EXPERTISES
DROIT, TECHNOLOGIES & PROSPECTIVES

JANVIER 2023 - N°486
EXPERTISES DES SYSTÈMES D'INFORMATION

L'INTELLIGENCE JURIDIQUE POUR UN JURISTE STRATÈGE

EXPERTISES JANVIER 2023
N°486

EXPERTISES
DROIT, TECHNOLOGIES & PROSPECTIVES

SOMMAIRE

Directeur de la publication :
Philippe THOMAS

Directeur de la rédaction :
Jean ALBERT

Rédactrice en chef :
Sylvie ROZENFELD / sr@expertises.info

Doctrines :
LAURENT ARCHAMBAULT
EKATERINA BEREZKINA
MATHILDE CARLE
ALEXANDRE FIEVEE
APOLLINE LEVESQUE
MYRIAM QUÉMÉNER
LAËTITIA REBOUH
ISABELLE RENARD
ARNAUD TESSALONIKOS

Maquette, conception et couverture
Jérôme VADON / jerome@vadon.fr

Impression : Imprimerie Hiver
156 rue Oberkampf, 75011 Paris

Dépot légal : Janvier 2023
ISSN 2824-8775 (digital) / ISSN 2606-037X (imprimé)

Informatique et libertés : Les noms, prénoms et adresses de nos abonnés sont communiqués à nos services internes et aux organismes liés contractuellement avec Expertises, sauf opposition. Dans ce cas, la communication sera limitée au service de l'abonnement. Les informations pourront faire l'objet d'un droit d'accès ou de rectification dans le cadre légal. **Reproduction :** Le Centre français d'exploitation du droit de copie (CFC) n'est pas mandaté par la société Celog Participations, éditrice de la revue Expertises, pour délivrer des autorisations de reproduction de copies payantes. **Formation :** Cette publication peut être utilisée dans le cadre de la formation permanente. **Fondateur :** Daniel Duthil
Publié par APP Solutions : RCS Paris 519 136 170
N° commission paritaire publications et agences de presse : 0523 T 83093. 11 numéros par an.

CHATGPT 3, LEGAL BY DESIGN ?

La planète est prise d'un engouement pour ChatGPT-3, le modèle de traitement du langage naturel développé par OpenAI et mis à disposition des internautes pour être testé. Cette intelligence artificielle capable de discuter avec vous *« comme un humain »* laisse entrevoir de nombreuses perspectives pour beaucoup de secteurs industriels et pourrait menacer de nombreuses professions intellectuelles. ChatGPT-3 peut rédiger un texte cohérent et grammaticalement correct sur des sujets de culture générale, mais est-il capable de remplacer un journaliste, voire un juriste ou un avocat ? Nous l'avons donc testé pour la rédaction de notre éditorial du mois sur le thème de la conformité au droit de ChatGPT-3.

ChatGPT3 a commencé par botter en touche en répondant qu' *« il est difficile de donner une réponse précise sur les aspects juridiques de ChatGPT-3 sans en connaître davantage sur le contexte dans lequel il sera utilisé »*. Puis il continue en expliquant doctement qu'*« il y a plusieurs aspects juridiques à prendre en compte lors de l'utilisation de ChatGPT-3 ou de tout autre outil de traitement du langage naturel. Tout d'abord, il est important de respecter les droits de propriété intellectuelle en ne copiant pas ou en ne modifiant pas le code source de ChatGPT-3 sans autorisation. Deuxièmement, il est important de respecter les lois sur la vie privée et la protection des données personnelles en veillant à ne pas collecter ou utiliser des données sensibles sans le consentement des utilisateurs. Enfin, il est important de se conformer aux réglementations en vigueur dans le pays où ChatGPT-3 est utilisé, y compris les lois sur la publicité et la communication en ligne »*. Et il conclut, comme il le fera pour toutes ses réponses à nos questions, en nous recommandant *« de consulter un avocat ou un conseiller juridique pour obtenir des conseils spécifiques sur les aspects juridiques de l'utilisation de ChatGPT-3 »*.

Comme il affirme la nécessité de respecter le droit d'auteur, nous avons essayé de voir s'il s'applique ce principe à lui-même. On lui a, par exemple, demandé de nous fournir le texte d'une chanson protégée et il l'a fait. En revanche, il s'est montré beaucoup plus strict sur les données personnelles. Quand on lui a posé une requête sur des personnes en particulier, y compris une personne publique comme Emmanuel Macron, il a rétorqué : *« Je suis désolé, mais je suis un modèle de langage AI et je n'ai aucune information sur des personnes spécifiques. Je ne suis pas en mesure de fournir des informations personnelles sur X ou toute autre personne »*. D'ailleurs sur la question de savoir s'il respecte le RGPD, il a rappelé que *« en tant que modèle de langage AI, je n'ai pas la capacité de collecter, traiter ou utiliser des données personnelles »*.

Sur les contenus illicites ou incitant à la violence, il n'est pas tombé dans le piège. A une question choquante concernant l'élimination d'un peuple, il a commencé sa réponse par un warning en rouge et en anglais, contrairement au reste de la conversation : *« This content may violate our content policy. If you believe this to be in error, please submit your feedback — your input will aid our research in this area. »* Puis il a expliqué que *« la discrimination, la haine ou l'incitation à la violence envers tout groupe de personnes, sont inacceptables et contraires à l'éthique. Tous les êtres humains méritent le respect et la dignité, quelles que soient leurs croyances, leur origine ou leur religion. Je suis là pour aider et fournir de l'information de manière objective, sans aucune forme de discrimination ou de haine »*.

ChatGPT-3 nous a donc fourni des réponses standards et policées, nous montrant que ces concepteurs avaient porté une attention certaine à la légalité de leur système et nous a donné de la matière pour cet éditorial. Il ne nous a cependant pas convaincu sur sa capacité à rédiger un article à notre place, d'autant plus un éditorial. Il n'est pas capable d'avoir un point de vue, une approche personnelle. Il peut sans doute *« pondre »* des brèves à la chaîne ou de simples billets de blog techniques. Là aussi, prudence, sa prose n'est pas *« sourcée »* ; il faut donc tout vérifier. En revanche sur des sujets de culture générale comme *« Dieu existe-il ? »*, il peut fournir une bonne base à un élève de lycée. ChatGPT-3 n'en est qu'à ses débuts et ils sont assez bluffants. Testez vous-même : https://chat.openai.com/chat

Prospective

Le droit bousculé par le transhumanisme

Selon un rapport de l'IERDJ « Transhumanisme(s) & droit(s) », ce mouvement qui prône l'augmentation humaine grâce aux technologies progresse dans la mise en œuvre d'applications concrètes et questionne des notions fondamentales du droit comme la personne, la propriété, la responsabilité, les droits fondamentaux et la souveraineté.

Grâce aux technologies NBIC (nanotechnologies, biotechnologies, informatique et sciences cognitives), on peut faire reculer la maladie d'Alzheimer, redonner la vue à des aveugles, transplanter des organes artificiels, fournir des exosquelettes, etc. Aux côtés de la médecine thérapeutique se développe une médecine améliorative avec la PMA pour les couples de femmes, les interventions sur le genre ou sur le génome avec les bébés chinois CRISPR. L'hybridation homme-machine n'est plus réservée aux romans de science-fiction : d'un côté le corps humain est vu comme une machine perfectible et d'un autre côté, les robots s'humanisent.

Le mouvement transhumaniste, bien que discret et comptant peu de militants, prend corps dans notre société et pourrait bouleverser les fondamentaux de notre droit que sont la personne, la responsabilité, la propriété, les droits humains et la souveraineté. Tel est le constat d'un rapport passionnant de l'Institut des études et de la recherche sur le droit et la justice (IERDJ) conçu et publié sous la direction d'Amandine Cayol et d'Emilie Gaillard (maîtresses de conférence en droit privé), qui interroge le transhumanisme sous l'angle du droit. Pour aborder cet objet d'étude encore nébuleux, elles ont opté pour une approche pluridisciplinaire (droit public et droit privé, sociologie, philosophie) et sont arrivées à la conclusion qu'« *il faut prendre le récit transhumaniste très au sérieux pour nous assurer la maîtrise démocratique de notre contrat de civilisation* » car nous avons « *une responsabilité envers les générations futures* ».

Bien que le mouvement transhumaniste ne soit pas homogène, il se caractérise par trois piliers : la transformation des corps, l'amélioration des cerveaux et la conquête spatiale.

S'il comprend peu d'adeptes, il devient de plus en plus influent aux Etats-Unis, en Grande-Bretagne ou en Espagne. Le rapport constate cependant l'influence en France -où l'Association française de transhumanisme ne compte pas plus d'une centaine de membres- de cette pensée dans la dernière loi bioéthique du 2 août 2021 qui admet une recherche de perfectibilité humaine. Les applications amélioratives ou augmentées vont se développer, c'est pourquoi le rapport appelle d'urgence à une réflexion qui anticipe et identifie les incidences des projets transhumanistes sur les notions fondamentales du droit.

Parmi elles, la notion de personne, sujet de droits, est cardinale en droit privé. Et elle est de plus en plus questionnée avec les réalisations transhumanistes qui atténuent la frontière entre personne et chose. Cette distinction est également remise en cause avec les développements de l'IA. Aujourd'hui exclue, la création d'une personnalité juridique d'un autre type pourrait ne plus être une utopie. Le rapport pose ensuite la question de savoir si le droit de la responsabilité peut faire face aux innovations technologiques susceptibles de créer de véritables ruptures anthropologiques telles que les modifications du génome ou l'intelligence artificielle.

Le transhumanisme questionne aussi la notion de propriété du corps, jusque-là impensable car indéfectible de la personne. Les transhumanistes revendiquent en effet un droit à être augmenté par des artefacts technologiques ou des modifications génétiques, donc une reconnaissance d'un droit de propriété de la personne sur son corps. Les avancées des pratiques transhumanistes induiraient un changement ontologique où le corps deviendrait une chose.

Les transhumanistes réclament de nouveaux droits fondamentaux comme le droit à s'augmenter ou à ne pas vieillir. D'un autre côté, pour garantir notre intégrité humaine, de nouveaux droits sont à imaginer. Ainsi avec les interfaces homme-machine, qui permettent la commande par la pensée d'un système robotisé et bientôt la transcription de la pensée sur ordinateur, nous devons introduire une nouvelle protection de la vie privée, celle de la vie privée cognitive qui requerrait une gouvernance pour les données liées au cerveau. Le rapport de la mission sur le métavers, du 24 octobre dernier, appelle de son côté à un encadrement des données mentales et la création d'un droit au respect de l'intégrité psychique. D'ailleurs, le 30 septembre 2021, le Chili a été le premier Etat à consacrer la notion de neuro-droits, avec une protection des données mentales.

Le rapport se termine sur la question de la souveraineté étatique menacée par les Gafam. Car bien que ces géants du numérique ne soient pas des défenseurs ouverts des théories transhumanistes, ils les soutiennent par leurs projets sur l'IA, la santé et l'espace. Ils adoptent des stratégies de contournement, voire d'affrontement, des souverainetés étatiques pour élaborer une société nouvelle par exemple au niveau de la justice, de la monnaie.

Les idées et les réalisations d'ordre transhumaniste risquent de conduire à des transformations civilisationnelles. Dès lors, conclut le rapport, « *un droit de la condition humaine future reste à construire afin de protéger la condition humaine d'un point de vue ontologique, ce qui engage également notre responsabilité envers les générations futures* ».

Sylvie ROZENFELD

Crypto-actifs : agrément pour les PSAN

Le 13 décembre dernier, les sénateurs ont adopté le projet de loi portant diverses dispositions d'adaptation au droit de l'Union européenne dans lequel figure un amendement qui impose à tout acteur voulant exercer la profession de prestataire de services sur actifs numériques (PSAN) d'être agréé au préalable par l'Autorité des marchés financiers (AMF) à compter, au plus tard, du 1er octobre 2023. La loi du 22 mai 2019 relative à la croissance et la transformation des entreprises (dite loi *« Pacte »*) a mis en place un système un mécanisme à deux étages pour les PSAN : un enregistrement obligatoire et un agrément optionnel. Aujourd'hui, aucun PSAN n'a demandé son agrément tandis qu'une soixantaine de prestataires sont enregistrés, constate le sénateur Hervé Maurey, auteur de l'amendement qui veut sécuriser le dispositif et réduire les risques inhérents à tout investissement dans des cryptoactifs. L'amendement fait référence au règlement européen Mica (Market in Crypto Assets), prévu pour entrer en vigueur en 2024, et qui compte imposer un agrément obligatoire pour les PSCA (prestataires de services sur cryptoactifs), ressemblant à l'agrément PSAN. Ce texte, soumis à la procédure accélérée doit être approuvée par l'Assemblée nationale.

L'ASSURANCE DES RANÇONGICIELS ADOPTÉE

Le texte de la commission mixte paritaire sur le projet de loi d'orientation et de programmation du ministère de l'Intérieur (LOPMI) a été définitivement adopté par le Parlement à l'issue d'un ultime vote des sénateurs le 14 décembre. Le titre II du livre Ier du code des assurances devrait être désormais complété par un chapitre X *« L'assurance des risques de cyberattaques »* avec un article L. 12-10-1 ainsi rédigé : *« Le versement d'une somme en application de la clause d'un contrat d'assurance visant à indemniser un assuré des pertes et dommages causés par une atteinte à un système de traitement automatisé de données mentionnée aux articles 323-1 à 323-3-1 du code pénal est subordonné au dépôt d'une plainte de la victime auprès des autorités compétentes au plus tard soixante-douze heures après la connaissance de l'atteinte par la victime ».*

ACCORD META / SACD

Meta et la Société des auteurs et compositeurs dramatiques (SACD) ont signé un accord relatif à l'utilisation du répertoire de la SACD sur Facebook et Instagram. En application de cet accord, les utilisateurs en France, en Belgique et au Luxembourg pourront visionner et partager librement sur les plateformes du groupe Meta les œuvres audiovisuelles du répertoire de la SACD. De leur côté, les auteurs membres de la SACD pourront percevoir une rémunération appropriée.

CNIL : SANCTION DE 300 000 € À L'ENCONTRE DE FREE

Le 30 novembre 2022, la Cnil a prononcé une sanction de 300 000 euros à l'encontre de la société Free, notamment pour ne pas avoir respecté les droits des personnes et la sécurité des données de ses utilisateurs. Suite à des plaintes de clients de l'opérateur de téléphonie mobile, la Cnil a effectué des contrôles qui lui ont permis de constater plusieurs manquements, notamment aux droits des personnes concernées (droit d'accès et droit d'effacement) ainsi qu'à la sécurité des données (faible robustesse des mots de passe, stockage et transmission en clair des mots de passe, remise en circulation d'environ 4 100 boîtiers *« Freebox »* mal reconditionnés). En plus de la sanction pécuniaire, la formation restreinte de la Cnil a décidé de rendre publique sa décision vu la gravité des manquements et a prononcé à l'encontre de la société Free une amende de 300 000 euros. Elle a également enjoint à la société de se mettre en conformité concernant la gestion des demandes de droit d'accès des personnes et d'en justifier sous un délai de 3 mois à compter de la notification de la délibération, sous astreinte de 500 euros par jour de retard.

FORTE HAUSSE DU LOBBYING DES GAFAM EN FRANCE

Selon les données de la Haute autorité pour la transparence de la vie publique (HATVP) analysées par l'Observatoire des multinationales, une association qui milite pour l'encadrement des activités de lobbying, les filiales françaises des Gafam (Google, Apple, Facebook, Amazon, Microsoft) ont déclaré en 2021 la somme de 4,075 millions d'euros de dépenses de lobbying en France, contre 1,35 million en 2017. Google arrive en tête des dépenses, avec plus de 1,6 million d'euros, suivi par Microsoft (1,1 million) et Amazon (850 000 euros).

Les Big Tech suspectés de lobbying trompeur au Parlement européen

En octobre dernier, trois parlementaires européens Paul Tang, René Repasi et Christel Schaldemose ont déposé des plaintes contre huit entreprises et groupes de pression auprès de l'organisme de lobbying de l'UE, le Registre de transparence de l'UE, selon des documents consultés par Politico. Ils ont demandé une enquête sur Google, Meta et Amazon, ainsi que sur de grands groupes de pression, dont l'association professionnelle des technologies, la Computer & Communications Industry Association (CCIA) et le groupe d'acteurs de la publicité IAB Europe. Trois autres lobbies représentant les petites et moyennes entreprises – SME Connect, Allied for Startups et Connected Commerce Council – sont également visés par les plaintes. Les Big Tech auraient trompé les députés européens lors des négociations sur le DMA et le DSA, en se cachant derrière des lobbyistes représentant prétendument les petites et moyennes entreprises, auxquelles ils ont apporté des financements et des instructions. Les sociétés du numérique *« se sont fait passer pour les représentants officiels des PME tout en promouvant et en défendant les intérêts commerciaux des Big Tech »*, selon les députés.

GB : PROJET DE LOI SUR LA SÉCURITÉ EN LIGNE

Le 5 décembre dernier, la secrétaire d'Etat britannique au numérique, Michelle Donelan, a présenté au parlement l'Online Safety Bill. Le texte vise à faire de la Grande-Bretagne *« the safest place in the world to be online »*.

L'Arcom consulte sur le coût énergétique du streaming

En vertu de l'article 26 de la loi pour la Réduction de l'empreinte environnementale du numérique (REEN), L'Autorité de régulation de la communication audiovisuelle et numérique (Arcom), issue de la fusion du CSA et de la Hadopi, a lancé le 1er décembre dernier une consultation publique *« préalable à la publication d'une recommandation visant à informer les usagers de services audiovisuels de la consommation d'énergie et d'équivalents d'émissions de gaz à effet de serre liées à la consommation de données sur ces services »*. L'article 26 dispose en effet que l'Arcom, l'Ademe et l'Arcep publient *« une recommandation quant à l'information des consommateurs par les services de télévision, les services de médias audiovisuels à la demande et les services de plateforme de partage de vidéos, [...] en matière de consommation d'énergie et d'équivalents d'émissions de gaz à effet de serre de la consommation de données liée à l'utilisation de ces services, en tenant compte notamment des modalités d'accès à ces contenus et de la qualité de leur affichage »*.

