Baromètre DataBreach

PUBLICATION #1
Janvier 2020

UNE PUBLICATION

FIC 2020

EN PARTENARIAT AVEC

BESSÉ
CONSEIL EN ASSURANCES

pwc

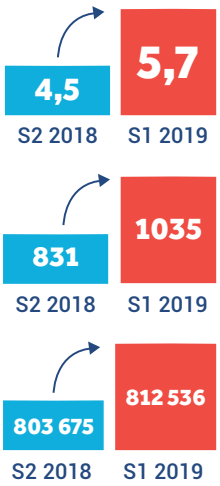
Baromètre
Data Breach

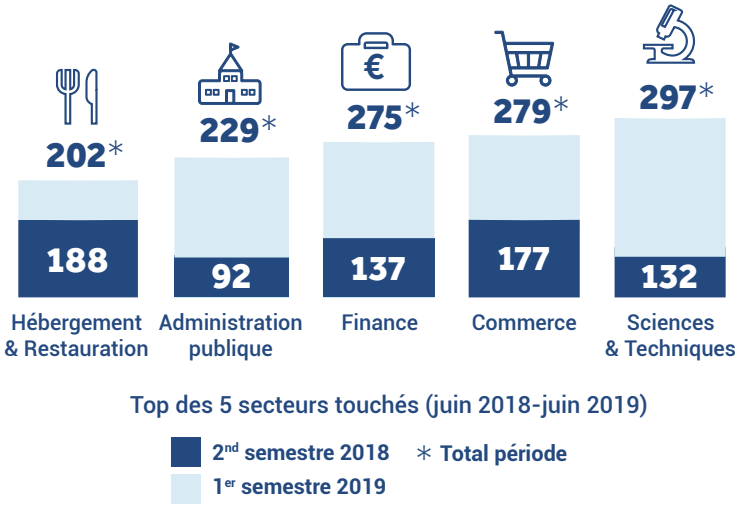
Ce baromètre est animé par le Forum International de la Cybersécurité (FIC) en partenariat avec PwC et Bessé et avec la participation de la CNIL. Les données exploitées sont issues des publications de la CNIL sur la plateforme data.gouv.fr.

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Les violations de données personnelles, notifiées à la CNIL et publiées en *open data*, représentent une source d'enseignements précieux pour tous les organismes traitant des données personnelles. Ce partage d'informations permet d'identifier quels sont, actuellement, les risques qui pèsent sur un organisme, sur les données qu'ils traitent et, finalement, sur les personnes concernées. Anticiper les incidents en se basant sur des cas concrets permet de cibler plus facilement les éléments à améliorer, chez soi, afin de ne pas être exposé et de se retrouver, à son tour, victime d'une violation. Valoriser ces informations profite au plus grand nombre et permet, *in fine*, de mieux protéger les données personnelles.

Tendances globales





Qu'est-ce qu'une donnée personnelle ?

→ **Toute information associée à un nom**	Manon Lambert est au chômage
→ **Toute information permettant d'identifier une personne**	L'adhérent G3701 est schizophrène
→ **Toute donnée permettant une identification indirecte des personnes**	Données biométriques

Qu'est-ce qu'une violation de données ?

Une violation de données à caractère personnel est constituée par tout incident de sécurité, accidentel ou illicite, entraînant l'altération, la destruction, la perte ou la divulgation de données à caractère personnel (Art. 4.12 du RGPD). Depuis le 25 mai 2018, date d'entrée en vigueur du RGPD, les organismes qui traitent des données personnelles doivent non seulement mettre en place des mesures pour prévenir les violations de leurs données, mais également réagir pour endiguer la violation et en atténuer les effets (Art.33 et 34 du RGPD).

