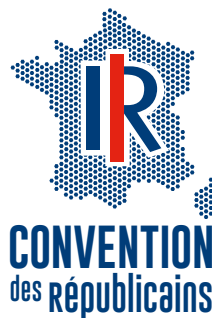


CONVENTION SOVERAINETÉ NUMÉRIQUE

FÉVRIER 2021



SOMMAIRE

LES CONSTATS	5
RÉSULTATS DU QUESTIONNAIRE DE LA CONVENTION «SOVERAINETÉ ET NUMÉRIQUE »	10
NOS PROPOSITIONS	13
BÂTIR LA SOVERAINETÉ NUMÉRIQUE EUROPÉENNE	15
METTRE EN ŒUVRE UNE STRATÉGIE NUMÉRIQUE POUR LA FRANCE	19
AMÉLIORER L'EFFICACITÉ DE NOS SERVICE PUBLICS GRÂCE AU NUMÉRIQUE	19
RENDRE NOS ENTREPRISES FRANÇAISES PLUS COMPÉTITIVES SUR LE MARCHÉ NUMÉRIQUE	20
LUTTER CONTRE LA FRACTURE NUMÉRIQUE	22
SE PROTÉGER CONTRE LES EFFETS NÉFASTES DU NUMÉRIQUE	25



Convention SOVERAINETÉ NUMÉRIQUE

Février 2021

Loin d'être l'apanage d'une prétendue « *start-up Nation* », le numérique est avant tout un enjeu de souveraineté pour la France et l'Europe.

La crise sanitaire et économique inédite que nous connaissons depuis un an a accéléré la numérisation de la société française : recours accru au télétravail, numérisation de nos échanges, explosion de la télémédecine et du e-commerce.

Mais cette crise a aussi révélé le retard numérique que nous trainons depuis des années : nos petites entreprises sont insuffisamment numérisées, certaines ont dû cesser complètement leurs activités pendant les confinements et ne font pas le poids face aux géants du commerce. 87 % du chiffre d'affaires généré par le secteur numérique en France est réalisé par 5 % des sites marchands étrangers. Plusieurs fractures numériques subsistent encore en France : en 2020 notre pays était seulement treizième au classement européen de la couverture 4G ; 6,8 millions de Français sont privés d'un accès de qualité minimale à Internet et 13 millions de Français maîtrisent mal les outils numériques.

Nous confions trop souvent à des puissances étrangères la gestion de nos données numériques. A chaque connexion, nous fournissons gratuitement des données aux géants du numérique, qui peuvent ensuite les revendre, sur lesquelles nous n'exerçons qu'un contrôle très limité. La cybercriminalité s'est aussi beaucoup professionnalisée et menace chaque citoyen, chaque entreprise et nos institutions.

En Europe, il est urgent de bâtir une vraie souveraineté digitale, en défendant la préférence européenne dans nos infrastructures de télécommunications et de stockage, pour protéger les données des Européens, celles de nos entreprises, de nos administrations, de nos concitoyens.

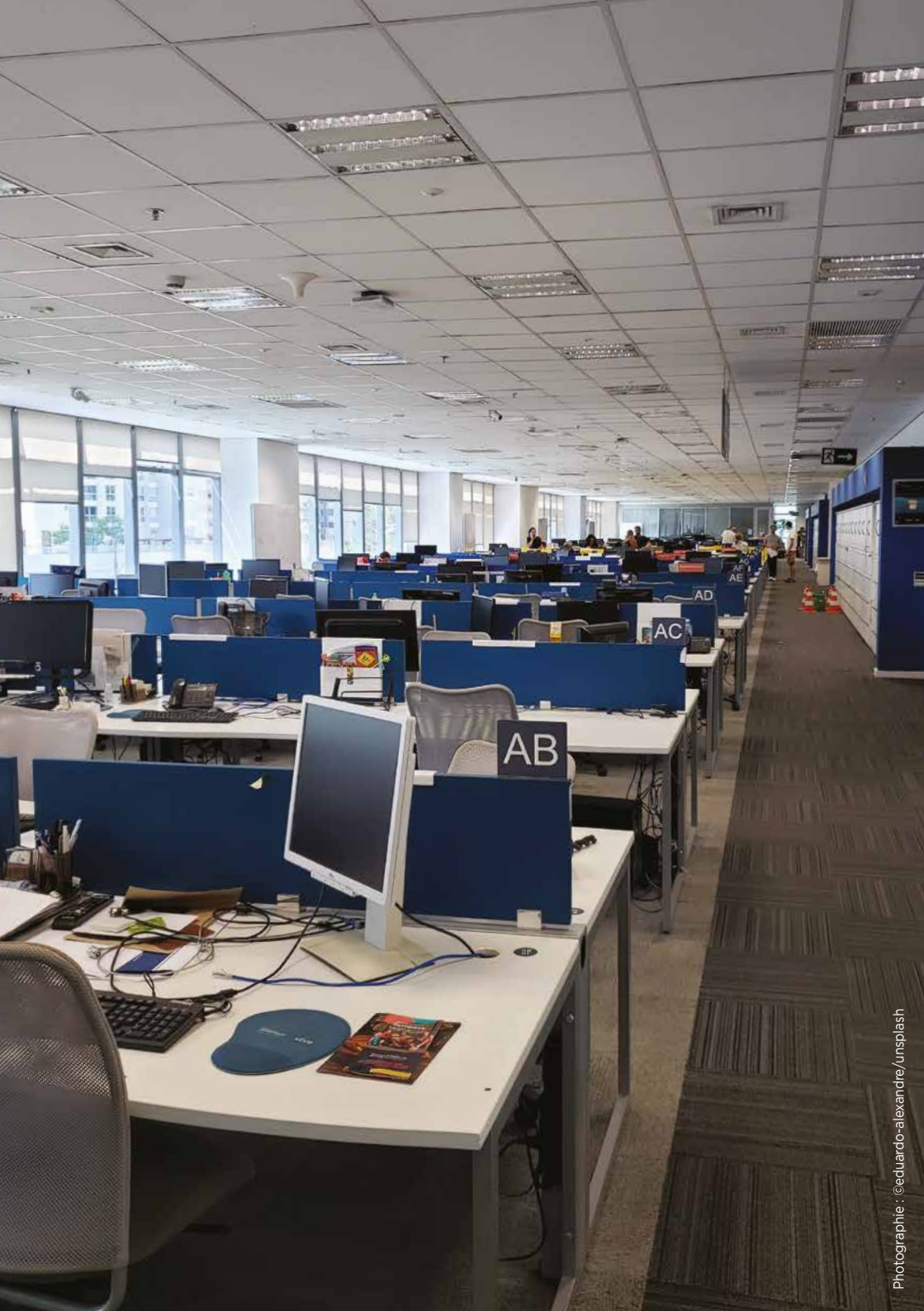
En France, nous devons mieux accompagner nos entreprises dans leur numérisation, pour les rendre plus compétitives et mieux financer nos pépites numériques, en incitant les Français à investir leur épargne pour les soutenir. Dans ce virage numérique, nous devons aussi garantir à chaque Français un accès au numérique, avec une connexion Internet de qualité dans tous les territoires et un plan ambitieux de lutte contre l'exclusion numérique.

