# Numérique

Margo Bernelin, Jessica Eynard

Margo Bernelin et Jessica Eynard, Chronique « mars 2021- septembre 2021 », *Cahiers Droit, Sciences & Technologies*, octobre 2021, n°13. p. 173-216.
https://doi.org/10.4000/cdst.4237



## Panorama

1**Droit du travail et plateformes numériques.** Discutée en mai 2021, la proposition de loi visant à protéger les agents des grandes plateformes numériques en leur reconnaissant la qualité de salarié et en leur offrant un certain contrôle sur les algorithmes qui allouent leurs tâches a finalement été rejetée par le Sénat**1**. Elle établissait un lien entre l'algorithme et la qualification du contrat de travail en précisant que « tout travailleur, dont au moins les deux tiers du revenu professionnel annuel résultent de l'utilisation d'un algorithme exploité directement ou indirectement par une personne, est présumé être lié à cette dernière par un contrat de travail ». Pour rejeter la proposition de loi, les sénateurs ont fait valoir que le cadre juridique unique posé par la proposition se prête mal à la diversité des situations auxquelles sont assujettis les travailleurs du numérique. Ils ont alors souligné les apports de la récente ordonnance du 21 avril 2021 relative aux modalités de représentation des travailleurs indépendants recourant pour leur activité aux plateformes, laquelle devrait permettre d'engager des négociations collectives sur ce thème, et cela sans recourir à une loi**2**. Le rejet de cette proposition tranche avec des décisions judiciaires prises dernièrement, à l'étranger comme en France. C'est le cas d'une décision de la Cour suprême du Royaume-Uni qui, saisie d'un litige opposant l'entreprise UBER à ses chauffeurs, les a qualifiés de salariés au regard du droit du travail britannique**3**. L'année passée, c'est la chambre sociale de la Cour de cassation qui avait, elle, validé le raisonnement des juges du fond reconnaissant l'existence d'un lien de subordination entre les chauffeurs et l'entreprise de VTC**4**. Prenant acte des enjeux en termes d'accession à un statut professionnel, la Commission européenne vient de lancer une nouvelle phase de concertation pour juger de l'opportunité d'établir un texte européen en vue de préciser, entre autres, le statut professionnel des travailleurs des plateformes, et d'encadrer l'information et les voies de recours des travailleurs confrontés à l'usage de décisions automatisées par des algorithmes**5**.

2**Cybersécurité.** La cybersécurité est au cœur de l'actualité juridique européenne. Elle fait référence à la protection des réseaux et infrastructures numériques contre les attaques malveillantes susceptibles de causer des dommages, notamment aux personnes physiques qui participent à ces réseaux et infrastructures ou en dépendent. Notant que : « La cybersécurité peut […] être renforcée en sensibilisant aux menaces en la matière et en développant les compétences, les moyens et les capacités dans l'ensemble de l'Union, tout en prenant pleinement en compte les implications et préoccupations d'ordre social et éthique », l'Union a créé son Centre européen de cybersécurité par l'adoption d'un règlement le 20 mai 2021**6**. De son côté, le Parlement européen a adopté une résolution exigeant un renforcement des règles de protection des objets connectés afin de lutter contre des menaces hybrides composées d'actions de désinformation et de piratage informatique**7**. Quant à la Commission européenne, elle a mis un coup d'accélérateur à la réforme du règlement e-IDAS**8** en publiant une proposition**9**, laquelle envisage notamment de mettre en œuvre des portefeuilles d'identité numérique qui

permettront aux utilisateurs d'accéder à des services en ligne sans la nécessité d'utiliser des moyens d'identifications privés ou de partager inutilement des données personnelles. En application du principe de l'identité auto-souveraine**10**, les utilisateurs devraient pouvoir contrôler le partage des données avec ce nouveau dispositif. De nouveaux services de confiance font aussi leur apparition dans cette proposition, à savoir l'archivage électronique de documents numériques, l'enregistrement de données électroniques dans des registres électroniques, la gestion de dispositifs de création de signature et de cachet électronique à distance, et l'émission d'attestations électroniques d'attributs.

3À l'échelle nationale, les menaces sur la cybersécurité sont également prises au sérieux, comme en témoigne un avis rendu par le Conseil supérieur du numérique et des postes. Il recommande de créer un parquet national dédié à la cyberdélinquances, de former les magistrats aux enjeux du numérique ou encore de « développer un dispositif de régulation du paiement des rançons par les entreprises françaises, soit pour l'interdire, soit pour rendre obligatoire la déclaration aux autorités françaises d'une demande de rançon et de son traitement »**11**.

4**Sécurité intérieure et outils numériques**.

5– GendNote : Depuis de nombreuses années maintenant, les outils numériques sont déployés au soutien de politiques qui entendent assurer la sécurité sur le territoire national. C'est le cas de GendNote, une application qui doit faciliter le recueil de données effectué par les gendarmes dans le cadre de leurs missions**12**. Saisi par des associations, le Conseil d'État (CE) a eu l'occasion de se prononcer sur la légalité de ce dispositif de collecte de données personnelles**13**. Validant le dispositif en lui-même, le CE rappelle que les informations qui seront collectées seront strictement nécessaires pour assurer les missions des gendarmes. En cas de nécessité, elles pourront inclure des données « relatives à la prétendue origine raciale ou ethnique, aux opinions politiques, philosophiques ou religieuses, à l'appartenance syndicale, à la santé ou à la vie sexuelle ou l'orientation sexuelle ». Une partie du décret est néanmoins annulée, celle qui permet l'exploitation ultérieure des données collectées par d'autres systèmes de traitement de données. Le CE indique qu'elle manque de précision quant à l'objet, à la nature et aux conditions de mise en œuvre de ces traitements ultérieurs.

6– Loi pour une sécurité globale préservant les libertés : Adoptée le 15 avril 2021**14**, cette loi étend, entre autres, le déploiement d'outils de captation d'images dans l'espace public. Saisi, le Conseil constitutionnel (CC) valide certains dispositifs comme le port individuel de caméras par les agents de la police nationale, des polices municipales et de la gendarmerie**15**. Toutefois, le CC a émis des réserves et a déclaré certaines dispositions contraires à la Constitution, notamment celle qui autorise à placer sous vidéosurveillance les personnes retenues dans les chambres d'isolement des centres de rétention administrative.

7– Système d'information sur les armes : Créé par un décret du 28 avril 2020**16**, le Système d'information (SI) sur les armes vise à assurer la traçabilité des armes de catégories A, B et C. Ce SI a fait l'objet d'une demande en annulation pour excès de pouvoir auprès du juge administratif. Pour les demandeurs, en autorisant le traitement de données sensibles à l'image des données de santé, le décret ne respecterait pas, entre autres, le droit de la protection des données personnelles. Dans un arrêt du 27 mai 2021, le Conseil d'État rejette cette demande, considérant que le SI ne méconnaît aucune obligation légale, le règlement général sur la protection des données (RGPD) permettant un tel traitement de données, mais aussi la limitation des droits des personnes en raison de l'objectif du traitement, à savoir assurer la sécurité des personnes**17**.

8**Données de connexion.** Le 21 avril 2021**18**, le Conseil d'État a rendu un arrêt important en jugeant que la conservation généralisée des données d'identité, de trafic et de localisation des internautes prévue par le droit français était justifiée par la menace existante pour la sécurité nationale. Dans cette affaire, le Conseil d'État avait saisi la Cour de justice de l'Union européenne (CJUE) pour l'inviter à préciser la portée des règles issues du droit européen (directive 2002/58, dite « vie privée et communications électroniques », et RGPD)**19** afin de juger de la légalité des textes nationaux organisant la conservation des données de tous les internautes par les opérateurs de télécommunication pendant un an pour les besoins du renseignement et des enquêtes pénales. Conformément à ses arrêts *Digital Rights Ireland***20** et *Tele2 Sverige et Watson e.a.***21**, la CJUE avait considéré comme non conformes au droit de l'Union les lois nationales prévoyant une conservation généralisée et indifférenciée des données de connexion**22**, sauf cas particulier, notamment quand l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, sous réserve d'adopter les garanties appropriées (contrôle préalable d'une autorité indépendante et contrôle d'un juge en aval lors de l'exploitation des données conservées). Sur la base d'un « raisonnement complexe et, par certains aspects, ambigu »**23**, le Conseil d'État juge que la conservation généralisée aujourd'hui imposée aux opérateurs par le droit français est bien justifiée par une menace pour la sécurité nationale, et il impose au gouvernement de procéder, sous le contrôle du juge administratif, à un réexamen périodique de l'existence d'une telle menace. Il invalide la conservation généralisée des données de connexion (sauf données présentant peu de risques pour les libertés et droits fondamentaux comme l'adresse IP par exemple, mais également l'état civil) pour les besoins autres que ceux de la sécurité nationale, en particulier la poursuite des infractions pénales. Il souligne également le fait que l'avis rendu par la Commission nationale de contrôle des techniques de renseignement (CNCTR) avant toute autorisation d'exploitation des données conservées pour les besoins du renseignement n'est pas contraignant, et en conclut que le régime ainsi posé est insuffisant et doit être modifié.

9Dans un autre arrêt du 5 juillet 2021 (n° 433539), le Conseil d'État a dû s'interroger sur la validité du traitement de données mis en œuvre dans le cadre de la procédure dite de « riposte graduée » déclenchée à l'initiative de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (HADOPI), notamment à la lumière de la directive *e-Privacy*. Cette procédure implique en effet que la HADOPI traite des données personnelles concernant les abonnés, et qu'elle puisse requérir des opérateurs de communications électroniques qu'ils communiquent les données nécessaires à l'identification de l'abonné dont l'accès a été utilisé pour porter atteinte à des droits de propriété intellectuelle. Les associations de défense des droits et libertés souhaitaient que le décret fixant les modalités du traitement de données personnelles soit abrogé. Saisi d'un recours pour excès de pouvoir à l'encontre de la réponse défavorable donnée à cette demande, le Conseil d'État commence par valider la conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques dans un but de recherche, de détection et de poursuite des infractions pénales en général, sans qu'il soit nécessaire que ces infractions soient graves. Puis, il sursoit à statuer pour poser plusieurs questions préjudicielles à la CJUE afin de déterminer si l'accès aux données relatives à l'identité civile par la HADOPI exige qu'un contrôle préalable soit effectué par une juridiction ou une entité administrative indépendante dotée d'un pouvoir contraignant. Il note cependant qu'un tel contrôle est rendu très compliqué par le nombre important de recueils des données relatives à l'identité civile opéré par la HADOPI dans le cadre de la mise en œuvre de la « riposte graduée ». La validité du mécanisme de la « riposte graduée » repose désormais sur les épaules de la CJUE.

10Cet arrêt est à mettre en parallèle d'une décision rendue par la CJUE le 17 juin 2021**24**, laquelle indique que le droit de l'Union « ne s'oppose, en principe, ni à l'enregistrement

systématique, par le titulaire de droits de propriété intellectuelle ainsi que par un tiers pour son compte, d'adresses IP d'utilisateurs de réseaux de pair à pair dont les connexions Internet ont été prétendument utilisées dans des activités contrefaisantes, ni à la communication des noms et des adresses postales de ces utilisateurs à ce titulaire ou à un tiers afin de lui permettre d'introduire un recours en indemnisation devant une juridiction civile pour un dommage prétendument causé par lesdits utilisateurs ». La Cour note toutefois que les initiatives et demandes d'information d'un titulaire des droits de propriété intellectuelle devaient respecter plusieurs conditions : être justifiées, être proportionnées et non abusives, être prévues par une mesure législative nationale qui limite la portée des droits et des obligations relevant du droit de l'Union.

11**Données personnelles et contrat de sous-traitance**. Dans une décision d'exécution du 4 juin 2021**25**, la Commission européenne précise les modalités de la relation contractuelle entre le responsable de traitement et le sous-traitant visée à l'article 28, paragraphe 7) du RGPD. Elle prévoit notamment la possibilité pour un tiers d'adhérer aux clauses et apporte des éclairages sur les mesures de sécurité qui doivent être mises en œuvre (voir Annexe 3). Elle détaille les modalités de l'assistance apportée par le sous-traitant au responsable du traitement et revient sur les notifications des violations de données, en apportant des précisions sur le contenu de la notification.

12**Fraude fiscale**. L'État se dote d'un nouveau dispositif numérique permettant le traitement de données diverses, notamment celles provenant des réseaux sociaux, afin de mettre en lumière de possibles fraudes fiscales. Les contenus visés sont ceux « librement accessibles et manifestement rendus publics sur les sites internet des opérateurs de plateforme en ligne »**26**. Le traitement permettra d'entraîner un algorithme à identifier les caractéristiques des comportements susceptibles de révéler la commission d'infractions et manquements. Il servira « la mise en place des dispositifs de croisement avec des bases de données de lieux géographiques et des moteurs de recherche spécialisés dans l'identification des lieux correspondant à des images, afin d'identifier des indicateurs de lieux géographiques ».

13**Écologie.** Déposée en octobre 2020, la proposition de loi visant à réduire l'empreinte environnementale du numérique en France a été adoptée par l'Assemblée nationale en deuxième lecture le 18 juin 2021**27**. La proposition comprend des mesures en faveur de l'éducation et de la réduction des dépenses énergétiques liées au numérique. Elle suggère ainsi la formation des étudiants du secondaire et du supérieur aux impacts environnementaux des technologies numériques. Le texte propose également la création d'un observatoire de recherche des impacts environnementaux du numérique qui aurait la charge d'analyser et de quantifier « les impacts directs et indirects du numérique sur l'environnement ainsi que les gains potentiels apportés par le numérique à la transition écologique et solidaire ».

14**Diffusion au public de données d'infractions**. La CJUE a jugé que le RGPD s'oppose à « une législation nationale qui fait obligation à l'organisme public chargé du registre dans lequel sont inscrits les points de pénalité imposés aux conducteurs de véhicules pour des infractions routières de rendre ces données accessibles au public, sans que la personne demandant l'accès ait à justifier d'un intérêt spécifique à obtenir lesdites données ». Ainsi, tout accès par des tiers à ces données doit être justifié. Les juges précisent aussi que le RGPD s'oppose à ce que cet organisme public transfère les données à des opérateurs économiques pour des traitements ultérieurs des données**28**.

15**Cour de cassation**. Le rapport de la Commission de réflexion sur la Cour de cassation 2030, publié en juillet 2021, fait de nombreuses références au numérique. Eu égard au fait que les

réseaux sociaux permettent de prolonger les débats judiciaires, le numérique est tout d'abord envisagé comme un défi nécessitant une stratégie adaptée afin d'asseoir la légitimité démocratique de la Cour. Le rapport revient également sur la politique active d'*open data* de la Cour, et indique qu'un « moteur de recherche en cours de développement permettra aux utilisateurs extérieurs d'accéder à cette immense quantité de décisions par l'intermédiaire du site public de la Cour, dont la rénovation sera prochainement réalisée ». Le rapport poursuit en précisant que : « L'intelligence artificielle, dont l'*open data* permettra un puissant développement, suscite des mises en garde multiples : rigidité de la jurisprudence, profilage des juges, tentatives peu sérieuses d'anticipation des décisions, etc. Ces risques sont réels. Pour contribuer à les réduire, il faudra que la Cour de cassation s'inspire de la Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement élaborée par la Commission européenne pour l'efficacité de la justice (CEPEJ) »**29**. Toutefois, le rapport juge que l'IA peut également offrir de véritables opportunités à la Cour de cassation. Dans cette perspective, la Cour est engagée dans « un projet de recherche visant à étudier les affaires déjà jugées afin d'identifier les arguments et les questions juridiques qui lui sont présentés, les connexités entre les dossiers, les critères objectifs de complexité et les voies optimales de traitement ».

16**Actualité internationale**.

– En Allemagne, le Commissaire de Hambourg pour la protection des données et la liberté d'information a ordonné à la Société Facebook de ne pas traiter pour son propre compte les données personnelles provenant de l'application de sa filiale WhatsApp**30**. Cette décision fait suite aux nouvelles conditions générales d'utilisation de l'application mobile appliquées depuis mai 2021 et qui prévoient explicitement ces transferts et traitements de données par Facebook.

– La Chine s'est dotée d'une loi de protection des données personnelles le 20 août 2021**31**. Elle encadre notamment la prise de décision automatisée fondée sur le traitement de données personnelles en rendant obligatoire l'information des individus concernés par la décision et en leur offrant des possibilités de recours. Par ailleurs, le texte permet la captation d'images dans l'espace public lorsque des raisons de sécurité l'imposent.

– Le protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe (2018 conv. n° 108+), qui consiste à moderniser et à renforcer les règles qui furent posées en 1981, fait l'objet de processus de ratification par les différents États parties au Conseil, et notamment par la France grâce à un projet de loi déposé le 5 mai 2021**32**.

