ODOXA

L'Opinion tranchée

Le rendez-vous de l'innovation

La sécurité et la surveillance en ligne

LEVÉE D'EMBARGO : JEUDI 13 MAI 2021 À 6H

Sondage réalisé pour LEYTON dentsu CONSULTING BFM BUSINESS L'USINE NOUVELLE Stratégies 01net

Méthodologie

Recueil

Enquête réalisée auprès d'un échantillon de Français interrogé par Internet les 5 et 6 mai 2021.

Echantillon

Echantillon de 1 005 personnes représentatif de la population française âgée de 18 ans et plus.

La représentativité de l'échantillon est assurée par la méthode des quotas appliqués aux variables suivantes : sexe, âge, niveau de diplôme et profession de l'interviewé après stratification par région et catégorie d'agglomération.

ODOXA
L'Opinion tranchée

Précisions sur les marges d'erreur

Chaque sondage présente une incertitude statistique que l'on appelle marge d'erreur. Cette marge d'erreur signifie que le résultat d'un sondage se situe, avec un niveau de confiance de 95%, de part et d'autre de la valeur observée. La marge d'erreur dépend de la taille de l'échantillon ainsi que du pourcentage observé.

	Si le pourcentage observé est de …					
Taille de l'Echantillon	5% ou 95%	10% ou 90%	20% ou 80%	30% ou 70%	40% ou 60%	50%
200	3,1	4,2	5,7	6,5	6,9	7,1
400	2,2	3,0	4,0	4,6	4,9	5,0
500	1,9	2,7	3,6	4,1	4,4	4,5
600	1,8	2,4	3,3	3,7	4,0	4,1
800	1,5	2,5	2,8	3,2	3,5	3,5
900	1,4	2,0	2,6	3,0	3,2	3,3
1 000	1,4	1,8	2,5	2,8	3,0	3,1
2 000	1,0	1,3	1,8	2,1	2,2	2,2
3000	0,8	1,1	1,4	1,6	1,8	1,8

Lecture du tableau : Dans un échantillon de 1000 personnes, si le pourcentage observé est de 20%, la marge d'erreur est égale à 2,5%. Le pourcentage réel est donc compris dans l'intervalle [17,5 ; 22,5].

ODOXA
L'Opinion tranchée

Principaux enseignements

L'œil du sondeur : Emile Leclerc, directeur d'études

Sécurité : 61% des Français estiment que la France n'utilise pas assez le digital

1) Un Français sur deux (49%) poste des contenus ou envoie des documents sensibles sur sa vie privée, des pratiques particulièrement répandues chez les plus jeunes (72%).

2) 68% des salariés pensent que leur employeur n'a pas le droit d'examiner les contenus de leurs outils professionnels et 27% se sentent parfois surveillés par leurs supérieur.

3) 61% des Français jugent que la France n'a pas suffisamment recours aux outils numériques dans ses politiques de sécurité.

4) Les Français souhaitent l'usage des drones (66%), algorithmes de surveillance (52%) voire reconnaissance faciale (50%).

5) Cybersécurité : les Français attendent un financement de l'Etat (71%) et une obligation de s'assurer pour les entreprises (67%).

Synthèse détaillée du sondage *(1/3)*

L'œil du sondeur : Emile Leclerc, directeur d'études

Sécurité : 61% des Français estiment que la France n'utilise pas assez le digital

1) Un Français sur deux (49%) poste des contenus ou envoie des documents sensibles sur sa vie privée, des pratiques particulièrement répandues chez les plus jeunes (72%).

L'émergence à la démocratisation des outils numériques a produit une révolution sans précédent dans l'histoire de l'humanité. La vie privée et les informations personnelles sont devenues accessibles à tous. Nous ne parlons pas ici de piratage de ces contenus mais bien de ceux que les individus diffusent eux-mêmes. Et le phénomène est massif.

Un Français sur deux déclare ainsi poster des contenus ou envoyer des documents sensibles.