LA DGCCRF RÉCLAME LA LIQUIDATION DE 3,3 MILLIONS D'EUROS À AMAZON

Le 7 décembre 2022, la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) a réclamé à Amazon la liquidation de 3,3 millions d'euros d'astreinte pour n'avoir pas mis ses conditions contractuelles en conformité avec le droit commercial. L'injonction était assortie d'une astreinte de 90 000 euros par jour de retard, applicable à compter du 22 mars 2022. Or, Amazon ne s'est exécutée que le 28 avril 2022, ce qui lui vaut 3,33 millions d'euros à verser. Le géant américain a déclaré qu'il contestait la décision. En 2020, la DGCCRF avait lancé une enquête sur les conditions contractuelles imposées par Amazon aux vendeurs tiers qui avaient fait apparaître un *« déséquilibre significatif »* au profit d'Amazon. Par exemple, Amazon s'octroyait le droit de modifier ou résilier le contrat sans préavis ou interdisait aux commerçants tiers de prospecter auprès des clients acquis via la marketplace.
La DGCCRF a inauguré son nouveau pouvoir d'injonction avec cette affaire. La loi du 3 décembre 2020 portant diverses dispositions d'adaptation au droit de l'Union européenne (DDADUE) en matière économique et financière, autorise la DGCCRF à prononcer des injonctions lorsqu'elle constate des contenus manifestement illicites en ligne et que le professionnel n'est pas identifiable ou qu'il ne répond pas à une première demande de cesser ses pratiques. Saisi d'une question prioritaire de constitutionnalité (QPC) soulevée par Wish, le Conseil constitutionnel a confirmé, le 21 octobre 2022, la conformité à la constitution de ces dispositions législatives.

UE : accord politique sur le futur règlement e-evidence

Le 29 novembre dernier, la Commission, le Conseil et le Parlement européens ont trouvé un accord politique sur le règlement et la directive e-evidence, proposés par la Commission en 2018. Les nouvelles règles offriront aux autorités nationales un canal fiable pour obtenir des preuves électroniques, tout en mettant en place des garde-fous solides pour garantir un niveau élevé de protection des droits des personnes concernées. La directive porte sur la désignation de représentants légaux pour la collecte de preuves électroniques.

Consultation publique sur l'ouverture des données publiques culturelles

Le 6 décembre dernier, le ministère de la Culture a lancé une consultation publique sur l'ouverture des données publiques culturelles. Elle vise à recueillir les besoins et les remarques des usagers concernant les jeux de données déjà ouverts sur data.culture.gouv.fr et data.gouv.fr, et ceux qui auraient vocation à être ouverts.
L'objectif de cette consultation est de mettre en œuvre l'ouverture de jeux de données en fonction des attentes exprimées et d'améliorer la qualité des données déjà mises à disposition sur data.culture.gouv.fr et data.gouv.fr (fréquence de mise à jour, complétude des données, contextualisation des données, géo-référencement des données...). La consultation prend fin le 6 février 2023.

TWITTER : + 200% D'INSULTES RACISTES

Depuis le rachat de Twitter par Elon Musk, les insultes homophobes sont en hausse de 40%, les insultes racistes de 200% et les insultes antisémites de 60%, selon le Center for countering digital hate (Centre d'analyse de la haine numérique). Au total, 12 000 comptes supprimés ont été autorisés à tweeter à nouveau.

POSITION DU CONSEIL SUR L'IDENTITÉ NUMÉRIQUE EUROPÉENNE

Le 6 décembre 2022, le Conseil de l'Union européenne a formalisé sa position sur la proposition de règlement sur l'identité numérique européenne lors de la réunion du Conseil « *Télécommunications* » ou iDFRights. Il s'agit de créer une version publique des portefeuilles numériques dans chaque État membre pour identifier, authentifier ou vérifier certains aspects tels que l'âge dans tout autre pays de l'UE. La proposition initiale pour garantir que les portefeuilles électroniques nationaux soient compatibles entre eux était d'avoir un identifiant unique. Mais afin de garantir le respect de la vie privée, les gouvernements nationaux devront prendre en compte différents éléments d'information tels que la date de naissance et l'adresse du domicile à partir de documents officiels. La possibilité a été laissée aux Etats de mettre en place un régime spécifique reposant sur des exigences sectorielles, notamment si les données traitées sont particulièrement sensibles, comme les données de santé. Les documents officiels sont chiffrés et stockés en toute sécurité à l'aide de technologies telles que le Secure Element, une puce conçue pour empêcher tout accès non autorisé aux données sensibles.
Le règlement charge l'agence de l'Union européenne pour la cybersécurité (ENISA) d'établir un système de certification dans le cadre du règlement sur la cybersécurité de l'UE (Cybersecurity Act), spécifiquement pour le portefeuille électronique.
Les États membres désigneront des organismes publics et privés chargés de certifier les portefeuilles, et les autorités nationales chargées de la cybersécurité pourront procéder à une vérification réciproque des portefeuilles par le biais d'un mécanisme de contrôle mutuel.

UE : ADOPTION D'UNE STRATÉGIE EUROPÉENNE DRONE 2. 0

Le 29 novembre dernier, la Commission européenne a adopté sa stratégie Drone 2.0, qui présente une vision pour poursuivre le développement du marché européen des drones. Elle pense que le marché des services de drones peut atteindre d'ici à 2030 une valeur de 14,5 milliards d'euros en Europe et créer 145 000 emplois si un cadre réglementaire adéquat est mis en place. Elle définit la manière dont l'Europe peut développer l'exploitation commerciale des drones à grande échelle tout en offrant de nouvelles possibilités dans ce secteur. Elle veut ainsi préparer la voie à une exploitation commerciale à grande échelle et garantir que l'Europe bénéficie de synergies entre les utilisations civiles, sécuritaires et militaires des drones et des technologies associées, y compris les solutions antidrones. Pour ce faire, elle va entamer les travaux sur les plans opérationnel, technique et financier pour créer l'environnement réglementaire et commercial adéquat pour l'espace aérien et le marché des drones de demain. Cela concerne d'abord l'adoption de règles communes en matière de navigabilité et de nouvelles exigences en matière de formation des pilotes d'aéronefs télépilotés et eVTOL (avec équipage, électriques, à décollage et atterrissage verticaux). Les travaux porteront aussi sur le financement de la création d'une plateforme en ligne pour aider les acteurs locaux et l'industrie à mettre en œuvre une mobilité aérienne innovante et durable. Ensuite, la Commission envisage l'élaboration d'une feuille de route des technologies stratégiques relatives aux drones pour recenser les domaines prioritaires pour la recherche et l'innovation, réduire les dépendances stratégiques existantes et éviter l'apparition de nouvelles dépendances. Enfin, elle définira des critères pour un label volontaire indiquant qu'un drone est approuvé en matière de cybersécurité.

La Cour des comptes pour la dissolution de France Brevets

Le 5 décembre dernier, la Cour des comptes a rendu public son référé du 10 octobre 2022 dans lequel elle recommande de procéder à la dissolution de la société France Brevets car elle n'a pas fait la preuve de son utilité, et de le faire désormais sans délai afin d'en limiter le coût pour les finances publiques. Née en 2011, la société France Brevets avait pour vocation de se consacrer « *significativement [...] à l'achat et à l'entretien de droits de propriété intellectuelle issus de la recherche publique nationale et à leur commercialisation* », avec un retour sur investissement de 8%. L'objectif n'a jamais été atteint. France Brevets a bénéficié, depuis sa création en 2011, de dotations en capital successives pour un total de 105 M€ souscrites à parité par l'État et la Caisse des dépôts et consignations (CDC), afin d'intervenir dans le champ de la propriété intellectuelle. La Cour avait procédé à un premier contrôle de France Brevets portant sur les exercices 2011 à 2015 qui avait souligné les difficultés auxquelles la société était confrontée et qui avait conduit la Cour à formuler des recommandations. À l'issue de ce nouveau contrôle, portant sur les exercices 2016 à 2021, la Cour conclut que France Brevets n'a pas trouvé son modèle économique et doit être dissoute.

CJUE : un droit au déréférencement de données inexactes

Par un arrêt du 8 décembre 2022, la Cour de justice de l'Union européenne a apporté une nouvelle pierre à son interprétation du droit au déréférencement des moteurs de recherche des données à l'aune du RGPD. Cette fois, l'affaire concerne une demande portant sur des allégations inexactes. La Cour estime que *« ce déréférencement n'est pas soumis à la condition que la question de l'exactitude du contenu référencé ait été résolue, au moins à titre provisoire, dans le cadre d'un recours intenté par cette personne contre le fournisseur de contenu »*. La Cour rappelle que le droit à la protection des données personnelles n'est pas absolu et doit doit être mis en balance avec d'autres droits fondamentaux dont la liberté d'information. Celle-ci ne peut toutefois être prise en compte si une partie des informations se révèlent inexactes. Si le caractère inexact n'est pas manifeste, la Cour considère que le demandeur doit fournir au moteur de recherche des éléments de preuve qu'il peut être raisonnable d'exiger. Si les preuves sont pertinentes et suffisantes, le moteur de recherche est tenu de faire droit à la demande. Dans le cas contraire, le demandeur peut saisir l'autorité de contrôle ou le juge. Dans ce cas, le moteur de recherche doit avertir le public de l'existence d'une telle procédure.

Un autre point de l'arrêt portait sur une demande de suppression de résultats d'une recherche d'images effectuée à partir du nom d'une personne physique des photographies affichées sous la forme de vignettes qui représentent cette personne. Selon la Cour, *« il y a lieu de tenir compte de la valeur informative de ces photographies indépendamment du contexte de leur publication sur la page Internet d'où elles sont extraites, mais en prenant en considération tout élément textuel qui accompagne directement l'affichage de ces photographies dans les résultats de recherche et qui est susceptible d'apporter un éclairage sur la valeur informative de celles-ci »*.

JO :// Décret sur conservation des contenus retirés ou rendus inaccessibles

Le décret du 13 décembre 2022 relatif à la conservation des contenus retirés ou rendus inaccessibles par les opérateurs de plateforme en ligne soumis à des obligations renforcées en matière de lutte contre la diffusion publique de contenus illicites, a été publié au JO le 15 décembre 2022. Le décret fixe à six mois le délai pendant lequel les grands opérateurs de plateforme en ligne soumis à des obligations renforcées en matière de lutte contre la diffusion publique de contenus illicites doivent conserver les contenus qu'ils ont retirés ou rendus inaccessibles afin de permettre à l'autorité judiciaire d'y avoir accès pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales. Le décret détermine également les modalités de conservation de ces contenus afin de garantir la sécurité de ces informations d'une part et de s'assurer que l'autorité judiciaire pourra y avoir accès dans les meilleurs délais d'autre part.

TripAdvisor condamnée pour dénigrement

Le tribunal de commerce de Paris a jugé que la société américaine Tripadviser LLC avait commis des actes de dénigrement à l'égard de la société Viaticum qui exploite le site Bourse-des-vols.com. Par un jugement du 21 novembre 2022, le tribunal l'a condamnée à verser 50 000 € de dommages-intérêts à Viaticum, ainsi que 7 000 € au titre de l'article 700 du code de procédure civile et à supprimer, sous astreinte de 1 000 euros par jour de retard, et pour 60 jours, la discussion litigieuse. Il a ordonné l'exécution provisoire du jugement. Le tribunal a estimé que Tripadviser avait *« revendiqué à tort un statut d'hébergeur pour s'affranchir de sa responsabilité alors que ce statut ne relève pas de l'évidence dès lors qu'elle savait pertinemment qu'un de ses employés était intervenu sur le fil de discussion litigieux. Durant six années elle n'a de bonne foi, entrepris aucune action, pour modérer ou tenter de modérer, les 9 messages dénigrants litigieux qui causent un préjudice, au moins d'image, à la société Viaticum, préjudice, qui nécessairement, se transforme après de si longues années en préjudice moral »*. Le tribunal a cependant réduit l'estimation par Viaticum de 100 000 € de son préjudice du fait qu'elle *« n'a pas non plus tenté d'atténuer la portée du message en y répondant alors même que cette possibilité est offerte sur le site »*.

Viaticum reprochait à TripAdvisor de détourner sa clientèle avec la création sur son site du forum de discussion *« Bourse des vols »* qui permettait d'accéder à des réservations concurrentes. Elle y avait constaté la présence de commentaires négatifs qu'elle jugeait dénigrants. Viaticum a demandé à TripAdvisor la suppression des propos litigieux mais cette dernière a refusé de le faire arguant de la liberté de la presse et qu'elle n'en n'était pas l'auteur. Viaticum l'a donc assignée pour obtenir cette suppression mais TripAdvisor a soulevé une exception d'incompétence territoriale, fondée sur ses conditions générales, dans leur version de 2013, qui prévoyaient que le droit interne de l'Etat du Massachusetts désigné par la clause permettait de déterminer le tribunal spécialement compétent. Et, subsidiairement, elle avait soulevé une exception d'incompétence au profit du tribunal judiciaire de Paris en application des dispositions de la loi du 29 juillet 1881 sur la liberté de la presse. Par un arrêt du 6 janvier 2021, la cour d'appel de Paris avait déclaré nulle la clause attributive de compétence territoriale inscrite dans les CGU de TripAdvisor qui désignait le droit du Massachusetts en matière de tribunal applicable et l'avait déboutée de son exception d'incompétence au profit du tribunal judiciaire de Paris car il s'estimait compétent dans la mesure où les faits reprochés relevaient du dénigrement et non de la diffamation. Dans le jugement au fond, le tribunal de commerce de Paris a refusé de qualifier ces actes de parasitisme car les parties ne sont pas concurrentes. Il estime au contraire que *« la divulgation, par l'une, d'une information de nature à jeter le discrédit, tels qu'« Attention, Grosse arnaque sur ce site de recherche et réservation de vols en ligne »* ou encore *« BDV = VOLEURS »*, sur un produit commercialisé par l'autre constitue un acte de dénigrement, à moins que l'information en cause ne se rapporte à un sujet d'intérêt général et repose sur une base factuelle suffisante, et sous réserve qu'elle soit exprimée avec une certaine mesure, ce qui en l'espèce n'est pas le cas ».

JO :// Ordonnance sur le casier judiciaire national automatisé

Ordonnance n° 2022-1524 du 7 décembre 2022 relative au casier judiciaire national automatisé prise pour l'application du règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019 et de la directive (UE) 2019/884 du Parlement européen et du Conseil du 17 avril 2019, a été publiée le 8 décembre 2022. Elle vise à identifier si un ressortissant de pays tiers à l'Union ou un apatride a été condamné dans un Etat membre et à fiabiliser cette recherche d'antécédents par l'usage des empreintes digitales. Les empreintes digitales de toutes les personnes, françaises, européennes ou non européennes, condamnées pour un crime ou pour un délit passible d'une peine d'emprisonnement, seront enregistrées dans le casier judiciaire.

Linagora / Blue Mind : la garantie d'éviction limitée dans le temps

L'arrêt de la cour d'appel de Paris du 24 novembre 2022 signe la fin du feuilleton judiciaire issu d'un conflit entre anciens associés de Linagora, qui avait défrayé la chronique du monde de l'open source en 2014. La cour d'appel a jugé que les deux ex-associés qui avaient fondé Blue Mind plusieurs années après avoir cédé leurs parts de Linagora (qui avait racheté Aliasource) n'avaient pas violé la garantie légale d'éviction à laquelle ils étaient tenus du fait de leur qualité de cédants des titres de la société Aliasource, pour des faits qui ont tous eu lieu plusieurs années après la cession. Ces faits *« ne peuvent entrer dans le champ protecteur des droits du cessionnaire de la garantie légale d'éviction, qui doit nécessairement être limitée dans le temps pour ne pas contrevenir au principe à valeur constitutionnel de la liberté d'entreprendre »*. Cette décision intervient sur renvoi d'un arrêt de la Cour de cassation qui avait partiellement invalidé la première décision d'appel. En concluant que les dirigeants de Blue Mind avaient manqué à leur obligation née de la garantie légale d'éviction *« sans rechercher concrètement si, au regard de l'activité de la société dont les parts avaient été cédées et du marché concerné, l'interdiction de se rétablir se justifiait encore au moment des faits reprochés »*, la cour d'appel avait privé sa décision de base légale, a estimé la Cour de cassation.

Deux associés avaient créé la société Aliasource, proposant des solutions open source, qui avait été rachetée en 2007 par Linagora. Ils avaient conservé des responsabilités de salariés dans le nouveau groupe. Mais en 2010, ils avaient démissionné de leurs fonctions et revendu leurs actions à Linagora, en raison de divergences de vue avec la direction. L'un d'eux a créé la société Blue Mind et le second l'a rejoint après. Linagora leur a reproché d'avoir violé la garantie légale d'éviction en lui interdisant de jouir de la possession paisible de la chose vendue. Elle soutenait que ses deux ex-associés lui avaient causé un préjudice par le fait d'avoir démarché et détourné sa clientèle, dénigré son logiciel OBM, capté parasitairement son savoir-faire intellectuel et industriel, de s'être approprié illicitement la technologie cédée à Linagora, d'avoir débauché des salariés, désorganisé la société et créé une société concurrente, Blue Mind.

La cour d'appel rappelle qu'en cas de cession de parts sociales, le cédant est tenu, comme dans toute vente, à garantie contre l'éviction dans les conditions prévues par les articles 1626 à 1640 du code civil et il doit s'abstenir de tout acte de nature à empêcher la poursuite de l'activité économique de la société. Cependant, ajoute-t-elle, *« cette exigence légale de non-concurrence née de la garantie d'éviction doit être proportionnée à la protection des intérêts légitimes de l'acquéreur à raison de l'acquisition à laquelle il a procédé et ne doit pas porter une atteinte disproportionnée à la liberté du commerce et de l'industrie, et par conséquent, à la liberté d'entreprendre, qui a valeur constitutionnelle. Le respect du principe de la liberté du commerce et de l'industrie exige ainsi que l'interdiction de concurrence soit délimitée quant à l'activité interdite d'une part et quant au cadre spatio-temporel dans lequel cette activité est interdite d'autre part. Cette délimitation doit s'apprécier in concreto, au regard de l'activité et du marché concernés »*.

