Le recours aux technologies dans l'obligation de conformité

Emmanuel Netter

Le recours aux technologies dans le droit de la conformité

Emmanuel Netter
Professeur de droit privé à l'université de Strasbourg
Centre de droit privé fondamental (UR 1351)

L'hypothèse d'une technologie manquante. « Bonjour ! Je m'appelle Cherie Deville. Comme vous le savez, vos représentants élus nous demandent de vérifier votre âge avant de vous accorder l'accès à nos services. Même si nous faisons de la sécurité des utilisateurs et de la conformité à la réglementation des principes cardinaux, vous demander de présenter votre carte d'identité à chaque fois que vous souhaitez visiter un site pour adulte n'est pas la solution la plus adéquate pour protéger nos visiteurs. En réalité, cela mettrait en danger tant les enfants que votre vie privée (…) »[1]. Ce message filmé, délivré par une actrice courtoise et souriante, était opposé par la plateforme Pornhub début 2023 à certains internautes en lieu et place de l'accès au service. Les utilisateurs visés n'étaient pas français, comme on aurait pu le croire, notre pays s'étant récemment distingués par ses projets de vérifications d'âge renforcées à l'entrée des sites pour adultes. Il s'agissait des résidents de l'Utah, l'État fédéré américain ayant développé les mêmes préoccupations. La suite du discours de Mme Deville montre que, partout dans le monde, la discussion s'oriente de la même façon : ces sites spécialisés affirment manquer de la technologie qui leur permettrait tout à la fois d'opérer un contrôle d'âge crédible, et d'éviter des intrusions disproportionnées dans l'intimité de leurs visiteurs. L'objectif assigné serait donc louable, mais il manquerait les moyens concrets de l'atteindre.

***Compliance*, conformité**. Une telle situation est peu susceptible de se produire dans un paradigme normatif classique, dans lequel le législateur indique plus nettement quels sont les comportements qu'il entend prohiber, et ceux qu'il veut promouvoir. A l'inverse, comme l'a théorisé Mme Frison-Roche, le droit de la *compliance* se distinguerait par sa définition de grands objectifs (qu'elle appelle « buts monumentaux ») assignés aux destinataires de la règle, les voies permettant d'atteindre ces buts restant quant à elles relativement indéterminées. Cette manière d'orienter les comportements se distinguerait ainsi par sa plus grande souplesse. Elle se justifierait chaque fois qu'il est impossible aux pouvoirs publics de déterminer eux-mêmes le cap à suivre avec finesse, parce que la matière est trop complexe, qu'elle est trop technique, qu'elle nécessite d'articuler des libertés antagonistes dans des contextes excessivement variés, ou tout ceci à la fois. Le « but monumental » ayant été proclamé, il appartiendra aux acteurs de terrain de dessiner eux-mêmes un chemin cohérent pour l'atteindre, en déployant pour ce faire quantité d'outils : auto-diagnostics, mesures d'atténuation des risques, documentation, procédures de toutes sortes. Une autorité administrative indépendante est généralement chargée d'observer l'attitude ainsi adoptée.

Dans la pensée de Mme Frison-Roche, alors que la « compliance » désigne le paradigme normatif basé sur la désignation de buts monumentaux, le terme français de « conformité » renvoie à l'ensemble plus vil des moyens concrets que l'on se propose d'employer pour atteindre les grands objectifs, qui prend rapidement l'allure d'une couche probatoire : comment puis-je démontrer, par la tenue de registres, par la production d'analyses d'impact, par la mise à jour de « checks-lists » de toutes sortes, que mes procédures sont saines ? Surgit d'ailleurs le risque qu'on se focalise excessivement sur ces indicateurs concrets, en perdant de vue le « but monumental » qu'ils sont

1 Libre traduction de la vidéo consultable à l'adresse : https://www.youtube.com/watch?v=09Ovt2t6SgQ.

censés servir. La « conformité » ainsi définie nous semble correspondre assez bien au concept « d'accountability » (imparfaitement traduit par « responsabilité ») tel qu'il résulte de l'article 5.2 du règlement général sur la protection des données.

