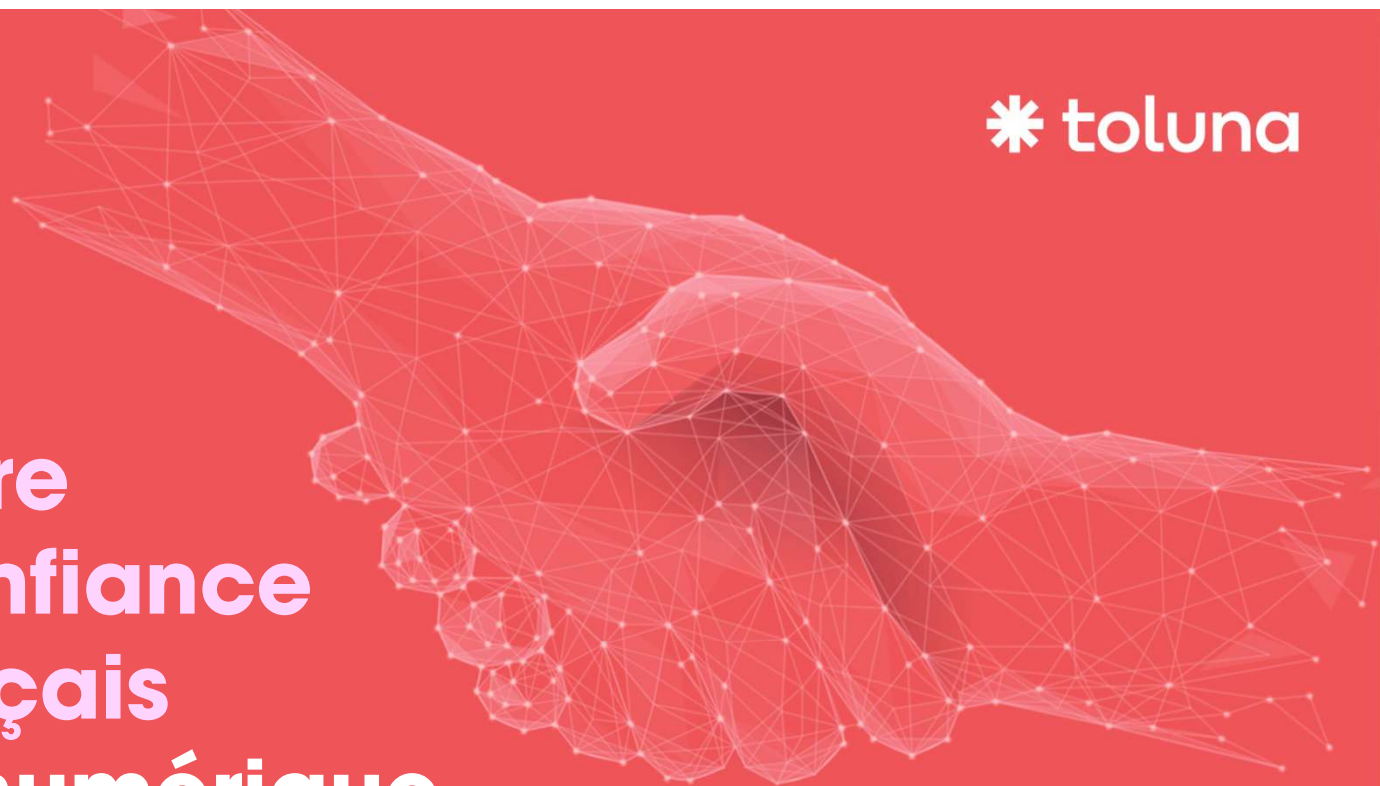


ACSEL

* toluna

13^e
ÉDITION

Baromètre de la confiance des Français dans le numérique



Méthodologie d'enquête



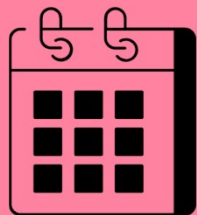
*** toluna**

Étude online
réalisée sur le
panel de Toluna



1307 répondants

Échantillon représentatif des
internauts français âgés de
15 ans et plus.



Dates de terrain :
Du 01 au 11 décembre 2025



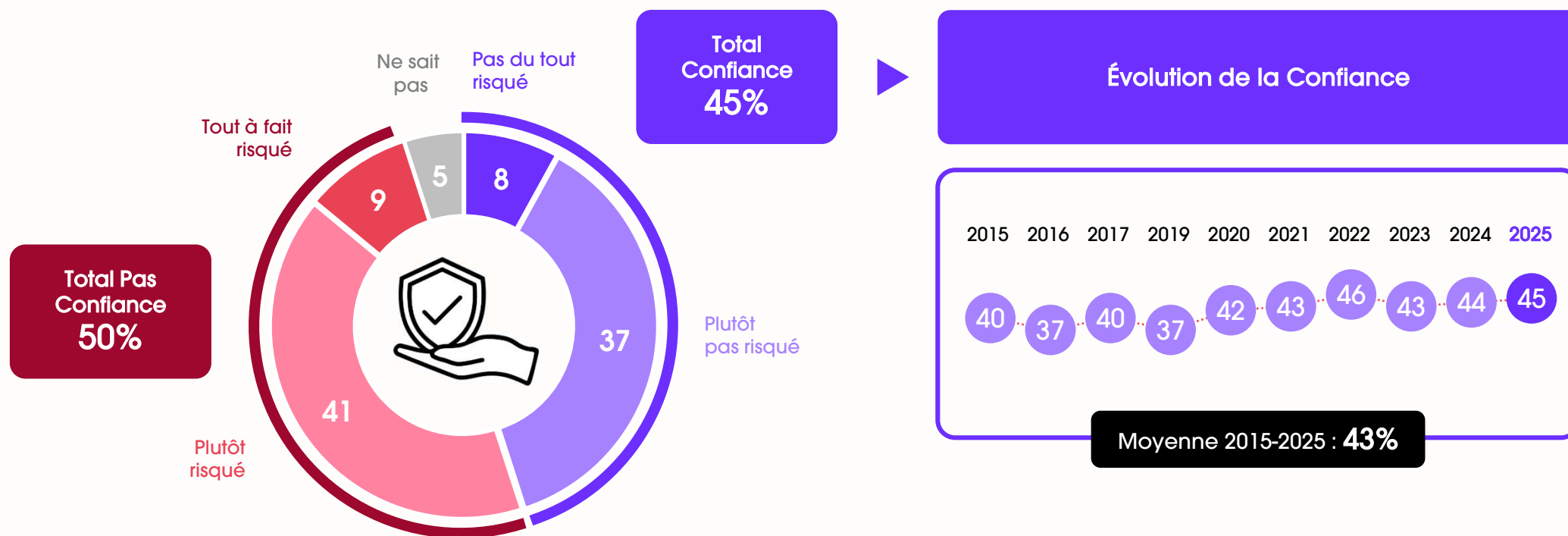
Méthode des quotas et
redressement appliqués aux
variables suivantes : sexe, âge,
catégorie socioprofessionnelle,
taille d'agglomération et
fréquence d'utilisation d'Internet.



