SIMON ASSOCIÉS

La Lettre du Numérique

L'actualité juridique et économique des acteurs du numérique par Simon Associés

JUILLET-AOÛT 2022

SOMMAIRE

PROPRIETE INTELLECTUELLE	
L'encadrement par la CNIL des caméras augmentées : le prisme d'une société démocratique Décision de la CNIL du 8 juin 2022 : Google Analytics et transferts de données : comment mettre son outil de mesure d'audience en conformité avec le RGPD ?	p. 2
Les mises à jour de IOS d'Apple pour que l'iPhone ne soit pas un outil au service de l'espionnage Article du journal Silicon : Apple répond à l'épisode Pegasus avec un « mode isolement »	p. 3
DATA / DONNEES PERSONNELLES	
La signature électronique et l'exigence de fiabilité : vers un encadrement européen et national unifié Le règlement européen du 23 juillet 2014 (UE) n° 910/2014 (autrement appelé l'eIDAS)	p. 4
ACTUALITES NUMERIQUES	
Le DMA et DSA : un droit du numérique européen protecteur face aux GAFAM Conseil de l'UE Communiqué de presse du 18 juillet 2022 : le Conseil approuve définitivement les nouvelles règles sur la concurrence loyale en ligne	p. 6
Depuis le 1er septembre 2022 la circulation des voitures autonomes de niveau 3 est autorisée Décret n° 2021-873 du 29 juin 2021 portant application de l'ordonnance n° 2021-443 du 14 avril 2021 relative au régime de responsabilité pénale applicable en cas de circulation d'un véhicule à délégation de conduite et à ses conditions d'utilisation	p. 7

PARIS - NANTES - LYON
MONTPELLIER - LILLE
TOULOUSE - NICE

Bureaux intégrés

AIX-EN-PROVENCE
BLOIS - BORDEAUX
BOURG-EN-BRESSE
CLERMONT-FERRAND
LE HAVRE - MARSEILLE - METZ
MONTLUÇON - NANCY - NICE
OYONNAX - PONTARLIER - ROUEN
TOURS - VICHY

Réseau SIMON Avocats

ALGÉRIE - ARGENTINE
ARMÉNIE - AZERBAÏDJAN
BAHAMAS - BAHREÏN
BANGLADESH - BELGIQUE
BIRMANIE - BOLIVIE - BRÉSIL
BULGARIE - BURKINA FASO
CAMBODGE
CAMEROUN - CHILI - CHINE
CHYPRE - COLOMBIE
COREE DU SUD - COSTA RICA
CÔTE D'IVOIRE - ÉGYPTE
EL SALVADOR
ÉMIRATS ARABES UNIS
ESTONIE - ÉTATS-UNIS - GRECE
GUATEMALA - HONDURAS
HONGRIE - ÎLE MAURICE
ÎLES VIERGES BRITANNIQUES
INDE - INDONÉSIE - IRAN
ITALIE - KAZAKHSTAN
KOWEÏT - LUXEMBOURG
MADAGASCAR - MALTE
MAROC - MEXIQUE - NICARAGUA
OMAN - PANAMA - PARAGUAY
PÉROU - PORTUGAL - QATAR
RD CONGO - RÉPUBLIQUE
DOMINICAINE - SENEGAL
SINGAPOUR - SUISSE - THAÏLANDE
TUNISIE - URUGUAY
VENEZUELA - VIETNAM
ZIMBABWE

Conventions transnationales

www.simonassocies.com
www.lettredunumerique.com

PROPRIETE INTELLECTUELLE

L'encadrement par la CNIL des caméras augmentées : le prisme d'une société démocratique
Rapport de juillet 2022 CNIL

Ce qu'il faut retenir :

L'intelligence artificielle, permet aujourd'hui le déploiement de technologies plus performantes mais également plus intrusives de nos libertés individuelles. Nouvel enjeu sociétal mais également juridique, la question est donc de savoir quelles en seront les limites et les instruments légaux les plus efficaces.