Conformité et progrès technologiques. Parmi ces outils de la conformité figureront évidemment, et en bonne place, des progrès technologiques récents. Protéger les données à caractère personnel des utilisateurs, améliorer la concurrence sur un marché, empêcher l'utilisation frauduleuse de moyens de paiement… nombreux sont les objectifs fondamentaux qui nécessitent l'emploi de raffinements technologiques, mais aussi la lutte contre des technologies employées par des adversaires.

La difficulté principale de notre étude se laisse aisément deviner : le paysage des technologies de pointe est sans cesse changeant. Le paradigme de la *compliance* semble au premier abord particulièrement adapté à un tel contexte, qui constitue d'ailleurs, on l'a dit, l'une de ses raisons d'être. Les pouvoirs publics ne s'étant pas arc-boutés sur des moyens précis mais s'étant contentés de définir des fins, ils laisseraient un large espace aux autorités administratives pour faire évoluer, au jour le jour, la traduction technologique de ces attentes, en sécrétant quantité de droit plus ou moins souple, sous la forme de lignes directrices, de référentiels ou de conseils individualisés. Décrire ce phénomène de constante adaptation constitue nécessairement l'un des aspects d'une étude des rapports entretenus par le droit de la conformité avec les technologies. Mais on ne peut s'en tenir là. Une situation, aussi inquiétante pour la pratique qu'elle est passionnante pour la théorie, est susceptible de surgir : celle dans laquelle les pouvoirs publics ont édicté un objectif qui n'est plus vraiment monumental, comme « la protection des mineurs en ligne », mais intermédiaire, et en tout cas bien plus concret, comme « l'obligation de vérifier rigoureusement l'âge des internautes à l'entrée d'un service en ligne ». La souplesse du système diminue alors drastiquement, et il peut advenir que l'objectif assigné soit inatteignable en l'état des technologies existantes. Le but fixé s'interprète alors quasiment comme un ordre de développer une technique encore absente.

Ainsi, après avoir envisagé l'attitude du droit de la conformité à l'égard des technologie existantes (I), nous verrons quels rapport il entretient avec les technologies simplement potentielles (II).

I – Conformité et technologies existantes

Le droit de la conformité impliquera parfois une interdiction ou une restriction forte des usages de certaines technologies, lorsque celles-ci sont intrinsèquement contraires à ses grands objectifs : ce seront des technologies proscrites (A). Dans d'autres situations, le droit de la conformité cherchera à se mettre constamment à jour des progrès les plus récents : il tiendra compte des technologies disponibles (B).

A – Les technologies proscrites

Explicabilité. Dans le paradigme de la *compliance*, les pouvoirs publics n'ont pas délimité eux-mêmes avec précision l'espace des comportements vertueux et celui des comportements prohibés. Cela explique la place très importante dévolue, dans un tel modèle, aux principes de transparence et d'explicabilité : puisqu'on ne sait pas à l'avance comment les acteurs vont se comporter, on attend d'eux qu'ils s'expliquent, encore et encore, sur leurs actions comme sur leurs abstentions. Il en résulte une forme d'hostilité aux technologies dont le fonctionnement n'est pas explicable, ou du moins pas expliqué. Ainsi, par exemple, de l'article 22 du RGPD, relatif aux décisions entièrement

automatisées produisant, à l'égard des individus, des effets juridiques[2]. Il peut s'agir de pré-sélectionner, à l'aide d'un logiciel, les candidatures les plus adaptées à une offre d'emploi, les autres étant mises à la corbeille sans avoir été mises sous les yeux d'un être humain. Cela peut encore prendre la forme d'une décision de refus ou d'octroi automatisée de prêt bancaire et, dans la seconde hypothèse, de la fixation automatique du taux d'intérêt. Le principe posé par le RGPD est la prohibition de ces méthodes[3]. Ce choix s'explique largement par la montée en puissance des techniques d'intelligence artificielle de type *machine learning* qui sont *intrinsèquement* inexplicables, mais aussi par l'emploi d'algorithmes plus traditionnels (tels ceux employés par des systèmes experts) dont le fonctionnement *pourrait* théoriquement être expliqué, mais est en réalité inaccessible aux destinataires des décisions. La prohibition de principe souffre certes quelques exceptions, mais celles-ci font alors naître le droit à une intervention humaine, si la personne concernée le demande[4]. Cela revient de fait à débrancher la technologie employée pour lui substituer une intervention humaine.

