Baromètre fuite des données

2023

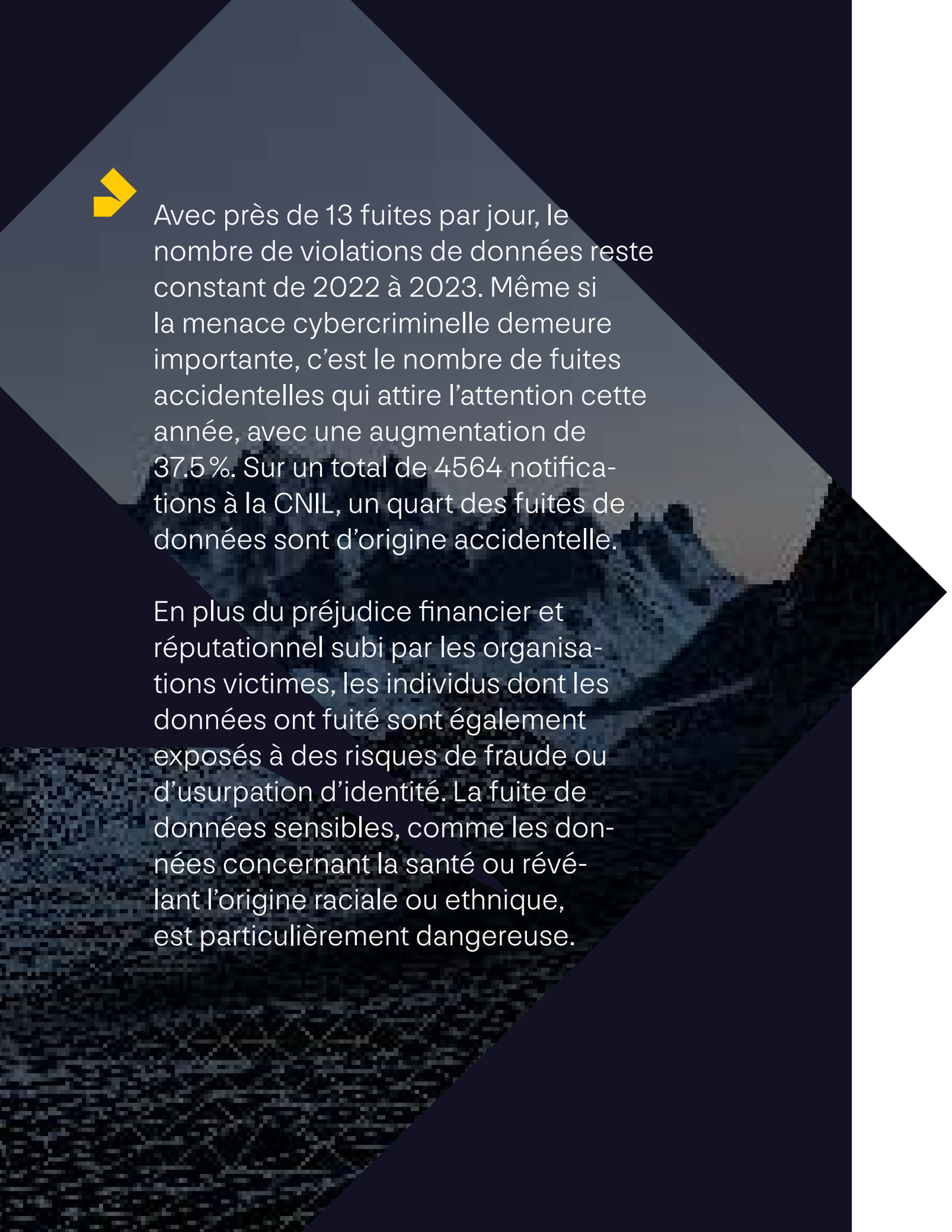
Ce baromètre est animé par INCYBER NEWS en partenariat avec Forward Global et Lexfo, avec la participation de la CNIL.

INCYBER NEWS
LE MÉDIA DE LA CONFIANCE NUMÉRIQUE

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Forward

Lexfo



Avec près de 13 fuites par jour, le nombre de violations de données reste constant de 2022 à 2023. Même si la menace cybercriminelle demeure importante, c'est le nombre de fuites accidentelles qui attire l'attention cette année, avec une augmentation de 37.5 %. Sur un total de 4564 notifications à la CNIL, un quart des fuites de données sont d'origine accidentelle.

En plus du préjudice financier et réputationnel subi par les organisations victimes, les individus dont les données ont fuité sont également exposés à des risques de fraude ou d'usurpation d'identité. La fuite de données sensibles, comme les données concernant la santé ou révélant l'origine raciale ou ethnique, est particulièrement dangereuse.

