COMMISSION
EUROPÉENNE

Bruxelles, le 10.12.2021
COM(2021) 819 final

RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS

Protéger les droits fondamentaux à l'ère numérique-

Rapport annuel 2021 sur l'application de la charte des droits fondamentaux de l'UE

Protéger les droits fondamentaux à l'ère numérique —

Rapport annuel 2021 sur l'application de la charte des droits fondamentaux de l'UE

Table des matières

1. Introduction

La charte des droits fondamentaux de l'Union européenne[1] est un instrument puissant, qui sert à protéger, promouvoir et consolider davantage les droits des personnes au sein de l'Union européenne. Non seulement les droits fondamentaux protègent les personnes des ingérences indues telles que la censure ou la surveillance de masse mais ils leur donnent également les moyens de profiter pleinement de leurs droits et des possibilités que leur offre la vie. Il est toujours possible d'améliorer les conditions et la mesure dans lesquelles les personnes peuvent jouir de leurs droits. La charte peut guider les activités menées par les pouvoirs publics dans l'ensemble de l'Union. Plus les personnes connaissent les droits garantis par la charte et savent comment s'en prévaloir, plus ceux-ci ont de poids.

La pandémie de COVID-19 a mis à rude épreuve la protection et les garanties de nos droits et libertés fondamentaux. Toute restriction aux droits fondamentaux doit être nécessaire et proportionnée. C'est ce qu'exige la charte des droits fondamentaux de l'Union européenne, qui est un acte législatif contraignant. Elle protège et promeut un large éventail de droits liés à la dignité humaine, à la liberté, à l'égalité et à la solidarité, et toutes les juridictions nationales peuvent l'appliquer dans les cas où le droit de l'Union est mis en œuvre et est pertinent pour la décision judiciaire définitive.

Depuis 2009, la charte a le même statut juridique que les traités, le droit primaire de l'Union sur lequel se fonde la législation de l'Union européenne. Les institutions européennes doivent s'y conformer dans toutes leurs actions et les États membres de l'UE doivent s'y conformer lorsqu'ils mettent en œuvre le droit de l'Union.

Quand les États membres doivent-ils se conformer à la charte?

– Lorsque les États membres conviennent au Conseil et avec le Parlement européen d'adopter une nouvelle législation de l'Union, il est souvent nécessaire de donner effet à cette législation par des mesures nationales d'exécution de cette législation.

– Lorsque les États membres adoptent ou modifient des lois sur une question où le droit de l'Union impose des obligations concrètes, leurs lois ne peuvent pas être contraires au droit de l'Union, charte incluse, car cette action législative constitue une mise en œuvre du droit de l'Union.

– Les programmes de financement de l'Union sont inscrits dans la législation de l'Union européenne. Les États membres doivent s'assurer que cet argent est dépensé conformément aux règles de cette législation. Lorsqu'ils mettent en œuvre des programmes de financement, ils appliquent le droit de l'Union.

– Lorsqu'ils adoptent ou modifient des lois dans un domaine où l'Union n'est pas compétente et où il n'existe aucune législation de l'Union, les États membres ne mettent pas en œuvre le droit de l'Union. Dans ce cas, ils ne sont pas liés par la charte. Toutefois, de nombreux droits fondamentaux inscrits dans la charte sont en même temps énoncés dans les constitutions et la jurisprudence des États membres ainsi que dans la convention européenne des droits de l'homme, dont tous les États membres de l'Union sont signataires.

[1] Charte des droits fondamentaux de l'Union européenne (JO C 326 du 26.10.2012, p. 391).

Afin d'améliorer la connaissance de la charte par tous, la Commission européenne publie depuis 2010 des rapports sur son application. Cette édition est la première à suivre une nouvelle approche, annoncée dans la **stratégie visant à renforcer l'application de la charte des droits fondamentaux dans l'UE** (la stratégie relative à la charte)[2]. Le rapport annuel s'intéressera à un sujet spécifique régi par le droit de l'Union et examinera de plus près les bonnes pratiques adoptées et les difficultés rencontrées par les États membres dans ce domaine. Cette nouvelle approche permet d'étudier les évolutions systémiques, de façon à illustrer la manière dont différents droits peuvent se renforcer mutuellement et dont les changements politiques, sociétaux et économiques peuvent affecter un certain nombre de droits en même temps.

L'édition 2021 a pour thème la **protection des droits fondamentaux à l'ère numérique** et va dans le même sens que l'accent stratégique que la Commission européenne a placé sur la transition numérique.

Sur quelles informations repose le présent rapport?

Le présent rapport a été établi à partir:

– des contributions des États membres de l'Union, qui ont été invités à fournir des informations en fonction de leurs perspectives nationales respectives[3];

– d'une consultation ciblée menée auprès des organisations faîtières des organisations de la société civile (OSC) européennes actives dans le domaine des droits fondamentaux; et

– de rapports préparés par des agences de l'Union, notamment des rapports annuels sur les droits fondamentaux de l'Agence des droits fondamentaux de l'Union européenne (FRA)[4], qui contiennent une section sur les droits fondamentaux et la numérisation.

2. Mettre en œuvre la nouvelle stratégie visant à renforcer l'application de la charte des droits fondamentaux dans l'Union européenne

La stratégie relative à la charte, adoptée par la Commission en 2020, vise à garantir que la charte est appliquée au maximum de son potentiel, faisant des droits fondamentaux une réalité pour tous. Elle fixe le cadre des travaux conjoints sur les droits fondamentaux dans l'ensemble de l'Union pour les dix prochaines années et bénéficie du soutien total des États membres[5]. Les quatre priorités qui guident la mise en œuvre des objectifs fixés dans la stratégie relative à la charte sont expliquées ci-dessous.

2.1 Garantir et suivre l'application effective de la charte par les États membres

Les administrations nationales et locales, les parlements et les services chargés de faire respecter la législation jouent un rôle essentiel dans la promotion et la protection des droits

[2] Communication de la Commission — Stratégie pour renforcer l'application de la charte des droits fondamentaux dans l'UE, COM(2020) 711 final.
[3] Les États membres ont apporté leurs contributions dans le cadre du groupe «Droits fondamentaux, droits des citoyens et libre circulation des personnes» du Conseil (FREMP).
[4] https://fra.europa.eu/en/publication/2021/fundamental-rights-report-2021
[5] https://data.consilium.europa.eu/doc/document/ST-6795-2021-INIT/fr/pdf

consacrés par la charte et dans la création d'un environnement favorable aux organisations de la société civile et aux défenseurs des droits. La Commission travaille en étroite collaboration avec les États membres afin de les aider à mettre en œuvre le droit et les politiques de l'Union de manière effective et dans le plein respect de la charte.

La Commission aide également les États membres à mettre en œuvre les **programmes financés par l'Union** tout en se conformant à la charte. Le règlement portant dispositions communes[6] définit les règles à respecter pour l'utilisation de plusieurs fonds de l'Union[7]. Il exige des États membres qu'ils mettent en place et utilisent des mécanismes efficaces pour garantir le respect de la charte par les programmes financés par l'Union, tels que des modalités d'information du comité de suivi en ce qui concerne les cas de non-respect de la charte dans des opérations soutenues par les fonds et les plaintes concernant la charte. La Commission continuera de fournir une assistance technique afin d'aider les États membres à s'assurer que les programmes soutenus par des fonds de l'Union sont conçus et mis en œuvre dans le respect de la charte.

Dans le cadre d'un programme de financement spécifique, à savoir le programme «Citoyens, égalité, droits et valeurs» (CERV), la Commission a créé de nouvelles **possibilités pour les autorités nationales, régionales et locales** de recevoir un financement pour des projets visant à promouvoir une culture des valeurs et à mieux faire connaître la charte[8]. Les villes jouent un rôle important dans la promotion de cette culture et la protection des droits fondamentaux. Un certain nombre de villes ont rejoint un réseau de «villes des droits de l'homme» et intègrent les droits fondamentaux dans leurs politiques[9]. La FRA a publié un rapport intitulé «Human Rights in the EU: a framework for reinforcing rights locally» [«Les droits de l'homme dans l'UE: un cadre pour renforcer les droits au niveau local»] lors de son forum sur les droits fondamentaux organisé en octobre 2021[10]. Le cadre comprend des outils pour aider les maires, les gouvernements et administrations locaux et les organisations de base à intégrer les normes relatives aux droits de l'homme dans leur travail. Dans le cadre du suivi du plan d'action de l'UE contre le racisme 2020-2025[11], la Commission a lancé un «Prix de la ou des capitales européennes de l'inclusion et de la diversité» en novembre 2021[12]. Ce prix récompensera les bonnes pratiques qui peuvent constituer une

[6] Règlement (UE) 2021/1060 du Parlement européen et du Conseil du 24 juin 2021 portant dispositions communes relatives au Fonds européen de développement régional, au Fonds social européen plus, au Fonds de cohésion, au Fonds pour une transition juste et au Fonds européen pour les affaires maritimes, la pêche et l'aquaculture, et établissant les règles financières applicables à ces Fonds et au Fonds «Asile, migration et intégration», au Fonds pour la sécurité intérieure et à l'instrument de soutien financier à la gestion des frontières et à la politique des visas (JO L 231 du 30.6.2021, p. 159).

[7] Pour la période 2021-2027: le Fonds européen de développement régional, le Fonds de cohésion, le Fonds social européen plus, le Fonds pour une transition juste, le Fonds européen pour les affaires maritimes et la pêche, le Fonds «Asile, et migration», le Fonds pour la sécurité intérieure et l'instrument relatif à la gestion des frontières et aux visas.

[8] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/cerv. Dans le cadre de l'appel à propositions pour le jumelage de villes et les réseaux de villes, le programme CERV met à disposition 4,2 millions d'EUR en 2021. De plus amples informations sont disponibles à l'adresse suivante: Funding & tenders (europa.eu).

[9] https://humanrightscities.net/.

[10] https://fra.europa.eu/en/publication/2021/human-rights-cities-framework.

[11] Communication de la Commission «Une Union de l'égalité: plan d'action de l'UE contre le racisme 2020-2025», COM (2020) 565 final.

[12] https://eudiversity2022.eu/the-award/apply/.

source d'inspiration pour d'autres villes et régions européennes dans la création d'environnements plus diversifiés et inclusifs pour leurs habitants.

Dans la stratégie relative à la charte, la Commission a invité les États membres à désigner un **point focal pour la charte** afin de faciliter davantage la coopération et l'échange d'informations sur l'application de la charte. À ce jour, 17 États membres en ont désigné un. Ces points focaux jouent un rôle essentiel dans la diffusion d'informations et de bonnes pratiques pour faire connaître la charte et coordonner les efforts de renforcement des capacités dans chaque pays. Leur travail contribue à étoffer la nouvelle page web consacrée aux meilleures pratiques des États membres en ce qui concerne la charte, lancée sur le portail européen e-Justice en décembre 2021[13].

En tant que gardienne des traités, la Commission a pris des mesures concrètes pour garantir le respect des droits consacrés par la charte dans les cas où la législation ou les pratiques nationales mettant en œuvre le droit de l'UE violent ces droits, par exemple en engageant des procédures d'infraction. En particulier, la Commission a pris des mesures afin de garantir le respect des droits suivants:

- le droit à la liberté d'association des organisations non gouvernementales et à la protection des données à caractère personnel de leurs donateurs;
- le droit à la liberté académique;
- le droit à la liberté d'expression et au pluralisme des médias;
- le droit à la dignité humaine;
- le droit au respect de la vie privée;
- le droit de chacun, y compris des personnes LGBTIQ, de ne pas faire l'objet de discriminations fondées sur le sexe et l'orientation sexuelle.

La Commission a suivi, dans tous les États membres, les mesures d'urgence prises pendant la pandémie de COVID-19 et leurs conséquences, notamment sur l'état de droit, sur les droits fondamentaux et sur le respect des autres dispositions du droit de l'Union, comme en témoigne le **rapport 2021 sur l'état de droit,** avec les chapitres par pays[14].

2.2 Donner des moyens d'action aux organisations de la société civile, aux défenseurs des droits et aux professionnels de la justice

Les organisations de la société civile (OSC) et les organismes nationaux indépendants de défense des droits de l'homme sont des partenaires essentiels des institutions de l'Union et des États membres lorsqu'il s'agit de promouvoir et protéger les droits fondamentaux, la démocratie et l'état de droit. Ces organisations contribuent à sensibiliser les citoyens aux droits que leur confère la charte et à les aider à bénéficier d'une protection juridictionnelle effective. Elles doivent pouvoir travailler dans un environnement favorable, exempt de contraintes réglementaires excessives, d'obstacles au financement ou même de campagnes de dénigrement[15], et elles doivent également être en mesure de renforcer leurs capacités. Certains États membres ne disposent toujours pas d'**institutions nationales de défense des**

[13] https://e-justice.europa.eu/37134/FR/member_states_best_practices_on_the_charter?init=true.
[14] COM(2021) 700 final, disponible à l'adresse suivante: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/rule-law-mechanism/2021-rule-law-report_fr.
[15] FRA, Protecting the civic space, 2021, https://fra.europa.eu/en/publication/2021/civic-space-challenges.

droits de l'homme pleinement opérationnelles, qui constituent des maillons essentiels entre les pouvoirs publics et la société civile[16]. Les États membres sont invités à mettre en place de telles institutions et à veiller à ce que celles-ci aient les moyens de travailler en toute indépendance.

La Commission **suit** de près **la situation des OSC** et rend compte des évolutions relatives au cadre de la société civile dans son rapport annuel sur l'état de droit. Le rapport 2021 sur l'état de droit indique que les OSC ont été touchées par la pandémie de COVID-19, non seulement en raison des limites imposées à la liberté de circulation et de réunion, mais aussi du point de vue des financements. Il ressort du rapport que, dans l'ensemble, la société civile n'a que faiblement participé à l'élaboration et à la mise en œuvre des mesures relatives à la COVID-19[17]. Le rapport 2020 sur l'état de droit avait recensé des mesures qui restreignaient la liberté d'expression des OSC[18]. Les données recueillies par la FRA[19] montrent en effet que de nombreuses OSC estiment que les mesures nationales de lutte contre la pandémie ont une incidence négative sur leurs activités depuis mars 2020. Bien qu'elles aient fait état d'une demande croissante, la majorité d'entre elles ont rencontré des difficultés pour continuer à fournir leurs services. Au rang des difficultés pratiques figurent l'annulation d'activités, les conséquences psychologiques sur le personnel et la réduction de la contribution des bénévoles au travail.

La Commission continue de **soutenir les défenseurs des droits et les OSC** au moyen de financements spécifiques, tels qu'un appel à propositions, doté d'un budget de 51 millions d'EUR pour la période 2021-2022, sur la protection et la promotion des valeurs de l'Union, qui s'adresse entièrement aux petites OSC et aux OSC de base[20]. Un appel spécifique d'un montant de 2 millions d'EUR a été lancé pour soutenir les contentieux et le renforcement des capacités liés à l'application de la charte[21].

La Commission promeut également le renforcement des capacités et la **sensibilisation des juges et autres professionnels de la justice à la charte**. En décembre 2020, la Commission a adopté une nouvelle stratégie européenne de formation judiciaire pour la période 2021-2024[22]. En mars 2021, elle a lancé un appel à propositions afin de soutenir des projets de formation judiciaire incluant les droits fondamentaux, comme l'une de ses principales

[16] Voir stratégie relative à la charte, op.cit., section 2 «Donner des moyens d'action aux organisations de la société civile, aux défenseurs des droits et aux professionnels de la justice». Voir rapport de la FRA «Strong and effective national human rights institutions – challenges, promising practices and opportunities», disponible à l'adresse suivante: https://fra.europa.eu/en/publication/2020/strong-effective-nhris. Les chapitres par pays du rapport 2021 sur l'état de droit rendent compte du statut de l'accréditation des institutions nationales de défense des droits de l'homme (https://ec.europa.eu/info/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/rule-law-mechanism/2021-rule-law-report/2021-rule-law-report-communication-and-country-chapters_fr).

