, les assureurs mettent de plus en plus en place des polices d'assurances en cyberprotection, certaines offres étant spécialement adaptées aux particularités du notariat. Avec cette configuration particulière, que proposent les assureurs ? Éléments de réponse.

Le Conseil Supérieur du Notariat avait récemment alerté sur la recrudescence des tentatives de fraudes et d'usurpation d'identité et de sites internet des notaires[1]. Plus largement, les actes cybermalveillants font peser un risque sur toutes les données personnelles et professionnelles détenues ou créées par les offices notariaux. Les atteintes notamment à la confidentialité des données sont autant de causes potentielles d'engagement de la responsabilité civile professionnelle des notaires.

L'originalité de la responsabilité civile professionnelle des notaires.

Pour le notaire, officier ministériel investi d'une mission d'autorité publique, les conséquences d'un cyber incident viennent en conflit direct avec ses obligations à l'égard de ses clients, notamment celle, générale et absolue, du secret professionnel. Or cette règle de déontologie, si elle est rompue, peut emporter non seulement une fragilisation de lien de confiance, mais aussi une responsabilité importante.

Rappelons que le notariat bénéficie de deux mécanismes assurantiels. Le premier, individuel, décrit à l'article 13 du décret du 20 mai 1955, prévoit que tous les notaires sont tenus d'assurer leur responsabilité civile professionnelle. Le second, collectif, permet au notariat français (la profession dans son ensemble), de couvrir les conséquences pécuniaires des fautes et négligences intentionnelles ne pouvant pas être prises en charge par les techniques classiques d'assurance[2]. Il s'agit là d'une « *garantie unique en son genre* » dans le monde des professions du droit. Le Conseil Supérieur du Notariat garde ainsi la main sur l'assurance des notaires via notamment une société de courtage, détenue en partie par l'institution notariale[3].

Une tendance semble se dessiner depuis quelques années allant vers un alourdissement de la responsabilité des professionnels du droit. Les notaires n'en sont pas dispensés. Et, dans ce cadre, les potentielles défaillances techniques et humaines en cybersécurité, mêmes involontaires, sont autant de risques supplémentaires pour l'activité et le praticien. Le mécanisme de l'assurance s'avère alors « *indispensable non seulement dans l'intérêt de*

1 - « Cyberattaques contre les sites des notaires : appel à la vigilance », *Village des Notaires*, févr. 2021.
2 - « Responsabilité et obligations du notaire », *Conseil Supérieur du Notariat*, nov. 2017.
3 - « Notaires, une responsabilité civile très réglementée et originale », Argus de l'assurance, mai 2019.

la sécurité des victimes mais également pour protéger le patrimoine du professionnel et assurer la pérennité des activités[4] ».

L'assurance cyber, un outil de gestion des risques indispensable.

Il est certain que l'obligation de confidentialité qui pèse sur les professionnels du droit peut être mise à mal par un piratage informatique. Or, avec l'entrée en vigueur du RGPD, et l'obligation pour chaque organisation de mettre en œuvre des mesures de sécurité afin de protéger les données personnelles de ses clients contre les risques de perte, de vol, de divulgation ou contre toute autre compromission, de nouveaux besoins en assurance sont apparus pour apporter des réponses aux risques cyber.

La notion de risque est une notion clé en matière d'assurance. La couverture de ces événements aléatoires redoutés est essentielle, particulièrement pour ceux qui émanent du cyber espace. Dans un contexte aussi difficile économiquement qu'est celui d'un confinement, toutes les organisations font face à une menace de plus en plus imposante[5] : les cyberattaques et, particulièrement les *ransomwares*[6]. Selon les derniers chiffres de l'ANSSI par exemple, il peut être constaté, en 2020, une augmentation de 255 % des signalements d'attaque par rançongiciel entrant dans son périmètre par rapport à 2019[7].

Les assureurs développent ainsi de plus en plus des produits assurantiels permettant de couvrir ces risques informatiques. Ce marché, du fait de la crise sanitaire et économique, et des besoins accrus en télétravail, devrait d'ailleurs bondir à partir de 2021[8]. Le chantier de la couverture des risques cyber est vaste pour les professionnels du secteur car il existe une multitude de cyber risques et parfois même des « *cyber risques cachés* » qui demeurent non détectés pendant longtemps[9].

L'objectif de telles polices d'assurance est d'accompagner les organisations pour qu'elles puissent surmonter l'incident cyber. Divers frais liés aux cyber-risques peuvent ainsi être pris en charge par l'assureur : dépenses liées aux investigations numériques, frais de reconstitution des données détruites, frais de contentieux, etc. Certaines compagnies d'assurance mettent en place une plateforme collaborative numérique pour assurer un suivi en temps réel du traitement du sinistre[10]. Elles font également appel à une *task force* d'expertises avec des partenaires de crise (juridique, communication et investigation numérique) pour, *in fine*, évaluer le préjudice, chiffrer les dommages et les frais et pertes d'exploitation. Les offres sur le marché sont assez variables ; auditez vos contrats actuels et, le cas échéant, complétez votre couverture. Un investissement qui s'avèrera probablement très utile !

Simon Brenot

4 - ARHAB-GIRARDIN Farida, « L'assurance et la responsabilité civile des professions du droit, questions choisies », *Revue Lamy Droit Civil*, mars 2018.
5 - Voir notamment « Pourquoi les cyberattaques se multiplient avec le télétravail ? », *Argus de l'assurance*, avril 2020.
6 - Ou « rançongiciel ». Il s'agit d'un logiciel malveillant prenant « en otage » les données présentes sur votre ordinateur en les chiffrant. Une fois les données rendues inaccessibles pour l'utilisateur, le pirate exige le paiement d'une rançon en contrepartie de la livraison de la clé de déchiffrement.
7 - ANSSI, 1er févr. 2021, État de la menace rançongiciel à l'encontre des entreprises et institutions, CERTFR-2021-CTI-001, 4.1, www.cert.ssi.gouv.fr.
8 - « Le marché de la cyberassurance promis à une croissance rapide. », *Les Echos*, octobre 2018.
9 - « Ces nouveaux risques qui inquiètent les assureurs. », *Les Echos*, mai 2018.
10 - *Diot Neotech* par exemple met en place ce genre de services pour le notariat.

