RSA

ENQUÊTE RSA 2019 : CONFIDENTIALITÉ ET SÉCURITÉ DES DONNÉES

Déconnexion croissante au sujet des données entre les consommateurs et les entreprises

BUSINESS-DRIVEN SECURITY™

LE RISQUE NUMÉRIQUE CRÉÉ PAR LES DONNÉES CLIENT

Au fur et à mesure que la concurrence augmente sur tous les marchés, les entreprises évoluent rapidement en termes de modèles et de services numériques pour offrir aux consommateurs des expériences numériques plus performantes, plus personnalisées et plus satisfaisantes.

Cependant, il existe une fracture croissante entre les entreprises qui capitalisent sur les données client et les attentes des consommateurs concernant la manière dont leurs données doivent être utilisées et sécurisées. L'année 2018 a été témoin d'une multitude de violations de données très médiatisées qui ont compromis des milliards de comptes. Au cours de ces incidents, les entreprises ont subi des dommages financiers sous la forme de dépenses liées aux violations et d'amendes pour infractions réglementaires, mais elles ont également subi une perte potentiellement irréversible de la confiance du client. Les consommateurs se sont rendu compte que leurs données avaient été non seulement exposées, mais également utilisées de manière inédite et non validée. Cette perte de confiance représente l'un des principaux risques cachés de la transformation numérique. Les cyberviolations pourraient devenir des événements capables de façonner le marché, annonçant le déclin et la disparition éventuelle de grandes marques si les consommateurs fuient vers des concurrents.

C'est dans ce contexte que nous avons mené notre deuxième enquête annuelle RSA® sur la confidentialité et la sécurité des données en nous attachant à un thème dont la pertinence est croissante pour l'environnement métier actuel : l'utilisation éthique des données.

SYNTHÈSE

Le battage médiatique régulier lié à la mauvaise utilisation des données et à la divulgation d'informations suite à des violations au cours des dernières années est à l'origine d'une évolution rapide des attitudes des consommateurs en matière de confidentialité de leurs données. Bien que les consommateurs pensent qu'il existe des moyens éthiques pour les entreprises d'utiliser leurs données, ils éprouvent des inquiétudes croissantes concernant leur confidentialité, se méfient des tendances telles que la personnalisation et le suivi des appareils, et blâment les entreprises lorsqu'elles sont piratées. De manière assez paradoxale, les consommateurs pensent également que leur responsabilité est limitée en matière de protection de leurs propres données, ce qui entraîne des pratiques assez laxistes pour les mots de passe et la manipulation des informations. Par conséquent, les entreprises doivent éduquer les consommateurs sur la manière dont les données sont partagées, obtenir leur consentement et leur confiance, et donner l'exemple. Celles qui choisiront cette option forgeront la réputation de leur marque sur l'utilisation éthique des données, tandis que les autres seront susceptibles d'en vivre le contrecoup sur un marché où les médias ont une place privilégiée.

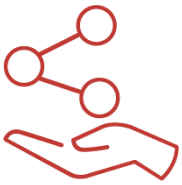
ENQUÊTE RSA® SUR LA CONFIDENTIALITÉ ET LA SÉCURITÉ DES DONNÉES : EN BREF

Notre deuxième enquête annuelle se consacre à l'utilisation éthique des données. Elle propose :

- une analyse des attentes des consommateurs en France, en Allemagne, au Royaume-Uni et aux États-Unis, selon les personnes interrogées ;
- la compréhension des différences entre les pays et les raisons de leur importance ;
- un regard sur les différences entre générations, y compris la génération Z, les jeunes Millennials et les Millennials plus âgés, la génération X et les baby-boomers ;
- des informations sur les attitudes des consommateurs à l'égard de la manière dont les différents types d'informations personnelles (tels que les mots de passe en ligne, les coordonnées, les données de navigation, les données médicales, etc.) doivent être protégés ;
- des recommandations pour les entreprises qui souhaitent créer des politiques de données à la fois éthiques et durables.

Le rapport RSA sur les points de vue des consommateurs au sujet de la collecte, de l'utilisation et du partage de données a permis de découvrir les informations suivantes pour les entreprises :

1. **Le contexte est important.** Les participants dans tous les pays interrogés s'inquiètent de leurs données financières/bancaires, ainsi que des données sensibles telles que les mots de passe. D'autres sujets de préoccupation varient considérablement en fonction de la génération, de la nationalité et même du sexe. Les entreprises doivent prendre en compte le contexte personnel de leurs utilisateurs lorsqu'elles établissent et communiquent les politiques et pratiques en matière de données.
2. **Les attentes en matière de confidentialité sont culturelles.** Bien que le Règlement général européen sur la protection des données (RGPD) couvre tous les états membres de l'Union européenne, les consommateurs répondent à la confidentialité des données différemment en fonction de leur nationalité en raison de facteurs culturels, d'événements actuels et de violations de données très médiatisées dans leurs pays respectifs. Les entreprises doivent prendre en compte la manière dont les réglementations et autres violations du partage des données façonnent et renforcent l'opinion publique sur l'ensemble de leurs marchés.
3. **La personnalisation reste un casse-tête.** D'innombrables études ont démontré que les expériences personnalisées augmentent l'activité des utilisateurs et leurs achats. Mais dans le même temps, les consommateurs ne sont pas d'accord avec l'affirmation selon laquelle les entreprises qui disposent de plus de données leur permettent de proposer des produits et des services de meilleure qualité et plus personnalisés. L'année dernière, nous avons assisté à une réaction violente de la part des médias comme des consommateurs lorsque les grandes marques ont révélé des pratiques de collecte et de partage de données allant très loin, ainsi que des violations de données. Il est impératif que les entreprises communiquent pourquoi et comment elles utilisent les données des clients afin de limiter les risques métiers pour le futur.