– Aux États-Unis, le Président Biden a annulé un décret présidentiel édicté par son prédécesseur qui visait à encadrer les suppressions de contenus faites par les réseaux sociaux pour assurer le respect de la liberté d'expression**33**. Cette annulation est prononcée dans un contexte où des réseaux sociaux ont suspendu les comptes de Donald Trump et/ou supprimé certains contenus comme l'entreprise Facebook dont le Conseil de surveillance a relevé de nombreuses infractions aux « Standards de la communauté » édictés par l'entreprise**34**.

## I. Le numérique en santé

17À mi-parcours de cette année 2021, l'actualité juridique dans le champ du numérique en santé est riche et reflète avec acuité les débats publics concernant la gestion de la crise sanitaire, et plus particulièrement l'usage d'outils numériques pour contrôler le respect des mesures adoptées (A). L'engouement pour le déploiement d'outils numériques en santé tranche avec

une autre facette de l'actualité de ces derniers mois : la mise en lumière des numéRisques, ces risques associés au numérique, qu'ils visent la vie privée ou encore la cybersécurité des structures, dont le contrôle s'avère délicat (B).

## A. Le contrôle numérique du respect des mesures sanitaires

18Alors que les dispositifs de lutte contre l'épidémie de Covid-19 évoluent et s'adaptent à l'amélioration ou à la dégradation des indicateurs sanitaires**35**, leur contrôle demeure crucial. Dans cette perspective, le législateur et le pouvoir exécutif ont opté pour des outils numériques permettant de contrôler l'application de certains dispositifs en laissant à des tiers la charge de leurs usages à l'image de la vidéosurveillance pour vérifier le port du masque dans certains lieux (1) ou de la mise en place du pass/passe sanitaire numérique**36**(2). Le recours aux outils numériques devait être encore étendu par la loi du 25 juillet 2021 relative à la gestion de la crise sanitaire qui prévoyait initiallement d'utiliser les données collectées auprès des patients et consignées dans le système d'information dédié au dépistage du virus (SI-DEP) afin de contrôler les mesures de placement en isolement des personnes infectées (3).

### 1. Contrôle du port du masque et vidéosurveillance

• Décret n° 2021-269 du 10 mars 2021 relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports.

• CNIL, délibération n° 2020-136 du 17 décembre 2020 portant avis sur un projet de décret relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports.

19Bien que le masque de protection ne soit plus obligatoire à l'extérieur, il reste imposé dans certains lieux publics comme les gares et les moyens de transport de voyageurs, le non-respect de la mesure étant assorti d'une amende de 135 euros. Dès 2020, dans ces lieux, des caméras avaient été déployées ou utilisées spécifiquement pour vérifier l'application de cette obligation. Toutefois, la CNIL avait alerté sur les risques pesant sur la vie privée des individus filmés et sur l'absence de base légale autorisant de tels traitements de données personnelles**37**. Eu égard à cette prise de position, le décret du 10 mars 2021 intervient pour permettre explicitement aux exploitants de services de transport public collectif de voyageurs ainsi qu'aux gestionnaires des espaces affectés à ces services, et qui ont la charge de veiller au respect de l'obligation du port du masque, d'utiliser des caméras fixes pour ce faire. Les images collectées seront traitées grâce à un logiciel intelligent qui repère les cas où le masque n'est pas porté ou mal porté**38**. L'outil technique propose alors des statistiques précises et actualisées, le tout sans conserver les images et sans les transmettre à des tiers. En ce sens, le décret propose d'utiliser des images, non pas pour identifier les voyageurs en infraction, mais plutôt pour cibler les actions de prévention dans des espaces où le masque serait peu porté. Cette mesure est assortie de limites temporelles, le recours aux caméras n'étant permis que pour une durée d'un an à compter de la publication du décret. Pour cette durée, le décret indique que les usagers de ces lieux et transports ne disposent pas des droits prévus par le Règlement général de protection des données (RGPD)**39**. Les voyageurs ne peuvent donc pas s'opposer à ces enregistrements, accéder à leurs données, ni demander leur rectification, effacement ou la limitation des captations. En contrepartie, le responsable du traitement doit informer les voyageurs de l'usage de la vidéosurveillance et des caractéristiques principales du traitement des données.

20Dans son avis de décembre 2020 sur le projet de décret, la CNIL avait validé le dispositif, estimant que l'impératif de santé publique justifiait ces dérogations au RGPD. Toutefois l'autorité indépendante avait précisé que, « même s'il est limité au cadre de l'état d'urgence sanitaire, un tel déploiement présente le risque réel de généraliser un sentiment de surveillance chez les citoyens, de créer un phénomène d'accoutumance et de banalisation de technologies intrusives et, en définitive, d'engendrer une surveillance accrue »**40**. Cette surveillance numérique est bien au cœur des critiques qui restent adressées à ce décret. Certaines font notamment valoir que le traitement des données manquerait encore de base légale et regrettent que les données personnelles collectées n'aient pas été qualifiées de « données biométriques », des données sensibles qui auraient imposé un encadrement plus strict de ces captations**41**.

## 2. Contrôle du passe sanitaire numérique et TousAntiCovid

• Loi n° 2021-689 du 31 mai 2021 relative à la gestion de la sortie de crise sanitaire.

• Décret n° 2021-724 du 7 juin 2021 modifiant le décret n° 2021-699 du 1er juin 2021 prescrivant les mesures générales nécessaires à la gestion de la sortie de crise sanitaire.

• Règlement (UE) 2021/953 du Parlement européen et du Conseil du 14 juin 2021 relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats Covid-19 interopérables de vaccination, de test et de rétablissement (certificat Covid numérique de l'UE) afin de faciliter la libre circulation pendant la pandémie de Covid-19a.

• Conseil d'État, juge des référés, 6 juillet 2021, 453505.

a. V. aussi son pendant, le Règl. (UE) 2021/954 du PE et du Cons., 14 juin 2021, relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats Covid-19 interopérables de vaccination, de test et de rétablissement (certificat Covid numérique de l'UE) destinés aux ressortissants de pays tiers séjournant ou résidant légalement sur le territoire des États membres pendant la pandémie de Covid-19, qui permet aux EM d'appliquer le Règlement n° 953 aux ressortissants d'états tiers séjournant ou résidant sur leur territoire.

« Dès le 21 juillet, le pass sanitaire sera étendu aux lieux de loisirs et de culture. Concrètement, pour tous nos compatriotes de plus de 12 ans, il faudra, pour accéder à un spectacle, un parc d'attraction, un concert ou un festival, avoir été vacciné ou présenter un test négatif récent. Ce pass est disponible sur l'application TOUSANTICOVID. Mais chacun peut utiliser la version papier remise au moment de la vaccination »**42**.

21Ce passe sanitaire a été étendu à d'autres lieux, à l'image des restaurants et cafés, grâce au vote du projet de loi relatif à l'adaptation de nos outils de gestion de crise**43**. Il correspond à la preuve que l'individu dispose d'une certaine immunité face aux virus du Covid-19 (grâce à la vaccination ou à une précédente contamination), ou qu'il n'est pas atteint par ce dernier (résultat négatif de diagnostic ou de dépistage)**44**. Le passe se compose d'éléments d'identification des individus (nom, prénom, date de naissance), de données de santé (vaccin, résultats de diagnostics ou de dépistages ou certificat de rétablissement), et d'éléments sur l'organisme qui a émis le passe. Ces informations se présentent sur support papier ou numérique en deux formats : l'un classique qui peut être lu par tout à chacun, l'autre un QR code qui nécessite une application numérique pour sa lecture. En France, l'application TousAntiCovid, permet à son utilisateur d'y inscrire son passe sanitaire composé alors du QR code et des mentions des

nom, prénom, date de naissance, justification précise du passe (par ex. vaccination, nom du vaccin et le nombre de doses).

22Ce passe sanitaire prend appui sur le décret n° 2021-724 du 7 juin 2021 et sur le règlement UE n° 2021/953 du 14 juin 2021**45**. Ce dernier texte offre un cadre juridique unique pour la délivrance, la vérification et l'acceptation des « certificats Covid numérique », autrement dit du passe sanitaire européen. Cela permet aux citoyens européens de présenter, dans différents États membres, le passe sanitaire émis par leur État, lequel sera, sans difficulté, contrôlé et accepté. À cette fin, le règlement définit le certificat Covid numérique comme un document « interopérable contenant des informations sur la vaccination, les résultats des tests ou le rétablissement du titulaire délivré dans le contexte de la pandémie de Covid-19 »**46** lequel se décline selon les justifications (vaccin, tests ou rétablissement)**47**. Le règlement impose la gratuité de l'émission du certificat et décrit précisément les indications qu'il doit comprendre afin d'uniformiser sa composition au sein de l'UE. Si les EM s'engagent à utiliser le certificat numérique européen, ils doivent alors s'abstenir d'imposer toute autre restriction aux libertés de déplacement telle que des tests de dépistage supplémentaires, sauf en cas de situation sanitaire exceptionnelle**48**.

23Le décret du 7 juin précise, lui, les modalités d'inscription du passe dans l'application française TousAntiCovid**49** et indique que l'enregistrement du passe ne conduit pas à transmettre toutes les données du certificat à un serveur central**50**, les données n'étant conservées que sur le téléphone portable de la personne utilisant l'application. Le contrôle du QR code, qu'il soit présenté sur support papier ou numérique, impose l'utilisation d'une autre application nommée « TousAntiCovid Vérif »**51**. Les personnes habilitées l'utilisent pour lire sans enregistrer les informations suivantes : nom, prénom, date de naissance, validité du certificat**52**. La conservation de ces données par le tiers vérificateur est punie d'un an d'emprisonnement et de 45 000 euros d'amende**53**.

24La mise en œuvre de ce passe sanitaire a fait l'objet de nombreuses critiques notamment relatives aux restrictions de libertés qu'elle implique. Dans ce cadre, l'Association La Quadrature du net a saisi le Conseil d'État pour obtenir la suspension de l'utilisation de ce passe dans sa version papier, mais aussi numérique, faisant entre autres valoir les risques de récupération des données de santé lors d'un contrôle du QR code. Balayant l'argument, les juges estiment que les données consultées lors des contrôles sont en nombre limité**54**. Parallèlement, ils précisent que les risques de captation malveillante des données lues par l'application sont, eux, peu élevés. L'utilisation du QR code est même recommandée par le Conseil scientifique Covid 19, qui note qu'à l'inverse du QR code, le format papier ne permet pas de « masquer des données personnelles et médicales, que le contrôleur du pass sanitaire n'a pas à connaître »**55**. Par opposition, le QR code empêche la lecture de toutes ces informations.

25En France, les applications TousAntiCovid et TousAntiCovid Vérif détiennent donc une place centrale pour le contrôle du passe sanitaire, faisant de l'application mère, TousAntiCovid, un véritable couteau suisse dans la lutte contre l'épidémie. En effet, l'application TousAntiCovid devient multifonctions et permet de consigner des données de santé. Dans ce cadre, l'application fonctionne ici comme un carnet de santé numérique et permet à son utilisateur de consigner des données personnelles de santé :

« – le statut Covid-19 sélectionné par l'utilisateur de l'application
– la date de début des symptômes
– la date de prélèvement positif
– la présence de fièvre après 7 jours

– la date de dernier contact (pour les personnes contact)
– le partage du foyer avec un cas Covid-19
– la date de fin de symptômes du cas malade
– la date de fin de symptômes du cas malade (cas index d'une personne contact) »**56**.

26Depuis le mois d'avril, l'outil permet également d'ajouter son propre passe sanitaire, mais aussi ceux de ses proches.

27À ce carnet de santé, il faut ajouter une deuxième fonction : l'information personnalisée sur l'évolution de l'épidémie de Covid. L'application propose ainsi une information ciblée en fonction du code postal de l'individu. Composée de chiffres clé, cette information se double de conseils sanitaires face au virus et d'un fil d'actualité visant des thématiques sanitaires, mais aussi les dernières évolutions du droit en lien avec l'épidémie. L'application livre aussi des informations sur les lieux de vaccination et de dépistage.

28Lors des confinements et couvre-feux, l'application permettait également de remplir des autorisations de déplacement en format numérique, troisième fonctionnalité d'une application protéiforme. On en oublierait presque la fonction première de l'application, à savoir de tracer et d'identifier les foyers infectieux ! Pour rappel, l'application a en effet été mise en place afin de pouvoir alerter les personnes qui ont croisé un individu infecté utilisant lui aussi l'application TousAntiCovid. Multi-usages, l'application témoigne de la confiance gouvernementale dans les outils numériques à des fins de gestion de la crise sanitaire, le gouvernement faisant fi des critiques qui lui sont adressées. À cet égard, le Défenseur des droits indiquait en avril 2020 : « L'application pose une grande difficulté, parce qu'elle laisse entrevoir un système de surveillance sociale générale. Il y a des exemples dans certains pays. Par conséquent, il est nécessaire que l'application d'une telle mesure [l'usage de TousAntiCovid] se fasse sur la base du volontariat, que les données recueillies ne remontent pas dans une base centrale, qu'elles soient très clairement supprimées à la fin des circonstances qui conduisent à la mettre en œuvre et que le dispositif fasse l'objet d'une information importante »**57**.

29Cette menace de la société de surveillance, fût-elle sanitaire, serait-elle exagérée ? Pour l'heure, l'application respecte tous les points mentionnés par le Défenseur des droits. Toutefois, au regard des évolutions techniques de l'application TousAntiCovid, de la variété des données qui peuvent y être consignées par les utilisateurs, cette menace ne doit pas être négligée pour autant. Dans cette perspective, l'application pourrait permettre, à l'avenir, le contrôle de nouvelles restrictions, dont le respect du placement à l'isolement des malades.

## 3. Contrôle de l'isolement des personnes infectées et le SI-DEP

• Projet de loi relatif à la gestion de la crise sanitaire (n° 4386), adopté le 5 août 2021 (loi n° 2021-1040 du 5 août 2021 relative à la gestion de la crise sanitaire).

• Conseil constitutionnel, décision n° 2021-824 DC du 5 août 2021.

30Le système d'information SI-DEP est une base de données nationale dédiée au dépistage et au diagnostic du Covid-19. Il consigne toutes les données relatives aux tests, à l'identification des personnes testées ou diagnostiquées, et comprend des informations utiles pour la prise en charge des patients (adresse, numéros de téléphone, médecin traitant, motifs de dépistage tels qu'un retour de voyage, symptômes, etc.). Cette grande base, alimentée principalement par les laboratoires d'analyse et les pharmaciens, doit permettre de suivre l'évolution de l'épidémie,

de prendre en charge les malades et leurs proches grâce aux données renseignées, mais aussi de pouvoir mener des recherches rétrospectives sur les données pour comprendre les chaînes de transmission du virus. Avec plus de 100 millions de tests effectués au 1er juillet 2021**58**, la base de données est considérable ! Face à la dégradation de la situation sanitaire en début d'été, le gouvernement a souhaité mettre à profit ce maillage numérique pour contrôler le placement à l'isolement des malades dépistés ou diagnostiqués. Ainsi, aux termes des articles 7 et 9 de la loi adoptée le 25 juillet 2021 relative à la gestion de la crise, le placement à l'isolement d'une durée de dix jours devait être contrôlé à l'appui des adresses et des informations médicales contenues dans le SI-DEP**59**.

31Pour mener à bien ces contrôles, des agents préfectoraux devaient recevoir les informations jugées « nécessaires » en provenance du SI-DEP. Validée par le Conseil d'État**60**, mais aussi par le rapport de la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République**61**, cette disposition n'en restait pas moins critiquable. L'absence de précision quant aux informations qualifiées de « nécessaires », tout comme l'absence d'indication des personnels habilités en préfecture à recevoir ces données, laissaient entrevoir des atteintes manifestes à la vie privées des personnes. Aussi lister, dans la loi, les données pouvant être transmises en préfecture, ainsi qu'identifier les catégories de personnel pouvant y avoir accès, auraient été plus protecteurs pour la vie privée des individus. De même, l'interdiction de l'utilisation de ces données pour enrichir d'autres fichiers informatisés détenus par la police ou la gendarmerie aurait été un garde-fou supplémentaire. En effet, le manque de précision de la loi ne permettait pas d'affirmer que les informations relatives à la composition du foyer de la personne concernée ou à ses symptômes ne seraient pas transmises avec leur adresse en préfecture, ni utilisées à d'autres fins que le contrôle de l'isolement**62**. De plus, la loi ne précisait pas le délai sous lequel ces données devaient être effacées, ce qui faisait courir un danger supplémentaire pour la protection de la vie privée des personnes concernées. Dans son avis sur le projet de loi, le Conseil d'État avait averti le gouvernement : les données ne pourraient être conservées que pour une durée « nécessaire à l'exercice de leur mission de contrôle », et cela en vertu de l'article 5 du RGPD**63**. Toutefois, le gouvernement n'avait pas modifié son projet pour intégrer une date de suppression des données.

