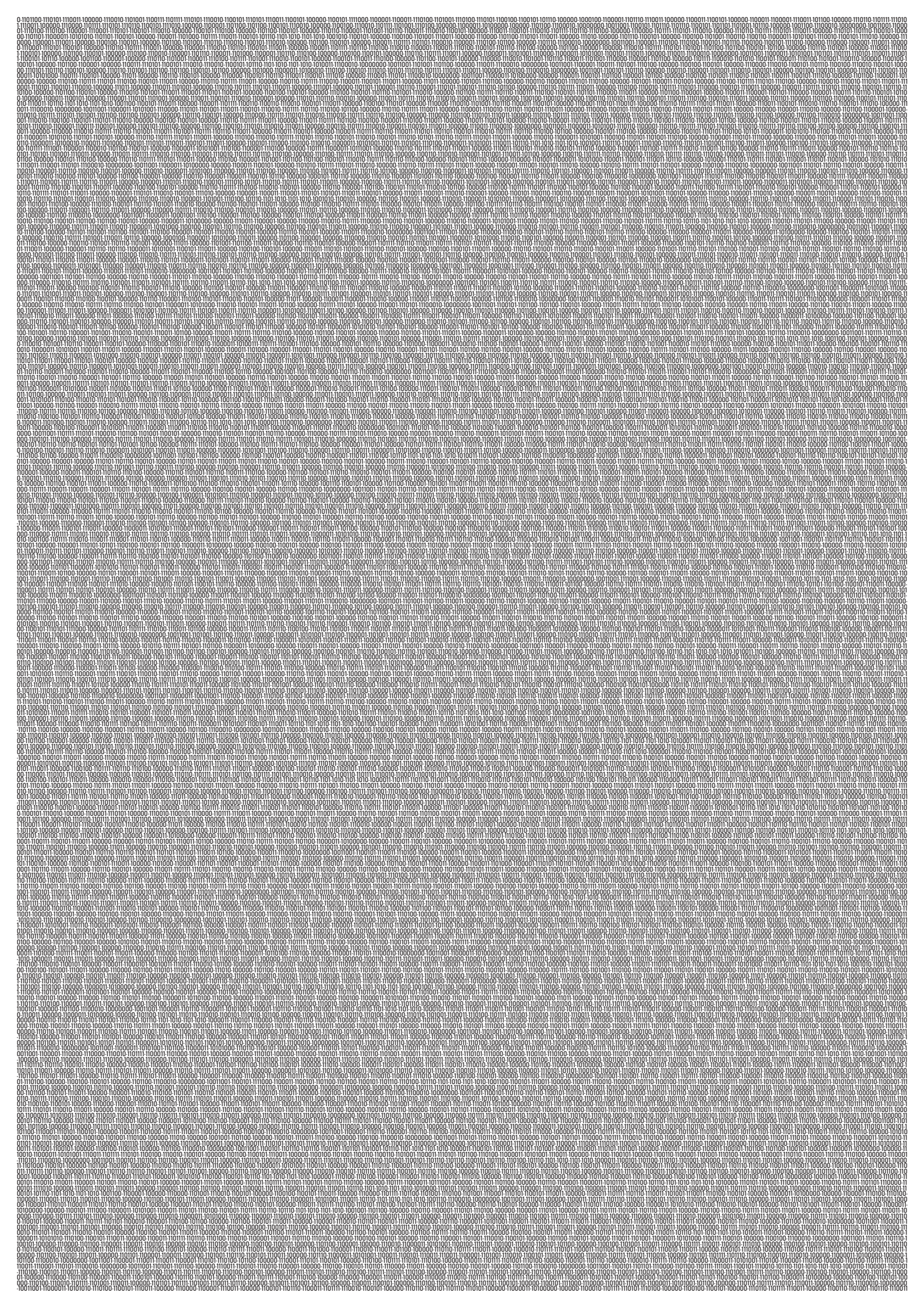
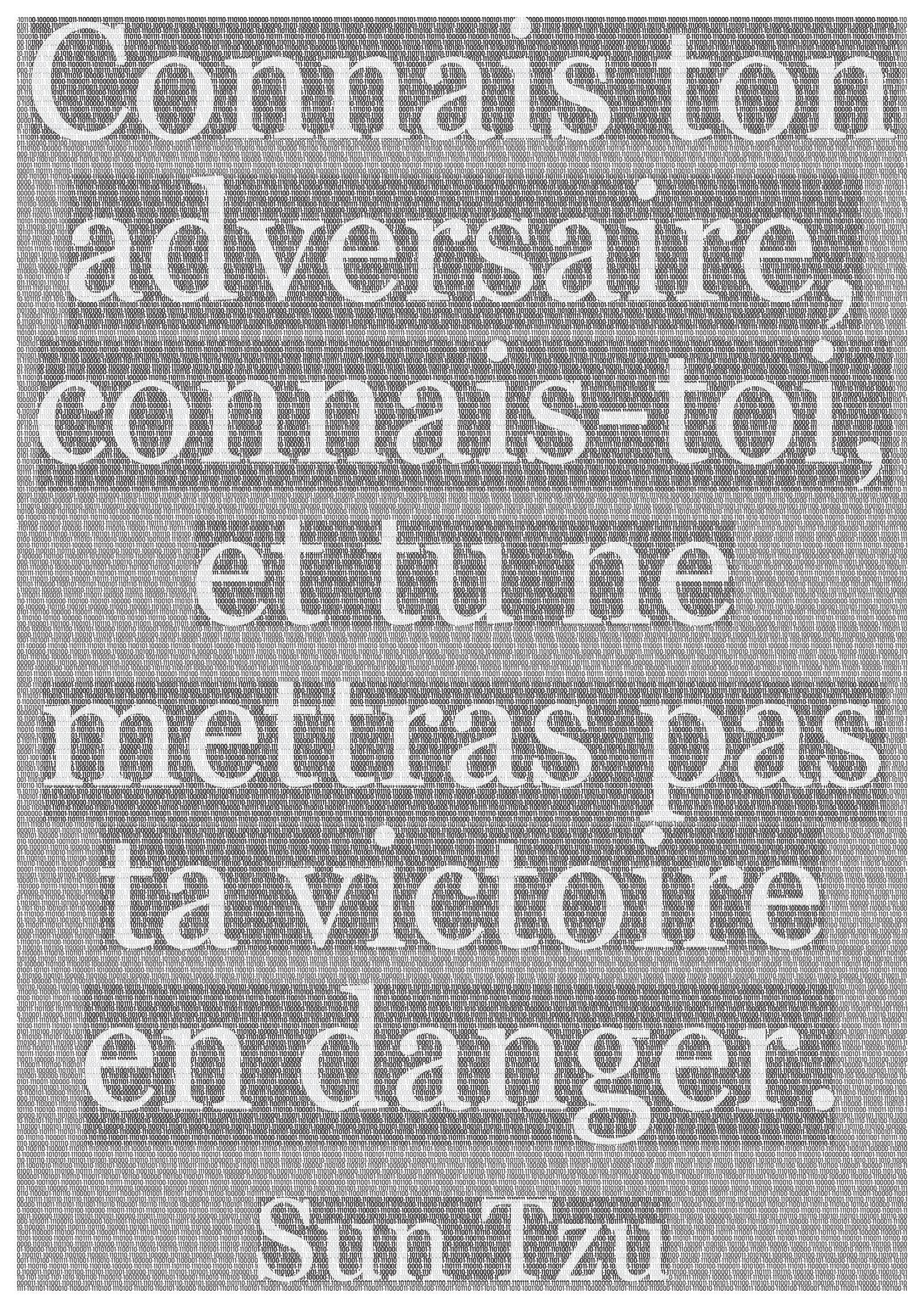
2023-2024

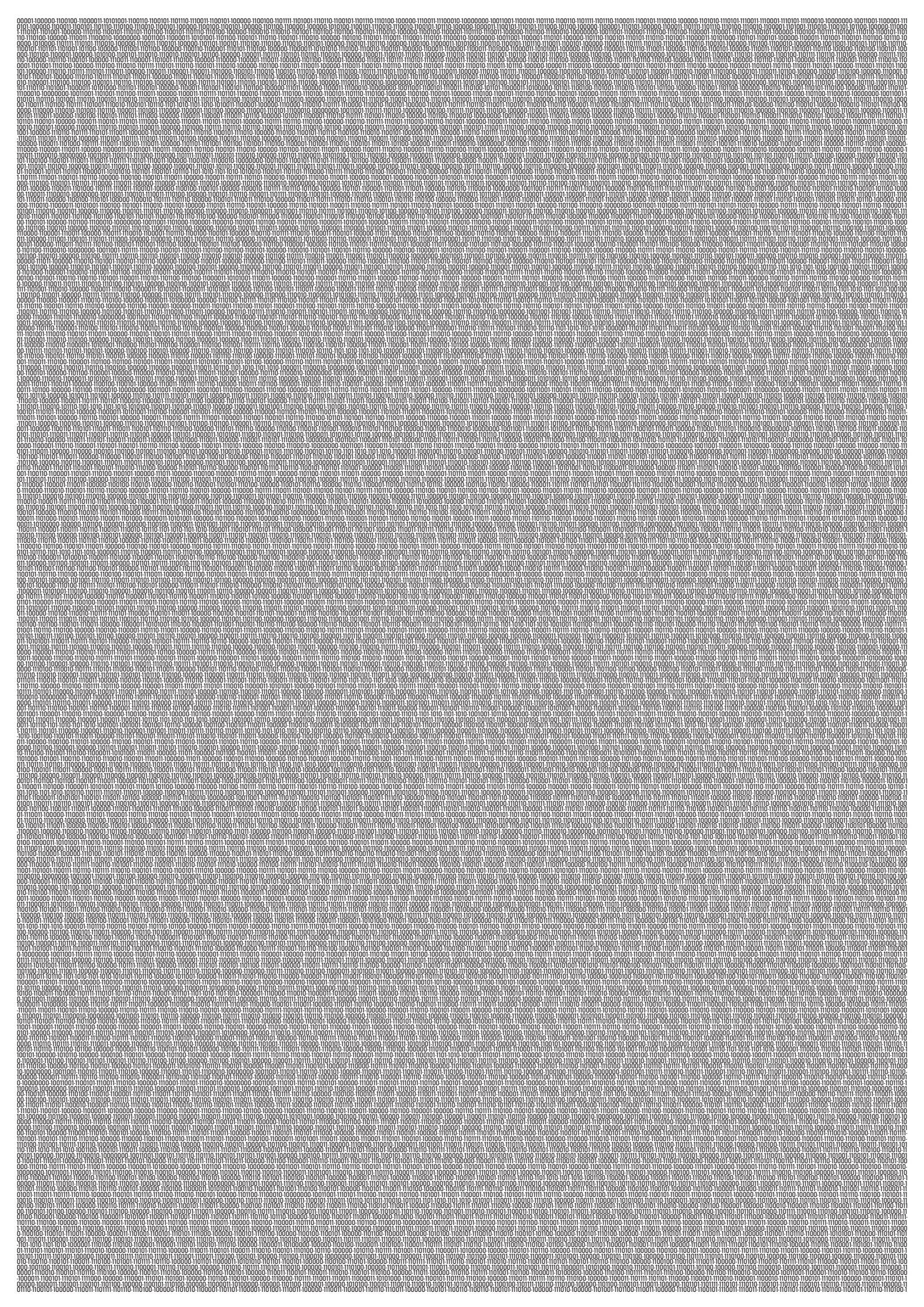
STEPHANIE ROUSSEAU & FABIEN CHANTREL – EILAD EXPERT
NADINE DE LA PALLIERE – UNIVERSITE BRETAGNE-SUD

PIERRE BERNFELD

LA SECURISATION DES DONNEES DANS LES CABINETS D'EXPERTISE COMPTABLE







« Tous connectés, tous impliqués, tous responsables. »

Manifeste de l'Agence nationale de la sécurité des systèmes d'information

« Le cyber est une priorité de Bercy !
D'ailleurs, "cyber", c'est "Bercy" à l'envers ! »

Olivia Grégoire, ministre déléguée chargée des Petites et moyennes entreprises, du Commerce, de l'Artisanat et du Tourisme, août 2023.

www.solutions-numeriques.com/93-des-tpe-et-pme-nont-pas-de-budget-dedie-cybersecurite-25-ont-une-couverture-assurance/

TABLE DES ABRÉVIATIONS ET SIGLES

AMRAE //
Association pour le management
des risques et des assurances de l'entreprise

ANSSI //
Agence nationale de la sécurité
des systèmes d'information

BIC //
Bénéfices industriels et commerciaux

BNC //
Bénéfices non commerciaux

CESIN //
Club des experts de la sécurité,
de l'information et du numérique

CNCC //
Compagnie nationale
des commissaires aux comptes

CNIL //
Commission nationale de l'informatique
et des libertés

CNOEC //
Conseil national de l'ordre
des experts-comptables

DGFiP //
Direction générale des finances publiques

DoS //
Deny of service (attaque par déni de service)

DPO //
Délégué à la protection des données

DSI //
Direction (ou directeur)
des systèmes d'information

GED //
Gestion électronique des documents

ITAC //
IT Application Control
(contrôles applicatifs)

ITGC //
IT general controls (contrôles informatiques
généraux)

LMNP //
Location meublée non professionnelle

MaaS //
Malware-as-a-Service

MEG //
Mon expert en gestion

MitM //
Man in the Middle

PCA //
Plan de continuité d'activité

PME //
Petites et moyennes entreprises

PRA //
Plan de reprise d'activité

OEC //
Ordre des experts-comptables

OGA //
Organisme de gestion agréé

RGPD //
Règlement général
sur la protection des données

RSSI //
Responsable de la sécurité
des systèmes d'information

SaaS //
Software-as-a-service

SASU //
Société par actions simplifiée
unipersonnelle

SI //
Système d'information

SMSI //
Système de management
de la sécurité de l'information

SQLi //
Injection SQL

TPE //
Très petite entreprise

SOMMAIRE

Il y a près de vingt ans, titulaire d'un master 2 en gestion et stratégie d'entreprise et d'un master 2 en lettres modernes, j'ai entamé une carrière dans l'édition, qui m'a comblé et passablement occupé pendant plus de 15 ans. En 2023, à la suite d'un licenciement économique, j'ai décidé d'opérer une réorientation professionnelle vers les métiers de la comptabilité. Je ne m'étendrai pas ici sur les multiples raisons ayant guidé ce choix, mais il a pour fondamentaux mon appétence pour les chiffres et le conseil, et la nécessité pour moi d'envisager un nouveau parcours professionnel au quotidien riche et varié, inscrit dans la vie locale.

Afin de mener à bien cette reconversion, j'ai décidé de postuler au master 2 « Comptabilité, contrôle et audit » de l'université de Bretagne-Sud (aujourd'hui IAE Bretagne-Sud), et ai eu la chance de voir ma candidature acceptée. À l'issue d'une période universitaire de près de 6 mois, j'ai effectué un stage de 4 mois dans le cabinet d'expertise comptable Eilad Expert, du 19 février au 7 juin 2024.

* * *

En décembre 2023, Coaxis, prestataire d'Eilad Expert hébergeant ses données, a subi une cyberattaque majeure, ce qui n'a pas été sans conséquences pour le cabinet et a suscité de sa part une réflexion de fond sur le sujet (toujours en cours à l'heure de bouclage du présent mémoire). La découverte de cet événement a confirmé l'intérêt et l'actualité du thème que j'avais choisi pour sujet de mémoire : la sécurité des données dans les cabinets d'expertise comptable.

Le présent travail s'inscrit dans le cadre du master 2 « Comptabilité, contrôle et audit », et présente une anatomie hybride : sa première partie sera concentrée sur un bref aperçu du stage réalisé chez Eilad Expert ; sa seconde partie s'intéressera à la problématique de la sécurisation des données dans les cabinets d'expertise comptable, dans un environnement où le numérique prend toujours plus de poids et où les diverses menaces lui étant liées évoluent sans cesse.

* * *

Je tiens à remercier ici le personnel enseignant de l'UBS, qui m'a accueilli avec une chaleureuse bienveillance et a fait preuve d'une grande disponibilité eut égard à mon parcours singulier. J'ai une pensée particulière pour Nadine de La Pallière, qui a accueilli ma candidature au Master 2 CCA (et, accessoirement, l'a acceptée), et est la tutrice sous l'égide de laquelle j'ai travaillé sur le présent mémoire.

Je remercie également les membres d'Eilad Expert, notamment Stéphanie Rousseau et Fabien Chantrel, les fondateurs du cabinet, qui ont fait le pari d'accueillir un profil atypique, Sébastien Kerouault, Mathieu Porchet, Laura Dudoret, Océane Galliot, Lionel Desdouets et l'inénarrable Loïc Parmentier, qui ont répondu à mes innombrables questions avec une patience remarquable.

Merci aussi à Anaïs et Arthur, qui ont tenu bon cette année, à Olive qui m'a soufflé les bons mots au bon moment, à Paul qui m'a inondé d'informations sans me noyer, et plus généralement à ma famille, mes amis et tous ceux qui m'ont aidé à franchir ce point de bascule professionnel qu'ont été les années 2023 et 2024.

Première partie

EILAD EXPERT

J'ai découvert Eilad Expert en rencontrant Fabien Chantrel et Sébastien Kerouault, à l'occasion d'une rencontre employeurs-étudiants organisée à l'université de Bretagne-Sud. Mon choix s'est rapidement porté sur Eilad Expert en raison de la typologie de clientèle du cabinet (plutôt TPE/PME, ce qui correspond à des réalités entrepreneuriales que j'ai pu approcher par le passé), de son approche centrée sur le besoin du client et le conseil, et de la vision entrepreneuriale de ses fondateurs, attachés au bien-être de leurs salariés et à la cohésion globale de l'équipe. De leur côté, les fondateurs d'Eilad Expert avaient eu plusieurs expériences positives de profils de reconversion, ce qui a sans doute favorisé ma candidature.

Ainsi, j'ai débuté un stage de découverte des métiers de la comptabilité le 19 février 2024, sous l'égide de Stéphanie Rousseau et Fabien Chantrel, experts-comptables et co-fondateurs du cabinet. L'objectif pour moi était d'appréhender le quotidien du métier, ses outils, ses enjeux. Grâce à la patience et au temps que m'ont accordé l'ensemble des membres du cabinet, j'ai pu en avoir un bon aperçu. Dans un premier temps, je présenterai Eilad Expert. Puis, je m'attarderai sur les missions qui m'ont été confiées et sur les outils grâce auxquels j'ai pu les mener à bien. Enfin, je conclurai cette première partie en évoquant ce que m'a apporté cette expérience de quelques semaines dans un cabinet d'expertise comptable.

1. Eilad Expert

Eilad Expert est un petit cabinet d'expertise-comptable fondé le 1er janvier 2020 par Stéphanie Rousseau et Fabien Chantrel, experts-comptables partenaires à la ville comme à la scène. Le cabinet a recruté son premier collaborateur l'année suivante, puis a grandi petit à petit pour atteindre une dizaine de membres en 2024 (dont une apprentie et un à deux stagiaires).

SITUATION AU REPERTOIRE SIRENE
À la date du 25/03/2024

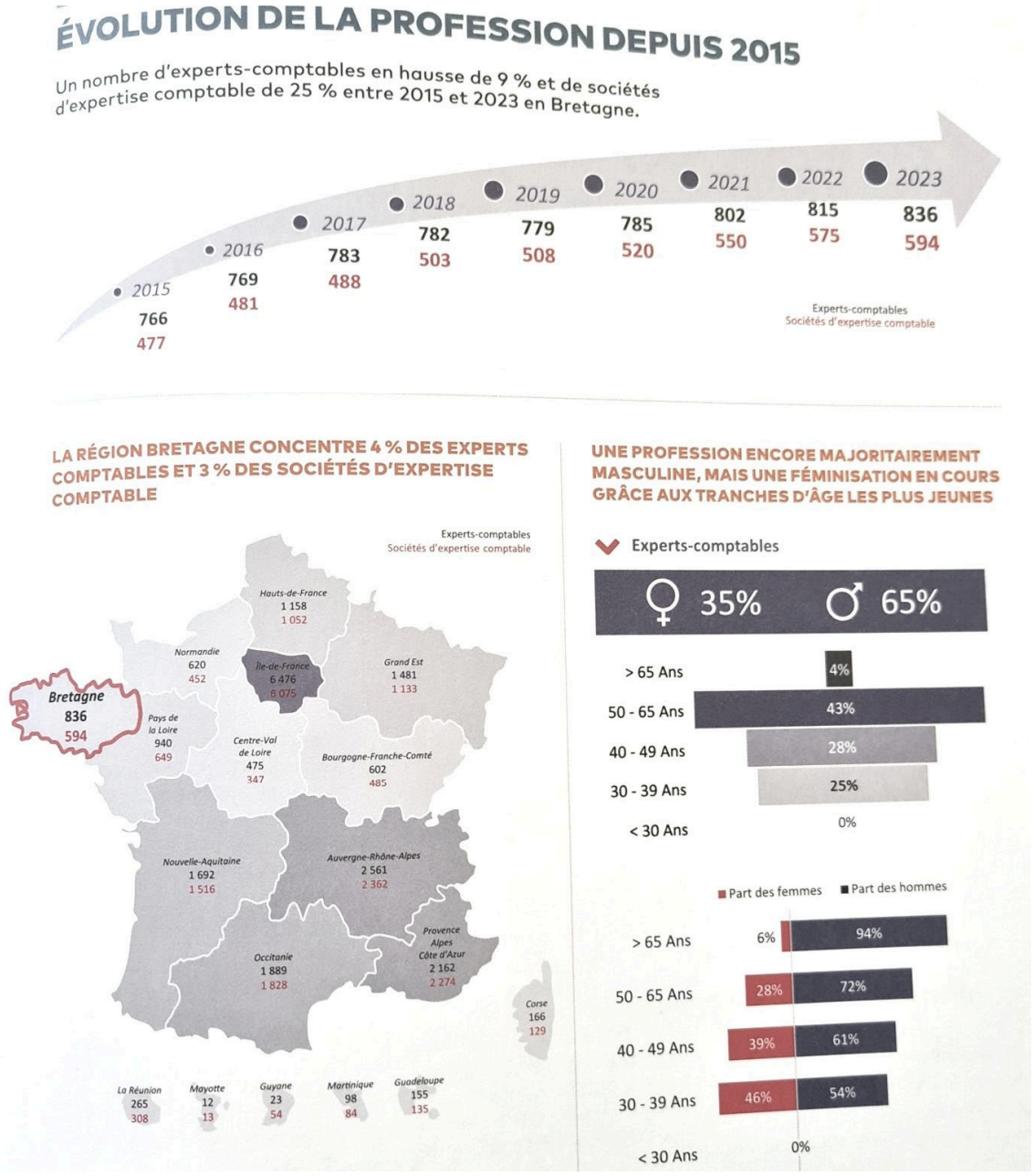
Description de l'entreprise	**Entreprise active depuis le 07/01/2020**
Identifiant SIREN	880 494 083
Identifiant SIRET du siège	880 494 083 00020
Dénomination	EILAD EXPERT
Catégorie juridique	5499 - Société à responsabilité limitée (sans autre indication)
Activité Principale Exercée (APE)	69.20Z - Activités comptables
Appartenance au champ de l'ESS[1]	Non
Appartenance au champ des sociétés à mission	

Description de l'établissement	**Etablissement actif depuis le 19/03/2021**
Identifiant SIRET	880 494 083 00020
Enseigne	EILAD EXPERT
Adresse	EILAD EXPERT 43 RUE GAL GIRAUD 56000 VANNES
Activité Principale Exercée (APE)	69.20Z - Activités comptables

EILAD
EXPERT
CONSEIL, GESTION, EXPERTISE-COMPTABLE

1.1. Le secteur

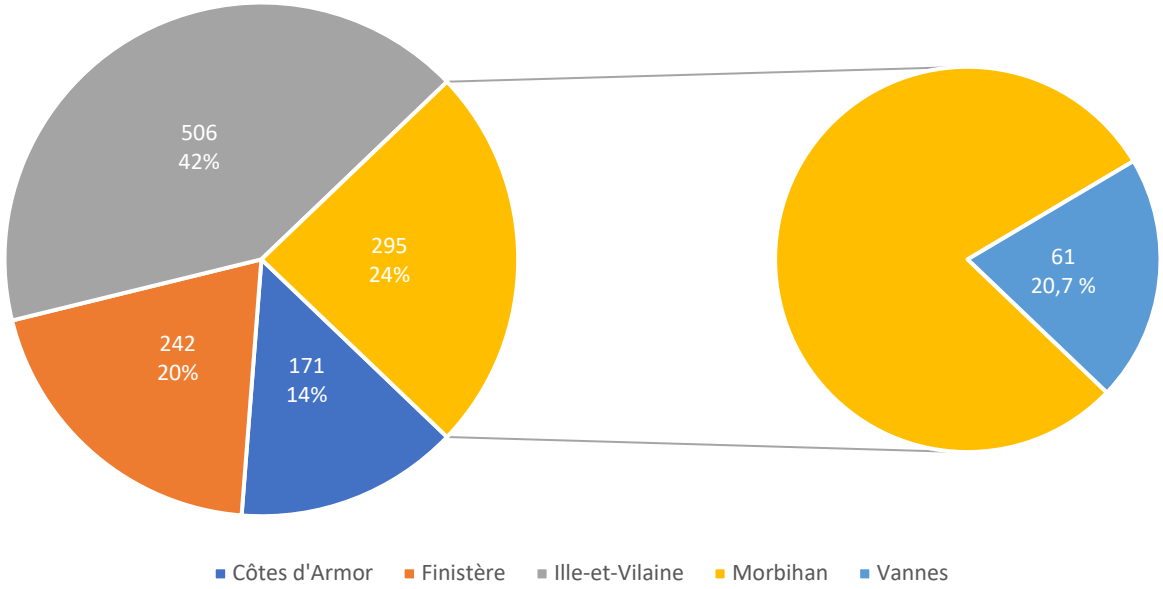
« De par ses compétences et son lien direct avec l'actualité économique et sociale des entreprises, l'expert-comptable contribue à la croissance des entreprises et au développement du tissu économique local[1]. » De fait, Eilad Expert s'inscrit dans un environnement dynamique qu'il contribue à vitaliser : l'expertise comptable en Bretagne. La profession est en constante évolution depuis 2015, et les inégalités de genre vont décroissant grâce aux nouvelles générations, même si d'importants progrès restent à faire sur ce sujet.



Source : Profession Experts, le magazine des experts-comptables de Bretagne, n° 143, mars-juin 2024.

[1] https://annuaire.experts-comptables.org/tous-les-cabinets-experts-comptables-par-region/bretagne.

Les cabinets d'expertise comptable en Bretagne sont répartis de la manière suivante[2] :



On note une prééminence de l'Ille-et-Vilaine, et une répartition plus harmonieuse sur le reste des départements bretons. Vannes, préfecture du Morbihan, abrite un peu plus de 20 % des cabinets du département.

1.2. La stratégie d'Eilad Expert

L'expertise comptable a aujourd'hui beaucoup de mal à recruter. Crise des vocations, sans doute, mais surtout pratiques managériales discutables conduisant à un *turnover* élevé. Le principal grief formulé à l'encontre des cabinets par les professionnels du secteur est la surcharge chronique de travail due à l'acceptation d'un trop grand nombre de dossiers par les associés.

Afin de fidéliser ses membres, Eilad a pris le parti de rompre avec les pratiques précitées et de n'accepter de clients que tant qu'ils peuvent effectivement être absorbés par les membres du cabinet. Cette stratégie produit plusieurs effets :

- **Au niveau des salariés :** bien-être conduisant à une fidélisation et à une grande implication. La bonne ambiance interne favorise également l'émulation de groupe. En 4 mois, je n'ai observé aucune situation de friction ou de concurrence interne. Au contraire, l'entraide est de mise et chacun des collaborateurs a son petit domaine de spécialité, ce qui permet de ne pas (trop) solliciter les associés ;

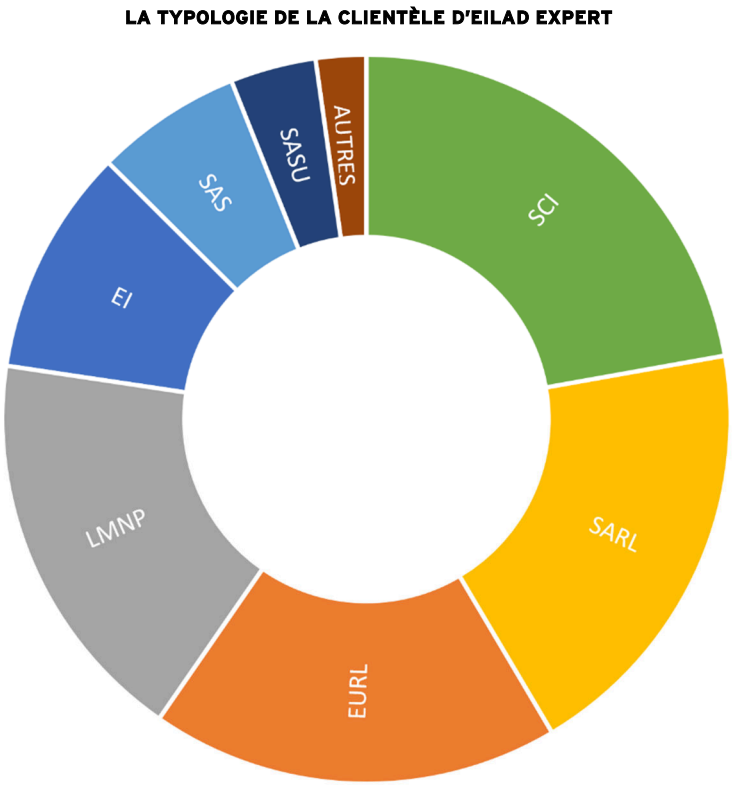
[2] https://annuaire.experts-comptables.org/tous-les-cabinets-experts-comptables-par-region/bretagne
(les données n'étant pas millésimées, on imagine qu'elles ne doivent pas avoir plus de 2 ans d'ancienneté).

- **Au niveau du cabinet :** croissance plus lente mais maîtrisée, meilleure connaissance de chaque dossier ;
- **Au niveau de la clientèle :** le cabinet ne surchargeant pas ses collaborateurs, ceux-ci ne sont pas poussés à l'abattage et ont le temps de s'occuper correctement des dossiers. Cet état de fait est perçu par la clientèle, qui se sent considérée et ainsi mise en confiance et fidélisée. On observe par ailleurs que cette attention portée à la clientèle fait de cette dernière le premier prescripteur du cabinet.

Eilad Expert place ses valeurs dans deux éléments indissociables : l'expertise et l'accompagnement. L'expertise est notamment assurée par le haut niveau d'expertise et l'implication des membres du cabinet. L'accompagnement, qui est son prolongement relationnel, est le credo du cabinet : son activité n'est pas simplement de produire des états financiers, mais de favoriser et d'accompagner le développement de ses clients.

1.3. La typologie de la clientèle

La clientèle d'Eilad Expert est principalement constituée de TPE. Du simple LMNP au groupe de sociétés, en passant par les activités libérales, ou les SARL réalisant plusieurs millions d'euros de chiffre d'affaires, elle se caractérise par sa taille humaine et son emplacement géographique, quasi exclusivement local.

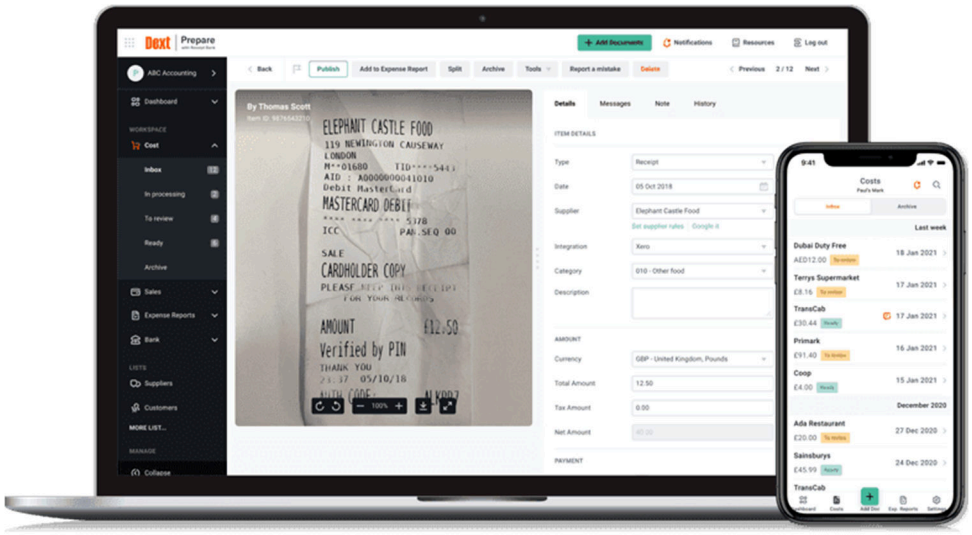


1.4. L'environnement applicatif

Afin de pouvoir se consacrer à cet accompagnement, Eilad Expert a choisi un écosystème applicatif impliquant de l'intelligence artificielle (par exemple, avec Dext pour la saisie des achats, ou Juriactes pour celle des actes juridiques). En ceci, le cabinet suit le mouvement général, tout en le devançant : sans bien connaître le monde de la comptabilité pour l'heure, j'ai cru comprendre que leur utilisation de l'intelligence artificielle est relativement plus poussée que la moyenne. Cela permet d'automatiser certaines tâches répétitives et chronophages pour concentrer les forces et l'énergie de l'équipe sur des taches à plus forte valeur ajoutée.

Plusieurs logiciels et applications interconnectés sont ainsi utilisés, parmi lesquels :

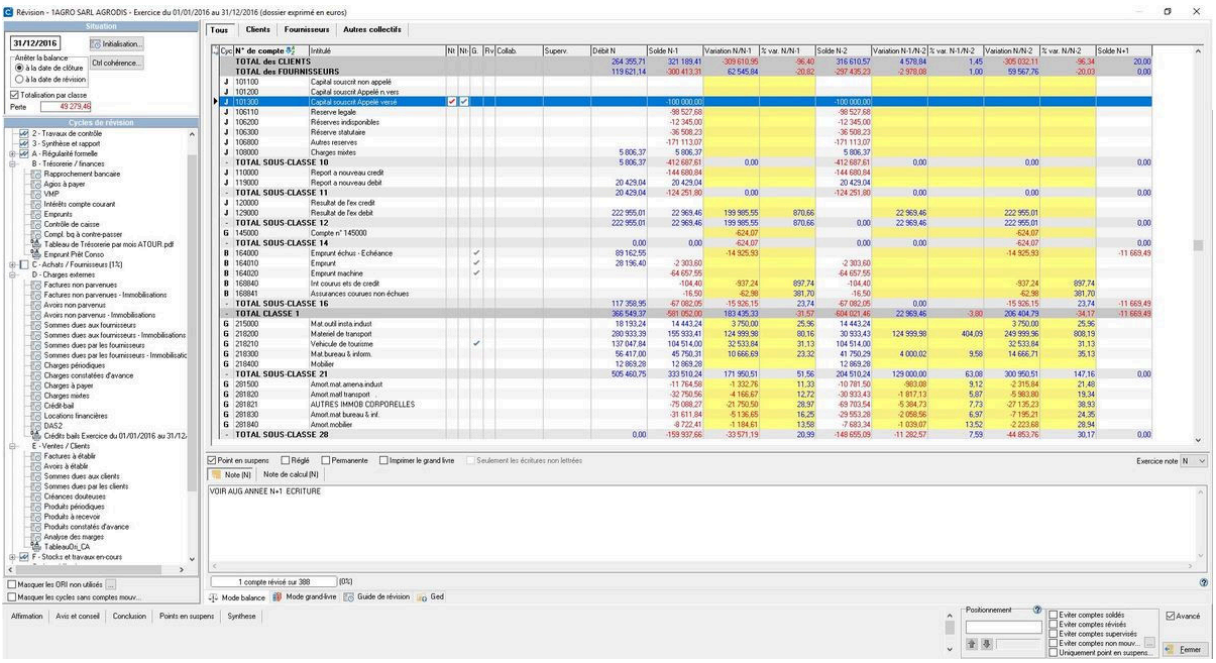
- **Dext :** un outil permettant aux clients de prendre en photo leurs factures, qui sont passées à la reconnaissance de caractère et, grâce à de l'intelligence artificielle (en partie en *machine learning*), enregistrées et comptabilisées presque sans intervention humaine dans le logiciel métier d'Eilad Expert



.

- **Mon Expert en Gestion (MEG) :** logiciel dont l'utilisation est suggérée au client pour créer et gérer ses devis, factures et avoirs. Cela permet au client de simplifier sa facturation, et au cabinet de récupérer facilement les ventes pour les intégrer dans son logiciel métier.

- iSuite Expert : une suite applicative en *software-as-a-service* (SaaS), dont les outils principaux sont la GED (gestion électronique des documents, sorte de coffre-fort abritant toutes les pièces comptables transmises par les clients ou enregistrées par les membres du cabinet) et Comptabilité Expert (l'outil de comptabilité et de production des états financiers).



Citons également les sites les plus utilisés dans le travail quotidien :

- Impots.gouv.fr
- Jedeclare.com
- Jesigneexpert.com
- Urssaf.fr
- Servi-paies.fr
- Pappers.com

2. Missions

Stéphanie Rousseau et Fabien Chantrel ont développé une méthode d'accueil de collaborateurs visant à favoriser leur apprentissage et à les responsabiliser. Cette méthode consiste à leur confier des dossiers qu'ils mèneront de A à Z, tout en étant accompagnés par le responsable du dossier – ainsi que par l'ensemble de l'équipe, chacun ayant son domaine d'expertise.

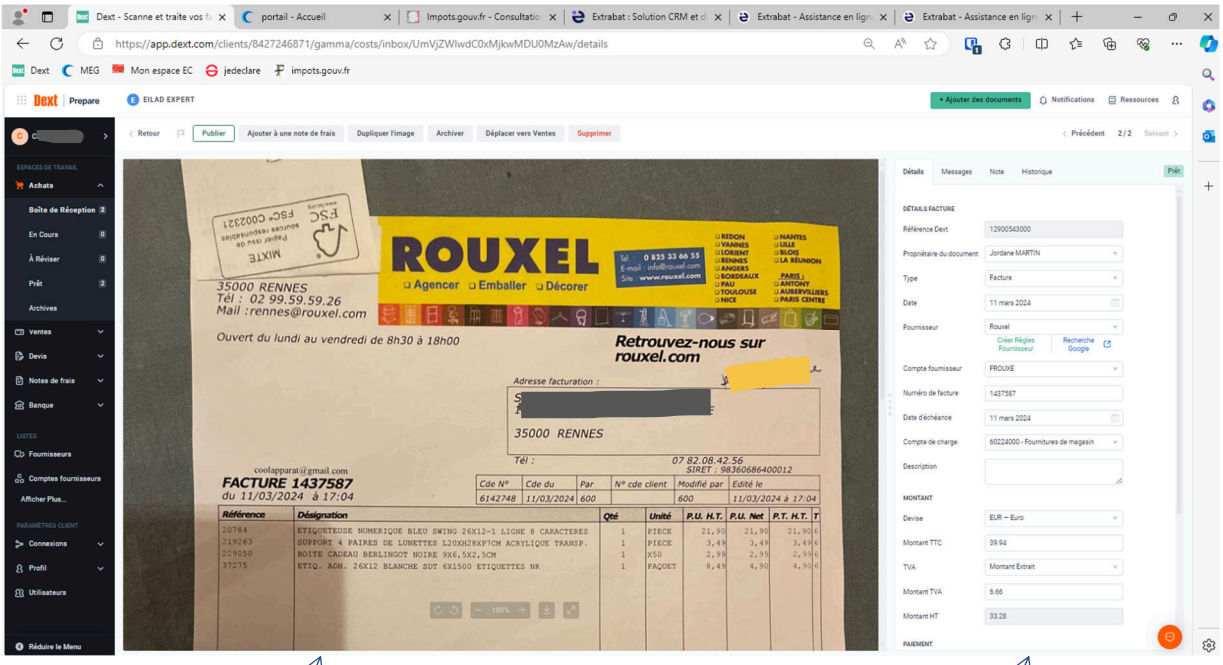
Les dossiers confiés sont au début relativement simples, et se complexifient par la suite au gré de l'évolution du collaborateur et éventuellement de ses affinités. Cette méthode permet de réellement comprendre l'enchaînement des tâches et missions conduisant de la saisie au rendez-vous de présentation des états financiers. Elle permet également une implication plus forte dans les dossiers, car le collaborateur, s'il n'est pas seul sur un dossier, en aura néanmoins une responsabilité sur la globalité de son traitement.

2.1. Apprentissage de l'environnement applicatif

Ma première tâche a été de commencer à apprivoiser l'environnement applicatif du cabinet. Pour ce faire, l'un des collaborateurs m'a initié aux applications Dext et MEG, ainsi qu'à l'utilisation d'ISuiteExpert (Comptabilité et GED).

Dext est très simple d'utilisation, très intuitif. L'objectif pour le collaborateur comptable est d'automatiser ses traitements au maximum, en créant des « règles », c'est-à-dire en « apprenant » au logiciel à imputer les factures dans les bons comptes comptables, ainsi qu'à paramétrer les TVA le cas échéant.

INTERFACE DEXT

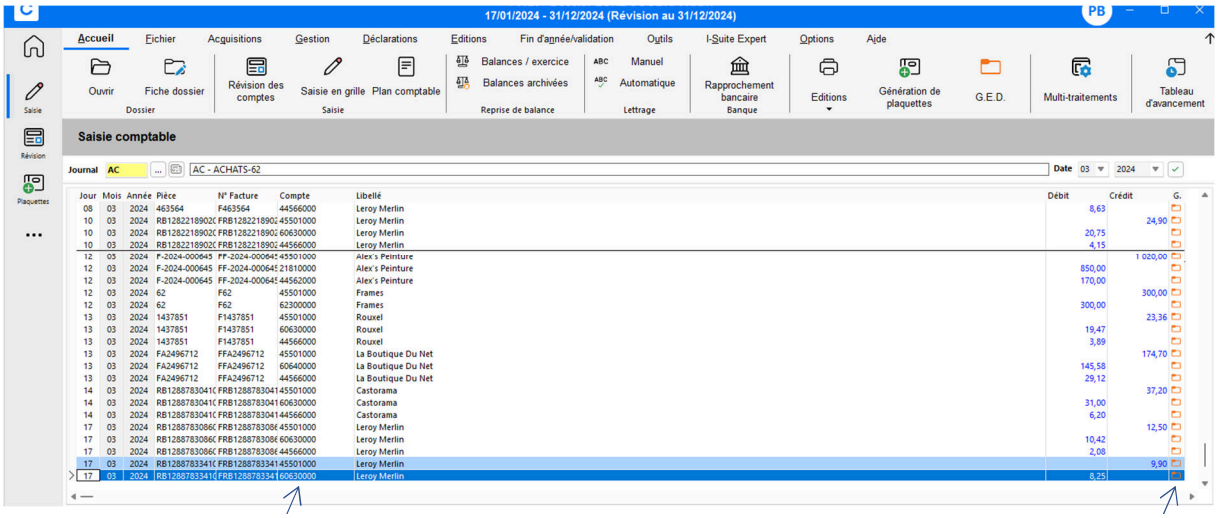


La facture originale prise en photo par le client

Les informations reconnues par Dext, paramétrables et modifiables, qui seront entrées en comptabilité

Ceci fait, le logiciel est d'une efficacité surprenante, et il ne reste qu'à vérifier son travail et à imputer les rares factures représentant des cas particuliers qu'il n'a pas su traiter (à noter tout de même que les paramétrages de la gestion de l'autoliquidation de TVA gagneraient à être plus intuitifs). Puis, d'un simple clic, les factures sont « publiées » en comptabilité, c'est-à-dire transférées dans le logiciel métier, produisant pour chacune d'elles l'écriture comptable correspondante, avec la photo de la facture en pièce jointe.

