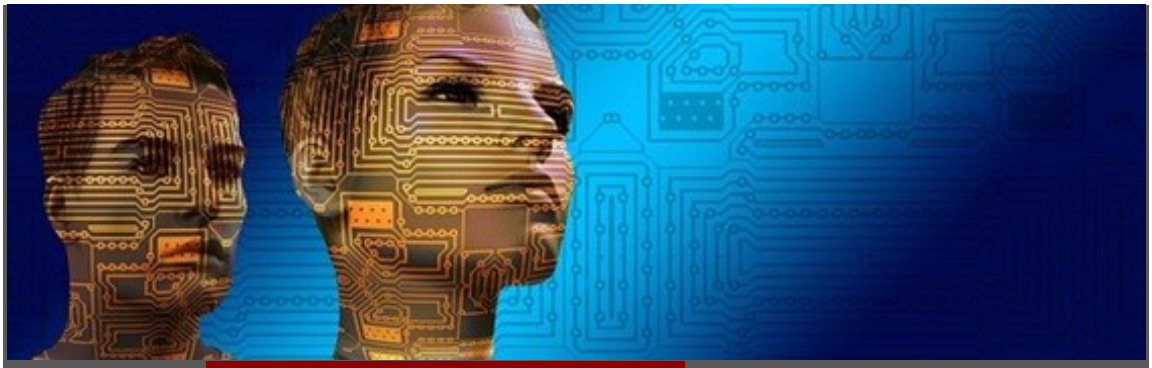
La Newsletter dédiée au Droit du Numérique

par @DerriennicParis

DERRIENNIC ASSOCIÉS

NEWSLETTER NTIC N°34

#NewsDerriennicNTIC



LES MATINALES DE DERRIENNIC - SAVE THE DATE

14/01/2021 : Digital Services Act avec la participation exceptionnelle de Madame la députée Valéria Faure-Muntian

webinar ou présentiel (au cabinet @DerriennicParis - 5 avenue de l'opéra 75001 Paris)

François-Pierre Lani et Camille Rod, avocats, animeront cette Matinale.

INTELIGENCE ARTIFICIELLE

Intelligence artificielle et réglementation européenne : un pas de plus

- *Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission concernant un cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes (2020/2012(INL))*
- *Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission sur un régime de responsabilité civile pour l'intelligence artificielle (2020/2014(INL))*
- *Résolution du Parlement européen du 20 octobre 2020 sur les droits de propriété intellectuelle pour le développement des technologies liées à l'intelligence artificielle (2020/2015(INI))*

Le chantier juridique de l'Intelligence Artificielle (« IA ») a récemment progressé avec, en particulier, l'adoption de trois résolutions par le Parlement européen le 20 octobre dernier.

Les députés européens ont ainsi posé des principes et formulé des propositions de règlementations ou d'actions relativement à trois problématiques majeures : « Un cadre pour les aspects éthiques », « Un régime de responsabilité civile » et « Les droits de propriété intellectuelle ».

L'objectif est de « *réglementer au mieux l'intelligence artificielle afin de stimuler l'innovation et la confiance dans la technologie* ».

Quelques illustrations s'imposent.

- **« Un cadre pour les aspects éthiques »**

Cette résolution présente des principes directeurs (principes éthiques et obligations juridiques) pour le développement, le déploiement et l'utilisation de l'IA.

A titre d'exemples :

- une IA centrée sur l'humain et développée par l'homme ;
- la sécurité, la transparence et la responsabilité ;
- des garanties contre les préjugés et la discrimination ;
- le droit de recours ;
- la responsabilité sociale et environnementale ;
- le respect des droits fondamentaux dont la vie privée et la protection des données.

Il y est également précisé que les IA dites à « à haut risque » dont les IA avec « capacités d'auto-apprentissage » doivent être conçues de manière à permettre un contrôle humain à tout moment.

- **« Un régime de responsabilité civile »**

Dans cette résolution, les députés européens ont considéré qu'il est nécessaire de réviser complètement les régimes de responsabilité.

Pour l'IA à haut risque, un « régime commun de responsabilité objective » est requis.

Les règles devraient s'appliquer, en particulier, aux atteintes à la vie, à la santé, à l'intégrité physique, à la propriété.

- « Les droits de propriété intellectuelle»

