SOMMAIRE

DATA / DONNÉES PERSONNELLES

Bilan de l'année 2020 en protection des données personnelles

Quelles sont les principaux faits marquants de l'année 2020 en matière de protection de données personnelles ?

L'année 2020 a été très marquée par la crise sanitaire. Pour faire face à cette crise, les traitements de données à caractère personnel portant notamment sur des données sensibles se sont multipliés. Nous avons également assisté à une généralisation du télétravail qui a dû se faire dans des conditions précipitées et pas toujours assorties de garanties de sécurité.

Cette période a, par ailleurs, été marquée par une très forte augmentation d'opérations d'attaques informatiques concernant aussi bien des cybermarchands que des institutions. Les objectifs poursuivis par les cyberattaquants sont multiples et variés : détournement de fonds, demande de rançons, espionnage industriel, etc. Parmi les dernières attaques informatiques de grande importance, nous pouvons citer celles qui ont ciblé l'Agence Européenne du Médicament et le groupe pharmaceutique Fareva.

La seconde partie de l'année 2020 a, quant à elle, été marquée par la publication tardive et tant attendue des délibérations de la CNIL relatives aux cookies. A ce titre, deux délibérations ont ainsi été publiées, l'une posant le cadre juridique applicable aux cookies, et l'autre déterminant les recommandations pratiques de la CNIL pour se mettre en conformité aux nouvelles règles.

En juillet 2020, la Cour de justice de l'Union européenne a rendu une décision aux impacts importants puisqu'elle a invalidé les accords du Privacy Shield, accord permettant les transferts de données vers les États-Unis.

Enfin de nombreuses délibérations de la CNIL ont marqué la fin d'année 2020. La formation restreinte de la CNIL a ainsi sanctionné plusieurs opérateurs de manière assez inédite puisque les montants sont très importants et concernent des géants du numériques mais également des enseignes et des indépendants.

Pour ne citer que quelques exemples, la chaîne hôtelière Mariott a été sanctionnée à hauteur de 20 millions d'euros par l'autorité de contrôle britannique en coopération avec la CNIL pour des manquements à son obligation de sécurité. Carrefour France a été sanctionné à plus de 2 millions d'euros et Carrefour Banque a écopé d'une amende atteignant presque 1 million d'euros pour des manquements au RGPD concernant notamment l'information des personnes et le respect de leurs droits. La société Amazon quant à elle, s'est vu infligée une amende de 35 millions d'euros pour défaut de consentement préalable à l'installation de cookies publicitaires.

De manière plus inattendue, 2 médecins libéraux exerçant en cabinet individuel ont été sanctionnés. Le montant de leur amende est moins spectaculaire puisqu'ils ont été respectivement sanctionnés à hauteur de 3.000 et 6.000 euros d'amende. Néanmoins, si ces montants semblent moins dissuasifs, rapportés à l'échelle de leur chiffre d'affaires ils représentent plus de 3 et 6 % du chiffre d'affaires de ces médecins.

Que faut-il retenir de ces faits marquants ?

On retiendra tout d'abord de l'année 2020 que les situations au contexte exceptionnel ne sont assorties d'aucune dérogation en matière de protection des données. Pire, les climats particulièrement tendus et propices à la vulnérabilité de la sécurité des données doivent conduire à adopter une démarche toujours plus soucieuse du RGPD même lorsque cela ne paraît pas être la priorité ou qu'il existe de fait des urgences à traiter.

On retiendra ensuite que la CNIL multiplie ses contrôles et durcit sensiblement ses sanctions. Après avoir consacré une grande partie de son activité à l'accompagnement des entreprises pour les aider à comprendre le RGPD et à respecter leurs obligations depuis 2016, la CNIL consacre désormais davantage d'énergie à contrôler avec sévérité le suivi de ses préconisations.

Enfin, on retiendra que toutes les entreprises sont concernées quels que soit leur taille ou leur secteur d'activité et que personne n'est à l'abri d'une sanction.

Quel plan d'action pour 2021 ?

Plusieurs actions devraient être à l'ordre du jour du planning de la conformité 2021.

La conformité des sites internet au regard des délibérations relatives aux cookies est un premier point.

Les délibérations de la CNIL à ce sujet ont été publiées en septembre dernier et la CNIL a octroyé un délai de 6 mois pour s'y conformer qui prendra fin en mars 2020.

La mise à niveau des mesures de sécurité est une autre priorité, les sanctions prononcées à la suite de notifications de violation de données témoignent du fait que l'instruction dès notification de violation de données est aussi l'occasion de contrôler le RGPD au sein des entités ayant subi la violation. Les compétences et expertises techniques de la CNIL ne doivent pas être sous-estimées, les agents de contrôles sont parfaitement compétents pour réaliser des investigations particulièrement poussées pour vérifier les mesures de sécurité mises en place, les contrôler et les challenger.

L'encadrement des transferts, particulièrement vers les États-Unis doit également être poursuivi en 2021.

Enfin, une véritable réflexion sur les modalités d'information des personnes concernées par des traitements doit être menée. Cette obligation ne doit pas être prise à la légère et il ne suffit pas d'adopter des politiques de confidentialité ou des mentions d'information type. La CNIL sanctionne notamment le manque d'accessibilité à l'information et le manque de clarté.

La CNIL et la protection des données à caractère personnel face à la crise sanitaire du Covid-19 – Partie 2

Décret n°2020-1454 du 27 novembre 2020 ; Décret n°2020-1690 du 25 décembre 2020 ; Délibération n°2020-126 du 10 décembre 2020

Ce qu'il faut retenir :

Dans le contexte particulier de la crise sanitaire, la CNIL, autorité de contrôle française, est un acteur clé pour l'orientation tant des autorités publiques, que des professionnels et particuliers sur les enjeux relatifs à la protection des données à caractère personnel.

Pour approfondir :

La CNIL publie et centralise de nombreux avis, fiches et recommandations thématiques relativement à la crise sanitaire du COVID-19. Si la lutte contre la propagation du virus s'illustre actuellement par le déploiement d'une campagne de vaccination à l'échelle nationale, celle-ci est également rendue effective par l'existence d'une application de traçage des cas contacts : l'application TousAntiCovid ayant succédé à l'application StopCovid.

Déployée par le gouvernement le 22 octobre 2020, cette application vise à faciliter l'information des personnes ayant été en contact avec une personne testée positive au COVID-19 et permet à ses utilisateurs d'être alertés et d'alerter les autres individus contacts ayant été exposés au virus. Tout comme l'application StopCovid, l'application TousAntiCovid repose sur une démarche volontaire des utilisateurs mais se distingue de la précédente en ce qu'elle propose des informations actualisées sur la circulation du virus ainsi que des liens vers d'autres outils numériques de lutte contre le COVID-19.

Si cette nouvelle application n'était pas subordonnée à une saisine obligatoire de la CNIL, en l'absence de modifications substantielles du traitement de données personnelles, la CNIL précise qu'elle restera vigilante pour examiner et contrôler ses futures évolutions, et qu'elle devra être impérativement saisie en cas de modifications substantielles dudit traitement.

Il doit être rappelé que la CNIL s'est à plusieurs reprises prononcée en urgence en raison du caractère exceptionnel du contexte sanitaire. L'autorité de contrôle a en effet rendu deux avis relatifs à l'application StopCovid, le premier en date du 24 avril 2020 et relatif au principe de mise en œuvre de l'application, et le second en date du 25 mai 2020 relatif au projet de décret encadrant ladite application. Il doit être également noté que la CNIL rendait en urgence un avis le 8 mai 2020 sur la mise en œuvre de fichiers d'identification de personnes contaminées et de leurs cas contacts (fichiers SI-DEP et Contact Covid).

Dans le cadre du lancement de l'application TousAntiCovid, le gouvernement a opté pour l'envoi d'un SMS aux abonnés des opérateurs téléphoniques pour communiquer sur cette nouvelle application concomitamment à la réouverture des commerces. Cette opération de communication était réalisée dans le cadre du décret du 27 novembre 2020 lequel prévoit que l'opérateur prend les mesures nécessaires pour transmettre à ses utilisateurs les messages d'alerte et d'information des pouvoirs publics destinés au public

pour atténuer les effets de la catastrophe sanitaire. Le gouvernement s'est alors directement adressé aux opérateurs de télécommunications qui se sont ensuite chargés d'acheminer le message gouvernemental à leurs propres abonnés.