32Le manque de précision de la nouvelle loi était d'autant plus regrettable que les personnes concernées par les dépistages et diagnostics ne peuvent refuser l'inscription de leurs données au sein du SI-DEP, ni leur suppression. La mission première assignée à ce SI était alors largement modifiée : d'un outil de suivi épidémiologique et de prise en charge sanitaire qui justifie une collecte large et sans le consentement des intéressés, le SI devenait en effet un moyen de répression des comportements et de contrôle des mesures très strictes d'isolement prévues par le projet de loi**64**.

33La décision n° 2021-824 DC du 5 août 2021 du Conseil constitutionnel a purement et simplement invalidé le dispositif. Bien que reconnaissant que le placement à l'isolement des personnes infectées par le virus est une mesure qui poursuit l'objectif à valeur constitutionnelle de protection de la santé**65**, le Conseil constitutionnel estime qu'il constitue une mesure de privation de liberté qui devrait prendre en compte la situation personnelle de l'individu, faute de quoi il n'est pas démontré que la mesure est nécessaire, adaptée et proportionnée. Par conséquent, les Sages jugent que les articles 9 et 7 (1er) sont contraires à la Constitution et, sans se prononcer sur l'usage du SI-DEP, suppriment par là même le dispositif assez flou envisagé par le gouvernement.

## B. Le délicat contrôle des NuméRisques

34Le déploiement toujours plus important des outils numériques s'accompagne de risques pesant sur leurs utilisateurs et sur les personnes dont les données sont collectées pour les alimenter. Dans le domaine de la santé, les données sont sensibles et imposent un surcroît d'attention afin de protéger la vie privée des personnes dont l'intimité peut être dévoilée. Deux récentes décisions et un avis mettent en lumière ces risques protéiformes, qu'il s'agisse des risques posés par l'accès à des données personnelles par des États tiers (1) ou par des personnes malveillantes (2) ou du risque de cyberattaques pesant sur les infrastructures (3).

### 1. L'accès aux données par des États tiers. Le cas des données collectées par les plateformes privées de prises de rendez-vous médicaux

• Conseil d'État, ordonnance du 12 mars 2021, n° 450163, Association InterHop et autres.

35Depuis quelques années maintenant, les plateformes privées de prises de rendez-vous médicaux ont connu un grand essor. Permettant au patient de prendre rendez-vous en ligne pour consulter un professionnel de santé et partager des documents médicaux, les plateformes offrent des facilités de gestion aux professionnels en soulageant leur secrétariat et en automatisant la transmission aux patients d'informations nécessaires à la tenue du rendez-vous. Ces plateformes sont en pleine expansion et comptent dans leur rang la « licorne » Doctolib, leader dont la valorisation dépasse le milliard d'euros**66**. Pendant la crise sanitaire, le gouvernement s'est appuyé sur ces plateformes privées afin d'organiser et d'accélérer la prise de rendez-vous pour la vaccination**67**. Ainsi, les sites internet Doctolib, Keldoc et Maiia ont été mis à contribution et ont dédié une partie de leur contenu à cet effort. Pratiques pour certains, notamment pour les plus au fait des outils numériques, ces plateformes réactives ont permis de soulager les serveurs téléphoniques surchargés des centres de vaccination. Pour le patient, il suffisait de créer un compte en renseignant nom, prénom, adresse email et numéro de téléphone pour prendre rendez-vous. Toutefois, d'autres ont pu critiquer ce dispositif technique qui a pris une place de premier rang dans la communication sur la vaccination, le site internet Doctolib informant par exemple, avant même le gouvernement, que l'objectif du nombre de personnes vaccinées au 31 mai serait atteint avec de l'avance**68**. Ces critiques ont culminé avec la saisine du juge administratif par des associations et syndicats de professionnels de santé**69** enjoignant le Conseil d'État de suspendre le partenariat entre l'État et la plateforme Doctolib. Selon les demandeurs, l'hébergement des données, c'est-à-dire leur conservation, effectué pour le compte de Doctolib par une filiale d'une entreprise américaine (Amazon Web Services - AWS) faisait planer le risque d'un accès par les autorités américaines à ces données sensibles.

36Les requérants reprennent en sus les mêmes arguments que ceux invoqués devant le CE pour demander la suspension de l'hébergement des données du Health Data Hub par la société Microsoft en brandissant le RGPD**70**. Toutefois, dans cette espèce, comme dans l'autre, le CE ne suit pas les demandeurs. En tout premier lieu, les juges n'estiment pas qu'il s'agisse de données sensibles, lesquelles nécessiteraient des protections supplémentaires. Ils relèvent que les informations conservées sont davantage des « données d'identification des personnes et des données relatives aux rendez-vous, mais pas des données de santé sur les éventuels motifs médicaux d'éligibilité à la vaccination, les personnes intéressées se bornant, au moment de la prise de rendez-vous, à certifier sur l'honneur qu'elles entrent dans la priorité vaccinale, qui est susceptible de concerner des adultes de tous âges sans motif médical particulier ». S'il est vrai que les motifs médicaux précis permettant la prise de rendez-vous ne sont pas renseignés manuellement par l'utilisateur, des cases à cocher visent expressément des causes de

comorbidités afin de pouvoir accéder à la prise de rendez-vous pour certains centres de vaccination. Faut-il alors comprendre que ces données, qui ont fait l'objet d'une validation par le patient, ne sont pas conservées par la plateforme en ligne ? L'on peut en douter. Les juges poursuivent et tentent de rassurer : les « données sont supprimées au plus tard à l'issue d'un délai de trois mois à compter de la date de rendez-vous, chaque personne concernée ayant créé un compte sur la plateforme pour les besoins de la vaccination pouvant le supprimer directement en ligne ». À ces protections tenant à la minimisation des données collectées, à leur conservation limitée dans le temps et à la possibilité individuelle de supprimer ce compte, s'ajoutent les précautions contractuelles prises par Doctolib. Ainsi, aux termes de l'addendum complémentaire conclu entre la plateforme et la société AWS, les données hébergées font l'objet d'un chiffrement particulier, ce qui doit empêcher des tiers de lire les données. Par ailleurs, si la société AWS devait être sollicitée par une autorité publique pour obtenir un accès aux données de la plateforme, elle s'engage à contester « toute demande générale ou ne respectant pas la réglementation européenne », faisant de la filiale américaine la première garante du respect du droit de l'Union... ! Pour les juges, ces éléments sont suffisants pour garantir l'absence d'atteinte manifestement illégale au droit au respect de la vie privée.

37Ce nouveau rejet d'une demande de suspension d'un outil numérique utilisé dans la lutte contre l'épidémie de Covid témoigne d'une véritable politique jurisprudentielle qui ne sanctionne pas le risque potentiel, mais seulement le risque avéré d'atteinte aux libertés dans le contexte de crise sanitaire. Par ailleurs, les affaires ainsi portées devant le Conseil d'État, Doctolib, mais aussi le Health Data Hub avant elle, mettent en lumière les imbrications structurelles qui permettent à ces plateformes d'opérer, et témoignent de l'absence de souveraineté numérique quant à l'hébergement des données de santé.

## 2. L'accès aux données par des personnes malveillantes : le cas des cyberattaques visant les données de santé numérisées

• Tribunal judiciaire de Paris, ordonnance de référé, 4 mars 2021, n° RG 21/51823.

38Noms, âge, numéros de téléphone, de sécurité sociale, de mutuelle, adresses, nom du médecin traitant, groupe sanguin, pathologies, résultats de tests, etc. : voici autant de données personnelles piratées auprès de différents laboratoires d'analyses médicales en février 2021 et diffusées sur Internet, notamment sous la forme d'un fichier unique rassemblant toutes ces données. En tout, ce sont 500 000 personnes qui ont été concernées directement par ce qui a été bien mal nommé dans la presse une « fuite » de données**71**. Cette action malveillante a mis en lumière les failles de sécurité de certains serveurs utilisés par des laboratoires de biologie médicale, alors même que les données de santé, qualifiées de sensibles par le RGPD, sont soumises à un encadrement strict**72**. Selon le droit français, lorsqu'elles sont stockées par un tiers, les données doivent être conservées par un hébergeur certifié et ne peuvent être commercialisées**73**. Malgré ces dispositions qui se veulent protectrices de la vie privée, le risque zéro n'existe donc pas.

39Notant qu'il s'agit « effectivement d'une violation de données d'une ampleur et d'une gravité particulièrement importantes », la CNIL n'a pas tardé à réagir pour rappeler que les responsables de traitement de données concernés ont l'obligation de notifier et d'informer individuellement les personnes concernées par ces fuites**74**. De plus, l'autorité indépendante a précisé mener des contrôles pour faire la lumière sur les événements. Toutefois, cette réponse ferme de la CNIL n'a pas été suffisante pour enrayer la situation, et l'autorité a saisi le tribunal judiciaire (TJ) de Paris en référé afin de demander aux fournisseurs d'accès à Internet de

bloquer l'accès à un site hébergeant les données en cause**75**. Par une ordonnance rendue le 4 mars 2021, le TJ de Paris fait droit à cette demande**76**. Se fondant sur l'article 6.I-8 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, le TJ enjoint à Bouygues, Orange, SFR et Free « de mettre en œuvre ou de faire mettre en œuvre, sans délai et de manière définitive et illimitée, toutes mesures les plus adaptées et les plus efficaces de surveillance ciblées de nature à assurer le blocage effectif du fichier […] ou, à défaut, du service de communication au public en ligne ». Les arguments visant les difficultés techniques pour ce faire n'ont pas été suivis par les juges qui, sans surprise, ont considéré qu'il s'agissait bien d'une atteinte grave et immédiate aux droits des personnes concernées nécessitant d'imposer des mesures rapides.

40Cette affaire met en lumière à la fois les risques de cyberattaque pesant sur les données de santé, mais aussi les limites territoriales des mesures de protection pouvant être adoptées par la CNIL face à une telle action malveillante. En effet, l'ordonnance du tribunal révèle que le site internet hébergeant les données piratées utilise le domaine national internet de l'Île de Guernesey, mais que l'adresse de contact renvoie vers un message d'erreur. Impossible donc pour la CNIL d'entrer en communication avec les responsables du site pour obtenir la suppression du dossier comprenant les données de santé. L'hébergeur du site internet est quant à lui situé à San Francisco aux États-Unis et n'a pas donné suite aux courriers de la CNIL visant à demander la suspension de la diffusion du site internet. Ainsi, pour la CNIL peu d'autres options étaient offertes si ce n'est la saisine du juge judiciaire pour obtenir des fournisseurs d'accès français à Internet de bloquer l'accès au contenu litigieux afin d'empêcher la consultation des données. L'accès est donc bloqué, mais seulement sur le sol français. Un internaute situé aux États-Unis pourrait quant à lui accéder aux données diffusées sur le site internet litigieux et non bloqué dans son État. Partant, la protection accordée par le TJ est elle aussi restreinte au territoire national et donc bien limitée.

### 3. Cyberattaques : le cas des infrastructures

• CADA, avis n° 20210021 du 15 avril 2021.

41Comme l'a mis en lumière l'affaire précédente, la sécurité des systèmes d'information est primordiale pour garantir le respect de la vie privée des personnes dont les données de santé sont traitées. Pour renforcer la cybersécurité des établissements de santé, le gouvernement a présenté en février dernier sa stratégie en la matière, laquelle passe notamment par un investissement financier et des formations**77**. Dans le domaine de la santé, cette nécessaire sécurité semble imposer l'opacité sur le fonctionnement des structures publiques qui participent à la collecte des données personnelles, comme en témoigne une décision récente de la Commission d'accès aux documents administratifs (CADA) concernant la Plateforme nationale des données de santé. Cette plateforme, aussi nommée *Health Data Hub* (HDH), est coresponsable avec l'Assurance Maladie du Système national des données de santé (SNDS), lequel centralise et met à disposition des données de santé en très grands volumes pour la recherche scientifique. À ce titre, le SNDS comprend toutes les données personnelles collectées dans le cadre de la lutte contre l'épidémie de Covid-19**78**. Réformés en juin 2021**79**, les rôles et prérogatives du HDH sont nombreux : il assure l'enrichissement des bases de données du SNDS, l'information du public et des personnes concernées par les recherches menées sur les données grâce à son site internet et est dépositaire d'une copie de la base de données principale du SNDS, y compris celle de l'Assurance Maladie sur le remboursement des soins**80**.

42Le HDH a pu être accusé d'un manque de transparence, notamment sur la sélection de l'opérateur chargé de l'hébergement des données de santé**81**. Dans ce cadre, la saga de l'été 2020 devant le Conseil d'État n'avait pas permis aux opposants du HDH d'obtenir la suspension de ses activités de centralisation des données Covid. C'est alors la CADA qui fut saisie par le président du Conseil national du logiciel libre pour obtenir la publication des codes sources du Hub, c'est-à-dire de ses divers codes de programmation – pour les opposants au Hub, pouvoir consulter ces codes permettait de prendre la mesure des choix techniques opérés et des failles de sécurité d'un outil technique omniprésent dans le champ de la centralisation des données de santé**82**. Le ministre des Solidarités et de la Santé a refusé cette transmission, faisant valoir que la plateforme est « configurée selon le principe de "*Infrastructure as code*" ce qui signifie que la divulgation du code source revient à décrire techniquement l'ensemble des éléments déployés pour la sécurité et la gestion fonctionnelle de l'infrastructure ». Par conséquent, la publication de ces codes pourrait permettre à des tiers de détecter les failles de la plateforme et de l'attaquer, mettant à mal la sécurité des données dont il détient la copie, argument suivi par la CADA**83**. Les demandeurs ont toutefois obtenu la transmission du rapport du HDH sur la réversibilité de l'hébergement des données, c'est-à-dire sur la possibilité de changer d'opérateur pour le stockage des données du SNDS, document qui n'emporte pas les mêmes enjeux que les codes sources. La question de la transparence, ici appliquée à l'architecture technique de la plateforme, ne semble pas épuisée. Elle se pose à nouveau sur le terrain de la corruption. En effet, l'association Anticorps a saisi le parquet national financier (PNF) pour faire la lumière sur les conditions de conclusion du contrat liant la plateforme à son hébergeur des données, la société Microsoft**84**, en pointant l'absence de recours au marché pour la sélection de ce prestataire. Le HDH n'est donc pas prêt de quitter les lignes de cette chronique…

M. B.

## II. Vers un cadre juridique européen de l'IA

43Le 21 avril 2021, la Commission européenne a dévoilé sa proposition de règlement**85** établissant des règles harmonisées concernant l'intelligence artificielle**86**. Cette proposition était attendue puisqu'elle fait notamment suite à l'adoption d'un Livre blanc**87** et à la communication d'une stratégie sur l'IA**88**.

44Elle n'est pas isolée. Au niveau international, plusieurs instances ont d'ores et déjà dégagé les grandes lignes d'une régulation de l'IA, que l'on pense à l'UNESCO**89**, à l'OCDE**90** ou encore au Conseil de l'Europe. Au niveau de l'Union, cette proposition vient s'ajouter à un ensemble textuel déjà conséquent avec le DSA, le DMA**91**, le *Data Governance Act***92** ou les diverses résolutions du Parlement européen. La proposition européenne n'en demeure pas moins importante, car elle pose les bases d'un cadre contraignant applicable aux systèmes d'intelligence artificielle (SIA) en fonction des risques qu'ils présentent. L'objectif est de penser un ensemble de règles juridiques harmonisées et susceptibles de susciter la confiance pour le bon fonctionnement du marché intérieur. Le fondement légal de la proposition est en ce sens l'article 114 TFUE relatif au marché intérieur, avec un simple renvoi à l'article 16 du TFUE relatif au droit à la protection des données personnelles pour les traitements impliquant une identification biométrique à distance « en temps réel » dans des espaces accessibles au public à des fins répressives**93**.

45Pour créer cet écosystème de confiance, la proposition s'articule en douze titres et neuf annexes. Elle a vocation à s'appliquer à un nombre conséquent de SIA (A), dont la mise en œuvre engendre le respect d'obligations multiples (B).

## A. Un champ d'application large

46Telle qu'elle apparaît aujourd'hui, la proposition de règlement renvoie à une acception large de la notion de SIA (1), et tend à s'appliquer au-delà des frontières de l'Union (2) ainsi qu'à des acteurs nombreux et divers (3).