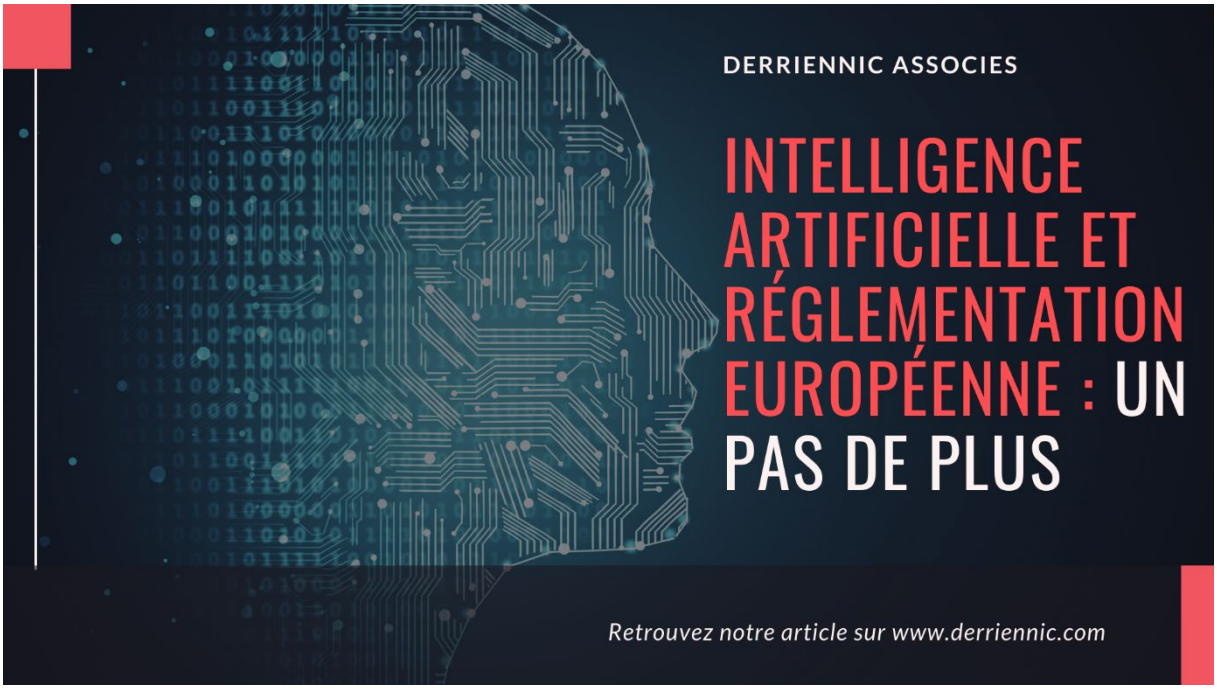
« *Une analyse d'impact* » est demandée sur le sujet en particulier au regard du régime actuel (des droits de propriété intellectuelle, y compris celui du secret industriel et commercial).

Aussi, le Parlement européen considère qu'il est essentiel de distinguer entre « *les créations humaines assistées par l'IA et les créations autonomes de l'IA* ».

Sa position est de ne pas « *doter les technologies de l'IA de la personnalité juridique* » ; en d'autres termes : seuls des êtres humains pourraient détenir des droits de propriété intellectuelle sur l'IA.

Ces tendances sont riches d'enseignements quant au cadre légal à venir autour de l'IA.

Comme vous le savez, Derriennic Associés travaille depuis plusieurs années sur l'IA et tout particulièrement sur la contractualisation de l'IA en partenariat avec l'AFNOR et de nombreuses entreprises. De nouvelles règles relatives à la contractualisation de l'IA vont bientôt être publiées par l'AFNOR. Nous ne manquerons pas d'en faire une synthèse. Les sujets de la responsabilité, de la propriété intellectuelle mais également de l'éthique y seront traités. A suivre.



INTERNET

La Cour de cassation apporte des précisions sur les conditions de la diffamation commise via un lien hypertexte

A l'occasion de deux arrêts rendus le 1er septembre 2020 (n°19-82.055 et n°19-84.505), la Cour de Cassation a pris soin de rappeler comment les juges du fond doivent articuler la jurisprudence de la Cour Européenne de Sauvegarde des Droits de l'Homme, fondée sur l'article 10 de la Convention EDH avec sa propre jurisprudence en matière de diffamation publique envers un particulier et de liens hypertextes.

La première espèce (n°19-82.055) : l'hyperlien des Inrocks

Au printemps 2013, le site des Inrocks publiait un article relatif à l'affaire dite « des financements libyens de la campagne présidentielle ». Au sein de cette publication figurait un hyperlien renvoyant vers un article contemporain du Monde apportant des précisions sur la nature du financement évoqué par l'article des Inrocks. Une plainte pour diffamation fut déposée à l'encontre du journal.

En 1ère instance, les juges déclarèrent l'action irrecevable. En appel, le jugement fut confirmé. La cour d'Appel retenant que si un lien hypertexte peut caractériser un élément extrinsèque d'indentification en ce qu'il peut permettre l'identification de la personne visée, il convient de prendre en compte le contexte dans lequel il est publié.

La Cour de Cassation appuya l'appréciation des juges du second degré en soulignant que d'une part le lectorat des Inrocks devait être pris en compte et d'autre part, que la présence d'une multitude d'autres liens ne pouvait permettre une identification certaine de la personne prétendument diffamée.