Afin d'accompagner la campagne de vaccination, l'autorité de contrôle française a été saisie par le ministre des solidarités et de la santé. Cette saisine pour avis portait sur la création d'un traitement de données à caractère personnel ayant pour objet la gestion et le suivi des vaccinations contre le coronavirus. Ce traitement intitulé « Système d'information (SI) Vaccin Covid » poursuit pour finalités l'organisation de la campagne de vaccination, le suivi et l'approvisionnement en vaccins et consommables (seringues), la réalisation de recherches et le suivi de pharmacovigilance. Parmi les données collectées figurent des catégories particulières de données, telles que le numéro de sécurité sociale (NIR) ou encore des informations relatives aux critères d'éligibilité à la vaccination. De telles données sont tant protégées par la réglementation relative à la protection des données que par le secret médical.

De manière générale, il convient d'adopter la plus grande vigilance dans le déploiement des dispositifs destinés à la surveillance de la propagation du virus en raison du risque prononcé d'une atteinte aux libertés individuelles.

Pour lutter contre la propagation du COVID-19, sont apparus des dispositifs de caméras dites « intelligentes » ou thermiques. Ces dispositifs permettent notamment la prise de température automatique, la détection du port du masque ou encore le respect de la distanciation sociale. Dans ce contexte, la CNIL appelle à la plus grande vigilance et demande une analyse au cas par cas de ces dispositifs qui peuvent conduire à traiter des données sensibles sans recueillir préalablement le consentement des personnes concernées ou sans leur permettre d'exercer leur droit d'opposition.

Enfin, il est à noter que la CNIL a également publié un certain nombre de recommandations thématiques destinées à accompagner l'ensemble des secteurs d'activités.

L'autorité de contrôle s'est ainsi adressée aux structures sportives souhaitant mettre en œuvre des dispositifs de limitation de propagation du virus et assurer la reprise de leurs activités. Il est rappelé que les relevés de température, les résultats aux tests virologiques et tout certificat médical constituent des données de santé. La CNIL indique que sauf en cas de recueil d'un consentement libre, spécifique, univoque et éclairé des personnes concernées, les structures sportives ne peuvent pas mettre en place de registres relatifs à la prise de température corporelle ou encore décider de pratiquer des tests virologiques préalables à l'organisation de manifestations sportives. Enfin, en l'absence de réglementation le prévoyant expressément, l'accès à une structure sportive ne peut être conditionnée à la production d'un test virologique négatif.

En raison de leur sensibilité, les données relatives à l'état de santé d'une personne sont en principe interdites et font l'objet d'une protection juridique particulière. L'autorité de contrôle rappelle que la collecte en dehors de toute prise en charge médicale de telles données doit être impérativement encadrée et respecter la réglementation relative à la protection des données.

Il est à noter que l'ensemble de ces recommandations est actualisé régulièrement au regard du contexte actuel inédit et s'accompagne de liens redirigeant vers des contenus exhaustifs de la CNIL et des autorités concernées pour chacune des thématiques abordées.

A rapprocher : Décret n°2020-1454 du 27 novembre 2020 modifiant le décret n° 2020-1310 du 29 octobre 2020 prescrivant les mesures générales nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire ; 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 ; Délibération n°2020-126 du 10 décembre 2020 portant avis sur un projet de décret autorisant la création d'un traitement de données à caractère personnel relatif à la gestion et au suivi des vaccinations contre le coronavirus SARS-CoV-2 (demande d'avis n°20020767) ; La collecte de données dans le cadre de la vaccination contre la Covid-19 : quelles garanties pour les personnes ? (CNIL, 30 déc. 2020) ; TousAntiCovid : le Gouvernement s'adresse aux abonnés des opérateurs téléphoniques (CNIL, 30 nov. 2020) ; Coronavirus (COVID-19) : les rappels de la CNIL sur la collecte de données personnelles par les employeurs (CNIL, 23 sept. 2020) ; COVID-19 et pratiques sportives : quel cadre juridique pour la collecte de données de santé ? (CNIL, 14 oct. 2020) ; « TousAntiCovid » : la CNIL revient sur l'évolution de l'application « StopCovid » (CNIL, 23 oct. 2020) ; Application TousAntiCovid (site du gouvernement)

La CNIL publie un livre blanc relatif aux enjeux des assistants vocaux

« A votre écoute » - Livre blanc, CNIL, 7 septembre 2020

Ce qu'il faut retenir :

La CNIL publie « A votre écoute », un livre blanc relatif aux enjeux éthiques, techniques et juridiques des assistants vocaux à destination des professionnels comme des utilisateurs.

Pour approfondir :

Face à la prolifération des assistants vocaux dans les objets du quotidien, la Commission Nationale de l'Informatique et des Libertés (CNIL) publie « A votre écoute », un livre blanc relatif à leurs enjeux éthiques, techniques et juridiques afin d'accompagner ceux qui les développent, les façonnent, les déploient ou encore les utilisent. En parallèle à la publication de ce livre blanc, la CNIL a mis à jour de nombreux contenus d'accompagnement pour appréhender les dispositifs d'assistance vocale.

Un assistant vocal est « *un ensemble de ressources logicielles permettant de réaliser les traitements de la voix et du langage afin de répondre à la requête d'un utilisateur* ». Ce dispositif repose sur une capacité de dialogue avec un utilisateur en langage naturel permettant de lui offrir un service suite à une requête vocale.

Afin d'appréhender cette technologie, la CNIL définit cinq grandes étapes du fonctionnement d'un assistant vocal :

- L'assistant vocal s'éveille à la prononciation par l'utilisateur d'un mot clé prédéfini ;
- L'assistant vocal reconnait l'utilisateur (optionnel) ;
- L'utilisateur énonce sa requête ;
- La requête orale de l'utilisateur est automatique retranscrite en texte puis interprétée par l'assistant vocal qui donne une réponse adaptée ;
- L'assistant vocal repasse en « veille ».

La question de l'encadrement de la protection des données à caractère personnel constitue un élément clé pour ceux souhaitant déployer des assistants vocaux ainsi que pour ceux qui les utilisent. Le livre blanc propose des cas d'usage pour étudier la manière dont la réglementation relative à la protection des données trouve à s'appliquer.

Pour l'ensemble de ces cas d'usage, la CNIL rappelle les principales étapes à réaliser pour garantir la conformité au RGPD du dispositif envisagé. Après avoir déterminé la nature des informations traitées, la CNIL préconise de définir le traitement, son responsable de traitement et sa base légale (1), de caractériser les données traitées et leurs durées de conservation (2), de procéder à l'information des personnes concernées et à la garantie de leur droit (3) et enfin, de mettre en place des mesures de sécurité adaptées (4).

Dans son livre blanc, la CNIL évoque le cas de l'utilisation « des fonctions de base » d'un assistant vocal. Il s'agit de l'usage le plus répandu de l'assistant vocal dit « généraliste » qui vise à répondre aux besoins fonctionnels récurrents des utilisateurs.

Dans cette hypothèse, le concepteur de l'assistant vocal est le responsable de traitement dans la mesure où il détermine les finalités du traitement (la fourniture du service d'assistance vocale) et les moyens du traitement (l'assistant vocal relié à un compte utilisateur). Pour aiguiller le responsable de traitement, la CNIL indique que ce dernier peut fonder son traitement sur l'exécution d'un contrat auquel l'utilisateur est partie. Concernant la durée de conservation des données traitées, la CNIL rappelle que les données ne peuvent être conservées au-delà de la durée nécessaire à la fourniture du service concerné, étant entendu que les données collectées ne doivent pas être traitées pour une autre finalité que celle de la fourniture dudit service.

D'autre part, concernant l'information des personnes concernées, la CNIL met en lumière le recours à une information vocale qui peut s'avérer pertinente pour les utilisateurs dans l'impossibilité d'utiliser un support écrit.