Face aux cyberattaques, nous proposons de doubler le budget alloué à la cybersécurité en France, afin de développer une filière industrielle française de cybersécurité fondée sur des partenariats entre la recherche privée et la recherche militaire et de créer un vrai parcours de formation pour nos cybercombattants.

Le numérique est également un moyen de rendre l'action de l'état plus efficace : les économies potentielles générées par la transformation digitale et la dématérialisation en France sont estimées à 12 milliards d'euros dans 5 ans. Nous devons accélérer la modernisation des services de l'Etat, comme par exemple la Justice, et pour lutter contre la fraude fiscale et sociale. Le numérique ne doit plus être le prétexte à une disparition des services publics dans les territoires ruraux, mais un moyen de faire des économies dans l'organisation de l'État.

Nous présentons aujourd'hui un plan complet pour bâtir une vraie souveraineté numérique en France et en Europe.

Christian Jacob
Président des Républicains



LES CONSTATS

La crise sanitaire et économique a accéléré la numérisation de la société française mais a aussi révélé son retard numérique

Un recours accru à la télé médecine : l'Assurance maladie a vu le nombre de téléconsultations multipliées par 15 entre le 1^{er} et le 28 mars 2020, et les vidéoconférences ont crû de 37%. Alors que la téléconsultation frôlait à peine 0,1% du total des consultations en février 2020, cette pratique a connu une accélération considérable en l'espace de six mois, atteignant 10% des rendez-vous entre professionnels de santé et patients (GERS Data, octobre 2020). Sur les 4,6 millions de consultations vidéo enregistrées depuis le lancement du service en ligne sur Doctolib en janvier 2019, la plateforme en compte 4,5 millions rien qu'au cours des six derniers mois.

Le développement massif du télétravail : le premier confinement a entraîné un recours massif au télétravail (en avril 2020, un actif français sur cinq pratiquait le télétravail à temps plein), et a fait tomber une barrière culturelle : il est désormais possible de travailler chez soi en étant efficace. Les outils digitaux le permettent et transforment durablement la manière de penser l'organisation sociale, l'espace de travail et le management des équipes. Même si un nouvel accord interprofessionnel sur le télétravail a été signé en décembre et crée un guide des bonnes pratiques pour les entreprises, les répercussions macroéconomiques du travail à distance sont encore loin d'être évaluées ainsi que les enjeux de droit du travail (éligibilité des postes au télétravail, volontariat, réversibilité -retour du salarié sur son lieu de travail-, dispositions précises sur le télétravail en temps de crise, droit à la déconnexion, vie privée).

Le bond du e-commerce : le confinement a eu pour effet d'accélérer la croissance de l'e-commerce en France. Les ventes e-commerce sont passées de 57 milliards en 2014 à 115 milliards en année 2020, soit une croissance constante de 101 % (Fédération du e-commerce et de la vente à distance, Fevad).

L'explosion des cyberattaques : dès le premier confinement, les chiffres des attaques informatiques sur les ordinateurs personnels ou d'entreprises pour le télétravail ont explosé, notamment contre de nombreuses cibles privées ou publiques (comme Bouygues Construction ou les services de Marseille Métropole, mais aussi des institutions médicales et des hôpitaux en première ligne contre le Covid-19). Pour les spécialistes, 100 % de la force de frappe des cybercriminels (hackers, groupes mafieux, groupes para étatiques) a été dirigée sur le Covid, avec l'utilisation de faux sites, logiciels malveillants, et arnaques : entre février et avril 2020, on constate un triplement des cyberattaques (+238 %) contre les institutions financières dans le monde et une multiplication par neuf des tentatives d'extorsion de données personnelles (étude de Moody's).

La difficulté d'adaptation à la crise de nos TPE et PME : de nombreuses entreprises et commerces ont subi une fermeture « sèche » pendant les confinements, faute de disposer d'un site internet et de moyens logistiques. Plusieurs éléments justifient ces retards : le déficit de compétences numériques (la France compte deux fois moins de développeurs qu'en Suède) ; le manque de trésorerie des entreprises (les marges opérationnelles des PME françaises sont de 10 points inférieurs à la moyenne européenne) ; le manque de temps des chefs d'entreprise....

Des confinements difficiles à vivre dans les zones mal équipées : si la fibre optique a joué un rôle essentiel dans le maintien d'activité, si le réseau télécoms existant a bien tenu, il y a toujours des problèmes de connexion dans certaines zones rurales, qu'il s'agisse de l'absence de fibre, d'accès à la 4G ou à la 3G. Concrètement, ce manque d'accès à internet a évidemment impacté les personnes en télétravail, mais aussi les élèves et étudiants contraints à l'enseignement à distance, et la vie quotidienne. 13 millions de Français sont aujourd'hui, éloignés des nouvelles technologies.

Avant même la crise économique, la France était en retard numérique par rapport à ses partenaires. Plusieurs zones blanches subsistent en France :

si le nombre de zones blanches se réduit chaque année dans les zones rurales, en 2020, seulement 484 nouvelles zones prioritaires à couvrir en 4G ont été annoncées par le gouvernement, alors que de nombreux autres sites restent dépourvus d'une couverture 4G de qualité et que le plan 4G a été fortement ralenti par la crise du Covid-19. En 2020, la France était seulement 13^e au classement européen de la couverture 4G. 6,8 millions de Français sont privés d'un accès de qualité minimale à Internet (étude d'UFC Que Choisir en 2019). Le « bon haut débit » n'est lui, pas accessible à 19,1 % de la population, soit 12,8 millions de consommateurs.

Un retard préoccupant dans la transition numérique des TPE-PME :

la France était en 2019 au 15^e rang sur 28 dans l'Union européenne en matière de numérisation (classement DESI). D'après un rapport du Sénat publié à l'été 2019, on estime que ce classement très médiocre de la France lui coûte au moins un point de croissance. Seules 63 % des TPE françaises ont un site internet contre 91 % en Allemagne et l'automatisation de la chaîne logistique n'a été engagée que par 25 % des PME françaises (et 11 % des TPE) contre 43 % au Danemark (26 % pour les TPE) ou 41 % en Allemagne (21 % pour les TPE) d'après une étude du cabinet *McKinsey* en 2019.

Un marché qui reste à conquérir pour les entreprises françaises :

la France représente 37,5 millions d'acheteurs en ligne, soit 85 % des internautes. Si on recense 182 000 sites e-commerce actifs à ce jour, 87 % du chiffre d'affaires généré par le secteur est réalisé par 5 % des sites marchands (principalement étrangers, comme Amazon, eBay, ou Aliexpress), qui trustent le marché (Fevad, 2019). Seuls 8 % des entreprises françaises vendent en ligne à des consommateurs dans d'autres pays européens, contre 10 % des entreprises allemandes.