Obsolescence. Le paradigme normatif de la *compliance* est particulièrement bien armé pour considérer qu'une technologie se trouve brutalement périmée, et que la poursuite des grands objectifs, comme assurer la sécurité des systèmes d'information ou la protection des données à caractère personnel des individus, commande de l'abandonner sans tarder. Une approche réglementaire classique aurait bien du mal à assurer un tel résultat. Ainsi, dans l'univers numérique, les algorithmes se périment. La recherche en mathématiques peut tout à coup démontrer que la recette employée pour sécuriser un canal de communication ou rendre des informations dormantes indéchiffrables souffre d'une faiblesse irrémédiable. Dans une approche par la conformité, il appartient aux professionnels de se tenir informés et de découvrir cette information nouvelle par eux-mêmes, puis d'en tirer les conséquences en recherchant un nouvel algorithme adéquat. Lorsqu'il s'agit d'un outil largement utilisé, il est toutefois certain que la CNIL et l'ANSSI serviront de surcroît de vigies et communiqueront largement sur la technologie à abandonner, et même sur les alternatives existantes, faisant la démonstration des vertus prêtées à ces autorités : expertise technique et réactivité[5].

Effets anti-concurrentiels. Le maintien d'un niveau élevé de concurrence fait partie des grands objectifs habituellement poursuivis dans le paradigme de la *compliance*. Simultanément, la technologie se révèle un instrument puissant lorsqu'il s'agit d'emprisonner des utilisateurs dans un écosystème fermé, en mêlant intimement des fonctionnalités théoriquement distinctes : l'achat d'une certaine marque de téléphone pourrait rapidement conduire à utiliser un certain moteur de

2 Sur ce sujet, V. not. L. Huttner, *La décision de l'algorithme : étude de droit privé sur les relations entre l'humain et la machine*, thèse Paris 1, 2022.

3 Une faille redoutée dans ce dispositif consistait, pour le responsable du traitement, à affirmer qu'il n'utilisait qu'un simple système « d'aide à la décision », le dernier mot revenant en apparence à un être humain, afin de ne pas appliquer l'article 22. La CJUE a toutefois jugé récemment que la production d'indicateurs quasiment toujours suivis par le décideur humain devait être assimilé à une décision entièrement automatisée : CJUE, 7 décembre 2023, C-634/21, Schufa.

4 Il convient également, en tel cas, de donner aux personnes concernées « des informations utiles concernant la logique sous-jacente » au traitement : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, (ci -après « RGPD »), art. 13.2, f et 14.2, g.

5 Pour l'exemple de l'abandon du protocole SSL au profit du TLS dans la navigation web : https://www.cnil.fr/fr/securite-securiser-les-sites-web et https://cyber.gouv.fr/publications/recommandations-de-securite-relatives-tls. Cependant, s'il n'existe aucune technologie de substitution, on se retrouvera dans la situation examinée dans la deuxième partie de cette étude.

recherche, un unique magasin d'applications ou un système de paiement particulier. Ces technologies-prison sont donc prohibées par le règlement sur les marchés numériques[6].

Intrusivité. Revenons à l'exemple cité en ouverture de cette étude : si l'on était prêt à abandonner toute protection de la vie privée des internautes, il n'y aurait aucune difficulté à imposer un système de vérification d'âge rigoureux à l'entrée des sites pour adultes, et à refouler les mineurs qui chercheraient à accéder à ces contenus. Il suffirait, comme l'Utah semble l'avoir fait, de demander une copie d'une pièce d'identité à tout visiteur. Mais les différents objectifs fondamentaux poursuivis par le droit de la conformité doivent s'articuler entre eux, et le droit des données à caractère personnel, dans une telle situation, ne peut céder entièrement devant l'objectif légitime de protection des publics fragiles. Un contrôle de proportionnalité doit s'ensuivre. Dans l'arsenal du RGPD, il s'incarnera dans l'article 5, c, selon lequel les données doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ». La CNIL en a tiré toutes les conséquences, en matière d'accès aux sites pornographiques, en rejetant un certain nombre de technologies trop intrusives[7] : le recours aux documents d'identité déjà évoqué, la vérification de l'âge à partir d'une captation en temps réel du visage en employant des techniques de *machine learning*, mais aussi l'utilisation du portail « France connect », qui n'a pas été pensé pour de tels cas d'usages. Dans ce dernier cas, on révélerait à l'État l'identité de sa citoyenne ou de son citoyen visitant un site pour adultes, et parfois même son orientation sexuelle. En revanche, le recours à une vérification d'âge reposant sur une transaction par carte bancaire à zéro euro, avec authentification forte, en passant par un tiers indépendant, a été considéré comme une solution certes imparfaite, mais tolérable en attendant mieux.