[17] Rapport 2021 sur l'état de droit, p. 24.

[18] Rapport 2020 sur l'état de droit, p. 16. EUR-Lex - 52020SC0316 - FR - EUR-Lex (europa.eu).

[19] https://fra.europa.eu/en/news/2021/findings-fra-consultation-covid-19-impact-civil-society. FRA, Protecting the civic space, op. cit., voir section 1.3. «COVID-19 exacerbates challenges faced by civil society», p. 16.

[20] Programme de travail du programme CERV pour la période 2021-2022.

[21] Call for proposals to promote capacity building and awareness on the EU Charter of Fundamental Rights.

[22] COM(2020) 713 final.

priorités[23]. Plusieurs projets de formation judiciaire relative à la charte, cofinancés par la Commission dans le cadre de son programme «Justice» (2014-2020), ont été mis en œuvre[24]. Du matériel de formation judiciaire sur les droits fondamentaux est mis à la disposition des professionnels de la justice sur une plateforme lancée en décembre 2020[25].

2.3 Faire pleinement usage de la charte des droits fondamentaux dans le processus décisionnel de l'Union européenne

Les institutions, organes et organismes de l'UE doivent respecter la charte dans toute action. La Commission renforce ses capacités internes en matière de respect de la charte et met à jour sa boîte à outils pour une meilleure réglementation[26], ainsi que les orientations de 2011 sur la prise en compte des droits fondamentaux dans les analyses d'impact[27]. Elle met également en place une formation spécifique sur la charte et un outil d'apprentissage en ligne pour aider le personnel à évaluer l'incidence des politiques et des propositions législatives de la Commission sur les droits fondamentaux. L'outil d'apprentissage en ligne sera mis à la disposition du public et pourrait constituer une ressource utile, avec la mise à jour de la boîte à outils pour une meilleure réglementation et des orientations, à la fois pour les autres institutions de l'Union et pour les législateurs et responsables politiques dans les États membres. La Commission est prête à aider le Parlement européen et le Conseil à faire en sorte qu'ils appliquent la charte de manière effective dans leurs travaux.

2.4 Sensibiliser davantage les citoyens

Parallèlement à l'adoption du présent rapport, la Commission lance une campagne de sensibilisation à la charte afin d'informer les citoyens sur leurs droits et sur les instances auxquelles s'adresser en cas de violation de leurs droits. La campagne sera menée en ligne, au moyen d'événements médiatiques et de médias sociaux, en utilisant le hashtag **#RightHereRightNow**. Elle sera axée sur une série de droits spécifiques, tels que la non-discrimination et l'égalité, les droits de l'enfant, la liberté d'expression et d'information, ainsi que le droit à un recours effectif et à accéder à un tribunal impartial. Des partenaires clés participeront aux actions de sensibilisation, comme les OSC, les institutions et les organes nationaux de défense des droits de l'homme, la FRA et encore d'autres organes et agences de l'Union. Des liens seront établis avec d'autres campagnes d'information sur les droits et avec la conférence sur l'avenir de l'Europe. La Commission a également traduit sa page web consacrée à la charte sur le site Europa dans toutes les langues officielles de l'Union[28] et a lancé une nouvelle version du portail européen e-Justice, qui contient des informations sur l'application de la charte et les services où obtenir de l'aide[29].

[23] Programme «Justice», JUST-2021-JTRA appel à propositions, disponible à l'adresse: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home.
[24] Par exemple: https://era-comm.eu/charter-of-fundamental-rights/seminar-materials/; http://charterclick.ittig.cnr.it:3000/; http://help.elearning.ext.coe.int/.
[25] La plateforme européenne de formation.
[26] Boîte à outils pour une meilleure réglementation |Commission européenne (europa.eu).
[27] Orientations opérationnelles sur la prise en compte des droits fondamentaux dans les analyses d'impact de la Commission européenne |Commission européenne (europa.eu).
[28] Vos droits dans l'UE |Commission européenne (europa.eu).
[29] https://e-justice.europa.eu/581/FR/fundamental_rights.

3. Faire de la charte la boussole de l'UE à l'ère numérique

La Commission européenne s'est donné comme priorité de façonner la transition numérique d'une manière qui profite à tous et ne laisse personne de côté. Le «monde hors ligne» et le «monde en ligne», comme on les appelait autrefois, deviennent aujourd'hui indissociables. Il en résulte un certain nombre de difficultés pour veiller à ce que les droits fondamentaux soient respectés dans un environnement numérique en mutation rapide.

Les technologies numériques deviennent peu à peu omniprésentes dans tous les domaines de notre société et peuvent être utilisées de nombreuses manières différentes et souvent bénéfiques. Les solutions numériques font progresser la recherche scientifique, permettent d'augmenter la production industrielle, simplifient la transition vers le développement durable, facilitent la fourniture d'une variété de services, et constituent aujourd'hui le principal moyen de communication privé et public. Elles augmentent les possibilités des citoyens de participer au débat démocratique et de s'informer sur n'importe quel sujet. Les systèmes d'intelligence artificielle, en particulier, peuvent être utilisés pour favoriser l'innovation et créer de la richesse. Ils peuvent servir d'outils aux citoyens dans tous les domaines de la vie, par exemple dans les soins de santé, pour les traductions ou pour aider à la prise de décision. L'automatisation numérique aide à organiser le travail de manière plus efficace et permet des niveaux de coordination sans précédent. La collecte de données sur les activités humaines et leurs effets aide les citoyens à comprendre et à façonner le monde.

Parallèlement, certaines utilisations de la technologie risquent de limiter l'efficacité de la protection garantie par les droits fondamentaux. La diffusion de contenus illicites tels que les discours de haine et la pédopornographie menace le droit à la dignité de la victime et la propagation de la désinformation met en péril le débat démocratique et notre droit d'accès à l'information. Lorsque les procédures ou même les décisions sont automatisées, il peut être difficile de garantir la transparence et la responsabilité des résultats, par exemple lorsqu'un logiciel complexe est utilisé pour décider de la répartition des tâches. Lorsque les informations font défaut ou sont difficiles à obtenir, il peut être compliqué d'apprécier les violations des droits fondamentaux et d'y remédier.

Plus un outil automatisé s'appuie sur des facteurs externes, comme des données, des entrées provenant de personnes ou d'autres systèmes pour produire un résultat, plus il est difficile de garantir qu'un tel outil n'enfreint pas d'emblée certains droits, par exemple parce qu'il intègre certains préjugés qui sont susceptibles d'influer en fin de compte sur la prise de décision dans des environnements de travail. Plus on recueille de données sur les citoyens, plus il est facile de les surveiller et de porter atteinte à leur vie privée. Les effets de réseau peuvent réduire le pouvoir des citoyens vis-à-vis des grandes organisations, par exemple sur les marchés en ligne ou les plateformes de travail, où ils ont peu de pouvoir de négociation ou de possibilités de s'organiser. Simultanément, les plateformes de médias sociaux sont également utilisées pour propager la haine et diffuser des contenus illicites, par exemple répandre des discours de haine illégaux, du matériel pédopornographique ou des contenus à caractère terroriste. En outre, il reste encore beaucoup de travail à accomplir pour que chacun puisse bénéficier de nouveaux outils utiles là où l'accès à l'internet, les équipements ou les connaissances sur la manière d'utiliser ces outils sont rares.

Ces difficultés peuvent se présenter de manière individuelle ou combinée, selon le contexte. Elles peuvent se renforcer mutuellement et affecter plusieurs droits fondamentaux à la fois, ce

qui doit être pris en compte au moment de leur trouver une solution. Le présent rapport décrit quelques-uns des principaux aspects au regard desquels l'utilisation des technologies numériques fait obstacle aux droits fondamentaux. Il montre quels droits sont affectés dans ces contextes, comment la situation évolue dans les États membres de l'Union, et comment les États membres et la Commission européenne ont recours à la charte pour surmonter les différents obstacles et sauvegarder et promouvoir les droits des citoyens.

4. Relever les défis liés à la modération des contenus en ligne

Les intermédiaires en ligne tels que les plateformes de médias sociaux jouent un rôle important dans la vie de chaque individu et favorisent de nouvelles formes d'interactions entre les citoyens, les administrations publiques et les entreprises. Leur utilisation a conduit à une augmentation significative des informations mises à la disposition des citoyens et offre à ces derniers de plus grandes possibilités d'exercer leur droit à la liberté d'expression et d'accéder à l'information, créant également de multiples espaces pour l'activisme en ligne et le rapprochement des citoyens et de la société civile.

Les grandes plateformes, les nouvelles places publiques

- Certaines plateformes en ligne sont devenues si importantes pour faciliter l'échange d'informations qu'elles jouent un rôle majeur dans le débat démocratique.
- Étant donné que plus de la moitié de la population de l'Union, dont près de 90 % des jeunes âgées de 16 à 24 ans, utilise les médias sociaux, les effets de la conception et des normes de ces plateformes ont une incidence sociétale considérable[30].
- Les outils et les mécanismes utilisés par ces plateformes pour modérer des contenus et encourager les internautes à passer le plus de temps possible à utiliser leurs services jouent un rôle majeur dans la formation des informations et des opinions que les internautes rencontrent en ligne.
- La lutte contre la diffusion des contenus illicites sur ces grandes plateformes est ardue car ces dernières sont devenues des espaces publics d'échange d'informations sans devoir légalement répondre de considérations d'intérêt public.

Parallèlement, l'utilisation des plateformes en ligne amplifie les problèmes sociétaux comme la polarisation[31] ou la diffusion de contenus illicites, avec souvent des effets négatifs importants sur les droits fondamentaux, tels que la protection des droits de l'enfant, la protection des consommateurs, la liberté de recevoir et de partager des informations et la protection de la propriété intellectuelle.

L'ampleur et la rapidité de la diffusion des contenus en ligne qui ne sont pas illicites en soi, comme la désinformation et les théories du complot, peuvent nuire au débat démocratique, à

[30] https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_sk_dskl_i.

[31] Voir les exemples de risques sociétaux systémiques émergents posés par les plateformes en ligne dans l'analyse d'impact accompagnant la proposition de règlement relatif à un marché intérieur des services numériques (législation sur les services numériques), SWD(2020) 348 final, p. 40 («analyse d'impact concernant la législation sur les services numériques»).

la confiance dans les institutions et, comme on l'a vu dans le sillage de la pandémie de COVID-19, à la santé, à la sécurité et à l'égalité de traitement.

La démocratie dans l'Union se heurte à de nombreux obstacles, parmi lesquels le populisme, l'accentuation des inégalités, un débat politique de plus en plus polarisé et l'érosion de la confiance du public dans les processus démocratiques due à la désinformation[32]. Ces phénomènes sont exacerbés par l'ingérence coordonnée de pays tiers ou d'intérêts privés dans les élections, par la diffusion de la désinformation et par le manque de transparence et de responsabilité des publicités politiques ciblées. Des préoccupations sont également exprimées quant au fait que certains groupes ne sont pas suffisamment inclus ou mobilisés, comme les jeunes, les personnes âgées ou les personnes handicapées. Les minorités ethniques, notamment les communautés roms, les personnes LGBTIQ et les femmes hésitent, à un degré variable et en fonction du contexte, à s'engager en tant que candidats politiques par crainte des intimidations, des menaces, du harcèlement et des discours haineux. Dans ces circonstances, les mesures visant à protéger les droits fondamentaux contribuent directement à préserver les valeurs de l'Union, à savoir une société durable, égalitaire, démocratique et participative, où règnent la tolérance, la non-discrimination et le pluralisme.

La liberté d'expression, y compris en ligne, est au cœur de toute démocratie. Toute mesure législative ou non législative relative à la modération des contenus et à la responsabilité des intermédiaires en ligne pour les contenus de leurs services doit tenir compte du fait que le droit à la liberté d'expression inclut le droit d'exprimer des idées qui peuvent être considérées comme critiques, offensantes, insultantes ou controversées et que le droit à la liberté d'expression ne peut être limité que dans des conditions très strictes, y compris en ce qui concerne la diffusion des contenus prétendument illicites comme du matériel pour discours de haine. La Cour européenne des droits de l'homme a toutefois également précisé que les États sont autorisés à prévenir, et peuvent même avoir l'obligation positive de le faire, toutes les formes d'expression qui propagent, incitent à, promeuvent ou justifient la haine à l'égard de personnes ou de groupes appartenant à une ethnie ou à une religion particulière[33].

Le plus souvent, la désinformation et la mésinformation ne sont pas illégales, même si elles peuvent être perturbantes ou offensantes. Si, pour les discours protégés par la liberté d'expression, l'obligation première de l'État est de s'abstenir de toute ingérence et de toute censure, l'État a également une obligation positive de garantir un environnement favorable à un débat public inclusif et pluraliste, notamment en ce qui concerne les élections, et à l'exercice de la liberté des médias. Ces mesures vont au-delà du domaine de la modération des contenus et vont de pair avec des actions d'éducation et d'information plus fondamentales.

Les acteurs privés tels que les plateformes en ligne définissent leurs propres conditions et leur propre modèle économique dans l'exercice de leurs droits à la liberté contractuelle et à l'exercice d'une activité, sans instructions de l'État quant au type de contenus qu'elles seraient tenues d'héberger. Dans ce contexte, elles pourraient prendre des mesures qui nuisent

[32] Étude du Parlement européen demandée par la sous-commission DROI «The impact of disinformation on democratic processes and human rights in the world», Carme Colomina, Héctor Sánchez Margalef, Richard Youngs, disponible à l'adresse: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf.

[33] Arrêt du 6 juillet 2006 dans l'affaire Erbakan c. Turquie, point 56.

de manière significative aux utilisateurs et à leurs droits. Il n'existe pas toujours de recours juridique contre ces décisions privées, permettant de les mettre en balance avec les droits et les intérêts légitimes des individus et de garantir un certain degré de prévisibilité. Lorsque les plateformes en ligne retirent de manière excessive des contenus licites, elles peuvent restreindre considérablement la liberté d'expression et d'information.

4.1 Situation au niveau des États membres

Lors de la **consultation ciblée** menée aux fins du présent rapport, les acteurs de la société civile ont fait état de problèmes dans les États membres causés par certains contenus illicites en ligne, tels que des campagnes de dénigrement et des attaques contre ceux et celles qui s'efforcent de protéger les droits d'autrui. Il a été indiqué que les femmes, en particulier les femmes de couleur ou celles appartenant à des groupes vulnérables tels que les migrants et les Roms, ainsi que les personnes LGBTIQ, sont visées de manière disproportionnée. Les enfants qui utilisent les plateformes en ligne sont exposés à des contenus inappropriés, préjudiciables et violents, ainsi qu'à des prédateurs en ligne, une situation qui augmente également les risques de manipulation psychologique et de recrutement dans des environnements extrémistes. La violence sexuelle à l'encontre des enfants a été jugée amplifiée par l'internet, par exemple en raison de l'augmentation de la demande de pédopornographie.

Les organisations de la société civile ont également pointé du doigt la désinformation comme étant un problème affectant la santé, la sécurité et le débat démocratique dans plusieurs États membres. Bon nombre des préoccupations exprimées avaient trait au manque de transparence (étiquettes, alertes de partage, notifications d'exposition) et au manque d'éducation aux médias concernant les contenus faux ou trompeurs.