Des start-ups qui peinent à émerger : la France compte seulement 9 licornes (start-up non cotée valorisée plus d'un milliard de dollars, comme Blablacar, Mirakl, Dataiku, OVHcloud, Doctolib) sur un objectif de 25 licornes d'ici à 2025.

Une personne sur 5 en France ne sait pas utiliser internet : alors que 88 % des Français de 12 ans et plus sont des internautes (Baromètre du numérique, 2019), 7 % de la population française est touchée par l'illectronisme (INSEE, 2019), et une personne sur cinq est incapable de communiquer via internet. Les plus âgés, les moins diplômés, les revenus modestes sont parmi les plus touchés.

Le numérique est un marché qui recrute mais qui manque de candidats : il manque 79000 professionnels du numérique en France (conseil d'orientation pour l'emploi, 2019). 71% des entreprises du numérique déclaraient avoir du mal à attirer les talents en 2018, notamment pour les métiers de la maintenance des matériels, de l'exploitation et de la sécurité, et du développement web. Pourtant, 191000 postes seraient à pourvoir d'ici à 2022 (DARES, 2015).

Des failles de cybersécurité qui entraînent des pertes colossales :

la cybercriminalité s'est beaucoup professionnalisée et concerne chaque citoyen, nos entreprises, et nos institutions. 128 attaques par rançongiciels ont été traitées par l'ANSSI entre janvier et septembre 2020, contre 54 sur l'ensemble de l'année précédente. Sur l'année 2019, l'ANSSI a déjà été amenée à traiter 81 incidents de sécurité numérique ayant affecté les ministères français, un chiffre en augmentation (+3 %) par rapport à 2018.

Les pertes financières subies par les entreprises françaises en raison de problèmes de cybersécurité sont estimées à 2,25 millions d'euros en moyenne (PwC, 2017), un chiffre en hausse de 50 % par rapport à l'année précédente.

Une naïveté française sur le marché international : par manque d'ambition numérique, la France se retrouve trop souvent obligée de recourir à des infrastructures étrangères pour stocker ses propres données. C'est par exemple le cas pour nos données de santé du *Health Data Hub*, hébergées par l'américain Microsoft, depuis avril 2020 avec la bénédiction du gouvernement (qui a depuis promis de rétro pédaler dans un délai de...2 ans).

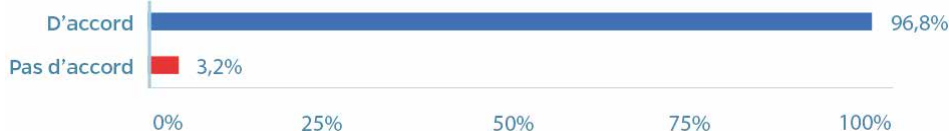
Après l'invalidation par la Cour de justice européenne du *Privacy Shield* (un texte attestant que la législation européenne garantissait les mêmes sécurités que le droit européen en matière de données) en juillet, la CNIL a même estimé que « *l'hébergement de la plateforme par une société de droit états-unien, pouvant être amenée à répondre à des demandes de communication de données, même pseudonymisées, était en soi problématique et devait conduire à changer d'opérateur ou à apporter des garanties spécifiques* ». Il en va de même pour la gestion des données de la DGSi (et notamment pour la lutte contre le terrorisme), assurée aujourd'hui par l'entreprise américaine *Palantir*. Il y a aujourd'hui urgence à faire monter en gamme nos industriels français.

Les retards de l'Union européenne dans l'innovation technologique :

L'Union européenne représente un quart du PIB mondial mais seulement 10 % de la technologie mondiale émergente (rapport de l'économiste Philippe Tibi de juillet 2018 pour le ministère de l'Economie). Les États-Unis, la Chine et le Japon consacrent chacun un milliard d'euros par an pour les supercalculateurs, contre seulement 100 millions dans l'UE. Le « *plan Intelligence artificielle* » présenté par Cédric Villani en mars 2018 prévoyait 1,5 milliard d'euros d'investissement sur 5 ans, là où la Chine et les États-Unis vont dépenser, chacun, environ dix fois plus.

Résultats du questionnaire de la convention «souveraineté et numérique »

1. Instaurer un « buy european act » et réviser le droit de la concurrence européenne pour constituer des champions numériques européens et lutter contre la dépendance technologique vis-à-vis des Etats-unis et de la Chine ?



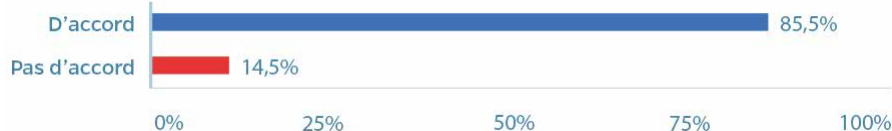
2. Lutter contre la haine en ligne et renforcer la responsabilité des plateformes en soutenant les règlements européens *Digital services Act* (DSA) et *Digital Market Act* (DMA) ?



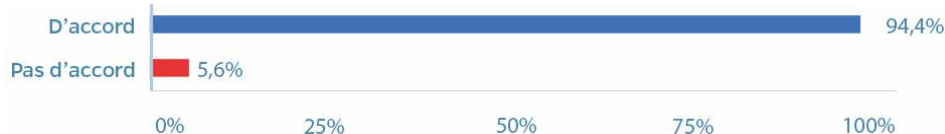
3. Donner la priorité aux nouvelles infrastructures européennes sur notre territoire pour le déploiement de la 5G ?



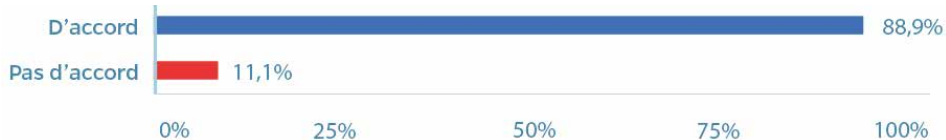
4. Mettre en place d'une taxation des grandes entreprises du numérique (taxe GAFA) au niveau européen plutôt qu'au niveau français ?



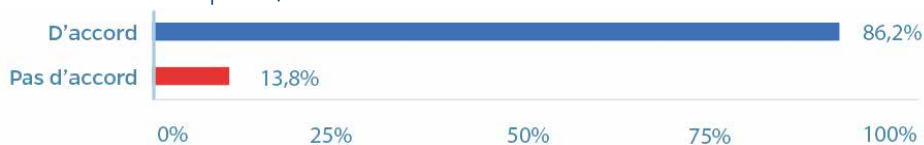
5. Systématiser l'utilisation du numérique dans la lutte contre le gaspillage de l'argent public et la fraude fiscale ?