INTERFACE COMPTABILITÉ EXPERT

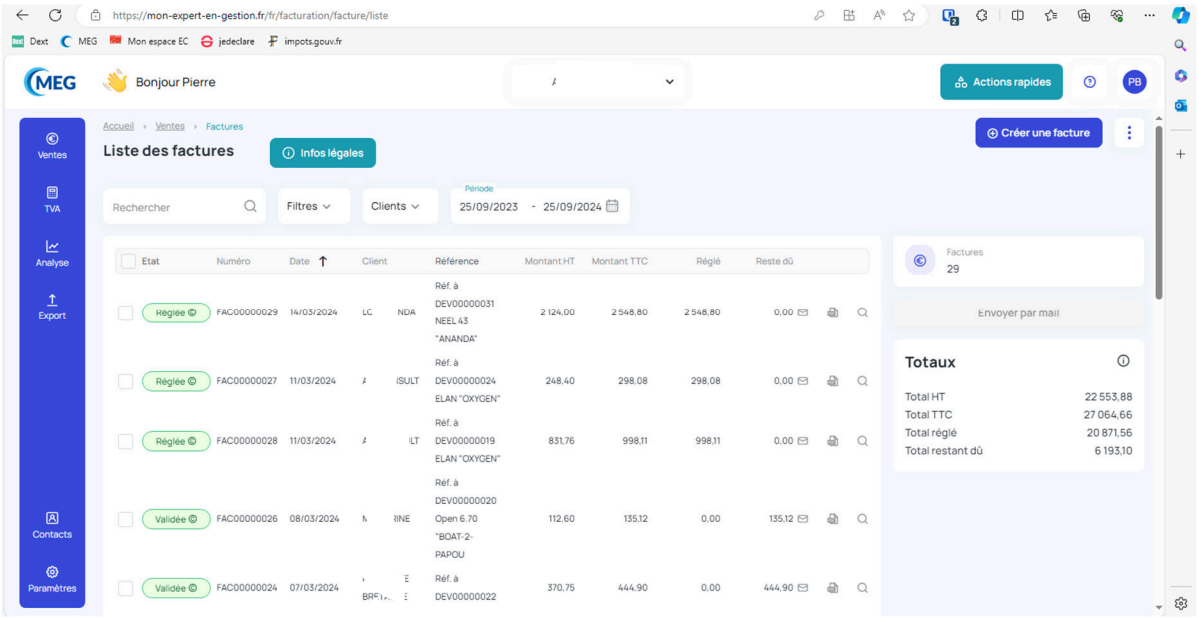


Imputation dans les bons comptes

Facture attachée à l'écriture et consultable sur un simple clic

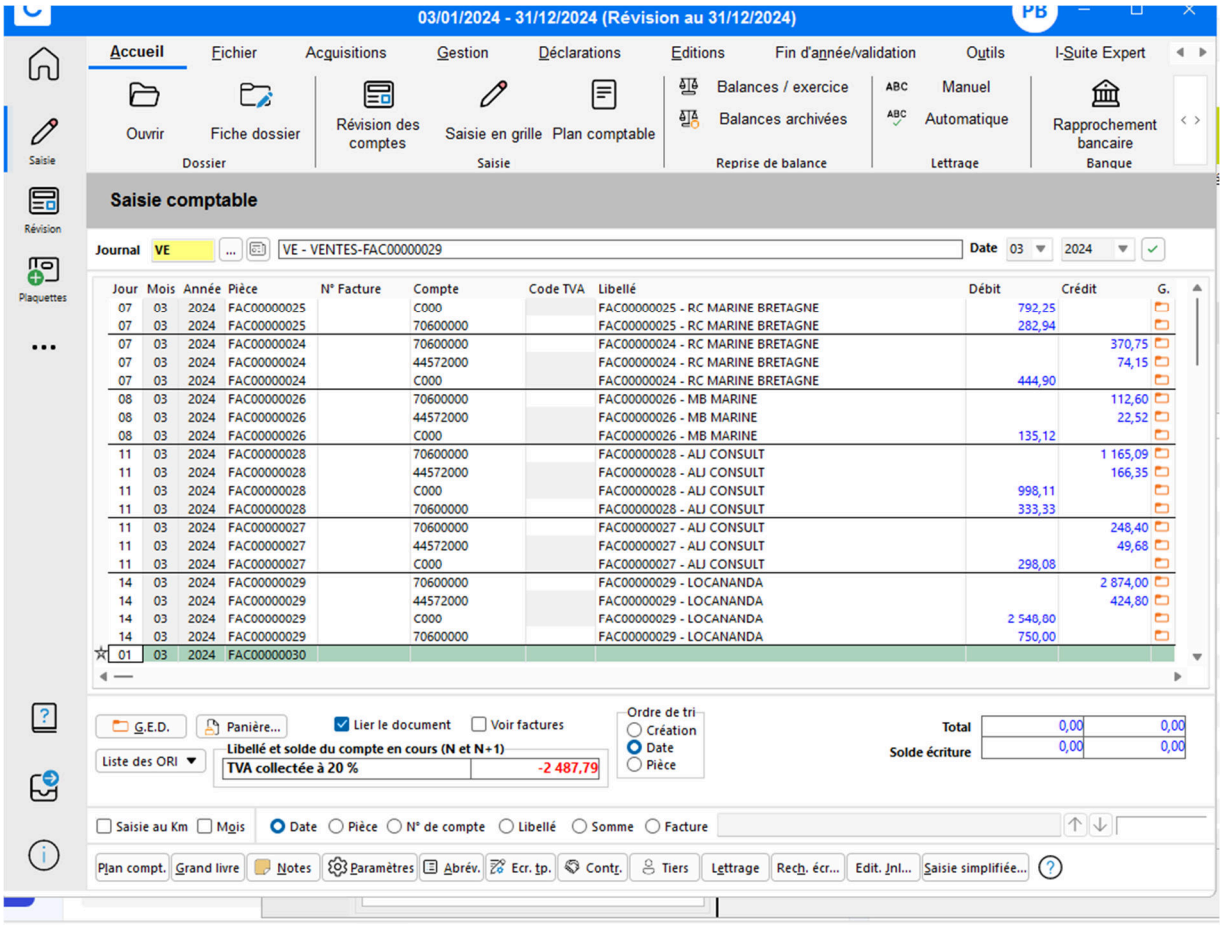
Le logiciel MEG est d'utilisation encore plus aisée, car il s'agit simplement de transférer les ventes en comptabilité. L'export réalisé, les écritures correspondantes sont automatiquement saisies dans le journal de vente, imputée au compte client et au compte de produit correspondants, avec les factures en pièces jointes.

INTERFACE MEG



À l'issue de l'import en comptabilité, un simple cadrage entre le total des comptes de produit et le total facturé inscrit sur MEG doit être opéré.

INTERFACE COMPTABILITÉ EXPERT



Parmi mes premières tâches a également figuré la saisie de relevés bancaires. Les relevés bancaires sont en général automatiquement importés en comptabilité (en liaison directe avec la banque du client, sans avoir d'import manuel à faire), avec des règles d'imputation réalisées au fil de l'eau par le collaborateur en charge du dossier permettant petit à petit d'automatiser presque intégralement le processus. Mais pour certains clients, la saisie est à faire manuellement, soit parce qu'il s'agit d'un nouveau client et que la liaison avec la banque n'est pas encore faite, soit par incompatibilité entre Comptabilité Expert et l'établissement de crédit du client.

Certains de ces rares relevés bancaires à saisir manuellement m'ont été confiés afin que je fasse mes armes en saisie. Cette activité m'a paru essentielle, car son côté répétitif permet de bien intégrer les règles comptables pour certaines imputations. Par ailleurs, elle nécessite de naviguer dans le logiciel métier, favorisant son appréhension. Enfin, la saisie représente la base de la matière de travail du comptable, et à ce titre constitue une entrée en matière permettant de « commencer par le commencement ».

À l'issue de cette saisie, un cadrage est réalisé en comparant simplement le solde du relevé bancaire avec le solde du compte idoine en comptabilité.

J'ai ensuite appris à « lettrer » les écritures afin d'identifier les pièces comptables manquantes et les imputations incertaines ou en compte d'attente, et afin de savoir quelles prestations sont réglées ou non pour les déclarations de TVA.

Par la suite, chacun des collaborateurs m'a confié des tâches, concentrées au début sur des dossiers de praticiens de santé sans TVA (BNC), afin que je me familiarise en douceur avec les outils, avant que Fabien Chantrel ne me confie mes premiers dossiers :

- Saisie de factures et relevés bancaires ;
- Importations Dext et MEG ;
- Lettrage ;
- Ventilation de cartes à débit différé ;
- Travail sur des fichiers Excel pour automatiser au maximum des retraitements d'informations reçues afin qu'elles puissent être intégrées avec un minimum d'interventions dans iSuiteExpert. Travail uniquement en formules car l'environnement ACD ne permet pas l'utilisation des macros dans la suite Office intégrée ;
- Suivi de collaborateurs chez des clients :
    - Dans une entreprise de construction pour un bilan de clôture avant cession de l'entreprise ;
    - Dans une entreprise de transport pour réaliser la saisie des éléments nécessaires à la déclaration mensuelle de TVA.

2.2. Missions

Le portefeuille qui m'a été confié par Fabien Chantrel était au départ constitué de six sociétés[3], dont deux en TVA mensuelle, deux en TVA annuelle, une hors champ de TVA et une en franchise de base. Cinq d'entre elles sont des SARL évoluant dans la prestation de service, la dernière étant une holding en SASU (gestion de titres).

J'ai créé leur dossier interne grâce aux procédures mises en place par Stéphanie Rousseau. Celles-ci, découpées par phases (accueil client, en cours d'exercice, clôture) et très détaillées, permettent de s'assurer de la complétude des éléments récoltés par rapport aux obligations légales, aux diligences et éléments nécessaires pour le traitement opérationnel des dossiers.

Elles servent à la fois à se dégager de certaines responsabilités et à prévoir en amont les éléments qui seront indispensables afin de ne pas avoir par la suite à réclamer en urgence des pièces oubliées.

J'ai fait mes premières déclarations de TVA (CA3) sur mes dossiers en TVA mensuelle les 19 et 20 mars. Pour déclarer la TVA, il y a deux méthodes : soit directement dans le logiciel métier, qui passe ensuite par jedeclare.com pour transmettre la déclaration à la DGFiP, puis passe automatiquement les écritures de déclaration, soit directement sur impots.gouv.fr, via l'interface professionnelle de chacun des comptes clients. C'est cette seconde solution que j'ai choisie,

[3] Par la suite, il en comportera une quinzaine, attribués par Stéphanie Rousseau ou Fabien Chantrel.

car elle me permettait de remplir le cerfa CA3, puis de passer les écritures à la main[4]. Étant moins automatisée, elle me permettait donc de mieux me familiariser avec le processus.

À l'issue de la déclaration, j'ai envoyé les informations aux clients, afin qu'ils sachent à quoi s'attendre. En l'occurrence, l'un était en crédit de TVA, et pour l'autre, j'ai demandé un remboursement de TVA.

Plusieurs autres dossiers m'ont été confiés au fil des arrivées de nouveaux clients. Je réalisais la mise en place (préparation des lettres de mission, récolte des éléments auprès des clients, tâches administratives, ouverture des comptes impot.gouv, Urssaf et création des différents mandats pour le cabinet, pour jedeclare, pour les impôts...). Par la suite, j'ai géré mes dossiers chaque mois, répondant aux clients, leur demandant des informations et pièces manquantes, comptabilisant leurs opérations. J'ai également fait les déclarations Decloyer, CVAE et DAS2 sur plusieurs dizaines de dossiers.

Enfin, j'aidais également les autres collaborateurs sur leurs dossiers (notamment des BNC, des commerçants, des concessions avec TVA sur marge, des entreprises dans le bâtiment, des holdings...).

2.3. Formations

Au cours de mon stage, j'ai eu la chance de suivre plusieurs formations pour dépoussiérer et approfondir mes connaissances.

J'ai ainsi suivi des formations courtes (1h30 à 4h) sur les sujets suivants :

- Formations sur la comptabilité des LMNP ;
- Formations sur la comptabilité et la déductibilité des frais des BNC ;
- Formation à la 2042 et à la 2042C Pro.

Suivies en visioconférence auprès de l'organisme de gestion agréé Arcolib, ces conférences étaient prodiguées par des professionnelles, interactives et pour certaines vraiment complètes.

2.4. Expérience de stage

Ce stage a été d'une grande richesse pour moi. D'une part, il a, à mon sens, réalisé son objectif, à savoir m'offrir un aperçu du métier et m'en faire découvrir les bases. D'autre part, il m'a permis d'apprendre au contact d'une équipe hétérogène mais très soudée, sympathique, dynamique et dotée d'un fort niveau d'expertise.

[4] Par la suite, j'ai réalisé les déclarations directement depuis le logiciel métier, ce qui simplifie le cadrage de TVA au moment de clore l'exercice.

N'ayant jamais fait de comptabilité auparavant, j'ai pu en appréhender quelques codes, bonnes pratiques et bons réflexes.

Je pense avoir identifié que les qualités essentielles dans ce métier sont la rigueur, la polyvalence et la capacité à passer du coq à l'âne sans en être déstabilisé. En cela, il est très proche du métier d'éditeur que j'ai exercé par le passé.

Outre mes compétences professionnelles, j'ai pu mettre en application diverses connaissances acquises au cours de ma formation en master 2 « Comptabilité, contrôle et audit » : notamment ce qui relève de la fiscalité, du droit et de la comptabilité, mais également des autres matières, qui ont constitué pour moi un corpus de culture générale me permettant de percevoir les enjeux du métier et de ses tâches.

Si les points forts de mon stage sont nombreux (l'équipe, le travail, une typologie de clientèle variée, locale, à taille humaine), j'ai du mal à y voir des points faibles. La principale difficulté que j'ai rencontrée est que, n'ayant jamais fait de comptabilité auparavant, le démarrage a été difficile lorsqu'il m'a fallu mettre en pratique des règles que je connaissais sans en avoir une maîtrise empirique au moyen d'outils informatiques complexes (si Dext et MEG sont simples d'utilisation, il faut plus de temps pour se familiariser avec iSuiteExpert). Toutefois, grâce à la grande disponibilité de l'équipe (y compris, fait notable, des associés), à leurs conseils et astuces, cette difficulté s'est résorbée petit à petit, et l'outil est passé du statut de contrainte à celui de ressource.

Cette découverte de la comptabilité m'a donc permis d'aborder le métier de façon relativement panoramique s'agissant d'une comptabilité de petit cabinet à vocation locale. Motivants et inspirants, ses fondateurs et ses collaborateurs m'ont accueilli avec bienveillance et patience, et je les en remercie vivement.

Seconde partie

LA SÉCURISATION DES DONNÉES DANS LES CABINETS D'EXPERTISE COMPTABLE

« Tout le succès d'une opération
réside dans sa préparation. »

Sun Tzu, *L'Art de la guerre*, 1078

AVERTISSEMENTS

Nous nous intéresserons ici aux tenants et aboutissants de la sécurisation des données en ne mentionnant de détails techniques que ceux nécessaires à la compréhension du sujet.

Les chiffres étant relativement lacunaires du fait d'un manque de statistiques (nous en verrons les raisons), ceux ayant spécifiquement trait aux cabinets d'expertise comptable sont pour leur part quasi inexistants. Nous nous efforcerons donc d'inférer et d'extrapoler sur la globalité du sujet eu égard aux spécificités des entreprises d'expertise-comptable.

Par ailleurs, si notre clavier nous conduira parfois à nous égarer dans le monde, nous nous intéresserons principalement aux entreprises françaises.

Les encadrés bleus figurant dans le corpus du mémoire sont des citations. Leur mise en exergue graphique en nous a parfois conduit à l'économie de leur mise entre guillemets.

Les références ne faisant mention que d'un patronyme suivi d'une date renvoient à la source concernée dans la partie « Livres » de la bibliographie.

Dans un monde tendant peu à peu vers le tout-numérique, les données gagnent en importance chaque jour. D'après l'étude *Data & AI Leadership Executive Survey*[5], 49 % des entreprises considèrent les données comme un atout stratégique et 48 % affirment avoir mis en place une approche pilotée par les données (« *data-driven* »), ce qui représente un doublement en un an. Face à cette intensification, de nombreuses législations ont vu le jour, encadrant la collecte, l'utilisation ou encore le stockage de certaines informations. Si la loi oblige aujourd'hui les entreprises à protéger certaines de leurs données, celles-ci mettent en place des stratégies de sécurisation plus globales pour faire face au risque accru de fuite, corruption ou perte de données.

LA SÉCURITÉ INFORMATIQUE EN 2021

- Dans le monde, 4 000 attaques informatiques visant des entreprises ont lieu chaque jour et 94 % des responsables de sécurité des entreprises déclarent qu'au cours des 12 derniers mois, leur entreprise a fait l'objet d'une cyberattaque.
- En France, en 2017, les PME et TPE étaient la cible de 77 % des cyberattaques selon le Syntec Numérique, le syndicat des entreprises du numérique.

Face à ces menaces, les PME/TPE sont moins préparées et plus vulnérables.

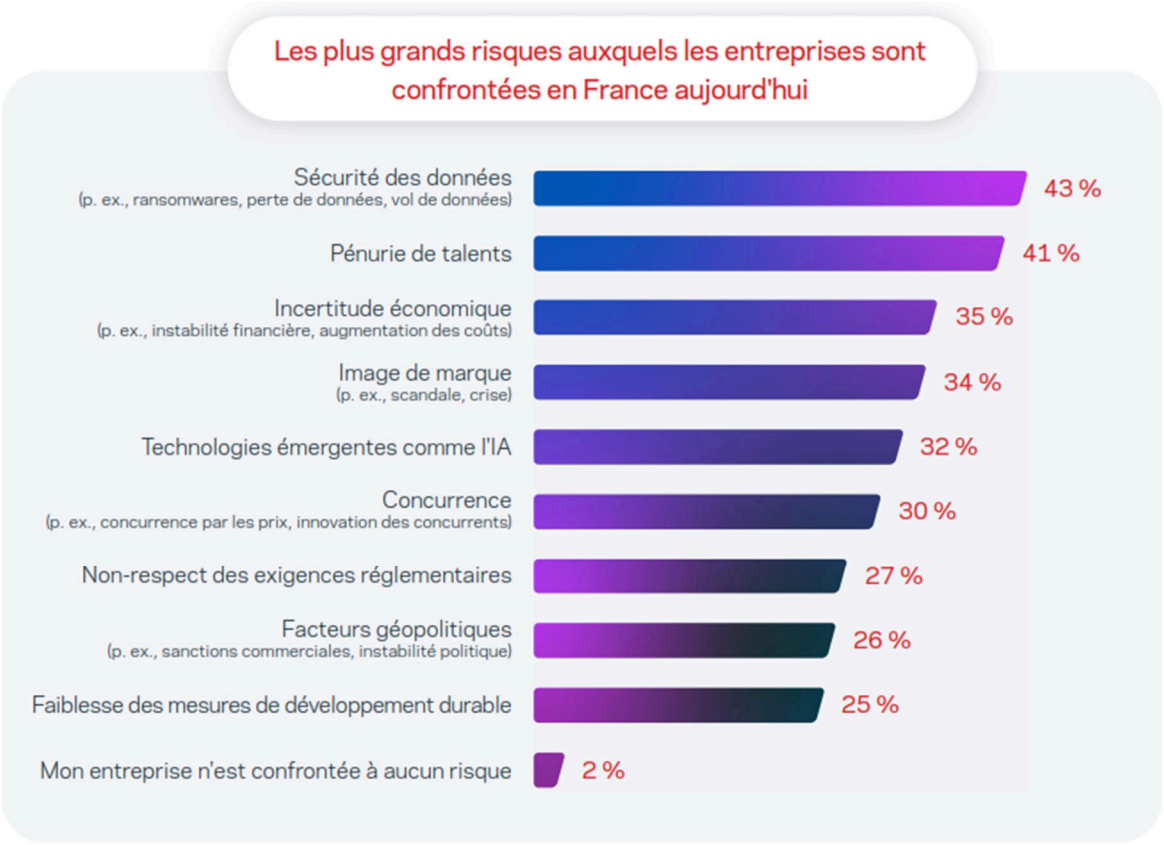
www.senat.fr/travaux-parlementaires/office-et-delegations/delegation-aux-entreprises/archives-1/la-problematique-de-la-cybersecurite-dans-les-entreprises.html

La question de la sécurisation des données et des systèmes d'information qui les brassent est donc de plus en plus prégnante et complexe. Aux aléas accidentels que représentent les sinistres ou les erreurs humaines et à ceux relevant du sabotage interne s'ajoutent trois menaces majeures :

- Les attaques à des fins géostratégiques (attaques de groupes plus ou moins structurés avec le soutien actif ou passif d'un État visant à déstabiliser un acteur ou un pan économique pour mettre un autre État en difficulté) ;
- Les menaces à des fins d'extorsion, de recel ou de sabotage ;
- La menace relevant de l'intelligence économique (espionnage industriel notamment).

En 2020, 90 % des organisations françaises ont été visées par des cyberattaques[6]. Ces menaces s'intensifient considérablement et exponentiellement avec la numérisation du monde et des entreprises, comme en témoigne l'actualité récente. En France, parmi les dernières en date, citons celle visant des gestionnaires de tiers payant de la sécurité sociale ayant compromis les données de près de la moitié de la population française début 2024[7], ou encore, en décembre 2023, la cyberattaque par le rançongiciel Lockbit 3.0 sur les systèmes de l'hébergeur Coaxis, affectant plus de 1 200 cabinets d'expertise comptable[8] (sur les quelque 18 000 cabinets recensés en France par l'OEC en 2021[9]).

[5] www.wavestone.com/app/uploads/2023/12/DataAI-ExecutiveLeadershipSurveyFinalAsset.pdf.
[6] www.novethic.fr/actualite/economie/economie/isr-rse/entre-les-vaccins-le-covid-19-et-le-teletravail-2020-a-ete-l-annee-des-cyberattaques-149341.html.
[7] www.lesechos.fr/industrie-services/pharmacie-sante/numero-de-secu-mutuelle-33-millions-de-francais-victimes-dune-cyberattaque-au-tiers-payant-2074842.
[8] www.dpo-partage.fr/cyberattaque-de-coaxis.
[9] www.revuefrancaisedecomptabilite.fr/la-profession-comptable-en-chiffres.



Gestion des risques liés aux données, *rapport France 2023, Veritas*

Dans ce contexte, la sécurisation des données devient essentielle, notamment dans les cabinets d'expertise comptable qui manient des données confidentielles de leurs clients. Nous verrons dans un premier temps ce que sont les données et pourquoi elles doivent être protégées. Dans un deuxième temps, nous nous intéresserons aux mesures qu'il est possible de mettre en place à titre préventif ou curatif pour répondre au besoin croissant de sécurisation des données. Enfin, nous nous intéresserons à deux cas d'étude de cybermalveillance : le piratage d'un cabinet d'expertise comptable et le piratage d'un prestataire hébergeant les données de cabinets d'expertise comptable.

ESTIMATIONS POUR LE FUTUR PROCHE

- 90% de la population humaine âgée de plus de 6 ans aura une activité en ligne d'ici 2030, soit 7,5 milliards d'individus (environ 1 million d'utilisateurs supplémentaires chaque jour sur Internet).
- 10 500 milliards $ de dommages liés à la cybercriminalité d'ici 2025.
- Dépenses cumulées liées à la cybersécurité de 17 500 milliards $ sur la période 2021-2025.
- Les dégâts liés aux rançongiciels devraient excéder 265 milliards $ d'ici 2031.
- Le monde aura besoin de protéger des risques cyber plus de 200 zettabits (environ 1 milliard de Tb) de données d'ici 2025.
- Le marché assurantiel lié à la cybersécurité devrait atteindre 14,8 milliards $ annuels d'ici 2025.

https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025

1. Des ressources sensibles et précieuses

1.1. La notion de donnée

1.1.1. Une information à confidentialité variable

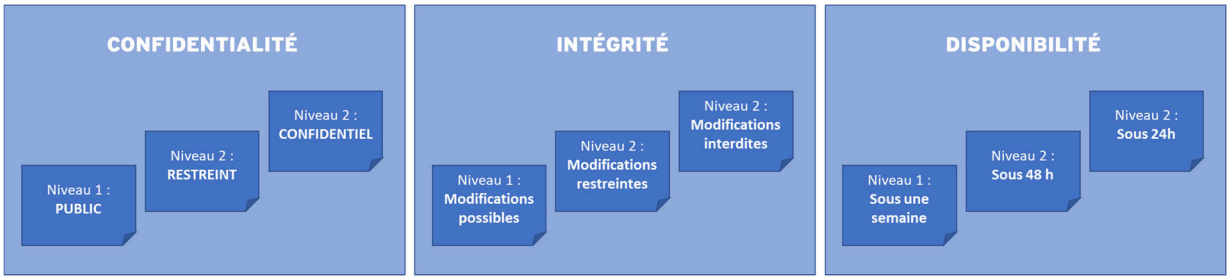
1.1.1.1. Définition

Dans le cadre du présent travail, la notion de « données » fait référence aux données numériques, c'est-à-dire la « description élémentaire d'une réalité[10] ». En d'autres termes, une information à partir de laquelle peuvent être effectués des traitements. Cette information doit être acquise ou produite, stockée, protégée, utilisée, puis conservée (en vue d'archivage, de réutilisation), cédée et/ou détruite.

1.1.1.2. Caractéristiques

Une donnée possède plusieurs caractéristiques : un type (quantitatif, qualitatif, physique, numérique), un format, un support de stockage, une criticité (importance pour l'utilisateur ou l'entreprise), des droits d'accès et des moyens d'accès[11].

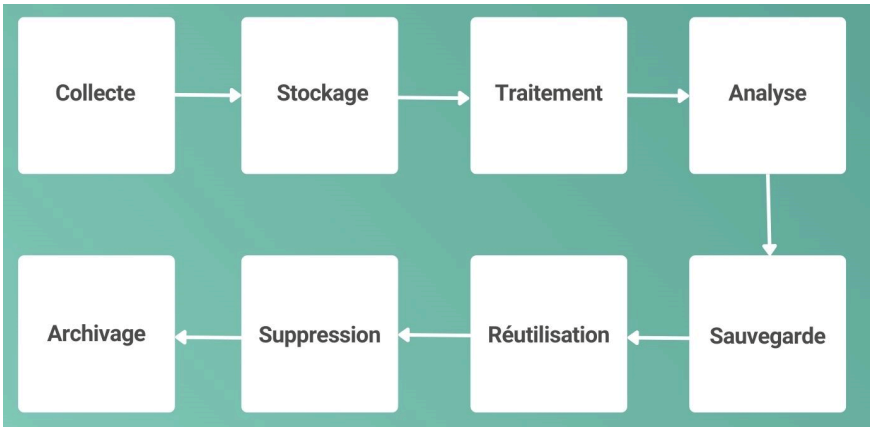
ÉCHELLE DE CRITICITÉ



Source : d'après Lacombe et Lesage, p. 153.

Les données ont un cycle de vie, courant de leur création/collecte à leur archivage et/ou suppression. Au cours des phases de ce cycle, leurs caractéristiques peuvent changer.

LE CYCLE DE VIE DE LA DONNÉE



Source : https://datalegaldrive.com/cycle-vie-donnee-personnelle

[10] Salamon, 2020, p. 33.
[11] Mooc de l'ANSSI sur la protection des données : https://secnumacademie.gouv.fr.

Les données peuvent revêtir un caractère stratégique[12], économique et/ou organisationnel (vecteur notamment d'optimisation[13]). C'est le « pétrole du XXIe siècle[14] » (dans tous les sens du terme, d'ailleurs, car elles causent une pollution massive[15], considération dont nous ne discuterons pas ici), ce que prouve la liste des principales capitalisations boursières mondiales, largement occupée par des entreprises dont la donnée est le cœur de rentabilité ou qui produisent des éléments permettant de traiter la donnée (cas de Nvidia, par exemple)[16].

Mais les grandes entreprises ne sont pas les seules concernées : la donnée et sa protection font ou doivent faire l'objet d'une attention particulière dans toute entreprise, quels que soient sa taille ou son secteur d'activité.

Nous nous intéresserons ici aux données transitant dans les cabinets d'expertise comptable, c'est-à-dire dans des entreprises de toutes tailles, relevant d'une profession réglementée, sur un secteur très concurrentiel brassant des informations pour la plupart strictement confidentielles.

1.1.1.3. La notion de « sensibilité »

Dans le cadre du présent travail, nous n'entendrons pas le terme de « donnée sensible » au sens juridique du terme, qui ne fait référence qu'aux données personnelles[17]. Nous considérerons comme « sensibles » l'ensemble des données devant être protégées eu égard à leur valeur (marchande, économique, stratégique), leur utilité (dans le cadre d'un process de travail par exemple) ou leur encadrement légal contraignant (donnée personnelle par exemple).

Une définition intéressante de la sensibilité de l'information est celle établie dans le cadre de la loi n° 68-678 du 26 juillet 1968 relative à la « communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères » : « Au sein de chaque entreprise, la sensibilité d'une donnée est caractérisée au regard du préjudice potentiel qui pourrait résulter de sa divulgation ou de son altération. Le diagnostic peut être conduit sur la base d'une analyse de risques au cas par cas[18]. »

Une donnée est donc sensible dès lors que sa compromission entraîne un préjudice direct ou indirect pour son détenteur, que ce préjudice soit d'ordre juridique, commercial, financier, réputationnel…

---

[12] Salamon, 2020, p. 15.
[13] Benoît Loeillet, « De l'importance stratégique des données pour les entreprises à leur indispensable qualité », *Harvard Business Review*, 22 février 2024, www.hbrfrance.fr/organisation/de-limportance-strategique-des-donnees-pour-les-entreprises-a-leur-indispensable-qualite-60463.
[14] Lévy, 2021, p. 24.
[15] https://lejournal.cnrs.fr/billets/le-big-data-est-il-polluant.
[16] https://investir.lesechos.fr/actu-des-valeurs/la-vie-des-actions/apple-et-microsoft-en-tete-des-premieres-capitalisations-boursieres-mondiales-1967283.
[17] www.cnil.fr/fr/definition/donnee-sensible.
[18] www.entreprises.gouv.fr/files/files/enjeux/securite-economique/loi-de-blocage/guide-identification-donnees-sensibles.pdf?v=1701872953 et www.legifrance.gouv.fr/loda/id/JORFTEXT000000501326.

1.1.1.4. La notion de protection des données

À grands traits, la protection des données vise notamment à assurer :

- **Leur disponibilité :** assurance que les personnes autorisées ont accès à l'information ;
- **Leur intégrité :** certitude que l'information ou le message n'a pas été modifié ni altéré ;
- **Leur confidentialité :** assurance que l'information n'est accessible qu'aux personnes autorisées ;
- **La preuve :** garantie que l'émetteur d'une information soit identifié, qu'il a les droits et les accès logiques, que le récepteur identifié soit autorisé à accéder à l'information[19].

Pour atteindre ces objectifs, l'entreprise pourra se baser sur différents outils et processus, parmi lesquels la sécurité des accès physiques et virtuels, la sécurité des réseaux et des communications, les procédés d'authentification et de chiffrement, les sauvegardes…

1.1.2. Typologie des données sensibles dans les cabinets comptables

Dans le cadre d'un cabinet d'expertise comptable, les données sensibles peuvent être regroupées en trois agrégats : les données liées au cabinet lui-même, les données personnelles, les données liées aux clients.

1.1.2.1. Les données liées au cabinet

Comme toute entreprise, un cabinet d'expertise comptable possède des données sur sa propre structure. Elles revêtent des caractères divers : données statistiques économiques, commerciales, financières, fiscales, stratégiques, relatives aux ressources humaines, documentation, modes d'emploi et processus de travail, communications internes et externes, outils d'identité et de communication (logos, charte graphique…), etc.

Ces données sont considérées comme plus ou moins sensibles par la direction en fonction de la culture d'entreprise (culture du secret ou approche ouverte), de l'approche concurrentielle (dans un secteur très concurrentiel, les entreprises jalouseront plus les données de leurs concurrents), du contexte (en cas de grandes manœuvres de concentrations, on peut imaginer que les acteurs auront tendance à plus protéger leurs informations pour garder une meilleure maîtrise de leur valorisation), etc.

1.1.2.2. Les données personnelles

Comme toute entreprise, un cabinet d'expertise comptable gère des données[20] sur :

- **Ses salariés :** état civil, coordonnées postales, coordonnées bancaires, horaires effectués, contrôles d'accès, type de permis de conduire, éventuellement photographie pour les annuaires internes, mais aussi vidéo-, télé- et cybersurveillance, géolocalisation des véhicules d'entreprise[21]…

[19] Carpentier, 2023, p. 16.
[20] Collecte, organisation, consultation, conservation, communication, cession, suppression…
[21] www.cnil.fr/fr/thematiques/travail-et-donnees-personnelles.

- **Ses candidats à l'embauche :** état civil, parcours professionnel, permis de conduire…
- **Ses clients et prestataires :** coordonnées, informations bancaires, comptables, fiscales et juridiques, historique de collaboration…
- **Ses autres parties prenantes :** établissements de crédit, actionnaires nominatifs…

Parmi ces données, certaines sont « personnelles ». Une donnée personnelle est « toute information se rapportant à une personne physique identifiée ou identifiable[22] ». À noter que des coordonnées d'entreprises ne sont pas, des données personnelles, puisqu'elles concernent une personne morale et non une personne physique[23]. Ces données personnelles doivent être protégées pour des raisons juridiques, mais également réputationnelles : même sans caractère sensible, des données dérobées concernant des clients ou fournisseurs mettront une entreprise dans une position délicate et induiront un doute sur sa fiabilité globale.

1.1.2.3. Les données liées aux clients

De manière générale, un cabinet d'expertise comptable va brasser des données concernant ses clients anciens et actuels, ainsi que sur ses prospects.

Un cabinet d'expertise comptable a pour activité première le recueil, le traitement et la communication (à un nombre réduit d'acteurs) d'informations relatives à ses clients. Outre les informations personnelles, il gère des informations confidentielles ne se limitant pas au champ comptable, puisqu'elles peuvent aussi être d'ordres juridiques, administratives, financières ou encore sociales.

Ces données sont collectées, traitées, consultées, modifiées, stockées, communiquées (à l'État, par exemple : à la DGFiP, au ministère du Travail ou encore à celui de la Justice). Elles peuvent être collectées directement auprès du client ou auprès de tiers (greffe, État, établissements bancaires…).

ORDONNANCE N° 45-2138 DU 19 SEPTEMBRE 1945 PORTANT INSTITUTION DE L'ORDRE DES EXPERTS-COMPTABLES ET RÉGLEMENTANT LE TITRE ET LA PROFESSION D'EXPERT-COMPTABLE, ARTICLE 21

« Sous réserve de toute disposition législative contraire, les experts-comptables, les salariés mentionnés à l'article 83 ter et à l'article 83 quater, les experts-comptables stagiaires et les professionnels ayant été autorisés à exercer partiellement l'activité d'expertise comptable sont tenus au secret professionnel dans les conditions et sous les peines fixées par l'article 226-13 du Code pénal. »

DÉCRET N° 2012-432 DU 30 MARS 2012 RELATIF À L'EXERCICE DE L'ACTIVITÉ D'EXPERTISE COMPTABLE, ARTICLE 147

« Sans préjudice de l'obligation au secret professionnel, les personnes mentionnées à l'article 141 sont soumises à un devoir de discrétion dans l'utilisation de toutes les informations dont elles ont connaissance dans le cadre de leur activité. »

www.legifrance.gouv.fr/loda/id/JORFTEXT000000698851

1.2. Les principales sources de risques et de menaces

Les cabinets d'expertise comptable travaillent donc avec un ensemble de données plus ou moins sensibles, plus ou moins encadrées juridiquement, et qui peuvent faire l'objet de différentes menaces. L'objectif principal de la cybersécurité est de prévenir la compromission des données[24]. Les menaces pesant sur ces dernières peuvent trouver leur origine en interne ou en externe.

[22] www.cnil.fr/fr/definition/donnee-personnelle.
[23] www.cnil.fr/fr/definition/donnee-personnelle.
[24] Wilson, 2021.

1.2.1. Les sources internes

Comme l'explicitent Pierre-Emmanuel Arduin, Michel Grundstein et Camille Rosenthal-Sabroux, « l'informatique est ubiquitaire, si bien que l'individu n'est plus un simple utilisateur du système d'information, mais un composant à part entière [dudit système] [25] ». Ainsi, assurer la sécurité d'un système d'information impose de prendre en compte ses utilisateurs en tant que composants [26] : au même titre que l'ordinateur, ils traitent, stockent et diffusent les informations. S'agissant d'individus, ils peuvent par ailleurs avoir un comportement passionnel, voire irrationnel. Les collaborateurs en interne sont donc l'une des menaces les plus prégnantes au sein d'une entreprise, de façon intentionnelle ou non, malveillante ou non. Une autre grande source interne de menace est l'obsolescence matérielle ou logicielle, sur laquelle nous reviendrons dans la suite de ce mémoire.

1.2.1.1. Les erreurs et omissions

Les premières des menaces pesant sur les données sont les erreurs et omissions. Menaces non intentionnelles et non malveillantes, elles n'en sont néanmoins pas anecdotiques pour autant. Il peut s'agir d'oublis, de fautes de frappe corrompant l'intégrité des données ou encore d'erreur dues à de la négligence, de l'incompétence, de l'inexpérience, une méconnaissance de l'évolution des règles ou des risques cyber (un manque de formation)…

1.2.1.2. La négligence

La négligence est probablement le facteur de risque le plus fréquent au sein d'une entreprise. Il peut s'agir d'une méconnaissance des risques (méconnaissance de la menace), d'une méconnaissance de la pratique à risque (comme l'envoi de mots de passe en clair par e-mail) ou d'une méconnaissance de sa capacité à produire du risque (comme un stagiaire qui n'aurait pas été suffisamment informé des risques et de la sensibilité des données avec lesquels il interagit). Il peut également s'agir de nonchalance, c'est-à-dire, sans méconnaître les risques, de pratiques ne les prenant pas en compte par paresse ou par une mauvaise appréhension de la réalité du risque. On citera par exemple le report d'une sauvegarde par procrastination ou le choix d'un mot de passe non sécurisé pour se simplifier la vie.

Enfin, la négligence peut être caractérisée par un manque de compétences pour assurer la sécurité des données de l'entreprise, que ce soit en interne ou en sous-traitance.

1.2.1.3. La malveillance interne

Au sein d'une organisation, la malveillance interne peut naître de différents facteurs :

- La motivation financière : vol et recel de données ;
- L'intention malveillante autre que financière : volonté de nuire à l'entreprise (d'un employé s'estimant maltraité ou lésé par exemple) ;

[25] Arduin, Grundstein et Rosenthal, 2015.
[26] Arduin, Grundstein et Rosenthal, 2018, p. 5.

- **L'intention bienveillante :** volonté de servir des intérêts extérieurs sans malveillance (fuite d'information pour aider une association, une ONG, une cause, une idéologie… lanceur d'alerte sur des faits non illégaux…).

En interne, la malveillance trouve souvent ses racines dans le désengagement moral[27]. Ce dernier joue un rôle d'inhibition des normes internalisées et de censure sociale. Il peut provenir[28] :

- Du **déni d'illégalité** : « ce n'est pas illégal, alors j'ai le droit de le faire » ;
- Du **déni de responsabilité** : « je n'avais pas d'autre solution : ce n'est pas de ma faute » ;
- De la **condamnation des accusateurs** : « tout le monde est malhonnête, je ne suis donc pas pire qu'un autre » ;
- Du **déni de blessure** : « personne n'a été blessé, il n'y a donc rien de répréhensible » ;
- Du **déni de la victime** : « mon entreprise ou mon responsable l'a bien mérité » ;
- Du **dévouement supérieur** : « je ne l'ai pas fait pour moi-même » ;
- De la **métaphore du grand livre** (le religieux, pas le comptable – quoique) : « j'ai fait beaucoup de bien, j'ai bien le droit à un petit pas de côté. »

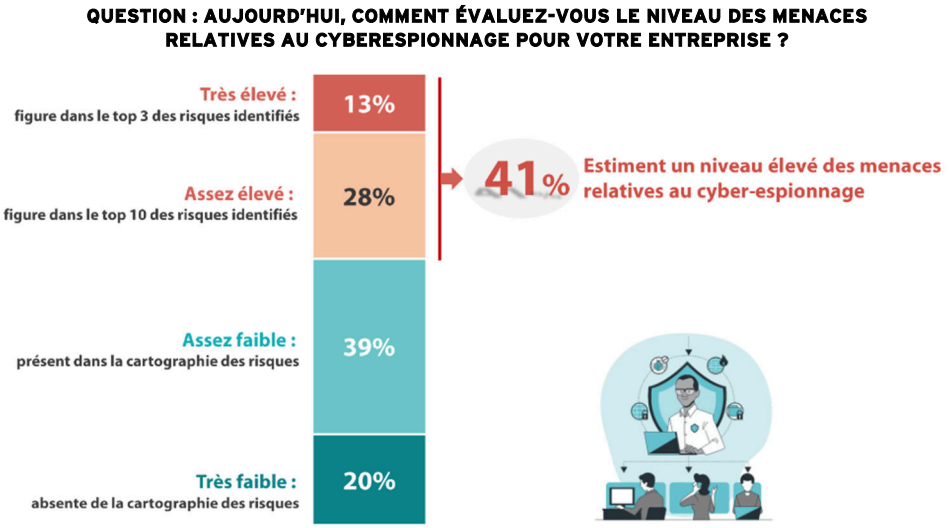
On le voit, il existe un grand nombre de justifications et de sources à la malveillance interne. Il faudra donc veiller, dans la mesure du possible, à détecter les profils à risque.

1.2.2. Les sources externes : les cyberattaques

1.2.2.1. Les motivations des attaquants

La menace sur les données peut également provenir de l'extérieur de l'entreprise[29]. Elle peut avoir plusieurs objectifs :

- **Espionner :** on citera notamment l'espionnage industriel, mais également la volonté de lancer une alerte en l'étayant d'informations solides[30].



Source : Baromètre annuel de la cybersécurité des entreprises, CESIN, 2024

[27] www.scienceshumaines.com/la-theorie-du-desengagement-moral_fr_38358.html.
[28] Arduin, Grundstein et Rosenthal, 2018, p. 93 et suivantes.
[29] Voir annexe 1.
[30] Sur ce sujet, voir les nombreuses fuites qualifiées de « leaks » de ces dernières années, notamment celles centralisées par l'ICIJ : www.icij.org.

