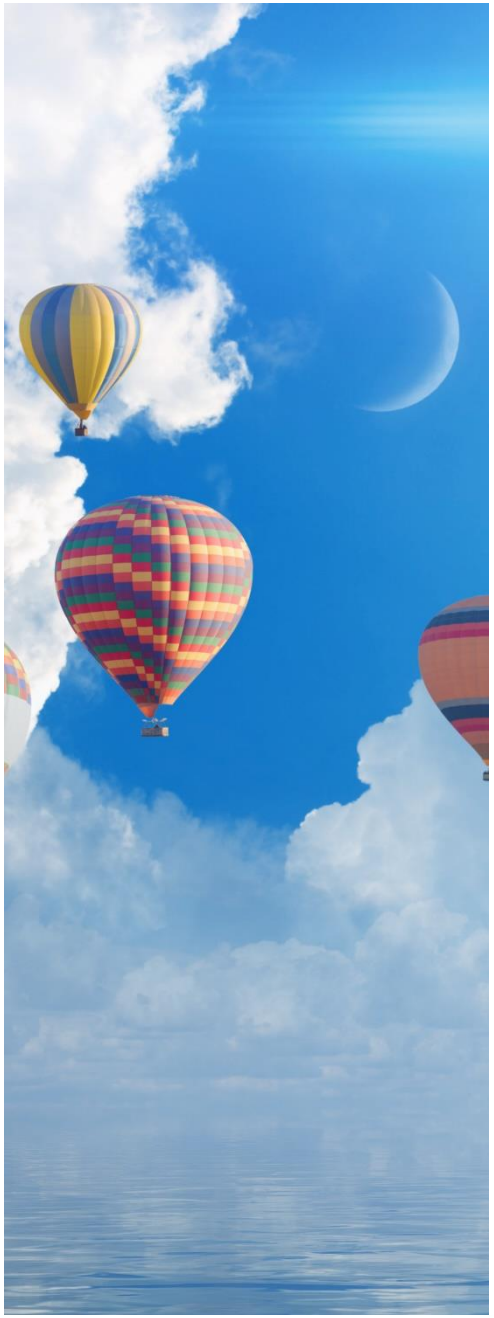
racine
AVOCATS



Entités critiques / essentielles / importantes

Les règles UE de cyber-sécurité pour 2024 (partie 1)

Racine, le Cabinet

Une culture unique

Proche de ses clients, Racine se positionne comme un partenaire.

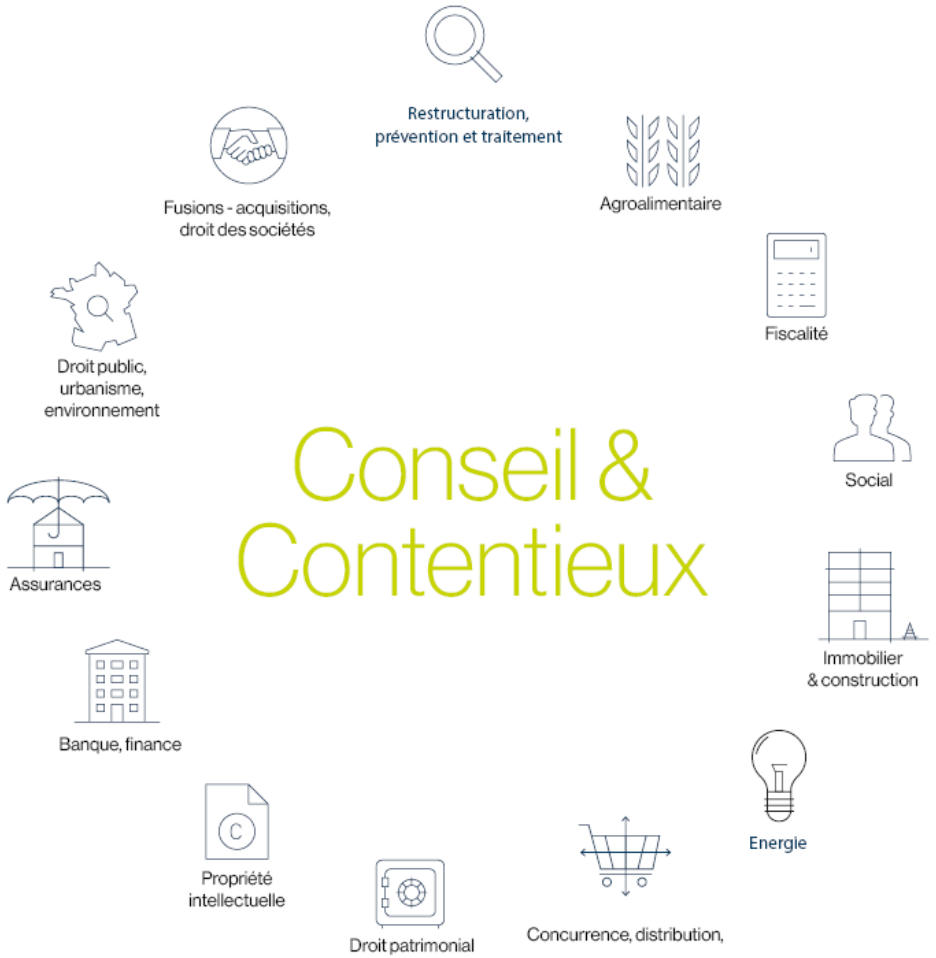
Sa forte technicité juridique lui permet de leur apporter des solutions concrètes et opérationnelles ; sa pratique transverse du contentieux lui confère une réelle capacité d'anticipation.