Sanctions administratives

- Amende jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires ou
- Amende jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires

Sanctions pénales

- Personne physique : 5 ans d'emprisonnement et 300 000 d'euros d'amende
- Personne morale : jusqu'à 1,5 million d'euros d'amende

Histoire vécue

Piratage d'un réseau d'entreprise

1 Une campagne de *spear phishing* vise une entreprise

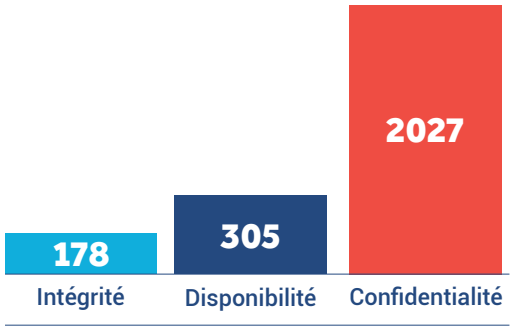
2 Ouverture d'un mail malveillant par un salarié et téléchargement d'une pièce jointe

3 Infection de la machine du salarié et latéralisation de l'attaquant sur le réseau

4 Exfiltration de données de plus de 15 000 clients

Quel impact sur l'entreprise ?

Si les impacts d'une violation de données varient, on peut néanmoins identifier des constantes. En effet, une société subit des **pertes financières** pendant l'attaque, dues à l'indisponibilité des données par exemple, mais aussi après l'attaque lorsqu'elle doit remettre ses systèmes en marche, dédommager des clients ou encore faire face à une chute de son activité en raison d'une perte de confiance des clients. L'**atteinte à la réputation** est un impact qui s'inscrit dans le temps long et auquel il est difficile de remédier. Une violation a aussi un **impact sur l'activité** d'une société et ce d'autant plus lorsqu'elle engendre une perte de propriété intellectuelle. Enfin, une violation de données peut avoir des **suites judiciaires** en cas de plaintes ou de non-respect des principes du RGPD par exemple.



Types d'atteinte aux données par violation
entre le 01/06/18 et 30/06/19

Intégrité	Disponibilité	Confidentialité
Altération des données (ex : la modification des coordonnées d'un utilisateur)	Des données sont rendues inaccessibles pour les personnes qui les traitent (ex : un compte institutionnel en ligne est bloqué)	Des données non publiques sont exposées virtuellement (des documents sont envoyés au mauvais destinataire) ou physiquement (des matériels contenant des données personnelles sont égarés)

Il n'y a pas que la confidentialité qui compte

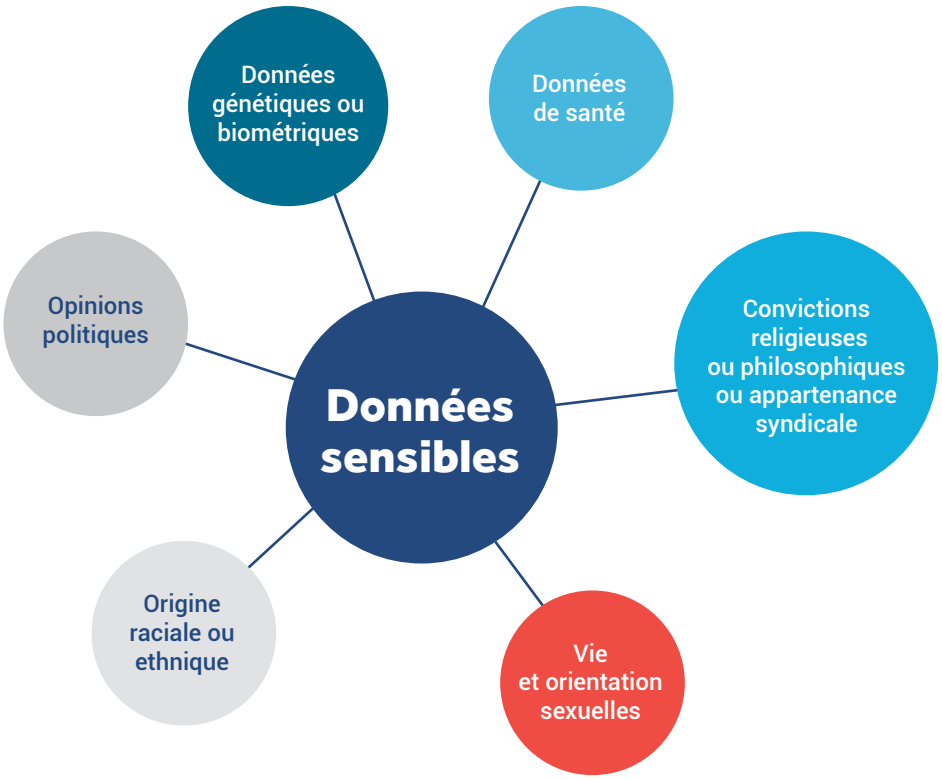
L'atteinte à la confidentialité est perçue, à tort, comme la plus grave des violations de données. Or, la manipulation illégitime d'un contenu peut également avoir de lourdes conséquences telles que l'altération d'informations fiscales comme ce fut le cas en août 2019, lorsque 2 000 comptes fiscaux ont été modifiés par des cyber attaquants. De même, rares sont les sociétés qui peuvent se passer de l'accès à leurs données : lorsqu'une attaque DDoS ou qu'un rançongiciel rend les données des salariés, des clients ou les données financières indisponibles, l'activité de la société est suspendue jusqu'à résolution de la crise. Il est par conséquent essentiel que la stratégie de sécurisation des sociétés intègre aussi bien la protection de la confidentialité que celle de l'intégrité et de la disponibilité des données.