La pratique la plus courante consiste à poster des photos de soi-même ou de ses proches ou encore d'indiquer les lieux où l'on se trouve en vacances : 36% de nos concitoyens le font. Les cambrioleurs raffolent de ces informations leur permettant de savoir quand les habitants d'un logement sont absents.

La dématérialisation de nombreux documents administratifs pousse aussi 23% d'entre eux à envoyer des informations sensibles à des contacts qu'ils connaissent peu. Il peut par exemple s'agir d'une pièce d'identité pour un dossier de logement. Les usurpations d'identité sont devenues plus aisées à cause de ce manque de vigilance.

Enfin, 16% des Français nous confient fournir des données de carte bancaire à des sites dans lesquels ils n'ont pas totalement confiance.

Notons que plus les Français sont jeunes, plus ces pratiques sont répandues : 72% des 18-24 ans sont concernés pour seulement 30% des 65 ans et plus.

Synthèse détaillée du sondage *(2/3)*

L'œil du sondeur : Emile Leclerc, directeur d'études

2) 68% des salariés pensent que leur employeur n'a pas le droit d'examiner les contenus de leurs outils professionnels et 27% se sentent parfois surveillés par leurs supérieur.

La loi est claire. L'employeur peut parfaitement consulter les historiques de navigation de l'ordinateur ou du smartphone professionnel mais il est interdit d'avoir recours à des techniques permettant d'automatiser ce procédé. Il en va de même pour les mails, dossiers et fichiers à moins que l'employé ait précisé qu'il s'agit d'un élément à caractère privé.

Et pourtant, les deux tiers des salariés français (68%) pensent que leur employeur n'a pas le droit d'examiner les contenus se trouvant sur un outil professionnel.

Dans les faits, ce type de surveillance reste minoritaire mais ce loin d'être inexistante : 27% des salariés déclarent se sentir parfois surveillés par leur employeur, leur manager ou une personne de la direction informatique.

3) 61% des Français jugent que la France n'a pas suffisamment recours aux outils numériques dans ses politiques de sécurité.

Les outils numériques sont devenus des mines d'informations pour les services de renseignements et les forces de l'ordre, en amont, comme en aval. Ils peuvent leur permettre de déjouer un attentat, de surveiller des individus suspects mais aussi de remonter une filière et d'apporter des preuves à la justice.

Mais aujourd'hui, les Français estiment que la France n'y a pas suffisamment recours. 61% d'entre eux et plus particulièrement les plus âgés (80%) affirment ainsi que la France n'utilise pas assez les outils de surveillance numérique dans ses politiques de sécurité.

Ces outils posent évidemment des questions éthiques qu'il ne s'agit pas de négliger. Les Français, dans nos enquêtes, affirment plus souvent leur penchant pour davantage de sécurité quitte à rogner sur les libertés individuelles, tout en adressant une injonction paradoxale aux autorités : ils ne comprennent pas que certains individus malveillants « passent entre les mailles du filet » tout en rejetant la surveillance de masse car ils ne veulent pas être espionnés individuellement.

Synthèse détaillée du sondage *(3/3)*

L'œil du sondeur : Emile Leclerc, directeur d'études

4) Les Français souhaitent l'usage des drones (66%), algorithmes de surveillance (52%) voire reconnaissance faciale (50%).

Parmi les outils de surveillance, les drones permettant d'assurer la sécurité de sites sensibles sont ceux qui recueillent le plus d'approbation dans la population : 66% des Français souhaitent leur usage.

Ils souhaitent aussi que la France ait recours aux algorithmes de surveillance des sites internet consultés (52%), comme le prévoit la loi terrorisme.

Ils sont partagés à l'égard de la reconnaissance faciale. 50% des Français y sont favorables, 49% y sont opposés.

Ils rejettent en revanche majoritairement le principe d'intercepter les conversations en ligne, sur les réseaux sociaux, les messageries, les mails ou encore sur les sites de jeux (55% ne souhaitent pas son usage).

Enfin, les deux tiers d'entre eux ne souhaitent pas que la France ait recours aux logiciels mouchards (65%).