Tout en considérant la diffusion de contenus illicites et de désinformation comme une menace, les OSC consultées ont également mis en garde contre les effets que peuvent avoir sur la liberté d'expression des politiques de modération mal calibrées qui seraient utilisées pour lutter contre ces menaces. Les OSC ont indiqué que la protection des droits d'auteur a été détournée pour faire taire des voix en ligne et que les lois sur la diffamation et l'apologie du terrorisme ont été utilisées pour réprimer des individus. La faible précision des systèmes automatisés de modération des contenus, en particulier lorsque ces systèmes sont appliqués à des contenus dont l'évaluation de légalité doit être fortement contextualisée, a suscité des inquiétudes quant à l'incidence injustifiée que peut avoir, sur la liberté d'expression, le fait de supprimer des contenus de manière excessivement globale et de passer sous silence certaines déclarations et opinions, y compris celles de minorités. Selon certains universitaires et répondants à la consultation ciblée, l'utilisation d'algorithmes pour personnaliser l'affichage des contenus pour les utilisateurs peut également fausser le débat démocratique, puisqu'elle vise souvent à accroître les recettes publicitaires et n'est guère guidée par l'objectif de fournir au public, dans son intérêt, des informations fiables. Des lanceurs d'alerte ont avancé des allégations similaires dans la presse, affirmant que les algorithmes utilisés pour adapter le contenu montré aux utilisateurs sont nocifs[34]. Au-delà des effets de leur utilisation sur les droits fondamentaux, il a été affirmé, par des répondants à la consultation ciblée, que ces systèmes étaient souvent utilisés de manière non transparente ou pas entièrement transparente, et avec peu de responsabilisation quant à leurs résultats.

[34] Voir par exemple https://www.theguardian.com/technology/2021/oct/10/frances-haugen-takes-on-facebook-the-making-of-a-modern-us-hero.

Plusieurs États membres de l'Union ont réglementé les services numériques établis sur leur territoire. Ces lois visent à garantir que les fournisseurs de services respectent certaines règles de procédure lorsque les utilisateurs ou les autorités signalent des contenus illicites. Elles couvrent parfois des catégories précises de contenus illicites, comme les violations de droits d'auteur ou les discours haineux illégaux. Toutefois, les exigences précises de ces lois divergent souvent sur plusieurs points, tels que:

- les informations nécessaires pour signaler des contenus illicites;
- la possibilité pour ceux qui ont publié ces contenus de réagir;
- le délai accordé aux prestataires de services pour réagir;
- les possibles mesures obligatoires contre les signalements abusifs; ou
- la possibilité de soumettre les cas litigieux à un tiers indépendant.

Plus récemment, face aux préoccupations croissantes suscitées par la propagation de discours haineux et de contenus à caractère terroriste, plusieurs États membres ont adopté, proposé ou envisagent d'adopter des règles supplémentaires axées notamment sur certaines catégories de discours haineux et couvrant parfois aussi les prestataires de services établis en dehors de leur territoire. Il existe toutefois une fragmentation juridique importante résultant des efforts individuels menés par les États membres pour lutter contre les contenus illicites en ligne et pour fournir différents types de garanties pour la liberté d'expression. Plusieurs États membres[35], ainsi que le Conseil[36] et le Parlement européen[37] ont demandé que ces préoccupations communes soient traitées à l'échelon de l'Union. En outre, un certain nombre d'États membres ont observé que le manque de coopération transfrontière entre les autorités nationales entravait la surveillance efficace des plateformes en ligne qui exercent des activités au-delà des frontières[38].

4.2 Réponse apportée par les politiques de l'Union

À la demande des États membres, plusieurs initiatives sectorielles ont été adoptées à l'échelle de l'Union pour s'attaquer au problème de certains types de contenus illicites, tels que ceux liés au terrorisme, aux abus sexuels commis sur des enfants, à l'incitation à la haine et à la violence, à la traite des êtres humains, aux produits dangereux et aux violations des droits d'auteur, tout en assurant simultanément la protection les droits fondamentaux.

La directive «Services de médias audiovisuels»

La **directive «Services de médias audiovisuels»** (directive SMA) révisée a été adoptée en 2018. Elle comprend des mesures visant à protéger les mineurs contre les contenus audiovisuels et les communications commerciales audiovisuelles susceptibles de leur causer un préjudice physique, mental ou moral. De même, les États membres doivent veiller à ce que

[35] https://digital-strategy.ec.europa.eu/en/summary-report-open-public-consultation-digital-services-act-package
[36] Conclusions du Conseil du 9 juin 2020 intitulées «Façonner l'avenir numérique de l'Europe» et conclusions de la réunion extraordinaire du Conseil européen des 1er et 2 octobre 2020.
[37] Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission concernant la législation sur les services numériques: améliorer le fonctionnement du marché unique [2020/2018 (INL)]; Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission concernant la législation sur les services numériques: adaptation des règles de droit commercial et civil pour les entités commerciales opérant en ligne [2020/2019(INL)].
[38] Analyse d'impact concernant la législation sur les services numériques, section 2.3.6. Limited cooperation among Member States and lack of trust.

les services de médias audiovisuels ne contiennent aucune incitation à la violence ou à la haine fondée sur l'un des motifs visés à l'article 21 de la charte des droits fondamentaux de l'Union européenne. La date limite de transposition de cette directive était le 19 septembre 2020. En novembre 2020, la Commission a engagé des procédures d'infraction (lettres de mise en demeure) contre 23 États membres qui n'avaient pas transposé la directive et ils ont été nombreux à la transposer l'année suivante. En septembre 2021, la Commission a adressé un deuxième avertissement (avis motivé) à neuf États membres pour non-communication de la transposition complète. La mise en œuvre de la directive SMA révisée est essentielle non seulement pour les acteurs du marché, mais aussi pour les individus (y compris les téléspectateurs et les mineurs).

Directive sur le droit d'auteur dans le marché unique numérique

La **directive sur le droit d'auteur**[39] a été adoptée en avril 2019 et vise à garantir aux titulaires de droits une compensation équitable pour l'utilisation de leur œuvre. Ce faisant, elle instaure un équilibre entre des droits fondamentaux concurrents tels que le droit à la propriété intellectuelle, la liberté d'expression et d'information, la liberté des sciences et le droit à l'éducation et à la diversité culturelle. La directive introduit des exceptions obligatoires au droit d'auteur qui protègent la liberté d'expression des utilisateurs qui génèrent et téléchargent du contenu sur les services de partage de contenus en ligne. En vertu de la directive, la Commission était tenue d'organiser un dialogue entre les parties prenantes afin qu'elles puissent discuter des bonnes pratiques en matière de coopération entre les fournisseurs de services de partage de contenus en ligne et les titulaires de droits, en tenant particulièrement compte de la nécessité de maintenir un équilibre entre les droits fondamentaux et le recours aux exceptions et aux limitations. À la suite de ce dialogue, la Commission a adopté, en juin 2021, des orientations visant à soutenir une application cohérente de l'article 17 de la directive qui établit de nouvelles règles sur l'utilisation de contenus protégés par les services de partage de contenus en ligne[40]. Les orientations fournissent des indications pratiques sur les principales dispositions de l'article 17, qui aident les acteurs du marché à mieux se conformer aux lois nationales fondées sur la directive et qui tiennent compte des avis recueillis auprès des États membres et des parties prenantes.

Code de conduite pour la lutte contre les discours haineux illégaux à caractère raciste et xénophobe

En 2016, la Commission a signé un **code de conduite** volontaire avec les principales plateformes en ligne afin de s'assurer que les notifications de **discours haineux illégaux à caractère raciste et xénophobe** sont rapidement évaluées au regard non seulement des conditions d'utilisation des plateformes, mais aussi des lois des États membres utilisées pour mettre en œuvre le droit de l'Union qui érige en infractions les discours haineux à caractère raciste et xénophobe[41]. Le respect du code de conduite est contrôlé régulièrement[42].

[39] Directive (UE) 2019/790 sur le droit d'auteur et les droits voisins dans le marché unique numérique, JO L 130 du 17.5.2019.
[40] Communication de la Commission, Orientations relatives à l'article 17 de la directive 2019/790 sur le droit d'auteur dans le marché unique numérique, COM(2021) 288 final.
[41] Décision-cadre 2008/913/JAI du Conseil du 28 novembre 2008 sur la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal, JO L 328 du 6.12.2008.

L'application du code donne de bons résultats et a également favorisé une approche collaborative entre les plateformes en ligne, les États membres et la société civile pour assurer une modération de haute qualité des contenus lorsqu'une compréhension approfondie du contexte culturel, linguistique et historique des contenus litigieux est nécessaire.

Recommandation sur la sécurité des journalistes et autres professionnels des médias

La sécurité est devenue une préoccupation majeure pour les journalistes en raison des incitations à la haine en ligne, des menaces de violence physique, mais aussi des risques en matière de cybersécurité et de surveillance illégale. Le 16 septembre 2021, la Commission européenne a publié **une recommandation sur la protection, la sécurité et le renforcement des moyens d'action des journalistes**[43]. Conformément à cette recommandation, les États membres sont encouragés à promouvoir la coopération entre les plateformes en ligne et les organisations qui possèdent une expertise dans la lutte contre les menaces visant les journalistes, par exemple en encourageant leur rôle potentiel de signaleurs de confiance. Les journalistes et les autres professionnels des médias ne sont pas seulement les cibles de l'incitation à la haine en ligne et des menaces de violence physique, mais peuvent également faire l'objet d'une surveillance illégale, et la recommandation indique que les organes nationaux compétents en matière de cybersécurité devraient, sur demande, aider les journalistes qui cherchent à déterminer si leurs appareils ou comptes en ligne ont été compromis à obtenir les services d'enquêteurs spécialisés dans la cybercriminalistique. Les États membres devraient également promouvoir un dialogue régulier entre ces organes chargés de la cybersécurité, les médias et l'industrie, notamment en vue de favoriser la sensibilisation à la cybersécurité et l'acquisition de compétences numériques chez les journalistes.

Règlement relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne

La sécurité et le respect des droits fondamentaux ne sont pas des objectifs qui se contredisent, mais qui se complètent et forment un tout cohérent. La sécurité des environnements tant en ligne que physiques exige de lutter contre les contenus illicites en ligne. Afin de garantir le retrait des contenus à caractère terroriste, le Parlement européen et le Conseil ont adopté un **règlement relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne** en 2021[44]. Ce règlement contient un certain nombre de garanties pour les droits fondamentaux, en particulier la liberté d'expression. Par exemple, les injonctions de retrait par les autorités nationales ne peuvent être émises que pour les contenus à caractère terroriste tels que définis par le règlement et ces injonctions doivent expliquer pourquoi le matériel est considéré comme du contenu à caractère terroriste. Le règlement exempte les contenus diffusés à des fins éducatives, journalistiques, artistiques ou de recherche et ceux diffusés à des fins de sensibilisation contre les activités terroristes. Les plateformes en ligne ne sont pas tenues d'utiliser des outils automatisés pour détecter de manière proactive ou retirer les

[42] Le dernier exercice d'évaluation a eu lieu en 2021: Le code de conduite de l'UE pour la lutte contre les discours haineux illégaux en ligne |Commission européenne (europa.eu).

[43] Voir la recommandation de la Commission concernant la protection, la sécurité et le renforcement des moyens d'action des journalistes et autres professionnels des médias dans l'Union européenne du 16 septembre 2021, C(2021) 6650 final.

[44] Règlement (CE) 2021/784 concernant la lutte contre la diffusion de contenus à caractère terroriste en ligne, JO L 172 du 17.5.2021.

contenus à caractère terroriste, mais, si des mesures techniques sont utilisées, des garanties, notamment une surveillance et une vérification humaines, doivent être prévues pour s'assurer de l'exactitude. À compter de mars 2023, les États membres et les plateformes en ligne devront également publier des rapports annuels sur les mesures prises pour retirer les contenus à caractère terroriste et sur le fonctionnement de tout outil automatisé susceptible d'avoir été utilisé.

Législation sur la lutte contre les abus sexuels commis contre des enfants en ligne

Alors que l'action réglementaire visant à lutter contre les contenus illicites s'est largement concentrée sur les contenus accessibles au public, tels que ceux publiés sur les médias sociaux ou les sites web, il convient également de relever le défi que représente la lutte contre le **matériel pédopornographique** diffusé par le biais de communications interpersonnelles, y compris dans les outils de communication interpersonnelle des services de médiaux sociaux. **Une législation provisoire**[45]**,** qui est entrée en vigueur en août 2021, fait en sorte que certains services de communication en ligne, tels que le courrier électronique en ligne ou les services de messagerie, peuvent continuer à utiliser, dans la mesure strictement nécessaire, des technologies spécifiques permettant de détecter, signaler et retirer le matériel pédopornographique, tout en instaurant des garde-fous protégeant la vie privée et les données à caractère personnel, conformément au règlement général sur la protection des données. Les mécanismes de détection des abus sexuels commis contre des enfants dans les communications interpersonnelles risquent d'interférer avec plusieurs droits fondamentaux, notamment la confidentialité des communications, la protection des données à caractère personnel ou la liberté d'expression. Le règlement provisoire vise à atténuer ces atteintes en limitant l'utilisation aux technologies les moins intrusives au regard de la vie privée en l'état actuel de la technique dans le secteur. Le règlement prévoit également des mécanismes de recours qui doivent être mis en place pour que les utilisateurs puissent introduire une réclamation auprès des fournisseurs si leurs contenus sont retirés à tort. La Commission élabore également une **proposition de législation** destinée à remplacer cette mesure provisoire et à donner aux fournisseurs de services une sécurité juridique tout en garantissant une approche uniforme de la détection, du retrait et du signalement du matériel pédopornographique et en assurant un juste équilibre entre les droits des enfants et la nécessité de les protéger contre les abus sexuels et le droit à la vie privée et aux communications de tous les utilisateurs de services en ligne.

Stratégie de l'UE visant à lutter contre la traite des êtres humains 2021-2025

La lutte contre le modèle économique en ligne des trafiquants constitue l'une des priorités de la stratégie de l'UE visant à lutter contre la traite des êtres humains 2021-2025[46], présentée par la Commission en avril 2021. Les fournisseurs de services internet et les entreprises connexes font partie de la solution pour renforcer les efforts de lutte contre la traite des êtres

[45] Règlement 2021/1232 relatif à une dérogation temporaire à certaines dispositions de la directive 2002/58/CE en ce qui concerne l'utilisation de technologies par les fournisseurs de services de communications interpersonnelles non fondés sur la numérotation pour le traitement de données à caractère personnel et d'autres données aux fins de la lutte contre les abus sexuels commis contre des enfants en ligne, JO L 274, 30.7.2021.
[46] Communication sur la stratégie de l'UE de lutte contre la traite des êtres humains pour la période 2021-2025, COM(2021) 171 final.

humains grâce à la détection et à la suppression des contenus en ligne associés à l'exploitation et à l'abus de victimes de la traite. La Commission mènera un dialogue avec les entreprises concernées dans le secteur de l'internet et des technologies, afin de réduire le recours aux plateformes en ligne pour le recrutement et l'exploitation des victimes. La Commission facilitera également les éventuels dialogues similaires que les États membres mèneront au niveau national.

Proposition de législation sur les services numériques (règlement)

La proposition de **législation sur les services numériques** (règlement)[47], adoptée par la Commission en décembre 2020 et actuellement en cours d'examen par les colégislateurs, encadre les responsabilités des intermédiaires en ligne. Sans préjudice des règles sectorielles de l'UE, telles que celles sur le droit d'auteur ou sur les contenus à caractère terroriste en ligne, elle établit un ensemble horizontal unique de règles dans l'Union afin de garantir une gouvernance équilibrée de la modération des contenus en ligne.

La proposition garantit une protection appropriée de tous les droits fondamentaux, dont le droit des utilisateurs à la liberté d'expression et à la vie privée, la liberté d'entreprise, la liberté contractuelle des plateformes et les droits de propriété intellectuelle. Elle vise également à atténuer les risques pour les personnes en situation de vulnérabilité et les groupes vulnérables afin de les protéger contre les menaces, les intimidations ou les comportements discriminatoires et entend protéger le droit à la dignité humaine de tous les utilisateurs de services en ligne.