Le contentieux, exercé par l'ensemble des avocats, fait partie de l'ADN de Racine depuis sa création et représente 50% de son activité.

La culture du cabinet transparait dans son organisation, pensée pour créer des interactions naturelles entre ses départements. Cette transversalité est un atout majeur pour la gestion des dossiers complexes ou pluridisciplinaires.

Les associés sont engagés personnellement dans chaque dossier, de la définition des lignes stratégiques à la résolution complète des problématiques, et en contrôlent le suivi opérationnel.

Enfin, le maillage du territoire national et la capacité de projection internationale de Racine assurent sa capacité d'intervention quel que soit le lieu où ses clients sont implantés.



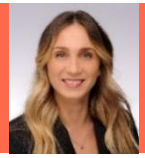
Qui sommes nous ?

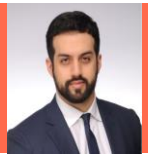
Associés

Eric Barbry
ebarbry@racine.eu

Charles Bouffier
cbouffier@racine.eu

Collaborateurs





Dans le domaine de l'IP (Intellectual Property) l'équipe intervient dans tous les domaines relatifs à la valorisation du patrimoine immatériel des entreprises et acteurs publics (marques, noms de domaine, brevets, concepts algorithmes, …).

En matière IT (information technology), l'équipe dispose d'une compétence tout à fait particulière. Elle intervient en conseil, contentieux et contrats dans les domaines suivant : internet, plateformes et commerce électronique, marketing digital, télécommunications, applications mobiles, dématérialisation ou encore sécurité des systèmes d'information.

En matière de Data, l'équipe intervient quotidiennement dans le domaine du droit des données à caractère personnel et le déploiement du RGPD. Mais elle intervient également sur le droit des data de manière plus générale (open data, données d'intérêt public, confidentiel entreprises, secret, …).

racine AVOCATS

8
AVOCATS DÉDIÉS

PROXIMITÉ

FULL TECHNOLOGY

RÉACTIVITÉ

racine
AVOCATS

PARTIE 1

Introduction

MON QUARTIER

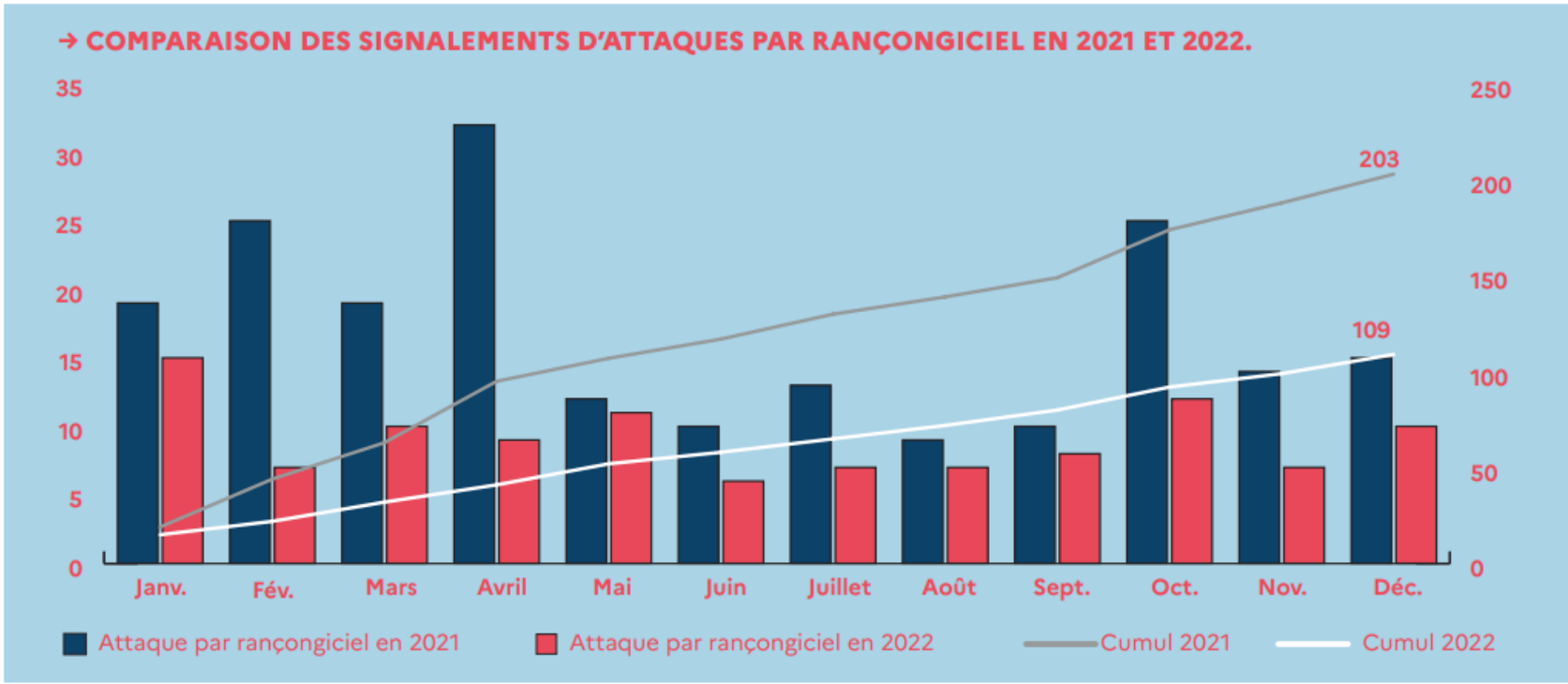
Bois-Blancs
Lille-Centre
Faubourg de Béthune
Fives
Lille-Moulins
Lille-Sud
St-Maurice Pellevoisin
Vauban-Esquermes
Vieux-Lille
Wazemmes