En moyenne, 48 % des personnes interrogées sont d'accord avec l'affirmation suivante : « il existe des méthodes éthiques selon lesquelles une entreprise peut utiliser mes informations/données personnelles ».

DIFFÉRENCES D'ATTITUDE ENVERS L'UTILISATION ÉTHIQUE DES DONNÉES

RSA

- **Les États-Unis sont en tête des pays interrogés pour l'acceptation des consommateurs.** Aux États-Unis, 60 % sont d'accord avec cette affirmation, contre seulement 48 % au Royaume-Uni, 45 % en France et 43 % en Allemagne.
- **Les consommateurs nés avec le numérique sont les plus à l'aise avec le partage de données.** Parmi les participants qui sont d'accord avec cette affirmation, il y 54 % de la génération Z (âgés de 18 à 24 ans pendant cette enquête) et 54 % des jeunes Millennials (25 à 34 ans pendant cette enquête), contre 49 % des Millennials plus âgés (35 à 44 ans dans cette enquête), 47 % de la génération X (45 à 54 ans pendant cette enquête) et 44 % des baby-boomers (55 ans et plus pendant cette enquête).

Étant donné que les attitudes des consommateurs varient selon les générations, les régions et le temps, il est essentiel que les politiques des entreprises soient durables. Pour atteindre cet objectif, les entreprises doivent reconnaître et protéger le droit des consommateurs à la confidentialité, tout en tenant compte de l'impact des technologies émergentes. Nous espérons que les entreprises puissent utiliser les informations tirées de cette enquête pour élaborer et peaufiner leurs propres politiques et normes en matière de données éthiques. Ainsi, elles pourront resserrer les liens avec leurs clients pour développer leur activité tout en répondant à des préoccupations très réelles en matière de protection des données et de confidentialité.

À PROPOS DE CETTE ENQUÊTE

Il s'agit de la deuxième enquête annuelle RSA® sur la confidentialité et la sécurité des données. L'objectif de cette enquête annuelle est de comprendre les valeurs générales des consommateurs en matière de confidentialité et de sécurité des données, ainsi que les changements d'une année sur l'autre. Ce faisant, nous cherchons à comprendre les tendances stratégiques en matière de collecte de données, d'utilisation, de stockage, de conformité et de sécurité qui peuvent avoir un impact sur les entreprises et leurs marchés en rapide évolution.

NOTRE MÉTHODOLOGIE

TAILLE D'ÉCHANTILLON TOTALE :

6 387

ADULTES EN FRANCE, EN ALLEMAGNE, AU ROYAUME-UNI ET AUX ÉTATS-UNIS


FRANCE


ALLEMAGNE


ROYAUME-UNI


ÉTATS-UNIS

- L'enquête a été réalisée en ligne par YouGov Plc.
- Tous les chiffres, sauf mention contraire, proviennent de YouGov Plc.
- L'enquête a été réalisée entre le 18 et le 27 décembre 2018, pour obtenir un véritable aperçu des attitudes des consommateurs sur l'année qui se termine.
- Les chiffres ont été pondérés de façon uniforme pour chaque pays afin de produire une valeur « moyenne ».

RSA

ÉVALUATION DE L'UTILISATION DES DONNÉES À TRAVERS LES GÉNÉRATIONS

Les personnes interrogées ont été interrogées sur plusieurs tranches d'âge :

- 18 à 24 ans (génération Z)
- 25 à 34 ans (Millennials les plus jeunes)
- 35 à 44 ans (Millennials les plus âgés)
- 45 à 54 ans (génération X)
- 55 ans et plus (baby-boomers)

TYPES D'INFORMATIONS PERSONNELLES QUE LES CONSOMMATEURS ENVISAGENT DE PROTÉGER

Les attitudes des consommateurs varient en fonction des informations personnelles qu'ils considèrent comme confidentielles. Dans le cadre de ce rapport, voici les catégories que nous définissons comme des informations personnelles :

- Données financières/bancaires
- Informations sur la sécurité
- Documents d'identité
- Dossiers médicaux
- Coordonnées
- Données biométriques
- Données génétiques
- Données de navigation
- Données de localisation
- Affiliation à un parti politique

INFORMATION CLÉ N° 1 EN MATIÈRE DE DONNÉES, LE CONTEXTE EST IMPORTANT

Bien que les consommateurs reconnaissent qu'ils créent et partagent de grandes quantités de données numériques, ils perçoivent différemment les différents types de données. Pour cette raison, toutes les informations personnelles ne sont pas créées ou protégées de la même façon.