Après avoir lutté contre le recours à certaines technologies, le droit de la conformité va commander d'en intégrer d'autres dans les pratiques des professionnels régulés.

B – Les technologies disponibles

Les technologies à employer si elles sont disponibles. Le RGPD offre deux exemples de dispositions qui se raccrochent expressément aux meilleures technologies utilisables, au service de l'objectif poursuivi, à un instant donné. On peut tout d'abord citer l'article 8, relatif au consentement des enfants en ce qui concerne les services de la société de l'information. Il pose une question cousine de celle de la vérification d'âge en matière de sites réservés à une catégorie d'âge. En effet, dans les situations qui requièrent un consentement des parents, parce que l'enfant est trop jeune pour consentir seul, le texte exige : « Le responsable du traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, **compte tenu des moyens technologiques disponibles** »[8]. Cela requiert de savoir qui tient la souris ou le smartphone à un instant donné, et passe par des mécanismes de vérification d'identité particulièrement délicat à déployer. Conscient de la difficulté, le législateur renvoie aux moyens disponibles à la fois pour relativiser la pression exercée sur les acteurs de terrain dans les premières années de vie du texte, et pour la faire croître dès que des progrès auront été enregistrés dans ce domaine. On peut ensuite citer l'article 17 :

6 Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique (ci-après « DMA), par ex. art. 6.4. Sur ce texte, V. not. J.-C. Roda, Le Digital Markets Act (1 re partie) – Contrôler les contrôleurs d'accès, CCE 2023, étude 4 ; Le Digital Markets Act (2 e partie) – Contraindre les contrôleurs d'accès, CCE 2023, étude 6.

7 https://www.cnil.fr/fr/verification-de-lage-en-ligne-trouver-lequilibre-entre-protection-des-mineurs-et-respect-de-la-vie.

8 Art. 8.2 du RGPD. Souligné par nous.

lorsqu'une demande d'effacement de données personnelles légitime lui a été adressée, le responsable du traitement doit avertir tous les tiers qui auraient traité les mêmes informations, « compte tenu des technologies disponibles » pour assurer cette propagation.

Les technologies à contrecarrer si elles sont disponibles. Une partie importante du droit européen du numérique repose sur une approche « par les risques »[9]. Il s'agit d'évaluer les dangers qui planent sur l'activité exercée et de s'y adapter, non pas ponctuellement, mais en continu. Or, parmi ces risques, figure évidemment l'utilisation offensive de technologies contre le service opéré. On peut donc considérer que toutes les textes mettant en œuvre ces approches intègrent naturellement la question de l'adaptation défensive aux nouvelles technologies disponibles, qu'il s'agisse par exemple des mesures attendues des très grandes plateformes dans le règlement sur les services numériques (dit DSA)[10], ou des entités concernées par la directive NIS 2 sur le cybersécurité[11]. Dans le RGPD, l'obligation de prendre toutes les mesures techniques et organisationnelles appropriées doit être déployée « compte tenu de l'état des connaissances », ce qui implique évidemment la prise en compte de technologies dangereuses émergentes[12]. Le même texte est plus explicite encore lorsqu'il évoque les attaques de réidentification : il s'agit, pour l'attaquant, de partir d'un jeu de données initialement supposées anonymes et, par l'application de déductions, croisements et recoupements, dévoiler néanmoins l'identité des personnes présentes dans le fichier. Or, « pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, **en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci** »[13]. Fait rare et peut-être unique dans le domaine des qualifications juridiques, des données anonymes un jour peuvent donc devenir à caractère personnel le lendemain, sans avoir été modifiées en rien, parce qu'un article de *data science* aura été publié entre-temps, ce qui en modifiera radicalement le régime juridique.