De surcroit, compte tenu des risques liés à l'utilisation d'un assistant vocal (enregistrement de conservations intimes après l'activation inopinée de l'assistant vocal suite à la prononciation du mot d'activation ou d'un mot s'en rapprochant), la CNIL préconise la mise en place de mesures de sécurité renforcées pour protéger l'espace intime des utilisateurs et des tiers. Dans ce contexte, il apparait que la mise en œuvre d'une analyse d'impact peut constituer un prérequis au déploiement d'un dispositif d'assistance vocale et il convient de systématiquement vérifier les critères de l'analyse d'impact.

Outre ces dispositifs génériques, notons que certains mettent en œuvre un mécanisme de reconnaissance de l'utilisateur. En effet, certains assistants vocaux proposent à l'utilisateur une option lui permettant de s'identifier à partir de sa voix afin d'accéder à un service. Dans ce contexte, il convient de souligner que la mise en œuvre d'un dispositif ayant pour but de reconnaitre un individu à partir des caractéristiques vocales constitue un traitement de données biométriques. Cette particularité s'illustre notamment au moment de l'étape de reconnaissance par l'assistant vocal de l'utilisateur.

Rappelons que les données biométriques sont définies par 4.14 du RGPD comme « *les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettant ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques* ». Si l'article 9 du RGPD interdit par principe les traitements de données biométriques aux fins d'identifier une personne physique de manière unique, ces derniers sont admis dans certains cas et notamment en cas de consentement explicite des utilisateurs.
Enfin, il est à noter que livre blanc met en avant les divergences d'opinion liées à l'utilisation d'assistants vocaux. Si les personnes disposants d'assistants vocaux revendiquent leur caractère innovant, celles n'en disposant pas pointent leur inutilité et font part de leurs concernant la protection de leurs données à caractère personnel. Force est de constater que parmi les individus ayant utilisé ces dispositifs, 46% des personnes interrogées ont déjà procédé un paramétrage de leur assistant vocal en vérifiant sa configuration ou encore en supprimant l'historique des commandes vocales passées. Cette information constitue un indice éloquent de l'essor de la sensibilisation des utilisateurs à la protection de leurs données à caractère personnel.

A rapprocher : « A votre écoute », Exploration des enjeux éthiques, techniques et juridiques des assistants vocaux, Livre blanc, CNIL, 7 septembre 2020

La CJUE s'oppose à la conservation généralisée et indifférenciée des données de connexion

Affaires C-623/17, C-511/18, C-512/18 et C-520/18

Ce qu'il faut retenir :

La CJUE s'oppose à une réglementation nationale prévoyant la conservation généralisée et indifférenciée des données de connexion à des fins de sauvegarde de la sécurité nationale et de lutte contre la criminalité.

Pour approfondir :

Aux termes de plusieurs arrêts du 6 octobre 2020, la Cour de Justice de l'Union Européenne (ci-après la « CJUE ») s'oppose à la conservation généralisée et indifférenciée des données de connexion par les fournisseurs de services de communications électroniques et à leur transmission aux autorités nationales de sécurité et de renseignement.

Il est à noter que ces arrêts se positionnent dans la lignée d'un arrêt remarqué du 21 décembre 2016, l'arrêt « Tel2 Sverige et Watson », aux termes duquel la CJUE avait estimé que les Etats membres ne pouvaient imposer aux fournisseurs de services de communications électroniques une obligation de conservation généralisée et indifférenciée des données dites de connexion.

A titre liminaire, il convient de préciser que les données visées recouvrent « *celles qui sont nécessaires pour retrouver la source d'une communication et la destination de celle-ci, déterminer la date, l'heure, la durée et le type de la communication, identifier le matériel de communication utilisé ainsi que localiser les équipements terminaux et les communications, données au nombre desquelles figurent, notamment, le nom et l'adresse de l'utilisateur, les numéros de téléphone de l'appelant et de l'appelé ainsi que l'adresse IP pour les services Internet* ». La CJUE rappelle dans ce contexte que sont exclus les contenus desdites communications.

La CJUE se fonde ainsi sur la directive 2002/58/CE du 12 juillet 2002 dite « *Vie privée et communications électroniques* » ou « *e-Privacy* » (ci-après la « Directive ») et rappelle que ce texte a pour dessein d'assurer un niveau de protection suffisant des droits fondamentaux dans le secteur des communications électroniques notamment eu égard « *à la capacité accrue de stockage et de traitement automatisés de données relatives aux abonnés et aux utilisateurs*. »

L'article 5 de la Directive consacre en effet le principe de confidentialité tant des communications électroniques que des données relatives au trafic y afférentes, et l'interdiction à toute autre personne autre que les utilisateurs de stocker ces communications et données, sans leur consentement.

Toutefois, cette même Directive offre par son article 15 la possibilité aux Etats membres de limiter la portée de cette interdiction sous certaines conditions. En effet, est consacrée une exception au principe lorsque la mesure législative poursuivie par l'Etat membre constitue une mesure « *nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques* ».

Dans ce contexte, la CJUE réaffirme le caractère disproportionné d'une conservation généralisée et indifférenciée de données relatives au trafic et à la localisation et précise que ces opérations ne peuvent être effectuées que dans certaines hypothèses définies strictement, aux fins notamment de sauvegarde de la sécurité nationale et de lutte contre la criminalité.

Dans une démarche pédagogique, la CJUE rappelle que la Directive s'oppose aux mesures législatives imposant aux fournisseurs de services de communications électroniques, tant la conservation généralisée et indifférenciée des données relatives au trafic et à la localisation à titre préventif, que la transmission généralisée et indifférenciée de ces données aux autorités compétentes.

La Haute juridiction précise cependant que dans des situations où l'Etat membre fait face à une menace grave, réelle, actuelle ou prévisible, pour la sécurité nationale, une mesure législative peut prévoir une injonction de conservation généralisée et indifférenciée des données de connexion aux fournisseurs de services de communication électroniques.

Dès lors, de telles mesures législatives sont envisageables sous réserve de soumettre la décision d'injonction à un contrôle effectif (juridictionnel notamment ou par une autorité indépendante dont la décision est dotée d'un effet contraignant) et de la circonscrire à une période temporellement limitée au strict nécessaire. Dans ces mêmes conditions, la CJUE estime qu'une analyse automatisée des données en cause de l'ensemble des utilisateurs est possible.

En outre, la CJUE estime que des mesures législatives peuvent permettre la conservation ciblée, temporellement limitée au strict nécessaire, des données de connexion, sous réserve que cette conservation soit délimitée sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique.

La CJUE ajoute que des mesures législatives peuvent prévoir le recueil en temps réel des données de connexion limitées au strict nécessaire et à la condition que ces opérations soient limitées aux personnes à l'égard desquelles il existe une raison valable de soupçonner qu'elles sont impliquées dans des activités de terrorisme et sous réserve de les encadrer par un contrôle effectif.

Enfin, il semble opportun de relever que la CJUE ne s'oppose pas à une mesure législative permettant la conservation rapide des données de connexion au-delà des délais légaux de conservation aux fins d'élucidation d'infractions pénales graves ou d'atteintes à la sécurité nationale, lorsque lesdites infractions ou atteintes ont déjà été constatées ou que leur existence peut être raisonnablement soupçonnée.

En illustrant ainsi les exceptions prévues par l'article 15 de la Directive, la CJUE met ainsi un frein aux incertitudes liées à son interprétation.

A rapprocher : Affaire C-623/17 *Privacy International* ; Affaires C-511/18 *La Quadrature du Net e.a.* et C-512/18, *French Data Network e.a.*, ainsi que C-520/18 *Ordre des barreaux francophones et germanophone e.a* ; CJUE, Communiqué de presse n°123/20 - Arrêts dans l'affaire C-623/17 *Privacy International* et dans les affaires jointes C-511/18 *La Quadrature du Net e.a.* et C-512/18, *French Data Network e.a.*, ainsi que C-520/18 *Ordre des barreaux francophones et germanophone e.a.*

PROPRIÉTÉ INTELLECTUELLE

Diffusion de vidéo eSport et droits attachés

Ce qu'il faut retenir :

La diffusion d'une vidéo sur le eSport est un sujet complexe qui n'est pas encore réglementé. Pourtant, cette situation mériterait une clarification étant donné les intérêts opposés qui sont en jeu : streamer, joueur, éditeur du jeu et plateforme. Ces différents acteurs ont des droits à faire valoir et seule la pratique pour le moment régit cette situation.