LES 5 TYPES D'INFORMATIONS PERSONNELLES IMPORTANTS AUX YEUX DES CONSOMMATEURS

Nous avons posé la question suivante aux personnes interrogées : « Dans l'ensemble, parmi les types d'informations/données personnelles suivants, lesquels (le cas échéant) suscitent pour vous un besoin de protection ? ». La réponse a été : toutes les données pouvant servir au vol de leur identité ou à la fraude. Voici une brève liste des types de données dont les consommateurs craignent de perdre le contrôle.

78 %
DONNÉES FINANCIÈRES/ BANCAIRES

75 %
INFORMATIONS SUR LA SÉCURITÉ

70 %
INFORMATIONS SUR L'IDENTITÉ

61 %
INFORMATIONS MÉDICALES

57 %
COORDONNEES

RSA

Les baby-boomers de tous les marchés interrogés s'intéressent davantage à ces cinq catégories principales d'informations personnelles que les autres groupes d'âges, alors que l'aisance générale quant à l'utilisation des données augmente dans les groupes d'âge plus jeunes. Toutefois, la génération Z montre une plus grande inquiétude à l'égard de son empreinte numérique (localisation, photos et vidéos) par rapport aux autres types de données. Ainsi, ses préoccupations s'alignent mieux sur les catégories démographiques plus âgées.

PROTECTION DES MOTS DE PASSE RECYCLÉS

Selon une autre enquête, malgré la sensibilité des utilisateurs à l'égard de la perte de mot de passe, jusqu'à 73 % d'entre eux réutilisent les mêmes mots de passe pour différents comptes en ligne, ce qui accroît le risque de vol de mot de passe et d'utilisation malveillante des informations d'identification.

Le désir des consommateurs de protéger ces types d'informations personnelles est compréhensible, car ces données peuvent être utilisées pour commettre un vol d'identité ou pire. Avec des expositions répétées de données, il n'a jamais été aussi simple pour les cybercriminels de créer des identités numériques, généralement pour commettre des fraudes financières, mais également pour usurper l'identité des victimes. Ces dernières années, les cybercriminels ont usurpé l'identité d'enfants (qui n'ont pas d'antécédents de crédit) pour commettre des fraudes financières qu'il faut des années pour détecter.

En outre, les techniques de piratage telles que le « credential stuffing » automatisent les attaques à l'aide d'informations d'identification volées, ce qui permet d'accéder plus rapidement à un réseau via un ou plusieurs comptes. Cette technique permet aux pirates informatiques de commettre des vols de données plus importants avant qu'ils ne soient identifiés et évincés du réseau par les équipes de sécurité.

LES FEMMES REVENDIQUENT LEUR DROIT À LA CONFIDENTIALITÉ NUMÉRIQUE

Les hommes et les femmes de tous les marchés interrogés ont le même sentiment de protection vis-à-vis de leurs informations personnelles, à une exception importante près : les femmes sont plus protectrices que les hommes pour leurs photos et vidéos.

Ainsi, la perte de contrôle sur ces données par une entreprise est considérée par les femmes comme une violation importante de la vie privée. Comme nous l'avons vu par le passé, c'est l'entreprise qui est blâmée pour ces incidents, même si ce sont les consommateurs qui créent ces risques en répondant aux attaques de spear phishing ou en utilisant des mots de passe faibles. Par conséquent, l'adoption de technologies telles que l'authentification multifacteur et l'analytique comportementale des utilisateurs est particulièrement importante pour les entreprises qui stockent des données sensibles.

Les femmes sont plus soucieuses de protéger leurs photos et vidéos (54 %) que les hommes (47 %).

RSA

INFORMATION CLÉ N° 2 LES ATTENTES EN MATIÈRE DE CONFIDENTIALITÉ DES DONNÉES SONT CULTURELLES

Le RGPD est entré en vigueur le 25 mai 2018. La France, l'Allemagne et le Royaume-Uni ont adopté des lois sur la confidentialité des données conformément au RGPD en les adaptant aux besoins de leur pays. Dès lors, les plaintes relatives à la confidentialité des données ont augmenté dans ces trois pays.

Ce qui est intéressant, c'est que les attitudes européennes envers la confidentialité des données ne sont pas homogènes. Pour illustrer ce point, notre enquête a révélé que les français étaient moins soucieux de leurs données personnelles qu'en Allemagne et au Royaume-Uni dans presque toutes les catégories de données sur lesquelles porte l'enquête.

CONFIDENTIALITÉ DES DONNÉES : SURPRISE SUR CE QUE LES CONSOMMATEURS NE SE SOUCIENT PAS DE PROTÉGER

Les consommateurs français et américains se sentent plus libres de partager leurs données que leurs homologues en Allemagne et au Royaume-Uni . Qui est concerné ?

SEULS
43 %
DES FRANÇAIS SONT SOUCIEUX DE PROTÉGER LEURS DONNÉES MÉDICALES

SEULS
37 %
DES FRANÇAIS ET AMÉRICAINS SONT SOUCIEUX DE PROTÉGER LEURS DONNÉES DE NAVIGATION

SEULS
42 %
DES AMÉRICAINS SONT SOUCIEUX DE PROTÉGER LEURS COMMUNICATIONS (MESSAGES, E-MAILS, ETC.)