1. L'évolution de la confiance

Une confiance qui peine à
se consolider dans un contexte
d'exposition croissante au piratage.

La confiance envers l'utilisation d'Internet est toujours minoritaire et confirme le constat des dernières mesures.



Le sentiment que les escroqueries en ligne sont de plus en plus fréquentes se consolide, y compris chez les plus jeunes.

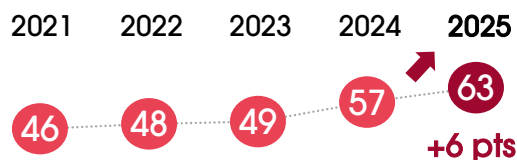
74%

des internautes estiment que les escroqueries sur internet sont de plus en plus fréquentes

Évolution



Évolution auprès des 15-24 ans



50-64 ans

81%

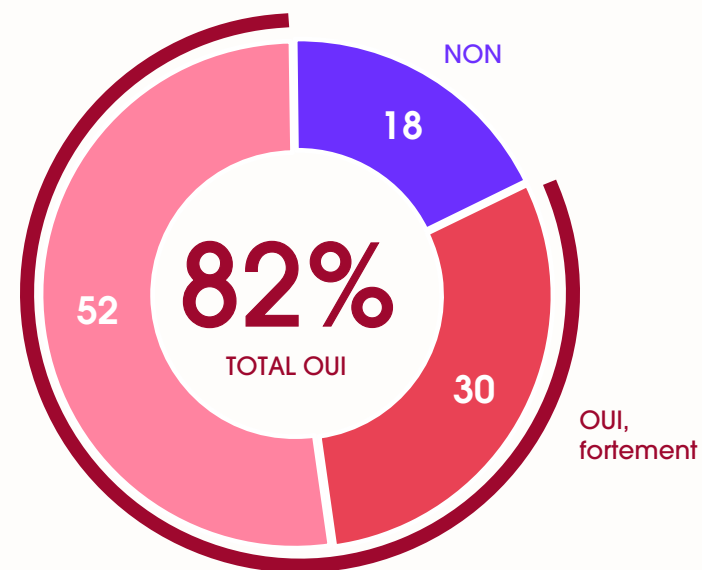
65 et +

83%

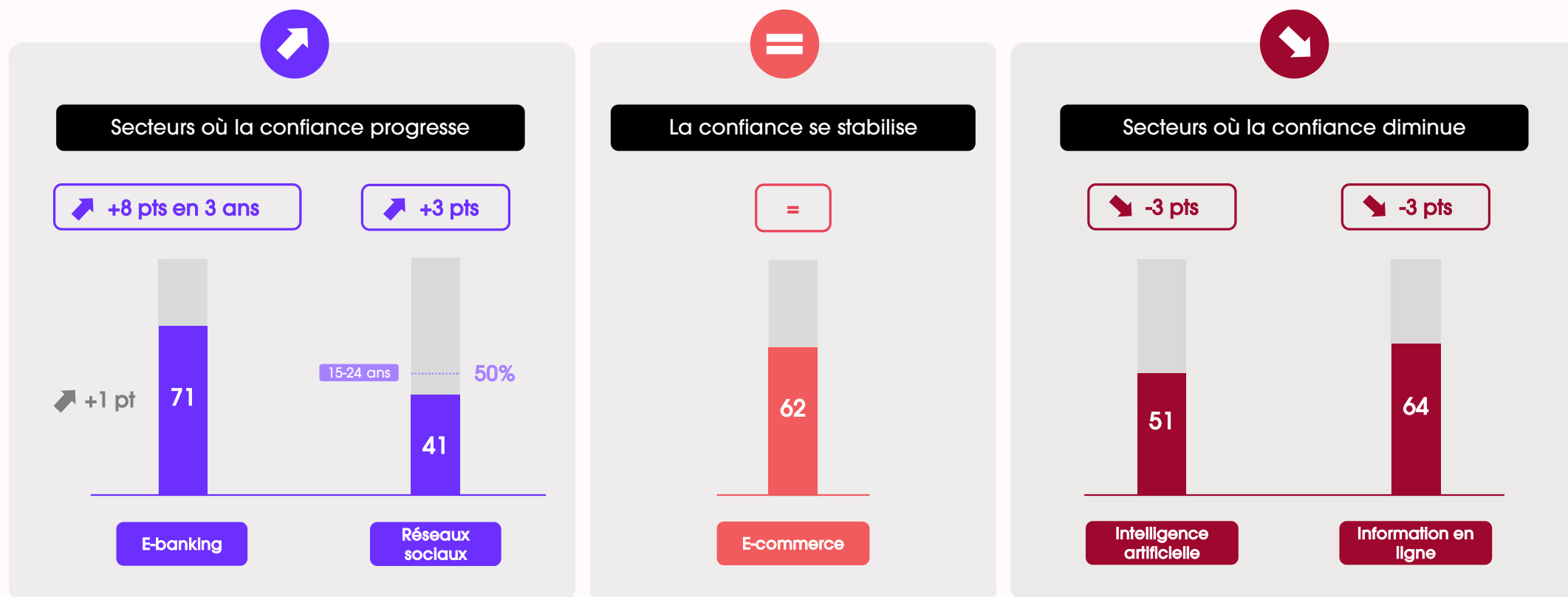
”

Les escroqueries en ligne dégradent la confiance

OUI,
un peu



Cette stabilité au global de la confiance s'accompagne de mouvements par secteur, certains en hausse, certains en baisse.



Base ensemble – en % (Hors ne sait pas)

Q30. Pensez-vous qu'il est risqué de consulter ses comptes bancaires sur Internet ou applications mobiles ?

Q35. Pensez-vous qu'il est risqué d'utiliser les réseaux sociaux ?

Q14. D'une manière générale, pensez-vous qu'il est risqué d'acheter sur Internet ?

Q203. De manière générale, avez-vous confiance ou non dans les techniques d'intelligence artificielle ?

Q551NEW. De manière générale, avez-vous confiance dans l'information que vous pouvez trouver en ligne ?

Les évolutions de la confiance sont souvent tirées par les non-utilisateurs : une confiance et une défiance qui reposent donc en partie sur l'imaginaire collectif et les idées reçues.



Le piratage des données, fléau de la confiance numérique : il s'affirme cette année comme le risque numéro un lié à l'usage du e-commerce et du e-banking.