La proposition de règlement vise à atteindre ces objectifs en:

- préservant pour l'essentiel le régime de responsabilité des services intermédiaires en ligne actuellement en place, y compris l'interdiction d'obligations générales de surveillance ou de recherche des faits. Cette approche repose sur la directive sur le commerce électronique[48]. Elle vise: i) à garantir la protection proportionnée et appropriée du droit à la liberté d'expression en limitant les incitations à retirer les contenus licites ainsi que du droit d'exercer une activité commerciale, en garantissant la proportionnalité des efforts demandés aux intermédiaires en ligne et en protégeant leurs utilisateurs commerciaux légitimes; et ii) à répondre aux préoccupations d'ordre public liées à la diffusion de différents types de contenus illicites, en veillant à ce qu'ils soient rapidement retirés par les intermédiaires dans les conditions prévues par la législation;

- fixant des obligations claires et proportionnées de diligence raisonnable pour les intermédiaires en ligne afin de garantir que les contenus illicites sont traités de manière appropriée et transparente et que les utilisateurs peuvent faire valoir leurs droits. La proposition prévoit également un ensemble de garanties rigoureuses pour les processus de modération des contenus, y compris ceux qui reposent sur des conditions générales fixées par le secteur privé;

[47] Proposition concernant un règlement relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE, COM(2020) 825 final.
[48] Directive 2000/31/CE relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»), JO L 178 du 17.7.2000.

- imposant aux très grandes plateformes en ligne, à savoir celles qui, en raison de leur audience, ont acquis un rôle central et systémique dans la facilitation du débat public, l'obligation d'évaluer et d'atténuer les risques que leurs services présentent, y compris pour certains droits fondamentaux: le respect de la vie privée et familiale, la liberté d'expression et d'information, la non-discrimination et les droits de l'enfant. Les stratégies d'atténuation des risques doivent également tenir compte des effets potentiellement négatifs des algorithmes d'amplification des contenus des plateformes, tels que les systèmes de recommandation ou de publicité. Les très grandes plateformes en ligne sont également davantage tenues de rendre des comptes, en offrant plus de choix aux utilisateurs dans leurs interactions en ligne et en permettant à des auditeurs indépendants et à des chercheurs agréés d'examiner leurs systèmes.

Lutter contre la désinformation et réglementer les annonces publicitaires à caractère politique en ligne

La diffusion de désinformations, de fausses informations et de mythes conspirationnistes peut entraîner une polarisation des débats et mettre en danger la santé, la sécurité et l'environnement. La désinformation peut également entraver la capacité des citoyens à prendre des décisions fondées sur des faits corrects. Dans certains cas, la désinformation constitue un discours que l'État peut légitimement restreindre (comme dans le cas de l'incitation raciste et xénophobe à la violence et à la haine). Très souvent toutefois, elle est protégée par le droit à la liberté d'expression, même si elle ne repose sur aucune preuve scientifique, ni fondement réel. Lorsqu'il s'agit de discours protégés, les États doivent s'abstenir de toute censure. Pour être efficaces, les actions visant à limiter la portée de la désinformation et des mythes conspirationnistes doivent s'accompagner de la promotion d'un environnement favorable à un débat public inclusif et pluraliste. Ce point revêt une importance particulière dans le cadre d'élections.

C'est dans ce contexte que la Commission a continué, en 2020-2021, à mettre en place plusieurs actions visant à rendre l'environnement en ligne plus transparent et ses acteurs plus responsables, à donner aux usagers des moyens d'agir et à favoriser un débat démocratique ouvert. Ces actions comprennent i) la fourniture d'un soutien aux vérificateurs de faits indépendants et aux chercheurs universitaires, notamment par l'intermédiaire de l'**Observatoire européen des médias numériques**[49], ii) l'adoption de mesures visant à améliorer l'éducation aux médias et iii) le suivi d'un **code de bonnes pratiques** autoréglementé **contre la désinformation**[50]. Se fondant sur le résultat de ces activités de suivi, la Commission a également publié des orientations sur la manière dont les signataires actuels et nouveaux du code de bonnes pratiques, y compris les applications de messagerie privée, le secteur de la publicité et les autres parties prenantes concernées, pourraient renforcer la portée et l'application du code et garantir un cadre de suivi plus robuste[51].

Afin de promouvoir le débat démocratique, le **plan d'action pour la démocratie européenne**[52] définit des mesures visant à promouvoir des élections libres et régulières, à

[49] EDMO – United against disinformation.
[50] Code de bonnes pratiques contre la désinformation | Façonner l'avenir numérique de l'Europe (europa.eu).
[51] https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_2585.
[52] Plan d'action pour la démocratie européenne |Commission européenne (europa.eu).

renforcer la liberté des médias et à lutter contre la désinformation. Parmi celles-ci figure notamment la proposition sur la transparence et le ciblage de la publicité à caractère politique[53], adoptée en novembre 2021, dans le cadre de mesures visant à protéger l'intégrité des élections et un débat démocratique ouvert. Les règles proposées exigeraient que toute annonce publicitaire à caractère politique soit clairement identifiée comme telle et contienne des informations par exemple sur les personnes qui l'ont payée et le montant dépensé. Les techniques de ciblage et d'amplification politiques devraient être expliquées publiquement avec un niveau de détail inédit et seraient interdites si elles utilisaient des données à caractère personnel sensibles sans le consentement explicite de la personne concernée. Enfin, le **nouveau plan d'action en matière d'éducation numérique (2021-2027)[54]** propose l'élaboration de lignes directrices à l'intention des enseignants et des éducateurs sur la lutte contre la désinformation et la promotion de l'habileté numérique.

Proposition d'un nouveau règlement relatif à la sécurité générale des produits

En outre, pour répondre à d'autres exigences sectorielles, la Commission a, dans le cadre de la révision du cadre de l'Union européenne pour la sécurité des produits, adopté et publié une proposition de nouveau **règlement relatif à la sécurité générale des produits**, en juin 2021[55]. Cette proposition, qui repose sur la proposition de législation sur les services numériques, introduirait des exigences supplémentaires pour les places de marché en ligne concernant les produits dangereux en tant que catégorie spécifique de contenus illicites. La proposition de la Commission est actuellement en cours d'examen par les colégislateurs.

5. Protéger les droits fondamentaux en cas d'utilisation de l'intelligence artificielle

L'utilisation des technologies d'intelligence artificielle (IA) peut avoir des effets positifs importants sur nos sociétés. L'IA peut accroître l'efficacité des procédures ou stimuler l'innovation et la recherche. Elle peut également être utilisée pour promouvoir une série de droits fondamentaux, tels que la liberté d'expression, la liberté d'information ou le droit aux soins de santé, et pour favoriser des questions importantes d'intérêt public comme la sécurité publique ou la santé publique.

En revanche, l'utilisation de l'IA sans garde-fous et contrôles de qualité appropriés, à des fins d'automatisation ou de soutien des processus décisionnels ou d'activités telles que la surveillance, peut également donner lieu à des violations des droits des citoyens. Ces violations peuvent se produire à grande échelle, en fonction de l'ampleur de l'utilisation d'un système et elles peuvent être difficiles à prévenir ou à détecter lorsque le système d'IA n'est pas suffisamment transparent ou que les citoyens ignorent son utilisation. Par exemple, l'utilisation de l'IA pour déduire des informations sur les citoyens peut nuire à la protection

[53] Proposition de règlement relatif à la transparence et au ciblage de la publicité à caractère politique, COM(2021) 731 final.
[54] Plan d'action en matière d'éducation numérique (2021-2027) |Éducation et formation (europa.eu).
[55] Proposition de règlement relatif à la sécurité générale des produits, modifiant le règlement (UE) nº 1025/2012 et abrogeant la directive 87/357/CEE du Conseil et la directive 2001/95/CE du Parlement européen et du Conseil, COM(2021) 346 final.

des données et à la vie privée. Les biais dans les algorithmes ou dans les données d'entraînement, tels que les préjugés liés au sexe ou à l'origine ethnique ou raciale, peuvent conduire à des résultats injustes et discriminatoires. Si un système permettant d'estimer le potentiel de réussite au travail est entraîné en utilisant principalement des données relatives aux hommes, il risque d'être moins performant lorsqu'il est utilisé pour analyser des données concernant les femmes, aboutissant vraisemblablement à une discrimination. En outre, l'utilisation de l'IA peut également nuire aux droits à la dignité humaine, à la bonne administration, à la protection des consommateurs, à la sécurité sociale et à l'aide sociale, à la liberté d'expression, à la liberté de réunion, à l'éducation, à l'asile, à la négociation et à l'action collectives, à des conditions de travail justes et équitables, à l'accès aux soins préventifs, à la diversité culturelle et linguistique, à la protection des données et au respect de la vie privée, ainsi qu'aux droits des groupes vulnérables tels que les enfants. Si ces systèmes sont utilisés dans un contexte répressif ou judiciaire, ils peuvent également porter atteinte à la présomption d'innocence, au droit à accéder à un tribunal impartial et aux droits de la défense. En outre, l'inaccessibilité aux informations pertinentes sur les systèmes automatisés ou l'inexistence de celles-ci entravent l'application effective des obligations en matière de droits fondamentaux et l'accès des citoyens aux voies de recours.

Qu'est-ce que l'IA et quelles sont les caractéristiques spécifiques potentiellement sources de risques?

– L'IA désigne un ensemble de technologies qui ont connu une évolution rapide ces dernières années. Dans le cas de certains types de systèmes d'IA, leurs fonctions suivent des règles générées automatiquement et non programmées explicitement par des personnes. Cette technologie peut parfois donner des résultats impressionnants, mais aussi poser des problèmes. S'appuyant sur la définition de l'IA de l'OCDE, la proposition de législation sur l'intelligence artificielle entend par «système d'intelligence artificielle» un logiciel qui est développé au moyen d'approches d'apprentissage automatique, d'approches fondées sur la logique et les connaissances ou d'approches statistiques, et qui peut, pour un ensemble donné d'objectifs définis par l'homme, générer des résultats tels que des contenus, des prédictions, des recommandations ou des décisions influençant les environnements avec lesquels il interagit.

– L'opacité (manque de transparence) et la complexité (fonctionnement avec de nombreux composants et processus différents) de certains systèmes d'IA rendent difficiles la détection et la preuve d'éventuelles violations de la législation, y compris des dispositions garantissant le respect des droits fondamentaux, et la recherche d'éventuelles erreurs ou d'éventuels dysfonctionnements du système.

– Un sous-ensemble précis d'applications d'IA peut faire l'objet d'une adaptation continue, même pendant leur utilisation, et changer et évoluer de manière imprévue, ce qu'il n'est pas facile de contrôler. Cette situation conduit à un certain degré d'imprévisibilité qui peut nuire à la sécurité ou aux droits fondamentaux.

– Le comportement autonome des systèmes peut avoir une incidence sur la sécurité, car certains systèmes d'IA ne nécessitent que peu ou pas d'intervention humaine dans l'exécution des tâches.

– La dépendance de certains systèmes à l'égard des données et les éventuels biais algorithmiques peuvent provoquer des biais et erreurs systémiques ou accroître leur nombre. Si ces systèmes ne sont pas correctement conçus, testés et utilisés, ils peuvent exacerber des résultats négatifs tels que la discrimination.

5.1 Situation et actions au niveau des États membres

Ces dernières années, les États membres de l'Union ont cherché à remédier aux difficultés posées par l'utilisation des technologies d'IA. Nombre d'entre eux ont mis en place des stratégies nationales en matière d'IA[56], dans lesquelles ils insistent sur la nécessité de garantir le respect des droits fondamentaux. En outre, les États membres ont défini ou prévoient de définir des lignes directrices et des normes éthiques qui aident ceux qui déploient des outils d'IA à garantir la transparence, la traçabilité et la solidité, à lutter contre les biais potentiels et à trouver des moyens efficaces de se conformer à leurs obligations en matière de respect des droits fondamentaux. Dans certains cas, les lignes directrices et l'expertise sont développées par des universitaires[57] ou des groupes d'experts créés à cette fin[58].

De même, lorsqu'ils ont agi ensemble à l'échelle de l'Union, les États membres ont insisté sur la nécessité de veiller à ce que les droits énoncés dans la charte soient pleinement respectés et ont demandé que la législation pertinente en vigueur fasse l'objet d'un réexamen en vue de s'assurer qu'elle est adaptée aux nouvelles possibilités qu'offre l'IA et aux nouveaux défis qui en découlent[59]. En octobre 2020, 26 des 27 États membres ont adopté un document intitulé «La charte des droits fondamentaux dans le contexte de l'intelligence artificielle et du changement numérique»[60], dans lequel ils ont demandé que soit remédié aux difficultés posées par l'opacité, la complexité, les biais, le degré relatif d'imprévisibilité et le comportement partiellement autonome de certains systèmes d'IA, afin de faire en sorte qu'ils soient compatibles avec les droits fondamentaux et de faciliter l'application des règles juridiques. Les États membres ont souligné l'importance d'associer diverses parties prenantes, y compris celles de la société civile, afin de bénéficier de leur expertise.

Au moment de l'adoption du présent rapport, aucun État membre de l'Union n'avait arrêté de législation spécifique pour remédier aux problèmes posés par l'utilisation de l'IA en ce qui concerne le respect des droits fondamentaux[61]. Il semble plutôt que les autorités des États

[56] En juin 2021, 20 États membres et la Norvège avaient publié leurs stratégies nationales en matière d'IA, tandis que 7 États membres étaient en phase de rédaction finale. https://knowledge4policy.ec.europa.eu/ai-watch/national-strategies-artificial-intelligence_en.

[57] Par exemple, des universitaires de l'université d'Utrecht ont élaboré en avril 2021 un code de bonne administration publique numérique pour les autorités néerlandaises, fondé sur les droits fondamentaux. https://www.rijksoverheid.nl/documenten/rapporten/2021/04/30/code-goed-digitaal-openbaar-bestuur.

[58] À titre d'exemple, on peut mentionner la «commission pour l'éthique des données» allemande et l'expertise qu'elle a produite en 2019: https://www.bmjv.de/DE/Themen/FokusThemen/Datenethikkommission/Datenethikkommission_node.html.

[59] Réunion du Conseil européen (19 octobre 2017) – Conclusions EUCO 14/17, p. 8., et Conclusions sur le plan coordonné dans le domaine de l'intelligence artificielle (11 février 2019) 6177/19, 2019.

[60] https://data.consilium.europa.eu/doc/document/ST-11481-2020-INIT/fr/pdf.

[61] La Finlande a indiqué que des travaux sont en cours pour élaborer un projet de proposition législative sur la prise de décision administrative automatisée d'ici à la fin de 2021. L'inclusion d'exemples d'actions des États membres (législation, financement ou autres) dans le présent rapport vise à illustrer différents types d'actions.

membres se soient appuyées sur la législation existante. En 2017, une juridiction italienne a ordonné au ministère italien de l'éducation de divulguer un algorithme de prise de décision automatisée qu'il utilisait pour la gestion de la mobilité des travailleurs, sur la base du droit d'accès aux documents, qui ouvre également le droit à un recours effectif[62]. En 2018, le tribunal national finlandais pour la non-discrimination et l'égalité a jugé discriminatoire un cas d'évaluation du risque de crédit basée sur des statistiques relatives au sexe, au lieu de résidence, à l'âge et à la langue plutôt que sur une évaluation individuelle[63]. En février 2020, un tribunal néerlandais a invalidé une loi néerlandaise qui avait mis en place un système de détection des fraudes, en s'appuyant sur le droit fondamental à la vie privée tel que consacré par la convention européenne des droits de l'homme[64]. Le «System Risk Indication» (SyRi) était utilisé pour analyser les données collectées par différentes autorités publiques afin de détecter les personnes susceptibles de commettre une fraude aux prestations sociales. Le tribunal néerlandais a estimé que l'utilisation de SyRi n'était pas suffisamment transparente et que son ingérence dans le droit à la vie privée n'était pas proportionnée à l'objectif de détection de la fraude.

Ces exemples montrent que les États membres se sont déjà heurtés à des difficultés liées à l'utilisation de l'IA en ce qui concerne le respect des droits fondamentaux. L'approche proposée par la Commission pour remédier aux difficultés posées par l'IA vise à renforcer la protection effective des droits fondamentaux, tout en favorisant l'innovation dans le domaine de l'IA.