LA CONFIDENTIALITÉ DES DONNÉES EST UNE PRÉOCCUPATION CROISSANTE DANS CHAQUE PAYS

La France était le pays le moins soucieux de la confidentialité de ses dossiers médicaux (bien que son intérêt augmente de 10 % chaque année).

En général, les Allemands sont moins à l'aise avec le partage de données et il est possible que le récent passage au RGPD ait augmenté la sensibilisation et la préoccupation liée au partage des données. Comme le montre le tableau ci-dessous, les Allemands sont devenus plus soucieux de protéger leurs données, avec notamment un désir croissant de protéger leurs données de localisation.

RSA

Voici comment l'attitude des Allemands en matière de confidentialité des données a évolué au cours des mois qui ont suivi l'implémentation du RGPD :

LES ALLEMANDS SONT PARTICULIÈREMENT SOUCIEUX DE LA CONFIDENTIALITÉ DES DONNÉES

	2018	comparé à 2017
SOUCIEUX DE LA PROTECTION DES DONNÉES MÉDICALES :	70 %	63 %
SOUCIEUX DE LA PROTECTION DES COMMUNICATIONS :	62 %	52 %
SOUCIEUX DE LA PROTECTION DES DONNÉES DE LOCALISATION :	42 %	29 %

Les allemands protègent également de plus en plus la vie privée de leurs enfants, en interdisant la vente de jouets IoT et de montres intelligentes qui peuvent être utilisés pour surveiller et suivre le comportement des enfants.

LES CONSOMMATEURS N'ONT JAMAIS ÉTÉ AUSSI SOUCIEUX DU VOL D'IDENTITÉ

Lorsqu'il s'agit de données volées, les consommateurs du monde entier s'inquiètent du vol d'identité qui entraîne une perte financière. Toutes les personnes interrogées ont exprimé leur inquiétude liée à la perte monétaire, en particulier le Royaume-Uni .

« »

Les participants britanniques étaient particulièrement inquiets par le vol d'identité entraînant une perte financière. C'était le cas pour environ 78 % d'entre eux, contre une moyenne de 72 % de tous les pays interrogés.

Le chantage est également une préoccupation, mais pas pour tout le monde. La génération Z s'en soucie de manière disproportionnée (42 %) par rapport aux générations précédentes. Cela est probablement dû au fait que la génération Z est la plus connectée de toutes les générations. Elle utilise les réseaux sociaux et la messagerie de manière compulsive, et consomme du contenu en ligne tout au long de la journée. Ainsi, la génération Z possède la plus grande empreinte numérique à protéger.

À partir des Millennials les plus jeunes, les inquiétudes liées au chantage s'estompent. Seuls 35 % des Millennials (tous âges confondus), 32 % de la génération X et 31 % des baby-boomers sont inquiets.

Cela est probablement dû au fait que les générations les plus anciennes hésitent plus à partager des informations personnelles et publient donc moins d'informations dignes de chantage. En outre, la génération X et les baby-boomers, qui se trouvent proches ou au début de la retraite, sont moins susceptibles de s'inquiéter des risques professionnels que leurs homologues plus jeunes.

RSA

La génération Z est plus préoccupée par le chantage que les autres générations. En 2018, environ 42 % craignaient le chantage. En moyenne, 34 % seulement des personnes interrogées étaient inquiètes.

RÉFLEXE HABITUEL : SE REJETER LA FAUTE APRÈS UNE VIOLATION

Au lendemain d'une violation de données, il est facile de pointer des coupables du doigt : le PDG pour favoriser une culture de non conformité, le responsable marketing pour un marketing agressif, le DSI pour ne pas remédier aux vulnérabilités ou les pirates eux-mêmes.

Les participants britanniques et américains ont tendance à blâmer les sociétés plutôt que les pirates, tandis que les français et les allemands sont en désaccord. Cela peut venir des récentes violations, très médiatisées, au Royaume-Uni et aux États-Unis, dont nos participants se souviennent encore.

Ce qui est clair en tous cas, c'est que les consommateurs ne se blâment pas eux-mêmes. La plupart d'entre eux estiment qu'ils n'auraient pas d'ennuis s'ils perdaient des données confidentielles au travail. De même, lorsque les sociétés sont piratées en raison de mauvaises pratiques liées aux noms d'utilisateur et mots de passe des collaborateurs, elles sont tenues pour responsables. Souvent, ces piratages peuvent être reliés à des sites tiers et des médias sociaux, où les collaborateurs ont réutilisé les noms d'utilisateur et les mots de passe, ouvrant ainsi la voie à des pirates informatiques sur leur lieu de travail.

À ce jour, les violations de données en Allemagne et en France ont été de plus petite envergure, et les deux pays disposent d'une nouvelle législation rigoureuse alignée sur le RGPD. Pour ces raisons, les consommateurs de ces pays sont peut-être plus enclins à blâmer les pirates plutôt que les sociétés.