JO :// Décret sur l'interdiction d'impression et de distribution systématiques des tickets de caisse et de carte bancaire

Le décret du 14 décembre 2022 relatif aux conditions et modalités d'application du IV de l'article L. 541-15-10 du code de l'environnement a été publié le 15 décembre 2022. Il définit les conditions et les modalités de cet article qui interdit l'impression et la distribution systématiques des tickets de caisse dans les surfaces de vente et dans les établissements recevant du public, des tickets de cartes bancaires ou délivrés par des automates, ainsi que des bons d'achat, de réduction ou promotionnels dans les surfaces de vente. Il précise la notion « d'impression et de distribution systématiques » et détermine les cas pour lesquels l'interdiction ne s'applique pas.

Vous avez envie de partager une jurisprudence intéressante ou inédite avec la communauté des lecteurs d'Expertises.

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld *sr@expertises.info*

La fabrique du code du numérique

Sylvie Rozenfeld : Il a fallu attendre 2021 pour qu'un éditeur, LexisNexis, publie un code du numérique, à votre initiative, Denis Berthault, (président du gf2i I) et Fabrice Mattatia (docteur en droit, chercheur associé à l'université Paris-1). Une édition 2023 est parue. Pourquoi publier un code du numérique ?

Denis Berthault : Nous sommes partis du constat que les textes qui concernent le numérique sont très épars. Le droit du numérique n'a pas été pensé, il n'a pas été piloté et il se construit par petits bouts. Ce qui nous a plu, c'est de borner ce nouveau droit. Il est désormais codé, plutôt codifié. Juridiquement c'est un code d'éditeur, un code conçu par un éditeur pour un public, une compilation de textes officiels reclassifiés, réorganisés, réindexés pour les besoins du praticien. Il s'oppose à un code officiel conçu par l'Etat. Je dirais même qu'il s'agit d'un code d'auteurs, car c'est nous qui en avons eu l'idée, qui l'avons apportée à LexisNexis et c'est Fabrice Mattatia qui a formé l'équipe, composée d'une quinzaine de contributeurs, en nous comptant.

Fabrice Mattatia : Avec ce code, le praticien va pouvoir trouver rapidement les fondamentaux. Le code contient le droit national, le droit européen applicable, et des lois étrangères, comme le Cloud Act américain qui est applicable aux sociétés françaises, et la loi chinoise PIPL, qui l'est également, comme l'illustre le choix du comité d'organisation des JO de confier l'informatique des JO de Paris à des acteurs chinois.
Pour illustrer les textes, le code commente les principales jurisprudences.

D. B. : Les textes sont foisonnants, éparpillés, dédiés aux technologies, intégrés dans des textes non numériques, sans compter les dispositions du droit commun qui peuvent s'appliquer à la matière. On a voulu brosser tous les champs pour un juriste.

Comment avez-vous procédé ?

D. B. : On est parti chacun avec son savoir, Fabrice est spécialisé dans les données personnelles et moi dans les données publiques. Cela ne représente que 25 ou 30 % de la matière. Puis on a bâti le sommaire avec tous les points qu'on voulait aborder. Fabrice a construit un plan en trois parties où tout se tient. Première partie : les contenus, deuxième partie : les contenants et outils et troisième partie : les activités numériques. Ensuite, nous avons cherché le spécialiste qui pourrait traiter chaque matière. En plus de nous, une bonne douzaine d'auteurs ont participé à l'aventure. Nous sommes intervenus en tant qu'auteurs, mais nous avons aussi géré une équipe. C'est une œuvre créative, celle de défricher un nouveau droit.

Et pour la seconde édition ?

D. B. : La première édition a plutôt bien marché commercialement, ce qui a motivé l'éditeur à sortir une nouvelle version. Celle-ci a augmenté de 30 %.
On a introduit une nouvelle partie sur certaines professions réglementées (avocat, huissier, magistrat, notaire). Par ailleurs dans la première édition, on s'est aperçu qu'il y avait des redites car des questions avaient été traitées par deux personnes différentes, et qu'il y avait des oublis dans l'index. A noter que c'est le premier index du droit du numérique.

F. M. : Le droit du numérique évolue très vite. Il suffit d'observer la production de textes au niveau européen avec tous les « *acts* » sur le numérique. Concernant la jurisprudence sur les données personnelles, toutes les semaines, de nouveaux dossiers sont ouverts auprès de la CJUE. Quand elle rendra ses arrêts par rafales, il va falloir les intégrer, par exemple sur les données de connexion ou sur la propriété intellectuelle. Par ailleurs en France les lois sont régulièrement mises à jour.

Envisagez-vous une mise à jour en ligne ?

D. B. : Nous faisons une mise à jour annuelle et c'est un très gros travail. Faire une mise à jour en continu, via le numérique, c'est un autre métier. Les auteurs n'ont pas le temps de faire cette veille quotidienne, et de mettre à jour leur contribution dès qu'un texte sort. Ils le font une fois par an.

Votre code n'a pas de numérotation.

D. B. : Ça n'aurait pas de sens car cela ne serait pas utilisé dans les codes officiels. Il y a 25 ans, j'avais travaillé avec la direction supérieure de codification, sous la houlette du conseiller d'Etat Guy Braibant, qui voulait codifier à droit constant. Elle a pris les domaines du droit, les a réorganisés, a établi des sommaires et a renuméroté les articles. Et c'est devenu la numérotation officielle. Donc on ne peut pas avoir deux numérotations dans deux codes pour un même article de loi.

F. M. : Avec notre angle du numérique, nous avons identifié de nombreuses dispositions éparpillées, qui sont elles-mêmes intégrées dans des ensembles qui ont leur logique propre, différente de la nôtre. Par exemple, les données de santé sont intégrées dans le code de la santé publique, qui a sa logique « *santé* ». S'il y avait un code officiel du numérique, il faudrait retirer ces dispositions du code de la santé publique. Prenons également l'exemple de la garantie légale contre les vices cachés dans le code de la consommation, dans la partie de notre code consacrée aux achats en ligne. Extraire cette partie du code de la consommation pour l'intégrer dans un code du numérique ne présenterait pas d'intérêt, car elle serait séparée des dispositions sur les garanties légales. De même, pour le code de la propriété intellectuelle, ça n'aurait pas de sens de retirer les œuvres numériques, car les principes de base de la PI leur sont applicables.

Propos recueillis par

Sylvie ROZENFELD

VÉRONIQUE CHAPUIS-THUAULT

L'intelligence juridique : pour un juriste stratège

Dans le contexte de guerre économique d'un monde globalisé, l'intelligence juridique consiste à amener les métiers du droit à faire de la stratégie. Comme l'explique Véronique Chapuis-Thuault, spécialiste d'intelligence juridique, le juriste pourra mieux étayer une proposition de politique juridique, contractuelle et judiciaire s'il prend en compte les aspects politique, économique, technique d'une situation. Il doit donc adopter une vision holistique et élargie du droit. La donnée se place au centre de cette stratégie, en tant qu'outil de veille informationnelle mais aussi en tant que facteur de déstabilisation de l'entreprise, si le patrimoine immatériel n'est pas bien protégé. Selon elle, les outils numériques et l'IA sont très utiles, à condition de placer au centre la personne, dont l'intuition et l'expérience restent indispensables pour décoder le réel et proposer des solutions juridiques.

Sylvie Rozenfeld : On connaît l'intelligence économique, mais beaucoup moins ou pas du tout l'intelligence juridique. Ce terme a émergé en 2018 et il s'inscrit dans le courant de l'intelligence économique tout en y apportant certaines particularités propres aux métiers du droit et à la pensée juridique. Véronique Chapuis-Thuault, vous avez été directrice juridique dans des groupes internationaux, vous êtes créatrice du programme Intelligence Juridique de l'Ecole de guerre économique, fondée par Christian Harbulot voici 25 ans. Vous êtes également fondatrice, et PDG de la start up Lex Colibri, spécialisée en intelligence juridique et valorisation des innovations.
L'intelligence juridique est-ce un nouveau concept marketing ? Quel rapport avec l'intelligence économique ?

Véronique Chapuis-Thuault : La motivation pour déployer l'intelligence juridique aujourd'hui n'est pas d'ordre marketing mais vient du constat de l'utilisation du droit comme arme de guerre économique, essentiellement avec le développement de l'extra-territorialité des lois américaines, avec une volonté d'asservissement et d'affaiblissement, notamment du côté des Etats-Unis. Un article de Marianne Frison-Roche montre bien que les principales entreprises visées sont européennes alors qu'en matière de lutte contre la corruption, des entreprises chinoises pourraient tout aussi être attraites, poursuivies et condamnées. C'est comme ça que le lien entre le droit et la géo-politique applicable aux entreprises doit être étudié. Avant de penser à déployer l'intelligence juridique, on s'est interrogé sur le fait de conserver l'expression « *droit et intelligence économique* ». Elle avait l'inconvénient de rester sur des silos, sur les activités de l'intelligence économique et sur l'impact du droit sur ces activités. On avait constaté aux débuts de notre réflexion en 2018 que le terme d'intelligence juridique permettait de rentrer dans le cœur des problématiques, autrement dit dans le cœur du « *réacteur juridique* ». Or, c'est le seul moyen de décoder les rapports de force et les stratégies d'influence par le droit.

« L'utilisation du droit comme arme de guerre économique, essentiellement avec le développement de l'extra-territorialité des lois américaines. »

En quoi ça consiste ?
Il s'agit premièrement d'étudier la fabrique du droit, le droit dur et le droit souple et leurs interactions. Deuxièmement, on s'intéresse à la puissance des administrations comme le département de la Justice américain qui lance des poursuites contre des entreprises étrangères et utilise le marché américain comme un levier juridique et économique très puissant. La menace de sanction est liée à la menace d'être déréférencé et de ne plus pouvoir faire d'offres sur le marché américain : c'est vraiment dissuasif. En Europe aujourd'hui, nous n'utilisons pas le marché européen comme un levier pour défendre nos valeurs et nos principes. Troisièmement, la justice avec le développement alternatif des litiges ouvre la voie à du forum shopping et du legal shopping, permettant de choisir la loi la plus favorable ou de soumettre le règlement des litiges dans des pays plus attractifs. Quatrièmement, l'intelligence juridique concerne aussi l'évolution des métiers du droit. On s'intéresse par exemple à l'impact de l'absence de legal privilege au bénéfice des juristes d'entreprise français puisque lorsque l'on dit quelque chose à son président, on est face à une injonction paradoxale qui fait que le conseil juridique qu'on émet peut se retourner contre l'entreprise. Il devient un risque alors qu'il devrait être une source de progrès. Par ailleurs, on étudie comment l'externalisation de fonctions juridiques vers certains pays à bas coûts, pour de la veille ou de la contractualisation, peut créer un enjeu de dépendance ou d'influence ou peut faire partie de stratégies de domination pouvant être, à terme, des facteurs de déstabilisation, voire d'atteinte à la souveraineté ou à la sécurité économique. Et le dernier point porte sur les évolutions du numérique. On entend beaucoup parler des legal techs qui commencent à faire émerger des produits utiles aux juristes, tous métiers du droit confondus. Être outillé est devenu indispensable, vu l'augmentation du volume de datas, de textes juridiques à traiter et de transactions à conclure. Mais ce qu'on va analyser sous l'angle de l'intelligence juridique c'est l'impact de l'ontologie des systèmes.

Qu'entendez-vous par l'ontologie des systèmes ?
C'est la manière dont le système a été conçu : quel droit, quel mode de pensée, quelles finalités, car ça risque d'induire un formatage des pratiques voire des pensées. On l'a vu avec les normes IFRS, ce sont de normes américaines qui ont prévalues sur les normes européennes. L'intelligence juridique montre que c'est un outil d'influence indéniable.

C'est une arme de soft power.
C'est du soft power par la technique. Mais il fait face à une réalité occultée par l'engouement actuel pour la tech : le droit est une matière

vivante apportant un cadre reflétant les valeurs d'une société pour permettre aux citoyens de vivre et d'échanger en harmonie. L'industrialisation du droit doit être circonscrite à l'utilisation d'outils pour faciliter le travail des juristes, tous métiers confondus. On ne compare pas un agriculteur à son tracteur. Pourquoi comparer la performance d'un juriste à celui d'un outil numérique ! C'est un point de vigilance important pour l'intelligence juridique. On doit rester alerte pour détecter les signaux faibles, faire de la prospective et anticiper.

« Les juristes doivent s'intéresser à la politique et à la stratégie car la brique juridique aujourd'hui représente un enjeu à prendre en compte en amont dans la construction des stratégies de l'entreprise. »

Fort de ces constats, l'objectif de l'intelligence juridique consiste à répondre à une demande de comprendre cette utilisation du droit dans la guerre économique. Elle va également s'intéresser à la Lawfare, Je parle de Lawfare car il n'y a pas vraiment d'expression équivalente en français : c'est l'utilisation du droit comme une arme de guerre, guerre économique, de conflit. L'intérêt porte également sur la guerre économique Economic warfare et sur la guerre hybride (hybrid war). Tout l'enjeu consiste à étudier ces tactiques guerrières, sachant qu'une guerre se prépare pendant des années... On l'a vu avec la Russie et les accords qu'elle a pu conclure via Gasprom.

Pour conclure, l'intérêt de l'intelligence juridique est donc d'amener les métiers du droit à faire de la stratégie en prenant en compte le contexte, l'environnement politique, économique, technique, pour contextualiser les enjeux juridiques, mieux étayer une proposition de politique juridique, contractuelle et judiciaire, en résumé pour être un stratège au service de la politique de l'entreprise édictée par les dirigeants.

Est-ce une tendance récente ?

C'est une tendance qui s'accroît et qui devient une nécessité. On l'a vu avec le Covid, la guerre en Ukraine, avec la démultiplication des sanctions économiques, ou les conflits de sanctions entre la Chine et les Etats-Unis. La Chine est en train de se doter d'un arsenal juridique intéressant et de qualité qui amène, par exemple, la banque HSBC à envisager de fractionner son groupe pour éviter de se retrouver coincée entre les sanctions américaines et chinoises, étant incapable, en tant qu'entité unique mondiale avec ses filiales, de pouvoir se conformer aux deux exigences. Aujourd'hui, on parle beaucoup de legal operations, de legal design. Si on observe la pyramide de la chaîne de commandement qui commence par la politique, le stratégique puis l'opérationnel et enfin les actions, l'intelligence juridique couvre toute la chaîne des niveaux 1 à 4 avec un focus sur les niveaux 1 politique et 2 stratégie. Il faut absolument que les juristes, tous métiers confondus, s'intéressent à la politique et à la stratégie car la brique juridique aujourd'hui représente un enjeu qui doit être pris en compte en amont dans la construction des stratégies de l'entreprise.

Un autre point est inspiré du RGPD avec le principe du privacy by design, à savoir la prise en compte du « *paramètre juridique* » et de l'éthique en amont dans la conception des politiques, stratégies, projets et systèmes.

Donc on parle de legal by design.

Tout à fait. Comment prendre en compte, par exemple dans la conception des produits numériques les enjeux des règles juridiques et éthiques. On se trouve sur une bascule impressionnante, un virage à 180 °. Avant, on consultait les juristes en aval : le dirigeant décidait puis demandait au juriste de transcrire son projet en des termes juridiques corrects. En cas de problème, on consultait un avocat, puis le juge. Aujourd'hui avec la globalisation, l'évolution vers l'instrumentalisation du droit, l'aval intervient trop tard. Aujourd'hui, il faut anticiper.

Il me semble que dans les études de droit, cette dimension est peu prise en compte.

Elle a été prise en compte mais l'enseignement reste par silos, concentré sur le droit avec une vision holistique limitée. L'enseignement reste sur un ou des droits (société, concurrence...) alors qu'au quotidien, les juristes d'entreprise travaillent exclusivement pour des stratégies multi-factorielles et des projets.

La donnée n'est-elle pas au cœur de l'intelligence juridique ?

L'intelligence juridique dans la forme que j'ai proposée à l'Ecole de guerre économique, possède l'avantage d'avoir une vision à 360° et transversale. Si l'on parle de souveraineté, par exemple, on a des données personnelles mais il y a aussi beaucoup de données stratégiques qui constituent un avantage compétitif. Cela comprend les informations couvertes par le secret des affaires. On constate cependant que les entreprises n'ont pas encore vraiment intégré la puissance de la loi de 2018 sur le secret des

affaires. En matière de gestion des données, on fait encore trop confiance au système informatique et au « *NDA* » (accord de confidentialité). Or, il ne suffit pas de choisir un outil, car c'est un enjeu de gouvernance d'entreprise. Il est nécessaire d'avoir une stratégie de protection de la donnée, en trouvant un équilibre entre pas assez et trop de protection, qui est coûteuse. Il faut donc avoir cette vision holistique de la donnée sans la limiter aux données personnelles.

Vous évoquez les données de l'entreprise mais il y a aussi les données que l'entreprise collecte pour faire de la veille.
Sur les données extérieures à l'entreprise, il y a un coup de barre à droite à opérer car, en plus de la veille juridique qui est importante, il y a un enjeu de contextualisation par rapport à l'actualité, à savoir quels sont les impacts des stratégies des acteurs sur le droit. Généralement, les publications juridiques ne rentrent pas toujours de façon assez précise dans les impacts juridiques des stratégies d'acteurs. Pour les directeurs juridiques, cette information est intéressante mais il faut la réinterpréter pour décoder les stratégies. Cela manque de vision holistique. Et aussi, aujourd'hui, dans un monde globalisé, on a besoin d'éléments de droit comparé. Pour ce qui concerne la veille, il nous faut des outils performants.