Quelles sont les données affectées ?

10,4%
de données sensibles

Dans les violations de données personnelles notifiées
entre le 01/06/18 et 30/06/19

Qu'est-ce qu'une donnée sensible ?



Comment reconnaître une donnée sensible ?

1. **Est-elle nominative ?**
2. **Peut-elle affecter la vie de son propriétaire ?**

Autre type de données personnelles dites « non sensibles » :

Manon Lambert Nom	Photographie	Date de naissance	Adresse postale
Adresse mail	Numéro lié à une personne Téléphone, sécurité sociale, etc.	Adresse IP 172.16.254.1	Identifiant de connexion

Analyse d'impact mode d'emploi

1. **Circonscrire puis décrire les opérations de traitement**
2. **Evaluer la nécessité et la proportionnalité des opérations de traitement au regard de leur(s) finalité(s)**
3. **Apprécier les risques pouvant atteindre les droits et libertés des personnes**
4. **Prévoir des mesures et des mécanismes de protection adaptés aux risques identifiés**

Le rôle clé du DPO

Par Sandrine Cullaffroz-Jover, Avocate, PwC Société d'Avocats

Qu'il soit interne, externe, ou sous certaines conditions, mutualisé auprès de plusieurs organismes, le délégué à la protection des données (ou data protection officer) est en charge de la protection et de la sécurité des traitements de données à caractère personnel au sein d'une entreprise ou d'un organisme public.

Sa désignation est obligatoire pour (i) les autorités et organismes publics, (ii) les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle, (iii) les organismes dont les activités de base les amènent à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions. Toutefois, la désignation d'un délégué est toujours encouragée en ce qu'elle facilite l'identification et la mise en œuvre des actions de conformité au sein d'une structure.Tel un chef d'orchestre, il a notamment pour mission de piloter la gouvernance des données, d'informer et de conseiller l'organisme qui l'a désigné sur les traitements opérés, de sensibiliser les collaborateurs, de s'assurer et de contrôler la conformité des mesures prises en application du Règlement général sur la protection des données (RGPD) et des lois nationales.

Dans ce cadre, le délégué à la protection des données doit bénéficier d'une part, de solides compétences juridiques et d'une bonne compréhension de l'environnement technique de la donnée, et d'autre part, de moyens matériels et organisationnels, des ressources et du positionnement lui permettant d'exercer ses missions.