5.2 Proposition de la Commission visant à réglementer les systèmes d'IA à haut risque

En avril 2021, la Commission a présenté une proposition de règlement sur l'IA (législation sur l'intelligence artificielle)[65]. Les principaux objectifs de la proposition de législation sont la protection des droits fondamentaux et de la sécurité et la création d'un marché unique pour des systèmes d'IA dignes de confiance. La proposition vise à garantir que les systèmes d'IA à haut risque sont conçus et utilisés dans le respect des droits fondamentaux et que les autorités et juridictions nationales compétentes peuvent enquêter plus efficacement sur les éventuelles violations des obligations en matière de droits fondamentaux et y remédier.

La proposition suit une approche fondée sur le risque. Certains systèmes d'IA sont purement et simplement interdits, comme ceux qui emploient des techniques subliminales et ceux qui sont utilisés par les autorités publiques à des fins de notation sociale, en raison de leur caractère contraire aux valeurs de l'Union. L'utilisation de systèmes d'identification biométrique à distance dans des espaces accessibles au public à des fins répressives est également interdite, à moins que des exceptions et des garanties clairement définies ne s'appliquent.

Toutes les initiatives ne peuvent pas être mentionnées pour chaque thème et la sélection repose en grande partie sur les informations soumises par les États membres en juin 2021.

[62] T.A.R., Rome, sect. III-bis, 22 mars 2017, nº 3769.

[63] https://www.yvtltk.fi/material/attachments/ytaltk/tapausselosteet/45LI2c6dD/YVTltk-tapausseloste-_21.3.2018-luotto-moniperusteinen_syrjinta-S-en_2.pdf.

[64] https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878.

[65] Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, COM(2021) 206 final.

Les systèmes d'IA à haut risque devront se conformer à un ensemble d'exigences et suivre des procédures d'évaluation de la conformité avant leur mise sur le marché ou leur mise en service. Ces exigences garantissent une documentation et des tests appropriés des systèmes d'IA à haut risque, ainsi qu'une qualité des données, une traçabilité, un contrôle humain, une robustesse, une exactitude et une cybersécurité adéquats. Elles s'appliqueront lorsque les systèmes d'IA sont utilisés dans des domaines cruciaux, tels que l'identification biométrique, l'éducation, l'emploi, les services essentiels publics et privés, comme les crédits ou les prestations d'aide sociale, l'appareil répressif, la migration et le contrôle des frontières, et l'appareil judiciaire. Les systèmes d'IA qui constituent des composants de sécurité de certains produits réglementés (les machines, les dispositifs médicaux, par exemple) seront également couverts par les mêmes exigences et devront être contrôlés avant d'être mis sur le marché de l'Union ou mis en service.

La proposition veille à ce que les utilisateurs de systèmes d'IA, tels que les entreprises qui interagissent avec leurs clients ou les autorités publiques qui prennent des décisions, reçoivent des informations adéquates de la part des développeurs des systèmes afin de garantir une utilisation appropriée de leurs applications et de leur permettre de remplir les obligations qui leur incombent en vertu de la législation sur les droits fondamentaux.

En cas de violations des droits fondamentaux par l'utilisation de systèmes d'IA, les personnes concernées disposeront de possibilités de recours efficaces rendues possibles grâce à la transparence et à la traçabilité des systèmes d'IA, associées à de solides contrôles ex post effectués par les autorités compétentes. Les autorités de surveillance chargées de faire respecter les droits fondamentaux, telles que les autorités chargées de la protection des données, les organismes de promotion de l'égalité ou les organismes de défense des consommateurs, auront accès à toute la documentation relative aux systèmes d'IA à haut risque qui relèvent de leur mandat. Elles pourront coopérer avec les autorités de surveillance du marché afin de tester les systèmes d'IA respectifs si nécessaire.

En ce qui concerne certains systèmes d'IA, les obligations de transparence à l'égard des personnes concernées réduiront le risque de manipulation, notamment dans le cas des dialogueurs (programmes informatiques capables de répondre à des questions dans le cadre d'un dialogue en ligne) ou des trucages ultra-réalistes (contenus image, audio ou vidéo générés artificiellement ou manipulés qui ressemblent à des personnes, des objets, des lieux ou d'autres entités ou événements existants et qui semblent faussement authentiques ou véridiques). Les personnes devraient également être informées lorsque des systèmes de reconnaissance des émotions ou de catégorisation biométrique sont utilisés, ce qui les aidera à faire valoir leurs droits au titre de la législation existante en matière de protection des données.

Cette proposition est en cours de négociation par les colégislateurs.

5.3 Interaction avec la législation sectorielle: l'exemple de la solvabilité et de la notation de crédit

La proposition de législation sur l'intelligence artificielle fonctionnera conjointement avec d'autres actes législatifs établissant des règles de fond pour l'utilisation des systèmes d'IA dans des contextes clairement ciblés. Par exemple, les fournisseurs de crédit utilisent souvent

des techniques de prise de décision automatisée, y compris des systèmes d'IA, aux fins de l'évaluation de la solvabilité ou de la notation de crédit. Ces fournisseurs s'appuient sur différentes données, dont beaucoup ne sont pas fournies par le consommateur ou lui sont inconnues. Ce constat soulève des inquiétudes concernant la protection des données à caractère personnel, la discrimination directe ou indirecte[66] et la protection des consommateurs[67]. La **directive sur le crédit aux consommateurs[68]** et la **directive sur le crédit hypothécaire[69]** contiennent des dispositions sur les évaluations de solvabilité. En juin 2021, la Commission a adopté une **nouvelle proposition de directive relative aux crédits aux consommateurs** abrogeant et remplaçant l'actuelle directive sur le crédit aux consommateurs. Cette proposition contient des règles relatives à l'octroi de crédits aux consommateurs en vertu desquelles les États membres devront veiller à la documentation des procédures et aux informations utilisées aux fins de l'évaluation de la solvabilité. En outre, les évaluations devront reposer sur des informations pertinentes et précises concernant la situation financière et économique (les revenus et les dépenses, par exemple) et non sur des données telles que celles des médias sociaux. Les consommateurs auront également le droit d'obtenir une explication sur la manière dont une décision concernant leur solvabilité a été prise, d'exprimer leur point de vue et d'obtenir une intervention humaine, reflétant les principes du règlement général sur la protection des données (RGPD)[70] concernant la prise de décision automatisée. La nouvelle proposition comprend également un article sur la non-discrimination, précisant que les conditions à remplir pour se voir accorder un crédit ne doivent pas être discriminatoires à l'égard des consommateurs résidant légalement dans l'Union en raison de leur nationalité ou de leur lieu de résidence ou pour tout autre motif visé à l'article 21 de la charte des droits fondamentaux de l'UE. Cette proposition est en cours de négociation par les colégislateurs.

5.4 Compétences

Lorsque des systèmes d'IA sont utilisés, les travailleurs doivent être suffisamment qualifiés pour garantir le respect des droits fondamentaux et un contrôle humain approprié. Les autorités de surveillance auront également besoin de personnel possédant des compétences techniques spécifiques pour remplir efficacement leur mandat. En septembre 2020, la Commission a adopté un **plan d'action en matière d'éducation numérique** (2021-2027)[71]. Ce plan vise à promouvoir les compétences numériques, notamment en ce qui concerne

[66] Par exemple, en avril 2019, le médiateur finlandais de la protection des données a ordonné à la société de crédit financier Svea Ekonomi de corriger ses pratiques d'évaluation de la solvabilité, considérant qu'une limite d'âge supérieure n'était pas acceptable comme facteur, car l'âge ne décrit pas la solvabilité ou la volonté de payer.

[67] Rapport d'analyse d'impact accompagnant la proposition de directive concernant les contrats de crédit aux consommateurs abrogeant et remplaçant la directive 2008/48/CE, COM(2021) 347 final.

[68] Directive 2008/48/CE du Parlement européen et du Conseil du 23 avril 2008 concernant les contrats de crédit aux consommateurs et abrogeant la directive 87/102/CEE du Conseil (JO L 133 du 22.5.2008, p. 66).

[69] Directive 2014/17/UE du Parlement européen et du Conseil du 4 février 2014 sur les contrats de crédit aux consommateurs relatifs aux biens immobiliers à usage résidentiel et modifiant les directives 2008/48/CE et 2013/36/UE et le règlement (UE) nº 1093/2010 (Texte présentant de l'intérêt pour l'EEE) (JO L 60 du 28.2.2014, p. 34).

[70] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

[71] Plan d'action en matière d'éducation numérique (2021-2027) |Éducation et formation (europa.eu).

l'IA[72], et prévoit l'élaboration de lignes directrices en matière d'éthique dans le domaine de l'IA et des données dans l'éducation et la formation. En outre, tous les États membres qui ont adopté des stratégies nationales en matière d'IA ont intégré un volet «compétences» dans leurs stratégies, par exemple au moyen de réformes des systèmes éducatifs visant à renforcer la pensée informatique ou d'initiatives visant à adapter les politiques d'apprentissage tout au long de la vie et de reconversion professionnelle[73].

6. Combler la fracture numérique

Pour participer activement à la société, il faut être connecté au monde numérique et compétent en la matière. Un nombre croissant d'activités essentielles migre vers l'univers en ligne, qu'il s'agisse de la recherche d'un emploi, de l'exécution d'une activité professionnelle en télétravail, de la poursuite d'une formation ou des interactions avec une administration publique, ou encore de la prise d'un rendez-vous chez le médecin. Mais tout le monde n'est pas en ligne. Ne pas avoir de connexion internet peut avoir des répercussions sur l'exercice des droits des personnes. Cela peut, par exemple, nuire aux droits des citoyens dans une société démocratique, y compris à leur droit à la liberté d'expression et d'information, et à leur droit de se présenter comme candidat aux élections municipales puisque les campagnes politiques se déroulent de plus en plus en ligne. L'apparition de la pandémie de COVID-19 a exacerbé ces difficultés d'accès aux services publics pour ceux qui ne disposent pas de l'équipement ou des connaissances numériques nécessaires, les bureaux ayant été fermés et les citoyens invités à communiquer avec leurs administrations nationales en ligne.

Ce phénomène est souvent appelé «fracture numérique». Aujourd'hui encore, 46 % des Européens ne possèdent pas les compétences numériques de base[74]. Ce constat est reconnu dans le **socle européen des droits sociaux**, qui inclut les communications numériques parmi les services essentiels auxquels chacun devrait avoir accès et demande des mesures de soutien pour ceux qui en ont besoin[75]. Les personnes qui ne disposent pas d'un accès régulier à l'internet, qui n'ont pas les compétences nécessaires pour utiliser ces services ou qui ne peuvent pas accéder à un produit ou service numérique en raison d'un handicap physique ou cognitif risquent de plus en plus d'être exclues et éprouvent des difficultés à faire valoir leurs droits.

Dans le cas de services publics exclusivement accessibles par voie numérique, les personnes qui ne disposent pas d'une connexion à l'internet peuvent se trouver dans l'incapacité d'exercer leurs droits ou avoir besoin d'aide pour ce faire. Le Haut conseil du travail, organe consultatif auprès du ministère français des affaires sociales, estime par exemple qu'une personne sur cinq en France rencontre des difficultés pour accomplir des démarches administratives en ligne, et met en garde contre le fait que la numérisation peut nuire au principe d'égalité d'accès aux services publics si d'autres moyens d'accès ne sont pas

[72] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan/action-8_fr.
[73] https://knowledge4policy.ec.europa.eu/ai-watch/national-strategies-artificial-intelligence_en.
[74] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52020DC0624 et Statistiques | Eurostat (europa.eu).
[75] Les vingt principes clés du socle européen des droits sociaux | Commission européenne (europa.eu), voir principe 20.

maintenus[76]. De même, comme de plus en plus d'activités économiques ont une composante numérique, l'exercice du droit d'accès aux services d'intérêt économique général est de plus en plus conditionné par l'accès à l'internet. Les enfants qui ne disposent pas d'un appareil connecté à la maison éprouvent des difficultés à poursuivre leur apprentissage scolaire à distance, ce qui porte préjudice aux droits de l'enfant et au droit à l'éducation. En outre, lorsque les sites web et les applications mobiles ne sont pas adaptés aux besoins des personnes handicapées, leur droit à l'intégration peut être entravé.

Face au défi que constitue la fracture numérique, la Commission et certains des États membres mettent en œuvre une série de mesures visant à garantir que nul ne soit laissé pour compte. Comme annoncé dans le **plan d'action sur le socle européen des droits sociaux**[77], la Commission publiera en 2022 un rapport sur l'accès aux services essentiels, portant aussi sur l'accès aux communications numériques, dans lequel elle présentera une vue d'ensemble de la situation dans l'EU-27 et recensera les mesures et les bonnes pratiques adoptées par l'Union et les États membres afin de favoriser l'accès des personnes ayant besoin d'aide.

6.1 Réduction générale de la fracture numérique

Le fait que, pendant la pandémie, de nombreuses activités aient migré vers l'univers en ligne ne constitue pas seulement un défi, mais également une chance. Les États membres ont élaboré des projets que l'Union financera pour aider l'économie à se remettre du ralentissement causé par la pandémie. Ces projets comprennent des mesures qui visent à réduire la fracture numérique et à garantir des droits numériques inclusifs et qui portent sur la numérisation du travail. Deux plans nationaux peuvent être mentionnés à titre d'exemple. La **Roumanie** prévoit d'investir dans la création de contenus éducatifs et de ressources accessibles, tels que des vidéos et des leçons interactives, et de mettre en place des programmes d'habileté numérique à l'intention des étudiants souffrant d'un handicap. L'**Allemagne** veut contribuer à l'acquisition d'appareils numériques pour les enseignants dans tout le pays. En outre, elle créera une plateforme pour l'apprentissage numérique tout au long de la vie et accordera une attention particulière au soutien des personnes les moins dotées de qualifications formelles.

Plus généralement, un certain nombre d'initiatives prometteuses ont été mises en place dans différents États membres[78]. En février 2021, la **Belgique** a lancé un appel public à projets afin de soutenir les femmes entrepreneures touchées par la pandémie de COVID-19, notamment en proposant un accompagnement vers la numérisation. La Belgique investit également dans des organisations locales qui visent à accroître les compétences numériques des jeunes en situation économique précaire.

Le **Portugal** mobilise de jeunes volontaires pour aider à former les adultes à la transition numérique, en s'appuyant sur un réseau national de 1 500 centres de formation et sur un

[76] https://solidarites-sante.gouv.fr/IMG/pdf/pourquoi_et_comment_les_travailleurs_sociaux_se_saisissent_des_outils_numeriques.pdf, p. 4.
[77] Plan d'action sur le socle européen des droits sociaux (europa.eu).
[78] Toutes les initiatives ne peuvent être mentionnées dans le présent rapport et la sélection suivante vise à illustrer différents types d'actions. Elle repose sur les informations soumises par les États membres en juin 2021.

certain nombre d'outils et de ressources gratuits. Ce programme d'inclusion numérique devrait bénéficier à un million de personnes et sera mis en œuvre en partenariat avec les autorités et organisations locales[79].

Suivant une logique similaire à celle de l'initiative WiFi4EU[80], l'**Italie** subventionne l'accès à l'internet pour certaines personnes et a lancé le projet «Piazza Wifi Italia»[81] qui permet à plus de 400 000 personnes de se connecter facilement et gratuitement, à l'aide d'une application prévue à cet effet, à un réseau wifi gratuit réparti dans tout le pays. En mars 2020, ce projet a été étendu aux établissements de santé, y compris aux hôpitaux.