Principal risque identifié

Acheter sur internet

Le piratage de mes données bancaires



54

➔ +7 pts

Être victime d'une malversation



41

L'usurpation de mon identité



35

Une mauvaise qualité du service



25

L'utilisation de mes données personnelles à des fins commerciales



23



Principal risque identifié

Consulter son compte bancaire sur internet

Que mon compte bancaire soit piraté



48

Le fait que mes données bancaires soient utilisées abusivement par quelqu'un d'autre



32

➔ -4 pts

Le fait que mes comptes bancaires puissent être consultés par quelqu'un d'autre



28

➔ -3 pts

Un mauvais fonctionnement du site ou de l'application



24

➔ +3 pts

L'utilisation de mes données personnelles et données de consommation à des fins commerciales



24

➔ -3 pts

Les craintes liées à la sécurité des données progressent également dans l'usage des réseaux sociaux.

38%



des internautes estiment que
les réseaux sociaux garantissent
suffisamment la protection des
données personnelles

Évolution totale OUI

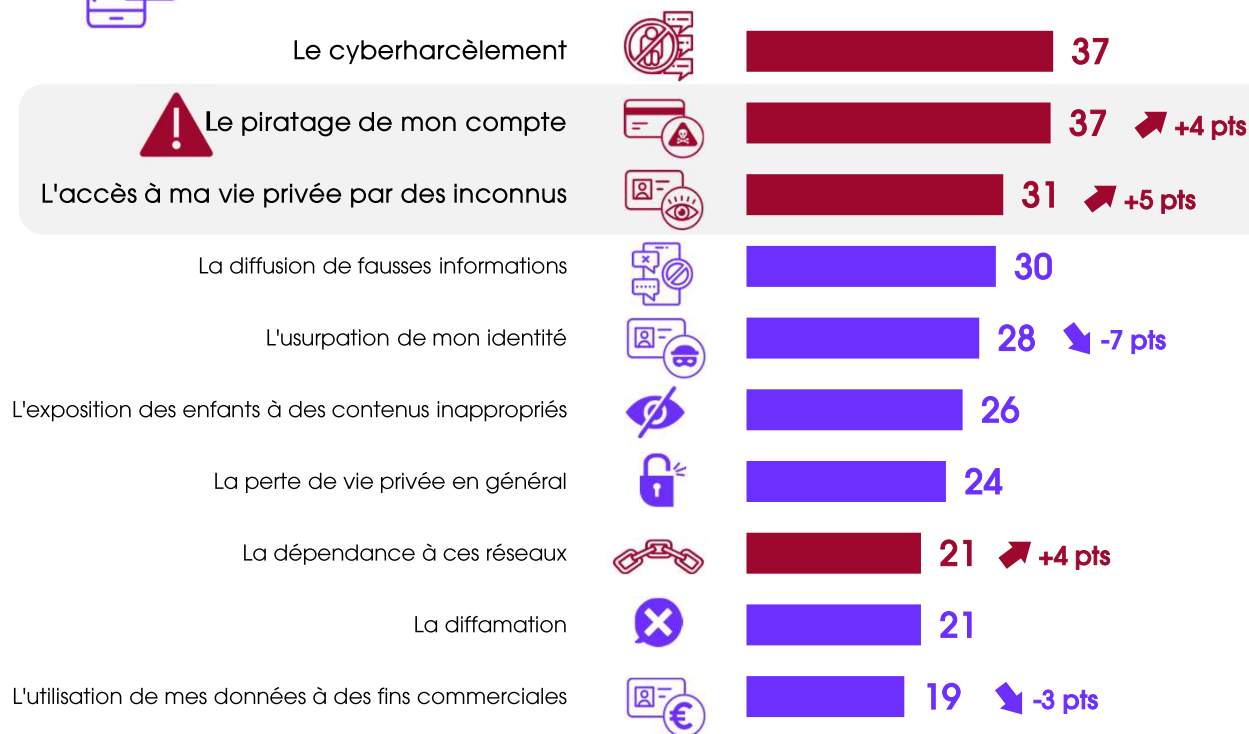
2016 2017 2019 2020 2021 2022 2023 2024 2025



↓ -5 pts



Principaux risques identifiés d'usage des réseaux sociaux



Base à ceux qui utilisent les réseaux sociaux (94%) – en %

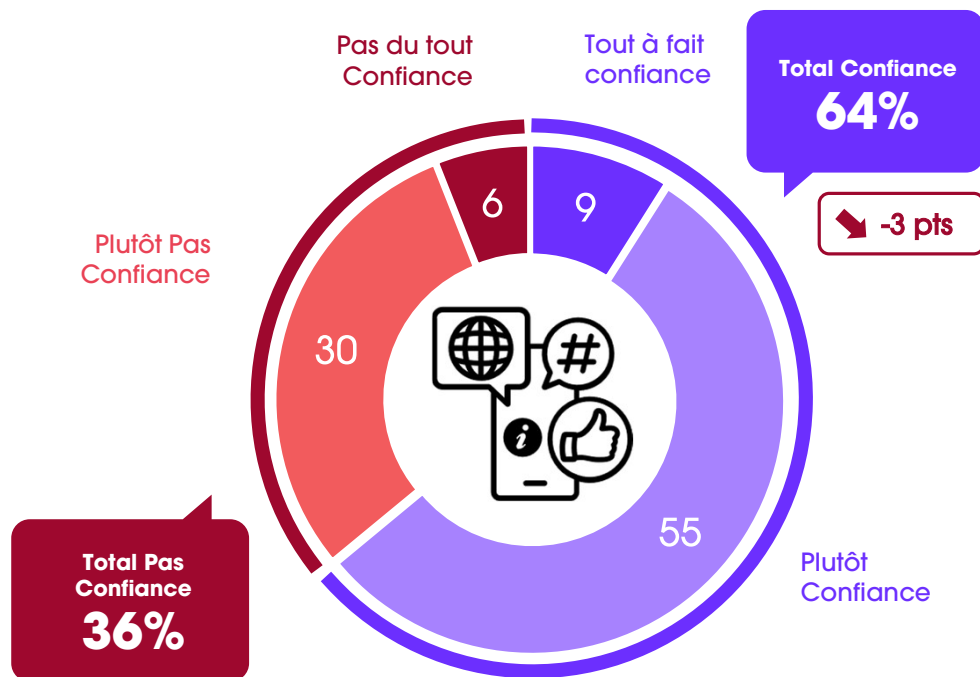
Q38. Estimez-vous que les réseaux sociaux garantissent suffisamment la protection des données personnelles (âge, adresse mail, préférences, photos, messages) que vous avez enregistrées sur le site ?

Base ensemble – en %

Q36. Selon vous, quels sont les risques d'utiliser les réseaux sociaux ? (5 réponses maximum)

La baisse de confiance dans l'information en ligne est de son côté très liée au risque fort de désinformation, et d'escroquerie.