### 1. L'application de la proposition sous l'angle matériel

47Le cœur de la proposition a pour objet d'établir des règles portant sur la mise sur le marché, la mise en service et l'utilisation de SIA. Le SIA est compris de façon très large. Il s'agit d'un logiciel répondant à trois conditions. Premièrement, un SIA est développé au moyen de certaines techniques, parmi lesquelles l'apprentissage automatique (ou *machine learning*) est inclus, mais aussi les approches fondées sur la logique, les connaissances, les statistiques, l'estimation bayésienne et les méthodes de recherche et d'optimisation. Deuxièmement, le SIA a pour objectif de produire des résultats tels que des contenus, des prédictions, des recommandations ou des décisions influençant les environnements avec lesquels il interagit. Troisièmement, il produit ces résultats sur la base d'un ensemble d'objectifs définis par l'homme.

48La proposition opère une gradation des SIA en fonction du risque qu'ils présentent. Certaines pratiques en matière d'intelligence artificielle sont purement et simplement interdites, quand d'autres sont autorisées librement ou sous réserve de respecter des obligations diverses, notamment en termes de transparence. Dans le premier cas, le risque est considéré comme inacceptable, ce qui justifie l'interdiction. Sont ici visés certains SIA qui ont pour effet d'altérer substantiellement le comportement d'un utilisateur et qui peuvent lui porter préjudice, les SIA exploités par ou pour les pouvoirs publics pour classer les personnes en fonction d'une note sociale, ainsi que les SIA exploités à distance en temps réel dans des espaces accessibles au public pour procéder à une identification biométrique à des fins répressives. À chaque fois, la catégorie des SIA considérée est réduite par l'accumulation de conditions à remplir. Pour cette raison, les cas dans lesquels une interdiction de recourir à une technique d'intelligence artificielle est posée se révèlent limités**94**.

49Quand le risque est considéré comme acceptable, la proposition organise le cadre juridique à respecter en différenciant les SIA à haut risque de certains SIA spécifiquement visés. Les premiers font l'objet d'une attention particulière. La classification d'un SIA comme étant à haut risque repose sur la finalité du système et sur les modalités spécifiques pour lesquelles il est utilisé. Un SIA doit être considéré à haut risque quand il constitue un composant de sécurité d'un produit tel qu'un jouet, un ascenseur, un dispositif médical.., ou quand il est le produit lui-même. Ce sera également le cas quand le produit dont le composant de sécurité est le SIA ou quand le SIA lui-même est soumis à une évaluation avant une mise sur le marché. Enfin, le texte renvoie à une annexe pour fixer une liste de SIA à haut risque que la Commission européenne pourra faire évoluer à l'avenir. La lecture de cette annexe laisse apparaître une liste assez longue pointant différents secteurs tels que l'éducation et la formation professionnelle, l'emploi, l'activité des autorités répressives, la gestion de la migration ou encore l'administration de la justice. On y trouve aussi les SIA destinés à être utilisés pour l'identification biométrique à distance, en temps réel et *a posteriori*, des personnes physiques. Ce faisant, la proposition de règlement admet le recours à la reconnaissance faciale au moment où le Conseil de l'Europe exprime ses inquiétudes à son sujet. Pour ce dernier, « dans les environnements non contrôlés, le recours aux technologies de reconnaissance faciale à la volée devrait être soumis à un débat démocratique comprenant la possibilité d'un moratoire en

attendant une analyse complète du fait de leur nature intrusive pour la vie privée et la dignité des personnes, ajoutée à un risque d'impact préjudiciable sur d'autres droits de l'homme et libertés fondamentales »**95**.

50La proposition ne s'applique en revanche pas aux SIA développés ou utilisés à des fins militaires.

## 2. L'application de la proposition sous l'angle territorial

51L'article 2 de la proposition délimite le champ d'application territorial des dispositions prévues. Le texte s'applique quand les fournisseurs mettent sur le marché ou mettent en service des SIA dans l'Union, quel que soit le lieu de leur établissement. La proposition trouve également à jouer quand les utilisateurs des SIA sont situés dans l'Union, mais aussi quand les résultats produits par le SIA sont utilisés dans l'Union. Trois critères alternatifs ressortent ainsi de l'article 2 : la mise sur le marché ou en service du système, le lieu de situation des utilisateurs du système et le lieu d'utilisation des résultats du système. La proposition a donc vocation à s'appliquer largement, y compris à l'extérieur des frontières de l'Union européenne. Une exclusion est toutefois visée par le texte, qui ne s'appliquera pas aux autorités publiques d'un pays tiers, ni aux organisations internationales utilisant des SIA dans le cadre d'accords internationaux de coopération des services répressifs et judiciaires avec l'Union ou avec un ou plusieurs États membres. Le Comité européen de la protection des données et le Contrôleur européen de protection des données se sont dits très préoccupés par cette exclusion, jugeant qu'elle créait un risque significatif de contournement (par exemple, les pays tiers ou les organisations internationales exploitant des applications à haut risque sur lesquelles s'appuient les autorités publiques dans l'UE)**96**.

## 3. Application à des acteurs nombreux et divers

52Certains acteurs sont directement concernés par les obligations issues de la proposition (a), quand d'autres ont pour mission de veiller à l'application de ces obligations (b).

### a. Les acteurs concernés par la mise en œuvre du texte

53Sous le terme d'« opérateur », la Commission renvoie à divers acteurs que sont le fournisseur, l'utilisateur, le mandataire, l'importateur et le distributeur du SIA. Le fournisseur est l'acteur clé de la proposition, car c'est sur lui que reposent la plupart des obligations inhérentes au dispositif de protection pensé dans le texte. Il s'agit d'« une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui développe ou fait développer un système d'IA en vue de le mettre sur le marché ou de le mettre en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit ». Quand il n'est pas établi dans l'Union, le SIA peut être mis sur le marché ou en service par un importateur. Ce dernier est défini comme la personne physique ou morale qui met sur le marché ou en service un SIA qui porte le nom ou la marque d'un fournisseur établi hors de l'Union. L'importateur ou le fournisseur lui-même peut faire appel à un distributeur dont la mission est de mettre un SIA à disposition sur le marché de l'Union, sans altérer ses propriétés, de façon à ce que le système puisse être utilisé dans le cadre d'une activité commerciale, à titre onéreux ou gratuit. Enfin, en l'absence d'importateur identifiable, le fournisseur qui n'est pas établi dans l'Union européenne

doit recourir à un mandataire pour que ce dernier s'acquitte en son nom et pour son compte des obligations et des procédures lui incombant en vertu du règlement à venir. Une fois mis sur le marché, le SIA a vocation à devenir un outil aux mains d'un utilisateur, c'est-à-dire de « toute personne physique ou morale, autorité publique, agence ou autre organisme qui utilise un système d'IA sous son autorité » et à titre professionnel.

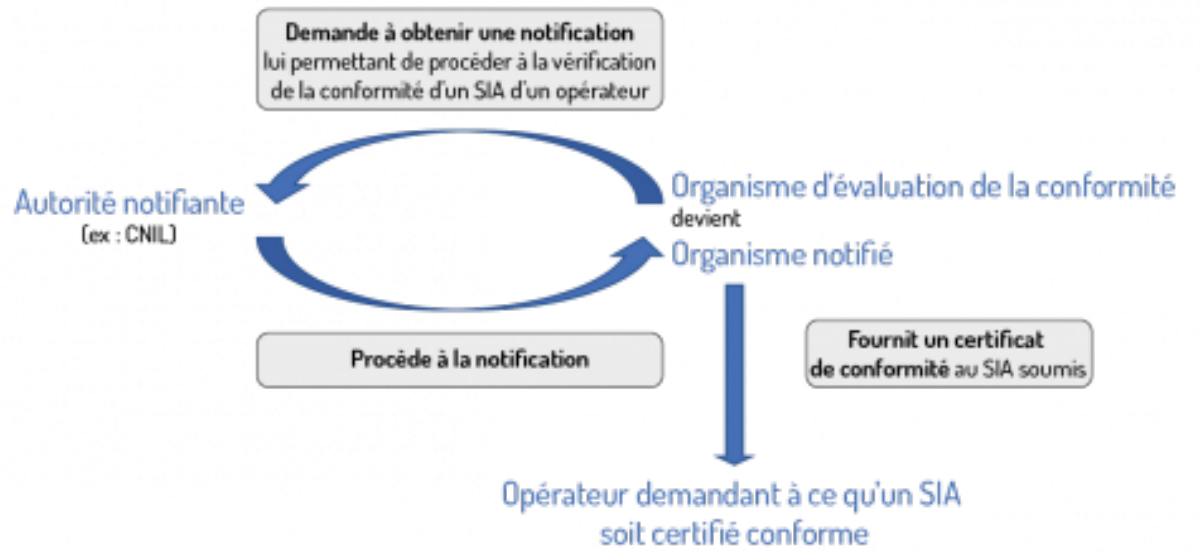
54On le voit, la proposition prend en compte l'ensemble des acteurs impliqués dans la chaîne de valeur du SIA. Le fournisseur du système à haut risque est le principal responsable (art. 16 et s. de la proposition), mais des obligations similaires sont prévues pour le fabricant de produits de sécurité (énumérés à l'annexe II, section A) auquel est appliqué un SIA à haut risque (art. 24). Également le distributeur, l'importateur, l'utilisateur ou un autre tiers doivent être considérés comme fournisseurs et sont soumis aux obligations inhérentes à ce statut quand ils mettent sur le marché ou en service un SIA à haut risque sous leur propre nom ou leur propre marque, s'ils modifient la destination d'un SIA à haut risque déjà mis sur le marché ou mis en service ou s'ils apportent une modification substantielle au SIA à haut risque (art. 28). L'importateur et le distributeur doivent en outre procéder à des vérifications avant toute mise sur le marché du SIA de façon à s'assurer que ce dernier est conforme aux exigences requises en matière de SIA à haut risque. Ils peuvent être amenés à communiquer des informations et documents démontrant cette conformité aux autorités nationales compétentes et doivent coopérer avec elles à toutes mesures qu'elles auraient prises relativement au système (art. 26 et 27). Le distributeur peut avoir à prendre des mesures correctives ou à vérifier que ces mesures ont été prises par le fournisseur, l'importateur ou tout autre opérateur concerné. L'utilisateur, quant à lui, doit utiliser le SIA conformément aux instructions fournies. Il s'assure de la pertinence des données d'entrée, surveille le fonctionnement du système et peut aller jusqu'à suspendre l'utilisation du système en cas de risques déraisonnables ou inacceptables pour la santé, la sécurité ou la protection des droits fondamentaux des personnes ou en cas d'incident grave ou de dysfonctionnement du système. Il gère la tenue des journaux générés par le SIA qui sont sous son contrôle (art. 29). Enfin, les mandataires demeurent tenus, conformément au mandat écrit les liant aux fournisseurs et qui les habilite à répondre aux demandes d'une autorité nationale compétente concernant le SIA, à tenir à la disposition de celle-ci une copie de la déclaration de conformité UE et de la documentation technique et à coopérer avec elle le cas échéant (art. 25).

### b. Les acteurs veillant à l'application du texte

55La proposition de règlement s'intéresse tour à tour à plusieurs autorités et organismes chargés de veiller à sa bonne application.

56Il s'agit d'abord de l'autorité notifiante. Chaque État membre doit en désigner une, sachant que celle-ci a pour mission principale de mettre en place et d'accomplir les procédures nécessaires à l'évaluation, à la désignation et à la notification des organismes d'évaluation de la conformité et à leur contrôle (art. 30). Concrètement, l'autorité notifiante agit comme une autorité d'accréditation d'un organisme chargé de vérifier qu'un SIA soumis par un fournisseur est conforme. Simplement l'accréditation prend ici le nom de notification. Pour que ce dispositif fonctionne, il faut au préalable qu'un organisme d'évaluation de la conformité soumette une demande de notification à l'autorité notifiante de l'État dans lequel il est établi. Si cette demande aboutit favorablement, l'organisme devient un organisme notifié dont l'activité est soumise au contrôle de l'autorité notifiante. Il obtient à ce titre un numéro d'identification, et une publicité est organisée par la Commission européenne. Le rôle de l'organisme notifié est

de vérifier la conformité du SIA à haut risque aux règles établies par la proposition et de délivrer des certificats de conformité le cas échéant.




Agrandir Original (png, 49k)

57L'organisme notifié peut avoir recours à une filiale ou à un sous-traitant, auquel cas il en informe l'autorité notifiante, et doit obtenir l'accord du fournisseur concerné. Il veille à ce que la filiale ou le sous-traitant présente les qualités requises et dispose des ressources nécessitées par la tâche à accomplir. Point important, il assume l'entière responsabilité des tâches qu'elle ou il a effectuées. La notification peut être restreinte, suspendue ou même retirée en cas de manquement de l'organisme notifié par l'autorité notifiante, qui en informe la Commission européenne. Celle-ci peut également diligenter une enquête visant à s'assurer que l'organisme notifié respecte les exigences posées en termes d'indépendance, de ressources propres, d'expertise.

58Au-delà de sa mission de notification, l'autorité notifiante joue un rôle important en qualité d'autorité de contrôle nationale. Selon le texte de la proposition, l'autorité de contrôle nationale est choisie parmi les autorités nationales compétentes qui sont désignées par chaque État membre pour assurer la mise en œuvre du règlement établissant les règles harmonisées en matière d'IA (art. 59). En pratique, chaque État membre désignera plusieurs autorités nationales compétentes, de façon très probablement à ce que ces autorités couvrent un éventail de secteurs suffisamment large pour répondre à la variété des SIA et des risques possibles. Ces autorités devront présenter des qualités d'impartialité et d'objectivité et devront bénéficier de ressources financières et humaines suffisantes eu égard aux missions qui leur sont confiées. Ce dernier point devrait d'ailleurs faire l'objet d'une surveillance de la part de la Commission européenne, aidée du Comité européen de l'intelligence artificielle. Elles devront créer des bacs à sable de façon à proposer un environnement contrôlé facilitant le développement, la mise à l'essai et la validation des SIA innovants avant leur mise sur le marché ou mise en service**97**.

59Enfin, l'autorité notifiante agit également en principe en tant qu'autorité de surveillance du marché (art. 59 2). À ce titre, elle communique régulièrement à la Commission les résultats des activités de surveillance du marché pertinentes. Si une information est susceptible de présenter un intérêt en matière de droit de la concurrence, elle la communique à la Commission, mais

aussi aux autorités nationales de la concurrence concernées (art. 63). Pour mener à bien sa mission, elle est autorisée à accéder aux jeux de données d'entraînement, de validation et de test utilisés par le fournisseur, et peut même accéder au code source du SIA dans certains cas. Elle est informée dès lors qu'une autorité ou un organisme public national, dont la mission est de protéger les droits fondamentaux, demande à accéder à toute documentation en lien avec un SIA présentant un haut risque (annexe III). Sur demande motivée de cette autorité ou de cet organisme public national, elle peut aussi organiser des tests du SIA en vue d'établir une violation aux obligations en lien avec la préservation des droits fondamentaux (art. 64). Pour certains SIA présentant des risques spécifiques, elle a la pouvoir de procéder à une évaluation du système, et peut demander à ce que des mesures correctives soient adoptées, à défaut de quoi elle peut prendre des mesures provisoires visant à interdire ou restreindre la mise à disposition du SIA sur son marché national, pour le retirer du marché ou pour le rappeler (art. 65). Ces mesures provisoires peuvent faire l'objet d'une objection de l'autorité de surveillance du marché d'un autre État membre qui estime que les mesures prises ne sont pas justifiées. Ce mécanisme fait penser à bien des égards à celui mis en place par le Règlement général sur la protection des données (RGPD), qui permet à une autorité de contrôle de soulever une objection pertinente et motivée quand elle estime que la décision projetée par l'autorité de contrôle d'un autre État membre (autorité chef de file) est critiquable**98**.

60Au final, les multiples rôles assumés par l'autorité notifiante font d'elle un organe central du dispositif mis en place par la proposition de règlement. Plusieurs indices laissent penser que la Commission nationale de l'informatique et des libertés (CNIL) pourrait devenir l'autorité notifiante française. Parmi ceux-ci, on peut citer le fait que le Contrôleur européen de la protection des données soit expressément désigné par le texte pour assumer ce rôle au niveau des organes, agences et institutions de l'Union européenne (art. 59 8. et 63 6.), alors qu'il a été institué pour veiller à la conformité des traitements de données à caractère personnel effectués par les institutions et organes de l'Union**99**. Également, l'article 63.5 fait référence aux autorités de contrôle nationales chargées de veiller au respect du RGPD pour en faire les autorités de surveillance du marché pour les SIA destinés à être utilisés pour l'identification biométrique à des fins répressives à distance en temps réel et *a posteriori* des personnes physiques, ou pour certains SIA mis en œuvre pas les autorités répressives ou dont la finalité est la gestion de la migration, de l'asile et des contrôles aux frontières**100**. D'autres autorités pourraient néanmoins être plus pertinentes si bien qu'il faut rester vigilant sur les choix qui seront opérés à l'avenir.