L'infrastructure numérique continuera probablement à évoluer et l'UE a pris des mesures dans toute une série de domaines pour améliorer la connectivité. Le principal objectif en matière de connectivité durant la **décennie numérique** est que chaque ménage européen ait accès à une couverture internet à haut débit d'ici à 2025 et à une connectivité en gigabit d'ici à 2030[82]. En mars 2021, la Commission et les États membres se sont accordés sur une **boîte à outils pour la connectivité** afin de favoriser le déploiement de réseaux numériques et de faciliter l'accès au spectre 5G. Le réexamen de la directive sur la réduction du coût du déploiement du haut débit, prévu pour 2022, a pour but de soutenir davantage le déploiement des réseaux numériques en réduisant la charge administrative ainsi que le coût et la rapidité de ces déploiements. En outre, la **vision** à long terme **pour les zones rurales**[83], publiée par la Commission en juin 2021, vise à remédier à la fracture urbaine/rurale en permettant l'accès à une connectivité internet rapide, à la 5G (y compris au moyen d'un financement de l'UE[84]) et aux technologies numériques, ainsi qu'en renforçant les compétences numériques. La connectivité à haut débit est un élément central de la transition numérique et de la reprise après la crise de la COVID-19. La Commission est déterminée à réduire la fracture numérique en matière d'accessibilité dans les zones rurales et l'Union investira dans les infrastructures de réseau, dans une norme pour la transmission de données sans fil et dans la fibre optique afin de garantir que tous les habitants de l'Union ont accès à une infrastructure de connectivité numérique efficace sur le plan énergétique et à l'épreuve du temps.

6.2 Administrations publiques

Les technologies numériques permettent aux personnes de bénéficier d'un accès plus large aux services publics et aux informations qui peuvent les aider à gérer leur quotidien et à exercer leurs droits, en particulier les libertés d'établir et de fournir des services. Depuis la **déclaration de Malmö**, signée lors d'un sommet organisé en Suède en 2009, les États membres de l'Union ont accompli des progrès constants pour moderniser les administrations

[79] Resolução do Conselho de Ministros n.º 30/2020 – DRE.
[80] https://digital-strategy.ec.europa.eu/fr/activities/wifi4eu.
[81] https://www.wifi.italia.it/it/.
[82] Communication de la Commission «Une boussole numérique pour 2030: l'Europe balise la décennie numérique», COM(2021) 118 final.
[83] Une vision à long terme pour les zones rurales de l'UE |Commission européenne (europa.eu).
[84] Des fonds provenant du Fonds européen de développement régional, du Fonds européen agricole pour le développement rural, du volet numérique du mécanisme pour l'interconnexion en Europe et de la facilité pour la reprise et la résilience seront disponibles pour atteindre les objectifs de connectivité fixés par l'Union pour 2025.

publiques[85]. La **déclaration de Tallinn** de 2017 a donné une impulsion à la numérisation des services publics pour les citoyens et des services publics transfrontières pour les entreprises[86]. Plus récemment, la **déclaration de Berlin** de décembre 2020 a inclus parmi les engagements des États membres les mesures à prendre pour protéger les droits fondamentaux en ligne[87] tandis que la **déclaration de Lisbonne** de juin 2021 vise à garantir que «personne ne soit laissé pour compte». Les efforts déployés par les États membres portent également sur la numérisation de la justice[88].

Les États membres suivent des approches différentes pour assurer l'accès aux services publics, essayant simultanément de réduire cette fracture numérique tout en répondant aux exigences de cette ère du numérique. La **France**, par exemple, a choisi de maintenir plusieurs modes d'accès aux services publics afin d'éviter tout obstacle. Les citoyens ne sont pas obligés de contacter l'administration par voie électronique. Le **Danemark** a suivi une autre voie, définissant une stratégie axée sur le «numérique par défaut» et rendant obligatoire, en 2014, l'utilisation de moyens électroniques pour tous les contacts avec l'administration. Pour combler la fracture numérique, l'État finance des mesures telles que l'accompagnement personnalisé gratuit dans les bibliothèques[89], l'aide à l'achat de matériel et la contribution aux abonnements internet. Dans le même ordre d'idées, aux **Pays-Bas**, le gouvernement et les bibliothèques locales ont lancé l'«Information Point Digital Government» (point d'information sur les services publics numériques), une initiative dans le cadre de laquelle un employé de bibliothèque formé répond aux questions et aide les citoyens à utiliser les services publics numériques traditionnels, comme les déclarations d'impôts et les services sociaux, ainsi que des services plus récents tels que les applications en rapport avec la COVID-19.

6.3 Soins de santé

La pandémie a entraîné une augmentation des prestations de soins de santé en ligne, par exemple au moyen de consultations virtuelles ou d'applications et de logiciels mis au point à des fins diagnostiques ou thérapeutiques. Pour certains, comme les habitants des zones rurales ou des petites îles, cette approche facilite l'accès à l'assistance médicale, tandis que, pour d'autres, elle constitue un nouvel obstacle. Pour ceux qui n'ont pas d'accès ou de compétences, des mesures visant à réduire la fracture numérique peuvent améliorer la situation. Par exemple, la **Pologne** a introduit le «Patient's Internet Account» (compte internet du patient), un outil en ligne qui permet aux patients d'accéder à des informations sur leur traitement médical passé, actuel ou prévu et de régler un certain nombre de points (ordonnance électronique, historique des visites, orientation électronique, congés médicaux

[85] https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/ministerial-declaration-on-egovernment-malmo.pdf.

[86] https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration.

[87] https://ec.europa.eu/isa2/news/eu-member-states-sign-berlin-declaration-digital-society_en.

[88] Les avancées dans ce domaine sont reflétées dans le rapport 2021 sur l'état de droit publié par la Commission: https://ec.europa.eu/info/sites/default/files/communication_2021_rule_of_law_report_fr.pdf.
Voir également la communication de la Commission sur la numérisation de la justice dans l'UE, COM(2020) 710 final et le document qui l'accompagne, SWD (2020) 540, du 2 décembre 2020.

[89] Ce type d'assistance existe également ailleurs, mais pour illustrer l'approche, quelques exemples suffisent. L'objectif du présent rapport n'est pas de dresser une liste exhaustive des mesures, mais plutôt de donner un aperçu des idées et des approches.

électroniques et prestations sociales) sans devoir se rendre en personne dans un établissement de soins de santé.

6.4 Éducation

Plusieurs États membres ont mis en place des politiques et des programmes visant à favoriser l'accès aux technologies et à renforcer les compétences numériques dans le cadre de l'enseignement formel. La **Grèce**, par exemple, fournit aux élèves et aux étudiants qui en ont besoin des bons pour acheter des équipements tels que des tablettes ou des ordinateurs et propose des programmes éducatifs pertinents par l'intermédiaire d'une «Digital Skills Academy» (académie des compétences numériques) virtuelle lancée en 2020.

À l'échelon de l'Union, le **plan d'action en matière d'éducation numérique**[90] (2021-2027), lancé en septembre 2020, a défini une vision stratégique à long terme pour une transformation numérique durable et inclusive du secteur de l'éducation et de la formation. Au titre de ce plan, la Commission promeut le droit d'accès à une éducation numérique de qualité pour tous et l'égalité d'accès aux infrastructures, en s'attachant particulièrement à encourager la participation des filles et des femmes dans les matières STIM (sciences, technologies, ingénierie et mathématiques).

6.5 Intégration des personnes handicapées

Le **code des communications électroniques européen**[91] garantit aux utilisateurs finaux handicapés un accès et un choix équivalents pour ce qui concerne les services de communications électroniques, facilitant ainsi leur participation à la société numérique. La **législation européenne sur l'accessibilité**[92] entrera en vigueur en 2025 et améliorera l'inclusion des personnes handicapées et des personnes âgées dans le monde numérique en rendant plus accessible un ensemble de produits et de services clés du secteur privé et public. La **directive relative à l'accessibilité de l'internet** de 2016[93] exige des États membres qu'ils veillent à ce que les sites web et les applications mobiles des organismes du secteur public soient accessibles aux personnes handicapées, telles que les personnes souffrant d'un handicap visuel, auditif ou moteur. Ce faisant, elle promeut la liberté d'expression et d'information, le droit à l'éducation, la liberté professionnelle et le droit de travailler, la non-discrimination, l'intégration des personnes handicapées, l'accès aux services d'intérêt économique général, le droit d'accès aux documents, le droit de circuler et de séjourner librement sur le territoire de l'Union, la liberté d'établissement et la libre prestation de services.

La mise en œuvre de la directive peut se faire de différentes manières. Par exemple, la **Slovénie** a modernisé le portail de son administration publique en ligne de manière à ce qu'il puisse être utilisé par les aveugles et les malvoyants, les sourds et les malentendants, les

[90] Plan d'action en matière d'éducation numérique (2021-2027) |Éducation et formation (europa.eu).
[91] Directive (UE) 2018/1972 établissant le code des communications électroniques européen (refonte), JO L 321 du 17.12.2018.
[92] Directive (UE) 2019/882 relative aux exigences en matière d'accessibilité applicables aux produits et services, JO L 151 du 7.6.2019.
[93] Directive (UE) 2016/2102 relative à l'accessibilité des sites internet et des applications mobiles des organismes du secteur public, JO L 327 du 2.12.2016.

personnes atteintes de dyslexie et les utilisateurs souffrant de troubles de la compréhension. Les descriptions textuelles des procédures sont par exemple accompagnées de courtes vidéos, qui comportent également des interprétations en langue des signes. En **Grèce**, pendant la pandémie, les livres scolaires numériques ont été adaptés de façon à ce que les personnes souffrant de toutes les catégories de handicap puissent y accéder.

7. Protéger les personnes travaillant par l'intermédiaire de plateformes

Les plateformes en ligne comprennent un large éventail de places de marché, de médias sociaux, de points de vente de contenu créatif, de boutiques d'applications, de sites de comparaison de prix, de plateformes d'économie collaborative ainsi que de moteurs de recherche. Elles facilitent l'interaction entre les utilisateurs et les entreprises. Les plateformes de travail numériques, en tant que sous-ensemble distinct des plateformes en ligne, sont apparues comme un élément caractéristique de l'économie numérique.

Le travail via une plateforme a ouvert de nouvelles perspectives économiques aux citoyens, en leur permettant par exemple de poursuivre des activités à temps partiel et d'accéder au marché du travail en général. Il pose toutefois des difficultés lorsqu'il s'agit de garantir les droits fondamentaux, notamment le droit à la protection des données à caractère personnel, le droit au respect de la vie privée, le droit à l'information et à la consultation des travailleurs, le droit de négociation et d'actions collectives, et le droit à des conditions de travail justes et équitables. Sur les 28 millions de personnes qui, selon les estimations, travailleraient par l'intermédiaire de plateformes de travail numériques, il pourrait y avoir jusqu'à 5,5 millions de «faux» indépendants[94]. Alors que les termes du contrat que ces personnes ont conclu avec les plateformes par l'intermédiaire desquelles elles travaillent les qualifient de travailleurs indépendants, elles subissent en réalité un contrôle et une surveillance caractéristiques du statut de «salarié». Des problèmes découlent également des modèles économiques basés sur les algorithmes, comme le manque d'information et de consultation des personnes travaillant par l'intermédiaire de plateformes et de leurs représentants sur la manière dont les algorithmes sont utilisés et affectent les conditions de travail via une plateforme. De même, les voies de recours sont insuffisantes et les responsabilités au regard de l'utilisation des algorithmes sont floues.

Le travail via une plateforme

Le travail via une plateforme met généralement en jeu trois parties: la **plateforme**, la **personne qui travaille par l'intermédiaire de celle-ci** et le **client** (particuliers ou entreprises). Dans certains cas, une quatrième partie pourrait également intervenir, par exemple les restaurants qui livrent des aliments.

Les plateformes de travail numériques se définissent généralement comme des intermédiaires et qualifient la relation entre les parties de relation de travail indépendant. Les tâches effectuées sur les plateformes de travail numériques peuvent aller de tâches complexes telles que la programmation informatique et la conception graphique, à des tâches simples comme

[94] Voir le rapport d'analyse d'impact accompagnant la proposition de directive relative à l'amélioration des conditions de travail dans le cadre du travail via une plateforme, SWD (2021) 396 final.

le marquage d'images.

La présidente de la Commission, Ursula von der Leyen, soulignait dans ses orientations politiques la nécessité d'améliorer les conditions du travail effectué via des plateformes[95]. Cette nécessité apparaît encore plus clairement sous l'effet de la crise liée à la COVID-19 et de la diffusion accélérée des modèles économiques des plateformes. Dans une résolution récente[96], le Parlement européen souligne que le travail via une plateforme suscite des inquiétudes concernant la précarité et de mauvaises conditions de travail, l'impossibilité ou la difficulté d'accéder à une protection sociale adéquate, des revenus fragmentés et instables, ainsi qu'un manque de mesures en matière de santé et de sécurité au travail. Il demande une action forte de l'UE pour remédier à la classification erronée du statut professionnel et améliorer la transparence dans l'utilisation des algorithmes, y compris pour les représentants des travailleurs.

7.1 Situation et actions au niveau des États membres

Afin d'éviter une concurrence déloyale au détriment des travailleurs et un nivellement par le bas des pratiques d'emploi et des normes sociales, l'Union a créé un socle minimal de droits du travail qui s'applique aux travailleurs de tous les États membres. Le corpus législatif de l'Union concernant le travail et les affaires sociales s'est étoffé au fil des ans. En outre, les réponses nationales aux difficultés posées par le travail via une plateforme diffèrent selon les États membres. Certains ont adopté une législation nationale visant à améliorer les conditions de travail ou l'accès à la protection sociale dans le cadre du travail via une plateforme. Les juridictions se sont prononcées sur la question de la classification erronée du statut professionnel dans un nombre important d'États membres. Dans certains États membres, les partenaires sociaux et les entreprises de plateformes ont entamé des négociations sur des conventions collectives.

En 2016, la **France** a adopté une loi prévoyant des droits du travail et des droits sociaux pour les personnes travaillant par l'intermédiaire de plateformes, quel que soit le secteur d'activité économique, dans le cadre d'une révision du code du travail. La loi s'applique aux travailleurs indépendants, qui sont technologiquement et économiquement dépendants. Elle donne accès à un régime d'assurance volontaire contre les accidents du travail, oblige les plateformes à payer des primes d'assurance ou à fournir une assurance collective à leurs travailleurs, et garantit le droit de mener des actions collectives et de poursuivre des études. En outre, la plus haute juridiction en matière de travail privé (la Cour de cassation) a souligné dans deux arrêts que les travailleurs de plateformes dans le domaine du covoiturage doivent être reconnus comme ayant le statut de salarié lorsque la plateforme peut donner et faire appliquer des instructions[97]. Le statut réel des personnes travaillant par l'intermédiaire de plateformes continue toutefois de faire débat, y compris dans d'autres secteurs.

[95] COM(2021) 762.
[96] Résolution du Parlement européen du 16 septembre 2021 intitulé «Conditions de travail, droits et protection sociale justes pour les travailleurs de plateformes – nouvelles formes d'emploi liées au développement numérique» [2019/2186(INI)].
[97] Take Eat Easy (18 novembre 2018, affaire 17-20.079) et Uber (4 mars 2020, affaire 19-13.316).

En 2019, la région **italienne** du Latium a adopté une loi[98] visant à améliorer les conditions de travail et la protection sociale de tous les travailleurs de plateformes, quel que soit leur statut professionnel. Cette loi comprend des mesures de protection contre les accidents du travail, une formation adéquate en matière de sécurité et une assurance responsabilité civile et accidents. Elle interdit également le paiement à la tâche. Toujours en 2019, l'Italie a adopté une loi nationale visant à améliorer les conditions de travail des livreurs de nourriture indépendants[99]. De même, en juillet 2021, l'autorité italienne chargée de la protection des données a infligé à Deliveroo Italie une amende de 2,5 millions d'EUR en raison de l'utilisation non transparente d'algorithmes et de la collecte disproportionnée de données des travailleurs. L'autorité a constaté des violations de certaines dispositions du règlement général sur la protection des données et de la législation nationale sur la protection de la vie privée, du statut des travailleurs italiens et de la loi susmentionnée protégeant les travailleurs[100].

En mai 2021, l'**Espagne** a adopté une loi introduisant une présomption selon laquelle les personnes travaillant par l'intermédiaire de plateformes dans le domaine de la livraison de nourriture et de colis étaient considérées comme des salariés, déplaçant sur les plateformes la charge de prouver qu'elles ne le sont pas[101]. En outre, cette loi oblige les plateformes à fournir aux syndicats des informations sur la gestion algorithmique, y compris sur le contrôle numérique des performances et l'attribution automatisée des missions. Cette loi établit que toutes les entreprises (pas seulement les plateformes de livraison) doivent informer leurs travailleurs des paramètres et des règles sur lesquels reposent les systèmes automatisés, qui peuvent avoir une incidence sur les conditions de travail, l'accès à l'emploi et la conservation de l'emploi.