Confiance dans l'information en ligne



Les 3 plus gros risques identifiés liés à l'information en ligne

La désinformation et les fake news			58
Les arnaques et escroqueries			40
La manipulation de l'opinion publique, par exemple lors d'élections			38



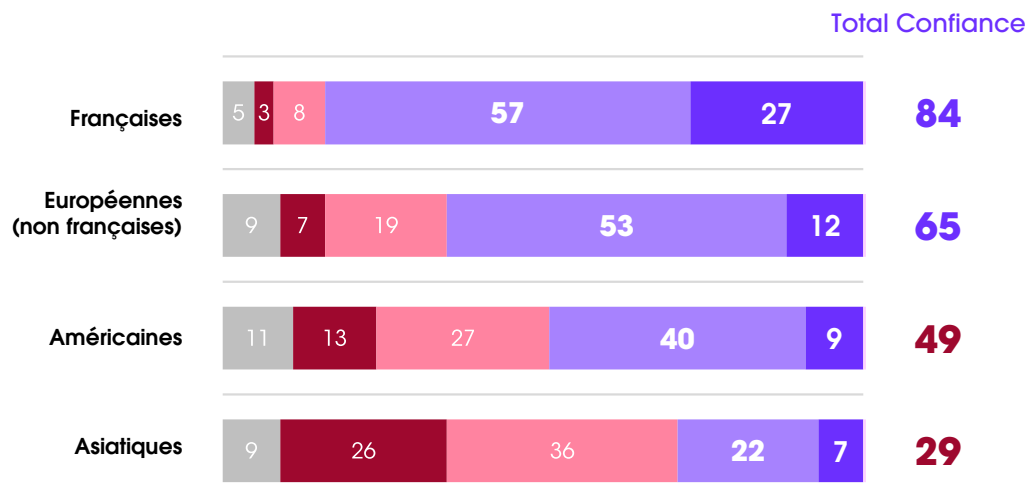
2. La clé de la confiance

**Des acteurs de confiance
et des outils de protection
qui ont fait leurs preuves.**

La confiance est nettement plus accordée aux plateformes françaises et aux sites des grandes enseignes, opérateurs télécoms et plateformes en ligne bien installés.

Confiance selon l'origine des plateformes

■ Ne sait pas ■ Pas du tout confiance ■ Plutôt pas confiance
■ Plutôt confiance ■ Tout à fait confiance



Confiance selon le site ou la plateforme d'e-commerce

Total Confiance



Sur le site de grandes enseignes qui ont des magasins en physique comme la Fnac, Darty, Carrefour, Auchan...

71

Sur des sites ou applis des opérateurs télécoms : Free, Orange, Bouygues, SFR

68

Sur des plateformes existant uniquement en ligne comme Amazon, Temu, Cdiscount, ManoMano...

67



Sur des sites de promotions / bons plans / ventes privées comme Veepee, Groupon, BazarChic, iGraal...

50

Sur des plateformes d'achat entre particuliers comme le Bon Coin, Vinted...

47

L'Etat et ses services au cœur de la consolidation de la confiance pour l'adoption d'un portefeuille d'identité numérique.

✓ 59%

des internautes se disent **prêts à passer à un portefeuille d'identité numérique...**



Mais ils n'accordent **pas la même confiance** à tous les acteurs pour **le stockage**



Acteurs privilégiés pour le stockage des documents d'identité numérique

L'État
(avec le service France Identité)



42

Votre banque



39

Une grande entreprise privée mondiale
Apple, Google, Facebook, Microsoft.



13

Même constat en ce qui concerne la certification de l'identité numérique : la confiance se porte surtout sur l'Etat.

✓ 69%

des internautes déclarent que disposer d'un compte unique d'identification en ligne **certifié par l'Etat** leur donnerait **davantage confiance pour effectuer les démarches en ligne.**



Confiance selon le service pour certifier l'identité numérique

■ Pas du tout confiance ■ Plutôt pas confiance ■ Plutôt confiance ■ Tout à fait confiance

Une identité numérique certifiée par l'État (ex : France Identité)
ou un service de l'État (ex : ameli.fr, impots.gouv.fr)



Une identité numérique certifiée par l'ANSSI
(Agence nationale de la sécurité des systèmes d'information)
(ex : Identité Numérique La Poste, YRIS, France Identité)



Une identité numérique passant par un système
fourni par votre établissement bancaire (ex : B. Connect)



Une identité numérique fournie par un acteur mondial
(ex : Facebook, Google, Apple etc.)



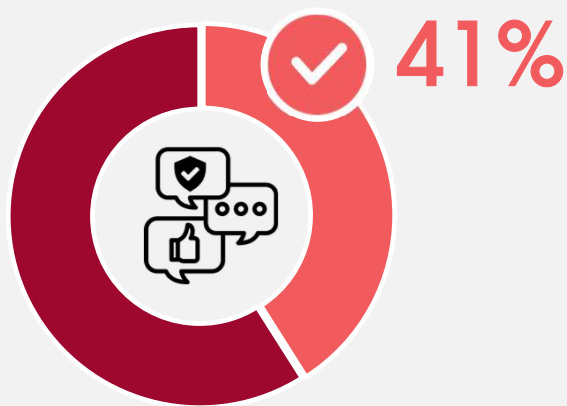
Base ensemble – en %

Q44bis. Est-ce que le fait de disposer d'un compte unique d'identification en ligne certifié par l'Etat (comme France Connect) pour l'ensemble de vos démarches en ligne auprès des administrations vous donnerait davantage confiance pour effectuer ces démarches en ligne ?

Q507bis. Et faites-vous confiance à chacun des services suivants pour certifier l'identité numérique d'un utilisateur ?

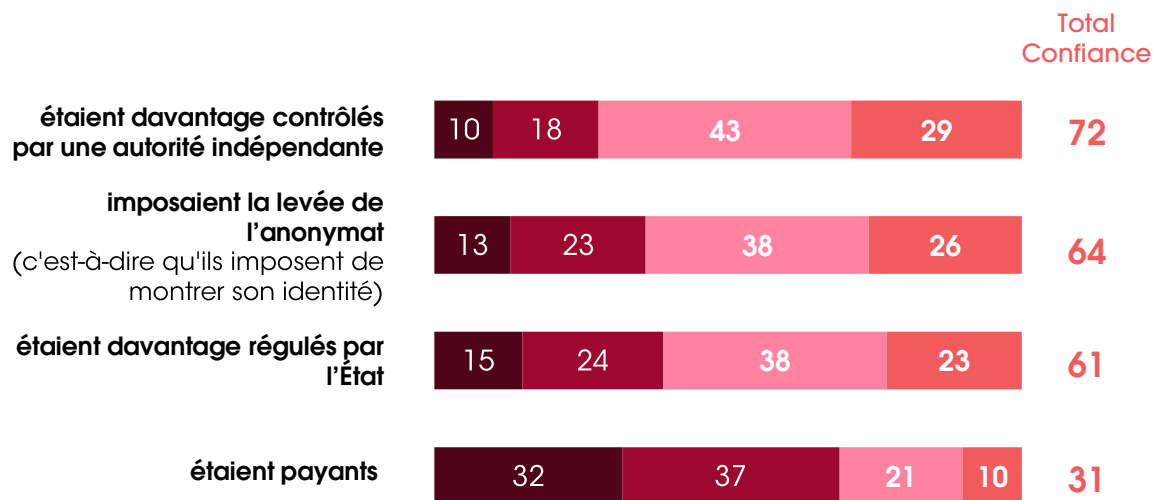
De même, concernant l'usage des réseaux sociaux, la confiance pourrait être renforcée par le contrôle d'une autorité indépendante ou la régulation de l'Etat.