Village des Notaires

Le site 100% notaires

- Actualité juridique et immobilière
- Management et logistique de l'étude
- Quartier des associations
- Annonces immobilières
- Emploi
- Quartier des partenaires

www.village-notaires.com

legi team Editions

LEGI TEAM

Téléphone : 01 70 71 53 80
Mail : smorvand@village-notaires.pro
www.legiteam.fr

La cybersécurité, un enjeu de réputation et de gouvernance pour le notariat

Les impacts des incidents de cybersécurité sont multiples, que l'événement soit ou non rendu public. Par exemple, « *en étant visible publiquement, [une attaque telle que] la défiguration démontre que l'attaquant a pu prendre le contrôle du serveur, et donc, accéder potentiellement à des données sensibles (personnelles, bancaires, commerciales…) : ce qui porte directement atteinte à l'image et à la crédibilité du propriétaire du site auprès de ses utilisateurs, clients, usagers, partenaires, actionnaires…*[11] ».

Faire l'expérience d'un tel incident est une épreuve pour tout professionnel. Même si l'assurance joue son rôle de couverture et d'accompagnement de la victime dans le sinistre, il n'en demeure pas moins que les conséquences d'un tel incident sont préjudiciables pour l'activité et pour la gouvernance de la structure, selon des degrés variables selon la gravité de l'événement.

En tant que conseiller juridique de premier ordre, devant faire preuve d'un sens humain affirmé particulièrement lors de certaines périodes de la vie et de la construction d'opérations juridiques très importantes pour ses clients, le notaire a une place particulière dans le cœur des gens. Que dire de cette relation de confiance si une cyberattaque, venait à permettre à un assaillant d'usurper l'identité d'un notaire, de faire irruption dans le système pour prendre connaissance de données sensibles et de les divulguer sans autorisation ? Cela pourrait évidemment s'avérer très problématique pour l'image et l'activité non seulement du praticien concerné, mais aussi de la profession elle-même, à plus long terme. Une brèche dans l'édifice, même mineure, pourrait bien en effet, petit à petit, conduire certains à interroger la solidité des fondations. Le notariat, en raison de sa mission et de sa crédibilité à l'échelle de la société, est donc particulièrement exposé.

Conscientes de ces enjeux, les institutions notariales veillent. La profession a démontré ces dernières années sa volonté, parfois avant-gardiste dans le paysage des professionnels du droit, d'assurer sa transition numérique. Sans pour autant faire abstraction de la sécurité des données hébergées dans les offices, qui est une préoccupation essentielle des praticiens et de leurs institutions représentatives. C'est d'ailleurs la raison pour laquelle les opérateurs et fournisseurs de solutions souhaitant offrir leurs services sont tenus de se soumettre à une procédure d'agrément de la part du CSN. Un véritable gage de la sécurité *by design* des outils utilisés au quotidien par les notaires.

Pendant le premier confinement lié à la crise sanitaire de la Covid-19, cette même institution avait su faire preuve de solidité, garantissant à ses membres la continuité de leurs activités. Et la sécurité informatique avait notamment pu être assurée grâce au partage confraternel des outils de visio-conférence agréés. Nul doute que cette solidarité et cette prise en main des progrès technologiques sont acquises ; elles lui seront utiles pour continuer à avancer vers un avenir, toujours au service du citoyen.

11 - « Cyberattaques contre les sites des notaires : appel à la vigilance. », *Village des Notaires*, février 2021.

Village des Notaires

Immobilier : une année 2021 source de bouleversements dans les comportements des Français ?

Les chiffres de l'immobilier en fin d'année 2020 témoignent d'après le Conseil Supérieur du Notariat de sa forte résilience. Néanmoins, les interrogations demeurent et sont majeures pour 2021 alors qu'une crise économique se profile. La Rédaction du Village des Notaires s'est penchée sur la dernière note de conjoncture et vous en livre les principaux enseignements.

L'analyse de volumes faite par le Conseil Supérieur du Notariat prévoit une année 2020 proche du million de transactions, du fait notamment d'un volume à 1 020 000 transactions à fin novembre 2020. Cette performance s'explique par plusieurs facteurs d'après les Notaires de France.

Les banques continuent à jouer leur rôle « solvabilisateur » sur un marché porté notamment par un taux de crédits à l'habitat de +5,5 % en octobre 2020 et par l'action de la Banque centrale européenne (BCE) qui permet aux taux d'atteindre progressivement leur plancher historique. Sans oublier les recommandations désormais encourageantes du Haut Conseil de stabilité financière (HCSF) qui favorisent les primo-accédants.

Un mouvement de fond synonyme de déplacement de marché semble se dessiner et conduire à des nouveaux projets d'investisseurs ou d'utilisateurs en province ou en Grande couronne plutôt qu'à Paris. Cela s'illustre par une importante différenciation des volumes entre l'Ile-de-France et « *la province* », la première étant victime d'une chute de plus de 15 % ce qui occasionne une décélération de la hausse des prix (+0,5 % entre le 2e et le 3e trimestre 2020, après +1,8 % et +2 %).

La crise sanitaire puis économique et les confinements qui s'en sont suivi ont suscité une **prise de conscience collective en milieu urbain** qui a durablement marqué les stratégies de logements des franciliens et notamment des parisiens et des urbains plus globalement. Un exode a débuté vers des contrées plus vertes. La pratique du télétravail ayant fait son chemin, de manière brutale certes, dans l'esprit de l'employeur et du salarié, celui-ci peut s'organiser différemment, et privilégie donc un confort de vie familiale « au vert » avec deux lieux de vie (l'un proche de son lieu de travail en présentiel et l'autre pour son cadre familial). Ceci s'illustre dans les chiffres par une baisse du volume des transactions moindre au plan national que sur le marché parisien (- 4% et - 18%)

L'expérimentation d'encadrement des loyers qui s'étend : aujourd'hui Paris et Lille et demain, peut-être, huit intercommunalités et métropoles souhaitent rejoindre le mouvement. Cela pourrait impacter les projets d'investissements auparavant orientés vers la pierre et les rediriger vers des villes plus moyennes qui connaissent un regain de vitalité. Cette tendance serait renforcée par l'opposition de certaines grandes villes à la bétonisation, soucieuses d'attirer les investisseurs qui cherchent à se loger dans un cadre plus « vert ».

L'avenir reste pourtant trouble pour le marché immobilier, ce d'autant plus que la part des investisseurs étrangers non-résidents frôle son plus bas depuis 10 ans (1,5 % en 2019). Leur logique, à l'instar des Français, est de déplacer leur choix des pôles urbains vers les zones rurales.

Les projections des avants-contrats, selon les notaires, témoignent d'une **poursuite de la tendance générale actuelle de hausse des prix jusqu'en février 2021**, à un rythme similaire sur le marché des appartements à +0,6 % (contre +0,7 % au 3e trimestre 2020) mais à un rythme plus soutenu sur celui des maisons à +1,6 % (contre +0,3 % au 3e trimestre 2020). Cette tendance serait plus marquée en province notamment en décembre (+3 % en maisons, +2 % en appartements), et se replierait légèrement fin février 2021 (+1,5 % sur chacun des marchés). À Paris, le mois de novembre 2020 verrait un point culminant avec un prix autour de 10 900 € avant de se replier très légèrement sur trois mois consécutifs et s'établir à 10 700 €. À l'année, l'évolution serait à la hausse (+ 3,4%) compte tenu de la vigueur affichée pendant l'année 2020.