Pour approfondir :

Le eSport est un secteur en plein développement et certains pensent que son succès sera comparable à la retransmission des matchs de NBA ou de football d'ici quelques temps. Même la pandémie et les confinements ne l'ont pas affecté, bien au contraire (***ESport : enjeux juridiques d'un secteur qui ne connait pas la crise*, Lettre du Numérique, 16 sept. 2020**).

Pourtant, le cadre juridique applicable à la diffusion de ces contenus reste encore aujourd'hui assez flou. Comme souvent, la technique est en avance sur le législateur.

Aucun texte juridique, ni en France, ni à l'étranger, n'encadre cette situation pourtant assez complexe.
L'une des difficultés de la diffusion du eSport d'un point de vue juridique est le nombre d'acteurs considéré et les droits qui leur sont attachés :

- Le streamer ;
- Le joueur ;
- L'éditeur du jeu vidéo ;
- La plateforme de vidéo.

Les droits d'auteur du streamer

Le streamer est la personne physique qui réalise la vidéo et qui la met en ligne sur une plateforme comme Twitch.

Étant donné qu'il réalise la vidéo, qu'il commente par exemple des actions de jeux, il est titulaire de droits d'auteur sur ce contenu. Cependant, au moment où il met en ligne sa vidéo sur une plateforme, le streamer concède à tout le moins une licence à la plateforme pour que sa vidéo puisse être diffusée par la plateforme.

Les contours de cette licence sont définis généralement par les conditions générales de licences acceptées par le streamer au moment où il met en ligne la vidéo.

Le droit à l'image du joueur

Le joueur dont la partie est diffusée en ligne est lui aussi potentiellement titulaire de droits qui doivent être réglés.

Son droit à l'image lorsqu'il est filmé en jouant est une question à traiter.

Le streamer peut s'être filmé lui-même en train de jouer dans ce cas il est à la fois streamer et joueur ce qui limite les problématiques. En revanche, lorsque ce sont deux personnes différentes, un contrat peut être conclu entre les deux personnes, pour régir les droits de chacun, car le joueur est également titulaire de droits.

Les droits d'auteur de l'éditeur du jeu

Les jeux vidéo sont protégés par le droit d'auteur en tant qu'œuvre de l'esprit. Plus spécifiquement, un jeu vidéo est œuvre collective, c'est-à-dire une œuvre divulguée sous le nom d'une personne morale : l'éditeur.

En tant que telle, l'éditeur du jeu vidéo est titulaire de droits d'auteur sur le jeu vidéo, et sur ses composantes : musique, son, vidéo, etc.

Ainsi, lorsqu'un joueur joue à un jeu vidéo, il accepte une licence d'utilisation rédigée par l'éditeur du jeu vidéo et qui lui confère uniquement un droit d'utilisation privé, à des fins non commerciales.

Aussi, la diffusion d'une partie d'un jeu vidéo ne semble pas rentrer dans le cadre de cette licence, car à des fins commerciales. Par conséquent, une telle diffusion doit par principe être soumise à l'autorisation préalable de l'éditeur du jeu vidéo concerné, étant donné que la diffusion constitue une représentation, prérogative primordiale du droit d'auteur.

Un éditeur pourrait donc interdire la diffusion de vidéos tirées de ses jeux vidéo sur une plateforme, en l'absence de contrat conclu avec la plateforme ou le streamer.

Les droits d'auteurs cédés à la plateforme

La plateforme qui héberge la vidéo est également titulaire de droits qui lui sont cédés ou licenciés par le streamer en acceptant les conditions générales d'utilisation, préalable nécessaire à la diffusion d'une vidéo par un utilisateur.

Ainsi, la plateforme dispose de droits sur les contenus également qui doivent faire l'objet d'une appréciation.

Conclusion

On voit donc que la diffusion de vidéo de eSport constitue une situation complexe qui intéresse de nombreux acteurs différents, ayant des centres d'intérêts également très différents.

Pourtant, en pratique, il y a peu d'actions en justice intentées par des éditeurs de jeu vidéo sur le fondement du droit d'auteur, alors que de telles actions pourraient prospérer. Les éditeurs ont constaté que la diffusion d'images de leurs jeux par le eSport leur fournissait une publicité particulièrement intéressante et à prix réduit.

Ainsi, les éditeurs ont mis en balance leurs droits d'auteur avec les revenus générés par la diffusion de eSport et ont choisi d'accepter tacitement cette diffusion au regard des bénéfices générés.

On voit donc ici que la pratique a dépassé les enjeux juridiques concernés. On peut rapprocher cette adaptation de ce qui s'est passé entre Youtube et les éditeurs de musique il y a maintenant plusieurs années.

A rapprocher : *ESport : enjeux juridiques d'un secteur qui ne connait pas la crise*, Lettre du Numérique, 16 sept. 2020

SERVICES NUMÉRIQUES

Le Règlement internet ouvert consacré par la CJUE
CJUE, 15 sept. 2020, Aff. jointes. C-807/18 et C-39/19

Ce qu'il faut retenir :

La Cour de Justice de l'Union Européenne (CJUE) a consacré, dans son arrêt du 15 septembre dernier, la neutralité du net alors que la tendance outre atlantique est de vouloir remettre en cause cette neutralité du net. Pour commenter cette décision, il nous faut rappeler ce qu'est la neutralité du net (I) pour ensuite présenter la portée de cette décision de la CJUE qui pour la première fois devait se prononcer sur le règlement de l'internet ouvert adopté en novembre 2015 par le Parlement européen et le Conseil de l'Union européenne (II).

Pour approfondir :

I. La définition de l'internet ouvert

La neutralité du net est inscrite dans le postulat de départ du web : garantir l'égalité de traitement et d'acheminement de tous les flux d'information sur internet, quel que soit leur émetteur ou leur destinataire. En fait, il s'agit d'un principe simple de non-discrimination : tout le monde doit avoir un égal accès à Internet et aucun contenu (vidéo, site web, ...) ne doit bénéficier d'un traitement préférentiel et s'afficher plus vite que les autres.

La neutralité du net (ou « *network neutrality* ») a été conceptualisée en 2003 par le juriste américain Tim WU, dans la revue ***Journal of Telecommunications and High Technology Law***. À l'époque, ce concept est le reflet des valeurs d'ouverture qui ont conduit à l'émergence et au succès d'internet puisqu'il recouvre l'idée que les flux d'informations ne peuvent être ni bloqués, ni dégradés, ni favorisés par les opérateurs de télécommunications.

Alors que les équipements techniques du réseau Internet rendent possible depuis les années 2000 une gestion sélective, voire discriminatoire, du trafic, d'importants débats politiques ont lieu depuis le début de la décennie 2010 pour décider si ce principe doit être garanti par la législation.

Aujourd'hui, la protection de la neutralité du net répond à une ambition démocratique : internet est devenu une « infrastructure essentielle » dans l'exercice des libertés, un bien commun sur lequel les États doivent veiller au profit de tous les utilisateurs.

Avec la crise sanitaire du Covid-19, la neutralité du net a trouvé tout son sens et a illustré le besoin et la nécessité de l'utilisateur final à rester connecté à son environnement professionnel, personnel et culturel depuis son domicile.

Question d'autant plus d'actualité que **cette neutralité du net a été remise en cause par les Etats-Unis fin 2017** engendrant ainsi une différence d'approche économique pour l'accès à un réseau qui depuis sa conception se voulait mondial engendrant une dichotomie entre les deux continents.

Les États européens avaient anticipé cette éventuelle remise en cause de principe fondateur de l'internet **en adoptant en 2015 un Règlement** qui avait pour motifs :

> *« (..) d'adopter, au niveau de l'Union, des règles communes pour garantir le caractère ouvert de l'internet et éviter une fragmentation du marché intérieur due aux mesures prises individuellement par les États membres. »* (ci-après : le Règlement de l'internet ouvert)

C'est cet écueil de fragmentation du marché intérieur que la CJUE a voulu éviter en consacrant l'accès à l'internet ouvert dans l'espace de l'Union Européenne par son arrêt du 15 septembre dernier.