RAPPEL :
Confiance dans l'usage
des réseaux sociaux



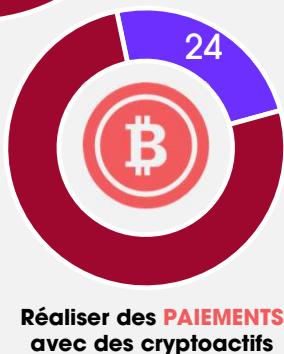
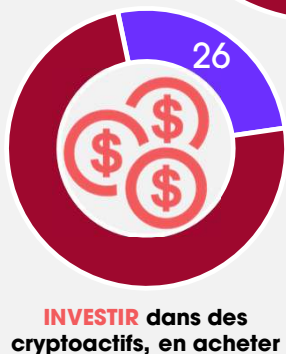
Leviers de la confiance dans les réseaux sociaux, s'ils...

■ Non pas du tout ■ Non, plutôt pas ■ Oui, plutôt ■ Oui, tout à fait

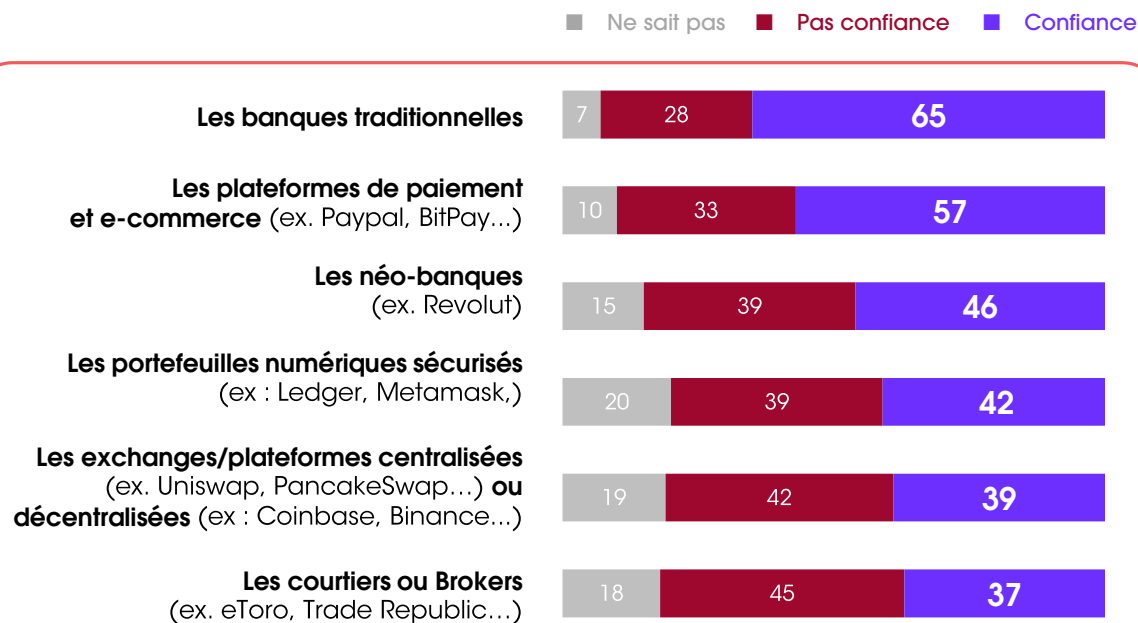


Les banques traditionnelles et les plateformes de paiement en ligne sont les plus propices à se voir accorder la confiance des non-réfractaires pour des opérations liées aux cryptoactifs.

26%
CONFIANCE
dans les
cryptoactifs*



Confiance dans les acteurs pour réaliser les opérations liées aux cryptoactifs



* Pour la vague de 2025, le terme cryptomonnaie a été remplacé par cryptoactif

Pour lutter contre le piratage des données, l'authentification forte et les outils de cybersécurité sont plébiscités, à l'inverse de solutions faisant appel au machine learning et à l'IA.

Moyens pour lutter contre l'escroquerie en ligne

	La mise en place de l'authentification forte	Total Efficace 68
	Le développement de solutions de cybersécurité	61
	Le développement de l'authentification par reconnaissance faciale ou empreinte digitale	59
	Le développement des identités numériques (France Identité, Google, Facebook, Identité Numérique La Poste...)	58
	Les plateformes pour signaler en ligne les sites malveillants, les listes noires de spameurs ou sites frauduleux	57
	L'information des consommateurs	56
	Les modules de formation / de sensibilisation aux risques sur Internet	54
	Le développement de solutions technologiques d'analyse du risque grâce à la data, au machine learning et à l'IA	46

Moyens de paiement les plus sécuritaires

TOP 5		Total Confiance
1	 Avec double authentification	68
2	 En ligne avec un numéro de carte bancaire à usage unique	61
3	 Sans contact via sa carte en magasin sur un terminal de paiement électronique (TPE)	53
4	 Avec empreinte digitale	52
5	 Par reconnaissance faciale	50

Les outils de cybersécurité sont même un des principaux leviers de la confiance dans les pratiques sur Internet, aux côtés des garanties financières, techniques et réglementaires.

Leviers de la confiance numérique (top 4)



ACSEL

* toluna



3. Intelligence artificielle

Avec l'usage qui s'étend,
une défiance et des inquiétudes

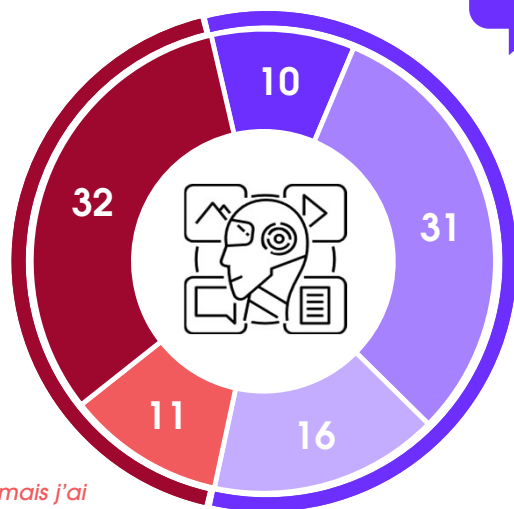


L'usage de l'IA générative est en hausse croissante depuis deux ans, tout comme la capacité à reconnaître les contenus d'IA générative.