Simon Brenot

Smart cities : *un nouveau défi pour la protection des données*

La multiplication des projets de *smart city* et la hausse constante des cyberattaques posent la question de la sécurisation des données qui y transitent. Les opérations liées l'immobilier, piliers du développement de ces villes du futur, impliquent directement le notaire, qui doit ainsi redoubler d'attention pour garantir la sécurité juridique y compris dans ses aspects numériques et, dans le prolongement, rassurer ses clients. Une occasion pour le notariat de renforcer encore sa position de partenaire de confiance et élargir son champ d'expertise.

La ville intelligente est un nouveau concept de développement urbain, à l'aide de nouvelles technologies s'appuyant sur un écosystème d'objets et de services interconnectés. Il s'agit d'améliorer la qualité de vie des citadins, en rendant la ville plus adaptative et efficace. Loin d'être limité aux grandes métropoles, le sujet se diffuse au-delà, auprès des villes de taille intermédiaire et aux territoires de faible densité. On parle alors de « *territoires intelligents* », de « *smart territoires* » ou, pour les plus petites communes, de « *smart village* ». Indépendamment de l'ampleur des projets, les enjeux restent les mêmes.

La sécurité des données dans les *smart cities*

Si le tableau paraît idéal et que le discours est séduisant, il n'en reste pas moins que la performance d'une *smart city* repose sur l'interconnexion des fichiers et des objets connectés afin de construire un réseau fluide de données, bénéficiant à tous les habitants. Si la vulnérabilité des objets connectés contre les attaques informatiques est déjà connue, elle prend une nouvelle dimension à l'échelle d'une smart city. Qu'il s'agisse d'un bug informatique ou une cyber attaque, des pans des réseaux peuvent être endommagés ou paralysés, avec pour conséquence de nuire non seulement à l'infrastructure, mais aussi aux personnes physiques et morales, en cas de vol ou de perte de données personnelles ou, plus largement, d'informations confidentielles.

Pour éviter une cybercatastrophe, la *smart city* doit donc appliquer une cybersécurité *by design*, dès sa conception, en s'appuyant non seulement sur des moyens technologiques de sécurisation, mais aussi en s'apuyant sur l'humain, par la sensibilisation aux risques. Dans l'immense majorité des cyber-incidents, la cause de l'atteinte aux données est en effet liée à une imprudence humaine. Une stratégie d'accompagnement et de pédagogie qui, *in fine*, ne peut que produire des effets bénéfiques. La démarche n'est, pour une *smart city*, pas différente de celle à adopter dans les entreprises et les autres organisations.

Vers un nouveau champ de l'accompagnement notarial ?

Habitués aux nouvelles technologies, les notaires ont depuis longtemps investi le champ de la transformation numérique. Prenons quelques exemples. La chambre des notaires de Paris a créé en 2018 un fonds d'innovation pour développer de nouveaux outils numériques, dont la blockchain.

Celle-ci fait partie de ces nouvelles technologies testées et, peut-être bientôt généralisée, dans les *smart city* avec pour force ses caractéristiques : décentralisation, automatisation contractuelle, transparence, traçabilité et sécurité des échanges entre tous les protagonistes d'un projet immobilier grâce à un système inviolable. L'intelligence artificielle est également mise à profit pour « *[offrir] à terme des estimations instantanées et fiables pour toutes les typologies de logements anciens en Ile-de-France* ». Comme le disait Bertrand Savouré, ancien président de la chambre des notaires de Paris, « *ce projet ambitieux offre une opportunité pour le notariat de développer un nouvel outil d'estimation automatique performant au service des clients, ancré dans le XXIe siècle*[1] ».

En outre, parmi les clients du notariat figurent bien sûr les collectivités territoriales, gestionnaires des « *villes intelligentes* », pour lesquelles les notaires fournissent un conseil juridique en droit de l'urbanisme, en aménagement du territoire, en droit de l'environnement et en droit des collectivités territoriales. Le label « *Notaires, conseil des personnes publiques* », créé en 2019[2], est une certification qui permet d'ailleurs aux notaires intéressés par le développement d'une activité en droit public d'appréhender l'ensemble de ces thématiques. Plus spécifiquement, quel meilleur exemple que celui de l'implication des notaires dans l'élaboration de modèles de *smart cities* avec l'appel d'offre lancé par le gouvernement mauricien, et remporté par le Conseil Supérieur du Notariat et l'Ordre des géomètres-experts, en 2017 dans le cadre du lancement de son programme *Smart Cities*. Celui-ci vise à « *mieux appréhender les enjeux des villes de demain et répondre au défi de l'urbanisation croissante de l'Ile Maurice* [3]».

Cette capacité d'adaptation de l'expertise notariale et la propension de la profession à maîtriser les innovations technologiques pourraient-elles à l'avenir faire du notaire un acteur encore plus incontournable ? Le maniement par les professionnels du notariat des données personnelles et leur sécurisation au sein des offices leur donne déjà une pluralité de compétences susceptibles de rassurer ses potentiels futurs clients. Et si les *smart cities* contribuaient encore à en faire des référents incontournables des questions de protection des données personnelles ?

Le Congrès des Notaires édition 2018 mettait déjà à l'honneur la question de l'avenir de la ville, les notaires étant conscients des nouveaux enjeux d'un territoire en pleine mutation[4]. La 117e édition, qui se tiendra en 2021, aura pour thème « *le numérique, l'Homme et le droit. Accompagner et sécuriser la révolution digitale* ». Si, pour l'instant, le sujet des *smart cities* ne fait pas explicitement partie des thématiques abordées, espérons qu'il y soit intégré pour nous puissions, tous, profiter du regard expert de la profession sur ces enjeux !

Simon Brenot

1 - Communiqué de presse de la Chambre des notaires de Paris, 2 mars 2020, « Intelligence Artificielle : la Chambre des Notaires de Paris choisit PriceHubble pour développer un nouvel algorithme d'estimation immobilière », https://paris.notaires.fr.
2 - Banque des territoires, 22 juillet 2019, « Label «Notaires, conseil des personnes publiques»: une expertise reconnue en matière de droit public », www.banquedesterritoires.fr.
3 - Communiqué de presse du Conseil supérieur du Notariat, 24 sept. 2019, « Le Conseil supérieur du notariat et L'Ordre des géomètres-experts accompagnent l'Île Maurice dans la mise en oeuvre d'un régime juridique pour son programme Smart Cities », www.notaires.fr.
4 - 114e Congrès des notaires, « Réfléchir à la répartition et à l'équilibre du territoire », www.congresdesnotaires.fr.