AUGMENTATION DES FUITES ACCIDENTELLES

Malgré la légère diminution (-3,5 %) du nombre total de notifications de fuites de données en 2023 (4 564 notifications) comparativement à l'année précédente (4 731 notifications), celui-ci reste élevé avec près de **13 fuites par jour.**

Alors que les fuites malveillantes sont légèrement en baisse (-3,3 % comparativement à 2022), les **fuites accidentelles** ont pour leur part **largement augmenté** (+37,5 %).

Ces fuites accidentelles proviennent plus souvent **de l'intérieur** (704 notifications, ou **60.7 %** du total des fuites accidentelles) que **de l'extérieur** (137 notifications, ou 11,8 % du total des fuites accidentelles) des organisations.

Les causes des fuites accidentelles d'origine interne sont multiples. Parmi celles notifiées à la CNIL en 2023, près de 40 % ont été causés par l'envoi de données personnelles à un mauvais destinataire, tandis que près de 30 % résultent de la publication involontaire d'informations. Les fuites accidentelles d'origine interne sont donc principalement le résultat d'une erreur humaine, de la perte d'un équipement ou de la mauvaise configuration d'une infrastructure informatique.

Parmi les contenus des fuites accidentelles d'origine interne, près de 20 % contenaient des données sensibles.

Parmi les contenus des fuites accidentelles d'origine interne, **près de 20 % contenaient des données sensibles.** La CNIL définit ce type particulier de données comme « [révélant] la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ». L'exposition de données sensibles est particulièrement dangereuse pour les individus touchés. La CNIL rappelle d'ailleurs qu'en cas de fuite de données « susceptible d'engendrer un risque élevé pour les droits et les libertés », l'organisme responsable a « l'obligation d'informer individuellement les personnes concernées du fait que leurs données ont été compromises et publiées en ligne. »

Les conséquences peuvent également être lourdes pour les organisations : atteinte à la réputation, perte de confiance des clients, impact financier lié à l'indemnisation des clients touchés, frais juridiques, éventuelles amendes… Rappelons que les organisations qui enfreignent le RGPD peuvent se voir infliger une amende allant jusqu'à 4 % de leur chiffre d'affaires annuel mondial ou 20 millions d'euros, le montant le plus élevé étant retenu.

L'effet papillon des fuites de données

par Alexis Pinon

Directeur des enquêtes numériques
Forward Global

L'Hexagone a été le pays d'Europe le plus lourdement touché en 2023 par les fuites de données. Un triste constat qui s'accompagne de lourdes conséquences, et pas uniquement pour les entités ciblées en première instance.

On imagine fort bien les répercussions pour les acteurs ayant fait l'objet d'une cyberattaque (remise en place de l'infrastructure en urgence, perturbation de l'activité, etc.), tout comme pour les individus dont les données (état civil, adresse postale, date de naissance, etc.) ont été dérobées. Ces derniers peuvent en effet être en proie à des tentatives d'usurpation d'identité, d'extorsion de fonds, etc… En revanche, d'autres acteurs, en apparence non concernés par l'attaque, peuvent en faire les frais, parfois des mois après.

Il n'est en effet pas rare que, parmi les données dérobées lors de cyberattaques, se trouvent des adresses mail professionnelles, ainsi qu'un ou plusieurs mots de passe associés. Or, du fait de la propension des individus à réutiliser les mêmes mots de passe, à quelques légères variations près, de telles informations peuvent permettre à des acteurs malveillants de prendre la main sur certains comptes et profils liés à la sphère professionnelle de leurs victimes. Et donc de pénétrer de manière illicite dans le système d'information de l'employeur de ces dernières.

C'est ce que l'on pourrait appeler un effet papillon, ou comment le piratage d'un acteur peut entraîner la compromission d'un autre, alors qu'ils n'ont en apparence rien en commun.

Cette réalité implique pour les entreprises, peu importe leur taille et leur secteur d'activité, d'avoir un dispositif leur permettant de détecter au plus tôt la survenance de fuites de données, et ce bien au-delà de celles pouvant les impliquer directement. La présence de l'adresse mail professionnelle de l'un de leurs collaborateurs dans une fuite de données impliquant une marketplace, un intermédiaire de paiement ou encore un comparateur de billets d'avion doit leur être notifiée, afin que des mesures préventives soient prises dans les plus brefs délais.

Plus encore, il est indispensable de regarder au-delà des fuites de données dites "classiques". Les acteurs malveillants innovent en permanence. Depuis plusieurs mois, ce sont par exemple les « *infostealers* » qui ont le vent en poupe. Encore méconnus du grand public, une fois installés sur l'ordinateur de leur victime, ces *malwares* tristement efficaces permettent de récupérer de nombreuses informations (mots de passe, *cookies*, *usernames*, etc.), qui vont ensuite être vendues sur des *marketplaces* du *deep* et *dark* Web. Et les acheteurs de s'en servir pour usurper l'identité numérique de leurs victimes, afin d'accéder aux plateformes utilisées à des fins personnelles comme professionnelles par celles-ci.