Usage de l'intelligence artificielle générative

Oui tous les jours ou presque

Total OUI
57%

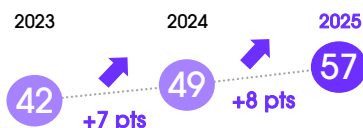


Oui quand l'occasion se présente

Non, mais j'ai l'intention de le faire

Oui une fois pour essayer

Usage de l'IA générative (évolution)



15-24 ans **87**

25-34 ans **84**

Contenus d'IA générative auxquels les internautes ont été confrontés

Des images, des vidéos, de la musique générés par de l'IA générative



45

➔ +10 pts

Des textes générés par de l'IA générative



43

➔ +6 pts

Je saurais reconnaître ce type de contenus



63

➔ +11 pts

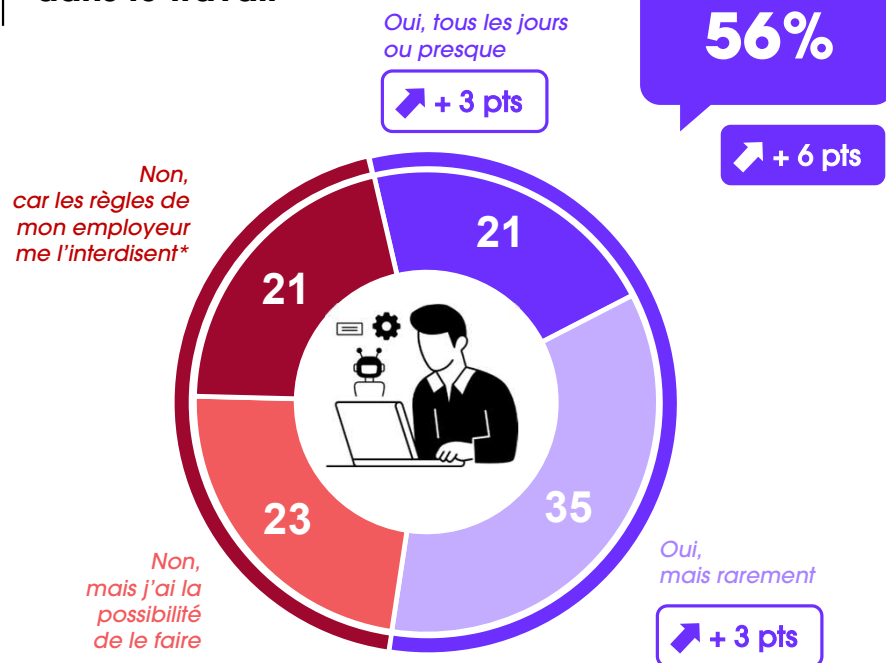
Base ensemble - en %

Q545 - Avez-vous déjà eu recours à de l'intelligence artificielle générative (création de texte, d'images, de vidéos, de musique, de présentation, de voix, de résumés, de codes ou d'objets 3D, demande de conseil, etc.) ?

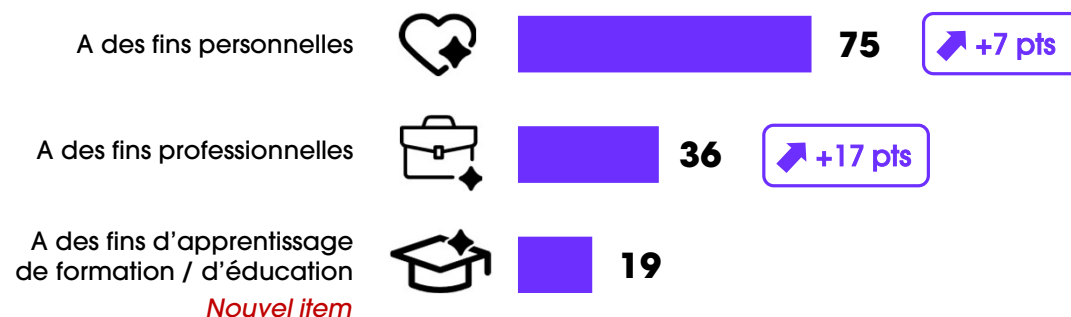
Q544 - Avez-vous déjà été confronté(e) à des contenus générés par de l'IA générative ?

La hausse du recours à l'IA et plus spécifiquement à l'IA générative se retrouve particulièrement dans les usages professionnels.

Utilise des outils / solutions faisant appel à l'IA dans le travail



Usages de l'IA générative



Cette hausse de l'usage de l'IA générative s'accompagne d'une perception grandissante d'un danger pour l'emploi en général.

Perception de l'IA générative



UN DANGER

Base ensemble – en %

...pour l'emploi

67

↗ +7 pts

Base aux actifs – en %

...pour votre emploi

42

UNE OPPORTUNITÉ



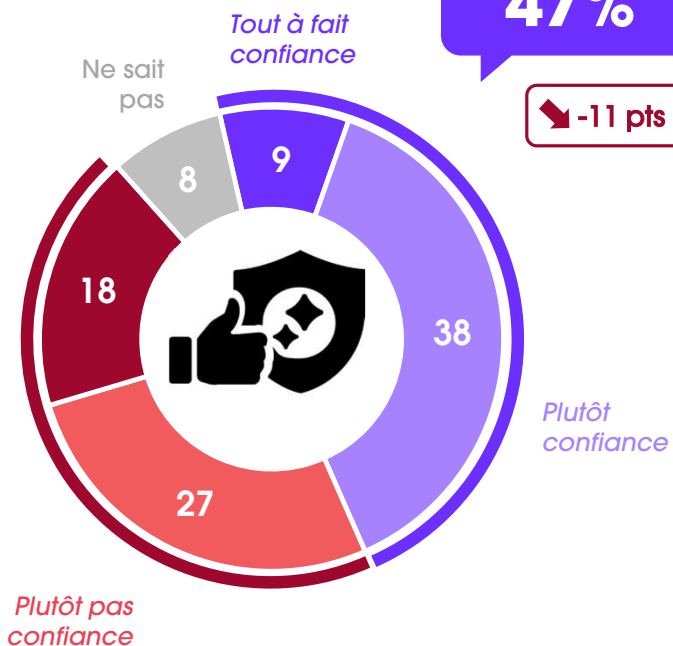
44

↘ -3 pts

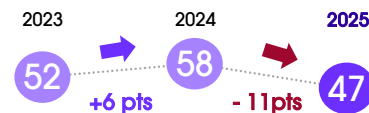
47

La confiance envers la qualité des contenus générés par les outils d'IA générative se réduit fortement : elle est désormais minoritaire.