Cyberattaque : faut-il dire ou ne pas dire *?*

En matière de cybersécurité, il y a la prévention des risques, mais aussi la réalité statistique. Et celle-ci dit qu'un piratage a de fortes chances de vous impacter quelles que soient les précautions que vous prenez. Pour le gérer au mieux, l'idéal est d'avoir préparé un plan d'action, la communication faisant partie intégrante de la gestion de crise. Quels sont les enjeux et les dynamiques d'une communication de crise cyber ? Pour y répondre, le *Journal du Village des Notaires* a interviewé Emmanuelle Hervé, experte de la gestion de crise et de la communication de crise.

Quelles sont les particularités de la communication de crise cyber ?

Il faut d'abord bien prendre conscience qu'on ne reprochera pas à une étude notariale de s'être fait hacker, quand cela arrive à trois mairies par jour et aux plus grandes entreprises, même à celles qui travaillent dans les nouvelles technologies ! Le cœur de la démarche est : « *nous sommes responsables, mais pas coupables* ». Les anglais disent *accountable* : cela veut dire assumer ce qui s'est produit parce que c'est notre structure, notre périmètre. Mais il n'y a pas d'idée de faute, ni de culpabilité. La culpabilité relève de la justice, et arrive dans un deuxième temps.

> ***« En communication de crise, le sujet essentiel, c'est la confiance. »***

La gestion de crise et la communication de crise ont cela de difficile qu'elles sont très contre-instinctives. Et donc, si l'on n'a jamais réfléchi en amont, si on ne s'est pas préparé, on va avoir les mauvais réflexes. Le sujet essentiel, c'est la confiance, et comment la préserver : la confiance des clients, des autorités, des partenaires. Par contre, si la réaction n'est pas rapide, factuelle, transparente, alors la confiance risque d'être complètement mise à mal. Et il est très grave de ne plus avoir confiance dans son notaire quand c'est lui qui a tous les secrets de famille.

Un autre point majeur est l'étroitesse de la fenêtre de tir pour réussir une bonne communication de crise. Suite à une attaque, pour garder sa crédibilité, il faut parler au bon moment et partir avec les bons éléments. Si vous perdez votre crédibilité, parce que vous avez commis une grossière erreur, vous n'êtes plus audible.

Que faut-il dire ? Qui doit parler ?

Dans un premier temps, comme toutes les entreprises avant vous et toutes les entreprises après, vous ne savez rien sur ce qui s'est passé : est-ce qu'il y a de la data dehors ? Si oui, combien ? Comment faire pour restaurer le système ? L'enquête est en cours et, pourtant, il faut communiquer. Il faut que ce soit un associé qui parle, quelqu'un qui ne manie pas la langue de bois. Il y a des gens très communicants mais qui, en temps de crise, ne sont pas rassurants. Or, pour rassurer, il faut « parler vrai », être capable de montrer de l'empathie, être proche des gens. C'est à cette personne que l'on va faire confiance. Si la posture est trop jargonneuse, trop arrogante, on ne va pas obtenir l'effet recherché, cet effet de compétences.

Ce qui importe, ce sont les faits, les actions, la compassion, l'engagement et la transparence. Dans le premier message à diffuser, c'est donc assez facile, il suffit de remplir ces cases-là.

Il ne faut surtout pas oublier l'empathie vis-à-vis des clients qui ont des informations privées à l'étude et qui commencent à stresser. Il va donc falloir être proactif et aller parler à chacun d'entre eux et trouver un *storytelling* « qui va bien ». Dans le premier temps, celui de la communication, il faut avoir cette attitude responsable qui prend en compte les événements. Si ça n'est pas fait, le public va se dire qu'il y a quelque chose de louche.

Dans un deuxième temps, il est également possible d'élaborer un peu sur toutes les mesures qui avaient été mises en place pour que ça n'arrive pas. Il peut aussi être intéressant de dire que vous allez tout faire pour comprendre ce qui a pu arriver et faire le maximum pour que cela ne se reproduise pas. Vous

augmentez ainsi votre capital confiance, et c'est positif pour l'avenir de votre activité.

Que ne faut-il surtout pas faire en communication de crise ?

Dans ma pratique, j'ai notamment identifié un certain nombre d'attitudes contre-indiquées.

La première, c'est le déni : quand on pense que ce n'est pas grave, que cela va s'arranger. Parce que si deux jours après, les mails ne marchent toujours pas par exemple, votre écosystème va vite s'apercevoir que votre fonctionnement n'est pas normal. Comment la confiance est-elle possible avec une étude notariale qui dissimule une cyberattaque ? Il faut au contraire raconter ce qui se passe et comment on s'y prend.

> ***Un certain nombre d'attitudes sont contre-indiquées.***

La deuxième est de tenter de dissimuler, voire de mentir : votre crédibilité sera durablement entachée quand, bien entendu, cela se saura. Et là, vos clients se mettent à vous contacter pour savoir si leurs données sont compromises. En plus, vous avez tout simplement la loi et l'obligation de déclarer à la CNIL dès qu'il y a un doute sur la compromission de données personnelles. C'est une situation très particulière, vous êtes à la fois victime – du pirate – et coupable – de ne pas avoir protégé les données qu'on vous confie.

Une autre stratégie perdante, c'est le bouc émissaire : se défausser sur le pirate ne sert à rien, on ne vous pardonnera pas pour autant. Il faut assumer et adopter un comportement responsable.

Une posture qui ne marche pas non plus est la globalisation : ce genre de choses arrive à tout le monde. Même si c'est vrai, cette attitude ne va pas protéger la confiance des autorités et de vos clients.

Confondre réponse juridique et communication est aussi un écueil fréquent. Il faut certes aller déposer plainte, prendre contact avec les autorités, etc. Mais ce n'est pas une stratégie de communication.

Un autre défaut récurrent est l'arrogance. Laisser entendre à ses clients ou aux médias qu'ils n'ont pas à se mêler de la situation, par exemple, alors qu'ils sont concernés au premier chef. Il est important de comprendre que les clients se posent en victimes de votre étude.
Il faut donc parler ! Mais une erreur qui peut être coûteuse serait de faire, par exemple, un communiqué de presse si cela n'est pas nécessaire. Tant que les journalistes ne posent pas de question, votre priorité reste les clients, les partenaires et les autorités, pas le grand public. En revanche, il serait contre-indiqué de ne pas donner suite si les médias viennent demander des détails. Ils ne font pas leurs publications sans essayer de contacter les intéressés, donc il faut répondre, à la fois vite, car ils publieront dans tous les cas. Pour avoir la bonne manière, il faut s'entraîner pour faire attention à la façon dont on dit les choses. Ici comme ailleurs, la meilleure des stratégies consiste à anticiper !