61La proposition de règlement crée par ailleurs le Comité européen de l'intelligence artificielle, composé de représentants des autorités de contrôle nationales et présidé par la Commission européenne. Ce nouvel organe n'est pas sans rappeler le Comité européen de la protection des données institué par le RGPD ou le Comité européen des services numériques prévu dans le projet de *Digital Services Act* pour assurer la surveillance des fournisseurs de services intermédiaires**101**. *A priori*, ce Comité aurait un rôle purement consultatif**102**, donc non contraignant. Il lui appartiendra de fournir des conseils et une assistance à la Commission européenne, en recueillant l'expertise et les bonnes pratiques, en contribuant à l'harmonisation des pratiques administratives dans les États membres, en formulant des avis, des recommandations ou des contributions écrites sur des questions liées à la mise en œuvre du règlement. Il devra contribuer à la mise en place d'une coopération efficace des autorités de contrôle nationales et de la Commission, et aider les premières à assurer une application cohérente du règlement (art. 56 et 58).

## B. La mise en œuvre du SIA

62En application de la proposition de règlement, la mise en œuvre d'un SIA implique de respecter des obligations dont le nombre varie en fonction du risque que le SIA présente (1) et qui peuvent donner lieu à des sanctions importantes (2).

## 1. Les obligations du fournisseur de SIA

63Une partie conséquente de la proposition de règlement est consacrée aux obligations à respecter en présence d'un SIA à haut risque (a) quand une obligation de transparence est prévue pour certains systèmes d'IA (b).

### a. Les obligations en présence d'un SIA à haut risque

64Les obligations à respecter en présence d'un SIA à haut risque ressortent principalement des chapitres 2 et 3 du titre 3 de la proposition de règlement. Si le chapitre 3 explicite l'acteur sur lequel repose chaque obligation qu'il liste, tel n'est pas le cas du chapitre 2, qui édicte les exigences applicables aux SIA à haut risque sans préciser qui doit les mettre en œuvre. Le fournisseur semble néanmoins particulièrement concerné par ces obligations, l'article 16 prenant soin de préciser que le fournisseur doit veiller à ce que le SIA à haut risque soit conforme aux exigences énoncées au chapitre 2, alors que les autres acteurs doivent simplement être en mesure de prouver que le SIA est conforme à ces exigences**103** et que les conditions de son stockage et de son transport ne compromettent pas sa conformité à ces exigences**104**. Le distributeur est en outre soumis à l'obligation de prendre des mesures correctives s'il estime qu'un SIA à haut risque qu'il a mis sur le marché n'est pas conforme aux dispositions du chapitre 2**105**.

65Au sein de ce chapitre, l'article 9 dispose qu'un système de gestion des risques doit être mis en œuvre, documenté et tenu à jour. Ce système « consiste en un processus itératif continu qui se déroule sur l'ensemble du cycle de vie d'un système d'IA à haut risque et qui doit périodiquement faire l'objet d'une mise à jour méthodique ». Il prend en considération l'ensemble des risques connus ou prévisibles, mais aussi des estimations et évaluations de risques susceptibles d'apparaître, ainsi que les mesures appropriées prises. Il implique de mettre en œuvre des procédures de test tout au long du cycle de vie du système et, en tout état de cause, avant la mise sur le marché ou la mise en service (art. 9 7). Les données utilisées pour entraîner, valider ou tester le SIA font l'objet d'une attention particulière (art. 10). La proposition de règlement établit une liste de caractéristiques que les jeux de données doivent présenter, mais les moyens pour parvenir à les atteindre sont souvent passés sous silence. On a l'impression d'un idéal à atteindre, manquant parfois de pragmatisme. Les données doivent être adéquates, pertinentes, représentatives, exemptes d'erreurs. Les jeux de données doivent être complets, posséder les propriétés statistiques appropriées et prendre en compte les caractéristiques du contexte géographique, comportemental ou fonctionnel dans lequel le SIA est destiné à être utilisé. Ces jeux doivent en outre pouvoir faire l'objet d'un examen de façon à limiter le risque de biais et à détecter les lacunes et déficiences dont les données pourraient être affectées. Dans le but de lutter contre les biais, le règlement autorise le fournisseur du système à traiter des données sensibles au sens du RGPD, sous réserve de prendre les garanties appropriées telles qu'une procédure d'anonymisation des données.

66Le texte prévoit encore l'obligation d'établir une documentation technique avant toute mise sur le marché ou mise en service, qui devra être tenue à jour (art. 11). Il impose d'enregistrer

les journaux générés automatiquement tout au long de la vie du système (art. 12 et 20) de façon à pouvoir surveiller une adaptation de son fonctionnement à sa destination, et édicte une obligation de transparence avec l'obligation de fournir une notice d'utilisation aux utilisateurs du SIA, ces derniers devant être en capacité d'interpréter les résultats du système et de l'utiliser de manière appropriée (art. 13). De façon prévisible**106**, le texte dispose qu'un contrôle humain effectif du SIA doit au surplus être possible pendant la période d'utilisation du système afin de prévenir ou réduire les risques pour la santé, la sécurité ou les droits fondamentaux qui pourraient apparaître (art. 14). Enfin, le SIA doit présenter certaines qualités. Il doit être suffisamment sécurisé pour résister aux tentatives de tiers non autorisés, robuste, mais également atteindre un niveau approprié d'exactitude (art. 15).

67Le chapitre 3 de la proposition de règlement est consacré aux « obligations incombant aux fournisseurs et autres utilisateurs de système d'IA à haut risque et à d'autres parties ». Les termes utilisés sont si larges qu'il est possible d'en déduire que tous les acteurs sont ici concernés. Aussi la dichotomie opérée entre les exigences posées au chapitre 2 et celles posées aux chapitre 3 interroge. Certes le chapitre 2 insiste sur les exigences applicables aux SIA à haut risque, et non pas sur les obligations auxquelles sont soumis les acteurs de la chaîne, mais, en substance, ce chapitre expose bien des obligations incombant à ces différents acteurs. On peut d'ailleurs noter que plusieurs dispositions du chapitre 3 renvoient aux exigences prescrites dans le chapitre 2. En ce sens, le fournisseur est contraint d'établir un document technique (art. 16 c) et art. 18) et de tenir et conserver les journaux générés automatiquement par le système d'IA qui est sous son contrôle (art. 16 d) et art. 20). Il doit veiller à la conformité du SIA aux exigences du chapitre 2, prendre les mesures correctives qui s'imposent (art. 16 g) et 21) et être en mesure d'apporter la preuve de la conformité à toute autorité nationale compétente qui en fait la demande (art. 16 a) et j) et art. 23).

68Au-delà de la reprise des dispositions du chapitre 2, le chapitre 3 prescrit de nombreuses obligations au fournisseur d'un SIA à haut risque. Il lui appartient de mettre en place un système de gestion de la qualité (art. 16 b) et art. 17) et de veiller à ce que le SIA soit soumis à la procédure d'évaluation de la conformité avant sa mise sur le marché ou en service (art. 16 e) et 19). Si le SIA est considéré conforme aux exigences du chapitre 2, le fournisseur doit établir une déclaration UE de conformité (art. 19 et art. 48) et apposer le marquage « CE » sur le SIA (art. 16 i), art. 19 et art. 49). Il procède à l'enregistrement du SIA dans la base de données de l'UE pour les systèmes d'IA à haut risque autonomes (art. 16 f), art. 51 et art. 60). Le fournisseur est encore tenu d'informer les autorités nationales compétentes concernées et l'organisme notifié qui a délivré un certificat pour le SIA le cas échéant, de la non-conformité du SIA et de toute mesure corrective qu'il a prise (art. 16 h) et art. 22).

69La suite de la proposition de règlement (titre VIII) s'intéresse aux obligations qui s'imposent postérieurement à la commercialisation du SIA et que l'on qualifie d'obligations *ex post*. À ce moment, l'article 61 impose aux fournisseurs d'établir et de documenter un système de surveillance reposant sur un plan de surveillance inclus dans la documentation technique. Le système a pour but de permettre au fournisseur d'évaluer le SIA et de déterminer s'il continue à respecter les exigences posées au chapitre 2, même après sa commercialisation. Pour ce faire, le système consiste à collecter, documenter et analyser, « de manière active et systématique, les données fournies par les utilisateurs ou collectées *via* d'autres sources sur les performances » du SIA tout au long de son cycle de vie. En dernier lieu, l'article 62 prévoit l'obligation pour le fournisseur de notifier tout incident grave ou tout dysfonctionnement d'un SIA à haut risque qui porterait atteinte à des droits fondamentaux protégés par le droit de l'UE, aux autorités de surveillance du marché des États membres où a eu lieu l'incident ou la violation au droit de l'Union. Le texte indique que la notification doit être immédiate, tout en précisant un délai

maximum de 15 jours à compter de la connaissance de l'incident ou du dysfonctionnement pour y procéder. De nouveau, ce système de notification fait écho à celui mis en place dans d'autres textes de l'Union, que l'on pense au RGPD**107** ou à la directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union**108**.

### b. L'obligation de transparence pour certains SIA

70L'article 52 de la proposition vise plusieurs types de systèmes. On y trouve ceux qui sont destinés à interagir avec des personnes physiques telles que les *chatbots*. Dans ce cas, les utilisateurs doivent savoir qu'ils sont en relation avec une machine afin de pouvoir décider en connaissance de cause de poursuivre ou non. L'article 52 renvoie aussi à des SIA présentant des risques en termes de manipulation, qu'il s'agisse de ceux de systèmes de reconnaissance des émotions, de catégorisation biométrique ou de génération et/ou manipulation « d'images ou de contenus audio ou vidéo présentant une ressemblance avec des personnes, des objets, des lieux ou d'autres entités ou événements existants et pouvant être perçus à tort comme authentiques ou véridiques ». Concernant ces systèmes, l'utilisateur doit être informé du fonctionnement et, le cas échéant, du fait que les contenus ont été générés ou manipulés artificiellement. Il s'agit ici de lutter contre la désinformation, avec les difficultés posées par les *deepfakes*.

71Pour les SIA présentant un risque minime pour les droits et la sécurité des personnes, une utilisation libre est prévue. La Commission souligne que cette catégorie concerne la grande majorité des SIA. Sont notamment visés les systèmes utilisés dans le cadre des jeux vidéo ou des filtres anti-spams.

## 2. Les sanctions

72En vertu de l'article 71 de la proposition, les sanctions applicables doivent être « effectives, proportionnées et dissuasives ». Elles s'inscrivent dans un contexte économique avec le fait qu'elles doivent tenir compte des intérêts des petits fournisseurs et des jeunes entreprises ainsi que de leur viabilité économique. La Commission européenne n'hésite pourtant pas à prévoir des amendes administratives élevées, échelonnées selon trois seuils en fonction des violations commises. Elle propose ainsi une amende pouvant aller jusqu'à 30 millions d'euros ou 6 % du chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent si des SIA interdits car présentant des risques inacceptables sont mis en œuvre, ou si les règles en matière de qualité et de gouvernance des données ne sont pas respectées. Pour toutes les autres infractions, à l'exception de celles liées à la fourniture d'une information inexacte, incomplète ou trompeuse aux organismes notifiés ou aux autorités nationales compétentes, on retrouve**109** la sanction de 20 millions d'euros et 4 % du chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent.

73Bilan : En proposant ce cadre transversal contraignant, l'Union européenne est, une nouvelle fois, précurseur en matière de régulation des aspects de nos vies liés à la technologie numérique. Cette position lui permet de servir de modèle et d'influencer les régimes adoptés au-delà de ses frontières. Ce faisant, elle joue un rôle fondamental pour véhiculer les valeurs qu'elle porte et la volonté de mettre en œuvre une IA centrée sur l'humain, durable, sûre, inclusive et digne de confiance. En cela le dynamisme régulatoire dont fait preuve l'Union doit être salué et

encouragé. Le travail à fournir pour parvenir à un texte définitif, validé par le Parlement et le Conseil, est encore grand, et certains points de la proposition nécessiteront d'être précisés. Il n'est pas certain non plus que la proposition soit parvenue à la souplesse qu'elle visait. Un œil attentif doit donc être gardé sur ce texte qui, à n'en point douter, constitue un texte « historique »**110**.

## III. Vers un cadre clarifié applicable au traitement de données personnelles dans un contexte transfrontalier

74Les actualités récentes apportent des précisions sur les moyens auxquels il est possible de recourir pour transférer des données hors de l'Union. (A). Elles fournissent également un éclairage sur le fonctionnement des mécanismes de coopération mis en œuvre au niveau de l'Union européenne par le RGPD (B).

### A. Les données personnelles, des données à confiner dans l'Union ?

75Le 6 octobre 2015**111**, la Cour de justice de l'Union européenne invalidait la décision de la Commission européenne ayant reconnu comme adéquate la protection des données personnelles assurée dans le cadre des principes du *Safe Harbor* ou « sphère de sécurité »**112**. Pour rappel, ces principes permettaient aux entreprises américaines qui y avaient adhéré de pouvoir traiter des données personnelles provenant de l'Union européenne. À la suite de la décision de la Cour, une période transitoire s'était ouverte au cours de laquelle la Commission européenne avait négocié un nouvel accord avec les États-Unis, et les responsables de traitements avaient adopté de nouveaux outils à même de donner un fondement légal aux flux de données outre-Atlantique, notamment des clauses contractuelles types. Le 12 juillet 2016, le *Privacy Shield* ou « bouclier de protection » était reconnu comme adéquat par la Commission européenne. De nouveau, il était possible de transférer des données vers les États-Unis sur le fondement de cette décision d'adéquation**113**. Cette possibilité fut néanmoins de courte durée.

76Dans la continuité de l'affaire qui l'avait amenée à se prononcer le 6 octobre 2015, la Cour de justice a dû évaluer la validité de la décision d'adéquation relative au *Privacy Shield*, ainsi que celle de la décision relative aux clauses contractuelles types pour le transfert de données personnelles vers des sous-traitants établis dans des pays tiers**114**. Dans un arrêt notoire du 16 juillet 2020 (affaire C311/18, *Schrems II*), elle a invalidé la première et a reconnu la validité de la seconde sous d'importantes conditions**115**. Le transfert de données vers les États-Unis s'apparentait alors à un casse-tête. Des précisions étaient attendues de la part des divers organes concernés pour accompagner les responsables de traitement à mettre en œuvre des flux de données hors de l'Union légaux. Ces précisions ont été apportées dans plusieurs documents : une décision d'exécution de la Commission européenne du 4 juin 2021**116** (1), des recommandations du Comité européen de la protection des données du 18 juin 2021**117** (2), ainsi que deux décisions reconnaissant l'adéquation du niveau de protection des données personnelles assuré par le Royaume-Uni**118**. (3).

#### 1. L'adoption de clauses contractuelles types plus contraignantes119

77À la suite de l'adoption du RGPD et de l'arrêt *Schrems II* de la Cour de justice en date du 16 juillet 2020, un réexamen des clauses contractuelles types permettant le transfert de données hors de l'Union était devenu nécessaire. La Commission a répondu à cette nécessité en publiant de nouvelles clauses, lesquelles devront s'appliquer obligatoirement après une durée de 18 mois. Ces clauses présentent les spécificités principales suivantes.

78Premièrement, la Commission abandonne la dichotomie de textes opérée sur le fondement de la qualité des acteurs pour adopter un seul texte, incluant les divers cas de transferts possibles. En ce sens, la décision d'exécution est dite « modulaire », car elle précise les clauses respectivement applicables aux quatre types de transferts envisageables : 1) le transfert de responsable du traitement à responsable du traitement, 2) celui de responsable du traitement à sous-traitant, 3) celui de sous-traitant à sous-traitant et 4) celui de sous-traitant à responsable du traitement.