ACTUALITÉS

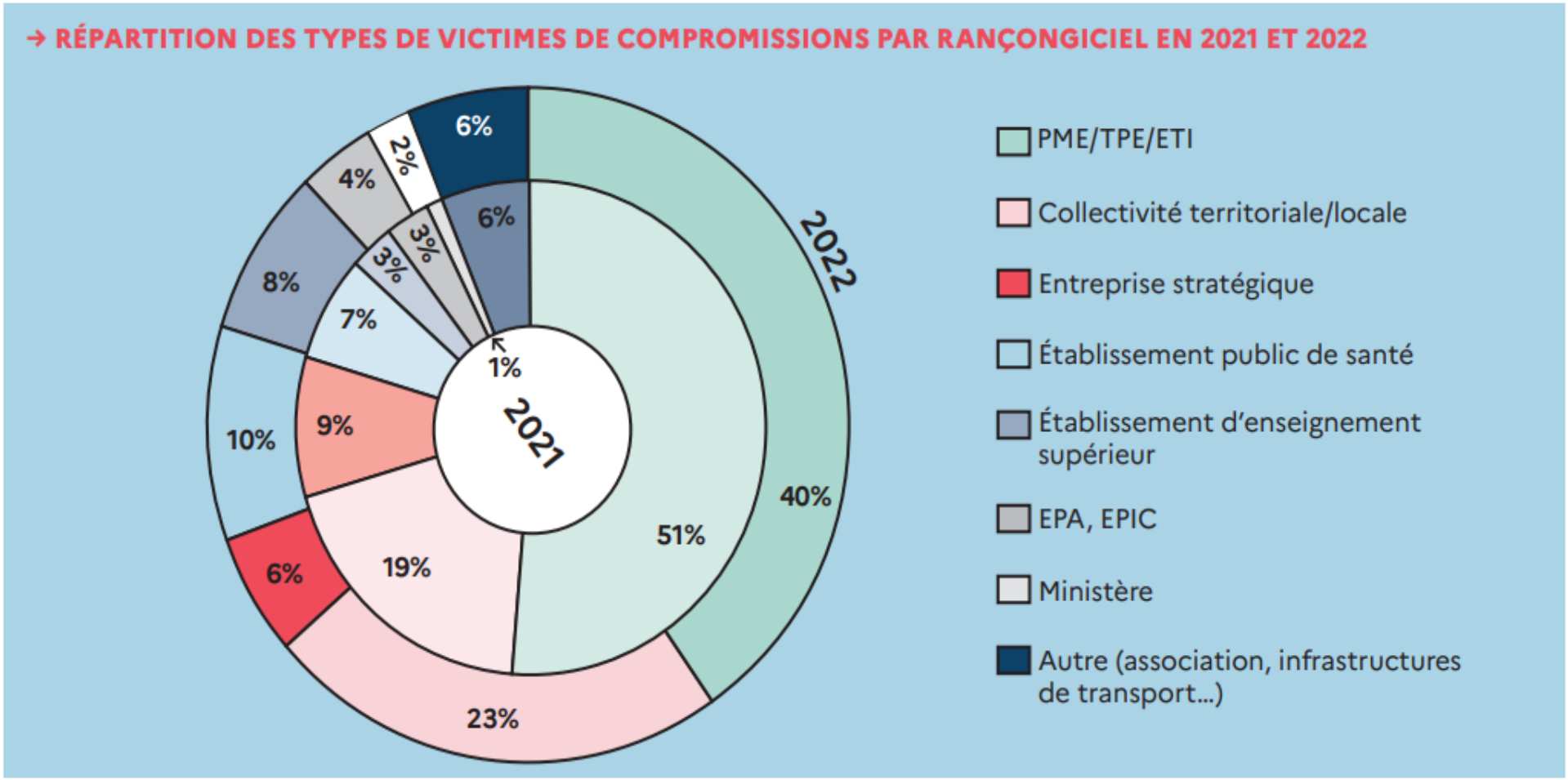
RETROUVEZ TOUTES NOS ACTUALITÉS SUR

VOIR TOUTES LES ACTUALITÉS

Rapport Anssi



Rapport Anssi



Rapport Cnil

Vision opérationnelle

Moyenne 2 / semaine

Surtout le vendredi vers 19h – Idéalement le 23 décembre 9h33 !