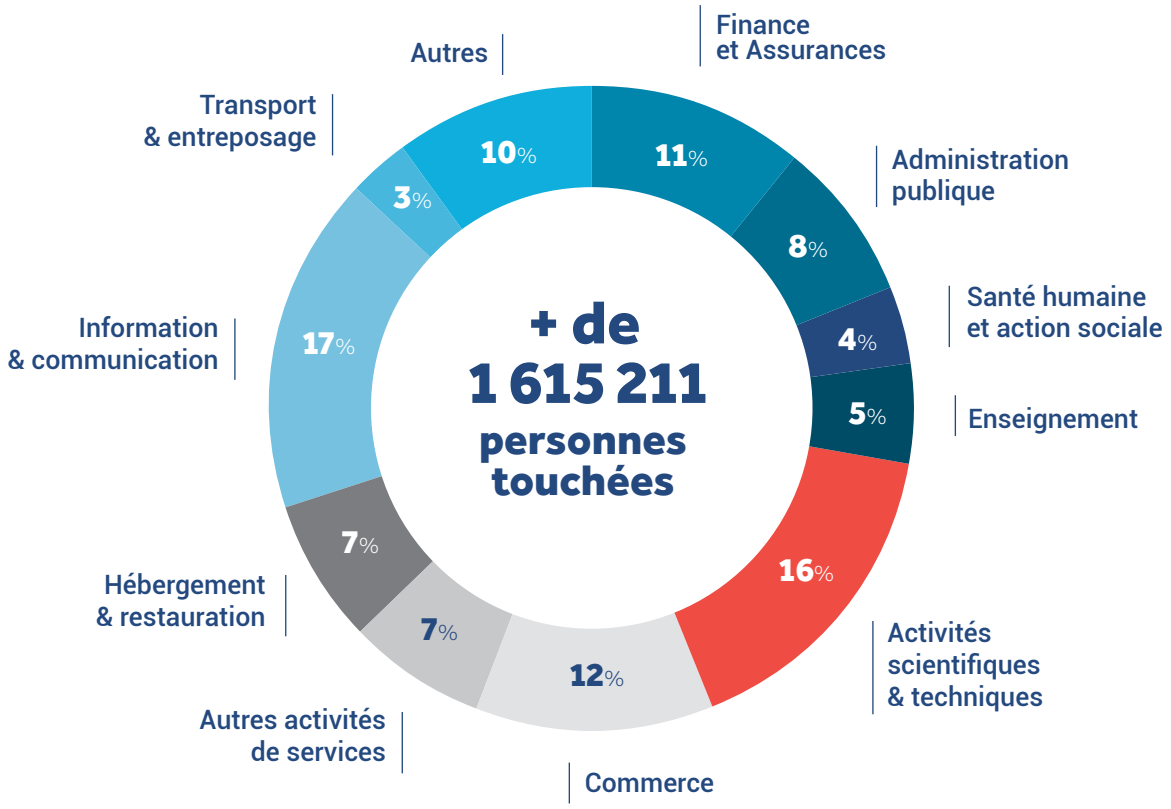
Quels sont les secteurs affectés ?

Aucun secteur n'est à l'abri...

Par Thierry Delville, Associé Cyber Intelligence, PwC France

Les chiffres sur les fuites de données souffrent encore d'une insuffisance de recul lié au caractère récent de l'obligation de déclarer celles-ci. Les premières observations permettent d'affirmer qu'aucun secteur n'est à l'abri : finance, commerce, médias, communication, industrie... la réalité des fuites de données suit de près celle des cyber menaces. Tous concernés : secteur public comme secteur privé, marchand ou non marchand, tel est l'enseignement que l'on peut tirer plus d'un an après la mise en place du RGPD.

Répartition des personnes touchées par secteur d'activité (juin 2018-juin 2019)

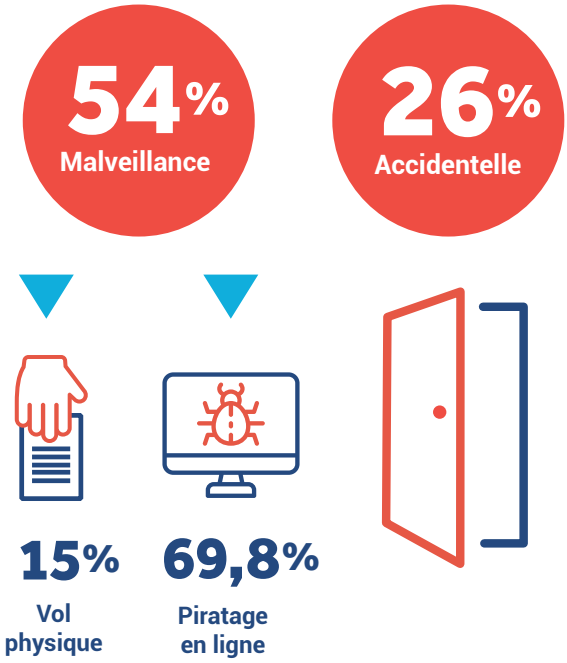


Note

Ce schéma est réalisé à partir du chiffre minimal indiqué dans les notifications de juin 2018 à juin 2019. Le nombre de personnes touchées par secteur est donc sans doute supérieur à celui présenté ici.