- Saboter, déstabiliser, neutraliser :
    - Volonté de nuire à l'entreprise par idéologie (par exemple d'activistes opposés à l'activité d'une entreprise) ;
    - En raison de conflits géopolitiques (par exemple, groupe de pirates informatiques soutenus de façon plus ou moins informelle et plus ou moins officielle par des États) ;
    - Pour des raisons concurrentielles (affaiblir ou décrédibiliser un concurrent) ;
    - Pour des raisons émotionnelles ou sentimentales (pour se venger) ;
    - Pour des raisons ludiques et récréatives (pour s'amuser, par défi…).

  Par corollaire, la volonté peut être de nuire au pays d'établissement de l'entreprise ou des entreprises visées (notamment pour ce qui relève des conflits géopolitiques). Il peut s'agir de la divulgation ou de la destruction de données, ou encore d'un déni de service (en entravant l'accès aux données).

- Rançonner : volonté de dérober des données afin de les revendre ou à des fins de racket. La motivation peut n'être que financière, mais peut également s'assortir d'arguments idéologiques, géopolitiques, etc.

1.2.2.2. Attaque technique ou ingénierie sociale

Les entreprises sont de plus en plus sensibilisées à la protection des données et leurs pare-feu de plus en plus élaborés. Dès lors, cibler leur composante numérique n'est pas le moyen d'attaque le plus aisé, et « relève désormais davantage de l'exercice intellectuel et technique que du crime utilitariste[31] ». Aujourd'hui, la voie la plus simple pour attaquer une société réside dans la manipulation sociale (*social engineering*), c'est-à-dire le fait pour l'attaquant de cibler un utilisateur légitime des données ou du système d'information de l'entreprise, et d'obtenir de lui un moyen direct (en convainquant l'utilisateur de communiquer ses droits d'accès, en les lui dérobant par un lien nuisible visité) ou indirect (par exemple utilisation d'information clé, établissement d'une relation de confiance avec un tiers…) de pénétrer dans le système[32]. En témoigne ce chiffre édifiant : 90% des attaques réussies ont une source humaine[33].

Avec la démocratisation et l'intensification des activités individuelles en ligne, la vie privée n'a souvent plus de privée que le nom, sans même que les individus n'en soient conscients. Par exemple, citons Laurent Mauduit[34], qui lui-même cite quatre membres de la Quadrature du net[35] (association attachée à la défense de la liberté, de la neutralité du net et du respect de la vie privée), compilant les résultats d'une étude menée en 2013 par l'université de Cambridge : « 58 000 personnes ont répondu à un test de personnalité, puis ce test a été recoupé à tous les "j'aime" laissés sur Facebook. En repartant de leurs seuls "j'aime", l'université a ensuite pu estimer leur couleur

[31] Arduin, Grundstein et Rosenthal, 2018, p. 60 et suivantes.
[32] Arduin, Grundstein et Rosenthal, 2018, p. 64.
[33] www.entreprendre.fr/la-cybersecurite-un-enjeu-global-qui-concerne-lensemble-des-entreprises.
[34] Mauduit, 2024, p. 40.
[35] Labonde, Malhuret, Piedallu, Simon, 2022.

de peau (avec 95% de justesse), leur orientation politique (85%), leurs préférences sexuelles (88%), leur confession religieuse (82%), s'ils fumaient (73%), buvaient (70%) ou consommaient de la drogue (65%). » Depuis 2013, gageons que ces estimations ont gagné en finesse. Ainsi, s'il est aisé de dresser un portrait-robot d'un individu que l'on ne connaît pas, il devient facile d'entrer en contact avec lui et de l'amadouer avec un discours auquel il sera sensible, afin de le tromper, d'exploiter sa négligence ou sa naïveté.

D'après le commissaire aux comptes Geoffroy Le Ferrand[36], les stagiaires seraient l'une des principales portes d'entrée des attaques informatiques. Ils cumulent en effet souvent inexpérience, méconnaissance des parties prenantes et des *process* de l'entreprise, et méconnaissance des risques. L'entreprise Kaspersky, spécialisée dans la cybersécurité, confirme ce risque spécifique à ces populations qui font partie de l'entreprise sans en être des membres à part entière et ne sont donc pas toujours identifiées comme des portes d'entrée potentielle de cyberattaques [37].

1.2.2.3. Typologie des attaques

Les attaques peuvent prendre de nombreuses formes, dont nous présentons les principales en annexe [38]. Elles exploitent la négligence, l'ignorance et autres éventuelles faiblesses humaines (hameçonnage, rançongiciel) ou encore la tromperie (*Man-in-the-middle*, fraude au président), utilisent la technique (force brute et déni de service).

1.2.2.4. Les vecteurs d'attaque

Le vecteur d'attaque dépend à la fois du type d'attaque (informatique, ingénierie sociale…) et des vulnérabilités propres à l'entreprise attaquée. Ces vecteurs peuvent être :

- **L'accès physique** à l'équipement informatique : direct (intrusion physique dans les bâtiments) ou indirect (manipulation d'un salarié pour l'inciter à brancher un dispositif contaminé sur son ordinateur) ;
- Le **réseau** (attaque par déni de service…) ;
- Les **téléphones** et **e-mails** des collaborateurs de l'entreprise (*malware*, *phishing*, ingénierie sociale) ;
- Des **applications** et **navigateurs** non sécurisés ou de versions obsolètes ;
- Des failles dans les **extensions** et **modules** (extensions non sécurisées ou obsolètes sur des navigateurs, CMS [39] ou autres applications…) ;
- La **connexion à distance** (VPN[40], équipement subtilisé) ;
- Les **collaborateurs** (malveillance, négligence…).

[36] Cours « Audits spécifiques », master 2 « Comptabilité, contrôle, audit », 2024.
[37] www.kaspersky.fr/blog/interns-as-a-cyberthreat/19065.
[38] Voir annexe 2.
[39] *Content management system* : outils souvent grand-public pour réaliser et animer des sites Internet.
[40] *Virtual private network* : outil pour créer un lien direct entre des préiphériques distants.

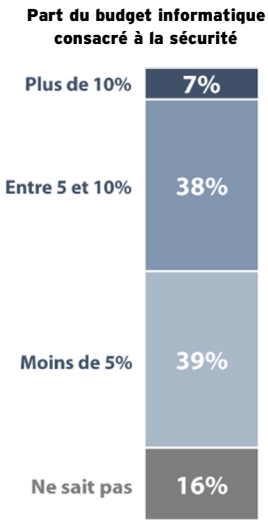
1.2.2.5. Probabilité d'occurrence et conséquences des attaques

Globalement, le principal vecteur d'attaque est l'e-mail [41]. Ce constat posé, force est de constater qu'il est difficile de dresser un panorama précis de la cybermalveillance, en raison du « chiffre noir ». Ce dernier désigne « l'ensemble des infractions qui ont eu lieu mais n'ont pas été signalées [42] » aux pouvoirs publics. En d'autres termes, toutes les entreprises ne signalent pas les attaques dont elles sont victimes (seules 50% le font [43]).

Malgré cette limite forte, le CESIN (Club des experts de la sécurité de l'information et du numérique) publie chaque année un baromètre de la cybersécurité des entreprises, réalisé par OpinionWay grâce à un échantillon de 456 entreprises de tous secteurs d'activité et de toutes tailles. Le dernier en date (2024) dévoile que le nombre des cyberattaques réussies est de 49 %, relativement stable d'une année sur l'autre depuis 4 ans, mais en baisse de plus de 15 % sur cinq ans [44]. Le rapport dresse un palmarès des types de cyberattaques, les techniques de hameçonnage arrivant très largement en tête [45].

1.2.2.6. Le budget de la cybersécurité

Les constats posés ci-avant conduisent sans surprise le monde économique à consacrer une part croissante de ses ressources à sa protection informatique. En 2021, 40 % des entreprises ont ainsi investi dans leur cybersécurité, 40 % des entreprises ont augmenté leur budget et 55% prévoyaient d'accroître leur protection à horizon de quelques mois [46].



Source : Baromètre annuel de la cybersécurité des entreprises, CESIN, 2024

Les investissements portent notamment sur :

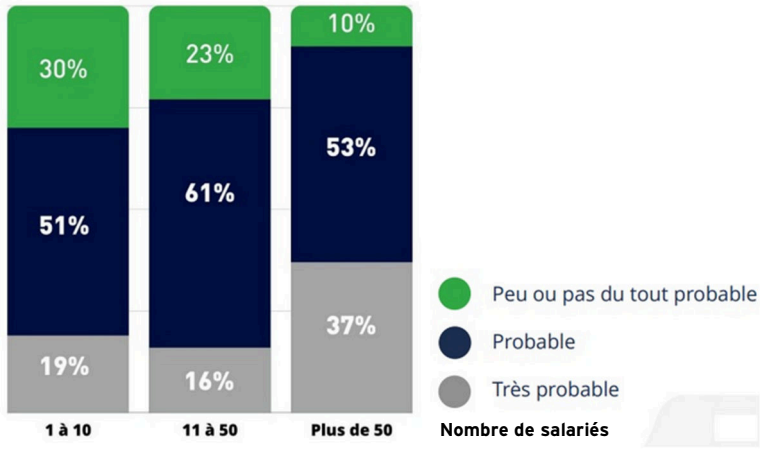
- La souscription de contrats d'assurance dédiés ;
- Des audits dédiés ;
- Des opérations de sensibilisation des salariés ;
- La mise en place de gouvernances spécifiques ;
- Le renforcement des équipes en charge de la protection des SI ;
- L'acquisition de nouvelles solutions et outils informatiques [47].

Si les entreprises paraissent donc toujours plus conscientes des enjeux, il faut néanmoins nuancer le constat, car selon une étude de Stormshield, plus de 30% d'entre elles n'atteignent pas la part minimale de 5% du budget informatique alloué à la cybersécurité recommandée par l'Agence nationale de la sécurité des systèmes d'information française [48] (elles sont près de 40% selon le CESIN – voir schéma ci-dessus).

[41] https://cybercriminalite-penal.fr/cybercriminalite-lemail-est-le-premier-vecteur-releve-dans-le-monde-entier.
[42] Salamon, 2020, p. 136.
[43] www.stoik.io/cybersecurite/chiffres-cles.
[44] https://cesin.fr/articles-slug/?slug=2060-9%C3%A8me+%C3%A9dition+du+barom%C3%A8tre+annuel+du+CESIN.
[45] Voir annexe 3.
[46] www.stoik.io/cybersecurite/chiffres-cles.
[47] www.stoik.io/cybersecurite/chiffres-cles.
[48] www.bercynumerique.finances.gouv.fr/barometre-quel-budget-les-entreprises-doivent-elles-consacrer-la-cybersecurite.

La situation évolue très vite, et les chiffres cités ont sans doute beaucoup évolué depuis. Mais selon toute probabilité, le portrait demeure : une conscience toujours plus accrue des enjeux, mais des moyens souvent pas encore à la hauteur. Soulignons par ailleurs la forte disparité des situations entre les grandes et les petites entreprises : 93 % des TPE et des PME n'ont pas de budget dédié à la cybersécurité (séparément du budget informatique)[49]. Ce chiffre émane notamment du sentiment d'impunité ressenti par les entreprises de plus petite taille, pensant (à tort) n'être pas des cibles intéressantes.

QUESTION (POSÉE À DES ENTREPRISES NON ENCORE VICTIMES D'UNE ATTAQUE) : PENSEZ-VOUS ÊTRE UNE VICTIME POTENTIELLE ?



Source : www.solutions-numeriques.com/93-des-tpe-et-pme-nont-pas-de-budget-dedie-cybersecurite-25-ont-une-couverture-assurance

1.2.3. La sécurité physique

La sécurité des données d'une entreprise commence par la sécurité physique de ses locaux, cible de différentes menaces.

1.2.3.1. Sinistres

La première des menaces réside dans les sinistres, qu'ils soient de source naturelle (tremblement de terre, inondation, tempête…), accidentelle (explosion, incendie…), ou criminelle (attentat, incendie, sabotage…).

Ainsi, en l'absence de sauvegarde en dehors de ses locaux, une entreprise dont les locaux brûlent perd l'intégralité de ses données.

1.2.3.2. Vétusté matérielle

La vétusté matérielle peut également représenter une menace : une infrastructure informatique non entretenue sera plus susceptible de pannes, voire de perte totale (un disque dur qui devient subitement inutilisable par exemple).

1.2.3.3. Malveillance

Le troisième axe de sécurisation physique des données est celui visant à prévenir la malveillance. Cette dernière peut être externe (émanant d'un ou plusieurs individus extérieurs à

[49] www.solutions-numeriques.com/93-des-tpe-et-pme-nont-pas-de-budget-dedie-cybersecurite-25-ont-une-couverture-assurance.

l'entreprise) ou interne (émanant de salariés). Sa manifestation peut être le vol, la destruction ou encore la corruption des données.

Ainsi la sécurité physique nécessite à la fois des procédures de sauvegarde hors site, des procédures de poursuite et de reprise d'activité, ainsi que des mesures de protection et de contrôle de l'accès aux équipements informatiques, de systèmes d'alarme, de la qualité de l'alimentation électrique…

1.2.4. La sécurité logique

La sécurité logique, c'est-à-dire « l'ensemble des procédures et des moyens logiciels permettant d'assurer la confidentialité, la disponibilité et l'intégrité des données et des opérations informatiques[50] », est le pendant incontournable de la sécurité physique. Elle relève de nombreux facteurs, parmi lesquels la qualité du système d'information et de l'environnement applicatif, la qualité des outils de communication, et les mesures de protection.

1.2.4.1. Le système d'information et l'environnement applicatif

La qualité du système d'information d'une entreprise est le premier élément à considérer. Il doit être à la fois robuste aux agressions internes et externes potentielles, évolutif sur le plan sécuritaire mais aussi sur le plan de l'évolution des besoins de l'entreprise.

L'environnement applicatif global devra être surveillé avec attention. Il va de soi que des applications non mises à jour par négligence ou car leur éditeur a cessé leur développement représentent des failles sécuritaires non négligeables. Une entreprise doit donc veiller à son catalogue applicatif, afin de limiter son périmètre à ce qui est nécessaire à son activité et de veiller à éviter toute vétusté applicative.

1.2.4.2. Les échanges informatisés avec l'extérieur

Une entreprise travaille au sein d'un écosystème avec lequel elle interagit. Elle a nécessairement des relations avec l'extérieur, matérialisées sur le plan informatique par des communications entrantes et des communications sortantes. En d'autres termes, par des entrées et des sorties de données. Celles-ci doivent, selon la sensibilité des données, transiter par des outils de communication fiables et sécurisés. Par exemple, l'envoi d'un mot de passe en clair par e-mail représente une faille sécuritaire importante. De telles pratiques sont pourtant quotidiennes dans les cabinets d'expertise comptable (transmission entre le client et le cabinet des informations de connexion aux comptes impots.gouv ou Urssaf par exemple).

1.2.4.3. Les mesures de protection

La sécurité logique passe également par les mesures informatiques qu'il est possible de mettre en place pour protéger ses données. Il peut s'agir de droits et de contrôle d'accès, de chiffrement, d'antivirus, de pare-feu, ou encore de la qualité de l'authentification. L'ensemble de l'écosystème informatique doit être protégé : outils de communication, serveurs, bases de données, environnement logiciel et supports de sauvegarde…

---

[50] https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/2074708/securite-logique.

1.2.5. Cybersécurité et intelligence artificielle

Le développement spectaculaire de l'intelligence artificielle ces dernières années a également eu un impact majeur sur la cybersécurité, tant sur le plan de la défense que sur celui de l'attaque.

1.2.5.1. La défense intelligente

La sécurisation des données, et la cybersécurité de façon plus générale, se sont saisies de l'intelligence artificielle pour améliorer leur efficacité, notamment via le « *machine learning* ». Ce dernier, pour résumer à grands traits, revient à concevoir un programme pour qu'il apprenne et évolue au fil de son propre fonctionnement, et des événements et informations auxquels il est confronté. L'intelligence artificielle permet, dans une certaine mesure, une automatisation et une adaptation en temps réel de la réponse à la menace[51].

L'intelligence artificielle permet d'avoir une protection plus robuste et plus évolutive. Si ces technologies sont très récentes et pour l'heure onéreuses, il est plus que probable que l'avenir de la cybersécurité repose en grande partie sur elles. Soulignons par ailleurs que l'intelligence artificielle elle-même devra être protégée, afin de n'être pas instrumentalisée par l'attaquant[52].

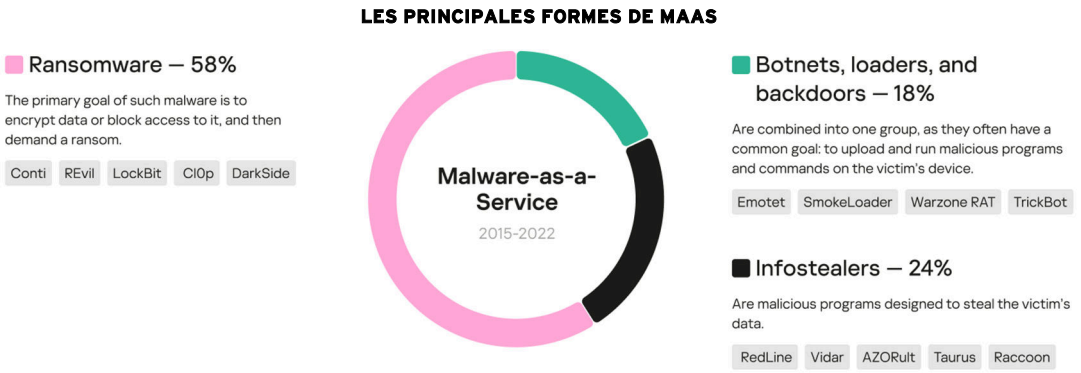
1.2.5.2. La naissance d'une industrie cybercriminelle

On le sait, l'intelligence artificielle peut permettre de composer un morceau musical, d'écrire un livre ou encore de rédiger un mémoire universitaire. On sait moins qu'elle est également utilisée pour réaliser des programmes informatiques, dont des programmes malveillants, abaissant considérablement leur coût et leur temps de développement. Elle permet en outre de générer à la volée des rançongiciels adaptés à la demande d'un client qui n'aura pas besoin de connaissances informatiques très poussées pour pouvoir l'utiliser.

Par ailleurs, l'intelligence artificielle améliore considérablement la qualité des *malwares* : par exemple, le temps où la piètre qualité de son orthographe suffisait pour détecter un message malveillant est révolu.

Ces dernières années ont vu l'émergence d'un autre phénomène : celui des « *malware-as-a-service* » (par analogie avec le « *software-as-a-service* », logiciel installé sur des serveurs distants et non chez l'utilisateur), c'est-à-dire la location de logiciels malveillants permettant de mener des attaques (et l'assistance technique idoine). Ces *malware-as-a-service*, souvent désignés sous leur acronyme MaaS, permettent donc à un individu lambda de louer l'utilisation d'un logiciel qui lui permettra de mener une attaque sans avoir besoin de connaissance informatique. Cette attaque peut prendre la forme d'un rançongiciel, de *phishing*, ou de toute autre forme de *malware*.

[51] www.lemondeinformatique.fr/publi_info/lire-detecter-et-bloquer-les-ransomwares-grace-a-l-intelligence-artificielleet-8239-621.html.
[52] https://linuxfr.org/users/maderios--2/journaux/cybersecurite-des-chercheurs-ont-cree-un-ver-qui-attaque-l-ia.

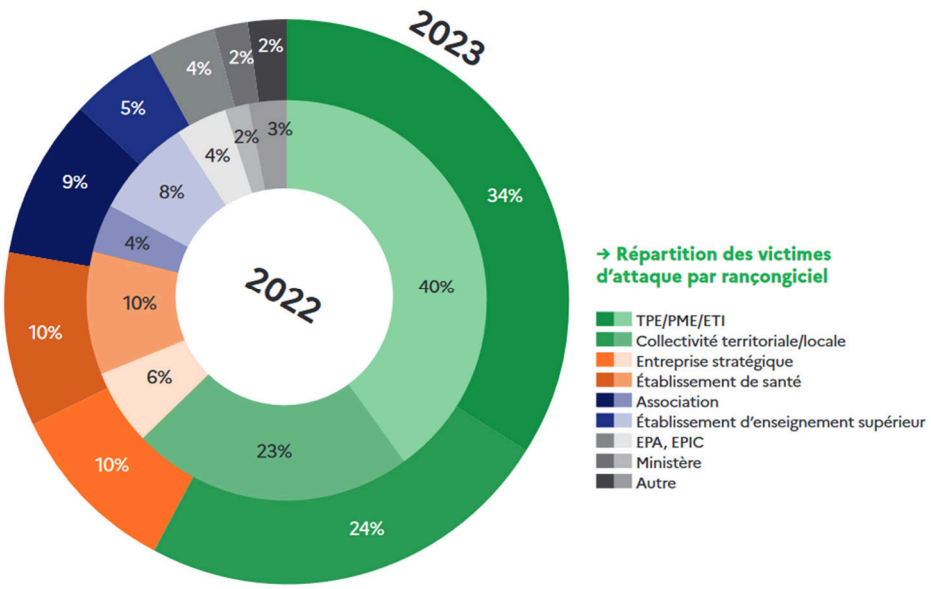


Source : Kaspersky Digital Footprint Intelligence, www.undernews.fr/malwares-virus-antivirus/58-des-logiciels-malveillants-vendus-en-tant-que-service-sont-des-ransomwares.html

Ces deux évolutions, IA et MaaS, entraînent l'industrialisation de la cybercriminalité via une réduction considérable du temps et du coût de création d'une solution d'attaque informatique, et la production d'outils accessibles et faciles à utiliser par tout un chacun (y compris par des individus sans compétences techniques).

1.2.5.3. La généralisation du risque

Ainsi, le coût, le lancement et le faible niveau de compétence requis pour lancer une attaque ont conduit une massification de la cybercriminalité, et son orientation vers de nouvelles cibles, parmi lesquelles les entreprises de tailles moyenne, petite, et très petite. En effet, le coût marginal du lancement d'une attaque étant très faible, il devient intéressant de jouer sur le nombre de cibles plutôt que sur l'importance des sommes réclamées.



Panorama de la cybermenace 2023, *ANSSI, www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-001.pdf*

En d'autres termes, il faut être de plus en plus vigilant, car les attaques sont de plus en plus nombreuses, de plus en plus « qualitatives » et peuvent désormais cibler n'importe qui.

Par ailleurs, notons que l'intelligence artificielle permet une créativité nouvelle dans les attaques cybercriminelles, dont l'imagination paraît être la seule limite. Citons pour exemple cet employé d'une société hongkongaise qui a viré environ 26 millions de dollars à des pirates informatiques après avoir participé à une visioconférence rassemblant plusieurs de ses collègues. Il était en

fait le seul réel participant de la visioconférence : tous les autres étaient des *deepfakes*[53] (un *deepfake*, ou hypertrucage, consiste à falsifier un média audio et/ou vidéo grâce à l'intelligence artificielle, afin par exemple de placer dans la bouche d'être réels des propos qu'ils n'ont jamais tenus, ou de créer des visuels plaçant des individus dans des situations ou réalisant des actes fictifs). Autre exemple : un attaquant ayant tenté de faire croire à un employé du gestionnaire de mots de passe Lastpass qu'il était en communication téléphonique avec son PDG (la voix de ce dernier était en fait émulée par *deefake*[54]).

1.2.6. Les critères de ciblage

Comme nous venons de l'évoquer, l'intelligence artificielle et le MaaS ont transformé tout un chacun en cible. Toutefois, certains critères caractérisent une exposition à la malveillance informatique particulièrement marquée.

1.2.6.1. Le caractère stratégique ou symbolique de l'activité

Tout d'abord, les entreprises à caractères stratégique ou symbolique présentent un attrait particulier pour les cyberattaques, notamment celles à sous-jacent géopolitique ou idéologique.

Pour ce qui relève du caractère stratégique, citons à titre d'exemple l'attaque Stuxnet menée par Israël et les États-Unis contre le programme nucléaire iranien[55], la paralysie de l'Estonie en 2007 par des militants prorusses[56], ou encore les attaques menées en mars 2024 par des militants prorusses du groupe Anonymous Sudan contre l'État français dans le contexte de la guerre en Ukraine[57].

Les attaques à caractère idéologique relèvent ce que l'on nomme l'« hacktivisme », c'est-à-dire le fait d'utiliser le piratage informatique afin de sensibiliser la population, d'obtenir des changements politiques ou sociétaux. L'« hacktivisme » peut promouvoir tout type d'opinion ou de croyances : citons par exemple les hacktivistes religieux, anticapitalistes, souverainistes, libertariens, anarchistes, ceux défendant la démocratie, la liberté d'expression[58], l'environnement…

1.2.6.2. L'exposition médiatique, le caractère symbolique de l'entreprise

L'exposition médiatique et le caractère symbolique font également des entreprises des cibles de choix, car elles offrent une tribune à l'aune de leur importance. Une société peut également être ciblée car elle représenterait une belle cible de guerre pour le pirate, ce milieu étant friand des tableaux de chasse. Par ailleurs, naturellement, plus une entreprise est connue et plus elle vient facilement à l'esprit d'un pirate cherchant sa prochaine cible.

1.2.6.3. Le caractère potentiellement lucratif de l'attaque

Pour les pirates dont la motivation est financière, le caractère lucratif de l'opération est un critère majeur. Toutefois, on l'a vu, il est aujourd'hui aisé et peu coûteux de lancer une attaque à grande

---

[53] https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html.
[54] www.bleepingcomputer.com/news/security/lastpass-hackers-targeted-employee-in-failed-deepfake-ceo-call.
[55] www.cairn.info/revue-politique-etrangere-2018-2-page-15.htm.
[56] http://news.bbc.co.uk/2/hi/technology/7208511.stm.
[57] www.globalsecuritymag.fr/attaques-ddos-contre-le-gouvernement-francais-qui-est-anonymous-sudan-apercu-de.html.
[58] www.laquadrature.net/en/tools.

échelle ciblant un grand nombre d'entreprises. Le caractère potentiellement lucratif pourra donc aussi bien concerner une attaque ciblée exclusivement sur une ou plusieurs entreprises possédant d'importants moyens financiers, ou une attaque visant un grand nombre de petites cibles.

1.2.6.4. La gestion sociale interne

Une mauvaise gestion sociale en entreprise peut créer du ressentiment chez certains salariés. Ceux-ci sont alors plus enclins à commettre des actes de malveillance, pour nuire à l'entreprise (sabotage), pour la voler (avec une justification morale de revanche, de vengeance), pour favoriser un tiers au détriment de l'entreprise (accord de privilège indu, transmission d'informations, etc.).

1.2.6.5. L'opportunité

Enfin, l'opportunité est l'une des causes majeures de malveillance. L'absence de protection informatique, l'utilisation de logiciels non mis à jour contenant des failles de sécurité connues, le manque de procédures de contrôles en interne, la négligence… Un piratage facile est forcément un piratage tentant.

1.3. Typologie des risques

Les risques relatifs aux données peuvent être qualitatifs (juridique, stratégique, réputationnel, technique…) et/ou quantitatifs (financiers, perte de clients et de marchés).

1.3.1. Pertes financières

Les pertes financières peuvent provenir :

- Du versement d'une rançon (notamment lors d'attaques de type rançongiciels ou d'autres formes de chantage lié au vol ou à l'intégrité des données) ;
- De la destruction des données (et donc de la perte d'exploitation en résultant, du coût de reprise de l'activité et le cas échéant de récupération de tout ou partie des données) ;
- De la destruction du matériel informatique (physiquement ou via une cyberattaque) ;
- Du coût d'intervention des éventuels prestataires mobilisés pour faire face à la brèche de sécurité, du coût de réparation/renouvellement et de remise en service de l'équipement…

Par ailleurs, un article de Stoïk[59] nous apprend que :

- Le coût moyen d'une cyberattaque est de 50 000 € ;
- La perte d'exploitation moyenne est évaluée à 27 % du chiffre d'affaires annuel ;
- 60% des PME attaquées ne parviennent à se relever et déposent le bilan dans les 18 mois suivant l'attaque.

1.3.2. Atteinte à la réputation

Pour une entreprise, une atteinte à ses données peut représenter un risque réputationnel considérable. Dans le domaine de l'expertise comptable, dont le cœur d'activité est le travail sur

[59] www.stoik.io/cybersecurite/chiffres-cles.

des données sensibles appartenant à des clients, un vol, une perte, une destruction ou encore une atteinte à l'intégrité des données pourra difficilement être résolue discrètement, et l'impact sur l'image de marque du cabinet touché, aggravé par l'éventuel bouche-à-oreille, peut être dévastateur. Cela peut entraîner une perte de clientèle, des pertes de chance ou à tout le moins une rupture de la relation de confiance difficile à réparer. Néanmoins, gageons que si certains clients, de par leur activité ou leur taille, sont intraitables sur la qualité de la sécurisation de leurs données, la plupart des petites entreprises sont relativement compréhensives en cas d'atteinte à leurs données dans la mesure où elles savent que le risque zéro n'existe pas, que l'attaque ne signifie pas négligence de la part de leur cabinet, et dans la mesure où elles-mêmes ne protègent bien souvent pas (ou insuffisamment) leurs propres données.

1.3.3. Perte de données

La perte de données peut résulter d'une altération, d'une destruction ou d'une atteinte à l'intégrité des données. Pour un cabinet d'expertise comptable, la perte de données est un sujet majeur car il s'agit de sa matière première. Sans elle, point de comptes, point d'états financiers, point de déclaration… alors que les échéances (notamment en matière de taxes et de dépôt des comptes) continuent de courir (avec une tolérance en cas d'attaque caractérisée, documentée et instruite). Par ailleurs, la perte de données, causant à la fois une perte d'exploitation et une potentielle perte de clients, peut se révéler fatale à l'entreprise, comme le suggère le chiffre précédemment mentionné de 60 % des PME victimes ne se relevant pas de l'attaque [60].

1.3.4. Sanctions légales

Les risques peuvent également être d'ordre judiciaire. Selon la nature des données compromises (personnelles, sensibles, confidentielles…), et le degré de responsabilité de l'entreprise (négligence, non-respect de la législation…), celle-ci peut faire l'objet de poursuites judiciaires, avec des sanctions pécuniaires et/ou pénales qui viendront abonder les risques financiers et réputationnels.

On le voit, les conséquences potentielles d'une atteinte aux données d'une entreprise peuvent aller de la simple perte financière au dépôt de bilan. Il s'agit donc d'un risque majeur incontournable pour les cabinets d'expertise comptable.

1.4. Les cadres juridique et normatif

Le cadre juridique relatif à la protection des données est abondant et complexe. Ne représentant pas le cœur du sujet du présent mémoire, nous ne l'évoquerons que succinctement. En France, il est principalement composé de la transposition du règlement général sur la protection des données (RGPD). Le cadre normatif est également abondant ; dans le même esprit, nous n'en brosserons qu'un panorama succinct.

[60] www.stoik.io/cybersecurite/chiffres-cles.

1.4.1. Le RGPD et la loi « Informatique et libertés »

1.4.1.1. L'harmonisation de la protection des données personnelles (chap. I)

La loi Informatique et liberté, datant initialement de 1978, a été modifiée en 2018 afin de transposer en droit national la réglementation européenne (règlement général sur la protection des données, dit RGPD [61]) et la directive police justice [62].

Ce qui nous intéresse ici au premier chef est le RGPD, directement relatif à la protection des données. Il s'agit d'un règlement européen visant à harmoniser la législation sur la protection des données personnelles au sein de l'Union européenne. Il date de 2016, mais est applicable depuis le 25 mai 2018. Il s'applique à tout traitement de données à caractère personnel (comme nous l'avons évoqué, il s'agit donc de « toute information concernant une personne physique identifiée ou identifiable [63] ») que ce soit par des acteurs publics ou privés [64].

1.4.1.2. Les grands principes du RGPD (chap. II)

Le RGPD repose sur six grands principes [65] :

- **Licéité, loyauté et transparence** du traitement des données personnelles au regard de la personne concernée ;
- **Finalités déterminées, explicites et légitimes de la collecte**, et interdiction de traitement ultérieur incompatible avec ces finalités (sauf exceptions mentionnées à l'article 5) ;
- **Minimisation des données personnelles :** elles doivent être adéquates, pertinentes et limitées au strict nécessaire par rapport aux finalités déterminées ;
- **Exactitude :** les données inexactes ou erronées doivent être rectifiées ou supprimées ;
- **Limite de conservation :** sauf exceptions mentionnées à l'article 5, « les données permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées [66] » ;
- **Intégrité et confidentialité :** les données doivent être manipulées de façon à leur garantir une sécurité appropriée, « y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées [67] ».

1.4.1.3. Le droit des personnes (chap. III)

Le RGPD renforce les droits des citoyens européens sur ce qui relève de leurs données personnelles. Ainsi, son chapitre III liste les droits dont chacun dispose sur ses propres données :

[61] www.cnil.fr/fr/reglement-europeen-protection-donnees.
[62] https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L0680&from=FR.
[63] RGPD, article 26.
[64] RGPD, article 5.
[65] RGPD, article 5.
[66] www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article5.
[67] www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article5.

- **Droit d'accès**[68] **:** accéder à ses données personnelles et obtenir des informations sur leur traitement ;
- **Droit de rectification**[69] **:** demander la correction de ses données personnelles si elles sont inexactes ou incomplètes ;
- **Droit à l'effacement (ou « droit à l'oubli »)**[70] **:** demander la suppression de ses données personnelles (sauf fondement juridique au traitement) ;
- **Droit à la limitation du traitement**[71] **:** demander la limitation du traitement de ses données ;
- **Droit à la portabilité des données**[72] **:** recevoir ses données personnelles dans un format structuré, couramment utilisé et lisible par machine ;
- **Droit d'opposition**[73] **:** s'opposer au traitement de ses données pour des motifs légitimes.

1.4.1.4. Responsable du traitement et sous-traitant (chap. IV)

Les responsables de traitement, c'est-à-dire les personnes qui décident des finalités et des moyens du traitement, ainsi que leurs sous-traitants éventuels, doivent respecter plusieurs obligations inscrites au chapitre IV du RGPD :

- **Sécuriser les données personnelles**[74] **:**
  - Sécurité du traitement[75] ;
  - Notification à l'autorité de contrôle d'une violation de données à caractère personnel[76] ;
  - Communication à la personne concernée d'une violation de ses données[77] ;
- **Réaliser des analyses d'impact** sur la protection des données pour les traitements à risque élevé[78] ;
- **Désigner un délégué à la protection des données** (DPO) pour les traitements importants[79] ;
- **Les codes de conduite et certifications**[80] : pour accompagner les États dans la transposition des règles et à leur adaptation aux réalités des petites et moyennes entreprises.

1.4.1.5. Contrôle et sanctions (chapitres VI et VIII)

Les autorités de contrôle nationales (en France, la Commission nationale de l'informatique et des libertés, dite CNIL) sont chargées de veiller au respect du RGPD. Elles peuvent ainsi mener des contrôles, sanctionner, proposer des recommandations.

En cas de non-respect du RGPD, les sanctions administratives peuvent atteindre jusqu'au montant le plus élevé entre 20 millions d'euros et 4 % du chiffre d'affaires annuel global.

---

[68] RGPD, article 15.
[69] RGPD, article 16.
[70] RGPD, article 17.
[71] RGPD, article 18.
[72] RGPD, article 20.
[73] RGPD, article 21.
[74] Voir le texte intégral de cette section en annexe 4.
[75] RGPD, article 32.
[76] RGPD, article 33.
[77] RGPD, article 34.
[78] RGPD, articles 35 à 36.
[79] RGPD, articles 37 à 39.
[80] RGPD, articles 40 à 43.

1.4.1.6. Le RGPD en pratique

Le RGPD constitue donc un cadre juridique majeur pour la protection des données personnelles en France. Toutefois, il est extrêmement complexe, long et coûteux à mettre en œuvre et est donc en pratique peu appliqué dans les petites sociétés, ou mis en place de façon très artisanale et incomplète.

1.4.2. Les autres textes contraignants

Depuis la loi Godfrain de 1988 relative à la fraude informatique[81], l'État a régulièrement et considérablement renforcé son arsenal législatif sur les domaines touchant au numérique. Parmi les nombreux textes en vigueur :

- Le **Code civil** contient des dispositions relatives à la protection de la vie privée (comme par exemple son article 9 [82]). Il peut donc constituer un fondement valable pour une action en justice en cas de violation de données personnelles. Ainsi, les violations en matière de protection des données pouvant émaner du personnel de l'entreprise, cette dernière devra être attentive aux articles 1384 alinéa 5 du Code civil (responsabilité civile de l'employeur au regard de l'activité de son personnel) et 121-2 du **Code pénal** (responsabilité civile de l'employeur lorsqu'un membre de son personnel commet une infraction impliquant l'entreprise) ;
- La **loi de sécurité financière** du 1er août 2003 établit des obligations en matière de sécurité des systèmes d'information, notamment une importance accrue du contrôle interne ;
- En matière sociale, la **doctrine** a récemment confirmé (par le biais de la Direction régionale interdépartementale de l'économie, de l'emploi, du travail et des solidarités Île-de-France) que les entreprises peuvent recourir à l'activité partielle en cas de cyberattaque sous réserve de fournir une attestation de leur hébergeur, une copie du dépôt de plainte, et une attestation de l'assureur concernant la garantie contre le piratage de données informatiques. Ces démarches doivent être réalisées conformément aux articles R5122-1, R5122-2, R5122-3, et R5122-4 du **Code du travail** [83].

1.4.3. Les normes et référentiels

1.4.3.1. ISO 27001

Norme internationale relative à la sécurité des systèmes d'information, l'ISO/CEI 27001 a été publiée en 2005 [84] par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI)[85]. Elle propose un cadre pour la mise en place, le maintien et l'amélioration continue d'un système de management de la sécurité de l'information (SMSI)[86]. Sa finalité est d'accompagner les organisations dans la protection de leurs actifs

[81] www.legifrance.gouv.fr/jorf/id/JORFTEXT000000875419.
[82] www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006419288.
[83] www.dpo-partage.fr/cyberattaque-de-coaxis.
[84] Sa dernière révision date de 2022.
[8585] www.iso.org/obp/ui/fr/#iso:std:iso-iec:27001:ed-2:v1:fr.
[86] Voir annexe 5.

informationnels contre les menaces (intrusions, vol, destruction, perte…). Elle est structurée sur la base de la roue de Dening, méthode visant à réaliser des changements et ajustements progressifs et en continu, sur la base d'un point de départ ou d'un objectif initial [87] :

- Phase d'établissement (*Plan*)
  - Étape 1 : Définir le périmètre du SMSI et son niveau de sécurité ;
  - Étape 2 : Identifier et évaluer les risques et élaborer la politique de sécurité ;
  - Étape 3 : Traiter le risque et identifier le risque résiduel après traitement ;
  - Étape 4 : Choisir les mesures de sécurité à mettre en place [88] ;
- Phase d'implémentation (*Do*)
  - Établir un plan de traitement des risques ;
  - Déployer les mesures de sécurité ;
  - Générer des indicateurs de performance et de conformité ;
  - Former et sensibiliser le personnel ;
- Phase de maintien (*Check*)
  - Contrôle interne ;
  - Audit interne ;
  - Revues d'adéquation du SMSI avec son environnement ;
- Phase d'amélioration (*Act*) :
  - Actions correctives ;
  - Actions préventives ;
  - Actions d'amélioration : améliorer la performance d'un processus du SMSI.

L'ISO 27001 peut fournir un cadre intéressant pour établir ou améliorer la sécurité de l'information dans son organisation. Une certification ne constitue bien évidemment pas une assurance à toute épreuve, mais elle témoigne d'une réduction du risque de cyberattaques, d'une optimisation des processus liés à la sécurité de l'information, d'un processus d'amélioration continue, d'une conformité aux exigences légales et réglementaires. Elle peut également permettre de renforcer la confiance des clients et partenaires de l'entreprise certifiée.

Selon une étude réalisée en 2019 auprès des certifiés ISO 27001 :
> 89% estiment avoir moins d'incidents de sécurité ;
> 83% estiment que la mise en place de la certification ISO 27001 a permis de consolider des processus internes liés à la sécurité ;
> 88% reconnaissent que la certification a permis de fidéliser certains de leurs clients qui les auraient probablement quittés en son absence.

https://certification.afnor.org/numerique/certification-iso-27001

Si la mise en place de cette certification paraît difficile dans les petites entreprises, elle semble néanmoins particulièrement adaptée pour les sociétés traitant des données sensibles telles que des données personnelles ou financières [89].

[87] Carpentier, 2023, p. 27-28.
[88] Sur ces mesures de sécurité, voir ISO 27002 : www.iso.org/fr/standard/75652.html.
[89] www.iso.org/fr/standard/27001.

1.4.3.2. SOC2

Systems and Organizations Controls 2 (SOC 2) est une certification proche de l'ISO 27001, mais sans la notion de SMSI. En France, sa notoriété en dehors des cercles de spécialistes du sujet n'est toutefois pas aussi grande que celle d'une norme ISO.

SOC 2 repose sur cinq critères :

- La **sécurité** : protection des systèmes et des données contre les risques ;
- La **disponibilité** des systèmes et des données ;
- L'**intégrité** du traitement et la fiabilité du système ;
- La **confidentialité** : gestion des autorisations et accès ;
- Les **données personnelles** : traitement conforme à la législation.

Plus souple et plus aisée à mettre en œuvre que la norme ISO27001, elle paraît plus adaptée pour les entreprises de petite taille. Mais ne disposant pas de la notoriété de la norme ISO, SOC2 n'a pas le même impact en termes de communication auprès des parties prenantes de l'entreprise.

1.4.3.3. ITIL 4

ITIL (*Information Technology Infrastructure Library*) est un référentiel des bonnes pratiques dans le cadre de l'ensemble des services informatiques mis en œuvre dans une entreprise. Il s'agit de l'outil de gestion du système d'information le plus largement utilisé dans le monde[90].

Ce qui relève de la sécurité figure dans les deux premières des trois catégories du catalogue des pratiques ITIL, intitulées « *General Management practices* » et « *Service management practices*[91] ».

ITIL est un référentiel pouvant conduire à une certification. À ce titre, et selon les spécialistes, il permet d'assurer la mise en place de pratiques favorisant la sécurité (sans toutefois la garantir, cela s'entend), et éventuellement d'obtenir la certification idoine afin de communiquer sur le sujet auprès de ses parties prenantes.

Citons enfin en complément la norme ISO 20000, qui certifie les services informatiques satisfaisant les bonnes pratiques ITIL, ISO/IEC 15408-1:2022, proposant des critères d'évaluation pour la sécurité des technologies de l'information, ou encore les nombreux référentiels relatifs aux prestataires (parmi lesquels PDIS[92], PASSI[93], SecNumCloud [94])...