Tous secteurs

Toutes tailles

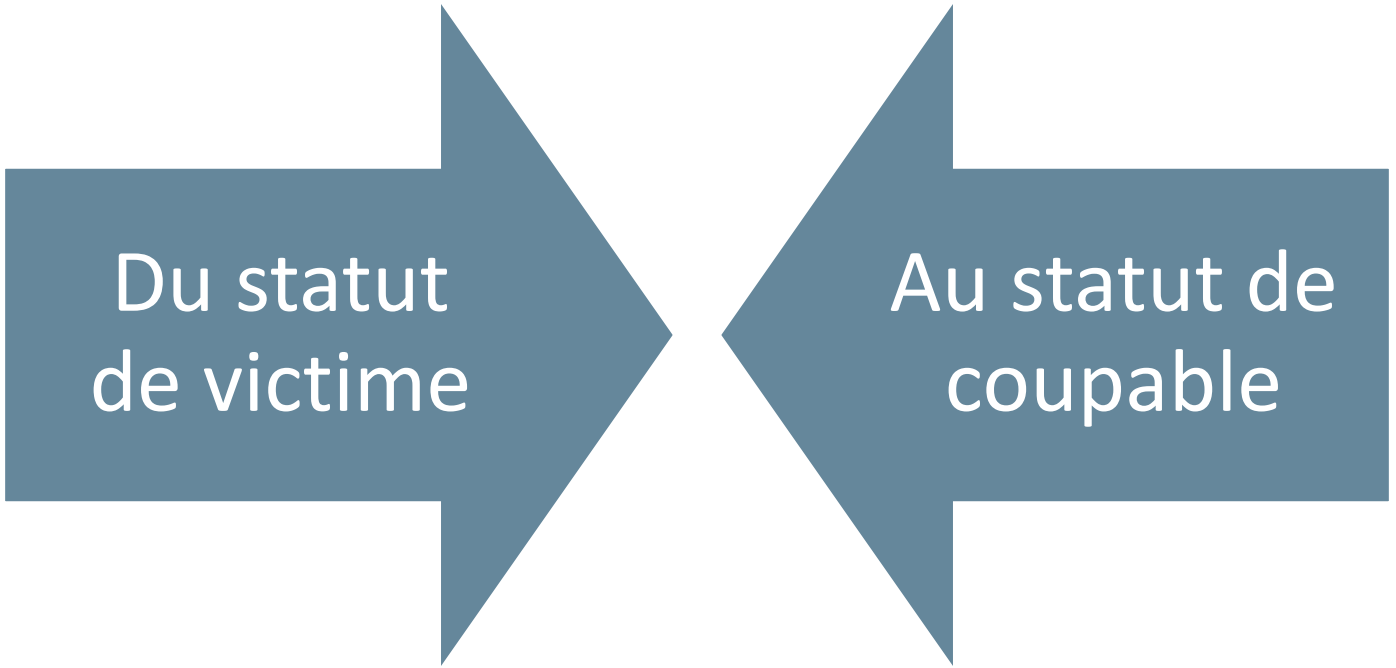
Demande de rançons

racine
AVOCATS

PARTIE 2

Le paradoxe juridique

Le paradoxe juridique



Victime de type 1

Article 323-1 (Modifié par LOI n°2023-22 du 24 janvier 2023 - art. 6)

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement (avant 2) et de 100 000 € d'amende (avant 60.000).

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de cinq ans d'emprisonnement (avant 3) et de 150 000 € d'amende (avant 100.000).

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement (avant 5) et à 300 000 € d'amende. (avant 150.000)

Victime de type 2

Article 323-2

Le fait d'entraver ou de fausser ~~frauduleusement~~ le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende.

Victime de type 3

Article 323-3

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.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende.

Victime de type 4

Art. 226-18

Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Victime de type 5

Article L151-5 – code de commerce

L'utilisation ou la divulgation d'un secret des affaires est illicite lorsqu'elle est réalisée sans le consentement de son détenteur légitime par une personne qui a obtenu le secret dans les conditions mentionnées à l'article L. 151-4 ou qui agit en violation d'une obligation de ne pas divulguer le secret ou de limiter son utilisation.

La production, l'offre ou la mise sur le marché, de même que l'importation, l'exportation ou le stockage à ces fins de tout produit résultant de manière significative d'une atteinte au secret des affaires sont également considérés comme une utilisation illicite lorsque la personne qui exerce ces activités savait, ou aurait dû savoir au regard des circonstances, que ce secret était utilisé de façon illicite au sens du premier alinéa du présent article.