Chaque jour, des dizaines de gigaoctets de données piratées par *infostealers* sont mises en vente. Ajoutées à celles issues de bases de données compromises, ce sont les données de milliers de victimes qui se retrouvent ainsi entre les mains d'acteurs malveillants. Monitorer la survenance de fuites de données revêt dès lors une importance vitale pour les entreprises.

LA MENACE CYBERCRIMINELLE

Malgré l'augmentation des fuites accidentelles, la cybercriminalité demeure la menace la plus importante. Sur les 4 564 notifications enregistrées par la CNIL en 2023, **plus de la moitié (59 %) sont dûes à des actes malveillants externes (2 671 notifications).** Ce chiffre est toutefois en baisse de 11 % comparativement à l'année précédente, avec 3011 notifications.

Parmi les méthodes les plus souvent employées par les acteurs malveillants pour exfiltrer les données d'une organisation, on retrouve l'hameçonnage (*phishing*), l'exploitation de vulnérabilités informatiques ou encore, les attaques par force brute, destinées à déchiffrer les mots de passe en testant très rapidement une myriade de possibilités.

Dans 85 % des cas de violations d'origine externe malveillante, la **confidentialité** des données est affectée, tandis que dans près de 13 % de ces violations, des données ont été rendues **inaccessibles**. Les trois quart des fuites recensées dans le cadre des violations de données d'origine externe malveillante contenaient des **données liées à l'état civil,** comme le nom, le sexe, la date de naissance ou encore l'âge des personnes touchées.

Bien que la menace cybercriminelle externe demeure la cause la plus fréquente, **le risque d'exfiltration de données par des acteurs internes** ne doit pas non plus être négligé puisqu'il représente **20 % de toutes les fuites d'origine interne,** en augmentation de 16 % par rapport à l'année précédente. Parmi les motivations des acteurs internes : la détresse financière, la vengeance, ou encore l'influence d'un agent externe, comme une organisation criminelle ou une agence de renseignement.