APRÈS LE PIRATAGE : QUI EST RESPONSABLE

Lorsque leurs données sont piratées, les consommateurs tiennent généralement les sociétés pour responsables. En réponse à la question « Si une société perd mes données/informations personnelles, j'ai tendance à la tenir pour responsable plus que toute autre entité, y compris le pirate lui-même » :

LES PARTICIPANTS AMÉRICAINS SONT D'ACCORD À

64 %

LES FRANÇAIS SONT PARTAGÉS À

50 %

MOINS D'ALLEMANDS SONT D'ACCORD AVEC

41 %

LES PARTICIPANTS DU ROYAUME-UNI SONT D'ACCORD À

72 %

RSA

C’est de votre faute, pas de la mienne ! La plupart des personnes interrogées ne sont pas inquiètes des conséquences d’une perte de données confidentielles au travail. Voici qui s’inquiète :

22 %  FRANÇAIS

16 %  ALLEMANDS

15 %  ROYAUME-UNI

8 %  ÉTATS-UNIS

Les sociétés sont responsables de l’éducation de leurs collaborateurs : la formation à la sécurité des informations et les campagnes de sensibilisation aux risques peuvent contribuer à la création d’une culture des risques. En règle générale, les collaborateurs ne sont pas tenus pour responsables des incidents liés aux risques d’information dans toutes les zones géographiques, sauf en cas de négligence extrême ou de comportement contraire aux politiques. Les lois européennes du travail protègent généralement les droits des collaborateurs. Il est donc logique que les personnes interrogées dans ces zones géographiques ne soient pas préoccupées par un licenciement. Ce qui est surprenant, c’est que les collaborateurs aux États-Unis, qui peuvent être licenciés facilement, n’aient pas peur des conséquences de la perte des données de l’entreprise.

INFORMATION CLÉ N° 3
LES CONSOMMATEURS SONT EN DÉSACCORD AVEC LES ENTREPRISES SUR LA PERSONNALISATION

Au cours des 20 dernières années de transformation numérique, les consommateurs et les entreprises ont conclu un pacte : de nombreux consommateurs ont accepté de partager des données en échange de produits gratuits ou à prix réduit, et les entreprises ont accepté d’utiliser les données pour personnaliser leurs expériences et innover. La personnalisation est un élément clé de la vie numérique des consommateurs. Ils naviguent sur les sites de commerçants en ligne via les suggestions « recommandées pour vous » ou « les personnes qui ont acheté ceci ont également acheté » pour filtrer et prendre des décisions d’achat. Ils collaborent avec les plates-formes de diffusion en streaming et les agrégateurs de sites d’actualité pour filtrer le contenu et générer des flux d’actualité sur les réseaux sociaux. Et la liste est longue.

Mais désormais, le point de vue des consommateurs sur cet avantage partagé, ou au moins leur compréhension, a changé. En raison de la couverture médiatique constante, les utilisateurs sont bien informés que le suivi de leur comportement par la technologie a été plus répandu qu’ils ne l’imaginaient, et que leurs données personnelles ont été partagées avec des tierces, voire des quatrièmes parties d’une manière qu’ils considèrent comme abusive. Il n’est donc pas surprenant que les utilisateurs aient un regard de plus en plus cynique sur les affirmations, les promesses et les politiques de protection des données des sociétés.

Celles-ci doivent trouver une façon de se connecter aux consommateurs et de répondre aux besoins à la fois partagés et éprouvés, tout en respectant la confidentialité. Ce défi devient encore plus difficile à mesure que l’Internet of Things (IoT) est répandu sur le lieu de travail et qu’il permet d’équiper des maisons intelligentes, des voitures connectées et des villes intelligentes. Dans un avenir proche, l’IoT, l’utilisation des appareils et l’intelligence artificielle se développeront au point que la technologie connaîtra les consommateurs encore mieux qu’ils ne se connaissent eux-mêmes.

Selon 52 % des personnes interrogées, l'utilisation des données éthiques se fait lorsqu'une société ne prend que les informations personnelles nécessaires à la prestation des services que les clients reçoivent et rien de plus.

Le fait de fournir davantage de données peut-il conduire à de meilleurs produits et services ?

2018 comparé à 2017

	2018	2017
PARTICIPANTS À L'ENQUÊTE RÉPONDANT OUI	29 %	31 %

L'IoT EST OMNIPRÉSENT, ET C'EST EN PARTIE UN PROBLÈME

En moyenne, 60 % de tous les consommateurs interrogés trouvent que les wearables sont effrayants. Cependant, les pionniers dans leur adoption les apprécient pour leur capacité à optimiser l'alimentation, la forme physique, la productivité et d'autres objectifs.

Pour ce qui est de l'utilisation éthique des données, il existe des différences notables entre les pays. Les personnes interrogées aux États-Unis sont plus à l'aise pour partager des données. Il n'est donc pas surprenant qu'elles se sentent plus optimistes quant à la façon dont les sociétés utilisent leurs données.

LES AMÉRICAINS SONT CEUX QUI ACCEPTENT LE MIEUX L'UTILISATION ÉTHIQUE DES DONNÉES

PEUT-ON SE METTRE D'ACCORD SUR L'UTILISATION ÉTHIQUE DES DONNÉES ?