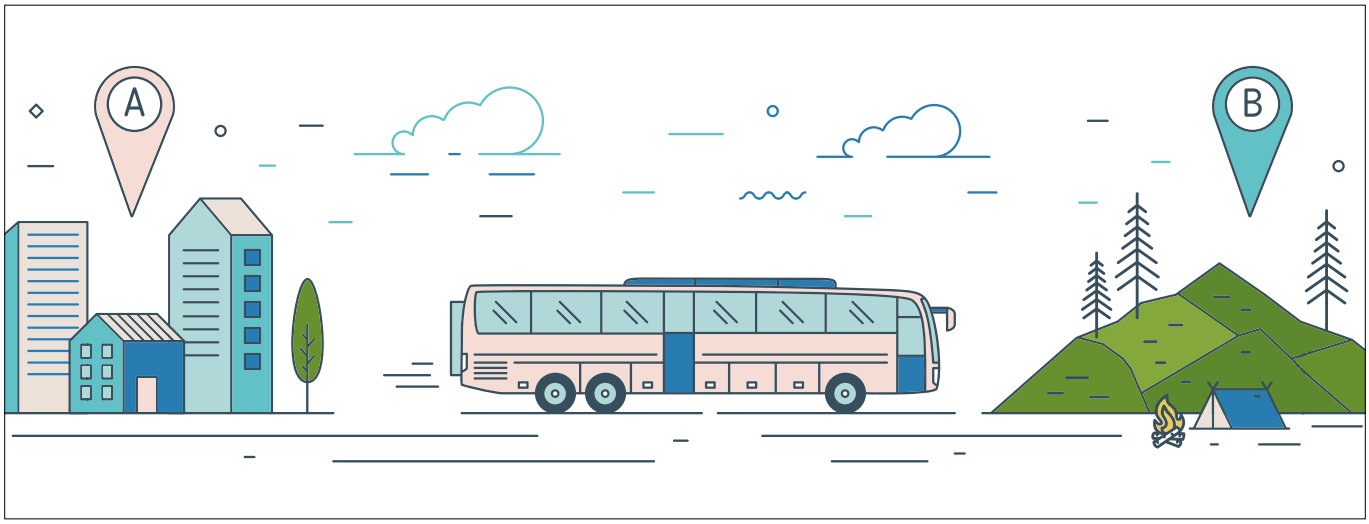
Propos recueillis par Jordan Belgrave

Communication et gestion de crise

La meilleure des stratégies consiste déjà à anticiper. Cela peut prendre la forme d'une cartographie des parties prenantes qui seraient concernées dans une telle situation. D'une part, les autorités : CNIL, ANSI, instances notariales... Mais aussi les clients, en fonction de l'importance des informations détenues – entreprises, clients importants. Surtout, ne pas oublier l'interne : associés, employés… Les impacts d'un piratage informatique ne se font pas seulement sentir sur les données professionnelles, mais sur toutes les données contenues dans les ordinateurs de l'office : photos perso, historique web… Il peut y avoir un impact intime non négligeable. L'idéal serait de faire préventivement une petite tournée d'information dans les bureaux pour expliquer que, en cas de cyberattaque, tout ce qui est dans les ordinateurs peut être volé et sera, dans le meilleur des cas, revendu sur le darknet et, au pire, exposé sur Google. Je pense qu'un tel message va avoir son effet pour convaincre qu'il est préférable de séparer les usages pro et perso.

Emmanuelle Hervé
EH&A Consulting

ZOOM SUR



Trouvez le **séjour insolite** *qui vous correspond*

Dans ce « Zoom sur », le *Village des Notaires* vous propose d'explorer des possibilités variés qui pour vivre une expérience belle, originale et dépaysante, sans avoir à traverser les frontières.

Être au plus près des animaux sauvages est une tentation pour beaucoup, mais elle requiert aussi des précautions particulières, les amateurs de safari le savent bien. Pour séjourner au plus près des loups, le parc animalier de Sainte-Croix en Moselle propose divers hébergements soit face à l'enclos des loups, soit avec vue sur la meute de cerfs ou sur les ours noirs du parc. Une des chambres propose même un jacuzzi avec des loups de l'autre côté de la cloison transparente. Le Zoo de la Flèche a également créé des lodges immersifs, qui permettent de séjourner au contact de l'enclos des tigres, des guépards, des loups blancs d'Arctique, des lémuriens, des ours polaires ou des grizzlys. Au Parrot World, des lodges s'ouvrent sur des paysages d'Amérique du Sud reconstitués pour admirer les perroquets, les ibis rouges, les jaguars, ou encore les loutres géantes dans leur rivière.

Comment partir loin sans traverser les frontières ? En choisissant des séjours conçus pour vous emmener dans des univers lointains. Comme de passer un week-end dans un tipi de luxe du Domaine Arvor à Lanvallay. Si vous préférez vous projeter en Afrique, Planète Sauvage en Loire-Atlantique vous propose de dormir au cœur d'un parc naturel peuplé de gazelles et d'antilopes, avec contes et chants africains pour rythmer les soirées.

Pour les imaginaires plus portés sur l'Asie, Hosomi Ryan vous accueille dans ses chambres traditionnelles à la manière japonaise, de type Jokari, à Combe fa dans le Tarn, accompagné d'une offre de massages japonais. Ou encore les lodges à la manière japonaise du très beau et très zen Le Bruit de l'eau, situé à Saint-Quentin-en-Tourmont près de la baie de Somme.

Devenez gardien de phare le temps d'un week-end en louant le Phare Berkeley, à Riante, aménagé en studio cosy et moderne. À 25 mètres de hauteur, vous aurez vue sur l'océan et sur l'île de Croix. Pour une ambiance plutôt Robinson Crusoé, réservez entièrement l'île de la Jument, dans le très beau golfe du Morbihan, ou bien l'île de Loubet, dans la baie de Morlaix.

Pour ceux qui aiment flotter, les cabanes et maisons flottantes sont de plus en plus belles. Parmi les offres les plus raffinées, on peut citer la Cabane en l'air, situé à Chassey-lès-Montbozon en Haute-Saône, dont la cabane accessible uniquement en barque comporte un bain nordique privé, afin de profiter pleinement du magnifique environnement ; ou encore le Nid sur l'eau, proposé par l'Échappée Belle à Sauvignon, dans l'Oise.