A ce titre, la cybersurveillance et plus particulièrement les caméras « augmentées », ont en juillet 2022, fait l'objet d'une étude menée par la Commission nationale de l'informatique et des libertés « CNIL »). La CNIL, dans ce rapport, s'est exprimée concernant l'utilisation des caméras « augmentées » dans l'espace public (voies et transports publics, centres culturels…) et ce afin d'encadrer leurs utilisations abusives tout à la fois dans le secteur privé et public.

Il apparaît également nécessaire de rappeler que ledit rapport fait suite à une consultation publique sur une première version proposée par la CNIL. Au travers de cette démarche, la Commission souhaite mobiliser et sensibiliser les acteurs tant privés que publics aux nouveaux enjeux de société.

Enfin, comme le rappelle l'autorité administrative, la frontière est poreuse entre ce qui est technologiquement possible et ce qui relève d'une démocratie effective, stable et forte.

Pour approfondir :

Le rapport de la CNIL se focalise sur les caméras dites « augmentées » analysant des images en temps réel et de manière continue. En revanche, sont exclues du rapport la reconnaissance biométrique ainsi que les usages dans des lieux privés ou domestique et en différé.

L'autorité administrative, a néanmoins constaté qu'en France, le Code de la sécurité intérieure était outrepassé. Selon la Commission trois éléments doivent en ce sens faire l'objet d'une étude approfondie :

- ✓ La protection des données personnelles
- ✓ La nécessité d'une loi
- ✓ Le droit d'opposition

L'usage des caméras dites « traditionnelles », fonctionne sur la base d'un accès restreint et d'une recherche ciblée. Force est de constater qu'aujourd'hui de tels outils ont une puissance d'analyse considérable, chose qu'un œil humain ne peut réaliser. Ainsi, l'utilisation des algorithmes change le prisme de lecture et conduit inévitablement au traitement automatisé de données personnelles voire sensibles.

D'une part cette technologie doit alors s'entendre comme l'analyse d'une attitude comportementale d'un individu isolé dans des lieux où s'exercent les libertés individuelles (d'aller et venir, de manifester…).

D'autre part, l'utilisation des caméras dites « augmentées » semble objective mais elle n'en demeure pas moins discriminante et ce, même si l'algorithme fonctionne sur la base de données factuelles. En effet, les données « d'entrée » peuvent cibler certaines catégories de personnes. L'algorithme étant auto-apprenant, il se nourrira de ces seules informations. Mais comment peut-on imaginer vivre dans un espace plus sécurisé et perfectionné si les principes fondamentaux de notre démocratie sont écartés ?

Pour préserver ce principe, la CNIL rappelle que l'usage des caméras augmentées ne doit pas être utilisé à des fins d'identification de la personne. Ces technologies sont permises par la CNIL si elles répondent à des fins statistiques de sécurité ou encore publicitaires. Dans son rapport la CNIL énumère le référentiel des finalités.

Il importe également que ces données ne soient conservées que sur une échelle de temps limité. Dans cette perceptive, il peut être envisagé que la caméra puisse directement procéder au comptage, sans qu'aucune donnée ne soit conservée. Le risque de toute réidentification est alors écarté.

Il faut donc noter que tout dépendra de la finalité du traitement qui doit être déterminé, explicite et légitime.

La nécessité d'une loi est également un élément essentiel de ce rapport. En effet, dans le cas où le droit d'opposition s'avère impossible à mettre œuvre, l'utilisation des caméras augmentées devra être permis au regard d'une finalité statistique (comme vu précédemment) ou sous réserve de l'édiction d'un cadre légal spécifique a minima réglementaire.

L'édiction de ces lois devra néanmoins se conformer aux principes de légitimité et de proportionnalité du traitement. Il ne faut cependant pas selon la CNIL, encourager les initiatives locales, position par ailleurs partagée par le Sénat en mai 2022.

Force est de constater qu'au sein des services de police administrative ou judiciaire, le traitement des données peut affecter l'exercice des libertés publiques. Des lois s'avèrent donc primordiales. La difficulté réside alors dans cet équilibre entre la sauvegarde de l'ordre public et la protection des droits.