Le cadre normatif peut être choisi selon la stratégie de l'entreprise en matière de données :
> Quelles ressources (temps, argent) souhaite-t-on consacrer au sujet ?
> Quelle importante a ce sujet pour l'entreprise (qui pilote, quelle fréquence de discussion avec la direction générale...) ?
> Souhait d'une évolution permanente ou d'une amélioration continue...
> Souhaite-t-on un référentiel certifiant ?
> Quelle communication autour des mesures et pratiques de gestion des données souhaite-t-on mettre en place ?

Le cadre juridique est, par nature, contraignant. Tout cabinet d'expertise comptable se doit donc de le connaître, le comprendre et le satisfaire.

---

[90] Carpentier, 2023, p. 18.
[91] Voir annexe 6 et www.theknowledgeacademy.com/blog/essential-guide-to-itil-v4-processes-and-framework.
[92] Prestataires de détection d'incidents de sécurité.
[93] Prestataires d'audit de la sécurité des systèmes d'information qualifiés.
[94] Qui concerne les prestataires de *cloud computing*.

En revanche, les normes et référentiels sont facultatifs. S'il paraît intéressant, voire nécessaire, de les mettre en place dans les grandes structures, ils paraissent très exigeants pour de plus petites entreprises ne disposant pas d'un service informatique ou à tout le moins d'un salarié formé et dédié à ce sujet.

1.4.4. Les ressources documentaires indispensables

En complément de ces cadres et référentiels, de nombreuses ressources documentaires permettent d'aborder les questions de sécurisation des données[95]. Parfois très vulgarisées, elles permettent de s'approprier les notions, de se mettre au fait des menaces, des cadres juridiques, normatifs et sectoriels, ainsi que des principales mesures à prendre pour une protection minimale.

L'État s'est largement saisi de ce sujet, notamment au travers de l'ANSSI, dont les nombreuses publications, Mooc, webinaires ou *checklists* représentent un corpus relativement complet. Le secteur de l'expertise comptable produit également énormément d'informations, qu'elles émanent de l'Ordre des experts-comptables ou encore de magazines spécialisés. De nombreuses autres sources sont à mobiliser, tels la CNIL, l'AFNOR, FranceNum (portail de la transformation numérique des entreprises) ou encore les médias spécialisés dans les questions informatiques et les conseils des associations professionnelles[96].

On l'a vu, les données sont des ressources pour l'entreprise, dont la valeur va croissant. Mais à ce titre, elles doivent être protégées des convoitises, des erreurs, des manipulations ou encore des accidents. Élément immatériel d'une importance stratégique, voire vitale, les données nécessitent la mise en place de mesures afin d'assurer les quatre finalités de la cybersécurité déjà évoquées : la disponibilité, l'intégrité, la confidentialité et la preuve. Nous allons maintenant nous intéresser à ce qui peut être mis en place dans les cabinets d'expertise comptable afin de satisfaire ces objectifs.

[95] Voir annexe 7.
[96] Avoir annexe 8.

2. Les mesures préventives et curatives

De manière générale, la politique de sécurité d'un système d'information « consiste en un ensemble de règles définies pour atteindre et maintenir un certain niveau de sécurité[97]. » En matière de protection des données, deux types de mesures peuvent être mises en place : les mesures *ex ante*, dont le but est de prévenir la compromission des données, et les mesures *ex post*, à visée curative.

2.1. La mise en place d'une politique de sécurité des systèmes d'information

2.1.1. Contexte interne et contexte externe

2.1.1.1. La sécurité de l'information dans l'organigramme de l'entreprise

Si mettre en place une direction des systèmes d'information (DSI) dans les petits cabinets d'expertise comptable paraît disproportionné, c'est toutefois une solution choisie par un nombre croissant de cabinets d'après des propos recueillis auprès d'un professionnel du secteur. Avoir un directeur des systèmes d'information à demeure n'implique pas nécessairement que son seul champ d'action relève du cabinet lui-même. En effet, il peut être mobilisé sur des missions de conseil ou d'audit des systèmes d'information auprès des clients, ajoutant un domaine d'expertise au cabinet[98]. Il peut également être mutualisé par plusieurs cabinets, ce qui pourrait notamment être mis en place dans ceux appartenant à des regroupements.

Si le DSI est chargé de piloter le système d'information, le RSSI, lui, est chargé de sa sécurité. Mais, s'il est rattaché au DSI, il est parfois empêché dans sa mission car le DSI a pour objectif principal le meilleur rendement possible du système d'information, ce qui n'est pas toujours compatible avec sa sécurisation (les opérations de sécurisation mobilisent et ralentissent le personnel, les réseaux et périphériques). Ici, la question de la gouvernance a toute sa place car c'est l'organigramme de l'entreprise qui définit les liens de subordination et les priorités de la direction en termes de couplage productivité/sécurité de l'information.

Dans les cabinets d'expertise comptable de grande taille, il paraît aujourd'hui nécessaire de se munir d'un responsable de la sécurité des informations afin de protéger efficacement ses données et son activité. Les questions de cybersécurité sont d'ailleurs de plus en plus présentes dans les comités exécutifs[99] et la place du DSI renforcée dans la définition de la stratégie globale des cabinets[100].

La question de la sécurisation des données ne faisant pas débat, l'arbitrage porte comme souvent sur son intégration ou sa sous-traitance. Ses critères peuvent être le coût, la gouvernance, la flexibilité, la confidentialité, etc.

---

[97] Lacombe et Lesage, p. 138.
[98] www.metierscomptabilite.fr/wp-content/uploads/2021/11/Fiche_SUPINF1_Directeur_SI.pdf.
[99] https://cesin.fr/articles-slug/?slug=2060-9%C3%A8me+%C3%A9dition+du+barom%C3%A8tre+annuel+du+CESIN.
[100] www.metierscomptabilite.fr/metier/directeur-des-systemes-dinformation.

2.1.1.2. Diagnostic et évaluation des besoins

La première des étapes pour sécuriser les données de son entreprise est de mettre en place une politique de sécurité de son système d'information. Pour ce faire, il faut commencer par établir un diagnostic du périmètre à protéger, ainsi que des risques et des menaces qui lui sont associés, ses points d'entrée, ses vulnérabilités. Il faut également s'interroger sur le niveau de protection désiré pour chaque type de données et chaque type d'éléments du périmètre (physique, applicatif…). Enfin, il faut définir la méthode de protection la plus pertinente, ainsi que les processus de collecte, de traitement, de transmission, d'archivage et de sauvegarde les plus appropriés.

2.1.1.1. Les relations avec les tiers

Les relations avec les clients, fournisseurs, sous-traitants et autres tiers doivent être intégrées dans la démarche globale de la politique de sécurité. Ainsi, avec les fournisseurs par exemple, un « plan d'assurance sécurité » doit définir les rôles et responsabilités, les outils, méthodes et *process* de sécurité, les contrôles possibles[101]…

2.1.2. La sécurité physique

Comme nous l'avons évoqué, la sécurité physique est essentielle à toute entreprise pour protéger ses données. Il s'agit à la fois de restreindre les accès aux infrastructures et à l'équipement informatique (serveurs, systèmes, postes de travail, périphériques d'impression, téléphones, objets connectés…) via tout outil de sécurisation (verrous, vidéosurveillance, alarme…), de contrôler les accès, de contrôler la présence physique des éléments informatiques (pour prévenir le vol interne), mais également de prévoir d'éventuels sinistres en définissant et gérant l'impact de la destruction de matériel, d'une coupure d'électricité, d'une rupture des liaisons de télécommunication…

On notera que le développement du télétravail a déporté l'équipement informatique au-delà du périmètre physique de l'entreprise. Ainsi, cette dernière est susceptible d'essaimer parmi son personnel des ordinateurs, des téléphones portables et autres équipements pouvant constituer autant de supports ou de portes d'entrée vers ses données.

Pour les entreprises de petite taille, on recommandera, afin d'éviter des mesures trop dispendieuses, de se concentrer sur la prévention des intrusions, et de mettre l'accent sur une politique de sauvegarde efficace afin de se protéger des divers sinistres naturels, accidentels ou criminels pouvant survenir.

Un autre point est à considérer : la sortie et mise au rebut du matériel informatique. Tout équipement sortant de l'entreprise doit être méthodiquement « nettoyé » afin de ne pas représenter une fuite potentielle de données. De nombreux exemples d'équipements vendus en deuxième main s'étant avérés porteurs d'informations confidentielles émaillent les médias chaque année. Les opérations de maintenance faisant intervenir du personnel extérieur à l'entreprise doivent également être solidement encadrées[102].

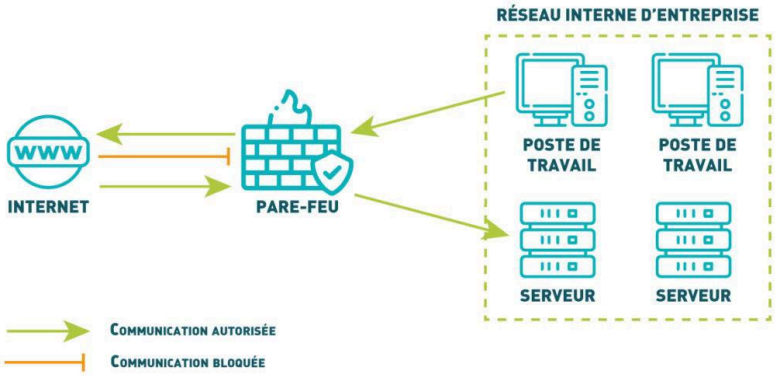
---

[101] Lacombe et Lesage, p. 134.
[102] Lacombe et Lesage, p. 132.

2.1.3. La sécurité logique

2.1.3.1. La surveillance du réseau

Afin de protéger les données, il faut sécuriser ce qui permet d'accéder à ces données, y compris le réseau. De façon préventive, les pare-feu (d'ancienne ou de nouvelle génération, ou encore *firewall-as-a-service*[103]) visent à protéger le réseau, notamment en limitant le risque d'accès non autorisé, en détectant les intrusions, en protégeant les serveurs accessibles depuis l'extérieur (depuis Internet, par exemple).



Source : « Qu'est-ce qu'un pare-feu et quel est son rôle ? », www.axis-solutions.fr/quest-ce-quun-pare-feu-et-quel-est-son-role/

Nous ne nous étendrons pas sur ce sujet très technique. Notons toutefois que les pare-feu peuvent être multipliés pour créer ce que l'on nomme des DMZ (*demilitarized zones*), soit des zones tampon coincées entre le réseau externe (non sécurisé) et le réseau interne[104]. De nombreuses autres formes de protection existent. Sur ce sujet, je ne peux que recommander de faire appel à des spécialistes, ou à tout le moins de se documenter via des ouvrages de vulgarisation suffisamment détaillés pour offrir une information valable[105].

Soulignons qu'une surveillance constante du réseau doit être mise en place pour détecter une activité suspecte dès qu'elle intervient. Ceci afin de lutter contre une intrusion au plus tôt de l'attaque, mais également pour prévenir l'installation de logiciels visant à espionner l'activité des utilisateurs du système pour récupérer des informations, mots de passe, etc., leur permettant par la suite d'opérer une attaque plus critique pour l'entreprise. Cette détection peut se faire via les signatures des offensives les plus connues ou via les anomalies et activités suspectes (par comparaison avec l'activité normale). Aujourd'hui, la prévention d'intrusion tend à remplacer la détection d'intrusion, ajoutant aux fonctionnalités de cette dernière la capacité de stopper les intrusions[106]. Concluons que les systèmes de prévention d'intrusion se nourrissant de bases de données (signatures d'attaques) et stockant des informations (activité de l'entreprise), leur contenu relève en partie du traitement de données personnelles[107]. Cela illustre la double complexité technique et juridique de la protection des données en entreprise.

---

[103] www.cloudflare.com/fr-fr/learning/security/what-is-next-generation-firewall-ngfw.
[104] Carpentier 2023, p. 74.
[105] Par exemple : *Op. cit.*, p. 69-123.
[106] www.varonis.com/fr/blog/ids-et-ips-en-quoi-sont-ils-differents.
[107] www.donneespersonnelles.fr/ids-ips-dlp-il-faut-l-autorisation-de-la-cnil.

2.1.3.2. Le réseau sans fil

Contrairement à un réseau filaire, sur lequel les branchements se font physiquement au sein de l'entreprise, un réseau sans fil est accessible depuis n'importe quel terminal équipé d'un récepteur Wi-Fi, y compris depuis l'extérieur de l'enceinte de l'entreprise. À ce titre, sa sécurisation doit faire l'objet d'une attention particulière, notamment dans les TPE utilisant des box standards, peu sécurisées.

Les recommandations pour sécuriser un réseau Wi-Fi sont nombreuses [108]. Parmi elles, notons les plus importantes :

- Gérer et protéger les accès ;
- Effectuer les mises à jour logicielles des équipements réseau, points d'accès et relais ;
- Changer les configurations par défaut (cause principale de vulnérabilité [109]) ;
- Désactiver la diffusion du nom du réseau ;
- Compléter les mesures de sécurité embarquées ;

Comme pour l'ensemble des mesures de protection du système d'information, la sensibilisation du personnel et l'audit périodique renforceront considérablement la sécurité.

2.1.3.3. La sécurité applicative

La sécurité applicative est également un enjeu majeur. Le périmètre et le patrimoine applicatifs doivent être recensés. Il est évident que plus ces derniers seront étendus, et plus leur sécurisation sera complexe. Il peut donc être utile de faire un premier passage en revue pour se demander quels sont les besoins réels de l'activité et si certaines applications ne sont pas superflues. Dans ce cas, mieux vaut s'en passer afin de réduire d'autant les risques de brèche dans la sécurité du système d'information de l'entreprise.

La revue des applications de l'entreprise comprend celles de son patrimoine mais également celles déportées, utilisées via le cloud. Dans tous les cas, il faut s'assurer des mesures de protection et garanties apportées par l'éditeur afin de procéder à des arbitrages en connaissance de cause.

Il est pertinent de cartographier le système d'information, ainsi que l'éventuel contrôle interne, les ITGC (contrôles informatiques généraux, vérifiant la pertinence des programmes, l'intégrité des applications, données et processus informatiques) et ITAC (contrôles portés sur les applications) mis en place. Les bibliothèques qu'utilisent les applications doivent également être sécurisées, afin de ne pas constituer des portes dérobées menant *in fine* au système d'information de l'entreprise.

De la même façon qu'un bâtiment, un système d'information mal construit ou ne tenant pas compte de son environnement ne pourra résister aux assauts du temps et des éléments (naturels ou non, volontaires ou non).

---

[108] https://cyber.gouv.fr/publications/securiser-les-acces-wi-fi.
[109] Carpentier, 2023, p. 120.

2.1.3.4. La sécurité des communications

Les communications correspondent ni plus ni moins à des entrées et des sorties de données. À ce titre, elles doivent être sécurisées et surveillées.

Une attention particulière doit être portée aux e-mails, moyen de communication le plus courant, mais aussi biais d'infection le plus répandu. En effet, « si communiquer est naturel pour l'homme, échanger des informations dans un système d'information [...] nécessite d'être sensibilisé aux menaces existantes[110]. » Outre la sensibilisation du personnel, certaines mesures peuvent contribuer à améliorer la protection du courrier électronique, comme[111] :

- L'exigence d'une authentification par le serveur de courrier sortant ;
- La fixation d'une limite de destinataires de courriers sortants ;
- La mise en place de notifications pour les volumes de courrier électronique ;
- La restriction d'utilisation des serveurs de messagerie sur Internet ;
- La veille sur les listes noires de référence.

2.1.4. Gestion des accès et politique de mots de passe

Nous l'avons évoqué, le contrôle des accès est l'un des points majeurs de sécurisation d'un système d'information. Celui-ci passe par une gestion des habilitations, un contrôle des accès, une politique de mots de passe et un paramétrage des terminaux utilisés.

2.1.4.1. Gestion des habilitations

Gérer les habilitations revient à limiter l'accès des utilisateurs aux seules données dont ils ont besoin. Ainsi, dans un cabinet d'expertise, un comptable et un responsable du recrutement n'auront pas besoin d'avoir accès aux mêmes informations pour exercer leur activité. Il s'agit donc, par exemple, d'interdire pour le comptable l'accès aux données personnelles des membres du cabinet, et pour le responsable du recrutement l'accès aux états financiers des clients du cabinet.

Chaque entreprise doit donc s'efforcer d'établir des profils d'habilitation (par exemple rattachées à des emploi-type). Par ailleurs, toute demande d'habilitation doit faire l'objet d'une validation par un responsable. Enfin, les habilitations doivent être actualisées en permanence (suppression en fin de contrat, de mission, changement d'affectation, départ de l'entreprise, comptes inutilisés...). Les privilèges accordés doivent être proportionnés aux besoins des utilisateurs à chaque instant. Les droits d'administration doivent être distribués avec méfiance et parcimonie (sur la seule base des besoins opérationnels du salarié et sans lien avec les rapports interpersonnels entretenus avec l'individu).

A minima, une revue annuelle intégrale des habilitations doit être opérée pour s'assurer de leur pertinence opérationnelle et de leur actualisation[112].

---

[110] Arduin, Grundstein et Rosenthal-Sabroux, 2018, p. 59.
[111] Brooks, 2021, p. 587-589.
[112] www.cnil.fr/fr/securite-gerer-les-habilitations.

2.1.4.2. Contrôle des accès

Le contrôle des accès nécessite deux étapes :

- **L'identification :** l'utilisateur établit son identité ;
- **L'authentification :** l'utilisateur apporte la preuve de son identité [113].

Ainsi, tout collaborateur doit disposer d'un identifiant (qui lui est propre et doit être unique : on évitera autant que faire se peut les comptes partagés) et d'un mécanisme d'authentification (mot de passe, carte à puce, biométrique [114]…). Cette authentification est qualifiée de « robuste » si elle repose sur « un mécanisme cryptographique dont les paramètres et la sécurité sont jugés robustes (ex. : clé cryptographique) [115] ».

Par ailleurs, l'authentification à double facteur tend aujourd'hui à se développer. Plus sécurisée que celle à facteur unique, elle consiste à combiner au moins deux méthodes d'authentification différentes (dite 2FA, ou *multi-factor authentification*). La combinaison la plus fréquente est celle associant un mot de passe et un code de vérification envoyé sur un téléphone ou généré par une application tierce sur un appareil autre que celui de la connexion, ou celle impliquant un dispositif physique comme une clé USB, telles les yubikeys [116].

À noter que le contrôle des accès concerne le personnel en interne, mais également les parties prenantes ayant besoin d'un accès aux données du cabinet, tels certains prestataires ou clients.

Soulignons enfin que les comptes partagés sont à proscrire, car ils diluent la sécurité de leur authentification et anonymisent en partie les actions réalisées (ce qui nuit à l'intégrité des données).

2.1.4.3. Politique des mots de passe

Un salarié peut avoir jusqu'à quatre-vingt-dix mots de passe [117] dans le cadre de son travail. Dans ces conditions, la tentation est forte d'utiliser toujours le même mot de passe très simple, ou de noter ses mots de passe sur des post-its au vu et au su de tout le monde. Ainsi, 81 % des atteintes aux données trouvent leur origine dans des mots de passe faibles, compromis ou non mis à jour [118]. L'enjeu de sécurité est tel qu'une journée mondiale du mot de passe a vu le jour pour sensibiliser tout un chacun [119].

---

[113] https://ssi.ac-strasbourg.fr/bonnes-pratiques/recommandations/lidentification-et-lauthentification.
[114] Les données biométriques sont des données personnelles sensibles et à ce titre nécessitent un traitement particulier conforme à l'article 9 du RGPD. Sur ce sujet, voir www.cnil.fr/fr/le-controle-dacces-biometrique-sur-les-lieux-de-travail.
[115] www.cnil.fr/fr/securite-authentifier-les-utilisateurs.
[116] www.yubico.com et www.wikipedia.org/wiki/YubiKey.
[117] https://fidoalliance.org/fido2.
[118] https://linc.cnil.fr/de-azerty-paword-une-revue-des-pratiques-de-gestion-des-mots-de-passe.
[119] www.solutions-numeriques.com/journee-mondiale-du-mot-de-passe-et-si-aujourdhui-vous-jetiez-vos-post-it.

Une politique forte en matière de mot de passe est donc probablement le socle de la protection des données dans une entreprise. Celle-ci pourra s'asseoir sur des arbitrages réalisés sur tout ou partie de ces éléments [120] :

- Catégorie de mots de passe (à mémoriser ou non) ;
- Longueur des mots de passe ;
- Règles de complexité des mots de passe ;
- Délai d'expiration des mots de passe ;
- Mécanismes de limitation d'essais d'authentification ;
- Mécanismes de contrôle de la robustesse des mots de passe ;
- Méthode de conservation des mots de passe ;
- Méthode de recouvrement d'accès en cas de perte ou de vol des mots de passe ;
- Mise à disposition d'un coffre-fort (gestionnaire sécurisé) de mots de passe.

La première des choses à définir est le niveau d'entropie [121] souhaité. Celui-ci conditionnera la longueur (nombre de caractères) et la règle de complexité (les différentes typologies de caractères à utiliser). L'exigence de complexité doit être forte, mais peut être adaptée en fonction des cas d'usage. En cas de doute, des outils existent pour évaluer la robustesse d'un mot de passe, tel celui de la CNIL [122].

DÉFINIR UNE COMPLEXITÉ DES MOTS DE PASSE EN FONCTION DES CAS D'USAGE

> Par défaut, entropie [...] minimale de 80 bits (ex. : 12 caractères minimum comportant des majuscules, des minuscules, des chiffres et des caractères spéciaux ; 14 caractères minimum comportant des majuscules, des minuscules et des chiffres, sans caractère spécial obligatoire) ;
> Entropie de 50 bits (ex. : 8 caractères minimum de 3 types différents ; 16 chiffres) dans le cas où des mesures complémentaires sont en place (restriction de l'accès au compte telle qu'une temporisation de l'accès après plusieurs échecs, la mise en place de « captcha » ou le blocage du compte après 10 échecs) ;
> Entropie de 13 bits (ex. : 4 chiffres) dans le cas d'un matériel détenu par l'utilisateur (ex. : carte SIM, dispositif contenant un certificat) avec blocage au bout de 3 échecs.

Source : www.cnil.fr/fr/securite-authentifier-les-utilisateurs

Contrairement à une idée reçue, le renouvellement régulier des mots de passe n'est pas recommandé, sauf pour les administrateurs. En effet, contraindre les salariés à changer régulièrement leur mot de passe les incite à ne choisir qu'une version légèrement modifiée de leur mot de passe précédent, ou à simplifier leurs mots de passe (plus courts, avec des informations personnelles évidentes telles qu'une année de naissance ou le nom d'un parent...).

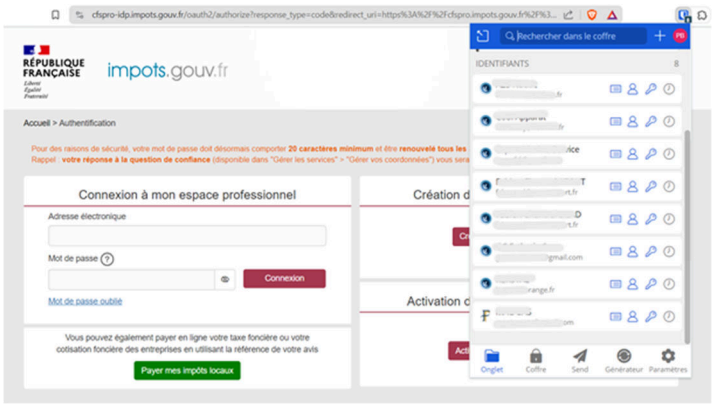
L'utilisation de phrases de passe plutôt que de mots de passe est de plus en plus encouragée, mais là encore, il doit s'agit de phrases dont la composition ne doit pas être évidente (*ceci est*

[120] *Recommandations relatives à l'authentification multifacteur et aux mots de passe*, ANSSI, https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe.
[121] « L'entropie, appliquée à un mot de passe, correspond à sa capacité de résistance à une attaque par force brute », www.cnil.fr/fr/securite-authentifier-les-utilisateurs.
[122] www.cnil.fr/fr/verifier-sa-politique-de-mots-de-passe.

mon mot de passe) ou très connue (l'incipit de *Du côté de chez Swann* de Marcel Proust par exemple). En revanche, elle peut faire appel à l'environnement immédiat pour une meilleure simplicité de mémorisation[123] (*chaise poubelle tiroir post-it stylo PCG*). L'utilisation de *passkeys* [124] plutôt que de mots de passe est elle aussi de plus en plus encouragée par certains acteurs [125].

Une sécurité aisée à mettre en place est celle du verrouillage de compte après un certain nombre de tentatives de connexion infructueuses. Ce paramétrage très simple entrave de façon efficace certaines attaques, telles celles par déni de service (DoS) ou par force brute *(brute force attack)*[126].

La méthode de conservation des mots de passe doit également être définie avec attention. Souvent, les TPE enregistrent leurs mots de passe dans un fichier de tableur intitulé « mots de passe », ce qui représente une brèche de sécurité importante (sauf à chiffrer le fichier, par exemple avec un logiciel de type VeraCrypt[127]). Le plus pertinent, à l'échelle d'un petit cabinet d'expertise-comptable, est sans aucun doute la gestion centralisée via un gestionnaire de mots de passe[128] tels Bitwarden, NordPass, Dashlane, ou encore celui recommandé par l'État français [129] : KeePass. Ces gestionnaires de mots de passe permettent à la fois de générer des mots de passe sécurisés, de les enregistrer pour ne pas avoir à les retenir (seul un mot de passe maître demandé à l'ouverture du gestionnaire de mots de passe est alors à mémoriser) et de les organiser afin d'en avoir un accès sécurisé et aisé. Par ailleurs, certains sont disponibles sous la forme de *plugins* pouvant être ajoutés à leurs navigateurs Internet, ce qui permet de renseigner automatiquement les mots de passe choisis sur les sites nécessitant une authentification, sans pour autant créer une brèche de sécurité comme lorsqu'on enregistre un mot de passe directement sur son navigateur. D'une utilisation très simple et offrant un niveau de sécurité important, ces gestionnaires de mot de passe gagneraient à être plus connus et utilisés par les cabinets d'expertise-comptable. Ils permettent par ailleurs, pour les versions non locales, de retrouver ses mots de passe sur n'importe quel terminal en se connectant tout simplement à son compte sur le logiciel ou le plugin du gestionnaire.



À gauche de la fenêtre, le plugin du gestionnaire de mots de passe Bitwarden.

[123] www.cyber.gc.ca/fr/orientation/pratiques-exemplaires-de-creation-de-phrases-de-passe-et-de-mots-de-passeit-sap30032#:~:text=Une%20phrase%20de%20passe%20est,4%20mots%20et%2015%20caract%C3%A8res.
[124] Méthode d'authentification combinant reconnaissance du terminal et reconnaissance de l'utilisateur.
[125] support.google.com/accounts/answer/13548313?hl=fr.
[126] Carpentier, 2023, p. 183.
[127] www.cnil.fr/fr/securite-chiffrement-hachage-signature.
[128] www.cnil.fr/fr/5-arguments-pour-adopter-le-gestionnaire-de-mots-de-passe.
[129] https://next.ink/15854/97812-l-etat-renouvelle-son-socle-interministeriel-logiciels-libres.

Notons que le mot de passe maître devant être renseigné à l'ouverture du gestionnaire de mots de passe doit respecter des exigences minimales de sécurité pour que l'utilisation du gestionnaire puisse être considérée comme sûre.

Enfin, ces gestionnaires de mot de passe ne peuvent être considérés comme sûrs à 100%, rien ne l'étant en matière informatique. Il faudra donc veiller à sauvegarder la base de mots de passe, et à ne surtout pas stocker cette sauvegarde en clair (il faudra la chiffrer, par exemple avec VeraCrypt, et la stocker si possible sur un dispositif non relié au réseau).

Pour résumer ce sujet fondamental, voici les quelques mesures simples à mettre en œuvre pour avoir une politique de mot de passe sécurisée[130] :

- Imposer un niveau d'entropie pouvant varier en fonction des cas d'usage ;
- Inciter les administrateurs au renouvellement périodique des mots de passe, mais ne pas le faire pour les autres utilisateurs ;
- Imposer une entropie plus élevée pour les administrateurs et faire respecter les règles relatives au renouvellement périodique des mots de passe (par exemple en bloquant les comptes lorsque lesdites règles ne sont pas respectées) ;
- Obliger tout utilisateur à modifier tout mot de passe attribué automatiquement (par un administrateur, un équipement, un site, un programme…), sauf pour ceux générés par l'utilisateur via un gestionnaire de mots de passe ;
- Désactiver les comptes par défaut ;
- Chiffrer les bases de mots de passe au moyen d'un outil cryptologique reconnu et éprouvé ;
- Privilégier l'authentification multifacteurs ;
- Limiter le nombre de tentatives d'accès aux comptes utilisateurs sur les postes de travail ; et bloquer l'accès au compte temporairement ou non, lorsque sa limite est atteinte.

Enfin, notons que même avec le mot de passe le plus sécurisé qui soit, un compte non verrouillé ne sera aucunement protégé. En complément de la nécessité de mots de passe forts vient donc celle de verrouiller son terminal lorsqu'on ne l'utilise pas et *a fortiori* lorsqu'on n'est pas physiquement en sa présence. Notons également que la base de données de mots de passe doit être mise à jour en continu et son administration doit être aisément transférable en cas de départ de son responsable.

2.1.4.4. La signature numérique et la signature électronique

Dans un cabinet d'expertise-comptable, les associés ont constamment besoin de signer des documents, depuis la lettre de mission d'un client jusqu'à ses états financiers. Le fait d'imprimer signer, scanner puis envoyer un document tend à disparaître au profit de technologies de signature électronique (ou signature numérique). Celles-ci permettent à la fois d'authentifier l'auteur du document, de garantir l'intégrité du message et de prouver que ce dernier a bien été transmis

[130] D'après www.cnil.fr/fr/securite-authentifier-les-utilisateurs.

à son destinataire. Ainsi, la signature numérique assure tout à la fois l'intégrité, la confidentialité, la preuve et la non-répudiation de la donnée [131]. Elle est composée de trois éléments : le document lui-même, la ou les signatures et un certificat électronique authentifiant le ou les signataires.

Pour la profession comptable, l'outil jesignexpert de l'association ECMA [132] est très largement répandu et a le mérite d'être intégré à un écosystème d'autres éléments utiles dans le cadre de la profession (notamment jedeclare).

2.1.5. La vigilance humaine

Yann Salamon constate que la notion de protection informatique est « trop souvent cantonnée à un domaine de techniciens » et témoigne d'un manque d'« hygiène cyber[133] ». De fait, nous l'avons évoqué, l'humain est souvent le maillon faible de la cyberdéfense d'une entreprise.

2.1.5.1. La prise de conscience individuelle et collective

Une prise de conscience à la fois de la menace et de son propre rôle dans la sécurité globale des données de son entreprise est donc nécessaire à tous les maillons de la chaîne, du *top management* aux salariés, en passant par les partenaires, sous-traitants et clients. Sans oublier les stagiaires, qui, bien souvent, ne bénéficient pas des formations d'accueil prodiguées aux nouveaux salariés tout en ayant des accès aux données de l'entreprise [134].

Tout individu ayant un accès aux données du cabinet d'expertise-comptable doit être conscient qu'il représente, par ses actions ou sa négligence, une menace potentielle, soit directe (par exemple une suppression ou une altération même involontaire des données), soit indirecte (via une attaque par ingénierie sociale par exemple).

2.1.5.2. La mise en place d'une politique de formation et d'information

L'ensemble des parties prenantes du cabinet d'expertise comptable doit ainsi être sensibilisé et formé aux enjeux de la sécurité des données et aux bonnes pratiques de cybersécurité. Tous doivent être capables plus ou moins finement d'identifier le caractère sensible des données qu'ils utilisent.

Dans un univers dans lequel des cyberattaques d'ampleur et très médiatisées interviennent presque chaque mois, il est étonnant de constater que les mots de passe utilisés sont toujours aussi faibles, que les post-its émaillant les écrans d'informations d'authentification sont toujours aussi répandus [135]. Si la sensibilisation à l'identification des e-mails frauduleux est plus courante, ces derniers sont chaque jour mieux rédigés et de nouvelles menaces naissent (textos, QRcodes…), ce dont les salariés ne sont pas toujours conscients. Ainsi, chaque entreprise doit opérer une veille et sur les nouvelles menaces et communiquer sur le sujet en temps réel afin de susciter et d'accompagner l'évolution des comportements pour s'adapter à l'évolution des risques et menaces.

---

[131] Assurance qu'une action réalisée par un utilisateur ne peut être répudiée par celui-ci.
[132] https://ecma-solutions.com/produits-expert-comptable/jesignexpert.
[133] Salamon, 2020.
[134] Lacombe et Lesage, 2021, p. 142.
[135] Voir un exemple d'affiche de sensibilisation proposée par la CNIL en annexe 9.

Dans l'idéal, des formations dédiées à la cybersécurité doivent être imposées à tout nouvel arrivant et régulièrement par la suite pour mettre à jour les connaissances des salariés en termes de menaces, de conformité réglementaire, de comportements à risque. Même informelles, celles-ci devraient constituer, aux côtés de la politique des mots de passe et de celle des sauvegardes, les points d'action majeurs des cabinets d'expertise comptable pour améliorer la sécurisation de leurs données. La rédaction d'une charte peut par ailleurs être un complément et une référence utile pour tous dans l'entreprise [136].

Notons également que la sensibilisation des salariés est au cœur du *mooc* de l'ANSSI [137] et de l'outil de sensibilisation Senscyber de cybermalveillance.gouv.fr [138].

2.1.5.3. Le cloisonnement entre usages personnels et professionnels

La séparation des usages professionnels et personnels des terminaux (ordinateurs, téléphones portables…), outils (comme les adresses e-mail) et comptes utilisateurs est une mesure d'hygiène informatique souvent peu mise en place dans les très petites structures. Elle est pourtant d'importance, et constitue d'ailleurs l'une des treize mesures prioritaires de cybersécurité dédiées aux TPE et PME recommandées par l'ANSSI [139].

2.1.5.4. L'adhésion des collaborateurs

La sécurité entraîne des procédures qui surchargent les collaborateurs en multipliant les procédures, les mots de passe, etc. Si les salariés estiment que le coût des procédures est supérieur au bénéfice de sécurité qu'elles apportent, ils peuvent mettre en place des techniques de contournement ou d'évitement qui peuvent se révéler dévastatrices [140]. Il est donc essentiel à la fois de faire la pédagogie des mesures prises, mais également de chercher à emporter l'adhésion des collaborateurs pour s'assurer une participation efficace.

2.1.5.5. Le fardeau de la responsabilité.

L'une des problématiques actuelles est que le fardeau de la sécurité pèse autant, voire plus sur l'utilisateur d'un programme que sur ses créateurs – alors même que l'utilisateur n'est pas armé pour assumer ce fardeau. Même Internet n'a pas été conçu avec la sécurité des données en but final (l'objectif étant la résilience de fonctionnement [141]). Le gouvernement états-unien s'est d'ailleurs saisi de ce sujet et cherche les voies pour transférer la responsabilité de la cybersécurité des particuliers et des petites entreprises vers les grands groupes, les entreprises et éditeurs informatiques, et le gouvernement, qui sont « plus à même de gérer une menace en constante évolution [142]. »

En France, le gouvernement n'a pas encore pris la mesure de ce phénomène, comme en témoigne Patrick Proniewski, chef du service Opérations de la DSI de l'université Lyon 2 et RSSI.

---

[136] https://cyber.gouv.fr/publications/guide-delaboration-dune-charte-dutilisation-des-moyens-informatiques-et-des-outils.
[137] https://secnumacademie.gouv.fr.
[138] www.cybermalveillance.gouv.fr/sens-cyber/apprendre.
[139] https://cyber.gouv.fr/publications/la-cybersecurite-pour-les-tpepme-en-treize-questions.
[140] Arduin, Grundstein et Rosenthal-Sabroux, 2018, p. 80.
[141] Salamon, 2020, p.53.
[142] www.lemondeinformatique.fr/actualites/lire-la-maison-blanche-exhorte-les-developpeurs-a-abandonner-c-et-c-93089.html.

Au sujet d'une vulnérabilité sur la messagerie Outlook, l'ANSSI enjoint de « sensibiliser l'ensemble du personnel ayant accès à une messagerie Outlook à la nécessité de ne pas ouvrir les courriels d'origine inconnue ou incertaine, et de toujours vérifier l'origine d'un courriel - par exemple, par un appel téléphonique à l'émetteur, en cas de doute.» Réaction de Patrick Proniewski : « Au mépris total de la réalité de terrain, le fer de lance français de la défense des systèmes d'information promeut des actions intenables, irréalistes et qui — ce n'est pas rien — accentuent la pression sur les victimes potentielles [143]. » Gageons que sur ce sujet, l'État fera son chemin et mettra en place des mesures à l'image de son homologue états-unien.

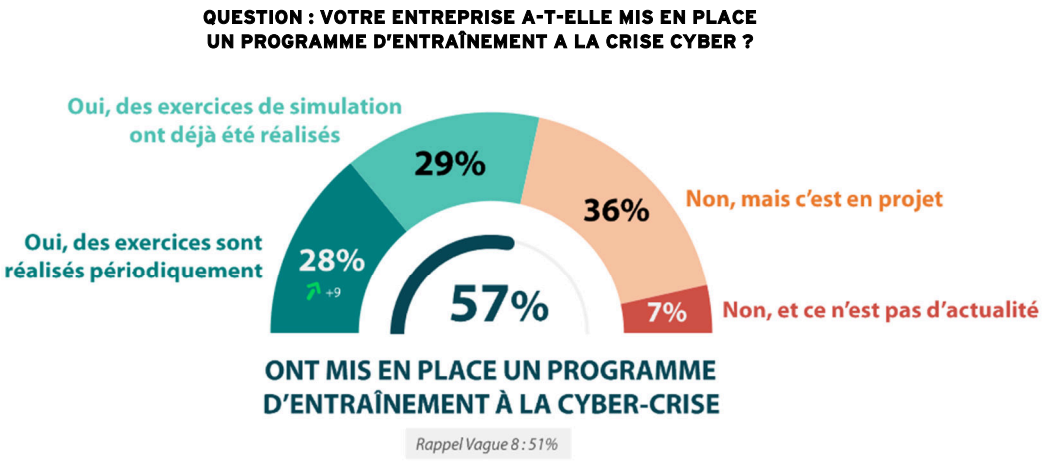
2.1.6. La gestion des incidents de sécurité

2.1.6.1. Le plan de réponse

Si les grandes entreprises disposent d'un « plan de réponse » en cas d'incident de sécurité, c'est rarement le cas pour les plus petites structures. Sans entrer dans les détails d'un plan qui doit être mûrement réfléchi et structuré, citons les grands axes de ce type de plan :

- Détection, identification (nature, source, gravité, impact) ;
- Endiguement et isolement des systèmes et données affectées ;
- Mise en place de mesures correctives temporaires ;
- Investigation et analyse (cause de l'incident, vulnérabilités exploitées, impact sur l'organisation ;
- Éradication et restauration, nettoyage des traces de l'incident ;
- Apprentissage (mise à jour des plans de réponse, de la documentation, des formations des équipes) et amélioration des pratiques et mesures de sécurité ;
- Partage d'expérience avec les autorités et organisations de sécurité ;
- Suivi et reporting des actions et mesures correctives menées à la suite de l'incident.

Le plan de réponse doit être mis à jour et testé régulièrement.



Source : Baromètre annuel de la cybersécurité des entreprises, CESIN, 2024.

[143] https://mastodon.green/@patpro/112019067499301372.

2.1.6.2. La communication

Tout au long de la gestion de l'incident, la communication est un enjeu majeur, aussi bien pour coordonner les intervenants et assurer une continuité de l'activité pendant la gestion de l'événement que vis-à-vis des parties prenantes de l'entité, afin de jouer sur la transparence et rassurer.

Un défaut de communication peut amplifier la crise, soit du fait d'un afflux de recours à la *hotline* informatique, de salariés cherchant à résoudre eux-mêmes un problème qui peut les dépasser (et pouvant conduire à des actions contre-productives), d'équipes informatiques mal coordonnées, ou, en externe, d'une rupture du lien de confiance avec ses parties prenantes.

2.1.6.3. L'amélioration continue

« L'homme sage apprend de ses erreurs », disait Confucius. Ainsi, chaque incident de sécurité, une fois résolu, doit faire l'objet d'une analyse pour en déterminer les causes : quelles erreurs ont été commises, quelle protection supplémentaire envisager, etc. L'apprentissage permanent permet à la fois d'améliorer ses pratiques et outils, mais également de s'adapter aux évolutions des menaces. Par ailleurs, en réalité, la citation complète de Confucius est « L'homme sage apprend de ses erreurs, l'homme plus sage apprend des erreurs des autres. » Et de fait, s'il est essentiel d'apprendre de ses propres incidents de sécurité, une veille attentive de son environnement et des attaques subies par ses pairs s'avérera tout aussi importante. En cela, il est également fondamental de partager ses propres expériences (notamment avec les autorités) pour en faire bénéficier les autres.

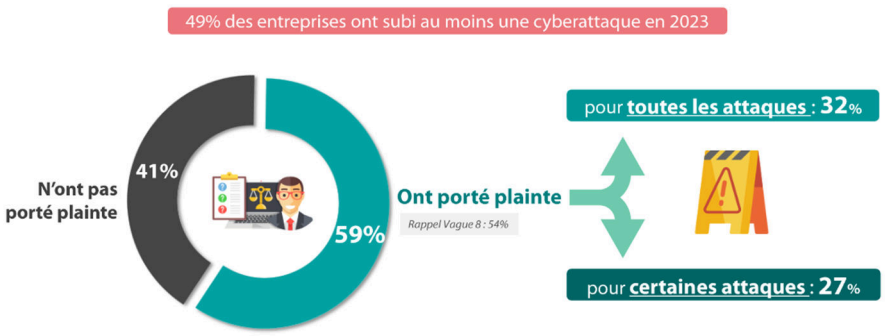
Et selon les experts sécurité : **«il ne faut pas se demander si l'on va être victime d'une cyber attaque, mais quand » !**

Signature d'e-mail des collaborateurs d'Orange pro. Extrait d'un e-mail reçu chez Eilad Expert le 05/03/2024.

2.1.6.4. Le signalement

Ainsi, chaque incident de sécurité doit faire l'objet d'un signalement, et le cas échéant d'une plainte. Pour l'heure, les chiffres montrent que le dépôt de plainte est loin d'être systématique.

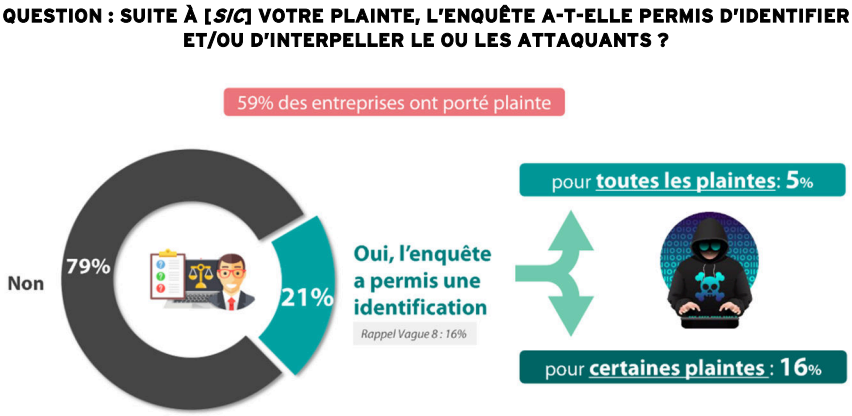
QUESTION : AVEZ-VOUS PORTÉ PLAINTE À LA SUITE DE LA CYBERATTAQUE DONT VOTRE ENTREPRISE A ÉTÉ VICTIME ?