5) Cybersécurité : les Français attendent un financement de l'Etat (71%) et une obligation de s'assurer pour les entreprises (67%).

Les annonces d'attaques informatiques contre des multinationales, des entreprises de toutes tailles, des hôpitaux ou tout type de structure se multiplient ces derniers mois.

Face à ce phénomène, les Français estiment que l'Etat doit intervenir. Ils sont très majoritairement favorables à deux principes.

71% d'entre eux soutiennent l'idée de subventions et de financement de l'Etat pour aider les entreprises à mieux s'équiper en outils de cybersécurité.

Ils considèrent aussi que la loi devrait obliger les entreprises à souscrire une assurance contre les cyberattaques ; 67% y sont favorables.

Emile Leclerc, directeur d'études

L'œil de l'expert *(1/2)*

Téoman Atamyan, Directeur Innovation du groupe Leyton

1°) Face à l'insouciance des jeunes, l'évangélisation de la cyber sécurité doit redoubler

Les 18-24 ans sont les moins vigilants lorsqu'il s'agit de poster des éléments relatifs à la vie privée sur internet ou les réseaux sociaux. 72% postent sans se méfier contre 49% pour l'ensemble des sondés. Une telle insouciance chez ceux qui devraient être les plus concernés pose question.

L'évangélisation de la cyber sécurité doit donc redoubler, pour changer les comportements. Premières concernées, les entreprises doivent s'en emparer. Comment en effet celui qui ne protège pas ses données personnelles pourrait-il être attentif à la sécurité digitale dans son activité professionnelle…

D'autant qu'avec la 5G et les IOT, les cyberattaques auront demain encore plus d'impact sur notre intégrité physique. Les salariés d'ailleurs ne souhaitent pas (à 68%) que leur employeur puisse examiner les contenus sur leur téléphone ou leur ordinateur, et près d'un sur trois (27%) se sent même surveillé.

Il est paradoxal bien sûr de vouloir être protégé tout en continuant à poster sans se soucier.

L'enjeu est donc culturel. C'est pourquoi l'éducation nationale travaille sur l'intégration de programmes cyber, et ce dès le collège, mais il faut aller plus vite et c'est l'entreprise qui aujourd'hui peut instaurer un vrai « réflexe » cyber sécurité.

2°) Les Français veulent plus de surveillance numérique, une aubaine pour l'innovation

En plein débat passionnel sur le projet de loi « relatif à la prévention d'actes de terrorisme et au renseignement », une majorité de Français souhaitent un recours plus important aux outils de surveillance numérique dans les politiques de sécurité. 61% des sondés estiment en effet que la France ne les utilise pas assez.

Toutefois le sujet -qui touche à l'utilisation d'outils intrusifs- divise clairement. 52% des sondés souhaitent ainsi que le pays recoure aux algorithmes de surveillance des sites internet consultés, mais 47% sont contre. 50% soutiennent le recours à la reconnaissance faciale, mais 49% sont contre. Et 65% sont contre l'utilisation des logiciels mouchards, 33% pour.

L'œil de l'expert *(2/2)*

Téoman Atamyan, Directeur Innovation du groupe Leyton

Les outils digitaux pour contrer la menace sécuritaire rassurent, ou font peur. Normal, la cyber guerre est une réalité. Depuis la déclaration en janvier 2020 de la ministre de la Défense Florence Parly, le cyber est désormais une « arme » que la France pourrait utiliser à des « fins offensives ».

Dans ce contexte, les entreprises qui développent ce type de technologies ont donc un boulevard devant elles. Nous le constatons au quotidien chez nos clients de la Tech, les défis sécuritaires à relever boostent déjà l'innovation. Pour les particuliers comme les entreprises, les systèmes intelligents de détection de fraudes ou de crimes bénéficient désormais de technologies très avancées d'Intelligence Artificielle, de Machine Learning, ou encore de Big Data.

3°) Face aux ravages potentiels des attaques, les entreprises doivent davantage s'assurer

Sur un sujet aussi sensible une majorité s'en remet au régalien pour défendre le pays contre les cyberattaques : 71% des sondés souhaitent ainsi que l'État subventionne et finance l'accès aux outils de cyber sécurité pour les entreprises.