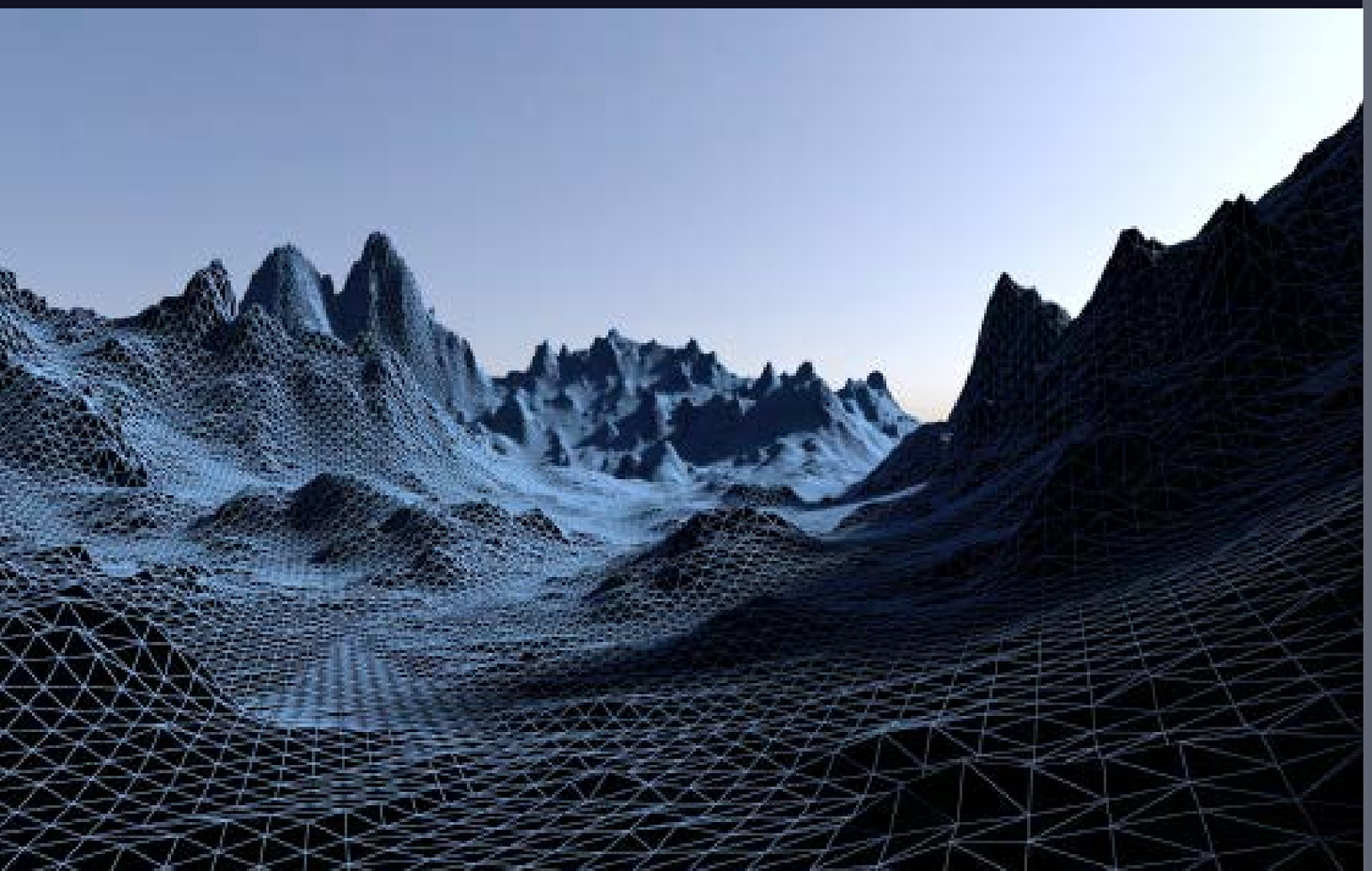
LES SECTEURS LES PLUS TOUCHÉS

Le secteur d'activité le plus touché par les violations de données demeure celui de l'**administration publique** avec 823 notifications, ce qui représente 18 % du total des violations de données enregistrées par la CNIL en 2023. **Plus de la moitié (52 %)** des violations de données du secteur de l'administration publique ont résulté d'un **acte externe malveillant**, ce qui témoigne de l'intérêt des cybercriminels pour les données du secteur public.

Les deux autres secteurs les plus touchés en 2023 arrivent presque ex-aequo : alors que celui des activités financières et des assurances a été victime de 544 fuites de données (11,9 % du total), le secteur de la santé et de l'action sociale comptabilise 540 fuites de données (11.8 % du total). Le secteur des activités spécialisées, scientifiques et techniques a également connu son lot de violations en 2023, avec un total de 536 notifications, dont **72 % étaient d'origine malveillante.**

Parmi les secteurs les moins touchés en 2023, on retrouve l'agriculture, la sylviculture et la pêche (3 violations de données), les activités extra-territoriales[1] (3 violations) et finalement, les industries extractives (une seule violation de données).

1 Ambassades, consulats, organisations internationales.



Comment réagir face à une fuite de données ?

par Valentin Baumont
Responsable du pôle CTI
Dataleak / Lexfo

Lors de la détection d'une fuite de données, la première réaction est d'abord la surprise, voire la stupeur. Il faut toutefois garder la tête froide pour déployer un plan d'action. Si ce dernier est déjà documenté, cela permettra d'être plus lucide dans la gestion de l'évènement. Dans tous les cas, il convient de prendre le contrôle de la situation pour sortir de la crise en minimisant les impacts légaux et/ou réputationnels.

La première étape consiste à évaluer l'étendue et la nature de la fuite pour pouvoir déterminer quelles sont les données compromises et le nombre de personnes potentiellement concernées.

Parmi les questions à se poser :

— Quelle semble être l'origine de la fuite (partenaire, site compromis, etc...) ?

— En cas de fuite revendiquée par un acteur malveillant, quelle est sa « réputation » et donc sa crédibilité ?

— Quelle est la « fraîcheur » de l'information ? Une fuite de données récentes aura en effet plus de conséquences que si les données dérobées ont déjà plusieurs années

Ces questions posées permettront également d'évaluer les risques et leur portée : le risque est-il lié à des usurpations d'identités ? Est-il financier, légal, réputationnel ? S'agit-il d'une exposition de données financières, personnelles, techniques ? Cette première appréciation permettra, en premier lieu, de mettre en place les actions d'isolation et de mise en quarantaine des éléments compromis (coupure de serveurs, désactivation de comptes, etc.) puis par la suite de mettre en œuvre les différentes notifications qui s'imposent :

— De prime abord, aux autorités compétentes afin de se conformer à la législation en vigueur dans le pays, a fortiori si des données personnelles sont impliquées

— Ensuite, en fonction de la sensibilité des données, aux parties concernées, qu'il s'agisse de collaborateurs ou de clients, auprès desquels il faut communiquer de manière claire, transparente et indiquer des actions possibles à mener de leur côté pour se prémunir de toute exploitation malveillante des données

Une communication continue, ouverte et transparente doit suivre ces notifications. Cela contribuera à minimiser les répercussions négatives tout en préservant, autant que faire se peut, la confiance.

Une fois ces actions mises en œuvre, il est essentiel d'identifier les causes de la fuite de données pour éviter une répétition de l'incident. Des missions de type « *forensic* » ou de levée de doute sur les sources probables de la fuite peuvent permettre d'en comprendre l'origine.