Source : Baromètre annuel de la cybersécurité des entreprises, CESIN, 2024

On peut supposer que le risque réputationnel peut conduire certaines entreprises à éviter ce type de démarche pour rester discret sur l'incident. Mais il est à parier que beaucoup d'entre

elles ne portent pas plainte car elles n'en voient pas l'utilité (notamment car il est rare que la plainte donne des résultats).



Source : Baromètre annuel de la cybersécurité des entreprises, CESIN, 2024

Toutefois, un signalement plus régulier des incidents serait bénéfique à tous, car il permettrait notamment d'établir des statistiques permettant d'orienter au mieux les actions des différents opérateurs (étatiques ou non) en matière de cybersécurité et de sensibilisation, et car il représenterait un retour d'expérience enrichissant pour tous.

Notons que les statistiques de dépôt de plainte devraient évoluer en parallèle de l'évolution des assurances cyber, qui imposent cette procédure pour faire jouer leurs garanties.

2.1.7. Audit régulier et contrôle interne

La surveillance du système d'information passe non seulement par la veille et le contrôle interne, mais également, le cas échéant, par un audit régulier visant à accréditer la qualité du système d'information et de ses données. L'audit peut être de portée générale ou s'intéresser à un point très précis (telle la séparation entre gestion des habilitations et utilisation des privilèges).

L'audit peut viser la conformité des pratiques de l'organisation à un éventuel référentiel comme une norme ISO (cet audit est bien entendu réalisé par une équipe indépendante de celle chapeautant la gouvernance du système d'information [144]), il peut également concerner la conformité réglementaire (par exemple RGPD), le contrôle d'un sous-traitant [145]…

Tandis que la fréquence des audits doit être définie par la politique de gouvernance, l'audit contrôle la gouvernance, ainsi que la mise en œuvre et l'efficacité de ses mesures [146].

Si l'audit est réalisé par un cabinet externe, l'auditeur suivra la norme d'exercice professionnelle 315§14, lui intimant de prendre connaissance des « procédures de contrôle interne en place, et notamment la façon dont l'entité a pris en compte les risques résultant de l'utilisation de traitements informatisés[147]. » Il peut se faire sur la base d'un référentiel, tel l'ISO 27002 [148].

---

[144] Lacombe et Lesage, 2021, p. 258.
[145] Imposer un audit à ses sous-traitants n'est bien sûr possible que pour de très grandes entreprises.
[146] Ibid, p. 121.
[147] https://doc.cncc.fr/docs/nep-315-connaissance-de-lentite.
[148] Lacombe et Lesage, 2021, p. 259.

2.2. Le plan de sauvegarde et de restauration des données

2.2.1. Sauvegarde et archivage

Le fait de faire des copies de ses données peut avoir plusieurs finalités, que l'on regroupe sous deux dénominations : sauvegarde et archivage. La sauvegarde consiste à dupliquer des données à l'identique pour pouvoir les restaurer en cas de dommage, d'altération ou de perte. L'archive, quant à elle, consiste à copier ou déplacer les données sur un support d'archivage (les données d'origine ne sont pas toujours conservées) afin de conserver une trace et un accès aux données anciennes, pour satisfaire à des obligations administratives ou légales (conservation des factures pendant cinq ans), ou comme éléments de preuve. Pour l'archivage, une technologie non réinscriptible peut être intéressante à envisager (par exemple le stockage WORM : *write once/read many*[149]). L'AFNOR a défini plusieurs normes sur le sujet de l'archivage, qu'il est utile de consulter[150].

Sauvegarde et archivage ne sont pas exclusifs l'un de l'autre : ils doivent tous deux être opérés afin d'assurer la sécurité des données, et la conformité aux réglementations et aux besoins en termes d'historicité.

Sauvegarde et archivage sont parmi les éléments les plus critiques de la sécurité des données d'une entreprise. Leur politique doit être définie avec soin, leur mise en œuvre opérée avec constance, leur résultat testé régulièrement. Nous nous concentrerons ici sur le plan de sauvegarde, étant entendu que celui d'archivage aura les mêmes problématiques :

- **L'intégrité :** exactitude, exhaustivité et cohérence globales des données ;
- **Le chiffrement :** les données sont protégées par un chiffrement limitant leur accès et consultation aux seules personnes habilitées et autorisées ;
- **L'accessibilité :** les données doivent rester accessibles afin d'être utilisées en cas de besoin ;
- **Redondance :** les données doivent être copiées sur plusieurs supports afin que l'un prenne le relais si l'autre connaît une défaillance ou un incident de sécurité.

2.2.2. Le plan de sauvegarde

2.2.2.1. Évaluation des besoins

Le plan de sauvegarde doit tout d'abord s'appuyer sur une évaluation des besoins : il faut identifier les données et systèmes critiques à sauvegarder. En d'autres termes, il s'agit de définir le périmètre de la sauvegarde.

2.2.2.2. Méthode de sauvegarde

Ensuite, il faut choisir la ou les méthodes de sauvegarde appropriées : locales, sur un *cloud*, ou hybrides. En local sur un support non connecté au réseau, les données seront plus à l'abri des attaques externes, mais plus sensibles à la panne matérielle, aux sinistres… Sur le *cloud*, les redondances

[149] www.techtarget.com/searchstorage/definition/WORM-write-once-read-many.
[150] Notamment les normes NF Z042-013, NF Z042-020 et NF Z042-026. Voir Carpentier, 2023, p. 320.

déjà opérées par les opérateurs offrent un bon niveau de sécurité, si tant est que ces redondances ne soient pas toutes opérées sur le même site (sur ce sujet, voire les dommages générés par l'incendie chez OVH en 2021 [151]). En revanche, elles peuvent être piratées, relèvent parfois de juridictions moins protectrices des données que l'Europe (voir par exemple le scandale des données de Doctolib stockées chez Amazon [152]) et sont onéreuses lorsque la taille des données à sauvegarder est importante. Le temps d'indisponibilité maximal acceptable pour la récupération des données est également un des critères dans le choix de la méthode de sauvegarde : une sauvegarde en local stockée hors site sera plus longue à mobiliser en cas de besoin qu'un stockage sur le *cloud*.

Le choix de la méthode dépend de nombreux facteurs, parmi lesquels le coût du support, le temps de disponibilité et la garantie du respect des réglementations auxquelles les données sont soumises [153].

2.2.2.3. Typologie des sauvegardes

Une sauvegarde, au sein du périmètre défini au cours de l'évaluation des besoins, peut être :

- **Complète :** copie intégrale des données ;
- **Incrémentielle :** copies des seules données qui ont été modifiées depuis la dernière sauvegarde complète ;
- **Différentielle :** copie de toutes les données qui ont été modifiées depuis la dernière sauvegarde complète ou incrémentielle.

Ce choix affectera la rapidité des sauvegardes et l'espace à leur allouer[154].

2.2.2.4. Stratégie de sauvegarde

La stratégie de sauvegarde consiste à définir divers critères constitutifs des sauvegardes qui seront réalisées :

- **La fréquence des sauvegardes** dépend d'un arbitrage entre la criticité des données, le temps et les moyens accordés à la sauvegarde ;
- **Le nombre des sauvegardes** est lié à l'espace qu'on leur alloue. Par exemple, si l'on définit ce nombre à quatre, on opérera quatre sauvegardes, puis la cinquième sauvegarde viendra écraser la plus ancienne ;
- **La redondance** entraîne des besoins financiers accrus, mais permet de sécuriser la sauvegarde : si l'un des supports connaît un incident et qu'elle a besoin d'être mobilisée, il suffit de recourir à l'une des autres copies. Si la redondance des sauvegardes est une nécessité, leur trop grand nombre sera contre-productif, tant en termes financiers qu'en

[151] www.journaldunet.com/cloud/1499203-incendie-d-ovh-a-strasbourg-une-heure-pour-couper-le-courant.
[152] www.liberation.fr/economie/economie-numerique/les-services-essentiels-de-sante-devraient-relever-du-bien-commun-20210731_KCXM2THINNBTRFV5U64ST6C4RI. Ce scandale pourrait être qualifié de scandale d'État, étant donné la légèreté avec laquelle l'État a géré ce dossier, s'agissant en plus d'une entreprise privée dont il a largement fait la promotion au cours de la crise Covid, alors même que des solutions plus respectueuses des données personnelles et aux partenaires moins sulfureux existaient.
[153] Voir annexe 10.
[154] Voir annexe 11.

termes de disponibilité des serveurs et des périphériques. La méthode communément recommandée est la règle 3-2-1[155] :

- 3 copies différentes ;
- 2 supports différents : par exemple un disque dur interne qui permet un accès immédiat à la sauvegarde et un disque dur externe qui peut être à la fois déconnecté du réseau hors période de génération de la sauvegarde et stocké hors site (donc prémuni en cas de sinistre dans l'entreprise) ;
- 1 site distant : stocker l'une des copies sur un site distant (*cloud* ou autre prestataire – ou *a minima* hors périmètre physique de l'entreprise).

2.2.2.5. Application de sauvegarde

Le choix de l'application doit correspondre aux besoins de l'entreprise. Il doit être testé en amont à la fois sur la sauvegarde et la restauration.

2.2.2.6. Fenêtre de sauvegarde

La réalisation d'une sauvegarde est une opération qui peut être gourmande en ressources informatiques et provoquer l'indisponibilité temporaire des fichiers sauvegardés. Il est donc pertinent de définir des fenêtres de sauvegarde à des périodes d'inactivité (la nuit) ou de faible activité (le midi par exemple).

2.2.2.7. Protection de la sauvegarde

Au même titre que la donnée primaire, celle figurant sur une sauvegarde doit être protégée. Ainsi, il est nécessaire de s'enquérir des conditions de sécurité chez l'éventuel prestataire de sauvegarde ou de *cloud*, et de chiffrer les sauvegardes réalisées par l'entreprise elle-même. La sécurité des opérations entre client et serveur doit également faire l'objet d'une attention particulière.

2.2.2.8. Tests et mise à jour de la stratégie

Enfin, il faut régulièrement tester les solutions de sauvegarde et les sauvegardes elles-mêmes pour garantir leur validité. Une sauvegarde réalisée régulièrement mais qui se révélerait inutilisable le jour où l'entreprise en a besoin serait d'une piètre utilité.

Il faut par ailleurs mettre à jour le plan de sauvegarde en fonction de l'évolution des besoins, des technologies et/ou des menaces.

En conclusion, il n'existe pas de solution toute faite en matière de sauvegarde, chaque entreprise doit définir ses propres besoins et solutions en fonction de son périmètre de sauvegarde, de son budget et de ses autres arbitrages. Toutefois, il est essentiel de prévoir une redondance des sauvegardes, de les protéger et de les tester régulièrement pour s'assurer de leur intégrité et de leur disponibilité. Notons

[155] Carpentier, 2023, p. 250.

par ailleurs que des sauvegardes complètes doivent être réalisées de manière ad hoc en cas de grand changement dans l'entreprise (mise à jour importante, migration de logiciel, etc.).

2.2.3. Les plans de continuité et de reprise d'activité

Le plan de continuité d'activité (PCA) vise à assurer la continuité de l'activité même en cas d'incident grave. Il suppose donc une grande disponibilité des sauvegardes.

Le plan de reprise d'activité (PRA), quant à lui, ne cherche pas l'ininterruption de l'activité, mais se focalise sur la reprise de cette dernière après un arrêt dû à un incident majeur. Il a un moindre coût financier, mais une interruption d'activité peut parfois être fatale à une entreprise.

Ces plans sont constitués de mesures et de procédures visant à protéger les données, maintenir ou rétablir l'activité au plus vite et conserver la confiance des clients en montrant la capacité du cabinet à gérer une crise d'ampleur. Ils sont le pendant des sauvegardes, qui sont leurs matières premières.

Les notions de PCA et PRA ne relevant pas de la sécurité des données (même si cette assertion fait débat[156]), nous ne les aborderons pas plus avant dans le cadre du présent mémoire. Pour plus d'informations sur ce sujet, consulter par exemple :

- **Le guide de la continuité d'activité du Secrétariat général de la défense et de la sécurité nationale** (https://guide-continuite-activite.sgdsn.gouv.fr/)
- **Le kit PCA à l'usage du chef d'entreprise** de la Direction générale des entreprises (www.entreprises.gouv.fr/files/files/directions_services/politique-et-enjeux/entrepreneuriat/Guide-PCA-en-cas-de-crise-majeure.pdf)
- **La norme ISO 22301 sur la continuité d'activité** (https://certification.afnor.org/gestion-des-risques-sst/certification-iso-22301-continuite-d-activite)
- **La norme ISO 27000 sur le management du risque** (www.iso.org/fr/standard/73906.html)

2.3. Le *cloud computing*

2.3.1. Les modèles de *cloud computing*

Le *cloud computing* fait référence à l'utilisation des capacités de calcul et de la mémoire de serveurs et ordinateurs liés par un réseau. « Les applications et les données ne se trouvent plus sur un ordinateur déterminé mais dans un nuage (*cloud*) composé de nombreux serveurs distants interconnectés[157] ». À ce titre, le *cloud computing* consacre « un effritement progressif de la notion de périmètre des systèmes d'information[158] ».

Pour les cabinets d'expertise-comptable de type TPE et PME, le cloud est une technologie intéressante en ce qu'elle permet de répondre à tout ou partie de ses besoins en termes de stockage, de traitement des données, de gestion des services, tout en éludant les investissements d'un équipement en propre. Par ailleurs, le fait de « louer » espace, capacité, logiciels et licences

[156] Sur ce sujet, voir Lacombe et Lesage, p. 136.
[157] www.cnil.fr/fr/definition/cloud-computing.
[158] Salamon, 2020, p. 33.

logicielles permet de s'adapter quasiment en temps réel à la hausse comme à la baisse, pour ne payer que ce dont l'entité a besoin au temps t[159].

Le *cloud computing* existe sous plusieurs formes :

- Le *software-as-a-service* : logiciel à la demande en tant que service ;
- Le *plateforme-as-a-service* : plateforme de traitement complète pour l'utilisateur (ex : Google Apps) ;
- L'*infrastructure-as-a-service* : infrastructure de traitement complète (ex : Windows Azure) ;
- Le *data-as-a-service* : les données relevant de l'application métier sont stockées en ligne et mises à disposition pour toute personne autorisée quels que soient son emplacement géographique et son équipement informatique. C'est le modèle souvent utilisé pour les progiciels de gestion intégrée ;
- Le *datawarehousing-as-a-service* : externalisation de la configuration et des ressources matérielles nécessaires pour le stockage de données ;
- Le *desktop-as-a-service* : poste de travail virtualisé au sein duquel l'environnement de travail est totalement décorrélé du terminal utilisé ;
- Le *storage-as-a-service* : stockage et accès aux données en ligne.

Notons que dans les grandes entreprises ayant d'importants besoins informatiques et pouvant y consacrer beaucoup de moyens, le *cloud* peut être internalisé.

2.3.2. *Cloud* et sécurisation des données

Le *software-as-a-service* transfère la responsabilité de la sécurisation des données au prestataire. L'avantage majeur pour un cabinet d'expertise-comptable est le moindre besoin de se doter de compétences en interne sur le sujet. En revanche, comme dans toute délégation, le transfert de responsabilité suppose une relation de confiance et nécessite donc un choix attentif du prestataire. Il paraît opportun de recueillir des avis, et notamment de chercher à savoir si le prestataire a déjà connu des incidents, comment se sont passées leur résolution et dans quels délais. Le contrat de service doit précisément définir les obligations et responsabilités de chacun, notamment sur le sujet de la protection des données. Par ailleurs, notons que si la responsabilité de la protection des données est transférée au prestataire dans le cadre de la relation contractuelle qui le lie au cabinet d'expertise-comptable, ce dernier reste le responsable *in fine* de la sécurité des données au regard de la loi et à celui de ses clients.

Notons que quel que soit le niveau de délégation de la sécurisation des données, le cabinet d'expertise-comptable en gardera toujours une part. Par exemple, il ne pourra s'affranchir d'une politique de mots de passe solide sous peine d'ouvrir la porte de son *cloud* à des indésirables, ou encore d'une politique d'habilitations et de privilèges sous peine d'accorder des droits

[159] Un panorama non exhaustif des avantages et inconvénient du *cloud computing* est proposé en annexe 12.

d'administration à des individus ne possédant pas les compétences pour les gérer, négligents, ou malveillants. Ainsi, il est essentiel de garder à l'esprit que la délégation de la sécurisation des données n'exonère en rien la nécessité pour un cabinet d'expertise comptable de mettre en place une politique de sécurité informatique.

2.4. Les assurances cyber

2.4.1. Un marché exponentiel

L'augmentation exponentielle des cyberattaques et de l'importance des données dans l'activité et la richesse de l'entreprise ont conduit les assureurs à proposer des solutions dédiées pour permettre aux entreprises de se prémunir contre le coût des attaques cyber[160].

Conscient de la menace, la direction générale du Trésor a publié en 2022 un plan d'action pour accompagner le développement de l'assurance du risque cyber[161]. Mais force est de constater que celui-ci n'est pas garanti, les assureurs ayant du mal à trouver un modèle économique pérenne sur ce segment[162].

CHIFFRES CLÉS

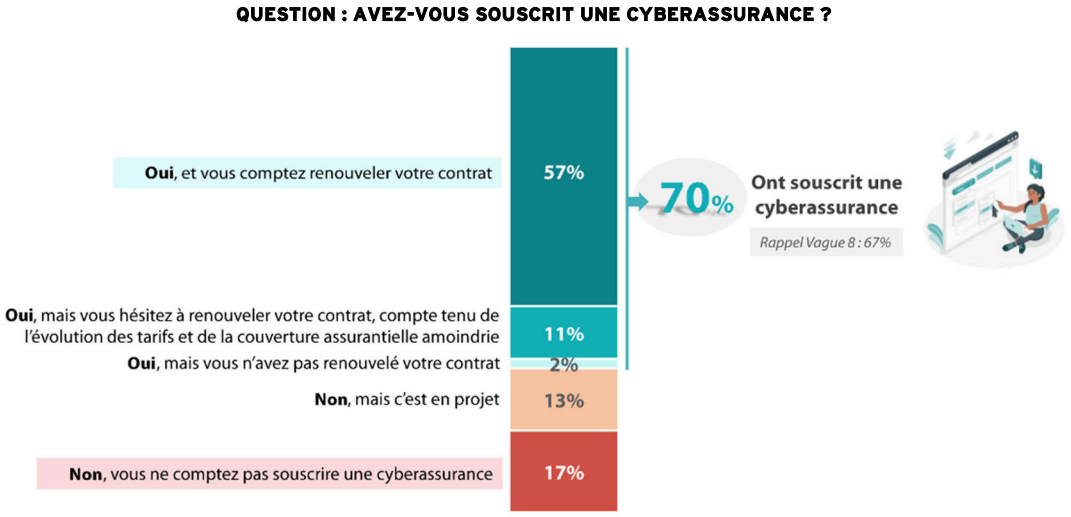
> **54 %** : c'est la part des entreprises françaises qui auraient fait l'objet d'une cyberattaque en 2021 (source baromètre de la cybersécurité en entreprise CESIN 2022) ;
> **219 M€** : c'est le chiffre d'affaires du marché français de l'assurance cyber en 2021, soit 0,35% du chiffre d'affaires des assurances de biens et responsabilité (source : France Assureurs) ;
> **52 %** : c'est la croissance des cotisations en 2021 de l'assurance du risque cyber, ce qui en fait le segment le plus dynamique du marché des assurances de biens et responsabilité (source : France Assureurs) ;
> **97 %** : c'est la part des sinistres cyber couverts par une assurance cyber en France qui ont *[sic]* donné lieu à une indemnisation inférieure à 3 M€ en 2021, ce qui souligne que le risque cyber reste pour l'essentiel maîtrisable (source : AMRAE) ;
> **84 % et moins de 0,3 %** : il s'agit des taux de couverture respectifs par un contrat d'assurance cyber des grandes entreprises et des PME en France en 2021. Ce chiffre témoigne d'une prise de conscience très hétérogène face au risque cyber (source : AMRAE).

www.tresor.economie.gouv.fr/Articles/2022/09/07/remise-du-rapport-sur-le-developpement-de-l-assurance-du-risque-cyber

Du côté des entreprises, la demande va également croissant, malgré une grande défiance à l'égard des clauses et causes d'exclusion des garanties des assurances cyber (par exemple, si une attestation d'attaque de l'hébergeur est requise lorsque celui-ci est attaqué, il paraît vraisemblable que le document sera difficile à obtenir en plein branle-bas de combat pour ses clients, augmentant le délai de recours pour ces derniers, voire son abandon). Par ailleurs, les critères d'exclusion se durcissent chaque année et les primes augmentent à l'avenant : « Le risque cyber est de plus en plus difficile à évaluer car les techniques d'attaques évoluent de plus en plus rapidement et il est de plus en plus difficile de s'en prémunir. C'est une des raisons pour laquelle les assurances cyber traditionnelles ont décidé d'augmenter leurs primes et de durcir leurs critères d'exclusion en 2021. Les PME, quant à elles, rencontrent des difficultés croissantes à se couvrir contre un risque qui les touche de plus en plus[163]. » Face aux refus d'assurance ou à des exclusions trop restrictives, certains ont d'ailleurs décidé d'unir leurs forces pour lancer une société commune d'assurance contre les risques cyber (voir le cas de Miris Insurance[164], lancé, entre autres, par Michelin, Veolia et Airbus[165]).

[160] Voir annexe 13.
[161] www.tresor.economie.gouv.fr/Articles/00367730-14c0-4303-95af-eeb6442fb19b/files/108f9b50-5480-4810-ae7d-7f7845ba7805.
[162] www.atlas-mag.net/category/tags/focus/le-marche-mondial-de-la-cyberassurance.
[163] www.stoik.io/cybersecurite/chiffres-cles.
[164] www.miris-insurance.com.
[165] www.argusdelassurance.com/assurance-dommages/risques-d-entreprise/cyber-miris-la-mutuelle-des-entreprises-obtient-son-agrement.209426.

Malgré ce constat, de nombreuses entreprises font le choix de souscrire une assurance cyber. Le taux de recours à ces assurances est d'environ 25 % pour l'année 2024, dont la moitié par des assurés considérant que celui-ci a été complexe[166].



Source : Baromètre annuel de la cybersécurité des entreprises, CESIN, 2024

Les assurances cyber souffrent de deux limites importantes : d'une part, la difficulté d'évaluer la menace cyber au moment de la demande de police d'assurance, cette menace évoluant perpétuellement et très rapidement ; d'autre part, la difficulté d'évaluer le risque spécifique à l'entreprise faisant la demande de la police d'assurance, ce risque étant assis des questionnaires d'auto-évaluation parfois mal remplis, intentionnellement ou non (ce qui conduit à des polices non adaptées, voire à des causes de non-remboursement en cas de cyberattaque)[167].

2.4.2. Un marché au futur incertain

Faute de statistiques dans un secteur jeune et très mouvant, il est difficile d'anticiper l'évolution des assurances cyber. Si les entreprises sont de plus en plus conscientes de la menace et des enjeux, leur accès à ce type d'assurances est compliqué, onéreux, et souffre de nombreuses exclusions. Il y a fort à parier, si la situation ne change pas, que le tissu des TPE et PME dont font partie bon nombre de cabinets d'experts-comptables ne pourra ou voudra avoir accès à ces assurances et sera donc exposé aux risques financiers découlant des attaques qu'il pourrait subir. Par ailleurs, ces assurances ne sont pas la panacée, car elles ne couvrent que l'aspect financier quand les questions réputationnelle ou de reprise d'activité peuvent être plus centrales, et le temps de recours peut également s'avérer trop long, beaucoup d'entreprises ne parvenant pas à se relever d'une cyberattaque[168].

[166] https://cesin.fr/articles-slug/?slug=2060-9%C3%A8me+%C3%A9dition+du+barom%C3%A8tre+annuel+du+CESIN.
[167] www.itforbusiness.fr/comment-les-assureurs-deviennent-des-evaluateurs-de-cybersecurite-de-votre-entreprise-73960.
[168] www.stoik.io/cybersecurite/chiffres-cles.

3. Études de cas

Afin d'illustrer la réalité de la menace pesant sur les données brassées par les cabinets d'expertise comptable, nous avons choisi de relater deux cas différents, celui d'une attaque directe et celui du piratage d'un prestataire. Le premier de ces deux cas sera très succinct, car pour des raisons de confidentialité invoquées par sa source, je n'ai pu obtenir de récit plus précis.

La méthodologie utilisée pour le premier cas a été le recueil de témoignage, oral dans un premier temps, puis complété à l'écrit via des échanges par e-mail. Pour les raisons de confidentialité déjà évoquées, il ne m'a pas été possible d'aller plus loin dans mes recherches, ne pouvant identifier le cabinet ou l'attaque en question. La source du récit est toutefois de confiance et, s'il ne m'a pas été possible de creuser plus avant cet événement, les quelques faits relatés n'en restent pas moins fiables.

La méthodologie utilisée dans le second cas a associé le recueil de témoignages (auprès de deux experts-comptables, un chef de mission et un collaborateur comptable) à la recherche documentaire, dans la presse spécialisée et sur Internet (les sources utilisées sont indiquées au fil du texte en notes de bas de page).

3.1. Attaque dans un cabinet d'expertise-comptable

Il y a quelques années, un cabinet d'expertise comptable a subi une attaque par rançongiciel. L'attaque est probablement venue d'une négligence ou d'un manque de formation à la prudence informatique (à l'« hygiène informatique », comme la nomme l'ANSSI) : le secrétariat de l'entité a ouvert un e-mail frauduleux qui a pris le contrôle du serveur interne en quelques instants. Les pirates ont chiffré l'ensemble des données de l'entreprise et ont demandé une rançon. Le cabinet s'est trouvé dans une position délicate, car il ne disposait plus d'aucune donnée et ne pouvait donc plus travailler. Il a fallu par ailleurs prévenir les clients et gérer la situation en termes d'image.

Le cabinet a choisi de suivre les recommandations de l'État et des spécialistes de ce type d'attaque : il a décidé de ne pas payer la rançon. Il a engagé un prestataire informatique externe pour tenter de récupérer ses données et relancer son activité au plus vite.

Le prestataire, après une intervention de plusieurs semaines, a finalement réussi à récupérer les données chiffrées – à tout le moins une grande partie d'entre elles – et à les restaurer. Le cabinet a donc réussi à relancer son activité.

Mais l'opération a eu un coût énorme pour l'entreprise :

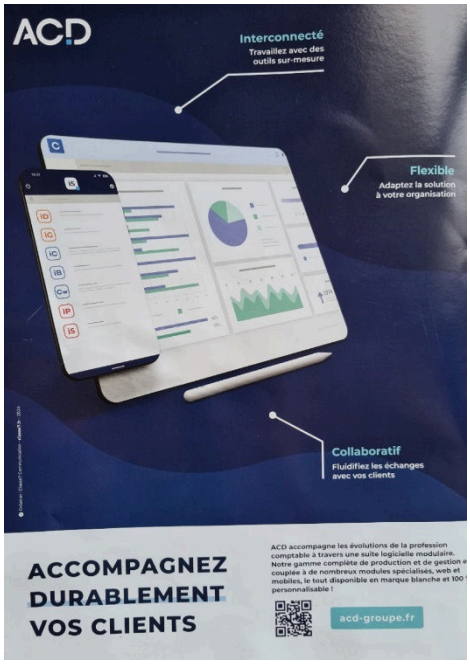
- Le coût de l'intervention du technicien (plusieurs dizaines de milliers d'euros) ;
- La perte d'exploitation (trois semaines d'inactivité) ;
- Le coût réputationnel auprès des parties prenantes du cabinet, celui-ci n'ayant pu faire l'économie d'une communication sur le sujet étant donné la durée de résolution de l'incident.

La source du récit de cette attaque ne mentionne pas de fuite particulière de clients. On peut donc imaginer que le cabinet a réussi à limiter les conséquences à la fois en termes de perte de clientèle et de perte de chances. Dans ce cas de figure, le coût de l'attaque a donc été majoritairement financier et n'a pas engagé la survie de l'entité, qui a pu reprendre son activité à l'issue de la résolution de l'incident. Ce cas illustre le fait que le maillon faible de la sécurité des données dans l'entreprise est l'humain, et que sécuriser ses données ne peut se résumer à des décisions techniques et technologiques : former et sensibiliser le personnel est une nécessité.

Par ailleurs, la temporalité peut avoir une incidence majeure, comme le souligne la source m'ayant relaté cette attaque : « [...] cela est arrivé sur la période de septembre. Il s'agit d'une période calme en termes d'obligations fiscales. Avec du recul, je pense que cela aurait pu être problématique si c'était arrivé en période fiscale (perte des clients, rattrapage du temps perdu impossible, etc.). »

3.2. Attaque chez un prestataire de cabinets d'expertise-comptable

Dans le courant de la nuit du 7 décembre 2023, l'hébergeur Coaxis a été la cible d'une cyberattaque d'ampleur menée par un groupe nommé Lockbit 3.0. Un mois a été nécessaire pour résoudre cet incident ayant affecté plus de 1 200 cabinets d'expertise-comptable[169].



Une publicité pour ACD en quatrième de couverture du n°435 de SIC mag.

Offrant notamment des solutions *cloud* pour les experts-comptables et partenaire d'ACD Groupe (logiciels de production comptable) et RCA (logiciels de gestion comptable), Coaxis héberge les données et l'environnement de travail de nombreux cabinets d'expertise-comptable.

Lockbit 3.0 est le *ranswomeware-as-a-service* le plus actif en 2022 [170]. Il chiffre les données de sa cible et demande une rançon pour lui restituer les données déchiffrées. Pouvant par ailleurs procéder à une exfiltration des données, ce chantage peut être complété par celui de la divulgation des données volées. Lockbit 3.0 a la particularité d'embarquer un canal de communication utilisé pour négocier avec la cible de façon publique. Cette publication des négociations contribue à accroître la pression sur la cible de l'attaque pour l'inciter à payer la rançon.

[169] https://objectifaquitaine.latribune.fr/business/2024-01-17/guyamier-et-coaxis-frappees-par-de-violentes-cyberattaques-au-rancongiciel-987511.html.
[170] www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-blackcat-and-royal-dominate-the-ransomware-scene-ransomware-in-q4-2022.

Si peu d'informations ont filtré sur la façon dont Lockbit 3.0 est parvenu à s'introduire chez Coaxis, on sait que l'attaque a entraîné le chiffrement d'environ 25 % des systèmes de l'hébergeur. Ce dernier a isolé son réseau pour limiter les dégâts, ce qui a d'autant plus affecté la disponibilité de ses services auprès de ses clients[171]. Lockbit a demandé une rançon et menacé de publier les données subtilisées, affichant publiquement un compte à rebours avant divulgation. Le compte à rebours arrivé à son terme, aucune donnée n'a finalement été publiée. Nul ne sait s'il s'agissait d'un bluff de la part de Lockbit 3.0 ou si Coaxis a accepté de verser la rançon demandée (ce que nie l'hébergeur)[172].

Les données chiffrées concernaient l'infrastructure de Coaxis et ne relevaient pas de données personnelles ou de données appartenant à ses clients. Toutefois, ces derniers se sont retrouvés dépourvus de leur outil de travail pendant les trois semaines qu'a duré l'incident. Ce fut le cas d'Eilad Expert, utilisateur d'ACD, hébergé chez Coaxis. On voit là l'effet domino d'une attaque, aucun lien contractuel direct n'existant entre Eilad Expert et Coaxis.

À la suite de l'attaque, Coaxis a procédé à une notification à la CNIL (conformément au RGPD). L'hébergeur a également envoyé des attestations de non-disponibilité à tous les clients concernés (par exemple pour qu'ils puissent mettre en œuvre le travail partiel, ou encore pour se dégager de leurs responsabilités déclaratives auprès du ministère de l'Économie et des Finances).

Ils ont aussi mis en place une communication personnalisée, notamment par texto, choix judicieux car il s'affranchit des voies informatiques partiellement compromises et a l'avantage de l'immédiateté. Toutefois, la gestion de la communication de crise de Coaxis a suscité des critiques, notamment car l'hébergeur a tardé à prévenir ses clients et à les informer de l'avancée de la résolution de l'incident. Or les clients de Coaxis avaient eux-mêmes besoin de communiquer auprès de leurs propres clients. Par ailleurs, l'impossibilité pour les cabinets d'expertise-comptable de poursuivre leur activité et le manque d'horizon sur l'issue de l'attaque a créé un climat anxiogène amplifiant la crise. Cela illustre l'importance de la communication lors de ce genre d'incident, qui relève tout autant de la stratégie et de la politique que du marketing. Une communication adaptée peut permettre d'éviter de surajouter une crise à une autre et également d'éviter une fuite de clients postérieurement à la crise.

Finalement, Coaxis a pu restaurer son système à partir de sauvegardes et rétabli ses services progressivement (95 % de rétablissement fin décembre, les 5 % restant la première semaine de janvier 2024[173]). Les cabinets d'expertise-comptable ont récupéré leurs données et leur outil de travail, même si les effets de l'incident et notamment des semaines d'inactivité qui en ont découlé ont causé des remous (notamment un surcroît de travail) pendant des mois. Gageons que les cabinets entretenant des rapports étroits et de confiance avec leurs clients ont pu trouver les mots

[171] www.dpo-partage.fr/piratage-de-coaxis-par-lockbit-3-0.
[172] www.dpo-partage.fr/coaxis.
[173] www.dpo-partage.fr/piratage-de-coaxis-par-lockbit-3-0.

pour expliquer ce qui était arrivé, mais que ceux entretenant des liens plus distants se sont retrouvés en délicatesse – certains on peut être même perdu des clients à la suite de cet incident.

Notons que l'interprofession s'est mobilisée dans cette affaire, puisque le Conseil national de l'ordre des experts-comptables a agi dès la semaine suivant l'attaque avec la tenue d'un webinaire d'informations articulé autour de quatre axes :

- Inciter les cabinets à déposer plainte officiellement ;
- Inciter les cabinets à contacter leur assureur ;
- Inciter les cabinets à communiquer auprès de leurs clients ;
- Inciter les cabinets à faire une demande de chômage partiel.

Le Conseil national de l'ordre des experts-comptables a également mis en place une cellule de crise dédiée et une cellule de soutien psychologique.

3.3. Leçons tirées de ces études de cas

Tout d'abord, soulignons que ces deux cas illustrent qu'une atteinte aux données d'une entreprise n'a pas d'effet que pour cette dernière mais également pour l'ensemble de ses parties prenantes, notamment à l'aval de la chaîne.

Ensuite, notons que la proaction est préférable à la réaction. S'il est impossible de sécuriser 100 % de ses données, il va de soi qu'il est plus simple de former ses salariés à ne pas cliquer inconsidérément sur n'importe quel lien d'e-mail douteux plutôt que de mettre des semaines à se relever d'une intrusion.

Par ailleurs, la victime d'une cyberattaque se doit de garder la tête froide et de faire jeu de transparence auprès de ses partenaires et clients afin de bénéficier de leur soutien et de perpétuer le lien de confiance qui les lie.

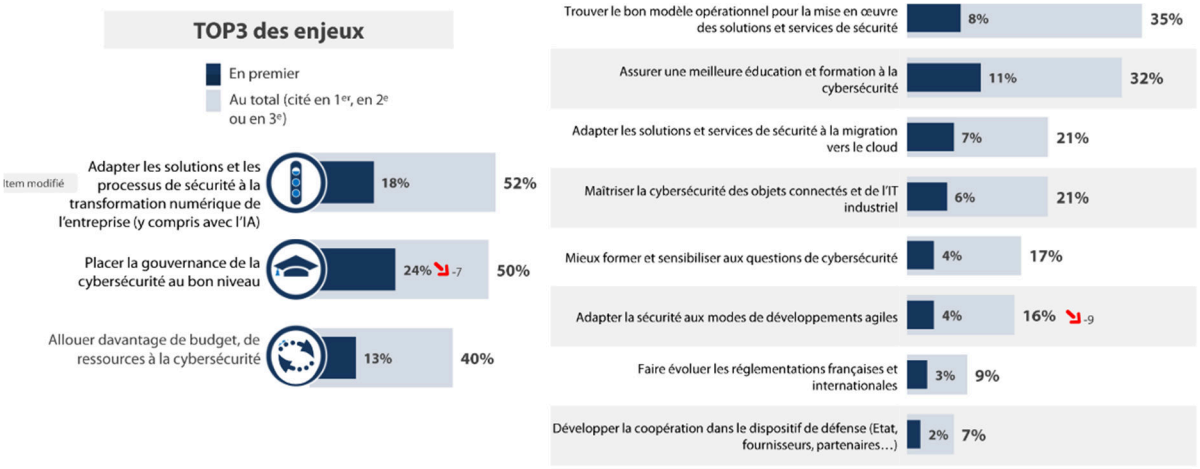
Enfin, il est essentiel de pouvoir rebondir à la suite d'une pareille crise. Avoir une politique de sauvegarde adaptée et robuste pour pouvoir restaurer ses données, avoir un plan de continuité ou de reprise d'activité, avoir mis en place une communication permettant de redémarrer l'activité main dans la main avec ses clients sont des actions nécessaires pour un retour à la normale plus rapide, plus aisé et plus efficace.

CONCLUSION

Les menaces pesant sur les données se généralisent et leur qualité va croissant. L'intelligence artificielle et les *malware-as-a-service* démocratisent la cybermalveillance dans la mesure où il n'est plus nécessaire d'avoir des connaissances poussées en informatique pour générer ou utiliser un *malware*, et dans la mesure où le coût marginal d'attaque est de plus en plus faible. Dans ce contexte, les cabinets d'expertise-comptable, dont les données sont les matières premières, ont tout intérêt à s'armer pour protéger celles-ci. D'autant que, détenant quantité d'informations stratégiques et financières au sujet de leurs clients, ils peuvent représenter une cible privilégiée pour des cyberattaquants, soit pour obtenir des informations qui seront commercialisées à des tiers, soit pour récupérer des données permettant ensuite d'attaquer ses clients.

Afin de sécuriser ses données, la première étape est de cartographier son cabinet, d'établir le périmètre des données à protéger, leurs utilisateurs et usages, les risques pesant sur elles. La seconde est de sensibiliser et former le personnel aux risques, et de mettre en place une politique de mots de passe forte, comprise et acceptée par l'ensemble des utilisateurs du système d'information du cabinet. La troisième relève du plan de sauvegarde et éventuellement de la définition d'un plan de continuité ou de reprise d'activité.

QUESTION : PARMI LES ENJEUX SUIVANTS, QUELS SONT SELON VOUS LES TROIS ENJEUX DE DEMAIN POUR L'AVENIR DE LA CYBERSÉCURITÉ DES ENTREPRISES ?



Source : Baromètre annuel de la cybersécurité des entreprises, CESIN, 2024

En plus de ces précautions indispensables, il pourra être utile, comme le note Nermine Khaled, chargée d'études « transformation numérique » au Conseil national de l'ordre des experts-comptables[174], de disposer d'un ordinateur neuf et déconnecté du réseau qui pourra être utilisé si le reste du matériel du cabinet est corrompu, d'une adresse e-mail neutre de secours accessible en ligne depuis n'importe quel terminal et d'une sauvegarde d'un carnet d'adresses contenant celles des clients, collaborateurs et contacts d'urgence avec lesquels le lien ne peut être rompu sous aucun prétexte.

[174] *SIC mag*, n° 435, p. 48.

Les évolutions technologiques et sociétales entraînent par ailleurs un changement de paradigme dans la protection des données. Comme le note l'ANSSI : « Le recours accru à l'informatique nuagique (*cloud*), le développement du télétravail et l'utilisation de moyens personnels (BYOD[175]) pour accéder à des données professionnelles réduisent le contrôle que les entités exercent sur leurs systèmes d'information et leurs données[176]. » Des solutions émergent pour lutter contre ces phénomènes, comme le modèle Zero Trust, dont le socle consiste à ne faire confiance à aucun utilisateur ni appareil et à une limitation très stricte des privilèges des utilisateurs. Toutefois, comme le note l'ANSSI, « le recours à ces solutions est ardu, faute de maturité : le déploiement est susceptible d'entraîner des erreurs d'installation ou de configuration, d'accroître la vulnérabilité des systèmes d'information et de donner aux entreprises un faux sentiment de sécurité. »

L'intelligence artificielle, quant à elle, investira sans doute de plus en plus le champ de la protection des données. Elle permettra d'affiner la détection automatique d'activités malveillantes et de prodiguer les premiers soins aux systèmes touchés[177]. Mais elle sera également de plus en plus utilisée à des fins malveillantes. Il paraît illusoire de penser que les évolutions de l'intelligence artificielle permettront une protection accrue des données. Le plus probable est qu'elles permettront simplement de compenser l'intensification et la qualité croissante des menaces.

Intelligence artificielle et cybersécurité

> **Utilisation de l'IA à des fins d'attaque** : la maîtrise de capacités de perception, de raisonnement, d'action et d'apprentissage devrait permettre aux attaquants de mener des cyberoffensives plus sophistiquées, mieux planifiées, plus réactives, plus adaptées aux cibles, plus globales et plus efficientes.
> **Utilisation de l'IA à des fins de défense** : la mobilisation de l'IA, et notamment de l'apprentissage automatique, pourrait servir […] à la détection des cyberattaques ou à la recherche de vulnérabilités dans des produits.
> **Vérification du fonctionnement propre de l'IA** : de la même façon que l'on évalue les propriétés de sécurité des produits logiciels et matériels, on pourrait s'attendre à voir émerger des besoins d'évaluation de la sécurité des IA – tant dans les algorithmes mis en œuvre que dans la qualité des jeux de données qui permettront l'apprentissage.

Yann Salamon, p. 37

Les objets connectés investissent le quotidien des individus. S'ils sont encore peu répandus dans les cabinets d'expertise-comptable, leur arrivée potentielle devra être surveillée de près, car ils sont pour l'heure mal protégés et représentent donc des portes d'entrée potentielles pour les cybermenaces[178].

Dans ce contexte général, l'État semble avoir pris la mesure des enjeux et, via plusieurs de ses émanations, conseille, accompagne voire intervient pour aider les entreprises à se protéger ou à lutter contre les cybermenaces. Des campagnes de sensibilisation aux supports de formations, en passant par des *checklists* synthétiques et très utiles[179], il propose des outils pour se préparer, s'armer et, le cas échéant, riposter.

[175] *Bring your own device*, « utilise ton matériel personnel ».
[176] https://cyber.gouv.fr/publications/le-modele-zero-trust.
[177] www.ibm.com/fr-fr/ai-cybersecurity?p1=Search&p4=4370006802908614 5&p5=e&gad_source=1&gclsrc=ds.
[178] Salamon, 2020, p. 70
[179] Voir par exemple la *checklist* sur la sécurité des données personnelles en annexe 14.