L'**Allemagne** a publié des documents d'orientation sur l'avenir du travail, concernant l'inclusion des travailleurs indépendants travaillant par l'intermédiaire de plateformes dans les régimes de retraite et d'assurance, et la mise à niveau de leur assurance contre les accidents du travail.

En novembre 2020, le **Portugal** a également publié un document d'orientation sur l'avenir du travail, concernant la création d'une présomption légale sur le statut des personnes travaillant par l'intermédiaire de plateformes, les moyens d'augmenter la protection sociale des travailleurs indépendants et les moyens de favoriser la représentation collective des travailleurs de plateformes. En 2018, le Portugal a adopté une loi sur le transport individuel rémunéré de passagers, fixant des limites au temps de travail des conducteurs[102].

7.2 Une approche commune de l'Union

Compte tenu des approches adoptées par les États membres pour remédier aux différentes difficultés posées par le travail via une plateforme, il existe un risque de fragmentation entre les différentes initiatives législatives nationales. La Commission a recensé un certain nombre

[98] Regione Lazio, Legge Regionale 12 avril 2019, n° 4, disponible en ligne.
[99] Loi du 2 novembre 2019, n° 128, Conversione in legge, con modificazioni, del decreto-legge du 3 septembre 2019, n° 101, disponible en ligne.
[100] Décision de l'autorité italienne chargée de la protection des données, disponible en ligne.
[101] Décret-loi royal nº 9/2021 du 11 mai, disponible en ligne.
[102] Lei nº 45/2018 Regime jurídico da atividade de trasporte individual e remunderado de passageiros em veículos descaracterizadosa partir de plataforma electrónica. Disponible en ligne.

de ces difficultés et a interrogé les partenaires sociaux européens, en deux étapes, sur la nécessité d'une initiative sur le travail via les plateformes et son éventuelle orientation. Les partenaires sociaux européens se sont accordés sur les défis à relever mais pas sur la nécessité d'une action concrète au niveau de l'UE. De plus, la Commission a échangé avec de nombreuses parties prenantes, notamment lors de réunions ad hoc bilatérales avec des plateformes, des associations de travailleurs des plateformes, des syndicats, des représentants des États membres, des experts du monde universitaire et d'organisations internationales et des représentants de la société civile[103]. La Commission a proposé une directive visant à améliorer les conditions de travail des travailleurs des plateformes au niveau de l'UE en garantissant la détermination correcte de leur statut professionnel, en promouvant la transparence, l'équité et la responsabilité dans la gestion algorithmique du travail via les plateformes et en améliorant la transparence du travail via les plateformes, y compris dans les situations transfrontières, tout en soutenant les conditions propices à la croissance durable des plateformes de travail numériques dans l'Union.

8. Superviser la surveillance numérique

La protection des données et le respect de la vie privée sont des droits fondamentaux essentiels à l'ère numérique. Il s'agit également de droits «de base» qui facilitent et renforcent la protection d'autres droits fondamentaux susceptibles d'être affectés par une surveillance étatique ou privée, comme la dignité humaine, la liberté d'expression, la liberté de pensée, de conscience et de religion, la liberté de réunion, le droit à un recours effectif et à accéder à un tribunal impartial ou la non-discrimination. Le règlement général sur la protection des données (RGPD), la directive en matière de protection des données dans le domaine répressif et la directive relative à la vie privée et aux communications électroniques ont placé l'Europe à l'avant-garde de la protection des droits fondamentaux en ligne. La numérisation croissante dans tous les domaines de la vie complique la protection des données et le respect de la vie privée et familiale. D'autres actes législatifs, tels que l'acte sur la gouvernance des données, sur lequel les colégislateurs viennent de trouver un accord politique, visent à favoriser l'émergence d'une économie des données solide en réglementant les services d'intermédiaires de données, l'altruisme en matière de données et la réutilisation des données publiques protégées, en vertu et dans le respect du régime de protection des données.

Quelle est la relation entre le droit au respect de la vie privée et le droit à la protection des données?

Il s'agit de droits fondamentaux distincts mais qui se recoupent, ancrés aux articles 7 et 8 de la charte des droits fondamentaux.

– Le droit au respect de la vie privée et familiale protège la sphère privée contre les intrusions illégales. Par exemple, la confidentialité des communications interpersonnelles ainsi que les terminaux électroniques des utilisateurs sont protégés contre les intrusions non autorisées par ce droit.

[103] Voir l'annexe A.3.1 du rapport d'analyse d'impact accompagnant la proposition de directive relative à l'amélioration des conditions de travail dans le cadre du travail via une plateforme, SWD(2021) 396 final.

– Le droit à la «protection des données» ne s'applique que lorsque des données à caractère personnel sont traitées soit par des moyens automatisés, soit sous une forme structurée manuellement. Ce droit ne se limite pas aux informations relatives à la sphère privée d'une personne, mais couvre toute donnée à caractère personnel la concernant, y compris sur sa vie professionnelle. Les principes fondamentaux de la protection des données sont la transparence, la loyauté et la légalité des activités de traitement des données à caractère personnel. La protection des données signifie également que les données à caractère personnel ne doivent être traitées qu'à des fins déterminées et explicites, qu'elles doivent être exactes, limitées au nécessaire et conservées en sécurité et seulement aussi longtemps que nécessaire.

Dans la pratique, le solide cadre juridique de l'Union est constamment mis à l'épreuve. Les organisations de défense des consommateurs et les OSC actives dans le domaine de la protection des droits fondamentaux déplorent un manque de répression en cas de violations du RGPD[104]. Ces dernières années, l'UE et ses États membres ont pris diverses mesures destinées à préserver la sécurité publique et à relever les défis en matière de sécurité en utilisant les technologies modernes. Des préoccupations ont été exprimées dans ce contexte par les organisations de la société civile à propos de la proportionnalité des politiques de surveillance et de sécurité, par exemple en ce qui concerne la surveillance des frontières de l'Union[105], ou dans le cas d'une législation adoptée ou proposée qui permettrait aux autorités de numériser les communications privées à des fins de sécurité[106]. Les organisations de la société civile et de l'industrie ont également fait connaître leur inquiétude face à ce qu'elles perçoivent comme des tentatives des États membres d'affaiblir le chiffrement[107].

Les autorités nationales chargées de la protection des données et les juridictions nationales ont été les garants d'un recours effectif lorsque des mesures de surveillance, prises par des acteurs tant privés que publics, ont constitué une violation des droits fondamentaux. On peut citer pour exemple: i) la décision de l'autorité suédoise chargée de la protection des données concernant l'utilisation de caméras-piétons par les contrôleurs des transports publics de Stockholm, qui, critiquant le manque de transparence et la collecte excessive de données, a donné lieu à une amende de 16,1 millions de SEK[108]; ou ii) la décision du Conseil d'État français en vertu de laquelle la police devait cesser d'utiliser des drones pour contrôler le

[104] P. ex. https://www.beuc.eu/publications/beuc-x-2020-074_two_years_of_the_gdpr_a_cross-border_data_protection_enforcement_case_from_a_consumer_perspective.pdf et https://www.accessnow.org/cms/assets/uploads/2021/05/Three-Years-Under-GDPR-report.pdf.
[105] https://edri.org/our-work/technological-testing-grounds-border-tech-is-experimenting-with-peoples-lives/.
[106] Voir par exemple https://edri.org/wp-content/uploads/2020/10/20201020-EDRi-Open-letter-CSAM-and-encryption-FINAL.pdf ou https://netzpolitik.org/2021/finfisher-wir-verklagen-das-bka-auf-den-staatstrojaner-vertrag/.
[107] Voir par exemple https://www.statewatch.org/news/2020/november/eu-council-set-to-adopt-declaration-against-encryption/ ou https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf?utm_source=dsms- or https://www.bitkom.org/sites/default/files/2020-12/201211_pp_bitkom_grundsatzerklarung-verschlusselung_0.pdf auto&utm_medium=email&utm_campaign=Encryption%3A+Council+adopts+resolution+on+security+through+encryption+and+security+despite+encryption.
[108] https://edpb.europa.eu/news/national-news/2021/unlawful-use-body-cams-stockholms-public-transport_en; https://www.imy.se/tillsyner/storstockholms-lokaltrafik-sl/.

respect des règles de distanciation sociale, car ces drones avaient la capacité technique d'identifier des personnes et n'étaient pas utilisés dans le respect de la loi sur la protection des données[109].

Le cadre européen relatif à une identité numérique, actuellement proposé, offrira à tous les citoyens et résidents de l'UE qui le souhaitent un portefeuille numérique fiable et sécurisé, dont l'utilisateur aura le contrôle intégral et qui lui servira de passe «autonome» pour accéder aux services publics et privés numériques et partager toute une série d'attributs et de justificatifs[110].

8.1 Conservation des données

Depuis 2014, les lois nationales prévoyant la conservation des métadonnées de télécommunications (données relatives au trafic et données de localisation) à des fins de répression et de renseignement ont été jugées contraires aux exigences du droit de l'Union par la Cour de justice de l'UE. La Cour a considéré que ces législations nationales constituaient une ingérence grave et disproportionnée dans le droit au respect de la vie privée et le droit à la protection des données car les métadonnées de communication peuvent révéler des informations sur un nombre significatif d'aspects de la vie privée des personnes concernées[111]. Tout en reconnaissant que les mesures de conservation des données poursuivent des objectifs légitimes d'intérêt public, la Cour a souvent jugé, à quelques exceptions près[112], que le droit de l'Union s'opposait aux mesures législatives qui imposaient aux fournisseurs de services de communications électroniques, à titre de mesure préventive, une obligation de conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation. Dans la **stratégie de l'UE visant à lutter contre la criminalité organisée 2021-2025** publiée le 14 avril 2021, la Commission a annoncé qu'elle analyserait et présenterait les approches envisageables en matière de conservation des données, conformément aux arrêts de la Cour, afin de répondre aux besoins des services répressifs et judiciaires d'une manière qui soit utile sur le plan opérationnel, techniquement possible et juridiquement solide, notamment en respectant pleinement les droits fondamentaux, et qu'elle consulterait les États membres avant la fin du mois de juin 2021. À l'heure actuelle, la Commission est engagée dans le processus consultatif et examinera attentivement les résultats de cette consultation avant de prendre une décision sur la possible marche à suivre.

8.2 Chiffrement

Le chiffrement est essentiel pour protéger les droits fondamentaux et sécuriser les systèmes et les transactions. La législation de l'Union prévoit le chiffrement en tant que mesure destinée à assurer la protection des droits fondamentaux tels que le respect à la vie privée, la

[109] https://www.conseil-etat.fr/actualites/actualites/le-conseil-d-etat-ordonne-a-l-etat-de-cesser-immediatement-la-surveillance-par-drone-du-respect-des-regles-sanitaires.
[110] COM(2021)281 final.
[111] Voir, par exemple, arrêt du 2 mars 2021, Prokuratuur, affaire C-746/18, ECLI:EU:C:2021:152.
[112] Voir arrêt du 6 octobre 2020, La Quadrature du Net e.a., affaires jointes C-511/18, C-512/18 et C-520/18, ECLI:EU:C:2020:791, dans lequel la Cour a autorisé la conservation généralisée des données relatives au trafic et des données de localisation pour se prémunir contre des menaces graves pour la sécurité nationale, celle des adresses IP de la source d'une communication pour lutter contre les infractions graves et celle des données relatives à l'identité civile pour lutter contre la criminalité en général.

protection des données à caractère personnel[113] et la liberté d'expression, ainsi qu'à garantir la cybersécurité[114]. En outre, le chiffrement est également important pour la protection des secrets d'affaires et aide ainsi les personnes à jouir de leur droit à la liberté d'entreprise. Depuis le début de la pandémie de COVID-19, et conjointement à l'utilisation croissante des outils numériques dans tous les domaines de la vie, le nombre de cyberattaques a augmenté. Ces attaques ont causé des dommages importants à des entreprises et à des services essentiels, notamment des systèmes de soins de santé, et ont mis en péril les droits des personnes, mettant en évidence l'importance du chiffrement pour les acteurs publics et privés, car il protège la confidentialité des informations[115].

Toutefois, l'utilisation du chiffrement permet également aux criminels de masquer leur identité et de dissimuler le contenu de leurs communications. En réaction aux appels lancés par les États membres, la Commission s'est engagée à étudier des solutions équilibrées d'ordre technique, opérationnel et juridique aux difficultés rencontrées. Ces solutions doivent préserver l'efficacité du chiffrement pour ce qui est de la protection de la vie privée et de la sécurité des communications, tout en apportant une réponse efficace à la criminalité et au terrorisme[116]. La Commission entend proposer, en 2022, une voie à suivre pour permettre un accès légal et ciblé aux informations cryptées dans le cadre d'enquêtes et de poursuites pénales, sur la base d'une cartographie détaillée de la manière dont les États membres traitent le chiffrement, ainsi que d'un processus multipartite visant à explorer et à évaluer les options concrètes (juridiques, éthiques et techniques)[117].

8.3 Identification biométrique à distance

Les règles de l'Union en matière de protection des données interdisent en principe le traitement de données biométriques aux fins d'identifier une personne physique de manière unique, sauf dans des conditions précises[118]. Le traitement de ces données doit reposer sur une base juridique fondée sur la législation relative à la protection des données. Une telle base juridique pourrait être le consentement librement donné de toutes les personnes concernées, difficile à obtenir dans la pratique, ou bien un acte législatif de l'Union ou d'un

[113] Article 32, paragraphe 1, point a), article 34, paragraphe 3, point a), article 6, paragraphe 4, point e), et considérant 83 du règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE; considérant 60, article 31, paragraphe 3, point a), de la directive en matière de protection des données dans le domaine répressif; considérant 20, en liaison avec l'article 4 de la directive 2002/58/CE «vie privée et communications électroniques».

[114] Article 40, paragraphe 1, et considérant 96 du code des communications électroniques européen; considérant 40 du règlement (UE) 2019/881 sur la cybersécurité.

[115] Le comité européen de la protection des données (EDPB) a adopté ses «Guidelines 1/2021 on Examples regarding Data Breach Notification» (version pour consultation publique). Le chiffrement joue un rôle important dans la réduction des risques de violation des données à caractère personnel.

[116] Cet engagement s'inscrit dans le cadre de la stratégie pour l'union de la sécurité, de juillet 2020.

[117] Stratégie visant à lutter contre la criminalité organisée, adoptée le 14 avril 2021.

[118] Voir article 9 du règlement général sur la protection des données et article 10 de la directive en matière de protection des données dans le domaine répressif. En vertu du RGPD, un tel traitement ne peut avoir lieu que pour un nombre limité de motifs, le principal étant qu'il soit nécessaire pour des raisons d'intérêt public important. Dans ce cas, il doit avoir lieu sur la base du droit de l'Union ou du droit d'un État membre, sous réserve des exigences en matière de proportionnalité, de respect du contenu essentiel du droit à la protection des données et de garanties adéquates. En vertu de la directive en matière de protection des données dans le domaine répressif, le traitement doit être strictement nécessaire, il doit être en principe autorisé par le droit de l'Union ou le droit d'un État membre et être assorti de garanties adéquates.

État membre qui poursuit un intérêt public important, comme la prévention d'une menace concrète et immédiate d'attaque terroriste. Dans le domaine répressif, le traitement sera autorisé par la loi. Lorsque le traitement de données biométriques est fondé sur la loi, l'acte législatif doit être proportionné au but poursuivi, respecter l'essence du droit à la protection des données et des autres droits fondamentaux et prévoir des mesures appropriées et spécifiques de protection des droits fondamentaux et des intérêts des personnes concernées.