Quelles sont les origines des violations de données ?

Les origines des fuites de données*



***Analyse des violations notifiées**
du 01/06/18 au 30/06/19 par cause

Note : 20% des origines de violations sont « inconnues » ou « autre »

Spear phishing : attention danger !

Par Thierry Delville, Associé Cyber Intelligence, PwC France

Le spear phishing est une évolution ciblée et plus élaborée du classique phishing. On passe d'une attaque indifférenciée adressée à une importante quantité de victimes à un travail personnalisé ou l'attaquant cible sa future victime, lui adresse un mail personnalisé, après avoir travaillé sur son environnement (ingénierie sociale). Une fois la cible infectée, le plus souvent en ayant ouvert une pièce jointe ou suivi un lien vers un site malveillant, il ne reste plus à l'attaquant qu'à s'installer dans le système d'information puis après s'être attribué des droits administrateurs, de voler des identités ou encore d'exfiltrer des données qu'il revendra ou utilisera comme monnaie d'échange dans le cadre, par exemple, d'une demande de rançon.

Cette pratique s'est beaucoup développée au point d'en faire une activité très lucrative pour les cybercriminels et de devenir selon Europol, la forme la plus fréquente d'ingénierie sociale. Elle connait d'autres variantes que le mail avec le vishing (voix via téléphone) ou le smishing (sms).

Le caractère élaboré de ce type d'attaque les rend plus difficile à détecter et ceci est d'autant plus inquiétant que le spear phishing représenterait selon Europol 65% des primo infections relevées chez les entreprises victimes. Prévention du personnel mais aussi des clients ou usagers, règles de sécurité sur l'IT et mise en place de solutions de cyber protection sont les réponses adaptées à ce type de menace.*

**https://www.europol.europa.eu/newsroom/news/europol-publishes-law-enforcement-and-industry-report-spear-phishing*

Top 3 des incidents et leurs origines

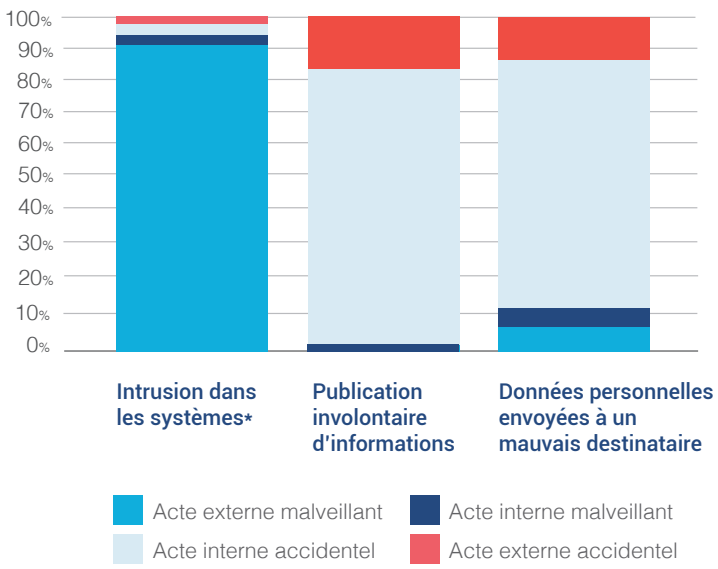
*Errare humanum est, perseverare diabolicum**

Le graphique ci-contre illustre la part encore non négligeable de violations de données ayant pour origine un acte **interne accidentel**. C'est le cas notamment pour les publications et les envois de données.

Plus largement, qu'il s'agisse d'accidents ou d'attaques, le **facteur humain** demeure au **cœur** des incidents de sécurité informatique. En effet, nombreux sont les salariés qui tombent encore dans le piège du *phishing* et seule l'organisation de campagnes de **sensibilisation** au sein des entreprises et des institutions permettra d'inverser la tendance.

De ce point de vue, le thème du FIC 2020 « Replacer l'humain au coeur de la cybersécurité » est tout à fait d'actualité.

** L'erreur est humaine, persévérer [dans son erreur] est diabolique*



* Intrusion dans les systèmes : ce terme renvoie à la catégorie « Piratage, logiciel malveillant (par exemple rançongiciel) et/ou hameçonnage » de la CNIL

Quelles réponses ?