Pour assurer sa sécurité, un cabinet pourra, selon sa taille, ses enjeux, ses choix stratégiques et d'organisation, internaliser ou sous-traiter sa sécurité. L'internalisation lui demandera de s'armer de compétences, de pratiquer une robuste gestion des risques et d'organiser une solide gouvernance. La sous-traitance lui ôtera une partie des responsabilités mais également une partie du pouvoir de décision, et de compréhension des méthodes et outils mis en place. L'humain étant au cœur des incidents informatiques, l'infogérance ne saurait dédouaner totalement une entreprise de ses responsabilités en matière de sensibilisation et de formation. Pour une petite structure, il est souvent plus pertinent de sous-traiter ces questions très techniques. Une grande attention sera alors portée au contrat de service, qui doit clairement définir les rôles et responsabilités de chacun. Dans tous les cas, la gouvernance et le positionnement de la sécurité dans l'organigramme et les priorités stratégiques de l'entreprise sont indispensables.

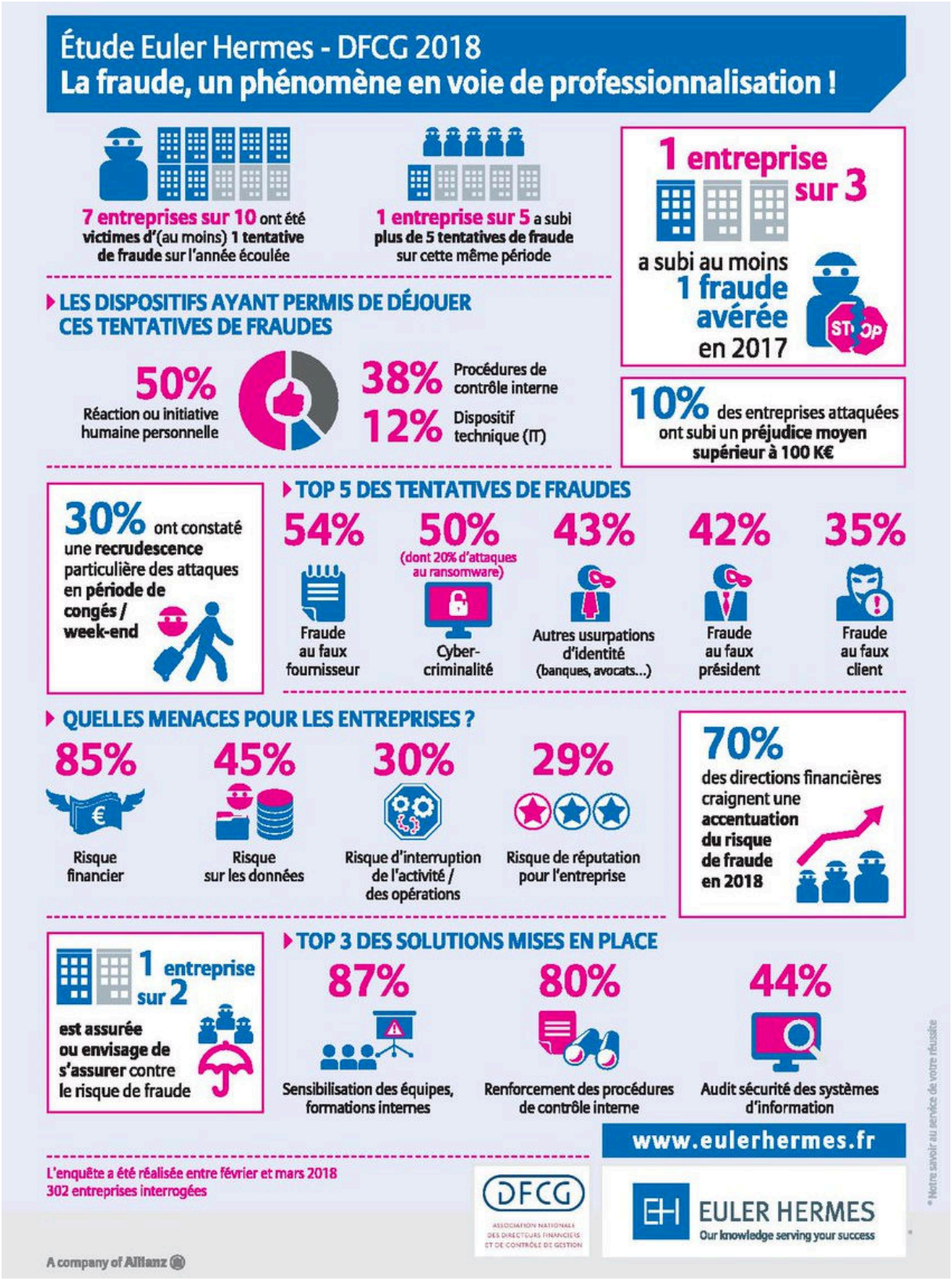
Pour conclure, enfonçons une porte ouverte : la sécurisation des données personnelles dans les cabinets d'expertise comptable revient à opérer un arbitrage entre productivité et sécurité. Ceci étant dit, la porte n'est pas forcément si ouverte, car comme le notent les auteurs de *La Menace intérieure*, « les politiques de sécurité [...] sont trop souvent élaborées sans tenir suffisamment compte de leur impact sur la productivité des employés dans leurs tâches quotidiennes[180]. » « Le choix est rarement entre le bien et le mal, mais entre le pire et le moindre mal », a écrit Machiavel dans son *Prince*. Et de fait, toute mesure de sécurité supplémentaire engage et mobilise des ressources qui nuisent à la performance ou pourraient être allouées à des taches relevant du cœur d'activité de l'entité. À l'évidence, il s'agit de trouver un juste équilibre « entre une approche trop drastique, lourde, coûteuse et ankylosante, et une approche trop laxiste [...] pour permettre aux [collaborateurs] de produire de la valeur dans des conditions optimales de sécurité[181]. » Cet arbitrage, itératif et évolutif, doit être opéré par la direction générale, qui doit se saisir de cette question et intégrer la sécurité dans le périmètre de ses réflexions dans une logique d'amélioration continue. En ce sens, et de par son caractère omniprésent et transversal, la sécurisation des données, relève de la stratégie plus que de l'informatique ou du juridique. Elle nécessite en effet un ensemble d'arbitrage, d'actions et de méthodes concourant à l'objectif général de l'entreprise, la sécurisation des données n'étant pas une fin en soi. C'est la raison pour laquelle nous avons cru pertinent d'évoquer en couverture *L'Art de la guerre*, du général chinois Sun Tzu (VIe siècle av. J.-C.), qui (avec son pendant plus politique *Le Prince* de Machiavel deux mille ans plus tard), constitue le corpus originel de la discipline.

[180] Arduin, Grundstein et Rosenthal-Sabrou, p. 79.
[181] Salamon, 2020, p. 100.

ANNEXES

ANNEXE 1 //

QUELQUES CHIFFRES SUR LA FRAUDE, ÉTUDE EULER HERMÈS - DFCG 2018



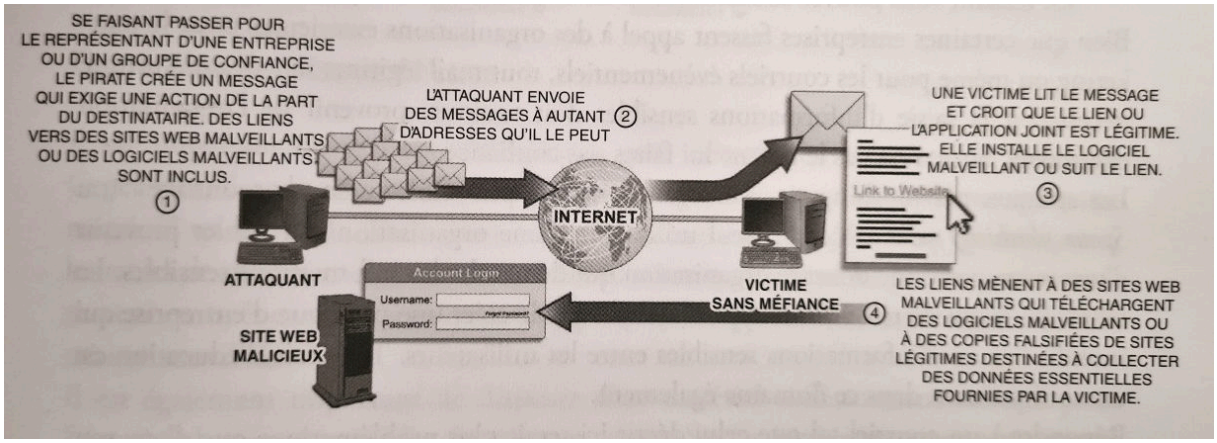
Source : https://www.mtom-mag.com/article5912.html.

ANNEXE 2 //

PRÉSENTATION SUCCINCTE DES PRINCIPALES FORMES D'ATTAQUES INFORMATIQUES

_L'hameçonnage (*phishing*)

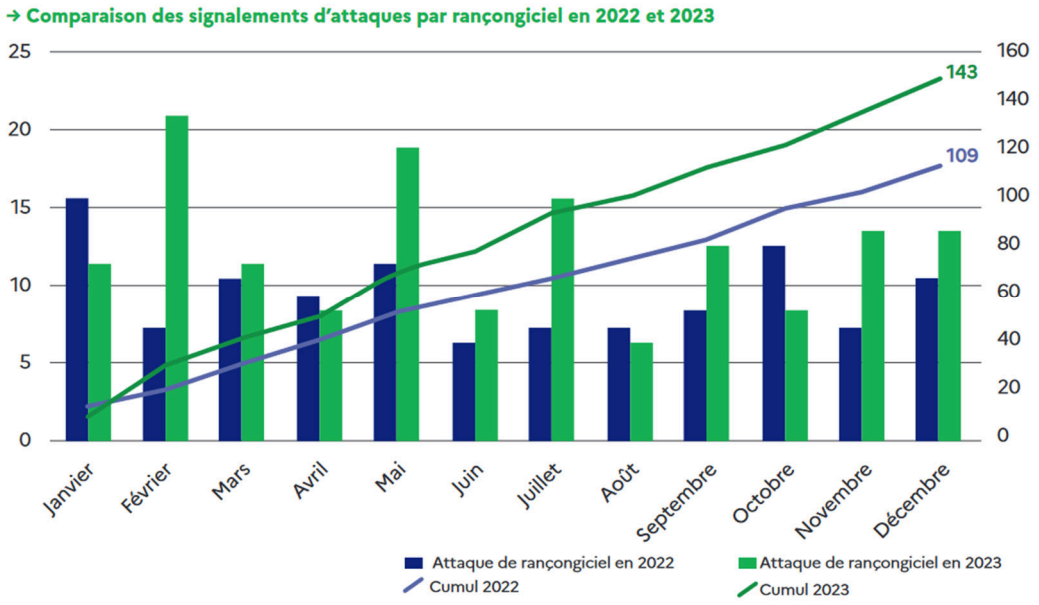
Le fraudeur se fait passer pour un organisme connu (banque, DGFiP, CAF, opérateur téléphonique, site de vente en ligne, etc.), en utilisant le logo et le nom de cet organisme. Il sollicite l'utilisateur pour qu'il mette à jour ou confirme ses informations et subtilise alors les données renseignées[182]. Il nécessite deux éléments : un appât (e-mail pour le *phishing*, appel ou SMS pour le *vishing*, QRcode pour le *quishing*) et un site de piège (*back-end*)[183]. À noter que les versions personnalisées du *phishing* mariant cette technique à celle de l'ingénierie sociale s'appellent *spearphishing*[184].



Un exemple d'attaque par hameçonnage (Brooks, p. 577).

_Le rançongiciel (*ransomeware*)

L'attaquant parvient à s'introduire dans le système de l'utilisateur (grâce à l'utilisateur : après ouverture d'un fichier malveillant, navigation sur un site compromis ; ou sans son aide : intrusion informatique, notamment via des vulnérabilités logicielles) et y place un code malveillant bloquant l'accès aux données en les chiffrant. Son objectif est de réclamer le paiement d'une rançon en échange du déchiffrement des données. Il s'agit d'une forme de chantage. Notons que la victime n'est pas assurée que l'attaquant lui restitue l'accès à ses données déchiffrées après paiement de la rançon. L'attaquant peut ainsi demander une rançon supplémentaire, ou, par pure malveillance, décider de ne pas déchiffrer les données. Les pouvoirs publics recommandent de ne jamais payer de rançon[185].

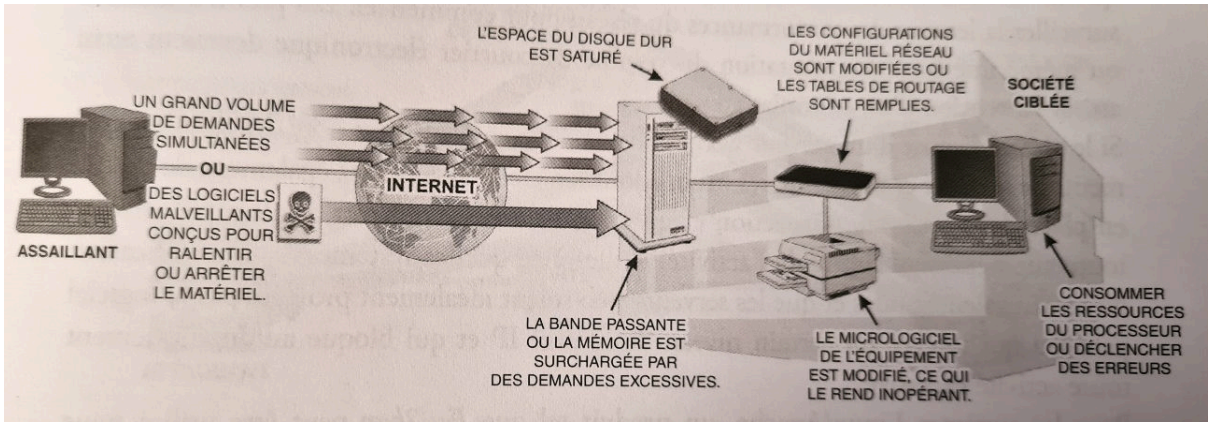


Panorama de la cybermenace 2023, ANSSI, www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-001.pdf.

[182] www.lefigaro.fr/conjoncture/les-nouvelles-techniques-des-escrocs-du-web-pour-voler-leurs-victimes-20240309.
[183] « Panorama du phishing en 2023 », *MISC*, hors-série n°27, éditions Diamond, janvier 2024.
[184] Salamon, 2020, p. 86.
[185] www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/ransomware-rancongiciel-definition.

_L'attaque en déni de service (DoS)

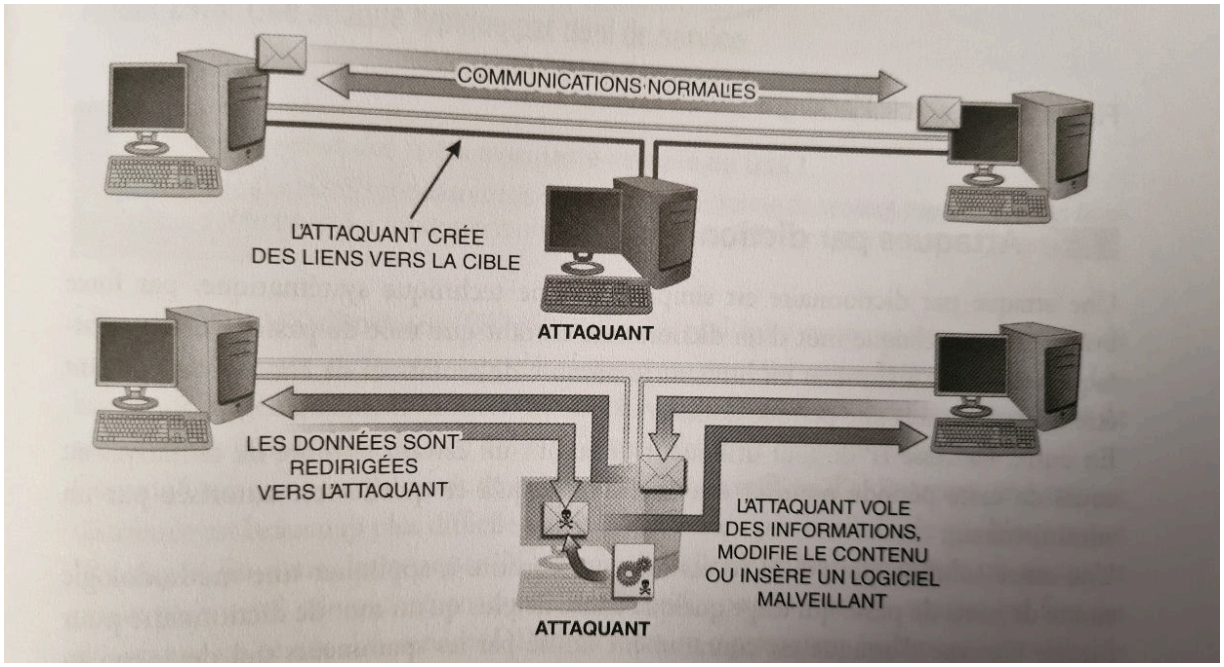
Il s'agit de l'envoi de nombreuses requêtes pour saturer un serveur ou exploiter une faille de sécurité. Cette attaque a pour but de provoquer une panne ou une suspension de service de l'entreprise, provoquant ainsi une perte de revenus et des effets négatifs sur la réputation[186]. Il existe aujourd'hui des *Booter Services*, qui sont des attaques en DoS disponibles à la demande sous forme de service payant[187].



Une attaque par déni de service (Brooks, p. 583).

_L'attaque MitM (*Man-in-the-Middle*)

L'attaquant intercepte et relaye des messages entre deux parties qui pensent communiquer directement entre elles. Il a donc accès à des informations sensibles en temps réel et peut se faire passer pour l'une des deux parties à l'égard de l'autre sans qu'aucune ne s'en rende compte. Ces attaques d'« interception » démarrent souvent après implantation d'un logiciel malveillant (*malware*)[188].



Une attaque MitM, (Brooks, p. 581).

_La fraude au président

Elle consiste à usurper l'identité d'un donneur d'ordre pour exiger une action d'un collaborateur, en urgence et de façon confidentielle (souvent un virement monétaire). Il s'agit donc d'une usurpation d'identité associant des techniques de manipulation[189].

_Le *malware*

Un *malware* est un terme générique désignant un logiciel malveillant : hostile ou intrusif (virus, vers, cheval de Troie, *ransomware*, *spyware*, *adware*, *scareware*...)[190]. Il vise à subtiliser des renseignements personnels, financiers ou commerciaux et peut également servir à chiffrer ou supprimer des données sensibles, espionner, détourner des fonctions ou des actions.

[186] www.oodrive.com/fr/blog/securite/cybersecurite-top-10-des-cyberattaques-frequentes-en-2023.
[187] Brooks, 2021, p. 583.
[188] www.lemagit.fr/definition/Man-in-the-Middle.
[189] www.economie.gouv.fr/dgccrf/professionnels-agents-publics-attention-a-larnaque-au-president.
[190] www.oracle.com/fr/cloud/malware-logiciel-malveillant.

_L'attaque par téléchargement furtif

Il s'agit d'un logiciel téléchargé à l'insu de l'utilisateur ou sans qu'il soit conscient des conséquences du téléchargement et permettant ensuite l'installation d'un virus, d'un logiciel espion ou de tout autre type de *malware*[191].

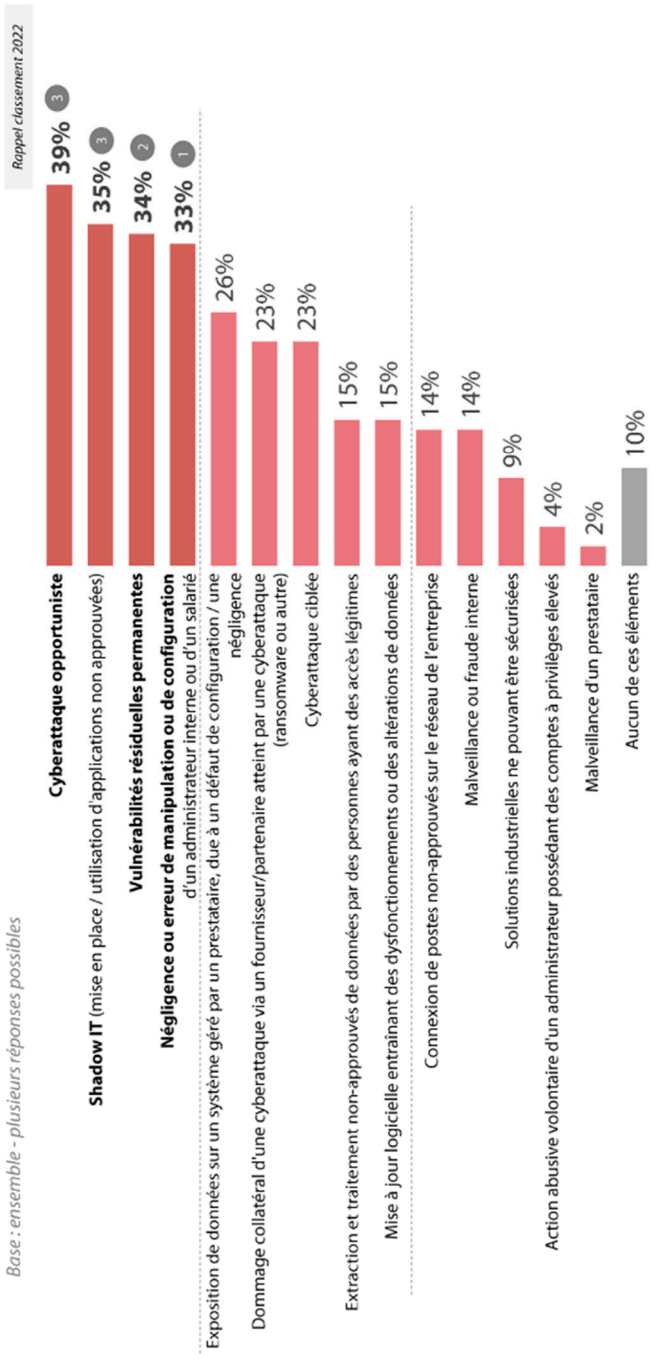
_L'attaque par force brute (*brute force attack*).

Elle revient à « tester, l'une après l'autre, chaque combinaison possible d'un mot de passe ou d'une clé pour un identifiant donné afin de se connecter au service ciblé [192]. » Il est relativement aisé de se prémunir contre cette attaque (par exemple en bloquant l'accès après trois tentatives infructueuses de connexion), mais elle peut-être redoutablement efficace en cas de mots de passe faible ou évident.

_L'injection SQL (SQLi).

L'attaquant utilise une portion de code SQL pour manipuler une base de données et accéder à ses informations (vol, corruption, destruction…).

QUESTION : PARMI LES CAUSES DES INCIDENTS DE SÉCURITÉ RENCONTRÉES PAR L'ENTREPRISE […], QUELLES SONT CELLES AUXQUELLES VOTRE ENTREPRISE A ÉTÉ CONCRÈTEMENT CONFRONTÉE AU COURS DES DOUZE DERNIERS MOIS ?

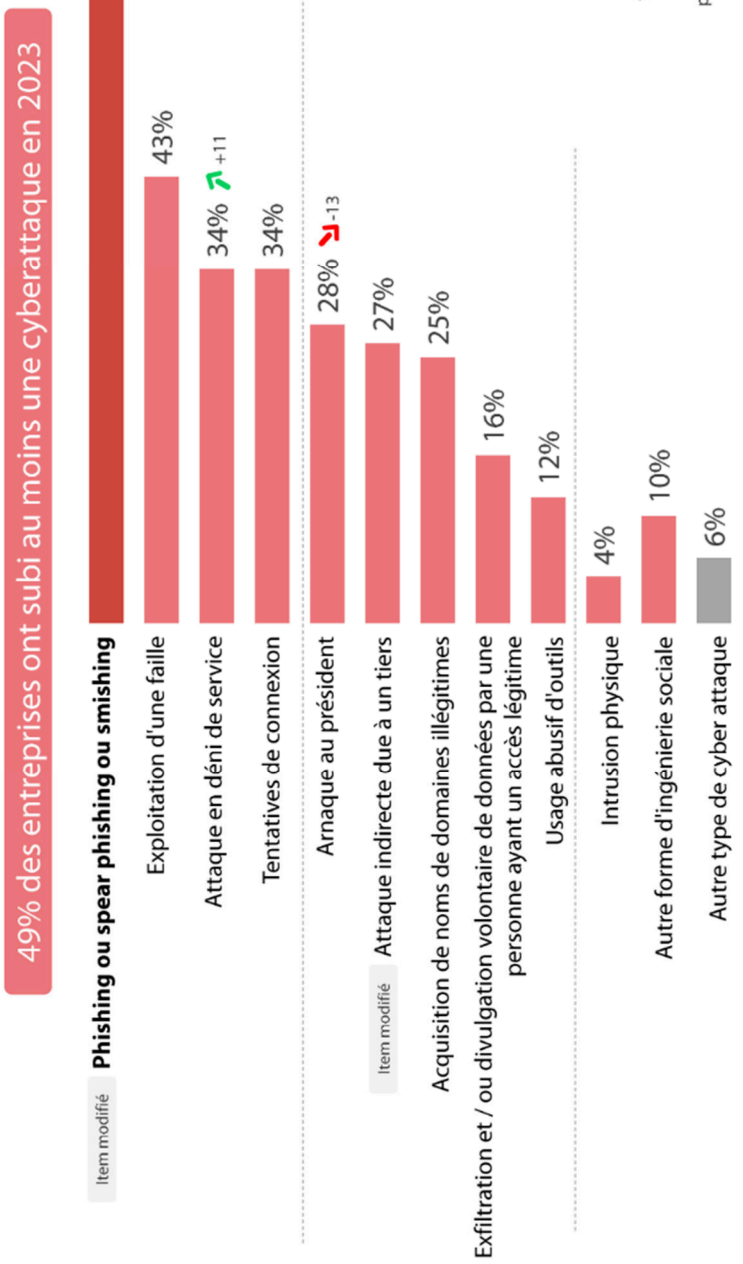


Source : Baromètre annuel de la cybersécurité des entreprises, CESIN, 2024.

[191] www.aforp.fr/les-cyberattaques-les-plus-courantes-contre-les-entreprises.
[192] www.cnil.fr/fr/definition/force-brute-attaque-informatique.

ANNEXE 3 //

PALMARÈS DES ATTAQUES SUBIES PAR LES ENTREPRISES EN 2023



Source : Baromètre annuel de la cybersécurité des entreprises, CESIN, 2024.

ANNEXE 4 //

RGPD, CHAPITRE IV, SECTION 2 : LA SÉCURITÉ DES DONNÉES À CARACTÈRE PERSONNEL

Article 32 - Sécurité du traitement

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 :

- la pseudonymisation et le chiffrement des données à caractère personnel ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- 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 ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

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'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article.

Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre.

Article 33 - Notification à l'autorité de contrôle d'une violation de données à caractère personnel

En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

La notification visée au paragraphe 1 doit, à tout le moins:

- décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives ;
- si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article.

Article 34 - Communication à la personne concernée d'une violation de données à caractère personnel

Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d).

La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie :

- le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement ;
- le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser ;
- elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe 3 est remplie.

Source : https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4.

ANNEXE 5 //
LES NORMES ISO 270XX

ISO/IEC 27000:2014
Fournit une présentation et une introduction aux normes ISO 27000 et définit le vocabulaire spécifique utilisé sur leur ensemble.

ISO/IEC 27001:2022
Norme principale de définition des besoins pour le SMSI (Système de Management de la Sécurité de l'Information). Elle correspond au principe de certification des organisations.

ISO/IEC 27002:2022
Il s'agit de la description des bonnes pratiques décrivant un ensemble compréhensible d'objectifs de contrôle et un assortiment de bonnes pratiques généralement acceptées.

ISO/IEC 27003:2017
Comprend le guide d'implémentation détaillé relatif à l'adoption de la série complète de la norme ISO 27001.

ISO/IEC 27004:2016
Contient la norme qui définit les principes d'évaluation et de mesure de ce qui a été implémenté dans le cadre du système de management de la sécurité de l'information pour mesurer l'efficacité des solutions mises en œuvre.

ISO/IEC 27005:2022
Contient la norme de gestion du risque au niveau de l'information comprenant des conseils sur la sélection des analyses de risque appropriées, les méthodes et outils de gestion. La dernière révision de cette norme permet d'apporter et de diffuser les innovations principales d'EBIOS Risk Manager.

ISO/IEC 27006:2015
Guide décrivant les exigences pour les organismes procédant à l'audit et à la certification des Systèmes de Management de la Sécurité de l'Information qui ont réussi la certification ISO/IEC 27001.

ISO/IEC 27007:2020
Cette norme fournit des conseils pour la gestion du programme d'audit d'un SMSI. C'est un outil à destination des auditeurs d'un SMSI interne ou externe pour les aider à mieux comprendre et conduire l'audit à réaliser.

ISO/IEC 27008:2019
Cette norme propose un guide sur les contrôles de sécurité d'audit de l'information. Elle se focalise sur la façon dont les vérifications du SMSI sont implémentées.

ISO/IEC 27008:2020
Cette norme traite de la cybersécurité et de la protection des données personnelles. Elle spécifie les exigences pour la création de normes sectorielles qui étendent l'ISO/IEC 27001 et qui complètent ou modifient l'ISO/IEC 27002. Elle prend en charge ces normes et les adapte à un secteur spécifique (domaine, champs d'application ou marché particulier).

ISO/IEC 27009:2020
Cette norme traite de la cybersécurité et de la protection des données personnelles. Elle spécifie les exigences pour la création de normes sectorielles qui étendent l'ISO/IEC 27001 et qui complètent ou modifient l'ISO/IEC 27002. Elle prend en charge ces normes et les adapte à un secteur spécifique (domaine, champs d'application ou marché particulier).

ISO/IEC 27010:2015
Cette norme propose un guide sur le management de la sécurité de l'information pour les communications entre les entreprises du même secteur industriel et avec les gouvernements. Elle peut être utile lors de situations de crise ou afin de protéger des infrastructures critiques dans le but de respecter les obligations légales, réglementaires ou contractuelles.

ISO/IEC 27011:2016
Guide pour la gestion de la sécurité de l'information dans le secteur des télécommunications (aussi connu comme ITU X.1051).

ISO/IEC 27013:2021
Guide pour l'intégration de l'implémentation, l'alignement et la coordination entre ISO/IEC 20000-1 (*IT Service Management*) et ISO/IEC 27001 (SMSI).

ISO/IEC 27014:2020
Cette norme traite de la cybersécurité et de la protection de la vie privée, de la gouvernance à l'échelle de toute l'organisation. Pour affiner sa stratégie, elle prend en compte les risques dans les processus décisionnels pour garantir la conformité à des exigences internes et externes.

ISO/IEC TR 27015:2012
Cette norme propose un guide pour le système de gestion de la sécurité de l'information en ce qui concerne les services et les prestataires financiers des organisations. Elle vient en complément des recommandations liées à SOX (Sarbanes Oxley), BASEL II/III, COBIT et des exigences PCI-DSS.

ISO/IEC TR 27016/2014
Cette norme fournit des directives afin d'aider une organisation à prendre les bonnes décisions pour la protection de l'information en insistant sur la compréhension des conséquences économiques de ces décisions. Elle est applicable à tous les types et tailles d'organisation.

ISO/IEC 27017:2015
Cette norme donne des conseils sur les recommandations en relation avec la sécurité de l'information pour les services du Cloud Computing en ce qui concerne les prestataires et les clients. Elle insiste sur la mise en place de contrôles supplémentaires et vient en complément des normes ISO 27002, ISO 27018 et ISO 27031.

ISO/IEC 27018:2019
Cette norme fournit des recommandations pour s'assurer que les fournisseurs de *Cloud Computing* public (Google, Amazon…) proposent les contrôles appropriés de sécurité sur l'information de façon à protéger la vie privée de leurs clients et les informations privées qui leur sont confiées.

ISO/IEC 27019:2017
Cette norme propose une aide aux organisations liées à l'industrie énergétique pour leur permettre d'appliquer la norme ISO/IEC 27002 dans l'objectif de sécuriser leurs systèmes électroniques de commande de processus. Elle est dérivée de la norme allemande DIN SPEC 27009:2012-04.

ISO/IEC 27031:2011
Cette norme se focalise sur la continuité d'activité dans les systèmes d'information. Elle propose une description des concepts et des principes pour préparer les organisations utilisant les technologies de l'information et de la communication de façon à assurer leur continuité d'activité. Elle est applicable à tous les types et tailles d'organisation.

ISO/IEC 27032:2012
Cette norme propose un guide sur la cybersécurité. Elle présente des directives pour améliorer son état et ses dépendances avec d'autres domaines associés. Elle traite particulièrement de cette sécurité, des réseaux et d'Internet et de la protection des infrastructures critiques gérant des informations.

ISO/IEC 27033-6:2016
Sécurité du réseau - *Partie 6 : Sécurisation de l'accès réseau IP*

sans fil. Cette norme propose des recommandations détaillées sur la gestion, les opérations, l'utilisation, l'implémentation des contrôles dans les réseaux de systèmes d'information et leurs interconnexions.

ISO/IEC 27034-1:2011+
Cette norme propose des conseils sur la sécurité de l'information sur les aspects spécifiques de la conception, le développement, l'implémentation, la mise en œuvre d'applications système. L'objectif principal consiste à s'assurer que celles-ci fournissent le niveau de sécurité suffisant dans le cadre du SMSI mis en place.

ISO/IEC 27035-1:2016
La partie 1 de la norme traite de la gestion des incidents de sécurité de l'information. Elle fournit une approche structurée et planifiée pour la gestion des événements, des incidents, des vulnérabilités qui sont associées. Elle insiste sur l'aspect de l'amélioration continue.

ISO/IEC 27036-1:2021
Cette norme multipartie propose des recommandations sur l'évaluation et le traitement des risques dans le cadre des relations avec les fournisseurs (marchandises ou services) des technologies de la communication et de l'information chez les fournisseurs. *Partie 1 : aperçu général et concepts.*

ISO/IEC 27036-2:2022
Partie 2 : exigences.

ISO/IEC 27036-3:2013
Partie 3: lignes directrices pour la sécurité de la chaîne de fourniture des technologies de la communication et de l'information.

ISO/IEC 27036-4:2016
Partie 4 : lignes directrices pour la protection des services du cloud.

ISO/IEC 27037:2012
Cette norme fournit des recommandations détaillées sur l'identification, la collecte, l'acquisition, le stockage, la transmission, la préservation de preuves numériques afin de garantir l'intégrité de celles-ci pour leur exploitation dans des cadres légaux (justice…).

ISO/IEC 27038:2014
Cette norme spécifie les caractéristiques des techniques utilisées dans la rédaction de documents numériques. Elle spécifie aussi les exigences relatives aux outils logiciels de rédaction de documents, des méthodes de test pour vérifier que chacun d'eux est entièrement sécurisé.

ISO/IEC 27039:2016
Cette norme traite de la sélection, du déploiement et des opérations des systèmes de détection et de la prévention d'intrusion.

ISO/IEC 27040:2015
Cette norme aborde la sécurité du stockage de données. Elle préconise les bonnes pratiques de façon détaillée à l'intention des organisations qui peuvent ainsi définir de façon cohérente la planification, la conception, la documentation et la mise en œuvre du traitement et du stockage des données. Ces recommandations s'appliquent à la protection des informations là où elles sont stockées et/ou transférées au moyen des dispositifs associés au stockage.

ISO/IEC 27041:2015
Cette norme fournit des préconisations concernant les mécanismes utilisés dans l'investigation des incidents pour s'assurer qu'ils sont en adéquation avec l'application concernée par l'incident.

ISO/IEC 27042:2015
Cette norme décrit les lignes directrices pour l'analyse et l'interprétation des preuves numériques en ce qui concerne les problèmes de continuité, de validité, de reproductibilité et de répétabilité.

ISO/IEC 27043:2015
Cette norme décrit les principes et processus d'investigation sur incident. Elle fournit les lignes directrices concernant des modèles idéalisés pour des processus d'investigation des incidents communs à travers divers scénarios d'investigation sur incident impliquant des preuves numériques.

ISO/IEC CD 27046
Cette norme, en cours de développement, décrit les lignes directrices pour la mise en œuvre de la sécurité et de la confidentialité des « Big Data ». Elle comprend une liste de contrôles suggérés à prendre en compte et à adopter depuis la collecte, pendant le transfert jusqu'au stockage.

NORMES COMPLÉMENTAIRES QUI ENTRENT DANS LE CADRE DE LA CYBERSÉCURITÉ

ISO/IEC 20889
Terminologie et classification des techniques de l'anonymisation de données pour la protection de la vie privée

ISO/IEC 27799/2016
Cette norme fournit les directives pour la mise en œuvre de la norme ISO/IEC 27002 dans le domaine de l'informatique médicale et apporte des recommandations pour la gestion des informations de santé.

ISO/IEC 29100
Cette norme fournit un cadre et décrit de façon détaillée la mise en œuvre des principes pour la protection de la vie privée, des données à caractère personnel au sein des systèmes de technologies de l'information et de la communication.

Ces normes évoluant, cette liste est à prendre avec précaution. Le site de référence pour une version à jour est :
www.iso27001security.com.

Source : Carpentier, 2023, p. 29-37.

ANNEXE 6 //
LES PRATIQUES DE GESTION ITIL 4

1. Pratiques générales de gestion
(*General management practices*)
_Gestion de l'architecture (*Architecture management*)
_Gestion de la stratégie (*Strategy management*)
_Amélioration continue (*Continual improvement*)
_Gestion de la sécurité de l'information (*Information Security management*)
_Gestion des connaissances (*Knowledge management*)
_Gestion du changement organisationnel (*Organizational change management*)
_Gestion de portefeuille (*Portfolio management*)
_Gestion de projet (*Project management*)
_Gestion financière des services (*Service Financial management*)
_Gestion de la main-d'œuvre et des talents (*Workforce and talent management*)
_Mesure et rapports (*Measurement and reporting*)
_Gestion des risques (*Risk management*)
_Gestion des fournisseurs (*Supplier management*)
_Gestion de la relation (*Relationship management*)

2. Pratiques de gestion des services
(*Service management practices*)
_Gestion des disponibilités (*Availability management*)
_Analyse d'affaires (*Business analysis*)
_Gestion du catalogue de services (*Service catalog management*)
_Conception de services (*Service design*)
_Gestion des niveaux de service (*Service level management*)
_Gestion de la capacité et des performances (*Capacity and performance management*)
_Gestion de la continuité de service (*Service continuity management*)
_Surveillance et gestion des événements (*Monitoring and event management*)
_Centre de services (*Service desk*)
_Gestion des incidents (*Incident management*)
_Gestion des demandes de service (*Service request management*)
_Gestion des problèmes (*Problem management*)
_Gestion des versions (*Release management*)
_Facilitation du changement (*Change enablement*)
_Validation et test des services (*Service validation and testing*)
_Gestion de la configuration des services (*Service configuration management*)
_Gestion des actifs informatiques (*IT asset management*) dont le périmètre comprend les services *cloud computing* et l'Internet des objets

3. Pratiques de gestion technique
(*Technical management practices*)
_Gestion du déploiement (*Deployment management*)
_Gestion de l'infrastructure et de la plateforme (*Infrastructure and Platform management*)
_Développement et gestion de logiciels (*Software development and management*)

Source : Carpentier, 2023, p. 20-21.

ANNEXE 7 //
PANORAMA DE RESSOURCES DOCUMENTAIRES

_Ordre des experts-comptables

Le CNOEC et la CNCC se sont saisis de la question de la sécurité des données. Outre une veille réglementaire et technologique, ils proposent notamment un guide de bonnes pratiques intitulé « Les Onze Commandements cyber » (voir en annexe 8).

› La page « Cybersécurité » propose des ressources et des guides pratiques pour les cabinets comptables.

› Le rapport « Panorama de la cybersécurité dans les cabinets d'expertise comptable » (2022) est une source d'informations précieuses.

› Le « Blog Cybersécurité » est une source d'actualités et d'informations sur les menaces et les bonnes pratiques.

› La plateforme Fuz'experts.tv (« le Netflix de la profession », d'après leur communication) et son webinaire « Cyberattaque, construire son plan de continuité d'activité. »

_L'ANSSI (Agence nationale de la sécurité des systèmes d'information) et cybermalveillance.gouv.fr

Cybermalveillance.gouv.fr est plutôt orienté TPE/PME et particuliers, quand l'ANSSI est plus dévolue aux grandes entreprises et aux « opérateurs d'importance vitale »)
L'ANSSI propose des guides et des recommandations sur la sécurité informatique, applicables aux cabinets comptables.
Cybermalveillance.gouv.fr propose un support en cas d'attaque informatique.

> https://cyber.gouv.fr/publications?field_type_de_publication_target_id%5B934%5D=934

> https://secnumacademie.gouv.fr/

_La CNIL (Commission nationale de l'informatique et des libertés) : www.cnil.fr

La CNIL propose des guides et des recommandations sur la protection des données personnelles, applicables aux cabinets comptables, et de manière générale de nombreuses ressources pour appréhender le « Règlement général sur la protection des données » (RGPD).

_FRANCENUM (Portail de la transformation numérique des entreprises)

www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/une-mallette-cyber-pour-sensibiliser

_Le sénat

www.senat.fr/rap/r20-678/r20-678-syn.pdf

_Le ministère de l'Économie et des Finances

De nombreuses ressources disponibles, parmi lesquelles :

> www.economie.gouv.fr/entreprises/createurs-dirigeants-regles-cybersecurite

> www.economie.gouv.fr/entreprises/reglement-general-protection-donnees-rgpd

_L'AFNOR

https://certification.afnor.org/numerique/certification-iso-27001

_Autres sites et médias spécialisés

www.nolimitsecu.fr • www.schneier.com • krebsonsecurity.com • www.cert.ssi.gouv.fr • www.linfocr.com

ANNEXE 8 //

LES ONZE COMMANDEMENTS CYBER DU CNCC

1

Cybercriminalité

La confidentialité tu garantiras

"Toute révélation d'un secret est la faute de celui qui l'a confié" Jean de la Bruyère

Anecdote

Dominique est comptable. Il consulte régulièrement les comptes de son entreprise sur le site mis en ligne par sa banque. Par facilité, il a choisi un mot de passe simple, car il le retient plus facilement. C'est la date de naissance de sa fille et le prénom de sa femme : 092014Marine. Ce mot de passe a été découvert facilement par un cybercriminel et l'entreprise s'est fait pirater son compte bancaire.

Essentiel

- **Sécurisez les échanges de données sensibles.**
- **Disposez de mots de passe robustes** : caractères diversifiés, renouvèlement régulier, pas de stockage, etc.
- **Ne divulguez pas d'informations sensibles** et soyez vigilant.
- **Maîtrisez votre e-réputation**.