La Commission souligne néanmoins que la frontière est mince avec la surveillance généralisée et nécessite de ce fait, une vigilance accrue. A titre d'exemple le système chinois repose aujourd'hui sur le « scoring social ». En effet, sans ces caméras, il serait impossible de surveiller de façon permanente les citoyens afin de leur attribuer une note en fonction de leurs comportements. Ces technologies ont donc pour conséquences de réduire voire supprimer leurs droits sociaux selon cette note.

Dans l'esprit de ce rapport il ressort que chaque Etat, dès lors qu'il se confronte à une crise doit rester soucieux de la démocratie. La crise du Covid 19 en Chine, a accentué ces pratiques. En France, des modèles expérimentaux ont également été mis en place dans les transports ou espaces publics afin d'évaluer sous forme de pourcentage le taux de port du masque.

Au travers de ces différentes prises de position, la CNIL cherche à instaurer un traitement de donnée au cas par cas et au regard du principe du « privacy by design ». L'encadrement des caméras « augmentées » ne se fera pas postérieurement mais en amont de leur utilisation. Il faut alors revoir la base du système juridique existant et les adapter afin d'assurer un avenir protecteur de nos libertés et des droits fondamentaux. Les lieux publics devant à tout prix rester un espace démocratique et non le reflet des dérives dont certains pays font déjà l'expérience.

A rapprocher :

*1 Délibération de la CNIL

Les mises à jour de IOS d'Apple pour que l'iPhone ne soit pas un outil au service de l'espionnage
Article du journal Silicon : Apple répond à l'épisode Pegasus avec un « mode isolement »

Ce qu'il faut retenir :

Apple, a enregistré au cours de son dernier trimestre en 2021, un bénéfice net de 31 milliards d'euros. La firme se place ainsi comme le vendeur n°1 au niveau mondial. L'enjeu est donc de taille, si elle souhaite rester compétitive. Cependant, l'affaire Pegasus qui pose la question des failles de sécurité d'Apple pourrait remettre en question cette place de leader.

Apple a proposé une nouvelle mise à jour en version beta puis en version publique le 12 juillet 2022, il s'agit de la 16ème version d'IOS. IOS 16, serait selon Apple, plus sécurisé et garantirait plus efficacement la protection des données des utilisateurs de la marque à la pomme.

Il apparait que l'amélioration du système d'exploitation d'Apple est optionnelle et permet de faire face à des logiciels espions. Il s'agit du mode dit « isolement ».

Pour approfondir :

Il semble essentiel de faire un rappel de l'affaire Pegasus. Le laboratoire Citizen Lab a révélé que le système d'exploitation d'Apple avait été attaqué par le logiciel espion Israélien, Pegasus de la société « NSO group » L'entreprise NSO Group a été fondée en 2010 par Niv Carmi, Shalev Hulio et Omri Lavie,. Avec le logiciel PEGASUS la messagerie « iMessage » d'Apple pouvait être piraté sans que la personne concernée ait besoin de cliquer sur un lien la renvoyant à un malware. Cette technique plus poussée et plus discrète, ne laissera ainsi pas à la victime l'opportunité de déceler l'attaque. En bref, il s'agit de la méthode du « zéro clic » exploitant seulement la vulnérabilité d'iMessage.
Concrètement, cette dernière a permis de dévoiler les données personnelles de millions d'utilisateurs de la marque à la pomme et notamment de certains journalistes ou hommes politiques. Selon le rapport de Mediapart, cinq ministres français auraient été ainsi espionnés.

Le logiciel Pegasus présenté au départ comme permettant de lutter contre le terrorisme et la criminalité a agi dans cette affaire en dehors de ce cadre. Alors, comment encadrer et renforcer les systèmes de sécurité ?
Dans un communiqué de presse du 23 novembre 2021, Apple attaque en justice la NSO, mais le groupe ne s'arrête pas là.
Il a initié plusieurs nouvelles mises à jour. L'iOS 14.8 est l'une d'entre elle et constitue un argument de vente pour redorer l'image de la marque. Apple a introduit le mécanisme du « BlastDoor ». Celui-ci permet de filtrer les messages avant même que ceux-ci parviennent à l'utilisateur. Il s'agit donc d'un « SAS de sécurité » qui fonctionne indépendamment de l'iOS.

