

## SOMMAIRE

PARIS - NANTES - LYON  
MONTPELLIER - LILLE  
TOULOUSE - NICE

*Bureaux intégrés*

AIX-EN-PROVENCE  
BLOIS - BORDEAUX  
BOURG-EN-BRESSE  
CLERMONT-FERRAND  
LE HAVRE - MARSEILLE - METZ  
MONTLUÇON - NANCY - NICE -  
OYONNAX PONTARLIER - ROUEN -  
TOURS VICHY

*Réseau SIMON Avocats*

ALGÉRIE - ARGENTINE  
ARMÉNIE - AZERBAÏDJAN  
BAHAMAS - BAHREÏN  
BANGLADESH - BELGIQUE  
BIRMANIE - BOLIVIE - BRÉSIL  
BULGARIE - BURKINA FASO  
CAMBODGE  
CAMEROUN - CHILI - CHINE  
CHYPRE - COLOMBIE  
CORÉE DU SUD - COSTA RICA  
CÔTE D'IVOIRE - ÉGYPTE  
EL SALVADOR  
ÉMIRATS ARABES UNIS  
ESTONIE - ÉTATS-UNIS - GRECE  
GUATEMALA - HONDURAS  
HONGRIE - ÎLE MAURICE  
ÎLES VIERGES BRITANNIQUES  
INDE - INDONÉSIE - IRAN  
ITALIE - KAZAKHSTAN  
KOWEÏT - LUXEMBOURG  
MADAGASCAR - MALTE  
MAROC - MEXIQUE - NICARAGUA  
OMAN - PANAMA - PARAGUAY  
PÉROU - PORTUGAL - QATAR  
RD CONGO - RÉPUBLIQUE  
DOMINICAINE - SENEGAL  
SINGAPOUR - SUISSE - THAÏLANDE  
TUNISIE - URUGUAY  
VENEZUELA - VIETNAM  
ZIMBABWE

*Conventions transnationales*

[www.simonassociés.com](http://www.simonassociés.com)

[www.lettredunumerique.com](http://www.lettredunumerique.com)



<p><b>DATA / DONNÉES PERSONNELLES</b></p> <p><b>Sanction de 1.5 million d'euros pour un éditeur-intégrateur de progiciel à destination des laboratoires d'analyse médicale</b></p> <p>Délibération de la CNIL du 15 avril 2022</p> <p><b>Le rapport de la CNIL pour l'année 2021 met en lumière la prise de conscience du citoyen dans la protection de leurs données personnelles</b></p> <p>42e rapport d'activité de la CNIL (année 2021) « Protéger les données personnelles, Accompagner l'innovation, Préserver les libertés individuelles »</p>	<p>p. 2</p> <p>p. 2</p>
<p><b>PROPRIÉTÉ INTELLECTUELLE</b></p> <p><b>Le groupe Louis Vuitton condamné à payer 700.000 euros à une ancienne designer pour avoir enfreint ses droits d'auteurs</b></p> <p>Cour d'Appel de Paris du 11 mars 2022 (n°20/08972)</p>	<p>p. 3</p>
<p><b>CONTENUS ILLICITES / E-RÉPUTATION</b></p> <p><b>L'Europe impose aux grandes plates-formes, comme Facebook (Meta) ou Amazon, de mieux éradiquer les contenus illicites et dangereux en ligne</b></p> <p>Digital Service Act (DSA) : COM(2020) 842 final – 15 décembre 2020</p>	<p>p. 4</p>
<p><b>SYSTÈME D'INFORMATION</b></p> <p><b>Le DSI de l'ancienne région Rhône-Alpes poursuit pour espionnage informatique, la procureure de la République requiert six mois d'emprisonnement avec sursis et 5.000 euros d'amende</b></p> <p>Article 226-15, 323-1 et 323-3 du Code pénal</p>	<p>p. 5</p>

## DATA / DONNÉES PERSONNELLES

### Sanction de 1.5 million d'euros pour un éditeur-intégrateur de progiciel à destination des laboratoires d'analyse médicale

Délibération de la CNIL du 15 avril 2022

Délibération de la CNIL du 15 avril 2022, sanction de 1,5 million d'euros pour un éditeur-intégrateur de progiciel à destination des laboratoires d'analyse médicale

**L'affaire en bref**

En février 2021, les données personnelles médico-administratives de près de 500 000 personnes ont été diffusées sur internet.