Lorsque l'on a demandé s'il existait des façons éthiques pour une société d'utiliser des informations personnelles, 48 % des personnes interrogées ont répondu oui. La génération Z et les jeunes Millennials sont en tête avec 54 % des deux groupes estimant que les données peuvent être utilisées de manière éthique par les sociétés.

45 %	43 %	48 %	60 %
FRANÇAIS	ALLEMANDS	ROYAUME-UNI	ÉTATS-UNIS

Ces statistiques montrent clairement qu'il est évident que les sociétés sont confrontées à un défi de taille pour convaincre les consommateurs que le partage de données est à leur avantage. Il existe des critères spécifiques pour ce que les consommateurs considèrent comme un partage de données éthique, notamment la commodité ou la protection des identités. Par exemple, les moteurs de fraude modernes utilisent désormais les données de localisation pour authentifier les voyageurs et leurs transactions lorsqu'ils se déplacent d'un pays à un autre.

RSA

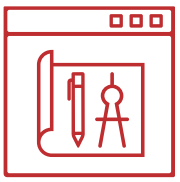
Le même moteur de fraude pourrait détecter les anomalies, telles que des transactions atypiques dans d'autres pays, et refuser ces transactions. Cependant, il a besoin d'obtenir l'autorisation d'accéder aux données de localisation des consommateurs pour proposer cette fonctionnalité pratique.

L'UTILISATION ÉTHIQUE DES DONNÉES SELON LES CONSOMMATEURS

Qu'attendent les consommateurs ? Notre enquête a approfondi des cas d'utilisation spécifiques afin de comprendre comment évoluent les attentes des consommateurs.

Nous avons posé une série de questions pour sonder les attitudes des personnes interrogées au sujet du marketing numérique et de la personnalisation du contenu, utilisée de manière généralisée par les entreprises. Les attitudes des consommateurs en matière de personnalisation ressemblent-elles à « Fais ce que je dis, pas ce que je fais » ? Les preuves semblent le confirmer.

LA PERCEPTION DES CONSOMMATEURS OCCIDENTAUX SUR LA PERSONNALISATION NUMÉRIQUE



Les consommateurs rejettent la personnalisation, même s'ils apprécient ses avantages au quotidien. Dans tous les pays ayant participé à l'enquête, ils perçoivent de plus en plus la personnalisation comme envahissante et contraire à l'éthique.

- *Fils d'actualité personnalisés* : seulement 24 % des personnes interrogées estiment qu'il s'agit d'une pratique éthique (31 % aux États-Unis) et 59 % jugent cette pratique contraire à l'éthique.
- *Recommandations basées sur l'historique des achats/de la navigation* : 25 % des personnes interrogées estiment qu'il s'agit d'une pratique éthique (37 % aux États-Unis), et 59 % jugent cette pratique contraire à l'éthique (67 % au Royaume-Uni).
- *Utilisation de l'historique des mentions « J'aime » pour recommander du contenu* : 28 % estiment qu'il s'agit d'une pratique éthique (38 % aux États-Unis), et 55 % jugent cette pratique contraire à l'éthique.
    - Ce sentiment est plus fort à l'étranger : 61 % au Royaume-Uni et 60 % en France trouvent cela contraire à l'éthique. Mais il existe une limite notable : en moyenne dans tous les pays participants, une parti plus grande de la génération Z considère cette pratique comme éthique (41 %) contre 38 % pour qui cette pratique est contraire à l'éthique.
- *Suivi des activités en ligne pour personnaliser les publicités* : 17 % des personnes interrogées estiment qu'il s'agit d'une pratique éthique et 68 % jugent cette pratique contraire à l'éthique.
- *Suivi des appareils et de la localisation pour identifier les accès non autorisés* : environ 36 % jugent cette pratique éthique, contre 46 % aux États-Unis
    - Remarque : en France, 27 % seulement estiment que cette pratique est éthique et 58 % la jugent contraire à l'éthique.
- *Suivi des habitudes d'achat et de la localisation pour surveiller la fraude* : 45 % des personnes interrogées considèrent cette pratique comme éthique. Par zone géographique : 56 % des personnes interrogées aux États-Unis considèrent cette pratique comme éthique, contre seulement 28 % en Allemagne et 34 % en France. En moyenne dans tous les pays, seulement 39 % des personnes interrogées considèrent cette pratique comme contraire à l'éthique, contre 52 % en France.
- *Habitudes de déplacement* : environ 42 % des personnes interrogées considèrent ce type de suivi comme éthique, en particulier 47 % aux États-Unis et 50 % au Royaume-Uni. Seulement 40 % le considèrent comme contraire à l'éthique, sauf en Allemagne et en France où cette proportion est supérieure : 42 % des allemands et 48 % des français trouvent cette pratique contraire à l'éthique.