Ainsi la notion de « technologie disponible » permet-elle, dans le paradigme normatif de la *compliance*, d'imposer aux acteurs de terrain, et aux autorités qui les encadrent, d'actualiser perpétuellement leurs outils pour exploiter ou contrecarrer les inventions les plus récentes.

Mais il peut arriver que le droit aille plus loin encore, et fasse référence à des technologies qui n'existent pas encore.

II – Conformité et technologies potentielles

S'appuyer sur des technologies qui n'existent pas encore n'a pas le même sens selon que ces inventions sont manifestement réalisables à court terme (A) ou que leur faisabilité même n'est pas certaine dans un horizon prévisible (B).

9 A. Latil, Le droit du numérique : une approche par les risques, Dalloz, 2023.

10 Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE, art. 34 et s.

11 Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, art. 21.

12 RGPD, art. 32.

13 RGPD, cons. 26.

A – Les technologies en germe

Données personnelles. Le « droit à la portabilité » des données à caractère personnel est le droit, pour la personne concernée par un traitement, et à certaines conditions, d'obtenir communication des informations qu'elle avait fournies, « dans un format structuré, couramment utilisé et lisible par machine »[14]. Nous aurions pu faire figurer une telle formule dans la partie de l'étude consacrée aux technologies « disponibles », puisque le responsable du traitement reçoit l'ordre de mettre les informations en forme conformément à l'état de l'art, qui est par nature changeant. Ce droit a plusieurs usages possibles, mais permettra par exemple au client d'un service de stockage de photos dans le cloud de télécharger l'ensemble de ses images en quelques clics, afin de les téléverser auprès d'un prestataire concurrent. S'il avait à rapatrier chacune de ses milliers d'images une par une, il serait dissuadé. La partie du texte qui nous intéresse véritablement ici est celle-ci : « Lorsque la personne concernée exerce son droit à la portabilité des données en application du paragraphe 1, elle a le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, **lorsque cela est techniquement possible** »[15]. L'approche nous semble différente. Se référer aux technologies « disponibles » implique que des acteurs ont déjà pris l'initiative de les développer et de les proposer, de sorte que les professionnels régulés n'ont plus qu'à s'en saisir. Viser le « techniquement possible » implique qu'un produit qui n'existe pas, mais que l'état de l'art permettrait de concevoir, doit être développé si nécessaire. L'autorité de la concurrence italienne avait ainsi reproché à Google de n'avoir pas permis le transfert direct de données entre responsables de traitement, en se fondant directement sur le RGPD, et la société de Mountain View a annoncé qu'elle développerait les solutions nécessaires[16].

Paiements sécurisés. Afin de limiter les phénomènes de fraude impliquant des cartes ou des données faciales de cartes bancaires volées, la directive dite « services de paiement 2 » a imposé aux banques le développement d'un mécanisme dit « d'authentification forte »[17]. Un règlement délégué a ensuite été adopté sous l'égide de l'Autorité Bancaire Européenne, afin de mettre en place des « normes techniques » appropriées[18]. Même ce texte, toutefois, décrit moins une technologie précise qu'un cahier des charges, qui se veut technologiquement neutre. Par exemple, il est exigé de l'authentification forte qu'elle mobilise deux catégories de preuve d'identité parmi les trois possibles que sont la possession (la maîtrise physique d'un élément, comme une carte, ou le téléphone du client), la connaissance (le fait d'être en possession d'un secret, comme un code PIN ou un mot de passe) et l'inhérence (une caractéristique biométrique de l'individu susceptible d'être testée, comme une empreinte digitale ou l'aspect du visage). Les établissements sont libres, dans ces limites, de leur façon de procéder. L'ensemble a néanmoins contraint les banques à développer, à marche forcée, des technologies qui n'existaient pas sous cette forme exacte au moment de l'adoption de DSP2, et que chacun utilise désormais presque quotidiennement lorsqu'il procède à des paiements en ligne[19]. Il n'y avait cependant pas d'aléa : toutes les briques élémentaires

14 RGPD, art. 20.
15 RGPD, art. 20.2.
16 Autorité italienne de la concurrence, communiqué du 31 juillet 2023 : https://en.agcm.it/en/media/press-releases/2023/7/A552.
17 Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, spéc. Art 97.
18 Règlement délégué (ue) 2018/389 de la Commission du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication
19 Fédération bancaire française, La DSP2 et les enjeux de sécurité : https://www.fbf.fr/fr/la-dsp2-et-les-enjeux-de-securite/.

nécessaires au développement d'applications idoines pour smartphones, par exemple, préexistaient, mais il restait à en réaliser une combinaison inédite, offrant simplicité d'utilisation et haut niveau de sécurité.