La fuite provenait d'un serveur FTP non protégé ayant servi à l'éditeur-intégrateur pour procéder à la migration des données d'un logiciel dont il cessait la maintenance vers un autre des logiciels qu'il édite.

**Le droit en cause**

- Article 28 paragraphe 3 du RGPD relatif à l'obligation de mettre en place un contrat entre le responsable de traitement et son sous-traitant.
- Article 29 du RGPD relatif aux traitements effectués sous l'autorité du responsable de traitement.
- Article 32 du RGPD relatif à la sécurité des traitements.

Au regard de ces articles, trois manquements ont été constatés.

**Article 28 RGPD**

Il a été reproché à l'éditeur-intégrateur ayant statué de sous-traitant au titre du RGPD l'absence de contrat de sous-traitance avec son client, responsable de traitement au sens du RGPD.

L'obligation d'encadrer, par un acte juridique formalisé les traitements effectués pour le compte du responsable de traitement, incombe tant au responsable de traitement qu'au sous-traitant et peut engager la responsabilité propre du sous-traitant.

Doivent comprendre les mentions obligatoires de l'article 28 RGPD notamment les OGV et les contrats de maintenance.

Il importe peu que la société ait ensuite entamé des démarches pour se mettre en conformité avec le RGPD dès lors qu'elle n'est pas effectivement en conformité lors des constatations de la CNIL.

**Article 29 RGPD**

Il a été reproché à l'éditeur-intégrateur de n'avoir pas respecté son obligation d'opérer sur instruction de son client au sens du RGPD.

Manque à l'obligation de ne traiter les données à caractère personnel que sur instruction du responsable de traitement, l'éditeur-intégrateur, sous-traitant au sens du RGPD, qui extrait un volume de données plus important que celui requis dans le cadre de la migration demandée par son client, responsable de traitement.

L'éditeur-intégrateur doit pouvoir justifier de la validation de son client sur l'extraction opérée, un ticket ne pouvant constituer une instruction au sens du RGPD.

Il importe peu que la société ait un outil inadéquat pour justifier avoir outrepassé les instructions données par ses clients.

La CNIL relève quelle aurait pu gérer pour un autre outil lui permettant de respecter les instructions ou à minima supprimer toutes les données qui n'auraient pas dû être extraites.

**Article 32 RGPD**

Il a été reproché à l'éditeur-intégrateur des manquements à son obligation de sécurité.

Aucune mesure de sécurité n'a été mise en œuvre s'agissant des opérations de migration des données, alors même que leur volume et leur caractère sensible aurait dû conduire à mettre en place des procédures spécifiques. Ce manquement de l'éditeur-intégrateur a fait peser un risque de compromission facilement évitable sur ces données.

L'éditeur-intégrateur a ignoré toutes les alertes relatives à ses manquements en matière de sécurité, ce qui a abouti à la violation des données.

Les mesures élémentaires de sécurité n'ont pas été mises en place.

- Techniques : les données n'étaient pas chiffrées, stockage de données sur la zone publique du serveur en ligne, aucun effacement automatique à l'issue des opérations de migration, aucune procédure de supervision et de remontée d'alerte sur le serveur ;
- Organisationnelles : plusieurs salariés utilisant un même compte pour accéder à la zone privée du serveur, faisant peser un risque disproportionné sur la sécurité.

**Sanction**

Article 83 RGPD

La sanction a été prononcée au regard des manquements eux-mêmes, et pas de leur conséquence grave pour les personnes concernées, quand bien même cet élément a été pris en considération.

Amende administrative d'un montant de 1 500 000 €.

Publication sur le site de la CNIL de la délibération, non anonymisée pour une durée de deux ans.