Article L151-6

L'obtention, l'utilisation ou la divulgation d'un secret des affaires est aussi considérée comme illicite lorsque, au moment de l'obtention, de l'utilisation ou de la divulgation du secret, une personne savait, ou aurait dû savoir au regard des circonstances, que ce secret avait été obtenu, directement ou indirectement, d'une autre personne qui l'utilisait ou le divulguait de façon illicite au sens du premier alinéa de l'article L. 151-5.

Article L152-1

Toute atteinte au secret des affaires telle que prévue aux articles L. 151-4 à L. 151-6 engage la responsabilité civile de son auteur.

Slimpay – 180.000€ décembre 2021

La société [Slimpay] est un établissement de paiement agréé, qui propose des services de paiements. Elle propose à ses clients, les " marchands " qui sont des personnes morales, des solutions de gestion des abonnements et des paiements récurrents.

A la suite d'un projet de recherche interne, la société a stocké un certain nombre de données sur un serveur **ne faisant pas l'objet d'une procédure de sécurité et accessible librement depuis internet**, provoquant une violation de données concernant 12 millions de personnes.

Au titre de l'article 32 du RGPD, il est reproché à la société d'avoir laissé en service ledit service alors qu'il était possible d'y accéder depuis internet, permettant ainsi l'accès à des adresses postales et courriel, numéros de téléphone, et plus grave encore, des informations bancaires.

En outre, la formation restreinte reproche à la société de ne **pas avoir mis en œuvre de mesure de journalisation des accès au serveur**, ce qui aurait permis de détecter les actions effectuées. La CNIL reprend d'ailleurs les recommandations de l'ANSSI qui relève que « les journaux d'évènements constituent une brique technique indispensable à la gestion de la sécurité des systèmes d'information " dans la mesure où ils peuvent être utilisés a priori pour détecter des incidents de sécurité " et a posteriori pour " comprendre le cheminement d'une attaque et évaluer son impact »

La Cnil considère que la circonstance selon laquelle le manquement aurait pour origine **une erreur humaine n'est pas recevable**, notamment au titre que le manquement n'était pas ponctuel mais correspondait à une répétition des mêmes insuffisances. Le serveur n'aurait dû être accessible qu'aux seuls utilisateurs habilités. La formation restreinte conclu en affirmant que la sécurité d'un système d'information repose sur un ensemble de mesures techniques et procédurales et non pas sur la seule compétence des personnes, ces mesures permettant justement de pallier à l'erreur humaine.

Deladus Biologie – 1,5 millions d'euros – 15 avril 2022

La société DEDALUS BIOLOGIE commercialise des solutions logicielles à destination de laboratoires d'analyses médicales, appelées solutions de gestion de laboratoire. Environ trois mille laboratoires de biologie médicale privés et entre trente et cinquante laboratoires d'analyses d'établissements publics de santé sont équipés des solutions éditées par la société DEDALUS BIOLOGIE.

Cette décision fait suite à une fuite de données de 500 000 personnes, comprenant l'identité, le numéro de sécurité sociale, l'identité du médecin prescripteur et des informations médicales sensibles (traitements, données génétiques, Séropositivité, cancers, maladies génétiques, etc.). La société a été condamnée à payer une amende de 1.5 millions d'euros.

Les manquements relatifs à la sécurité concernaient les lacunes de cette dernière dans le cadre des opérations de migration du logiciel vers un autre :

- absence de chiffrement des données personnelles stockées sur le serveur siège de la violation;
- absence d'effacement automatique des données après migration vers l'autre logiciel ;
- absence d'authentification requise depuis internet pour accéder à la zone publique du serveur ;
- utilisation de comptes utilisateurs partagés entre plusieurs salariés sur la zone privée du serveur ;
- absence de procédure de supervision et de remontée d'alertes de sécurité sur le serveur.

Accor – 600.000€ - 3 aout 2022

Manque de robustesse des mots de passe pour l'accès à l'outil e gestion d'envoi de communications aux clients : uniquement 8 caractères contenant seulement deux types de caractère (sept lettres majuscules et un caractère spécial). Lesdits comptes permettaient d'accéder à l'outil de gestion d'envoi des communications aux clients.

En cas de suspicion de connexion frauduleuse, les clients souhaitant voir lever la suspension de leur compte devaient communiquer leur carte d'identité par courriel. la formation restreinte sanctionne cette transmission de données non chiffrées.

Infogreffe – 250.000€ - 8 septembre 2022

Le site web " infogreffe.fr " permet de consulter des informations légales sur les entreprises et de commander des documents certifiés par les greffes des tribunaux de commerce.

Manquements

- Manque de robustesse des mots de passe : 8 caractères sans aucun critère de complexité et ne sont associés à aucune mesure de sécurité complémentaire. En outre, le nombre de caractère maximum était de 8 de telle sorte qu'un utilisateur ne pouvait pas choisir d'améliorer la sécurité de son compte.

- Transmission en clair par courriel des mots de passe. Lesdits mots de passe n'étant pas temporaire, ils auraient pu être dérobés plus facilement par un attaquant.