1 Prévenir

Ne pas se limiter aux mesures visant à empêcher l'attaque. Préparer les équipes techniques et non techniques à la gestion de l'attaque en elle-même afin d'endiguer ses effets notamment financiers et réputationnels.

2 Détecter

La détection passe soit par le *Security Operations Center* (SOC) ; soit par une équipe de *cyber intelligence*.

3 Assurer

Souscrire une assurance sur-mesure qui couvre les conséquences d'une violation de données : frais de gestion de crise, de réponse à incident, de notification et préjudices financiers.

4 Réagir

Mettre d'abord fin à la violation (équipes techniques). Il est possible de faire appel à une équipe de réponse sur incident pour enquêter sur la violation. La CNIL doit être notifiée dans les 72h suivant la violation.

5 mesures préventives

Des mesures simples permettent de prévenir l'essentiel des violations, qu'elles soient d'origine malveillante ou accidentelle :

- Sensibilisation des personnels aux techniques du phishing ;
- Sensibilisation des personnels au verrouillage d'écrans ;
- Interdiction de l'utilisation des adresses mail professionnelles pour toute autre activité ;
- Application des principes du moindre privilège et du cloisonnement ;
- Utilisation de technologies de protection de données (chiffrement et vérification de l'authenticité).

Les bons réflexes en cas de violation de données

Il est essentiel de collecter des informations sur la violation de données et de la documenter en interne (nombre de personnes touchées, leur catégorie, etc.). Ce premier travail permet d'anticiper les conséquences de la violation et de prendre les mesures adéquates.

Votre enquête interne permet de répondre notamment aux questions de la notification de la violation de données à la CNIL. Le délai de notification est de 72h après la constatation de la violation. Le récapitulatif de la notification à la CNIL peut constituer le document interne.

Lorsqu'un risque élevé est identifié, les personnes exposées par une violation de données doivent être informées (données bancaires, identifiants de connexion pouvant mener à une usurpation d'identité, etc.).

L'assurance cyber : un maillon de la chaine de valeur de la cybersécurité

Par Jean-Philippe Pages, Directeur Industrie et Services, Bessé

Le transfert à l'assurance du risque cyber renforce la chaîne de valeur de la cybersécurité. Le développement récent de solutions d'assurance dédiées le favorise pleinement. En effet, le jour où le risque se réalise, la mise en œuvre des mesures d'accompagnement prévues, l'indemnisation des frais de gestion de crise, d'investigation, de remédiation et de notification ainsi que la couverture des préjudices financiers participent de manière significative à ***augmenter le niveau de cyber résilience de l'entreprise****.*

Le dimensionnement et l'efficacité de l'assurance face à ce risque complexe nécessitent une approche sur-mesure. L'objectif est d'appréhender le meilleur niveau de couverture, tant en termes de montant que de nature des garanties à structurer.

Le contrat d'assurance dédié au cyber s'intégrera ainsi parfaitement dans le plan d'assurance global de l'entreprise.

L'entreprise cyber résiliente est celle qui met en œuvre tous les maillons de cette chaine de valeur : gouvernance du risque, prévention, protection et transfert du risque résiduel au marché de l'assurance.

Comparaison France / Pays-Bas

Les Pays-Bas sont le pays européen notifiant le plus les atteintes à la protection des données. Entre l'entrée en vigueur du Règlement général sur la protection des données (RGPD) en mai 2018 et février 2019, 15 400 notifications ont été enregistrées d'après le cabinet DLA Piper, contre 1 548 en France sur la même période. Cet écart peut s'expliquer par une plus grande maturité des sociétés néerlandaises qui notifient plus systématiquement les atteintes.

Ressources

- **Notifier une violation de données à caractère personnel auprès de la CNIL : http://www.cnil.fr**
- **Porter plainte : https://www.pre-plainte-en-ligne.gouv.fr/**
- **Trouver un prestataire référencé grâce à la plateforme d'assistance aux victimes d'actes de Cybermalveillance ACYMA : http://www.cybermalveillance.gouv.fr**
- **Retrouver le cadre européen : https://edpb.europa.eu**

Baromètre
Data Breach