II. L'arrêt de la CJUE renforce le Règlement de l'internet ouvert

Fin 2018 et début 2019, la Cour de Budapest a saisi la CJUE de questions préjudicielles portant sur des offres de « *zero-rating* » proposées par l'opérateur national TELENOR (*Les offres de zero-rating sont des offres où le volume de données consommées par une ou plusieurs applications particulières n'est pas décompté du forfait data du client final*).

Ainsi les offres du fournisseur d'accès hongrois avaient pour particularité de ne pas décompter le trafic de données lors de l'accès à certains sites ou services, comme Facebook, Facebook Messenger, Instagram, Twitter, Viber ou WhatsApp, ou à des sites de streaming musical, comme Apple Music, Deezer, Spotify et Tidal. Une fois épuisé le volume de données pour lequel ils avaient payé, les utilisateurs pouvaient ainsi continuer à accéder aux services en question, alors que le reste de leur navigation était soumis à des mesures de blocage ou de ralentissement.

Les demandes de décision préjudicielle à la CJUE portaient pour la première fois sur l'interprétation du **Règlement de l'internet ouvert**, établissant des mesures relatives à l'accès à un internet ouvert et notamment à son l'article 3 qui protège la neutralité du net, en reconnaissant notamment :

- **le droit des utilisateurs** *« d'accéder aux informations et aux contenus et de les diffuser, d'utiliser et de fournir des applications et des services et d'utiliser les équipements terminaux de leur choix, quel que soit le lieu où se trouve l'utilisateur final ou le fournisseur, et quels que soient le lieu, l'origine ou la destination de l'information, du contenu, de l'application ou du service, par l'intermédiaire de leur service d'accès à l'internet »* (Article 3 §2) ;

- **le devoir des fournisseurs d'accès internet de traiter** *« tout le trafic de façon égale et sans discrimination, restriction ou interférence, quels que soient l'expéditeur et le destinataire, les contenus consultés ou diffusés, les applications ou les services utilisés ou fournis ou les équipements terminaux utilisés »* (Article 3 §3) .

Ce sont sur ces deux dispositions de l'article 3 du Règlement de l'internet ouvert que la CJUE a considéré pour l'utilisateur final que :

> *« il convient de relever, tout d'abord, qu'un accord par lequel un client donné souscrit à une offre groupée impliquant que, une fois épuisée le volume de données compris dans le forfait acheté, ce client ne dispose d'un accès sans restriction qu'à certaines applications et à certains services relevant d'un 'tarif nul', est susceptible d'emporter une limitation de l'exercice... »*

...des droits de cet utilisateur final, dans des conditions telles que :

> *« la compatibilité d'un tel accord avec l'art. 3, § 2, du Règlement doit être évaluée au cas par cas ».*

La juridiction européenne de préciser ensuite à l'égard des Fournisseurs d'Accès à l'Internet :

> *« de telles offres groupées [...] sont, eu égard à l'incidence cumulée des accords auxquels elles peuvent conduire, de nature à amplifier l'utilisation de certaines applications et de certains services spécifiques, à savoir celles et ceux qui peuvent être utilisés sans restrictions à un 'tarif nul' une fois épuisé le volume de données compris dans le forfait acheté par les clients, et, corrélativement, à raréfier l'utilisation des autres applications et des autres services disponibles ».*

Et de considérer, en conséquence, que :

> « *il en résulte que la conclusion de tels accords sur une partie significative du marché est susceptible de limiter l'exercice des droits des utilisateurs finals, au sens de l'art. 3, § 2, du Règlement* »

La Cour de conclure pour consacrer la neutralité du net :

> *« dit pour droit » que l'art. 3 du Règlement (UE) 2015/2120 « doit être interprété en ce sens que des offres groupées mises en œuvre par un fournisseur de services d'accès à Internet au moyen d'accords conclus avec des utilisateurs finals, aux termes desquelles ces derniers peuvent acheter un forfait leur donnant le droit d'utiliser sans restrictions un volume de données déterminé, sans que soit décomptée l'utilisation de certaines application et de certains services spécifiques relevant d'un 'tarif nul', et, une fois épuisé ce volume de données, peuvent continuer à utiliser sans restrictions ces applications et ces services spécifiques, pendant que des mesures de blocage ou de ralentissement de trafic sont appliquées aux autres applications et services disponibles : sont incompatibles avec le § 2 de cet art., lu conjointement avec le § 1 de celui-ci, dès lors que ces offres groupées, ces accords et ces mesures de blocage ou de ralentissement limitent l'exercice des droits des utilisateurs finals, et sont incompatibles avec le § 3 dudit art.* ***dès lors que lesdites mesures de blocage ou de ralentissement sont fondées sur des considérations commerciales*** » (nous soulignons).

Au regard de cette décision qui consacre la neutralité du net et en même temps face à l'incertitude engendrée par la décision des autorités fédérales des États-Unis qui ont remis en cause la neutralité du net, il serait utile de relancer en France la proposition de François de Rugy qui voulait en janvier 2018 lorsqu'il était Président de l'Assemblée Nationale « *reconnaître le numérique comme un droit fondamental* » et faire figurer dans la Constitution *« un droit d'accès à l'information publique »* et d'inscrire la neutralité du net dans le texte de la Constitution pour lui donner le statut de norme supérieure dans le droit français.

A rapprocher : CJUE, 15 sept. 2020, Aff. jointes. C-807/18 et C-39/19 ; Règlement (UE) 2015/2120 du Parlement Européen et du Conseil du 25 novembre 2015 ; Règlement (UE) N°531/2012 du Parlement Européen et du Conseil du 13 juin 2012 ; Directive 2002/22/CE du Parlement Européen et du Conseil du 7 mars 2002 ; ***Network Neutrality, Broadband Discrimination (Journal of Telecommunications and High Technology Law, Vol. 2, p. 141, 2003)***

INTERNATIONAL

Loi sur la protection des renseignements personnels en Chine
Projet de loi soumis le 13 octobre 2020

Ce qu'il faut retenir :

Le projet de la première loi spéciale chinoise sur la protection des renseignements personnels (« Projet ») a été soumis le 13 octobre à la session bimensuelle du Comité permanent de l'Assemblée populaire nationale, la plus haute législature du pays, pour un premier examen.

Pour approfondir :

Les législateurs chinois ont commencé mardi à examiner le Projet afin de réglementer davantage la collecte et l'utilisation des données personnelles.

Le Projet a été publié afin de recueillir l'avis public du 13 octobre au 19 novembre 2020.

Conformément au Projet, les propriétaires des informations personnelles devront être pleinement informés du traitement desdites informations, notamment leur collecte, leur stockage et leur utilisation, et leur autorisation devra être sollicitée.

Le Projet dispose que les propriétaires d'informations personnelles ont le droit de retirer leur autorisation de collecte, de stockage, d'utilisation, de traitement, de transmission et de divulgation de ces informations.

De même, a indiqué le Projet, si des individus ou des organisations ont besoin d'actualiser les informations personnelles des utilisateurs de leurs produits ou services, ils devront demander à nouveau l'autorisation des utilisateurs.

Le Projet est le fruit du fait que, durant ces dernières années, la Chine a intensifié ses efforts pour protéger les informations personnelles par le biais du Code civil, de la loi sur la cybersécurité et de la loi sur le commerce électronique, mais, il est difficile de répondre aux demandes croissantes des gens à l'ère d'un Internet en plein développement.

Le Projet vise à renforcer la protection des informations personnelles et à rendre les recours juridiques plus pratiques et systémiques.
Le consentement personnel doit être obtenu sur la prémisse d'une notification préalable pour le traitement des renseignements personnels et les individus ont le droit de retirer leur consentement, indique le projet, ajoutant que lorsque des questions importantes sont modifiées, le consentement personnel sera obtenu à nouveau.

Aucun produit ou service ne peut être refusé sur la base d'un désaccord personnel.

A rapprocher : Texte du projet

La loi restrictive des exportations technologiques des entreprises chinoises
Entrée en vigueur le 1er décembre 2020

Ce qu'il faut retenir :

La loi restrictive des exportations technologiques des entreprises chinoises (« Loi » - 出口管制法) entrera en vigueur le 1er décembre 2020 et concernera effectivement le contrôle des exportations technologiques des entreprises chinoises à l'étranger.

Pour approfondir :

La Chine présente la Loi comme une question de sécurité nationale pour le pays.