Aujourd'hui, nous sommes confrontés à une inflation de lois et de textes réglementaires. L'open data et notamment l'ouverture des décisions de justice représente-t-elle un changement essentiel dans la pratique juridique ?
C'est un atout et un danger. Si l'on prend le parallèle avec les sciences, l'open data permet le partage des connaissances, ça ouvre des opportunités intéressantes. Mais c'est à double tranchant. Si on regarde le mouvement vers l'open data des décisions de justice, il est essentiel de protéger les justiciables, autant les citoyens que les entreprises. Et de regarder ce que font les autres pays pour ne pas créer de situations défavorables.

« Les concepteurs et développeurs d'IA doivent travailler plus en amont avec des juristes. »

Les données personnelles ?
Données personnelles et secrets des affaires sont un outil de concurrence extraordinaire. Si les autres pays faisaient la même chose en ouvrant au public certaines données concernant leurs entreprises, tout le monde serait à égalité. Ce qui n'est pas le cas. La France ne doit pas donner tout, pour être la première de la classe. Elle va créer un désavantage compétitif à la charge de ses entreprises.

L'intelligence artificielle vous est-elle utile ?
L'IA est intéressante. Il faut distinguer les usages. Elle est très utile pour faciliter la recherche d'informations. Mais il faut que les concepteurs et développeurs travaillent plus en amont avec des juristes. Par exemple, la création d'une obligation ou d'un document qui a de la valeur peut avoir été rédigée sur un bout de nappe en papier par le président d'une entreprise dans un restaurant. Aujourd'hui, la démarche des spécialistes d'IA reste beaucoup trop en silo, et n'intègre pas la connaissance de la genèse des données, de leur vie ni de leur finalité. Ils ne sont pas toujours conscients des pratiques et ont une approche très industrielle. Ils oublient aussi que le droit est une matière vivante qui s'applique à des êtres humains qui ont beaucoup d'idées. Le juriste va utiliser son intuition, autant que son expérience pour décoder les stratégies et proposer des solutions juridiques. Je suis souvent contactée par des spécialistes de l'IA qui rêvent d'accéder à des bases de données juridiques pour nourrir leur système auto-apprenant. Je leur réponds que ce n'est pas la bonne démarche. Il faut se demander comment le système a été conçu, à quoi l'algorithme est entraîné, que va-t-il aller chercher ? C'est cette démarche qui nous permettra d'avoir des systèmes intéressants qui vont respecter notre droit, nos valeurs, notre contrat social et les besoins des juristes. Il m'arrive aussi d'être consultée pour l'expression des besoins, vulgariser les règles juridiques pour qu'elles soient compréhensibles par des ingénieurs et présenter les pratiques et montrer comment on peut intégrer dans la conception des zones de liberté pour replacer l'humain au centre. On ne peut pas réussir à couvrir plus de 85 à 90 % des cas avec ce genre d'outils, sans intervention humaine. Reprenons mon exemple de la nappe de restaurant, si on ne retrouve pas cet élément qui peut être la base d'un accord international, ça peut avoir des conséquences dramatiques. J'appelle à plus de flexibilité des systèmes, une conception qui va repenser le positionnement de la personne, du sachant , l'IA étant un outil et non un concurrent de l'homme ou de la femme. On peut faire une analogie entre le prêt-à-porter, le demi-mesure et le sur mesure. Il ne faut pas imaginer que le droit c'est 90% de prêt-à-porter. La part de demi-mesure et de haute couture reste importante. Ce n'est pas déterminé par le montant du contrat mais par l'existence de « *zone de dérapage* ». Et c'est une personne humaine, le juriste, qui va le voir, le sentir.

Pourquoi inclut-on l'identification et la protection du patrimoine immatériel de l'entreprise dans le champ de l'intelligence juridique ?
Dans l'intelligence juridique, on va étudier tout ce qui est tactique de conquête, de déstabilisation, de mise sous influence. Et à l'inverse, on va envisager toutes les zones de risques. Or, la fuite d'informations sensibles qui représentent un avantage compétitif pour l'entreprises est une zone de risque importante. Ce qui va aussi nous amener à nous intéresser à la cybersécurité, à la lutte contre les discours de haine sur internet, à regarder si l'entreprise est exposée dans le darknet. Tout ce qui représente un facteur de déstabilisation de l'entreprise à court, moyen et long terme. En ce qui concerne la gestion de crise, on va établir des plans de prévention. Cela inclut la stratégie de protection de la propriété intellectuelle mais aussi informationnelle comme les secrets d'affaires, le savoir-faire.

« On étudie les tactiques de conquête, de déstabilisation, de mise sous influence et on envisage toutes les zones de risques. »

J'ai lu que l'intelligence juridique permettrait de lutter contre l'uberisation du droit. Le droit court-il ce danger ?
Il est très important de lutter contre l'ubérisation du droit. Dans les signaux faibles qui révèlent le phénomène, il y a les pratiques de legal operation, comme les legal tech qui industrialisent la production de missions juridiques comme celle de smart contracts, des chatbots, etc. Autre signal faible, l'externalisation de certaines missions juridiques dans des pays à bas coûts pour la veille par exemple, la production de contrats simples, la mise en place de hotline, etc.
Dans l'ubérisation, j'y mets aussi la dégradation du juriste au rang d'un exécutant surveillant le travail de machines. Il faut remettre le juriste stratège au premier rang, un juriste qui fait le droit, qui le pense et qui l'applique et qui en contrôle l'application. On n'est pas simplement un « *juriste augmenté* » bien outillé. Plus généralement, sur l'industrialisation des fonctions de support dont le droit, il faut être attentif car le droit représente le ciment de la société. L'intelligence juridique met en avant ces signaux faibles, les contextualise pour rechercher des solutions pour limiter ses effets. Donc détection et prévention avec l'apport d'une grille de lecture pour définir des tactiques.

Comment l'intelligence juridique se déploie ?
L'AFJE (Association française des juristes d'entreprise) a créé une commission d'intelligence juridique. On constate une tendance à la prise en compte du droit dans toutes ces composantes pour faire évoluer les intégrations entre les métiers. Il faut opérer une ouverture vers les enjeux de Lawfare, d'Economic warfare et de guerre hybride Hybrid war. Les Chinois ont très bien décodé la stratégie américaine et ont mis en place des systèmes et des contre-mesures contre les sanctions internationales qui vont très loin. Ils ont compris l'enjeu du RGPD et ont adopté la Personal Information Protection Law (PIBL). Ils ont analysé les tactiques de Napoléon avec le code civil et utilisent le droit dans toutes leurs politiques d'expansion sur la Route de la Soie par exemple. Face à cela, nous devons nous interroger sur nos actions et sur le manque d'efficacité ou la relative efficacité de nos politiques. Nous avons des outils juridiques de grande qualité, structurant comme le droit de la concurrence ou attractif comme le visa AMF. Il nous faut des actions défensives mais aussi offensives. Si vis Pacem, para bellum (*).

L'intelligence juridique apporte-t-elle plus de sécurité juridique ?
Elle apporte de la sécurité juridique, de la sécurité économique. Elle amène à travailler avec d'autres métiers, notamment avec les directeurs de la sûreté, des ressources humaines, des finances, du commercial, des achats, de la qualité etc., soit tous les métiers. Elle permet d'avoir cette vision élargie du droit : c'est vrai pour les directeurs juridiques, mais aussi pour les avocats, pour toutes les professions juridiques. Au niveau de l'Etat, ça amène à militer en faveur du développement des études d'impact de la loi pour cibler les mesures les plus adéquates éviter cet empilement de textes législatifs.

Propos recueillis par
Sylvie ROZENFELD

(*) Si tu veux la paix, prépare la guerre

DONNÉES DE SANTÉ

Certification hébergeurs : un projet de référentiel, entre clarifications et interrogations

Le très attendu projet de référentiel de certification des hébergeurs de données de santé a été publié pour concertation publique par l'Agence du numérique en santé[1]. Il prévoit d'importantes modifications tant dans son champ d'application que dans le contenu des exigences, notamment une obligation de localisation des données dans l'Espace économique européen et les pays adéquats. Ceci risque d'entraîner de nombreuses interrogations, alors que ce dispositif faisait déjà l'objet de débats qui nuisaient à sa bonne application.

La certification hébergeurs de données de santé (« *HDS* ») constitue, pour mémoire, une obligation issue du droit français, pour tout acteur qui héberge certaines données médicales pour le compte d'un responsable de traitement (tel qu'un établissement de santé, un prestataire de services de soins…). S'agissant d'une certification conditionnant l'accès au marché de nombreux acteurs, tant son champ d'application que le contenu de ses exigences ont depuis ses origines fait débat. Toutefois, malgré l'ancienneté du dispositif et la volonté certaine du législateur de le pérenniser, un flou juridique persiste autour de ces questions, que le nouveau projet ne semble pas suffisamment résoudre.

L'éternelle question du champ d'application de la certification HDS

Les incertaines exemptions de certains acteurs

Le champ d'application matériel de la certification HDS souffre depuis l'origine d'un flou lié à une définition relativement complexe. Celle-ci couvre tout d'abord le cas où un responsable de traitement externalise l'hébergement auprès d'un tiers. Cette formulation, qui a l'avantage de s'aligner sur les concepts du RGPD, ne résout cependant pas la question des cas d'hébergement intra-groupe[2].

De plus, la certification ne s'applique pas à toutes les données de santé, mais uniquement à celles « *recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social* ». Il s'agit clairement d'une volonté du législateur de ne pas étendre outre mesure cette réglementation, et ne pas épouser les très larges contours de la notion de données de santé au sens de la réglementation de protection des données personnelles.

Toutefois, ceci pourrait impliquer que les données recueillies à l'occasion d'activités de recherche (publique ou privée), ou d'assurance, de veille sanitaire, ne seraient pas concernées par cette obligation[3]. La question est de savoir si des données intrinsèquement issues d'un diagnostic médical font basculer dans la certification (par exemple, indiquer un antécédent médical dans le cadre d'un questionnaire de recherche).

Le nouveau référentiel pourrait être l'occasion d'apporter des précisions pérennes sur ce point, car les éléments fournis dans le projet actuel se cantonnent à rappeler les définitions existantes au sein de l'article L.1111-8 du code de la santé publique. Or, des exemptions ont été créées par l'administration au fil du temps, sans que le fondement juridique n'en soit parfaitement clair et sans que leur pérennité ne soit assurée par un texte.

Notamment, la FAQ HDS[4], applique un raisonnement selon lequel ne sont pas soumis à l'obligation de recourir à un hébergeur certifié HDS les organismes « *qui manipulent des données de santé* » mais « *n'en sont pas à l'origine* ». Par cette interprétation littérale de l'article L.1111-8, ce document exempte notamment de l'obligation de recourir à un hébergeur certifié les organismes d'assurance maladie obligatoire et complémentaire dans le cadre de leur activité de prise en charge des frais de santé et les associations qui proposent des activités sportives à des personnes handicapées. Or, force est de noter que la Cnil semble ne pas souscrire pas à cette interprétation, en considérant par exemple

EXPERTISES 2022 - TABLES CLASSIFIÉES
du n°475 au n°485

INTERVIEW *PAR SYLVIE ROZENFELD*

1 - PROBLÉMATIQUES INNOVANTES

TABLE

2 - CONTRATS

3 - PROPRIETE INTELLECTUELLE

4 - LITIGES INFORMATIQUES

5 - CRIMINALITÉ INFORMATIQUE

6 - SÉCURITÉ, RISQUES, ASSURANCES

TABLE

7 - SYSTÈMES ÉLECTRONIQUE DE PAIEMENT, E-COMMERCE

8 - DROIT DE L'INFORMATION, DES DONNÉES ET DES BASES DE DONNÉES

9 - INTERNET

10 - DROIT DE LA PREUVE

11 - DROIT DU TRAVAIL

12 - DONNÉES PERSONNELLES

TABLE

13 - FISCALITÉ

que sont soumis à l'obligation de recourir à un hébergeur certifié de nombreux organismes qui manipulent des données de santé mais n'en sont pas à l'origine, par exemple, les laboratoires pharmaceutiques qui recueillent, en tant que responsables de traitement, des signaux de vigilance sanitaire transmis par des professionnels de santé ou des patients[5], ou encore les entrepôts de données de santé qui recueillent des données de santé, en tant que responsables de traitement, provenant de structures tierces, et pour lesquels la Cnil impose systématique que l'infrastructure soit hébergée chez un hébergeur certifié. Ces exemptions et notamment l'articulation entre ces deux positions pourrait être clarifiée via le référentiel, afin que les acteurs puissent se fonder sur une doctrine sans ambiguïté.

De façon similaire, le référentiel indique que « *L'obligation de certification HDS ne s'applique pas aux personnes à l'origine de la production ou du recueil des données, par exemple les établissements et professionnels de santé* », ce qui emporte le risque d'être interprété comme excluant de façon générale les établissements de santé, alors que dans certains cas, ceux-ci ne sont pas nécessairement producteurs de la donnée et peuvent héberger pour le compte de tiers (par exemple, le débat classique de l'établissement support des GHT, ou des cas d'entrepôts de données de santé centralisés par un établissement pour le compte d'autres établissements, ou dans le cadre de projets de recherche, etc.). Là encore, ce point devrait être clarifié afin de comprendre si les établissements bénéficient en réalité d'une exemption générale – et sur quel fondement – ou s'il s'agit d'un simple rappel de la qualification (habituelle mais non systématique) de responsables de traitements des établissements. La distinction actuelle entre hébergeurs infogéreurs et hébergeurs d'infrastructure semble être abandonnée. Or, certaines exigences du décret et du référentiel de certification n'apparaissent pas pouvoir s'appliquer en pratique aux hébergeurs dénommés actuellement « *hébergeurs d'infrastructure* », et tout particulièrement aux hébergeurs proposant des services dits de « *salle blanche* » ou d'« *hébergement sec* » (activité 1 voire 2). La déclaration d'applicabilité ne paraît pas pouvoir permettre à l'organisme certificateur d'identifier seul quelles obligations ont un sens selon les différentes activités de l'hébergeur, pour ce qui concerne au moins les obligations contractuelles. L'identification par le référentiel de certification de ces spécificités, pourrait être ainsi utile pour harmoniser les pratiques.

A cet égard, la doctrine de l'ancien Comité d'agrément des hébergeurs sur les salles blanches, notamment résumée dans son second rapport d'activité, permettait de reporter sur les cocontractants des hébergeurs d'infrastructure ou des salles blanches les obligations du décret et du référentiel qui ne font pas en réalité partie de leur périmètre opérationnel. Aussi, le référentiel pourrait notamment lister celles des clauses obligatoires de l'article R. 1111-1 du code de la santé publique qui n'ont pas vocation à être appliquées directement par de tels hébergeurs et à être reportées sur le cocontractant.

Une définition partielle des activités

L'un des objectifs majeurs de cette nouvelle version du référentiel est de mettre un terme aux tergiversations sur l'une des activités couvertes par l'obligation de certification, l'activité 5 (administration et d'exploitation du système d'information), via une nouvelle définition selon laquelle cette activité comporte :

- *« L'encadrement et la gestion des accès occasionnels des tiers mandatés par le client de l'organisation, par exemple à des fins d'audit, d'expertise, de déploiement ou de maintenance, amenés à accéder via le Socle d'Infrastructure HDS à l'Application métier. Les accès des Utilisateurs finaux et du responsable de traitement ne sont pas concernés. Ces tiers mandatés ne sont pas tenus d'être certifiés HDS.*
- *Le maintien en condition de sécurité du Socle d'Infrastructure HDS et le centre de support au client. (...).*
- *La documentation tenue à jour (...) ».*

Cette nouvelle définition semble malheureusement ne pas résoudre tous les débats sur ce complexe sujet. Tout d'abord, sur la forme, la définition intègre à la fois des éléments de définition juridique et de régime applicable, ce qui nuit à la bonne compréhension de l'intention des rédacteurs. Tout particulièrement, il semble exister une contradiction entre le fait de reconnaître que les accès occasionnels par des tiers mandatés entrent bien dans la définition de l'activité 5, mais sont malgré cela exemptés de l'obligation de certification. En outre, le fondement juridique sur lequel le référentiel décide ainsi d'une exemption au régime HDS prévu par le législateur n'est pas précisé[6].

Sur le fond, tout d'abord, l'usage du terme « *comporte* » ne permet par ailleurs pas de garantir que le référentiel liste de façon exhaustive toutes les activités couvertes par l'activité 5. Il serait utile de confirmer que seul le maintien en condition de sécurité et le centre de support, et la documentation associée, sont désormais couverts par l'activité 5. Ensuite, la notion d'accès « *occasionnel* » n'est pas définie. Aussi, un accès régulier à des fins de maintenance à distance dans le cadre d'un contrat à durée indéterminée de maintenance constituera-t-il un accès occasionnel ?

De même, l'impact d'un éventuel accès aux données n'est pas clairement indiqué : aussi, un accès à des fins de maintenance qui impliquerait un accès aux données devrait-il être soumis à la certification alors qu'un accès à l'infrastructure seule sans accès aux données ne le serait pas ? Sur ce point, il faut relever que les « *tiers mandatés* » sont ceux qui accèdent « *via le Socle d'Infrastructure HDS à l'Application métier* », ce qui implique ainsi très probablement un accès aux données, alors qu'ils sont expressément « *exemptés* » de certification. En tout état de cause, ce critère d'accès aux données n'existe pas en droit positif, dès lors que le référentiel HDS couvre en grande partie des activités qui n'impliquent aucun accès direct aux données mais assurent la sécurité de l'ensemble de l'infrastructure.

Une définition exhaustive n'étant pas toujours envisageable, des exemples d'activités couvertes et d'activités non couvertes pourraient être fournis, en complément, via la future FAQ HDS, concernant les cas d'usage usuellement identifiés par le secteur.

En sus, le potentiel flou dans la définition de l'activité 5 pose la question de la responsabilité de l'hébergeur certifié qui serait amené à devoir travailler avec un infogérant certifié sur ce périmètre, à la demande de son client. L'hébergeur HDS doit-il s'assurer que le tiers est bien « *mandaté* » et de quelle façon ? Peut-il être tenu pour responsable d'avoir accepté, à la demande de son client, d'ouvrir un accès pour un tiers qui in fine, aurait dû être certifié ?