79La frontière entre ces divers acteurs ne s'est pas toujours révélée évidente à tracer en pratique. Pour cette raison, le Comité européen de la protection des données (CEPD) a adopté des lignes directrices le 7 juillet 2021 dans lesquelles il revient sur ces notions clés du RGPD**120**. Faisant suite à un premier avis datant de 2010**121** et à trois arrêts de la Cour de justice de l'Union européenne**122**, ces lignes directrices doivent permettre de faciliter l'identification des différents acteurs impliqués dans un traitement de données personnelles de façon à déterminer les obligations et responsabilités de chacun. En ce sens, le CEPD qualifie les notions envisagées de « fonctionnelles ». Il les considère en outre comme des notions « autonomes », dans la mesure où elles doivent être lues à la lumière des textes de l'Union européenne en matière de protection des données à caractère personnel uniquement. Le responsable du traitement est classiquement défini comme celui qui détermine les moyens et les finalités du traitement. Il s'agit donc de la personne qui prend les décisions importantes relativement au traitement. Toutefois, le CEPD note que le sous-traitant peut lui aussi être amené à prendre des décisions relativement au traitement de données qui lui a été délégué. Aussi, pour le CEPD, les décisions relatives à la finalité du traitement sont clairement toujours du ressort du responsable du traitement alors que les moyens peuvent relever du sous-traitant. Il propose de faire une distinction entre les moyens essentiels et ceux non essentiels. Les premiers sont étroitement liés à la finalité et à la portée du traitement, tels que le type de données à caractère personnel qui sont traitées, la durée du traitement, les catégories de destinataires et les catégories de personnes concernées. Ils portent aussi sur la question de savoir si le traitement est licite, nécessaire et proportionné. Ces moyens essentiels sont réservés au responsable du traitement. Les moyens non essentiels concernent, quant à eux, des aspects plus pratiques, tels que le choix d'un type particulier de matériel ou de logiciel, ou les mesures de sécurité adoptées. Ils peuvent relever de l'appréciation du sous-traitant. Ce dernier dispose ainsi d'une marge de manœuvre pour déterminer la manière de servir au mieux les intérêts du responsable du traitement, en choisissant les moyens techniques et organisationnels les plus appropriés. S'il va au-delà des instructions du responsable du traitement et commence à traiter les données pour ses propres finalités, il doit être considéré lui-même comme un responsable du traitement mis en œuvre sur la base desdites données, et sa responsabilité pourra être recherchée à ce titre. Enfin, un mot peut être dit du responsable conjoint. Pour l'identifier, le CEPD recourt au critère de la participation conjointe aux objectifs et aux moyens du traitement. Il indique que « la participation peut prendre la forme d'une décision commune prise par deux ou plusieurs entités ou résulter de décisions convergentes de deux ou plusieurs entités, lorsque ces décisions se complètent et qu'elles sont nécessaires à la réalisation du traitement de telle sorte qu'elles ont un impact tangible sur la détermination des finalités et des moyens du traitement. Un critère important est que le traitement ne serait pas possible sans la participation des deux parties en ce sens que le traitement par chaque partie est inséparable, c'est-à-dire inextricablement lié ».

80Deuxièmement, les nouvelles clauses contractuelles types prévoient qu'il devient possible pour un tiers d'adhérer aux clauses signées, soit en tant qu'exportateur de données soit en tant qu'importateur de données.

81Troisièmement, la Commission apporte aussi et surtout des éclaircissements en réponse à l'arrêt de la Cour de justice du 16 juillet 2020. Cette décision, outre qu'elle a invalidé le *Privacy Shield* ou bouclier de protection, aboutit à soumettre le transfert fondé sur des clauses contractuelles types à la mise en place de mesures supplémentaires dès lors que la législation du pays tiers ne permet pas le respect du niveau de protection requis. Cette difficulté se pose notamment à l'égard des États tiers dont les législations autorisent les autorités publiques à prendre connaissance des données personnelles traitées.

82La Commission crée une section III dans les clauses pour apporter un cadre à cette situation. Il en ressort une charge importante imposée aux acteurs en présence. Ainsi de l'obligation d'opérer une évaluation de la législation du pays tiers en matière de divulgation et d'accès aux données par des autorités publiques afin de garantir que cette législation n'est pas de nature à empêcher l'importateur de données de s'acquitter des obligations qui lui incombent en vertu des clauses contractuelles types conclues. Cette obligation s'accompagne, pour l'importateur des données, de l'obligation d'informer l'exportateur s'il a des raisons de croire qu'il est ou est devenu soumis à une législation ou à des pratiques qui ne sont plus compatibles avec les clauses signées. Des garanties appropriées peuvent alors être prévues. À défaut, le transfert doit être suspendu et le contrat peut être résilié. L'importateur est aussi tenu d'une obligation de notification en cas d'accès ou de demande d'accès juridiquement contraignante par les autorités publiques de l'État vers lequel les données ont été transférées. Il lui appartient enfin de contrôler la légalité de la demande de divulgation, en particulier de vérifier si elle s'inscrit dans les limites des pouvoirs conférés à l'autorité publique requérante, et de la contester si, après une évaluation minutieuse, il conclut qu'il existe des motifs raisonnables de considérer qu'elle est illégale en vertu de la législation du pays de destination, des obligations applicables en vertu du droit international et des principes de courtoisie internationale.

83Ces obligations ne sont pas sans interroger, tant leur mise en œuvre peut paraître complexe pour des acteurs dont le traitement de données personnelles est bien souvent l'accessoire d'une activité relevant de leur cœur de métier. Finalement, on peut se demander si l'effet de ces clauses ne serait pas de maintenir les données dans l'Union.

84Quatrièmement, la Commission donne une liste non exhaustive des mesures techniques et organisationnelles pouvant être mises en œuvre pour garantir la sécurité des données (Annexe II).

## 2. La mise en œuvre de mesures complémentaires

85En vertu du RGPD, les entités peuvent recourir à divers outils quand elles souhaitent transférer des données personnelles à l'extérieur de l'Union. Le plus simple demeure de fonder le flux sur l'existence d'une décision d'adéquation adoptée par la Commission européenne, qui reconnaît que le système étranger assure un niveau de protection adéquat. Cette solution exige donc que la Commission européenne ait rendu une telle décision, ce qui n'est pas le cas pour la majorité des États. En l'absence d'une telle décision, l'entité doit prendre des mesures pour compenser l'insuffisance de la protection des données dans le pays tiers par des garanties appropriées en faveur de la personne concernée. Elle peut alors se tourner vers les outils listés à l'article 46 du RGPD, tels que des clauses contractuelles types, des règles d'entreprise contraignantes (ou *Binding Corporate Rules – BCR*), un code de conduite, ou encore un mécanisme de certification approuvé.

86Dans son arrêt *Schrems II* du 16 juillet 2020, la Cour reconnaît la légalité des clauses contractuelles types, mais met à la charge des responsables et sous-traitants exportateurs de données, en collaboration avec l'importateur, l'obligation de vérifier que la législation ou la pratique du pays tiers n'empiète pas sur l'efficacité des garanties appropriées contenues dans ces clauses, ou, le cas échéant, dans les outils visés à l'article 46 du RGPD. Si la vérification aboutit à l'existence de lacunes dans la protection mise en œuvre, l'exportateur est tenu de prendre les mesures supplémentaires appropriées pour combler ces lacunes. En application du principe d'« *accountability* », c'est à lui d'identifier quelles mesures doivent être prises en fonction du contexte et de conserver une preuve des actions menées, en cas de contrôle.

87Les recommandations du CEPD**123** ont pour objet d'accompagner l'entité exportatrice dans cette démarche. À ce dessein, un processus composé de six étapes est proposé. Dans un premier temps, il appartient au responsable ou au sous-traitant d'identifier les transferts de données mis en œuvre au sein de la structure. Puis, il doit déterminer quel outil est utilisé pour permettre ces transferts (clauses contractuelles, règles d'entreprise contraignantes…). Dans un troisième temps, le CEPD met à sa charge le soin d'évaluer la législation ou pratique étrangère pour apprécier si elle impacte le niveau de protection. De nouveau, on peut s'interroger sur la capacité du responsable ou du sous-traitant à mener à bien cette mission. Le cas échéant, il devra décider de mesures à prendre : soit suspendre le transfert, soit poursuivre le transfert en prenant ou non des mesures complémentaires. Pour procéder à cette évaluation, l'entité exportatrice peut s'aider de la liste des sources d'informations fournie par le CEPD dans l'annexe 3 de ses recommandations. S'il estime que des mesures complémentaires doivent être prises, il lui reviendra d'identifier et d'adopter lesquelles, en s'aidant s'il le souhaite d'une liste indicative de mesures pouvant être prises et des conditions dans lesquelles les mettre en œuvre fournie à l'annexe 2 des recommandations. Le CEPD l'enjoint à prendre toutes les mesures procédurales formelles que l'adoption des mesures complémentaire peut exiger, en fonction de l'outil de transfert de l'article 46 du RGPD sur lequel est appuyé le transfert. En dernier lieu, il est tenu de réévaluer à intervalles appropriés le niveau de protection offert aux données personnelles transférées hors de l'Union européenne.

## 3. Le cas particulier du Royaume-Uni

88Grâce à deux décisions d'adéquation du 28 juin 2021 (C(2021) 4800 final et C(2021) 4801 final), la Commission européenne donne un fondement légal aux transferts de données personnelles vers le Royaume-Uni. Avant cela, les transferts reposaient sur l'accord de commerce et de coopération entre l'Union européenne et le Royaume-Uni qui autorisait la libre circulation des données, mais jusqu'au 30 juin 2021 seulement.

89Dans ces décisions, la Commission européenne relève l'ensemble des éléments qui jouent en faveur de la reconnaissance d'un niveau adéquat de protection assurée par la législation outre-Manche. Elle commence par souligner le fait que le cadre légal applicable est issu des textes européens puisque adopté avant le Brexit, au moment où le Royaume-Uni était encore tenu de mettre en œuvre les textes votés au niveau de l'Union. Ce cadre intègre donc les principes, droits et obligations inhérents au traitement de données personnelles. Ce point est renforcé par le fait que le Royaume-Uni est membre du Conseil de l'Europe, qu'il adhère à la Convention européenne des droits de l'homme et est soumis à ce titre à la compétence de la Cour européenne des droits de l'homme. Concernant l'accès aux données par les pouvoirs publics pour des fins répressives ou de sécurité nationale, elle observe l'existence de garanties suffisantes, avec notamment l'intervention d'un organe judiciaire indépendant pour autoriser la collecte et l'existence d'un recours effectif pour les personnes concernées.

90En revanche, la Commission européenne exclut de ces décisions les données transférées au Royaume-Uni à des fins de contrôle de l'immigration ou qui relèvent du champ d'application de l'exemption de certains droits des personnes concernées aux fins du maintien d'un contrôle efficace de l'immigration conformément au paragraphe 4, point 1, de l'annexe 2 de la loi britannique sur la protection des données (art. 1er 2.). Cette exclusion trouve son origine dans une décision de la cour d'appel d'Angleterre et du Pays de Galles du 21 juin 2021 dans laquelle la cour d'appel a jugé que « l'exemption en matière d'immigration est, dans sa forme actuelle, incompatible avec le droit britannique, étant donné que la mesure législative ne contient pas de dispositions spécifiques énonçant les garanties énumérées à l'article 23, paragraphe 2, du règlement général sur la protection des données du Royaume-Uni (RGPD britannique) » (point 6). L'opportunité de l'exclusion du traitement des données personnelles en lien avec l'immigration pourra être réévaluée quand cette situation d'incompatibilité aura été traitée.

91En définitive, ces décisions d'adéquation sont les bienvenues. Elles sont source de facilité dans un contexte de transferts de données personnelles hors de l'Union européenne qui se complexifie pour les responsables et les sous-traitants. Il faut toutefois noter que ces décisions d'adéquation sont temporaires puisqu'elles contiennent une clause dite de « suppression automatique ». Par ce mécanisme, la Commission européenne a souhaité que les décisions prises viennent automatiquement à expiration au terme d'un délai de quatre ans. À ce moment, le cadre juridique britannique devra faire l'objet d'une nouvelle réévaluation et, le cas échéant, du renouvellement des décisions d'adéquation. Pendant ce laps de temps, la Commission indique qu'elle gardera un œil sur l'évolution de ce cadre afin de pouvoir intervenir si le niveau de protection assuré venait à ne plus être adéquat. En sa qualité d'acteur avisé à la suite de l'invalidation du *Privacy Shield* par la Cour de justice de l'Union européenne, la Commission pense ici notamment au cas dans lequel un accord serait signé entre le Royaume-Uni et les États-Unis, permettant un transfert de données outre-Atlantique.

## B. Les données personnelles, des données protégées à travers le mécanisme de la cohérence

92Dans un arrêt du 15 juin 2021, la Cour de justice de l'Union européenne est revenue sur le mécanisme de la cohérence instauré par le RGPD. Ce dispositif a pour but de permettre une coopération entre les autorités de contrôle de plusieurs États membres concernées par une même affaire, et ainsi d'assurer une application cohérente du RGPD. Dans son arrêt, la Cour admet la possibilité, pour une autorité de contrôle qui n'est pas l'autorité chef de file, d'agir devant un tribunal national**124** (1). Ce faisant, l'autorité chef de file voit sa compétence contournée. À l'inverse, dans une autre affaire, le CEPD conforte la place de l'autorité chef de file en refusant d'exiger que les mesures prises par une autorité nationale qui n'est pas chef de file deviennent définitives et en exigeant de l'autorité chef de file qu'elle diligente une enquête plus approfondie**125** (2).

### 1. La possibilité de contourner l'autorité chef de file en cas d'inaction de sa part

93Dans l'arrêt du 15 juin 2021, la Cour de justice s'est prononcée sur la possibilité pour l'autorité de contrôle belge d'agir à l'encontre de Facebook, pour les collectes d'informations opérées *via* l'utilisation de diverses technologies (cookies, pixels, …) alors même que l'autorité chef de file est l'autorité censée agir en vertu du principe du « guichet unique » est l'autorité irlandaise.

94En effet, en application du RGPD, l'autorité compétente pour agir en cas de traitements de données personnelles impliquant plusieurs États membres est en principe celle du lieu de l'établissement principal du responsable du traitement. Cette autorité prend alors le nom d'autorité chef de file. En l'espèce, Facebook ayant son établissement principal en Irlande, l'autorité compétente pour rendre les décisions à son encontre était l'autorité de contrôle irlandaise. En vertu de l'article 60 du RGPD, le *Data Protection Commissioner* irlandais aurait dû mettre en œuvre des mesures de coopération entre les autorités de contrôle concernées et aurait dû collaborer avec elles pour élaborer un projet de décision, adopter une position et notifier celle-ci au responsable du traitement mis en cause. Sans action de sa part, l'autorité de contrôle belge avait décidé de poursuivre Facebook. Se posait dès lors la question de la capacité de celle-ci à agir contre Facebook Belgium (a) et, le cas échéant, des modalités de cette action (b).

**a. La capacité à agir d'une autorité de contrôle qui n'est pas chef de file**

95Se fondant sur la lettre du RGPD, la Cour de justice rappelle le principe de la compétence de l'autorité chef de file, avant de revenir sur les exceptions qui autorisent une autre autorité de contrôle à agir en justice en cas de violation au texte.

96Ainsi, l'autorité d'un État membre qui n'est pas l'autorité chef de file peut agir si le traitement litigieux concerne uniquement un établissement dans l'État membre dont relève l'autorité de protection ou affecte sensiblement les personnes concernées dans cet État membre uniquement. Dans ce cadre, c'est le caractère territorialisé des violations qui justifie la compétence par dérogation de l'autorité de contrôle de l'État concerné. En l'espèce, il semblait difficile de se fonder sur ce texte pour admettre la compétence de l'autorité belge au regard du type de violations considérées. Aussi, c'est sur le fondement d'une autre dérogation à la compétence de l'autorité chef de file que l'action de l'autorité de contrôle belge a été analysée.

97Aux termes de l'article 66, paragraphe 1, une autorité de contrôle d'un État membre peut, quand l'urgence le requiert, adopter des mesures provisoires, limitées dans le temps et sur le territoire de l'État membre dont elle relève. Il lui appartient ensuite de saisir le Comité européen de la protection des données (CEPD) si elle considère que des mesures définitives doivent être adoptées. Pour qu'une autorité de contrôle autre que celle ayant qualité d'autorité chef de file puisse agir valablement, il faut donc apporter la preuve d'une urgence à agir. Or, en vertu de l'article 61, paragraphe 8, du RGPD, cette urgence est caractérisée dès lors qu'une autorité de contrôle ne fournit pas les informations demandées par une autre autorité de contrôle dans un délai d'un mois à compter de la réception de la demande. Dans ce cas, l'autorité de contrôle requérante peut adopter une mesure provisoire sur le territoire de l'État membre dont elle relève et doit requérir une décision contraignante d'urgence du CEPD. En l'espèce, l'autorité belge avait procédé à une demande d'assistance mutuelle auprès de l'autorité irlandaise, mais cette demande semble n'avoir pas reçu de réponse. Dès lors, il est possible de présager de la solution de la juridiction nationale, qui devrait selon toute vraisemblance conclure à la possibilité d'agir pour l'autorité belge.