La dernière version proposée par Apple s'inscrit dans cette nouvelle démarche de sécurisation. L'iOS 16, propose ainsi des correctifs qui seront installés silencieusement et ne nécessiteront pas de redémarrage. Il permet notamment dans l'app messages, un blocage des pièces jointes. Dans le navigateur la désactivation des compilations Just-In Time (JIT) qui visent à améliorer des système type JAVA. Enfin le blocage pour facetime des contacts avec

lesquelles l'utilisateur n'a pas interagi ainsi que des connexions filaires aux ordinateurs et accessoires lorsque l'iPhone est verrouillé.

Force est de constater qu'une prise de conscience générale s'opère dans le domaine de la cybersécurité. Comme il l'a été démontré plus haut, les grandes entreprises elles-mêmes ne sont pas infaillibles et peuvent-être vulnérables.
L'objectif est donc de restaurer la confiance des utilisateurs dans des systèmes plus fiables et plus performants. Outre les usagers, se pose la question de la souveraineté des Etats. En effet, à titre d'exemple, l'affaire Pegasus a permis d'espionner des hommes politiques hauts placés. Les informations détenues et traitées illégalement seront stratégiques et pourront permettre d'affaiblir politiquement, voir économiquement le pays concerné. L'enjeu est donc de taille.
Aujourd'hui, les moyens mis à disposition des pirates de l'informatique sont sans précédents et nécessitent des développements techniques afin d'établir des systèmes d'exploitation plus sûrs.
Il apparait également important de garder à l'esprit que cette affaire s'inscrit dans la continuité d'une problématique qui est celle de la surveillance de masse. Bien que cette fois-ci Apple soit la victime.

A rapprocher :

- Article 1 : https://www.silicon.fr/apple-pegasus-mode-isolement
- Article 2 : https://www.journaldugeek.com/quest-ce-que-blastdoor
- Article 3 : https://www.mediapart.fr/journal/international/dossier/le-dossier-pegasus
- Communiqué de presse Apple : https://www.apple.com/fr/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/

DATA / DONNEES PERSONNELLES

La signature électronique et l'exigence de fiabilité : vers un encadrement européen et national unifié

Le règlement européen du 23 juillet 2014 (UE) n° 910/2014 (autrement appelé l'eIDAS)

Ce qu'il faut retenir :

De nos jours, les évolutions technologiques permettent un partage plus rapide et efficace de la donnée. Pourtant, il ne faut pas perdre de vue que la sécurité des informations est tout aussi importante. A ce titre, sont mis au service de leur sécurité et fiabilité ces mêmes progrès techniques.
Le contexte sanitaire suite à la crise du covid 19, a permis de mettre en lumière de nouvelles pratiques telle que la signature électronique.
Cette dernière par définition, doit remplir deux fonctions qui sont : l'identification du signataire et son adhésion à l'acte. Pour ce faire la signature électronique doit-être « fiable », c'est-à-dire être intègre.
Ainsi, l'ambition affichée par la réglementation est de mettre sur un pied d'égalité la signature électronique et la signature manuscrite.
Pour justifier de cette démarche, il est essentiel de mettre en avant les avantages de la signature électronique. En effet, au-delà des aspects purement pratiques (rapidité des échanges, économie, simplicité…), la signature électronique dispose juridiquement d'une présomption de fiabilité contrairement au support papier. Par ailleurs, grâce aux mécanismes de la blockchain, ces systèmes dès lors qu'ils sont certifiés, apportent une sécurité considérable aux documents concernés.