Pour ceux qui préfèrent les bateaux, la péniche l'Atlas mérite le détour, amarrée sur le canal latéral à l'Oise, au niveau de Roulotte ; ou la Toue Reine, construite sur le modèle des toues cabanées, bateaux traditionnels de la Loire, et aménagée en hébergement écot-responsable au port de Prémontré. Le château de Chambord a eu l'excellente idée

d'installer une autre toue cabanée sur son canal, afin de pouvoir passer la nuit avec vue sur ce bijou du patrimoine français.

Pour ceux qui aiment prendre de l'altitude, pourquoi ne pas séjourner dans le plus haut village d'Europe, à Saint-Véran, et profiter de la terrasse et de la piscine ouverte chauffée situées à 2 060 mètres d'altitude en plein cœur du Parc du Queyras. Ou passer une nuit au sein de l'observatoire astronomique du Pic du Midi, dans les Hautes-Pyrénées, pour profiter, après la vertigineuse ascension en téléphérique depuis La Mongie, des terrasses panoramiques, du « *Ponton dans le ciel* » et de son plancher transparent, de l'incroyable vue sur la chaîne des Pyrénées, et des télescopes pour l'observation des astres. Pour pousser la démarche, pourquoi ne pas dormir dans un igloo, sur un lit de glace. Comme ceux situés sur les stations de la Plagne et de Chamrousse. À La Plagne, les plus frileux pourront toujours opter pour un igloo chauffé. Aventure Nordique vous propose 3 types d'hébergement insolite au cœur des Pyrénées dans le village nordique de Gourette : selon vos envies, votre résistance au froid et votre budget, vous aurez le choix entre l'Igloo, le Snow Pod et le Wild Dôme. Avoriaz et Les Arcs ont créé de véritables hôtels de glaces dans lesquelles les chambres ont leur décoration directement sculptée dans la neige.

Si vous êtes plus à l'aise sous la montagne que dessus, les luxueuses chambres troglodytiques du Manoir des Roches à Montrichard Val de Cher sont pour vous.

Pour les amateurs d'histoire, séjourner dans un bâtiment historique est un moment privilégié. C'est encore plus vrai au château-fort médiéval de Tennessus dans les Deux-Sèvres où les hôtes vous proposent de vous vêtir à la manière de l'époque et de s'imprégner de la décoration d'époque. Une autre proposition historique, plus orientée bien-être, se trouve à l'Abbaye-École de Sorèze, située entre Toulouse et Albi, monument historique dont les cellules et dortoirs de religieux ont été réaménagées en chambres, et dont les anciennes écuries ont été transformées en spa. Enfin, une proposition particulièrement originale, à Blois, où la Tour Beauvoir, l'un des plus vieux donjons-prisons de France, est devenu une chambre d'hôtes avec une superbe vue sur la ville.

Pour vivre heureux, vivons perchés ! D'autant que les cabanes sont désormais très confortables et offrent des perspectives et des panoramas sans pareil. Loire Valley Lodges propose ainsi de luxueuses cabanes nichées en pleine forêt à quelques pas des châteaux d'Amboise ou de Chenonceau, chacune est unique et décorée par un artiste contemporain différent, avec, en plus, des offres massages réalisées sur votre terrasse privée entourée par les arbres.

À Labastide-de-Penne dans le Tarn et Garonne, Pella Roca a construit quatre sublimes cabanes perchées, avec un bain suédois et un sauna privatif dans chaque cabane. Une des cabanes est réalisée en bois brûlée à la manière traditionnelle japonaise (Shu Sugi Ban). Parmi les autres propositions intéressantes en matière de cabanes haut de gamme : les cabanes d'Entre Terre et Ciel, avec terrasse privée et vue sur le Mont-Blanc, à Saint Nicolas La Chapelle en Savoie ; les igloos en bois bâtis sur pilotis, à La Motte-d'Aveillans en Isère ; le château dans les arbres du Domaine de Puybéton en Dordogne. La Corse regorge de propositions alléchantes, comme les cabanes de Pignata, ou celles du Cocoon Village, cinq bulles et cocons suspendus à la roche avec vue sur le golfe de Porto Vecchio et la Sardaigne. Bénéficiant d'une grande proximité avec Paris, Lov'nid propose des cabanes douillettes à Rosoy-en-Multien dans l'Oise, avec un spa privatif et la vue sur les bois.

Les développements technologiques aidant, les habitats transparents se font mieux isolés et plus esthétiques.

À Maureillas-las-illas, dans les Pyrénées-Orientales, découvrez notamment la Pyramide Diamant constitué de miroirs sans teint qui vous donnent une visibilité sur la nature et le ciel tout en étant vous-même dissimulés. Par ailleurs des chambres-bulles se développent et peuvent être trouvées dans plusieurs cadres de qualité : le Perchoir des Pyrénées en propose une à Gerde dans les Hautes-Pyrénées ; pour un décor plus alpin, choisissez la chambre-bulle de Nuit Nature, située dans les alpages de Combloux avec vue sur Chamonix ; pour ceux qui aiment le terroir provençal, Attrap'rêve a installé des bulles à Allauch, au cœur d'une pinède près des calanques de Marseille.

Parmi les autres propositions particulièrement originales, nous avons particulièrement apprécié : un gîte dans des roulottes-tonneaux à Cornillé en Ille-et-Vilaine, des lodges semi-enterrés, dans l'esprit des hobbits de Tolkien, à La Poizelière en Vendée et à Melgven dans le Finistère, un bus anglais à deux étages reconverti en logement, et installé en face du massif des Maures, ou encore l'avion Grumman, en Loire-Atlantique, construit en 1962 et aménagé avec tout le confort moderne, tout en gardant sa décoration d'origine – sièges, panneaux de sortie et cockpit...

Jordan Belgrave

Partie 2 : les ACTES COURANTS *(Suite)*

Par un arrêt rendu le 23 janvier 2018, la cour d'appel de Pau rejette la demande du couple. En effet, les juges de la cour d'appel constatent que les statuts de l'ASL, adoptés à l'unanimité des colotis, prévoyaient que la décision portant sur une modification des pièces du lotissement devait être prise à la majorité qualifiée de **l'article L.315-3 du Code de l'urbanisme**, et que la résolution du 1er juin 2007 respectait cette majorité. De ce fait, les juges retiennent que la résolution litigieuse avait été valablement adoptée. Le couple, forme alors un pourvoi en cassation aux motifs que le cahier des charges constitue un document contractuel qui ne peut être modifié que par la seule décision de l'assemblée générale des colotis à l'unanimité et qu'une ASL ne constitue pas une autorité compétente susceptible de modifier unilatéralement le cahier des charges d'un lotissement.

C'est ainsi que le 27 juin 2019, les juges de la troisième chambre civile de la Cour de cassation, rendent un arrêt par lequel ils rejettent le pourvoi formé par le couple. En effet, les juges estiment que la modification du cahier des charges ne créait aucune disparité de traitement entre les colotis riverains de la voie et que cette modification n'était aucunement issue de procédés frauduleux tendant à utiliser la majorité dans un intérêt autre que collectif.