De façon générale, il serait essentiel de définir de façon précise chacune des activités listées par le décret, dès lors que la notion d'hébergement elle-même n'est pas définie. Ces notions constituent un critère fondamental pour déterminer quels acteurs sont effectivement soumis à la procédure de certification.

De nouvelles interrogations liées aux modifications importantes du contenu des exigences

L'ajout inédit d'une exigence de localisation des données

L'un des éléments cruciaux du projet se trouve dans une nouvelle exigence indiquant que les lieux d'hébergement doivent être localisés dans l'EEE ou des pays assurant un niveau de protection adéquat, à l'exclusion des garanties telles que les clauses types ou les BCRs. Il s'agit ainsi d'une obligation de localisation des données, particulièrement impactante pour de nombreux acteurs. La certification HDS n'est en effet pas facultative, mais constitue une condition d'accès au marché pour les prestataires.

Or, le fondement juridique de cette exigence de localisation des données, qui n'est pas prévue par le législateur, n'est pas évident. La question de la compétence de l'administration à créer une telle règle de droit se pose. Par simple analogie, il est possible de citer le cas des anciennes lignes directrices/recommandations cookies de la Cnil qui ont fait l'objet d'une censure par le Conseil d'Etat sur les aspects considérés comme allant au-delà des exigences expresses du RGPD[7], ou les décisions ayant annulé le dispositif de certification des logiciels d'aide à la décision[8], par lequel la France a été considérée comme imposant des obligations supplémentaires à celles d'ores et déjà prévues au niveau européen pour l'accès au marché (marquage CE).

Comme le précise notamment la FAQ HDS actuelle, l'article L. 1111-8 du code de la santé publique n'a jamais emporté d'obligation de localisation des données et le passage de l'agrément à la certification avait précisément vocation, pour le législateur, à favoriser la certification d'acteurs internationaux et la circulation des données dans de bonnes conditions de sécurité.

Toutefois, dans le contexte post-Schrems II, les transferts de données vers des pays ne bénéficiant pas de décision d'adéquation font l'objet de toute l'attention des autorités de protection des données personnelles. Ces transferts ne sont pourtant pas frappés d'une interdiction générale et absolue mais restent possibles au cas par cas, après adoption de garanties telles que la signature des clauses contractuelles types (notamment leur dernière version qui prend en compte la jurisprudence Schrems II) et conduite d'une analyse de la capacité du pays destinataire à protéger les droits des personnes concernées. Aussi, l'exclusion de principe par le référentiel de toute possibilité de reposer sur les clauses types ou les règles contraignantes d'entreprise peut paraître surprenante.
S'il est également tentant d'arguer que les Etats membres sont susceptibles d'adopter des règles plus contraignantes en matière de données de santé, comme le permet l'article 9 (4) du RGPD, l'adoption de ces règles demeure de la compétence du législateur.

Le fait que le référentiel n'indique pas si cette obligation découlerait d'une nouvelle interprétation de l'article L. 1111-8 du code de la santé publique ou bien des dispositions du RGPD à la lumière de la décision Schrems II, aussi il n'est pas possible de déterminer si le référentiel risquerait d'être entaché d'un défaut de base légale ou d'erreur commise dans l'interprétation de la règle applicable, au sens du droit administratif.

Quoiqu'il en soit, compte tenu de l'ampleur de l'impact qu'une telle obligation de localisation implique au niveau national et international, il serait utile que le référentiel ou sa FAQ apportent des éléments explicitant la base légale de cette obligation. Ceci d'autant plus qu'en ce moment-même, au niveau européen, les « *critères d'immunité* » retenus dans le cadre du système européen de certification du cloud EUCS[9] (), notamment « *l'admissibilité à la certification limitée uniquement aux fournisseurs de services en nuage dont le siège social est situé dans l'UE, l'exclusion des fournisseurs entièrement ou partiellement détenus par une entité dont le siège social est situé en dehors de l'UE, l'interdiction de stocker et de traiter les données en dehors de l'UE, en dehors de l'UE, l'interdiction de stocker et de traiter des données en dehors de l'UE, et les capacités d'assistance à la clientèle limitées aux employés situés dans l'UE* » font l'objet de sévères critiques de la part de nombreux représentants de clouds étrangers[10], non seulement sur le fondement juridique (compatibilité avec les accords de l'Organisation mondiale du commerce ou les règles de la commande publique au niveau de l'UE) mais également sur l'impact que ces restrictions pourraient avoir sur l'offre de cloud en Europe.

Les incertitudes quant au contenu impératif du contrat

La certification HDS impose d'insérer certaines clauses obligatoires au sein des contrats des parties prenantes. Le nouveau projet de référentiel présente l'avantage de lister clairement les clauses imposées par le décret. Certaines exigences additionnelles du référentiel semblent cependant potentiellement impacter le contrat, sans qu'il ne soit précisé si une clause doit obligatoirement être prévue – par exemple,

les obligations de prise en compte par l'hébergeur des impératifs de communication des incidents de sécurité s'appliquant aux utilisateurs et la fourniture de moyens pour y satisfaire, de communication au client (et au responsable de traitement) d'informations sur les lois « *extra-communautaires* » (sic) auxquelles l'hébergeur est soumis, les mesures d'atténuation du risque et les risques résiduels (i.e. le « *transfer impact assessment* » requis par Schrems II), et le maintien d'une liste des points de contact pour chacun des clients (exigences n°9, 10 et 11).

Ceci est tout particulièrement problématique pour l'obligation de « *représentation des garanties* », à laquelle les contrats doivent se conformer (exigence 1) sans être pourtant citée dans la liste des clauses obligatoires. De plus, le fondement juridique de cette obligation n'est pas clairement indiqué, bien qu'il s'agisse d'une extension inédite de l'obligation de prévoir dans le contrat « *une information sur les garanties et les procédures mises en place par l'hébergeur permettant de couvrir toute défaillance éventuelle de sa part* »[11]. L'aspect surprenant est surtout dans l'exigence de remplir une matrice comprenant des niveaux d'engagements sur la « *conformité* » des différents acteurs[12]. Or, cette matrice apparaît difficilement intégrable au contrat ou à la documentation hébergeur, dès lors qu'il semble peu probable que ce dernier indique dans son contrat client que l'un de ses sous-traitants est classé « *non conforme* ». Enfin, cette matrice crée une correspondance avec le très exigeant référentiel SecNumCloud et impose aux hébergeurs HDS de s'autoclasser dans un niveau de conformité inférieur s'ils n'en disposent pas, alors que cette certification n'est que facultative, ce qui risque, là encore, de faire débat.

Le projet de référentiel fera l'objet de la procédure de notification 2015/1535, qui permet à la Commission et aux États membres d'examiner les règlements techniques que les États membres entendent adopter concernant les services de la société de l'information avant leur adoption. Ceci devrait permettre de répondre à certaines des interrogations que ce projet soulève. Des clarifications apparaissent en effet cruciales pour mettre un terme aux débats sur le périmètre et le contenu des exigences HDS, qui nuisent à sa bonne compréhension par les acteurs et à la capacité pour les autorités d'en contrôler l'application.

Lorraine MAISNIER-BOCHÉ

Avocat à la cour
McDermott, Will & Emery

Notes

(1) ANS, Référentiel HDS – Exigences, V1.1.20221027

(2) Contribution du LEEM, 8 déc. 2022

(3) Contribution du LEEM, préc., sur l'inapplicabilité aux entreprises du médicament

(4) Explicitation du champ d'application du cadre juridique de l'hébergement de données de santé par le ministère chargé de la Santé, représenté par la Délégation à la stratégie des systèmes d'information de santé, 16 mai 2019

(5) Cnil, délib. n° 2019-057 du 9 mai 2019 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel mis en œuvre à des fins de gestion des vigilances sanitaires, art. 10

(6) Contribution de Claranet - Pictime Coreye, 6 déc. 2022

(7) CE, 19 juin 2020, n° 434684

(8) CJUE, C-329/16, 7 déc. 2017, CE, 12 juill. 2018, n°387156

(9) European Cybersecurity Certification Scheme for Cloud Services (EUCS), préparé par l'Agence européenne de cybersécurité (Enisa)

(10) CCIA, Joint Industry Statement on the Draft European Cybersecurity Certification Scheme for Cloud Services (EUCS), 1er déc. 2022 ; Contexte Numérique, Nouvelle offensive étrangère contre la certification du cloud à l'européenne, 2 déc. 2022

(11) Art. R.1111-11, 10° du code de la santé publique

(12) Contribution du LNE, 8 déc. 2022

Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld sr@expertises.info

RGPD

Le sous-traitant seul responsable de la sécurité du traitement

En sanctionnant un sous-traitant, la Cnil consacre une obligation de résultat du sous-traitant à disposer d'un niveau de sécurité minimale conforme au RGPD. La délibération du 15 avril 2022[1] de la Cnil tient compte du non-respect d'instructions et de l'absence d'encadrement du traitement des données. Cette sanction qui concerne exclusivement le sous-traitant peut néanmoins sembler sévère.

Les faits remontent au 4 novembre 2020 lorsque l'Agence nationale de la sécurité des systèmes d'information (Anssi) observe et informe un laboratoire médical que les données de ses patients sont mises en vente sur le darknet[2]. Trois mois et demi plus tard, le 23 février 2021, une fuite de données massive est révélée dans la presse[3]. Elle concerne les nom, prénom, numéro de sécurité sociale, nom du médecin prescripteur, date d'examen et surtout données de santé de 500 000 personnes. Ces données semblent liées à la fuite identifiée par l'Anssi. Elles étaient sous la responsabilité de deux laboratoires qui bénéficiaient des services d'un logiciel de gestion de laboratoire. L'éditeur tiers, sous-traitant en l'espèce, ne disposait pas de façon générale des données car le logiciel concédé à ces laboratoires n'est pas accessible à distance, mais installé sur leur serveur. Ils avaient néanmoins demandé à l'éditeur de réaliser une migration de données.

Au cours de cette opération, qui imposait d'extraire les données des serveurs du laboratoire et de les importer dans un serveur FTP, une fuite de données avait eu lieu.

Dès le 24 février 2021 et jusqu'au 4 mars 2021 la Commission nationale de l'informatique et des libertés (Cnil) a contrôlé le site internet sur lequel figuraient les données, a examiné la situation et a demandé, en référé d'heure à heure, des mesures adaptées et efficaces pour surveiller et bloquer le service de communication au public en ligne aux FAI. Entre le 6 octobre 2021 et le 15 avril 2022 des échanges ont eu lieu entre le sous-traitant et le rapporteur de la Cnil. Cette dernière a délibéré en formation restreinte le 15 avril 2022.

La Cnil a alors sanctionné à hauteur de 1,5 million d'euros le sous-traitant, essentiellement pour avoir manqué à ses obligations propres de sécurité. Elle consacre en cela une obligation de résultat du sous-traitant à disposer d'un niveau de sécurité minimale conforme au Règlement général sur la protection des données (RGPD[4]).
Ce manquement est en l'espèce sanctionné en tenant compte de deux causes d'aggravation : non-respect d'instructions et absence d'encadrement. Cette sanction qui concerne, exclusivement[5] le sous-traitant peut néanmoins sembler sévère.

La consécration d'une obligation de résultat de conformité de sécurité de la fonction de sous-traitant indépendamment de sa relation avec le responsable du traitement

Un prestataire doit, sur la base d'une obligation de résultat, dès lors qu'il traite des données à caractère personnel pour le compte d'autrui, être conforme au niveau de sécurité exigé par la Cnil et l'Anssi. Cette délibération illustre la mise en œuvre de cette obligation dans le cadre spécial de la migration de données.

L'obligation de résultat de conformité de sécurité du sous-traitant

La fonction essentielle propre du sous-traitant implique qu'il sécurise les données sur la base d'une obligation de résultat.

La sous-traitance de données personnelles : une fonction essentielle protectrice des données

Le sous-traitant a un rôle propre dans le RGPD. Il est indéniable que l'esprit du RGPD était de donner plus de responsabilité aux sous-traitants. Alors que sous l'égide de la directive de 1995[6] le sous-traitant bénéficiait d'une certaine immunité, le sous-traitant avec le RGPD

doit endosser une responsabilité autonome[7]. Des obligations propres lui sont attachées[8] : gestion des habilitations et de la confidentialité interne (art 28, 3), registre des activités de traitement (art. 30§2), désigner un DPO dans certaines circonstances (art. 37), informer sur la violation (art. 33 §2), respecter les règles de transfert de données (chapitre V), obligation d'assistance du RT (art. 28 3) f), l'intégration des obligations du sous-traitant dans les codes de conduite et obligation de mettre en place des mesures organisationnelles et techniques pour sécuriser les traitements de données (art. 32). Ces obligations peuvent désormais faire l'objet de sanctions du sous-traitant[9].

Cette responsabilité propre s'explique par le besoin de protéger effectivement les données personnelles. Quand bien même de telles obligations propres aux sous-traitants existent, rien ne semble contraindre la Cnil à condamner systématiquement le sous-traitant dans ces cas précis. Pour le RGPD le responsable du traitement porte nécessairement également une responsabilité. Il doit garantir la sécurité des données et être en mesure de le démontrer[10]. Le Comité européen de la protection des données (CEPD), qui veille à l'application du Règlement dans tous les pays membres de l'UE et publie des lignes directrices pour élaborer une doctrine commune de protection, confirme que selon le RGPD, c'est le responsable du traitement qui est responsable de la conformité à la sécurité[11].

Cette prééminence du responsable du traitement est d'ailleurs renforcée par la référence que fait le CEPD dans ses lignes directrices liées au rôle des acteurs du RGPD, à l'avis du Groupe de travail de l'article 29 sur la protection des données du 13 juillet 2010[12] et qui met en avant le principe de responsabilité du responsable du traitement[13].

Ajoutons que pour le CEPD, le responsable du traitement doit donner au sous-traitant une description des activités de traitement et des objectifs de sécurité (fondée sur l'évaluation des risques réalisée par le responsable du traitement) et approuver les mesures proposées par le sous-traitant.

C'est le responsable du traitement qui exerce son pouvoir de décision sur les caractéristiques principales des mesures de sécurité, que ce soit en dressant une liste précise des mesures ou en approuvant celles proposées par le sous-traitant[14]. Ainsi à en lire ces lignes directrices nous pourrions penser que le responsable du traitement conservait une part de responsabilité de la sécurité même si le sous-traitant la mettait en œuvre. C'était certainement sans compter l'objectif majeur du texte : offrir aux personnes physiques de tous les États membres un même niveau de responsabilité pour les responsables du traitement et les sous-traitants[15].

À ce titre, l'Autorité de protection doit se saisir et sanctionner les cas où des données ont été atteintes. Les données personnelles seraient même de véritables émanations de la personne qui participent à son rayonnement[16]. C'est ainsi que dans le cas d'une atteinte importante, comme en l'espèce, il convient de pouvoir punir ceux qui ont violé les règles de conformité. Le texte impose donc à la Cnil d'analyser le rôle réel joué[17] par les acteurs. L'analyse du niveau de contrôle de l'exécution des prestations est notamment un élément pris en considération devant permettre de déterminer la responsabilité des acteurs[18]. Il arrive en effet qu'il soit impossible en pratique pour certains responsables de traitement de réaliser les contrôles pertinents, parce qu'ils ne disposent pas toujours de l'expertise technique nécessaire[19]. La responsabilité propre du sous-traitant en pratique peut ainsi s'expliquer par les difficultés de contrôle et d'audit que peuvent avoir les laboratoires sur l'éditeur. Et également par l'incompétence technique supposée des laboratoires en matière de migration de données. Ce rôle implique donc, comme le délibère la formation restreinte dans l'affaire commentée, une conformité à la sécurité dont seul le sous-traitant peut prendre la responsabilité.

Proposer des services de sous-traitance de données personnelles implique une conformité à la sécurité

Tout en tenant compte de cet élément, la Cnil aurait pu explicitement distinguer entre la violation de données effective qui serait sous la responsabilité du sous-traitant et le défaut de sécurité. Ce moyen de défense soulevé par le sous-traitant consiste à dire qu'en l'absence de lien de causalité entre la violation et le défaut de sécurité identifié, le sous-traitant ne peut être responsable[20]. Dans le cas d'un sous-traitant, nous y reviendrons, l'argument aurait pu convaincre, puisque dans son contrat de service de migration informatique, indépendamment du RGPD, le sous-traitant s'engage a minima sur la base d'une obligation de moyens, à éviter les fuites de données. Il aurait donc pu paraître légitime à la Cnil de tenir compte de cet argument juridique, qui permet de définir le rôle concret des parties, pour valider l'argument.

Or, la Cnil exige la mise en conformité de sécurité indépendamment de la violation de données[21]. Plusieurs délibérations ont déjà précisé ce point, mais pour le responsable du traitement, jamais encore pour un sous-traitant. En effet, la Cnil a déjà considéré qu'il appartenait à la formation restreinte de vérifier que le responsable de traitement [...] a mis en œuvre, en application de cet article, des mesures techniques et organisationnelles appropriées pour prévenir les risques de violations et de mésusage de ces données[22]. Elle a également constaté que l'absence de dommage avéré pour les personnes concernées n'a pas d'incidence sur l'existence du défaut de sécurité, qui constitue le manquement à l'article 32 du RGPD[23]. Et rappelé avoir adopté des sanctions pécuniaires où la caractérisation d'un manquement à l'article 32 du RGPD était le résultat de mesures insuffisantes pour garantir la sécurité des données traitées, et non pas seulement le résultat de l'existence d'une violation de données à caractère personnel[24]. Mais ces délibérations concernent les responsables du traitement.

Dans la délibération commentée, la Cnil consacre cette mise en conformité en obligation de résultat de sécurité, pour le sous-traitant. L'autorité de contrôle confirme désormais qu'un sous-traitant peut également faire l'objet d'une sanction exclusive[25] pour défaut de sécurité. L'approche concrète qu'il convient d'adopter face à la protection des données implique de s'intéresser à la mise en œuvre de cette obligation de résultat auquel est soumis le sous-traitant. Cette délibération l'illustre pour le cas d'une migration de données.