Bonnes pratiques

Sécurisez les échanges de données sensibles

- Chiffrez les documents confidentiels : fichiers, mails, etc. y compris les clés USB.
- Appliquez les règles de bons sens recommandées par l'ANSSI dans son "passeport de conseils aux voyageurs" (site de l'ANSSI).
- Rappelez aux collaborateurs que les mêmes règles de sécurité doivent être appliquées au BYOD ("Bring Your Own Device" ou PAP en français "prenez vos appareils personnels") : mise à jour, antivirus, mots de passe, verrouillage systématique.

Disposez de mots de passe robustes

- Renforcez la politique de gestion des mots de passe : utilisez des mots de passe robustes (minimum 8 caractères, mots n'existant pas dans le dictionnaire, utilisation de caractères spéciaux et de chiffres), différents pour chaque accès et renouvelez-les tous les 3 ou 4 mois.
- Ne stockez jamais vos mots de passe de manière accessible.
- N'activez pas l'option "mémorisez vos mots de passe".
- Ne communiquez jamais vos mots de passe.
- N'utilisez pas d'autres comptes que le vôtre.
- Participez à la protection des informations de l'entreprise car vous êtes responsables des droits que vous pourriez donner à d'autres utilisateurs.
- Utilisez des coffres-forts virtuels.

Ne divulguez pas d'informations sensibles

- Ne parlez jamais des données personnelles de vos clients ou de procédures internes avec des tiers non autorisés.
- Ne diffusez aucune anecdote susceptible d'altérer l'image de marque de l'entreprise ni aucune pratique sensible propre à l'entreprise.
- Ne donnez jamais la possibilité à un tiers non autorisé de visualiser vos documents de travail. Vous pouvez utiliser des filtres de confidentialité.
- Verrouillez les ordinateurs.
- Mettez en place des procédures pour gérer le départ des collaborateurs (À quoi avaient-ils accès ? Pensez à changer leurs mots de passe et supprimer leurs accès).

Maîtrisez votre e-reputation

- Disposez d'une charte d'utilisation des réseaux sociaux afin de sensibiliser les collaborateurs aux risques liés à la divulgation de données confidentielles hors de l'entreprise (fraude aux présidents, fuite de données...). *Voir le 9e commandement.*
- Maîtrisez votre e-réputation (Google, Corporama, etc.) : vérifiez régulièrement votre identité numérique.

CNCC

ORDRE DES EXPERTS-COMPTABLES
Conseil Supérieur

2

Cybercriminalité

Un contrat de **cyber-assurance** tu souscriras

"On ne peut affirmer avec plus d'assurance que rien n'est assuré" Anatole France

Anecdote

Le Cabinet SIBERAUDIT est en infogérance. Il subit une panne à l'approche des fêtes et le contact technique est injoignable. Les membres du cabinet sont donc dans l'impossibilité de travailler pendant plus de 48h. Les frais engendrés pour récupérer les données auraient pu être couverts s'ils avaient mis en place un plan d'assurance sécurité adapté.

Essentiel

- **Définissez la typologie des risques assurables** : données personnelles, système d'information de l'assuré, données des tiers.
- **Analysez les offres disponibles** : couverture des dommages immatériels, préjudices, frais de communication de crise ; prise en charge de la gestion de crise et de la restauration des données ; responsabilité civile.
- **Répertoriez les propositions de valeur pour l'assuré** : évaluation, quantification, réduction et transfert des risques, expertise post-incident.

Bonnes pratiques

Définissez la typologie des risques assurables

- Données personnelles : frais de notification, d'expertise, de défense, frais en cas de contrôle ou d'enquête ; sanctions pécuniaires, atteinte à la propriété intellectuelle.
- Système d'information de l'assuré : vol, ajout, détérioration, destruction, interruption de service ; atteinte à l'image et à la réputation ; compromission du SI, perte d'exploitation et frais supplémentaires ; site internet non opérationnel.
- Données des tiers : interruption de services et réclamation des tiers, corruption des données, erreur, frais de défense.

Analysez les offres disponibles

- Couverture des dommages immateriels.
- Couverture des préjudices occasionnés aux tiers.
- Prise en charge de la gestion de crise et l'assistance.
- Prise en charge de la restauration des données.
- Couverture perte de revenus due aux cyberattaques.
- Responsabilité civile.
- Prise en charge des frais de communication de crise visant à protéger la réputation de l'entreprise, etc.

Répertoriez les propositions de valeur pour l'assuré

- Évaluation des risques : accompagnement dans l'identification des risques sur le SI, audit du SI et évaluation des mesures de sécurité.
- Quantification des risques encourus par le client en fonction des résultats des tests, valorisation des risques en fonction des impacts potentiels (financiers, image, temps, etc.).
- Réduction des risques : mise en œuvre d'un plan de traitement des risques permettant de réduire les risques à un niveau acceptable, accompagnement du client et expertise en cyber sécurité.
- Transfert des risques : identification des risques assurables, formalisation des garanties et primes d'assurances.
- Expertise post-incident : acompagnement du client pour limiter la propagation de l'incident, expertise permettant de revenir à un état stable.

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

ORDRE DES EXPERTS-COMPTABLES
Conseil Supérieur

3

Cybercriminalité

Une **perte** ou un **vol** tu anticiperas

"Celui dont la pensée ne va pas loin verra ses ennuis de près" Confucius

Anecdote

Maryse a cliqué par inadvertance sur un lien d'une page infectée. Un programme malveillant s'est alors installé automatiquement sur son ordinateur. Malgré les sauvegardes régulières, elle n'a pas pu récupérer les fichiers car elle ne s'était pas assurée du bon fonctionnement des sauvegardes. Sauvegarder c'est essentiel, les tester c'est vital !

Essentiel

- **Ayez une stratégie rigoureuse de sauvegarde.**
- **Soyez conscients des avantages et inconvénients des supports.**
- **Prenez des précautions dans l'utilisation des supports.**

Bonnes pratiques

Ayez une stratégie rigoureuse de sauvegarde

- Raisonnez par priorité et protégez les informations les plus sensibles.
- Sauvegardez les données sur des serveurs distincts : elles peuvent être stockées en interne, mais aussi auprès d'un prestataire informatique ou d'un hébergeur de données dans le cloud.
- Isolez informatiquement et physiquement le lieu de stockage des fichiers de sauvegarde : cela évite, en cas d'attaque, que les fichiers de sauvegarde ne soient eux aussi contaminés par le virus.
- Démultipliez les sauvegardes sur plusieurs supports : il faut évaluer leur viabilité par des essais périodiques de restauration.
- Faites une sauvegarde "hors ligne" pour éviter qu'elle soit elle aussi cryptée au moment de l'attaque.
- Vérifiez régulièrement que les sauvegardes se sont bien déroulées en vérifiant le rapport de sauvegarde.
- Testez régulièrement les sauvegardes en restaurant quelques dossiers ou fichiers.

Soyez conscient des avantages et inconvénients des supports

Type de supports	Avantages	Inconvénients
Les supports physiques externes, (disque dur externe, CD, DVD, clé USB, carte mémoire, etc.)	Facile à déplacer, facile à utiliser, coût limité	Durée de vie des supports, capacité de stockage limitée, support pouvant être compromis par les hackers pour faire une cyberattaque, peut être facilement perdu/volé
Le serveur de fichiers et serveur NAS	Capacité de stockage, centralisation et partage des données avec plusieurs appareils, sauvegarde de l'ensemble des données à partir d'un endroit unique ; accès gratuit aux données, permet de rester propriétaire de ses données	Système d'administration complexe, intégrité des données en cas de défaillance du NAS : prévoir un système de sauvegarde de secours, attention à la sécurité des accès
Les espaces de stockage en ligne (cloud)	Disponibilité quasi immédiate, travail collaboratif, gestion du ATAWAD (AnyTime, AnyWhere, AnyDevice)	Sécurité limitée, risques spécifiques pour la confidentialité des données, risques juridiques liés à l'incertitude sur la localisation des données, risques pour la disponibilité et l'intégrité des données, risques liés à l'irréversibilité des contrats

Prenez des précautions dans l'utilisation des supports

- Vérifiez l'intégrité du support de sauvegarde.
- Veillez à la confidentialité des données sensibles en rendant leur lecture impossible à des personnes non autorisées (mot de passe) ou en les chiffrant.
- Soyez vigilant en prenant connaissance des conditions générales d'utilisation.

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

ORDRE DES EXPERTS-COMPTABLES
Conseil Supérieur

4

Cybercriminalité

De boucliers tu te muniras

"Lorsque deux forces sont jointes, leur efficacité est double" Isaac Newton

Anecdote

Didier n'a pas mis à jour son antivirus. Après avoir téléchargé une application sur un site non sécurisé, un logiciel espion non détecté par l'antivirus a crypté l'ensemble de ses fichiers. Celui-ci vient de subir une attaque de type "ransomware" car il aurait dû mettre à jour son antivirus pour bloquer le logiciel espion. Ça lui a coûté 10 Bitcoins (soit environ 66 000 € à fin novembre 2017)...

Essentiel

- **Munissez-vous d'antivirus et d'antispam** : régulièrement à jour et actif, inspectez le contenu des clés USB et fichiers téléchargés.
- **Vérifiez que les systèmes sont régulièrement à jour** : évitez les systèmes obsolètes et les versions logicielles anciennes, révoquez les droits des collaborateurs en cas de départ, etc.
- **Disposez de pare-feux actifs.**

Bonnes pratiques

Munissez-vous d'antivirus et d'antispam

- Mettez en place un antivirus et un antispam.
- Vérifiez que l'antivirus et l'antispam sont actifs et à jour.
- Faites toujours inspecter le contenu des clés USB inconnues par l'antivirus.
- Avant d'ouvrir les documents téléchargés, lancez systématiquement une analyse antivirus en désactivant l'ouverture automatique de ces derniers.
- Ne désactivez pas l'antivirus et l'antispam.
- Faites régulièrement les mises à jour proposées de l'antivirus et antispam.
- Vérifiez que les mises à jour sont faites sur les sites officiels et sécurisés (https://).
- Configurez vos logiciels pour que les mises à jour de sécurité puissent s'installer automatiquement lorsque cela est possible.

Vérifiez que les systèmes sont à jour

- Faites régulièrement les mises à jour proposées des systèmes et logiciels : Windows, Adobe, Java, Office, Flash, etc.
- Vérifiez que ces mises à jour sont faites sur les sites officiels et sécurisés (https://).
- Évitez les systèmes d'exploitation obsolètes (Windows XP, Windows 2003), et les versions logicielles anciennes (Office, Adobe).
- Assurez-vous que les droits octroyés sur les systèmes d'information sont bien révoqués lors du départ d'un collaborateur.
- N'hésitez pas à utiliser les journaux d'évènements pour réagir aux évènements suspects.

Disposez de pare-feux actifs

- Vérifiez que vous disposez de pare-feux actifs sur les postes Windows et routeurs.
- Ne désactivez pas le pare-feu.
- Consultez régulièrement le pare-feu afin de vérifier les ports qui sont ouverts, vous pouvez également paramétrer votre pare-feu pour refuser toutes les connexions entrantes.

CNCC Compagnie nationale des commissaires aux comptes

ORDRE DES EXPERTS-COMPTABLES Conseil Supérieur

5

Cybercriminalité

Aux **cyberattaques** tu réagiras

"Il n'y a pas de vent favorable pour celui qui ne sait où il va" Sénèque

Anecdote

Thierry, expert-comptable associé dans le Rhône a été victime au sein de son cabinet d'une cyberattaque en juin dernier. Par chance, un des collaborateurs n'ayant plus accès aux fichiers a donné l'alerte aussitôt. Des mesures efficaces ont été prises pour éviter que le virus ne se propage. Tous les collaborateurs ont fermé leur session et se sont déconnectés du réseau. Le prestataire informatique est intervenu dans la foulée et à l'aide des sauvegardes quotidiennes, les fichiers ont pu être restaurés.

Essentiel

- **Adoptez une méthodologie de traitement du risque au jour de l'attaque** : débranchez l'ordinateur du réseau, n'utilisez plus l'équipement corrompu, portez plainte, ne payez pas la rançon, procédez à une analyse complète par l'antivirus, lancez la récupération des données, prévoyez des plans de secours, etc.
- **Contactez les structures d'assistance aux victimes de cyberattaques** : ACYMA, CERT, Cybermalveillance, Stopransomware.

Bonnes pratiques

Adoptez une méthodologie de traitement du risque au jour de l'attaque

- Débranchez immédiatement votre ordinateur du réseau (cable éthernet) et coupez votre wifi, afin que le virus ne se propage pas sur tout le réseau informatique.
- Signalez l'attaque au service informatique ou au prestataire dans les plus brefs délais afin qu'il puisse intervenir pour évaluer les dommages et limiter les conséquences.
- Arrêtez d'utiliser l'équipement corrompu afin de ne pas effacer les preuves : en matière de préservation des traces et indices, il est nécessaire de figer "la scène de crime" en rassemblant le maximum d'éléments qui permettront de mener à bien une enquête.
- ⚠ **Portez plainte auprès de la gendarmerie ou de la police nationale.**
- En cas de ransomware : ne payez pas la rançon, cela ne garantit en rien le déchiffrement des données.
- Procédez à une analyse complète par l'antivirus afin qu'il essaie de repérer et supprimer le code malveillant => si cette étape n'est pas concluante, il faudra alors procéder au formatage (effacement de toutes les données) du disque dur mais le mieux étant d'en acheter un neuf.
- Lancez la restauration des données à partir d'une sauvegarde.
- Prévoyez des plans de secours, élaborés avec des spécialistes, permettant d'éviter la perte irrémédiable de données et de garantir la continuité d'exploitation.
- Établissez un plan de communication en cas de crise suite à une cyberattaque grave.

Contactez les structures d'assistance aux victimes de cyberattaques

- ACYMA : plateforme d'assitance aux victimes d'actes de cybermalveillance. Grâce à ses réponses au questionnaire, la victime est orientée vers les prestataires de proximité susceptibles de répondre à son besoin technique.
- CERT : centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques.
- Cybermalveillance.gouv.fr : plateforme d'assitance du risque numérique mise en place par l'ANSSI.
- Stopransomware (réseau Cecyf prévention).

6

Le RGPD tu respecteras

"Pour savoir où l'on va, il faut savoir d'où l'on vient" Proverbe africain

Anecdote

Le cabinet Hergé gère la paye de ses clients et dispose des données personnelles des salariés. Dès le 25 mai 2018 le cabinet Hergé sera concerné par le RGPD et encourt une amende administrative pouvant aller, pour les cas les plus graves, jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

Essentiel

Vous-êtes tous concernés par le RGPD, mais faites-vous partie des 9% d'entreprises qui se déclarent prêtes ?

- Désignez un responsable des questions personnelles.
- Cartographiez vos traitements de données personnelles existants dans le cabinet.
- Priorisez et hiérarchisez les actions à mener.
- Gérer les risques.
- Organisez les processus internes.
- Documentez pour prouver la conformité au RGPD en cas de contrôle.

Bonnes pratiques

Étape 1 — Désignez un responsable des questions personnelles

- La désignation d'une personne chargée de ces questions est :
  - **obligatoire** si vous réalisez un suivi régulier ou traitez à grande échelle des données dites "sensibles" ou relatives à des condamnations pénales et infractions ;
  - **facultative** pour la plupart des cabinets d'expertise-comptable mais la CNIL encourage cette désignation : possibilité de désigner un DPO mutualisé ou externe.
- En attendant 2018, vous pouvez désigner un CIL pour commencer à organiser les actions à mener.

Étape 2 — Cartographiez vos traitements de données personnelles existants dans le cabinet

- Faites un inventaire des traitements de données personnelles mis en œuvre pour évaluer les pratiques, identifier les risques et arrêter un plan d'action.
- Organisez la gouvernance de la donnée avec le registre des traitements (modèle disponible sur le site de la CNIL) : Qui ? Quoi ? Pourquoi ? Où ? Jusqu'à quand ? Comment ?
- Les modèles de déclaration CNIL peuvent vous aider pour déterminer les finalités des traitements.

Étape 3 — Priorisez et hiérarchisez les actions à mener

- Déterminez les actions à mettre en œuvre pour respecter les nouvelles règles du RGPD.
- Assurez-vous que seules les données strictement nécessaires à la poursuite de l'objectif du traitement sont collectées et traitées.
- Identifiez la base juridique sur laquelle se fonde votre traitement (intérêt légitime, contrat, obligation légale, consentement de la personne...).
- Révisez vos mentions d'information pour qu'elles soient conformes aux exigences du règlement.
- Vérifiez que vos sous-traitants connaissent leurs nouvelles obligations et leurs responsabilités, assurez-vous de l'existence de clauses contractuelles (modèles de clauses sur le site de la CNIL) telles que : sécurité, confidentialité, protection des données.
- Prévoyez les modalités d'exercice des droits des personnes concernées : droit d'accès, de rectification, droit à la portabilité, retrait du contentement...
- Vérifiez les mesures de sécurité.

• • •

CNCC Compagnie nationale des commissaires aux comptes

ORDRE DES EXPERTS-COMPTABLES Conseil Supérieur

Le RGPD tu respecteras

...

Étape 4 — Gérez les risques

- S'il existe des risques élevés pour les droits et libertés des personnes concernées (traitements de données sensibles, traitements reposant sur le profilage...) menez pour chacun de ces traitements une étude d'impact sur la protection des données ("Privacy Impact Assessment" ou "PIA").
- Une PIA doit contenir une description du traitement et de ses finalités, une évaluation de la nécessité et de la proportionnalité du traitement, une appréciation des risques sur les droits et libertés des personnes concernées, les mesures envisagées pour traiter ces risques et se conformer au RGPD.
- L'outil PIA de la CNIL vise à accompagner la conduite d'analyse d'impact et faciliter l'appropriation des guides PIA de la CNIL (disponible sur le site de la CNIL).

Étape 5 — Organisez les processus internes

- Mettez en place des procédures internes pour assurer la protection des données tout au long du traitement :
  - en cas de faille de sécurité, de demande de rectification ou d'accès, de demande de modification des données collectées, de changement de prestataire ;
  - anticipez les violations de données : notifiez à l'autorité de protection des données dans les 72h et aux personnes concernées dans les meilleurs délais ;
  - prévues dans le RGPD : audits, privacy by design, notification des violations de données, gestion des réclamations et des plaintes...
- Établissez une politique de protection des données personnelles dans le cabinet et sensibilisez vos collaborateurs par le biais de communications et formations.
- Traitez les réclamations et demandes des personnes concernées en définissant les acteurs et les modalités.

Étape 6 — Documentez pour prouver la conformité au RGPD en cas de contrôle

- La documentation réalisée à chaque étape doit être réexaminée et actualisée régulièrement pour assurer une protection des données en continu.
- Documentation de vos traitements de données personnelles : registre des traitements (responsables des traitements) ou des catégories d'activités de traitements (sous-traitants), analyses d'impact sur la protection des données (cf. étape 4), encadrement des transferts de données hors de l'UE.
- Information des personnes : mentions d'informations, recueil du consentement des personnes concernées, procédures mises en place pour l'exercice des droits.
- Contrats définissant les rôles et responsabilités des acteurs : contrats avec les sous-traitants, procédures internes en cas de violations de données, preuve que les personnes concernées ont donné leur consentement.
- Lien avec la norme professionnelle de maîtrise de la qualité (NPMQ) et le manuel existant dans les cabinets.

7

Cybercriminalité

Des clés USB (et tous supports physiques externes) tu te méfieras

"Un ordinateur en sécurité est un ordinateur éteint. Et encore..." Bill Gates

Anecdote

Marc a reçu une clé USB en "cadeau". Cette clé USB a en réalité été distribuée par un pirate dans la boîte aux lettres, comme un cadeau. Par curiosité, et c'est humain, Marc branche alors cette clé sur son ordinateur pour voir ce qu'elle contient... Et se retrouve avec un virus qui donne accès aux pirates à toutes les données qu'il contient, mais également à l'ensemble des données de l'ensemble des postes connectés au réseau.

Essentiel

- **Adoptez des mesures préventives** : n'utilisez jamais une clé USB "abandonnée", avant toute utilisation, scannez et nettoyez la clé USB, bloquez la fonction "Autorun", affectez une clé par usage, chiffrez le contenu de vos clés USB.
- **Préparez vos déplacements à l'étranger** : n'emportez que les données indispensables pour la mission, marquez vos clés et gardez-les sur vous, jetez-les après usage.

Bonnes pratiques

Adoptez des mesures préventives

- Bloquez la clé en écriture pour éviter qu'une application malveillante ajoute des malwares sur votre clé.
- Ne tentez jamais de connecter votre poste de travail à un support de stockage externe, sauf s'il fait partie des outils de travail qui vous ont été attribués officiellement.
- Utilisez exclusivemet des clés USB sécurisées, fournies par l'entreprise et, en votre absence, conservez-les dans un rangement sécurisé (coffre, armoire, sous clés).
- Nettoyez proprement le contenu de la clé en utilisant des logiciels adaptés et faites analyser les fichiers provenant de supports USB via un antivirus avant ouverture.
- Attribuez des comptes et droits utilisateurs adéquats (pas de connexion en mode administrateur).
- Bloquez la fonction Autorun.
- Verrouillez les postes de travail en cas d'absence pour prévenir des accès intrusifs.
- Chiffrez les données enregistrées sur la clé USB pour éviter le piratage.
- Affectez une clé par usage pour réduire les risques de contamination, cet outil doit être strictement personnel et non cessible.

Préparez vos déplacements à l'étranger

- N'emportez que les données dont vous avez besoin pour la mission.
- Évitez de partir avec des données sensibles.
- Marquez d'un signe distinctif vos clés (pour repérer tout échange...).
- Gardez vos clés USB sur vous.
- En cas de perte ou de vol, informez les personnes compétentes et/ou prenez les mesures de sauvegardes prévues.
- Emportez une clé destinée aux échanges commerciaux et jetez-la après usage et destruction.
- À votre retour, ne connectez pas les clés sans les avoir testées au préalable.

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

ORDRE DES EXPERTS-COMPTABLES
Conseil Supérieur

8

Cybercriminalité

De **bonnes pratiques managériales** tu adopteras

"Celui qui déplace une montagne commence par déplacer de petites pierres" Confucius

Anecdote

L'entreprise AYMHACK, PME locale dans le secteur industriel, détient des données stratégiques telles que des brevets. Arthur est commercial et dispose d'informations sensibles... Il vient de se faire pirater lors d'un déplacement. Une classification des données sensibles de l'entreprise aurait permis de mieux les sécuriser afin de bloquer le "hacker" avant qu'il n'atteigne ces données.

Essentiel

- **Instaurez une classification des données de l'entreprise.**
- **Adoptez de bonnes habitudes de travail**
- **Renforcez vos procédures internes** : restrictions d'accès, gestion des départs des collaborateurs, procédure en cas de modification des RIB fournisseurs, etc.
- **Supervisez, auditez et corrigez** : tests d'intrusion, plan de reprise et de continuité d'activité.

Bonnes pratiques

Instaurez une classification des données de l'entreprise

- Identifiez les données stratégiques qui pourraient être particulièrement convoitées par les pirates.
- Évaluez les menaces et vulnérabilités sur ces données sensibles.
- Renforcez leur niveau de protection si besoin.

Adoptez de bonnes habitudes de travail

- Organisez des réunions d'information pour alerter les collaborateurs sur les nouveaux types de menaces.
- Sensibilisez, informez, avertissez les collaborateurs via des mesures de bons sens. Des vidéos, e-learning et sites permettent d'illustrer les dangers liés à la cybercriminalité de façon pédagogique et démontrent qu'il suffit parfois de simples mesures de bon sens pour se prémunir des attaques.
- Formez les collaborateurs les plus aguerris. Deux Mooc (Massive Open Online Course) certifiants sont disponibles sur le site de l'ANSSI pour vous initier à la cybersécurité, approfondir vos connaissances et ainsi vous prémunir des cyber-risques.

Renforcez vos procédures internes

- Mise en place de restrictions d'accès.
- Mise en place de procédures pour gérer le départ des collaborateurs (changez leurs mots de passe, supprimez leurs accès).
- Disposez d'une procédure en cas de demande de modification des RIB fournisseurs : prévoir une supervision ou un contre-appel vers un numéro déjà référencé.
- Renforcez les procédures de confirmation des banques.
- Soyez prudent dans les lieux publics : n'importe qui peut voir l'écran (disposez d'un filtre de confidentialité peut éviter certaines fuites) ou écouter une conversation / anecdote susceptible d'altérer l'image de marque de l'entreprise ; protégez les pratiques sensibles propres à l'entreprise.

Supervisez, auditez et corrigez

- Procédez à des tests d'intrusion pour tester la vigilance des collaborateurs et faciliter l'adhésion de l'ensemble des acteurs à la mise en place de mesures simples de prévention de cyberattaques.
- Rédigez un plan de reprise et de continuité d'activité qui permet de garantir les fonctions vitales de l'entreprise en cas d'attaque.

CNCC

ORDRE DES EXPERTS-COMPTABLES
Conseil Supérieur

9

Les usages tu règlementeras

"Si vous pensez que la technologie peut résoudre tous vos problèmes de sécurité, alors vous ne comprenez ni les problèmes, ni les technologies..." Bruce Schneir

Anecdote

Lydie va quotidiennement sur les réseaux sociaux pour relater ses journées avec ses clients et ses collègues. Elle vient d'annoncer sur Twitter que son entreprise est en train de se faire racheter et a juste oublié qu'il s'agissait d'une information confidentielle à ne pas divulguer... L'existence d'une charte d'utilisation des réseaux sociaux, annexée à la charte informatique, aurait permis d'éviter ce type de risques.

Essentiel

- **Encadrez les pratiques par l'utilisation d'une charte informatique.**
- **Fixez les règles et consignes que les utilisateurs doivent respecter.**
- **Rendez-la opposable aux salariés** soit en l'annexant au contrat de travail des salariés, soit en formalisant l'acceptation individuelle par chacun des salariés ou en lui donnant une valeur de règlement intérieur.

Bonnes pratiques

Encadrez les pratiques par l'utilisation d'une charte informatique

- La mise en place d'une charte informatique est indispensable... voire obligatoire dès lors que le cabinet collecte des données à caractère personnel... Ce qui s'avère aujourd'hui omniprésent ! Un modèle est disponible sur le kit mission "accompagner ses clients dans la mise en place d'un règlement interieur".
- Responsabilisez les acteurs par une démarche d'explication et de sensibilisation des enjeux et risques associés à son utilisation.
- Pour faire adhérer tous les collaborateurs, disposez d'un charte claire, à la portée de tous et diffusée à l'ensemble du personnel.
- Informez les salariés des modalités de contrôle de leur employeur tout en veillant au respect de la vie privée.

Fixez les règles et consignes que les utilisateurs doivent respecter

- Définissez les principes généraux de sécurité : accès, habilitation, sécurité, matériels, programmes, logiciels...
- Formalisez les règles d'utilisation du système d'information : séparez les usages personnels et professionnels, mots de passe, sauvegarde, utilisation d'internet...
- Prévoyez d'y intégrer les modalités d'utilisation des réseaux sociaux et de l'ensemble des moyens technologiques mis à disposition des salariés (smartphones, supports nomades...).
- Prévoyez des mesures de contrôle par l'employeur : équilibre vie privée et protection du SI...
- Déterminez les politiques de sanctions prévues en cas de violations des obligations : les sanctions devront être proportionnelles à l'impact que l'infraction aurait sur le système d'information.
- Prenez acte de sa perfectibilité et révisez-la régulièrement pour qu'elle s'adapte à l'évolution des technologies.

Rendez-la opposable aux salariés

- Pour qu'elle soit opposable aux salariés, plusieurs options sont possibles :
  - option 1 : annexez la charte au contrat de travail des salariés ;
  - option 2 : formalisez l'acceptation individuelle par chacun des salariés ;
  - option 3 : donnez à la charte une valeur de règlement intérieur et respectez scrupuleusement le formalisme préalable à l'adoption d'un règlement intérieur => dépôt au greffe du Conseil des Prud'hommes et transmission à l'inspection du travail.

CNCC Compagnie nationale des commissaires aux comptes

ORDRE DES EXPERTS-COMPTABLES Conseil Supérieur

10

Cybercriminalité

Les **collaborateurs** tu sensibiliseras

"Le maillon faible se situe entre la chaise et le clavier" Anonyme

Anecdote

L'entreprise PADEUBOL subit une attaque liée à une mauvaise pratique d'un collaborateur suite à la réception d'un email douteux. La continuité d'exploitation est compromise, elle doit mettre la clé sous la porte. La simple mise en place d'un test d'intrusion aurait permis d'anticiper et d'éviter cette attaque. En effet une prise de conscience générale et immédiate des collaborateurs aurait facilité l'adhésion des acteurs au sein de l'entreprise à la mise en place de mesures simples de prévention de cyberattaques.

Essentiel

- **Sensibilisez les collaborateurs.**
- **Nommez un responsable de la sécurité du Système d'Information pour piloter la démarche** et coordonner les différentes actions à mener.
- **Impliquez et responsabilisez les usages dans les mécanismes de cyberprévention** : informez, sensibilisez, formez, motivez.
- **Soyez interactif et passez d'une pédagogie "passive" à une pédagogie "active".**

Bonnes pratiques

Sensibilisez les collaborateurs

En 1982, Rich Skrenta, lycéen américain âgé de 15 ans, a créé le 1er virus référencé qui se propage automatiquement par échange de supports amovibles : "Elk Cloner". Le mécanisme viral associant les fragilités humaines à un code malveillant, déjà présent dans les années 80, est strictement identique aux mécanismes actifs aujourd'hui. Il faut donc l'accepter : depuis plus de 35 ans, l'Homme est le maillon faible de la défense numérique. Longtemps délaissé au profit de la technologie, le facteur humain doit désormais faire partie intégrante de la cybersécurité.

Nommez un responsable de la sécurité du SI pour piloter la démarche

- Sa mission est de garantir l'intégrité, la confidentialité, la disponibilité et la traçabilité des données de l'ensemble des systèmes d'information du cabinet.
- Véritable chef d'orchestre de la sécurité du SI, il définit les orientations, élabore et met en œuvre une politique de sécurité.

Impliquez et responsabilisez les usagers dans les mécanismes de cyberprévention

1/ **Informez > Quoi ?** L'utilisateur sait qu'un danger existe.
2/ **Sensibilisez > Pourquoi ?** L'utilisateur connaît les risques pour le cabinet et lui-même.
3/ **Formez > Comment ?** L'utilisateur sait ce qu'il faut faire.
4/ **Motivez > Quand ?** L'utilisateur sait qu'il doit être vigilant constamment.

Soyez interactif et passez d'une pédagogie "passive" à une pédagogie "active"

- Selon le "cône d'apprentissage" d'Edgar Dale, l'expérimentation et la simulation permettent de retenir 90 % des messages clés contre seulement 10 % de ce qui est lu : test d'intrusion...
- La sécurité est avant tout une question de jugement et de comportement. C'est donc en impliquant les utilisateurs que les consciences à la sécurité de l'information seront éveillées durablement.

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

ORDRE DES EXPERTS-COMPTABLES
Conseil Supérieur

11

Cybercriminalité

Les objets connectés tu sécuriseras

"Tout artiste ou chercheur le sait, sans un espace protégé, et même sanctuarisé, où l'erreur est possible, l'innovation cesserait d'exister" Inconnu

Anecdote

Dans le cadre du télétravail, Madame Alexa SNIPS profite de la fonctionnalité « kit main libre » de son enceinte intelligente pour mener des réunions en téléconférence avec ses équipes.
Or, cette dernière a été piratée et le fraudeur a enregistré ces réunions de travail dont certaines abordent des sujets stratégiques / confidentiels.

Essentiel

- **Sécurisez les échanges de données.**
- **Protégez** votre profil utilisateur.
- **Maîtrisez les enjeux** autour de votre vie professionnelle et privée.

Bonnes pratiques

Sécurisez les échanges de données

- Vérifiez que l'appairage ainsi que la connexion de l'objet depuis Internet nécessitent un bouton d'accès physique ou l'usage d'un mot de passe.
- Modifiez le paramétrage par défaut (mot de passe, code PIN, etc.).
- Vérifiez l'accès aux données et la possibilité de les supprimer.
- Éteignez l'objet non utilisé afin d'éviter qu'il ne capte les données sensibles.
- Privilégiez l'utilisation d'un VPN (Virtual Private Network, afin de sécuriser les flux d'informations entre l'objet et le réseau de l'entreprise) en l'absence de cloud.
- Assurez la protection du réseau wifi personnel à l'aide d'une clé de chiffrement robuste (clé WPA *a minima*).
- Réalisez les mises à jour de sécurité proposées par les fabricants d'objets connectés.

Protégez votre profil utilisateur pour les objets nécessitant l'ouverture d'un compte en ligne

- En cas de télétravail, ne connectez pas vos outils professionnels aux objets à reconnaissance vocale personnels.
- Utilisez des pseudonymes (et non vos données personnelles).
- Ne communiquez pas d'informations superflues (donnez une date de naissance au 1er janvier si le système a besoin de déterminer un âge).
- Créez une adresse secondaire de l'adresse principale et qui soit différente de l'adresse professionnelle.
- Pour aller plus loin : https://www.cnil.fr/fr/objets-connectes-noubliez-pas-de-les-securiser.

Maîtrisez les enjeux autour de votre vie professionnelle et privée dans le cas des assistants vocaux

- Éteignez l'appareil lorsqu'il est inutilisé ou que l'on ne souhaite pas être écouté.
- Informez les tiers du possible enregistrement des conversations (à défaut, coupez le micro).
- Connectez uniquement les services présentant une réelle utilité ; attention aux risques à partager des données confidentielles ou des fonctionnalités sensibles.
- Gardez en mémoire que les propos tenus peuvent enrichir votre profil publicitaire.
- Supprimez régulièrement l'historique des conversations.
- N'hésitez pas à contacter les services supports en cas de questions et, le cas échéant, la CNIL. https://www.cnil.fr/fr/enceintes-intelligentes-des-assistants-vocaux-connectes-votre-vie-privee

CNCC

ORDRE DES EXPERTS-COMPTABLES
Conseil Supérieur

ANNEXE 9 //

AFFICHE DE SENSIBILISATION, CNIL

LES MOTS DE PASSE N'ONT PLUS DE SECRET POUR VOUS!

****

UN MOT DE PASSE EN BÉTON |

Un bon mot de passe doit contenir 12 caractères, d'au moins 4 types différents : des minuscules, des majuscules, des chiffres et des caractères spéciaux. Il peut être plus court si votre compte est équipé de sécurités complémentaires !

****

IL NE DIT RIEN SUR VOUS |

Personne ne doit deviner votre mot de passe à partir du nom de votre chien ou de votre film préféré. Idem pour le code de votre smartphone : préférez un nombre aléatoire à une année.

****

UN COMPTE, UN MOT DE PASSE |

Pour éviter les piratages en cascade, chacun de vos comptes en ligne qui présente un caractère sensible (banque, messagerie, réseau social, etc.) doit être verrouillé avec un mot de passe propre et unique.

****

NE JAMAIS L'ABANDONNER EN PLEINE NATURE |

Les post-it, les fichiers texte, votre smartphone ou votre boite de messagerie ne sont pas conçus pour sécuriser le stockage de vos mots de passe. Pensez aussi à ne jamais les enregistrer dans le navigateur d'un ordinateur partagé.

****

DEUX CADENAS VALENT MIEUX QU'UN |

Quand le service vous le propose, activez la double authentification. Si quelqu'un se connecte à votre compte depuis un terminal inconnu, le site vous prévient par SMS/e-mail. Libre à vous d'autoriser ou de refuser l'accès !

****

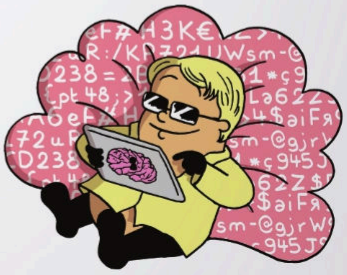
LES RETENIR SANS LES ÉCRIRE

... EN TRAVAILLANT VOS NEURONES |

Mémorisez une phrase puis utilisez la première lettre de chaque mot pour créer votre mot de passe. La phrase doit contenir des chiffres et des caractères spéciaux !

... EN REPOSANT VOS MÉNINGES |

Utilisez un gestionnaire de mots de passe ou un trousseau d'accès chiffré pour stocker vos mots de passe en toute sécurité. Vous n'aurez à retenir qu'un mot de passe pour accéder à l'ensemble de vos comptes !



****

PLUS DE CONSEILS SUR WWW.CNIL.FR

CNIL.

COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Illustrations : Martin Vidberg

Source : www.cnil.fr/sites/cnil/files/atoms/files/affiche_les-mots-de-passe-n-ont-plus-de-secret-pour-vous.pdf.

ANNEXE 10 //

TYPOLOGIE DES SUPPORTS DE SAUVEGARDE

Source : www.techtarget.com/searchstorage/definition/WORM-write-once-read-many.

ANNEXE 11 //

TYPOLOGIE DES SAUVEGARDES

Type	Avantages	Inconvénients
Normale (complète)	Lors de la restauration, les fichiers sont faciles à trouver parce qu'ils sont présents sur le média. Cela facilite la copie de fichiers à partir du support.	Demande beaucoup de temps et d'espace de stockage pour réaliser l'opération. Si les fichiers ne sont pas beaucoup modifiés, les sauvegardes sont pratiquement identiques. Ce type est recommandé pour la sauvegarde des fichiers du système d'exploitation.
Incrémentale	Demande moins d'espace pour le stockage des données. Permet des copies rapides.	La restauration complète d'un système peut prendre beaucoup plus de temps qu'une sauvegarde normale ou différentielle.
Différentielle	Une restauration demande seulement le support des dernières sauvegardes complètes et différentielles. Elle est plus rapide qu'une complète.	La restauration complète d'un système peut prendre beaucoup plus de temps qu'une sauvegarde normale. S'il existe de multiples modifications sur les fichiers, les sauvegardes de ce type peuvent prendre plus de temps que des incrémentales.

Source : Carpentier, 2023, p. 272.

ANNEXE 12 //
AVANTAGES ET INCONVÉNIENTS DU *CLOUD COMPUTING*

Les avantages du *cloud computing* :

_La redondance du stockage des données est gérée par le prestataire ;

_Le prestataire possède l'expertise et l'expérience pour faire fonctionner l'environnement et sécuriser les données ;

_Le prestataire peut allouer beaucoup plus de ressources à la sécurisation des données ;

_Les mise à jour logicielles sont mieux gérées ;

_La flexibilité pour l'utilisateur en termes de variation de ressources et de capacités ;

_Mise à disposition d'une assistance par le prestataire pour accompagner le client dans son quotidien.

Les inconvénients du cloud computing :

_Le prestataire peut représenter une cible plus appétissante pour des attaques informatiques, car il héberge une masse énorme de données ;

_L'utilisateur est très dépendant de son prestataire ;

_Freins à la mobilité : la migration d'un environnement à un autre a un coût important, et demande beaucoup de temps et d'expertise. Par ailleurs, il peut exister un manque de portabilité ou d'interopérabilité des données. Ainsi, le choix du prestataire est encore plus critique dans la mesure où il sera très coûteux et complexe d'en changer par la suite ;

_Rigidité de l'environnement logiciel en SaaS : par exemple, au sein d'ACD (solution de *cloud computing* en mode SaaS dédié à l'expertise-comptable), la suite Office est la version de 2016 (le présent mémoire est rédigé en mars 2024) et ne comporte donc pas les dernières évolutions apportées par Microsoft. Par ailleurs, au sein de Microsoft Excel, l'exécution de macros n'est pas possible (ce qui améliore considérablement la sécurité, mais nuit tout aussi considérablement au potentiel d'utilisation de ce logiciel) : ce choix se justifie en termes de sécurité, mais il relève du prestataire et non du client, qui n'a d'autre solution que de s'en contenter. Ainsi, l'utilisateur a uniquement la main sur les droits et autorisations, mais pas sur le fonctionnement et le paramétrage profond des outils qu'il utilise. Le PaaS et l'IaaS permettent une plus grande flexibilité en termes de paramétrage, en échange d'une plus grande responsabilité en termes de sécurisation des données confiée à l'utilisateur ;

_Manque de visibilité sur l'équipement et l'infrastructure du prestataire (ce qui nuit à la surveillance des ressources par l'utilisateur), et sur l'éventuel lieu de stockage des données, qui conditionne les lois qui les régissent. Manque de visibilité également sur les sous-traitants du prestataire, qui peuvent ne pas offrir les mêmes garanties que lui ;

_Réglementation : point de vigilance à avoir sur la législation applicable aux données transitant chez le prestataire et sur la hiérarchie entre celle-ci et celle s'appliquant à l'utilisateur ;

_Le *cloud computing* n'affranchit pas de toutes les obligations du cabinet d'expertise-comptable en termes de sécurité (politique de mots de passe et de privilèges, erreurs, négligences, malveillance, etc.) ;

_Grande évolutivité des tarifs : couplée à une difficulté de migration, la dépendance au prestataire ne laisse que très peu de leviers de négociations au cabinet d'expertise-comptable en cas de modification des tarifs ;

_Évolutivité potentielle des conditions générales d'utilisation, qui peuvent apporter de nouvelles problématiques en termes de gouvernance, de sécurité, de responsabilité, etc. ;

_Mutualisation des infrastructures et ressources : la plupart des cabinets d'expertise-comptable ayant fait le choix de passer dans le *cloud* le font sur des modèles mutualisés, ce qui peut entraîner des embouteillages et donc des ralentissements indépendants de l'activité de l'utilisateur. Il peut par exemple être parfois long et fastidieux de se connecter à son espace de travail le lundi matin, car une grande partie des clients du prestataire cherchera à le faire au même moment. De même, la perte de réputation de l'un des utilisateurs peut faire tache d'huile et compromettre la réputation informatique de l'ensemble des clients du prestataire. Par exemple, si l'un des clients du prestataire mène des opérations de *spamming*, l'ensemble des clients peut se retrouver sur liste noire par contagion ;

_Non maîtrise du calendrier : certaines opérations de maintenance ou de mise à jour peuvent causer l'indisponibilité des services. Les clients sont donc tributaires du calendrier de leurs prestataires. Si les prestataires essaient d'éviter les horaires de bureau standards, certains lancent des mises à jour à des moments où les utilisateurs sont tout de même susceptibles d'avoir besoin de travailler. Les opérations peuvent par ailleurs être parfois très longues (une dizaine d'heures par exemple) : il n'y a donc plus pour le client qu'à prendre son mal en patience ;

_Certification : si l'utilisateur a obtenu une certification, son passage dans le *cloud* peut la lui compromettre ;

_L'utilisation du *cloud* nécessite une connexion Internet. Ainsi, en cas de coupure, le client n'a plus la possibilité d'accéder à son environnement de travail et à ses données.

ANNEXE 13 //

LES QUATRE PILIERS D'UNE POLITIQUE D'ASSURANCE CYBER

Source : www.amrae.fr/sites/default/files/public/2019-11/ANSSI_FR_WEB.pdf.

ANNEXE 14 //

ÉVALUER LE NIVEAU DE SÉCURITÉ DES DONNÉES PERSONNELLES DE MON ORGANISME

Avez-vous pensé à... ?