Il est ainsi loisible aux pouvoirs publics de contraindre des acteurs à développer des technologies qui n'existent pas encore sous la forme exacte envisagée, mais qui résultent simplement d'une combinaison – même difficile ou coûteuse à mettre en œuvre – d'inventions déjà disponibles. C'est autre chose d'exiger la mise en œuvre de technologies dont les éléments constitutifs n'existent pas encore, et pourraient même se révéler impossibles à développer dans un horizon prévisible.

B – Les technologies imaginaires

La vérification de l'âge en ligne. Il arrive que le législateur ordonne l'accomplissement non pas d'un grand objectif abstrait, mais d'un but bien plus concret, qui nécessiterait le déploiement d'une technologie relativement précise, sans paraître se demander si cette technologie existe, ni même si elle est susceptible d'exister. Nous avons laissé entendre que ce pouvait être le cas de l'injonction à contrôler rigoureusement l'âge des visiteurs d'un site internet pour adultes.

Telle semblait effectivement être l'approche de la loi de 2020 visant à lutter contre les violences conjugales. Celle-ci prévoyait que « Lorsqu'il constate qu'une personne dont l'activité est d'éditer un service de communication au public en ligne permet à des mineurs d'avoir accès à un contenu pornographique (…) le président du Conseil supérieur de l'audiovisuel adresse à cette personne, par tout moyen propre à en établir la date de réception, une mise en demeure lui enjoignant de prendre **toute mesure de nature à empêcher l'accès des mineurs au contenu incriminé** »[20]. « Débrouillez-vous comme vous voudrez », en somme. Le CSA, qui n'était pas encore l'Arcom, avait été rapidement saisi par plusieurs associations de défense des familles, et avait saisi le TJ de Paris[21]. Puis un décret avait été pris, en octobre 2021, en application de la loi sur les violences conjugales, précisant que « Le conseil supérieur de l'audiovisuel **peut** adopter des lignes directrices concernant la fiabilité des procédés techniques[22] ». Autrement dit, il n'en avait pas l'obligation, et pouvait théoriquement laisser les acteurs se débrouiller. Ce décret a été attaqué devant le Conseil d'État, et la décision est encore pendante au moment où nous écrivons ces lignes. Environ un mois plus tard, le CSA constatait d'ailleurs que le site Pornhub était accessible moyennant une simple « déclaration de majorité » et le mettait en demeure sur ce seul constat, sans chercher à caractériser qu'une technologie existait, auquel on aurait manqué de recourir[23]. Ce faisant, on l'a vu, il ne faisait qu'appliquer la loi.

Sautons quelques étapes de cette riche saga, et mentionnons la question prioritaire de constitutionnalité posée par Pornhub. Elle était libellée ainsi : « Les dispositions de l'article 23 de la loi n° 2020-936 du 30 juillet 2020 et de l'article 227-24 du code pénal tel que modifié par l'article 22 de la loi n° 2020-936 du 30 juillet 2020 (auquel l'article 23 renvoie) sont-elles conformes aux droits et libertés que la Constitution garantit que sont le principe de légalité des délits et des peines et la liberté d'expression et de communication, respectivement en ce que ces dispositions ne

20 Art. 23 du 30 juillet 2020 visant à protéger les victimes de violences conjugales. Souligné par nous.

21 « Des associations saisissent le CSA pour bloquer des sites pornographiques accessibles aux mineurs », article leparisien.fr du 27 novembre 2020.

22 Décret n° 2021-1306 du 7 octobre 2021 relatif aux modalités de mise œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique, art. 3. Souligné par nous.