- Les questions et réponses secrètes permettant de renouveler son mot de passe étaient également stockées en clair.

Discord – 800.000€ - 10 novembre 2022

Discord est un logiciel de VoIP et de messagerie instantanée permettant aux utilisateurs de créer leurs propres serveurs de discussion vocale ou écrite.

•Un manquement à l'obligation de garantir la protection des données par défaut.
Il est reproché à Discord de ne pas avoir prévu la fermeture des salons vocaux lorsque l'utilisateur ferme la fenêtre de l'application. En effet, le fait de fermer la fenêtre de l'application fait passer l'application en arrière-plan au lieu de la fermer complètement comme la plupart des applications de bureau. Par conséquent, l'utilisateur peut penser qu'il a quitté le salon vocal et donc s'exprimer librement, or tel n'est pas le cas, les autres membres du salon vocal pouvant toujours entendre l'entrée de son micro.

•Un manquement à l'obligation de sécurité. Le rapporteur a constaté qu'un mot de passe de six caractères était accepté, sans mesure de sécurité complémentaire. Ce système ne permettait pas de protéger l'accès au compte des utilisateurs.

Et c’est pas fini

Notification Cnil

Information des personnes concernées

Dépôt de plainte 23 aout 2023

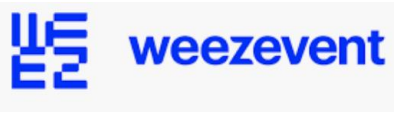
Registre des violations

racine
AVOCATS

PARTIE 3

Avant d’être une entités critiques / essentielles / importantes, vous êtes une « entité »

L’obligation de sécurité, vue système d’information (STAD)



L’obligation de sécurité, vue données personnelles

Sécurité des données à.caractère personnel

Article 32

Sécurité du traitement

1. Compte tenu de l’état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins:

a) la pseudonymisation et le chiffrement des données à caractère personnel;

b) des moyens permettant de garantir la confidentialité, l’intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l’accès à celles-ci dans des délais appropriés en cas d’incident physique ou technique;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l’efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

2. Lors de l’évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l’altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d’une autre manière, ou de l’accès non autorisé à de telles données, de manière accidentelle ou illicite.

L’obligation de sécurité, vue données personnelles

Article 35

Article 35

Analyse d’impact relative à la protection des données et consultation préalable

« Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires ».

L’obligation de sécurité, vue données personnelles

Délibération Darty

Article 28

Sous-traitant

1. Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée.

Pré-requis juridiques pour choisir un sous-traitant compliant

Audit du sous-traitant

L’obligation de sécurité, vue données personnelles

Article 28 3)

a) Traitement des données sur instruction documentée du responsable de traitement	b) Obligation de confidentialité des personnes qui « traitent » les données	c) Respecte les exigences de sécurité du règlement
d) Définition des règles de sous-traitance du sous-traitant	Encadrement par un contrat ou autre acte juridique liant le sous-traitant au responsable de traitement	e) Aide le responsable de traitement pour donner suite aux demandes d’exercice des droits des personnes concernées
f) Aide le responsable de traitement à assumer ses obligations de sécurité (sécurité + notification + communication)	g) Suppression ou renvoi des données au responsable de traitement au terme de la prestation (sauf si le droit de l’UE ou de l’Etat membre exige la conservation des données)	h) Mise à disposition du responsable de traitement des informations nécessaires pour apporter la preuve du respect de ses obligations et permettre la réalisation d’audits

racine
AVOCATS

PARTIE 4

Le cas particulier des acteurs critiques / essentielles / importantes

Installation d’importance vitale (OIV)

Article L1332-1 code de la défense

Les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, sont tenus de coopérer à leurs frais dans les conditions définies au présent chapitre, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative.

Article L1332-2 code de la défense

Les obligations prescrites par le présent chapitre peuvent être étendues à des établissements mentionnés à l'article L. 511-1 du code de l'environnement ou comprenant une installation nucléaire de base visée à l'article L. 593-1 du code de l'environnement quand la destruction ou l'avarie de certaines installations de ces établissements peut présenter un danger grave pour la population. Ces établissements sont désignés par l'autorité administrative.

Installation d'importance vitale (OIV)

Section 2 : Dispositions spécifiques à la sécurité des systèmes d'information (Articles L1332-6-1 à L1332-6-6)

Article L1332-6-1 code de la défense

Le Premier ministre fixe les règles de sécurité nécessaires à la protection des systèmes d'information des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 et des opérateurs publics ou privés qui participent à ces systèmes pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou pourrait présenter un danger grave pour la population. Ces opérateurs sont tenus d'appliquer ces règles à leurs frais.
Les règles mentionnées au premier alinéa peuvent notamment prescrire que les opérateurs mettent en œuvre des systèmes qualifiés de détection des événements susceptibles d'affecter la sécurité de leurs systèmes d'information. Ces systèmes de détection sont exploités sur le territoire national par des prestataires de service qualifiés en matière de sécurité de systèmes d'information, par l'autorité nationale de sécurité des systèmes d'information ou par d'autres services de l'Etat désignés par le Premier ministre.
Les qualifications des systèmes de détection et des prestataires de service exploitant ces systèmes sont délivrées par le Premier ministre.