Il subventionne déjà indirectement ces technologies. Des investissements importants de R&D sont pris en charge via le Crédit Impôt Recherche -qui reste absolument déterminant pour nos entreprises- mais également via certaines subventions à l'innovation. La BPI a ainsi créé un appel à projets pour un concours Grand Défi cyber sécurité.

De même, une vaste majorité de Français (67%) souhaite également que la loi oblige les entreprises à souscrire des assurances contre les attaques. C'est là un sujet clé car l'Europe encaisse à peine 10% des primes d'assurances cyber dans le monde. La France perçoit ainsi moins de 100 millions d'euros sur un total de 4 milliards de primes encaissées.

Les entreprises sont trop souvent inconscientes de leur exposition. Un constat d'autant plus surprenant qu'en Grande Bretagne 99% des risques cyber assurés ont bien été indemnisés, selon l'association des assureurs britanniques. A méditer quand on sait que la France a connu en février 2020 son premier redressement judiciaire suite à une attaque informatique, celui de la société Lise Charmel.

Résonance sur les réseaux sociaux

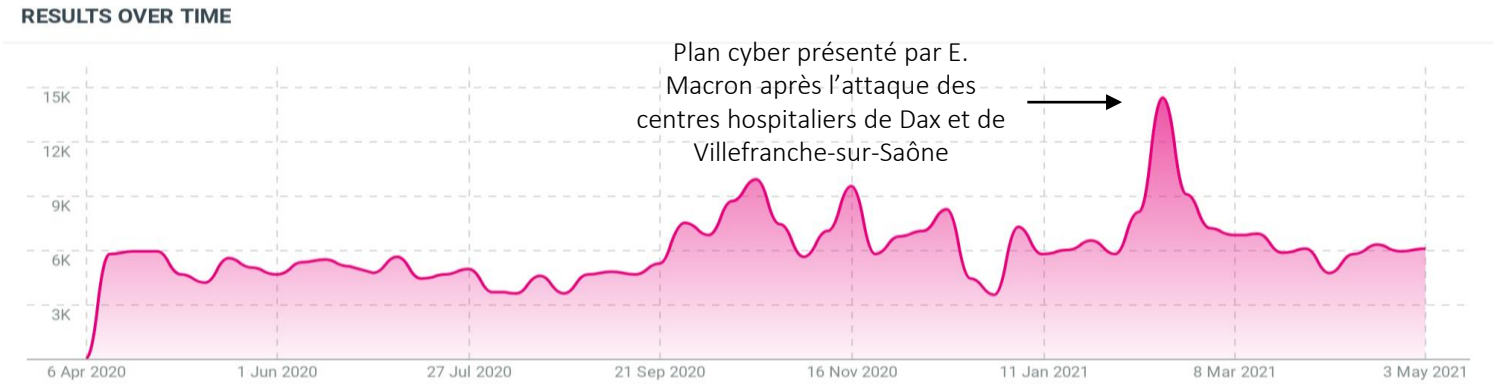
Benjamin Grange, Président de Dentsu Consulting

Les internautes sont de plus en plus matures vis-à-vis de l'usage d'Internet.

Si leurs pratiques sont encore parfois risquées, les Français sont de plus en plus matures en ligne. Et c'est une bonne nouvelle ! Les campagnes d'information qui mettent en avant les usages déviants d'internet (fake news, cyber harcèlement, piratage de carte bancaire, arnaque par ruse, actes inamicaux, rançongiciels …) et des réseaux sociaux ont porté leurs fruits. Les Français sont de plus en plus responsables dans leur usage au quotidien dans un monde où la technologie est davantage intégrée à nos vies. Ils partagent leurs « bonne pratiques » sur les réseaux sociaux et se renseignent pour se protéger. D'ailleurs, le sujet de la cybersécurité est un thème récurrent des conversations des Internautes, témoins plus de 340 000 conversations en français en 13 mois.