**SIMON ASSOCIÉS**

### Le rapport de la CNIL pour l'année 2021 met en lumière la prise de conscience du citoyen dans la protection de leurs données personnelles

42e rapport d'activité de la CNIL (année 2021) « Protéger les données personnelles, Accompagner l'innovation, Préserver les libertés individuelles »

Ce qu'il faut retenir :

Madame Marie-Laure Denis, présidente de la CNIL affirmait que « plus que jamais, c'est le respect d'un équilibre entre accompagnement de la transformation numérique et protection des droits des personnes qui permettra de relever les défis soulevés par la numérisation de notre environnement quotidien ».

L'engagement de la CNIL et de sa présidente a permis d'encourager la mobilisation citoyenne dans la prévention et la garantie de leurs droits. Une réelle prise de conscience des citoyens à l'égard de leurs données personnelles a été soulignée dans son dernier rapport publié le 11 mai 2022 pour l'année 2021.

Pour approfondir :

Le rapport rappelle que « les personnes ont de plus en plus conscience de leurs droits : cette tendance, déjà relevée en 2019 et en 2020 se caractérise également par une plus grande volonté de les exercer ».

Le nombre élevé de plaintes reflète cette importante mobilisation citoyenne. Ont été notifiées 5 037 violations de données en 2021 soit 79 % de plus qu'en 2020. Parmi ces notifications, 973 plaintes concernent la publicité par courrier électronique, SMS ou encore par téléphone. De plus, 1436 plaintes visent le droit d'accès aux données personnelles.

Dans son rapport, la CNIL constate que la grande majorité des plaintes sont réalisées via des plateformes en ligne et notamment 85 % via les formulaires « nous contacter » ou « besoin d'aide » mis à disposition sur le site de la CNIL.

La CNIL souligne également le succès de la campagne « histoires vécues » qui a permis aux internautes de partager leurs expériences personnelles concernant la violation de leurs données personnelles. Il s'agit d'une campagne générale de sensibilisation qui implique directement le citoyen. C'est un format qui a bien fonctionné et qui est prometteur pour les années à venir.

Enfin, il faut constater que le signalement des violations n'est pas le seul élément qui témoigne de cette mobilisation. La volonté du citoyen à se voir appliquer ces droits démontre également de cette prise de conscience. À ce titre, la CNIL a reçu 5.882 demandes d'exercice indirect des droits, soit 35% de plus qu'en 2020. En effet, elle a été appelée à agir pour le compte des usagers en matière de droits d'accès, de rectification ou d'effacement des données personnelles.

Il apparaît incontestable que les réseaux sociaux ont permis de mettre en place une campagne de sensibilisation auprès du grand public. Ces plateformes sont un intermédiaire efficace entre la CNIL et les usagers. La commission a en effet posté sur le réseau social LinkedIn des guides pratiques du RGPD et du DPO. Un accès rapide, gratuit et facile permet ainsi de toucher un plus large public.

Dans cette même dynamique, le nombre d'abonné de la CNIL sur les réseaux sociaux est toujours plus important. En 2021, la CNIL compte 5% d'abonnés en plus sur Twitter. Sur Facebook elle enregistre une hausse d'abonnement de plus de 17 %. Enfin, sur LinkedIn, la CNIL a répertorié une hausse de 16 % d'abonnés.

Même si une prise de conscience du public et des professionnels est notable, les perceptions d'évolutions sont importantes. La CNIL devra mener une politique de sensibilisation encore plus percutante et d'autant plus auprès des plus jeunes.