La Loi a été adoptée le 17 octobre 2020 lors de la 13ème Assemblée populaire nationale et vise à empêcher les entreprises basées en Chine de réaliser des exportations ou des transactions technologiques sans avoir obtenu une licence du gouvernement.

Même si les détails sont rares, l'Assemblée populaire nationale a déclaré que la Loi comprend une disposition d'interdiction réciproque, couvre les biens à usage civil et militaire, et inclut les technologies et les données les concernant.

Cette Loi permet à la Chine de bloquer les exportations technologiques, juste au moment où ByteDance a besoin de céder une partie de TikTok à une entreprise américaine.

Alors l'application TikTok peut-elle être vendue sans ses algorithmes ? C'est toute la question. La réponse semble plutôt s'orienter vers la négative. Les algorithmes du réseau social déterminent quelles vidéos les internautes vont voir et sont considérés comme la sauce secrète de TikTok. Il semble donc difficile d'imaginer que le réseau social puisse être vendu sans ces technologies.

Avec cette Loi, la Chine pourrait également décider de s'en prendre aux autres nations qui ont décidé de bannir Huawei ou du moins de trouver un prétexte pour faire basculer leurs infrastructures 5G vers les fournisseurs Nokia et Ericsson. C'est notamment le cas de l'Australie.

Certains analystes du marché chinois estiment que l'adoption de la Loi rendra plus difficile la mondialisation des entreprises chinoises. Elles auront en quelques sortes une excuse pour ne pas vendre à l'étranger, mais cela signifie également qu'il leur sera très difficile de devenir des acteurs mondiaux.

A rapprocher : Texte de la Loi

Cryptomonnaie vs. Monnaie digitale de banque centrale
Actualités

Ce qu'il faut retenir :

Si les cryptomonnaies (du type Bitcoin, Bitcoin Cash, Ether, Litecoin) se sont développées au cours des dernières années, l'année 2020 a vu apparaitre de nouvelles monnaies digitales actuellement testées par certaines banques centrales.

C'est ainsi que la Chine teste depuis juillet 2020 sa monnaie digitale de banque centrale dans 4 villes (Shenzhen, Chengdu, Suzhou et Xiong'an).

Côté européen, certaines banques centrales nationales dont la Suède, ont également déjà lancé leurs propres projets pilotes de monnaie digitale de banque centrale.

Pour mémoire :

Les monnaies digitales de banque centrale sont de nouvelles formes de monnaie électronique directement émises par la banque centrale d'un Etat souverain.

Selon une **étude menée en 2019 par la Banque des règlements internationaux** (BRI) auprès de 66 banques centrales, 80 % d'entre elles travaillent sur le sujet de la monnaie numérique. 10 % d'entre elles ont développé un projet pilote.

Plusieurs monnaies digitales de banque centrale sont donc susceptibles de voir le jour au cours des années à venir, et cela pour de nombreuses raisons : gérer la disparition des espèces, contrer la menace que font peser les cryptomonnaies privées (Libra, Bitcoin, Ehtereum, etc) sur la souveraineté, ou encore limiter le pouvoir de marché des prestataires de paiements privés.

En Chine, la Banque centrale chinoise (Banque populaire de la Chine) a entamé des tests de sa monnaie digitale en juillet 2020.

En Europe, la Banque de France a annoncé début décembre 2019 vouloir tester sa propre monnaie digitale ; la Banque centrale suédoise a déjà lancé un projet pilote depuis le mois de février 2020 sur sa monnaie digitale de banque centrale.

Quant à la Banque nationale suisse (BNS) qui travaille également sur la monnaie numérique, celle-ci a annoncé le 3 décembre 2020 avoir réussi une étude de faisabilité dans ce domaine, en collaboration avec la BRI et l'opérateur de la bourse suisse, SIX.

Pour approfondir :

En 2021, les 346 millions de clients de PayPal pourront utiliser les cryptos et bitcoin dans les 26 millions de marchands de son réseau devenant ainsi un instrument de paiement.

Selon l'article L.111-1 du Code monétaire et financier, « ***la monnaie de la France est l'euro*** ». C'est donc la **seule monnaie ayant cours légal** en France. Si un professionnel a le droit de refuser de se faire payer en cryptomonnaie, rien ne l'empêche non plus de les accepter...

Définition

- Cryptomonnaie

Une cryptomonnaie est une devise électronique, ou virtuelle, car elle n'a aucune forme physique.

C'est une monnaie émise de pair à pair, s'échange sur un système informatique décentralisé, ou blockchain, tenu à jour en permanence et (réputé) inviolable, sans nécessité de banque centrale.

Le code source d'une blockchain se base sur les principes de la cryptographie pour valider les transactions et émettre la monnaie elle-même.

Le cadre légal applicable aux cryptomonnaies nécessite de les qualifier juridiquement : il faut pour cela distinguer la monnaie ayant cours légal de la cryptomonnaie (sans cours légal).

En France, les cryptomonnaies sont définies et encadrées par la Loi n°2018-1317 du 28 décembre 2018 de finances pour 2019 ainsi que par le code monétaire et financier.

L'article L.315-1 du Code monétaire et financier définit la monnaie électronique comme : « *une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement définies à l'article L.133-3 et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique* ».

L'article L.54-10-1 du Code monétaire et financier définit les actifs numériques, qui comprennent les cryptomonnaies, comme : « *toute représentation numérique d'une valeur qui n'est pas émise ou garantie par une banque centrale ou par une autorité publique, qui n'est pas nécessairement attachée à une monnaie ayant cours légal et qui ne possède pas le statut juridique d'une monnaie, mais qui est acceptée par des personnes physiques ou morales comme un moyen d'échange et qui peut être transférée, stockée ou échangée électroniquement* ».

- Monnaie digitale de banque centrale

Une monnaie digitale de banque centrale (« **MDBC** ») **est un actif numérique émis par la seule banque centrale**, s'échangeant au pair avec les billets et les réserves, disponible en permanence et dans des transactions de pair-à-pair et circulant sur des supports numériques au moins en partie différents de ceux utilisés de nos jours.

La MDBC est la forme numérique de l'argent fiduciaire, c'est-à-dire une monnaie établie comme monnaie par la réglementation gouvernementale, l'autorité monétaire ou la loi.

Le concept actuel a été directement inspiré par le Bitcoin, mais c'est différent des cryptomonnaies qui ne sont pas émises par l'État.

Les implémentations proposées peuvent même ne pas utiliser n'importe quel type de registre distribué.

Les MDBC sont testées dans un nombre croissant de pays, notamment de la Suède à la Chine en passant par la France.

Exemple de la Chine

Le programme pilote de la MDBC chinoise est réalisé avec l'appui des 4 grandes banques d'Etat (ICBC, Bank of China, Agriculture Bank of China, et China Construction Bank).

Les premiers tests de cette monnaie digitale souveraine ont été annoncés officiellement le 8 juillet 2020 par le géant du VTC (Voiture de Transport avec Chauffeur) chinois Didi Chuxing (équivalent d'Uber en Chine) et la Banque centrale chinoise.

Par ailleurs, certains fonctionnaires chinois ont aussi commencé à recevoir une partie de leur salaire dans cette monnaie virtuelle.

Plus récemment, un test à grande échelle a été mené en Chine du 11 (veille d'un jour de soldes) au 27 décembre 2020 dans 10.000 boutiques de la ville de Suzhou (à l'ouest de Shanghai) où les clients ont pu payer en *e-yuan (*ou *yuan numérique* ou encore *renminbi numérique)*.

L'objectif du gouvernement chinois est de fournir un moyen de paiement plus sécurisé que les espèces ou les paiements électroniques existants.

La MDBC chinoise ne consiste pas en une cryptomonnaie décentralisée de type Bitcoin. Au contraire, cette monnaie est émise de manière traditionnelle par la Banque centrale chinoise, sous une forme purement numérique.

Comme un moyen de paiement digital, rien de très nouveau à première vue pour **des centaines de millions de Chinois qui utilisent chaque jour les solutions de paiement via des applications mobiles comme Alipay ou WeChat Pay, qui représentent déjà 16% du PIB en 2019**.

Les cryptomonnaies, Bitcoin et Ethereum en tête, y ont rencontré un certain succès avant que leur usage ne soit restreint par les autorités chinoises.