Le second arrêt (n°19-84.505) : la publication d'une députée sur Facebook

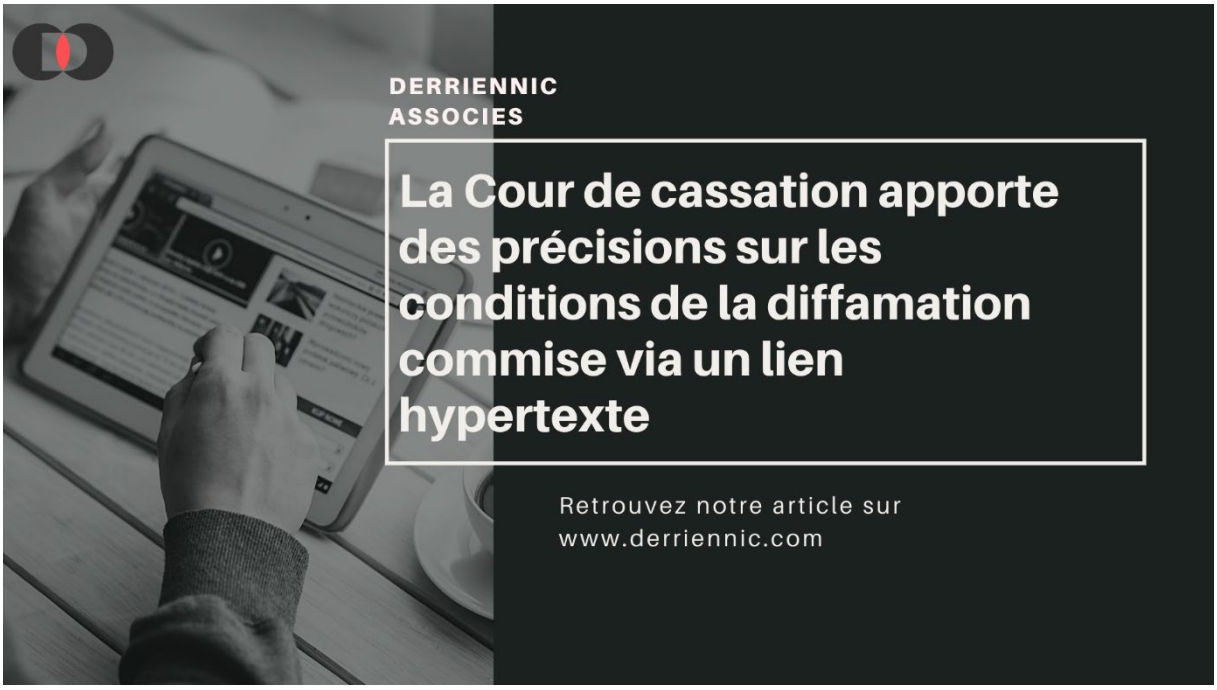
En 2017, une élue locale avait, inséré un lien hypertexte dans sa publication commentant la gestion par l'organisation Alternative libertaire d'un de ses membres soupçonné d'avoir commis un viol. Le suspect présumé s'estimant diffamé par les propos de la rédactrice porté plainte à son encontre.

L'action fut déclarée irrecevable en première instance par le tribunal correctionnel de Paris. En appel, les juges accueillirent l'action. La Cour de Cassation devait alors trancher.

C'est en visant la jurisprudence de la Cour Européenne de Sauvegarde des Droits de l'Homme ainsi que la sienne qu'elle retint :

- Que le recours à un lien hypertexte renvoyant vers un contenu diffamatoire fait courir un nouveau délai de prescription,
- Que l'appréciation de la réunion des éléments constitutifs du délit de diffamation publique impose d'une la prise en compte des modalités et du contexte dans lequel le lien est inséré, d'autre part la teneur du texte dans lequel est incrusté le lien.

En l'espèce, les propos de la prévenue prenaient le parfait contrepied de ceux vers lesquels son lien renvoyait. De telle sorte que l'infraction ne pouvait être constituée.



Quand le législateur met les influenceurs mineurs à l'abri du coup de grisou (numérique)

Le 20 novembre 2019, la Convention Internationale des Droits de l'Enfant fêtait ses 20 ans. Anticipant cet anniversaire, dès le 10 juillet, la France adoptait la loi relative à l'interdiction des violences éducatives ordinaires, passée à la postérité affublée du sobriquet de « loi anti-fessée ».

C'est donc dans ce mouvement législatif tendant au « renforcement de la politique de sensibilisation, de soutien, d'accompagnement et de formation à la parentalité à destination des futurs parents » que s'est insérée la loi du 19 Octobre 2020.

Désireuse d'encadrer l'exploitation commerciale de l'image de mineurs de 16 ans sur les plateformes en ligne, cette loi aspire à protéger explicitement les « *enfants influenceurs* ». Pour ce faire, elle :

- S'intéresse, d'une part, à l'applicabilité de la qualification de travail à l'activité de l'enfant,
- D'autre part, elle responsabilise les parties destinées à tirer profit des mineurs que sont leurs parents et les plateformes.
- En outre, elle place dans les mains expertes du Conseil supérieur de l'audiovisuel (CSA), le contrôle du respect de l'esprit du texte. Pour ce faire, il est habilité à saisir le juge des référés.
- Enfin, l'exercice direct par les mineurs du droit à l'oubli est facilité.