**À rapprocher : 42e rapport d'activité de la CNIL**

## PROPRIÉTÉ INTELLECTUELLE

**Le groupe Louis Vuitton condamné à payer 700.000 euros à une ancienne designer pour avoir enfreint ses droits d'auteurs**

Cour d'Appel de Paris du 11 mars 2022 (n°20/08972)

*Ce qu'il faut retenir :*

**Une designer qui avait conçu et réalisé des fermoirs de sac à main de ville et de sac de voyage pour la société Louis-Vuitton a fait condamner cette dernière par la Cour d'Appel de PARIS à lui payer la somme de**

**700.000 euros pour non-respect de la convention qui régissait ses droits d'auteur sur les dites fermoirs.**

*Pour approfondir :*

**I. Un contrat de commande pour la conception et la réalisation d'un fermoir pour sac de ville et sac de voyage**

En l'espèce, en 1987 une designer travaillant à son compte, passe un contrat dit de « concession de savoir-faire » avec la société Louis Vuitton Malletier portant sur la collaboration d'une gamme de sac à main de ville. Elle conçoit alors pour la marque un fermoir dénommé « LV tournant ». En contrepartie, la société lui reverse une rémunération fixe ainsi que des redevances sur chaque sac vendu.

Par suite de ce contrat, un second a été conclu en 1988. Ce dernier prévoyait la réutilisation de ce fermoir pour une collection de bouclerie ainsi que pour des sacs de voyage et de loisir. En contrepartie de la cession de ces droits sur sa création, une rémunération forfaitaire devait lui être versée.

Enfin, en 1992, la marque de luxe et la designer signent une convention qui porte sur la cession de tous les droits de reproduction et représentation attachés aux collections concernées par les deux autres contrats, c'est-à-dire sur les sacs de ville, voyage et loisir ainsi que sur les collections de bouclerie.

Le rachat des droits de propriété est consenti dès lors que la société Louis Vuitton verse à la designer une contrepartie financière, ce versement annulant toutes redevances futures sur la commercialisation de sur de nouvelles collections concernant les sacs de ville, voyage et loisir ainsi que sur les collections de bouclerie comme le prévoyait les conventions initiales.

Cependant, quelques années plus tard la designer découvre que la société Louis Vuitton avait exploité son fermoir « LV tournant » pour de nouveaux produits qui n'étaient pas prévus par la convention de 1992. Elle sollicite alors la société Louis Vuitton pour le paiement des sommes dues au titre de la convention signée en 1992.

**II. La société Louis Vuitton ne respecte pas la convention de 1992 en utilisant le fermoir « LV tournant » sur des portefeuilles, bracelets, chaussures, ceintures et porte-clés**

En 2014 la société Louis Vuitton a lancé deux nouvelles lignes de sacs intégrant le fermoir «LV tournant » sans informer la designer puisque sa création ayant été réutilisée sur des nouvelles collections, elle aurait dû recevoir une contrepartie financière.

En effet toute autre utilisation du fermoir « LV tournant » sur des portefeuilles, bracelets, chaussures, ceintures et porte-clés ne faisaient pas partie de la convention.

Celle-ci prévoyant une réutilisation exclusive sur les sacs de ville, de voyage et de loisir ainsi que les collections de bouclerie. L'utilisation de la création avait donc été effectuée sans l'accord de l'auteur car aucune convention de cession de ses droits n'avait été passée sur ces nouveaux objets commercialisés par la société Louis Vuitton.

### III. Les sanctions alléguées : une action en contrefaçon

C'est la raison pour laquelle la Cour d'appel a relevé l'existence d'une contrefaçon des créations artistiques et du design et plus spécifiquement dans le cas d'espèce des dessins et modèles conçus et réalisés par la designer.

La Cour d'appel a donc jugé notamment qu'au « vu de l'ensemble de ces éléments et des pièces produites par les parties, [...], de fixer la réparation intégrale du préjudice subi par Mme A à la somme de 700.000 euros pour l'utilisation sans autorisation du «LV tournant » sur des portefeuilles, bracelets, chaussures, ceintures et porte-clés ».

Louis Vuitton a donc été condamné en contrefaçon d'une création artistique ou d'un design pour une utilisation non autorisée du fermoir « LV tournant ».

### Conclusion

Il s'agit d'une décision sévère à l'encontre de la société Louis Vuitton.

La société Louis Vuitton a formé un pourvoi devant les juges de la Cour de cassation.

Affaire à suivre ...