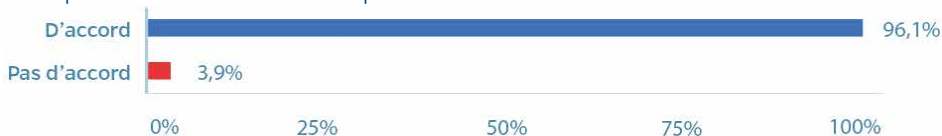
6. Créer un crédit d'impôt à la formation et à l'équipement numérique pour les artisans, les commerçants et leurs salariés, pour réduire de 50 % et à hauteur de 5 000 € leur coût d'équipement en appareils numériques pour commercialiser leur production sur le e-commerce ?



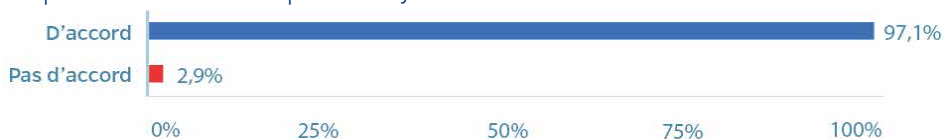
7. Créer un « super IR-PME » pour rediriger l'épargne des Français vers le financement de nos entreprises numériques innovantes, avec une réduction d'impôt massive de 50% du montant investi dans une start-up innovante (dans la limite de 100 000 € d'investissement par an) ?



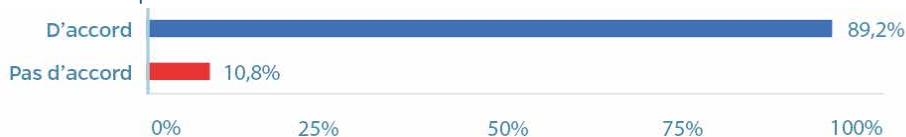
8. Garantir à chaque Français une connexion internet de qualité, au plus tard en 2023, et lutter contre l'illectronisme partout en France en développant massivement les espaces de formation numérique dans les territoires ?



9. Doubler le budget de la cybersécurité en France, pour arriver à 250 millions d'euros par an investis dans l'accélération de nos capacités nationales de cyberdéfense, afin de développer une filière industrielle française de cybersécurité fondée sur des partenariats entre la recherche privée et la recherche militaire, et de créer un vrai parcours de formation pour nos cybercombattants ?



10. Se protéger contre les effets néfastes du numérique, en menant une campagne nationale de sensibilisation « zéro écrans avant trois ans », en faisant figurer un message sanitaire sur les emballages des jouets numériques disposant d'un écran et en interdisant les écrans pour les jeunes enfants dans les crèches et les tablettes numériques dans les écoles maternelles ?





NOS PROPOSITIONS

Bâtir la souveraineté numérique européenne

1. Instaurer un « *buy european act* » et réviser le droit de la concurrence européenne pour constituer des champions numériques européens et lutter contre la dépendance technologique vis-à-vis des Etats-Unis et de la Chine.
2. Lutter contre la haine en ligne et renforcer la responsabilité des plateformes en soutenant les règlements européens *Digital services Act* (DSA) et *Digital Market Act* (DMA).
3. Donner la priorité aux nouvelles infrastructures européennes sur notre territoire pour le déploiement de la 5G.
4. Mettre en place d'une taxation des grandes entreprises du numérique (« taxe GAFA ») au niveau européen plutôt qu'au niveau français.

Mettre en œuvre une stratégie numérique pour la France

5. Systématiser l'utilisation du numérique dans la lutte contre le gaspillage de l'argent public et la fraude fiscale.
6. Créer un crédit d'impôt à la formation et à l'équipement numérique pour les artisans, les commerçants et leurs salariés, pour réduire de 50 % et à hauteur de 5 000 € leur coût d'équipement en appareils numériques pour commercialiser leur production sur le e-commerce.
7. Créer un « super IR-PME » pour rediriger l'épargne des Français vers le financement de nos entreprises numériques innovantes, avec une réduction d'impôt massive de 50% du montant investi dans une start-up innovante (dans la limite de 100 000 euros d'investissement par an).
8. Garantir à chaque Français une connexion internet de qualité, au plus tard en 2023, et lutter contre l'illectronisme partout en France en développant massivement les espaces de formation numérique dans les territoires.
9. Doubler le budget de la cybersécurité en France, pour arriver à 250 millions d'euros par an investis dans l'accélération de nos capacités nationales de cyberdéfense, afin de développer une filière industrielle française de cybersécurité fondée sur des partenariats entre la recherche privée et la recherche militaire, et de créer un vrai parcours de formation pour nos cybercombattants.
10. Se protéger contre les effets néfastes du numérique, en menant une campagne nationale de sensibilisation « zéro écran avant trois ans », en faisant figurer un message sanitaire sur les emballages des jouets numériques disposant d'un écran et en interdisant les écrans pour les jeunes enfants dans les crèches et les tablettes numériques dans les écoles maternelles.



BÂTIR LA SOUVERAINETÉ NUMÉRIQUE EUROPÉENNE

Instaurer un « buy european act » et réviser le droit de la concurrence européenne, pour défendre la préférence européenne et lutter contre la dépendance technologique : il ne faut plus traiter sur un pied d'égalité les entreprises européennes soumises à l'interdiction des aides d'État et les entreprises non européennes qui n'ont pas à respecter ces règles. La Commission européenne doit favoriser les entreprises européennes : la constitution de champions européens numériques doit être une priorité, quitte à limiter la concurrence au sein de l'Union européenne.

Aujourd'hui, le fractionnement du marché européen est nuisible aux entreprises européennes du numérique (et notamment de l'intelligence artificielle), qui ne peuvent compter sur de grands marchés intérieurs unifiés, comme c'est le cas des deux champions mondiaux, les États-Unis et la Chine. Les Européens peuvent pourtant peser dans le système numérique international : nous sommes le 1^{er} marché mondial économique, et le 1^{er} marché des datas.

Il n'est pas acceptable que les autorités de la concurrence ne fassent aucune différence entre une entreprises européenne et une entreprise chinoise.

La dépendance technologique est une vraie arme que nous devons prendre au sérieux : du jour au lendemain, les logiciels, les systèmes d'exploitation, les processeurs et autres équipements informatiques d'une nation peuvent être suspendus par une autre. Les conditions d'utilisation de la plupart des services numériques que nous acceptons autorisent ces services à être interrompus pour des périodes indéfinies sans une quelconque compensation. D'ici à 2022, l'administration chinoise a annoncé vouloir supprimer tous ses logiciels étrangers, et ses forces armées travaillent à se doter de leur propre système d'exploitation pour remplacer Windows.

Renforcer le contrôle des investissements étrangers dans nos secteurs stratégiques, notamment numériques : en créant un comité pour l'investissement étranger français, sur le modèle du *Committee on Foreign Investment in the United States* (CFIUS) chargé de protéger toutes les entreprises considérées comme stratégiques par un strict contrôle des investissements étrangers.

Le CFIUS est une structure interministérielle chargée d'examiner tout projet de fusion, d'acquisition ou de reprise pouvant mener au contrôle d'une entreprise américaine par une entité étrangère, dans le but d'en évaluer l'impact sur la sécurité nationale et peut s'autosaisir d'une opération, à tout stade du processus. Il s'agit d'un dispositif systématique plus ambitieux que ce que prévoient aujourd'hui les décrets Montebourg, Villepin et Le Maire.