Les OSC se sont dites alarmées par l'utilisation croissante des technologies d'identification biométrique à distance dans plusieurs États membres et ont demandé l'interdiction de leur utilisation[119]. Le recours aux systèmes biométriques à distance a également été critiqué par le contrôleur européen de la protection des données, le comité européen de protection des données qui regroupe les autorités nationales chargées de la protection des données[120], et d'autres organismes nationaux de défense des droits fondamentaux, comme le défenseur des droits en France[121]. Il existe un certain nombre d'exemples où les autorités chargées de la protection des données sont intervenues pour mettre fin à l'utilisation illégale de ces technologies, par exemple dans une école en France, par la police en Suède ou par un supermarché néerlandais[122].

En plus du cadre existant, le règlement sur l'IA proposé par la Commission en avril 2021 (voir chapitre 4) prévoit une interdiction de l'identification biométrique à distance en temps réel dans des espaces accessibles au public et l'autorise à des fins répressives à titre d'exception dans trois situations limitées et à condition que des garanties spécifiques s'appliquent[123].

8.4 Éducation

Pendant la pandémie de COVID-19, les établissements d'enseignement et de formation ont utilisé différentes plateformes et outils en ligne. L'utilisation de solutions et de logiciels commerciaux d'apprentissage en ligne, souvent en tant que «solutions à court terme», pour surveiller les étudiants qui passent des examens à distance a suscité des inquiétudes quant à la

[119] https://edri.org/our-work/biometric-mass-surveillance-flourishes-in-germany-and-the-netherlands/ et https://reclaimyourface.eu/.
[120] https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-call-ban-use-ai-automated-recognition_en.
[121] https://www.defenseurdesdroits.fr/fr/communique-de-presse/2021/07/technologies-biometriques-la-defenseure-des-droits-appelle-au-respect.
[122] Autorité néerlandaise chargée de la protection des données: Dutch DPA issues Formal Warning to a Supermarket for its use of Facial Recognition Technology |Comité européen de protection des données; l'autorité suédoise chargée de la protection des données inflige une amende à la police pour l'utilisation de Clearview: Sweden fines police for illegal facial recognition tech use - POLITICO Pro; l'autorité française chargée de la protection des données se prononce sur l'utilisation de la reconnaissance biométrique dans les écoles: French privacy watchdog says facial recognition trial in high schools is illegal - POLITICO Pro.
[123] L'article 5, paragraphe 1, point d), de la proposition prévoit que cette utilisation doit être strictement nécessaire pour i) la recherche ciblée de victimes potentielles spécifiques de la criminalité, notamment d'enfants disparus; ii) la prévention d'une menace spécifique, substantielle et imminente pour la vie ou la sécurité physique des personnes physiques ou d'une attaque terroriste; ou iii) la détection de l'auteur ou du suspect d'une infraction pénale visée par le mandat d'arrêt européen et qui est assortie d'une sanction, dans l'État membre concerné, d'une durée maximale d'au moins trois ans. L'utilisation doit également être autorisée par une instance judiciaire ou un autre organe indépendant et est soumise à des limitations appropriées concernant la durée, la portée géographique et les bases de données consultées.

possibilité que leur conception exploite les données des utilisateurs à des fins lucratives, plutôt qu'à des fins de pratiques pédagogiques significatives.

Le pôle européen d'éducation numérique, institué dans le cadre du plan d'action en matière d'éducation numérique, est un forum destiné à élaborer des mesures visant à garantir une collaboration intersectorielle plus solide, à favoriser les échanges entre éducateurs, à mettre en place des moyens d'assurance de la qualité et à garantir le respect de la protection des données et de la vie privée. Parmi ceux-ci, l'assurance de la qualité et la confiance joueront un rôle crucial: la première pour promouvoir une compréhension commune des principales normes de qualité en matière d'éducation numérique; la seconde pour garantir le respect de principes clés en matière d'utilisation des données, d'éthique et de respect de la vie privée. Ces deux éléments, outre qu'ils renforcent le degré de préparation numérique des établissements d'enseignement et de formation européens, peuvent accroître la coopération et améliorer la qualité globale des solutions numériques disponibles.

8.5 Santé

De nombreux éléments de la **réponse à la pandémie de COVID-19** impliquent le traitement de données à caractère personnel, y compris de données de santé, qui, en raison de leur caractère sensible, sont soumises à des règles supplémentaires en vertu du RGPD. Le traitement des données à caractère personnel doit être limité à ce qui est nécessaire et proportionné pour atteindre l'objectif et se conformer aux exigences du RGPD. C'est ce qui a guidé l'approche adoptée par l'Union. Par exemple, la Commission a fourni des orientations[124] aux États membres sur les applications de lutte contre la pandémie et soutenu leur travail d'élaboration d'une boîte à outils, en formulant des exigences relatives aux applications[125] et des spécifications techniques pour garantir l'interopérabilité[126] entre les applications d'alerte nationales dans l'Union. La Commission a mis en place une passerelle pour permettre l'envoi de ces alertes par-delà les frontières et entre les applications des différents États membres. Elle a également proposé une plateforme pour l'échange de données provenant des formulaires de localisation des passagers[127] afin de soutenir le suivi transfrontière des contacts dans le cadre des transports. Dans un deuxième temps, elle s'est engagée à proposer un cadre juridique de l'UE pour une approche coordonnée concernant l'enregistrement des déplacements récents, dans la mesure nécessaire pour endiguer la propagation de la COVID-19, en s'appuyant sur l'expérience acquise avec les formulaires de localisation des passagers.

Qui plus est, le Parlement européen et le Conseil ont adopté, le 14 juin 2021, un règlement établissant le système des certificats COVID numériques de l'UE, destiné à faciliter la libre circulation pendant la pandémie de COVID-19[128]. Une infrastructure a été mise en place pour permettre la délivrance et la vérification des certificats de vaccination, de test et de rétablissement, afin de simplifier la vérification des mesures de santé publique lors des déplacements (pour les exemptions aux exigences de quarantaine, par exemple). Afin de faciliter leur utilisation, les certificats sont disponibles en format numérique et sur papier.

[124] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52020XC0417(08).
[125] https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.
[126] https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf.
[127] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A02017D0253-20210726.
[128] http://data.europa.eu/eli/reg/2021/953/oj, accompagné par https://eur-lex.europa.eu/eli/reg/2021/954/oj.

Dans tous les cas, les catégories de données et le traitement sont limités à ce qui est nécessaire pour atteindre l'objectif déclaré. Ainsi, il est interdit à ceux qui vérifient les certificats de conserver leur contenu après vérification. En outre, le cadre de confiance mis en place pour le certificat COVID numérique de l'UE garantit que les certificats peuvent être vérifiés hors ligne, sans que l'émetteur ou tout autre tiers soit informé de la vérification. La transparence est toujours un élément essentiel, tant pour garantir le respect de la charte et de la législation applicable que pour créer et maintenir la confiance. Le résultat montre que, lorsque les mesures sont soigneusement conçues, la protection des données est compatible avec des mesures de santé publique efficaces, peut contribuer à les faire accepter et garantir que le cadre de l'UE en matière de protection des données offre la flexibilité requise.

La Commission élabore actuellement une proposition législative sur l'**espace européen des données de santé**, qui devrait être adoptée au début de 2022. Cet espace vise à faciliter la fourniture de services de santé numériques et à promouvoir l'accès aux données de santé aux fins de la recherche, de l'innovation, de l'élaboration des politiques et des activités réglementaires, tout en améliorant encore le contrôle que les personnes ont sur leurs données à caractère personnel. Cette initiative sera pleinement conforme aux règles de l'Union applicables en matière de protection des données.

8.6 Contrôle du respect

Les autorités de surveillance nationales compétentes pour le suivi et le contrôle du respect des règles en matière de protection des données et de vie privée constituent la pierre angulaire du système de gouvernance de la protection des données de l'Union. Ces autorités et les juridictions nationales sont chargées du suivi et du contrôle du respect des règles prévues par le RGPD, par les lois nationales transposant la directive en matière de protection des données dans le domaine répressif[129] et par la directive relative à la vie privée et aux communications électroniques. Pour la Commission, l'un des principaux objectifs est que les États membres appliquent ces règles de manière correcte et efficace. En vertu du droit de l'Union, les États membres sont tenus de veiller à ce que leurs autorités chargées de la protection des données soient indépendantes et de leur allouer les ressources suffisantes pour qu'elles puissent mener à bien leurs tâches de surveillance[130]. La Commission suit l'évolution de la situation en ce qui concerne l'indépendance, les tâches, les pouvoirs et les ressources des autorités de surveillance et, en cas de non-respect des règles de l'Union par les États membres, elle recourt à des procédures d'infraction pour garantir l'application effective de ces règles.

Les autorités chargées de la protection des données collaborent au sein du comité européen de la protection des données (CEPD) afin de garantir une application cohérente du RGPD, en particulier dans les cas transfrontières. Après trois ans d'application du RGPD, l'efficacité de cette coopération a fait l'objet de critiques[131] et le CEPD poursuivra ses efforts afin de rendre cette collaboration plus efficace[132]. La Commission partage l'avis du Conseil[133], du

[129] https://eur-lex.europa.eu/eli/dir/2016/680/2016-05-04?locale=fr.
[130] CEPD, «Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities», 5 août 2021, publié le 11 août: https://edpb.europa.eu/system/files/2021-08/edpb_report_2021_overviewsaressourcesandenforcement_v3_en_0.pdf.
[131] Voir, par exemple, résolution du Parlement européen [2020/2717(RSP)].
[132] Stratégie 2021-2023 du CEPD, adoptée le 15 décembre 2020, disponible à l'adresse https://edpb.europa.eu/sites/default/files/files/file1/edpb_strategy2021-2023_fr.pdf(europa.eu).

Parlement européen et du CEPD[134] selon lequel il faut désormais se concentrer sur l'amélioration de la mise en œuvre de la législation de l'Union en matière de protection des données et sur les actions visant à renforcer son application.

8.7 Protection des données à caractère personnel en dehors de l'UE

Un aspect essentiel de la protection des droits fondamentaux dans un environnement en ligne réside dans la continuité de la protection assurée aux personnes lorsque leurs données sortent de l'UE. Étant donné que les données à caractère personnel traversent facilement les frontières dans le monde interconnecté d'aujourd'hui et que les flux de données font désormais partie intégrante du commerce, de la coopération réglementaire et même de l'interaction sociale, les protections garanties par le RGPD et la directive en matière répressive seraient inefficaces si elles se limitaient au traitement des données au sein de l'UE.

C'est en tenant compte de ce contexte que la Commission a poursuivi l'ambitieux programme par lequel elle entend promouvoir un niveau élevé de protection en cas de transfert de données des Européens vers l'étranger, tout en facilitant les flux de données. Cela impliquait de collaborer avec des partenaires clés pour parvenir à un «constat d'adéquation», selon lequel un pays tiers offre un niveau de protection des données «substantiellement équivalent» à celui garanti dans l'Union. Il en a découlé des résultats importants, comme l'adoption de deux décisions d'adéquation vis-à-vis du Royaume-Uni (au titre du RGPD et de la directive en matière de protection des données dans le domaine répressif) et la conclusion de pourparlers sur l'adéquation avec la Corée du Sud.

En outre, à la suite de l'invalidation par la Cour de justice de ses conclusions antérieures quant au caractère adéquat du bouclier de protection des données, l'UE et les États-Unis ont intensifié les négociations sur un nouveau cadre UE-États-Unis en matière de protection de la vie privée pour les transferts transatlantiques de données, garantissant le plein respect de l'arrêt de la Cour.

En outre, en juin 2020, la Commission a adopté des clauses contractuelles types modernisées pour le transfert de données à caractère personnel vers des pays tiers, qui reflètent les nouvelles exigences du RGPD et sont adaptées aux besoins de l'économie numérique moderne. Il s'agit de clauses types de protection des données qu'un exportateur de données et un importateur de données peuvent — sur une base volontaire — intégrer dans leurs arrangements contractuels (un contrat de service nécessitant le transfert de données à caractère personnel, par exemple), dont le but est d'offrir des garanties appropriées en matière de protection des données.

La Commission continue également de participer à une initiative intitulée «Libre circulation des données en toute confiance», lancée par le Japon en 2019 et approuvée ensuite par le G20 et le G7. Un élément central de ce concept, actuellement discuté à l'Organisation de coopération et de développement économiques (OCDE) avec la participation active de l'Union et de ses États membres, consiste à tracer une ligne de démarcation entre l'accès

---

[133] Position et conclusions du Conseil relatives à l'application du règlement général sur la protection des données (RGPD) – Adoption, 14994/1/19 REV 1, 19 décembre 2019, disponible en format pdf (europa.eu).
[134] CEPD, rapport annuel 2020, 2 juin 2021, voir EDPB Annual Report 2020 | Comité européen de la protection des données (europa.eu)].

légitime des pouvoirs publics, assorti de limitations et de garanties appropriées, et la surveillance abusive de l'État.

9. Unir les forces afin que l'ère numérique soit bénéfique à la protection des droits fondamentaux

Si l'on considère les défis interdépendants et les mesures correspondantes qui sont examinés dans le présent rapport, il ne fait aucun doute que l'Union et ses États membres sont déterminés à protéger et à promouvoir les droits fondamentaux à l'ère numérique et qu'ils travaillent ensemble pour cerner les meilleurs moyens d'y parvenir. Les exemples mentionnés dans les chapitres précédents sont autant d'occasions d'apprendre les uns des autres et de façonner positivement les changements induits par la transition numérique.

La Commission utilise de nombreux outils pour garantir le respect des droits inscrits dans la charte, tant dans la conception de ses initiatives législatives et politiques que durant la mise en œuvre du droit de l'Union. Elle évaluera en particulier de près les effets sur les droits fondamentaux et s'efforcera d'équilibrer ces effets dans ses initiatives à venir en 2022, par exemple dans les propositions législatives sur:

- un droit à la réparation,
- la cyberrésilience,
- les services de mobilité numérique,
- le paiement instantané,
- un accès réciproque aux informations relatives à la sécurité pour les agents de première ligne entre l'Union et les principaux pays tiers,
- une législation sur la liberté des médias, et
- des normes contraignantes pour les organismes pour l'égalité de traitement.

En outre, dans le contexte de la décennie numérique, la Commission proposera d'inclure un ensemble de principes numériques dans une déclaration solennelle interinstitutionnelle entre la Commission européenne, le Parlement européen et le Conseil. Cette déclaration permettra à la fois d'informer les utilisateurs sur la voie européenne pour la transformation numérique et de guider les décideurs politiques et les opérateurs numériques.

La Commission invite le Parlement européen, le Conseil et les États membres à utiliser le présent rapport annuel sur l'application de la charte des droits fondamentaux de l'UE pour entamer des échanges sur les difficultés posées et les perspectives offertes par la protection des droits fondamentaux à l'ère numérique. Elle se félicite de l'engagement du Conseil à procéder à un échange de vues sur la base des rapports de la Commission[135] et accueillerait également favorablement une discussion au Parlement européen. Ces échanges pourraient notamment permettre de mieux remédier aux difficultés à venir, en particulier de lutter contre les discours haineux et la désinformation, ainsi que de réfléchir à la manière de garantir un équilibre des pouvoirs en ce qui concerne les mesures de surveillance et plus généralement

[135] Conclusions du Conseil sur le renforcement de l'application de la charte des droits fondamentaux de l'Union européenne du 8 mars 2021, point 26.

d’appliquer efficacement les législations visant à protéger les droits fondamentaux dans l’environnement numérique. Ces échanges peuvent contribuer à encadrer l’évolution des politiques de manière constructive et bénéfique.

Ces efforts menés conjointement afin d’assurer l’effectivité, à l’ère numérique, aussi bien de la charte que du plan d’action pour la démocratie européenne[136] et du mécanisme européen de protection de l’état de droit[137], illustrent la détermination de l’Union à promouvoir et à protéger les valeurs sur lesquelles elle repose.

[136] Communication relative au plan d’action pour la démocratie européenne, COM(2020) 790.
[137] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/rule-law-mechanism_fr.