**A rapprocher : Cour d'appel de Paris - Pôle 05 ch. 02, 11 mars 2022 / n° 20/08972**

## CONTENUS ILLICITES / E-RÉPUTATION

### L'Europe impose aux grandes plates-formes, comme Facebook (Meta) ou Amazon, de mieux éradiquer les contenus illicites et dangereux en ligne

Digital Service Act (DSA) : COM(2020) 842 final – 15 décembre 2020

*Ce qu'il faut retenir :*

**Le DSA met à jour une directive sur l'e-commerce qui avait plus de vingt ans c'est-à-dire quand les plates-formes et autres réseaux sociaux aujourd'hui géantes étaient encore embryonnaires. L'objectif de ce règlement qui s'impose aux Etats de l'Union Européenne est de mettre fin aux dérives des réseaux sociaux qui ont souvent défrayé la chronique comme l'assassinat du professeur d'histoire Samuel PATY en France après une campagne de haine à son encontre, en octobre 2020 ; ou bien encore l'assaut de manifestants sur le Capitole aux Etats-Unis, en janvier 2021, en partie planifié grâce à Facebook et Twitter...**

*Pour approfondir :*

Thierry Breton, commissaire européen disait que « tout ce qui est interdit dans la vie réelle le sera désormais sur internet ». Dans cette dynamique le 15 décembre 2020, la Commission européenne a déployé un paquet législatif proposant deux règlements qui s'imposent aux Etats membres de l'Union Européenne, le DSA et le DMA respectivement, « Digital Service Act » et « Digital Market Act » afin de faire d'internet un environnement plus sûr pour les internautes et les consommateurs.

Ces textes mettent à jour la directive « e-commerce » 2000/31/CE qui avait plus de 20 ans et qui avait été appelé à réguler les plateformes alors qu'elles n'étaient encore qu'à leurs débuts. Ainsi, le DSA a dû et su s'adapter rapidement à de nouveaux enjeux liés au développement d'Internet et imposer une régulation ex-ante plus rigoureuse.

La directive « e-commerce » opérait une distinction entre le statut des hébergeurs et celui des éditeurs aux bénéfices des hébergeurs.

Les éditeurs de contenus étaient soumis à des obligations plus grandes du seul fait qu'ils définissaient le contenu devant être mis en ligne.

Le DSA vient alors combler cette lacune, les grands hébergeurs tels que Facebook ou YouTube devant désormais être responsable des contenus qu'ils hébergent.

### I. Les ambitions affichées par le DSA

Le DSA a pour ambition de lutter contre les contenus illicites mis en ligne et contraint les plateformes considérées comme hébergeurs à mettre en œuvre les mesures nécessaires afin de les supprimer ou de les rendre inaccessibles.

Ces derniers sont également soumis au principe de transparence. Ils sont contraints de publier des rapports à raison d'une fois par an minimum et à destination du public. Ces rapports doivent apporter des précisions sur le fonctionnement de leurs algorithmes ainsi que sur les modalités de modération du contenu jugé illicite.

### II. L'utilisateur : un acteur du projet européen

Par ailleurs, le DSA mobilise également l'utilisateur. Celui-ci doit avoir un comportement actif dans la prévention des contenus illicites.

À ce titre, l'accès à un service de plainte doit être possible pour tous. Le règlement prévoit donc des dispositifs gratuits et simples d'accès.

Pour s'inscrire dans cette démarche, les plateformes doivent mettre en place des systèmes internes (signaleur de confiance ou délégué à la conformité) qui favorisent l'efficacité du traitement des signalements. Toutefois, les abus seront sanctionnés.

### III. Les garanties d'une effectivité du DSA

L'effectivité du règlement dépend en grande partie des sanctions proposées. En effet, le DSA affiche des sanctions financières importantes en cas de non-respect du règlement. Les acteurs concernés s'exposent donc à des amendes pouvant atteindre jusqu'à 6% de leur chiffre d'affaires mondial alors même que le RGPD (Règlement général sur la protection des données) prévoit des amendes s'élevant au maximum à 4% du chiffre d'affaires mondial.