Lutter contre la haine en ligne et renforcer la responsabilité des plateformes en soutenant les règlements européens *Digital Services Act (DSA)* et *Digital Market Act (DMA)*. Le gouvernement a proposé un amendement au projet de loi confortant les principes de la République pour imposer de nouvelles règles aux réseaux sociaux, avec l'appui du CSA. Les plateformes numériques devront lui transmettre des rapports sur leurs actions pour lutter contre les propos illicites. Cette mesure ne pourra être fonctionnelle sans l'adoption des textes européens pour la régulation des plateformes.

Le DSA prévoit notamment de contraindre les services en ligne ayant plus de 45 millions d'utilisateurs en Europe (comme Facebook, Snapchat, TikTok, Twitter, ou Amazon) à assumer la responsabilité des contenus publiés sur leur plateforme. Le DMA a pour but de lutter contre les éventuels comportements abusifs et anticoncurrentiels des géants du numériques. La question de la suspension arbitraire par les réseaux sociaux de certains comptes, sans contrôle légitime et démocratique, devra aussi être posée dans les débats européens. Il est urgent d'organiser l'espace informationnel avec des droits, obligations et des garanties clairement définis.

Mieux protéger nos données européennes et mettre en place un nouveau statut juridique des données. Nos données doivent être protégées, à commencer par les plus sensibles : celles de l'Etat, de nos administrations, et de nos entreprises. Elles doivent pouvoir être stockées en lieu sûr, hors de portée des serveurs étrangers, dans un cloud public 100 % européen. Les données doivent être considérées comme un bien commun, régies par nos lois, localisées sur notre territoire, chiffrées par nos protocoles, transitant par des télécommunications sous nos lois, alimentant des algorithmes assujettis à nos règles et disposant de protections internationales, garanties par nos chiffrements souverains.

Soutenir massivement les projets européens numériques, comme le satellite de nouvelle génération Galileo, ou le cloud souverain européen Gaia-X.

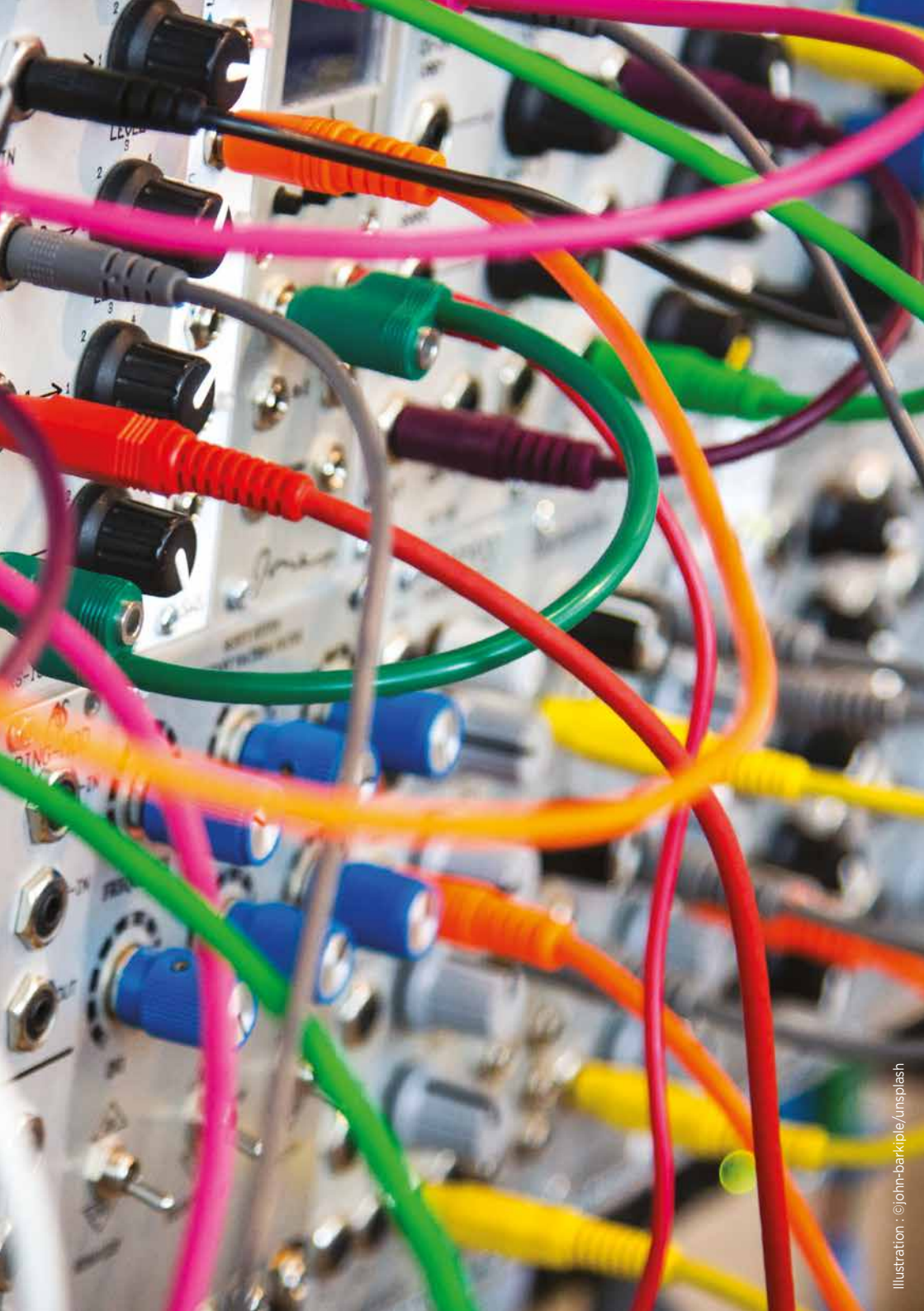
Il est urgent de renforcer nos conditions d'accès aux datas et garantir une meilleure protection de nos données. L'Europe ne doit plus être un « *open bar* » de la data, et nous devons empêcher nos concurrents de venir piocher dans nos données gratuitement. Il est par exemple inadmissible que ce soit l'américain *Microsoft* qui héberge les données de santé du *Health Data Hub* français. 80 % des principales entreprises du CAC 40 en France utilisent *Amazon Web Services*. Le *cloud* ne doit plus être « l'ordinateur d'un autre pays », souvent américain, alors que nous y stockons notre mémoire, notre propriété intellectuelle et notre activité économique. Une coupure de trafic, à ce niveau de dépendance, représenterait une interruption de notre Nation.

En Chine, une entreprise étrangère s'installant dans le pays pour y faire du commerce doit obligatoirement stocker ses données sur le territoire, ou se verra interdire la distribution de ses produits.