Confiance dans le contenu créé par l'IA générative



Confiance (évolution)



Confiance selon les usages

À des fins d'informations



47

À des fins d'éducation



46

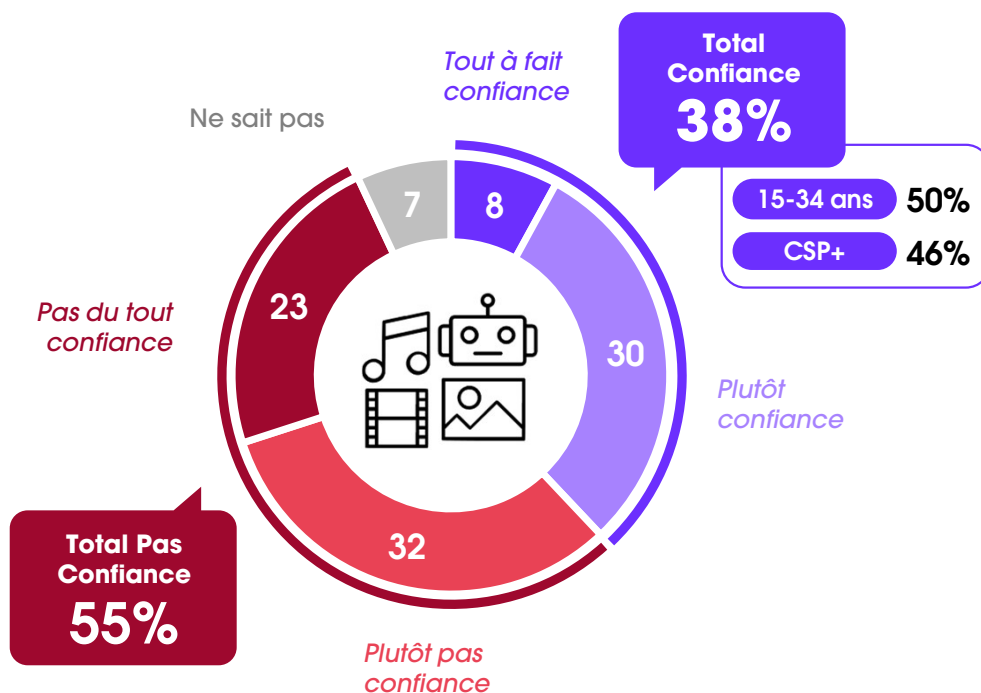
À des fins commerciales ou publicitaires



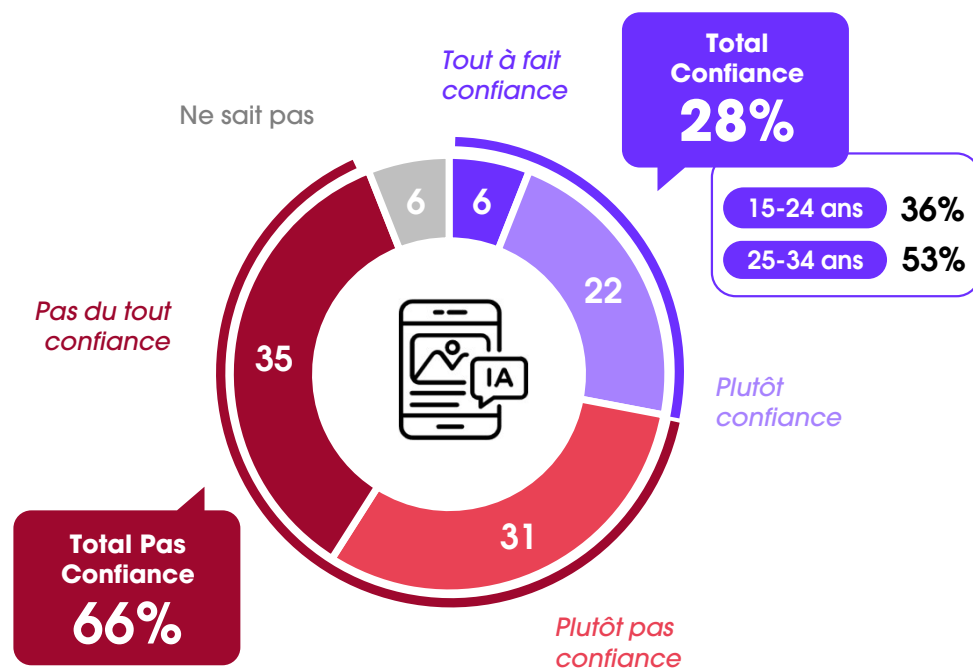
44

L'usage croissant de l'IA générative met aussi en péril la confiance accordée aux contenus que l'on trouve dans les médias et surtout sur les plateformes ou réseaux sociaux.