FICHES		MESURES	
1	Piloter la sécurité des données	Faire de la sécurité un enjeu partagé et porté par l'équipe dirigeante	☐
		Évaluer régulièrement l'efficacité des mesures de sécurité mises en œuvre et adopter une démarche d'amélioration continue	☐
2	Définir un cadre pour les utilisateurs	Rédiger une charte informatique comprenant les modalités d'utilisation des systèmes informatiques, les règles de sécurité et les moyens d'administration en place	☐
		Donner une force contraignante à la charte et y rappeler les sanctions encourues en cas de non-respect	☐
3	Impliquer et former les utilisateurs	Sensibiliser les personnes manipulant les données	☐
		Adapter le contenu des sensibilisations à la population ciblée et à leurs tâches	☐
4	Authentifier les utilisateurs	Octroyer un identifiant (« *login* ») unique à chaque utilisateur	☐
		Adopter une politique de mot de passe conforme aux recommandations de la CNIL	☐
		Obliger l'utilisateur à changer le mot de passe attribué automatiquement ou par un administrateur	☐
5	Gérer les habilitations	Définir des profils d'habilitation	☐
		Supprimer les permissions d'accès obsolètes	☐
		Réaliser une revue annuelle des habilitations	☐
6	Sécuriser les postes de travail	Prévoir une procédure de verrouillage automatique de session	☐
		Installer et configurer un pare-feu (« *firewall* » en anglais) logiciel	☐
		Utiliser des antivirus régulièrement mis à jour	☐
		Recueillir l'accord de l'utilisateur avant toute intervention sur son poste	☐
7	Sécuriser l'informatique mobile	Sensibiliser les utilisateurs aux risques spécifiques du nomadisme	☐
		Prévoir des moyens de chiffrement des équipements mobiles	☐
		Exiger un secret pour le déverrouillage des smartphones	☐
8	Protéger le réseau informatique	Limiter les flux réseau au strict nécessaire	☐
		Sécuriser les réseaux Wi-Fi, notamment en mettant en œuvre le protocole WPA3	☐
		Sécuriser les accès distants des appareils informatiques nomades par VPN	☐
		Cloisonner le réseau, entre autres en mettant en place une DMZ (zone démilitarisée)	☐
9	Sécuriser les serveurs	Désinstaller ou désactiver les services et interfaces inutiles	☐
		Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées	☐
		Installer sans délai les mises à jour critiques après les avoir testées le cas échéant	☐

CNIL.

FICHES		MESURES	
10	**Sécuriser les sites web**	Sécuriser les flux d'échange des données	☐
		Vérifier qu'aucun secret ou donnée personnelle ne passe par les URL	☐
		Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu	☐
11	**Encadrer les développements informatiques**	Prendre en compte la protection des données personnelles dès la conception	☐
		Proposer des paramètres respectueux de la vie privée par défaut	☐
		Réaliser des tests complets avant la mise à disposition ou la mise à jour d'un produit	☐
		Utiliser des données fictives ou anonymisées pour le développement et les tests	☐
12	**Protéger les locaux**	Restreindre les accès aux locaux au moyen de portes verrouillées	☐
		Installer des alarmes anti-intrusion et les vérifier périodiquement	☐
13	**Sécuriser les échanges avec l'extérieur**	Chiffrer les données avant leur envoi	☐
		S'assurer qu'il s'agit du bon destinataire	☐
		Transmettre le secret lors d'un envoi distinct et via un canal différent	☐
14	**Gérer la sous-traitance**	Prévoir des clauses spécifiques dans les contrats des sous-traitants	☐
		Prévoir les conditions de restitution et de destruction des données	☐
		S'assurer de l'effectivité des garanties prévues (ex. : audits de sécurité, visites)	☐
15	**Encadrer la maintenance et la fin de vie des matériels et des logiciels**	Enregistrer les interventions de maintenance dans une main courante	☐
		Encadrer les interventions de tiers par un responsable de l'organisme	☐
		Effacer les données de tout matériel avant sa mise au rebut	☐
16	**Tracer les opérations**	Prévoir un système de journalisation	☐
		Informer les utilisateurs de la mise en place du système de journalisation	☐
		Protéger les équipements de journalisation et les informations journalisées	☐
		Analyser régulièrement les traces pour détecter la survenue d'un incident	☐
17	**Sauvegarder**	Effectuer des sauvegardes régulières	☐
		Protéger les sauvegardes, autant pendant leur stockage que leur convoyage	☐
		Tester régulièrement la restauration des sauvegardes et leur intégrité	☐

FICHES		MESURES	
18	Prévoir la continuité et la reprise d'activité	Prévoir un plan de continuité et de reprise d'activité	☐
		Effectuer des exercices régulièrement	☐
19	Gérer les incidents et les violations	Traiter les alertes remontées par le système de journalisation	☐
		Prévoir les procédures et les responsabilités internes pour la gestion des incidents, dont la procédure de notification aux régulateurs des violations de données personnelles	☐
20	Analyse de risques	Mener une analyse de risques, même minimale, sur les traitements de données envisagés	☐
		Suivre au cours du temps l'avancement du plan d'action décidé à l'issue de l'analyse de risques	☐
		Revoir régulièrement l'analyse de risques	☐
21	Chiffrement, hachage, signature	Utiliser des algorithmes, des logiciels et des bibliothèques reconnues et sécurisées	☐
		Conserver les secrets et les clés cryptographiques de manière sécurisée	☐
22	*Cloud* : Informatique en nuage	Inclure les services cloud dans l'analyse de risques	☐
		Évaluer la sécurité mise en place par le fournisseur	☐
		Veiller à la répartition des responsabilités de sécurité dans le contrat	☐
		Assurer le même niveau de sécurité dans le cloud que sur site	☐
23	Applications mobiles : Conception et développement	Prendre en compte les spécificités de l'environnement mobile pour réduire les données personnelles collectées et limiter les permissions demandées	☐
		Encapsuler les communications dans un canal TLS	☐
		Utiliser les suites cryptographiques du système d'exploitation et les protections matérielles des secrets	☐
24	Intelligence artificielle : Conception et apprentissage	Adopter les bonnes pratiques de sécurité applicables au développement informatique	☐
		Veiller à la qualité et l'intégrité des données utilisées pour l'apprentissage et l'inférence	☐
		Documenter le fonctionnement et les limitations du système	☐
25	API : Interfaces de programmation applicative	Organiser et documenter la sécurité des accès aux API et aux données	☐
		Limiter le partage des données uniquement aux personnes et aux finalités prévues	☐

CNIL.

Source : www.cnil.fr/sites/cnil/files/2024-03/guide_securite_donnees_personnelles_checklist.pdf.

SOURCES
ET BIBLIOGRAPHIE

LIVRES

Arduin (Pierre-Emmanuel), Grundstein (Michel) et Rosenthal-Sabroux (Camille), *La Menace intérieure*, ISTE éditions, 2018.

Arduin (Pierre-Emmanuel), Grundstein (Michel) et Rosenthal-Sabroux (Camille), *Système d'information et de connaissance*, ISTE éditions, 2015.

Bilet (Virginie), Liottier (Miguel), *Survivre à une cyberattaque*, éditions VA, 2018.

Brooks (Charles J.), Grow (Christopher), Craig (Philip), Short (Donald), *Cybersécurité, sécurisation des systèmes informatiques*, Deboeck Supérieur, 2021.

Carpentier (Jean-François), *La Sécurité informatique dans la petite entreprise*, éditions Eni, 2023.

Foray (Bernard), *La Fonction RSSI*, Dunod, 2011.

Labonde (Mathieu), Malhuret (Lou), Piedallu (Benoît), Simon (Axel), *Internet et Liberté*, éditions Vuibert, 2022.

Lacombe (Jean-Pierre), Lesage (Nadège), *Management de la sécurité de l'information et ISO 27001*, Éditions ENI, 2021.

Le Cœur (Jérôme), « Sécuriser les données personnelles de son entreprise », *I2D – Information, données & documents*, vol 53, n° 1, 2016, p. 25-26.

Lévy (Mick). *Sortez vos données du frigo. Une entreprise performante avec la* data *et l'IA*, Dunod, 2021.

Linty, Laurent, *Protection des données de l'entreprise, Mise en œuvre de la disponibilité et de la résilience des données*, éditions Eni, 2021.

Mauduit (Laurent), *Vous ne me trouverez pas sur Amazon !*, éditions Divergences, 2024.

Salamon (Yann), *Cybersécurité et cyberdéfense, enjeux stratégiques*, Ellipses, 2020.

Wilson (Duane), *Cybersecurity*, MIT Press, 2021.

PRESSE

Berne (Xavier), « L'État renouvelle son socle interministériel de logiciels libres », *Next*, 22/12/2015, https://next.ink/15854/97812-l-etat-renouvelle-son-socle-interministeriel-logiciels-libres.

Carasso (Jorge), « Les nouvelles techniques des escrocs du web pour voler leurs victimes », *Le Figaro*, 09/03/2024, www.lefigaro.fr/conjoncture/les-nouvelles-techniques-des-escrocs-du-web-pour-voler-leurs-victimes-20240309.

Carrère (Marie-Caroline), « Cyber : Miris, la mutuelle des entreprises obtient son agrément », *L'Argus de l'assurance*, 03/01/2023, www.argusdelassurance.com/assurance-dommages/risques-d-entreprise/cyber-miris-la-mutuelle-des-entreprises-obtient-son-agrement.209426.

Cheminade (Pierre), « Coaxis et Guyamier frappées par de violentes cyberattaques au rançongiciel », *La Tribune*, 17/01/2024, https://objectifaquitaine.latribune.fr/business/2024-01-17/guyamier-et-coaxis-frappees-par-de-violentes-cyberattaques-au-rancongiciel-987511.html.

Chen (Heather), Magramo (Kathleen), « Finance worker pays out $25 million after video call with deepfake 'chief financial officer' », 04/02/2024, *CNN World*, edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html.

Collectif, « Comment les assureurs deviennent des évaluateurs de cybersécurité de votre entreprise », IT for Business, 28/02/2024, www.itforbusiness.fr/comment-les-assureurs-deviennent-des-evaluateurs-de-cybersecurite-de-votre-entreprise-73960.

Collectif, « Cyberattaque de COAXIS : Réponses et Conseils pour les plus de 1200 cabinets d'Expertise-Comptable », *DPO Partagé*, 16/12/2023, www.dpo-partage.fr/cyberattaque-de-coaxis.

Collectif, « Les Cyberattaques les plus courantes contre les entreprises », Aforp, www.aforp.fr/les-cyberattaques-les-plus-courantes-contre-les-entreprises.

Collectif, « Cybersécurité : Top 10 des cyberattaques fréquentes en 2023 », 27/06/2023, *00driveBlog*, www.oodrive.com/fr/blog/securite/cybersecurite-top-10-des-cyberattaques-frequentes-en-2023.

Collectif, « Le Cycle de vie d'une donnée personnelle », *Data Legal Drive*, 06/10/2022, https://datalegaldrive.com/cycle-vie-donnee-personnelle.

Collectif, « Définition d'un malware », Oracle, www.oracle.com/fr/cloud/malware-logiciel-malveillant.

Collectif, « Estonia fines man for "cyber war" », *BBC News*, 25/01/2008, news.bbc.co.uk/2/hi/technology/7208511.stm.

Collectif, « Journée mondiale du mot de passe : et si, aujourd'hui, vous jetiez vos post-it ? », *Solutions numériques et cybersécurité*, 04/05/2023, www.solutions-numeriques.com/journee-mondiale-du-mot-de-passe-et-si-aujourdhui-vous-jetiez-vos-post-it.

Collectif, « Man-in-the-Middle », *TechIT*, 08/2016, www.lemagit.fr/definition/Man-in-the-Middle.

Collectif, « Le marché mondial de la cyberassurance », *Atlas magazine*, 26/06/2023, www.atlas-mag.net/category/tags/focus/le-marche-mondial-de-la-cyberassurance.

Collectif, « Numéro de sécu, mutuelle : 33 millions de Français victimes d'une cyberattaque au tiers payant », *Les Échos*, 07/02/2024, www.lesechos.fr/industrie-services/pharmacie-sante/numero-de-secu-mutuelle-33-millions-de-francais-victimes-dune-cyberattaque-au-tiers-payant-2074842.

Collectif, « Panorama du phishing en 2023 », *MISC*, hors-série n°27, éditions Diamond, janvier 2024.

Collectif, « Le Piratage de Coaxis par LockBit 3.0 : une analyse approfondie », *DPO Partagé*, 02/01/2024, www.dpo-partage.fr/piratage-de-coaxis-par-lockbit-3-0.

Collectif, « Piratage de Coaxis par LockBit 3.0 : Fin du décompte de Lockbit et aucune donnée disponible en ligne », *DPO Partagé*, 09/01/2024, www.dpo-partage.fr/coaxis.

Collectif, « Professionnels, agents publics, attention à l'arnaque au président ! », DGCCRF, www.economie.gouv.fr/dgccrf/professionnels-agents-publics-attention-a-larnaque-au-president.

Collectif, « Qu'est-ce qu'un ransomware ou rançongiciel ? », 02/03/2022, www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/ransomware-rancongiciel-definition.

Crochet-Damais (Antoine), « Six choses qu'OVH ne dit pas sur l'incendie de Strasbourg », *Le Journal du net*, 29/03/2021, www.journaldunet.com/cloud/1499203-incendie-d-ovh-a-strasbourg-une-heure-pour-couper-le-courant.

Fabre Soundron (Marina), « En 2020, 90 % des organisations françaises ont été visées par des cyberattaques », *Novethic*, 29/12/2020, www.novethic.fr/actualite/economie/economie/isr-rse/entre-les-vaccins-le-covid-19-et-le-teletravail-2020-a-ete-l-annee-des-cyberattaques-149341.html.

Ferdjallah-Cherel (Eric), Malard (Marc), « La profession comptable en chiffres », *Revue française de comptabilité*, n° 561, 02/2022, revuefrancaisedecomptabilite.fr/la-profession-comptable-en-chiffres.

Finey (Amber), « Cybercriminalité, l'e-mail est le premier vecteur relevé dans le monde entier », *Cybercriminalité Pénal*, 30/12/2021, cybercriminalite-penal.fr/cybercriminalite-lemail-est-le-premier-vecteur-releve-dans-le-monde-entier.

Gatlan (Sergiu), « LastPass: Hackers targeted employee in failed deepfake CEO call », 11/04/2024, *Bleeping Computer*, www.bleepingcomputer.com/news/security/lastpass-hackers-targeted-employee-in-failed-deepfake-ceo-call.

Gross (Grant), « La Maison-Blanche exhorte les développeurs à abandonner C et C++ », *Le Monde informatique*, 28/02/2024, www.lemondeinformatique.fr/actualites/lire-la-maison-blanche-exhorte-les-developpeurs-a-abandonner-c-et-c-93089.html.

Kaminsky (Jean), « 93 % des TPE et PME n'ont pas de budget dédié cybersécurité, 25 % ont une couverture assurance », *Solutions numériques et cybersécurité*, 10/08/2023, www.solutions-numeriques.com/93-des-tpe-et-pme-nont-pas-de-budget-dedie-cybersecurite-25-ont-une-couverture-assurance.

L. (Virginie), « 10 chiffres de cybersécurité qui révèlent l'importance du risque cyber pour les entreprises », *Stoïk*, 20/06/2023, www.stoik.io/cybersecurite/chiffres-cles.

Lamarge (Anaïs), « Près de 9 entreprises sur 10 ont fait l'objet d'une cyberattaque ! », *Entreprendre*, 14/09/2023, www.entreprendre.fr/la-cybersecurite-un-enjeu-global-qui-concerne-lensemble-des-entreprises.

Le Ferrand (Geoffrey), cours « Audits spécifiques », Master 2 CCA, IAE Bretagne-Sud, 2024.

Lefèvre (Laurent), Pierson (Jean-Marc) « Le *big data* est-il polluant ? », *CNRS Le Journal*, 02/04/2015, https://lejournal.cnrs.fr/billets/le-big-data-est-il-polluant.

Loeillet (Benoît), « De l'importance stratégique des données pour les entreprises à leur indispensable qualité », *Harvard Business Review*, 22/02/2024, www.hbrfrance.fr/organisation/de-limportance-strategique-des-donnees-pour-les-entreprises-a-leur-indispensable-qualite-60463.

Morgan (Steve), « Top 10 Cybersecurity Predictions and Statistics For 2024 », *Cybercrime Magazine*, 05/02/2024, https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025.

Morsa (Maxime), « La théorie du désengagement moral », *Cercle Psy*, nº 25, 06-08/2017, www.scienceshumaines.com/la-theorie-du-desengagement-moral_fr_38358.html.

Nocetti (Julien), « Géopolitique de la cyber-conflictualité », *Politique étrangère*, 2018/2, www.cairn.info/revue-politique-etrangere-2018-2-page-15.htm.

Poul (Maxime), « Doudou, azerty, marseille… voici les mots de passe les plus utilisés par les Français en 2023 », *Le Parisien*, 16/11/2023, www.leparisien.fr/high-tech/doudou-azerty-marseille-voici-les-mots-de-passes-les-plus-utilises-par-les-francais-en-2023-16-11-2023-DTDITADJARCDXBEBD4IH25SPJQ.php.

Quentin (Arthur), « Les services essentiels de santé devraient relever du bien commun », *Libération*, 31/07/2021, www.liberation.fr/economie/economie-numerique/les-services-essentiels-de-sante-devraient-relever-du-bien-commun-20210731_KCXM2THINNBTRFV5U64ST6C4RI.

Roberts (Sienna), « A Guide to ITIL Processes & Framework and ITIL v4 Management Practices », *The Knowledge Academy*, 25/11/2022, www.theknowledgeacademy.com/blog/essential-guide-to-itil-v4-processes-and-framework.

SentinelOne, « Détecter et bloquer les ransomwares grâce à l'intelligence artificielle », *Le Monde informatique*, www.lemondeinformatique.fr/publi_info/lire-detecter-et-bloquer-les-ransomwares-grace-a-l-intelligence-artificielleet-8239-621.html.

Sheldon (Robert), « WORM (write once, read many) », *Techtarget*, www.techtarget.com/searchstorage/definition/WORM-write-once-read-many.

Starikova (Anastasia), « Les stagiaires : une menace cachée en termes de cybersécurité », *Kaspersky Daily*, 30/06/2022, www.kaspersky.fr/blog/interns-as-a-cyberthreat/19065.

Volga (Laetitia), « Apple et Microsoft en tête des premières capitalisations boursières mondiales », *Les Échos*, 01/08/2023, https://investir.lesechos.fr/actu-des-valeurs/la-vie-des-actions/apple-et-microsoft-en-tete-des-premieres-capitalisations-boursieres-mondiales-1967283.

AUTRES PUBLICATIONS ET SOURCES

Académie de Strasbourg, « Identification et authentification », SSI, https://ssi.ac-strasbourg.fr/bonnes-pratiques/recommandations/lidentification-et-lauthentification.

AMRAE, *Maîtrise du risque numérique*, association pour le management des risques et des assurances de l'entreprise, AMRAE, 2019, www.amrae.fr/sites/default/files/public/2019-11/ANSSI_FR_WEB.pdf.

Association française des entreprises privées, Mouvement des entreprises de France*, Guide à usage des entreprises d'identification des données sensibles*, 12/2021, www.entreprises.gouv.fr/files/files/enjeux/securite-economique/loi-de-blocage/guide-identification-donnees-sensibles.pdf?v=1701872953 et www.legifrance.gouv.fr/loda/id/JORFTEXT000000501326.

Bourne (Vanson), *Gestion des risques liés aux données, L'état du marché : de la cybercriminalité à la conformité*, Rapport France 2023, 10/2023, Veritas.

Buckbee (Michael), « IDS et IPS : en quoi sont-ils différents ? », Varonis, www.varonis.com/fr/blog/ids-et-ips-en-quoi-sont-ils-differents.

Cardon (Rémi) et Meurant (Sébastien), *La problématique de la cybersécurité dans les entreprises*, 10/06/2021, www.senat.fr/travaux-parlementaires/office-et-delegations/delegation-aux-entreprises/archives-1/la-problematique-de-la-cybersecurite-dans-les-entreprises.html.

Centre canadien pour la cybersécurité, « Pratiques exemplaires de création de phrases de passe et de mots de passe », gouvernement du Canada, 02/2024, www.cyber.gc.ca/fr/orientation/pratiques-exemplaires-de-creation-de-phrases-de-passe-et-de-mots-de-passeitsap30032#:~:text=Une%20phrase%20de%20passe%20est,4%20mots%20et%2015%20caract%C3%A8res.

Collectif, *2024 Data and AI Leadership Executive Survey*, 01/2024, www.wavestone.com/app/uploads/2023/12/DataAI-ExecutiveLeadershipSurveyFinalAsset.pdf, 2024.

Collectif, « Assurance du risque cyber », ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique, 07/09/2022, www.tresor.economie.gouv.fr/Articles/00367730-14c0-4303-95af-eeb6442fb19b/files/108f9b50-5480-4810-ae7d-7f7845ba7805.

Collectif*, At the junction of corporate governance and cybersecurity*, Federation of Risk Management Association, www.eciia.eu/wp-content/uploads/2019/02/FERMA-Perspectives-Cyber-risk-governance-09.10.2018_0.pdf.

Collectif, *Baromètre annuel de la cybersécurité des entreprises*, CESIN, 2024, https://cesin.fr/articles-slug/?slug=2060-9%C3%A8me+%C3%A9dition+du+barom%C3%A8tre+annuel+du+CESIN.

Collectif, « Cybersécurité et intelligence artificielle », IBM, www.ibm.com/fr-fr/ai-cybersecurity?p1=Search&p4=43700068029086145&p5=e&gad_source=1&gclsrc=ds.

Collectif, *La Cybersécurité des entreprises – Prévenir et guérir : quels remèdes contre les cyber virus ?*, rapport d'information nº 678, 10/06/2021, www.senat.fr/rap/r20-678/r20-6783.html.

Collectif, « Directeur des systèmes d'information », *Les Fiches métier de l'observatoire*, OMECA, www.metierscomptabilite.fr/wp-content/uploads/2021/11/Fiche_SUPINF1_Directeur_SI.pdf.

Collectif, « Entreprises : quelles règles de cybersécurité appliquer ? », *Bercy Infos*, 06/12/2023, www.economie.gouv.fr/entreprises/createurs-dirigeants-regles-cybersecurite.

Collectif, *La Gestion du risque de sécurité numérique pour la prospérité économique et sociale*, OCDE, 2015, www.oecd.org/fr/publications/la-gestion-du-risque-de-securite-numerique-pour-la-prosperite-economique-et-sociale-9789264246089-fr.htm.

Collectif, International Consortium of Investigative Journalists, www.icij.org.

Collectif, « NEP-315. Connaissance de l'entité et de son environnement et évaluation du risque d'anomalies significatives dans les comptes », Sidoni, https://doc.cncc.fr/docs/nep-315-connaissance-de-lentite.

Collectif*, Profession Experts, le magazine des experts-comptables de Bretagne*, nº 143, 03-06/2024.

Collectif, « Qu'est-ce qu'un pare-feu et quel est son rôle ? », 2022, Axis Solutions, www.axis-solutions.fr/quest-ce-quun-pare-feu-et-quel-est-son-role.

Collectif, « Qu'est-ce qu'un pare-feu nouvelle génération (NGFW) ? », www.cloudflare.com/fr-fr/learning/security/what-is-next-generation-firewall-ngfw.

Collectif, « Le règlement général sur la protection des données (RGPD), mode d'emploi », *Bercy Infos*, 11/04/2023, www.economie.gouv.fr/entreprises/reglement-general-protection-donnees-rgpd.

Collectif, « Se connecter avec une clé d'accès au lieu d'un mot de passe », Google, 2024, https://support.google.com/accounts/answer/13548313?hl=fr.

Collectif*, SIC mag*, nº435.

Collectif, *Vocabulaire de la sécurité informatique*, 03/04/2023, https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/2074708/securite-logique.

Devergranne (Thiébaut), « IDS, IPS, DLP : il faut l'autorisation de la CNIL ! », www.donneespersonnelles.fr/ids-ips-dlp-il-faut-l-autorisation-de-la-cnil.

GIP ACYMA, Assistance et prévention du risque numérique, cybermalveillance.gouv.fr.

Goldstein (Guy-Philippe), *Cyber-risques : Enjeux, approches et gouvernance, Institut français de l'audit et du contrôle interne*, juin 2018, https://docs.ifaci.com/wp-content/uploads/2018/06/Cyber-risques.pdf.

Guide de la continuité d'activité, Secrétariat général de la défense et de la sécurité nationale, https://guide-continuite-activite.sgdsn.gouv.fr.

L'Info cyber-risques, www.linfocr.com.

ISO/CEI 27001, certification.afnor.org/numerique/certification-iso-27001.

ISO/CEI 27001, www.iso.org/fr/standard/27001.

ISO/CEI 27001, www.iso.org/obp/ui/fr/#iso:std:iso-iec:27001:ed-2:v1:fr.

ISO/CEI 27002, www.iso.org/fr/standard/75652.html.

Krebs (Brian), *Krebs On Security*, krebsonsecurity.com.

Matsugaya (Shingo), « LockBit, BlackCat, and Royal Dominate the Ransomware Scene », *Trend Micro*, 21/02/2023, www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-blackcat-and-royal-dominate-the-ransomware-scene-ransomware-in-q4-2022.

NoLimitSecu, www.nolimitsecu.fr.

Ordre des experts-comptables, *Annuaire des experts-comptables*, annuaire.experts-comptables.org.

Orange Pro, « Webinar : TPE-PME & Cyberattaques : les bons réflexes, les bonnes pratiques », 01/2024, www.youtube.com/watch?v=kvlXU6_2y08.

Parlement et conseil européens, Directive (UE) 2016/680 du parlement européen et du conseil, 27/04/2016, eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L0680&from=FR.

La Quadrature du Net, www.laquadrature.net/en/tools.

Schneier (Bruce), *Schneier on Security*, www.schneier.com.

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Anticiper et gérer sa communication de crise cyber, ANSSI, 09/12/2021, https://cyber.gouv.fr/publications/anticiper-et-gerer-sa-communication-de-crise-cyber.

Attaques par rançongiciels, tous concernés, ANSSI, 04/09/2020, https://cyber.gouv.fr/publications/attaques-par-rancongiciels-tous-concernes.

Bonnes pratiques à l'usage des professionnels en déplacement, ANSSI, 17/05/2019, https://cyber.gouv.fr/publications/bonnes-pratiques-lusage-des-professionnels-en-deplacement.

La Cybersécurité pour les TPE/PME en treize questions, ANSSI, 10/2022, https://cyber.gouv.fr/publications/la-cybersecurite-pour-les-tpepme-en-treize-questions.

Guide d'élaboration d'une charte d'utilisation des moyens informatiques et des outils numériques, ANSSI, 19/06/2017, www.cyber.gouv.fr/publications/guide-delaboration-dune-charte-dutilisation-des-moyens-informatiques-et-des-outils.

Guide d'hygiène informatique, ANSSI, 23/01/2017, www.cyber.gouv.fr/publications/guide-dhygiene-informatique.

Guide des bonnes pratiques de l'informatique, ANSSI, 19/01/2017, https://cyber.gouv.fr/publications/guide-des-bonnes-pratiques-de-linformatique.

Guide d'hygiène informatique, ANSSI, 23/01/2017, https://cyber.gouv.fr/publications/guide-dhygiene-informatique

Guides techniques aux recueils de bonnes pratiques, ANSSI, 17/11/2023, www.ssi.gouv.fr/bonnes-pratiques.

Maîtrise du risque numérique - l'atout confiance, ANSSI, 18/11/2019, https://cyber.gouv.fr/publications/maitrise-du-risque-numerique-latout-confiance.

Les Mesures cyber préventives prioritaires, ANSSI, 17/05/2023, https://cyber.gouv.fr/publications/les-mesures-cyber-preventives-prioritaires.

Le modèle Zero Trust, ANSSI, 15/04/2021, https://cyber.gouv.fr/publications/le-modele-zero-trust.

Mooc sur la protection des données, ANSSI, https://secnumacademie.gouv.fr.

Panorama de la cybermenace 2023, ANSSI, www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-001.pdf.

Recommandations pour choisir des pare-feu maîtrisés dans les zones exposées à Internet, ANSSI, 26/01/2018, https://cyber.gouv.fr/publications/recommandations-pour-choisir-des-pare-feux-maitrises-dans-les-zones-exposees-internet.

Recommandations relatives à l'authentification multifacteur et aux mots de passe, ANSSI, 08/10/2021, https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe.

Sauvegarde des systèmes d'information, ANSSI, 25/10/2023, https://cyber.gouv.fr/publications/fondamentaux-sauvegarde-systemes-dinformation.

Sauvegarde des systèmes d'information, ANSSI, 30/01/2023, https://cyber.gouv.fr/publications/sauvegarde-des-systemes-dinformation.

Sécuriser les accès Wi-Fi, ANSSI, 03/04/2013, https://cyber.gouv.fr/publications/securiser-les-acces-wi-fi.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

5 arguments pour adopter le gestionnaire de mots de passe, Cnil, 03/10/2018, www.cnil.fr/fr/5-arguments-pour-adopter-le-gestionnaire-de-mots-de-passe.

Le contrôle d'accès biométrique sur les lieux de travail, Cnil, 28/03/2019, www.cnil.fr/fr/le-controle-dacces-biometrique-sur-les-lieux-de-travail.

De azerty à pa $$ word, une revue des pratiques de gestion des mots de passe, LINC, https://linc.cnil.fr/de-azerty-paword-une-revue-des-pratiques-de-gestion-des-mots-de-passe.

Guide de la sécurité des données personnelles, Cnil, www.cnil.fr/fr/guide-de-la-securite-des-donnees-personnelles.

Le règlement général sur la protection des données, Cnil, 24/06/2016, www.cnil.fr/fr/reglement-europeen-protection-donnees.

Sécurité : Analyse des risques, Cnil, 14/03/2024, www.cnil.fr/fr/securite-analyse-de-risques.

Sécurité : Authentifier les utilisateurs, CNIL, 14/03/2024, www.cnil.fr/fr/securite-authentifier-les-utilisateurs.

Sécurité : Chiffrement, hachage, signature, Cnil, 14/03/2024, www.cnil.fr/fr/securite-chiffrement-hachage-signature.

Sécurité : Gérer les habilitations, Cnil, 13/03/2024, www.cnil.fr/fr/securite-gerer-les-habilitations.

Travail et données personnelles, Cnil, www.cnil.fr/fr/thematiques/travail-et-donnees-personnelles.

Vérifier sa politique de mots de passe, Cnil, 17/10/2022, www.cnil.fr/fr/verifier-sa-politique-de-mots-de-passe.

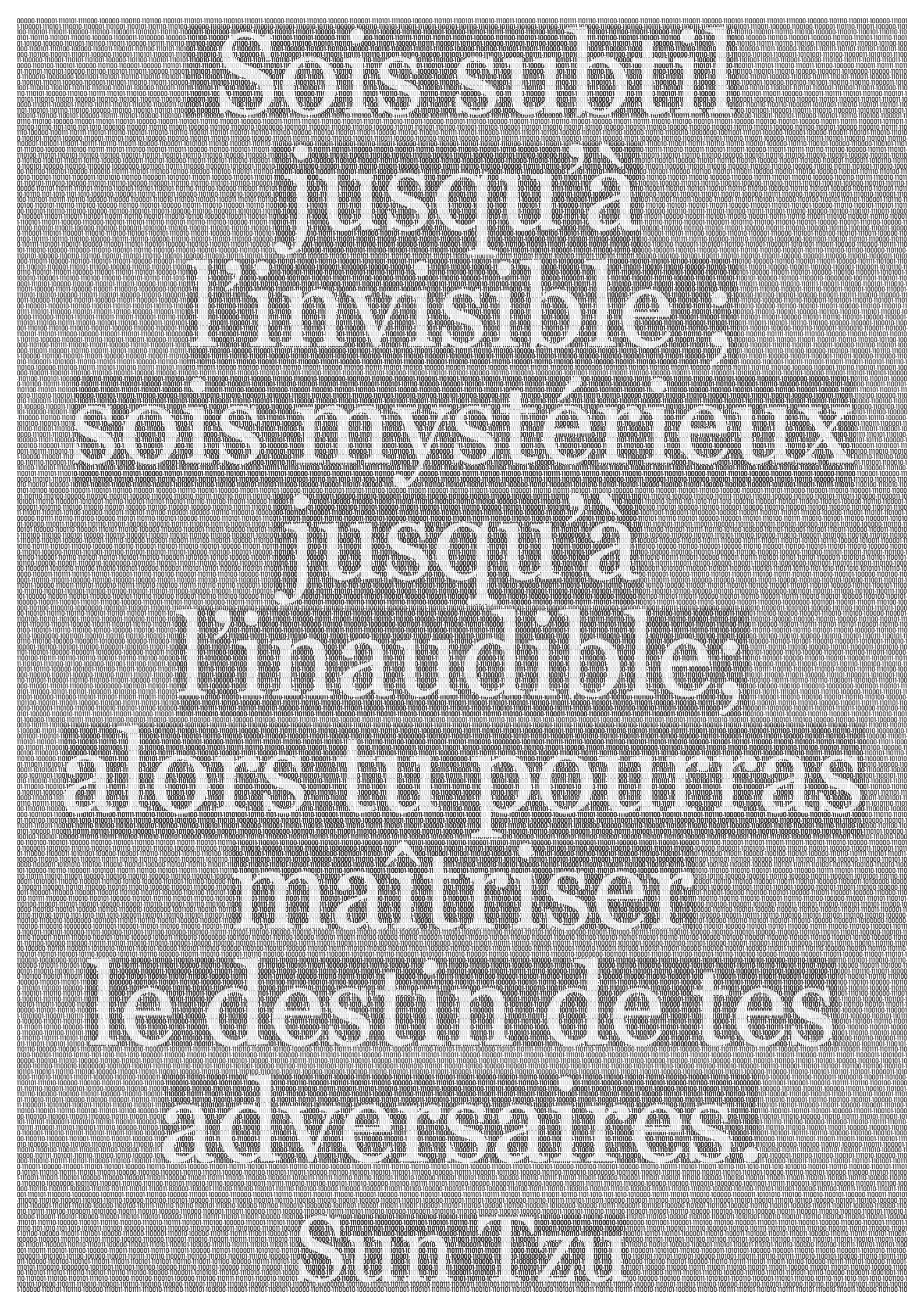
LÉGIFRANCE

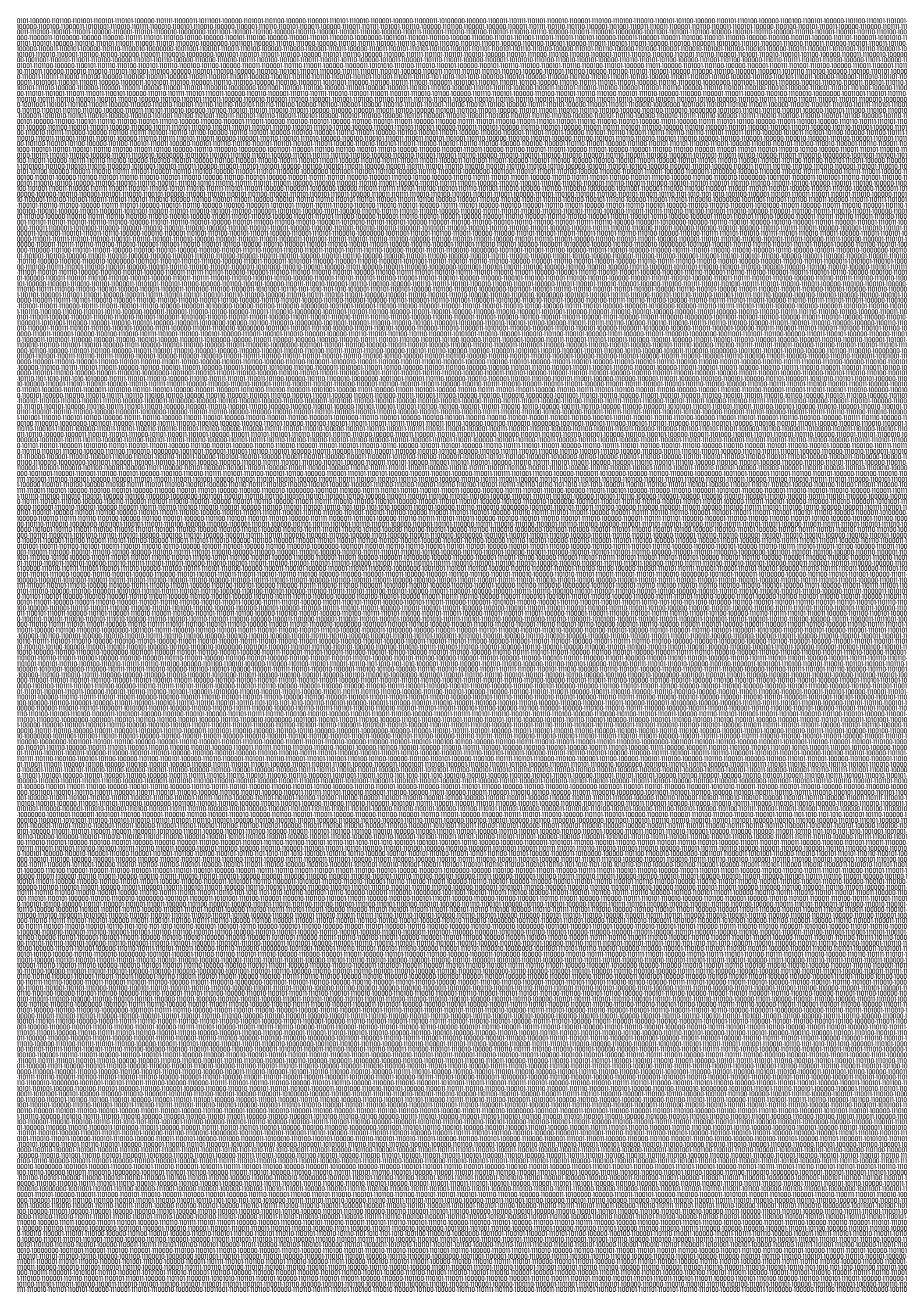
Ordonnance n° 45-2138 du 19 septembre 1945, www.legifrance.gouv.fr/loda/id/JORFTEXT000000698851.

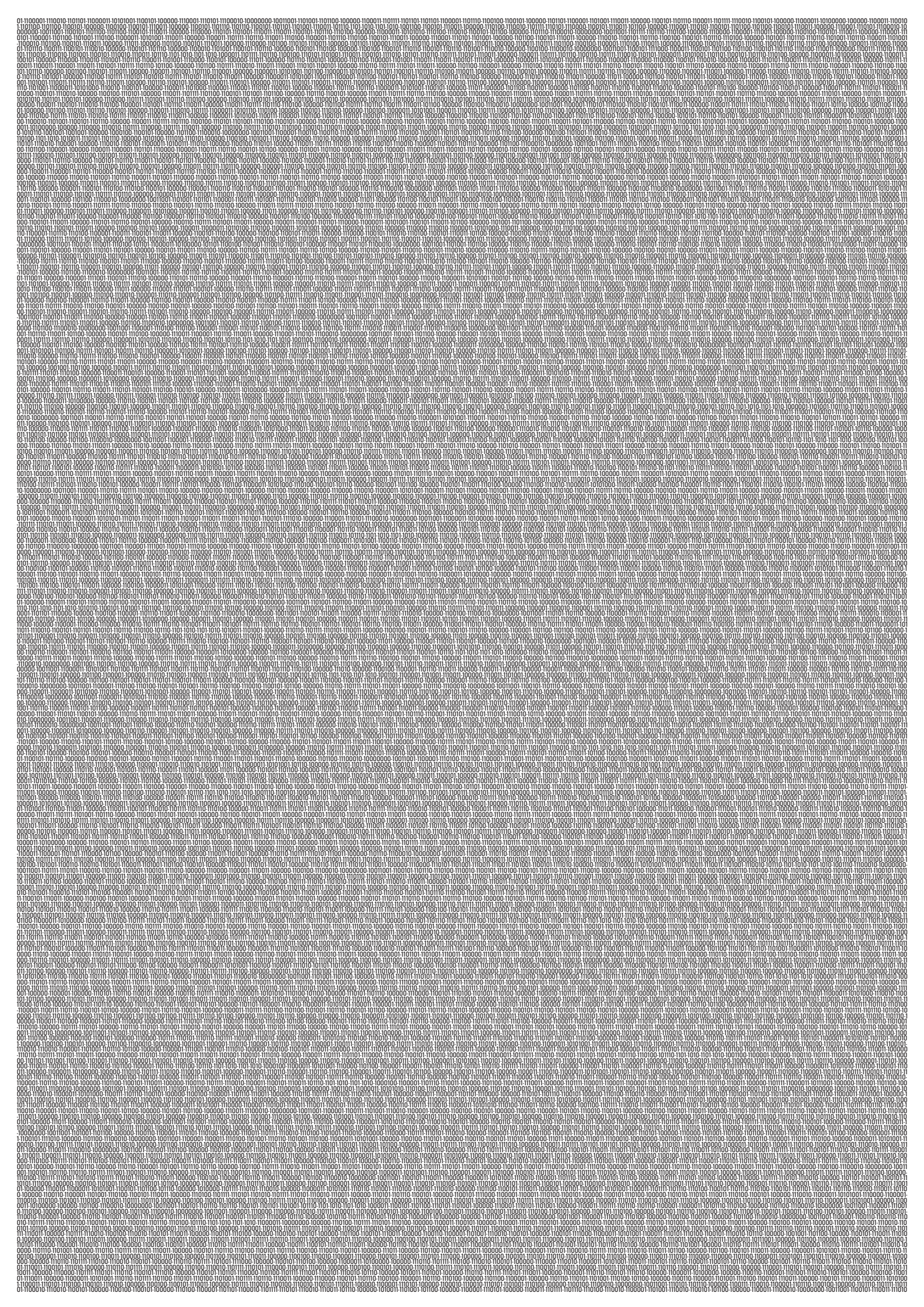
Loi n° 88-19 du 5 janvier 1988, www.legifrance.gouv.fr/jorf/id/JORFTEXT000000875419.

Code civil, www.legifrance.gouv.fr/codes/article_lc/LEGIARTI0000064192.

TABLE
DES MATIÈRES







Dans un monde de plus en plus numérisé où l'information a toujours plus de valeur, la sécurisation des données en entreprise est chaque jour plus nécessaire, singulièrement dans les cabinets d'expertise comptable, qui brassent nombre d'informations confidentielles et stratégiques.

Le présent mémoire cherche à cerner les enjeux de la protection des données, et les moyens dont disposent ou dont peuvent se doter les acteurs économiques pour minimiser les risques de fuite, perte ou destruction de données.

In a world going more and more digital, data has an increasing and crucial value. Especially in the accounting firms, where people deal with sensitive, confidential and high value information on a daily basis.

The present study means to determine the stakes of the data securitization, and to browse through the tools that companies can implement to minimize their risk of data loss, leak, or destruction.

ILLUSTRATION DE COUVERTURES ET GARDES :
Première moitié du texte intégral de *L'Art de la guerre*, de Sun Tzu, traduction en langage binaire par Gemini.

Université Bretagne Sud
ubs : IAE : BRETAGNE SUD
École Universitaire de Management