Soutenir la mise en place d'une taxation des grandes entreprises du numérique (« *taxe GAFA* ») au niveau européen plutôt qu'au niveau français. Faute de réussir à faire aboutir les négociations au sein de l'OCDE pour mettre en place une taxation sur les GAFA (Google, Apple, Facebook, Amazon), le gouvernement français a mis en place en juillet 2019 une taxe de 3 % sur le chiffre d'affaires des géants du numérique. Mais le périmètre de cette taxe française frappe également les entreprises du numérique françaises, comme Critéo, pourtant domiciliée sur notre territoire et respectant notre droit de la concurrence

Donner la priorité aux nouvelles infrastructures européennes sur notre territoire pour le déploiement de la 5G : depuis le début de l'année 2021, la 5G est proposée dans plusieurs villes françaises, et continuera son déploiement jusqu'en 2030, où le réseau français sera intégralement couvert par la 5G. Pour déployer la 5G en France, les opérateurs télécoms doivent s'appuyer sur des équipements télécoms de 5G. Aujourd'hui, seuls 3 équipementiers télécoms, les européens Nokia et Ericsson et le chinois Huawei, sont capables de fournir les équipements pour les futurs réseaux 5G. De multiples soupçons d'espionnage pèsent sur l'entreprise chinoise, très soutenue par le gouvernement chinois, et la législation chinoise fait obligation aux entreprises ayant leur siège en Chine de collaborer avec les services de renseignement de ce pays.

Alors que le gouvernement français propose seulement une sortie progressive de Huawei des réseaux 5G en France à l'horizon 2028, nous proposons de donner la priorité aux équipementiers européens dans ce déploiement dès maintenant. L'objectif étant aussi de lutter contre le pillage de nos technologies par l'espionnage industriel au profit des puissances étrangères.



METTRE EN ŒUVRE UNE STRATÉGIE NUMÉRIQUE POUR LA FRANCE

Améliorer l'efficacité de nos service publics grâce au numérique

Systématiser l'utilisation du numérique dans la lutte contre le gaspillage de l'argent public et la fraude fiscale. Dans une étude de mars 2017, le cabinet Ernst & Young évalue les économies potentielles générées par la transformation digitale et la dématérialisation en France à 12 milliards d'euros dans 5 ans. Selon un rapport de la Cour des Comptes en 2016, « *l'État n'a pas encore tiré tout le bénéfice du potentiel offert par le développement des nouveaux outils numériques* ». D'après la stratégie de services publics en ligne lancée en 2012 au Royaume-Uni, le même service opéré via une technologie numérique coûte 50 fois moins cher que le service en face-à-face et 30 fois moins cher que par échange postal (Digital efficiency report, Cabinet Office, 2012). Après la création réussie d'une identité numérique pour chacun de ses citoyens, l'Estonie a dématérialisé 99 % de ses services publics, ce qui lui a permis d'économiser 2 points de PIB de dépenses publiques (ce qui représenterait en France jusqu'à 50 milliards d'euros).

Le numérique doit aussi permettre de lutter plus efficacement contre la fraude fiscale : le *data mining* consiste à analyser de grandes quantités de données avec des algorithmes. Il est utilisé depuis peu de temps en France. L'Irlande apparaît en avance : le *data mining* y a permis de détecter environ 2,5 milliards d'euros supplémentaires de fraude à l'impôt sur le revenu. Le programme *CONNECT* au Royaume-Uni a aussi permis de vérifier la fiabilité des déclarations fiscales et des demandes de crédits d'impôts et a abouti à un doublement des résultats des contrôles en moins de 10 ans. La France doit rejoindre le meilleur standard des pays développés en termes de taux de fraude rapporté au montant des impôts collectés.

Beaucoup d'économies sont ainsi à attendre du numérique dans l'amélioration de la productivité de notre action publique (12 milliards d'euros après 5 ans de transformation digitale d'après Ernst & Young).

Une partie de ces économies nous permettra de financer de nouvelles politiques publiques de développement du numérique.

Rendre nos entreprises françaises plus compétitives sur le marché numérique

Créer un crédit d'impôt à la formation et à l'équipement numérique pour les artisans, les commerçants et leurs salariés, pour réduire de 50 % et à hauteur de 5 000 € le coût d'équipement en appareils numériques en vue de commercialiser leur production sur le e-commerce. En 2016, 19 % des TPE françaises n'avaient pas accès à internet (contre 7 % en Allemagne), 32 % avaient un site internet (64 % en Allemagne) et seulement 6% vendaient en ligne (INSEE, 2017).

L'accompagnement à la transformation numérique des entreprises est aujourd'hui trop inadapté aux entreprises françaises. L'État laisse souvent au réseau des Chambres de commerce et d'industrie (CCI) le soin de piloter la numérisation des PME alors qu'il réduit leurs moyens financiers dans le même temps. Les mesures que le gouvernement propose dans son plan de relance (présenté en septembre 2020) pour numériser nos TPE, PME et ETI sont insuffisantes (« une sensibilisation à la numérisation », « un accompagnement dans la mise en place de solutions d'intelligence artificielle ») avec un budget prévu de 385 millions d'euros pour « l'accompagnement dans la transformation numérique des TPE, PME ». Nous proposons de réorienter ces crédits pour créer un crédit d'impôt pour favoriser la formation au numérique des artisans et commerçants de détail pour faciliter leur initiation aux techniques commerciales sur internet, aux méthodes d'animation commerciale et d'accueil.

Ce crédit d'impôt d'environ 1,25 milliard d'euro par an (en partant de l'hypothèse qu'un tiers des 1,5 million de commerçants et artisans éligibles aient recours entièrement à ce crédit d'impôt), sera financé par le plan de relance et par notre plan de numérisation des services publics.

Créer un « super IR-PME » pour rediriger l'épargne des Français vers le financement de nos entreprises numériques innovantes : nous proposons une réduction d'impôt massive de 50 % du montant investi dans une start-up innovante (dans la limite de 100 000 euros d'investissement par an). La réduction d'impôt IR-PME est un dispositif fiscal qui permet en France à un contribuable de bénéficier d'une réduction d'impôt sur le revenu au titre des souscriptions au capital initial ou aux augmentations de capital des PME. Sans toucher à ce dispositif, nous proposons de créer en complément un « super IR-PME » pour inciter davantage les Français à investir leur épargne dans les entreprises innovantes françaises. Nous proposons de nous inspirer du modèle du *Seed Enterprise Investment Scheme* (SEIS) anglais, qui propose une réduction d'impôt massive de 50 % du montant investi dans une start-up innovante (dans la limite de 100 000 livres d'investissement par an).

Entre 2017 et 2018, 2 320 entreprises ont levé un total de 189 millions de livres avec ce mécanisme fiscal. En conséquence, il y a trois fois plus de business angels au Royaume-Uni qu'en France : ils représentent 1,7 % du PIB français contre 4,4 % au Royaume-Uni.

Cela représente une dépense fiscale d'environ 100 millions d'euros par an, que nous financerons avec notre plan de numérisation des services publics.