Conséquence de cette montée en maturité, **l'exigence des Français vis-à-vis du rôle régalien de l'Etat progresse.** Si l'État a le devoir d'assurer la sécurité des personnes, des biens et des prérogatives de la République, les Français expriment clairement que cette obligation s'étend aussi sur Internet. A l'heure où la criminalité de masse se développe sur Internet, les Français acceptent que leur sécurité passe par le déploiement par l'Etat d'outils technologiques plus élaborés. Si cela se confirme, c'est un vrai changement qui est en train de s'opérer dans les mentalités des français.

341K MENTIONS EN FRANÇAIS SUR LES 13 DERNIERS MOIS SUR LE SUJET DE CYBERSÉCURITÉ :

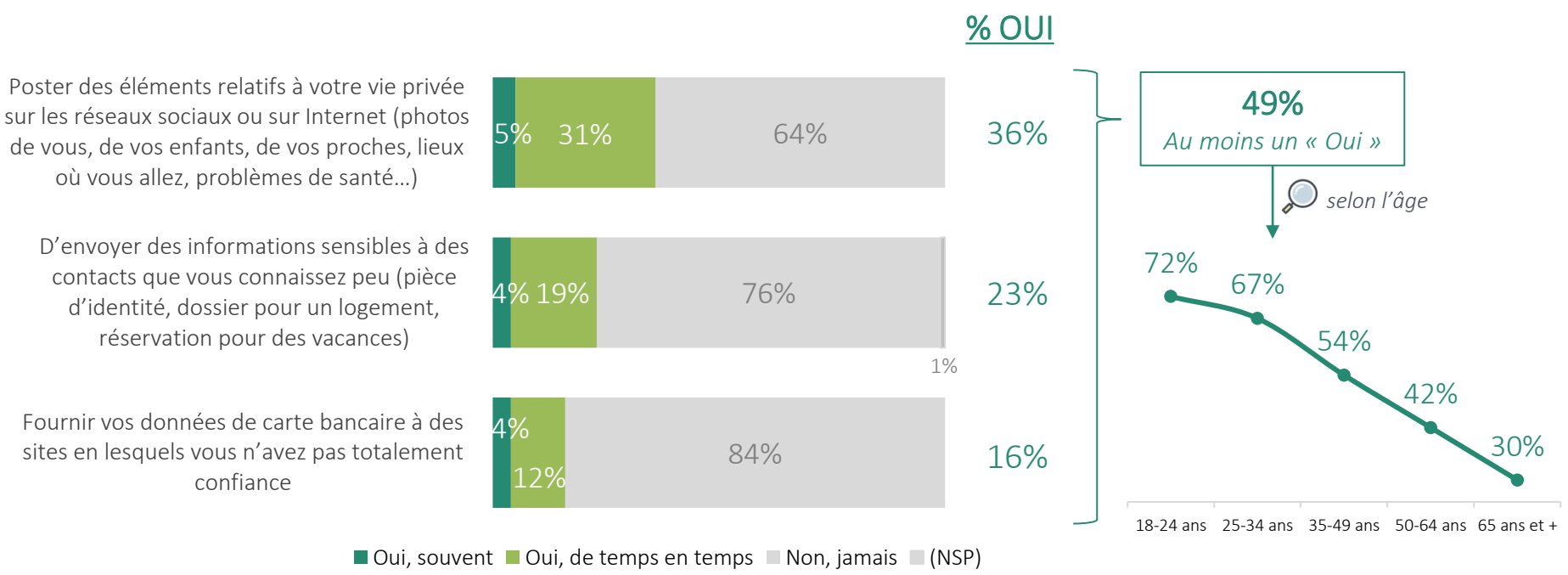