Deux problèmes se sont posés dans la situation d'espèce. Tout d'abord celui de savoir si la décision de l'assemblée générale de l'ASL ayant décidé à la majorité qualifiée de **l'article L.315-3 du Code de l'urbanisme** de modifier le cahier des charges est valable ?

Ainsi que celle de savoir si l'ASL a été régulièrement constituée, alors même que les statuts n'ont pas été publiés, dès lors que le consentement unanime des propriétaires intéressés a été constaté par écrit ?

Les juges de la troisième chambre civile de la Cour de cassation estiment que, la décision de l'assemblée générale de l'ASL ayant décidé, à la majorité qualifiée de **l'article L.315-3 du Code de l'urbanisme**, de modifier le cahier des charges est valable. De plus, la Cour de cassation considère que l'ASL a été régulièrement constituée dès lors que le consentement unanime des propriétaires intéressés a été constaté par écrit, peu importe l'absence de publication des statuts.

La Cour de cassation avait déjà eu à se prononcer sur la modification du cahier des charges dans un arrêt rendu le 12 juillet 2018 par la troisième chambre civile. Dans cet arrêt elle avait précisé que les clauses du cahier des charges d'un lotissement qui n'avaient pas un caractère règlementaire peuvent être modifiées à la majorité prévue par les statuts, sans que l'autorité compétente ait à approuver cette modification.

Le principal apport de cet arrêt résulte dans l'affirmation selon laquelle, l'assemblée générale d'une ASL peut valablement adopter une modification de son cahier des charges à la majorité renforcée prévue par ses statuts d'origine, adoptés à l'unanimité, en application du principe de liberté contractuelle, sans que l'unanimité ne puisse être exigée, et sans que soit nécessairement requise l'approbation par l'autorité administrative.

CONSEIL PRATIQUE

Face aux restrictions imposées par les voies règlementaires de modification, la voie conventionnelle demeure la plus à même de prévenir les risques de contestation. Il peut sembler intéressant de prévoir des règles de modifications du cahier des charges de manière conventionnelle.

2 - Possibilités nouvelle d'une application différée du statut de la copropriété pour les ventes de logement HLM à des personnes physiques

Ordonnance n°2019418 du 7 mai 2019 relative à la vente de logements appartenant à des organismes d'habitations à loyer modéré à des personnes physiques avec application différée du statut de la copropriété

Cette **ordonnance du 7 mai 2019** est composée de quatre articles. Elle a vocation à modifier les articles L.443-15-5-1 à L.443-15-5-8 ainsi que les articles L.443-15-2 à L.443-15-2-2 du Code de la construction et de l'habitation.

L'article 4 de l'ordonnance précise que les articles dans leur forme modifiée entreront en vigueur à partir du 1er janvier 2020.

Cette ordonnance a été prise sur le fondement de **la loi du 23 novembre 2018** portant évolution du logement, de l'aménagement et du numérique. Elle permet à l'occasion de la vente - par un organisme HLM à une personne physique - d'un logement, de différer le transfert de la propriété de la quote-part correspondante des parties communes, à l'issue d'une période qui ne peut excéder 10 ans à compter de la conclusion de la vente du premier lot de l'immeuble selon ce nouveau régime. **La loi du 10 juillet 1965** ne sera donc applicable qu'à partir de l'issue de ce délai. Il s'agit d'un outil facultatif. S'il est choisi, c'est l'organisme HLM qui prendra à sa charge la gestion des parties communes pendant toute la durée d'application du régime.

Ce texte définit en outre les obligations de l'organisme HLM, celle de l'acquéreur, ainsi que ses droits et les conditions de sa contribution aux charges de l'immeuble.

À NOTER

Ces obligations prévues par l'ordonnance seront transmises lors des ventes successives pendant toute la durée de l'application du régime.

3 - Conséquences néfastes d'une rédaction défectueuse d'une résolution et d'un avancement de fonds par le syndic

Cass. 3e civ., 4 juill. 2019, n° 17-27.743

La troisième chambre civile de la Cour de cassation dans un **arrêt rendu le 4 juillet 2019** s'est prononcée sur les conséquences d'une avance de fonds du syndic au syndicat des copropriétaires.

En l'espèce, certains désordres affectaient tant les parties communes que privatives d'une résidence et ainsi, le syndicat des copropriétaires a souhaité engager la responsabilité du constructeur et des intervenants et garants. Un jugement les a alors condamnés au paiement d'une certaine somme, mais a été infirmé par un arrêt déclarant partiellement irrecevable l'action du syndicat en raison de l'irrégularité du pouvoir donné à la société de gestion immobilière de Lorraine (Sogilor), son ancien syndic.

De ce fait, le syndicat des copropriétaires de la résidence a assigné en responsabilité la société Sogilor pour avoir dépassé le budget des travaux de reprise voté en assemblée générale et avoir rédigé de manière défectueuse la résolution l'autorisant à agir en justice. Une demande reconventionnelle est formée par la société Sogilor qui sollicite alors la condamnation du syndicat à lui rembourser une avance faite à son profit.

Le 12 septembre 2017, la cour d'appel de Nancy rend un arrêt par lequel elle rejette la demande de condamnation de Sogilor en considérant qu'il était toujours possible pour le nouveau syndic de prendre acte de l'irrégularité et de faire adopter une nouvelle décision afin de la régulariser.

D'autre part, l'arrêt rendu par les juges du fond, accueille la demande en remboursement des fonds avancés par Sogilor, en considérant qu'il n'est pas légalement interdit à un syndic d'avancer des fonds pour le compte de la copropriété et d'en demander ensuite le remboursement sur le fondement de l'article 1999 du Code civil, notamment en cas d'urgence sur le chantier.

C'est ainsi qu'un pourvoi est formé et que la troisième chambre civile de la Cour de cassation rend un arrêt le 4 juillet 2019, qui casse partiellement la décision de la cour d'appel de Nancy. En effet, les juges de la Haute Cour cassent l'arrêt de la cour d'appel en ce qu'il rejette la demande du syndicat des copropriétaires en condamnation de la Sogilor et condamne le syndicat des copropriétaires à rembourser la somme avancée par le syndic.

Effectivement, les juges de la Cour de cassation retiennent que le fait pour le syndic d'abonder sur ses deniers propres, le compte du syndicat des copropriétaires constitue une faute sanctionnée par la non-restitution de ce solde et ce, même en cas d'urgence pour éviter un retard de chantier.

D'autre part, le syndic de copropriété qui a rédigé de manière défectueuse le procès-verbal d'assemblée générale, a commis une faute engageant sa responsabilité en application de **l'article 1992 du Code civil**.