23 Décision du 13 décembre 2021 mettant en demeure la société MG Freesites Ltd en ce qui concerne le service de communication au public en ligne « Pornhub ».

définissent pas en des termes suffisamment clairs et précis une infraction pénale et le comportement pouvant donner lieu à une sanction ayant le caractère d'une punition et portent une atteinte qui n'est pas nécessaire, adaptée et proportionnée à l'objectif poursuivi par le législateur de prévention de l'accès des mineurs aux contenus pornographiques sur Internet ? »[24]. La Cour de cassation refusa de la transmettre. Il nous semble que les rédacteurs de la question ont eu tort de ne pas soulever l'atteinte à la liberté d'entreprendre que constitue l'ordre de déployer une technologie qui n'existe pas : son sort aurait été, nous semble-t-il, plus incertain.

Le législateur, toutefois, ne devait pas en rester là : dans un projet de loi « visant à sécuriser et réguler l'espace numérique » (SREN), du 17 octobre 2023, qui n'est pas encore définitivement adopté au moment où nous écrivons, c'est un mécanisme très différent de celui de 2020 qui est prévu. Aux termes de ce texte, en effet, l'ARCOM « « établit et publie (…) après avis de la Commission nationale de l'informatique et des libertés, un référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge. Ces exigences portent sur la fiabilité du contrôle de l'âge des utilisateurs et sur le respect de leur vie privée ». Il ne s'agit plus d'une faculté de publier des lignes directrices, mais d'une obligation de publier un référentiel, qui de surcroît doit articuler les libertés en cause, y compris le droit à la vie privée. Dans ce nouveau système, la mise en demeure qui pourra ensuite être délivrée par l'ARCOM consistera à ordonner le respect de ce référentiel. Dès lors, si l'ARCOM se révélait incapable d'adopter un référentiel crédible, les sites ne pourraient plus être mis en difficulté. Si ce projet SREN devait être adopté, la faisabilité technologique deviendrait donc la condition centrale du dispositif.

A cet égard, il convient de souligner que le laboratoire de prospective de la CNIL, en partenariat avec un chercheur de l'école Polytechnique, a publié une preuve de concept à propos d'un système permettant une vérification d'âge présentant apparemment toutes les qualités attendues[25]. Voilà qui modifierait les termes du débat. Soulignons toutefois que si le système proposé est probablement irréprochable sur le plan théorique, il pourrait se révéler si pénible d'utilisation en pratique que plusieurs comportements sont à prévoir de la part des utilisateurs : la renonciation à consulter un site pornographique ; la consultation de sites plus confidentiels, ayant échappé à l'attention des régulateurs, et potentiellement encore plus dangereux – un argument soulevé par Pornhub, dans la vidéo citée en introduction de cette étude – ou encore l'utilisation d'un dispositif, tel qu'un VPN, permettant de faire croire qu'on se connecte depuis un pays n'exigeant pas de vérification d'âge. Dans toutes ces scénarios, et en l'absence au moins provisoire de technologie d'un maniement plus léger, il est probable que les sites feraient valoir qu'on porte une atteinte disproportionnée à leur liberté d'entreprendre, au regard de la protection effective des mineurs qui serait obtenue.

Il semble cependant que les recherches de la CNIL nous aient privé d'une hypothèse dans laquelle les pouvoirs publics demanderaient la mise en œuvre d'une technologie encore purement imaginaire. Mais un tel cas de figure se présente peut-être dans un autre domaine.

L'interopérabilité des messageries sécurisées. Nous avons vu plus tôt que le règlement sur les marchés numériques est susceptible d'abattre les murs qui pourraient enfermer les utilisateurs dans des prisons techniques. Au premier abord, les « obligations incombant aux contrôleurs d'accès concernant l'interopérabilité des services de communications interpersonnelles non fondés sur la numérotation » semblent relever du même esprit[26]. Il s'agit de rendre obligatoire la possibilité de

24 Cass. 1Ère civ. 5 janv. 2023, QPC, n° 22-40.017.
25 https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee.
26 Règlement 2022/1925 précité, art. 7.