Pour approfondir :

Le règlement européen du 23 juillet 2014 (UE) n° 910/2014 (autrement appelé l'eIDAS), distingue trois niveaux de définition de la signature électronique :
✓ La signature dite simple : qui n'est pas assez complexe pour permettre d'identifier de manière univoque le signataire ;
✓ La signature dite avancée : qui repose sur quatre conditions, l'identification unique et formelle de la signature, le contrôle exclusif du signataire et l'impossible modification de la signature ;
✓ La signature dite qualifiée : à laquelle ajoute une condition exigeant un certificat dit « qualifié » ainsi qu'une clé cryptographique.
Ce même règlement a d'ailleurs précisé dans son article 25.3 qu'une « signature électronique qualifiée qui repose sur un certificat qualifié délivré dans un État membre est reconnue en tant que signature

électronique qualifiée dans tous les autres États membre ». Ce règlement cherche donc à établir un cadre unifié ainsi que des procédures communes. Par ailleurs, le point 2 de ce même article pose le principe de non-discrimination entre les signatures manuscrites et électroniques. L'objectif étant de créer une interopérabilité entre tous ces moyens.
L'encadrement juridique de la signature électronique permet d'établir la validité de tout acte juridique, qu'il s'agisse d'un contrat, d'un acte notarié. L'article 1367 Code civil dispose que la signature « lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire […] ».
Par ailleurs, le décret du 30 mars 2001 (n°2001-272) et abrogé par celui du 28 septembre 2017, posait trois conditions pour considérer la signature électronique comme fiable. Ainsi, il fallait qu'elle soit propre au signataire ; qu'il en garde le contrôle exclusif et que toute modification ultérieure de l'acte soit détectable (définition de la signature avancée).

Cependant, le décret en Conseil d'État du 28 septembre 2017 va plus loin dans son approche. En effet, l'article 1er pose trois conditions.
Il s'agit :
✓ D'une signature électronique avancée
✓ D'un dispositif de création de signature électronique qualifié
✓ D'un certificat qualifié
De plus, un horodatage qualifié est un gage d'intégrité et prouve ainsi que le fichier n'a pas été modifié depuis la date indiquée sur le document signé. En outre, c'est seulement dans ces conditions que le document peut bénéficier d'une présomption d'exactitude.
D'un point de vue purement technique, cette sécurité repose généralement sur la blockchain et plus particulièrement sur la cryptographie à clés asymétriques. En effet, le signataire est détendeur d'une clé publique hachée et partagée par les parties au contrat ainsi que d'une clé privée. Cette dernière permet de garantir l'identité du signataire, celle-ci étant considérée comme sa « carte d'identité ».
Conformément à l'article 288-1 du Code de procédure civile « lorsque la signature électronique bénéficie d'une présomption de fiabilité, il appartient au juge de dire si les éléments dont il dispose justifient le renversement de cette présomption ».
En ce sens, le 26 juin 2019, la Cour de cassation a jugé « qu'une signature préimprimée, scannée par un procédé informatique, n'est pas une signature électronique et ne garantit pas l'identité du signataire ». Elle souligne également « […] que la signature imprimée figurant sur la déclaration de créance litigieuse avait été certifiée par l'acte notarié [mais] permettait seulement au notaire de certifier l'authenticité de la signature imprimée sur les documents qui lui seraient présentés, et ne certifiait pas en lui-même l'authenticité de la signature imprimée sur la déclaration de créance litigieuse ». Principe réaffirmé par la Cour de cassation le 12 mai 2022, qui a jugé que l'apposition d'une image numérique d'une signature ne permet pas d'identifier clairement le signataire.
La Cour d'appel Riom a également précisé le 06 avril 2022 que « l'identification de l'auteur de la signature par l'usage d'une boîte aux lettres électronique apparaît insuffisante pour authentifier la signature du client ».
Enfin, la Cour d'appel de Douai a le 25 mars 2021, considéré qu'un document décrivant la procédure de conclusion d'un contrat ne permet pas de prouver l'utilisation d'un « certificat électronique qualifié ».
Les principaux acteurs concernés par ces réglementations sont les concepteurs de logiciels de signature électronique. En effet, ils se doivent d'être vigilant afin d'offrir un système conforme aux exigences légales. De même, la personne morale (notaire, établissement public, banque assurance…) qui propose un service de signature électronique doit s'assurer de la fiabilité dudit service.
Ainsi, pour les accompagner au mieux, des systèmes de certification sont mis en place. Ils fonctionnent sur la base d'une collaboration entre la direction centrale de la sécurité des systèmes d'informations (DCSSI) et un centre d'évaluation choisit par le prestataire qui souhaite établir sa certification. En ce sens, la Cour d'appel de Chambéry a pu juger le 10 février 2022 que la société qui demandait le paiement des sommes dues au titre du contrat n'apportait pas la preuve qu'elle disposait de la qualification pour la certification des signatures électroniques.