Source : Talkwalker, Analyse : Dentsu Consulting

Résultats du sondage

Actions réalisées sur Internet ou les réseaux sociaux

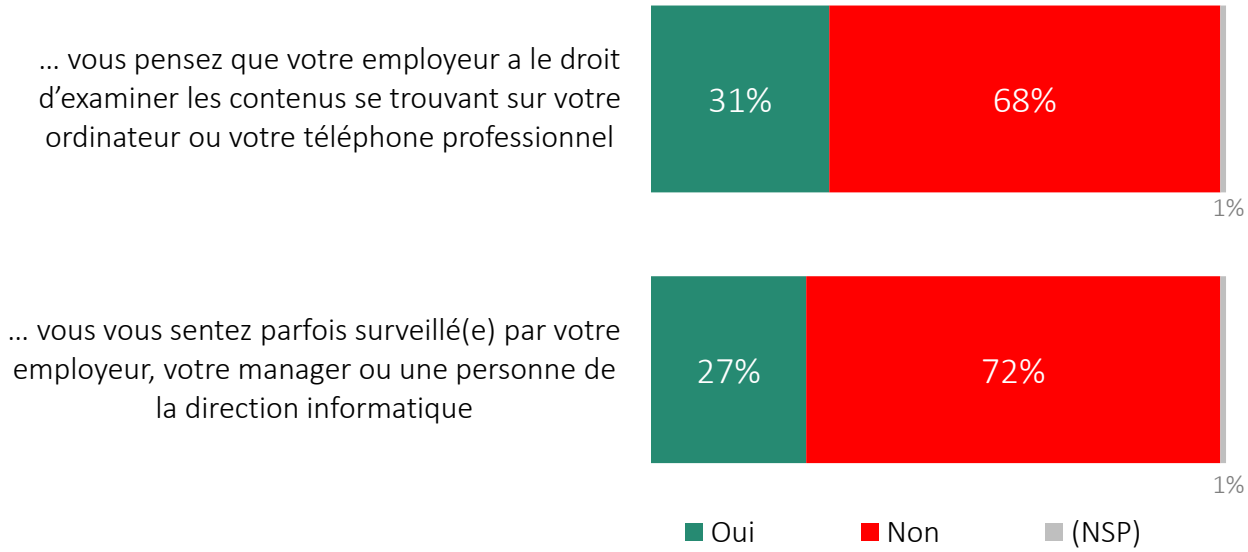
Vous-même, vous arrive-t-il de …



Regard porté sur la vie numérique personnelle sur les outils fournis par l'employeur

Aux salariés :

S'agissant des informations et de votre vie numérique personnelle sur des outils fournis par votre employeur (ordinateur, smartphone…), dites-nous si …



Emploi des outils de surveillance numériques dans les politiques de sécurité

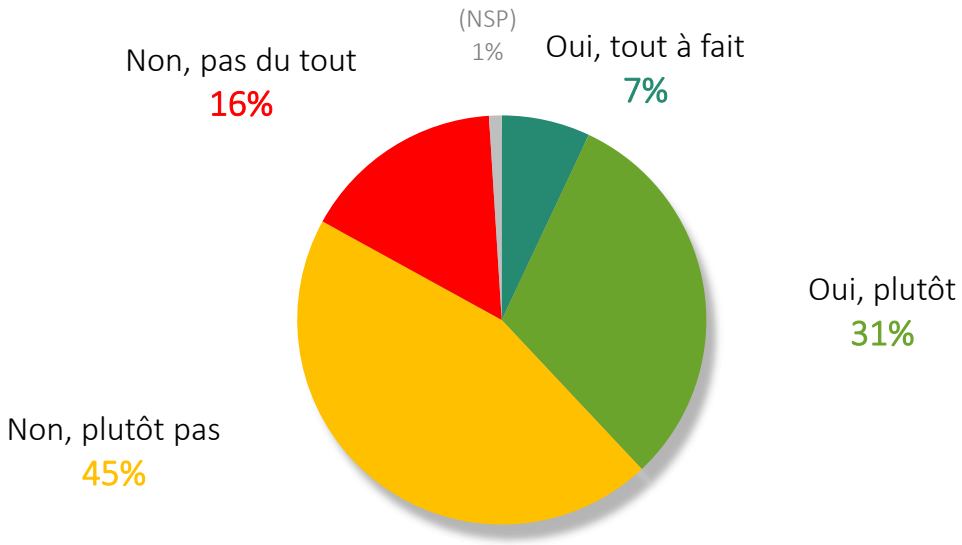
Pour vous, la France utilise-t-elle suffisamment les outils de surveillance numériques dans ses politiques de sécurité ?