Il s'agit dans cette affaire, d'un rappel fait par la Cour de cassation des dispositions légales déjà applicables à ces situations.

Master II Droit Notarial UNIVERSITE MONTPELLIER I Promotion 2019-2020

Travaux réalisés par Leopoldo PANIZZA, Julia PUJOL, Lucie ROCHE, Louis-Romain ROUSTAN et Elisa VRIGNAUD.

NOS RECOMMANDATIONS

Annonces d'emploi

Village des Notaires
www.village-notaires.com

Scan me

RÉDACTEUR NOTARIAL (H/F) - SAINT-CHAMOND

Étude notariale à Saint-Chamond (42), à **40 minutes de Lyon**
Directement rattaché au notaire, vos missions sont les suivantes :
- Rédaction d'actes
- Formalités préalables
- Rendez-vous intermédiaires éventuels (selon affinités)

Vos missions peuvent **évoluer** en fonction de vos **souhaits et compétences**.
H/F avec **4 ans d'expérience minimum** en droit notarial (spécialisation en droit de la famille appréciée)
Vous êtes organisé, rigoureux et savez faire preuve de proactivité.
La connaissance de GenApi est un plus.
Télétravail possible (4 j/sem maximum)
Merci de candidater par email à ocamus@eada.net.

NOTAIRE ASSISTANT (H/F) – CDI LYON 3E

SBC Recrutement, spécialisé dans les métiers du Droit et de l'Expertise Comptable, recherche pour un de ses clients, étude de notaires situé dans le centre de Lyon (69), un Notaire Assistant H/F en CDI.
Au sein d'une étude de notaires à taille humaine, en collaboration directe avec un Notaire Associé, vos missions seront les suivantes :
- La gestion et le suivi des dossiers en droit immobilier (compromis, ventes immobilières, mise en revente...)
- La rédaction d'actes
- Contact permanent avec les tiers (impôts, banques, assurances, agences immobilières...)
Cette liste de tâches est non-exhaustive.

De formation Bac+5 dans le domaine, vous avez a minima une première année d'expérience sur un poste similaire.
Notaire Stagiaire accepté.

Vous disposez de solides connaissances en Droit Immobilier.
Vous êtes à l'aise avec l'informatique (Pack office, Internet...).
Vous disposez d'une bonne orthographe et vitesse de frappe.
La connaissance du logiciel GENAPI est appréciée.
Poste à pourvoir en CDI dès que possible.

Merci d'envoyer votre CV à l'adresse mail
sbc-lyon-bloch.46416952@applicount.com

FORMALISTE (H/F) – PARIS 1ER

Gitec recherche pour une étude parisienne Un/Une Formaliste H/F dans le cadre d'une mission en intérim de 1 mois, renouvelable. Le poste est situé à PARIS 01.

Vos missions seront les suivantes :
- Le contrôle des actes.
- La collecte des pièces.
- Les formalités d'enregistrement.
- La tenue du registre (répertoire officiel, refus, rejets, gestion des mains levées)
Vous avez au moins 2 ans d'expérience en tant que formaliste au sein d'une étude notariale.

Merci de candidater par email à
gitec.46037182@applicount.com

Agenda

Formations Juridiques .com

ANGLAIS JURIDIQUE, PARCOURS AFFAIRES INTERNATIONALES, DROIT SOCIAL, IP/IT, NOTARIAT

Du 15 février au 15 octobre 2021
À distance

Objectifs pédagogiques :
• Maîtriser les spécificités de l'anglais appliqué au domaine juridique, à sa profession ou à ses études.
• Maîtriser la grammaire et la conjugaison anglaise
• Être à l'aise à l'oral
• Développer ses connaissances en Common Law (parcours anglais)

Organisateur :
Languages for Lawyers
06 83 73 17 58
Mail : languagesforlawyers@gmail.com

117EME CONGRES DES NOTAIRES DE FRANCE

Septembre 2021
Nice

Thèmes : Le numérique, l'Homme et le droit
Accompagner et sécuriser la révolution digitale

Organisateur :
Association Congrès Notaires de France
www.congresdesnotaires.fr

LE VILLAGE DE LA LEGALTECH S'AGRANDIT ET DEVIENT LES RENDEZ-VOUS TRANSFORMATIONS DU DROIT

#TRANSFODROIT

Open Law* le droit ouvert et le *Village de la Justice* vous invitent les 18 et 19 novembre 2021 au Palais des Congrès à Paris pour les Rendez-vous Transformations du droit !
Juristes de près ou de loin, à vos agendas !

Organisateur :
Village de la Justice & Open Law* le droit ouvert,
https://transformations-droit.com

www.transformations-droit.com

#transfodroit

Le Village de la LegalTech se transforme et devient

les rendez-vous
TRANSFORMATIONS
du DROIT
18/19 nov 2021 | PARIS

Pour vous accompagner dans votre transformation, Open Law*, le droit ouvert et le *Village de la Justice* vous donnent rendez-vous sur les 5 Villages du Salon.

VILLAGE DE LA LEGALTECH
aux RDV « TRANSFORMATIONS DU DROIT »
18/19 nov 2021 | PARIS

VILLAGE DU LEGAL DESIGN
aux RDV « TRANSFORMATIONS DU DROIT »
18/19 nov 2021 | PARIS

VILLAGE DES TRAJECTOIRES PROFESSIONNELLES
aux RDV « TRANSFORMATIONS DU DROIT »
18/19 nov 2021 | PARIS

VILLAGE DES INNOVATEURS PUBLICS
aux RDV « TRANSFORMATIONS DU DROIT »
18/19 nov 2021 | PARIS

VILLAGE DE LA REGTECH
en 2020 avec Le Cercle Montesquieu
aux RDV « TRANSFORMATIONS DU DROIT »
18/19 nov 2021 | PARIS

Un événement organisé par

OPEN LAW*
*Le droit ouvert

VILLAGE DE LA JUSTICE
La communauté des métiers du droit
BY LEGI TEAM

Fondation des Monastères

Un défi plein d'avenir

L'engagement d'un

conseil expert

aux côtés des **notaires**

et de leurs collaborateurs

www.fondationdesmonasteres.org

Espace Notaires

Legs, donations, assurances-vie

à la Fondation des Monastères et en faveur des communautés religieuses chrétiennes et de leur patrimoine

01 45 31 02 02

legsetdonations@fondationdesmonasteres.org

14 rue Brunel - 75017 Paris

Reconnue d'utilité publique par décret du 21 août 1974. Fondation exclusivement financée par la générosité de donateurs privés ou d'entreprises. Ses comptes sont certifiés par le cabinet Mazars.