Dans les médias

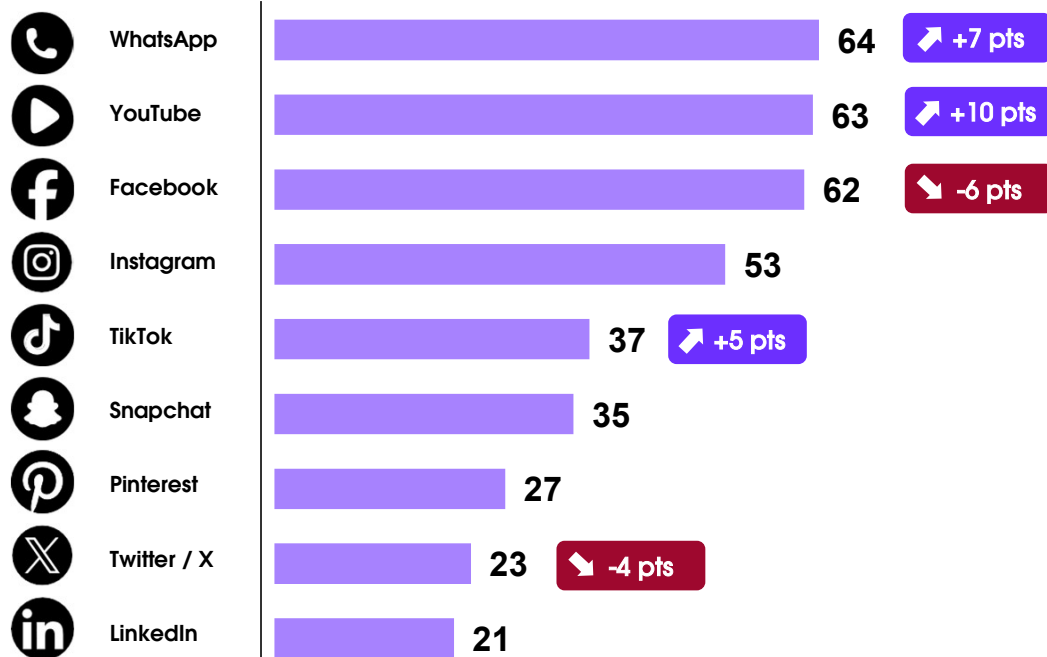


Sur les plateformes ou réseaux sociaux

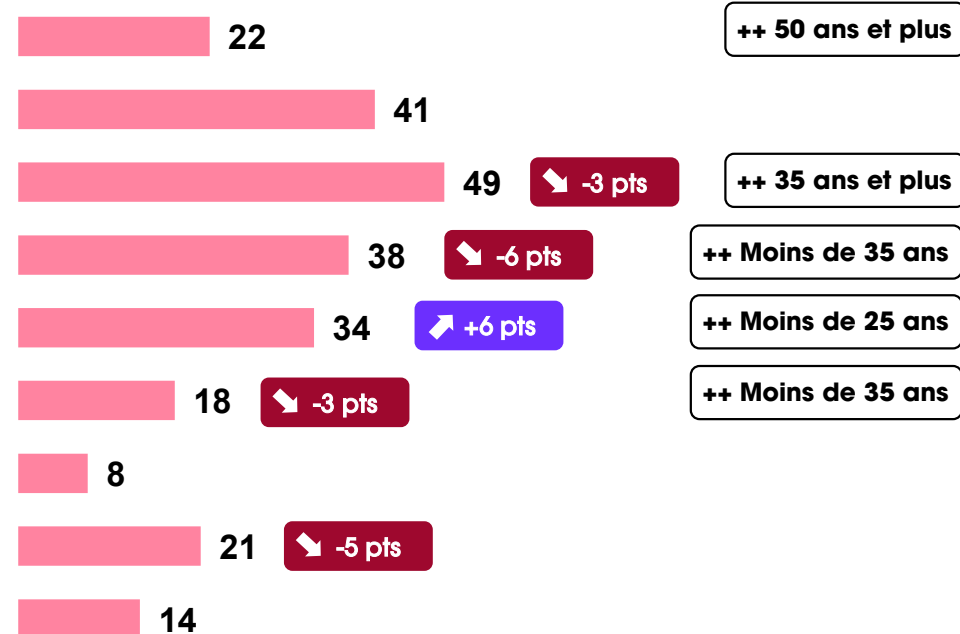


Dans un contexte où les plateformes utilisées pour s'informer évoluent fortement ...

Plateformes les plus utilisées

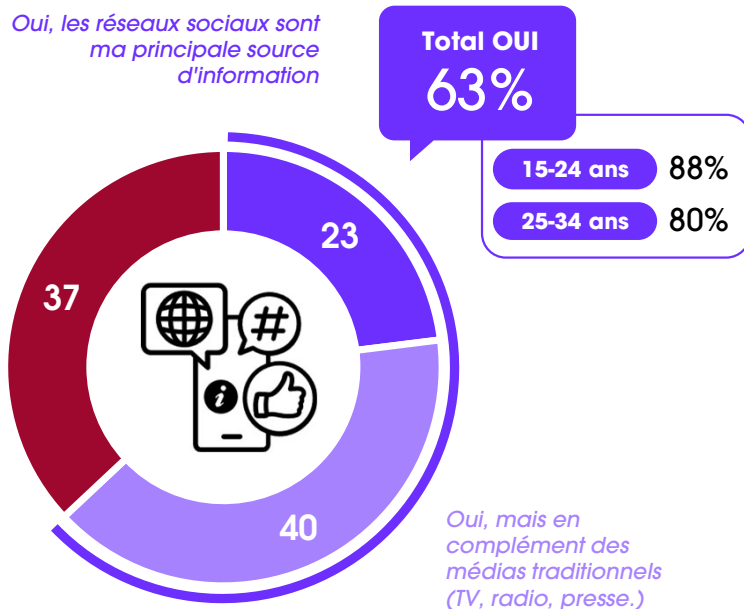


Plateformes utilisées pour s'informer

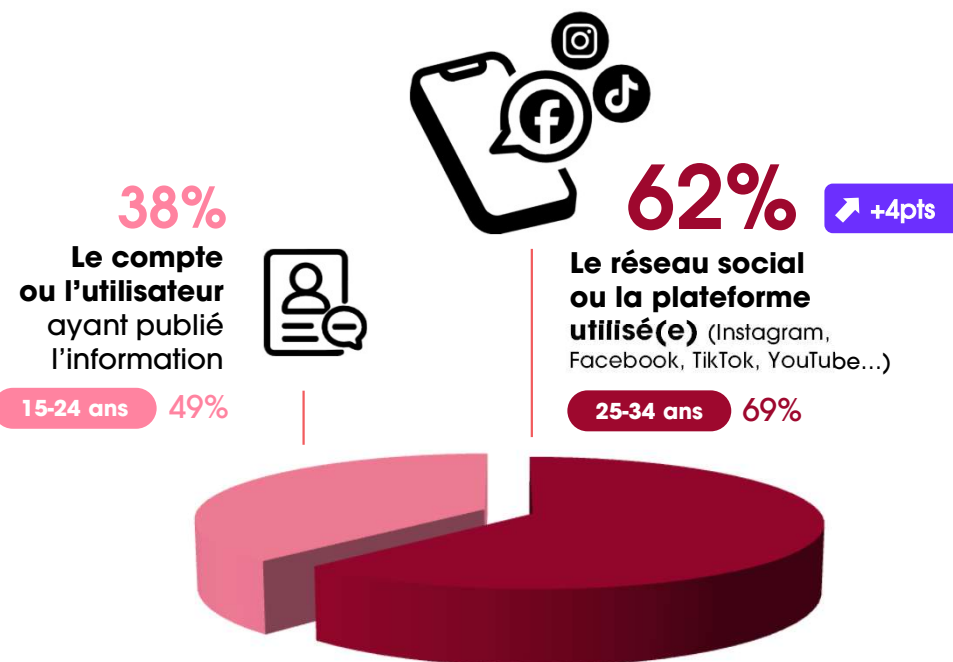


... et où la majorité des internautes déclarent aujourd'hui s'informer sur les réseaux sociaux, et même un quart d'entre eux exclusivement sur ces derniers.

S'informer via les réseaux sociaux



Critère de choix principal de la source d'information



ACSEL

* toluna

13^e
ÉDITION

Baromètre de la confiance des Français dans le numérique