L'incidence de la qualification de travail sur l'encadrement de l'activité de l'enfant

Le mineur exerce une activité telle qu'elle s'assimile à un travail

Dans ce cas, il a paru opportun au Législateur d'établir une filiation avec le régime applicable aux enfants mannequins, du spectacle et de la publicité.

En amont de toute préparation de contenu vidéo, les parents ou titulaires de l'autorité parentale devront solliciter une autorisation individuelle ou un agrément auprès de l'administration. Un rappel de leurs obligations financières (consignation d'une partie des revenus de l'enfant et du pécule à la Caisse des dépôts jusqu'à la majorité ou l'émancipation) et des conséquences de la surexposition d'un enfant sur internet.

Le mineur exerce une activité ne pouvant parfaitement s'assimiler à un travail

Il incombe aux parents d'effectuer une déclaration, au-delà de certains seuils de durée ou de nombre de vidéos ou de revenus tirés de leur diffusion, amenés à être précisés par décret. Là aussi les obligations financières s'appliquent.

Le défaut d'autorisation, d'agrément ou de déclarations des parents ouvrira à l'administration le droit de saisir le juge des référés.

Les articles L. 7124-1, L. 7124-4, en plus de l'insertion d'un article L. 7124-4-1, art. L. 7124-5, art. L. 7124-9 du Code Travail sont modifiés.

La responsabilisation des plateformes de partage de vidéos

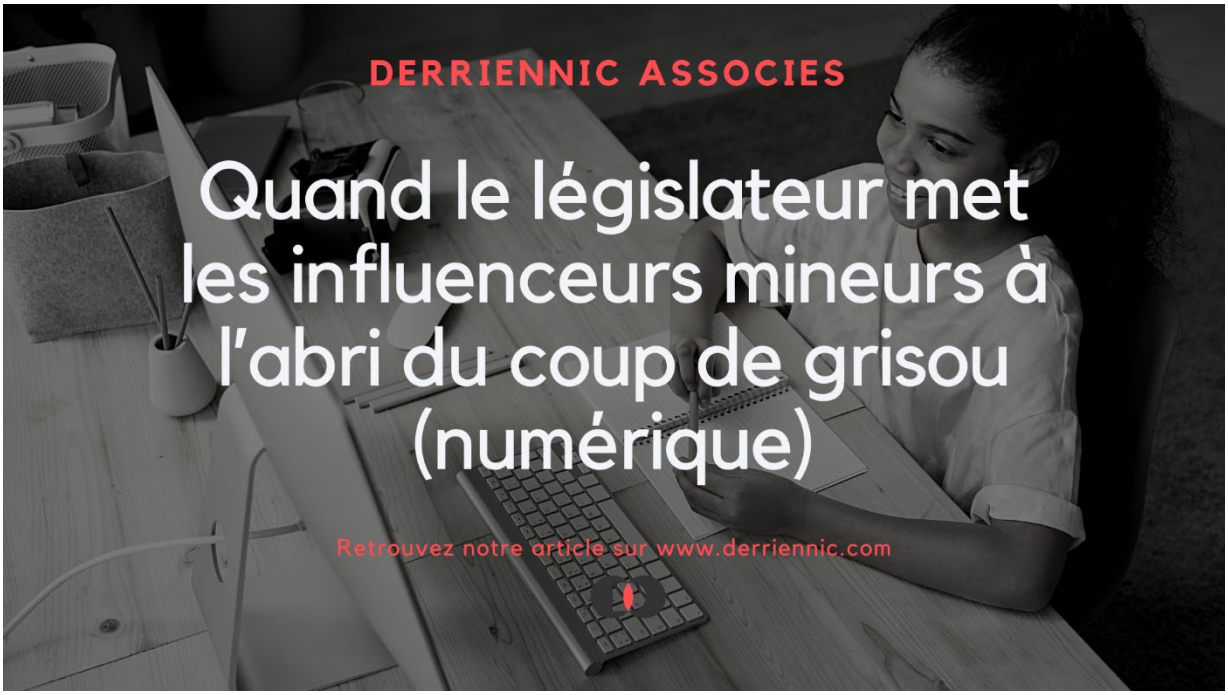
Ce sont les grands acteurs du numérique plébiscités par les mineurs de 16 ans (Snapchat, YouTube et autres TikTok…) qui sont placés dans le viseur du CSA. On rappellera à cette occasion que l'usage des réseaux sociaux est interdit aux mineurs de 13 ans.

Les articles 2 et 4 incitent les plateformes à adopter des chartes afin de favoriser l'information et la sensibilisation des mineurs sur les conséquences de la diffusion de leur image, de leur vie privée ainsi que des conséquences juridiques et psychologiques afférentes à leurs activités. Le censeur du milieu audiovisuel devant notamment « *promouvoir* » la signature de ces chartes (article 5)

L'exercice facilité du droit à l'oubli par les mineurs

« *Le consentement des titulaires de l'autorité parentale n'est pas requis pour la mise en œuvre, par une personne mineure* ». Le texte n'aurait pu être plus clair. Il souhaite permettre l'exercice par les mineurs de leur droit à l'oubli, tel que consacré par la loi du 6 janvier 1978 et le RGPD, sans qu'aucune entrave, même parentale, ne puisse s'opposer à leur désir de suppression des contenus mis en ligne.