Mieux informer les entreprises sur leurs possibilités de recours en cas de dysfonctionnement des opérateurs dans le déploiement numérique,

notamment avec la saisie systématique de l'autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep). Aujourd'hui, les PME et TPE sont trop souvent victimes des défaillances pour le déploiement de la fibre. Beaucoup d'immeubles accueillant des entreprises ou des commerces sont « oubliés » du déploiement de la fibre par les opérateurs, alors qu'ils se situent parfois dans des zones très denses où les immeubles voisins, accueillant des logements et donc des clients résidentiels, sont parfaitement raccordés au réseau fibré (FttH). Certains spécialistes auditionnés au Sénat en 2019 ont mentionné le chiffre de 40 000 adresses ainsi « oubliées ». Les entreprises concernées ne peuvent donc pas bénéficier de la fibre rapidement, mais de surcroît se voient réclamer des sommes très élevées pour que le raccordement soit opéré (des tarifs allant de plusieurs milliers à plusieurs dizaines de milliers d'euros).

Créer un nouveau baccalauréat professionnel « services numériques »,

pour renforcer l'orientation vers les métiers du numérique. Ce nouveau diplôme proposera des cours de gestion des organisations (comptabilité, marketing, relation client,) de développement web, d'analyse de données, d'hygiène numérique. Si des cursus existent déjà (baccalauréat professionnel « systèmes électroniques numériques » et le titre professionnel « technicien d'assistance en informatique »), avec également l'option numérique introduite par la réforme du lycée, l'offre de formation n'est pas suffisante pour se spécialiser dans le développement et l'exploitation d'infrastructures numériques. C'est dans ce secteur que les entreprises ont le plus de difficultés à recruter, faute de formations qualifiantes.

Soutenir les investissements des collectivités locales dans les projets numériques locaux :

- **En encourageant les coopérations entre les aides nationales au développement numérique et les fonds régionaux pour accompagner le développement des start-ups.** Dans le plan de relance, plusieurs investissements ont été annoncés pour développer les entreprises numériques innovantes : 500 millions d'euros sur 2 ans en soutien

aux fonds propre des start-ups ; 800 millions d'aides à l'innovation sur 5 ans pour les créateurs d'entreprise avec des prêts d'amorçage ou de recherche et développement ; 2,2 milliards d'euros pour les technologies de rupture. Nous proposons de développer davantage de partenariat entre les aides nationales et locales, et qu'elles viennent en appui de l'action des fonds régionaux, déjà mobilisés depuis des années pour renforcer les capitaux des entreprises numériques innovantes régionales, ou de leurs sous-traitants. Les régions sont notamment des partenaires stratégiques pour amorcer des opérations de financement ; de nombreuses start-ups arrivent à renforcer leurs capitaux au niveau régional, puis français et européen.

- **En renforçant les partenariats de financement entre l'Etat et les territoires pour encourager la création de centres de données** (data centers) locaux. Les centres de données permettent à une collectivité de prendre la main sur le contrôle physique de ses données, en gérant elle-même ses serveurs, et d'économiser plusieurs millions d'euros : plus de service extérieur à payer, plus d'hébergement à payer, et la possibilité de louer ses infrastructures à d'autres. Ils renforcent également l'attractivité d'un territoire pour les entreprises, et répondent à l'enjeu de souveraineté numérique nationale. En France, ces centres de données se développent encore de façon anarchique sur les territoires (nous en comptons environ 150 contre 328 en Allemagne et 250 au Royaume-Uni). Il est urgent de les développer, face à la croissance massive des échanges de données et des besoins de stockage des entreprises.

Lutter contre la fracture numérique

Garantir à chaque Français un accès à une connexion Internet de qualité, au plus tard en 2023. Dans son programme présidentiel, Emmanuel Macron s'engageait à couvrir l'ensemble du territoire en très haut débit d'ici la fin du quinquennat. Aujourd'hui, cette ambition a déjà été repoussée de 3 ans, en 2025. Nous voulons que le calendrier soit tenu pour 2023.

Les crédits budgétaires pour lutter contre la fracture numérique représentent une enveloppe de 420,5 millions d'euros est consacrée à l'accélération du déploiement de la fibre en France ; une enveloppe de 150 millions d'euros du Plan France très haut débit vise à couvrir tout le territoire français ; le plan de relance prévoit 88 millions d'euros pour la transformation et l'outillage numérique des collectivités. Ces crédits (soit un total de 658,8 millions d'euros) doivent être mis au service d'un seul objectif : garantir une connexion Internet de bonne qualité à chaque Français au plus tard en 2025.

Lutter contre l'illectronisme partout en France. Aujourd'hui, les lieux d'inclusion numérique spécifiques ou les espaces publics numériques (EPN) sont en échec dans les territoires, n'arrivant pas à attirer tous les publics illectronistes, et très connotés « geek ». Le gouvernement a annoncé récemment le recrutement d'ici à fin 2022 de 4 000 nouveaux conseillers numériques, financés par 250 millions d'euros du plan de relance de septembre 2020. Ce recrutement n'améliorera pas la situation pour les publics exclus du numérique si ces conseillers n'interviennent pas dans des structures visibles et connues dans les territoires. Nous proposons de réaffecter ces crédits pour :

- **Développer massivement les espaces de formation numérique dans des lieux locaux identifiés :** dans les maisons de quartier, maisons de seniors, résidence autonomie, mairie, salles des communes. L'objectif est d'aller à la rencontre des publics dans les lieux qu'ils fréquentent déjà. Les formateurs viendront avec leur matériel informatique, dans un lieu connu localement, pour y dispenser des cycles de formation spécifiques sur l'utilisation du numérique et la cybersécurité.
- **Renforcer le maillage local et élargir les missions des bus France Service, qui assurent aujourd'hui des permanences polyvalentes et itinérantes** dans les quartiers prioritaires de la ville et les territoires ruraux pour accompagner les Français qui le souhaitent dans les principales démarches administratives du quotidien. Ces bus pourraient ainsi également proposer des cycles de formation au numérique.

Rendre systématique l'évaluation PIX (certifications des compétences numériques) pour tous les enseignants et les élèves dans les écoles, du primaire au lycée, pour garantir l'acquisition de compétences numérique.

Aujourd'hui, la plateforme PIX est un service gratuit qui permet d'évaluer les compétences numériques et délivre une certification qui remplace le Brevet informatique et internet (B2i) et la Certification informatique et internet (C2i). Ce test permet également de développer des compétences tout au long de la vie, de suivre une formation adaptée en fonction des scores obtenus, d'être encadré et suivi par des professionnels et de valoriser ses compétences.

They... we've been spoon-
 fed... we've been dominated by sadists, or ignored by
 the world now... the world of it
 ready existing without paying for what could be dirt-cheap if it
 and you call us criminals. We seek after knowledge... You
 nationality, without religious bias... and you call us criminals... Yes
 and try to make us believe it's for our own good, yet we're
 or curiosity. My crime is that of judging people by what they say and think.
 this is my manifesto. My crime is that of outsmarting you. something that you with
 individual, but you can't stop us all... after all, we're all alike

Illustration : ©FreePik

Se protéger contre les effets néfastes du numérique

Doubler le budget de la cybersécurité en France, pour arriver à 250 millions d'euros par an investis dans l'accélération de nos capacités nationales de cyberdéfense.