A rapprocher :

- **Lexis 360 - Encyclopédies - JurisClasseur Civil Code - Art. 1364 à 1368 - Fasc. unique : PREUVE DES OBLIGATIONS. – Modes de preuve. – Notion d'écrit. Écrit électronique**
- **https://www.affiches-parisiennes.com/reglementation-et-utilisation-de-la-signature electronique.html**
- **Cour d'appel, Riom, 3e chambre civile et commerciale réunies, 6 avril 2022 – n° 20/01114**
- **Cour d'appel, Chambéry, 2e chambre, 10 février 2022 – n° 20/00880**
- **Cour de cassation, Chambre commerciale financière et économique, 26 juin 2019 – n° 18-15.33**
- **Cour de cassation, 2e chambre civile, 12 mai 2022 – n°2021367**
- **Cour d'appel, Douai, 8e chambre, 1re section, 25 mars 2021 – n° 18/06933**

ACTUALITES NUMERIQUES

Le DMA et DSA : un droit du numérique européen protecteur face aux GAFAM

Conseil de l'UE Communiqué de presse du 18 juillet 2022 : le Conseil approuve définitivement les nouvelles règles sur la concurrence loyale en ligne

Ce qu'il faut retenir

« L'UE est la première juridiction au monde à établir une norme complète pour réglementer l'espace numérique ». Au travers de cette position exprimée par Thierry BRETON Commissaire Européen, il apparait essentiel de souligner que le mardi 05 juillet 2022, le Parlement Européen a approuvé 2 textes fondateurs du droit du numérique européen : le DMA et DSA respectivement « Digital Market Act » et « Digital Service Act ».

Ces textes ont rencontré un franc succès auprès des parlementaires européens. En effet, pour ce qui est du DMA il a obtenu 588 voix pour, 11 contre et 31 abstentions. Le DSA quant à lui a obtenu 539 pour 54 contre et 30 abstentions.

Ces textes devaient encore faire l'objet d'une validation par le Conseil européen. Ainsi, le 18 juillet 2022, le Conseil européen a validé définitivement le DMA. Cette prise de position amènera à établir définitivement et de manière pérenne un environnement numérique équitable et compétitif dans le secteur des plateformes en ligne.

Pour approfondir :

I. Un rappel des objectifs du DMA et du DSA

Les objectifs du « Digital Market Act » et « Digital Service Act » sont respectivement :

- D'accroître la responsabilité et limiter le pouvoir sur le marché des géants de la technologie (notamment GAFAM) ;
- Protéger les utilisateurs contre les contenus illégaux.

II. Le contexte de l'adoption

Pour faire un bref rappel de procédure, le droit d'initiative législative appartient à la Commission européenne qui présente une proposition au Conseil Européen et au Parlement européen. En première ou seconde lecture, ces deux institutions adoptent ladite proposition. Néanmoins si à l'issue de ces échanges il n'y a pas d'accord trouvé, un comité de conciliation est convoqué.

En ce qui concerne le DMA et le DSA, c'est en décembre 2020 que la Commission européenne avait présenté son projet de règlementation pour mieux réguler l'activité des plateformes sur le marché et services numériques.

Le 24 mars 2022, pour donner suite à cette proposition, un accord politique provisoire avait été conclu entre le Conseil européen et le Parlement européen.