La loi fait l'objet d'une entrée en vigueur différée et prévue au mois avril 2021.



PROPRIETE INTELLECTUELLE

L'appréciation de la notion de consentement de l'artiste-interprète à l'exploitation de sa performance face au régime dérogatoire au bénéfice de l'INA

Cour de cassation, 1ère chambre civile, 22 janvier 2020, n°17-18.177

Le régime dérogatoire au principe d'autorisation préalable des artistes-interprètes accordé au bénéfice de l'INA est une présomption simple d'autorisation, laquelle ne supprime pas l'exigence de ce consentement et ne remet pas en cause le droit exclusif de l'artiste-interprète d'autoriser ou d'interdire la reproduction de sa prestation ainsi que sa communication et sa mise à la disposition du public.

La Cour de cassation est ici saisie suite à une procédure fleuve, après deux arrêts de Cours d'appel, trois arrêts rendus par la Cour de Cassation et une décision de la Cour de Justice de l'Union Européenne saisie sur question préjudicielle.

L'affaire porte sur la contestation par les ayants droit d'un jazzman de l'exploitation commerciale par l'Institut national de l'audiovisuel (ou « INA ») sur son site Internet des prestations du musicien, sans son autorisation et ce, en violation des dispositions de l'article L. 212-3 du Code de la propriété intellectuelle et du sacro-saint principe d'autorisation écrite préalable de l'artiste-interprète avant toute fixation, reproduction et communication au public de sa performance.

La question posée à la Haute juridiction était de savoir comment concilier ce principe avec le régime dérogatoire au bénéfice de l'INA et la présomption de consentement de l'artiste-interprète institués par la loi Léotard n°86-1067 du 30 septembre 1986 au titre de l'exploitation des prestations des artistes-interprètes constituant son fonds et ce, à l'aune des dispositions européennes de la Directive 2001/29/CE du 22 mai 2001 sur le droit d'auteur et les droits voisins.

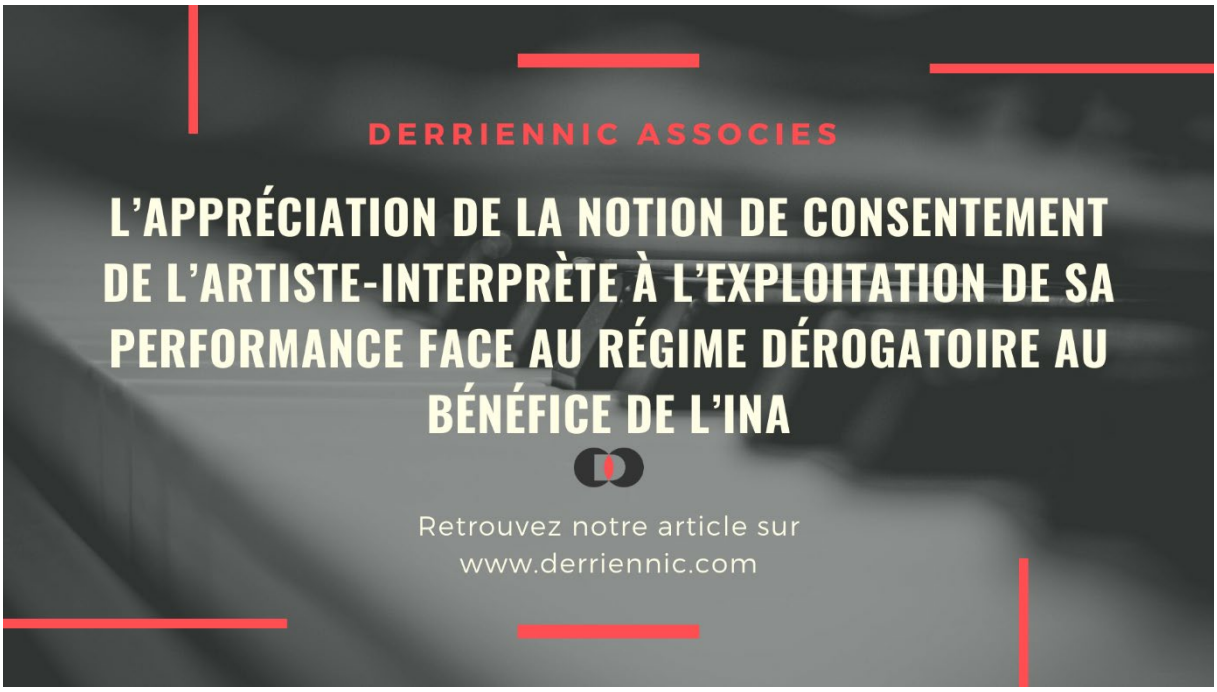
La Cour de cassation suit le raisonnement de la CJUE, selon laquelle les dispositions de « *la directive 2001/29 doivent être interprétés en ce sens qu'*[elles] *ne s'opposent pas à une législation nationale qui établit, en matière d'exploitation d'archives audiovisuelles par une institution désignée à cette fin, une présomption réfragable d'autorisation de l'artiste-interprète à la fixation et à l'exploitation de sa prestation, lorsque cet artiste-interprète participe à l'enregistrement d'une œuvre audiovisuelle aux fins de sa radiodiffusion* » (CJUE, 14 novembre 2019 aff. C-484/18).