Article L1332-6-2 code de la défense

Les opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 informent sans délai le Premier ministre des incidents affectant le fonctionnement ou la sécurité des systèmes d'information mentionnés au premier alinéa de l'article L. 1332-6-1.

Article L1332-6-3 code de la défense

A la demande du Premier ministre, les opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 soumettent leurs systèmes d'information à des contrôles destinés à vérifier le niveau de sécurité et le respect des règles de sécurité prévues à l'article L. 1332-6-1. Les contrôles sont effectués par l'autorité nationale de sécurité des systèmes d'information ou par des services de l'Etat désignés par le Premier ministre ou par des prestataires de service qualifiés par ce dernier. Le coût des contrôles est à la charge de l'opérateur

Opérateurs de service essentiel (OSE)

Les opérateurs, publics ou privés, offrant des services essentiels au fonctionnement de la société ou de l'économie et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux et systèmes d'information nécessaires à la fourniture desdits services sont soumis aux dispositions du présent chapitre. Ces opérateurs sont désignés par le Premier ministre. La liste de ces opérateurs est actualisée à intervalles réguliers et au moins tous les deux ans.

Les dispositions du présent chapitre ne sont pas applicables aux opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense, pour les systèmes d'information mentionnés au premier alinéa de l'article L. 1332-6-1 du même code.

Opérateurs de service essentiel (OSE)

Dispositions relatives à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels

Article 5 - Les opérateurs, publics ou privés, offrant des services essentiels au fonctionnement de la société ou de l'économie et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux et systèmes d'information nécessaires à la fourniture desdits services sont soumis aux dispositions du présent chapitre. Ces opérateurs sont désignés par le Premier ministre. La liste de ces opérateurs est actualisée à intervalles réguliers et au moins tous les deux ans.

Les dispositions du présent chapitre ne sont pas applicables aux opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense, pour les systèmes d'information mentionnés au premier alinéa de l'article L. 1332-6-1 du même code.

Article 6 - Le Premier ministre fixe les règles de sécurité nécessaires à la protection des réseaux et systèmes d'information mentionnés au premier alinéa de l'article 5. Ces règles ont pour objet de garantir un niveau de sécurité adapté au risque existant, compte tenu de l'état des connaissances. Elles définissent les mesures appropriées pour prévenir les incidents qui compromettent la sécurité des réseaux et systèmes d'information utilisés pour la fourniture des services essentiels ou pour en limiter l'impact afin d'assurer la continuité de ces services essentiels. Les opérateurs mentionnés au même article 5 appliquent ces règles à leurs frais.
Les règles prévues au premier alinéa du présent article sont définies dans chacun des domaines suivants :
1° La gouvernance de la sécurité des réseaux et systèmes d'information ;
2° La protection des réseaux et systèmes d'information ;
3° La défense des réseaux et systèmes d'information ;
4° La résilience des activités.
Les règles prévues au même premier alinéa peuvent notamment prescrire que les opérateurs recourent à des dispositifs matériels ou logiciels ou à des services informatiques dont la sécurité a été certifiée.

LOI n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité

Les fournisseurs de service numérique

Article 10

Pour l'application du présent chapitre, on entend :

1° Par service numérique tout service fourni normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services ;

2° Par fournisseur de service numérique toute personne morale qui fournit l'un des services suivants :

a) Place de marché en ligne, à savoir un service numérique qui permet à des consommateurs ou à des professionnels, au sens du dernier alinéa de l'article liminaire du code de la consommation, de conclure des contrats de vente ou de service en ligne avec des professionnels soit sur le site internet de la place de marché en ligne, soit sur le site internet d'un professionnel qui utilise les services informatiques fournis par la place de marché en ligne ;

b) Moteur de recherche en ligne, à savoir un service numérique qui permet aux utilisateurs d'effectuer des recherches sur, en principe, tous les sites internet ou sur les sites internet dans une langue donnée, sur la base d'une requête lancée sur n'importe quel sujet sous la forme d'un mot clé, d'une phrase ou d'une autre entrée, et qui renvoie des liens à partir desquels il est possible de trouver des informations en rapport avec le contenu demandé ;

c) Service d'informatique en nuage, à savoir un service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées.

Les PSCO – eIdas 1

Article 19 Exigences de sécurité applicables aux prestataires de services de confiance

1. Les prestataires de services de confiance qualifiés et non qualifiés p**rennent les mesures techniques et organisationnelles adéquates pour gérer les risques** liés à la sécurité des services de confiance qu'ils fournissent. Compte tenu des évolutions technologiques les plus récentes, ces mesures garantissent que le niveau de sécurité est proportionné au degré de risque. Des mesures sont notamment prises en vue de prévenir et de limiter les conséquences d'incidents liés à la sécurité et d'informer les parties concernées des effets préjudiciables de tels incidents.