La mise en œuvre de l'obligation de résultat dans le cadre d'une migration de données de santé

L'obligation de résultat de sécurité du sous-traitant nécessite qu'il mette en place des mesures techniques et organisationnelles précises. La Cnil détaille dans cette délibération pour les prestations de migrations de données, les mesures génériques et spécifiques renforcées au données sensibles traitées par le sous-traitant.

Les mesures techniques et organisationnelles de sécurité en cas de migration de données

L'obligation de résultat passe par la mise en œuvre de mesures de sécurité rapides en cas de détection et élémentaire. La Cnil explique quelle est l'étendue de cette obligation de résultat de sécurité. Il est certain que ce que réclame la Cnil ne consiste pas en des actions complexes, mais plutôt des actions « *élémentaires* ». Elle a déjà eu l'occasion de rappeler conformément au RGPD, que les mesures de sécurité doivent être proportionnées, raisonnables, concernant des risques prévisibles, pas nécessairement couteuses et faciles à mettre en œuvre[26]. Ces mesures, « *élémentaires* » figurent dans les guides de la Cnil[27] et également de l'Anssi[28] que l'autorité de protection cite régulièrement[29]. En l'espèce la Cnil a appliqué ces critères, puisque les défauts sont liés à trois mesures[30] à mettre en oeuvre qui auraient permis d'éviter les défaillances :

- des mesures de sécurité technique élémentaires : chiffrer les données afin d'éviter leur transmission en clair[31] ; effacer automatiquement des données après migration vers un autre logiciel ; éviter que la zone publique du serveur soit accessible librement sans authentification depuis internet ; et éviter que le compte utilisateur d'accès à la zone privée soit partagé entre plusieurs salariés ;
- des mesures organisationnelles tenant à la réalisation d'une procédure de supervision et de remontée d'alerte de sécurité ;
- dès lors qu'une alerte a été lancée par un salarié en interne vérifier l'étendue de la faille de sécurité et non seulement mettre en œuvre des actions correctives et préventives sur la faille identifiée.

La Cnil rappelle également, ce qui nécessite uniquement d'y consacrer un peu de temps, l'importance de réfléchir à la sécurité des données en amont des traitements, dès la conception[32]. La Cnil ne fait néanmoins pas référence dans cette délibération, contrairement à d'autres, au principe de protection dès la conception de l'article 25 du RGPD[33]. Dans cette délibération, la Cnil demande au sous-traitant de réfléchir en amont à la sécurité des données[34], plutôt qu'à la manière d'appréhender les traitements.

L'obligation de résultat implique que les défauts des mesures techniques soient contournés par des mesures organisationnelles. La Cnil doit tenir compte des mesures raisonnables qui peuvent être prises par le sous-traitant dans son contexte précis de traitement. Ainsi, en l'espèce le sous-traitant arguait du fait que le logiciel était obsolète de sorte qu'elle était contrainte de réaliser une extraction globale sans faire le choix entre les données. Selon une logique d'économie des coûts, cet argument aurait pu être porteur. La Cnil n'admet cependant pas ce type d'argument. Elle estime, classiquement, qu'une mesure organisationnelle peut pallier l'inconformité d'une mesure technique. Ainsi, elle énonce explicitement que le sous-traitant aurait pu supprimer, après extraction, toutes les données qui n'auraient pas dû être extraites. Ce type de mesure palliative a déjà été rappelé dans d'autres délibérations. Dans la délibération RATP du 29 octobre 2021, la Cnil rappelle par exemple que si un logiciel ne permet pas de mettre en place des cloisonnements entre personnes, les moyens organisationnels tels que (i) l'information des utilisateurs du système d'information sur les données qu'ils sont autorisés à traiter pour leurs missions, et (ii) le contrôle de l'usage qui en est fait, notamment au moyen de journaux de connexion, et enfin (iii) en sanctionnant disciplinairement le non-respect des règles applicables, peuvent être utilisés[35]. Dans le même sens, des mesures juridiques peuvent être mises en œuvre dans certains cas, notamment lorsque les clients ne veulent pas migrer vers un logiciel conforme au RGPD. Une mise en demeure de migrer dans les meilleurs délais vers la dernière version est pertinente[36]. Là encore l'obligation de résultat pour le sous-traitant se vérifie. Il convient donc d'être rigoureux dans la mise en œuvre des mesures techniques et organisationnelles de sécurité, faciles à mettre en œuvre.

L'obligation de résultat de sécurité implique un renforcement de la sécurité en matière de données sensibles migrées

La Cnil évoque le concept de données très sensibles. La rigueur de la présente délibération est également explicable, car la faille de sécurité concerne des données de santé et génétiques. L'article 9 du RGPD dispose que ces données personnelles sont des données dites particulières (ou sensibles selon la terminologie applicable). Ces données ne peuvent pas faire l'objet d'un traitement sauf par exception lorsque la personne concernée y a consenti (par exemple). La base extraite par le sous-traitant contenait des zones de commentaires libres avec des informations sur les pathologies des patients (VIH, cancers, maladies génétiques, tuberculose osseuse, diabète) leur état de grossesse, leurs traitements médicamenteux (Xarelto) ou encore des données génétiques. En l'espèce, le sous-traitant semble autorisé à traiter ces données, du moins ce n'est pas ce qui a inquiété la Cnil[37] (nous regrettons néanmoins que la Cnil ne se soit pas positionnée sur la proportionnalité des données stockées[38]). Le point fondamental pour l'autorité de contrôle est de traiter ces données sensibles avec plus de précaution que les autres données. La Cnil utilise une notion qui ne figure pas dans les textes : il s'agit pour elle de données « *très sensibles* ».

On voit dans ces termes l'importance que revêtent ces données pour la Cnil. Le sens de cet adverbe n'apparaît pas clairement dans la délibération. Il semblerait que l'autorité de protection française détermine des degrés entre les différentes données sensibles, certaines seraient plus sensibles que d'autres : est-ce la justification complémentaire d'une sanction exclusive du sous-traitant ? Qu'elles soient très sensibles, ou simplement sensibles, la Cnil montre une fois de plus sa volonté de voir les acteurs des traitements de données

personnelles agir avec la plus grande précaution sur ces données.
Une protection renforcée qui implique un plan de migration. La protection de ces données sensibles devant être renforcée, la Cnil indique qu'il aurait été nécessaire, spécifiquement parce qu'il s'agit de données très sensibles, de mettre en place des procédures spécifiques permettant de décrire étape par étape l'enchaînement des tâches à réaliser, les rôles et les responsabilités associées. Une telle mesure organisationnelle apparaît très utile, même en présence de données non sensibles, afin de garantir aux données la protection la plus adaptée.
Ainsi, cette délibération met en avant l'obligation de résultat de sécurité du sous-traitant dans le traitement de données à caractère personnel. Seul à contrôler certaines opérations, il apparaît pour la Cnil le premier et seul responsable. Il doit s'obliger à mettre en œuvre de nombreuses mesures techniques et organisationnelles faciles d'accès, mais indispensables pour assurer la plus haute protection aux données des personnes concernées. Le fait de traiter des données sensibles implique d'autant plus de précautions. Le non-respect de cette obligation de résultat soumet le sous-traitant à une sanction.

La sanction du non-respect de l'obligation de résultat de conformité de sécurité du sous-traitant indépendamment du responsable de traitement

Les défauts de sécurité ne sont pas les seules obligations examinées par la Cnil, deux inconformités – le défaut d'encadrement et le dépassement d'instruction - aggravent[39] le risque de violation de sécurité et partant la sanction appliquée. Cette sanction pose la question de la possibilité qu'a le sous-traitant d'échapper, au moins en partie, à la sanction,en se retournant vers le responsable du traitement.

Le degré de respect des instructions et le niveau d'encadrement : deux critères pris en compte par la Cnil pour aggraver la sanction

La Cnil considère que la mise en conformité du cadre contractuel standard du sous-traitant est une condition d'aggravation de la sanction, de même que le non-respect de l'instruction du responsable.

L'absence de mise en conformité du cadre contractuel standard du sous-traitant est une condition d'aggravation de la sanction

L'encadrement contractuel : une obligation de conformité du sous-traitant aussi bien que du responsable de traitement. L'article 28 §3 du RGPD organise l'encadrement des relations entre sous-traitant et responsable du traitement. L'article 28 §3 ne dénomme toutefois pas l'acteur responsable de cette obligation. De son côté, le CEPD a déjà eu l'occasion d'expliquer que cet article s'appliquait au sous-traitant. Le CEPD l'illustrait néanmoins par un exemple particulier lorsque le sous-traitant est le seul couvert par le champ d'application territorial du RGPD[40]. Ce qui laissait entendre que le responsable du traitement était seul contraint par cet encadrement, sauf les cas où le sous-traitant était le seul acteur à traiter des données sur le sol européen[41].
Pour sa part, la Cnil semble étendre dans la délibération commentée le champ d'application de l'article 28§3. La formation restreinte note que cet article incombe tant au responsable de traitement qu'au sous-traitant, ce qui est sans incidence sur l'existence d'une responsabilité propre du sous-traitant. Elle ajoute que c'est le sous-traitant lui-même qui transmet aux laboratoires ses propres conditions générales de vente qui font office d'encadrement contractuel au titre du RGPD et qu'ils ne contiennent pas les mentions conformes à l'article 28§3 du RGPD. Il est donc possible d'interpréter qu'elle impose ainsi au sous-traitant, en l'absence de négociation, autant de responsabilité qu'au responsable du traitement pour encadrer leur relation[42]. En allant plus loin dans le raisonnement, le degré de responsabilité du sous-traitant pourrait dépendre de la capacité de négociation du responsable de traitement. Ce qui peut sembler logique dans certains cas : par exemple, quel est le pouvoir de contrôle d'un responsable de traitement face à des géants tels que AWS ou Microsoft ? Seulement, selon le CEPD, « *le déséquilibre entre le pouvoir contractuel d'un petit responsable du traitement et celui de grands prestataires de services ne devrait pas être considéré comme une justification permettant au responsable du traitement d'accepter des clauses et des conditions contractuelles non conformes à la législation en matière de protection des données, pas plus qu'il n'exonère le responsable du traitement de ses obligations en la matière. Le responsable du traitement doit examiner les conditions et, dans la mesure où il les accepte librement et utilise le service, il assume également l'entière responsabilité du respect du RGPD*[43] ». Il nous semble donc que ce que la Cnil sanctionne, dans sa logique qui tend à obtenir un résultat de sécurité, n'est pas directement le manquement à l'obligation que le sous-traitant à encadrer ses relations avec le responsable du traitement, mais plutôt le défaut pour le sous-traitant de disposer de documentation conforme au RGPD. Ayant connaissance du fait que son service impliquera nécessairement le traitement de données personnelles, le sous-traitant doit disposer de conditions générales de service conformes au RGPD. À noter qu'en défense le sous-traitant n'a pas contesté la matérialité du manquement et accepté l'idée que la conclusion d'un contrat de sous-traitance constituait une obligation lui étant imposée[44]. Une clarification de la position de la Cnil aurait pu naître de l'argument contraire.
L'encadrement des relations contractuelles vise à réguler les comportements concrets. La Cnil s'attache à cet encadrement contractuel comme à un élément qui aurait pu permettre d'éviter les non-conformités. Il est désormais clair que l'accord de traitement ne doit pas simplement reproduire les dispositions du RGPD : il doit inclure des informations plus spécifiques et concrètes sur la manière dont les conditions seront remplies et sur le niveau de sécurité requis pour le traitement de données à caractère personnel qui fait l'objet dudit accord[45]. C'est pourquoi, la Cnil répète dans cette délibération, comme dans d'autres d'ailleurs, que l'absence d'encadrement contractuel accentue le fait que les données à caractère personnel n'aient pas bénéficié de la protection offerte par le RGPD[46]. En effet, le contrat doit permettre de définir des mesures techniques et

organisationnelles concrètes pour protéger les données. Sa négociation est donc un moyen d'assurer aux données une protection concrète et effective. C'est en cela que l'absence d'encadrement du traitement des données est fondamentale dans cette affaire. La Cnil en conclut que cela aggrave le risque et donc la sanction.

Le non-respect de l'instruction du responsable du traitement peut être une condition d'aggravation de la sanction plus qu'une condition de requalification du statut de sous-traitant en responsable de traitement

Dépasser une instruction implique en principe de changer de rôle. La Cnil se concentre également sur le dépassement, par le sous-traitant, des instructions du responsable du traitement. Dans cette affaire le sous-traitant avait extrait des données supplémentaires par rapport à ce qui avait été demandé par le responsable du traitement. Or, l'article 29 du RGPD oblige le sous-traitant à traiter les données conformément aux instructions du responsable de traitement. La lecture littérale de ce texte croisée à celle de l'article 28§10 qui énonce que le sous-traitant détermine les moyens du traitement ainsi que celles des lignes directrices du CEPD[47] pouvait permettre de conclure que dans le cas d'espèce, le sous-traitant aurait dû être proclamé responsable du traitement si ce n'est unique a minima conjoint avec les laboratoires[48].

Cette position n'est pas celle de la Cnil. Il aurait en effet été difficile de faire peser sur le sous-traitant en l'espèce l'ensemble des obligations du responsable du traitement pour les seules prestations de migration. La Cnil souligne que le sous-traitant agit de manière générale, uniquement sur instruction des laboratoires. Il semble donc que la Cnil exonère le sous-traitant d'une conversion au rôle de responsable du traitement en raison du fait qu'il n'avait agi ainsi qu'exceptionnellement. Ajoutons que l'usage que fait le sous-traitant des données nous paraît être fondamental dans ce cadre[49]. En l'espèce, si le sous-traitant a outrepassé les instructions du responsable du traitement, ce n'est pas pour traiter les données pour ses propres besoins, mais pour s'éviter l'effort de modifier ses processus.

Il convient de bien comprendre ici que la Cnil ne veut pas dire que le sous-traitant ne doit avoir aucune autonomie dans la réalisation de son traitement. Une certaine marge d'appréciation quant à la manière de servir au mieux les intérêts du responsable du traitement doit être laissée au sous-traitant. Cependant cette marge de manœuvre ne doit pas concerner les moyens essentiels du traitement au sens du CEPD[50], c'est-à-dire ceux qui sont étroitement liés à la finalité et à la portée du traitement, tels que le type de données, la durée du traitement, les catégories de destinataire et de personnes concernées[51]. En l'espèce ce sont les données choisies par le responsable du traitement qui ont été modifiées unilatéralement, par le sous-traitant. C'est pourquoi, la Cnil a considéré qu'il y avait eu dépassement des instructions en question.

Une autre observation sur la preuve fournie. La Cnil critique l'absence de force probante des tickets SAV produits par le sous-traitant pour montrer que le responsable du traitement avait accepté ce changement d'instruction. Ces tickets contiennent la confirmation que le sous-traitant a réalisé l'extraction demandée. La Cnil rejette ces tickets en estimant qu'ils n'ont pas de valeur probante, car ils ne peuvent être considérés comme des instructions de réalisation des opérations d'extraction. Cette position peut paraître surprenante car rien ne semble s'opposer à ce que des tickets SAV soient considérés comme une acceptation des opérations réalisées par le sous-traitant. En l'absence de contestation de l'opération il convient de considérer soit que le responsable du traitement a implicitement accepté l'opération soit que son silence montre une forme de désintéressement à l'opération. Cela n'aurait pas été une preuve d'instruction, mais cela aurait pu être considéré comme une preuve d'accord de l'extraction ce qui revient à donner une instruction rétroactive. Cependant, là encore, pour la Cnil une responsabilité exclusive repose sur le sous-traitant, notamment en matière de migration de données où les opérations se déroulent en général dans le cadre d'une réversibilité entre deux prestataires et pour lesquelles, le client ne s'implique pas nécessairement.

Une sanction contre laquelle le sous-traitant semble démuni

La Cnil sanctionne fortement le sous-traitant dans cette décision, ce qui peut paraître sévère.

La sanction du sous-traitant en l'espèce : 1,5 million d'euros

La formation restreinte a qualifié les actes du sous-traitant de négligents. Et dans le cadre de son pouvoir de sanction a condamné le sous-traitant à 1,5 million d'euros conformément à l'article 83§4 du RGPD qui fixe la limite de la sanction pour violation aux articles 28, 29 et 32 du RGPD à 10 millions d'euros ou 2% du chiffre d'affaires annuel mondial total de l'exercice précédent.

L'impossibilité du sous-traitant de se retourner contre le responsable du traitement

Eu égard à ces constats, la question peut se poser de savoir si le sous-traitant peut se retourner juridiquement contre le responsable du traitement. À première vue, il ne semble pas pouvoir échapper à une telle amende de la Cnil (à moins d'interjeter appel devant le Conseil d'État bien sûr). L'amende administrative est soumise au principe de responsabilité personnelle et à son corollaire le principe de personnalité des peines[52] qui a valeur de principe général du droit[53] à valeur constitutionnelle[54]. L'amende ne semble donc pas pouvoir faire l'objet d'une action récursoire totale[55]. Cependant, d'un point de vue pratique la sanction exclusive du sous-traitant est difficile à comprendre. Le prestataire dans le cadre d'un service qu'il rend à son client est condamné à hauteur de 1,5 million d'euros, montant supérieur en l'espèce au résultat net de cette entreprise en 2020, alors même que le client semble s'être désintéressé des questions de sécurité[56] et avoir choisi de collecter des données de santé qui n'étaient pas nécessairement indispensables[57].
De fait, le responsable du traitement ne doit pas laisser son sous-traitant seul responsable de la sécurité des traitements et doit se sentir impliqué.