**b. Les modalités de l'action engagée par une autorité de contrôle qui n'est pas chef de file**

98La Cour de justice s'attelle à préciser les contours d'une telle action en revenant dans un premier temps sur la compétence territoriale et matérielle d'une autorité de contrôle d'un État membre, avant de déterminer contre qui l'action doit être dirigée.

99Sur le premier point, il faut rappeler que le champ d'application territorial du RGPD repose principalement sur deux critères alternatifs : d'une part, le lieu de l'établissement du responsable du traitement et, d'autre part, le fait que les activités de traitement du responsable sont liées à l'offre de biens ou de services ou au suivi du comportement de personnes situées dans l'Union. En application de ce second critère, le RGPD trouve à s'appliquer quand bien même le responsable n'aurait pas d'établissement dans l'Union. Sur cette base, c'est logiquement que la Cour décide qu'une autorité de contrôle d'un État membre est compétente pour agir sur le fondement du RGPD à l'encontre d'un responsable qui met en œuvre des traitements transfrontaliers concernant l'État dont elle relève sans y avoir d'établissement. Elle ajoute que les violations qu'elle entend faire condamner peuvent avoir été commises avant ou après l'entrée en application du RGPD (point 105). Dans le premier cas, elle se fonde sur la directive du 24 octobre 1995**126** ; dans le second cas, sur le RGPD.

100Quant à savoir contre qui l'action doit être menée, la Cour de justice décide que l'autorité de contrôle d'un État membre qui n'est pas l'autorité chef de file peut diriger son action contre l'établissement principal, mais également contre l'établissement situé dans l'Etat dont elle relève, en l'espèce en Belgique, si l'action vise un traitement effectué dans le cadre des activités de cet établissement. Ici, la Cour fait le lien entre les traitements mis en cause pour lesquels Facebook Ireland est responsable, et les activités d'entretien des relations avec les institutions de l'Union et la promotion des activités publicitaires et de marketing de l'établissement du groupe Facebook situé en Belgique. Pour elle, les deux sont « indissociablement liés » (point 95) si bien que le traitement principal consistant en la collecte d'informations sur le comportement de navigation des internautes au moyen de différentes technologies (cookies, pixels, …) est effectué dans le cadre des activité de l'établissement situé en Belgique. Il en découle que l'autorité de protection belge est recevable à agir contre cet établissement.

101Enfin, la Cour décide qu'en vertu de l'effet direct de l'article 58 paragraphe 5) du RGPD octroyant le pouvoir aux autorités de contrôle des États membres d'agir en justice en cas de violation des règles issues du règlement, une autorité de contrôle nationale peut intenter ou reprendre une action contre des particuliers, même si une telle action n'a pas été prévue dans la législation de l'État membre concerné.

102En conclusion, si la décision de la Cour peut surprendre au premier abord tant elle semble pouvoir conduire à un éparpillement du contentieux et aller à contre-courant de l'homogénéité recherchée dans le RGPD, il semble qu'elle doive à l'inverse être saluée. L'équilibre trouvé entre le principe du « guichet unique » et ses exceptions semble en effet parvenir à répondre aux cas dans lesquels le mécanisme de coopération ne fonctionne pas correctement.

## 2. La possibilité de contraindre l'autorité chef de file à prendre des mesures et diligenter une enquête

103Contrairement au Groupe de l'article 29 qu'il a remplacé, le CEPD a le pouvoir de rendre des décisions contraignantes. C'est par exemple le cas pour les décisions contraignantes d'urgence, quand une autorité de contrôle d'un État membre le saisit afin que des mesures définitives soient prises. Le CEPD a rendu une telle décision pour la première fois le 12 juillet 2021 à propos de mesures prises par l'autorité de contrôle allemande à l'encontre de

la société Facebook afin que celle-ci cesse de traiter pendant trois mois les données personnelles des utilisateurs du service WhatsApp situés en Allemagne. Le CEPD refuse d'ordonner à l'autorité irlandaise chef de file de prendre des mesures définitives (a), mais lui enjoint de diligenter une enquête sur les pratiques mises en place par les sociétés en cause (b).

**a. Le refus de contraindre l'autorité chef de file à prendre des mesures définitives**

104Le contexte de cette affaire est différent de celle tranchée par la Cour de justice qui avait abouti à contourner la compétence de l'autorité chef de file. En effet, en l'espèce, la procédure de coopération prévue par le RGPD a bien été engagée par l'autorité irlandaise, qui a transmis les documents aux différentes autorités de contrôle intéressées et qui a requis leur avis. L'autorité chef de file n'était donc pas défaillante. L'autorité allemande pouvait néanmoins agir et enclencher la procédure d'urgence établie par le RGPD. En vertu de l'article 66 de ce texte, une autorité de contrôle concernée d'un État membre peut déroger au mécanisme de la cohérence et décider d'adopter des mesures provisoires visant à produire des effets juridiques sur son propre territoire et ayant une durée de validité déterminée qui n'excède pas trois mois dès lors qu'il existe des circonstances exceptionnelles et qu'il est urgent d'intervenir pour protéger les droits et libertés des personnes concernées. Ainsi, si elle estime que les mesures provisoires ne sont pas suffisantes et que des mesures définitives doivent être adoptées d'urgence, elle peut demander un avis d'urgence ou une décision contraignante d'urgence au CEPD. C'est précisément ce que l'autorité allemande a fait le 7 juin 2021.

105Pour déterminer si des mesures définitives doivent être adoptées, le CEPD cherche à savoir si les mesures provisoires prises par l'autorité allemande étaient légitimes. Pour ce faire, il essaie de déterminer si des circonstances exceptionnelles existaient au moment où les mesures ont été adoptées. Ses conclusions sur ce point sont plutôt décevantes. En effet, il ne peut que constater qu'il manque de preuve pour pouvoir retenir l'existence de violations au RGPD et, par suite, l'existence de circonstances exceptionnelles justifiant que des mesures provisoires soient prises, en dérogation au mécanisme de la cohérence. Quant à l'urgence qui aurait dû motiver l'adoption des mesures provisoires, le CEPD considère que la démonstration de celle-ci n'est pas faite en l'espèce. Pour lui, l'adoption des conditions d'utilisation actualisées, qui contiennent des éléments problématiques similaires à ceux de la version précédente, ne peut, à elle seule, justifier l'urgence.
C'est donc logiquement qu'il refuse d'ordonner à l'autorité irlandaise chef de file de prendre des mesures définitives. Cela dit, le CEPD décide de demander à l'autorité de contrôle irlandaise de diligenter une enquête.

**b. L'obligation pour l'autorité chef de file de diligenter une enquête**

106Prenant en considération la forte probabilité d'infractions et le manque d'informations sur certaines finalités poursuivies par Facebook, le CEPD décide d'utiliser son pouvoir de contrainte et d'enjoindre à l'autorité de contrôle irlandaise de diligenter une enquête. Celle-ci a principalement pour mission de déterminer si les traitements effectués par Facebook ont pour finalité la sûreté, la sécurité et l'intégrité ainsi que l'amélioration des produits, impliquant la combinaison ou la comparaison des données des utilisateurs du service WhatsApp avec d'autres ensembles de données traitées par d'autres sociétés Facebook dans le cadre d'autres applications ou services offerts par les sociétés Facebook. Au surplus, elle doit vérifier si

Facebook a déjà commencé à traiter les données des utilisateurs du service WhatsApp en tant que responsable conjoint du traitement à ses propres fins de communication marketing et de marketing direct ainsi que de coopération avec les autres sociétés de Facebook. La qualification de responsable conjoint pressentie devra être confirmée. Enfin, l'autorité irlandaise est chargée de contrôler si Facebook a déjà commencé ou commencera bientôt à traiter les données des utilisateurs du service WhatsApp en tant que responsable conjoint pour ses propres besoins en relation avec l'interface WhatsApp Business.

J. E.

**1** Proposition de loi visant à lutter contre l'indépendance fictive en permettant des requalifications en salarié par action de groupe et en contrôlant la place de l'algorithme dans les relations contractuelles, 4 mars 2021, Sénat, n° 426 ; Rapport n° 608. Jean-Luc Fichet, fait au nom de la Commission des affaires sociales, 2021.

**2** Ord. n° 2021-484, 21 avr. 2021 relative aux modalités de représentation des travailleurs indépendants recourant pour leur activité aux plateformes et aux conditions d'exercice de cette représentation.

**3** *Uber BV v Aslam* [2021] UKSC 5, https://www.supremecourt.uk/cases/docs/uksc-2019-0029-judgment.pdf, (dernier accès le 20 juillet 2021).

**4** Cass. soc., 4 mars 2020 (19-13.316).

**5** Commission européenne, *Travailleurs des plateformes numériques : deuxième phase de consultations*,
15 juin 2021, https://ec.europa.eu/france/news/20210615/lancement_deuxieme_phase_consultation_travailleurs_plateformes_fr, (dernier accès le 20 juillet 2021).

**6** Règl. (UE) 2021/887 du PE et du Cons., 20 mai 2021, établissant le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination.

**7** PE, Résol. 2021/2568(RSP), 10 juin 2021, sur la stratégie de cybersécurité de l'Union pour la décennie numérique.

**8** Règl. (UE) n ° 910/2014 du PE et du Cons., 23 juill. 2014, sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, *JOUE L.* 257, 28 août 2014, p. 73-114.

**9** Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Identity (SEC(2021) 228 final) - (SWD(2021) 124 final) - (SWD(2021) 125 final), 3 juin 2021.

**10** Selon ce principe, la personne doit contrôler les éléments de son identité. Sur ce sujet, v. par ex. le document de la Commission européenne intitulé « eIDAS supported self-sovereign identity », mai 2019.

**11** CSNP, avis n° 2021-03, 29 avr. 2021, portant recommandations dans le domaine de la sécurité numérique.

**12** D. n° 2020-151, 20 févr. 2020, portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « application mobile de prise de notes » (GendNotes)

**13** CE, 13 avr. 2021, n° 439360.

**14** L. n° 2021-646, 25 mai 2021, pour une sécurité globale préservant les libertés.

**15** Déc. n° 2021-817 DC, 20 mai 2021.

**16** D. n° 2020-487, 28 avr. 2020, portant création d'un traitement automatisé de données à caractère personnel dénommé « système d'information sur les armes ».

**17** CE, 10e-9e ch. réunies, 27 mai 2021, 441977.

**18** CE, ass., 21 avr. 2021, n° 393099, *French Data Network e.a.*

**19** CE, 26 juill. 2018, nos 394922 394925 397844 397851, Quadrature du Net et autres et Igwan.net, T.

**20** CJUE, 8 avr. 2014, aff. jtes C-293/12 et C-594/1.

**21** CJUE 21 déc. 2016, aff. jtes C-203/15 et C-698/15, *Tele2 Sverige.*

**22** CJUE, 6 octobre 2020, Privacy International, aff. C-623/17 ; La Quadrature du Net e.a., French Data Network e.a., aff. C-511/18 et C-512/18 ; Ordre des barreaux francophones et germanophone e.a., aff. C-520/18. La CJUE reprend son raisonnement dans un arrêt postérieur du 2 mars 2021 H.K./Prokuratuur, aff.C-746/18.

**23** B. Bertrand et J. Sirinelli, « Le Conseil d'État et la conservation des données de connexion : la quadrature du cercle », *Dalloz IP/IT* 2021, p. 408.

**24** CJUE, 17 juin 2021, *Mircom International Content Management & Consulting (M.I.C.M.) Limited c. Telenet BVBA*, aff. C-597/19.

**25** Décision d'exécution (UE) 2021/915 de la Commission, 4 juin 2021, relative aux clauses contractuelles types entre les responsables du traitement et les sous-traitants au titre de l'art. 28,

par. 7, Règl. (UE) 2016/679 du PE et du Cons., et de l'art. 29, par. 7, Règl. (UE) 2018/1725 du PE et du Cons., L. 199/18, *JO* 7 juin 2021.

**26** D. n° 2021-148, 11 févr. 2021 portant modalités de mise en œuvre par la Direction générale des finances publiques et la Direction générale des douanes et droits indirects de traitements informatisés et automatisés permettant la collecte et l'exploitation de données rendues publiques sur les sites internet des opérateurs de plateforme en ligne ; arrêté du 8 mars 2021 modifiant l'arrêté du 21 février 2014 portant création par la direction générale des finances publiques d'un traitement automatisé de lutte contre la fraude dénommé « ciblage de la fraude et valorisation des requêtes ».

**27** V. le dossier législatif sur le site internet de l'Assemblée nationale https://www.assemblee-nationale.fr/dyn/15/dossiers/alt/DLR5L15N40696 (dernier accès le 20 juillet 2021).

**28** CJUE, 22 juin 2021, aff. C-439/19.

**29** Cour de cassation, *Rapport de la Commission de réflexion sur la Cour de cassation 2030*, juill. 2021, p. 76-77.

**30** The Hamburg Commissioner for Data Protection and Freedom of Information, *Order of the HmbBfDI: Ban of further processing of WhatsApp user data by Facebook*, 11 May 2021.

**31** La traduction du projet de loi intitulée Personal Information Protection Law of the People's Republic of China (Draft) (Second Review Draft) est disponible à https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-draft-second-review (dernier accès le 20 juillet 2021). À noter qu'aux États-Unis, l'idée d'une loi fédérale pour la protection des données personnelles fait son chemin : https://siecledigital.fr/2021/05/21/loi-donnees-etats-unis/?utm_source=Newsletter+Si%C3%A8cle+Digital&utm_campaign=26c1dee56b-newsletter+quotidienne&utm_medium=email&utm_term=0_3b73bad11a-26c1dee56b-259702794 (dernier accès le 20 juillet 2021).

**32** Projet de loi autorisant la ratification du Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, n° 4365 , 5 mai 2021.

**33** Décret révoqué : *Executive Order 13925 of May 28*, 2020, v. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/14/executive-order-on-the-revocation-of-certain-presidential-actions-and-technical-amendment/ (dernier accès le 20 juillet 2021).

**34** Conseil de surveillance de Facebook, *Décision sur le cas 2021-001-FB-FBR*, 11 juill. 2021, https://www.oversightboard.com/decision/FB-691QAMHJ (dernier accès le 20 juillet 2021).

**35** Par exemple, sur l'évolution des systèmes d'information voir le décret n° 2021-930 du 13 juillet 2021 modifiant le décret n° 2020-551 du 12 mai 2020 relatif aux systèmes d'information mentionnés à l'article 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions et le décret n° 2020-1690 du 25 décembre 2020 autorisant la création d'un traitement de données à caractère personnel relatif aux vaccinations contre la covid-19.

**36** On retrouve les deux orthographes « pass sanitaire » et « passe sanitaire ». Cette chronique suivra la suggestion de l'Académie française en faveur de l'emploi de « passe », v. https://www.academie-francaise.fr/pass-sanitaire (dernier accès le 20 juillet 2021) mais ne corrigera pas les citations utilisant l'orthographe « pass ».

**37** V. la mise au point de la CNIL : *Caméras dites « intelligentes » et caméras thermiques : les points de vigilance de la CNIL et les règles à respecter,* 17 juin 2020, https://www.cnil.fr/fr/cameras-dites-intelligentes-et-cameras-thermiques-les-points-de-vigilance-de-la-cnil-et-les-regles (dernier accès le 20 juillet 2021).

**38** V. la présentation de l'outil précédemment utilisé par la RATP : https://www.datakalab.com/détection-de-masques (dernier accès le 20 juillet 2021).

**39** Règl. (UE) 2016/679 du PE et du Cons., 27 avr. 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)

**40** CNIL, délib. n° 2020-136, 17 déc. 2020, portant avis sur un projet de décret relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports, pt. 16.

**41** S. Slama et B. Le Querrec, « Comptage du port du masque dans les transports publics : la vidéo "intelligente" automatisée arrive (à peine) masquée », *Le Blog des juristes*, 16 mars 2021, https://blog.leclubdesjuristes.com/comptage-du-port-du-masque-dans-les-transports-publics-la-video-intelligente-automatisee-arrive-a-peine-masquee-par-serge-slama-et-bastien-le-querrec/ (dernier accès le 20 juillet 2021).

**42** E. Macron, « Déclaration sur la vaccination contre le coronavirus, le pass sanitaire, la réforme des retraites et la politique économique du gouvernement », Paris, 12 juill. 2021, https://www.vie-publique.fr/discours/280792-emmanuel-macron-12072021-pass-sanitaire-et-reforme-des-retraites, (dernier accès le 20 juillet 2021).

**43** Art. 1er, L. n° 2021-1040, 5 août 2021, relative à la gestion de la crise sanitaire, *JO* n° 0181, 6 août 2021.

**44** Le passe sanitaire est défini par le gouvernement comme consistant « en la présentation, numérique (*via* l'application TousAntiCovid) ou papier, d'une preuve sanitaire », https://www.gouvernement.fr/info-coronavirus/pass-sanitaire, (dernier accès le 20 juillet 2021).