La Cour de cassation relève que l'INA a une mission particulière de conservation, de valorisation et d'exploitation du patrimoine audiovisuel national, comprenant les archives audiovisuelles des sociétés nationales de programme.

La Cour relève, en outre, que le jazzman avait « *participé à la réalisation de ces œuvres aux fins de leur radiodiffusion par des sociétés nationales de programme et qu'il avait, d'une part, connaissance de l'utilisation envisagée de sa prestation, d'autre part, effectué sa prestation aux fins d'une telle utilisation* » et que « *c'est à bon droit que la cour d'appel (…) a énoncé qu'en*

exonérant l'INA de prouver par un écrit l'autorisation donnée par l'artiste-interprète, l'article 49, II, de la loi du 30 septembre 1986 modifiée, ne supprime pas l'exigence de ce consentement mais instaure une présomption simple d'autorisation qui peut être combattue et ne remet pas en cause le droit exclusif de l'artiste-interprète d'autoriser ou d'interdire la reproduction de sa prestation ainsi que sa communication et sa mise à la disposition du public ».

La Haute juridiction rejette en conséquence le pourvoi.



CYBERCRIMINALITE

Refuser de donner son code de déverrouillage de téléphone à un fonctionnaire de police lors d'une garde à vue peut être constitutif d'une infraction pénale autonome

Cass. crim., 13 oct. 2020, n° 20-80.150.

Résumé : Le refus de remettre le code de déverrouillage d'un téléphone portable peut être constitutif du délit de refus de remettre une convention secrète de déchiffrement d'un moyen de cryptologie à une autorité judiciaire prévu à l'article 434-15-2 du Code pénal lorsque (i) le téléphone est équipé d'un moyen de cryptologie et que (ii) ce refus fait suite à la réquisition d'un officier de police judiciaire.

Un homme est placé en garde à vue dans le cadre d'une enquête de flagrance pour des infractions présumées liées au trafic de stupéfiants. Lors des interrogatoires diligentés, les officiers de police judiciaire lui enjoignent de leur communiquer les codes de déverrouillage des téléphones portables retrouvés en sa possession. Ce dernier refuse.

Il est cité à comparaitre devant le Tribunal correctionnel compétent qui le reconnait coupable de diverses infractions à la législation relative aux stupéfiants et du délit de refus de remise d'une convention de déchiffrement d'un moyen de cryptologie, prévu par l'article 434-15-2 du Code pénal.

Le prévenu interjette appel et la Cour d'appel de Paris (CA Paris, 16 avr. 2019, n° 18/09267) le relaxe considérant (i) que la demande faite par un fonctionnaire de police ne constituait pas une réquisition émanant d'une autorité judiciaire et que (ii) un code de déverrouillage d'un téléphone portable « d'usage courant » ne constitue pas un moyen de cryptologie car il ne permet pas de déchiffrer des données ou messages cryptés mais ouvre simplement l'accès aux données qui y sont contenues.

Le procureur général près la Cour de cassation forme un pourvoi dans le seul intérêt de la loi et, dans un arrêt du 13 octobre 2020, la Cour de cassation va casser et annuler l'arrêt d'appel.

La chambre criminelle considère d'abord que la condition préalable du délit, à savoir l'existence de réquisitions émanant de l'autorité judiciaire est acquise lorsque « *la réquisition est délivrée par un officier de police judiciaire agissant en vertu des articles 60-1, 77-1-1 et 99-3 du code de procédure pénale, dans leur rédaction applicable au litige, sous le contrôle de l'autorité judiciaire, entre dans les prévisions* » du délit. En d'autres termes, la Cour considère que, dans le cadre d'une enquête de flagrance, les réquisitions peuvent émaner de l'officier de police judiciaire, voire d'un l'agent de police judiciaire dans la mesure où ils sont placés sous le contrôle de l'autorité du Procureur de la République.

En l'espèce elle considère toutefois, que l'injonction des officiers de police était une « *simple demande formulée au cours d'une audition, sans avertissement que le refus d'y déférer est susceptible de constituer une infraction pénale* » qui n'était pas constitutive d'une réquisition. Elle rejette donc la première branche du pourvoi.