Dans ces deux cas des paiements virtuels, les transactions échappent en partie au contrôle du gouvernement chinois, ce qui explique également sa volonté de mettre en place une MDBC chinoise.

La MDBC chinoise est aujourd'hui connu sous les initiales « **DCEP** » pour « Digital currency/electronic payment ».

La MDBC chinoise devrait permettre également à la Banque centrale chinoise de mieux contrôler le marché des paiements, qui est actuellement dominé par des entreprises du secteur privé telles que Alibaba et Tencent.

La Banque centrale chinoise met en avant que la MDBC chinoise a un cours légal et ne peut être refusée, contrairement aux autres cryptomonnaies que la Chine a toujours considérées comme des produits de spéculation ou un moyen illégal de sortir des capitaux de Chine.

Mark Carney, ancien gouverneur de la Banque centrale du Canada et, depuis 2013, gouverneur de la Banque centrale d'Angleterre, estime que cette voie technologique pourrait être une solution pour contrecarrer la puissance du US dollar. À terme, la MDBC chinoise pourrait constituer une alternative au US dollar pour les paiements internationaux.

Des analystes américains redoutent également que l'Iran et d'autres États ne l'utilisent pour échapper aux sanctions de Washington.

Un test à plus grande échelle devrait avoir lieu lors des Jeux olympiques d'hiver de Pékin, en 2022.

Exemple de l'Europe

En Europe, **la Banque Centrale Européenne (« BCE ») estime qu'aucun "business case" ne justifie pour l'instant le lancement de sa propre monnaie numérique**. Néanmoins cela ne l'empêche pas d'explorer cette piste qui pourrait s'avérer prometteuse.

La BCE et les banques centrales nationales de la zone euro, soucieuses que la monnaie unique continue de répondre pleinement aux besoins des Européens, examinent actuellement les avantages et les risques d'un tel projet.

La preuve : certaines banques centrales nationales ont déjà lancé leurs propres projets pilotes.

- **La France**

Début décembre 2019, la Banque de France avait annoncé vouloir lancer sa propre MDBC pour améliorer l'efficacité du système financier en fluidifiant les transactions.

L'institut monétaire a d'ailleurs lancé un appel à projet le 24 avril 2020 pour « *identifier des cas concrets d'intégration d'une monnaie digitale de banque centrale dans des procédures innovantes d'échange et de règlement d'actifs financiers tokénisés* ».

Cette annonce n'est pas une surprise.

Bruno Le Maire, Ministre de l'Economie, avait en effet émis une idée similaire début septembre 2019, lors de l'ouverture d'une conférence de l'Organisation de coopération et de développement économiques (« OCDE ») sur la blockchain. Il admettait alors qu'une MDBC pourrait résoudre « *certaines difficultés en matière de transaction financière* », comme la modulation des coûts de transactions différents en fonction des Etats, en particulier en Europe.

Le projet prend également en compte la dimension européenne que pourrait revêtir la nouvelle MDBC dans une perspective à long terme.

En effet, l'expérimentation française participera « *à l'étude d'un éventuel e-euro* » porté par l'Eurosystème (l'organe de l'Union européenne regroupant la BCE et les banques centrales nationales des Etats membres).

- **La Suède**

De son côté, la Banque centrale suédoise (Riksbank) a déjà lancé un projet pilote depuis le mois de février 2020 dont l'objectif est de « *montrer comment une e-couronne pourrait être utilisée par le grand public* ».

La Banque centrale de Suède a déclaré le 19 février 2020 qu'elle avait commencé à tester une MDBC.

La Suède veut se servir de cette MDBC pour simuler les activités bancaires quotidiennes comme les paiements, les dépôts et les retraits, à partir d'un portefeuille numérique.

La Suède part du constat que l'utilisation des espèces est en très forte diminution.

En 2018, les billets de banque ne représentaient que 1 % du PIB suédois, selon les données de la Riksbank, contre 11 % dans la zone euro, 8 % aux États-Unis et 4 % en Grande-Bretagne.

Pour le moment il ne s'agit que d'un test.

La Riskbank n'a pas encore pris sa décision finale sur l'émission de cette monnaie électronique.

Le test se terminera en 2021.

- **Mastercard**

Le spécialiste des paiements Mastercard veut aider les banques centrales à s'emparer des enjeux liés aux MDBC, et lance un environnement pour simuler l'émission, la distribution et l'échange de ces monnaies.

Mastercard a annoncé le 9 septembre 2020 le **lancement d'une plateforme permettant de tester les MDBC** (CBDC pour Central Bank Digital Currencies).

Cet environnement de test virtuel, exclusivement dédié aux banques centrales, permettra de simuler l'émission, la distribution et l'échange de ces monnaies entre les banques, les prestataires de services financiers et les utilisateurs.

Concrètement, cette plateforme permettra aux différents partenaires de tester un écosystème dédié, d'implémenter ces monnaies dans les réseaux et infrastructures de paiement existants, comme par exemple des cartes de paiement, de tester en temps réel ces modes de paiement « *partout où Mastercard est acceptée dans le monde* », ou encore de comparer différentes technologies afin de déterminer plus rapidement la valeur et la faisabilité sur un marché.

- **BCE**

Le 2 octobre 2020, la BCE publie un **rapport détaillé** concernant l'émission éventuelle d'un euro numérique, établi par le groupe de travail de haut niveau de l'Eurosystème sur la monnaie digitale de banque centrale et approuvé par le Conseil des gouverneurs.
Ce rapport examine, du point de vue de l'Eurosystème, l'opportunité de créer une monnaie digitale de banque centrale « Euro numérique ».

Christine Lagarde, présidente de la BCE, a déclaré : « *L'euro appartient aux Européens et notre mission est d'en être le gardien. Les Européens se tournent de plus en plus vers le numérique dans leurs modes de consommation, d'épargne et d'investissement. Notre rôle consiste à préserver la confiance dans la monnaie. Cela suppose de veiller à ce que l'euro soit adapté à l'ère numérique. Nous devons nous tenir prêts à émettre un euro numérique si cela s'avère nécessaire.* »

Le groupe de travail de l'Eurosystème, qui rassemble des experts de la BCE et des 19 banques centrales nationales de la zone euro, a identifié plusieurs scénarii dans lesquels l'émission d'un euro numérique s'imposerait.

Les scenarii comprennent les situations suivantes : hausse de la demande de paiements électroniques dans la zone euro rendant nécessaire un moyen de paiement numérique sans risque à l'échelle européenne ; forte diminution du recours aux espèces dans la zone euro ; lancement, à l'échelle internationale, de moyens de paiement privés qui soulèveraient des questions prudentielles et menaceraient la stabilité financière et la protection des consommateurs ; large utilisation de la monnaie numérique émise par des banques centrales extérieures à la zone euro.

L'Eurosystème consulte largement les citoyens, le monde universitaire, le secteur financier et les autorités publiques afin d'évaluer minutieusement leurs besoins, leurs attentes et leurs craintes concernant l'émission d'un euro numérique.

Une consultation publique s'est ouverte le 12 octobre 2020.

L'Eurosystème doit apporter des réponses à plusieurs considérations juridiques importantes liées à un euro numérique, notamment quant à la base juridique d'une éventuelle émission, aux implications juridiques des différentes conceptions possibles, ou encore à l'applicabilité de la législation de l'UE à l'Eurosystème en sa qualité d'émetteur, outre le sujet de la collecte massive d'informations (permettant notamment le contrôle de la sortie des capitaux) et de la protection des données personnelles eu égard à la traçabilité de la monnaie numérique .

En effet, les choix concrets de conception de l'euro numérique détermineraient la base juridique de son émission.

De plus, le droit primaire de l'UE n'interdit pas l'émission d'un euro numérique ayant cours légal (autrement dit, que tout bénéficiaire de paiement serait tenu d'accepter).

Certaines dispositions pratiques concernant la distribution de l'euro numérique et l'accès à ce dernier pourraient, en principe, être externalisées, en restant toutefois soumises à une surveillance stricte par l'Eurosystème.

L'Eurosystème devrait décider, vers la mi-2021, s'il y a lieu de lancer ou non un projet d'euro numérique, qui commencerait par une phase d'étude.