**45** Le règlement a été adopté en juin, mais il était en discussion depuis le mois de mars, V. : CE, communiqué de presse, « Coronavirus : la Commission propose un certificat vert numérique »,
17 mars 2021, https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_1181. V. European Data Protection Board, « Avis conjoint 04/2021 de l'EDPB et du CEPD concernant la proposition de règlement du Parlement européen et du Conseil relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats interopérables de vaccination, de test et de rétablissement afin de faciliter la libre circulation pendant la pandémie de Covid-19 (certificat vert numérique) », 31 mars 2021, https://edpb.europa.eu/system/files/2021-07/edpb_edps_joint_opinion_dgc_fr.pdf(derniers accès le 20 juillet 2021).

**46** Art. 2, Règl. (UE) 2021/953.

**47** Art. 3, Règl. (UE) 2021/953.

**48** Art. 11.

**49** V. l'art. 2-3, I, D. n° 2021-724, 7 juin 2021, modifiant le D. n° 2021-699, 1er juin 2021, prescrivant les mesures générales nécessaires à la gestion de la sortie de crise sanitaire. V. le décret étendant le passe sanitaire : D. n° 2021-955, 19 juill. 2021 modifiant le D. n° 2021-699, 1er juin 2021, prescrivant les mesures générales nécessaires à la gestion de la sortie de crise sanitaire.

**50** Ces mêmes données, si elles ne sont pas transmises à un serveur en ligne en lien l'application TousAntiCovid, font tout de même l'objet d'une centralisation nationale via le système d'information « Vaccin Covid », décrit dans la chronique « Numérique » du numéro 12 de cette revue.

**51** Art. 2-1 III, D. n° 2021-724.

**52** Art. 2-1 III, D. n° 2021-724. Comme le précise l'art. 1, 2 B, L. n° 2021-689, 31 mai 2021, relative à la gestion de la sortie de crise sanitaire : « La présentation, sur papier ou sous format numérique, des documents mentionnés au premier alinéa du présent B est réalisée sous une forme ne permettant pas aux personnes habilitées ou aux services autorisés à en assurer le contrôle de connaître la nature du document ni les données qu'il contient ».

**53** Art.1, L. n° 2021-689, 31 mai 2021, relative à la gestion de la sortie de crise sanitaire. À noter que les mêmes peines sont prévues pour les personnes qui exigeraient la présentation du passe alors même qu'elles ne seraient pas habilitées à le faire.

**54** Le Conseil d'État reprend ici la délibération de la CNIL, délib. n° 2021-067, portant avis sur le projet de décret portant application du II de l'article 1er de la loi n° 2021-689 du 31 mai 2021 relative à la gestion de la sortie de crise sanitaire, 7 juin 2021, pt. 24.

**55** Conseil scientifique Covid-19, Avis portant sur l'utilisation d'un pass sanitaire lors de grands rassemblements, 3 mai 2021, p. 7.

**56** *Analyse d'impacts relative à la protection des données personnelles de l'application TousAntiCovid*, version mise à jour au 17 février 2021, p. 6.

**57** Déf. droits, avis 20-03, 27 avr. 2021, relatif à la mise en œuvre de l'état d'urgence sanitaire pour faire face à la pandémie du Covid-19, ainsi que les ordonnances et décrets pris pour son application, p. 16.

**58** Science et Avenir, « Covid : plus de 100 millions de tests en France depuis le début de l'épidémie », 8 juill. 2021, https://www.sciencesetavenir.fr/sante/covid-plus-de-100-millions-de-tests-en-france-depuis-le-debut-de-l-epidemie_155694, (dernier accès le 20 juillet 2021).

**59** Ces contrôles ne pouvaient avoir lieu entre 23h et 8h ni entre 10h et 12h, plage horaire pendant laquelle les personnes placées en quarantaine étaient autorisées à sortir, article 3, projet de loi relatif à la gestion de la crise sanitaire.

**60** CE, avis, 19 juill. 2021, n° 403.629, sur un projet de loi relatif à la gestion de la crise sanitaire, pt. 27.

**61** J.-P. Pont, Rapport sur le projet de loi, après engagement de la procédure accélérée, relatif à la gestion de la crise sanitaire (n° 4386), n° 4389, 21 juill. 2021.

**62** Le Comité de contrôle et de liaison Covid-19 met en lumière le manque de précision de la loi à cet égard. V. l'avis portant sur le « Projet de loi n° 4386 relatif à la gestion de la crise sanitaire », 28 juill. 2021.

**63** CE, avis, 19 juill. 2021, n° 403.629, sur un projet de loi relatif à la gestion de la crise sanitaire, pt. 27.

**64** Le Conseil consultatif national d'éthique a indiqué récemment que « si le numérique et l'intelligence artificielle contribuent de manière majeure à la santé publique, les enjeux d'éthique sous-jacents sont néanmoins importants, par exemple, concernant les données personnelles de santé, obligeant à être particulièrement attentif à leur utilisation », avis Éthique et santé publique, n° 137, 20 mai 2021, p. 12.

**65** Point 114 de la décision.

**66** R. Karayan, « Mais pourquoi certaines start-up sont appelées "licornes" ? », *L'Express*, 30 nov. 2015, https://lexpansion.lexpress.fr/high-tech/blablacar-est-une-licorne-une-quoi_1716931.html, (dernier accès le 20 juillet 2021) ; T. Laurent, « Next 40 : Au cœur de la start-up nation », *Forbes*, 3 mars 2021, https://www.forbes.fr/business/dossier-complet-next-40-au-coeur-de-la-start-up-nation/ (dernier accès le 20 juillet 2021).

**67** Le gouvernement s'est reposé sur des initiatives bénévoles pour lutter contre l'épidémie à l'image des sites internet et applications Covid Tracker et « Vite ma dose ». Le Rapport d'information n° 673 (de la délégation sénatoriale à la prospective, de V. Guillotin, C. Lavarde et R.-P. Savary) du 3 juin 2021 intitulé « Crises sanitaires et outils numériques :

répondre avec efficacité pour retrouver nos libertés » souligne le rôle déterminant des acteurs bénévoles et de la société civile alors même que l'État s'est retrouvé dans l'incapacité à proposer seul de tels outils, p. 68.

**68** V. Guillotin, C. Lavarde et R.-P. Savary, préc., p. 69.

**69** Liste des demandeurs : l'association InterHop, l'association Constances, l'association Actions Traitement, l'association Les Actupiennes, l'association Actup santé sud-ouest, le Syndicat de la médecine générale (SMG), l'Union française pour une médecine libre (UFML), le Syndicat national des jeunes médecins généralistes (SNJMG), la Fédération des médecins de France (FMF), la représentante des usagers du Conseil de surveillance de l'AP-HP, la Fédération SUD Santé Sociaux et la Ligue des droits de l'homme.

**70** V. M. Bernelin, « Droit du numérique », *CDST* 2020, n° 11, p. 205-208.

**71** « Fuite massive de données médicales : une enquête judiciaire ouverte », *Le Monde*, 25 févr. 2021, https://www.lemonde.fr/pixels/article/2021/02/25/fuite-massive-de-donnees-medicales-une-enquete-judiciaire-ouverte_6071184_4408996.html, (dernier accès le 20 juillet 2021).

**72** Art. 9, cons. 51, RGPD.

**73** 1111-8 VII CSP.

**74** CNIL, Violation de données de santé : la CNIL rappelle les obligations des organismes à la suite d'une fuite de données massive annoncée dans les médias, 24 févr. 2021, https://www.cnil.fr/fr/violation-de-donnees-de-sante-la-cnil-rappelle-les-obligations-des-organismes-la-suite-dune-fuite-de (dernier accès le 20 juillet 2021).

**75** https://www.cnil.fr/fr/fuite-de-donnees-de-sante-le-tribunal-judiciaire-de-paris-demande-le-blocage-dun-site-web (dernier accès le 20 juillet 2021).

**76** TJ Paris, ord. réf., 4 mars 2021, n° RG 21/51823.

**77** Communiqués de presse d'Olivier Véran, « Sécurité des réseaux informatiques des établissements de santé : le gouvernement renforce sa stratégie », 22 févr. 2021, https://solidarites-sante.gouv.fr/actualites/presse/communiques-de-presse/article/securite-des-reseaux-informatiques-des-etablissements-de-sante(dernier accès le 20 juillet 2021). Pour mener à bien cette stratégie en garantissant l'essor du numérique en santé, le gouvernement poursuit ses investissements ajoutant 650 millions d'euros aux deux milliards prévus par le Ségur de la santé, v. W. Zirar, « Données de santé, télésurveillance, médecine des "5P" : les pouvoirs publics injectent 650 millions d'euros supplémentaires pour la santé numérique », *TIC Santé,* 7 juill. 2021, https://www.ticsante.com/story/5761/donnees-de-sante-telesurveillance-medecine-des-5p-les-pouvoirs-publics-injectent-650-millions-d-euros-supplementaires-pour-la-sante-numerique.html, (dernier accès le 20 juillet 2021).

**78** La légalité de cette disposition est assurée par l'art. 7, L. n° 2021-689, 31 mai 2021, relative à la gestion de la sortie de crise sanitaire, Cette disposition a été validée par le Conseil constitutionnel : Cons. const., 31 mai 2021, n° 2021-819 DC. Art. 5, D. n° 2021-848, 29 juin 2021, relatif au traitement de données à caractère personnel dénommé « système national des données de santé ».

**79** D. n° 2021-848 « Système national des données de santé ».

**80** Le HDH a également l'obligation de ne pas confier des données à un hébergeur des données de santé qui ne se trouverait pas sur le sol de l'Union européenne, art. 1er, D. n° 2021-848 « Système national des données de santé ».

**81** V. not. M. Bernelin, « Droit du numérique », *CDST* 2020, n° 11.

**82** Par ex. : https://www.nextinpact.com/lebrief/46913/le-ministere-sante-et-cada-refusent-rendre-public-code-health-data-hub (dernier accès le 20 juillet 2021).

**83** CADA, avis n° 20210021, 15 avr. 2021.

**84** V. le site de l'Association Anticor : https://www.anticor.org/2021/03/26/health-data-hub-anticor-saisit-le-pnf/ .

**85** À noter que cette proposition est accompagnée de deux autres documents : un nouveau plan coordonné avec les États membres et un nouveau règlement sur les « machines », qui vient remplacer une directive de 2006.

**86** 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, 21 avril 2020, COM(2021) 206 final.

**87** Livre blanc de la Commission intitulé « Intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance », COM(2020) 65 final, 2020.

**88** Communication de la Commission intitulée « L'intelligence artificielle pour l'Europe », 25 avril 2018, COM(2018) 237 final, suivie de « Building Trust in Human-Centric Artificial Intelligence », 8 avril 2019, COM(2019) 168 final.

**89** V. les recommandations éthiques rendues publiques en septembre 2020 et devant être approuvées en avril 2021, https://fr.unesco.org/artificial-intelligence/ethics et l'avant-projet de recommandation sur l'éthique de l'intelligence artificielle rédigé par le Groupe d'experts *ad hoc* (GEAH) pour l'élaboration d'un avant-projet de recommandation sur l'éthique de l'intelligence artificielle de l'UNESCO, 7 sept. 2020.

**90** V. les principes éthiques adoptés en mai 2019 (OECD/LEGAL/0449),

**91** Proposition de règlement du Parlement européen et du Conseil relatif à un marché intérieur des services numériques (législation sur les services numériques) et modifiant la directive 2000/31/CE (*Digital Services Act* ou *DSA*) (COM(2020) 825 final) et proposition de règlement du Parlement européen et du Conseil relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques) (*Digital Market Act* ou *DMA*) COM(2020) 842 final.

**92** Proposition de règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données), COM(2020) 767 final, 25 nov. 2020.

**93** Exposé des motifs, p. 7.

**94** C. Castets-Renard, « Quelle politique européenne de l'intelligence artificielle ? », *RTD eur*. 2021, p. 297 ; C. Crichton, « Intelligence artificielle : vers la fin du traitement massif des données biométriques ? », *Dalloz IP/IT* 2021, p. 373.

**95** Comité consultatif de la Convention pour la protection à l'égard du traitement automatisé des données à caractère personnel, *Lignes directrices sur la reconnaissance faciale*, T-PD(2020)03rev4, 28 janv. 2021, p. 4. V. égal. les points de vigilance soulevés par le Défenseur des droits, dans son rapport « Technologies biométriques : l'impératif respect des droits fondamentaux », 2021.

**96** EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 juin 2021.

**97** Art. 53 de la proposition.

**98** Art. 60, Règl. (UE) 2016/679 du PE et du Cons., 27 avr. 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), *JOUE* L119/1, 4 mai 2016.

**99** Règl. (UE) 2018/1725 du PE et du Cons., 23 oct. 2018, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le Règl. (CE) n° 45/2001 et la déc. n° 1247/2002/CE (texte présentant de l'intérêt pour l'EEE), *JOUE* L295, 21 nov. 2018.

**100** Il faut néanmoins noter ici qu'à côté des autorités de contrôle nationales compétentes en matière de traitement de données personnelles, le texte propose aussi les autorités nationales compétentes pour surveiller les activités des autorités répressives, des services de l'immigration ou des autorités compétentes en matière d'asile qui mettent en service ou utilisent les SIA mentionnés.

**101** Art. 47.1, préc.

**102** Cons. 76 de la proposition de règlement.

**103** Cette obligation s'impose aux mandataires (art. 25 2. b), aux importateurs (art. 26 5) et aux distributeurs (art. 27 5).

**104** Cette obligation s'impose aux importateurs (art. 26 4) et aux distributeurs (art. 27 3).

**105** Art. 27 4.

**106** L'article 22 du RGPD prévoyait déjà la possibilité de requérir une intervention humaine pour la personne à l'encontre de laquelle une décision prise sur le fondement d'un traitement de données automatisé avait été prise, *op.cit*. Les textes postérieurs ont systématiquement renvoyé à l'intervention humaine en tant que garantie au moment de l'utilisation d'algorithmes de prise de décision.

**107** Art. 33, préc.

**108** Art. 14, Dir. (UE) 2016/1148 du PE et du Cons., 6 juill.2016, *JOUE* L. 194, 19 juill. 2016.

**109** Art. 83 6. RGPD.

**110** M. Vestager, Communiqué de presse, 21 avr. 2021,

**111** Arrêt *Shrems I*, C-362/14.

**112** Déc. de la Commission, 26 juill. 2000 conformément à la Dir. 95/46/CE du PE et du Cons., relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du Commerce des États-Unis d'Amérique, *JO* 2000, L. 215, p. 7).

**113** Décision d'exécution de la Commission du 12 juillet 2016 conformément à la Dir. 95/46/CE du PE et du Cons., relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis, JO 2016, L. 207, p. 1.

**114** Décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la Dir. 95/46/CE du PE et du Cons., (*JO* 2010, L. 39, p. 5), telle que modifiée par la décision d'exécution (UE) 2016/2297 de la Commission du 16 décembre 2016 (*JO* 2016, L. 344, p. 100)

**115** Arrêt *Schrems II*, C-311-18.

**116** Décision d'exécution (UE) 2021/914 de la Commission du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu du Règl. (UE) 2016/679 du PE et du Cons., L. 199/31, 7 juin 2021.

**117** CEPD, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0, 18 juin 2021.

**118** Décision d'exécution de la Commission du 28 juin 2021 constatant, conformément au Règl. (UE) 2016/679 du PE et du Cons., le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni, C(2021) 4800 final, et Décision d'exécution de la Commission du 28 juin 2021 constatant, conformément à la Dir. (UE) 2016/680 du PE et du Cons., le caractère adéquat du niveau de protection des données à caractère personnel assuré par le Royaume-Uni, C(2021) 4801 final.

**119** Les développements ci-dessous sont la reprise d'une chronique publiée sur le site des Éditions législatives et reprise à l'adresse

**120** Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

**121** G29, avis 1/2010 on the concepts of "controller" and "processor" adopté le 16 févr. 2010, 264/10/EN, WP 169.

**122** *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, *Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:551, *Fashion ID*, C-40/17, ECLI:EU:2018:1039.

**123** CEPD, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0, 18 juin 2021.

**124** CJUE, G$^{de}$ ch., 15 juin 2021, *Facebook c. Gegevensbeschermings autoriteit*, C-645/19.

**125** CEPD, Urgent Binding Decision 01/2021 on the request under Article 66(2) GDPR from the Hamburg (German) Supervisory Authority for ordering the adoption of final measures regarding Facebook Ireland Limited, 12 juillet 2021.

**126** Dir. 95/46/CE du PE et du Cons., 24 oct. 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *JOCE*, L. 281, 23 nov.1995.