RSA

LA GÉNÉRATION Z AIME SES « J'AIME »

En ce qui concerne les résultats individuels, il n'est pas surprenant que la génération Z trouve que l'utilisation de la mention « J'aime » pour adapter le contenu est plus éthique que tout autre groupe d'âge interrogé. En général, la génération Z est une utilisatrice avide des sites sociaux tels que Instagram, Snapchat et Twitter, qui utilisent tous les mentions « J'aime » pour façonner l'expérience. En fait, certains utilisateurs de la génération Z utilisent plusieurs sites comme des comptes Instagram publics et privés, afin de restreindre le partage de contenu à certains groupes d'amis.

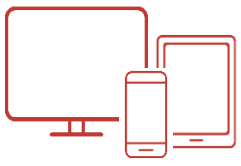
PERSONNE N'AIME LA PUBLICITÉ

Personne n'aime la publicité (conclusion qui s'aligne sur l'analyse de l'année dernière), car elle interrompt la navigation numérique et la consommation de contenu. Par conséquent, de nombreux consommateurs se sentent trompés lorsqu'ils lisent des publicités déguisées en articles. Les résultats de notre enquête reflètent l'opinion des consommateurs selon laquelle la publicité ciblée est une utilisation non éthique des données.

LE SUIVI DES APPAREILS EST CONTROVERSÉ

Le suivi des appareils est l'un des sujets qui souligne le mieux la déconnexion entre les attentes des consommateurs et la réalité de l'utilisation des données. De plus, il peut exposer les sociétés à un risque numérique si leurs politiques ne sont pas communiquées de manière transparente. Bien que les consommateurs apprécient la possibilité de protéger et de localiser leurs appareils, ils savent pertinemment que le suivi des appareils peut être utilisé pour connaître leur situation en continu. Aux États-Unis, les principales entreprises de télécommunications vendent des données sur la localisation des appareils mobiles qui peuvent être utilisées par les chasseurs de primes pour suivre la localisation des consommateurs en temps réel.

Les informations de suivi des appareils sont utilisées en toute légalité par les annonceurs, les prestataires de services financiers et médicaux, ainsi que par les services de sécurité publique. Le suivi des appareils permet d'authentifier les utilisateurs, d'activer les offres et les transactions marketing en temps réel, de prévenir les fraudes et d'aider à la prestation de services médicaux et de police, comme les interventions d'urgence. Bien que le suivi des appareils fasse partie de la vie quotidienne des consommateurs, il est possible que ses applications négatives se soient multipliées au détriment de ses avantages.



Les Français se démarquent particulièrement sur ce sujet : 58 % d'entre eux pensent que le suivi des appareils est contraire à l'éthique. Cette proportion est sensiblement plus élevée que celle des autres pays. Il est possible que les affrontements de fin 2018 en France entre les « gilet jaunes » et la police soient encore à l'esprit des personnes interrogées alors que notre enquête porte sur leur point de vue sur le suivi des données.

RSA

COMPORTEMENT ANTIFRAUDE ET SUIVI DE LOCALISATION, UNE VICTOIRE

Bien que les consommateurs ne veuillent pas que leur comportement ou leurs appareils soient suivis, ils sont disposés à faire une exception en matière de protection contre les fraudes. Le suivi des achats et de la localisation pour prévenir les fraudes sont éthiques pour la plupart des consommateurs aux États-Unis . Étant donné que la plupart des consommateurs ont peur du vol financier numérique ou des achats non autorisés, cela est compréhensible.

À l'exception de la prévention des fraudes, la déconnexion entre les préférences des consommateurs en matière de données et la réalité numérique actuelle représentent une quantité considérable de risques numériques, ce qui peut exposer les entreprises à des réactions, des boycotts ou des désinvestissements.

CONCLUSION : RÉSOUDRE PROACTIVEMENT LA DÉCONNEXION NUMÉRIQUE

Les sociétés doivent savoir que l'obligation de créer et de communiquer une politique des données relative à leur utilisation éthique deviendra la nouvelle norme. Bien que les consommateurs veuillent comprendre comment leurs données sont collectées, stockées, gérées et partagées, il est clair qu'ils n'appréhendent pas complètement la situation actuelle. Après une année ponctuée de plusieurs violations de données très médiatisées et de couverture médiatique négative sur les pratiques des sociétés, les consommateurs font preuve d'une opinion très marquée sur l'utilisation éthique des données. Il est également probable que le RGPD ait placé la barre plus haut pour les sociétés en termes de communication sur la collecte, l'utilisation et le partage des données.

Ainsi, nombre de consommateurs se sentent mal à l'aise vis-à-vis des processus de collecte des sociétés et refusent le partage de données. Faits marquants de l'enquête de cette année :

75 % des personnes interrogées limitent désormais la quantité d'informations personnelles qu'elles partagent en ligne.

57 % En plus de personnes interrogées au Royaume-Uni (57 % contre 43 % en moyenne dans les pays de l'étude) ont constaté une augmentation des fenêtres contextuelles de consentement par rapport à l'année précédente.

29 % LES PARTICIPANTS AMÉRICAINS sont beaucoup plus enclins que les européens à dire qu'ils ont ressenti des pressions de la part de leur employeur pour fournir des données de santé personnelles afin de bénéficier d'une remise sur les avantages médicaux ou d'autres mesures financières incitatives. (Environ 29 % des participants aux États-Unis ont indiqué subir des pressions contre 20 % en général.)