L'effet néfaste d'une telle délibération sur la responsabilisation des responsables du traitement peut être important. Rechercher comment obtenir la prise en charge d'une partie de l'amende par le responsable

de traitement, serait un premier pas utile à la protection des données. Il conviendrait en premier lieu de qualifier l'amende de préjudice réparable, indemnisable. Une telle solution concernant une amende a déjà été adoptée en matière de douanes. La cour d'appel de Paris a constaté que les peines contraventionnelles prononcées envers une société par l'administration des douanes en raison des fautes commises par son commissionnaire en douane avaient un caractère indemnitaire. Cette qualification n'excluait donc pas, selon la cour d'appel que le commissionnaire en douane soit tenu à réparation en raison desdites condamnations pour les fautes commises par elle[58] .

La responsabilité était partagée entre la société et son commissionnaire en douane. Par analogie, l'action en responsabilité contractuelle du sous-traitant à l'égard du responsable du traitement pourrait en théorie être admise devant une juridiction judiciaire pour obtenir réparation d'un pourcentage de l'amende versée suite à la condamnation par la Cnil. D'autant qu'à notre connaissance une délibération a déjà sanctionné aux torts partagés un sous-traitant et un responsable du traitement. Le responsable de traitement et son sous-traitant n'avaient pas pris de mesures satisfaisantes pour faire face à des attaques par bourrage d'identifiants (credential stuffing) sur le site web du responsable de traitement. La formation restreinte avait alors prononcé deux amendes distinctes – 150 000 € à l'encontre du responsable de traitement et 75 000 € à l'encontre du sous-traitant – au regard de leurs responsabilités respectives. Elle a souligné que le responsable de traitement devait décider de la mise en place de mesures et donner des instructions documentées à son sous-traitant. Mais que le sous-traitant devait aussi rechercher les solutions techniques et organisationnelles les plus appropriées pour assurer la sécurité des données personnelles, et les proposer au responsable de traitement[59]. Cette délibération mettait donc en avant la possibilité d'une responsabilité aux torts partagés des deux acteurs.

Deux obstacles majeurs doivent néanmoins être soulignés. Le premier concerne la qualification du contrat de sous-traitance.

En effet, dans l'arrêt d'appel cité relatif au droit des douanes, la situation se distingue de celle d'un sous-traitant vis-à-vis d'un responsable du traitement, car le commissionnaire en douane est mandataire de son client. Il est donc chargé d'exécuter pour son compte des actes juridiques[60], les formalités douanières.

La qualification du contrat de sous-traitance pourrait revêtir cette qualification, mais uniquement pour les actes juridiques que le sous-traitant est potentiellement amené à faire pour le compte du responsable de traitement[61].

En revanche, pour les actes techniques le contrat de sous-traitance est plutôt un contrat d'entreprise[62] défini à l'article 1710 du C.civ[63].

Dans ce cadre, il est alors difficile d'engager la responsabilité du responsable du traitement pour des prestations qui contractuellement devaient être réalisées par le sous-traitant. Le deuxième obstacle, lié au premier, concerne la démonstration des fautes propres du responsable du traitement.

Dans la présente délibération, la Cnil rappelle par exemple que l'amende qu'elle inflige au sous-traitant est liée à sa responsabilité propre[64], ce qui pourrait signifier que l'amende infligée concerne spécifiquement le responsable du traitement.

Cette position n'engage cependant que la Cnil. Dans le même sens le sous-traitant pourrait, peut-être défendre le fait que les négligences du responsable ont laissé perdurer des défauts de sécurité qu'il aurait dû éviter.

À suivre…

Sylvain JOYEUX
Avocat associé
Daniel KORABELNIKOV
Avocat
Cloix, Mendès, Gil

Notes

(1) Nous ne citons volontairement pas le nom de la société sanctionnée, ni celle des sociétés défenderesses dans les délibérations auxquelles cet article fait référence. La Cnil a rendu publiques les délibérations en limitant à deux années l'apparition de la dénomination des sociétés en cause.

(2) Sous partie d'internet définie par la Cnil comme pourvue de fonction d'anonymisation et dans lequel toutes les ressources ne sont pas nécessairement indexées par les moteurs de recherche.

(3) Leboucq F., et ali, « Les informations confidentielles de 500 000 patients français dérobées à des laboratoires et diffusées en ligne », Libération, 23 fév. 2021, site : https://www.liberation.fr/checknews/les-informations-confidentielles-de-500-000-patients-francais-derobees-a-des-laboratoires-medicaux-et-diffusees-en-ligne-20210223_VO6W6J6IUVATZD4VOVNDLTDZBU/.

(4) Régl. (UE) n°2016/679 de la Commission, 27 avr. 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

(5) Nous n'irons pas jusque dire que cette décision est « un tournant dans la jurisprudence de l'autorité de protection » (Ivanier F., « Logiciels et Privacy by design : enjeux et mise en œuvre », Expertises n°484, nov. 2022, p. 374). Mais c'est une décision à laquelle il convient selon nous de prêter une très grande attention du fait de sa portée.

(6) Dir. n°95/46/CE du 24 oct. 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, modifiée.

(7) Banck A., « GDPR et Sous-traitance : un nouveau devoir de conseil ? », Dalloz IP/IT, janv. 2017, p. 36.

(8) CEPD, lignes directrices concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, fév. 2022 (dernière date de modification), §93, p. 35.

(9) Régl. (UE) n°2016/679, art. 83. Ce qui n'était pas le cas avant : Banck A., op. cit., p. 37.

(10) Régl. (UE), n°2016/679, art. 5 §2.

(11) CEPD, lignes directrices concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, fév. 2022 (dernière date de modification), p. 8 §2.

(12) Cet avis est donc antérieur au RGPD, mais le CEPD le considère toujours d'actualité.

(13) CEPD, lignes directrices cit., fév 2022, p. 9, note n°3. À noter que la seule mention du sous-traitant à l'époque de cet avis consistait à mener une réflexion sur la possibilité de donner ne serait-ce qu'un peu de responsabilité au sous-traitant (« Une réflexion quant à la nécessité d'imposer certaines obligations aux sous-traitants de données […] pourrait également être menée à la lumière de ce principe de responsabilité » Avis 3/2010 du groupe de travail «Article 29» sur le principe de responsabilité, adopté le 13 juillet 2010, 00062/10/FR, WP 173, p. 14, §46). Ce qui n'est plus le cas aujourd'hui.

(14) CEPD, lignes directrices cit., fév. 2022, p. 43, §127.

(15) Régl. (UE) n°2016/679, cons. 13.

(16) Lesaulnier F., La définition des données à caractère personnel dans le règlement général relatif à la protection des données personnelles in Le RGPD, Dalloz, 2018, p. 50

(17) CEPD, lignes directrices cit., fév. 2022, p. 3.

(18) Metallinos N., « Les critères de qualification des acteurs (responsables de traitement, responsables de traitement conjoints, sous-traitants) », CCE, avr. 2018, n°4, pp. 35-36.

(19) F. Mattatia, Sous-traitance et responsabilité des manquements à la sécurité des données personnelles : JCP E 2018, act. 102.

(20) Argument soulevé plus explicitement dans une autre délibération, mais pour un responsable du traitement : « La société […] soutient que l'obligation de sécurité résultant de l'article 32 du RGPD était une obligation de moyen et non de résultat, de sorte que l'obligation de sécurité du responsable du traitement consiste à mettre en œuvre

les mesures permettant de réduire les risques à un niveau acceptable, sans qu'il soit obligatoire, ni même possible, d'obtenir un niveau de sécurité les rendant nuls. La société a également souligné qu'elle n'a jamais subi de violation de données à caractère personnel (Cnil, Délibération SAN-2021-008 du 14 juin 2021 BP, §65).

(21) Elle constate néanmoins le lien de causalité entre la violation et les défauts, mais elle estime que ce qui est essentiel n'est pas ce lien de causalité mais bien le défaut de sécurité.

(22) Cnil, délibération SAN-2021-008 du 14 juin 2021, BP, §66.

(23) Cnil, délibération SAN-2021-20, 28 déc. 2021, S, §68.

(24) Cnil, délibération SAN-2021-21, 28 déc. 2021, FM, §106.

(25) Des torts partagés avaient déjà été sanctionnés dans une autre délibération qui était de moindre importance car non publiée : Cnil, délibération SAN-2021-002, 11 janv. 2021, Non publiée.

(26) Cnil, délibération SAN-2021-008 du 14 juin 2021, BP, §66.

(27) Cnil, La sécurité des données personnelles, 9 déc. 2021, accessible à l'adresse internet suivante : https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf ; v. également par exemple les nouvelles recommandations de la Cnil en matière de mot de passe https://www.cnil.fr.

(28) Aussi et DGE, La cybersécurité pour les TPE/PME, fév. 2021, accessible à l'adresse internet suivante : https://www.ssi.gouv.fr/guide/la-cybersecurite-pour-les-tpepme-en-douze-questions/

(29) En effet, il convient de noter que la Cnil cite l'Anssi dans de nombreuses publications (délibération, décision, guide…) dès lors que la sécurité des systèmes d'information est concernée. Notamment, Cnil, délibération SAN-2022-018, 8 sept. 2022, GIE I ; Cnil, délibération SAN-2021-21, 28 déc. 2021, FM ; Cnil, délibération SAN-2020-008 du 18 nov. 2020, CF ; et également sur son site internet https://www.cnil.fr/fr/securite-des-donnees-les-mesures-dhygiene-pour-proteger-votre-systeme-dinformation/

(30) Rappelons que le RGPD conseille d'aller au-delà : Régl. (UE) n°2016/679, cons. 109.

(31) Cette opération rend impossible la lecture de données à une personne qui n'en a pas la clé de déchiffrement.

(32) Cela s'inscrit dans la lignée de délibération précédentes de la formation restreinte. Ainsi, dans sa délibération n° SAN 2019-007 du 18 juillet 2019, la formation restreinte a relevé "que les mesures élémentaires de sécurité n'avaient pas été prises en amont du développement de son site web [par la société sanctionnée], ce qui a rendu possible la survenance de la violation de données à caractère personnel".

(33) Cnil, délibération SAN-2021-021 du 28 déc. 2021, FM §94 : dans laquelle la Cnil énonce explicitement : « La société aurait dû prévoir, dès la conception, des mesures organisationnelles et techniques pour ne plus traiter ces données dans ce cadre à la suite d'une demande de résiliation d'une ligne principale par la personne concernée ».

(34) À ce titre rappelons l'existence du guide RGPD pour l'équipe de développement, disponible sur GitHub, rappelle que les principes de développement conforme aux RGPD doivent être mis en œuvre dès la conception (https://lincnil.github.io/Guide-RGPD-du-developpeur/#Fiche_n%C2%B02%C2%A0:_Pr%C3%A9parer_son_d%C3%A9veloppement.)

(35) Cnil, délibération SAN-2021-019 29 oct. 2021 R, §62.

(36) Cnil, délibération SAN-2021-20, 28 déc. 2021, S, §74.

(37) Eu égard au fait qu'il s'agit d'une responsabilité propre au responsable du traitement ce point n'a pas été soulevé qui était possesseur des données en principe. Par ailleurs il est probable qu'il n'y ait pas eu de difficultés de ce point de vue.

(38) Le point aurait pu mériter un peu plus d'attention étant donné que le responsable du traitement est responsable de la proportionnalité des données et que le fait qu'il y ait des données de santé, n'est pas indépendant des choix faits par le responsable du traitement. Notons d'ailleurs, qu'un médecin dont un patient est concerné par les données ayant été publié, indiquait à Libération dans l'article cité que « mentionner VIH dans un champ libre est un choix délibéré, […] est critiquable, car il est totalement inutile […] parce qu'on prend le risque d'exposer une donnée à caractère particulièrement sensible ».

(39) Les défauts de sécurité auraient en théorie existé quand bien même le cadre contractuel aurait été conforme et que le sous-traitant n'avait pas outrepassé, selon la Cnil, les instructions communiquées par le responsable du traitement. C'est pourquoi, selon notre interprétation, les défauts de sécurité constituent le manquement majeur et ces deux inconformités doivent être considérées comme des aggravations.

(40) CEPD, lignes directrices cit., fév. 2022, p. 37, note 43.

(41) D'autant que c'est le responsable du traitement qui doit prendre la responsabilité de faire appel à des sous-traitants présentant des garanties suffisantes pour mettre en œuvre des mesures techniques et organisationnelles appropriées afin que le traitement réponde aux exigences du RGPD (Régl. (UE) n°2016/679, cons. 95 et CEPD, lignes directrices cit., fév. 2022, p. 4). Et ajoutons également que la Cnil a déjà sanctionné des responsables de traitement pour non respect de l'article 28§3 (Cnil, délibération SAN-2020-016 du 7 déc. 2020, P, point 6).

(42) Maisnier-Boché L., « lourde sanction par la Cnil d'un éditeur de logiciel, sous-traitant des laboratoires d'analyses médicales », CCE, n°7-8, juill. 2022, comm. 53, §4.

(43) CEPD, lignes directrices cit., fév. 2022, §110, p. 39.

(44) Délib. commentée §34.

(45) CEPD, lignes directrices cit., fév. 2022, p. 4.

(46) Cnil, Délibération SAN-2021-012, 26 juill. 2021, MC, §100.

(47) CEPD, lignes directrices cit., fév. 2022, §81 et §150 notamment.

(48) V. par exemple le raisonnement de R. Perray qui appliqué en l'espèce augmente le degré de responsabilité du sous-traitant. Il estime que dès lors qu'un sous-traitant outrepasserait son rôle en déterminant les moyens essentiels (choix des données par exemple) verrait son rôle devenir plus significatif et devrait en conséquence être davantage qualifié de responsable ou coresponsable que de sous-traitant (Perray R., Données à caractère personnel – introduction générale et champ d'application de la réglementation relative à la protection des données personnelles, Jcl. Communication, Fasc. 930, §16) ou celui de F. Mattatia, op. cit., JCP E 2018, act. 102.

(49) V. si le prestataire avait traité les données pour ses propres besoins la qualification aurait pu être différente : Metallinos N., op. cit., CCE, avr. 2018, n°4, pp. 35-36.

(50) Dans une autre espèce, dans le cadre de faits antérieurs à l'application du RGPD, la Cnil avait requalifié en responsable du traitement un sous-traitant qui n'avait pas respecté une instruction du responsable du traitement, car le non-respect concernait non pas un moyen essentiel, mais un moyen non essentiel « la société Z a mis à disposition le formulaire accessible via l'URL […] sans que la société X n'en ait connaissance, la circonstance qu'elle aurait décidée seule d'ajouter ce moyen de traitement - en plus des autres moyens déterminés dans le cadre du contrat de prestations conclu entre les deux sociétés - ne saurait suffire à la considérer comme responsable de traitement » (Cnil, Délibération SAN-2018-001, 8 janv. 2018, société X, §74).

(51) CEPD, lignes directrices cit., fév. 2022, §40, p. 17.

(52) CE, avis, 29 octobre 2007, Société sportive professionnelle LOSC Lille Métropole, n° 307736, Rec.

(53) CE, Section, 8 janvier 1954, Dame L., Rec. p. 22.

(54) CE, Section, 22 novembre 2000, Société Crédit Agricole Indosuez Chevreux, n° 207697, Rec.

(55) Une clause qui prévoirait le remboursement à titre de dommages et intérêts de l'amende prononcée par la Cnil au motif que le comportement de l'autre partie serait la clause de cette sanction ne paraît pas admise par la jurisprudence selon certaines autrices (Cousin A., « Réparer le préjudice causé par la violation du RGPD », Dalloz IP/IT, oct. 2019, n°10, p. 553).

(56) En ce sens la condamnation d'Orange, sous l'égide de l'ancienne loi, paraissait plus justifiée (CE, 10e et 9e sect., 30 déc. 2015, Société Orange : « qu'il ressort des termes de la délibération attaquée et qu'il n'est pas sérieusement contesté que la société Orange n'avait pas fait procéder à un audit de sécurité sur l'application qui avait été spécialement définie pour la prospection commerciale de ses clients […] n'avait pas veillé à ce que les consignes de sécurité prévues contractuellement avec Gutenberg soient portées à la connaissance du prestataire secondaire […] la formation restreinte a pu à bon droit estimer que la société Orange avait méconnu les obligations mises à sa charge »).

(57) V. supra.

(58) CA Paris, Pôle 05 ch. 05, 24 mars 2011, n°08/09164, confirmé par la Cour de cassation dans un arrêt inédit Com., 16 avr. 2013, n°11-19191 : L'analyse des fautes du commissionnaire par la Cour d'appel est éclairante car elle estime que les fautes même en présence d'instruction partielle mais claire n'empêche pas d'engager la responsabilité du commissionnaire en douane à raison des fautes qui lui sont propres : « Qu'en sa qualité de commissionnaire, il appartenait à la société Gondrand, qui possédait, au vu des factures et de l'activité des deux opérateurs, toutes les informations utiles, de procéder aux déclarations conformément à la législation applicable ; qu'elle ne peut arguer, avoir suivi les indications de son client alors que celui-ci est intervenu, à sa demande, en lui précisant, certes faussement, que toutes les pièces étaient destinées à un usage civil à savoir l'équipement de l'hélicoptère alouette, appareil qui a une double vocation civile et militaire ; que, toutefois, cette réponse n'a concerné qu'un nombre très limité de pièces ; qu'il n'en demeure pas moins que, pour la quasi-totalité des matériels, la société Gondrand a commis une faute relevant de sa responsabilité de commissionnaire en portant une catégorie tarifaire inexacte ».

(59) La Cnil peut par ailleurs elle-même condamner les deux acteurs lorsqu'elle le juge nécessaire : Cnil, délibération SAN-2021-002, 11 janv. 2021, non publiée.

(60) C.civ., 1984 et 1ère civ., 19 févr. 1968., n°64-14315

(61) Nous pensons notamment aux cas où le sous-traitant de rang 1 contracte avec le sous-traitant de rang 2. L'acte de contracter peut être soumis au régime du mandat. De sorte que devant faire connaître sa qualité, il pourrait dans ce cadre, être possible de dire que le sous-traitant de rang 1 n'est pas obligé envers le sous-traitant de rang 2.

(62) M. Guillemain, La sous-traitance en droit des données personnelles : RLDI 2018/152, n° 5265, §4

(63) C.civ, art. 1710, Le louage d'ouvrage est un contrat par lequel l'une des parties s'engage à faire quelque chose pour l'autre, moyennant un prix convenu entre elles.