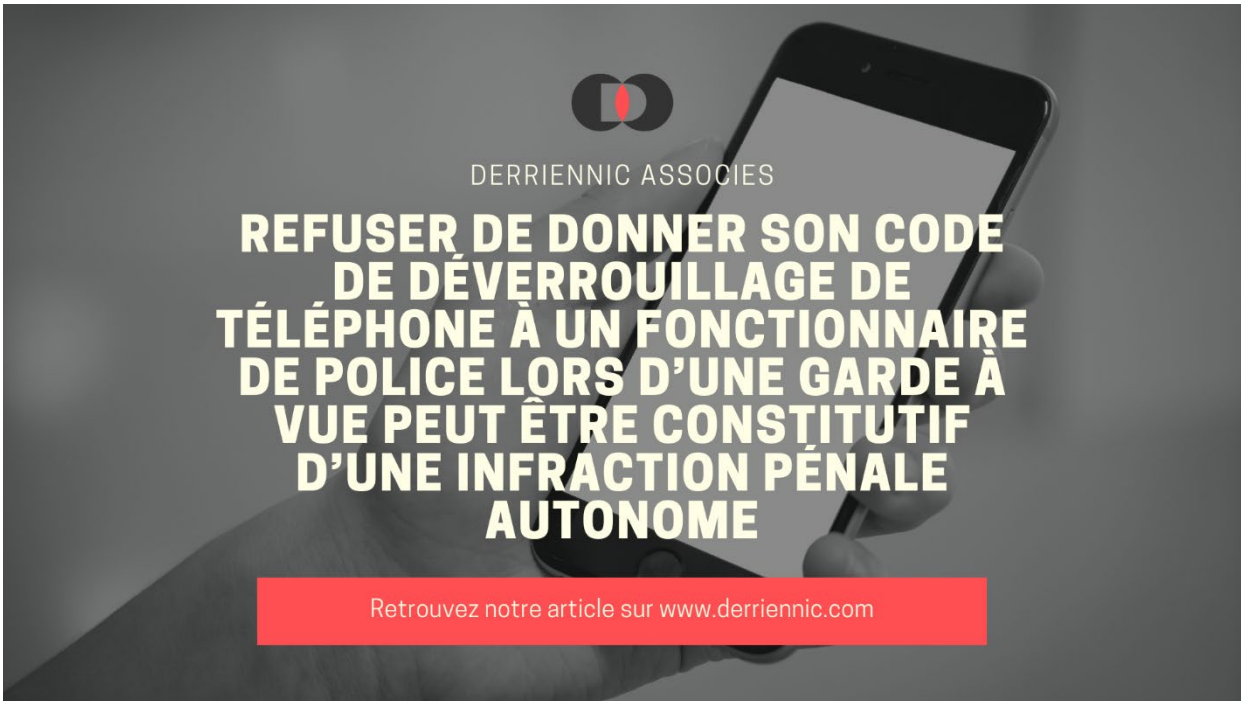
Sur la seconde branche du pourvoi, la chambre criminelle casse l'arrêt d'appel qui avait considéré qu'un code de déverrouillage d'un téléphone portable était « d'usage courant » et donc exclusif de toute qualification de convention secrète d'un moyen de cryptologie au titre de l'article 434-15-2 du code pénal. Celle-ci reproche à la Cour d'appel de s'être fondée sur « la notion inopérante de téléphone d'usage courant ».

La Haute juridiction rappelle la définition de la convention secrète d'un moyen de cryptologie tel que prévu par l'article 29 de la loi n° 2004-575 du 21 juin 2004 et précise que « *la convention secrète de déchiffrement d'un moyen de cryptologie contribue à la mise au clair des données qui ont été préalablement transformées, par tout matériel ou logiciel, dans le but de garantir la sécurité de leur stockage, et d'assurer ainsi notamment leur confidentialité* ».

Aussi, la chambre criminelle en déduit que le code de déverrouillage d'un téléphone portable peut constituer une telle convention lorsque ledit téléphone est équipé d'un moyen de cryptologie. La Cour d'appel a méconnu cette définition légale et son arrêt encoure la cassation.

L'application de la solution dégagée s'avérera certainement laborieuse pour les juges du fond dans la mesure où ils devront, au cas pas cas, déterminer si le téléphone portable dont le code de déverrouillage est demandé embarque ou non, un moyen cryptologie.

De manière plus générale, cette décision constitue un nouveau recul du droit de ne pas s'auto-incriminer au profit de la recherche de la vérité.



DONNEES PERSONNELLES

Conservation généralisée des données de connexion : la France doit revoir sa copie !

CJUE 6 octobre 2020 (affaires C-623/17, C-511/18, C-512/18, C-520/18)

Dans plusieurs arrêts rendus le 6 octobre dernier, la CJUE s'est prononcée sur la validité de règlementations nationales, dont celles de la France, imposant une obligation de conservation généralisée et indifférenciée des données de connexion (relatives au trafic et à la localisation) à des fins de sauvegarde de la sécurité nationale.

La Cour a tout d'abord jugé, par principe, que le droit de l'Union (en particulier la directive « vie privée et communication électroniques », la charte des droits fondamentaux et, dans une moindre mesure, le RGPD) s'oppose à une réglementation nationale imposant à un fournisseur de services de communications électroniques, à des fins de lutte contre les infractions en général ou de sauvegarde de la sécurité nationale, la transmission ou la conservation généralisée et indifférenciée de données de connexion.