faire communiquer les services de messagerie instantanée entre eux. Dès lors, si vos contacts utilisent un service, vous être libre d'en utiliser un autre et vous pouvez néanmoins communiquer avec eux : les courriers électroniques, par exemple, sont nativement interopérables. Mais l'exigence va ici, très loin, le texte prévoyant : « Le niveau de sécurité, y compris le chiffrement de bout en bout, le cas échéant, que le contrôleur d'accès fournit à ses propres utilisateurs finaux est maintenu dans l'ensemble des services interopérables ». Un chiffrement de bout en bout protège la confidentialité des messages échangés par des utilisateurs, en les rendant incompréhensibles puis en les remettant au clair directement sur leurs terminaux. Cela signifie que les opérateurs de télécommunication par lesquels transitent les données, mais aussi l'opérateur de messagerie lui-même, sont incapables d'accéder aux contenus dans une version non chiffrée. Un tel système nécessite des opérations complexes de gestion des clés de chiffrement alors même que, à l'heure actuelle, ces messageries ne sont pas interopérables. Dans un scénario d'interopérabilité, cette gestion pourrait atteindre un degré de difficulté confinant à l'impossible. Certains spécialistes estiment qu'il ne sera donc techniquement pas envisageable de faire dialoguer, par exemple, un utilisateur de WhatsApp et un partisan de Signal en maintenant un chiffrement de bout en bout. Un chercheur estime ainsi : « Essayer de réconcilier deux architectures cryptographiques différentes **est tout simplement impossible** ; un côté ou l'autre devra faire des changements majeurs. Une conception qui ne fonctionne que lorsque les deux parties sont en ligne sera très différente de celle qui fonctionne avec des messages stockés... Comment faites-vous pour que ces deux systèmes interagissent ? »[27]. Un autre va jusqu'à affirmer : « rédiger une loi ordonnant de "permettre une interopérabilité totale sans créer de risques pour la vie privée ou la sécurité" revient à ordonner aux médecins de guérir le cancer »[28]. L'image est forte. D'un point de vue juridique, quelle serait la conséquence ? Alors que l'implémentation d'un système de vérification d'âge très pesant, et aux effets positifs incertains, pouvait comme on l'a vu aboutir à une atteinte insuffisamment justifiée à la liberté d'entreprendre, il nous semble qu'ici le contrôle de proportionnalité ne pourrait même pas avoir lieu. L'ordre d'implémenter une technologie impossible devrait s'analyser en une atteinte automatiquement inacceptable à la libre entreprise.

S'agissant du cas précis des messageries chiffrées de bout-en-bout, cependant, il n'est pas exclu que le dénouement soit du même ordre que pour la vérification d'âge, et qu'un progrès technique à un moment supposé impossible se révèle finalement non seulement atteignable, mais qu'il le soit de surcroît rapidement. Un entrepreneur estimait en effet, à propos de l'exigence du DMA : « C'est le meilleur résultat possible imaginable pour l'internet ouvert. Plus jamais une grande entreprise technologique ne pourra retenir ses utilisateurs en otage dans un jardin clos, ni fermer arbitrairement ou saboter ses API »[29]. Surtout, de récentes annonces Facebook laissent entendre que l'interopérabilité sera bien au rendez-vous, au moins avec certains services[30]. Il est trop tôt pour savoir si le résultat sera tout à la fois parfaitement ouvert et sécurisé, interopérable et protecteur de la vie privée. Sans doute ne suffit-il pas d'ordonner aux médecins de guérir le cancer pour qu'ils y parviennent, mais créer le contexte le plus favorable à leur recherche pourrait les y aider. En exerçant une forte pression sur une entreprise comme Méta, on aura provoqué l'allocation des ressources considérables de cette entité en direction de l'objectif recherché par le législateur, ce qui aura apparemment fait progresser l'état de l'art. La méthode, typique de la *compliance*, consistant à

27 J.-M. Manach, « Le DMA et le casse-tête de l'interopérabilité des messageries », article next.ink du 31 mars 2022.
28 Ibid.
29 Ibid.
30 L. Renouard, « WhatsApp détaille le fonctionnement de son interopérabilité avec d'autres messageries », article les numeriques.com du 7 février 2024.

désigner l’objectif, et à laisser les acteurs trouver le chemin, aurait alors fait la preuve, dans ce contexte au moins, de son efficacité.