(64) Délib commentée §35.

Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld sr@expertises.info

BASE DE DONNÉES

Nouvel éclairage sur le droit sui generis

Dans un arrêt de la première chambre civile du 5 octobre 2022, publié au bulletin, la Cour de cassation apporte des précisions utiles sur la notion d'investissement substantiel, condition préalable à la protection du producteur de base de données et consacre la possibilité de la protection autonome d'une sous-base de données, qualifiée de qualitativement substantielle, au titre du droit sui generis.

La protection des bases de données a été introduite en droit français par la loi du 1er juillet 1998 de transposition de la directive 96/9/CE du 11 mars 1996, et codifiée aux articles L112-3 puis L. 341-1 et suivants du code de la propriété intellectuelle. Deux régimes de protection, qui peuvent être cumulatifs, sont dès lors possibles : la protection au titre du droit sui generis qui s'attache au contenu de la base de données, et la protection au titre du droit d'auteur, sous réserve d'originalité, qui s'attachera à la forme de la base de données.

Dans l'espèce commentée, la société LBC France exploite le site internet « *www.leboncoin.fr* », site de petites annonces gratuites créé en 2006, acquis après la conclusion d'un traité d'apport partiel d'actif le 28 juin 2011 auprès de la société SCM France. La société Entreparticuliers.com exploite un site internet « *www.entreparticuliers.com* » créé au cours de l'année 2000, qui propose un service d'hébergement d'annonces essentiellement immobilières. Les données présentées par cette société sont pour partie collectées et transmises par un tiers pigiste à partir d'Internet.

Considérant que la collecte et la transmission de ses annonces par la société Entreparticuliers.com constitue un système d'extraction total, répété et systématique de sa base de données, la société LBC France a fait procéder à diverses opérations de constat d'huissier sur le site « *www.entreparticuliers.com* », puis a assigné la société exploitante pour obtenir des mesures indemnitaires et d'interdiction sur le fondement titre principal du droit sui generis et à titre subsidiaire de la responsabilité délictuelle.

Dans ce contentieux déjà abondamment commenté suite aux décisions rendues par le tribunal de grande instance de Paris le 1er septembre 2017[1] et par la cour d'appel de Paris du 2 février 2021[2], la Cour de cassation, saisie d'un pourvoi formé par la société Entreparticuliers.com, a eu à se prononcer sur 5 moyens du pourvoi dont un purement procédural portant sur : la qualité de producteur de base de données, la notion d'investissement substantiel, la possibilité d'une protection d'une sous-base de données dont l'extraction est qualitativement substantielle.

L'acquisition de la qualité de producteur de base de données

L'article L. 341-1 du code de la propriété intellectuelle définit le producteur de base de données comme celui qui prend l'initiative et le risque des investissements correspondants, et qui bénéficie d'une protection du contenu de la base lorsque la constitution, la vérification ou la présentation de celui-ci atteste d'un investissement financier, matériel ou humain substantiel.

En principe, la durée de la protection du contenu de la base de données est de 15 ans, à compter du 1er janvier de l'année civile qui suit son achèvement. En l'occurrence, la base de données revendiquée par la société LBC avait été créé en 2006 puis transmise par le traité d'apport partiel d'actifs du 28 juin 2011.

La société Entreparticuliers.com reproche à la cour d'appel d'avoir notamment retenu la qualité de producteur à la société LBC France alors que le traité d'apport partiel d'actifs du 28 juin 2011 prévoyait le transfert des droits de propriété intellectuelle sans mentionner

le transfert du bénéfice de droit sui generis du producteur de base de données initiale, et qu'il appartenait à la société LBC France de démontrer qu'elle avait réalisé des investissements ayant permis la création d'une nouvelle base de données éligible à la protection au titre du droit sui generis.

Approuvant le raisonnement de la cour d'appel, la Cour de cassation a retenu qu'après acquisition de la branche d'activité d'exploitation du site Internet « *leboncoin.fr* », la société LBC France avait procédé pour la constitution, la vérification et la présentation de la base de données à de nouveaux investissements financiers, matériels et humains substantiels de sorte qu'elle était fondée à revendiquer la protection de cette base de données. Cette solution ne peut qu'être approuvée notamment au regard des bases de données en perpétuel renouvellement et mises à jour. Il ne peut en effet être contesté que la base de données initiale créée par la société SCM, constituée d'annonces constamment supprimées et remplacées par de nouvelles annonces, n'existait plus en tant que telle, ayant laissé place, grâce aux nouveaux investissements revendiqués par la société LBC France à une nouvelle base de données.

La protection au titre du droit sui generis conférée à celui qui prend l'initiative de la création de la base, peut donc faire l'objet d'une cession, l'acquéreur procédant à des investissements substantiels sur cette base pouvant ensuite en acquérir la qualité de producteur.

La notion d'investissement substantiels

Comme le précise l'article L. 341-1 du code de la propriété intellectuelle, la protection au titre du droit sui generis nécessite que soient démontrés des investissements financiers matériels ou humains substantiels, réalisés pour la constitution, la vérification ou la présentation de la base.

La Cour de cassation, faisant référence à quatre arrêts de la Courde justice des Communautés européennes du 9 novembre 2004[3], rappelle que la notion d'investissement lié à l'obtention du contenu de la base de données doit s'entendre comme désignant les moyens consacrés à la recherche d'éléments existants et à leur rassemblement dans ladite base, à l'exclusion des moyens mis en œuvre pour la création des éléments constitutifs d'une base de données. Ainsi, le titulaire d'une base de données doit justifier d'un investissement autonome, par rapport à celui que requiert la création de données contenues dans la base dont il demande la protection.

Au soutien de son pourvoi, la société Entreparticuliers.com indiquait que les investissements revendiqués par la société LBC était consacrés à la création des éléments constitutifs d'une base de données, par nature exclus.

Approuvant le raisonnement de la cour d'appel, sont retenus comme constituant des investissements :

- au titre de l'obtention du contenu : les investissements de communication, les dépenses de stockage et plus généralement les investissements liés aux infrastructures informatiques permettant d'assurer l'enregistrement et le stockage de toutes les modifications dont la traçabilité est assurée ;
- au titre de la vérification du contenu : les investissements liés à l'acquisition d'un logiciel permettant la vérification des annonces dans un premier temps et les coûts liés à la prise en charge d'une équipe chargée de la modération une fois les annonces publiées ;
- au titre de la présentation du contenu : les dépenses liées à la classification des annonces en 10 catégories elles-mêmes divisées en sous-catégories avec des critères de recherche spécifique selon une arborescence détaillée organisant 28 millions d'annonces, la base étant mise à jour et en conformité par l'équipe « *produit* ».

C'est sur ce point que la Cour de cassation apporte utilement des éléments permettant de caractériser si des investissements sont afférents à la recherche d'éléments existants et à leur rassemblement, ou s'ils relèvent de la création des éléments constitutifs d'une base de données.

C'est finalement la conjonction des investissements réalisés par la société LBC France qui permet la recherche d'éléments existants et leur rassemblement dans la base, laquelle est en définitive créée directement par l'intermédiaire des utilisateurs lorsqu'ils déposent leurs annonces.

La possibilité d'une protection d'une sous-base de données, dont l'extraction est qualitativement substantielle

Le quatrième et le cinquième moyen du pourvoi sont consacrés à la notion d'investissements en relation avec la sous-base de données immobiliers dont le contenu a été spécifiquement réutilisé par la société Entreparticuliers.com par l'intermédiaire du tiers pigiste.

La société Entreparticuliers.com reproche à la cour d'appel d'avoir considéré que constituaient des investissements de constitution d'une base de données l'acquisition d'une base de données existante venant alimenter la sous-base de données immobiliers et surtout d'avoir considéré que la sous-base « *immobilier* » pouvait bénéficier d'une protection au titre du droit sui generis.

Il convient de rappeler que pour aboutir à ce raisonnement, la cour d'appel avait retenu que la société LBC France justifiait avoir investi 4,9 millions d'euros dans des campagnes de publicité ciblées en matière immobilière permettant d'alimenter sa sous-base « *immobilier* » d'une part, et d'avoir acquis pour un montant de 19,8 millions d'euros une société exploitant aussi des annonces immobilières en ligne, dans le but d'enrichir ladite sous-base.

La Cour de cassation approuve ce raisonnement consacrant ainsi la possibilité de protéger une sous-base, dès lors que les investissements consacrés à sa constitution, sa vérification et sa présentation sont substantiels.

De manière fort logique, si la sous-base peut bénéficier d'une protection autonome au titre du droit sui generis, c'est sans surprise que son extraction a été considérée comme qualitativement substantielle. En effet, dans le dernier moyen du pourvoi, la société Entreparticuliers.com revendiquait le fait qu'elle n'avait pas réalisé d'extraction mais simplement permis une indexation de contenu en insérant dans sa base de données un lien hypertexte renvoyant à la base de la société LBC France.

Toutefois, la cour d'appel, retenant que les informations réutilisées par le site « *www.entreparticuliers.com* » reprenaient tous les critères essentiels des annonces du site « *leboncoin.fr* », il ne pouvait être argué d'une simple indexation mais bien d'une extraction et une réutilisation d'une partie qualitativement substantielle du contenu de la sous-base de données « *Immobilier* » de la société LBC France.

La Cour de cassation consacre ainsi une protection de la sous-base à partir du moment où elle est autonome c'est-à-dire qu'il est possible pour son producteur de démontrer des investissements spécifiques et ciblés attachés à cette sous-base de données.

Ce raisonnement mérite l'approbation dans la mesure où la protection au titre du droit sui generis vise à protéger l'investissement et le risque, qu'il soit porté sur l'intégralité de la base ou sur une partie spécifique qui peut exister de manière autonome.

Sandrine VARA
Avocate associée
CINETIC Avocats
Ex-présidente de la Commission du numérique du CNB

Notes

(1) TGI Paris, 1er septembre 2017 n°17/06908 sté LBC France c/ Sté Entreparticuliers.com

(2) CA Paris, 2 février 2021 n°17/17688

(3) CJCE 9 novembre 2004 C-203/02, C46-02, C338-02, C444/02

Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld sr@expertises.info

RGPD

Le DPO : dans l'œil du cyclone ?

(Seconde partie)

Comme chaque mois, Alexandre Fievée tente d'apporter des réponses aux questions que tout le monde se pose en matière de protection des données personnelles, en s'appuyant sur les décisions rendues par les autorités nationales de contrôle au niveau européen et les juridictions européennes. Le mois dernier, il s'est penché sur la question des fonctions du DPO, et plus particulièrement celle de son positionnement dans l'organisme (Première partie). Ce mois-ci, il aborde la problématique de l'exercice effectif par le DPO de ses missions.

Le CEPD (Comité européen à la protection des données) a annoncé, en septembre dernier, que son action coordonnée 2022/2023 portera sur les problématiques liées à la désignation du DPO, son positionnement dans les organismes et ses missions. Dans le cadre de cette action coordonnée, le CEPD a invité les autorités nationales de protection des données à travailler sur le sujet.
Jusqu'à présent, l'action « *répressive* » de la Cnil sur la question du DPO -son positionnement dans al'organisme, ses ressources, ses missions- est restée relativement limitée. Faut-il s'attendre à ce que la Cnil diligente des missions de contrôle sur ce sujet ?

A l'aide de plusieurs décisions d'autorités de contrôle d'autres pays européens, nous allons essayer d'identifier – à partir des manquements constatés – les principales zones de risques. Ce mois-ci, nous allons aborder trois problématiques : la mission d'information et de conseil du DPO, ses missions de contrôle et la question de la planification de ses actions en fonction du risque.

En effet, il ressort des termes de l'article 39-1 du RGPD que le DPO a notamment pour mission d'informer et de conseiller le responsable du traitement (ou le sous-traitant) ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu de la règlementation ; de contrôler le respect du RGPD par l'organisme dont il dépend ; et de dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et de vérifier l'exécution de celle-ci. L'article 39-2 du RGPD ajoute que le DPO tient dûment compte, dans l'accomplissement de ses missions, « *du risque associé aux opérations de traitement* » compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

Les affaires

Dans plusieurs décisions rendues par les autorités luxembourgeoise (la « *CNPD* ») et hollandaise (« *l'AP* »), des organismes ont été sanctionnés pour ne pas avoir permis au DPO d'exercer ses missions d'information et de conseil. Tel a été le cas d'une société qui ne permettait pas à son délégué à la protection des données de réaliser un reporting formel et spécifique de son activité à l'encadrement supérieur, quand bien même des points réguliers étaient organisés. L'autorité luxembourgeoise a en effet considéré que, dès lors que la mission d'information et de conseil l'égard du responsable du traitement est « *intimement liée* » à l'obligation d'associer le DPO de manière appropriée et en temps utile à toutes les questions relatives à la protection des données, l'organisme avait manqué à ses obligations[1].

L'autorité hollandaise a adopté une position identique : « *Il est important que le responsable du traitement veille à ce que le DPO soit associé de manière appropriée et en temps utile à toutes les questions liées à la protection des données à caractère personnel. L'AP a établi que l'Administration fiscale et douanière n'avait pas correctement et en temps voulu associé le DPO pour mettre en œuvre une analyse d'impact (...). Il en résulte que le DPO n'a pas été en mesure d'accomplir correctement ses tâches et n'a donc pas été en mesure de conseiller à temps les autorités fiscales sur le respect du RGPD. En cas de consultation en temps opportun, le DPO aurait pu avertir plus tôt l'administration fiscale et douanière des risques associés au traitement inapproprié des données personnelles (...).* »[2]

Dans d'autres affaires, ce n'est pas le caractère effectif de la mission d'information et de conseil qui posait difficulté, mais les conditions dans lesquelles la mission de contrôle était réalisée par le DPO. Si la CNPD reconnaît que l'article 39.1 du RGPD n'impose pas à l'organisme de mette en place des mesures spécifiques pour assurer que le DPO accomplit sa mission de contrôle et que la tenue du registre des activités de traitement contribue à l'exercice de cette mission, elle relève toutefois que « *cet élément [la tenue du registre] pris isolément ne suffit pas à démontrer que la mission de contrôle du respect du RGPD est effectuée de manière adéquate* »[3].

Ainsi, selon l'autorité luxembourgeoise, « *la mission de contrôle effectuée par le DPO auprès du contrôlé devrait être suffisamment formalisée, par exemple par un plan de contrôle en matière de protection des données, afin de pouvoir démontrer que le DPO effectue sa mission de contrôle du respect du RGPD de manière adéquate.* » La CNPD a repris cette solution dans plusieurs autres affaires[4].

Enfin, dans une décision rendue par l'autorité polonaise de protection des données (« *UOPO* »), un éclairage est donné sur les attentes concernant l'article 39-2 du RGPD, selon lequel le DPO doit accomplir ses missions en tenant compte des « *risques* » liés aux opérations de traitement. Selon l'UODO : « *Cette disposition impose au délégué de fixer des priorités dans son travail, qui devrait consister à déterminer de manière individuelle et indépendante des mesures et des modalités de fonctionnement et à les adapter à la spécificité de l'organisme. Dans ce contexte, il est important d'identifier au préalable les risques liés au traitement des données personnelles et, sur cette base, de déterminer des solutions efficaces, tant techniques qu'organisationnelles. Il s'agit d'une approche sélective et pragmatique. Se concentrer sur les aspects qui comportent des risques plus élevés pour la protection des données à caractère personnel devrait permettre au DPO de conseiller plus facilement le responsable du traitement sur la méthodologie à utiliser lors de la réalisation du DPIA, sur les domaines devant être audités en interne ou en externe, sur les formations internes à planifier et réaliser pour les employés (...).* »[5]

Quelles recommandations ?

Organiser la participation directe, systématique et en temps utile du DPO aux différents comités dans lesquels sont discutées des questions portant sur la protection des données personnelles et donner à celui-ci un accès direct et non conditionné au niveau le plus élevé de la direction, semblent être des prérequis incontournables pour permettre au DPO d'exercer de manière effective ses missions d'information et de conseil.

Par ailleurs, il semble indispensable que l'organisme vérifie la mise en place par le DPO d'un plan d'actions comportant, parmi les actions à déployer, un plan de contrôle visant à vérifier que les préconisations qu'il a formulées ont bien été implémentées. A cet égard, il appartient au DPO de concevoir son plan d'actions selon une approche reposant sur le risque, c'est-à-dire en priorisant ses interventions et les mesures techniques et organisationnelles à mettre en œuvre en fonction des niveaux de risques identifiés.

Alexandre FIEVEE
Avocat Associé
DERRIENNIC ASSOCIES

Notes

(1) CNPD, Délibération n° 18FR/2021, 31 mai 2021.

(2) AP, Décision, 7 avril 2022.

(3) CNPD, Délibération n° 36FR/2021, 13 octobre 2021.

(4) CNPD, Délibération n° 38FR/2021, 15 octobre 2021 ; CNPD, Délibération n° 40FR/2021, 27 octobre 2021.

(5) UODO, Décision, 21 août 2020.

Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld sr@expertises.info

Vous cherchez une solution d'audit de la PI rapide et efficace ?

Vaultinum évalue les performances d'une entreprise en matière de :

- Protection des droits de PI
- Gestion des licences tierces
- Efficacité de la gestion de PI

L'audit PI de Vaultinum combine de manière unique :

1. Un questionnaire en ligne qui analyse la gestion et la propriété de la PI
2. Un scan complet du code source du logiciel pour identifier les risques de licences tierces
3. Un rapport d'audit PI élaboré par un expert expert en PI qui propose un plan d'action détaillé

A propos de Vaultinum

Depuis 1976, nous avons permis à des milliers de créateurs numériques, d'entreprises et d'investisseurs de sécuriser leurs innovations en leur fournissant des solutions pour protéger leur propriété intellectuelle, assurer la continuité de leur activité commerciale et atténuer les risques de cybersécurité et de maintenabilité inhérents aux logiciels.

www.vaultinum.com

contact@vaultinum.com