% Non : 61%

65 ans et + : 80% / 25-34 ans : 45%

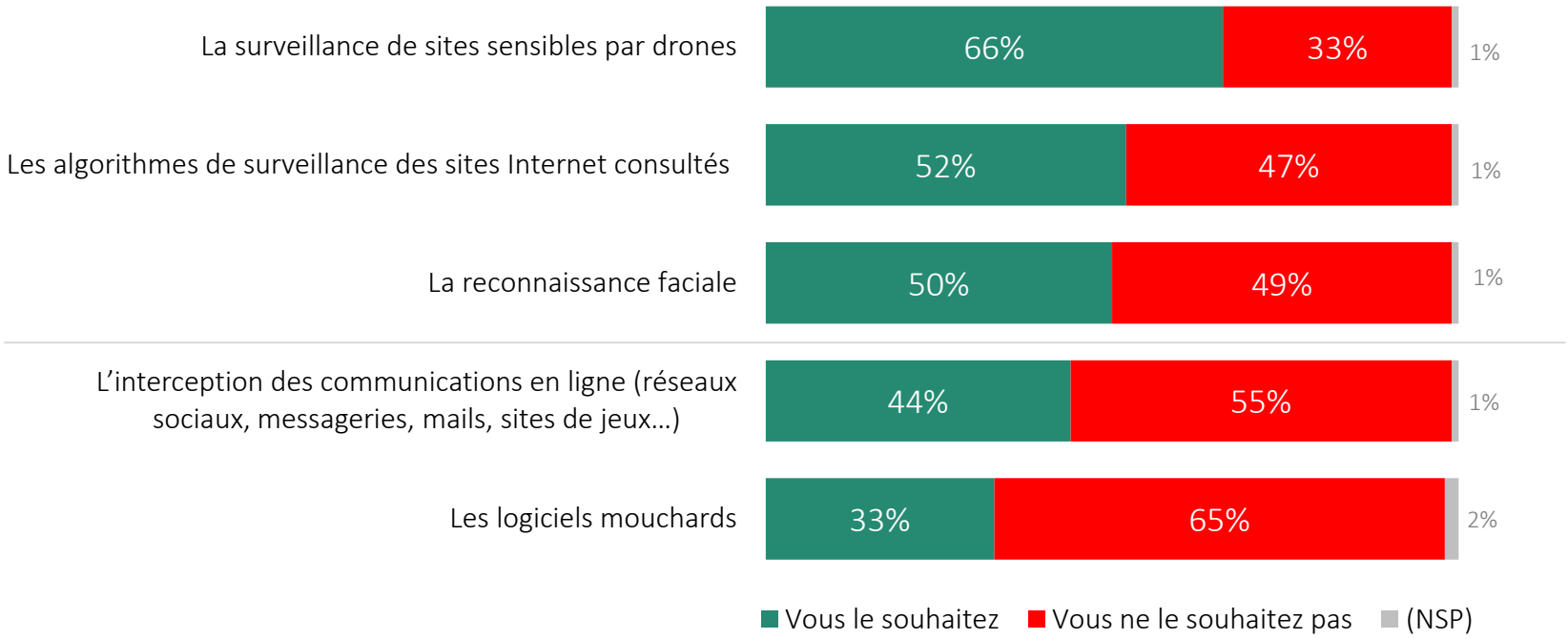
% Oui : 38%

25-34 ans : 55% / 65 ans et + : 19%



Souhait de l'emploi de certains outils numériques dans les politiques de sécurité en France

Et pour chacun des outils de surveillance suivants, dites-nous si vous souhaitez ou non qu'il soit utilisé par la France dans ses politiques de sécurité.



Approbation des différentes mesures de protection contre les cyberattaques

Et seriez-vous favorable ou opposé(e) à ce que…