Enfin, un **euro numérique** conserverait les avantages que l'euro apporte à chacun d'entre nous, mais il permettrait également de faire face à une éventuelle désaffection des Européens pour les espèces.

Il contribuerait en outre à atténuer les répercussions d'événements extrêmes (catastrophe naturelle, pandémie, etc.) susceptibles d'empêcher le bon fonctionnement des services de paiement traditionnels.

- **Pandémie Covid-19**

Alors que les paiements dématérialisés ont explosé avec la pandémie de Covid-19, **la BCE craint que cet engouement ne profite à des monnaies virtuelles privées ou à des devises étrangères**.

Le principal risque est la fuite des épargnants vers ces monnaies virtuelles privées, qui permet d'éviter les frais d'un compte de dépôt classique, ce qui fragiliserait les banques de la zone euro.

Le cours du bitcoin, lequel a battu record un record fin 2020 (à près de 30.000 USD), illustre ce mouvement.

Un risque d'autant plus important "en période de crise", où les épargnants, défiants vis-à-vis du système bancaire, pourraient convertir leurs comptes courants.

La BCE veut donc accompagner l'explosion des paiements dématérialisés.

Cet euro numérique serait également un nouveau canal pour les politiques monétaires de la banque centrale qui disposerait d'un accès direct aux citoyens et pourrait donc, notamment en fixant un taux de rémunération, « *stimuler directement la consommation des ménages ou les investissements des entreprises* », écrit la BCE.

A rapprocher : La Banque populaire de Chine dévoile sa monnaie numérique souveraine (Siècle Digital, 9 juil. 2020) ; La banque centrale suédoise est la première à tester une monnaie numérique (Siècle Digital, 21 fév. 2020) ; Le yuan virtuel, nouvelle incarnation de la surveillance chinoise (Korii, 4 juin 2020) ; La Chine teste sa monnaie numérique dans quatre villes (Les Echos, 8 sept. 2020) ; Mastercard lance une plateforme pour tester les monnaies numériques des banques centrales (L'Usine Digitale, 14 sept. 2020) ; La Banque centrale européenne n'est pas encore prête à lancer sa propre monnaie numérique (L'Usine Digitale, 11 mai 2020) ; La Banque de France veut lancer une cryptomonnaie dès 2020 (L'Usine Digitale, 5 décembre 2019) ; Des euros numériques ? L'idée d'une monnaie électronique émise par la Banque centrale, boostée par la pandémie (La Tribune, 12 oct. 2020)

STARTUP & LEGALTECHS / TENDANCES

ESport : enjeux juridiques d'un secteur qui ne connait pas la crise

Actualités

Ce qu'il faut retenir :

Les mesures de confinement ont favorisé l'expansion d'un secteur déjà en plein développement : l'eSport. En France, l'eSport est encadré par la loi pour une République Numérique de 2016 et ses décrets d'application. En réalité, les problématiques juridiques soulevées par l'eSport sont nombreuses : droit social, propriété intellectuelle, droit fiscal, etc.

Pour approfondir :

Alors que de nombreux secteurs d'activité ont subi des pertes importantes avec la crise sanitaire mondiale de la Covid-19, l'eSport lui, ne s'est jamais aussi bien porté et a au contraire profité de cette crise pour se développer un peu plus.

Pour rappel, l'eSport désigne les compétitions de jeux vidéo en réseau local ou sur internet sur console ou sur ordinateur (1). En principe, tous les jeux vidéo qui intègrent un mode multijoueur font partie du eSport, néanmoins en pratique dans les grandes compétitions on retrouve quasiment toujours les mêmes jeux, parmi lesquels :

- StarCraft 2 ;
- Call Of Duty ;
- FIFA ;
- ShootMania Storm ;
- Dota 2 ;
- League of Legends.

Classiquement, on estime que l'eSport serait né à la fin des années 1990 avec la première compétition du jeu de shoot Quake. Mais il s'est particulièrement développé dans les années 2000 avec une professionnalisation du sport et des dotations de compétitions (ou cash prize) qui atteignent à présent plusieurs millions de dollars, notamment grâce aux sponsors et aux montants d'inscription à ces tournois. L'eSport a pris une telle ampleur qu'une discussion est actuellement en cours avec le CIO afin de l'intégrer aux jeux olympiques (2).

La France compte de nombreux pro gamers de talent et plusieurs équipes de eSport reconnues, parmi lesquelles la team Vitality.

Pourtant, il aura fallu attendre le 7 octobre 2016, et la loi pour une République Numérique (3) pour qu'un cadre juridique dédié au eSport voit le jour en France.

Auparavant, sous l'empire de la loi du 17 mars 2014 (4), on assimilait l'eSport à la loterie publicitaire. Le problème est que la comparaison entre l'eSport et les jeux de hasard n'est pas adaptée car même si une part de hasard existe dans les jeux vidéo, comme d'ailleurs dans le sport classique, l'espérance de gain, contrairement aux jeux de hasard, est directement liée aux compétences des participants (des gamers). L'eSport méritait donc un cadre à part entière.

La loi pour une République Numérique est donc venue notamment définir le statut de joueur professionnel salarié et a inséré un nouveau chapitre « compétition de jeux vidéo » dans le Code de la sécurité intérieure.

Cette loi a été complétée par deux décrets en 2017 :

- Le décret n°2017-871 du 9 mai 2017 relatif à l'organisation des compétitions de jeux vidéo qui précise notamment les conditions relatives à l'organisation des compétitions de jeux vidéo, les conditions quant à la participation des joueurs mineurs et prévoit certaines sanctions.
- Le décret n°2017-872 du 9 mai 2017 relatif au statut des joueurs professionnels de jeux vidéo compétitifs qui définit notamment les conditions nécessaires pour employer des joueurs professionnels.

L'ensemble de ces normes forme le cadre juridique français applicable à l'heure actuelle au eSport.

En réalité, l'eSport soulève des problématiques juridiques à la croisée de plusieurs domaines classiques du droit et notamment :

- En droit social pour les contrats conclus entre les équipes et les pro gamers ;
- En droit de la propriété intellectuelle pour streamers par exemple ou encore pour les éditeurs des jeux vidéo objets de la compétition de eSport ;
- En droit fiscal pour les revenus des joueurs professionnels.

Or, c'est un secteur d'activité où la moyenne d'âge est particulièrement basse. Une majorité de pro gamers n'a en effet pas encore 30 ans et de nombreux gamers ou streamers ne sont même pas majeurs. Ces préoccupations sont donc parfois difficiles à appréhender.

Pourtant, comme nous l'a montré la crise de la Covid-19, c'est un secteur qui n'est pas appelé à disparaître, bien au contraire.

Par exemple, au mois de mars 2020, la plateforme Twitch, plateforme majeure pour la retransmission du eSport, a enregistré une hausse de 60% du nombre de vues par rapport à mars 2019 (5). Cette hausse est évidemment concomitante aux mesures de confinement et à l'annulation de la plupart des événements de sport classique mais ce chiffre ne fait que confirmer un constat : l'eSport ne cesse de prendre de l'ampleur.

A rapprocher :

1. **Jeux vidéo et eSport, site internet de Futura Sciences**
2. **ESport et CIO, une relation qui va au-delà des discussions sur les JO, site internet L'Equipe**
3. **LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique, Légifrance**
4. **LOI n° 2014-344 du 17 mars 2014 relative à la consommation, Légifrance**
5. **COVID-19 : l'eSport profite de la pandémie pour se développer, site internet Clubic**

***

ACTUALITÉ NUMÉRIQUE SIMON ASSOCIÉS

BONNE ANNÉE 2021 !

Simon Associés vous présente ses meilleurs vœux pour cette nouvelle année !

Cliquez ici

CYBERATTAQUE ET VIOLATION DE DONNEES PERSONNELLES

Vidéos « Réflexions d'Experts », par Amira BOUNEDJOUM

Episode 1 - Cyberattaque et violation de données personnelles : ces deux notions font-elles référence à la même chose ?

Episode 2 - Y a-t-il un type d'attaque informatique ou un mode opératoire particulier dans le contexte actuel ?

Episode 3 - Comment réagir aux attaques actuelles ?

LA PROTECTION DES DONNÉES PERSONNELLES

Vidéo « Réflexions d'Experts », par Thomas NOËL