Cette épreuve doit enfin alimenter un retour d'expérience qu'il convient d'utiliser à bon escient pour renforcer les procédures et politiques de sécurité, améliorer les processus de gestion de crise et développer une posture de cybersécurité proactive : surveillance de la surface d'exposition, réalisation de tests d'intrusions réguliers, surveillance continue des actifs critiques - par exemple avec des solutions comme Ambionics (https://www.ambionics.io/fr/)-, veille sur les menaces.

Les fuites de données font partie de notre quotidien. À nous d'adapter nos organisations !

Fuite de données, comment éviter la perte de confiance

par Charles-Etienne Lebatard
Associé
Forward Global

La valorisation de la donnée en fait un actif précieux pour les entreprises mais également un objet de convoitise pour les pirates informatiques. Face à cette menace, protéger ses données s'affirme aujourd'hui comme une préoccupation opérationnelle et stratégique pour toute organisation. Au-delà de la simple sauvegarde des informations sensibles, la gestion du risque cyber ne peut se limiter à une réponse technologique car la fuite de données peut provoquer une perte de confiance – et donc une grave atteinte au capital réputationnel de l'organisation.

Une des spécificités de la crise cyber est que la révolution numérique rend le risque de moins en moins aléatoire. Chaque organisation peut y être confrontée. Au cours des deux dernières années, environ 2,6 milliards de données personnelles ont ainsi été exposées à des fuites. L'anticipation et la préparation ne sont plus des *nice to have* pour les *geeks* de la DSI mais un *must have* qui implique l'ensemble de l'organisation. Autre spécificité de la fuite de données : le RGPD impose de notifier la CNIL et, dans certains cas, les clients. Il n'est donc pas possible de « garder » l'information. Et ce d'autant moins que les pirates informatiques ont largement intégré l'aspect communicationnel dans leur stratégie d'extorsion. Être en mesure de communiquer rapidement peut ainsi être un élément clé de la réponse à la crise en privant les pirates de cette possibilité de chantage. Être en mesure de communiquer rapidement, c'est pouvoir reprendre l'initiative et montrer à l'interne, aux clients, aux autorités et à l'ensemble des parties prenantes qu'on a conscience de la crise et qu'on a enclenché des mesures pour pouvoir y répondre.

L'anticipation et la préparation sont essentielles lors de crises cyber, car elles impliquent souvent des concepts techniques difficiles à comprendre pour les non-spécialistes. La capacité à expliquer clairement ces concepts est cruciale pour maintenir le contrôle de la communication et éviter que des « experts » échafaudent des hypothèses plus ou moins pertinentes.

Cette communication aura d'autant plus d'impact et d'autorité qu'elle sera incarnée par un porte-parole qui pourra, si nécessaire, gérer la dimension émotionnelle qui peut toujours survenir dans une crise. Cette incarnation est d'autant plus importante qu'elle est la preuve de la sincérité de l'organisation. Ou, à l'inverse, de son manque de transparence. Cette capacité d'une entreprise à offrir un « visage » pendant la crise est un élément indispensable pour pouvoir re(créer) la confiance - une confiance qui doit s'appuyer sur une communication régulière et proactive. Toute information ne doit pas être nécessairement communiquée mais celle qui est diffusée doit être authentique, vérifiable et vérifiée. Rien n'est pire que de revenir sur ses propres déclarations pour « rectifier le tir », par exemple sur le nombre de victimes potentielles. Cette communication doit être accessible. Il faut rester simple dans ses explications en s'appuyant sur des exemples et des cas concrets. Le jargonnage technique doit être réservé aux cibles techniques.

Enfin, il ne faut jamais négliger la sortie de crise. Le soulagement d'avoir résolu techniquement la crise ne doit pas faire croire que la crise est finie. Il faut pouvoir rassurer, montrer qu'on a pris non seulement des mesures pour réparer les dommages, indemniser le cas échéant les victimes, mais surtout qu'on a concrètement pris des mesures pour que cela ne se produise plus.

Regagner la confiance est souvent un travail de plus longue haleine que de restaurer les données.