Par suite de la validation des deux actes par le Parlement, c'est l'adoption par le Conseil Européen qui permettra l'application du DSA et du DMA. Cette validation est intervenue le 18 juillet 2022 pour le (DMA) et se poursuivra en septembre pour le (DSA). Enfin, les deux règlements rentreront en vigueur dans les 20 jours après sa publication au Journal officiel de l'Union européenne. Néanmoins, le DMA sera appliqué dans les 6 mois et le DSA dans les 15 mois.

III. Les conséquences de cette adoption

Aujourd'hui, l'Union Européenne compte sur son territoire 10 000 plateformes en ligne de PME actives dans l'économie numérique et témoigne des effets positifs de cette prise de conscience.
Par ces deux adoptions du mois de juillet, l'Europe s'inscrit dans une dynamique lui permettant de s'imposer comme le « chef de file » de cette régulation. En effet, le règlement étant un acte législatif contraignant, il doit être mis en oeuvre dans son intégralité et sur l'ensemble du territoire de l'Union Européenne et s'impose donc à chaque Etat.

L'arsenal juridique de l'Union européenne devient par conséquent une réalité et s'inscrit ainsi dans une dynamique d'encadrement législatif à long terme. En effet, la Commission européenne a invité le Conseil européen à se concentrer sur un programme d'action intitulé " boussole numérique pour 2030" qui vise à établir des objectifs et des étapes à atteindre d'ici 2030, notamment pour une protection des valeurs de l'UE et des droits fondamentaux ainsi que pour le renforcement de la souveraineté numérique de l'Europe. L'objectif est donc de s'imposer face aux GAFAM en leur imposant de nouvelles obligations et tout en revalorisant les petites et moyennes entreprises. L'Europe veut ainsi devenir un concurrent de taille face aux Etats-Unis.

Ces validations européennes permettront également une coopération avec les autorités nationales de la concurrence. Ainsi, en application de ces deux règlements, ces derrières enquêteront et sanctionneront toute atteinte au DMA. De plus, tout

individu victime des agissements, d'un contrôleur d'accès pourra s'appuyer sur les obligations et interdictions posée par le DMA pour demander des dommages et intérêts devant les juges nationaux. Ces validations garantissent ainsi la portée du DMA, et depuis peu celle du DSA.

IV. Ouverture

Malgré une législation européenne forte, il n'est pas impossible d'envisager une règlementation à l'échelle mondiale. Une déclaration pour l'avenir de l'internet a ainsi été signée par 60 pays et notamment par les États-Unis et l'UE. Josep Borrell, haut représentant de l'Union Européenne pour les affaires étrangères et la politique de sécurité, a en ce sens déclaré que « *cela montre que la diplomatie numérique de l'UE fait partie intégrante de notre boîte à outils en matière de politique étrangère.* »

A rapprocher

• Digital Market Act (DMA):

• Digital Service Act (DSA) :

• Conseil de l'UE Communiqué de presse du 18 juillet 2022

• Résolution législative du Parlement européen du 5 juillet 2022 : 2022-07-05-adoption par le parlement européen du DMA.pdf

• Résolution législative du Parlement européen du 5 juillet 2022 : 2022-07-05-adoption par le parlement européen du DSA.pdf

---

Depuis le 1er septembre 2022 la circulation des voitures autonomes de niveau 3 est autorisée

Décret n° 2021-873 du 29 juin 2021 portant application de l'ordonnance n° 2021-443 du 14 avril 2021 relative au régime de responsabilité pénale applicable en cas de circulation d'un véhicule à délégation de conduite et à ses conditions d'utilisation

Ce qu'il faut retenir :

Depuis ce jeudi 1er septembre, les constructeurs et les industriels, ont l'autorisation de faire circuler des voitures autonomes.
Le décret n° 2021-873 du 29 juin 2021, prévoit la circulation des véhicules « à délégation de conduite » et en pose les conditions d'utilisation. En effet, son entrée en vigueur étant placée au 01 septembre 2022, il s'impose comme le nouveau texte porteur de ces évolutions.