La cybersécurité est l'enjeu de tous : un attaquant peut pénétrer dans les systèmes d'information des grandes structures en passant par les plus petits fournisseurs.

Dans son plan de relance, le gouvernement a prévu 136 millions d'euros pour financer l'accélération en cybersécurité, ce qui ne représente même pas la moitié du budget de du *National Cyber Security Centre* britannique (250 millions de livres par an). Nous proposons de doubler ce budget, en rythme annuel, en profitant des économies de notre plan de numérisation des services publics afin de :

- **Renforcer les partenariats entre la recherche privée et la recherche militaire pour développer une filière industrielle française en cybersécurité**, et permettre à la société civile de s'emparer des innovations militaires dans ce secteur. Dans nombre de technologies-clés, l'excellence scientifique française est reconnue grâce au niveau de formation de ses mathématiciens et ingénieurs et à la qualité de ses organismes de recherche. Mais la constitution d'une industrie française de logiciels de cybersécurité tarde à venir, ce qui pose un problème pour l'autonomie de notre cyberdéfense et renchérit les coûts. Un exemple national souvent cité est celui d'Israël, qui a réussi à devenir une usine de *start-ups cyber*, en réutilisant les systèmes développés dans les laboratoires de l'armée pour les réinjecter dans la société civile. En Grande-Bretagne, le gouvernement a lancé une plateforme numérique de partage d'informations en temps réel entre les secteurs privé et public et a mis en place auprès un *National Cyber Security Centre*, interface entre le Gouvernement et l'industrie qui centralise l'ensemble des activités et des informations relatives à la cyberdéfense.
- **Renforcer les moyens de l'Autorité nationale en matière de sécurité et de défense des systèmes d'information (ANSSI) et des services enquêteurs spécialisés dans la lutte contre la cybercriminalité.** L'ensemble des procédures relatives à la pédopornographie en ligne (plus de 25 000 signalements de contenus pédopornographiques en 2019) ne sont traitées que par 13 enquêteurs en France, appartenant à l'office central de répression des violences aux personnes.

- **Créer un parcours de formation pour devenir cybercombattant**, en contrepartie d'un engagement dans la réserve de cyberdéfense pour un nombre minimum d'années. La France continue aujourd'hui à manquer d'experts en cybersécurité, et 80 % des entreprises françaises ont notamment des difficultés à recruter des cyberspécialistes (ANSSI, 2020). Lancée en mai 2016, la réserve de cyberdéfense se compose d'un réseau de volontaires organisé en unités militaires réparti en cellules régionales, encadrée par des réservistes des forces armées et par du personnel de l'Etat. Les cybercombattants seront notamment formés à la lutte contre la propagande digitale, sur le modèle de la 77^e brigade de l'armée britannique qui compte 2000 combattants mobilisés pour répondre à la communication sur les réseaux sociaux d'organisations terroristes comme l'État islamique ou Boko Haram, pour gagner la guerre de l'information.
- **Lancer une campagne publique sur le risque d'attaques numériques à destination des entreprises françaises, en y associant les acteurs économiques locaux** tels que les chambres de métiers et de l'artisanat et chambres de commerce et d'industrie. Nos entreprises françaises sont aujourd'hui très vulnérables aux cyberattaques (rançongiciel, hameçonnage, vol de données), et doivent être accompagnées pour sécuriser leur système d'information.
- **Mettre en place une certification de cybersécurité (« cyberscore », sur le modèle du « nutriscore ») des plateformes numériques destinées au grand public.** L'objectif est d'avertir le public de la fiabilité des plateformes dans la protection de leurs données en leur attribuant un score, en ciblant les plateformes numériques très fréquentées (comme Google Meet, Zoom, Whatsapp...).

Mener une campagne nationale de sensibilisation « zéro écran avant trois ans », en faisant figurer un message sanitaire sur les emballages des jouets numériques disposant d'un écran, et en interdisant les écrans pour les jeunes enfants dans les crèches :

depuis plus de 10 ans, le conseil supérieur de l'audiovisuel déconseille officiellement l'exposition des enfants de moins de 3 ans aux écrans (télévisions, smartphones, tablettes), qui entraîne des risques pour leur développement et santé physique. Déjà en 2013, l'Académie de Médecine soulignait qu'ils pouvaient provoquer des prises de poids, retards de langage, déficits de concentration et d'attention, et risques d'adopter une attitude passive face au monde. Pourtant, un enfant sur deux commence à regarder la télévision avant l'âge 18 mois (Inserm), et près d'un enfant de moins de 3 ans sur deux utilise déjà les écrans interactifs environ 30 minutes par semaine, et près d'un tiers l'utilise sans la présence d'un adulte (Association française de pédiatrie ambulatoire, AFPA).

96 % des parents savent que les risques ne sont pas inexistants, mais seulement un tiers d'entre eux les considèrent comme majeurs (Fondation pour l'enfance, 2018). Nous proposons donc de faire systématiquement figurer sur tous les emballages d'outils et jeux numériques disposant d'un écran un message sanitaire avertissant des dangers liés à leur utilisation par des enfants de moins de trois ans.

Interdire l'acquisition de tablettes numériques dans les écoles maternelles.

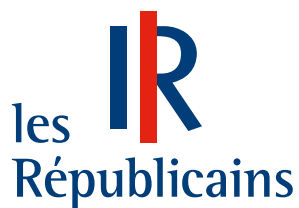
Dans une publication de novembre 2019, la revue médicale de référence *JAMA Pediatrics* conclue que les enfants passant le plus de temps devant leur écran ont de moins bons résultats cognitifs : ils ont moins de vocabulaire, plus de difficultés à lire et mettent plus de temps à nommer des objets. D'après le psychiatre Serge Tisseron, dès que les jeux numériques sont introduits dans la vie de l'enfant, ils accaparent toute son attention aux dépens des autres activités. Les influences négatives persisteraient « *au moins jusqu'à l'âge de 10 ans* » (Académie des sciences en 2013) : « *pour chaque heure supplémentaire hebdomadaire passée devant un écran non interactif par un enfant en bas âge, il a été noté une diminution de 7 % de l'intérêt en classe et de 6 % sur les habiletés en mathématiques à l'âge de 10 ans, sans impact démontré sur les capacités en lecture.* » En France, plusieurs académies achètent pourtant des tablettes pour les enfants en maternelle. Nous arrêterons cette pratique coûteuse, inefficace pour l'apprentissage et dangereuse pour les jeunes enfants.

Février 2021

Contacts :

Presse : servicedepresse@republicains.fr - 01.40.76.60.44

Etudes : forums@republicains.fr - 01.40.76.62.75



Retrouvez toute notre actualité sur
www.republicains.fr