Chiffres-clés

4564
notifications

1158
de naturelle accidentelle soit 25%
20% de ces fuites contiennent

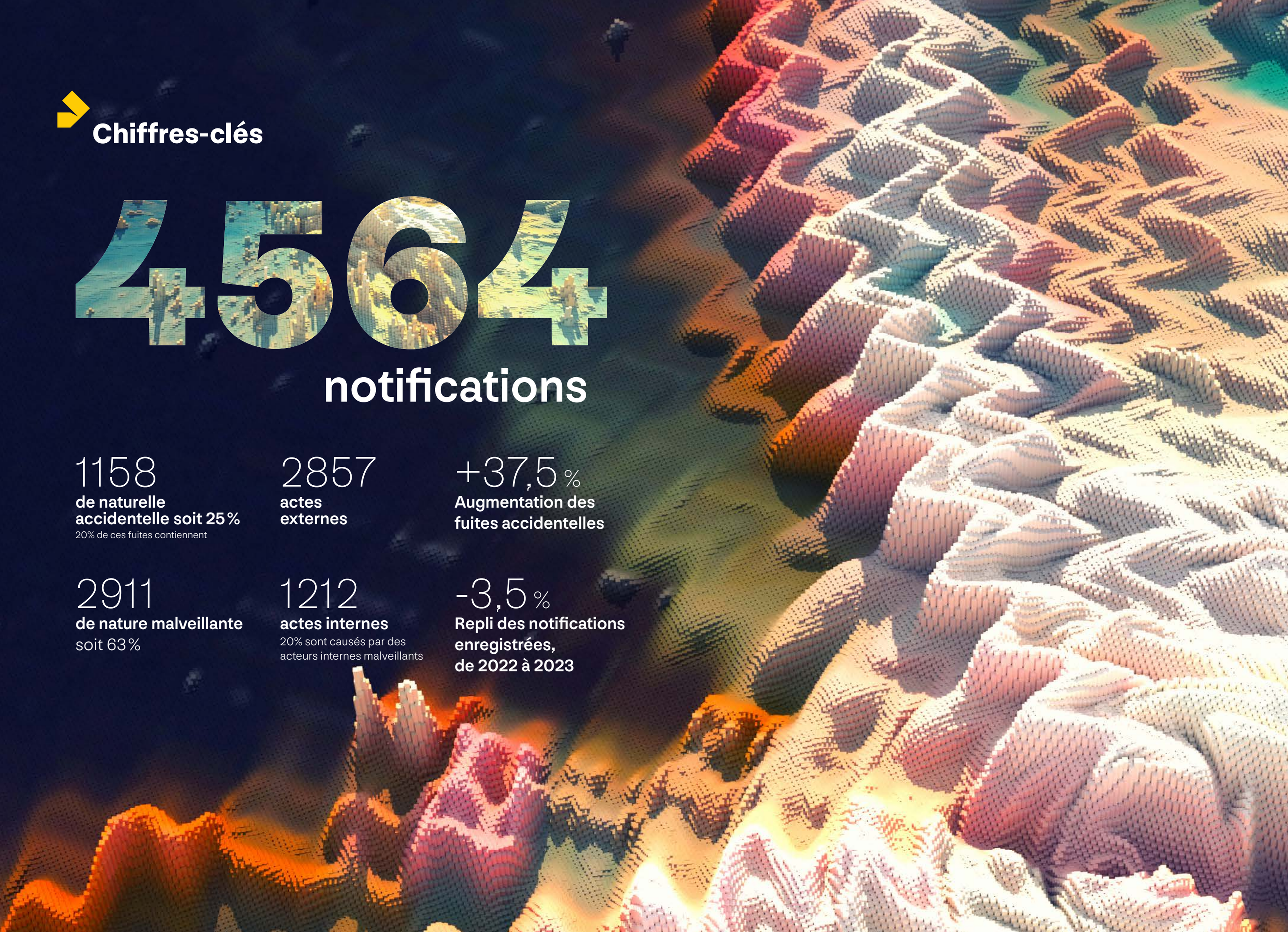
2857
actes externes

+37,5%
Augmentation des fuites accidentelles

2911
de nature malveillante
soit 63%

1212
actes internes
20% sont causés par des acteurs internes malveillants

-3,5%
Repli des notifications enregistrées, de 2022 à 2023



Chiffres-clés

Fuites internes accidentelles

40 %
dues à l'envoi de données personnelles à un mauvais destinataire

30 %
résultent de la publication involontaire de données

Secteur le plus touché

Total des violations

18 %*
Administration publique
*52 % résultent d'actes externes malveillants

11,9 %
Activités financières

11,8 %
Santé humaine et de l'action sociale

Définitions

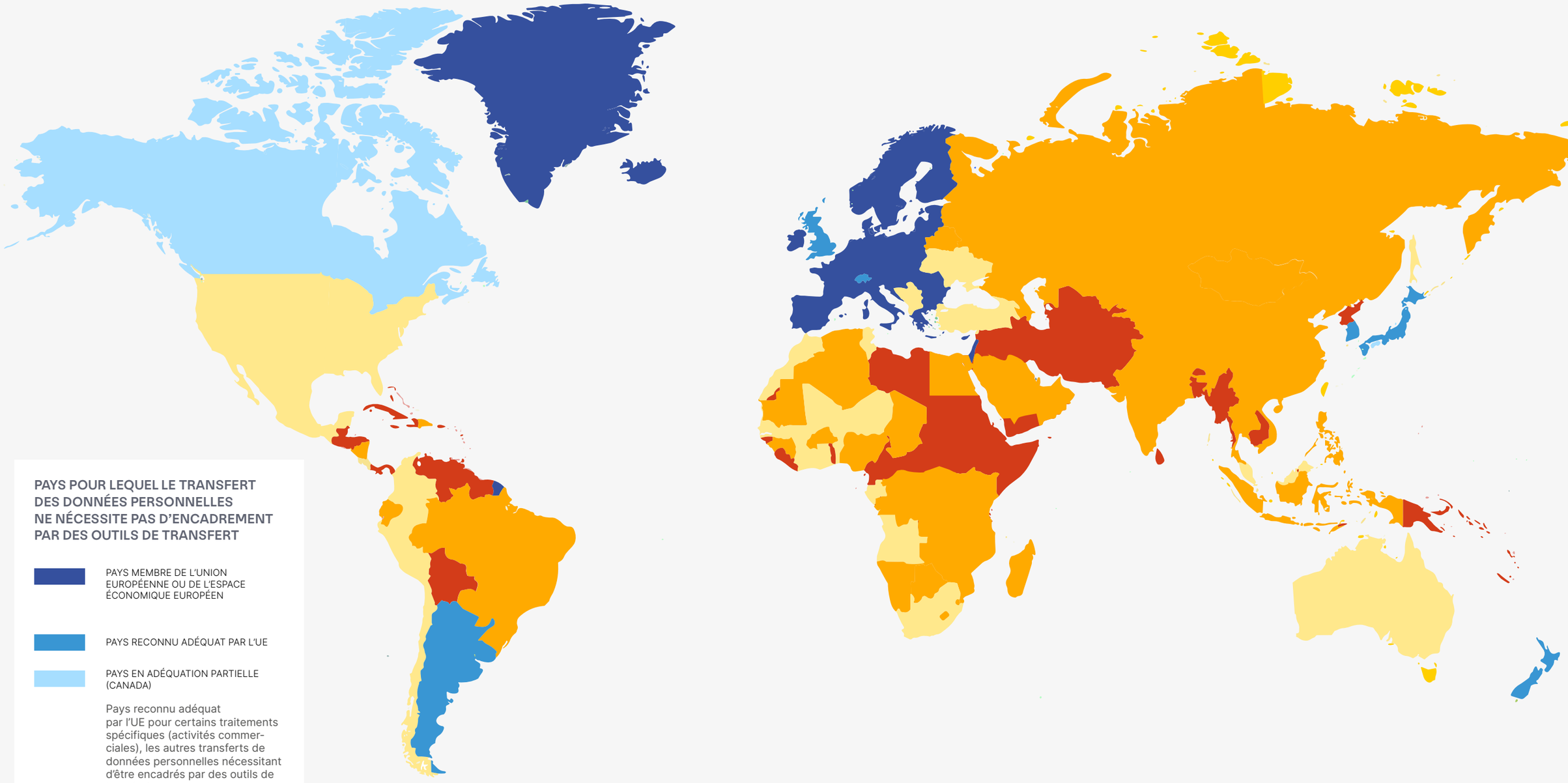
Acte externe accidentel : Situation où des données sont compromises en raison d'un événement non intentionnel qui provient de l'extérieur de l'entreprise (partenaire, sous-traitant, client…). Cela peut inclure des erreurs de paramétrage qui entraînent une exposition non intentionnelle des données sur Internet.

Acte externe malveillant : Situation où des données sont compromises en raison d'une action intentionnelle et malveillante provenant d'une source externe. Cela peut inclure des cyberattaques comme le piratage, l'utilisation de logiciels malveillants ou l'hameçonnage. Ces actions sont généralement menées par un tiers malveillant dans le but de voler, corrompre, ou exposer des données personnelles.

Acte interne accidentel : Situation où des données sont compromises en raison d'une erreur ou d'un incident non intentionnel qui se produit à l'intérieur de l'organisation. Cela peut inclure des erreurs humaines, comme l'envoi accidentel d'informations sensibles à une personne non autorisée, ou le non-respect des bonnes pratiques en matière de destruction de supports papiers ou numériques.

Acte interne malveillant : Situation où des données sont compromises en raison d'une action intentionnelle et malveillante provenant d'une source interne. Cela peut inclure des actions menées par un employé ou un sous-traitant de l'organisation dans le but de voler, corrompre, ou exposer des données personnelles.