RSA

Alors que le nombre de violations de données s'envole, nous souhaitions en comprendre l'impact sur les consommateurs. Nous avons demandé : « Vos informations personnelles ont-elles été compromises en ligne par une violation de données au cours des cinq dernières années ?

AVEZ-VOUS ÉTÉ VICTIME D'UNE VIOLATION DE DONNÉES ?

36 %
DE TOUS LES PARTICIPANTS ONT RÉPONDU OUI

45 %
DES PARTICIPANTS AMÉRICAINS ONT RÉPONDU OUI

39 %
DE TOUS LES PARTICIPANTS NE SAVAIENT PAS

21 %
DE TOUS LES PARTICIPANTS ONT RÉPONDU NON

Alors que des milliards d'enregistrements de données qui ont été violés à ce jour, nous estimons que le nombre réel de personnes touchées par les violations est probablement beaucoup plus élevé, exposant ainsi les marques qui ne sont peut-être pas encore au courant de leurs violations à plus de risques numériques.

CE QUE NOS RÉSULTATS SIGNIFIENT POUR L'ENTREPRISE

Comme l'indiquent les résultats de notre enquête, les sociétés peuvent se positionner comme leaders (et apprendre) du thème important qu'est l'utilisation éthique des données et en tirer des enseignements. La définition de politiques est constante car les attentes et les comportements des consommateurs évoluent en permanence.

Cependant, les sociétés doivent se méfier de la collecte agressive de données inutiles, de leur utilisation de manière intrusive ou de leur partage avec des partenaires via des méthodes que les consommateurs n'approuvent pas. Les sociétés peuvent utiliser leur position sur la manière dont elles utilisent les données de manière éthique pour renforcer la confiance des clients et leur fidélité vis-à-vis de leur marque, à l'instar des marques de loisirs de plein air qui utilisent la durabilité de l'environnement pour communiquer leurs valeurs et construire leur marque.

Toutes ces informations, telles que la collecte excessive de données, la personnalisation envahissante, le partage non autorisé, les contrôles défectueux et les retards de notification sur les violations, peuvent nuire aux sociétés. Les politiques de collecte agressive de données peuvent engendrer un contrecoup médiatique et public, avec des consommateurs supprimant les applications ou réduisant l'utilisation et le partage des données. Parallèlement, les contrôles défectueux et les violations de données créent des risques pour la réputation des sociétés, ce qui stimule la couverture médiatique négative, les boycotts importants (comme la décision du journaliste technologique Walt Mossberg de quitter Facebook et Messenger), la censure réglementaire, les sanctions et les poursuites.

La situation crée un véritable casse-tête pour l'éthique des données. Les consommateurs peuvent se sentir contraints et refuser les services personnalisés. Seuls 22 % des participants s'accordent à dire qu'ils partageraient leurs données pour améliorer leurs expériences, et environ 41 % d'entre eux ne sont pas d'accord. En réalité, les consommateurs utilisent des services personnalisés tout le temps, et de nombreuses études ont démontré qu'ils sont enclins à acheter et à dépenser plus lorsque l'expérience est personnalisée.

En outre, il faut tenir compte du fait que de nombreuses sociétés retardent l'annonce des violations de données (ce qui n'est plus possible dans le cadre du RGPD), car elles évaluent l'étendue de la perte de données et formulent leurs réponses aux médias et aux consommateurs. Bien que seul un tiers des personnes interrogées estiment que leurs informations personnelles ont été compromises dans le cadre d'une violation de données, les milliards de dossiers qui ont été victimes de violations l'année dernière indiquent que leur nombre est probablement beaucoup plus élevé.

RSA

La moitié des consommateurs interrogés (58 % des participants aux États-Unis) ont déclaré qu'ils envisagent de se détacher des sociétés qui montrent qu'elles n'ont aucun respect pour la protection des données des clients.

Presque toutes les entreprises de la planète sont en contact avec les données des consommateurs, mais les leaders numériques et les agrégateurs de données sont tenus de se conformer aux normes les plus strictes en matière de protection des informations personnelles. Comme l'indiquent les résultats de notre enquête, la plupart des consommateurs tiennent les sociétés responsables plutôt que les pirates informatiques en cas de violation de données, et les collaborateurs ne se sentent pas responsables s'ils perdent des informations confidentielles pendant leur travail.

Les entreprises doivent prendre leurs responsabilités en termes d'utilisation et de sécurisation des données client de manière éthique. L'hygiène des données et la sécurité doivent se compléter les unes les autres, et les sociétés doivent montrer leur volonté de gagner et de conserver la confiance des consommateurs.

Les sociétés qui définissent et communiquent des pratiques de données éthiques à leurs clients créeront des relations plus solides avec eux, en créant en toute transparence des expériences qui apportent un véritable avantage mutuel.

Comment votre société va-t-elle se positionner (et apprendre) pour favoriser une utilisation des données éthiques en 2019 ?

Prenez part à la discussion @RSAsecurity.

Contactez RSA pour obtenir de l'aide à la gestion des risques numériques : rsaglobalcomms@rsa.com

RSA