2. Les prestataires de services de confiance qualifiés et non qualifiés **notifient, dans les meilleurs délais et en tout état de cause dans un délai de vingt-quatre heures après en avoir eu connaissance, à l'organe de contrôle** et, le cas échéant, à d'autres organismes concernés, tels que l'organisme national compétent en matière de sécurité de l'information ou l'autorité chargée de la protection des données, toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées. Lorsque l'atteinte à la sécurité ou la perte d'intégrité est susceptible de porter préjudice à une personne physique ou morale à laquelle le service de confiance a été fourni, le prestataire de services de confiance notifie aussi, dans les meilleurs délais, à la personne physique ou morale l'atteinte à la sécurité ou la perte d'intégrité. Le cas échéant, notamment lorsqu'une atteinte à la sécurité ou une perte d'intégrité concerne deux États membres ou plus, l'organe de contrôle notifié informe les organes de contrôle des autres États membres concernés ainsi que l'ENISA. L'organe de contrôle notifié informe le public ou exige du prestataire de services de confiance qu'il le fasse, dès lors qu'il constate qu'il est dans l'intérêt public de divulguer l'atteinte à la sécurité ou la perte d'intégrité.

3. Une fois par an, l'organe de contrôle fournit à l'ENISA un résumé des notifications d'atteinte à la sécurité et de perte d'intégrité reçues de prestataires de services de confiance. 28.8.2014 Journal officiel de l'Union européenne L 257/95 FR 4. La Commission peut, au moyen d'actes d'exécution: a) préciser davantage les mesures visées au paragraphe 1; et b) définir les formats et procédures, y compris les délais, applicables aux fins du paragraphe 2. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Les PSCO eIdas 1

Article 20 Contrôle des prestataires de services de confiance qualifiés

1. Les prestataires de services de confiance qualifiés font l'objet, **au moins tous les vingt-quatre mois, d'un audit effectué à leurs frais par un organisme d'évaluation de la conformité**. Le but de l'audit est de confirmer que les prestataires de services de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent remplissent les exigences fixées par le présent règlement. Les prestataires de services de confiance qualifiés transmettent le rapport d'évaluation de la conformité à l'organe de contrôle dans un délai de trois jours ouvrables qui suivent sa réception.

2. sans préjudice du paragraphe 1, l'organe de contrôle peut à tout moment, soumettre les prestataires de services de confiance qualifiés à un audit ou demander à un organisme d'évaluation de la conformité de procéder à une évaluation de la conformité des prestataires de services de confiance qualifiés, aux frais de ces prestataires de services de confiance, afin de confirmer que les prestataires et les services de confiance qualifiés qu'ils fournissent remplissent les exigences fixées par le présent règlement. L'organe de contrôle informe les autorités chargées de la protection des données des résultats de ses audits lorsqu'il apparaît que les règles en matière de protection des données à caractère personnel ont été violées.

3. Lorsque l'organe de contrôle exige du prestataire de services de confiance qualifié qu'il corrige un manquement aux exigences prévues par le présent règlement et que le prestataire n'agit pas en conséquence, et le cas échéant dans un délai fixé par l'organe de contrôle, l'organe de contrôle, tenant compte, en particulier, de l'ampleur, de la durée et des conséquences de ce manquement, **peut retirer à ce prestataire ou au service affecté le statut qualifié** et informe l'organisme visé à l'article 22, paragraphe 3, aux fins de la mise à jour des listes de confiance visées à l'article 22, paragraphe 1. L'organe de contrôle informe le prestataire de services de confiance qualifié du retrait de son statut qualifié ou du retrait du statut qualifié du service concerné.

Et tellement d’autres…

PHAROS
PLATEFORME D'HARMONISATION, D'ANALYSE, DE RECOUPEMENT ET D'ORIENTATION DES SIGNALEMENTS

HAS
HAUTE AUTORITÉ DE SANTÉ

AGENCE DU NUMÉRIQUE EN SANTÉ

arcep

ACPR
BANQUE DE FRANCE

ars
Agence Régionale de Santé

Exemple santé

JE DÉCLARE MES INCIDENTS

Depuis le 1er octobre 2017, le Ministère des Solidarités et de la Santé s'est engagé dans la lutte contre les cyberattaques dans le secteur santé, en mettant en place un dispositif de traitement des signalements des incidents de sécurité des systèmes d'information (SSI) des structures de santé. Pour mettre en œuvre cette stratégie nationale de sécurité numérique, il s'appuie sur l'Agence du Numérique en Santé et plus particulièrement sur sa **cellule d'Accompagnement Cyber sécurité des Structures de Santé (ACSS) rebaptisée CERT Santé en avril 2021, après sa reconnaissance en tant que CERT sectoriel pour le domaine de la santé par le CERT-FR.**
Il est indispensable de déclarer ses incidents de sécurité, d'une part pour protéger sa structure mais aussi pour éviter tous risques similaires à une autre structure de santé.

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

ANJ
AUTORITÉ NATIONALE DES JEUX

VOUS TROUVEZ CA COMPLIQUE ?

VOUS N'AVEZ ENCORE RIEN VU…