Législations des États en matière de protection des données personnelles



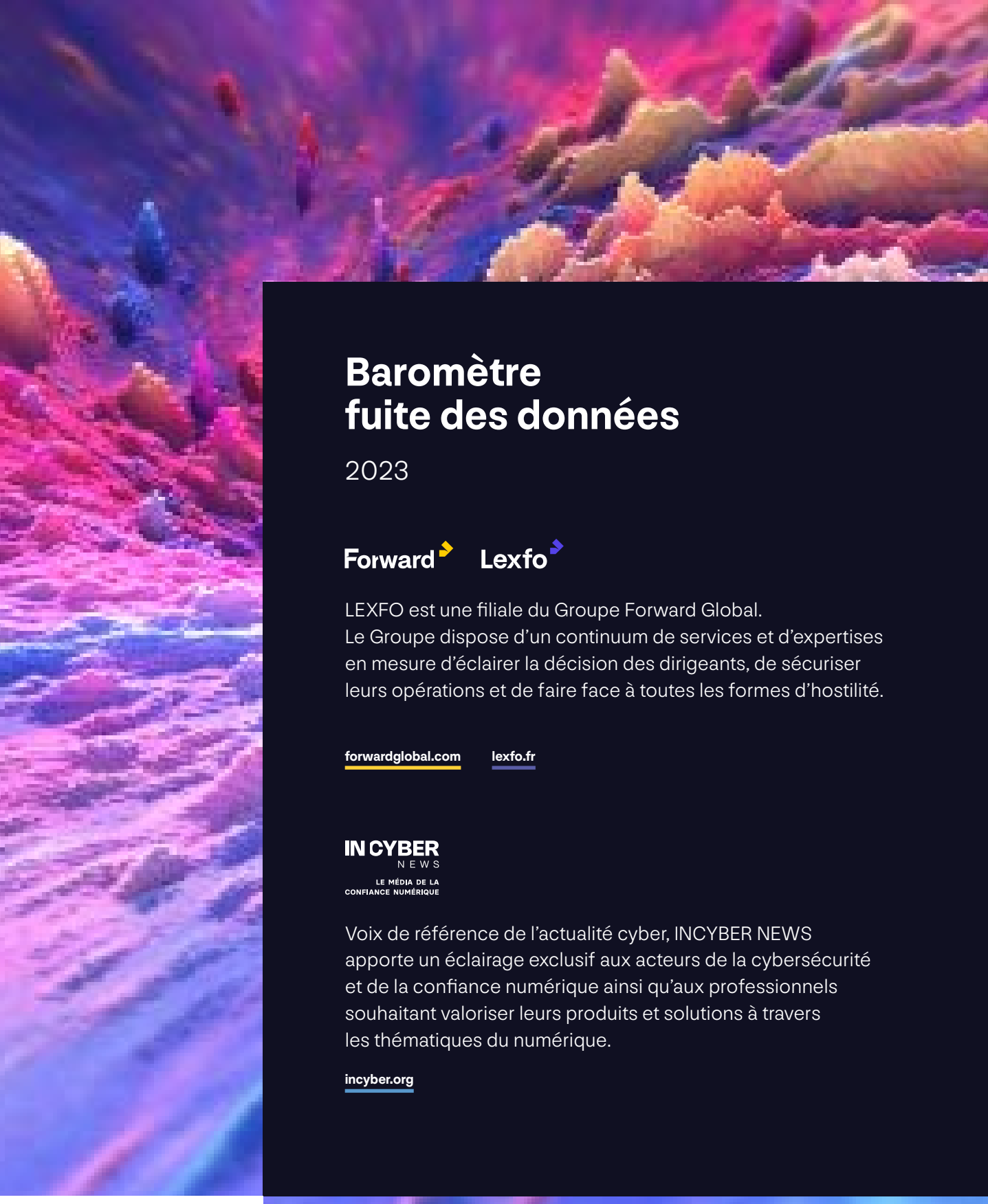
PAYS POUR LEQUEL LE TRANSFERT DES DONNÉES PERSONNELLES NE NÉCESSITE PAS D'ENCADREMENT PAR DES OUTILS DE TRANSFERT

- PAYS MEMBRE DE L'UNION EUROPÉENNE OU DE L'ESPACE ÉCONOMIQUE EUROPÉEN
- PAYS RECONNU ADÉQUAT PAR L'UE
- PAYS EN ADÉQUATION PARTIELLE (CANADA)

  Pays reconnu adéquat par l'UE pour certains traitements spécifiques (activités commerciales), les autres transferts de données personnelles nécessitant d'être encadrés par des outils de transfert

PAYS NON RECONNU COMME ADÉQUAT PAR L'UE ET DONT LE TRANSFERT DES DONNÉES PERSONNELLES NÉCESSITE D'ÊTRE ENCADRÉ PAR DES OUTILS DE TRANSFERT

- PAS DE LOI
- AVEC LÉGISLATION
- AUTORITÉ INDÉPENDANTE ET LOI



Baromètre fuite des données

2023

Forward Lexfo

LEXFO est une filiale du Groupe Forward Global.
Le Groupe dispose d'un continuum de services et d'expertises en mesure d'éclairer la décision des dirigeants, de sécuriser leurs opérations et de faire face à toutes les formes d'hostilité.

forwardglobal.com lexfo.fr

IN CYBER NEWS
LE MÉDIA DE LA CONFIANCE NUMÉRIQUE

Voix de référence de l'actualité cyber, INCYBER NEWS apporte un éclairage exclusif aux acteurs de la cybersécurité et de la confiance numérique ainsi qu'aux professionnels souhaitant valoriser leurs produits et solutions à travers les thématiques du numérique.

incyber.org