Cette démarche même si elle est limitée aux voitures de « niveau 3 », s'inscrit dans un contexte de développement économique et technologique important. C'est ainsi, que dans un communiqué de presse de juillet 2021, le ministère de la transition écologique et des transports avait déjà témoigné de sa volonté de « faire de la France le lieu privilégié en Europe du déploiement de services de mobilité routière automatisés ». La stratégie nationale à long terme, est donc de « [placer] l'innovation technique, le cadre réglementaire et la démonstration de sécurité au centre des actions publiques ». Ainsi dès 2021, par suite de cette adoption de ce cadre législatif et de ce communiqué de presse, la France se place en tête des pays européens ainsi que du G7.
Néanmoins, il est précisé que pour que la conduite automatisée quitte le statut des technologies « expérimentales » elle doit-être autorisée par une loi nationale. Dans ce contexte, la France adopte le décret n° 2022-1034 du 21 juillet 2022 portant publication de l'amendement à la Convention de Vienne du 8 novembre 1968 1. La France est donc sur la bonne voie afin d'établir un cadre législatif favorisant le développement des voitures autonomes.

Pour approfondir :

Pour faire un bref rappel, le décret le 29 juin 2021 vient compléter l'ordonnance du 14 avril de la même année et permet la circulation des véhicules automatisés, de « niveau 3 ». Un véhicule peut être considéré comme « autonome » de niveau 3 s'il répond à la définition suivante : « véhicule équipé d'un système de conduite automatisé exerçant le contrôle dynamique du véhicule dans un domaine de conception fonctionnelle particulier, devant effectuer une demande de reprise en main pour répondre à certains aléas de circulation ou certaines défaillances pendant une manœuvre effectuée dans son domaine de conception fonctionnelle »

Cette autorisation n'est pas sans limite. En effet, celle-ci ne vaut que si ces véhicules circulent :

✓ Sur les autoroutes et les voies rapides jusqu'à 60km/h ;

✓ Sur des voies interdites aux cyclistes et piétons ;

✓ Si le conducteur a la possibilité de reprendre le contrôle de sa voiture à tout moment.

En revanche, le niveau 4 et 5 ne supposent quant à eux plus l'intervention d'un humain, soit sur des tâches bien spécifiques (niveau 4) soit sur l'ensemble de la conduite (niveau 5).

Les deux premiers niveaux quant à eux se rapprochent plus de l'assistance. Le conducteur pouvant reprendre à tout moment le contrôle total du véhicule.2

Malgré un avenir prometteur, il faut s'interroger sur la place « réelle » de ces évolutions réglementaires. D'une part il faut attendre que les voitures soit homologuée et d'autre part que les constructeurs investissent dans ce type de véhicule afin de développer une technologie fiable.

Ces systèmes dans la pratique sont déjà très avancés aux Etats-Unis, en Allemagne ou en Chine. A ce titre, il faut noter que les voitures Mercedes Benz sont homologuées par les autorisées Allemandes pour la conduite autonome. Elles s'imposent ainsi comme les seules sur le marché européen ! En effet, cette technologie a été approuvée par l'Autorité fédérale des transports automobiles pour deux modèles de la marque, les Classe S et EQS. A l'inverse, son concurrent Telsa ne bénéficie pas encore de ce statut.

Pourtant, en France les industriels et constructeurs comme Mercedes ne bénéficient pas d'une homologation car la demander serait pour l'heure inutile.

En effet, il semblerait que le ministère de l'intérieur n'y soit pas favorable pour des raisons de sécurité routière. Alors même que des grandes firmes françaises comme VALEO s'affirment comme des experts dans ce domaine, le gouvernement reste craintif. Il faut alors observer une dichotomie entre les textes et la pratique. Même si la France semble être un pays avancé en termes de législation ce n'est pas le cas quant à la mise en œuvre de ses textes.

A rapprocher

- https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043729532
- https://www.ecologie.gouv.fr/mobilite-routiere-automatisee-et-connectee
- https://unece.org/DAM/trans/conventn/Conv_road_traffic_FR.pdf