Le droit de l'Union n'est donc pas compatible avec une règlementation telle que celle existant en France, imposant à un tel fournisseur, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation.

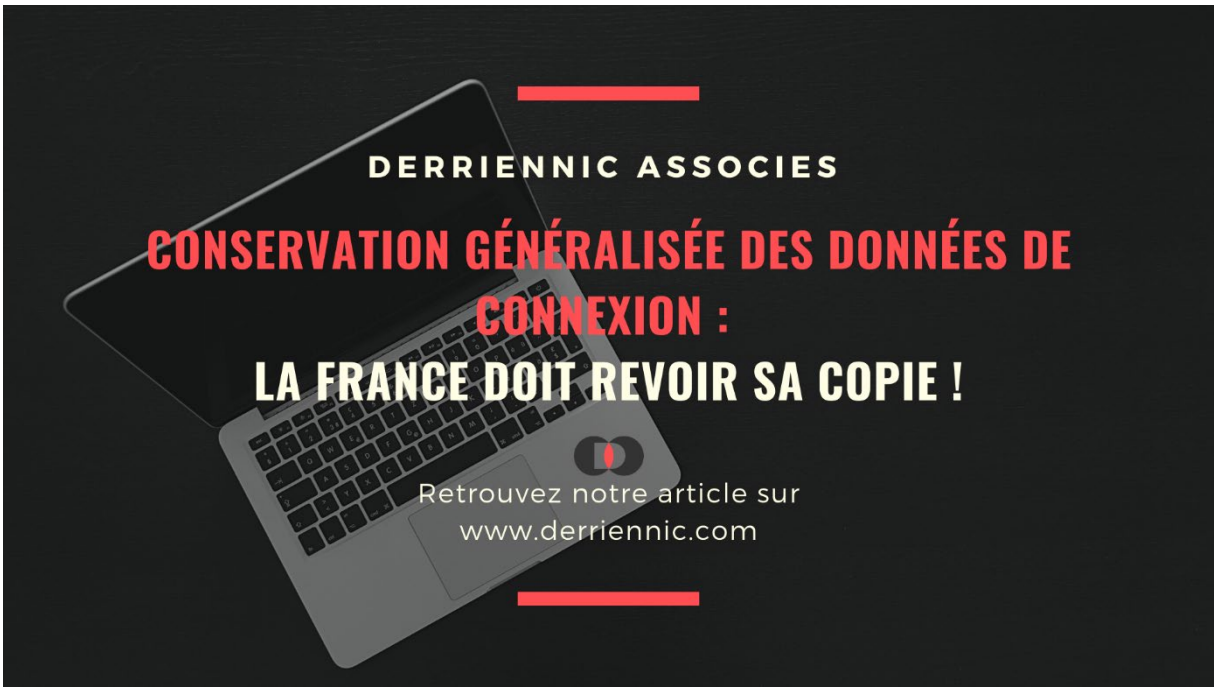
Ensuite, la Cour a admis certaines exceptions qu'elle définit et encadre de manière stricte :

- dans les situations de menace grave pour la sécurité nationale réelle et actuelle ou prévisible, un Etat membre peut prendre des mesures visant à enjoindre aux fournisseurs de services de communications électroniques une telle conservation généralisée et indifférenciée des données de connexion sous certaines réserves telles que : la soumission de la décision d'injonction à un contrôle effectif (par une juridiction ou une entité administrative indépendante) et à une période temporellement limitée au strict nécessaire ;
- dans ces mêmes conditions, une analyse automatisée des données des utilisateurs de moyens de communications électroniques est possible ;
- en outre, des mesures nationales peuvent permettre le recours à :
- une conservation ciblée, temporellement limitée au strict nécessaire, des données de connexion sous réserve qu'elle 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 ;
- une conservation rapide des données dont disposent les fournisseurs de services dans des situations où survient la nécessité d'une conservation de ces données au-delà des délais légaux de conservation aux fins de

l'élucidation d'infractions pénales graves ou d'atteintes à la sécurité nationale, lorsque ces infractions ou atteintes ont déjà été constatées ou lorsque leur existence peut être raisonnablement soupçonnée ;

- au recueil en temps réel, notamment des données de connexion, si cela est limité aux personnes pour lesquelles il existe une raison valable de soupçonner qu'elles sont impliquées dans des activités terroristes et sous réserve d'un contrôle préalable (par une juridiction ou par une entité administrative indépendante) pour s'assurer que cela n'est autorisé que dans la limite de ce qui est strictement nécessaire.

Ces décisions sont lourdes de conséquences : au-delà de la contrainte de revoir sa règlementation au regard de ces précisions, la France va devoir gérer le sort des actes et procédures réalisés et/ou en cours basés sur des règles contraires au droit de l'Union….



Le cabinet Derriennic et toute son équipe vous souhaitent de passer en famille de joyeuses fêtes de fin d'année.