Sont également imposé par le DSA, des « coordinateurs des services numériques » dans chaque Etat membre. Ces derniers doivent veiller au respect de la nouvelle réglementation au niveau national.

### IV. En conclusion

Le DSA s'efforce d'apporter à la fois une meilleure surveillance, un contrôle plus rapide et des sanctions plus dissuasives. Ces démarches permettent ainsi de renouveler la confiance de l'utilisateur dans les services numériques.

Ce règlement européen encourage ainsi les Etats de l'Union Européenne à s'inscrire dans cette nouvelle dynamique qui n'est encore qu'à ces débuts.

**A rapprocher : Digital Service Act (DSA) : COM(2020) 842 final – 15 décembre 2020 ; Digital Market Act (DMA) : COM(2020) 825 final – 15 décembre 2020**

## SYSTÈME D'INFORMATION

**Le DSI de l'ancienne région Rhône-Alpes poursuit pour espionnage informatique, la procureure de la République requiert six mois d'emprisonnement avec sursis et 5.000 euros d'amende**  
Article 226-15, 323-1 et 323-3 du Code pénal

*Ce qu'il faut retenir :*

**Le Tribunal correctionnel de Lyon a entendu le vendredi 20 mai 2022 le Directeur des Services d'Information (DSI) de la Région Rhône-Alpes (ci-après : la Région) à qui il était reproché de s'être octroyé un accès non autorisé aux boîtes mails des administrateurs de cette région (ex-Rhône-Alpe) et y compris celles des élus.**

**Cet accès permettait ainsi au DSI d'effectuer des prospections ciblées sur les sources d'un journaliste en entrant le mot clef « dangele » dans la barre de recherche. Ce terme correspondant à l'adresse courriel de l'ancien journal dénommé « les potins d'Angèle ».**

**Il est reproché au DSI plusieurs manquements au Code Pénal, à savoir, une atteinte au secret des correspondances par voie de télécommunication ainsi qu'un accès et maintien frauduleux dans un système de traitement automatisé des données.**

Pour approfondir :

Fin 2015, le DSI a eu accès à l'ensemble des échanges privés de la Région pour soi-disant des nécessités techniques et notamment de maintenance du système informatique.

Pourtant, le Procureur de la République n'est pas de cet avis et a considéré que l'accès et le maintien sur ces réseaux privés était illicite. En effet, pour le ministère public cette maintenance et la sécurité du système d'information de la Région aurait dû se faire sur des postes précis et seulement à des fins de maintenance et de contrôle de la sécurité.

Or, il semblerait que l'accès ait été généralisé à l'ensemble des boîtes mails et réalisé aux seules fins d'espionnage en vue de détecter les sources (administrateurs et élus) du journaliste. Cet accès ne se destine évidemment pas à la sécurité des réseaux.

Cet accès s'il devait être jugé frauduleux va à l'encontre de l'article 323-1 du Code pénal qui dispose que « *le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende* ».

Les faits d'espèce s'inscrivent dans le prolongement du jugement du Tribunal de Grande Instance de Paris du 27 janvier 2003 « Philippe D. c/ Lycos France, www.legalis.net ». Les juges avaient consacré le principe du respect du secret des courriers électroniques.

De la même manière cet accès à une messagerie privée des administrateurs et des élus de la Région peut alors être assimilé à de l'espionnage afin d'y trouver des informations confidentielles.

Cette infraction est également punie par le Code pénal à l'article 226-15 qui dispose que « *le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45 000 euros d'amende* »

Enfin, il peut être reproché au DSI d'avoir enfreint l'article 323-3 du Code pénal qui dispose que « *le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient*

*est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.* »

Le jugement sera rendu par le Tribunal correctionnel de Lyon le 1er juillet 2022 nous ne manquerons pas de vous tenir informé des suites ...

**À rapprocher : Jurisprudence TGI de Paris 23 janvier 2003, « Philippe D. c/ Lycos France » ; Article 226-15 du Code pénal ; Article 323-1 du Code pénal ; Article 323-3 du Code pénal**